Mandiant

Google Cloud Security

M-Trends

2024 Special Report

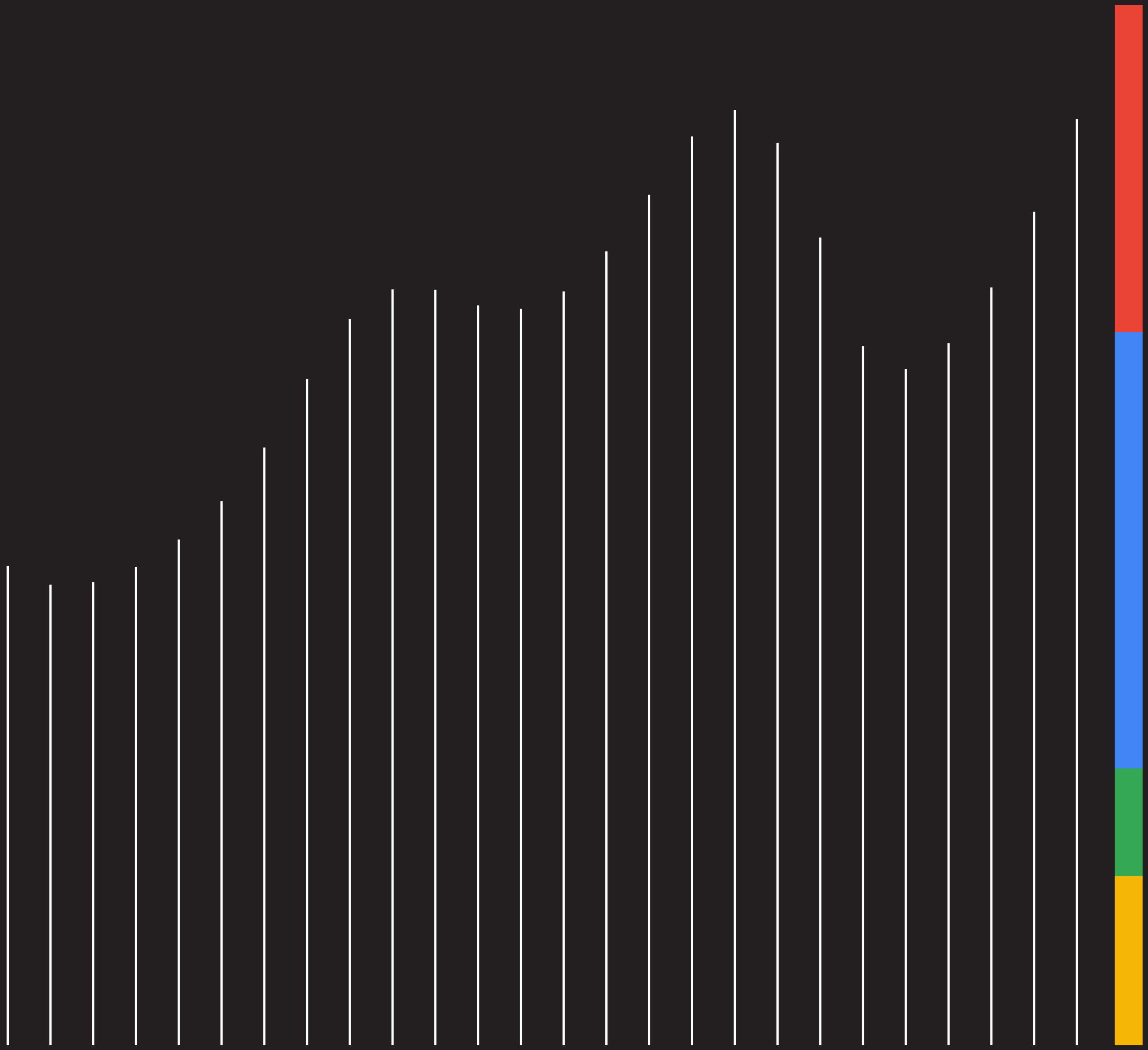
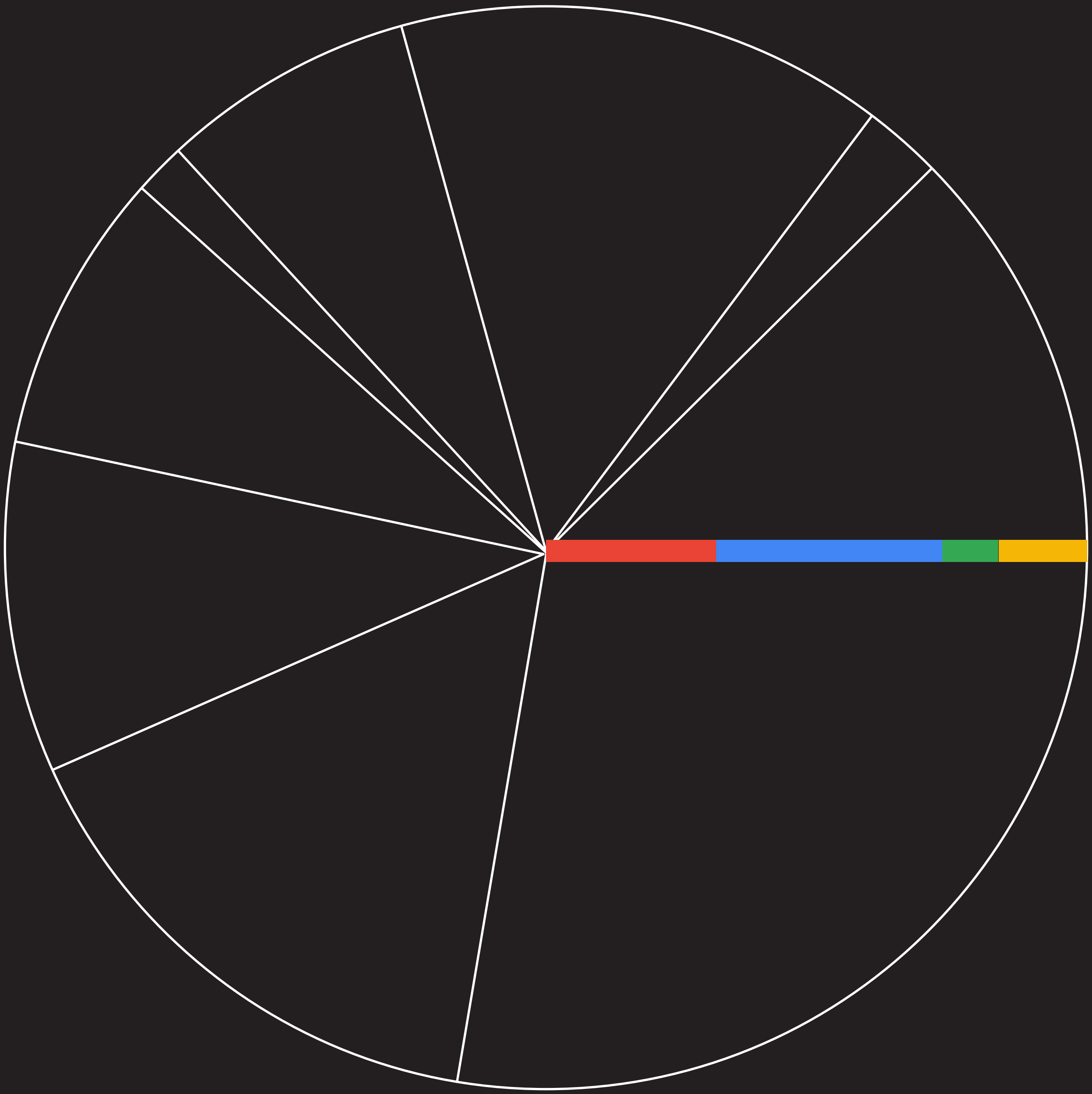


Table of Contents

Introduction



One of the big takeaways from our 2023 engagements, and consequently a key theme of M-Trends 2024, is that attackers are focusing more on evasion. They are aiming to avoid detection technologies (such as endpoint detection and response) and maintain persistence on networks for as long as possible, either by targeting edge devices, leveraging "living off the land" and other techniques, or through the use of zero-day vulnerabilities in security and other solutions prevalent throughout enterprises.

Despite attackers' efforts to evade detection, defenders are continuing to get better at identifying compromises. The global median dwell time—dwell time is the number of days an attacker is on a system from compromise to detection—continued its downward trend in 2023, and is now 10 days (from 16 days in the previous year). It's a big victory for the good guys, but ransomware is still a key factor in driving down dwell time since it tends to be detected more quickly. Furthermore, Mandiant red teams typically achieve their objectives in 5 to 7 days, so defenders must remain vigilant.

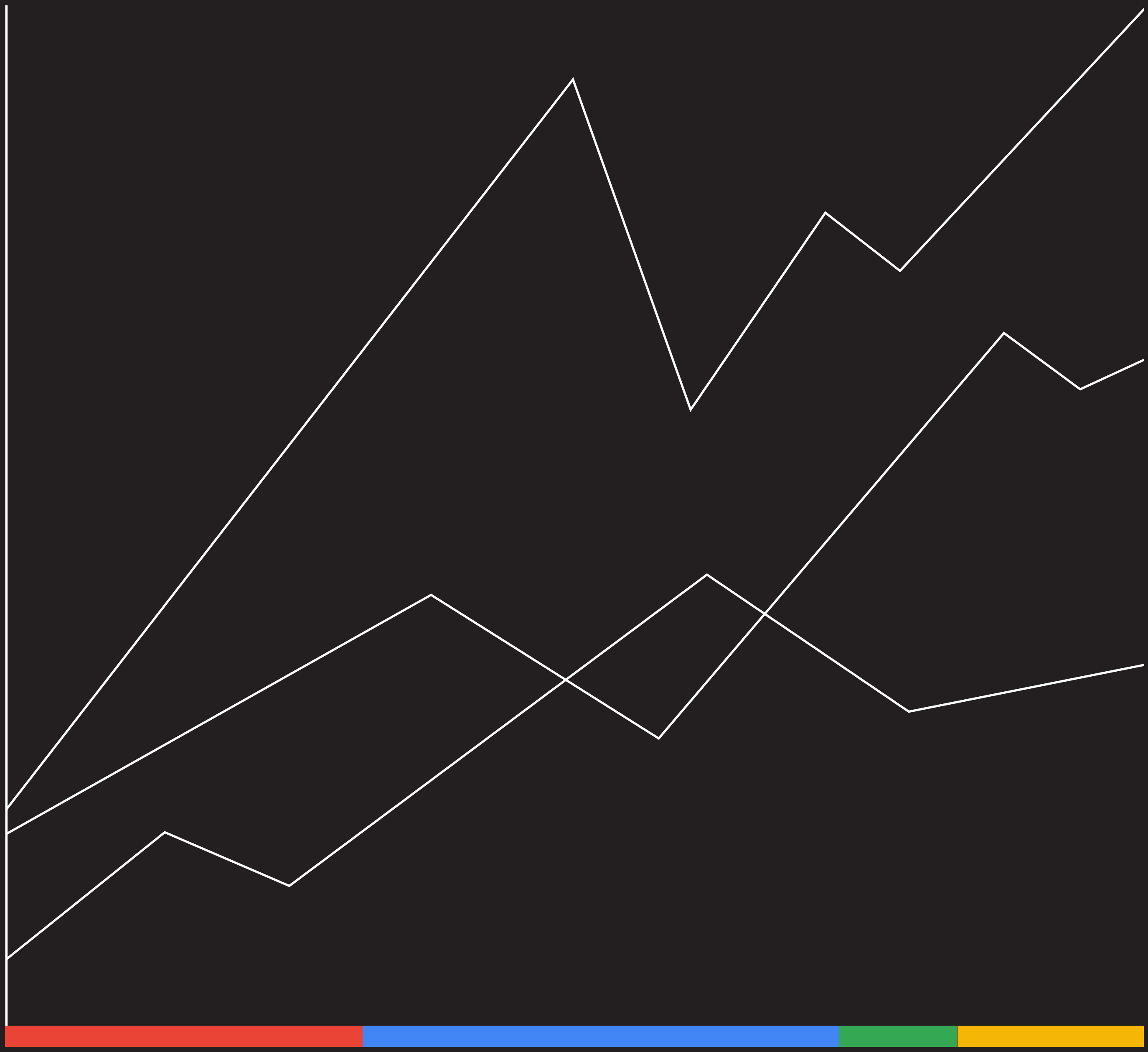
M-Trends 2024 features data and other security metrics that readers have come to expect, highlights zero-day use by espionage and financially-motivated attackers, and dives deep into evasive actions conducted particularly by Chinese espionage groups. Other key takeaways in this report include:

- Evolving phishing trends such as attacker use of social media, SMS and other communications technologies
- Tactics to bypass multi-factor authentication such as adversary-in-the-middle and other techniques
- Cloud intrusion trends such as targeting of cloud infrastructure as well as attacker use of cloud resources
- Use of AI in red and purple team engagements, with a focus on how new technologies can help produce better outcomes for organizations

Mandiant consultants are always on the frontlines, investigating and analyzing the latest cyber attacks, and understanding how best to defend against them. Consultants proactively assess clients against the latest attacker tactics, techniques and procedures, and help with remediation, transformation and education.

Through the release of our annual M-Trends report, we share our learnings with the greater security community, building on our dedication to providing critical knowledge to those tasked with defending organizations. The information in this report has been sanitized to protect the identities of victims and their data.

By the numbers



Global Trends

The metrics reported in M-Trends 2024 are based on Mandiant Consulting investigations of targeted attack activity conducted between January 1, 2023 and December 31, 2023.

Internal detection is when an organization independently discovers it has been compromised, such as through an internal security appliance alert or internal personnel notification of suspicious activity.

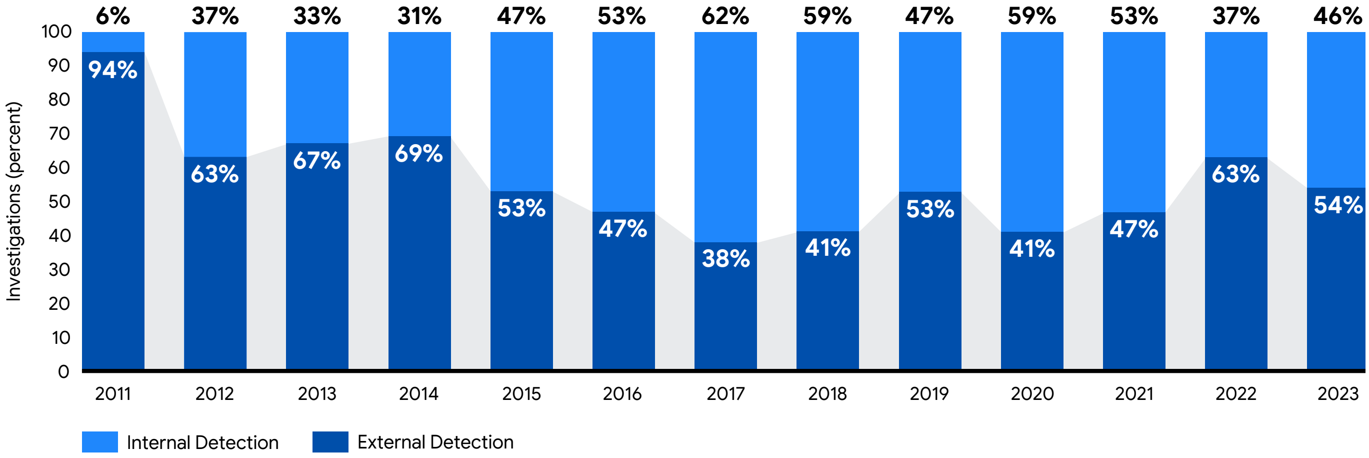
External notification is when an outside entity, such as law enforcement agencies, cybersecurity companies, or industry partners, informs an organization it has been compromised. In some cases, attackers will perform this notification, such as through a ransom note.

Detection by Source

In 2023, more than half of compromised organizations (54%) first learned of a compromise from an external source, while 46% first identified evidence of a compromise internally. However, separating out ransomware-related intrusions reveals that it was much more common for an organization to learn of a ransomware-related incident from an external source. For ransomware-related intrusions, 70% of organizations were externally notified, in most cases, via a ransom demand from the attacker. For intrusions that were not linked to ransomware, the ratio of internal versus external discovery was even, 50% to 50%. Of the internally discovered intrusions, 85% did not involve ransomware.

The percentage of externally notified intrusions decreased from 63% in 2022 to 54% in 2023. Mandiant also responded to more ransomware-related intrusions in 2023 than in 2022. Ransomware events are most often discovered through external means. Despite this, Mandiant observed a nine point drop in external notifications. This year-over-year shift, along with the high proportion of internally discovered compromises in cases other than ransomware, suggests that organizations are experiencing higher rates of success in detecting malicious behavior on their networks.

Detection by Source, 2011-2023

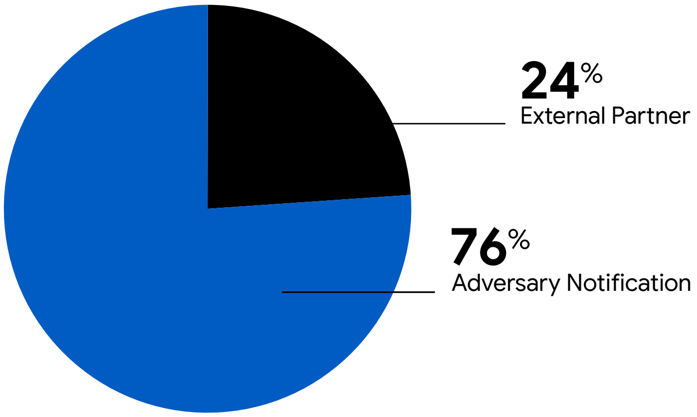


A ransomware-related intrusion provides access for or is associated with an attacker that has the primary goal of encrypting data, with the intention of extracting payment from the target in order to avoid further harm or to undo the malicious action.

