M Trends™

an evolving threat

MANDIANT®

M Trends

an evolving threat

TABLE OF CONTENTS

INTRODUCTION

There is no such thing as perfect security. Bad guys are compromising companies that have made expensive, responsible, and sustained efforts to defend their infrastructure. Security breaches are inevitable. When they occur — whether a small compromise or a massive intrusion — you want to be armed and prepared.

Having the right tools and processes will allow you to answer the unavoidable questions.

How and when did they get in?

What systems and information were compromised?

How will we know that we are secure?

In nearly a decade of responding to targeted attacks, one thing is constant — attackers get smarter and change tactics every year. The breadth of companies being targeted is growing and the rate of intellectual property theft is increasing faster than ever. Companies who have made responsible and sustained investments in information technology continue to be compromised.

In this **M-Trends**, we highlight the emerging trends we experienced in the past year and share approaches that organizations can take to improve the way they detect, respond to, and contain complex breaches. Of the four major types of attacks highlighted in Table 1, Mandiant focused primarily on criminal and economic espionage incidents, which form the basis of the trends and case studies in this report.

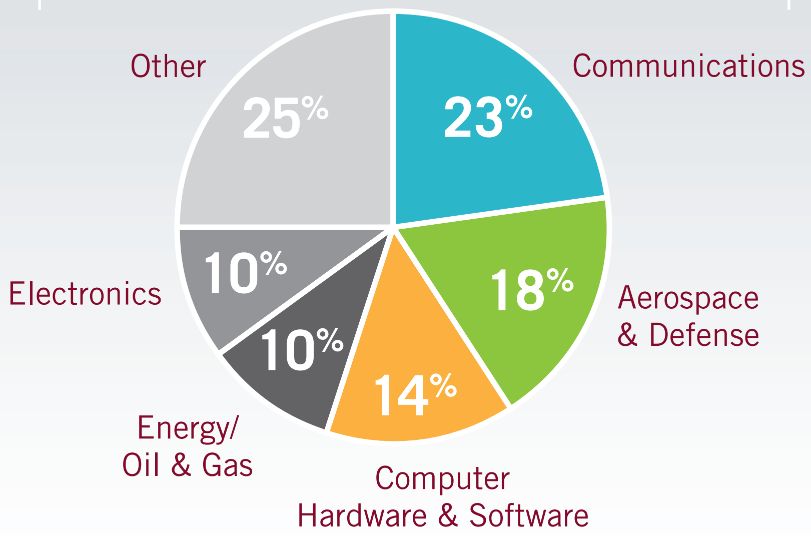
TABLE 1: FOUR MAJOR TYPES OF ATTACKS

THREAT ACTOR	EXAMPLE	TARGETS	OBJECTIVE
Criminal	Credit Card Theft	Enterprises that process credit cards or handle money such as retailers, banks, credit card processors.	Financial Gain
Hacktivists	Anonymous LulzSec	Anyone	Defamation, Press, Public Policy
Economic Espionage	Advanced Persistent Threat (APT)	Virtually any industry with an emphasis on blue chip companies and defense companies.	Economic Advantage
Nuisance	Botnets, Spam	Anyone, including individuals, small companies and large enterprises.	Launch points, nuisance, often consumer-based threats.

INTRUSIONS BY THE NUMBERS

This **M-Trends** focuses on Mandiant's observations while responding to targeted attacks over the last year. During our investigations, we observed **6 trends.**

What Industries Are Being Targeted By Advanced Attackers?



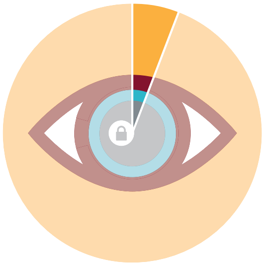
In What % of Cases Did the Bad Guys Use Valid Credentials?

100%

How Many Advanced Threats Used Publicly-Available Malware?

77%
of all intrusions Mandiant investigated

How Are Compromises Being Detected?



6%
of victims discovered the breach internally

94%
of victims were notified by an external entity

What Was the Time From Earliest Evidence of Compromise to Mandiant's Involvement?

April 2010
March 2011

416
median number of days that the attackers were present on a victim network before detection

TRENDS

1 Malware Only Tells Half the Story

Searching for malware identifies only 54% of systems compromised in an incident.

2 Everything Old Is New Again

Attackers are using passive backdoors to evade network- and host-based detection methods.

3 RATs!

The use of publicly available malware in targeted attacks is increasing.

4 M&A Is Being Served With a Side of Compromise

Organizations are buying and selling compromise during merger & acquisition activities.

5 Some Assembly Required

Attackers are targeting companies that collaborate together within a supply chain in order to assemble a comprehensive intellectual property portfolio.

6 It Pays to Be Persistent

Financially motivated attackers are shifting toward longer-term persistence on victim networks.

1

MALWARE ONLY TELLS HALF THE STORY

Searching for malware identifies only 54% of systems compromised in an incident.

Organizations have spent millions of dollars attempting to deter attacks by detecting malicious software on workstations and servers. They have invested millions more in network monitoring and antivirus capabilities. These investments frequently do little more than detect characteristics associated with common worms, botnets, and drive-by downloads. They do little to help organizations defend against targeted intrusions. As a result, most organizations operate with a false sense of preparedness.

Today, advanced attackers often use malware as a means to gain an initial foothold within an organization. After the initial compromise, though, they shift their tactics and use legitimate credentials from compromised accounts to move laterally, create staging sites and exfiltrate data from the targeted organization.

Mandiant's investigations show that only 54% of compromised hosts in our investigations actually contained malware. This malware went undetected by existing network monitoring and antivirus solutions. So how does one identify the other 46% of compromised systems? In short, this requires performing comprehensive forensic analysis of systems across your enterprise to look for evidence of compromise that goes beyond malware.

