

2013 THREAT REPORT



attack the security gap™

CONTENTS

INTRODUCTION	1
OUTSIDE IN	4
“X” MARKS THE SPOT	6
ONCE A TARGET ALWAYS A TARGET	8
OLD SCHOOL DRIVE-BYS WITH A TWIST	10
CASE STUDY 1: Global Financial Institution	12
CASE STUDY 2: Energy Company	14
CASE STUDY 3: Banking Industry.	17
BEST PRACTICES EMPLOYED BY TARGETED ORGANIZATIONS	19
APT1	20
CONCLUSION.	27
END NOTES	28



INTRODUCTION

There is no such thing as perfect security. Advances in technology will always outpace our ability to effectively secure our networks from attackers. At Mandiant, we call this the “Security Gap.” There is no technical or legislative solution that can eliminate this gap. Security breaches are inevitable because determined attackers will always find a way through the gap. This sounds disparaging, but it is not new information. Seasoned security professionals have been aware of the security gap throughout their careers.

While the problem is not going away any time soon, Mandiant saw companies make significant progress in their ability to Attack the Security Gap™ over the past year. In 2012, 37% of the organizations we responded to discovered the intrusion themselves, versus just 6% of the organizations we helped in 2011. We also saw more than a 40% improvement in the median time an attacker was present on a victim network — down to 243 days from 416 days in 2011. We note, however, that this downward shift in the median was accompanied by a higher mean days of compromise. In other words, more organizations are doing a better job of proactively identifying problems, but there are still outliers who are compromised for several years before they detect they are compromised.

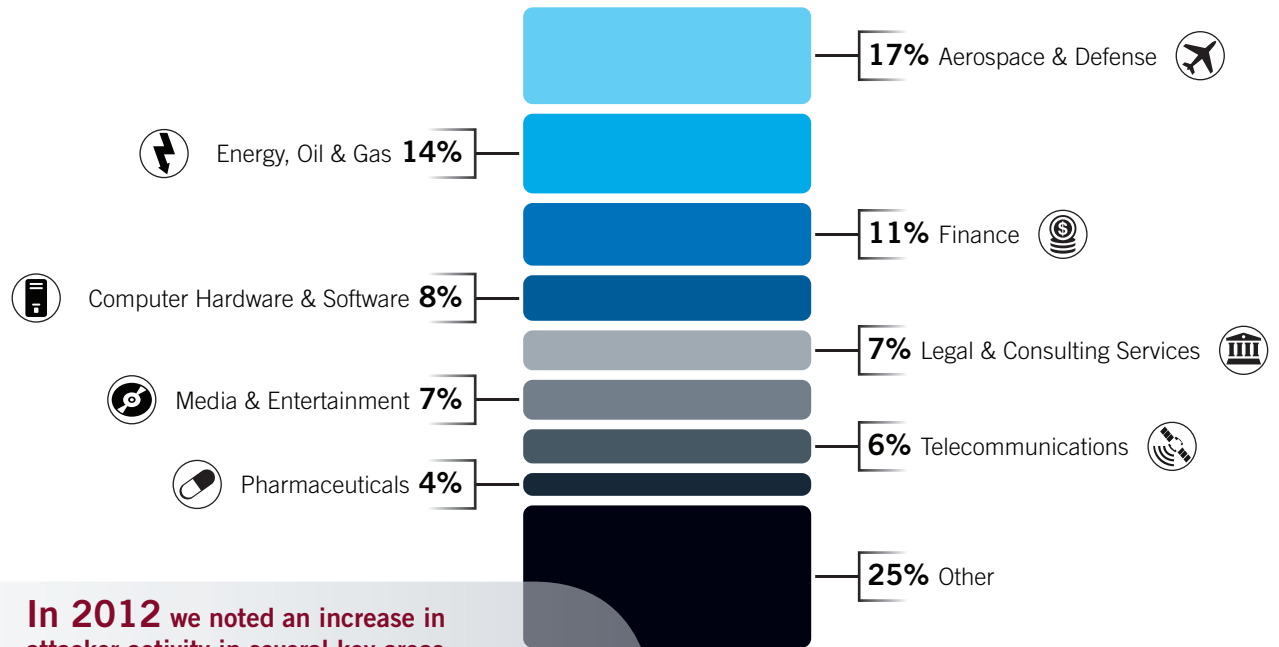
In this M-Trends report, we present two different perspectives. First, a look at the tactics that the adversary is using to compromise organizations: the subversion of IT contractors, the extensive reconnaissance used by attackers, the persistent re-compromise of valuable targets, and strategic Web compromises. These four trends are about the business side of exploitation.

We also provide an attacker’s perspective on a compromise with an overview of the APT1 threat actor, and a link to over 3,000 technical indicators that Mandiant is providing to the community.

Effectively attacking the security gap requires the best people, technology, and threat intelligence possible. It also requires collaboration and information sharing across our industry. It is our hope that the 2013 M-Trends and corresponding Web content can help your organization start to close this gap.

VICTIMS BY THE NUMBERS

Industries Being Targeted by Advanced Attackers



In 2012 we noted an increase in attacker activity in several key areas:

- ↑ Media & Entertainment — up from 2% to 7%
- ↑ Pharmaceuticals — up from 1% to 4%
- ↑ Finance — up from 7% to 11 %

How Compromises Are Being Detected



This **M-Trends** focuses on Mandiant's observations while responding to targeted attacks over the last year. During our investigations, we noted **4 trends**.

Time from Earliest Evidence of Compromise to Discovery of Compromise



1 OUTSIDE IN

Attackers are increasingly using outsourced service providers as a means to gain access to their victims.



2 "X" MARKS THE SPOT

Attackers are using comprehensive network reconnaissance to help them navigate victims' networks faster and more effectively.



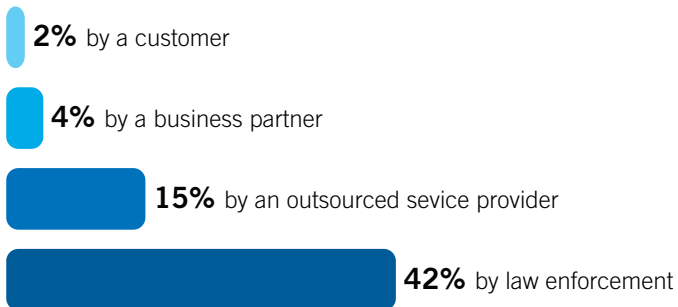
3 ONCE A TARGET ALWAYS A TARGET

Advanced Persistent Threat (APT) attackers¹ continue to target industries that are strategic to their growth including aerospace, computer software, high-tech manufacturing, and energy.



4 OLD SCHOOL DRIVE-BYS WITH A TWIST

Targeted attackers are adapting Internet drive-by attacks and stepping them up a notch to compromise victims and gain a foothold in their networks.





1

OUTSIDE IN

Attackers are increasingly using outsourced service providers as a means to gain access to their victims.

Outside vendors and business partners have access to organizations' networks like never before. In 2012, companies spent \$134 billion on outsourcing business processes such as finance, accounting, HR, and procurement.² Combine that with the estimated \$252 billion organizations spent on IT outsourcing in 2012³ and it adds up to a lot of organizations allowing outside vendors unfettered access to large portions of their networks.

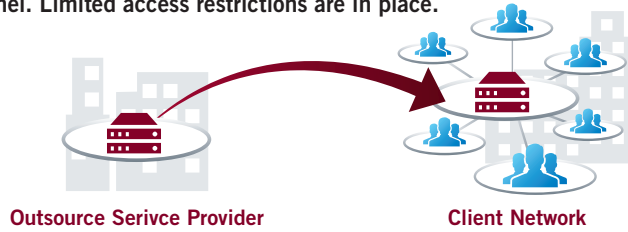
Advanced attack groups are increasingly taking advantage of outsourcing relationships to gain access to the organizations they are targeting. During our investigations in 2012, we found an increase in the number of outsourced and managed service providers who were compromised and used as a primary access point for attackers to gain entry to their victims' networks. We have worked with clients who were both the compromised outsourced service provider and the compromised clients who employ these services. In many instances, the attackers initially gained access to the service provider solely as a means to find a way into their real target — the client of the service provider. In those cases, we have seen the attackers compromise the first victim — the outsourced service provider — gather the intelligence they need to facilitate their compromise of the second victim, and then lay dormant at the first victim for months or even years, only accessing backdoors at those companies if they need to regain access to the second victim.

In other cases, we have seen examples where contracted service providers have been the primary target. For example, during one of our investigations we found evidence that attackers gained access to a large defense contractor who, as part of their services portfolio, provided IT support and managed services for a number of smaller defense contractors. We found these attackers accessed the networks of the smaller companies through the connections they shared with the vendor. Meanwhile, other divisions of the service provider produced products and performed services which were of interest to the attackers who stole email and other files related to these products and services.