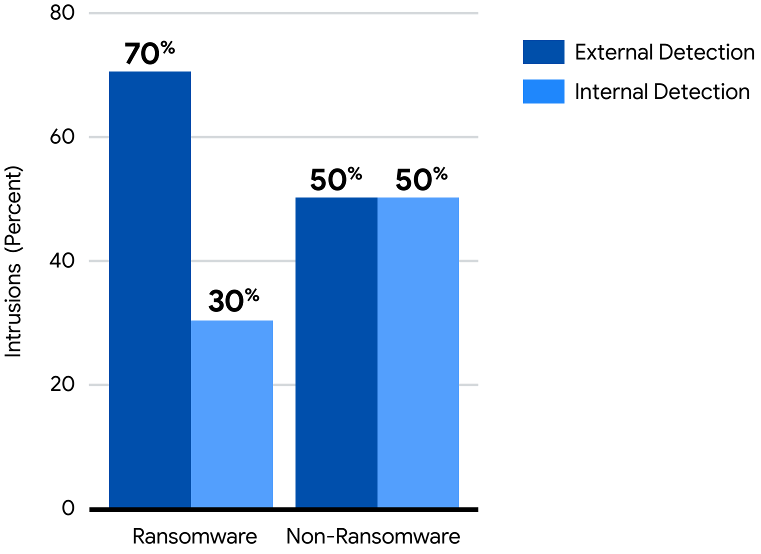
Ransomware-Related Intrusions

In 70% of cases, organizations learned of ransomware-related intrusions from external sources. Organizations were notified of a ransomware incident by an attacker ransom note in three fourths of those intrusions. This is consistent with the extortion business model in which attackers intentionally and abruptly notify organizations of a ransomware intrusion and demand payment. The remaining quarter of external notifications for ransomware intrusions came from external partners, such as law enforcement or security companies. In 2022, attacker notifications represented two thirds of external notifications for ransomware intrusions, compared to one third coming from external partners.

Ransomware External Notification Source, 2023



Detection by Source, 2023



Dwell Time

Global median dwell time continued a downward trend marking another notable shortest time period between initial intrusion and detection for all M-Trends reporting periods. In 2023, most organizations detected intrusions within 10 days of the initial intrusion. This is a decline of nearly one week compared to 16 days in 2022.

Mandiant defenders observed notable improvements in global median dwell time in 2023 across all notification sources. With the shortest periods across the board, global median dwell time for external notification sources decreased to 13 days in 2023 from 19 days in 2022. This likely indicates improved communication between organizations targeted and external parties making notifications. Another likely explanation for this decrease could be the increase of ransomware-related adversary notifications.

Maintaining the ongoing trend, when defenders detect adversary intrusions internally, they do so faster than the overall median dwell time. The global median dwell time for intrusions detected internally was nine days in 2023, down from 13 days in 2022 and from 18 days in 2021.

> **Dwell time** is calculated as the number of days an attacker is present in a compromised environment before they are detected. The median represents a value at the midpoint of a dataset sorted by magnitude.

Change in Median Dwell Time

16 ↘ **10**

days in 2022 days in 2023

Global Median Dwell Time, 2011-2023

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
All	416	243	229	205	146	99	101	78	56	24	21	16	10
External	—	—	—	—	320	107	186	184	141	73	28	19	13
Internal	—	—	—	—	56	80	57.5	50.5	30	12	18	13	9

Global Dwell Time Distribution

Dwell time distribution measures the percentage of Mandiant-investigated intrusions with a specific range of dwell time. In 2023, Mandiant experts continued to see intrusions detected earlier, with 43% of intrusions being detected in one week or less. Nearly two thirds of all intrusions in 2023 were detected within 30 days. This likely indicates that detection capabilities continue to improve across organizations, allowing defenders to be notified of threats during the initial infection or reconnaissance phases of the targeted attack lifecycle, similar to previous M-Trends reports.

Mandiant observed a decrease in intrusions that remain undiscovered for long periods of time compared to previous years. In 2023, 6% of investigations identified activity that remained undetected for between 1 and 5 years, compared to 11% in 2022 and higher percentages prior to 2020. Although organizations are still facing intrusions that go undetected for longer periods of time, defenders will likely see the distribution of dwell time move to the left as external parties, such as security vendors and law enforcement, increase their involvement and pace of notifications. However, detection capabilities and continuous hunting throughout environments have been effective at unearthing long-standing intrusions. As actionable information is shared, detection capabilities will continue to improve.

Broadly, the long-term trends of declining median dwell time and increasing rates of internal discovery of compromises indicate that organizations have made meaningful, measurable improvements in their defensive capabilities.

Global Dwell Time Distribution, 2018-2023

	1 week or less	30 days or less	6 months or less	1 year or less	5 years or less	5 years or more
2018	15.0%	16.0%	36.0%	13.0%	18.0%	1.1%
2019	22.2%	18.5%	29.2%	9.3%	18.5%	2.3%
2020	35.3%	17.2%	26.7%	6.6%	13.0%	1.2%
2021	37.4%	17.7%	26.2%	10.7%	7.8%	0.3%
2022	42.0%	16.0%	24.0%	7.0%	11.0%	0.0%
2023	43.3%	22.7%	22.3%	5.4%	6.0%	0.2%

Change in Global Investigations Involving Ransomware

18% in 2022 ↗ **23%** in 2023

Change in Global Dwell Time—Ransomware

9 days in 2022 ↘ **5** days in 2023

Change in Global Dwell Time—Non-Ransomware

17 days in 2022 ↘ **13** days in 2023

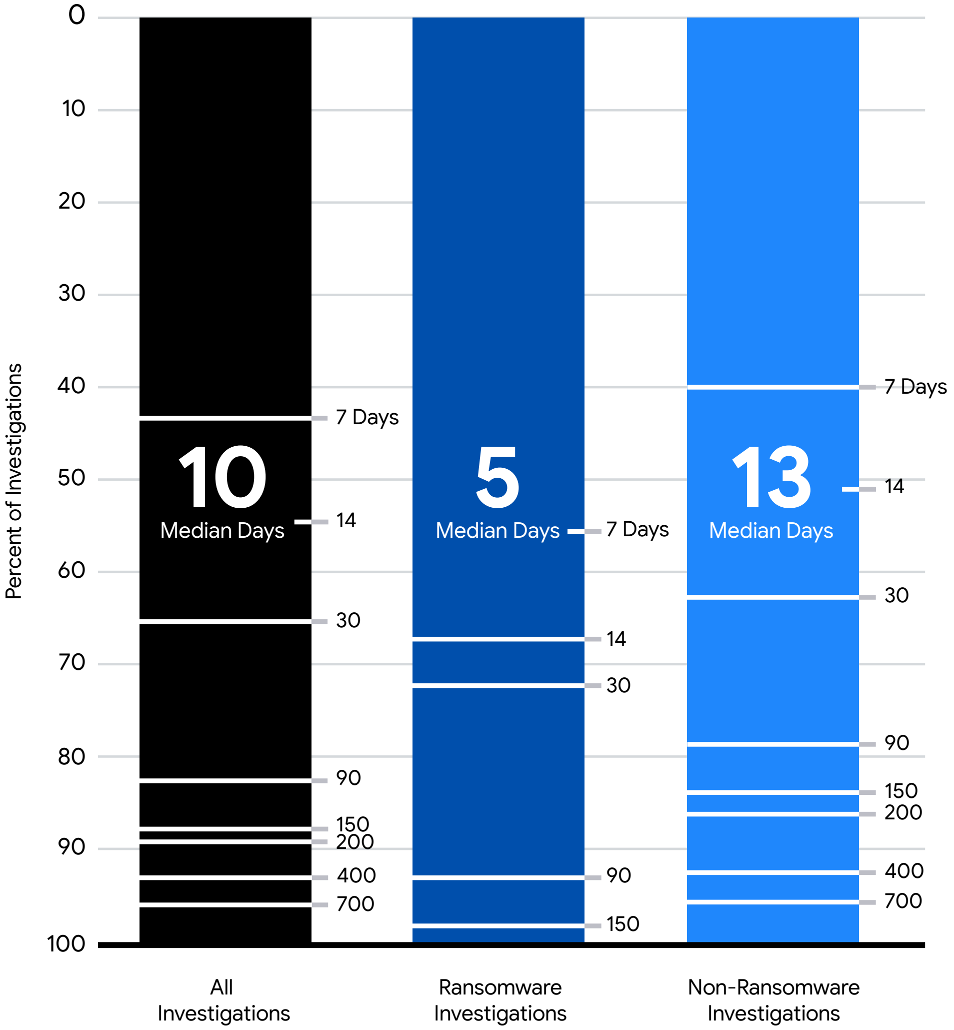
Investigations Involving Ransomware

In 2023, global investigations involving ransomware increased five percentage points to 23% of investigations in 2023 compared to 18% in 2022. This brings the percentage of ransomware-related intrusions back to where it was previously in 2021.

Globally, organizations detected ransomware or received a ransom demand faster in 2023–in five days compared to nine days in 2022–regardless of notification source. Non-ransomware-related intrusions were detected in 13 days, compared to 17 days in 2022.

Intrusions involving ransomware were detected in six days when the notification came from an internal source, compared to 12 days in 2022. Defenders were notified of ransomware-related intrusions from an external party in five days in 2023, two days quicker than what was observed in 2022.

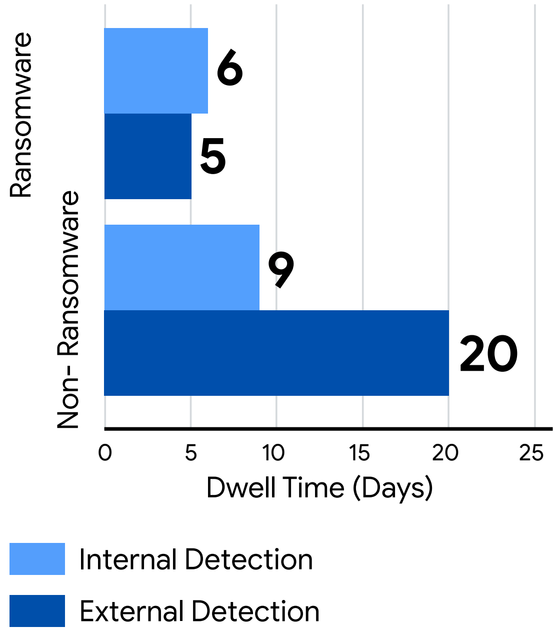
Global Dwell Time by Investigation Type, 2023



Ransomware attacks have continued to be a driving factor in reducing dwell time over the years. However, in 2023, Mandiant experts observed notable improvements in decreased dwell time across all notification sources and investigation types.

Intrusions that did not involve ransomware were identified in a shorter period of time in 2023. Notably, intrusions that occurred in 2023 were identified internally in little over a week, with nine days between initial intrusion and detection, compared to 13 days in 2022. Organizations were notified by an external party of an intrusion one week faster in 2023, resulting in a 20-day median dwell time for externally notified, non-ransomware-related intrusions, compared to 27 days in 2022.

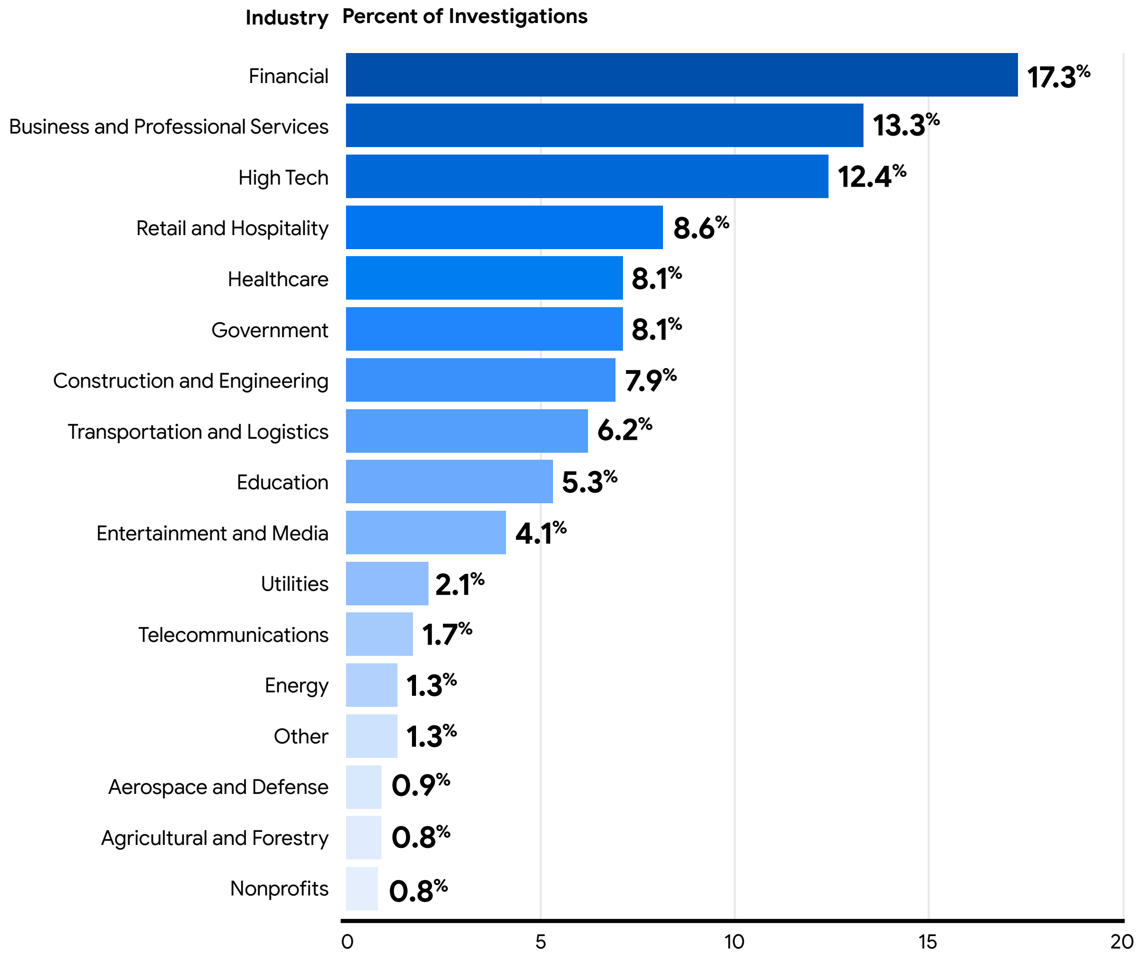
Global Median Dwell Time by Detection Source



Industry Targeting

In 2023, Mandiant most frequently responded to intrusions at financial services organizations, followed by business and professional services, high tech, retail and hospitality, and healthcare. All of these sectors have access to a variety of sensitive information, including proprietary business information, personally identifiable information (PII), protected health information (PHI), and financial data. Attackers have also abused service providers and technology organizations to facilitate third-party compromises or to obtain access to data or networks belonging to many organizations through a single compromise. Mandiant consistently finds these sectors toward the top of the list for share of investigations. Government sector investigations declined from first to tied for fifth with healthcare in 2023, potentially reflecting fewer new investigations related to the war in Ukraine compared to 2022.

Global Industries Targeted, 2023



Targeted Attacks

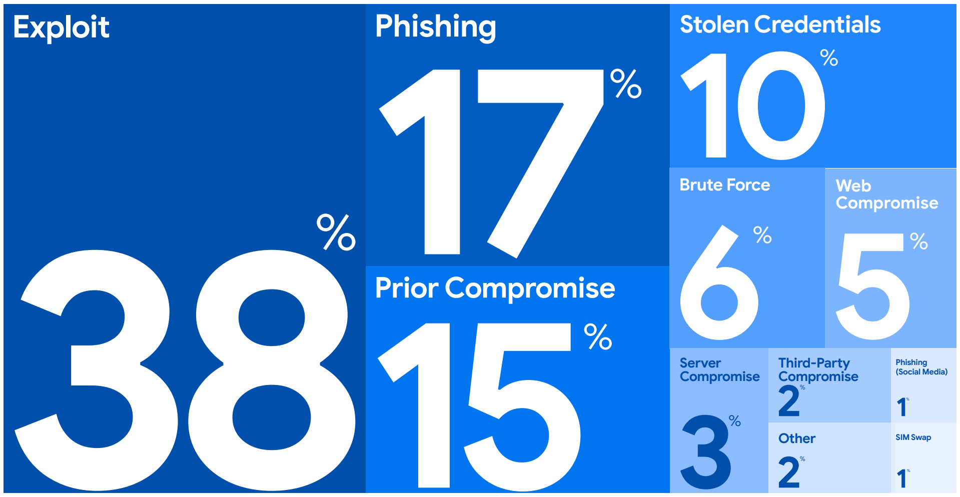
Initial Infection Vector

In 2023, Mandiant experts once again saw exploits used as the most prevalent adversary initial infection vector. In intrusions where the initial intrusion vector was identified, 38% of intrusions started with an exploit. This is a six percentage point increase from 2022, consistent with what defenders faced in 2021. For more information, please see “Attacker Operations Involving Zero-Days Vary Depending on Motivation”.

Phishing remained the second most common intrusion vector. However it declined in 2023, with 17% of intrusions, compared to 22% in 2022. Phishing remains an effective method to establish an initial foothold and a popular threat vector for adversaries. Full analysis can be found in “Evolution of Phishing Among Shifting Security Controls”.