Traditional investigative techniques emphasize malware detection and only tell half the story — under the best of circumstances. Typical techniques may involve running multiple antivirus products and rootkit detection utilities against suspect systems. This can destroy critical evidence, and if the attacker's backdoors and utilities avoid detection, they will maintain a presence indefinitely. More important, traditional incident response approaches miss systems attackers accessed using legitimate credentials including the data that was accessed on these systems.

To determine the full extent of a compromise, one must inspect the trace evidence the attackers leave behind that do not involve malware. Among these trace indicators of compromise we found the following to be most prevalent. More detailed examples from recent investigations can be found on pages 6–7.

TABLE 2: EVIDENCE OF COMPROMISE BEYOND MALWARE

EVIDENCE OF COMPROMISE	DESCRIPTION
Unauthorized Use of Valid Accounts	In 100% of the cases Mandiant responded to this year the attacker used valid credentials. Evidence of such account activity can be found through the examination of Windows event logs, registry entries, file ownership, and network traffic captures.
Remote System/File Access	Attackers use compromised systems to remotely access systems and files within the target environment. The Windows registry and web browser history often contains evidence of this activity.
Trace Evidence & Partial Files	Attackers frequently remove tools, scripts, and files generated by their activities. Remnants of attacker activity can be found in restore points, scheduled task logs, and the Windows event logs.

If only 54% of a compromise can be discovered by searching for malware, the other 46% must be identified through enterprise-wide analysis of registry entries, event logs, scheduled task logs, inventory management logs, network traffic captures, and file system artifacts. Systems identified as suspect during this process are triaged to determine if full forensic analysis is necessary.[1]

THE TAKEAWAY

Effective computer incident response teams combine software and intelligence to overcome issues of scale and limitations of malware-centric tools and techniques. Countering sophisticated threats requires technology that can rapidly sweep endpoints for indicators of compromise, extract evidence of an intrusion, and determine incident scope and impact.

[1] Mandiant created Mandiant Intelligent Response® to effectively respond to these incidents and provide an investigator the ability to discover the full scope of compromise. Responding in this fashion allows investigators to identify every aspect of an intrusion, accurately determine an attacker's actions, and effectively remediate the threat.

MALWARE ONLY TELLS HALF THE STORY

Mandiant's experience has proven that a malware-centric investigation of an advanced threat will lead to misses in coverage — and not just a few. In fact, just under half of all compromised systems we identified had no trace of actual malware files. Identifying these systems is critical, as any of them could serve as a re-entry point for an attacker after a difficult remediation exercise.

The Mandiant approach is to conduct mass-scale forensics across thousands of systems to identify the trace evidence of compromise that attackers leave behind: a forgotten registry entry, an entry in a log file, or a hint that files were exfiltrated. The graphics on this page illustrate how we found compromise in three investigations during 2011.

Read more about this trend on page 4.

Note: Indicators of compromised systems are generally found in more than one place during an investigation. For the sake of clarity, the graphics on this page indicate the location of the primary evidence used to identify the compromised system, and are not intended to represent the findings of a complete forensics report.

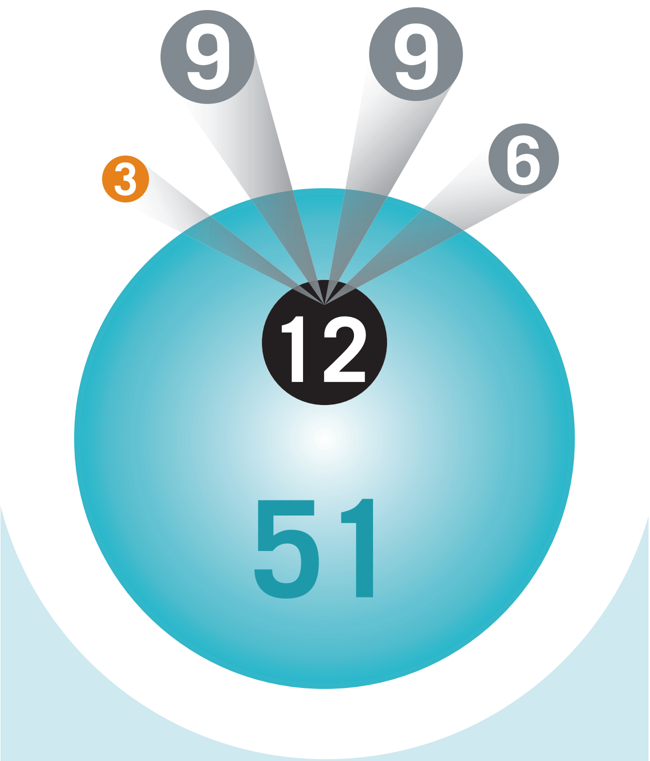
For the tables at the top of the page, note that systems may have had multiple malware families installed on them.

TECHNOLOGY COMPANY

63 TOTAL COMPROMISED SYSTEMS
TOTAL SYSTEMS = 30,000

12 SYSTEMS CONTAINING MALWARE

# OF SYSTEMS	TYPE OF MALWARE OR UTILITY PRESENT
12	**Malware Present**
3	**Proprietary Malware Only**
9	Poison Ivy Remote Access Trojan
6	Windows Credential Editor (WCE)
9	PsExec