Advanced attack groups are increasingly taking advantage of outsourcing relationships to gain access to the organizations they are targeting.

COMPROMISE VIA OUTSOURCED SERVICE PROVIDER (OSP)

- 1** OSP has access to client network through site-to-site VPN tunnel. Limited access restrictions are in place.



- 2** Attacker compromises OSP.



- 3** Attacker leverages site-to-site VPN tunnel and compromises client from OSP network.



THE TAKEAWAY Your network is only as secure as your outsourced service provider. Make sure your organization understands the security posture of these providers, and apply as stringent policies to their access as you would to your own employees.

2




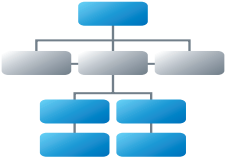


“X” MARKS THE SPOT


Attackers are using comprehensive network reconnaissance to help them navigate victims’ networks faster and more effectively.

Attackers can steal the data they want faster when they know where to look for it. While basic reconnaissance of victim networks is nothing new, over the last year we have seen evidence of attackers expanding the type of reconnaissance activities they perform and utilizing more sophisticated tools and tactics to map victims’ networks. In addition to network mapping, we saw multiple instances where the first documents the attackers stole were related to network infrastructure, processing methodologies and payment card industry (PCI) audit data. The attackers also took various system administration guides to identify human targets and to further scope the victim networks. We have also seen instances where the attackers opened native Microsoft tools (such as dns.msc) to gather the reconnaissance data they needed.

With this information in hand, the attackers identified network and system misconfigurations which they exploited to gain greater access within the victim network. In all of these cases, having intimate knowledge of the network topology allowed the attackers faster and more direct access to the areas of their victims’ networks that they were trying to compromise. In some instances, attackers sought entry to production environments where they stole intellectual property. In other cases, they were looking to identify network resources the victim shared with other organizations that were also on the attacker’s target list.

ITEMS ATTACKERS STEAL DURING THE RECONNAISSANCE PHASE OF AN INTRUSION

ITEM STOLEN	HOW THE ATTACKERS USE INFORMATION
 <p>Network Infrastructure Documentation Including Schematics and Configuration Files</p>	<p>Understand firewall and other IDS configurations and where vulnerabilities that can be exploited exist.</p>
 <p>Organization Chart</p>	<p>Establish individuals to target in spear-phishing campaigns or to target for email and data theft.</p>
 <p>Systems Documentation</p>	<p>Identify where targeted systems existing within a victim network.</p>
 <p>VPN Configuration Files</p>	<p>Identify what VPN users have access to within a victim's network and target VPN credential data to steal.</p>

 **THE TAKEAWAY** Information about your networks, systems, and organization provide a road map for attackers to quickly find what they are searching for. Apply the appropriate data classifications to such information and secure it accordingly.



ONCE A TARGET ALWAYS A TARGET

Advanced Persistent Threat (APT) attackers continue to target industries that are strategic to their growth including aerospace, computer software, high-tech manufacturing, and energy.

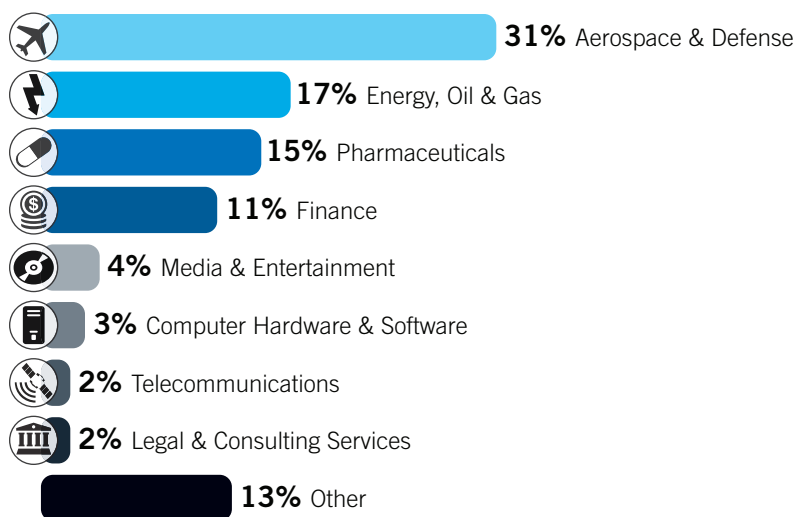
Mandiant once again observed a relationship between the strategic priorities of the People's Republic of China (PRC), the operations of PRC state-owned enterprises (SOEs), and data stolen through cyber intrusions from a wide variety of clients and industries.

Attackers choose their targets for different reasons. Financially motivated attackers seek victims who they can easily gain access to in order to steal money or credit/debit card numbers. Attackers conducting economic espionage, such as the APT, are motivated by economic gain and their victims are often directly correlated with their national interest. In 2012, Mandiant once again observed a relationship between the strategic priorities of the People's Republic of China (PRC), the operations of PRC state-owned enterprises (SOEs), and data stolen through cyber intrusions from a wide variety of clients and industries. Mandiant has also identified a larger number of situations where organizations that were initially compromised by the APT were repeatedly attacked once those organizations had eliminated the attackers from their network. Many of our investigations revealed a number of these organizations were targeted by more than one attack group, sometimes in succession.

Of the clients Mandiant responded to in 2012, 38% of them were attacked again once the original incident was remediated.

In economic espionage cases, we witnessed coordinated and continued APT activity against nearly all of the industries we work in. In particular, a large number of repeated attacks were lodged against companies in the aerospace, energy and pharmaceutical industries. Of the total cases we investigated in 2012, we saw attackers lodge over one thousand attempts to regain entry to former victims.

REPEATED ATTACKS BY INDUSTRY, 2012



THE TAKEAWAY

Attackers with an objective of economic espionage have specific goals and will return until their mission is complete. Treat incident detection and response as a consistent business process — not just something you do reactively. Constant vigilance and rapid response is necessary to keep an organization secure.

4



OLD SCHOOL DRIVE-BYS WITH A TWIST

Targeted attackers are adapting Internet drive-by attacks and stepping them up a notch to compromise victims and gain a foothold in their networks.

At Mandiant, we have seen attackers perpetrate strategic Web compromise⁴ attacks as a means of gaining entry to a victim network. Unlike Web compromises of old, the cases Mandiant observed over the past year were far more targeted than typical Internet drive-by attacks.

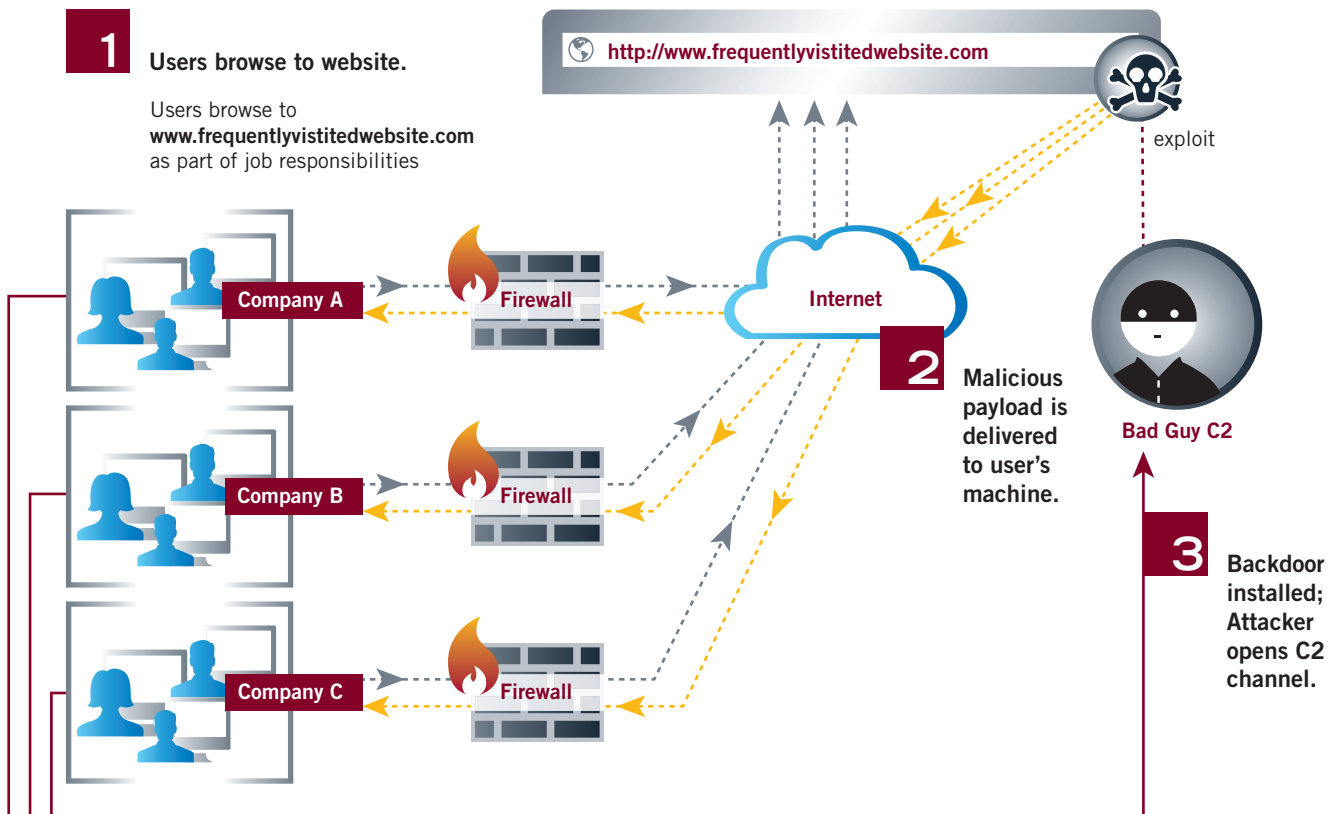
Attackers have long used spear phishing and other social engineering tactics to entice users to click on malicious files they receive via email. They send the target a well-crafted email with an attachment, the target clicks on the attachment, their machine becomes compromised, and the attacker gains access to the victim's network. As the use of this well-known technique has become more prevalent, technologies have been developed to combat these attacks — and they continue to improve.

