From: "Matt O'Flynn" <matt@hbgary.com>
To: "'Rich Cummings'" <rich@hbgary.com>; "'Aaron Barr'" <aaron@hbgary.com>
Cc: "'Greg Hoglund'" <greg@hbgary.com>; "'Phil Wallisch'" <phil@hbgary.com>; "'Ted Vera'" <ted@hbgary.com>; "'Penny Leavy'" <penny@hbgary.com>; "'Bob Slapnik'" <bob@hbgary.com>; "'Maria Lucas'" <maria@hbgary.com>
Sent: Thursday, January 28, 2010 7:40 PM
Attach: Mandiant M Trends APT.pdf
Subject: RE: Mandiants M-trends release party for APT @6pm DC3

Attached is the report that they distributed to our potential customers last night...

Best,

Matt

-----Original Message-----
From: Rich Cummings [mailto:rich@hbgary.com]
Sent: Wednesday, January 27, 2010 11:02 AM
To: 'Aaron Barr'; 'Matt O'Flynn'
Cc: 'Greg Hoglund'; 'Phil Wallisch'; 'Ted Vera'
Subject: RE: Mandiants M-trends release party for APT @6pm DC3

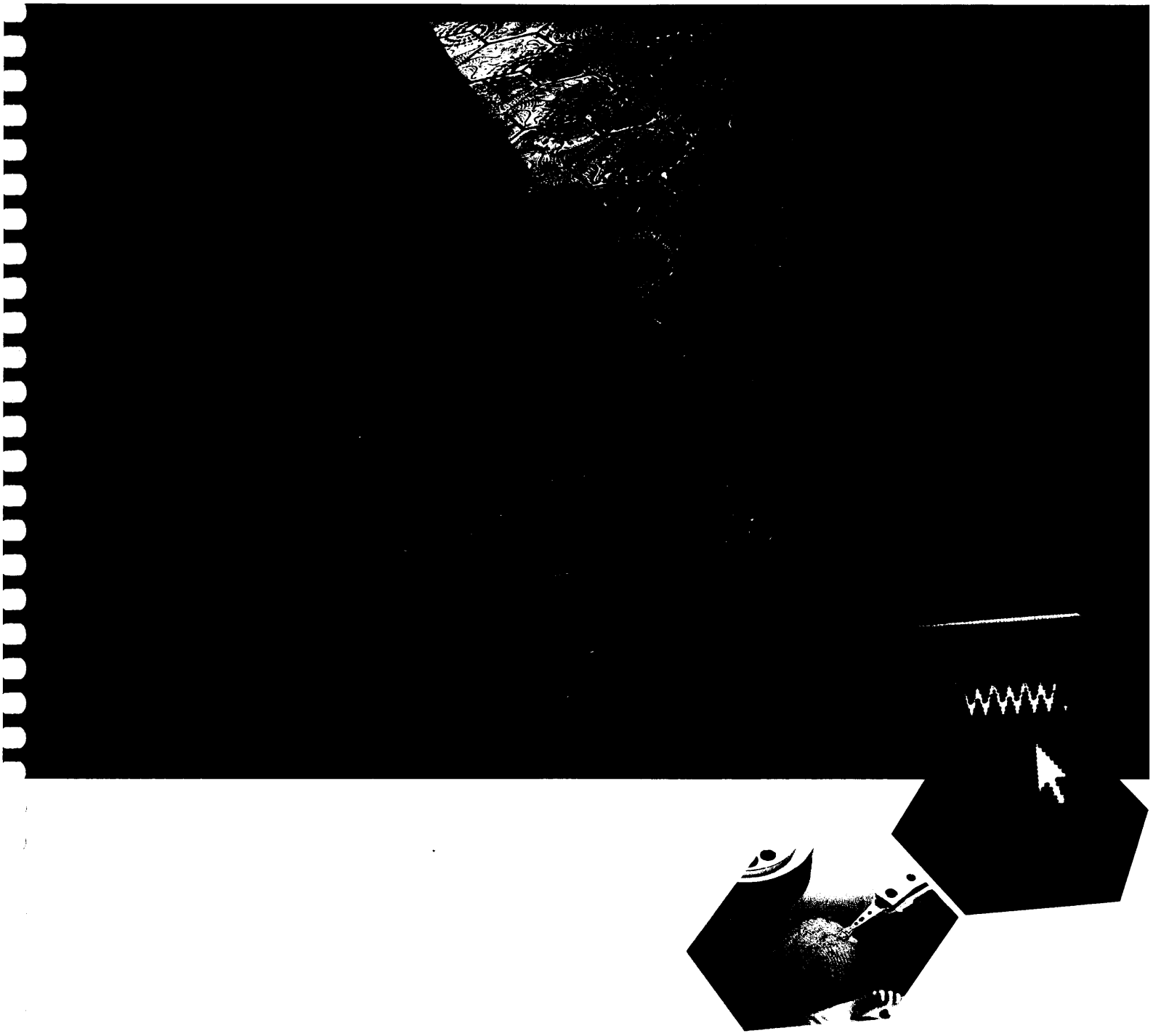
Matt and Phil are on it.

-----Original Message-----
From: Aaron Barr [mailto:aaron@hbgary.com]
Sent: Wednesday, January 27, 2010 10:54 AM
To: Matt O'Flynn
Cc: Greg Hoglund; Phil Wallisch; Ted Vera; Rich Cummings
Subject: Mandiants M-trends release party for APT @6pm DC3

Anyone working on getting any intel on this?

Aaron Barr
CEO
HBGary Federal Inc.

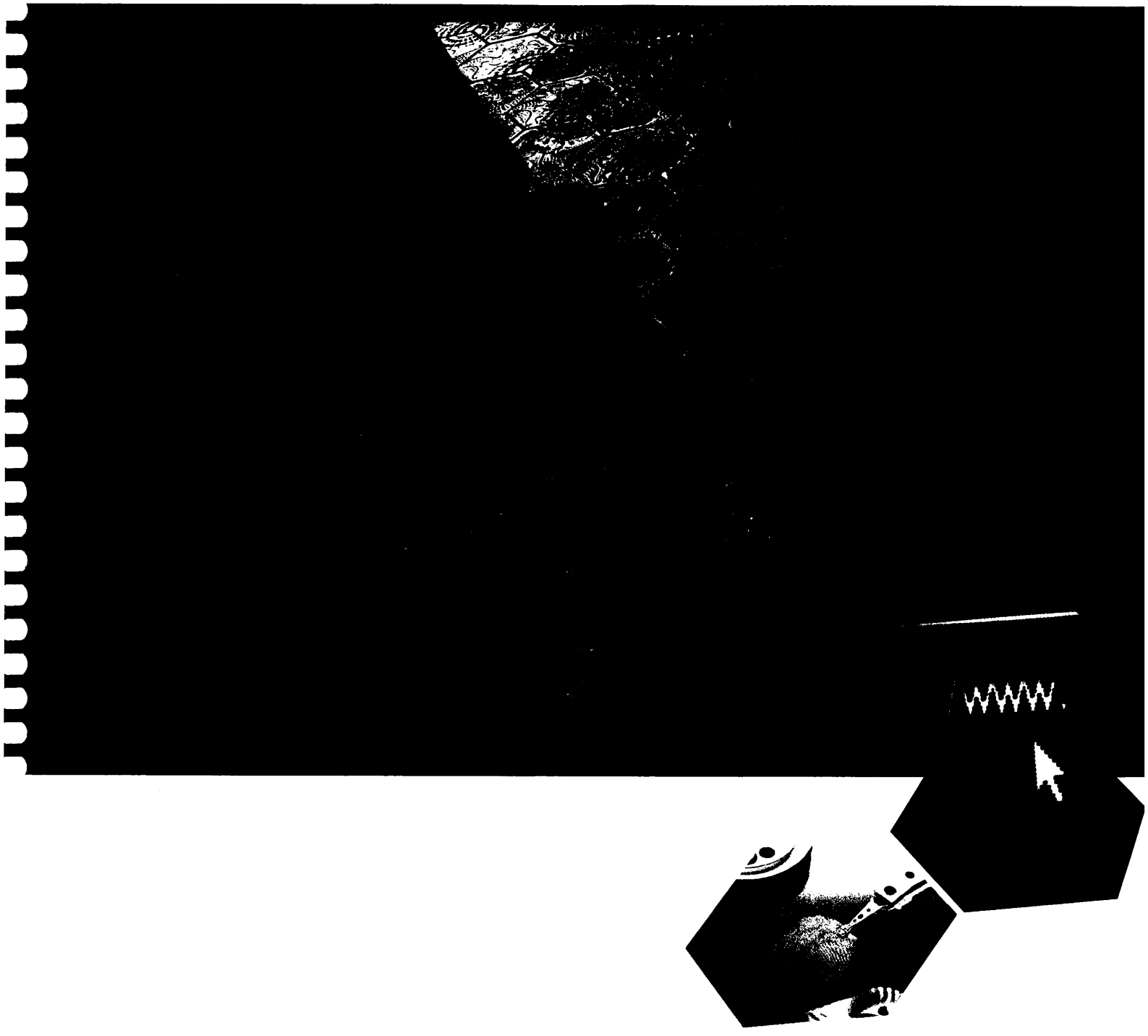
MANDIANT®



M Trends

the advanced persistent threat

MANDIANT®



M Trends

the advanced persistent threat

CONTENTS

WHAT IS M-TRENDS?

M-Trends is a report prepared by MANDIANT consultants and computer security professionals who specialize in investigating computer network intrusions. This report details threat intelligence learned while conducting intrusion investigations for the U.S. government, the defense industrial base, and commercial organizations.

All information contained in this report is derived from MANDIANT personnel in unclassified environments. Information has been sanitized to protect identities of victims and data.

The inaugural release of M-Trends focuses on the Advanced Persistent Threat (APT). MANDIANT defines the APT as a group of sophisticated, determined and coordinated attackers that have been systematically compromising U.S. government and commercial computer networks for years. The vast majority of APT activity observed by MANDIANT has been linked to China.

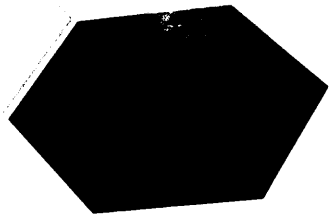
Because of the sensitive nature of any network intrusion, many organizations are reluctant to discuss the extent of the APT threat or disclose data gathered during a response to a breach. This reality makes it difficult to detect and correlate attack trends across multiple industries.