Prior compromises were the third most significant intrusion vector used by attackers in 2023. Mandiant investigators noted a three percentage point increase in 2023 compared to what was observed in 2022 with 15% of intrusions beginning with access provided by a prior compromise. This increase is likely related to the ransomware ecosystem and the continued partnership between ransomware affiliates and various malware operators selling initial access.

Initial Infection Vector (When Identified)



Stolen credentials pose a serious security risk to organizations and were the fourth most notable initial intrusion vector in 2023. Attackers often obtain credentials due to password reuse or users inadvertently downloading trojanized software on corporate devices. Infostealers are frequently delivered through trojanized software. In 2023, 10% of intrusions began with evidence of stolen credentials, compared to 14% observed in 2022. The prevalence of both widespread information stealer malware and credential purchasing continue to challenge defenders.

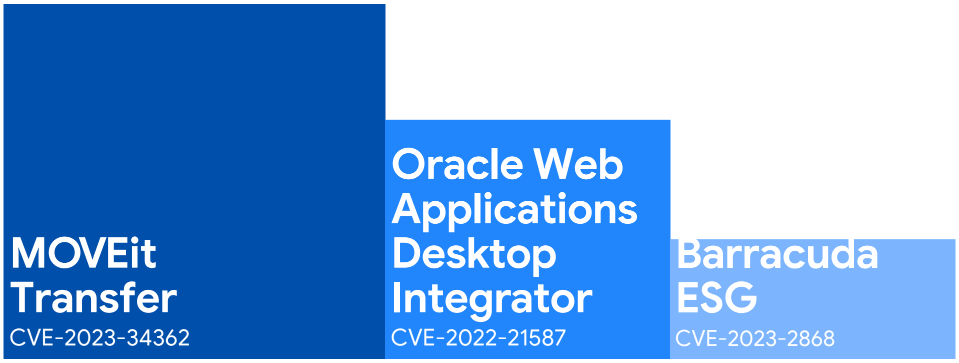
Brute-force attacks round out the top five initial intrusion vectors observed in 2023, representing 6% of intrusions. Proper implementation of multi-factor authentication has been pivotal to slowing down attackers in their attempts to compromise environments.

Attackers continue to leverage effective tactics to gain access to target environments and conduct their operations. While the most popular infection vectors fluctuate, organizations must focus on defense-in-depth strategies. This approach can help mitigate the impact of both common and less frequent initial intrusion methods.

In 2023, when the initial intrusion vector was identified, an exploit was observed 38% of the time. Mandiant continues to observe both cyber espionage and financially motivated attackers leveraging zero-day vulnerabilities to conduct their operations. The most prevalent vulnerability Mandiant investigators observed in 2023 was CVE-2023-34362,[1] an SQL injection vulnerability in MOVEit Transfer that Mandiant rated as high risk.[2] The second most prevalent vulnerability was CVE-2022-21587, a critical unauthenticated file upload vulnerability in Oracle E-Business Suite. The third most prevalent vulnerability in 2023 was CVE-2023-2868. CVE-2023-2868 is a critical command injection vulnerability in Barracuda Email Security Gateways (physical appliances). These vulnerabilities were heavily exploited by attackers, and notably the first and third most targeted vulnerabilities were related to edge devices. For more information on the continued targeting of these devices, please see Chinese Espionage Operations Targeting The Visibility Gap.

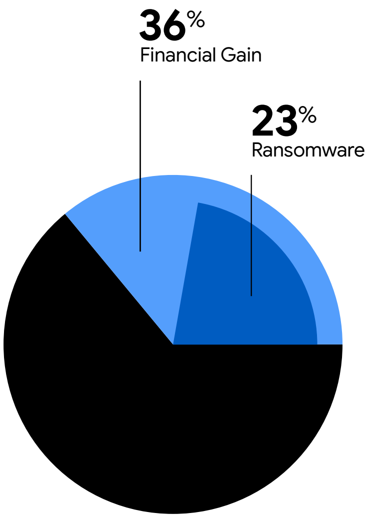
However, Mandiant experts also observed attackers' continued use of exploits throughout the attack lifecycle to maintain access, move laterally, and complete their mission. Mandiant continues to observe a handful of vulnerabilities related to older technologies, such as Microsoft Access 2003 (CVE-2008-2463),[3] Microsoft Windows Server 2016 (CVE-2017-0144),[4] and Telerik (CVE-2019-18935).[5]

Most Frequently Seen Vulnerabilities



Post-Compromise Activity

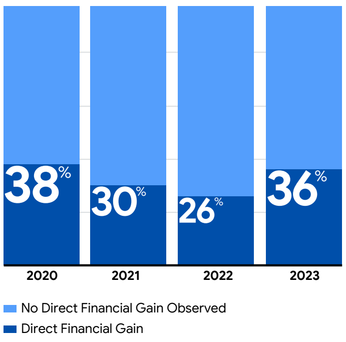
Financial Gain



The proportion of intrusions Mandiant responded to that served financially motivated objectives increased from more than a quarter of all investigations, 26%, in 2022 to more than a third, 36%, in 2023. Ransomware-related intrusions represented almost two thirds of financially motivated intrusions and 23% of all 2023 intrusions.

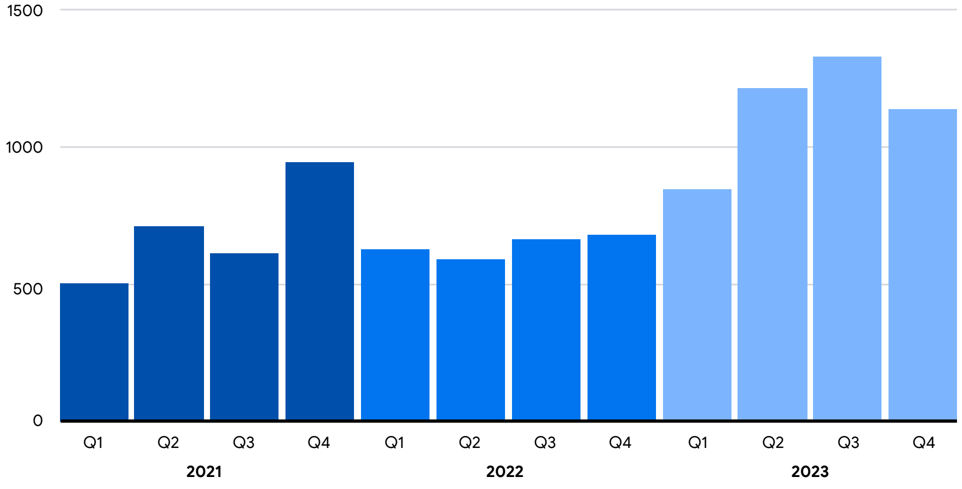
The remaining financially motivated intrusions included data theft extortion without ransomware encryption, attackers establishing initial access to facilitate other operations, business email compromise (BEC) fraud, and cryptocurrency theft events. Mandiant attributed several financially motivated intrusions to likely North Korean[6] state-sponsored attackers, including cryptocurrency theft and IT worker wage theft. Mandiant continues to track North Korean threat groups that conduct financially motivated activity to cover both operational costs as well as larger scale activity intended to generate revenue for the state.[7]

Financial Gain, 2020-2023

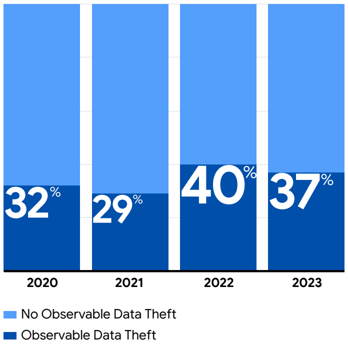


The upward trend in ransomware and other extortion-related investigations in 2023 is consistent with Mandiant and open-source observations of a marked increase in listings on data leak sites (DLS) and extortion revenue estimates.[8] DLS are websites where the illicitly retrieved data of companies that refuse to pay a ransom are published. While this data is skewed toward targets who refused to pay attackers' ransom demands, it is still useful for understanding broad trends in extortion operations. The FIN11 MOVEit exploitation campaign and UNC3944[9] activity described in the Evolution of Phishing section showcase the prevalence of extortion intrusions without ransomware encryption.

Count of DLS Listings per Quarter, 2021-2023

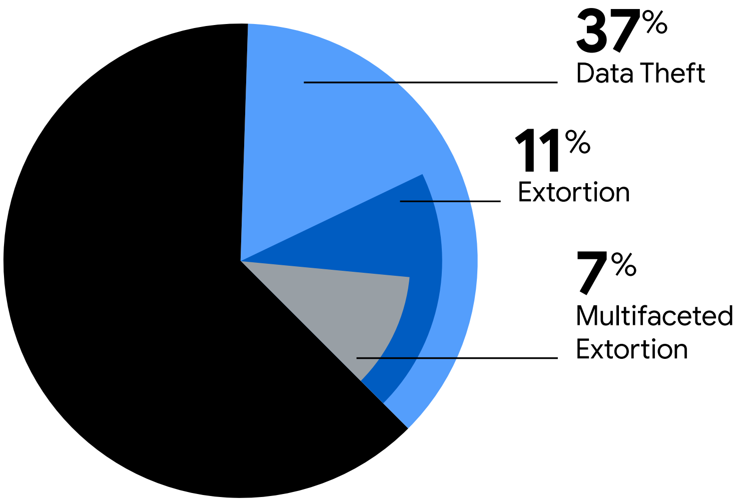


Data Theft, 2020-2023



Data Theft

Mandiant identified data theft in 37% of 2023 intrusions, which is slightly lower than the 40% of intrusions reported in 2022. In 11% of intrusions, attackers directly monetized stolen data through extortion. In an additional 7%, they used a combination of data theft, ransomware, and extortion, also known as multifaceted extortion. Mandiant also observed attackers steal credentials and other data likely to facilitate reconnaissance of target networks. Several cases involved large-scale data theft that included intellectual property. Mandiant also identified instances of targeted or selective data theft by groups such as the Russian cyber espionage group APT29[10] and the suspected Chinese cyber espionage cluster UNC4841.[11]



Compromised Architecture

6% → 6%

in 2022 in 2023

Multiple Threat Groups Identified (per environment)

27% ↘ 17%

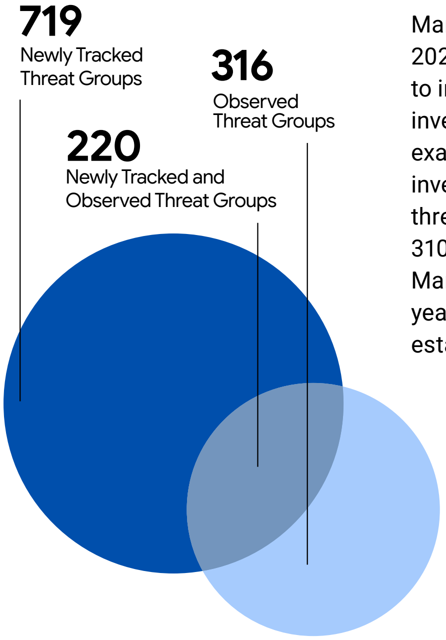
in 2022 in 2023

Environment

In 2023, Mandiant experts continued to observe attackers use compromised architecture to conduct email spam, distribute botnets, and perform some types of cryptomining activity. During the past three years, intrusions related to compromised architecture have been heavily automated following the mass exploitation of vulnerabilities. Publicly released proof-of-concept (PoC) code for new exploits increases the ease of automating attacks, accelerating the attack cycle for adversaries abusing compromised infrastructure. Publicly available PoC code for vulnerabilities makes it simple for attackers to automate their exploits using scanning tools.

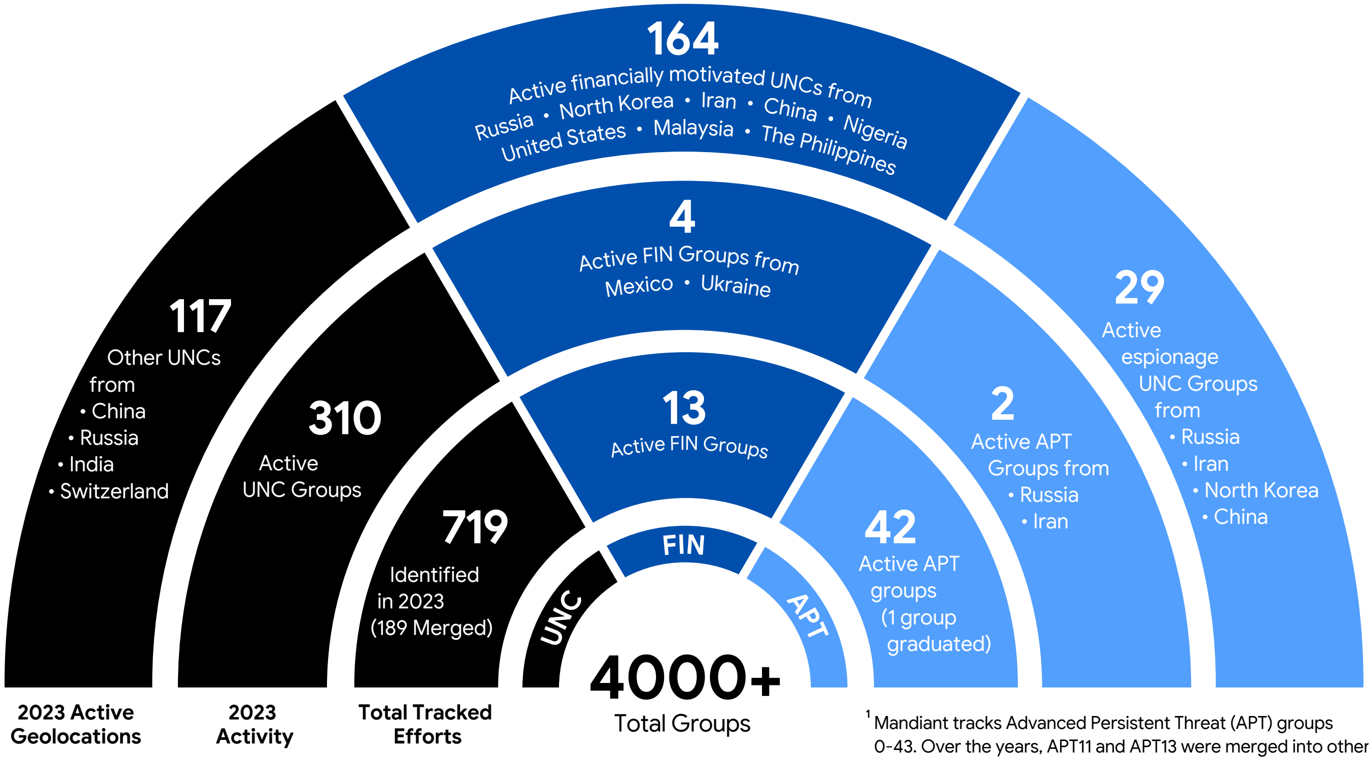
In 2023, Mandiant noted a decrease in the number of investigations that identified multiple threat groups in a single environment. In 17% of investigations, Mandiant experts uncovered more than one threat group operating in the target environment. This likely is related to the volume of targeted zero-days that Mandiant investigated. The 10 percentage point decrease from 2022 (27%) suggests a positive trend, potentially resulting from defenders' efforts to limit the ability of additional attackers to infiltrate environments.

Threat Groups



Mandiant tracks more than 4,000 threat groups, 719 of which were newly tracked in 2023. Mandiant investigators encountered 316 different threat groups when responding to intrusions in 2023, 220 groups were both newly tracked and observed in Mandiant investigations in 2023. These counts are largely in line with 2022 observations. For example in 2022, 265 groups were both newly tracked and observed in Mandiant investigations. In 2023, organizations faced intrusions by two named advanced persistent threat (APT) groups from Russia and Iran; four named financial threat (FIN) groups; and 310 uncategorized (UNC) groups. While 253 of these UNC groups were newly identified, Mandiant has tracked the remaining 57 UNC groups for periods ranging from one to 10 years. This distribution of threat groups suggests that organizations contend with both established and new threats on a regular basis.

Observed threat group is a threat group Mandiant investigators encountered during incident response investigations.

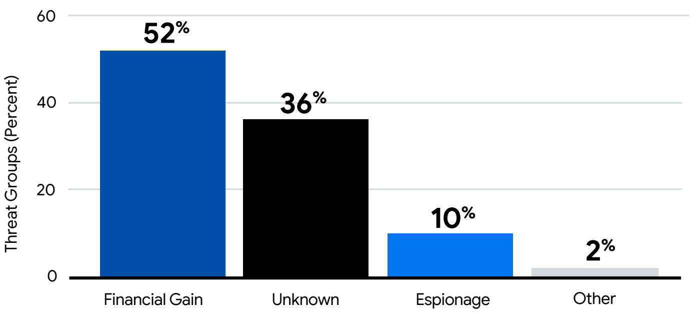


[1] Mandiant tracks Advanced Persistent Threat (APT) groups 0-43. Over the years, APT11 and APT13 were merged into other groups and subsequently deprecated resulting in 42 APT groups actively tracked by Mandiant.

UNC Group When Mandiant encounters new threat activity that cannot confidently be linked to an existing group, an UNC group designation is created to tie together observable artifacts associated with the activity cluster. As new information and artifacts are discovered that can be tied back to the same activity cluster, Mandiant analysts build on the initial understanding of the attacker, potentially merging it with other tracked threat clusters and ultimately graduating the UNC to an APT or FIN group.