51 OTHER COMPROMISED SYSTEMS

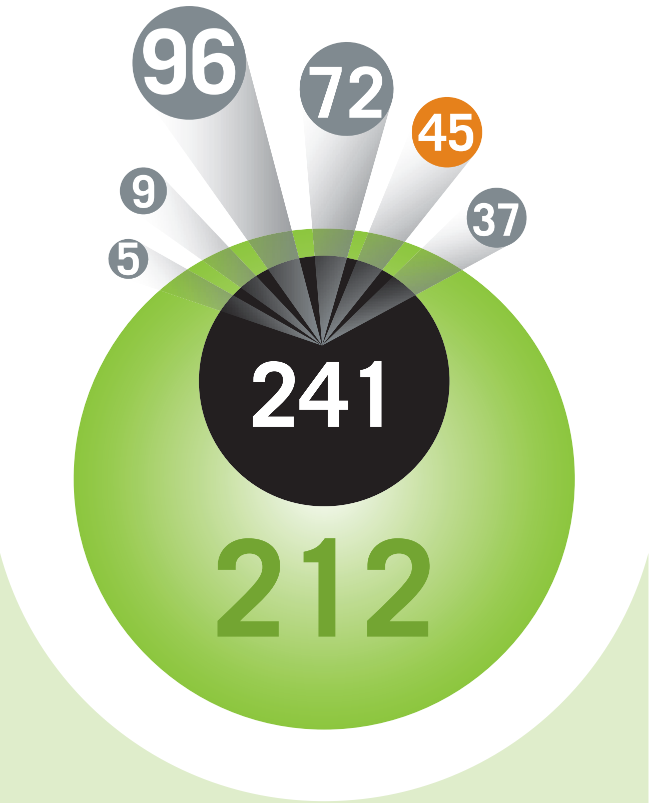
# OF SYSTEMS	TYPE TRACE EVIDENCE	METHOD OF DISCOVERY
12	Registry	Evidence of remote desktop sessions in HKCU\Software\Microsoft\Windows\Shell\BagMRU and related keys
10	File	Evidence of previously-used malware in a restore point
9	File	Batch/utility scripts left behind by attackers
8	File	Previously used commands in pagefile and hiberfile
6	File	Evidence of file mapping in unallocated space
4	File	File fragment in unallocated space
2	File	Malware config file left after removal

FINANCIAL COMPANY

453 TOTAL COMPROMISED SYSTEMS
TOTAL SYSTEMS = 50,000+

241 SYSTEMS CONTAINING MALWARE

# OF SYSTEMS	TYPE OF MALWARE OR UTILITY PRESENT
241	**Malware Present**
45	**Proprietary Malware Only**
96	Poison Ivy Remote Access Trojan
72	Htran
5	pwdump
9	Windows Credential Editor (WCE)
37	Hookmsgina



212 OTHER COMPROMISED SYSTEMS

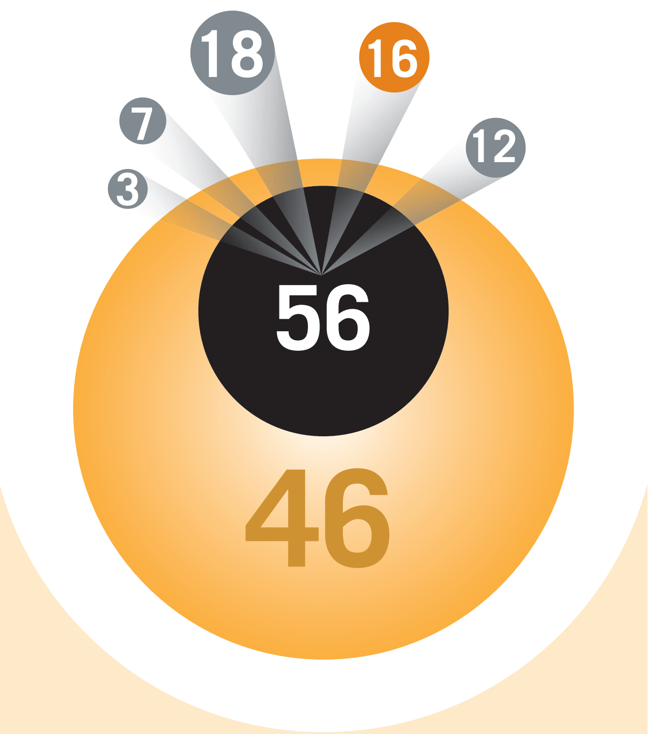
# OF SYSTEMS	TYPE TRACE EVIDENCE	METHOD OF DISCOVERY
80	File	Batch/utility scripts left behind by attackers
63	File	Evidence in SchedLgU.txt scheduler log
29	File	Malware file traces in pagefile
13	Registry	Recent search terms from HKEY_CURRENT_USER\Software\Microsoft\Search Assistant\ACMru
10	File	Traces of rar file compression in page files and unallocated space
7	File	Evidence of file access via internet history
6	Registry	Recent search terms from HKCU\Software\Microsoft\Search Assistant\ACMru
4	File	Evidence of remote directory listings in unallocated space

HIGH TECH DEFENSE

102 TOTAL COMPROMISED SYSTEMS
TOTAL SYSTEMS = 6,000

56 SYSTEMS CONTAINING MALWARE

# OF SYSTEMS	TYPE OF MALWARE OR UTILITY PRESENT
56	**Malware Present**
16	**Proprietary Malware Only**
18	Gh0st Remote Access Trojan
3	ASPXSpy
7	GetHashes
12	PsExec



46 OTHER COMPROMISED SYSTEMS

# OF SYSTEMS	TYPE TRACE EVIDENCE	METHOD OF DISCOVERY
13	Registry	Evidence of previously mapped network drives from multiple registry keys
9	File	Evidence pulled from attacker's keystrokes on remote systems (as culled from their own keystroke loggers they had placed)
8	File	Traces in hh.dat
5	File	Programs recently run in AppCompatCache
4	Registry	Evidence of remote desktop sessions in HKCU\Software\Microsoft\Windows\Shell\BagMRU and related keys
4	Registry	Application startup data in MUICache
3	File	Contents of prefetch directory

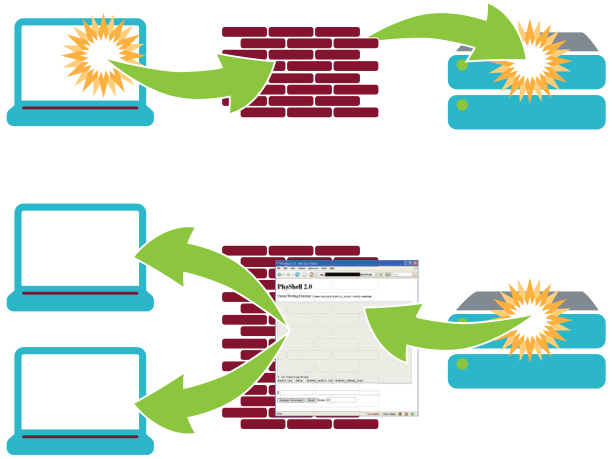
2

EVERYTHING OLD IS NEW AGAIN

Attackers are using passive backdoors to evade network- and host-based detection methods.