Because MANDIANT responds to hundreds of APT intrusions across a broad spectrum of government and commercial industries, we have a unique perspective on the widespread scope of the APT. As a result, M-Trends provides first-hand accounts of real intrusions that illustrate trends in attack methodologies; technology used to accomplish the attacks; and the types of data that have been stolen.

The intent of M-Trends is to provide valuable information to the security community, while protecting the trust of our clients.

For those not familiar with the APT, this report is intended to provide insight into why organizations should be concerned; how organizations get compromised; and the major challenges in dealing with the threat.

For those intimately familiar with the APT, this report provides a wide-angle perspective of the breadth of attacks that supports ongoing analysis of big-picture trends.



SECTION 1

EXECUTIVE SUMMARY

Over the past five years, MANDIANT has seen a dramatic change in information security incidents. Superbly capable teams of attackers successfully expanded their intrusions at government and defense-related targets... to researchers, manufacturers, law firms, and even non-profits.

These intrusions appear to be conducted by well-funded, organized groups of attackers. We call them the "Advanced Persistent Threat" — the APT — and they are not "hackers". Their motivation, techniques and tenacity are different. *They are professionals, and their success rate is impressive.*

The APT successfully compromises any target it desires. Conventional information security defenses don't work. The attackers successfully evade anti-virus, network intrusion detection and other best practices. They can even defeat incident responders, remaining undetected inside the target's network, all while their target believes they've been eradicated.

At first glance, the motivation behind these attacks seems familiar: access and steal information, and use it to gain a competitive advantage. That's not unusual, but the APT attackers are different. They also establish a way to come back later, to steal additional data, to remain undetected by their victim. *This is a very significant difference.*

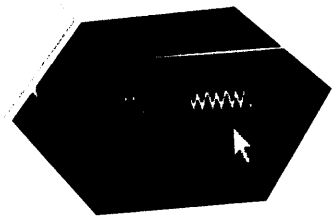
The scale, operation and logistics of conducting these attacks — against the government, commercial and private sectors — indicates that they're state-sponsored. The Chinese government may authorize this activity, but there's no way to determine the extent of its involvement. Nonetheless, we've been able to correlate almost every APT intrusion we've investigated to current events within China.

The APT successfully compromises any target it desires. Conventional defenses are ineffective.

Although the U.S. government and defense communities are aware of and countering APT attacks, many victims and targets are unaware and unequipped. *Often, these victims of the APT react in a way that does more harm than good.*

This report outlines trends, techniques, and real details of how the APT successfully compromises any target it desires. In future M-Trends reports, we will discuss what you can do in order to begin addressing this threat in your enterprise.

Thank you for reading our report. We hope you'll find it useful. If you'd like to discuss it, please contact us. You can reach us by telephone at +1 703 683 3141, or send e-mail to info@mandiant.com. For even more information about MANDIANT, including how to contact us in a computer security emergency, visit our web site at **www.mandiant.com**.



SECTION II

HIGH-LEVEL TRENDING AND CORRELATION

While the APT continues to adapt and become more sophisticated, the attackers still rely on simple techniques to gain access to a victim network. The following trends have been identified throughout the majority of engagements and incident responses MANDIANT has conducted.

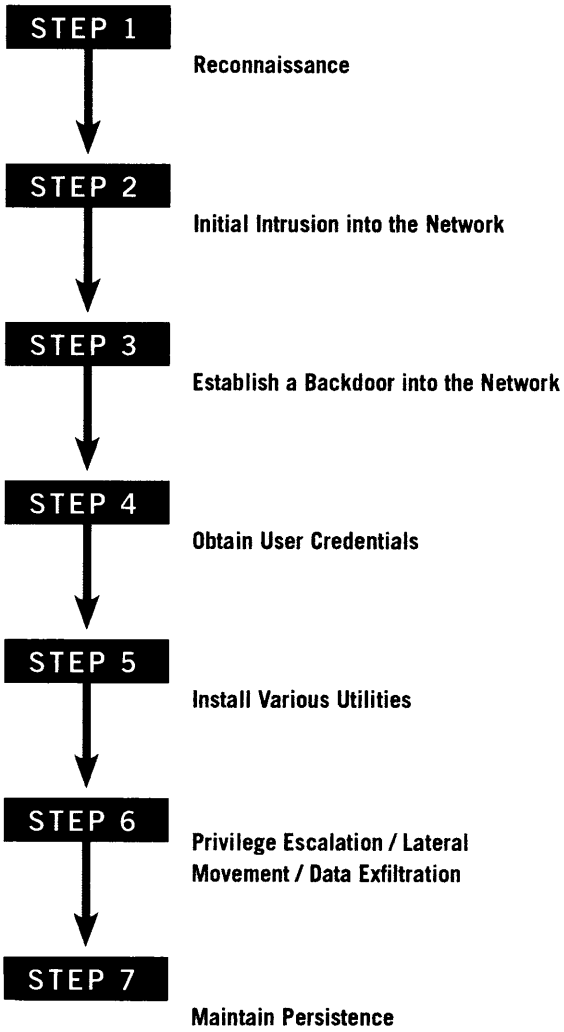
TREND: THE APT CONTINUES TO USE A REPETITIVE AND IDENTIFIABLE TARGETING AND EXPLOITATION CYCLE

STEP 1

Reconnaissance

In every intrusion investigated by MANDIANT, the APT used a consistent exploitation cycle. The attackers typically perform reconnaissance on the target prior to exploitation. Through this reconnaissance, the attackers identify individuals of interest and develop methods of potential access to the target. Targeted individuals range from senior leadership to researchers to administrative assistants. In multiple cases, MANDIANT identified a number of public website pages from which a victim's contact information was extracted and subsequently used in targeted social engineering messages.

EXPLOITATION LIFE CYCLE



STEP 2

Initial Intrusion into the Network

The APT may use several techniques to gain initial access to an organization. The most common and successful method has been the use of social engineering combined with e-mail. This is known as "spear phishing". The APT attackers target a small number of specific individuals with a spoofed e-mail. For example, if a number of employees recently attended a business conference, the APT attackers might send a spoofed e-mail addressed from a speaker at the conference. The spoofed e-mail will contain an attachment or a link to a ZIP file. The ZIP file will contain one of several different intrusion techniques:

» A CHM file containing malware.

» A Microsoft Office document exploit.

» Some other client software exploit, like an Adobe Reader exploit.

APT-associated activity typically occurs on any given weeknight except for foreign and major U.S. holidays. This indicates the attackers know when new information may be available for exfiltration. The attackers typically operate late in the night (U.S. time) between the hours of 10 p.m. and 4 a.m. These times correlate to daytime in China.

STEP 3

Establish a Backdoor into the Network

The attackers attempt to obtain domain administrative credentials (usually in encrypted form) from the targeted company and transfer the credentials out of the network. MANDIANT identified instances where attackers decrypted the credentials within minutes and used them to escalate privileges, either through a pass-the-hash or other legitimate tool. The attackers then established a stronger foothold in the environment by moving laterally through the network and installing multiple backdoors with different configurations. The APT intruders use stealthy malware that routinely avoids detection by host-based and network-based security safeguards. The malware is installed with system level privileges through the use of process injection, registry modification, or scheduled services.

MANDIANT has observed the following characteristics in most of the malware used by the APT:

» The malware is continually updated to ensure that it cannot be easily detected by host-based inspection looking for specific filenames, MD5 hashes, or file content searching.

» The malware uses encryption and obfuscation techniques of its network traffic to make analysis of Command and Control (C2) traffic and data being exfiltrated difficult.

» The attackers' malware uses built-in Microsoft libraries, when available, to reduce the size of the executable and other third-party dependencies.

» The attackers' malware uses legitimate user credentials so they can better blend in with typical user activity.

STEP 4

Obtain User Credentials

The APT intruders access the majority of compromised systems via valid credentials. They often target domain controllers to obtain user accounts and corresponding password hashes en masse. They also obtain local credentials from compromised systems. They use these credentials to perform NETBIOS log-ons to compromised systems in order to inspect and pilfer data. On average, APT intruders access approximately 40 systems on a victim network using compromised credentials, however MANDIANT has assisted companies with as few as 10 compromised systems and some with over 150. The most commonly-used credentials used have domain administrator privileges.

STEP 5

Install Various Utilities

The APT intruders use utility programs to perform common system administration tasks. They have multiple programs with similar functionality that can be used to install backdoors, dump passwords, obtain e-mail from servers, list running processes, and many other tasks. These utilities are often found on systems that do not contain backdoors. Therefore, we can conclude that the attackers install their utilities by using valid credentials.

STEP 6

Privilege Escalation / Lateral Movement / Data Exfiltration

Once a secure foothold is established, the APT exfiltrate data such as e-mails and attachments, or files residing on user workstations or project file servers. In most cases, the exfiltrated information is compressed using of an archival utility such as password-protected RAR or Microsoft Cabinet File. The data is exfiltrated from the compromised network to a server within the APT's command and control infrastructure. Following this session, the attacker typically ensures the malware is functioning properly on the compromised network and repeats the process of exfiltrating files from the network.

The APT intruders exfiltrate data in myriad ways, but MANDIANT has witnessed them using the same tactics at a number of victim organizations. The most common techniques are:

» The use of "staging servers" to aggregate the data they intend to steal.

» Encryption and compression of the data they steal.

» Deleting the compressed files they exfiltrated from the "staging server".

The staging servers are usually identified when a compression utility, such as RAR, is found on the system. A forensic review of the system can result in the recovery of many compressed RAR files. However, these RAR files may have originated from another system accessed by the intruder in the network.