More than half of the attackers observed in 2023 (52%) were primarily motivated by financial gain, and 10% principally pursued espionage activities. A very small percentage, just 2%, included threat clusters Mandiant judged to be operating for hacktivist motivations, attackers focused on disruption or destruction, and pentesters. For the remaining 36% of threat clusters, there was not sufficient evidence to determine a specific motivation with a high degree of confidence. Compared to 2022, Mandiant observed modest declines in the proportion of attackers pursuing objectives of espionage, disruption and destruction, hacktivism, and influence operations. Financially motivated groups made up a larger share of observed attackers in 2023, 52%, compared to 48% in 2022, a shift at least partially explained by the growth in ransomware- and extortion-related activity in 2023.

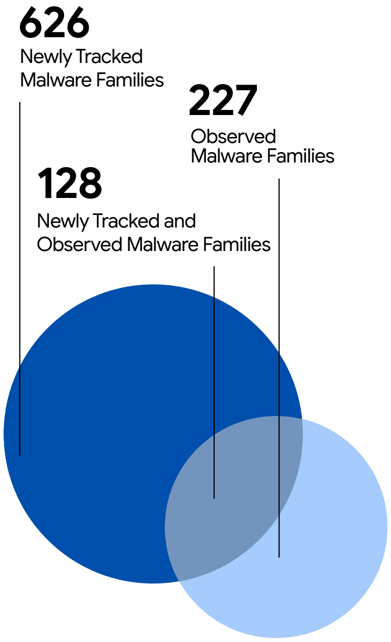
Observed Threat Groups by Goal, 2023



Graduation

In 2023, Mandiant graduated one new named threat group, APT43, and merged 189 activity clusters into other threat groups based on extensive research into activity overlaps. For details on how Mandiant defines and references UNC groups and merges, please see, “How Mandiant Tracks Uncategorized Threat Actors.”[12]

APT43 is a prolific cyber operator that supports the interests of the North Korean Government. The group combines moderately sophisticated technical capabilities with aggressive social engineering tactics, especially against South Korean and U.S. government organizations, academics, and think tanks focused on geopolitical issues surrounding the Korean Peninsula. In addition to its espionage campaigns, we believe APT43 funds itself through cyber crime operations to support its primary mission of collecting strategic intelligence. The group creates numerous spoofed and fraudulent personas for use in social engineering as well as cover identities for purchasing operational tooling and infrastructure. APT43 has collaborated with other North Korean espionage operators on multiple operations, underscoring the major role APT43 plays in North Korea’s cyber apparatus. For more details, see the full APT43 report.[13]



Malware

In 2023, Mandiant began tracking 626 new malware families, 128 of which were seen in incident response investigations. This is the highest number of net new malware families Mandiant has identified in a single year to date. However, this figure is not drastically higher than the 588 malware families that were newly tracked in 2022, which suggests that adversaries could be increasing their toolsets at a similar rate.

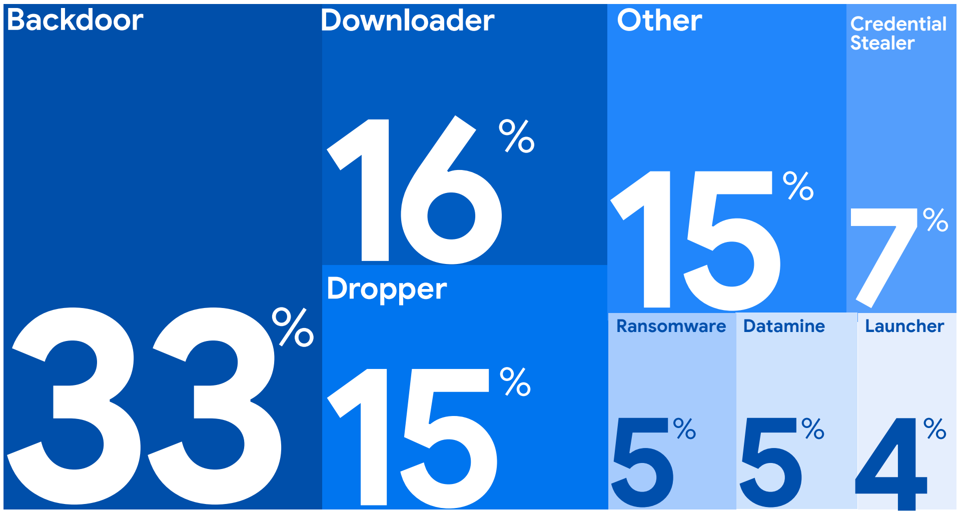
While Mandiant observed an increase in the number of newly tracked malware families in 2023, the total number of observed families declined from 321 to 277. This decrease may reflect the increased use of previously established tools and/or the rising number of compromises that use no malware at all. Of all 277 malware families observed in intrusions, 128 were newly tracked in 2023.

A malware category describes a malware family's primary purpose. Each malware family is assigned only one category that best describes its primary purpose, regardless of functionality for more than one category.

New Malware Families by Category

The top five malware categories have remained relatively consistent year over year. Of the 626 newly tracked malware families, the top five categories include backdoors (33%), downloaders (16%), droppers (15%), credential stealers (7%), and ransomware (5%). Newly tracked credential stealers return to the top five categories in 2023 after a brief hiatus observed in 2022. Another notable change in rankings is the decrease in newly tracked ransomware families, from 7% of malware families to 5% of newly tracked families in 2023. Although Mandiant responded to a similar proportion of ransomware intrusions in 2023 as in 2021, the decline in net new ransomware families may reflect the prevalence of ransomware strains that existed prior to 2023, such as LOCKBIT, ALPHV, BASTA, and ROYALLOCKER.

Newly Tracked Malware Families by Category, 2023



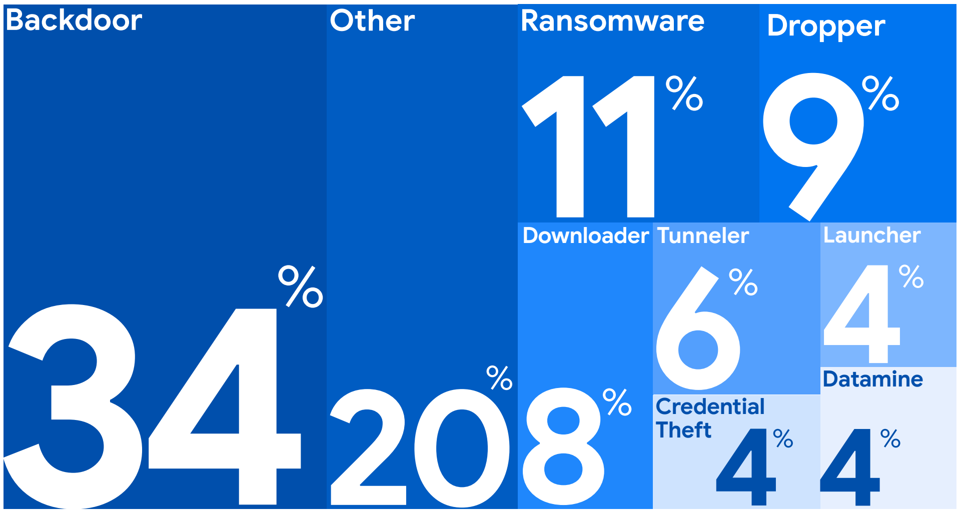
An observed malware family is a malware family identified during an investigation by Mandiant experts.

Observed Malware Families by Category

Observed malware family categories were also relatively consistent with the findings from previous years. Mandiant experts observed 277 malware families during investigations conducted in 2023. Backdoors remain the favorite among attackers, making up 34% of the observed malware dataset. This is up one percentage point from 2022. The remaining observed malware family categories show ransomware (11%), droppers (9%), downloaders (9%), and tunnelers (6%) rounding out the top five.

Mandiant continues to see a rise in attacker use of remote administration tools and other utilities to conduct their operations, noted in the continued increase in the "Other" category year over year. Of the 20% of malware families in this category, 8% represent legitimate utilities or remote administration tools. While not inherently malicious, attackers often leverage these tools in intrusions to evade detection, demonstrating their continued resourcefulness. To remain undetected and carry out further operations, attackers use living-off-the-land (LotL) techniques by employing system tools that are already in the environment or they abuse remote administrator tools that are less likely to be flagged by default in security technologies like Endpoint Detection and Response tooling.

Observed Malware Families by Category, 2023



Observed Malware Families 2022 to 2023

Backdoor

33% ↗ 34%

Downloader

10% ↘ 8%

Dropper

9% → 9%

Launcher

5% ↘ 4%

Tunneler

5% ↗ 6%

Ransomware

10% ↗ 11%

Other

28% ↘ 20%

Malware Category	Primary Purpose
Backdoor	A program whose primary purpose is to allow an attacker to issue interactive commands to the system on which it is installed.
Credential Stealer	A utility whose primary purpose is to access, copy, or steal authentication credentials.
Datamine	A utility whose primary purpose is to gather data, typically for theft. Excludes utilities that gather data such as credentials used for the purpose of escalating privileges or information used for system or network reconnaissance.
Downloader	A program whose sole purpose is to download (and perhaps launch) a file from a specified address and which does not provide any additional functionality or support any other interactive commands.
Dropper	A program whose primary purpose is to extract, install, and potentially launch or execute one or more files.
Launcher	A program whose primary purpose is to launch one or more files. Differs from a dropper or an installer in that it does not contain or configure the file, but merely executes or loads it.
Ransomware	A program whose primary purpose is to perform some malicious action (such as encrypting data) with the goal of extracting payment from the target in order to avoid or undo the malicious action.
Tunneler	A program that proxies or tunnels network traffic.
Other	Includes other categories, such as utilities, remote admin technologies, keyloggers, and point of sale.

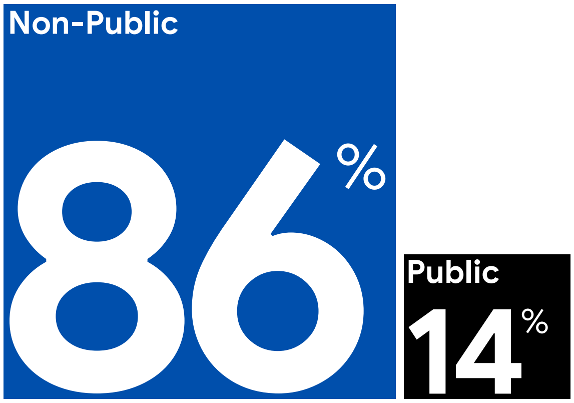
Malware by Availability

Malware family availability for both newly tracked and observed malware families remains more heavily weighted toward non-public in 2023, similar to previous M-Trends reporting. In both categories, malware families are more often privately developed or have restricted availability. Adversaries traditionally use a variety of non-public malware to conduct their operations. However, the share of publicly available malware families observed in investigations has increased by one percentage point from 2021 to 2022 and again from 2022 to 2023 to arrive at 30%. The increased use of publicly available malware likely reflects the rise in financially motivated attackers who prioritize speed and efficiency over long-term stealth.

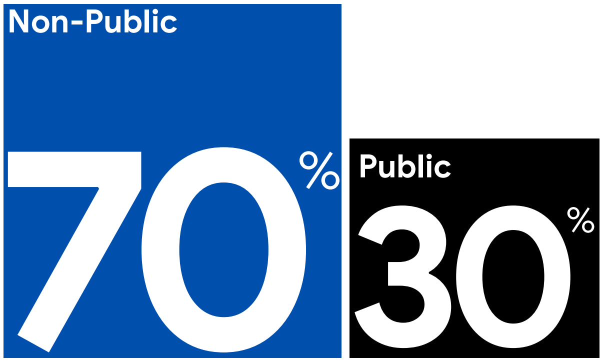
A publicly available tool or malware family is readily obtainable without restriction. This includes tools that are freely available on the internet as well as tools that are sold or purchased, as long as they can be purchased by any buyer.

A non-public tool or malware family is, to the best of our knowledge, not publicly available (either for free or for sale). They may include tools that are privately developed, held or used, as well as tools that are shared among or sold to a restricted set of customers.

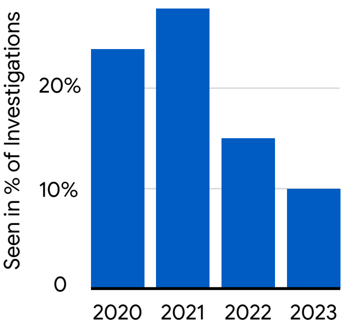
Newly Tracked Malware Families by Availability, 2023



Observed Malware Families by Availability, 2023



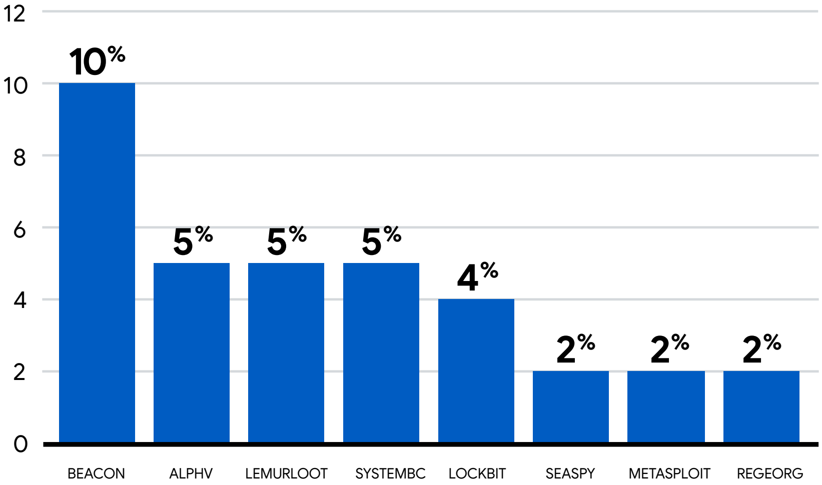
BEACON Usage, 2020-2023



Most Frequently Seen Malware

BEACON remains the most frequently observed malware family in Mandiant investigations globally and was identified in 10% of all intrusions. While BEACON remains the favorite among attackers, during the past three years Mandiant has seen a decrease in BEACON usage. In 2021, 28% of intrusions had at least one BEACON backdoor used. At the time, ransomware groups were actively compromising organizations across the globe and frequently used BEACON to conduct operations. In 2022, there was a global decrease in ransomware-related intrusions, and once again the usage of BEACON reflected that decrease. However, in 2023, Mandiant defenders noted BEACON usage at an all time low, despite an increase in ransomware intrusions.

Most Frequently Seen Malware Families, 2023



This decrease could align with attackers moving to evade endpoint security technology with memory resident malware, utilizing third-party remote administration tools, and employing more LotL techniques, or the abuse of native tools and processes on a system. Another possibility could be that attackers are migrating away from the command and control (C2) framework Cobalt Strike and the use of BEACON as their primary backdoor. As robust security community driven detections have created increased mitigations for the Cobalt Strike framework, attackers will increasingly turn to other C2 avenues such as SLIVER, Brute Ratel, and Mythic, to support operations.

ALPHV and LOCKBIT were the second and fifth most frequently observed malware families, respectively, in 2023. Mandiant encountered ALPHV ransomware in 5% of Mandiant led investigations in 2023 compared to 2% in 2022.

The third and sixth most prevalent malware families Mandiant observed were related to the first and third most exploited vulnerabilities. LEMURLOOT (5%) and SEASPY (2%) are backdoors used by attackers following exploitation of the MOVEit and Barracuda technologies respectively. The remaining frequently observed malware families have been used by multiple attackers, some also in conjunction with ALPHV, LOCKBIT, LEMURLOOT and SEASPY.

BEACON

A backdoor written in C/C++ that is part of the Cobalt Strike framework. Supported backdoor commands include shell command execution, file transfer, file execution, and file management. BEACON can also capture keystrokes and screenshots as well as act as a proxy server. BEACON may also be tasked with harvesting system credentials, port scanning, and enumerating systems on a network. BEACON communicates with a C2 server via HTTP or DNS. Mandiant has seen BEACON used by a wide range of named threat groups including APT19, APT32, APT40, APT41, FIN6, FIN7, FIN9, FIN11, FIN12 and FIN13, as well as more than 800 UNC groups.

ALPHV

Ransomware written in Rust. The ransomware may contain a plaintext JSON configuration that specifies the ransomware functionality. ALPHV may be able to escalate its privileges and bypass UAC, likely contains AES and ChaCha20 (or Salsa) encryption functionality, may use the Restart Manager as part of its operations, deletes volume shadow copies, may enumerate disk volumes and network shares, and may kill processes and services. Mandiant has seen more than 20 UNC groups with financial gain goals use ALPHV.

LEMURLOOT

LEMURLOOT is a web shell written in C# tailored to interact with the MOVEit Transfer platform. The malware authenticates incoming connections via a hard-coded password and can run commands that will download files from the MOVEit Transfer system, extract its Azure system settings, retrieve detailed record information, create and insert a particular user, or delete this same user. Data returned to the system interacting with LEMURLOOT is Gzip compressed.Based on Mandiant observations, FIN11 is the primary user of LEMURLOOT.

SYSTEMBC

A tunneler written in C that retrieves proxy-related commands from a C2 server using a custom binary protocol over TCP. A C2 server directs SYSTEMBC to act as a proxy between the C2 server and a remote system. SYSTEMBC is also capable of retrieving additional payloads via HTTP. Some variants may use the Tor network for this purpose. Downloaded payloads may be written to disk or mapped directly into memory prior to execution. SYSTEMBC is often used to hide network traffic associated with other malware families. Observed families include DANABOT, SMOKELOADER, and URSNIF. Mandiant has seen FIN12 and more than 40 UNC groups with financial gain goals use SYSTEMBC..