In response, Mandiant has seen attackers shift tactics by placing exploits on websites they know are frequently browsed by users in targeted organizations. The targeted users travel to the compromised website as part of their daily operations and when they click on the compromised website, malware is installed on their machines. Once installed, the malware collects usernames, passwords, browser cookies and the computer name of the system being used.

By using these strategic Web compromise attacks, the attacker is able to secure access to multiple individuals' systems within several targeted companies without having to send a single email; effectively enabling the attacker to defeat anti-phishing technology.

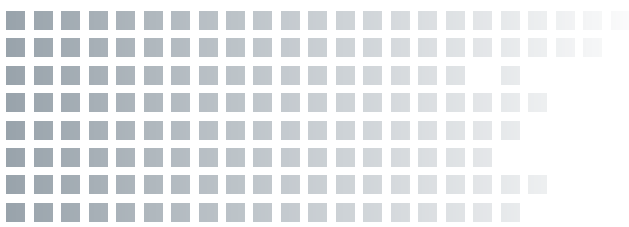
Exploiting Web servers used to be indicative of crimes of opportunity rather than targeted, pre-meditated attacks. However, in 2012, Mandiant witnessed compromised Web servers being used as an initial means of access by both criminal threat actors and attackers conducting economic espionage, such as the APT.

HOW STRATEGIC WEB COMPROMISE WORKS



THE TAKEAWAY

Advanced attackers are no longer relying solely on vulnerable Web applications and phishing emails to gain access to targeted companies. They are targeting individuals, conducting reconnaissance, and are willing to lie in wait while a user acts to compromise themselves. Ensure that your security operations incorporate data from intelligence services to identify when domains are compromised — and use this information to evaluate proxy or DNS logs for signs of access to these sites.



CASE STUDY 1:

Global Financial Institution

TREND



2

Mandiant was contacted in early 2012 to investigate a suspected compromise at a global financial institution.

In our experience, criminal intrusions are typically detected more quickly than corporate espionage intrusions because they involve the theft of credit/debit card numbers or money. In addition, the financial industry effectively uses a number of anti-fraud detection mechanisms. In this case, the client detected the compromise while reviewing IIS Web logs. Through review of the Web logs, the victim determined that an attacker had exploited a vulnerability within a Web application and created tools locally on the Web server. By the time the company discovered the breach, validated the presence of the tools and escalated the issue, it was too late to stop the attack. The attacker had already created multiple backdoors throughout the environment and was no longer accessing the victim network through the compromised Web server.

The attackers stole a large amount of data related to network infrastructure, processing methodologies and systems documentation.

The attackers stole a large amount of data related to network infrastructure, processing methodologies and systems documentation. From this information, they were able to gain a thorough understanding of the victim's network and its systems, including which access controls were in place and where critical data was stored. The attackers leveraged this knowledge to:

- » Determine which users interacted regularly with important systems;
- » Target these users to obtain their credentials;
- » Establish which systems had unfettered access to the Internet; and
- » Identify misconfigurations in the victim's network.

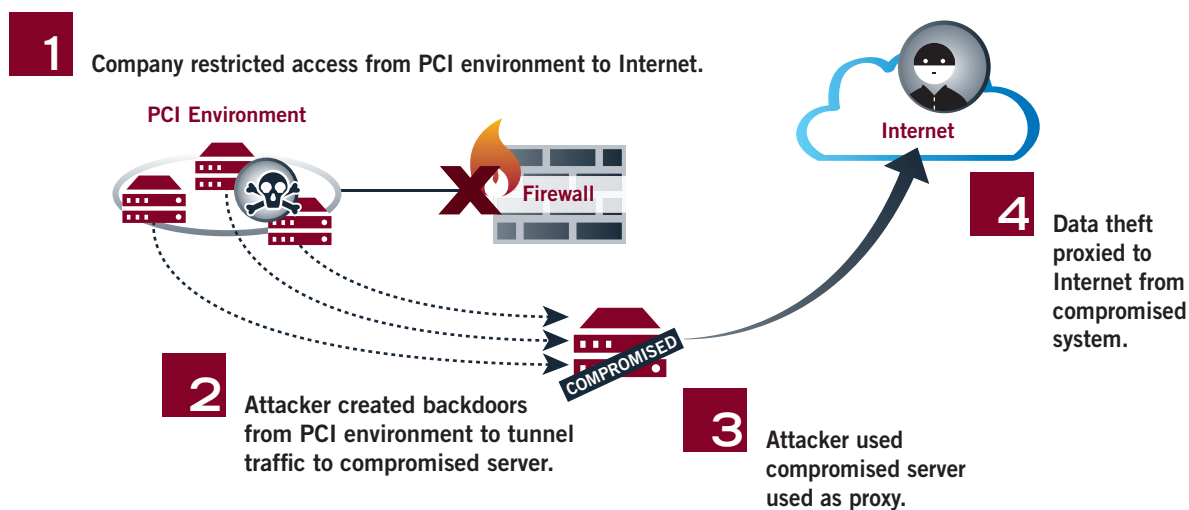
This particular group of attackers took advantage of multiple vulnerabilities and misconfigurations to perpetrate this crime. Each vulnerability and misconfiguration appeared to present a small risk on its own. However, when grouped together they allowed the attacker to compromise the organization. The attacker took advantage of a vulnerable Web application to gain access to the DMZ and move laterally throughout the DMZ until they gained access to a database. Next, the attacker used the database connection to gain access to the internal environment and moved laterally through the environment gaining elevated privileges and performing reconnaissance. Ultimately, they identified a jump server that provided them access to the card processing environment.

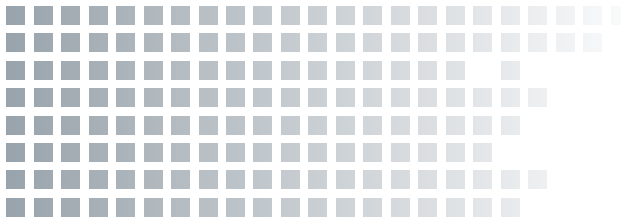
The card processing environment restricted outbound access to the Internet except where it was critical for business functionality. This hindered the attacker's attempts to steal data directly from the card processing environment. The attackers implemented a proxy infrastructure within the environment to route their connectivity from the Internet to the card processing environment and back so they could steal data. The attackers then configured their backdoors to communicate with specific C2 servers, but routed traffic through proxy utilities deployed on some compromised systems. The proxy utilities were configured to communicate with C2 servers that were often different from the destination address specified by the original backdoors. This caused some confusion during the investigation as to which C2 servers were actually being used. Analysis of the malware determined that a command line option specified whether the proxy utilities would send data to the pre-configured C2 servers or to the C2 servers specified by the backdoors.

One of the backdoors the attacker used leveraged IPv4 DNS A records for C2 (the malware also had the ability to leverage IPv6 DNS AAAA records). The subdomains were automatically generated and random, which made them difficult to detect and block. This technique was stealthy because most companies do not monitor their DNS traffic. The attacker chose to leverage Windows Scheduled Tasks to maintain persistence for this malware, which was odd because it allowed for easy detection of the malware.