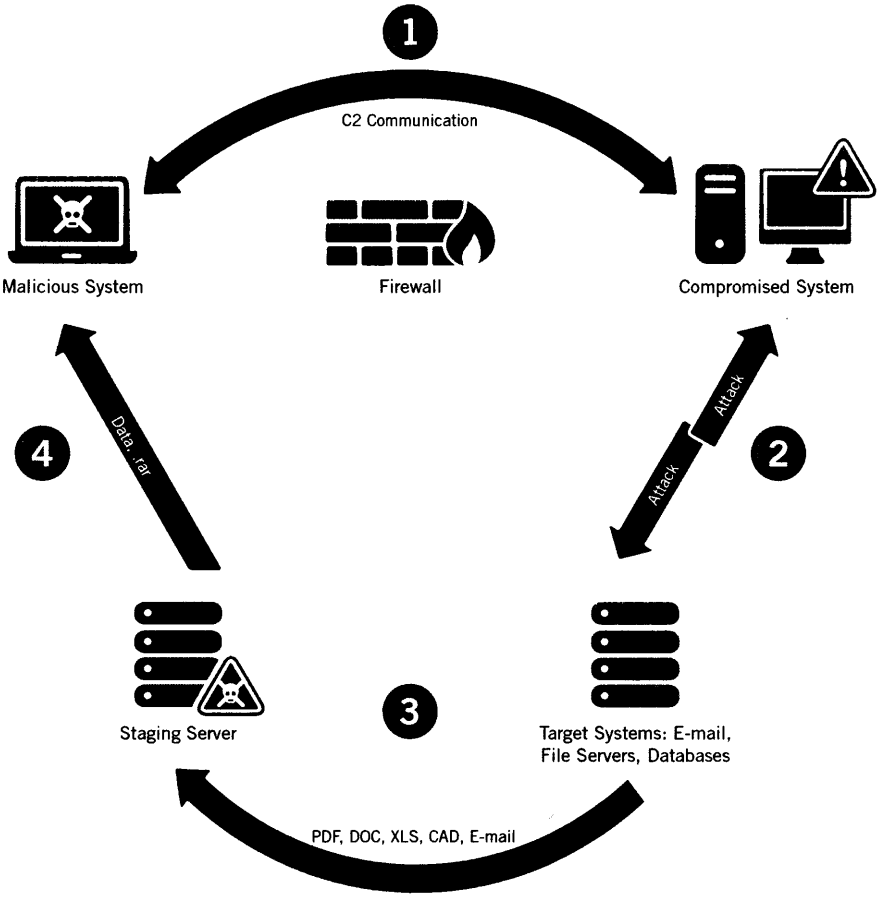
DATA EXFILTRATION METHODOLOGY

Step One: C2 Communication
The malware contacts C2 servers for instructions, such as downloading and executing new malware or opening a reverse backdoor — allowing the attacker full access to the compromised system, bypassing firewall restrictions.

Step Two: Attack
The attacker (through the reverse backdoor) compromises multiple sources of interest, such as database servers, email servers, and file share servers.

Step Three: Data Staging
The attacker sends data to a staging server. Once the data is set, the attacker then compresses the data (using the rar.exe utility) and password protects it.

Step Four: Data Exfiltration
The attacker uses malware to send the data through an encrypted tunnel to a malicious external IP address.



STEP 7

Maintain Persistence

The APT intruders will respond to remediation efforts in order to maintain access to victim networks. As they detect remediation, they will attempt to establish additional footholds and improve the sophistication of their malware.

TREND: THE APT HAS BECOME MORE SOPHISTICATED AT HIDING IN NORMAL NETWORK & HOST TRAFFIC

APT attackers are becoming more sophisticated in the way they hide command and control protocols in normal network traffic. While some APT traffic is fairly easy to identify, the use of more common user agent strings and better HTTP request headers makes it harder for an untrained eye to detect malicious activity.

The APT is starting to use more randomly-generated information within various protocols to make it harder for a static signature to be developed. Several backdoors use random information within HTTP GET and POST requests that do not match an identifiable pattern; however, the GET and POST headers remain HTTP compliant, so many proxy servers will assume the traffic is legitimate. Thus, detecting malicious activity requires additional knowledge about the network protocol. Advanced regular expressions can sometimes detect the malicious traffic; however, attackers using more than one encryption algorithm effectively scramble the encrypted C2 streams, which makes detection harder.

A FEW STATISTICS ILLUSTRATE JUST HOW DIFFICULT IT IS TO IDENTIFY APT TECHNIQUES.

APT Malware Analysis:

» Average File Size: 121.85 KB

» Only 10% of APT backdoors were packed

» Packing is not as common in Standard APT malware

» Packing is common in advanced APT Malware and used by more advanced APT groups

Most Common APT Filenames:

» svchost.exe (most common)

» iexplore.exe

» iprinp.dll

» winzf32.dll

APT Malware avoids anomaly detection through:

» Outbound HTTP connections

» Process injection

» Service persistence

The APT is also using website domain names and SSL certificates that appear legitimate at first glance. For example, the attackers have spoofed Microsoft, Yahoo! and AOL SSL certificates. They also use backdoors that appear to request a Microsoft Update web page. The attackers are also using a form of HTML comments identified as "ADSPACE" comments. With these comments, encoded commands to the malware are stored after what appears to be a comment for legitimate "adspace" revenue generators. Attackers also use .gif image header information to mask C2 activity as a legitimate file transfer.

Lastly, the APT uses backdoors that communicate over distinct chat protocols. The implant first establishes a connection to the chat service providers, and the attacker then logs into the session and connects. These full-featured backdoors offer the attackers command shells and file transfers to and from the infected machine. It is much more difficult to detect this kind of activity, because the legitimate chat services form a buffer between the victim network and the attacker's command and control infrastructure.

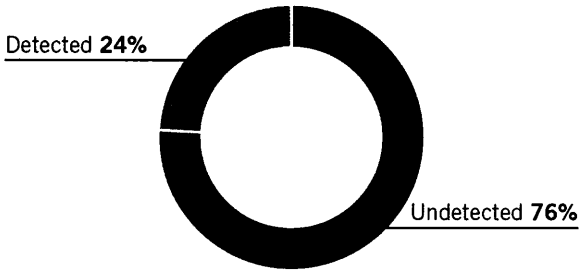
APT Malware Trends and Statistics

MANDIANT has identified, collected and analyzed hundreds of unique APT malware samples. A recurring theme is the APT recognizes that being an anomaly in the network leads to detection.

Standard security tools usually do not detect APT malware. When MANDIANT discovers new APT malware, we scan it with the anti-virus and anti-malware programs that most organizations use. Of the samples we discovered and examined, only 24% of all the APT malware was detected by security software.

The APT malware "hides in plain sight". It avoids detection by using common network ports, process injection and Windows service persistence. Every piece of APT malware initiated only outbound network connections. No sample listened for inbound connections. So, unless an enterprise network is specifically monitoring outbound network traffic for APT-related anomalies, it will not identify the APT malware beaconing attempts.

OVERALL APT MALWARE DETECTION RATE BY A/V



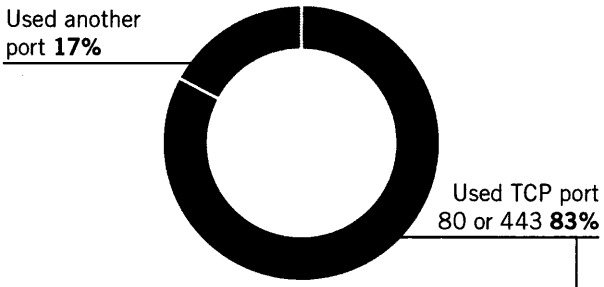
APT hides in network traffic through:

1. Encrypted web traffic.
2. Using web sites that use spoofed certificates.

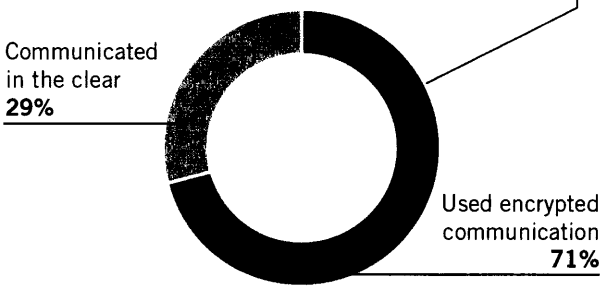
The encryption is not always SSL. We also found encrypted commands sent in cleartext HTML web pages.

Most APT malware is not packed, because packing is relatively easily detected. APT malware that is packed is often more advanced and may contain optimizations or routines that appear to be written directly in assembly language instead of a higher-level programming language. APT attackers that use packed malware are usually more advanced in their skills. They are typically found in more critical targets, such as those with access to more sensitive information.

APT MALWARE COMMUNICATION
100% of APT backdoors made only outbound connections



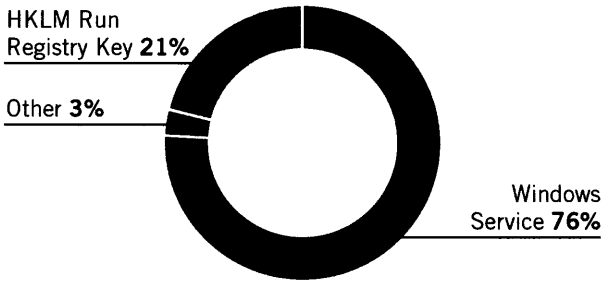
PORT 80 AND 443 COMMUNICATION



Because APT malware is difficult to detect, simple malware signatures such as MD5 hashes, filenames, and traditional anti-virus methods usually yield a low rate of true positives. APT malware shares similar characteristics, and profiling APT malware from multiple victims provides the best chance of positive identification.

APT MALWARE BACKDOORS

APT: Persistence Backdoors
60% of APT backdoor samples were persistent on the machine



APT: Non-Persistent Backdoors
30% used process injection to mask network communication

In no instance was any APT malware written or configured to listen for inbound connections.

TREND: COMPLEX INDICATORS ARE MORE LIKELY TO DETECT UNKNOWN APT-RELATED ACTIVITY

Detecting the APT is incredibly difficult and many organizations are not prepared to effectively identify that they have been compromised. In most cases, initial notification of an APT intrusion originated from a third-party, primarily law enforcement. The primary reason organizations fail to identify the APT is that most of their security devices examine inbound traffic at the perimeter. Most organizations rely solely on anti-virus solutions to provide host-based monitoring. In addition, implementing the ability to monitor internal to internal communications on a network is costly and challenging. In both instances, being able to respond quickly and to deploy APT indicators is difficult, as organizations' security arsenals are not configured to monitor using this methodology.

Host- and network-based signatures used to detect malicious activity have previously consisted of data like MD5, file size, file name, and service name, etc. Although useful, the lifespan of these type of signatures is often short because attackers can routinely modify their malware to avoid detection. Although those signatures will periodically work to identify attacker activity, MANDIANT has found greater success in adapting specific signatures into what are known as Indicators of Compromise ("IOC" or "indicators").

These indicators not only look for specific file and system information, but also use logical statements that characterize malicious activity in greater detail.

MANDIANT has determined that the majority of APT custom-developed tools typically contain code segments from other, similarly developed malware. The code segments could also be upgrades to previously identified malware. Indicators derived from this information remain fairly consistent between the various malware and their subsequent upgrades. Victims are more likely to detect APT-related activity using code segments when it is possible new APT malware might be used. In many cases, previously unidentified malware and backdoors were identified through the use of these indicators in both network traffic and host-based information.