Historically, the Advanced Persistent Threat (APT)[2] has used reverse backdoors for remote access to compromised environments. These backdoors initiate outbound network connections and use traditional persistence mechanisms such as ServiceDLL or ImagePath replacement and startup folders. These backdoors were detectable because they generated consistent and routine network traffic and resided in common locations.

During 2011, Mandiant has seen the APT diversify their backdoor mechanisms to be more resilient against detection and remediation efforts. Specifically, they are using a new persistence mechanism that we are calling "Passive Backdoors." These backdoors are harder to detect using standard network traffic analysis and traditional forensic techniques. They do not generate network traffic. They do not always use traditional persistence mechanisms, and they are frequently deployed outside of the known attack path. Two examples of passive backdoors are port listeners and web shells.



Port Listeners: A port listener is a sophisticated passive backdoor. In the past year, Mandiant identified low-level network drivers, such as miniport drivers, being used for command and control (C2). The low-level network driver allows network traffic to be examined, before higher-level drivers and applications, such as FTP, process the traffic. This allows the backdoor to identify its C2 traffic, activate the passive malware, and pass non-C2 traffic to the higher-level application. For example, the higher-level application might be an FTP server listening for connections on TCP port 21.

Web Shells: Web shells provide an attacker simple access to a number of administrative functions on the server — from enumerating users, to uploading files, to providing an interactive command shell. By utilizing HTTPS they blend in easily with legitimate web traffic. Web shells are typically created within an existing web directory, are timestomped[3] to match the date/time information from legitimate web pages and are disguised as a legitimate part of the application.

Port listeners and web shells have been most commonly associated with attacks initiated from outside an organization. They are typically deployed during the initial phases of the compromise as the attacker attempts to gain access to the internal network. However, in recent cases we have seen the relationship reversed. Compromised accounts from the internal network are used to deploy web shells and port listeners to DMZ hosts well after the initial compromise. These backdoors do not initiate network connections; rather, they wait silently for the attacker to connect to them.

Web shells and port listeners allow an attacker to initiate a connection to a compromised web or application server from virtually anywhere. More significantly though, the attacker can quickly shift the source of their activity if remediation is suspected. These backdoors act as a back-up remote access mechanism in situations where the attacker's other C2 mechanisms are removed.

The concept of passive backdoors is not new. Attackers have used web shells and port listeners for years. The significance of this trend is not in the technology, but in the increased prevalence of their use in advanced attacks and the corresponding impact on the investigation and remediation activities.

THE TAKEAWAY

Rather than solely rely on client-initiated backdoors, the APT attackers have blended the more traditional backdoor listening as a server. The use of passive backdoors is an indication that targeted attack methodologies continue to evolve as attackers seek to ensure continued access to environments and thwart detection mechanisms.

[2] 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.

[3] Timestomping is a common technique used by attackers to disguise their malware by modifying the standard file metadata attributes to match the timeframes for legitimate system binaries.

3

RATS!

The use of publicly available malware in targeted attacks is increasing.

In Mandiant investigations over the past year, we have seen an increase in attack groups using publicly available Remote Access Trojans (RATs), backdoors, and utilities to gain access into victim organizations. These tools are readily accessible and easy to configure. The use of these publicly available tools has added some complexity to identifying threat actors. For example, we have seen the same RATs used by APT groups as well as by financially motivated threat actors. In prior years, the majority of backdoors used to maintain persistent access to victim networks were custom implementations.

When organizations identify a piece of publicly available malware they usually cleanse the file or rely on an anti-virus quarantine to address the issue. Unfortunately, doing so could obscure a larger incident. Even routine malware alerts should be reviewed and placed into a broader context as part of a holistic monitoring system.

Some examples of publicly available RATs, privilege escalation tools, and legitimate utilities we commonly see during investigations are outlined in Table 3.