Although the investigation was made more difficult because of the way the various pieces of malware worked together, Mandiant employed traditional investigative doctrine to determine where the attacker had deployed malware or had accessed systems. Once we felt we understood the compromise, we assisted the client with a remediation effort that removed the attacker's access from the environment, plugged the vulnerabilities the attacker leveraged to gain access, improved the client's visibility, and improved their security posture such that a future attack had a smaller chance of success.

ATTACKER PLACED TUNNELING MALWARE ON COMPROMISED SERVER





CASE STUDY 2:

Energy Company



1

In mid-2012, a global energy company requested that Mandiant perform a threat assessment of their network to identify if attackers were active within their IT environment. The company had reason to believe they were compromised and were looking to confirm if that was the case. If so, the company wanted to identify what data the attackers had stolen.



2

Over the course of multiple investigations related to this intrusion, Mandiant encountered three organizations compromised by the same attack groups. Two of these companies — Company A and Company B had a partnership arrangement related to renewable energy projects they were jointly working on. The third organization — Company O — was an outsourced service provider who provided managed services to Company B, but who had no relationship to Company A.



3

As our investigation unfolded, we learned these attackers were determined to maintain access to Company B's network. When our investigation was complete, we determined the attackers had compromised both Company A and Company O in an attempt to gain access to Company B.



4

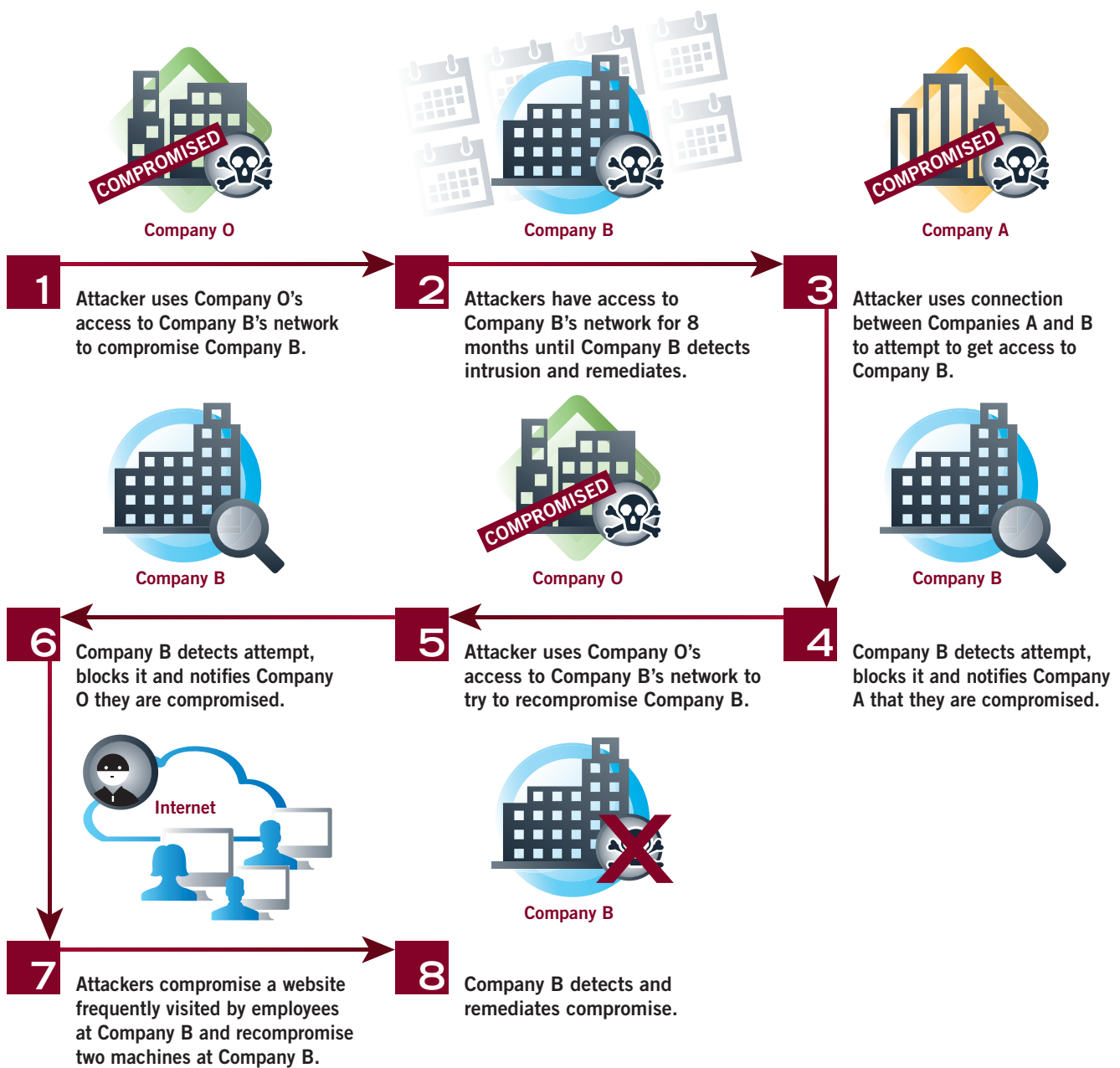
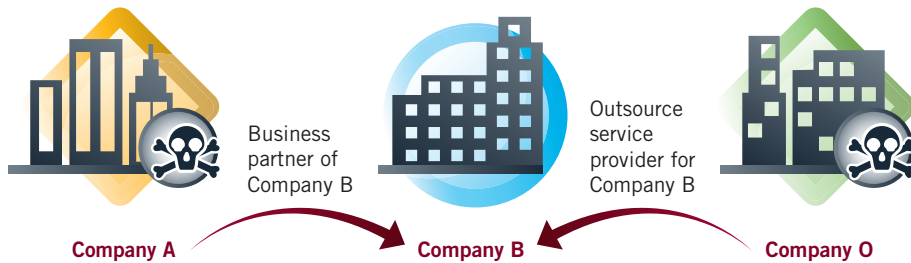
Due to the length of time the attackers were in Company B's network undetected — nearly nine months — we were unable to identify the initial attack vector. However, we did find evidence that Company O was compromised prior to Company B's compromise and believe that the attackers used Company O's access to Company B's network to compromise Company B.

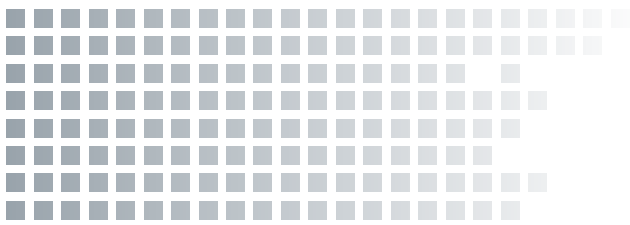
Once inside of Company B's network, the attackers used a combination of traditional backdoor malware, traffic redirectors and legitimate Windows mechanisms in conjunction with stolen user credentials to maintain access, move laterally through the network and access proprietary data. During this time, the attackers were actively stealing data from Company B.

Prior to the attackers' compromise of Company B, they also compromised a partner company, Company A. In Company A's network, the attackers performed reconnaissance activities viewing multiple files related to Company A's network topology, but they never stole any intellectual property. They installed multiple backdoors and then went dormant for approximately 13 months.

RELATIONSHIPS

Attacker is at two places: Company A and Company O





Once Company B detected the attackers, they contacted Mandiant and we worked with them to conduct an investigation of the incident and to perform remediation.

Upon completion of Company B's remediation, the attackers used the backdoors and webshells they installed at Company A and attempted to leverage a network connection between Companies A and B to regain access to Company B's network. We identified the attempts to try and move from Company A into Company B and worked with Company B to block the attacker's access. At this time, Company B notified Company A that Company A was compromised and Company A took a series of steps to block the attacker from further access to its network.

Once Company A started remediating their compromised devices, the attackers were effectively blocked from using the network connection between Companies A and B that they had previously leveraged for access to Company B. However, Company B's outsourced service provider, Company O, was still compromised. Because Company O provided outsourced information technology services to Company B, the attackers performed additional reconnaissance activities at Company O looking at and stealing files related to configuration changes Company B implemented during the remediation of their original incident. Armed with this information, they installed malware designed to circumvent new firewall controls Company B had put in place. Company B detected these attacks, blocked them and notified Company O that Company O was compromised.

At this point the attackers had been removed from Company B and been detected and blocked from Company A and Company O. They were still determined to regain access to Company B. Even though their other avenues of entry had been shut down, they still had information about Company B — knowledge of a website employees at Company B frequented as part of their work at the company. Using this information, the attackers compromised the website and posted a Java exploit on the site. Using this strategic Web compromise technique, the attackers successfully gained entry back into Company B. Company B quickly detected the compromise and remediated.