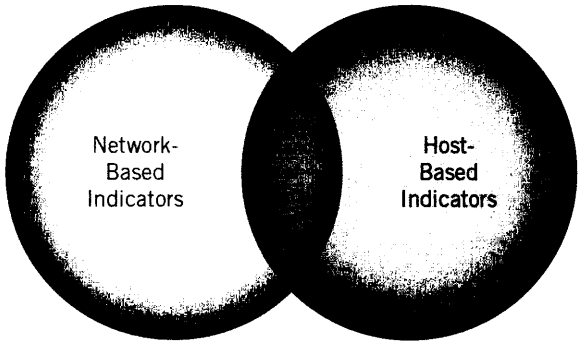
The combination of both host- and network-based indicators continues to be the most reliable way to identify APT-related malware on a network. In two separate investigations, network-based information from a generic packed file transfer revealed suspected malicious activity. Upon further research, the file transfer was identified as malicious activity that was then immediately validated through the use of host-based indicators and forensic analysis.

SECTION CONCLUSION: CORRELATING HOST AND NETWORK INDICATORS SHOWS THE APT CONSISTS OF MULTIPLE GROUPS OF ATTACKERS

Host- and network-based activity observed by MANDIANT indicates behavior consistent with multiple groups of APT attackers. The varying groups use unique tools and techniques to compromise a victim network. The major differences between these groups include:

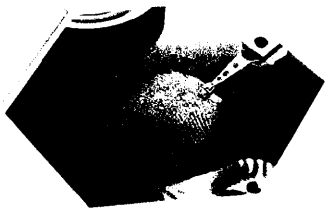
- The type of malware they use.
- Their methods for maintaining access (persistence mechanisms), including the use of:
  - Process injection.
  - Scheduled services.
  - Registry alterations.
- The method of privilege escalation.

OVERLAPPING METHODOLOGIES VS. HOST- AND NETWORK-BASED INDICATORS



At an operational level within individual victim networks, it is unlikely the different sets of attackers are working together towards a common goal. In engagements where multiple, unique groups have been identified, the activities conducted by the different attackers appeared uncoordinated. For example, one group conducted file transfers while another conducted additional exploitation and maintenance. Additionally, some compromised systems have been exploited by multiple groups of attackers. There is a high likelihood that at some victim locations, one attacker is unaware of the presence of another on the same system.

On an individual host-based forensic level, intrusion-related findings would be difficult to attribute to multiple sets of activity. Because MANDIANT is able to view these intrusions across multiple victims, we have observed that the various groups are going after specific targets. Each of the attackers appears to be tasked with obtaining information related to different sets of data. In all cases, information exfiltrated by each set of attackers correlates with a need for intelligence related to upcoming major U.S./China mergers and acquisitions, corporate business negotiations, or defense industrial base (DIB) acquisition opportunities. In the following sections, MANDIANT provides case studies that illustrate the points made above. The case studies are derived from the experiences of MANDIANT consultants who have worked with various, targeted organizations over the last five to seven years.



SECTION III

CASE STUDIES

The APT attackers have targeted particular organizations due to the type of intellectual property they maintain, and no organization should feel they are too large or small to be a victim. One need not look any further than the front page of the business section of the newspaper to determine who is probably a recent APT target.

GOVERNMENT CASE STUDIES

MANDIANT has worked with a number of different government agencies and the Department of Defense (DoD), all of whom have been targets for the greater part of the last decade or longer. Government entities will continue to be a target for the foreseeable future, as the APT appears to be conducting a data espionage campaign against the United States.

CASE STUDY: TARGETING COUNTER-TERRORISM ORGANIZATIONS WITHIN THE U.S. GOVERNMENT

When combined, singular events show strategic requirements of a targeted and sophisticated information campaign.

During 2009, MANDIANT witnessed the APT targeting multiple local, state and federal government entities whose commonality was their access to information related to terrorism. These attacks increased concerns regarding the type of information sought by the APT. One event involved a spear phishing e-mail containing a malicious file sent to multiple individuals from a fictitious account of an executive. A second event involved an attacker who conducted network exploitation that revealed passwords of user accounts with administrator privileges, networked critical assets and network topology. A third event involved data exfiltration of e-mails and attachments containing terrorism-related information.

When collectively viewed, these incidents clearly indicate an effort to satisfy an intelligence gap. The malicious e-mails in the first event were sent to an organization tasked with consolidating local, state and federal law enforcement agencies into a central location to foster information sharing among various levels of government. The second event involved a high-ranking counter-terrorism official whose e-mail account was targeted with pinpoint accuracy. The third event involved data belonging to a government coordinating authority that receives intelligence information from local, state and federal law enforcement. The stolen data was comprised of e-mail communications, e-mail attachments and networked file share directory file structure and file metadata.

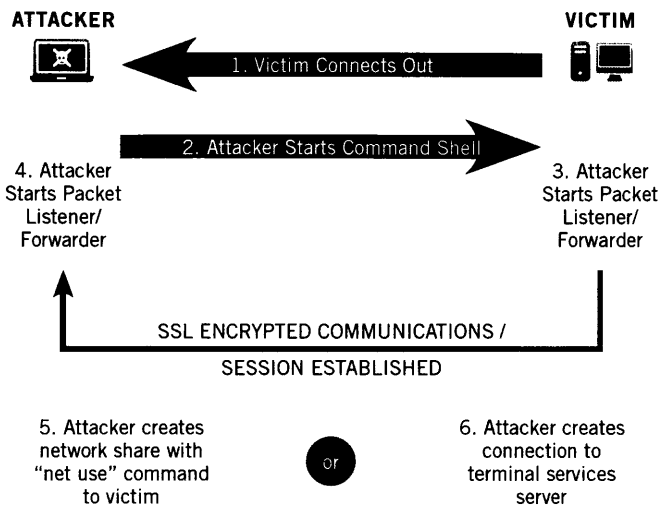
These events show the APT appears to have clear intelligence requirements including, among others, the suppression of internal political threats. Within each of these targeted organizations, persistence mechanisms were enabled so access to the penetrated networks remained. In these cases, the APT persisted through the use of multiple backdoors and sustained access via multiple network command and control channels. The backdoors were protected with known and/or custom packers. This indicates that the attackers in this instance were using more advanced APT malware. The command and control channels were masked through the use of SSL, custom base64 encoding or custom layered encoding involving XOR and/or base64 combinations.

This case demonstrates that the APT assigns critical targets to the most advanced APT groups using the most sophisticated malware and command and control communication methods. The degree to which the attackers protect their malware rendered traditional perimeter defense techniques nearly ineffective. Detection is challenging, but possible, with the right team armed with robust APT indicators. The need for a scalable, enterprise, host-based scanning capability and sophisticated indicators looking for components of APT malware is critical to the success of identifying and defending against the APT.

CASE STUDY: GOVERNMENT ENTITY

In most cases, the APT already knows what files and information to obtain and prefers targeted and persistent access to that information versus conducting smash and grab operations to obtain everything and anything possible.

TUNNELED NETWORK SHARE



Recently, MANDIANT investigated an intrusion at a federal government entity that maintained access to a wide variety of government databases. Previous methods of response to this incident would have identified the situation as three systems compromised over a period of three days. Prior to MANDIANT's investigation, the victim's response included pulling compromised systems offline immediately and collecting the malware in an attempt to identify callback domain names and IP addresses. This information was then used to block those systems' access to the network.

This tactic simply allowed the attackers to identify the compromised systems and malware that the victim discovered and to leverage other systems and malware that had not yet been detected. By decoding the APT command and control protocols, MANDIANT uncovered a keen insight into individual APT activities and provided a richer understanding of what and who was being targeted at the victim organization.

In this case, MANDIANT identified two additional compromised systems. We determined that the attacker created a network share directly from an internally compromised system to an external server associated with their command and control infrastructure. The attacker then used a tunneled network share to conduct queries on an internal application

server to pull requested files from other networked systems within the environment. The attacker explicitly specified that certain files were to be exfiltrated. The filenames of these files contained random numbers and letters, indicating the attacker knew exactly what files to capture based on previously obtained information.

SIGNIFICANT FINDINGS

In the preceding case studies, the attackers used the custom base64 encoding algorithm that was previously observed by MANDIANT at other commercial organizations and defense contractors. In some cases, the attacker used the additional security of encrypting the traffic with Secure Socket Layer (SSL) communications. This allowed the attacker to better blend in with legitimate network traffic. It also demonstrates that the attackers are constantly upgrading their tools. Based on the tactics observed, MANDIANT believes the attackers use the least secure tool for the job and upgrade only when necessary to avoid detection.

Additionally, a review of the exfiltrated files in the second case study indicated the files were actually publicly available online. Because the files were freely available, it is unknown why the attacker decided to remove them directly from the government agency rather than obtaining them through open source collection. In most cases, the attackers knew exactly what they were looking for, although not all data exfiltration is highly selective. Downloading the file directly from the government agency versus obtaining publicly available information may be a way to validate the authenticity of the information.

DEFENSE INDUSTRIAL BASE CASE STUDIES

The Advanced Persistent Threat continues to actively target and exploit cleared defense contractors (CDCs) and other members of the DIB. In the past, MANDIANT's visibility into the APT was limited to intrusions at medium-large to large CDCs. This group of victims continues to expand as MANDIANT responds to a higher number of intrusions at small to medium-sized defense contractors. All of the victims conduct advanced research for the Department of Defense and U.S. government.

CASE STUDY: A MEDIUM-SIZED CLEARED DEFENSE CONTRACTOR

Full scoping and understanding of APT-related activity is the best way to remove the APT from a network.

In early 2009, a medium-sized contractor (CDC1) contacted MANDIANT to assist them in remediating an APT intrusion. The victim was provided with a list of over 100 possibly compromised systems by external sources. The contractor attempted to remediate the attack by wiping and removing only the compromised systems. They brought MANDIANT in to confirm they had successfully removed the compromise from their network.

After a two-day investigation using APT indicators, volatile data analysis and traditional forensics, MANDIANT identified an additional 20 compromised workstations and servers. During the investigation, MANDIANT determined the APT initially gained access to the cleared defense contractor as far back as early 2007. Command and control malware placed throughout the enterprise was identified as having been

installed between 2007 and 2009. MANDIANT also identified that additional spear phishing campaigns were conducted between 2007 and 2009.