TABLE 3: OVERVIEW OF PUBLICLY AVAILABLE TOOLS USED IN TARGETED ATTACKS

TOOL NAME	DESCRIPTION	TYPE
ASPXSpy	This open-source ASP web application provides an intruder with the ability to perform remote command execution, upload/download files, interact with SQL databases, perform port scans, and query registry keys.	RAT
Cachedump	This tool obtains password hashes for domain logins that have been cached in the Windows registry.	Privilege Escalation
GetHashes	This tool obtains password hashes from the SAM file.	Privilege Escalation
Gh0st RAT	This widely available backdoor provides a graphical client builder and graphical server.	RAT
Gsecdump	This tool obtains hashes from the Windows registry, including the SAM file, cached domain credentials, and LSA secrets.	Privilege Escalation
Hookmsgina	This tool hooks the legitimate Microsoft Graphical Identification and Authentication DLL (msgina.dll) and dumps the username, domain, password and old password (in the event of a password change logout) to a file.	Privilege Escalation
Htran	The "Honkers Union of China Packet Transmit Tool" is a port director which takes incoming traffic on one port and sends it to a specified IP and port of another system.	Other
Incognito	This tool performs Windows access token manipulation.	Privilege Escalation
Pass-the-Hash toolkit	This set of tools accesses hashes of users who have interactively logged into a system and then allows an intruder to impersonate those users by "passing" those hashes to other systems.	Privilege Escalation
Poison Ivy	The Poison Ivy (PI) Remote Access Trojan (RAT) is a publicly available backdoor which provides comprehensive remote access capabilities on a compromised system. Poison Ivy variants are configured, built, and controlled using a graphical Poison Ivy management interface.	RAT
PsExec	The SysInternals tools, now distributed by Microsoft, also have myriad legitimate uses to allow system administrators to remotely invoke executable file across a network.	Lateral Movement
Pwdump	This tool obtains password hashes from the SAM file. Many password dumping tools are variants of Pwdump.	Privilege Escalation
Radmin	This remote administration tool is commonly used by legitimate system administrators.	RAT
Windows Credential Editor (WCE)	This tool is used to grab current sessions, modify credentials, and perform pass-the-hash.	Privilege Escalation
Xdoor	This backdoor's interface and server are displayed in Chinese. Its functions include key logging, audio and video capture, file transfers, HTTP proxy, retrieval of system information, reverse command shell, DLL injection, and command execution.	RAT
ZXshell	This backdoor functions include key logging, file transferring, SYN floods, the ability to launch processes, steal credentials, and disable local firewalls.	RAT

While it may seem counterintuitive that targeted threats are using more off-the-shelf tools as their operations mature, we identify three reasons for this change:

1. **They Already Exist:** If the right tool is freely available, the adversary does not need to spend time and effort creating a new one. As the APT expands its footprint, they consistently use the least sophisticated capabilities necessary to compromise an organization, and publicly available tools often satisfy the requirement.

2. **Organizations Allow Their Use:** Most anti-virus systems have categories for so-called "hacking tools" such as PsExec and radmin. However, since these tools are often legitimately used by system administrators, many organizations have disabled that category in their anti-virus policy. While blocking these tools will not thwart the APT, we have seen organizations make it more difficult for certain attack groups to move laterally if these common tools are quarantined and/or deleted by anti-virus programs.

3. **Even if Blocked, They Rarely Stand Out:** As overall malware in an environment proliferates, it is simply easier to blend into the "noise" of security operations. Some organizations process millions of security events each day, and the presence of Poison Ivy or PsExec will often not attract attention.

THE TAKEAWAY

Classifying incidents involving publicly available tools and malware as minor issues can be risky. Take advantage of anti-virus tools' alerts on publicly available malware to uncover potential larger issues. Look for trends and anomalous patterns in these alerts and investigate as appropriate.

4

M&A IS BEING SERVED WITH A SIDE OF COMPROMISE

Organizations are buying and selling compromise during merger & acquisition activity.

2011 was the busiest year for global merger & acquisition activity since the recession of 2008.[4] Based on Mandiant's experience, it was also the busiest year for the acquisition and divestiture of APT compromises. We responded to a record number of targeted intrusions that were discovered while the victimized organizations were in the process of integrating into their new parent organizations.

This trend is the result of two factors:

1) **Improved Detection by the Acquiring Companies:** Many large companies that have experience in combating targeted threats have improved their ability to detect evidence of compromise. As a result, checking for evidence of compromise is part of their due diligence process prior to (or during) the integration process. This helps ensure the acquiring company does not accidentally re-compromise itself.

2) **Increased Penetration Among Acquired Companies:** Targeted threats continue to impact a broader cross-section of businesses. As we detailed in the 2011 M-Trends report, targeted threats have evolved from their early focus on government/defense targets, into the defense industrial base and various commercial entities. This evolution has resulted in the compromise of many smaller organizations as well as the compromise of organizations that are partnering on larger projects.

While the majority of these incidents were only detected after network connectivity had been established to the parent company, one organization with a very mature security program had a policy that all acquisitions be swept for indicators of compromise prior to network integration. This policy worked effectively — the intrusion was detected and remediated prior to establishing connectivity between the two networks, avoiding a potentially costly expansion of the intrusion into the parent network.

THE TAKEAWAY

Organizations with a mature security program understand that incident detection and response is a continuous business process, not an isolated exercise. Defeating persistent threats requires technical, repeatable, and automated scrutiny of business units, acquisitions, divestitures, partners, suppliers, and outsourcers.

[4] http://www.mergermarket.com/pdf/Press-Release-for-Financial-Advisers-Year-End-2011.pdf

5

SOME ASSEMBLY REQUIRED

Attackers are targeting companies that collaborate within a supply chain in order to assemble a comprehensive intellectual property portfolio.

Over the last year, Mandiant identified a distinct trend of related organizations being targeted because they partnered on a specific project or because their technology was complementary to a targeted technology. Advanced attackers have learned that in order to gain full visibility into complex projects, data is required from all of the companies that partnered to design or build the targeted project.

As Mandiant has gained visibility into more and more companies, our ability to track compromised organizations across supply chains has improved. In multiple instances during 2011, Mandiant was able to track advanced intrusion sets across business partners, outsourcers, and direct competitors. In one instance, the victim organization named two supply chain partners who used their stolen technology, both of whom Mandiant had previously assisted with incident response.

In some cases we investigated the theft of intellectual property that appeared to be of low impact until a complementary theft was identified elsewhere. For example, Mandiant responded to an intrusion at a chemical manufacturer and determined that a proprietary formula had been stolen. The manufacturer deemed the loss to be relatively low risk to their business — this formula was only half of the input used to build a certain high-technology electrical component. The other half of the technology was developed by a separate organization, and the compound had limited use outside of this manufacturing process. The full extent of the loss was realized when the victim organization discovered that the partner organization had also been compromised, and that the second critical piece of intellectual property had also been stolen.