CASE STUDY 3:

Banking Industry

In late 2012, Mandiant worked with a bank investigating the theft of nearly \$2 million dollars via a fraudulent wire transfer. The bank began investigating the incident after they discovered that unauthorized messages were being sent using a Web-based banking management application. The bank used the application to administer and manage accounts in an online application used by its customers. The customers used the online service to manage their monetary transactions including ACH and wire transfers.

During their internal investigation, the bank identified and deleted a compromised banking management account. They also identified and reset passwords for compromised customer accounts and removed a compromised machine from its network.

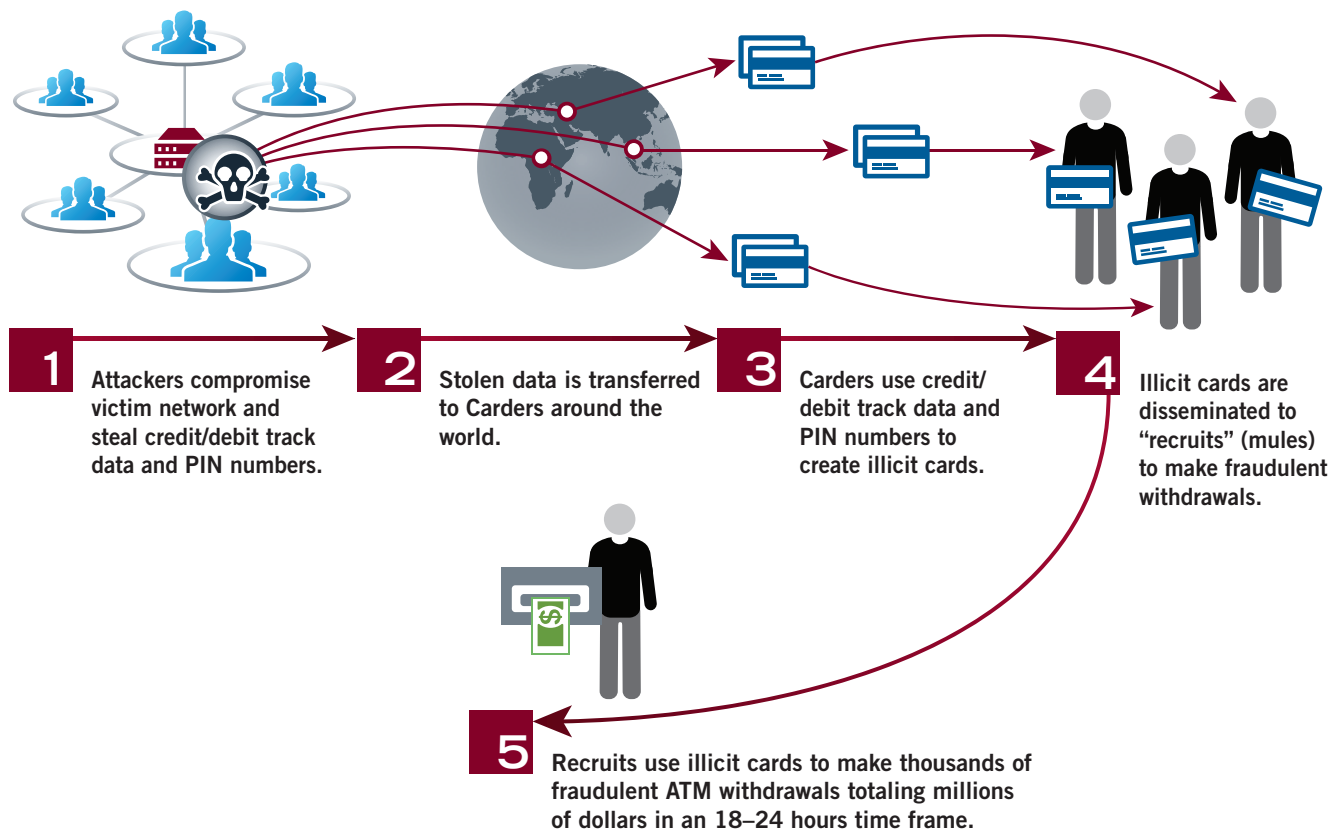
Mandiant was tasked with identifying whether the incident was ongoing and what the initial method of compromise was. The bank also needed to understand how the attackers were able to access the banking management application, determine the length of exposure and identify the total loss.

We performed forensic analysis on the machine the bank had taken offline and established that it had been compromised by a Java vulnerability installed when the user visited a local news outlet's website. Once the user visited the website, they were unknowingly redirected to a malicious Web server hosting the Java exploit. The exploit installed a backdoor on the victim's system and harvested credentials from the user's browser. The installed malware also included functionality to steal browser cookies and certificates, transfer files in and out of the environment, execute arbitrary programs and implement a SOCKS5 proxy.

The bank had IP whitelisting in place and access to the externally-hosted banking management application was restricted to the bank's external IP address. However, the attacker's use of a modified SOCKS5 proxy allowed them to tunnel traffic through the compromised system and to access the application.



HOW A "MONEY MULE" INFRASTRUCTURE OPERATES



We saw multiple instances of this type of attack throughout 2012. The attackers stole large sums of money in different ways, depending on the type of credentials they were able to obtain.

The attacker targeted banking employees who had active credentials to the banking management application and other applications with access to debit card and prepaid card numbers. Once the credentials were identified, the attacker used them to log into the banking management application and identify bank accounts with large sums of money. They then disabled two-factor authentication and reset the passwords for the targeted accounts. Once they reset the passwords, they logged into the online application as a targeted account holder and transferred money from the targeted accounts to an attacker-owned bank account.

We saw multiple instances of this type of attack throughout 2012. The attackers stole large sums of money in different ways, depending on the type of credentials they were able to obtain. In some instances they created wire transfers, in other instances they obtained debit card and PIN numbers and used a money mule infrastructure to withdraw the money. In all of the cases, the attackers compromised a local news outlet's website, hosted variants of the same Java exploit and leveraged the knowledge that bank employees would visit the site to compromise the banks' networks.

BEST PRACTICES EMPLOYED BY TARGETED ORGANIZATIONS

Over the years we have focused on how attackers shift and revise their tactics to maintain and regain access to targeted organizations. Organizations that successfully combat digital threats treat incident response as a continuous business process. They understand that intruders will eventually compromise the enterprise. Organizations win if they disrupt intruders before they can complete their missions. Top enterprises balance people, products, process, and partnerships to meet this goal. Below are four best practices we recommend to help these organizations better improve their security posture and attack the security gap.



1 First, high-performing organizations staff computer incident response teams (CIRTs) who successfully detect, respond to, and contain intruders. While bigger organizations have the budget and resources to build larger teams, even the smallest organizations hire at least one dedicated incident handler. The incident handler is responsible for hunting for intruders in the network. While the rest of the security or IT team plans for, and tries to resist compromise, the incident handler maintains eternal vigilance through detection and response operations.



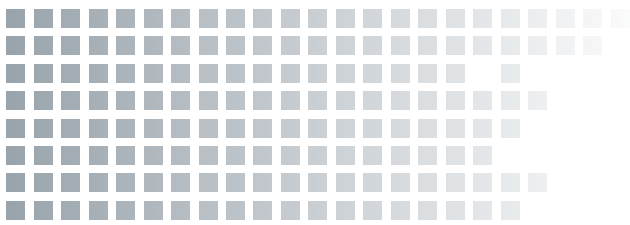
2 Second, successful organizations equip their CIRTs with tools that collect and analyze data from the network, computer, and applications. Top-end CIRTs use network security monitoring methodologies to gather and interpret full content, extracted content, session, transaction, statistical, meta, and alert data from traffic on the wire. They use host-centric tools to sweep for Indicators of Compromise (IOCs) on all endpoints and perform live response actions on suspected victims. They aggregate and index log data from applications, fulfilling security, compliance, and IT duties. These analytics platforms facilitate hunting by integrating advanced algorithms and heuristics. Organizations rely on these tools to accelerate their incident responders, not replace them.



3 Third, industry-leading CIRTs understand that incident detection, response, and containment means attacking the security gap on a *daily* basis. Security incident response management is an active process that requires constant vigilance and well-understood roles and responsibilities. CIRTs work with management, IT, risk, legal, human resources, and other teams to define expectations for IR work and define key metrics for success. The best CIRTs count and classify incidents, then measure the time from detection to response. The best teams strive to complete these tasks in one hour or less. They only achieve this level of performance by having thorough incident response plans, backed by exercises and tools that manage the IR process.



4 Fourth, top CIRTs partner with a variety of parties for mutual benefit and defense. CIRTs work with industry peers and teams from similar industries to share threat data in machine readable format, such as OpenIOC. CIRTs contract with trusted vendors who supply actionable intelligence, including IOCs and more comprehensive threat reporting. These teams also enlist the help of third parties to periodically assess their networks to find intruders who may have evaded detection. These partner organizations use onsite threat assessment tools (network, host, and application) and cloud platforms to help organizations uncover hidden threats. CIRTs also participate in industry conferences and associations such as MIRcon and the Forum of Incident Response and Security Teams (FIRST).