MANDIANT identified multiple pieces of APT malware that appeared to fit into at least two distinct categories of APT activity. The command and control communications included:

» C2 instructions contained in base64 encoded comments on webpages.

» Multiple web-based protocols that appeared to blend in with normal web-based traffic.

» Two custom encryption protocols.

» SSL.

Over time, it became obvious that the attackers continued to upgrade backdoors that were currently in place. In one instance they installed an implant that used a custom encryption algorithm. In a second instance they leveraged the same functionality and incorporated the same exact command set, but enabled more secure communications using SSL. A third capability leveraged the use of a custom backdoor that took advantage of a chat application programming interface (API) to conduct command and control activity. The use of chat sessions allowed the attacker to take advantage of the API while also providing secure log-on and communication capability.

There were several decisions made by the organization that ultimately hindered their ability to fully remediate the situation. To date, due to the rolling remediation, additional assessments continue to identify new systems compromised by the APT.

First, the organization decided to immediately disconnect any compromised system. The problem with immediately removing compromised systems from the network is that it typically alerts the attacker and lets them know an infected system has been identified. This forces the attacker to shift tactics and use a compromised system that may likely be unknown to the victim organization. The attacker will then likely use different malicious software to communicate with the victim network. This makes it very difficult for the security team to investigate and respond to the latest activity when that activity may be new and unknown.

Second, removing the compromised systems directly affected the victim's ability to identify the critical resources targeted by the APT. Without first scoping the incident and understanding the situation, it is difficult to determine who or what is targeted. Many times, systems that are compromised are not necessarily the systems that have true value to the APT. In most cases, the APT moves laterally through a network to maintain a safe harbor and then to acquire data of interest from critical network assets.

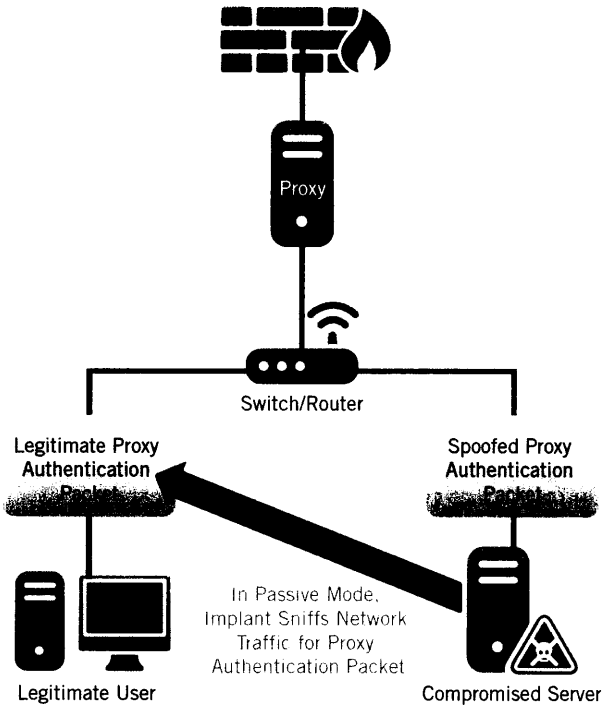
CASE STUDY: A LARGE-SIZED CLEARED DEFENSE CONTRACTOR

Host- and network-based indicators suggest multiple independent groups of APT-related activity. On an operational level, these groups do not appear to coordinate activities.

In 2009, a large contractor (CDC2) contacted MANDIANT to perform a threat assessment. The objective of the assessment was to determine the extent of APT activity on their corporate network. The contractor contacted MANDIANT because they knew there were problems, but had no way of identifying the scope of the ongoing compromise. MANDIANT deployed MANDIANT Intelligent Response™ (MIR) to sweep the enterprise network of 50,000+ systems. Additionally, MANDIANT deployed a set of known network-based indicators. Within 24 hours, we identified more than 10 compromised systems.

Within days, MANDIANT used deployed indicators to locate a previously known APT backdoor. Network forensics performed on the captured network traffic indicated backdoors were dormant for various

EXAMPLE OF PROXY-AWARE BACKDOOR



periods of time. By reverse engineering the malware, MANDIANT identified that the implants were configured to sleep for anywhere from a few weeks to a few months, with one implant configured to sleep for over a year. This is a clear example of how patient the APT attackers are and indicates the length of time they strategically invest in a victim network.

Based on forensic reviews of multiple systems and network traffic, additional backdoors were identified as communicating with systems associated with the APT command and control channel. In total, the same APT attack group used three unique families of backdoors. Each backdoor incorporated different custom encryption algorithms:

» One backdoor used a combination of three custom encryption algorithms wrapped within a modified base64 algorithm. MANDIANT observed that the APT preferred one backdoor over the other two, even though the three backdoors consisted of similar functionality. This functionality included the capability to conduct file transfers; conduct various host- and network-based reconnaissance; and to dynamically reconfigure the implants.

» MANDIANT identified additional backdoors that contained the ability to communicate via UDP and TCP network protocols. The malware also contained features that allowed it to operate in an environment where various proxies exist. The implant had the ability to "sniff" network traffic for packets containing "Proxy-Authentication" headers. Once identified, the backdoor dynamically generated proxy credentials that allowed the backdoor to successfully communicate with its APT operators.

A second type of APT activity revealed that the attackers used modified base64 encoded commands within comments on a legitimate web page. Through the encoded commands, the compromised system downloaded a total of seven malicious files, including two additional backdoors and the RAR archiving program.

One unique capability of the additional two backdoors was the ability to self-destruct. If the backdoors could not reach their intended destination, they would remove themselves from the system. The backdoors did not leave any additional backdoors or any traceable system modifications. As a result, the malicious files were more difficult to detect.

A third set of APT activity discovered three versions of malware with version information embedded within an encrypted Windows registry key. MANDIANT identified version revisions and was able to clearly identify additional features bundled with each subsequent version. These features included command and control channels over HTTP that subverted network proxy through supplying valid network credentials. MANDIANT determined that this malware was one of the more sophisticated families of implants used by the APT as it was very well concealed in outgoing web traffic.

A fourth set of masked web traffic was discovered during APT sweeps. When the backdoor beaconed to the attacker's external command and control server, the HTTP request seemingly requested a web page associated with Microsoft Update; however, the APT's server was not a legitimate Microsoft Update server. The APT's software on the server interprets the inbound request for the Microsoft Update page and translates the requests into commands. None of the web pages legitimately existed on the APT server. There are three types of requests that the command and control server would initiate:

» Command request beacons: One web page request represented command request beacons from compromised systems.

» Initial connection requests: Another request represented the initial connection from the APT's command and control server to the compromised system, indicating the APT was active on the server. This returned various host-based information from the compromised system to the command and control server.

» Command initiation: The last request passed commands from the APT's command and control server to the compromised system. Depending on the request, the contents may or may not contain encrypted data with a custom encoded key.

This type of command and control traffic has been detected through the validation of legitimate traffic, such as checking for Microsoft Update activity against known Microsoft net blocks, to check for oddities. In many circumstances, companies use third-party content distribution sites to host updates, including updates for Microsoft products.

MANDIANT discovered APT malware that read traditional base64 encoded comments looking for sleep activity, file transfers, or implant redirection for first stage malware. In addition, the sweep found malware using SSL communications to blend in with normal network. In total at this victim, MANDIANT identified over 150 compromised systems accessed by the APT.

MANDIANT's network forensics capability revealed that the attackers focused the majority of their efforts on enumerating multiple file servers that contained information related to sensitive research and development programs. The APT obtained recursive directory listings for nearly every directory contained on multiple file servers associated with various sensitive projects. In all, MANDIANT identified several hundred megabytes of exfiltrated data related to the enumeration of the file servers.

The attackers continued to move laterally through the corporate network, consistently starting and stopping backdoors. This allowed the attackers to decrease the likelihood of a compromised host being identified, as the systems communicating with the attackers' attack infrastructure continually changed. The presence of multiple backdoors allowed the attackers to continue to maintain a presence on the network. In most cases, systems only contained one backdoor; although a handful of systems contained two or more backdoors. Some overlap occurred between the callback IP addresses and domain names used by individual backdoors. In most cases, however, each set of backdoors contained different callback IP addresses or domain names.

The use of MANDIANT Intelligent Network Traffic System (MINTS) gave us the capability to determine what data was exfiltrated and provide leadership with a real-time damage assessment. This provided senior leadership with the knowledge necessary to determine the best course of action for remediation. The damage assessment provided the victim's senior leadership with the knowledge and actionable intelligence necessary to determine the best course of action for remediation to safeguard critical programs.

CASE STUDY: A LARGE-SIZED CLEARED DEFENSE CONTRACTOR

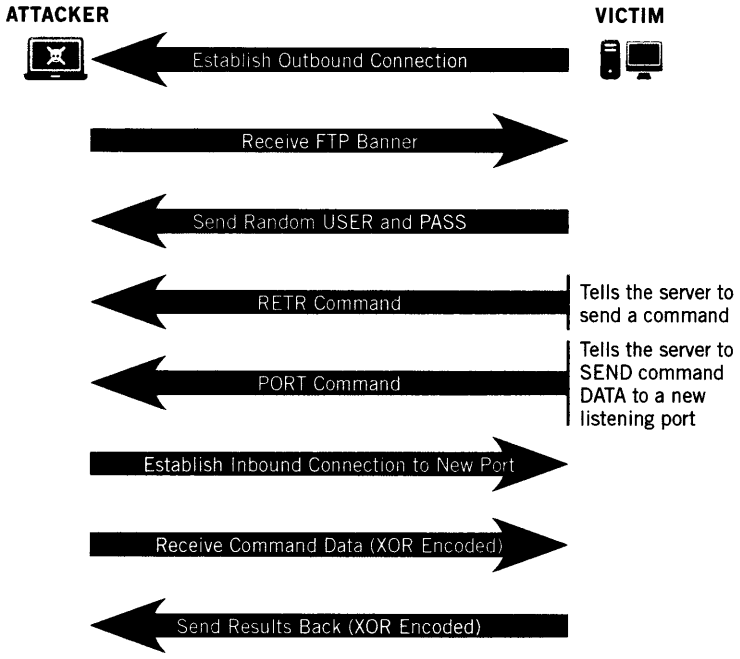
The APT continually adapts quickly to a changing environment.

In mid-2009, another large cleared defense contractor (CDC3) with over 45,000 hosts contacted MANDIANT for assistance detecting and remediating activity related to the APT. MANDIANT's incident response began shortly after response and remediation occurred at the previously-discussed large defense contractor. This is relevant because MANDIANT identified the same malware being used at both victims.

