MANDIANT®

Trends

[when prevention fails]

CONTENTS

SECTION I

[INTRODUCTION]

One year ago, Mandiant's first M-Trends report detailed how the Advanced Persistent Threat (APT)[1] successfully compromised its victims. Our case studies illustrated the attacker's willingness to target commercial America and multinational firms, as well as government entities.

Today, the attackers continue to expand their targets and innovate their techniques.

In this report, we'll further explore those attack techniques, and we'll provide key steps you can take to address the threat in your enterprise.

Over the last year, Mandiant consultants have helped a number of large, multi-national corporations investigate widespread intrusions by the APT. Using our Intelligent Response product we investigated millions of desktops, laptops and servers, and we worked on every continent but Antarctica.

And in all of these incidents, the APT attackers used many of the same tools and tactics as other intruders. Yet despite these similarities, there are enough differences between the APT intruders and non-targeted attacks to create additional challenges when responding. Some of these differences include:

It is no longer acceptable to rely solely on preventive measures. Combating targeted threats requires a sustained effort and the capability to perform rapid threat detection and response.

- They have thousands of custom versions of malicious code (malware) that circumvent common safeguards such as anti-virus.
- They escalate the sophistication of their tools and techniques as a victim's capability to respond improves.
- They maintain their presence within the victim network and, if lost, they repeatedly seek to regain that presence.
- They target vulnerable people more often than they target vulnerable systems.
- They specifically target victim firms — the intrusions are very different from commodity threats and other targeted attacks by organized crime syndicates.

[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 capabilities we describe will combat targeted attacks.

The most revealing difference is that when you combat the APT, your prevention efforts will eventually fail.

Because of these characteristics, APT intrusions present different challenges than addressing common computer security breaches. The most revealing difference is that when you combat the APT, your prevention efforts will eventually fail. Combating the APT requires a sustained effort and the capability to perform rapid threat detection and response.

In the rest of this report, we'll share our experience and recommendations to help you better position your organization's people, process and technology to fight a threat that can't be dealt with the old way.

DEFINING THE WIN

Winning against the APT may not mean you are preventing attacks. Instead winning for your organization may mean that:

- You are able to predict, detect and respond to the APT intruder's next move.
- You are increasing the cost and effort required by the APT intruders to compromise your network — ultimately approaching "too expensive".
- You have the host-based and network-based visibility to create your own threat intelligence and perform proactive threat detection and response.
- You have the enterprise host-based and network-based capability to rapidly deploy threat intelligence from industry and third parties.

ESSENTIAL HIGHLIGHTS IN THIS M-TRENDS

Steps to Overcome Common Challenges Organizations Face When Confronted by an APT Intrusion	
Define the Win	» Ensure your organization has a clear understanding of how it will define a successful recovery from a breach by APT attackers.
Assign Accountability	» Remediation plans fail when accountability for their execution is not clearly assigned to an individual. Each business unit should assign an individual who becomes responsible for the implementation of the plan.
Appropriately Assign or Obtain the Resources Required to Obtain Your Goal	» Remediation fails due to lack of resources — lacking the personnel, technology and processes to follow through on the remediation plan.
Establish Visibility	» Without host-based visibility, network-based visibility, proper logging and threat intelligence (knowing what to look for), you will not be able to determine the scale of the intrusion, or detect and recover from the APT with agility.

Potential Missteps When Responding to the APT	
Performing Noticeable Remediation Prior to Understanding the Full Scope of Compromise	» Removing compromised systems from the network prior to complete incident diagnosis. » Blocking malicious IP addresses and/or domain names prior to complete incident diagnosis. » Performing tactical and ongoing password changes rather than holistic and comprehensive password changes.
Submitting Malware to Anti-Virus Vendors Prior to Performing Your Remediation Event	» You want to remediate on your terms, not when AV companies decide you are remediating. » When AV signatures change, they usually trigger on only a small portion of the malware on the compromised hosts. » When AV updates, the attacker updates their malware to continue circumventing AV.

Items Needed to Establish Operational Readiness to Respond to the APT	
Total Visibility Across the Enterprise	» Host-based visibility » Network-based visibility » Increased logging » Log aggregation
Actionable Intelligence	Threat intelligence derived internally and from outside sources including: » Relationships with peer organizations » Defense industrial base » Law enforcement » Vendor-specific threat feeds

SECTION II

[EMERGING APT TARGETS AND TACTICS]

This section focuses on several different aspects of the APT's behavior including:

» victim organizations and their industries;

» the information targeted and stolen by the APT;

» the persistence mechanisms employed to maintain a foothold within a victim's network; and

» the use of social media sites to manage malicious command and control (C2) channels.

VICTIM COMPANIES AND ORGANIZATIONS TARGETED BY THE APT

Mandiant's consultants have been responding to incidents for over 15 years. During that time, we have seen the APT intruders expand their targets from attacking government agencies to attacking many commercial entities.

Mandiant has seen a growing number of commercial entities compromised within the past five years. In our experience, if your organization is doing merger and acquisition (M&A) activities in the Asia Pacific, or you are a law firm representing organizations conducting M&A activities in the Asia Pacific, you are more prone to being a target of the APT. Among the commercial entities targeted, Mandiant has helped victims in the following industries:

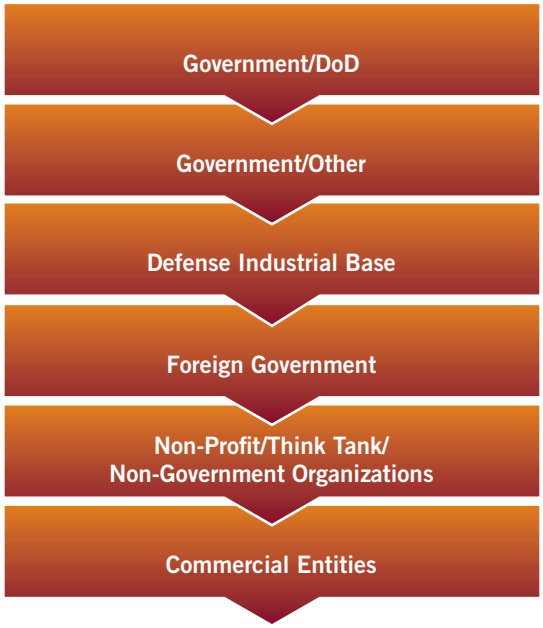
» Automotive

» Space and Satellites and Imagery

» Cryptography and Communications

» Mining

EVOLUTION OF TARGETS BY INDUSTRY



» Energy

» Legal

» Investment Banking

» Media/Public Relations

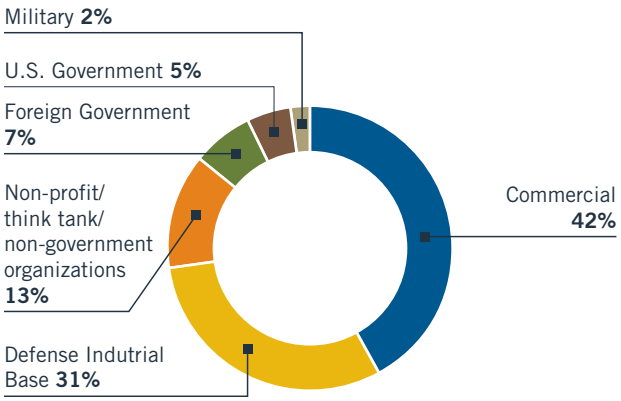
» Hospitality

» Chemical

» Technology

The following chart outlines the victim organizations categorized by industry. This information was derived from approximately 120 APT victims Mandiant had exposure to over the past 18 months.

PERCENT OF OVERALL VICTIMS BY SECTOR



Commercial Sector Breakdown	
Automotive	2%
Space and Satellites and Imagery	19%
Cryptograph & Communications	20%
Mining	2%
Energy	18%
Legal	9%
Investment Banking	3%
Media/Public Relations	10%
Hospitality	2%
Chemical	5%
Technology	10%

ASSETS TARGETED AND STOLEN BY THE APT

The primary goal of an APT attack group is the theft of data. We have seen the APT specifically target sensitive, engineering data along with non-sensitive, policy documentation. We have also seen evidence that the APT will compromise whatever is necessary to achieve this goal. For example, the APT attackers have compromised both soft certificate PKI credentials as well as hardware-based PKI credentials. The following sections detail how the attackers are able to steal data and compromise PKI credentials.