APT1

Exposing One of China's Cyber Espionage Units

Since 2004, Mandiant has investigated computer security breaches at hundreds of organizations around the world. The majority of these security breaches are attributed to advanced threat actors referred to as the “Advanced Persistent Threat” (APT). We first published details about the APT in our January 2010 M-Trends report. As we stated in the report, our position was that “The Chinese government may authorize this activity, but there’s no way to determine the extent of its involvement.” Now, three years later, we have the evidence required to change our assessment. The details we have analyzed during hundreds of investigations convince us that the groups conducting these activities are based primarily in China and that the Chinese Government is aware of them.⁵



The following pages include the executive summary to Mandiant’s comprehensive report on the cyber espionage threat group APT1.

The full report is available at www.mandiant.com/apt1.

Mandiant continues to track dozens of APT groups around the world; however, this report is focused on the most prolific of these groups. We refer to this group as “APT1” and it is one of more than 20 APT groups with origins in China. APT1 is a single organization of operators that has conducted a cyber espionage campaign against a broad range of victims since at least 2006. From our observations, it is one of the most prolific cyber espionage groups in terms of the sheer quantity of information stolen. The scale and impact of APT1’s operations compelled us to write this report.

The activity we have directly observed likely represents only a small fraction of the cyber espionage that APT1 has conducted. Though our visibility of APT1’s activities is incomplete, we have analyzed the group’s intrusions against nearly 150 victims over seven years. From our unique vantage point responding to victims, we tracked APT1 back to four large networks in Shanghai, two of which are allocated directly to the Pudong New Area. We uncovered a substantial amount of APT1’s attack infrastructure, command and control, and modus operandi (tools, tactics, and procedures). In an effort to underscore there are actual individuals behind the keyboard, Mandiant is revealing three personas we have attributed to APT1. These operators, like soldiers, may merely be following orders given to them by others.

Our analysis has led us to conclude that APT1 is likely government-sponsored and one of the most persistent of China’s cyber threat actors. We believe that APT1 is able to wage such a long-running and extensive cyber espionage campaign in large part because it receives direct government support. In seeking to identify the organization behind this activity, our research found that People’s Liberation Army (PLA’s) Unit 61398 is similar to APT1 in its mission, capabilities, and resources. PLA Unit 61398 is also located in precisely the same area from which APT1 activity appears to originate.

KEY FINDINGS

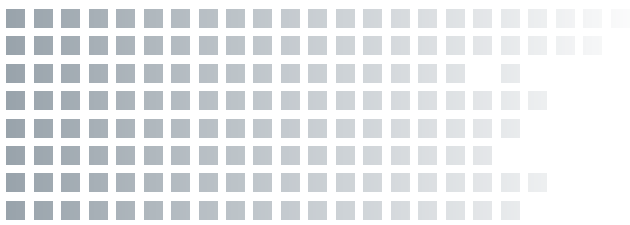
APT1 is believed to be the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department (总参三部二局), which is most commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398 (61398部队).

- » The nature of "Unit 61398's" work is considered by China to be a state secret; however, we believe it engages in harmful "Computer Network Operations."
- » Unit 61398 is partially situated on Datong Road (大同路) in Gaoqiaozen (高桥镇), which is located in the Pudong New Area (浦东新区) of Shanghai (上海). The central building in this compound is a 130,663 square foot facility that is 12 stories high and was built in early 2007.
- » We estimate that Unit 61398 is staffed by hundreds, and perhaps thousands of people based on the size of Unit 61398's physical infrastructure.
- » China Telecom provided special fiber optic communications infrastructure for the unit in the name of national defense.
- » Unit 61398 requires its personnel to be trained in computer security and computer network operations and also requires its personnel to be proficient in the English language.
- » Mandiant has traced APT1's activity to four large networks in Shanghai, two of which serve the Pudong New Area where Unit 61398 is based.

APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously.⁶

- » Since 2006, Mandiant has observed APT1 compromise 141 companies spanning 20 major industries.
- » APT1 has a well-defined attack methodology, honed over years and designed to steal large volumes of valuable intellectual property.
- » Once APT1 has established access, they periodically revisit the victim's network over several months or years and steal broad categories of intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and emails and contact lists from victim organizations' leadership.
- » APT1 uses some tools and techniques that we have not yet observed being used by other groups including two utilities designed to steal email — GETMAIL and MAPIGET.
- » APT1 maintained access to victim networks for an average of 356 days.⁷ The longest time period APT1 maintained access to a victim's network was 1,764 days, or four years and ten months.
- » Among other large-scale thefts of intellectual property, we have observed APT1 stealing 6.5 terabytes of compressed data from a single organization over a ten-month time period.
- » In the first month of 2011, APT1 successfully compromised at least 17 new victims operating in 10 different industries.

Once APT1 has established access, they periodically revisit the victim's network over several months or years and steal broad categories of intellectual property...



The industries APT1 targets match industries that China has identified as strategic to their growth, including four of the seven strategic emerging industries that China identified in its 12th Five Year Plan.

APT1 focuses on compromising organizations across a broad range of industries in English-speaking countries.

- » Of the 141 APT1 victims, 87% of them are headquartered in countries where English is the native language.
- » The industries APT1 targets match industries that China has identified as strategic to their growth, including four of the seven strategic emerging industries that China identified in its 12th Five Year Plan.

APT1 maintains an extensive infrastructure of computer systems around the world.

- » APT1 controls thousands of systems in support of their computer intrusion activities.
- » In the last two years we have observed APT1 establish a minimum of 937 Command and Control (C2) servers hosted on 849 distinct IP addresses in 13 countries. The majority of these 849 unique IP addresses were registered to organizations in China (709), followed by the U.S. (109).
- » In the last three years we have observed APT1 use fully qualified domain names (FQDNs) resolving to 988 unique IP addresses.
- » Over a two-year period (January 2011 to January 2013) we confirmed 1,905 instances of APT1 actors logging into their attack infrastructure from 832 different IP addresses with Remote Desktop, a tool that provides a remote user with an interactive graphical interface to a system.
- » In the last several years we have confirmed 2,551 FQDNs attributed to APT1.

In over 97% of the 1,905 times Mandiant observed APT1 intruders connecting to their attack infrastructure, APT1 used IP addresses registered in Shanghai and systems set to use the Simplified Chinese language.

- » In 1,849 of the 1,905 (97%) of the Remote Desktop sessions APT1 conducted under our observation, the APT1 operator's keyboard layout setting was "Chinese (Simplified) — US Keyboard". Microsoft's Remote Desktop client configures this setting automatically based on the selected language on the client system. Therefore, the APT1 attackers likely have their Microsoft® operating system configured to display Simplified Chinese fonts.
- » 817 of the 832 (98%) IP addresses logging into APT1 controlled systems using Remote Desktop resolved back to China.
- » We observed 767 separate instances in which APT1 intruders used the "HUC Packet Transmit Tool" or HTRAN to communicate between 614 distinct routable IP addresses and their victims' systems using their attack infrastructure. Of the 614 distinct IP addresses used for HTRAN communications:
 - 614 of 614 (100%) were registered in China.
 - 613 (99.8%) were registered to one of four Shanghai net blocks.

The size of APT1's infrastructure implies a large organization with at least dozens, but potentially hundreds of human operators.

- » We conservatively estimate that APT1's current attack infrastructure includes over 1,000 servers.
- » Given the volume, duration and type of attack activity we have observed, APT1 operators would need to be directly supported by linguists, open source researchers, malware authors, industry experts who translate task requests from requestors to the operators, and people who then transmit stolen information to the requestors.
- » APT1 would also need a sizable IT staff dedicated to acquiring and maintaining computer equipment, people who handle finances, facility management, and logistics (e.g., shipping).

In an effort to underscore that there are actual individuals behind the keyboard, Mandiant is revealing three personas that are associated with APT1 activity.

- » The first persona, "UglyGorilla", has been active in computer network operations since October 2004. His activities include registering domains attributed to APT1 and authoring malware used in APT1 campaigns. "UglyGorilla" publicly expressed his interest in China's "cyber troops" in January 2004.
- » The second persona, an actor we call "DOTA", has registered dozens of email accounts used to conduct social engineering and spear phishing attacks in support of APT1 campaigns. "DOTA" used a Shanghai phone number while registering these accounts.
- » We have observed both the "UglyGorilla" persona and the "DOTA" persona using the same shared infrastructure, including FQDNs and IP ranges that we have attributed to APT1.
- » The third persona, who uses the nickname "SuperHard," is the creator or a significant contributor to the AURIGA and BANGAT malware families which we have observed APT1 and other APT groups use. "SuperHard" discloses his location to be the Pudong New Area of Shanghai.