LOCKBIT

A ransomware written in C that encrypts files stored locally and on network shares. LOCKBIT can also identify additional systems on a network and propagate via SMB. Prior to encrypting files, LOCKBIT clears event logs, deletes volume shadow copies, and terminates processes and services that may impact its ability to encrypt files. LOCKBIT has been observed using the file extension ".lockbit" for encrypted files. Mandiant has seen more than 30 UNC groups with financial gain goals use LOCKBIT..

SEASPY

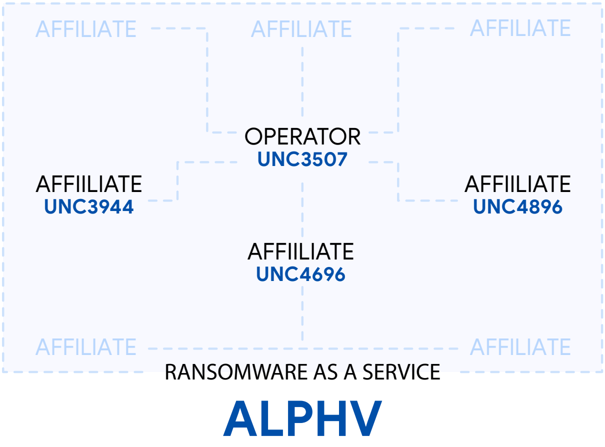
SEASPY is a backdoor that establishes a PCAP filter on port 25 (SMTP) and is activated when a "magic packet" is received. SEASPY masquerades as a legitimate Barracuda Network Service and changes its process in memory for further evasion. Mandiant has only seen UNC4841 use SEASPY.

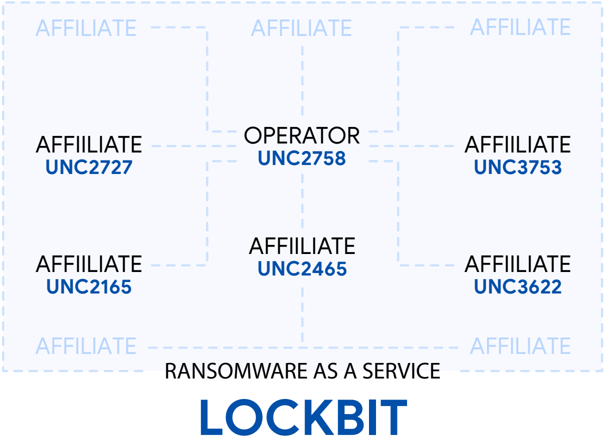
METASPLOIT

A penetration testing framework whose features include vulnerability testing, network enumeration, payload generation and execution, and defense evasion. The framework contains exploits for numerous applications and popular operating systems such as Windows, Linux, and macOS. METASPLOIT is commonly used to generate a stager payload, which is responsible for downloading and executing the framework's METERPRETER backdoor. Mandiant has seen APT32, APT41, APT43, FIN6, FIN7, FIN11, FIN13, and more than 160 UNC groups use Metasploit.

REGEORG

An open-source utility used to tunnel webshell traffic. Mandiant has seen APT28, APT29, APT41 and 30 UNC groups use REGEORG.





Notable Law Enforcement Actions

In a December 2023 press release, the United States Federal Bureau of Investigation (FBI) reported[14] that ALPHV, also known as BlackCat, had targeted more than 1,000 organizations. The FBI's press release also outlined the disruption campaign and the development of a decryption tool that allowed the FBI to offer help to a number of impacted organizations. Mandiant tracks the ALPHV ransomware operator as UNC3507, and several other clusters of activity as affiliates, most notably UNC3944, UNC4696, and UNC4896.

The fifth most frequently observed malware family across 2023 Mandiant investigations was LOCKBIT. LOCKBIT ransomware appeared in 4% of investigations compared to 2% in 2022. The LOCKBIT data leak site listed more targets than any other extortion group in 2023 by a significant margin. In June 2023, the United States Department of Justice (DOJ) announced criminal charges[15] against a LOCKBIT affiliate, the third individual charged by the DOJ for their role in the global LOCKBIT ransomware operation. Since LOCKBIT first appeared in early 2020, the DOJ has noted that there have been more than 1,400 attacks conducted by LOCKBIT ransomware-as-a-service (RaaS) affiliates. International law enforcement continued to pursue LOCKBIT activity, announcing seizure of the LOCKBIT data leak site and back-end infrastructure in "Operation Cronos" in February 2024.[16] Mandiant tracks the LOCKBIT ransomware operator as UNC2758 and five other notable affiliate groups.

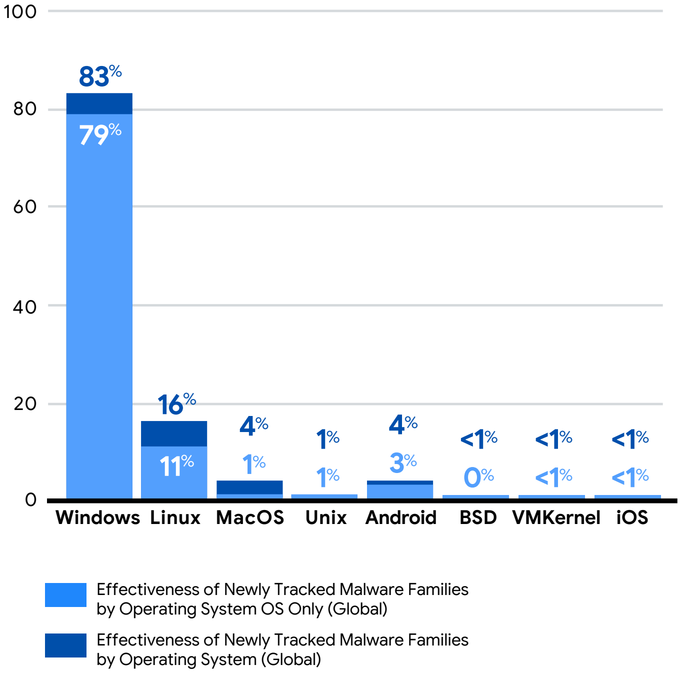
Ransomware families like ALPHV and LOCKBIT operate within their own criminal ecosystems. Following the December 2023 law enforcement disruption of ALPHV, the operators of the LOCKBIT ransomware service attempted to take advantage of the situation by appealing to ALPHV affiliates and attempting to undercut negotiation processes ALPHV targets had already engaged in. Despite these disruptions and arrests by law enforcement, ransomware groups remain resilient and adapt quickly, mitigating the impact on their operations. While law enforcement efforts have yielded decryptors and temporary slowdowns, the profitability of ransomware incentivizes financially motivated adversaries to continue their attacks, highlighting the need for organizations to maintain strong security practices.

Operating System Effectiveness

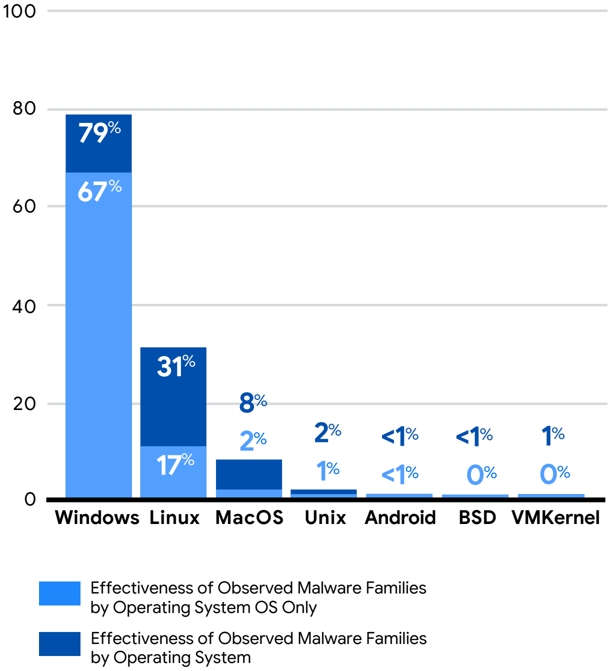
The operating system effectiveness of a malware family is the operating system(s) that the malware can be used against.

In 2023, Mandiant noted a slight increase in newly tracked malware effective on Linux systems at 16%, compared to 12% in 2022. Notably, observed malware effective on Linux has increased to 31% of all malware observed in 2023, compared to 15% in 2022. Similar to previous M-Trends reporting periods, most newly tracked and observed malware families still remain effective on Windows. The apparent decline in the percentage of Windows-related malware from 2022 to 2023 likely reflects the greater share of Linux-related malware rather than a true decline in malware effective on Windows.

Operating System Effectiveness of Newly Tracked Malware Families, 2023



Operating System Effectiveness of Observed Malware Families, 2023



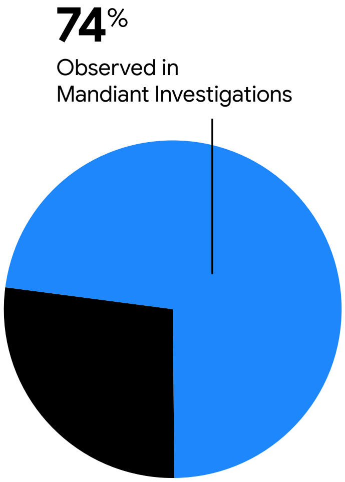
MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, government, and the cybersecurity product and service community.

Threat Techniques

Since M-Trends 2020, Mandiant has supported the community by mapping findings presented in M-Trends to the MITRE ATT&CK framework. As organizations continue to strengthen their security measures, they can work to prioritize implementing detection capabilities based on techniques and sub-techniques used in intrusions. Mandiant provides metrics around the most frequently observed techniques that adversaries used as a resource to organizations as they make decisions on how to further improve their security capabilities.

Mandiant has mapped an additional 1,200+ Mandiant techniques to the updated MITRE ATT&CK framework, bringing the total to 3,500+ Mandiant techniques and subsequent findings associated with the ATT&CK framework. In 2023, the MITRE ATT&CK framework was updated to version 14.1, resulting in ATT&CK for Enterprise now containing 201 techniques and 427 sub-techniques.

MITRE ATT&CK Techniques Used Most Frequently, 2023



MITRE ATT&CK Techniques Used Most Frequently, 2023

Mandiant experts observed adversaries use 74% of MITRE ATT&CK techniques and 44% of sub-techniques during 2023 intrusions. Nearly three quarters of mapped ATT&CK techniques and almost half of the sub-techniques were actively observed in intrusions Mandiant investigated in 2023. This breadth of techniques and sub-techniques is at the same magnitude that Mandiant defenders observed in 2022.

The techniques that attackers used in 2023 are consistent with those observed in 2022, with the top 10 most frequently seen techniques showing little variance over the last several years. In more than half of investigations, Mandiant investigators noted the use of a command or scripting interpreter (T1059) by attackers. Notable differences in the 2023 dataset is the presence of System Owner or User Discovery (T1033) and use of exploits against a public-facing application (T1190) in the top 10 list of observed techniques. These two techniques correlate with the rise of ransomware-related intrusions and the increase in exploit use, specifically mass exploitation campaigns observed in 2023.

It is unsurprising that the top five observed sub-techniques are PowerShell (T1059.001), Web Protocols (T1071.001), Remote Desktop Protocol (T1021.001), Service Execution (T1569.002), and File Deletion (T1070.004), as this is the fourth consecutive year they have dominated the charts. Attackers likely favor these sub-techniques because they utilize readily available tools within a system, making them easy to abuse. Their history of successful compromises, combined with the ability to sometimes evade security measures, makes them a highly effective part of an attacker's toolkit. This persistent trend reveals the standard tactics attackers employ to achieve their objectives. Organizations must prioritize detecting these sub-techniques if they haven't done so already.

Top 10 Most Frequently Seen Techniques

1	T1059: Command and Scripting Interpreter	52.3%
2	T1027: Obfuscated Files or Information	46.5%
3	T1083: File and Directory Discovery	38.6%
4	T1021: Remote Services	37.3%
5	T1082: System Information Discovery	37.1%
6	T1070: Indicator Removal	35.1%
7	T1071: Application Layer Protocol	34.0%
8	T1033: System Owner/User Discovery	31.7%
9	T1140: Deobfuscate/Decode Files or Information	31.5%
10	T1190: Exploit Public-Facing Application	28.7%

Top 5 Most Frequently Seen MITRE ATT&CK Sub-Techniques

1	T1059.001: PowerShell	32.3%
2	T1071.001: Web Protocols	29.6%
3	T1021.001: Remote Desktop Protocol	28.3%
4	T1569.002: Service Execution	26.8%
5	T1070.004: File Deletion	26.6%

The observed MITRE ATT&CK techniques mapped to the Mandiant Targeted Attack Lifecycle can be found in the appendix of this report.

Campaigns & Global Events

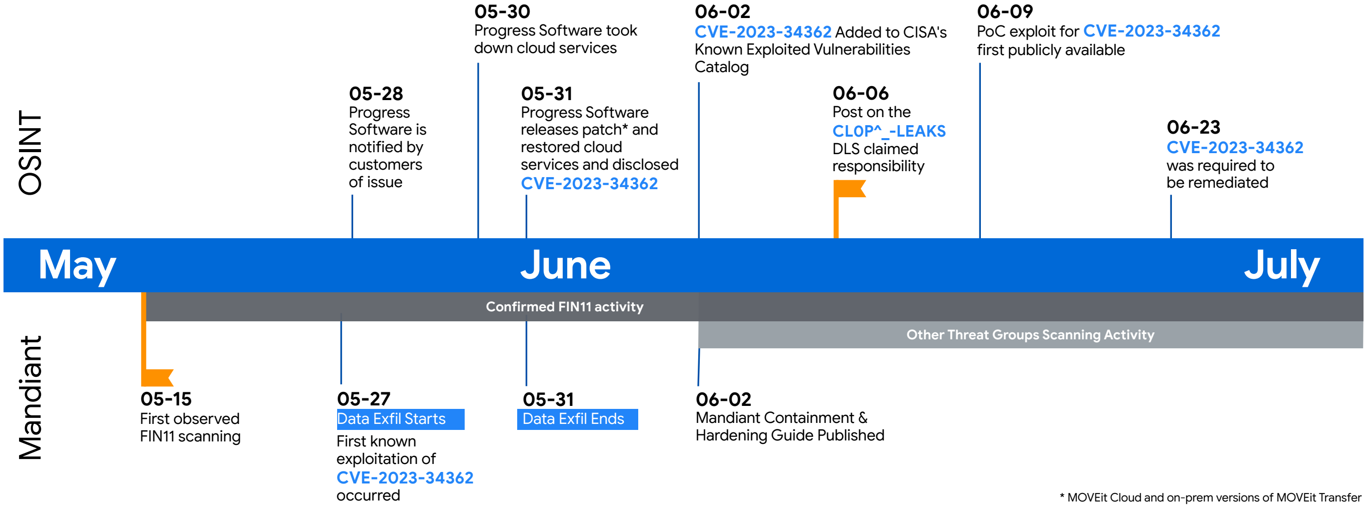
Campaigns are a set of impactful intrusions conducted by an attacker or multiple attackers in cooperation toward a single objective at multiple targets within a relevant timeframe.[17]

Global events are a set of impactful intrusions conducted by multiple unrelated adversaries in parallel campaigns involving a similar theme, target, or resource.

When Mandiant experts observe that multiple organizations are actively being impacted by similar threat activity, a campaign or global event is created. A Campaign is a set of activity in which one or more threat groups coordinate to achieve a single objective. Larger scale Global Events can encompass multiple threat groups pursuing multiple disparate objectives, but using similar tactics, often exploiting a vulnerability. Campaigns and Global Events (CGE) provide clients with notification of emerging and active threat activity. Over the course of each campaign and global event, Mandiant dynamically updates potential targets with new data as more information is received and analyzed. This intelligence includes indicators of compromise, context surrounding key events, and defensive and prevention measures based directly on data collected from Mandiant investigations and other Mandiant research.

Campaigns and Global Events provide Mandiant clients with the critical intelligence needed to defend against today's most dangerous threats. Early identification of active exploits means attacks can be halted quickly, minimizing damage. CGEs facilitate rapid collaboration between teams, ensuring a swift response. As Mandiant uncovers new threat data, CGE users receive immediate updates, enabling them to refine defenses and pinpoint the attack's full impact. Mandiant tracked and reported 25 campaigns and global events in 2023 related to Mandiant Consulting investigations. These campaigns affected organizations across the Americas, EMEA, and JAPAC from 21 industry verticals.