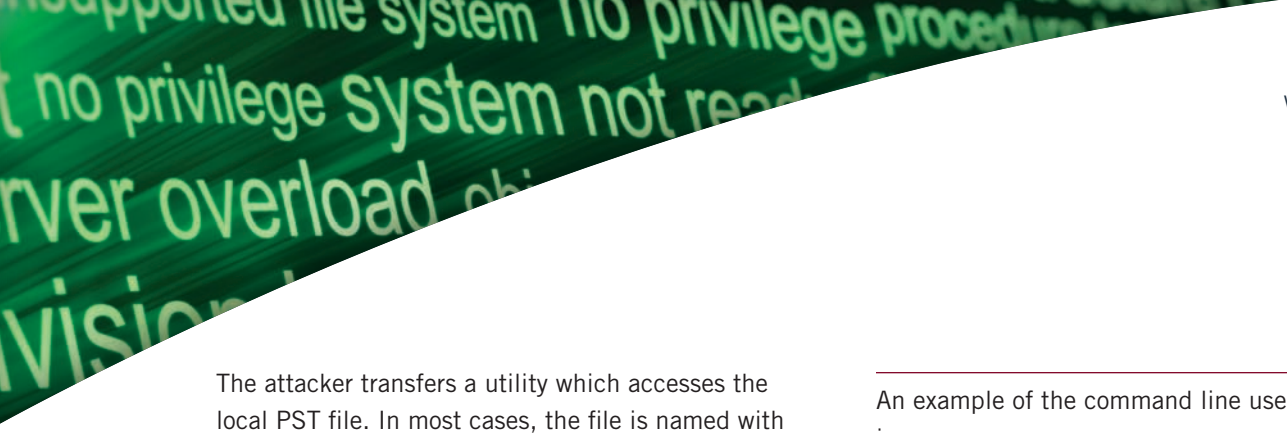
Theft of E-mail

E-mail harvesting continues to be the best method for attackers to obtain time-sensitive information and updates to confidential technical programs. The attackers use two avenues to acquire a targeted individual's e-mail: 1) they individually acquire local Windows Exchange e-mail files (PST files) from specific user systems; or 2) they harvest multiple e-mail mailboxes from the e-mail server (Windows Exchange or Lotus Notes) within a single session.

The acquired e-mail inboxes contain valuable information about senders and recipients, attached documents and revisions to documents, discussion threads and personal details about individuals. The attackers use this information to profile other organizations and individuals involved in the same projects as the original target. They also gain access to items they can use to create realistic spear-phishing e-mails, including authentic e-mail content and legitimate Office and PDF documents into which they insert malware.

The mechanics of e-mail harvesting

Mobile users tend to have the most recent e-mail within their local e-mail file (the local PST file). Mobile users may include those who are involved in negotiations abroad or executives who frequently travel. In most cases, attackers compromise the target's system via a spear-phishing e-mail and install a backdoor. After the initial compromise a second backdoor is installed.



The attacker transfers a utility which accesses the local PST file. In most cases, the file is named with a single letter, "g.exe" or "m.exe", and is transferred to the victim system. The e-mail extraction utility requires the location of the PST file, a timeframe from which to extract the contents of the e-mail and an output directory. Successful e-mail extraction requires authentication of the mobile user's account or a local administrator account. The e-mail output is directed to the attacker's working directory, then archived by the attacker and transferred from the compromised system to the attacker's C2 server. The attacker deletes all evidence of the e-mail output and e-mail extraction utility. E-mail harvesting, like any process, can be scripted for efficiency and executed from a lateral system against e-mail servers to acquire multiple e-mail mailboxes.

Extracting e-mail from individual systems is most effective early within the attacker's life cycle of compromise or when the information is of importance for the attacker. As e-mail compromises are protracted events, attackers script the e-mail harvesting to acquire multiple mailboxes at a time.

The attacker performs e-mail harvesting from a compromised internal system that has access to the central e-mail store (such as Exchange or Domino). This compromised system is usually not related in any fashion to the person who owns the targeted e-mail account. The attacker requires the user credentials for the victim e-mail accounts. The attacker authenticates to the e-mail server as the specified user, extracts e-mails within the time frame specified and saves all e-mails and attachments to the specified directory. The attacker automates this by using a tool called "mapi.exe", which passes the configuration information to the e-mail server.

An example of the command line used by the attacker is:

```
mapi.exe –s:exchangeserver.domain.com
–u:user1 –t:2011-01-10-01 –o:c:\windows\
help\help
```

In this example, the attacker has specified the Exchange server as "exchangeserver.domain.com", the user as "user1" (note that the application prompts the attacker for the user's password), the time frame as 01:00 January 10, 2011 through present, and the directory to save all data as "C:\windows\help\help". The result of using "mapi.exe" is that e-mail is stored as a numbered text file, and e-mail with attachments is stored in numbered directories.

```
Directory of C:\Windows\Help\help\user1\
11/29/2010  08:05AM       907,704 1-mail.txt
11/29/2010  08:05AM       568,110 2-mail.txt
11/29/2010  01:21AM    <DIR>              3
11/29/2010  09:28AM    <DIR>              4

Directory of C:\Windows\Help\help\user1\3
11/29/2010  08:05AM           1,024 mail.txt
11/29/2010  08:05AM  568,110 Attachmend1.PDF
11/29/2010  08:06AM  332,800 Attachmend2.XLS

Directory of C:\Windows\Help\help\user1\4
11/29/2010  08:06AM           1,024 mail.txt
11/29/2010  08:07AM  136,222 Attachmend1.PDF
11/29/2010  08:07AM  151,722 Attachmend2.PDF
```

The attacker can obtain the contents of multiple user e-mail accounts by using another utility, such as "mapiget.exe", which takes a text file as input. It should be noted that all MAPI traffic sent by the mapi.exe and mapiget.exe malware are indistinguishable from MAPI traffic sent by Microsoft Outlook.

Theft of Public Key Infrastructure (PKI) Data

Throughout the past year, the APT attackers have increasingly focused on obtaining PKI-related information resident within a compromised network. PKI implementations encrypt data or communication channels using a private key associated with a public certificate.

PKI data has many uses within an enterprise environment. For example, it may be associated with an individual system for Secure Socket Layer (SSL) sessions — such as HTTPS — or with an individual user for Virtual Private Network (VPN) communications.

The implications of compromised PKI credentials are significant for either implementation:

» Attackers can leverage a user's stolen PKI credentials to authenticate to a client VPN and masquerade as a legitimate account.

» Attackers can use stolen private keys and certificates to decrypt SSL traffic from servers and examine their contents.

Attackers have also used stolen PKI information to encrypt command and control traffic to victims. In the past, most SSL-based C2 communications were conducted using self-signed certificates created by the attackers. Mandiant has seen at least six different sets of stolen PKI credentials used to encrypt command and control traffic during investigations in 2010.

» Five of the six credentials had not been revoked and were still valid at the time of identification.

» Three of these six were signed by third-party organizations.

» Four of the six credentials were originally associated with PKI user credentials.

» Two of the six were used to encrypt SSL communications to identified web servers.

» The stolen PKI credentials were used to encrypt C2 activities at targeted victims that had no association with the original certificate owners.

» Stolen PKI information was re-used to encrypt C2 at multiple victims, implying that attackers have a finite supply of these credentials.

At organizations with widespread two factor authentication implementation, the percentage of systems with keystroke loggers has been as high as 60%, which is inconsistent with the low profile maintained by attackers during most APT compromises.

Identifying the use of stolen, third-party PKI credentials within a compromised environment can be extremely difficult, particularly since they are utilized by custom backdoors that provide no user-visible alerts for untrusted or revoked certificates. Even if the certificate is revoked, in most cases only the organization that actually owns the certificate would be able to identify when it was used on their own network for attempted legitimate access, such as for VPN authentication.