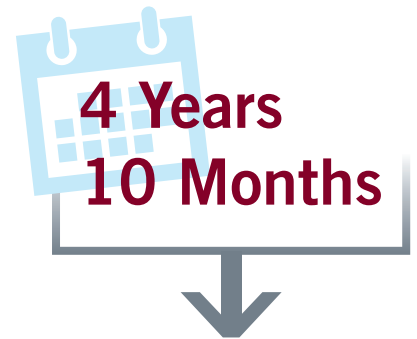
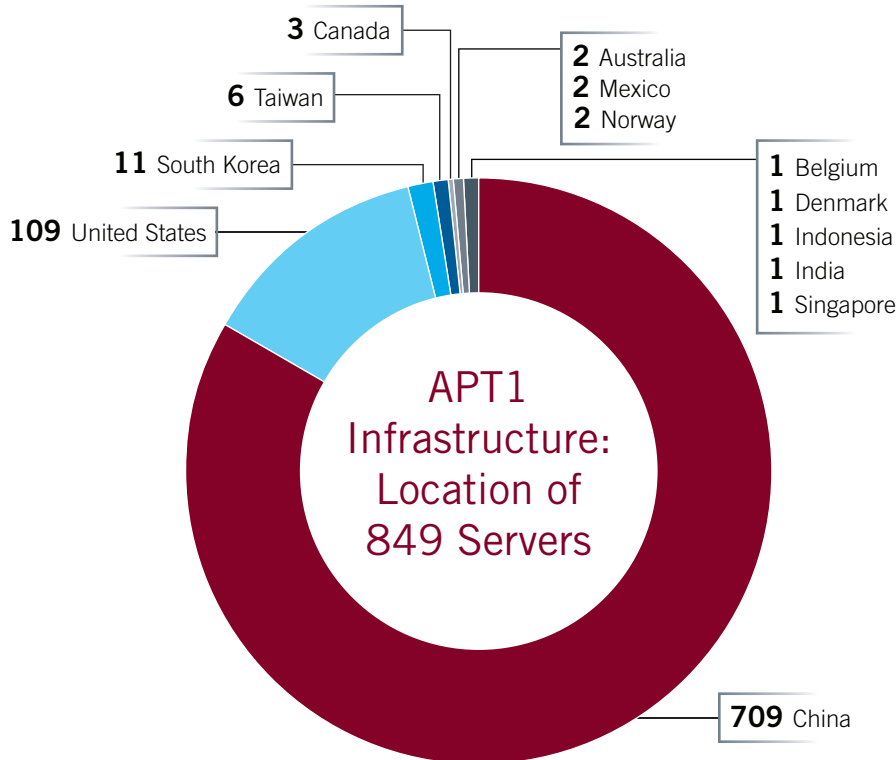
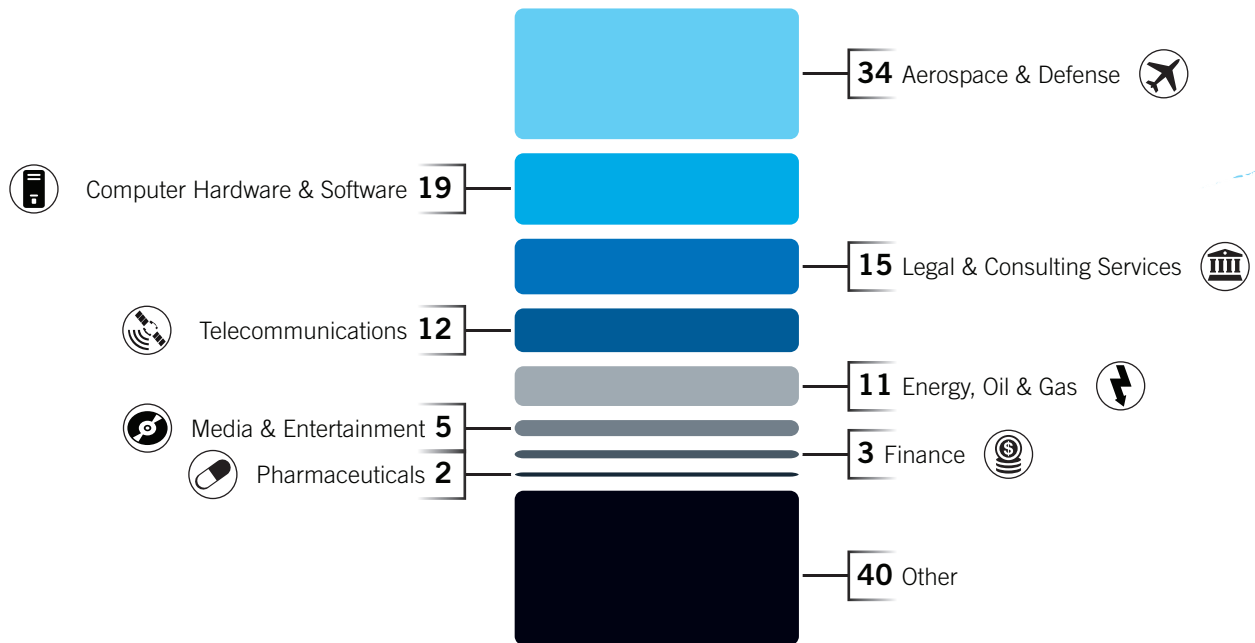
Mandiant is releasing more than 3,000 indicators to bolster defenses against APT1 operations.

- » Specifically, Mandiant is providing the following:
 - Digital delivery of over 3,000 APT1 indicators, such as domain names, IP addresses, and MD5 hashes of malware.
 - Sample Indicators of Compromise (IOCs) and detailed descriptions of over 40 families of malware in APT1's arsenal of digital weapons.
 - Thirteen (13) X.509 encryption certificates used by APT1.
 - A compilation of videos showing actual attacker sessions and their intrusion activities.
- » While existing customers of Mandiant's enterprise-level products, Mandiant Managed Defense and Mandiant Intelligent Response®, have had prior access to these APT1 Indicators, we are also making them available for use with Redline™, our free host-based investigative tool. Redline can be downloaded at www.mandiant.com/resources/download/redline.

Mandiant is releasing more than 3,000 indicators to bolster defenses against APT1 operations. The indicators are available at www.mandiant.com/apt1.

APT1 BY THE NUMBERS

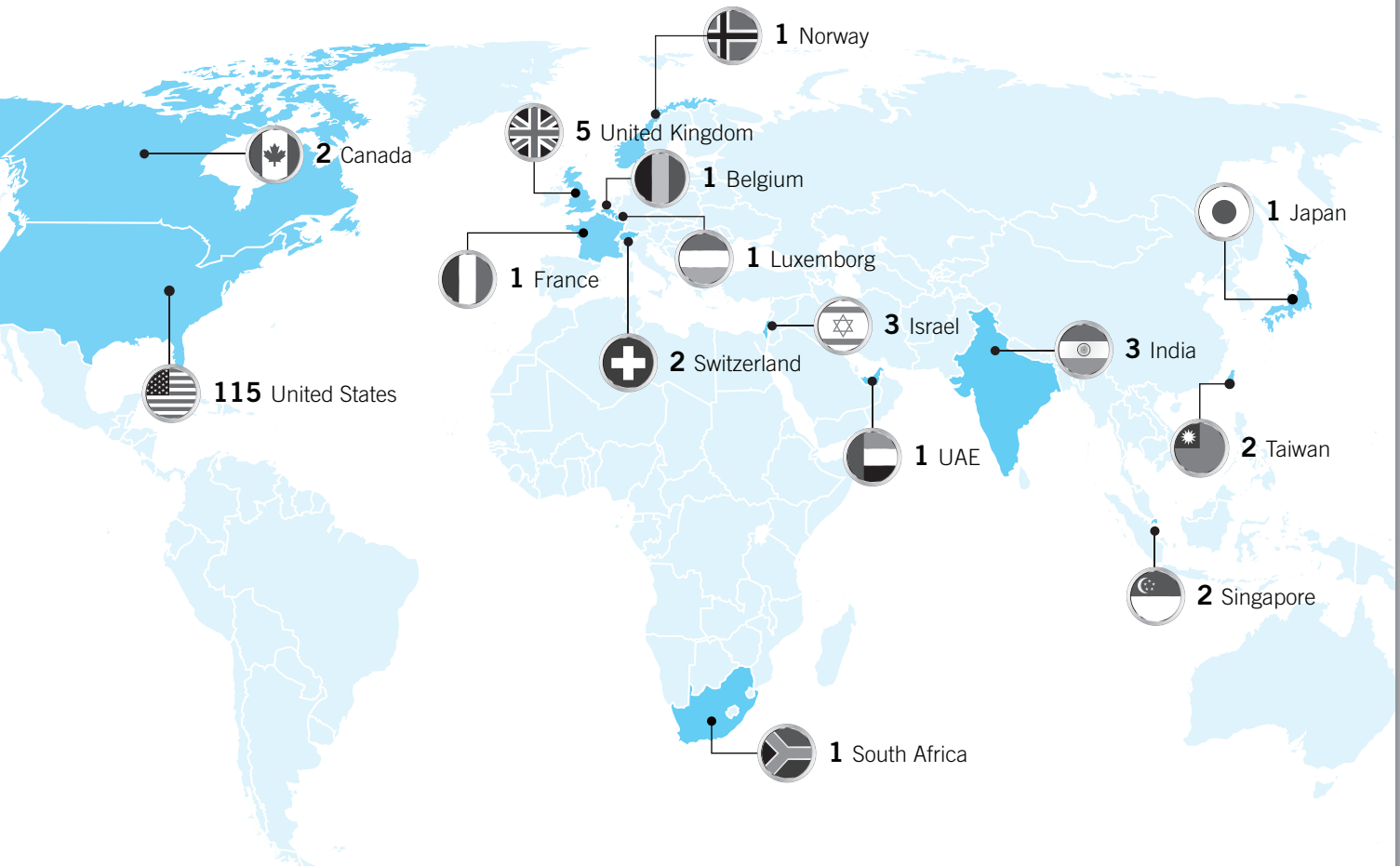
Companies Targeted by Industry, 2006–2012