CVE-2023-34362 Retrospective Timeline



OSINT

05-28 Progress Software is notified by customers of issue

05-30 Progress Software took down cloud services

05-31 Progress Software releases patch* and restored cloud services and disclosed CVE-2023-34362

06-02 CVE-2023-34362 Added to CISA's Known Exploited Vulnerabilities Catalog

06-06 Post on the CL0P^_-LEAKS DLS claimed responsibility

06-09 PoC exploit for CVE-2023-34362 first publicly available

06-23 CVE-2023-34362 was required to be remediated

Mandiant

05-15 First observed FIN11 scanning

05-27 Data Exfil Starts First known exploitation of CVE-2023-34362 occurred

05-31 Data Exfil Ends

06-02 Mandiant Containment & Hardening Guide Published

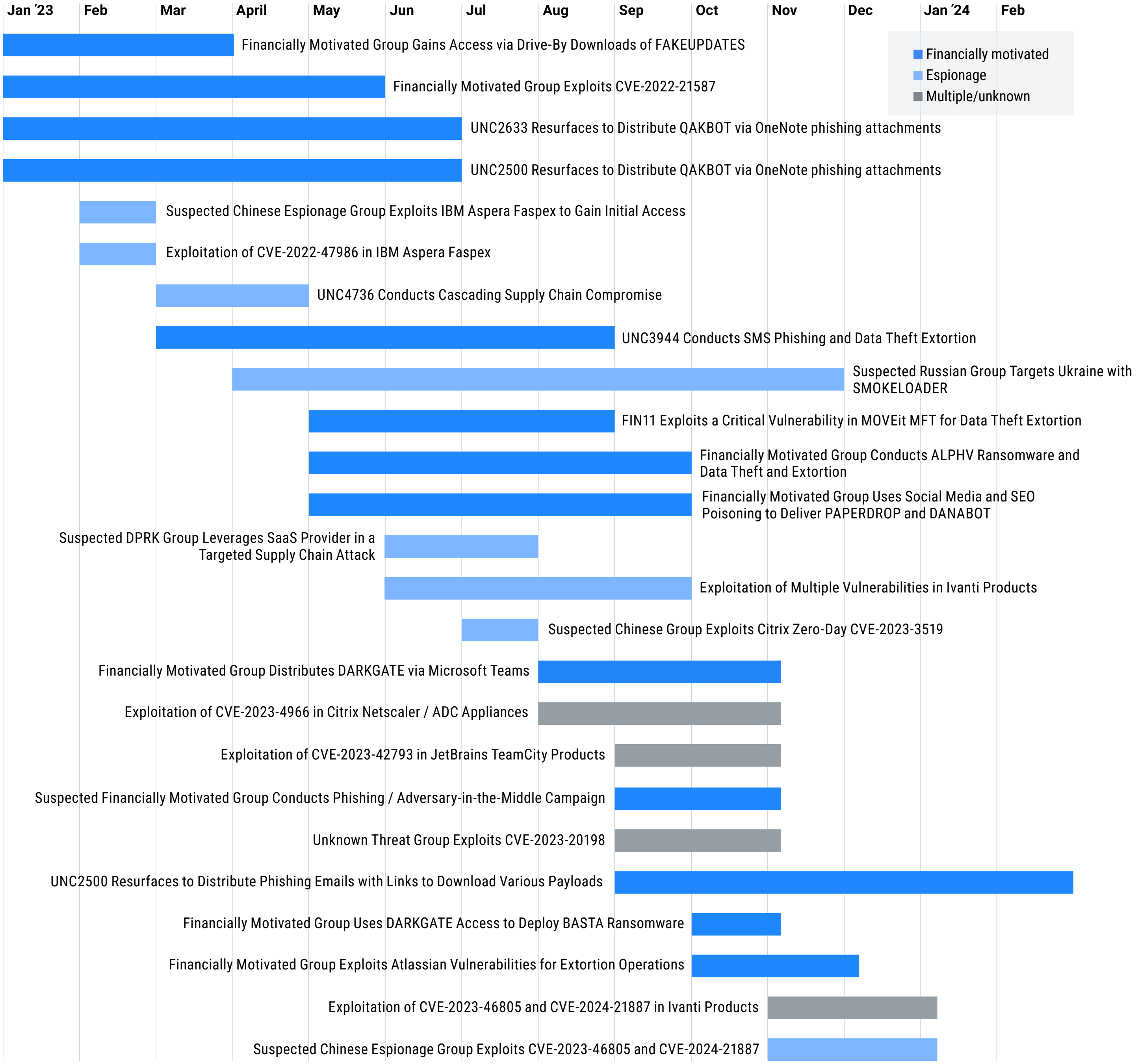
* MOVEit Cloud and on-prem versions of MOVEit Transfer

The FIN11 MOVEit exploitation campaign represents a prominent example of this type of event. The CVE-2023-34362 Retrospective Timeline illustrates observations related to FIN11's[18] exploitation of this vulnerability.[19]

Mandiant investigators observed FIN11 scanning the internet beginning on May 15, 2023, using infrastructure that was subsequently used to exploit the MOVEit zero-day vulnerability. Based on analysis from Mandiant incident response engagements, the earliest evidence of exploitation of CVE-2023-34362 occurred twelve days later, on May 27, 2023. The evidence also indicates that FIN11 began stealing data from numerous organizations via MOVEit technology within 16 hours of the first exploitation of the vulnerability. On May 31, 2023, Progress disclosed the vulnerability, patched its cloud-based service, and released a patch for on-premises implementations. It was not until 10 days following the first successful exploitation of the vulnerability, on June 6, 2023, that FIN11 claimed responsibility for the campaign on the CL0P^_- LEAKS DLS. The first PoC was made publicly available three days later, on June 9, 2023.

Notably, from late 2020 to 2023,[20] FIN11 demonstrated a pattern of exploiting vulnerabilities in four different file transfer applications, likely because this type of campaign offers FIN11 several advantages. A working exploit allows FIN11 to compromise many targets at once. Specific targeting of file transfer software provides tactical advantages and supports FIN11's business model of data theft extortion. FIN11 can obtain target files directly from the file transfer appliance without additional lateral movement into target environments, which would require time and effort on the part of the attacker and create more opportunities for defenders to detect the intrusion.

2023 Campaigns and Global Events Related to Mandiant Incident Response Investigations



Industries Affected
Manufacturing
Legal & Professional Services

Financial Services
Healthcare
Technology

Media & Entertainment
Chemicals & Materials
Education
Energy & Utilities

Retail
Insurance
Pharmaceuticals
Telecommunications

Automotive
Civil Society & Non-Profits
Construction & Engineering
Government

Oil & Gas
Transportation
Other

Regional Trends

Americas

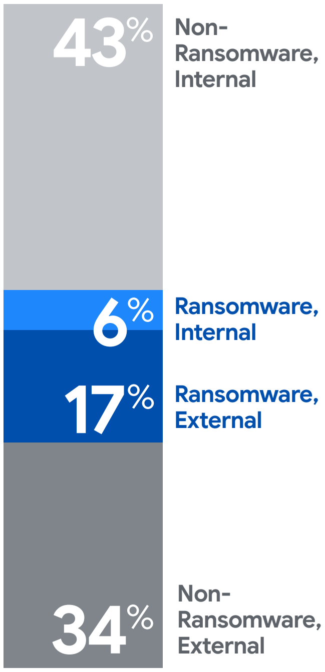
The metrics reported in this section are based on Mandiant Consulting investigations affecting organizations that are located in North, Central, or South America.

Detection by Source

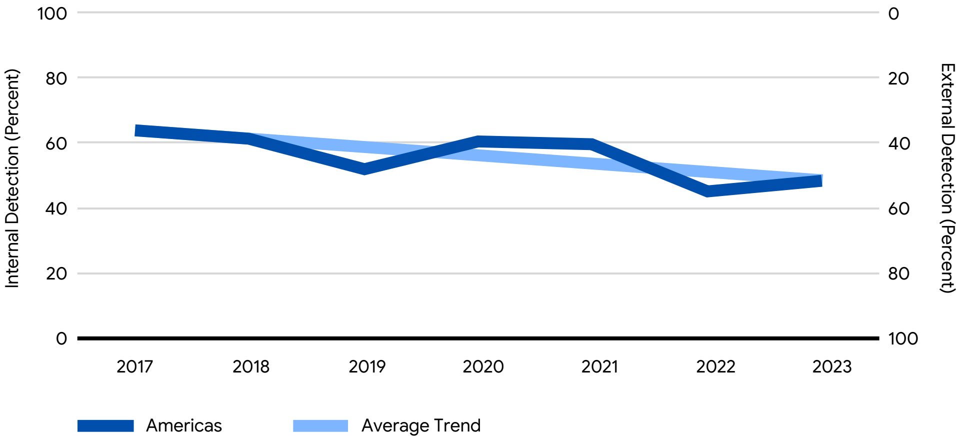
In the Americas in 2023, 51% of organizations first learned of a compromise from an external source, while 49% identified evidence of a compromise internally. This split appears to be consistent with a long-term global trend toward a balance of internal versus external discovery. This is also consistent with observations in the Americas from 2022, continuing a trend toward higher rates of external notifications overall compared to 2017–2021. Growth in ransomware-related intrusions over the last four years has likely contributed to this shift in notification source.

Isolating ransomware-related intrusions from all other compromises exposes a strong divergence in notification sources in ransomware versus non-ransomware-related intrusions. Approximately two thirds of ransomware-related intrusions in the Americas were externally notified—most frequently by the attackers themselves in the form of a ransom note. In contrast, organizations in the region first discovered evidence of a compromise internally in slightly more than half of cases that were not related to ransomware encryption events.

Detection by Source—Americas, 2023



Detection by Source—Americas, 2017-2023



Americas Median Dwell Time

In 2023, organizations located in the Americas detected intrusions at the same pace as in 2022. Median dwell time in the Americas was 10 days. External parties notified these organizations of intrusions in 13 days, compared to 12 days in 2022. However, when intrusions were detected internally, organizations uncovered malicious activity in eight days in 2023 compared to nine days in the previous year.

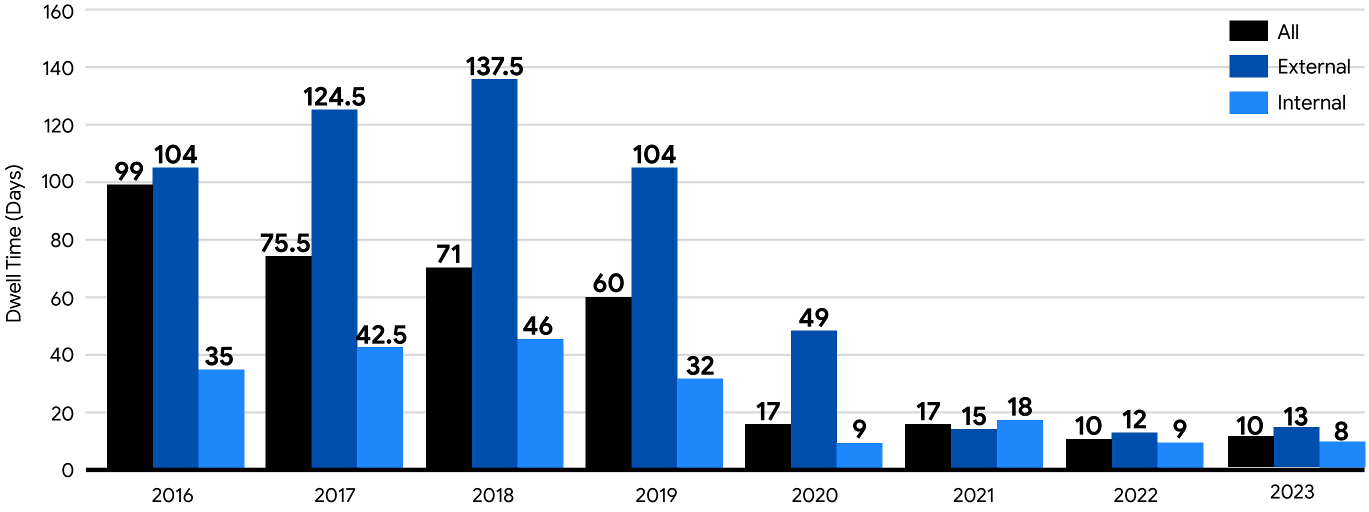
Dwell time is calculated as the number of days an attacker is present in a target environment before they are detected. The median represents a value at the midpoint of a dataset sorted by magnitude.

Change in Americas Median Dwell Time

10 → **10**

days in 2022 days in 2023

Americas Median Dwell Time, 2016-2023



Dwell Time Distribution

Organizations in the Americas region continue to improve their detection capabilities. Organizations detected 45% of intrusions in one week or less, a rate that is similar to that seen in 2022. In 68.5% of investigations conducted by Mandiant, defenders were made aware of intrusions in 30 days or less, a four percentage-point increase in investigations compared to 2022.

Consistent with trends seen globally, organizations continue to identify intrusions that had remained undetected for longer periods of time. Organizations located in the Americas region saw a small increase in intrusions detected in five years or less and a decrease in intrusions that were undetected for more than five years.

Americas Dwell Time Distribution, 2021-2023

	1 week or less	30 days or less	6 months or less	1 year or less	5 years or less	5 years or more
2021	38.8%	18.0%	28.2%	11.1%	3.6%	0.4%
2022	44.5%	19.4%	26.2%	4.5%	2.6%	2.8%
2023	45.0%	23.5%	22.3%	4.8%	4.2%	0.3%

Change in Americas Investigations Involving Ransomware

22% ↗ 23%

in 2022 in 2023

Change in Americas Median Dwell Time—Ransomware

5 ↗ 6

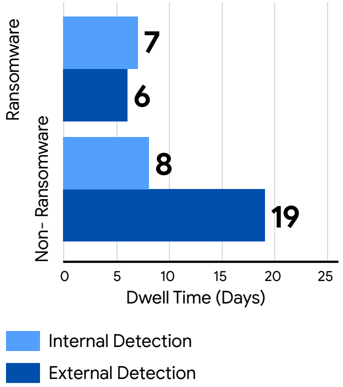
days in 2022 days in 2023

Change in Americas Median Dwell Time—Non-Ransomware

12 → 12

days in 2022 days in 2023

Americas Median Dwell Time by Detection Source

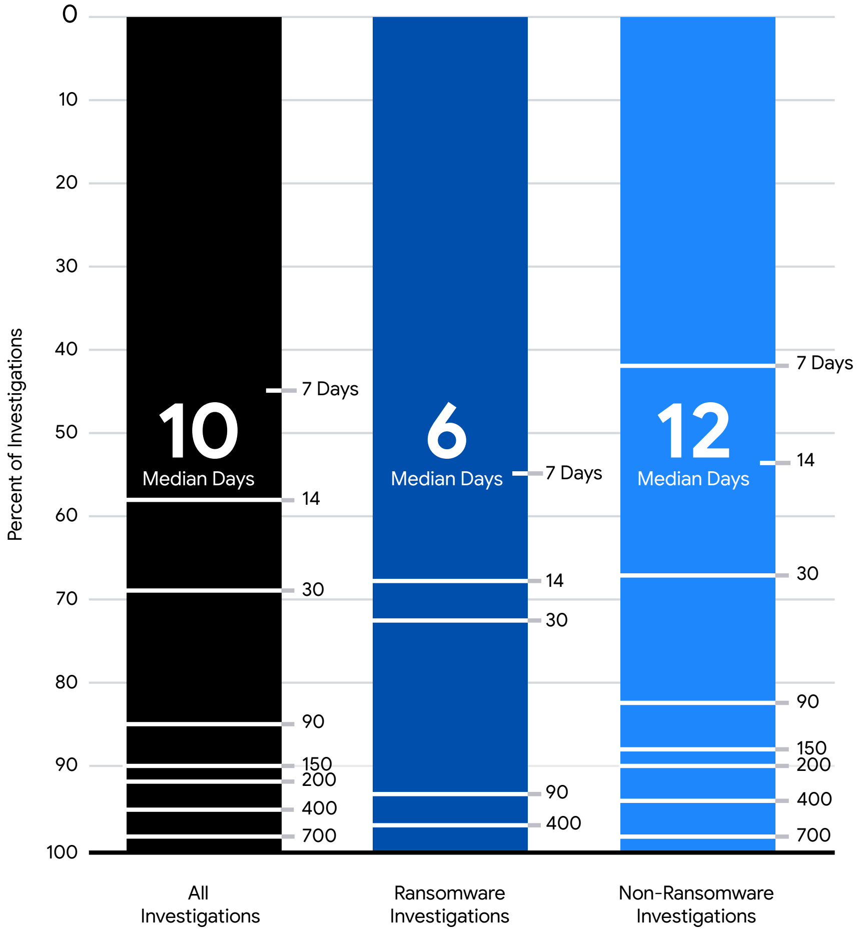


Investigations Involving Ransomware

Organizations located in the Americas detected overall intrusions related to ransomware in six days compared to five days seen in the previous M-Trends reporting period. This could be explained by the slight increase in investigations involving ransomware, or it could be a slight variation in the ransomware attackers' ability to conduct operations. In intrusions related to ransomware, targeted organizations detected malicious activity internally in seven days, compared to six days when an external party made organizations aware of an intrusion.

In intrusions that did not involve ransomware, internal detection remained the fastest way for organizations to be notified of an intrusion, with a dwell time of eight days. When they did not detect an intrusion internally, organizations in the Americas were notified of intrusions within a median of 19 days by an external party.

Americas Dwell Time by Investigation Type, 2023



AMERICAS

Exploit
41%

Phishing
18%

Prior Compromise
14%

Targeted Attacks

Initial Infection Vector

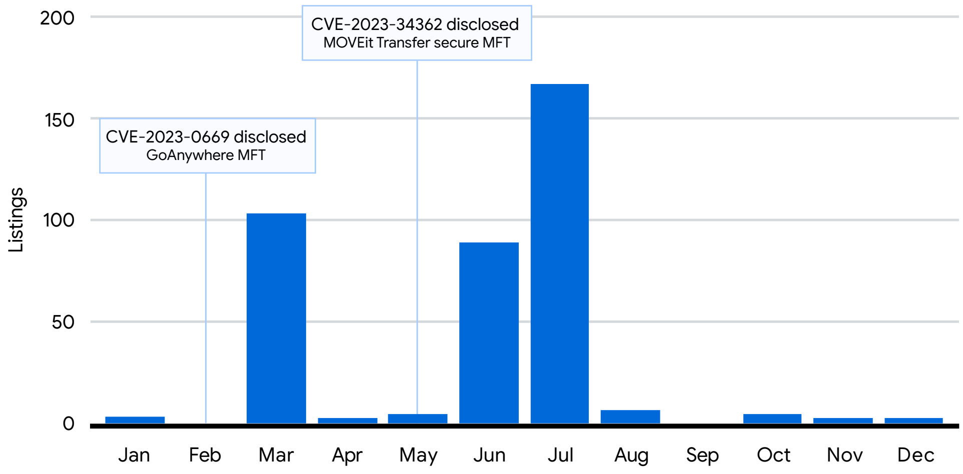
Organizations in the Americas faced threats similar to those experienced by organizations across the globe. In 41% of intrusions that had an initial infection vector identified, an exploit was the source of attacker activity in the region. Phishing was used as an initial vector in 18% of intrusions. Rounding out the top three, attackers leveraged prior compromised access gained from another threat group or malware in 14% of intrusions.