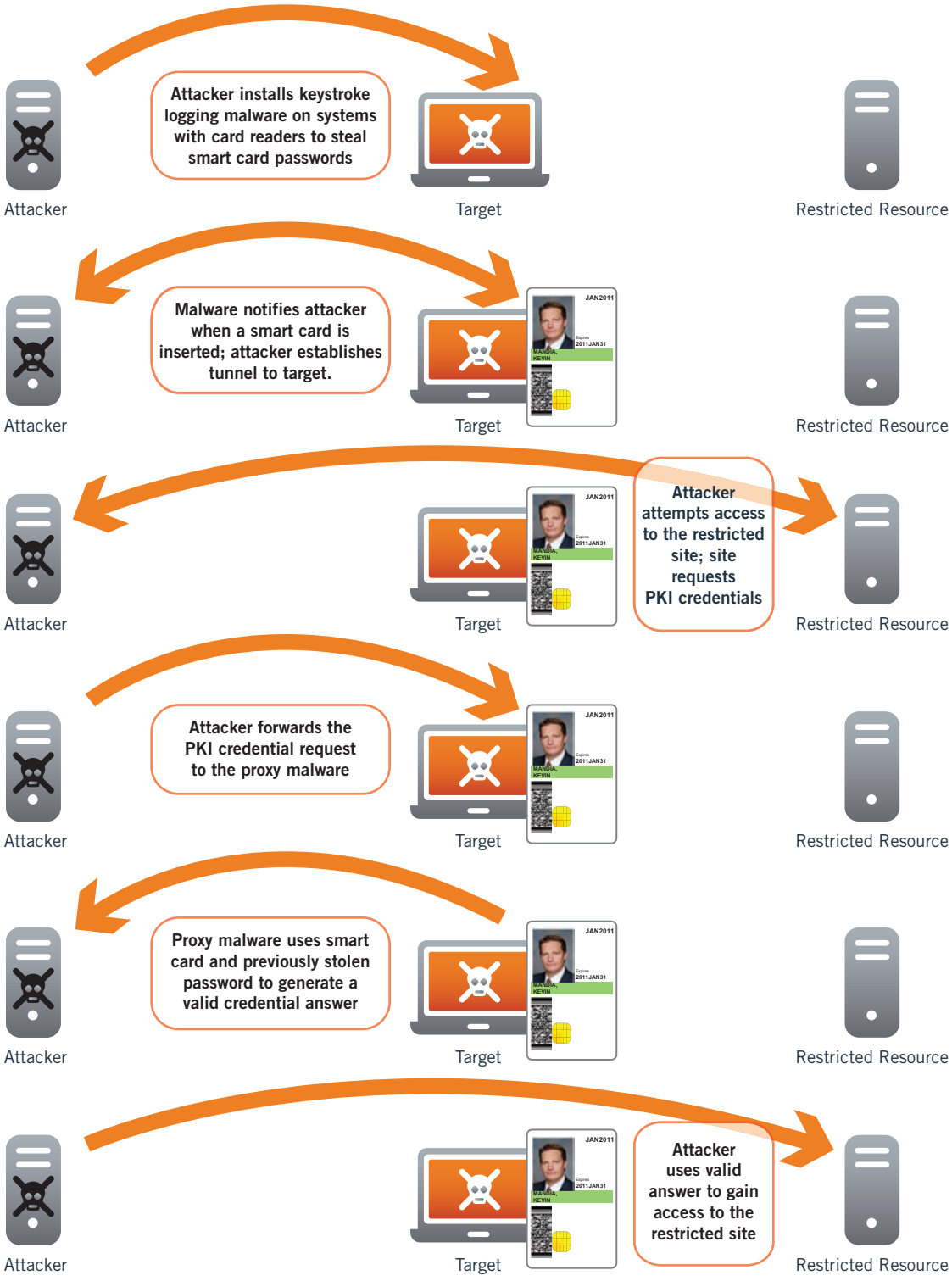
In light of this trend, organizations should review their existing security controls and processes to protect PKI-related information. Reliance on soft key and certificate technology, such as using VPN credentials in PKCS7 or PKCS12[2] format, should be limited wherever possible. A move to hardware-based PKI key technology also can reduce the impact of certificate and key theft. However, as discussed in the following section, attackers are also targeting these solutions.

Attacks on Hardware-Based PKI Technology

Hardware-based PKI implementation requires the use of a smart card and a smart card reader. A smart card reader is a device that reads information from a hardware token containing private keys and certificates, typically embedded into a card on a chip. When the hardware token is plugged into the smart card reader, the reader uses the information on the chip to authorize access to a restricted resource such as a computer system, network, or restricted

[2] See RSA Labs for PKCS standards: http://www.rsa.com/rsalabs/node.asp?id=2124

USING A SMART CARD PROXY



web site. When used in single-factor authentication, the mere presence of the hardware token within the reader authenticates the user to access the restricted resource. In two-factor authentication, the presence of a card in conjunction with a password allows the user to access the restricted resource.

Mandiant has investigated several cases where the APT attackers took advantage of smart card readers using a similar approach. In each case, the intruders first gained access to the victim's network and installed backdoors on multiple hosts to maintain persistence. The attackers then transferred and executed tools that were capable of detecting the presence of a smart card reader on the compromised systems, and identifying whether a card was inserted into the reader.

First, the attackers identified hosts with card readers used for two-factor authentication. Then, the attackers installed keystroke loggers on those hosts to obtain the password or personal identification number associated with the smart card.

In another case, attackers installed additional malware that beaconed to a command and control system when a smart card was inserted in the compromised system. Once the attackers had obtained the password associated with the smart card, and determined that the card was inserted in the compromised system, they could transform the compromised system into a "smart card proxy".

Attackers took advantage of this "smart card proxy" by running additional malware on the compromised system. The attackers issued a web request to the restricted resource which was redirected through an encrypted tunnel to the compromised system containing the smart card. The malware received the request and through third-party API calls, signed the data using the inserted smart card and the victim's password. The signed data was sent back to the attacker's command and control server and eventually back to the restricted resource. The restricted resource authenticated the user and sent the response back to the attacker. The attacker then had access to the restricted resource using legitimate user credentials without ever stealing the private key required to gain access.

There are several ways to reduce the likelihood an attacker would be able to compromise hardware-based tokens. Removing smart cards when not in use is the easiest way to mitigate risks, however moving to other hardware based technologies such as RSA Tokens with time-based sync of passwords is an effective way to thwart this threat.

INITIAL EXPLOITATION OF VICTIM NETWORKS

Of the approximately 120 organizations that Mandiant observed in the last 18 months, the majority of them were either compromised by a targeted e-mail campaign or were victims of a prior intrusion that was never appropriately remediated. In many APT investigations, we learn that Victim 0 in the current intrusion set was actually Victim 127 in an intrusion dating back years ago. In other words, there was no new exploit to obtain access to the victim networks, they had unknowingly remained in a compromised state for years. Therefore, since e-mail campaigns are by far the most common attack vector, we will provide an in-depth description of how an e-mail campaign is executed.

The majority of victims were either compromised by a targeted e-mail campaign or were victims of a prior intrusion that was never appropriately remediated.

Targeted E-mail Campaigns

Since the onset of perimeter hardening first began in the late 1990s, attackers have shifted tactics to focus on targeting end-users as a means by which to compromise private networks. Spear-phishing e-mails containing malicious attachments or links to hostile web sites have remained one of the most widespread

and persistent intrusion techniques since this time. Although organizations have been suffering from such attacks for many years, the process by which sophisticated threat groups develop, coordinate and execute targeted phishing campaigns are not always well understood or publicized.

During the course of several investigations, Mandiant observed a group of attackers perform multiple, concurrent, highly-targeted phishing campaigns over a six week period from mid-August through the end of September, 2010.

Starting in the second week of August 2010, attackers used third-party e-mail service providers to send targeted e-mails to a variety of organizations. At Victim A, attackers sent multiple e-mails that contained a link to a ZIP file with information about the organization's management team.

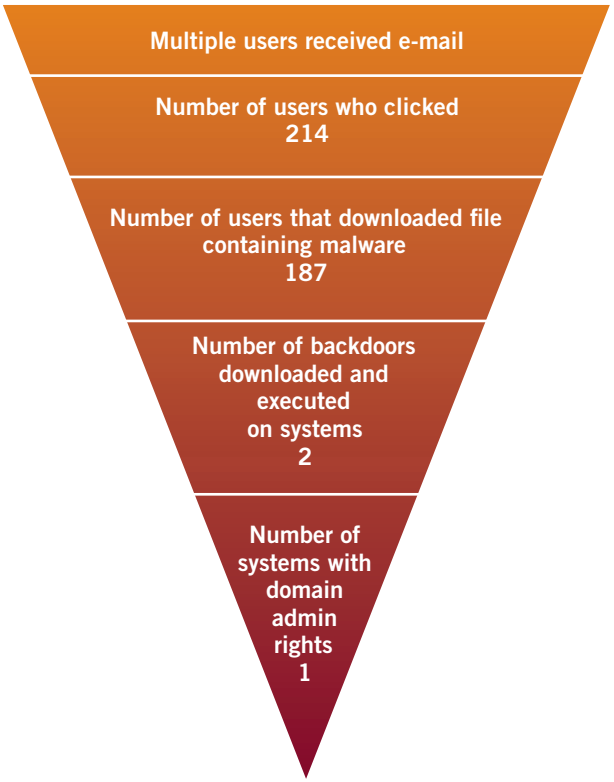
The ZIP archive contained several benign files and an executable disguised as a PDF document via a modified resources section. When executed, the malware beaconed to a domain that contained the organization's specific name as the third level of the address (such as "victimA.youareowned.com").

Less than a week later, Victims B and C were targeted by the same e-mail containing links to similar ZIP files. However, the malware in each ZIP file was customized to beacon to a different domain name distinct to each targeted organization (such as "victimB.youareowned.com"). The executable file was also disguised as different document file types, including Microsoft Word and Excel files, using the same types of modifications to their resources sections.