Longest time period Mandiant observed APT1 in a single victim's network

For the full dossier of this threat actor, including over 3,000 indicators, visit:
www.mandiant.com/apt1.

Victims Observed by Country, 2006–2012



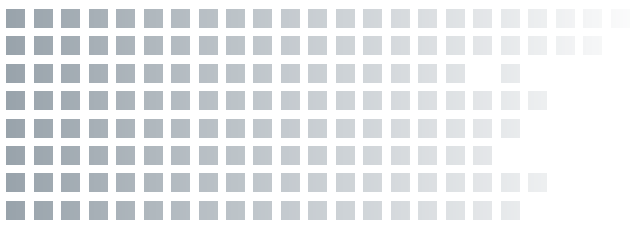
6.5 Terabytes
over 10 months

Largest APT1 data theft from a single organization

1 TB
equals
1,048,576 MB

1 digital image
equals
5 MB

6.5 TB equals 1,363,149 digital images



The sheer scale and duration of sustained attacks against such a wide set of industries from a singularly identified group based in China leaves little doubt about the organization behind APT1. We believe the totality of the evidence we provide in this document bolsters the claim that APT1 is Unit 61398. However, we admit there is one other unlikely possibility:

A secret, resourced organization full of mainland Chinese speakers with direct access to Shanghai-based telecommunications infrastructure is engaged in a multi-year, enterprise scale computer espionage campaign right outside of Unit 61398's gates, performing tasks similar to Unit 61398's known mission.

WHY WE ARE EXPOSING APT1

The decision to publish a significant part of our intelligence about Unit 61398 was a painstaking one. What started as a “what if” discussion about our traditional non-disclosure policy quickly turned into the realization that the positive impact resulting from our decision to expose APT1 outweighed the risk to our ability to collect intelligence on this particular APT group. It is time to acknowledge the threat is originating in China, and we wanted to do our part to arm and prepare security professionals to combat that threat effectively. The issue of attribution has always been a missing link in publicly understanding the landscape of APT cyber espionage. Without establishing a solid connection to China, there will always be room for observers to dismiss APT actions as uncoordinated, solely criminal in nature, or peripheral to larger national security and global economic concerns. We hope that this report will lead to increased understanding and coordinated action in countering APT network breaches.

At the same time, there are downsides to publishing all of this information publicly. Many of the techniques and technologies described in this report are vastly more effective when attackers are not aware of them. Additionally, publishing certain kinds of indicators dramatically shortens their lifespan. When Unit 61398 changes their techniques after reading this report, they will undoubtedly force us to work harder to continue tracking them with such accuracy. It is our sincere hope, however, that this report can temporarily increase the costs of Unit 61398's operations and impede their progress in a meaningful way.

We are acutely aware of the risk this report poses for us. We expect reprisals from China as well as an onslaught of criticism.

CONCLUSION

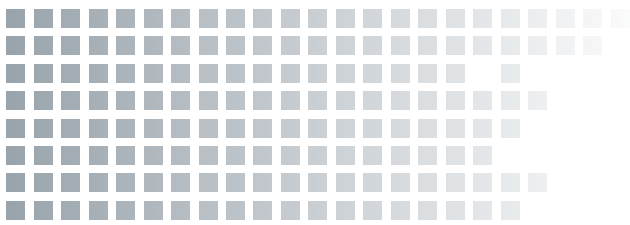
The adversary continues to evolve. That has not changed. Advanced attackers continue to routinely compromise organizations — even those that have made large and sustained investments in security.

As we noted last year, it is becoming harder to differentiate traditional APT attacks from attacks by criminal threat actors that adopt APT-style persistence mechanisms. The blurred line between the tactics used by these threat actors continued this past year. We saw the APT revert to older attack methods, such as “drive by” Web compromises, and revise them to circumvent the new technologies organizations are employing to thwart their efforts.

We also saw advanced attackers change the way they approach victim companies. In several cases, we observed APT groups compromise outsourced service providers as a means to gain access to their victims. We have also seen attackers perform more comprehensive network reconnaissance to help them navigate the networks of their victims faster and more effectively.

But targeted organizations are improving too. Over the past year we saw organizations improve their ability to identify their own compromises. Nevertheless, the median amount of time that attackers have access to a victim’s network before they are identified is still more than eight months.

One thing has not changed. Organizations will always have a security gap and determined attackers will always find a way through that gap. To attack that security gap organizations need smart people, visibility on both their networks and endpoints and threat intelligence that helps them find and stop the adversary. The way you respond — when the inevitable happens — is what will determine whether you become a headline or not.



END NOTES

- ¹ The Advanced Persistent Threat (APT) is a term used to describe a specific group of threat actors (multiple cells) that have been targeting the U.S. Government, Defense Industrial Base (DIB) and the financial, manufacturing and research industries for nearly a decade. Mandiant does not use this term in its diluted sense — as a generic category of threats. As increased awareness of the APT blossomed from Google's public disclosure of the attacks in early 2010, and explosive marketing around "Operation Aurora," organizations less familiar with the APT created a more diluted definition of the term APT, and changed its meaning to "advanced and persistent threats." Mandiant considers the APT a type of "targeted attack." The threat detection and response approaches we describe will combat both the APT and other types of targeted attacks.
- ² Outsourcing Trends 2013: Increase Productivity with Business Process Outsourcing, Gartner 17 January, 2013, Ruby Jivan & Cathy Tornbohm.
- ³ Gartner, (2012). Gartner Says Worldwide IT Outsourcing Services Spending on Pace to Surpass \$251 Billion in 2012. Retrieved from www.gartner.com/newsroom/id/2108715.
- ⁴ Strategic Web compromise is a term coined by Steven Adair and Ned Moran of Shadowserver in their blog post "*Cyber Espionage & Strategic Web Compromises — Trusted Websites Serving Dangerous Results*," May 15, 2012.
- ⁵ Our conclusions are based exclusively on unclassified, open source information derived from Mandiant observations. None of the information in this report involves access to or confirmation by classified intelligence.
- ⁶ We believe that the extensive activity we have directly observed represents only a small fraction of the cyber espionage that APT1 has conducted. Therefore, Mandiant is establishing the lower bounds of APT1 activities in this report.
- ⁷ This is based on 91 of the 141 victim organizations. In the remaining cases, APT1 activity is either ongoing or else we do not have visibility into the last known date of APT1 activity in the network.

ABOUT MANDIANT

Mandiant is the go-to company for the Fortune 500 and government agencies that want to protect their most valuable assets from advanced attack groups. Simply stated, we are the only information security company that can tell an organization when it has been compromised and to what extent its defenses have been violated.

The majority of advanced targeted attacks proceed undetected and proliferate undefended. When attacks are successful, Mandiant's unique combination of human intelligence and technology leadership help organizations detect, respond to and contain them before attackers reach their objective. Our engineers and security consultants hold top government security clearances, have written 11 books and are regularly quoted by leading media organizations. Mandiant is headquartered in Alexandria, VA, with offices in New York, Los Angeles and San Francisco.

To learn more about Mandiant visit www.mandiant.com, read our blog, *M-Union*, follow us on Twitter [@Mandiant](https://twitter.com/Mandiant) or Facebook at www.facebook.com/mandiantcorp.





www.mandiant.com