MANDIANT performed an APT sweep of the network using known indicators of compromise and identified malware domain names and callback IP addresses similar to those seen during the previous case study. Once again, these indicators clearly illustrated that different groups of attackers were accessing the network. Diverse exploitation methodologies also existed between the attackers. In some cases, the attackers used pass-the-hash tools to escalate privileges on the compromised system. In other instances, another group of attackers used legitimate domain administrative credentials to move laterally through the network. The attackers' primary targets were file servers containing sensitive program data. In addition to enumerating the file server to obtain the directory listings, the APT was also able to obtain — on a near daily basis — data related to different sensitive programs.

One of the unique APT backdoors found in this case revealed a different method of command and control over the file transfer protocol. This backdoor established the initial connection to the command and control server and waited for the server to send data back. The malware disregarded the initial data, which was consistent with an FTP banner returned from the log-on. The malware then responded with the USER and PASS commands with random strings as the username. To retrieve a command from the server, the malware used the FTP command RETR and a randomly generated filename which contained the encrypted command text. The fully functioning backdoor contained typical functionality, such as file transfers and built-in tools needed for host- and network-based reconnaissance.

APT FTP COMMAND AND CONTROL



In total, the abundance of malware associated with multiple groups of host- and network-based indicators showed an extensive compromise that spanned years. In one instance, over 96 separate malicious APT-related files comprising various backdoors and utilities were identified on an individual system. Over 150 total systems appeared to have been compromised at CDC3, with the earliest known compromise occurring at least two years prior.

Upon identification of sensitive data exfiltration, the cleared defense contractor removed certain specific sensitive program data targeted by the APT. The contractor kept the directory structure of the program data. In subsequent activity, the attacker attempted to obtain additional information related to the program. After the files were removed, the attacker enumerated the directory structure and exfiltrated the information from the compromised system. The following night, the attacker appeared to realize the data they were interested in was no longer available. The attacker then updated the domain names associated with the backdoor on the compromised system to reflect a change in the attackers' command and control infrastructure. This reaction occurred less than 24 hours after review, following nearly three weeks of using the same command and control IP address to conduct malicious activity. After updating the IP resolution of the backdoor's callback domain name, the attacker wasted no time, immediately exfiltrating data from a second sensitive program.

TIMELINE OF ATTACKERS RESPONSES TO PARTIAL REMEDIATION EFFORTS

DAY 1&2

Attacker bad domains resolve to IP

DAY 32

Client removes systems

DAY 34

Attacker discovers systems taken offline

- » Updates DNS information
- » Uses existing backdoors to install
  - New network protocol
  - New host signature

DAY 36&37

Client removes sensitive data from known compromised systems

DAY 38

Attacker exfiltrates empty directory listing

- » Attacker pushes 1 new malware
- » New Protocol/Domain/IP

DAY 39

Attacker pushes old malware to new systems

DAY 41

Attacker updates DNS information

- » Compromised systems with empty directory listing
- » Pushes same malware Day 34 to new systems

After this reaction, CDC3 initiated an active response strategy implemented by MANDIANT to corrupt data being exfiltrated. MANDIANT successfully manipulated network traffic that contained data exfiltration from a corporate network to make it appear as if the exfiltrated traffic was legitimate. In one critical case, MANDIANT prevented the exfiltration of sensitive ITAR related information to buy additional time needed for further scoping prior to remediation. This remediation tactic was successful on multiple occasions.

As a result of this active response, MANDIANT saw the APT shift their activities to adapt to the changing dynamic. In addition to the change in backdoor callback domain names, the attackers also changed the usage frequency of their current backdoors. Prior to the removal of data, the attackers were using a backdoor that generated network traffic appearing to be legitimate image file transfers. This protocol was used in the previous case study for the majority of the data exfiltration and file transfers. Once they determined the data was removed, the attacker started using additional backdoors and protocols more frequently, removing some of the original backdoors from identified compromised systems.

After successfully manipulating network traffic, MANDIANT identified that the attackers also used other protocols to perform file transfers to and from the network. In one case, MANDIANT identified malicious network activity early in the morning and manipulated the traffic in such a way that the protocol actually broke during the file transfer. The attacker attempted to connect to the system again before ending the session. The added capabilities for network traffic manipulation and near real-time decryption allowed MANDIANT to gain the additional time needed to finish scoping the extent of the compromise prior to remediation while protecting sensitive data of concern from falling into the hands of the attacker. Less than 24 hours after remediation, the attackers recognized that they no longer had access and started a new campaign to regain access to the network.

SIGNIFICANT FINDINGS

The APT has targeted cleared defense contractors and will continue to do so. They typically target information related to cutting-edge technologies and research and development conducted by the contractor. In most cases, unlike commercial and government victims, the cleared defense contractors' senior management is not the focus for data theft. Additionally, in the majority of cleared defense contractor engagements, MANDIANT has identified malicious APT activity using multiple sets of host- and network-based indicators. This suggests the presence of multiple independent APT groups conducting intrusion activity at a single organization. Finally, in cases of data exfiltration, most data appeared to come from file servers or individual users' workstations.

During the course of investigations, MANDIANT routinely requests victims to identify their critical sources of information. In almost every case, the victims responded that every program is equally as important. In addition, central file servers typically host multiple, perhaps unrelated, programs. At both CDC2 and CDC3, MANDIANT could clearly identify the company's critical host and network resources. In both cases, the attackers obtained sensitive data from different programs housed on the same set of file servers. Without MANDIANT's ability to perform network forensics, identifying the actual data that was taken may have been very difficult.

In MANDIANT's experience, once the CDC has identified critical information within a particular program, they want to begin remediation as soon as possible. As illustrated in the above case studies, early remediation without full scoping to understand the extent of the problem is essentially akin to playing "whack-a-mole". Additional compromises will occur within weeks, if not days, due to the attackers' persistence.

In the cases described, the victims chose distinct remediation paths. In the first case, remediation began before the compromise was fully scoped. As a result, the APT used lateral movement to maintain a foothold in the victim network, thwarting remediation efforts. In the last case, MANDIANT employed techniques to aid in the protection of critical data while maintaining visibility to the attacker's activities. Caution should be used when employing this methodology, as MANDIANT has seen the attacker change their tactics to circumvent protective activities.

COMMERCIAL CASE STUDIES

CASE STUDY: FORTUNE 500 MANUFACTURING COMPANY

In 2009, a U.S.-based Fortune 500 manufacturing company initiated discussions to acquire a Chinese corporation. During the negotiations, APT attackers compromised computers belonging to the executives of the U.S.-based company, most likely in an effort to learn more details of the negotiations. Sensitive data left the company on a weekly basis during negotiations, potentially providing the Chinese company with visibility to pricing and negotiation strategies.

Law enforcement notified the company of the intrusion into their networks. The APT had targeted executives involved in direct talks with the Chinese corporation. Law enforcement provided the victim organization with proof that the APT had exfiltrated critical e-mails containing details of the negotiation from the victim organization's executives just days prior to the negotiations.

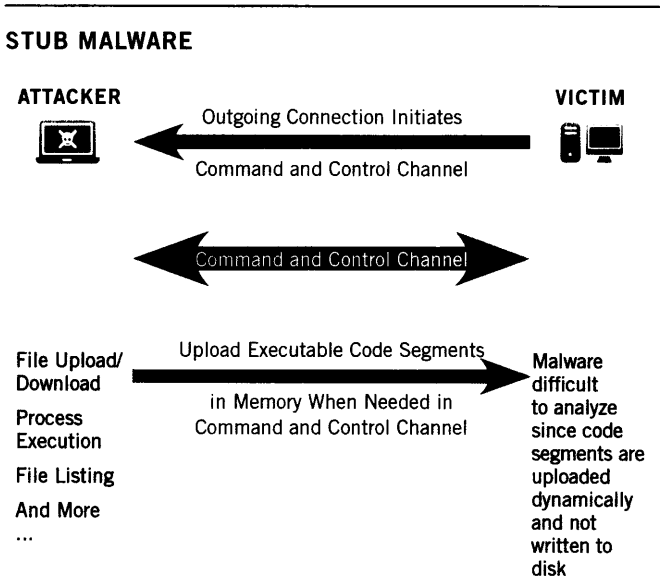
The attackers compromised multiple key executives' systems. The APT initially sent targeted, spear phishing e-mails to four company executives. The e-mail was crafted to look like it originated from a fellow employee and discussed a message from the CEO on conserving resources. One of the key executive's systems was compromised when he clicked on the link embedded within the e-mail, which then downloaded and executed a malicious file. The malicious file installed a fully functional command and control backdoor on their system that allowed the APT full access to the system from the Internet.

The APT copied malware to the executive's system. From there, the APT used password-stealing utilities to gain access to new systems on the network. The APT gained access to multiple user accounts with local administrative rights to the majority of the company's Microsoft Windows systems. The executive's system was also used to launch a successful SQL server attack. As is often the case, the APT was able to move laterally within the network by compromising a single system, performing network reconnaissance and utilizing privileged, valid credentials.

The APT performed a number of activities once the network had been compromised. The absence of detailed data allowed only a portion of the APT's activities to be identified. More robust logging and monitoring must be established in order to enable a victim organization to identify the major activities of the attacker. On page 26, a list of recommended actions to implement better logging is included in the Initial Data Compilation Checklist.

One of the most interesting elements in the case was the use of stub malware that left a minimal forensic footprint on a machine. The stub malware performed an HTTP-based network connect-out that allowed the attacker to upload command and control instructions dynamically. For example, when the stub malware connected to the command and control channel, the commands for executing a remote process or performing a file listing did not exist in the stub. Those commands would be uploaded to the machine only when needed and, upon termination, the only residue would exist in virtual memory. As a result, this allowed the stub to leave an extremely small footprint that was difficult to reverse engineer. The APT could easily upload new capabilities to memory via the stub, allowing them to have additional command and control capabilities.

If the APT wanted a new capability, they would simply code new executable segments that could be uploaded and executed via the stub's process in memory, without requiring a disk-write to succeed. One of the key points here is that when the stub malware was used, it was difficult to detect these additional capabilities unless memory was analyzed at the same time the new capability was uploaded and executed. This capability allowed the attacker to leave a minimal forensic footprint and easily upgrade the malware's capabilities.