Approximately two weeks later, attackers sent a second set of e-mails to multiple organizations, many of which were the same ones targeted during the first round of messages. The e-mails and the linked ZIP files were crafted in a similar manner but with a few small distinctions: the non-executable files in the ZIP contained information related to each organization's business leaders, and the hard-coded, second-level domain name had changed in each instance of the malware. The third-level names unique to each victim remained unchanged.

After another week, attackers sent a third and final round of e-mails to multiple organizations. The ZIP files linked from these messages contained press materials that appeared to originate from open source research on each organization. The executable malware also used a different hard-coded, second-level domain name once again (such as victimA.iamcompromised.com).

IT ONLY TAKES ONE VULNERABLE USER...



Across all three sets of targeted attacks, the executable within the ZIP file contained minimal changes. The executable read commands from a compromised web page. Based upon the command, the file either downloaded an additional backdoor or would sleep for a specified period of time. This targeted attack resulted in over one hundred compromised users at multiple organizations.

HOW THE APT MALWARE MAINTAINED PERSISTENCE

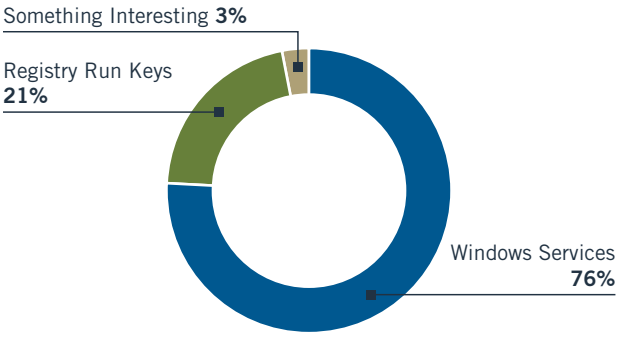
The APT attackers successfully install and run persistent malware on systems within a victim network. They have employed a diverse portfolio of techniques which heavily favor stability and simplicity over stealth. In our 2010 M-Trends report, we observed that 76% of APT malware specimens we collected used Windows Services for persistence and 21% used the Registry Run keys, leaving only 3% using other techniques. This small set of remaining outliers is the most intriguing, because it contains the majority of the creative and advanced techniques.

It may seem counter-intuitive that a successful and determined attacker would rely heavily upon well-known techniques. It remains a simple fact that these techniques are still effective in the majority of cases and remain difficult to detect by organizations that lack a dedicated incident response staff. More advanced techniques, such as rootkit functionality, often have stricter requirements of operating system version and privilege level or may introduce system instability. In highly targeted attacks, the benefits of these techniques are often not worth the "costs" associated with their research, development and reliability.

Windows Services

Windows Services continue to be the most common persistence mechanism used by the APT when installing malware. Although this feature is a fundamental and relatively simple component of the operating system, the overwhelming variety of native and third-party software services installed across hosts

USING WINDOWS SERVICES AS A PERSISTENCE MECHANISM



in a typical Windows environment provides an excellent opportunity for attackers to hide their malware "in plain sight".

Attackers can either install their malware as a new service on a compromised system or replace an existing service. Each approach has its own benefits and trade-offs. Installing malware as a new service is a more stable approach that avoids the need to alter an existing service's functionality or remove it from the system. However, the attacker must configure the new service with appropriate descriptive data in order for it to effectively blend in. A Windows Service will typically contain a short Name, Display Name (long form) and a detailed Description. This manufactured data can serve as indicators of compromise to be used by an incident responder when examining other systems on the network.

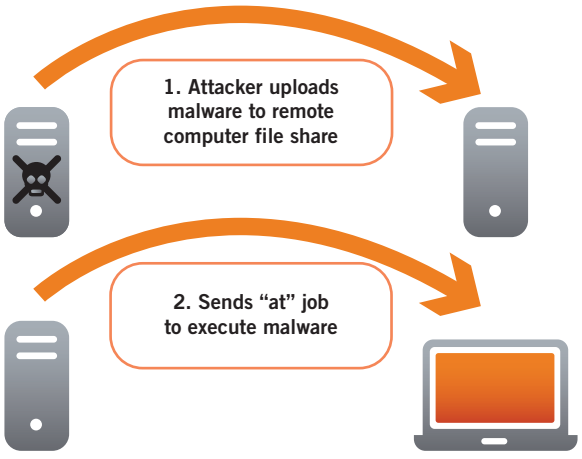
Service replacement is a stealthier approach that attackers use to maintain persistence. The Windows Registry keys for each service contain references to the binary that implements the service. By changing these values and restarting the service, the attacker can make their malicious code appear as though it was an existing service. A side effect of this approach is that the service chosen for replacement will no longer operate on the system. Not all services can be replaced in this fashion without consequences.

Services that are likely targets for replacement are often disabled by default or provide functionality that is not used by the system. For example, the "Wireless Zero Configuration Service" (wzcsvc) is often hijacked by attackers on servers since it is unlikely to be in use and can therefore be disabled without any deleterious effects. Specialized services such as the "RIP Listener service" are replaced on compromised workstations due to the low likelihood that an end-user's system would be making use of this routing protocol.

One of the most common ways the APT installs malware as a Windows Service is by using the at.exe (task Scheduler) command. The at.exe command is a native Windows utility that allows a user to view scheduled tasks or to schedule a program to run at a specific time. Oftentimes the malware executed is used to create a service or replace an existing service.

Execution of the at.exe command requires local or domain administrative privileges on the target system.

LATERAL MOVEMENT TECHNIQUES



Types of Activities Accomplished:

- list tasks
- obtain directory listings
- download passwords
- install backdoors

WINDOWS SERVICE REPLACEMENTS

- Attackers use services disabled by default
- Side Effect: Service no longer able to be used by system
- Popular Services used:
  - Wireless Zero Configuration Service (wzcsvc)
  - RIP Listener Service (IPRIP)
  - Background Intelligent Transfer Service (BITS)

The attacker elevates their privileges by using either the pass-the-hash technique or by creating a NetBIOS connection to the victim system.

An example of the attacker creating a NetBIOS session is:

```
net use \\<systemA> "password" /u:domain\
john.smith
```

This command will authenticate the attacker to systemA (victim system) as the "john.smith" user. Once authenticated, the attacker will execute malware on systemA using the at.exe command.

An example of the attacker using the at.exe command is:

```
at \\<systemA> 20:26 cmd /c "dfs.exe"
```

This command will execute the evil.exe malware on systemA at 20:26 (the specified time).

In this case, dfs.exe replaced the "RIP Listener Service" with iprinp.dll. All jobs executed by at.exe are logged in the SchedLgu.txt (specific location varies by operating system). Examination of the SchedLgu.

txt file for anomalous entries is a good way to detect malicious activity that used the at.exe command. Restricting NetBIOS communication between end-user systems is a good way to reduce the APT attacker's ability to move laterally through an environment.

Incident responders can use frequency analysis on combinations of service names, service binaries, and service descriptions across an enterprise to find malware installed through either approach. Malware installed as new services is likely to have a much lower frequency of occurrence than other common services installed throughout the enterprise. However, in practice these outliers can often blend in with services from legitimate third-party software or operating system modules enabled on a small number of systems. Validating these false positives can often be a laborious process.

Frequency analysis can likewise be used to identify replaced services that have been configured with a different binary than the default configuration. Once again, this can result in false positives from differences in service executable and DLL filenames among different versions of Windows or third-party software. Mandiant's approach to enterprise-wide identification of anomalous services uses a combination of frequency analysis, whitelisting, blacklisting and digital signature checks to construct more robust indicators of compromise.

Windows Services remains one of the simplest yet consistently effective mechanisms for running persistent malware. For this reason it has, and will likely continue to be, the most prevalent technique used by the APT for the foreseeable future.

Other Persistence Mechanisms

APT attackers have shown recent innovation in their experimental persistence techniques. These techniques occupy the outlying 3% we discussed earlier. The experimental techniques for persistence include:

» DLL search order hijacking;
» use of Group Policy Objects (GPO);
» use of COM objects; and
» modifying system binaries.

DLL Search Order Hijacking is easy to perform and difficult to detect. We expect to see more of this in the future.

DLL Search Order Hijacking

The most notable new technique in the attackers' repertoire is DLL search order hijacking. In some instances found to date, the attackers have placed their malicious DLL under the name ntshrui.dll in the C:\Windows directory. The malware is automatically loaded with no other forensic residue in the registry or file system due to the defined behavior of the Windows loader. The Explorer.exe process is responsible for loading the ntshrui DLL which should normally reside in the System32 folder. Since the Explorer.exe process is launched during each normal system boot cycle, the malware can be safely guaranteed to execute.