Threat Groups

Prevalent Threat Group Targeting Americas

The most frequently observed attacker in the Americas in 2023 was FIN11, a financially motivated threat group. The majority of FIN11 intrusions Mandiant investigated were related to the widespread campaign exploiting CVE-2023-34362 in the MOVEit Transfer secure managed file transfer (MFT) software.[21] Mandiant also investigated intrusions in which FIN11 exploited CVE-2023-0669 in GoAnywhere MFT. Although FIN11 has deployed the CLOP ransomware in the past, in these campaigns the attacker focused on data theft extortion with no ransomware encryption. Counts of listings from the CL0P^_- LEAKS DLS corroborate Mandiant's investigative findings and demonstrate the scale FIN11 was able to achieve through these focused vulnerability exploitation campaigns.

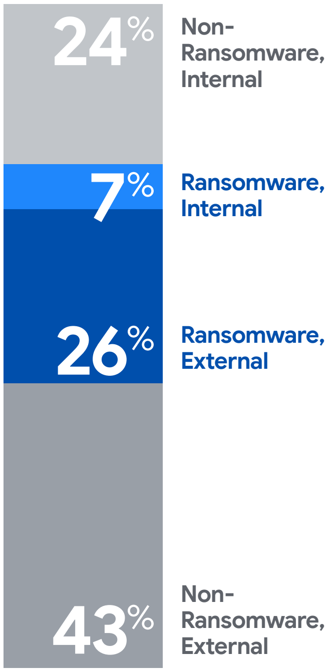
Listings Posted to CL0P^_- LEAKS DLS, 2023



JAPAC

The metrics reported in this section are based on Mandiant Consulting investigations affecting organizations in Japan and Asia Pacific (JAPAC).

Detection by Source—JAPAC, 2023

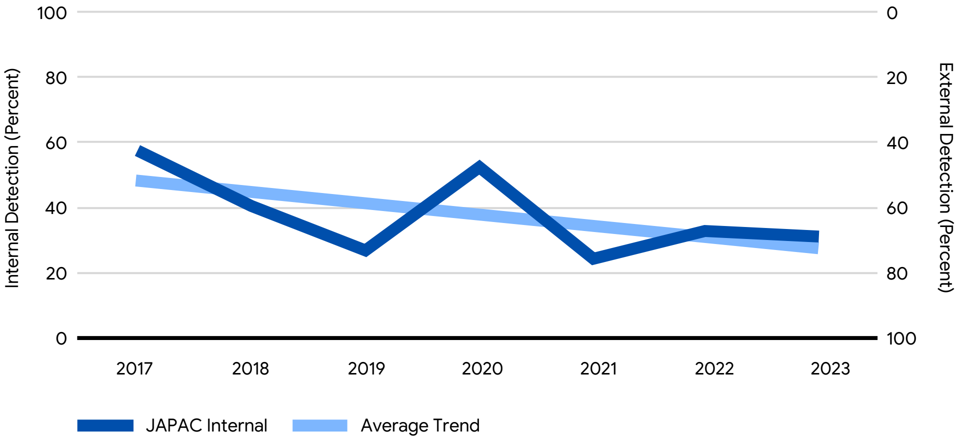


Detection by Source

For intrusions in the JAPAC region in 2023, organizations were notified of compromises from external sources in 69% of cases, while 31% of intrusions were discovered internally. This continues a long-term trend in JAPAC of internal detections representing a declining proportion of overall notification sources.

In line with global numbers, organizations located in JAPAC were notified more often of intrusions via external notifications. In 2023 in JAPAC, organizations learned of ransomware-related infections from external sources in three forths of cases.

Detection by Source—JAPAC, 2017-2023



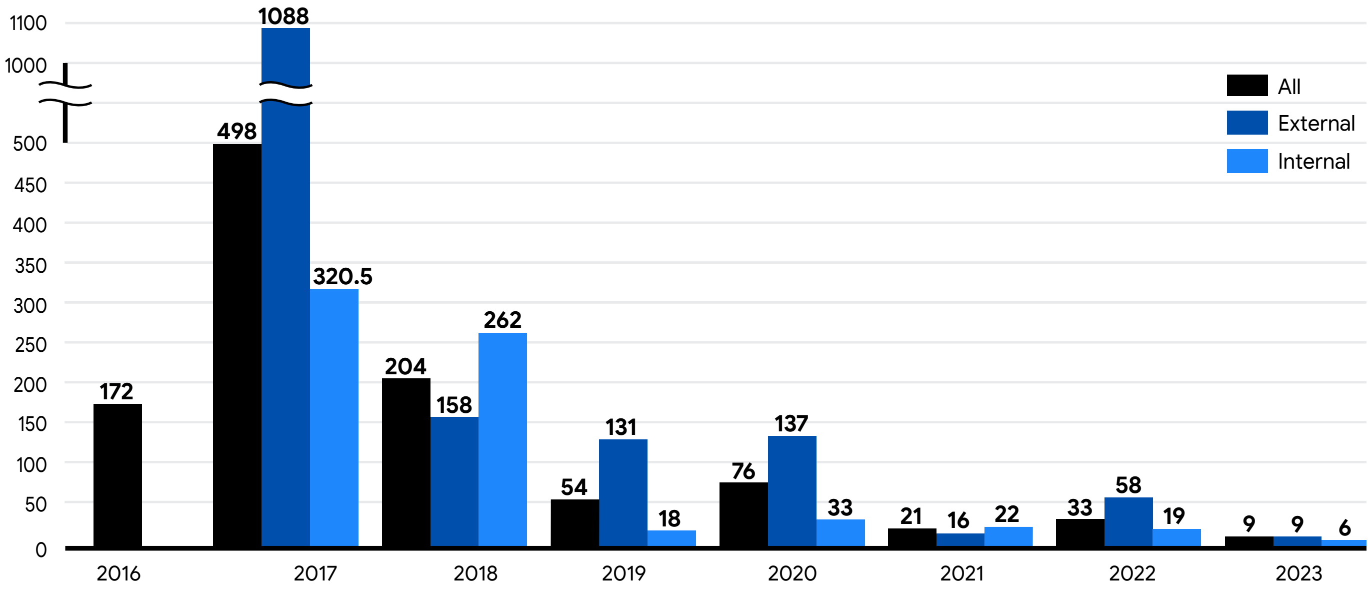
Change in JAPAC Median Dwell Time

33 days in 2022 ↘ **9** days in 2023

JAPAC Median Dwell Time

Organizations in the JAPAC region continued to detect intrusions more quickly year over year. This was true for both notification sources. Median dwell time in JAPAC achieved its quickest time of nine days from initial infection to detection, compared to 33 days in 2022. Organizations identified an intrusion internally in six days in JAPAC, compared to 19 days seen in 2022. Organizations received external notifications of malicious activity in nine days, just over one week, compared to nearly two months in 2022.

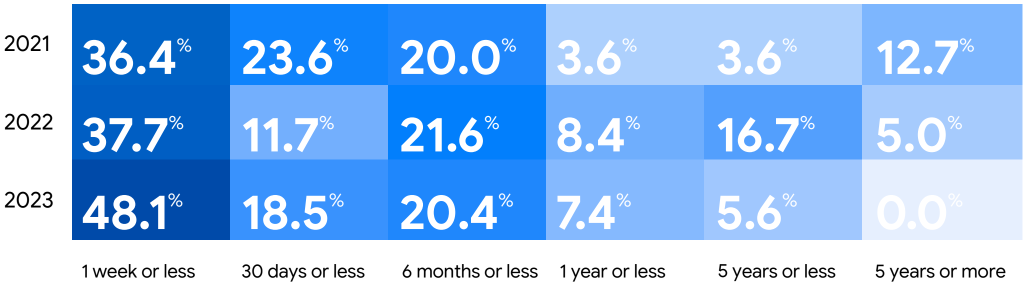
JAPAC Median Dwell Time, 2016-2023



Dwell Time Distribution

In 2023, targeted attacker activity was detected in 48% of intrusions in JAPAC in one week or less. Continuing with observations both globally and year over year in the region, the number of intrusions detected sooner continues to increase, showing the resilience of defenders. Over the past three years, Mandiant has seen fewer intrusions remain undetected for longer periods of time in the JAPAC region.

JAPAC Dwell Time Distribution, 2021-2023



	1 week or less	30 days or less	6 months or less	1 year or less	5 years or less	5 years or more
2021	36.4%	23.6%	20.0%	3.6%	3.6%	12.7%
2022	37.7%	11.7%	21.6%	8.4%	16.7%	5.0%
2023	48.1%	18.5%	20.4%	7.4%	5.6%	0.0%

Change in JAPAC Investigations Involving Ransomware

32% ↗ **33%**

in 2022 in 2023

Change in JAPAC Median Dwell Time—Ransomware

19 ↘ **3**

days in 2022 days in 2023

Change in JAPAC Dwell Time—Non-Ransomare

60 ↘ **26**

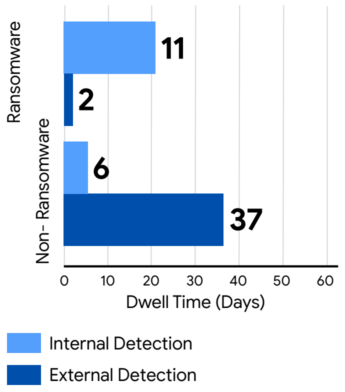
days in 2022 days in 2023

Investigations Involving Ransomware

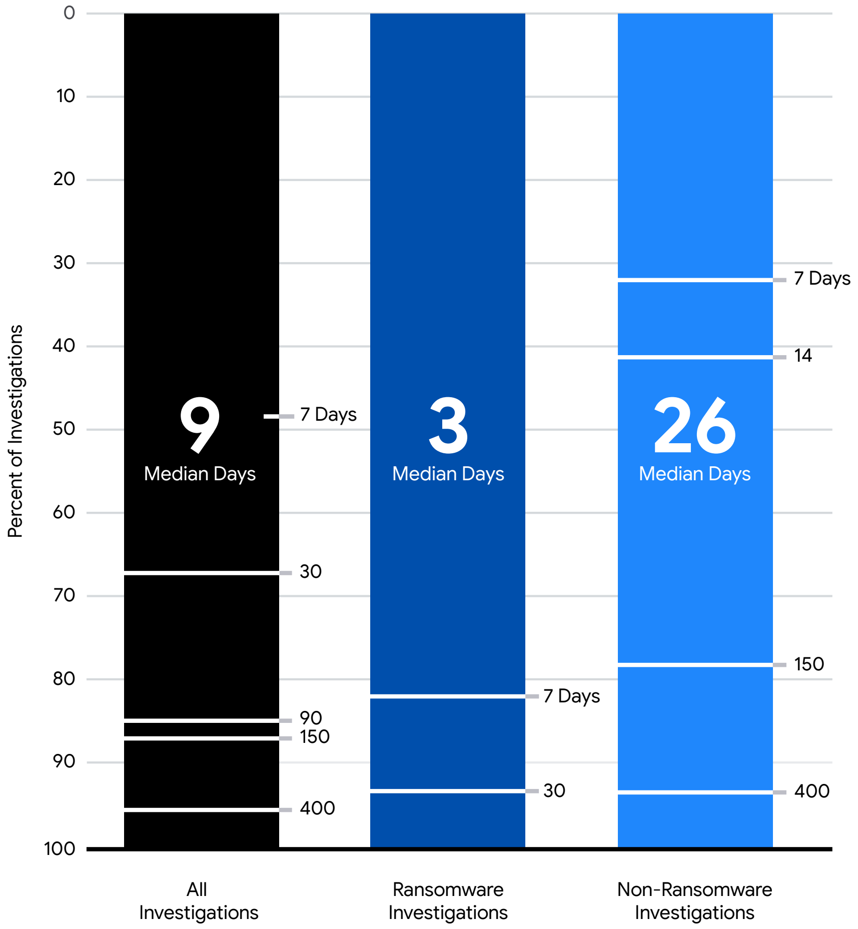
JAPAC saw little movement in the volume of ransomware-related intrusions, with a small increase to 33% of investigations conducted in the region in 2023. However, dwell time for ransomware-related intrusions declined to three days compared to 19 days in 2022. This sharp decrease is likely a cause of the quick moving ransomware families used in intrusions over the years. Mandiant has observed ransomware-related intrusions balance speed and thoroughness of compromise. Attackers who deploy ransomware want to move fast enough to reduce the chance of detection, but also be meticulous enough to ensure potential damage that is sufficient to increase the likelihood of maximum ransom payment.

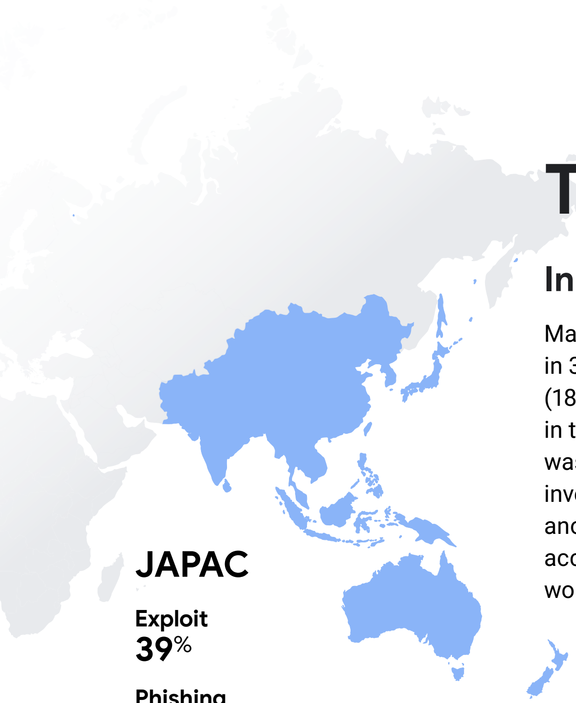
Organizations detected non-ransomware-related intrusions quicker in 2023 in slightly more than half the time observed in 2022. The median dwell time in the JAPAC region for non-ransomware-related intrusions was 26 days in 2023. Organizations were notified of an intrusion in six days by an internal security product or team member. Externally, however, organizations were notified of an intrusion 37 days after the malicious activity initially began.

JAPAC Median Dwell Time by Detection Source



JAPAC Dwell Time by Investigation Type, 2023





JAPAC

Exploit
39%

Phishing
18%

Prior Compromise
15%

Targeted Attacks

Initial Infection Vector

Mandiant investigators identified that organizations in JAPAC were impacted by exploits in 39% of investigations when an initial infection vector was identified. In nearly a fifth (18%) of investigations, attackers leveraged brute-force techniques to gain initial access in the region. Rounding out the top three most seen initial infection vectors in the region was the use of access obtained by a prior compromise. In 15% of intrusions, Mandiant investigators identified evidence that an attacker leveraged access originally obtained by another attacker through either purchased access or by leveraging unsecured backdoor access. The increase in prior compromise usage is likely representative of the inner workings of the criminal ransomware ecosystem.

Threat Groups

Prevalent Threat Group Targeting JAPAC

In the Japan and Asia Pacific region in 2023, Mandiant investigators most often encountered suspected Chinese cyber espionage cluster UNC4841.

Beginning in at least October 2022, UNC4841 exploited a zero-day vulnerability, CVE-2023-2868, in Barracuda Email Security Gateway (ESG) appliances in a campaign targeting public and private organizations worldwide.[22] In several cases, Mandiant observed evidence of UNC4841 searching for and exfiltrating data relevant to Chinese political or strategic interests. In the set of entities that UNC4841 selected for focused data theft, Mandiant uncovered shell scripts that targeted email domains and users from Ministries of Foreign Affairs of ASEAN member nations as well as individuals within foreign trade offices and academic research organizations in Taiwan and Hong Kong.

In this campaign, UNC4841 took a number of steps to disguise its activity. For example, it inserted malware in or used the names of legitimate Barracuda modules and phishing messages that were designed to be intercepted by spam filters and avoid further investigation by security teams. Notably, after the initial vulnerability disclosure and remediation efforts, UNC4841 responded aggressively, rapidly altering its malware, deploying additional persistence mechanisms, and moving laterally to maintain access to target environments. Further analysis on this can be found in Attacker Operations Involving Zero-Days Vary Depending on Motivation.

EMEA

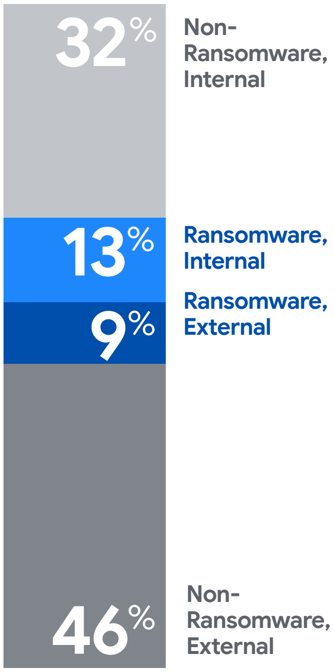
The metrics reported in this section are based on Mandiant Consulting investigations affecting organizations in Europe, the Middle East, and Africa (EMEA).