This intrusion had a significant impact on the victim organization. As a result of the compromise, the U.S. company terminated their acquisition plans. While it was not possible to determine all of the data that had been lost, the victim company was not able to complete the acquisition and accomplish their business objectives.

CASE STUDY: LAW FIRM

In 2008, MANDIANT investigated an APT compromise at a law firm. The law firm was representing a client who was the plaintiff in a Chinese civil litigation case. In this case, MANDIANT was able to monitor all of the activities performed by the attacker over a two-month period and gain insight into their preferred methods and tactics.

In this instance, the APT successfully compromised the environment and removed a significant amount of information from the network over an extended period of time. More than 30 user account and password hashes were obtained from the law firm's domain controllers. Using those valid credentials, the attacker was able to extract thousands of e-mail messages and their attachments by downloading the information from the firm's mail servers.

The valid credentials permitted the attacker to access any server, workstation, or laptop in the network. In order to achieve this level of access, the APT compromised approximately three-dozen workstations. On each of these systems, they either placed malware or used valid account credentials to create files, execute programs, and exfiltrate information and e-mail from the network.

Because the firm did not have system logs available from firewalls, intrusion detection systems, websites or individual systems, it was impossible to determine the initial attack vector. This, in turn, made it difficult to determine all of the information harvested from the network.

One of the first remedial steps the firm took was to enable full packet capture at the perimeter so that all future traffic could be monitored. This logging allowed the MANDIANT response team full visibility to all of the attacker's traffic. Once the traffic was identified, MANDIANT determined that it was encoded, but not encrypted. MANDIANT decoded the traffic and was able to view all command and control, as well as data exfiltration for a period of two months. The level of visibility was unprecedented and allowed MANDIANT to better understand how the attacker used their tools, how they removed evidence of their activities and what their work schedules were.

This insight allowed the law firm to monitor all activity and verify exactly what data had left the network. Steps were taken to remove sensitive data from mail servers during the time frame in question so that no client or sensitive information resided in accounts targeted by the attacker. This enabled the firm to craft a very effective remediation plan that addressed the tools and techniques used by the attacker.

The chart on the next page illustrates the steps taken by the attacker to harvest e-mail.

APT E-MAIL COLLECTION AND EXFILTRATION

Step One: Backdoor contacts APT for commands.
The installed backdoor periodically contacts a website to check for commands issued by the attacker. With the backdoor calling out of the network in this way, the attacker is able to bypass inbound firewall rules.

Step Two: Attacker instructs backdoor to download tools from a remote FTP site.
The tools are mapi.exe, mapiget.exe and rar.exe. These tools allow the attacker to harvest e-mail inboxes and pacakge the resultant files into a single rar file.

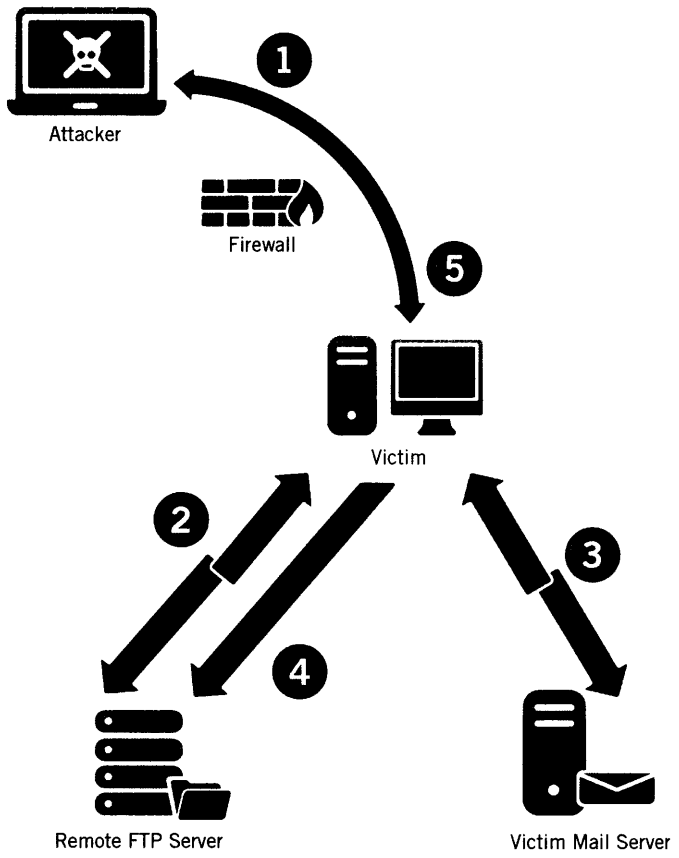
Step Three: The attacker runs "mapi.exe" and "mapiget.exe" against the mail server.
Various accounts are chosen and commands are issued to extract e-mails from their inboxes.

The e-mail is written to the victim computer as text documents. Thousands of these files have been observed on several occasions.

Step Four: Attacker "RARs" the e-mail files into a single file "new.rar".
This is done with rar.exe, a package and compression tool downloaded by the attacker.

This document is normally password protected to deter data loss determining efforts.

Step Five: Attacker deletes "new.rar" and tools.
New.rar and the tools used by the attacker are never left behind to be discovered. This is the attacker trying to cover his tracks. Evidence of this is seen in the Access Protection Logs.



Although the law firm was able to monitor all activity during the latter stages of the incident, they were never able to identify the initial attack vector. This was because attacker activity contained in log information dating back to the onset of the intrusion — more than a year before third-party notification — had not been retained. Consequently, it was not possible to identify evidence of the initial compromise.

This attack shows that the APT is willing to compromise a network and harvest a vast amount of e-mail and user account data over a sustained period of time. The impact of APT intrusions on this law firm is unknown, but a conclusion can be drawn that the APT targeted the law firm because of its work related to China.

MANDIANT has seen that the APT has increased its attacks on politically or socially motivated organizations that focus on issues stemming from current events in China. This includes not just law firms, but think-tanks and human rights organizations as well.

CASE STUDY: POLITICAL NON-PROFIT ORGANIZATION

In 2009, system administrators at a non-profit organization identified an ongoing intrusion affecting several core infrastructure servers. Upon initial investigation, the organization's security administrator identified a number of systems that had successfully established suspicious connections to servers external to the organization.

MANDIANT determined, during the course of the investigation, that the APT attackers sought information regarding the organization's work with the spread of democracy and free enterprise within China. The attackers targeted the firm's Chinese subject matter experts to obtain the latest U.S. views on United States-China economic and political relations. Insider knowledge of government personnel may have aided the attackers with the creation of better spear phishing e-mails.

This attack shared many characteristics with the previously discussed intrusion into the law firm. The APT harvested e-mail and additional account credentials. MANDIANT believes that the attacker's initial vector of access was through socially engineered e-mails.

SIGNIFICANT FINDINGS

The APT targets companies and organizations in the private sector that have corporate dealings with organizations in China. In the cases MANDIANT has investigated, executive officers and individuals responsible for corporate offerings are the intended targets of an APT attack. This is likely because they manage the most sensitive and current information of interest to the attackers.

Each of the commercial organizations discussed above appears to have been compromised by similar methodologies. The initial attack vector is generally a spear phishing e-mail that targets corporate executives. Lateral movements within an organization are executed by compromising valid credentials or by using additional exploits against servers internally. As illustrated in the DIB and government case studies, these methodologies do not shift depending upon the victim.

TAKEAWAYS FOR COMMERCIAL ORGANIZATIONS

- The APT selects their commercial victim — often based on current events.
- Senior executives are targeted with spear phishing attacks.
- The attackers compromise valid accounts and move laterally inside the victim's network.
- The APT identifies and exfiltrates sensitive data.

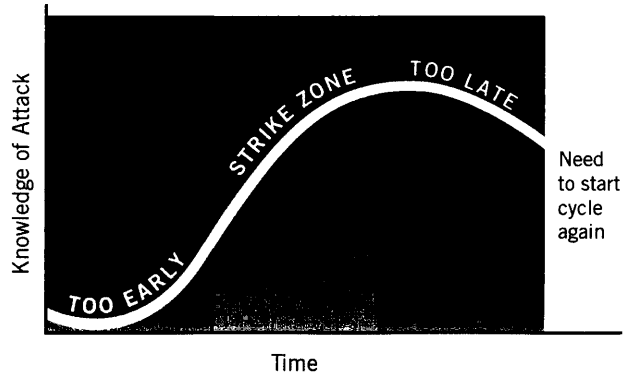
SECTION IV

WHAT TO EXPECT IF YOU ARE A VICTIM OF THE APT

MANDIANT has learned that rushed and unplanned remediation efforts almost always fail to resolve an incident. We have also witnessed that the majority of large organizations targeted by the APT remain compromised after numerous remediation efforts — unless those remediation efforts are planned, coordinated across business lines, incisive, and executed at the appropriate time. We have observed numerous challenges at many organizations during their efforts to resolve an APT compromise. Such challenges include, but may not be limited to, the following:

» Remedial efforts usually took more effort and determination than anticipated. It is a good principle to begin managing the expectations of your personnel as soon as possible, ensuring they are aware that the remedial efforts may involve continual effort, resources, and periodic adjustments based on the dynamics of the ongoing threat.

REMEDIATING IN THE STRIKE ZONE



...rushed and unplanned remediation efforts almost always fail to resolve an incident.

» An ineffective remediation was initiated because the plan was implemented prior to understanding the tools and techniques of the intruder.

» An ineffective remediation plan was initiated because the remediation plan took too long to develop. This allowed the compromise to become so widespread that remedial efforts became time-consuming and costly.

» The remediation plan failed because accountability for its execution was not clearly assigned to an individual.

» Remediation failed due to lack of resources: lacking the personnel, technology and processes to follow through on the remediation plan.

» The remediation plan failed because it involved panicked reactions such as purchases of technology or other activities that do not contribute to long-term or strategic IT security goals.

» The remediation efforts failed because the victim firm continually removed compromised hosts in an uncoordinated or ad-hoc manner prior to identify-

ing the full scope of compromise. After detection of malware on a system, the immediate removal of the compromised hosts from the network merely:

- Jeopardized the effectiveness of the remediation.
- Did little to impact or impede the intruder's access to the victim network.
- Promoted a false sense of protecting data.

In short, remediation fails if you wait too long to execute or move too fast. MANDIANT is a strong proponent that remediation can only succeed if the remediation plan is:

» Written.

» Coordinated with all appropriate business lines.

» Feasible.

» Executed after the appropriate posturing steps are performed.

» Executed when the team has identified all known compromised APT hosts and has methods in place to identify new compromises that occur during or after remediation. MANDIANT refers to this as remediating in the "strike zone."