The reason this technique is successful is that the Explorer.exe binary resides in the C:\Windows directory and the operating system checks the directory the EXE resides in before the System32 folder when searching for most DLLs. Therefore, the rogue ntshrui.dll is loaded simply by being in the same directory as the executable that loads it and benefiting from the preferential load order. This technique could be applied to many DLL names and processes other than Explorer.exe. If they expand this technique to install to a wider array of locations then detection may be difficult as there is no clear-cut forensic residue marking its use.

DLL Search Order Hijacking is a complex topic. For more technical information, refer to our M-unition blog at http://blog.mandiant.com.

Use of Group Policy Objects (GPO)

One simple, yet uncommon, technique employed recently was the use of a Group Policy Object (GPO) to trigger malware execution on user login. GPOs are typically managed by system administrators with the visual editor provided by the operating system. Their exact internal storage details are not commonly known or audited. By editing the file C:\Windows\System32\GroupPolicy\User\Scripts\scripts.ini, a line can be added to the Logon section to launch a command upon user logon. The attackers have recently used this to ensure that their malware is launched and persists across reboots.

Use of COM Objects

The Common Object Model (COM) provides a mechanism for applications to communicate with each other. Many applications, particularly Microsoft applications, provide the core of their functionality to third-party tools in the form of a COM component. For example, the Microsoft Outlook application makes use of the Microsoft Word COM component to provide MS Word's advanced text editing features seamlessly within the Outlook application.

A recent sample collected as part of an APT attack installed itself as a COM object. It replaced an existing COM object which was installed for use with the company's internal portal web page. Whenever an employee visited the page — which was the web browser's default homepage — from their workstation it would trigger the COM object to be loaded and used to provide functionality. The malware was designed specifically to fit this niche situation and provided the identical interface of the legitimate object, loaded the legitimate object and relayed all requests to the legitimate object as to appear seamless.

...the attackers showcase advanced programming capabilities in persistence techniques by modifying system binaries to launch their malware.

Modifying System Binaries

Occasionally, the attackers showcase advanced programming capabilities in persistence techniques by modifying system binaries to launch their malware. The challenge of modifying a system binary is that, ideally, the binary should be manipulated in such a way that it launches the malware, still operates as intended and is not detected by Windows File Protection (WFP). Since persistence is a goal, binaries that are commonly launched at startup are usually targeted and any flaw introduced in the modification process would have disastrous consequences for system stability. This reduces the availability and effectiveness of the malware installation.

A recent persistence technique observed in an APT attack involved modification of the services.exe binary. Services.exe is responsible for launching all system services and is one of the most critical processes in the system startup. The malware overwrote the code at the beginning of the binary in a way that it retained its original functionality and loaded a secondary DLL. The modification was particularly elegant in that it did not change the size of the binary nor leave any forensic residue that indicated that it was obviously a modified binary. In addition, the attacker called an undocumented API in sfc_os.dll to disable Windows File Protection (WFP), preventing the modified binary from being repaired.

The secondary DLL that was loaded was a custom Windows implementation of the "cron" program from UNIX. "Cron" is a task scheduler program that allows an administrator to configure an exact frequency to run a particular program. In this case, the attacker had supplied a configuration which launched their malware every day at 4:15 a.m. and 12:30 p.m.

USING LEGITIMATE SOCIAL NETWORKING SITES TO MANAGE MALICIOUS COMMAND AND CONTROL SERVERS

Mandiant has seen an increasing number of attackers hijack legitimate third-party Internet services for command and control and data theft. Mass-malware used by botnets and worms have employed similar techniques for many years; however, they have only recently been utilized by the APT. Examples identified during Mandiant's investigations include:

- a first-stage malware downloader that used Facebook messaging for command and control.
- backdoors that used MSN and Google Chat services for command and control.
- backdoors that parsed command and control instructions hidden in HTML comments in compromised web pages.
- a data theft utility that automatically transmitted multi-part RAR files via webmail (Hotmail).

In each of these cases, the attackers effectively camouflaged their remote access as normal SSL-encrypted traffic to popular Internet sites. These techniques were resilient to both packet inspection and netflow anomaly analysis. The data was SSL encrypted, protocol-compliant and transmitted to common endpoints.

Mandiant expects the APT and other threat actors to increasingly leverage the broad array of social networking, cloud computing and online storage sites to conduct their operations. These services are widely available, can easily be obtained without sacrificing anonymity and can provide more versatility than a self-managed attack infrastructure.

The impact to victims is clear: organizations cannot rely solely on standard network monitoring for rapid detection and response to such threats.

SECTION III

[EVOLVING TO COMBAT THE ADVANCED PERSISTENT THREAT]

Up to this point we have talked about whom the attackers are targeting, what they are taking from victim networks and how they are maintaining a presence on those networks. The question we have not answered and that we hear most often from organizations looking to strengthen their IT security programs is, "What's next?"

During the investigations into APT activity Mandiant has conducted over the past several years, we have learned that most organizations focus the majority of their security budgets and efforts on prevention techniques while largely ignoring response activities (detection and response).

While preventive measures such as anti-virus, patching, vulnerability management, network monitoring and intrusion detection are a necessary part of any fundamental information security program, these safeguards do not prevent all intrusions. A mature IT security program should include not only these industry accepted best practices, but should also incorporate a rapid threat detection and response capability.

In this section we discuss the need for total visibility across your enterprise and the importance of using actionable threat intelligence to remain vigilant against targeted and advanced threats.

TOTAL VISIBILITY ACROSS THE ENTERPRISE

The first thing Mandiant does when we respond to an incident is gain insight into what is going on across the enterprise at both the network and host levels. This provides us with a big picture understanding of the intrusion and allows the investigative team to gather the very detailed data needed to understand the compromise at a microscopic level.

This visibility provides the foundation for an organization's threat detection and response capabilities and provides the means to detect both known and unknown "bad".

Most security software prevents or detects a high number of known threats. While you need to have these capabilities in order to detect the botnets and viruses that cause interruptions to your organization's daily operations, they miss the advanced threats being used to target your most sensitive information. Additionally, much of this software — although not all of it — is designed to limit your control over what threats are detected, how the detection occurs and when you remediate.

Specialized monitoring systems should be used to complement these existing monitoring capabilities — not to replace them. These specialized systems should concentrate on detecting the tools, tactics and procedures (TTPs) of an attacker.

When we talk about achieving total and enhanced visibility we categorize it in four ways: host-based visibility, network-based visibility, increased logging and log aggregation.

Host-Based Visibility

Host-based threat detection tools utilize threat intelligence from both external and internal resources to look for specific indicators of compromise and detect the presence of known "bad." They are used to search for attacker TTPs on hosts and complement existing anti-virus solutions.

In addition, advanced techniques for identifying unknown malware can be implemented using these tools. As an example, by using such host-based detection, investigators can identify non-signed binaries residing in the Windows subdirectories that load as a service (note that these binaries will not always be malware). Upon reverse engineering the malware, they develop additional indicators that are then used to search for the attackers elsewhere in the network.

Network-Based Visibility

Network-based threat detection tools leverage or complement existing IDS and utilize threat intelligence to look for specific attacker TTPs within network traffic. In addition, these threat detection tools should record all malicious traffic for later analysis if needed.

This capability should provide a response team with real-time alerts and enable the retrieval of all traffic associated with an incident. An important consideration is whether the end host involved can be immediately identified, since network devices that obscure end hosts[3] are increasingly being used.

Ultimately a network alert tool can be integrated with a host-based monitoring and detection solution or a Security Information and Event Management (SIEM) to provide immediate capability to investigate an impacted host.

Log Aggregation

A SIEM capability will ideally reduce the number of potential alerts an analyst needs to investigate by correlating information from numerous sources, and highlighting the most critical information. In addition, a SIEM will enhance any investigation by storing in one place, all or most of the logs necessary to investigate an incident.

Another essential piece of the detection puzzle is the log management system, which indexes all incoming information and allows an analyst to quickly mine historical data to find additional compromised systems when an indicator of compromise is identified. This is a great way to locate sleeper malware, or malware that only communicates every once in a while.

Enhanced Logging

While most companies do not have a mechanism for centrally logging or archiving log data, we have found that data provided by the sources listed below can be critical to a successful investigation.

Internal DNS Server Logs

Many organizations utilize Microsoft's Active Directory integrated DNS servers for internal name resolution. These internal DNS servers are often configured to use external DNS servers (as in a split-DNS architecture) for external name resolution. The information stored in the Windows DNS event log does not include information about actual DNS queries made. This information is crucial in an investigation to identify systems communicating with malicious domains. In addition, it is sometimes possible to track lateral movement within your organization through the DNS queries performed by compromised systems to other internal systems. Enabling Microsoft DNS debug logging will provide all necessary information; the debug logs store information such as source system, queried domain, and returned IP address.

[3] Examples include NAT, load balancing and proxying.

DHCP Logs

DHCP logs are useful to determine the system an IP address was assigned to at a specific time. These logs are especially important for identifying the system that was the source of past activity.