THE TAKEAWAY

Defensive-minded enterprises recognize that their organization could be part of a targeted ecosystem and remain vigilant for intruders who steal and integrate intellectual property, business intelligence, methods, and other information assets from victims in other parts of their supply chain. Frustrating threat actors requires recognizing that no organization is too small for compromise as long as the data it possesses is important.

6

IT PAYS TO BE PERSISTENT

Financially motivated attackers are shifting toward longer-term presence on victim networks.

Financially motivated attackers have historically relied on relatively simple tools, tactics, and procedures (TTPs) to steal payment card data. These attacks were known as “smash and grab” compromises — the attacker would steal targeted data and never return to the victim organization. Maintaining persistent access was not considered essential. If access was necessary again, they would leverage the same exploit they used initially. This strategy simplified their operations as they did not need to deploy backdoors or maintain command-and-control networks.

Attackers faced a dilemma as IT environments grew more complex and they grew more ambitious. They needed to either be content with smash and grab theft or evolve their techniques to obtain longer-term access. Most financially motivated attackers chose the more lucrative option, which required that they enhance their TTPs with persistence mechanisms that ensure ongoing access to victim organizations.

Financially motivated attack groups have implemented persistence in a variety of ways. Mandiant has witnessed attack groups create custom backdoors, use publically available backdoors, use web shells, use Metasploit Meterpreter, or use a GUI-based remote access utility such as RDP, Dameware, or VNC. Maintaining persistence to a compromised organization allows the attacker to steal more data over a longer period of time, to gain access to more lucrative data, and to ensure their data is a fresh as possible.

THE TAKEAWAY

Financial organizations are as much a target of persistent attackers as the defense industrial base and government organizations. The financial industry can benefit from real-time threat intelligence and by continuing to improve their ability to detect and respond to targeted threats.

CASE STUDY

ELECTRONICS MANUFACTURER
THE PARTNER ORGANIZATION

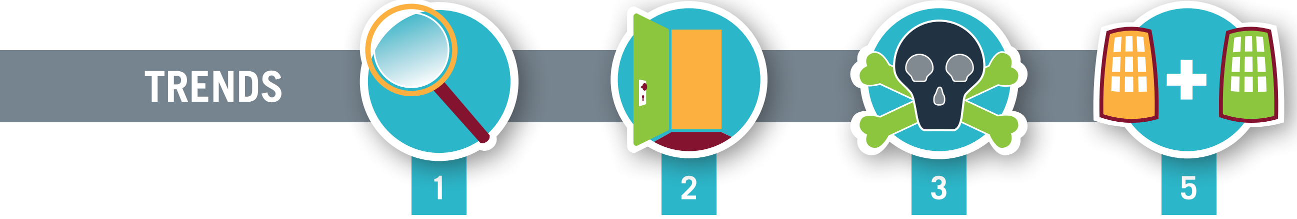
In early 2011, an electronics component manufacturer contacted Mandiant as the result of receiving a notification of compromise from a government agency.

After conducting sweeps to obtain forensic evidence, we realized that the attacker had been replacing their malware every six months during the two years they had been resident at the victim organization — and this replacement occurred again during the course of our investigation. Further analysis revealed that another company — also dealing with an intrusion by the same attackers — had been submitting their malware samples to their anti-virus vendor. While the second company had the best of intentions, their efforts resulted in the attacker constantly rotating their malware at our client (and most likely at the second organization as well).

To maintain persistence, the attacker used a variety of backdoors, including some publically available ones. **One interesting custom backdoor consisted of a custom miniport driver, which listened for a particular "magic packet."** Upon receiving this inbound stream of bytes, the "magic packet," the malware would become active. Further, the miniport driver listened for IP data that was specially encapsulated within another non-TCP protocol, more effectively hiding it from network monitoring devices.

Another characteristic of this intrusion was the use of non-persistent malware that required configuration information to be specified at runtime, helping to further cloak the attacker's activities. While not a unique or new attack technique, this made the investigation even more challenging. This particular malware was custom built and modular; functionality could be added or taken away at compile time. This malware was executed with run-time arguments supplied at the command line, to include the C2 server and proxy configuration information, as well as the actions to take. When finished with the malware, the attacker often left the malware on the system because it had been timestomped and was hidden in plain sight, thus allowing the attacker to use the malware later.

This use of non-persistent malware is an example of an attack method that would have been difficult for Mandiant to find without using a tool to search all systems at the company for indicators of compromise (IOCs). The MD5 hash, filename, and file path were distinct on nearly every compromised system. Common applications designed to look for malware failed to detect this malware on dozens of systems, even though the attacker was using this as a primary mechanism for interacting with systems. In addition, because the attacker supplied unique C2 IP addresses in most instances, detecting the network traffic was difficult without having a robust network signature that went beyond simple IP detection.



> It was only by connecting the dots between the two victims that the attacker's goal was clear: rather than targeting a single company for a particular technology, they had been tasked to acquire the more advanced, broader technology.

Our approach to investigate this diverse set of malware was to build comprehensive indicators of compromise for both the malware and the identified malicious activity. These IOCs were designed to detect the malware's custom protocol and encryption method, which allowed us to discover unknown variants of the malware. We then searched every system in the environment for all of the IOCs, investigated compromised systems, built new IOCs and continued this iteration process until the compromise had been fully scoped.

Of the approximately 100 compromised systems, the intruder installed malware on less than half of them. The attacker made extensive use of publicly available malware and normal windows commands in addition to custom malware. The usage of publically available malware and native Windows commands is consistent with the APT's trend to "hide in plain sight." As an example, the attacker ran full directory listings ("dir /s") on every compromised system and saved the results to a local text file; used FTP batch files to steal the data; used Windows administrator utilities like tlist.exe, local.exe, kill.exe to interact with the system; extensively used PsExec to remote execute binaries; and used the Windows "net" commands to move laterally throughout the network. Much of this activity would have been missed if the IOCs had not been designed to detect malicious activity as well as the malware itself.