To successfully address the APT during a protracted event, superior detection capability is needed because you cannot change end user behavior; and if you truly find nirvana and prevent a cyber security incident, then you will introduce a personnel security challenge — or simply escalate the sophistication of the cyber incidents.

The best chance organizations have for fighting the APT is improving how they perform host- and network-based detection and enhancing their capability to effectively respond at scale across their enterprise. Most organizations struggle to detect real incidents. Relying solely on automated security does not increase the likelihood an organization will be targeted, but it does increase the likelihood it will be in a state of continual compromise. A key in helping "define the win" in any organization is trained personnel. As the APT shifts their tactics and strategies it is not as simple as deploying a "conficker" signature and "blocking at the perimeter". Trained security personnel who can quickly identify threats and build their own lists of indicators of compromises will be the best defensive weapon a prepared organization can have.

Organizations must also implement tighter internal security controls and, at a minimum, follow industry compliance guidelines. Most compliance guidelines recommend implementing solid, basic information security measures. While following these guidelines is no guarantee against an intrusion, having good security practices in place can aid in slowing down the APT once a breach occurs. Logging will be more robust; servers and workstations will be more secure; user credentials will be harder to crack and security appliances will be strategically distributed. As a result, responders will have much better information available to aid in detecting and remediating an APT attack.

Organizations that take information security seriously and move beyond just meeting compliance guidelines have the best chance of detecting and remediating the APT. Most organizations realize that achieving a strong, grade-A security posture is costly, but this is a case where bigger upfront costs on the right personnel, processes and technology can save time and money down the road. Organizations that make an investment in computer security will be better positioned to detect and remediate APT intrusions within hours and days, not weeks or months.

The next page presents an initial checklist that articulates information you will need both prior to and during an investigation. Collecting this information before an event has occurred gives you a head start in determining the best course of action once a compromise has been confirmed. Additionally, maintaining this information can assist in scoping an incident more efficiently. This checklist is meant to be a minimum standard and is not an all-inclusive list.

INITIAL DATA COMPILATION CHECKLIST

TASK
Develop Overview of Enterprise Infrastructure
❑ Compile a list of all DNS & DHCP servers.
❑ Compile a list of all Internet points of presence.
❑ Compile a list of all VPN concentrators.
❑ Compile a list of all Windows domains.
❑ Create a network diagram of the core network infrastructure.
❑ Compile the rule set of the core Firewall(s).
❑ Compile all GPO(s) responsible for setting the level of logging enabled on Windows workstations and servers for both failed and successful log-on attempts.
❑ Compile information related to any centralized logging currently in place.
Centralize the Storage and Analysis of Key Logs
❑ Integrate key logs (such as firewall, VPN, DHCP, DNS, etc) into a Security Information Event Management (SIEM) solution.
❑ If a SIEM is not in place, store key logs in a central location.
Implement Robust Logging
❑ Implement logging on all DNS servers to include queried domain name and systems performing the query to centralized logging utility.
❑ Implement logging on all DHCP servers to log hostname and IP address pairing and date/time information to centralized logging utility.
❑ Implement logging on all VPN concentrators to log hostname and IP address pairing and date/time information to centralized logging utility.
❑ Ensure Windows application, system, and security event logs are appropriately sized and logging locally.
❑ Ensure both Success and Failure audits are being logged for all systems.
❑ Increase the storage of key logs (such as VPN, Firewall, DNS) to ensure they are not overwritten.
❑ Configure anti-virus and/or host-based intrusion prevention to log to centralized logging utility.
❑ Implement logging on all internal web proxy servers to log date/time, hostname and IP address pairing, and URL browsed information to centralized logging utility.
❑ Implement logging of all traffic on all firewalls to centralized logging utility. Note that packet contents are not required.

SECTION V

CONCLUSION

The APT isn't just a government problem; it isn't just a defense contractor problem; and it isn't just a military problem. The APT is everyone's problem. No target is too small, or too obscure, or too well-defended. No organization is too large, too well-known, or too vulnerable. It's not spy-versus-spy espionage. It's spy-versus-everyone.

Classic "prevent and detect" techniques do not effectively counter the APT. They can easily defeat normal defenses. The enemy successfully evades anti-virus software, network intrusion detection and underequipped incident responders. They use sophisticated techniques to conceal their presence: hiding malware on their target's own hosts and exfiltrating data in its own network traffic.

The APT's goals are twofold. Of course they steal information to achieve economic, political and strategic advantage. But more importantly, they establish and maintain an occupying force in their target's environment, a force they can call upon at any time. When the APT wants additional data from a target, they don't need to re-establish a presence. They simply call on their existing assets, locate, steal and exfiltrate the data they need.

You must accept two hard truths.

One, this is a war of attrition against an enemy with extensive resources. It is a long fight, one that never ends. You will never declare victory.

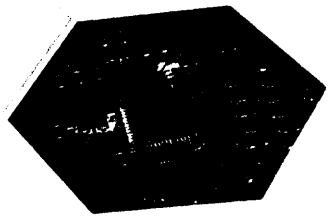
Two, panicked reactions tend to cause more harm than good. When you find an infected system, you should not clean it immediately. You must wait until you reach the "strike zone" and then swing effectively at the enemy. Until then, you need to employ a customized response strategy that meets the needs of your organization. This may include allowing the attackers to continue to operate as though you were unaware of their presence.

You must also raise your capabilities to match your attackers' capabilities.

You have to be able to look for complex signs of compromise; integrate host-based and network-based information; and go far beyond simple anti-virus and network intrusion detection. You need to look inside packets, files, e-mail — and even the live memory of systems that are still running.

This M-Trends report is the first in a series produced by MANDIANT. Future M-Trends reports will focus on what works for APT remediation and how to effectively posture your organization to defend against the Advanced Persistent Threat.

We hope you have found this report useful. If you'd like to discuss it, please contact us. You can reach us by telephone at +1 703 683 3141, or send e-mail to info@mandiant.com. For even more information about MANDIANT, including how to contact us in an emergency, visit our web site at **www.mandiant.com**.



APPENDIX A

GLOSSARY OF TERMS

API: API is an acronym that stands for application programming interface. Use of an API typically enables software programs to interact with other types of software programs.

Base64: Base64 is a method of encoding binary data by into an alphabet consisting of 64 characters.

Beacon: A beacon refers to malicious software that connects to a remote IP address that is likely controlled by the attackers. Beacons typically let the attacker know a system is ready and available to accept commands, however no commands are actually passed to the compromised system.

Cabinet: A cabinet is a single file, usually with a .cab extension, that stores compressed files in a file library. The cabinet format is an efficient way to package multiple files.

CHM file: A CHM file is a "Compiled HTML Microsoft Help File", that is displayed when a user clicks on the Help feature of any Microsoft application. CHM files can drop and execute an embedded executable on a user's system. As a result, this is a popular technique used by the APT to gain access to a system. Recently Microsoft disabled the ability to open. CHM files via Internet Explorer, but the APT has worked around this by embedding. CHM files inside of ZIP files so the user opens them locally.

Data harvesting: Data harvesting occurs when the APT searches for specific data to exfiltrate from the host. Data is usually e-mail or other files of interest. Data is usually archived using RAR.

Exfiltrate: Exfiltrate is used to describe data that has been removed from a victim network or host and transferred to a third-party location.

First stage malware: Refers to the first stage of malware that contains several stages of execution in order to work successfully.

Host-based indicator: Host- and network-based technical indicators refer to previously identified indicators of intrusion activity. Host-based indicators are designed to detect anomalous activity within information collected from individual systems.

Implant: A common hacker term used to describe a piece of malware that is active and persistent across system reboots and adjustments. Generally, most APT backdoors would be considered implants due to their need to consistently beacon or connect out and remain active despite what happens to the system. Malware sniffers would also be considered implants due to their need to continually collect network data. The APT uses sniffers routinely to collect valid credentials, such as proxy authentication credentials.

Indicators of compromise: Indicators of Compromise are collected from host- and network-based signatures used to identify APT related activity. These indicators are in many cases the only way to identify APT activity since regular anti-virus or intrusion detection systems fail to identify the APT presence.

Lateral network movement: This is a technique used by an attacker to move to one system to another within the same network segment. Usually the movement does not involve going through additional network security measures, as the systems are generally considered trusted.

Malware packing: Malware packing is a technique to compress and possibly encrypt a program to prevent easy detection and reverse engineering. Many packing techniques are custom-written which makes analysis challenging.

MANDIANT Intelligent Response™ (MIR): Performs complex inspection of each system in an enterprise, looking for hundreds of specific, host-based indicators of compromise.

Microsoft cabinet file: A cabinet is a single file, usually with a .cab extension, that stores compressed files in a file library. The cabinet format is an efficient way to package multiple files because compression is performed across file boundaries, which significantly improves the compression ratio.

Network-based Indicator: Host- and network-based technical indicators refer to previously identified indicators of intrusion activity. Network-based indicators are designed to detect anomalous activity within network packets going either to or from systems on the network.

Pass-the-hash: A technique to use the compromised, encrypted credentials of a higher-privileged user (typically a local host or domain administrative account) to escalate the attacker's privilege level. The technique takes advantage of the fact that the Local Security Authority validates the cryptographic credentials of the user and does not act on the user's password.

Process injection: Process injection inserts executable code into another running process, which helps conceal the course of malicious behavior by executing additional code through a known and trusted process.

Proxy server: A proxy server is a server (a computer system or an application program) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server. The proxy server evaluates the request according to its filtering rules.

RAR: RAR is an archiving method that usually is able to compress slightly better than the comparable .zip method. As a result, the APT has used the .rar archive in many of its data harvesting activities.

Registry modifications: Registry modification for malware usually takes place to store configuration parameters for a piece of malware or to enable a malware persistence mechanism through services or the "run at boot" registry keys.

Scheduled services: Scheduled services are processes that activate at system boot or at a specific time configured through a scheduled job. Malware uses scheduled services as a persistence mechanism to ensure the code is executed after the system is rebooted.

SSL: Secure Sockets Layer (SSL) are cryptographic protocols that provide security for communications over networks such as the Internet. The APT would use SSL enabled web-traffic to allow malware to communicate outside the network. Since SSL is encrypted and is used frequently on many websites, it provides an excellent way to cover SSL enabled command and control channels.

Sweep: Using MANDIANT Intelligent Response to look for APT host- and network-based indicators across an enterprise environment.

www.mandiant.com