Enhanced Microsoft Windows Event Audit Logs

Many organizations enable logging of failed authentications but neglect to log successful authentication. This prevents organizations from tracking the use of compromised accounts to better understand attacker activity. Storing these events in a centralized location will allow an investigator to quickly identify lateral movement on known compromised accounts.

Border Firewalls Logs with Ingress/Egress TCP Header Information

Organizations commonly log all denied inbound traffic. When investigating a compromise, allowed ingress and egress traffic is more interesting than blocked ingress traffic. These logs can be reviewed to determine how many internal systems were communicating with a malicious IP address identified during an investigation, as well as how much data was transferred and the time(s) the activity occurred.

External Webmail Access Logs

Attackers are increasingly using stolen credentials from targeted users to log into webmail to read the compromised user's e-mail. Logging and regularly reviewing webmail authentication may lead to the detection of a compromised account.

Internal Web Proxy Logs

Internal web proxy logging is often a good way to discover unique characteristics about how malware performs requests, such as the User Agent string, supported platforms, browser type, etc. In addition, if an organization restricts access to uncategorized web sites, web proxy alerts may assist in the detection of a compromised system.

VPN Logs

Attackers are increasingly leveraging VPN access after they have compromised an environment. This allows the attacker to interact with the environment virtually undetected. Ensuring that VPN logs contain at least the source IP address, hostname and user authenticating can assist in detecting a compromise.

HIDS/HIPS

Many end point protection software applications offer the ability to alert on suspicious activity, such as remote writes to the %systemroot%\System32 directory. When implemented and logged, this information can be critical during an investigation.

Netflow Logs

Netflow logs share similarities with firewall logs and web proxy logs, but are often valuable to determine internal system to system communication. Border devices often miss internal lateral movement because they are only aware of the communication between the external system and the compromised internal systems being used as an internal hop point.

Full Packet Capture Logs

Many security and IT professionals believe that full packet capture logs are too costly to implement at their major network boundaries. We have seen more than one company successfully implement full packet capture logging for 30 days of traffic, at their boundaries, so it can be done.

In the event of a compromise, the level of detail provided by a full packet capture is crucial. If a compromise is identified within 30 days of the initial intrusion, all aspects of the compromise can be investigated and understood (note that this depends on whether or not the attacker used network encryption). Additionally, if data theft occurs, storing full packet capture allows for a more specific damage assessment.

Specific network hardware exists that is designed to perform this type of activity and should reduce the overall cost to implement.

Ultimately, the objective of increasing visibility across the enterprise is to allow your organization's IT security team to determine an attacker's activity and anticipate where they may go next. By employing tools that comprehensively monitor targeted assets and personnel, it is possible to develop a greater understanding of the type of information the attacker covets, as well as greater knowledge about the tactics they use.

The essence of threat detection and response is developing a scalable, robust, process to develop indicators of compromise and to integrate them into existing network-based and host-based monitoring capabilities.

ACTIONABLE THREAT INTELLIGENCE

Once you have achieved total visibility across your enterprise, the next focus should be on obtaining and developing threat intelligence. Threat intelligence consists of comprehensive indicators that describe the trace evidence left behind by attackers, including common log file entries, malware characteristics, registry entries, configuration files and any other host-based indicators of compromise.

While some threat intelligence comes from external sources, a truly mature IT security program will have the capability to develop their own intelligence. They should also forge the relationships necessary to collect and share threat intelligence with external sources.

There are several external sources from which organizations can collect this intelligence, including law enforcement, peer organizations within an industry — such as the defense industrial base — and vendor-specific threat feeds. These sources can provide you with "known evil". You will also need the historical data to mine for this information and to artfully identify "unknown evil". It is virtually impossible to identify and detect "unknown evil" without the correct data and context.

Indicators of Compromise

We use the term indicators of compromise (IOCs) to describe the TTPs used by attackers.

IOCs are used to describe remnants or trace evidence of a computer crime, often a computer intrusion. Mandiant uses them to codify the characteristics that define the tools, techniques or processes used by an attacker. Historically, this threat intelligence has been provided as lists of MD5 hashes, file names and/or descriptions of malicious behavior. This information usually lacked actionable detail, lacked longevity and accuracy and did not provide adequate means to fully scope a compromise. Attackers learned long ago how to circumvent such rudimentary signatures. In order for your organization to fight back with the

THIRTY-SEVEN CHARACTERISTICS AN IOC CAN BE COMPOSED OF (OUT OF OUR CURRENT 233)

Characteristics	Definition of Characteristic
File Accessed Time	Last access time of a file
File Attribute	Attributes of a file (Read-only, Hidden, System Directory, etc.)
File Changed Time	File name modified of a file
File Compile Time	Checks the compile time of a file
File Created Time	Creation time of a file
File Digital Signature Description	Description of whether the signature is verified or not
File Digital Signature Exists	Verifies that a digital signature exists
File Digital Signature Verified	Verifies a digital signature is valid
File Export Function	Export function declared by a file
File Extension	Extension of a file
File Full Path	Full path for a file
File Import Function	Import function declared by a file
File Import Name	Import name declared by a file
File MD5	MD5 of the file
File Modified Time	Modified time of a file
File Name	Name of a file
File Owner	Owner of the file
File Path	Path of a file
File PE Type	Checks the PE type of a file

Characteristics	Definition of Characteristic
File PeakEntropy	Peak entropy of a file
File Raw Checksum	Calculated checksum of a file
File Size	Size of the file
File Strings	Readable strings of a file's binary data
Network DNS	DNS queries on a network
Network String URI	URI associated with network traffic
Network String User Agent	User agent associated with network traffic
Process Handle Name	Name of a process handle
Process Name	Name of a process
Registry Key ModDate	Modification time of a registry key
Registry NumSubKeys	Checks the total number of subkeys associated to a registry key
Registry Path	Path of a registry item
Registry Text	Contents of the registry text field
Service Descriptive Name	Description text of a service
Service DLL	DLL implemented by a service
Service Name	Name of a Service
Service Path	Path to the service file
Service Status	Checks the current status of a service

most advanced threat detection available, the industry must advance the means by which we codify and share threat intelligence. Therefore, industry experts have developed the OpenIOC project, which is an XML schema for the description of technical characteristics that identify a known threat, an attacker's methodology or other evidence of compromise. The OpenIOC Project was spurred by the lack of effectiveness or standards for sharing cyber intelligence.

An IOC is usually a Boolean decision tree that describes an indicator using any number of discrete characteristics — OpenIOC offers approximately 233 different criteria. The relationships between the characteristics define a single indicator. When the tree evaluates as true, trace evidence of a particular tool or technique is present on a system. The XMLformat is open, documented and, unlike many XML schemas, simple to edit.

For more information about indicators of compromise and the OpenIOC schema, refer to our M-unition blog at http://blog.mandiant.com.

It is worth noting that not all sources of data have the same value. It is important to filter sources so that you do not spend unnecessary time weeding out false positives, which is ultimately counterproductive. All threat intelligence should be reviewed and customized for your specific environment. For example, an indicator that flags a foreign language terminal services connection is not as useful to a company with operations around the world as it is to a company that operates strictly in one country.

The case study that follows demonstrates how a once compromised organization increased their network visibility and used actionable threat intelligence to be in a better position to combat future attempts by the APT to compromise their network.

SECTION IV

[CASE STUDY]

Victim X is a multinational, Fortune 500 company based in the United States with locations in several countries. In early 2010, Victim X was notified by Federal law enforcement they were compromised by APT attackers who had stolen sensitive information.

DAY 1

Victim X's Corporate CIO obtained executive support to conduct a thorough investigation and response to the compromise. Victim X hired Mandiant to augment their internal team due to the technical nature of the attackers, advice from Federal law enforcement and the immense resource demand an incident response of this magnitude requires.

DAYS 2–6

Victim X established a Virtual Response Team (VRT). The Corporate CIO assigned security personnel, IT and application administrators, division CIOs, business line managers and Mandiant consultants to the VRT team. The Corporate CIO assigned a lead investigator, remediation lead and overall project manager to manage the response. The investigative lead and remediation manager reported to the project manager, who maintained ownership and responsibility for the incident response.

...remediation should always be addressed on a case by case basis specific to the needs of the victim organization.