Finally, this case presented a unique twist during the impact assessment. Mandiant investigators were able to determine a partial list of filenames that had been stolen. The victim company did not place a high value on the stolen data since it was merely a sub-component of a more advanced technology, and the victim did not even produce the other component parts. While the more advanced product was extremely valuable, it could only be built by combining the victim's technology with parts from a second company in the supply chain. Within weeks, Mandiant received a call from that second company — they had also been the victim of an advanced attack, and they also lost intellectual property for a sub-component. It was only by connecting the dots between the two victims that the attacker's goal was clear: rather than targeting a single company for a particular technology, they had been tasked to acquire the more advanced, broader technology. The attackers had performed reconnaisance to determine what companies produced the component technologies, and then targeted those entities.

This piecing together of intellectual property for multiple sub-components across a supply chain has been observed several times in the last year, and marks a new trend in our multi-year observation of APT techniques.

CASE STUDY

FINANCIAL INSTITUTION
PERSISTENT ORGANIZED CRIME

In 2011, Mandiant responded to an incident at a financial institution where the attacker had maintained a presence for several months. The attackers initially compromised an internet-facing web server to gain access to the environment. The web server's administrative interface was misconfigured. The attacker established a foothold by installing a backdoor on the system using the administrative interface; this allowed him to execute commands against the web server's operating system. **This backdoor was passive and was hidden from casual discovery on the web server.**

Once the attacker had established a foothold, they took advantage of various configuration issues on workstations and servers to move laterally within the environment. With privileged access to several file servers, the attacker created local administrator accounts. Now that they had established a foothold in the environment and escalated privileges, they began to move laterally in search of financial information. As the attacker moved laterally, they installed several host-based backdoor variants in order to maintain a long-term presence in the environment.

One backdoor the attacker installed was the popular, and publically available, Remote Access Trojan (RAT) known as GhOst RAT. This malware provided the attacker remote access and the ability to log keystrokes. Some of the GhOst RAT instances were configured to capture keystrokes. Ironically, in some cases, the keystroke monitoring captured the attacker's own activity as well as the user's activities on those systems, which became useful during the course of the investigation.

The attacker did not limit their backdoors to publicly-available ones. A custom-written backdoor that provided remote command execution and file transfer capabilities was also used. While this backdoor did not have the full-featured capabilities of GhOst RAT, it had the advantage of being invisible to antivirus tools. If responders detected the systems infected with GhOst RAT this second backdoor would provide the attacker continued access to the environment. If they followed traditional incident response doctrine and removed the GhOst RAT-infected systems as they were detected, the attacker would still maintain undetected access to the environment through the custom backdoors.

The attacker moved laterally throughout the environment using the systems with backdoors as pivot points, targeting two types of systems in particular: Active Directory servers and databases containing Payment Card Industry (PCI) data. The attacker eventually gained access to every Active Directory server in the victim environment and successfully stole password hashes for all user accounts. Each Active Directory server was compromised with multiple backdoor variants, which the attacker used regularly to access the domain controllers and dump passwords.

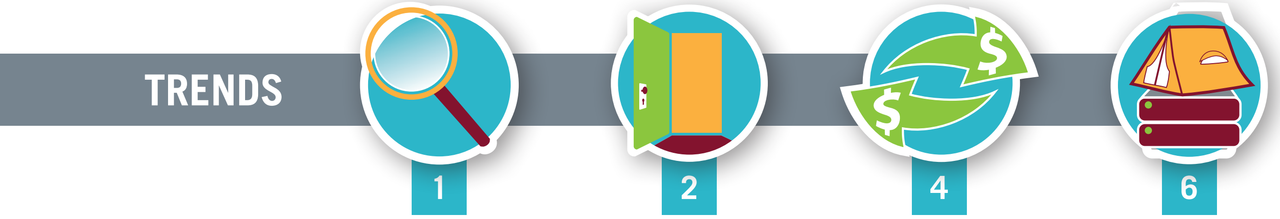
This long-term access would ensure the attacker enjoyed continued, unfettered access to the environment to continually steal more data.

Although the majority of the attacker's backdoors provided file transfer capabilities, the attacker instead chose a different avenue for data theft. **That avenue was to FTP data to a compromised external system controlled by the attacker.**

The attacker's primary objective was clearly financial fraud. However, the TTPs the attacker used during the compromise indicated his intent to maintain long-term access to the environment. This long-term access would ensure the attacker enjoyed continued, unfettered access to the environment to continually steal more data.

In total, the attacker compromised dozens of systems. The attacker used a total of five compromised user accounts throughout the environment. Approximately 80 systems were infected with backdoors, presenting the attacker with plenty of options to regain access to the network if some of them were discovered and mitigated. This illustrates the importance of executing a comprehensive investigation and remediation as a key component of the incident response process. If investigators had missed even one of these 80 systems, the attacker would have had the capability to instantly regain access to the environment.

In this incident, most of this information was harvested from systems without malware installed. In order to understand the complete scope of the compromise, and thus perform a full remediation, incident responders must ensure they investigate evidence of compromise, and not just malware.



CASE STUDY

DEFENSE INDUSTRIAL BASE
INTEGRATING COMPROMISED COMPANIES

A large European defense contractor contacted Mandiant just months after acquiring a specialty service provider. The service provider had received information indicating that they had been the victim of a targeted attack, and the parent company was concerned about the extent of the penetration.

The attack began with a phishing email containing a malicious PDF attachment. Prior to sending the email, the attacker had performed enough reconnaissance to uncover the name of an individual at a competing organization with whom the victim user had previously corresponded. The socially engineered email purported to be from that individual.

This tool silently captured usernames and passwords of all users authenticating to the system.