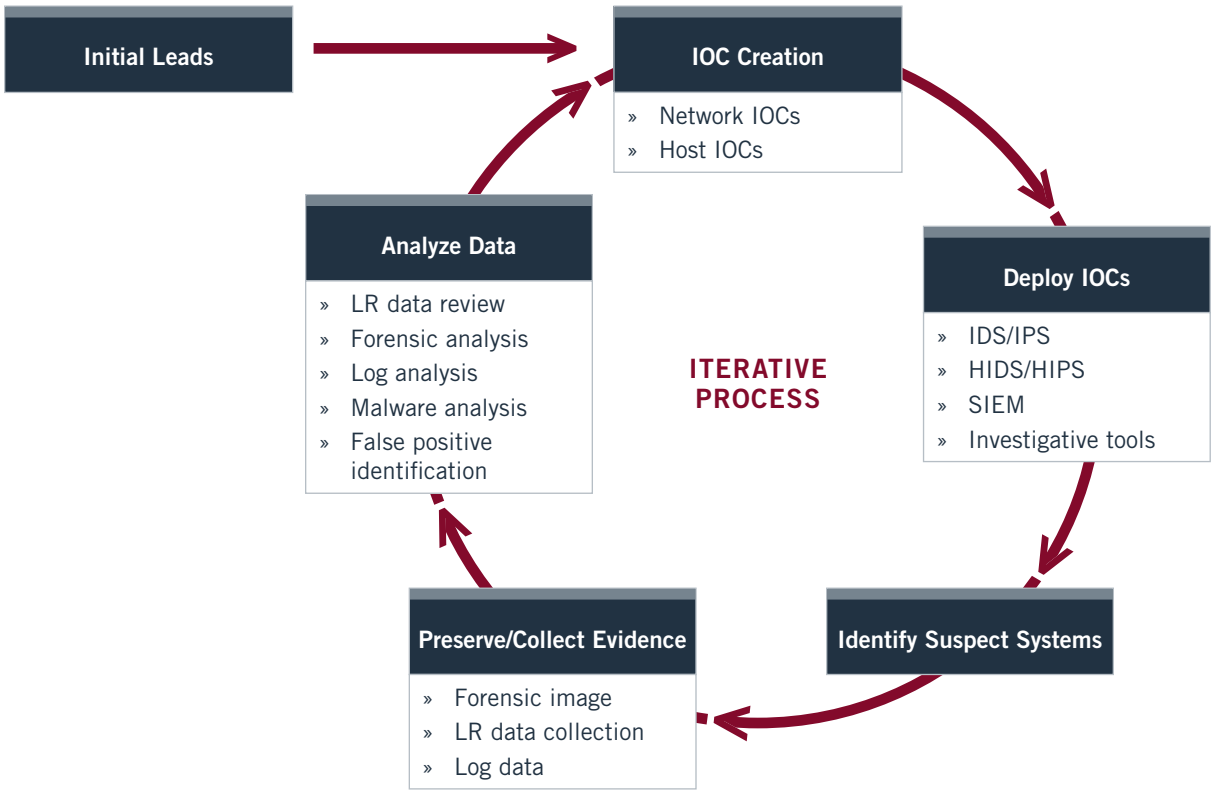
Guidelines were established for the incident response:

- No immediate remedial action was to occur unless a specific business need warranted it (required executive approval).
- No communication about the incident was to occur outside of the VRT except by the Corporate CIO.
- All communication about the incident must be encrypted.
- For operational security a code word was developed to refer to the incident.

The investigation started by ensuring the VRT had proper visibility. Mandiant's network sensors were installed at all major Internet points of presence and Mandiant Intelligent Response® (MIR) agents were installed on all systems. In parallel, all information provided to Victim X by law enforcement was catalogued and indicators of compromise were developed and used as the starting point for the investigative activities. The IOCs were fed into each monitoring and investigative tool.

Live response data collection was performed as suspected compromised systems were discovered. Once the live response data was collected, the data was thoroughly analyzed using MIR. Live response analysis entails reviewing enough data about the suspect systems to make a determination of

HIGH-LEVEL INVESTIGATIVE STEPS PERFORMED AT VICTIM X



compromise and to investigate malicious activity, without requiring a forensic image of each compromised system. The analysis is done at scale throughout the enterprise. This process drastically reduces the time it takes to identify and analyze compromised systems throughout an enterprise.

Forensic images were created and analyzed for "systems of special interest." Systems of special interest were defined as any system where:

» data theft occurred;

» data was staged prior to theft;

» network/DNS monitoring discovered malicious activity originating from a system and malware could not be discovered or linked to the network traffic; and

» the attacker recently deleted finds considered important to the investigation.

As new malware was discovered, each piece was thoroughly analyzed to ensure its functionality was understood. Indicators of compromise were developed from each piece of malware or unique attacker technique and fed back into the monitoring and investigative tools. Systems were re-reviewed on a periodic basis for the new indicators of compromise.

DAY 7

A week into the investigation, we discovered that Victim X had been compromised by the APT for more than two years. The initial intrusion was via an exploit of an unpatched vulnerability in Adobe's Acrobat Reader software. Evidence revealed that PDF files were opened on multiple systems around the earliest known time frame of compromise. Exploitation of an unpatched vulnerability allowed the APT to execute stage one malware on the system. Because all Victim X users possessed local administrative rights to their

systems, the APT was able to immediately install stage two malware without needing to escalate privileges on the victim system. The stage two malware provided the APT with remote access into Victim X's environment. The specific piece of malware injected itself into the system's Internet Explorer process to bypass Victim X's internal web proxies, which required user authentication. The malware was configured to communicate over TCP ports 80 (HTTP) and 443 (HTTPS).

Trace evidence revealed that common password hash dumping utilities and a pass-the-hash utility were executed on some of the compromised systems. The attacker was attempting to escalate privileges from a local administrator to domain administrator. Additionally, Victim X discovered that internal reconnaissance activity, such as user profile enumeration and recursive directory listings on file shares, had been performed. At this time the VRT started planning for remediation.

DAYS 8–9

Victim X arranged an in-person meeting of all VRT members over a two day period to develop the details of the remediation plan. Arranging for all key personnel to work with the investigative team for one or two days to jointly develop a remediation plan increased the feasibility and effectiveness of Victim X's remediation plan. During this two day meeting, the VRT identified posturing remediation steps that could be taken to suppress the impact of the incident, further increase Victim X's visibility of their network and posture their company for a successful remediation effort. The posturing actions needed to be surreptitious as Victim X did not want to alert the APT attackers they were aware of their presence and cause the attackers to modify their TTPs. Victim X implemented the following posturing steps:

» **Enabled Comprehensive DNS logging**
DNS logging was enabled on internal DNS servers to identify systems requesting connections to attacker controlled domains. Victim X used Microsoft DNS servers, which required DNS debug logging to be enabled in order to identify the systems performing the request, the requested domain, and the returned IP address.

» **Enabled DHCP Logging**
DHCP logging was enhanced to identify the hostname and IP address pairing at the time a DNS request or connection to a malicious IP address was made. Storing historical DHCP log information could also allow Victim X to perform historical data review during a future compromise.

» **Enabled VPN Logging**
VPN logging was enabled to identify the source system and user authenticating to the environment. This log information allowed Victim X to quickly identify compromised systems that rarely connected to the LAN.

» **Enhanced Windows Security Event Logging**
Windows Security event logging was modified to capture successful and failed logon events. Monitoring of successful authentications of known compromised accounts allowed Victim X to track attacker movement and provided insight into potential target systems.

» **Reduced the Number of Users With Administrative Privileges**
All users not requiring administrative rights for their job functions were identified. Both domain administrator and local administrator privileges were targeted. Administrative privileges were scheduled to be removed from these accounts during the remediation event. This action reduced Victim X's overall risk from successful social engineering attacks.

REMEDIATION MATRIX

	Initial Recon	Initial Compromise	Establish Foothold	Escalate Privileges	Internal Recon	Move Laterally	Maintain Presence
Prevent		✓	✓	✓	✓	✓	✓
Detect		✓	✓		✓		✓
Respond		✓	✓	✓	✓	✓	✓

» **Increased Password Complexity**
Increasing password complexity requirements for all users reduced the likelihood that an offline attack against password hashes would succeed. Additionally, the password length requirement for accounts with elevated privileges was greatly increased to reduce the efficacy of password cracking techniques.

» **Reduced Cached Credential Storage**
The storage of cached credentials on workstations and servers was reduced to two. Additionally, the storage of cached credentials on laptops was reduced to three. This action reduced the number of cached credentials that could be obtained by the attacker for offline password cracking.

» **Disabled the Use of LANMAN Hashes**
The creation of LAN Manager password hashes was disabled on all systems. Disabling the creation of the LAN Manager hashes on all systems reduced Victim X's risk from password cracking.

» **Implemented Aggressive Patch Management**
A plan for patching commonly targeted third-party applications was developed using LANGuard. This action reduced Victim X's risk from exploitation of vulnerable software.

» **Developed End-User Security Training**
Training to help users identify social engineering attacks was developed for all users, with advanced training planned for high risk users. High risk users were defined as executives, anyone with elevated privileges, mergers and acquisition personnel and senior engineers.

DAYS 10–30

Parallel to the investigative effort, Victim X implemented most of these posturing steps, which increased the security of their environment and provided them critical visibility. The remediation matrix visually depicts the breadth of Victim X's remediation strategy. Mandiant uses the remediation matrix to ensure that the key areas of a security program — prevention, detection, and response — are properly addressed in context of the current incident. The various stages of the attack are represented at the top of the matrix.

Once the number of compromised systems discovered on a weekly basis had diminished to near zero, all discovered malware and network indicators of compromise had been correlated, the monitoring activities were able to catch all of the attacker's activities and Victim X had implemented the posturing steps on the majority of systems/users, Victim X moved forward with the remediation event. A clearly defined window of time was chosen as the time frame to execute the remediation event.

DAYS 31–32

Victim X performed the following activities as part of their two-day remediation event:

» **Disconnected all Points of Presence from the Internet**
Victim X's connection to the Internet was disabled, including VPN and connections to business partners, but excluding site-to-site VPN connections. This ensured that the attacker did not have access to Victim X's network during the remediation effort, but that Victim X's administrators could remediate remote sites. It is important to note that there were a couple of exceptions to this rule and specific business critical applications remained accessible from the Internet, though internal connectivity to these systems was blocked.

» **Blocked all Known Malicious IP Addresses**
Malicious IP addresses were blocked at all Internet egress points to ensure any compromised system that had not been detected could not communicate with known C2 servers. Future attacks using known malicious IP addresses would also be prevented and detected.

» **Blocked all Known Malicious Domains**
Malicious domains were subjected to DNS blackholing. This ensures that any compromised system that had not been detected could not communicate with known C2 servers. Future attacks using known malicious domains would also be prevented and detected.

» **Simultaneously Took Compromised Systems Offline**
Compromised systems were rebuilt to ensure they were not accidentally reconnected to the corporate network in a compromised state. In specific instances where a complete system rebuild was not possible, the malware was removed the system.

» **Performed a Comprehensive Password Rollout**
An enterprise password reset was conducted to ensure the attacker could not access assets using stolen credentials. This password reset included all local accounts, domain accounts, service accounts, Oracle DBA accounts, and Microsoft SQL 'sa' accounts. Note that stored LAN Manager password hashes should not be removed until a password change has occurred.

» **Implemented Selective Application Whitelisting**
An application whitelisting solution was implemented on all domain controllers to prevent the execution of password dumping utilities and other malware in the future. Attackers frequently target domain controllers because they store user account and password information for all users in a domain. Installing application whitelisting software on domain controllers will help prevent attackers from gaining access to all user accounts and password hashes, and will not incur the high administrative cost of maintaining application whitelisting software on end user systems.

DAY 33+

Actions that were considered critical to the security posture of Victim X but that could not be implemented before or during the remediation event became strategic recommendations. Victim X planned to implement all or most of the strategic recommendations within a year of the remediation event.

Below are some of the strategic actions that were developed:

» **Enhanced Network Segmentation**
Victim X implemented ACLs restricting access between network segments with servers in their data centers and network segments with workstations and laptops. A network traffic analysis study was conducted and Victim X gradually eliminated all unnecessary communications protocols between workstations and servers. The goal was to eliminate all unnecessary communications including Netbios, Remote Desktop, and Microsoft SQL Server traffic (where possible). Victim X planned to complete the segmentation within six months.

» **Implemented Multi-factor Authentication for all Accounts**
Victim X implemented smart cards for all privileged, non-service user accounts—for example, domain administrator, enterprise administrator, backup operator and server operator accounts. Additionally, Victim X implemented two factor authentication for webmail and VPN access to the environment.

» **Implemented Software Designed to Reduce Privileges from at-risk Services**
While removing local administrative privileges from users greatly reduces the impact of a successful phishing attack, it can cause increased administrative burdens and cost on an organization's help desk. Victim X evaluated solutions offered by Cyber-Ark and BeyondTrust which would enable users to submit requests to the help desk to request privileged access to perform a specific action—for example, install a printer driver. This would enable the help desk to grant privileges to a user to perform a specific action during a defined time period.

» **Implemented Software to Manage Privileged Account Passwords**
Implementing a unique local administrator password is not difficult for technical reasons, but can be challenging for companies for operational — specifically help desk and pc tech support — reasons. Victim X implemented Lieberman Software's Enterprise Random Password Manager to help manage their privileged account passwords. This tool was integrated into IT administrators' work flows to allow them to "check out" credentials, for both local administrator and shared accounts, as necessary.

» **Installed Microsoft Windows 7 and Server 2008**
Victim X started by installing Windows Server 2008 on all domain controllers. Once compatibility testing was completed, they raised the functional level of the domain from 2003 to 2008 which enabled them to implement a multi-tiered password policy. Victim X implemented one password policy for users, one password policy for privileged administrators and one password policy for all service accounts. Windows 7 User Account Control (UAC) features allow a user to have administrative privileges to a system, but have all processes run in a non-privileged user context. Victim X implemented Windows 7 for all users that could not have administrative privileges removed and planned to deploy Windows 7 in a staged, enterprise-wide rollout over the next year.

» **Expanded Application Whitelisting Implementation**
Victim X expanded the deployment of their Bit9 application whitelisting solution to include systems of key personnel such as executives, individuals working with sensitive data and IT administrators, and groupings of servers with homogeneous installations such as mail servers and file servers.

» **Implemented Enhanced E-mail Controls**
Public e-mail services such as Yahoo! and Gmail are often used to send phishing e-mails. Victim X blocked e-mail attachments from common public e-mail providers with their IronPort mail gateways. To alleviate Victim X's concerns about blocking legitimate attachments, they set up an external collaboration environment for their employees to share files with outside parties.

Victim X configured their IronPort mail gateways to insert warnings to users to be suspicious of e-mails with hyperlinks and attachments and to remind users to submit any suspicious e-mails to the help desk.

Within three weeks of the remediation event, Victim X was able to detect an attempted re-compromise. The network monitoring system implemented by Victim X alerted them to a potential spear-phishing attack. The victim system was immediately investigated, discovered to be compromised and remediated. Unlike the original remediation effort, Victim X remediated compromised systems as soon as they were discovered in order to prevent the attacker from re-establishing a significant presence on their network.

AFTER YEAR 1

Victim X has been successful in detecting and immediately remediating re-compromised systems as the compromises occur. As with any large organization, they are not able to prevent or immediately detect every re-compromise, but their strategy has allowed them to prevent the APT from gaining such control over their enterprise that they need to perform another large remediation event such as the one described.

The lesson learned from Victim X is that by garnering executive level support and properly posturing your organization through the use of increased security controls, enhanced visibility and enterprise investigative tools, addressing an APT breach can become a problem measured in hours or days, rather than weeks or months.

SECTION V

[CONCLUSION]

Technology outpaces security. Likewise, the threats have evolved faster than our ability to reliably safeguard our assets. To better protect our information and intellectual property, we must adapt our organizational security programs to meet the emerging challenges. Until someone develops the mythical "silver bullet", our front-line cyber-warriors will have to establish and sustain our threat detection and response capabilities.

By developing effective threat detection and response capabilities, you will have the intelligence, visibility, processes and practitioners to withstand the threats. Done right, threat detection and response provides your IT security teams the situational awareness to rapidly detect incidents, suppress their impact, develop their own threat intelligence and rely on other timely intelligence to proactively inspect your networks for the fingerprints of compromise. With superior threat detection and response capabilities, you are armed and prepared to combat targeted threats.

MANDIANT is the leading provider of computer security incident response and computer forensics solutions and services. Headquartered in Alexandria, VA, with offices in New York, Los Angeles and San Francisco, MANDIANT provides products, education, professional and managed services.

Our customers range from firms in the Fortune 500, to financial institutions, U.S. and foreign governments and leading U.S. law firms. They engage us for our field expertise; our long experience responding to advanced attackers; and our discretion handling their most sensitive business information. We work throughout the U.S. and have helped customers on every continent except Antarctica.

MANDIANT's people form one of the industry's largest incident response and computer forensics forces. Authors of nine books, our consultants and engineers hold top government security clearances, certifications and advanced degrees in computer science from some of the most prestigious universities.

MANDIANT's consultants have been featured on news programs including CBS's *60 Minutes*, CNN's *Talkback Live*, NBC News and FOX News. We are also widely quoted in the industry and national press, from *The Wall Street Journal* to niche forensics and payment card industry journals.

To learn more about MANDIANT, or to register for one of our monthly webinars, visit www.mandiant.com. If you need urgent help, call our hotline at +1 (877) 962-6342 or, feel free to call our main office at +1 (800) 647-7020.

You'll find more information on the MANDIANT forums at https://forums.mandiant.com, in M-unition, the company blog: http://blog.mandiant.com, and by following us on Twitter @Mandiant and on Facebook at http://www.facebook.com/MandiantCorp.

www.mandiant.com