When the victim opened the attachment, a dropper malware was extracted and executed, installing the publicly available RAT known as GhOst to establish the attacker's foothold in the environment. The attacker leveraged this initial backdoor to move laterally throughout the environment, dropping other backdoors along the way. The attacker extracted password hashes from Active Directory, cracked some of the domain administrator account passwords, and cracked the local administrator account password. The attacker then proceeded to move freely throughout the environment using legitimate credentials and a combination of "net use," scheduled tasks, and PsExec.

The attacker installed a publicly available Graphical Identification and Authentication (GINA) replacement module on many of the compromised systems. This tool silently captured usernames and passwords of all users authenticating to the system. They targeted administrators' PCs in order to ensure continued access to domain administrator credentials.

The attacker archived harvested data into encrypted RAR files, which were temporarily stored in the C:\RECYCLER directory. In this case, the presence of any files in the root of C:\RECYCLER was an indicator of compromise. Targeted attackers frequently use the C:\RECYCLER directory as a staging area for data theft because the contents of this directory are not visible to casual observers. Ultimately, the attacker succeeded in stealing over 50,000 files.

At the time of the incident, the parent company had no plans to integrate the security operations of the two companies. However, the severity of the incident caused them to revisit their merger and acquisition process and make changes to their third-party risk management practices. Based on the lessons learned from this incident, they implemented a process requiring every new acquisition to be vetted by the Mandiant Intelligent Response tool prior to being allowed to join the corporate network. This process paid off in late 2011 when the company discovered an APT group actively operating at another company they were about to acquire. The integration was put on hold until a thorough remediation and damage assessment was completed.

TRENDS 1 3 4

APPROACH FOR TARGETED THREAT REMEDIATION

Successfully remediating a targeted intrusion requires a different approach than remediating non-targeted threats. Organizations that successfully remediate targeted intrusions execute a three-phased remediation plan. Remediating targeted threats from your network requires a concentrated remediation event that involves multiple steps taken in a concentrated period of time (vs. a rolling "whack-a-mole" approach). Prior to the remediation event, the victim organization executes posturing activities necessary to prepare for the event and to enhance the organization's security posture. During the posturing phase, the organization takes care not to disrupt the attacker or alert him to the upcoming remediation event.

After the initial remediation, organizations can then react individually to new compromised systems, moving to contain them at the first signs that the attacker has regained access.

REMEDIATION

1 POSTURING STEPS

Consider these activities prior to beginning remediation of an incident.

- » Enable comprehensive logging of DNS, DHCP, VPN, and Windows security events
- » Increase password complexity
- » Reduce cached credential storage
- » Disable the use of LANMAN hashes
- » Implement aggressive patch management
- » Develop end-user security training

2 REMEDIATION EVENT

Consider these activities to aggressively remove the attacker's access to your network.

- » Pull entire enterprise off of the internet until the remediation event steps are completed
- » Block known attacker C2 domains and IP addresses
- » Block dynamic DNS providers
- » Change all compromised passwords (if Active Directory has been compromised, this means changing all Active Directory passwords)
- » Rebuild or replacing systems on which the attacker has installed malware or utilities
- » Deny "uncategorized" web traffic at web proxy
- » Reconnect environment to the internet
- » Validate that key applications are working appropriately

3 STRATEGIC PLANNING

Consider these activities to ensure long-term success combatting targeted threats.

Improve Network Architecture

- » Document and understand critical applications' network data flows
- » Periodically validate network device rulesets
- » Implement network segmentation
- » Implement web application firewalls to reduce the risk of web application vulnerabilities
- » Implement web proxies for all users, restricting access to "uncategorized" web sites
- » Build restricted, high security zones for critical data and applications

Create Investigation-Ready Environment

- » Create inventory of systems that store sensitive data and designate a business and IT point of contact for each
- » Define the IR team's structure and responsibilities
- » Define an IR plan
- » Aggregate log sources into a SIEM tool
- » Record and preserve logs for at least one year
- » Tune host-and network-based intrusion prevention systems to alert on anomalies that indicate potential attacker activity
- » Augment monitoring mechanisms with a threat-based monitoring service
- » Conduct tabletop exercises to test the IR plan

Enhance Authentication and Authorization

- » Upgrade workstations to Windows 7 which implements User Account Control
- » Remove local administrator rights from the majority of users
- » Reduce the number of privileged domain-wide service accounts
- » Implement a set of accounts designed for use during an incident response. These accounts are normally disabled
- » Implement multi-factor authentication

Invest in People

- » Build or outsource a dedicated security team
- » Structure roles to provide the team time to focus on investigating suspicious events on a daily basis

4 GOING FORWARD

Enact immediate containment measures at first sign the attackers have regained access.

CONCLUSION

It is clear that the adversary is evolving — we have known that for years. However, in a decade of responding to advanced targeted threats, 2011 was an inflection point. Not only is the APT evolving its tactics, we see the entire information security industry elevating its game in ways that render traditional methods of detection and response obsolete.

It is becoming harder to differentiate traditional APT attacks from highly skilled intrusions that target financial data. And thanks to their use of off-the-shelf malware it is sometimes even difficult to discern an APT attack from the ongoing "noise" of everyday drive-by malware infections.

We have seen financially motivated attackers embrace APT-style persistence mechanisms while the APT gets more resourceful in cribbing backdoor communication mechanisms from Russian organized crime groups. Financial fraudsters are moving from opportunistic attacks toward performing reconnaissance on their targets, and we now see the APT stepping back to take their reconnaissance to a new level. Where we once worried about a company being specifically targeted for its data, we now see clear signs that entire technology platforms are the new target, and the adversary is patient enough to assemble the intellectual property portfolio from its component pieces.

Despite all of this, a few things have not changed: visibility is paramount, smart people are more important than any technology, and the way you respond — when the inevitable happens — is what will determine whether you become a headline or not.

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-Unition*, follow us on Twitter *@Mandiant* or Facebook at *www.facebook.com/mandiantcorp.*

MANDIANT®

MANDIANT®

www.mandiant.com