Detection by Source

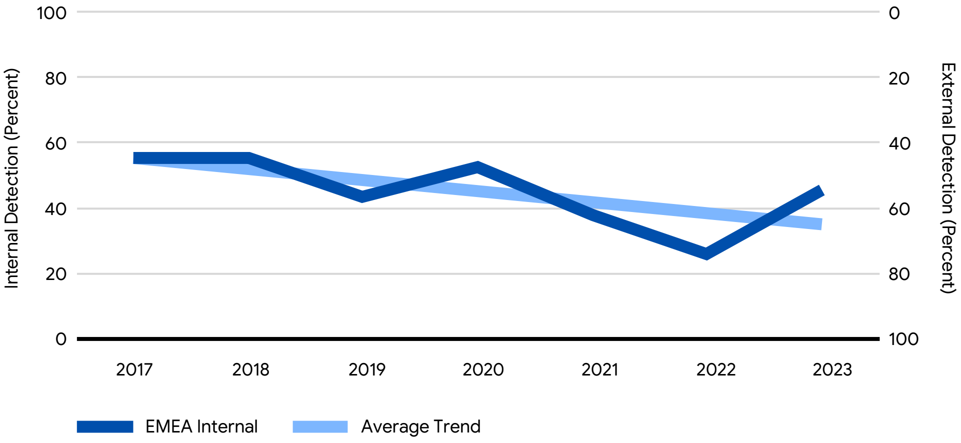
In cases Mandiant investigated in 2023 in EMEA, organizations first discovered evidence of a compromise internally 46% of the time, while organizations were externally notified of compromises in 54% of intrusions. This split matches global numbers for 2023 and reverses a long-term trend toward declining rates of internal notifications for the region.

Organizations in EMEA identified ransomware-related intrusions internally slightly more frequently than through external notifications such as a ransom note. The majority of non-ransomware-related intrusions were identified by external security partners.

Detection by Source—EMEA, 2023



Detection by Source—EMEA, 2017-2023



Change in EMEA Median Dwell Time

20 ↗ **22**

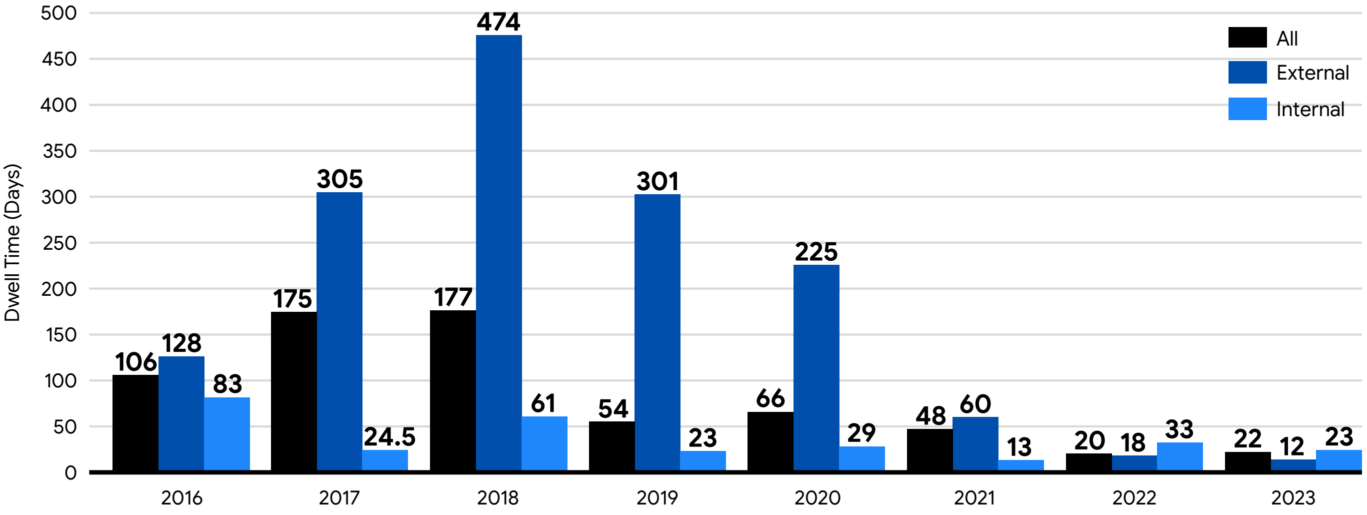
days in 2022 days in 2023

EMEA Median Dwell Time

Organizations in EMEA detected intrusions in 22 days in 2023 compared to 20 days in 2022. Dwell time for intrusions detected externally decreased to just under two weeks, at 12 days in 2023 compared to 18 seen in 2022. Organizations detected intrusions internally in 23 days in 2023 compared to 33 days in 2022.

Over the years, dwell time has varied across detection sources in EMEA. The general trend shows that median dwell time continues to decrease year over year, with median dwell time in 2022 resulting in the shortest time period seen in the region. The small variation seen in 2023 could be the result of regional data normalizing, following the notable portion of Mandiant's work in Ukraine in 2022.

EMEA Median Dwell Time, 2016-2023



Dwell Time Distribution

This year in EMEA, organizations saw intrusions go undetected for longer periods of time compared to previous years, with 14% of investigations conducted in the region remaining undetected for up to five years. However, in 2023, organizations saw less than 1% of investigations go undetected for more than five years.

EMEA Dwell Time Distribution, 2021-2023

	1 week or less	30 days or less	6 months or less	1 year or less	5 years or less	5 years or more
2021	33.0%	14.0%	22.0%	12.0%	14.0%	6.0%
2022	41.6%	12.2%	17.7%	10.2%	11.5%	7.0%
2023	35.9%	20.5%	23.1%	6.4%	14.1%	0.0%

Change in EMEA Investigations Involving Ransomware

7% ↗ **22%**

in 2022 in 2023

Change in EMEA Median Dwell Time—Ransomware

33 ↘ **8**

days in 2022 days in 2023

Change in EMEA Dwell Time—Non-Ransomare

19 ↗ **31**

days in 2022 days in 2023

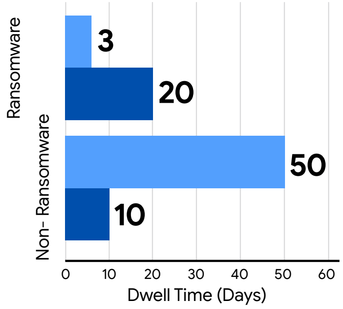
Investigations Involving Ransomware

Organizations working with Mandiant in EMEA saw ransomware-related intrusions return to a volume previously seen in 2021. Nearly a quarter of the investigations conducted in the region were ransomware-related, 22% in 2023 compared to 7% in 2022.

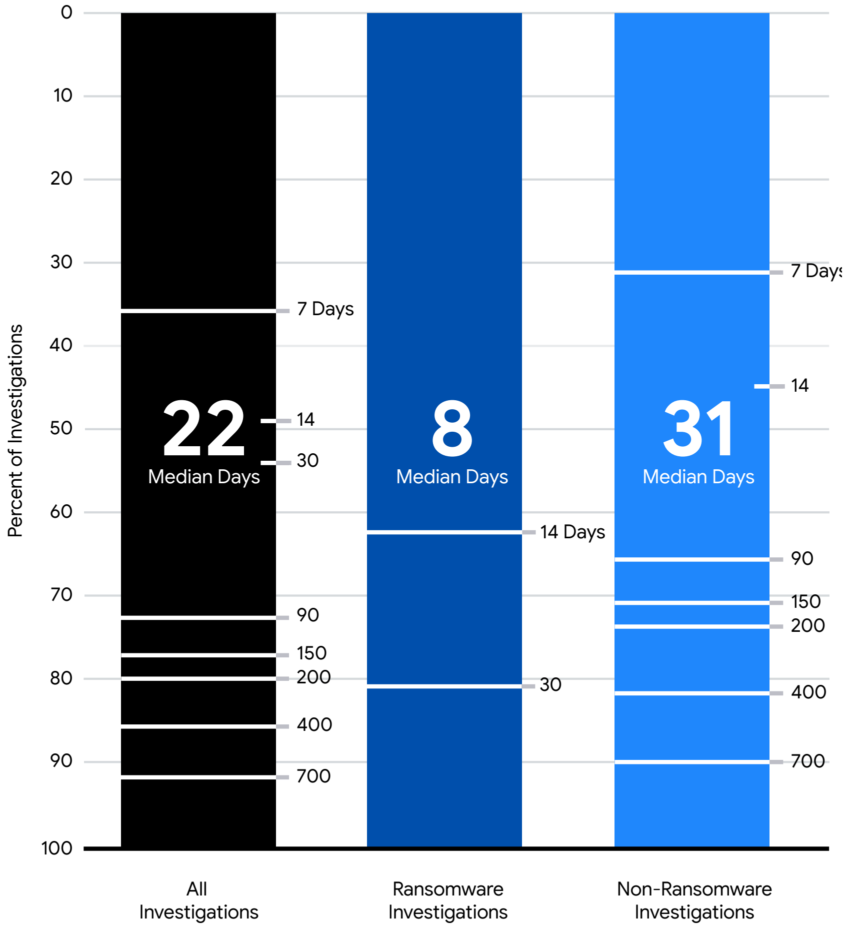
The median dwell time for ransomware-related intrusions decreased in the region. Ransomware intrusions were detected in little more than one week, with eight days compared to 33 days in 2022. Internal detection of ransomware intrusions in EMEA took 3 days, compared to 20 days for external notifications.

Intrusions not related to ransomware were detected in 31 days in 2023, compared to 19 days in 2022. Non-ransomware-related intrusions remain undetected for longer periods of time if they are detected by an internal source.

EMEA Median Dwell Time by Detection Source



EMEA Dwell Time by Investigation Type, 2023



EMEA
Exploit
37%
Prior Compromise
21%
Phishing
16%

Targeted Attacks

Initial Infection Vector

In EMEA, Mandiant investigators noted intrusions began with an exploit in 36% of intrusions when an initial infection vector was identified. Organizations in EMEA also faced attackers abusing prior access in 21% of intrusions and phishing in 16% of intrusions.

Threat Groups

Prevalent Threat Group Targeting EMEA

Mandiant investigated a variety of intrusions in EMEA in 2023, including compromises attributed to UNC4393. UNC4393 is a financially motivated threat cluster that has monetized access by deploying BASTA ransomware. This cluster does not work alone but rather relies on other attackers to obtain initial access into target environments. Throughout most of 2023, Mandiant found that UNC2500 and UNC2633 QAKBOT infections consistently preceded UNC4393 activity in target environments. In August 2023, an international law enforcement effort disrupted the QAKBOT botnet,[23] which forced UNC2500 to shift to alternative malware payloads to continue operations. Starting in mid-September 2023, Mandiant observed UNC2500 begin distributing DARKGATE payloads, which UNC4393 leveraged to ultimately deploy BASTA ransomware.

Mandiant regularly observes evidence that multiple attackers were involved in different stages of a compromise, and prior compromise was the third most common initial access vector for 2023 Mandiant incident responses. The complexity of multi-attacker intrusions and the speed with which attacker tactics, techniques, and procedures (TTPs) evolve underscores the importance of implementing defense-in-depth strategies to minimize the impact of an attacker gaining a foothold in an environment.

MITRE ATT&CK

Techniques Related to Mandiant Targeted Attack Lifecycle, 2023

Mandiant's Targeted Attack Lifecycle is the predictable sequence of events cyber attackers use to carry out their attacks.

Initial Reconnaissance

Reconnaissance

T1595: Active Scanning	1.1%	T1595.001: Scanning IP Blocks	0.6%
		T1595.002: Vulnerability Scanning	0.6%

Resource Development

T1608: Stage Capabilities	12.8%	T1608.003: Install Digital Certificate	6.6%
		T1608.005: Link Target	2.6%
		T1608.001: Upload Malware	2.1%
		T1608.002: Upload Tool	0.9%
		T1608.006: SEO Poisoning	0.9%
T1583: Acquire Infrastructure	5.4%	T1583.003: Virtual Private Server	5.4%
T1584: Compromise Infrastructure	3.2%		
T1587: Develop Capabilities	2.3%	T1587.002: Code Signing Certificates	1.3%
		T1587.003: Digital Certificates	0.9%
T1588: Obtain Capabilities	1.5%	T1588.004: Digital Certificates	1.1%
		T1588.003: Code Signing Certificates	0.4%
T1585: Establish Accounts	0.2%	T1585.002: Email Accounts	0.2%

Initial Compromise

Initial Access

T1190: Exploit Public-Facing Application	28.7%		
T1133: External Remote Services	20.3%		
T1566: Phishing	16.3%	T1566.001: Spearphishing Attachment	5.1%
		T1566.002: Spearphishing Link	3.2%
		T1566.004: Spearphishing Voice	1.9%
		T1566.003: Spearphishing via Service	0.8%
T1078: Valid Accounts	11.3%	T1078.004: Cloud Accounts	2.1%
		T1078.001: Default Accounts	0.2%
T1189: Drive-by Compromise	3.4%		
T1195: Supply Chain Compromise	0.8%	T1195.002: Compromise Software Supply Chain	0.6%
T1199: Trusted Relationship	0.8%		
T1091: Replication Through Removable Media	0.6%		
T1200: Hardware Additions	0.2%		

Establish Foothold

Persistence

T1543: Create or Modify System Process	28.3%	T1543.003: Windows Service	16.7%
		T1543.002: Systemd Service	0.9%
		T1543.004: Launch Daemon	0.4%
		T1543.001: Launch Agent	0.2%
T1098: Account Manipulation	18.6%	T1098.005: Device Registration	2.1%
		T1098.004: SSH Authorized Keys	1.7%
		T1098.001: Additional Cloud Credentials	0.4%
T1053: Scheduled Task/Job	18.0%	T1053.005: Scheduled Task	14.8%
		T1053.003: Cron	1.7%
T1003: OS Credential Dumping	16.9%	T1003.003: NTDS	7.1%
		T1003.001: LSASS Memory	5.4%
		T1003.002: Security Account Manager	3.0%
		T1003.008: /etc/passwd and /etc/shadow	2.4%
		T1003.006: DCSync	0.4%
		T1003.004: LSA Secrets	0.2%
T1505: Server Software Component	14.4%	T1505.003: Web Shell	14.3%
		T1505.001: SQL Stored Procedures	0.2%
		T1505.004: IIS Components	0.2%
T1136: Create Account	11.8%	T1136.001: Local Account	5.4%
		T1136.002: Domain Account	1.1%
		T1136.003: Cloud Account	0.6%
T1574: Hijack Execution Flow	10.3%	T1574.011: Services Registry Permissions Weakness	8.6%
		T1574.002: DLL Side-Loading	1.1%
		T1574.001: DLL Search Order Hijacking	0.4%
		T1574.008: Path Interception by Search Order Hijacking	0.4%
		T1574.006: Dynamic Linker Hijacking	0.2%
T1547: Boot or Logon Autostart Execution	9.6%	T1547.001: Registry Run Keys / Startup Folder	7.1%
		T1547.009: Shortcut Modification	2.6%
		T1547.004: Winlogon Helper DLL	0.4%
		T1547.011: Plist Modification	0.2%
T1552: Unsecured Credentials	8.8%	T1552.002: Credentials in Registry	2.4%
		T1552.004: Private Keys	1.7%
		T1552.001: Credentials In Files	1.3%
		T1552.003: Bash History	0.9%
		T1552.006: Group Policy Preferences	0.8%
		T1555.005: Password Managers	0.8%
T1056: Input Capture	8.1%	T1056.001: Keylogging	7.5%
		T1056.002: GUI Input Capture	0.6%
		T1056.003: Web Portal Capture	0.2%

T1110: Brute Force	7.3%	T1110.001: Password Guessing	2.8%
		T1110.003: Password Spraying	1.1%
		T1110.004: Credential Stuffing	0.8%
T1555: Credentials from Password Stores	5.4%	T1555.003: Credentials from Web Browsers	3.2%
		T1555.004: Windows Credential Manager	2.8%
		T1555.006: Cloud Secrets Management Stores	0.9%
		T1555.005: Password Managers	0.8%
		T1555.001: Keychain	0.2%
T1546: Event Triggered Execution	3.4%	T1546.003: Windows Management Instrumentation Event Subscription	2.8%
		T1546.008: Accessibility Features	0.4%
		T1546.010: AppInit DLLs	0.2%
		T1546.015: Component Object Model Hijacking	0.2%
T1111: Multi-Factor Authentication Interception	3.2%		
T1558: Steal or Forge Kerberos Tickets	3.2%	T1558.003: Kerberoasting	1.7%
T1556: Modify Authentication Process	1.7%	T1556.006: Multi-Factor Authentication	1.1%
		T1556.002: Password Filter DLL	0.2%
		T1556.003: Pluggable Authentication Modules	0.2%
T1037: Boot or Logon Initialization Scripts	0.9%	T1037.004: RC Scripts	0.6%
T1187: Forced Authentication	0.8%		
T1539: Steal Web Session Cookie	0.8%		
T1649: Steal or Forge Authentication Certificates	0.4%		
T1557: Adversary-in-the-Middle	0.2%	T1557.00: LLMNR/NBT-NS Poisoning and SMB Relay	0.2%
T1621: Multi-Factor Authentication Request Generation	0.2%		

Escalate Privileges

Privilege Escalation

T1543: Create or Modify System Process	28.3%	T1543.003: Windows Service	16.7%
		T1543.005: Scheduled Task	14.8%
		T1543.002: Systemd Service	0.9%
		T1543.004: Launch Daemon	0.4%
		T1543.001: Launch Agent	0.2%
T1055: Process Injection	25.1%	T1055.003: Thread Execution Hijacking	1.3%
		T1055.004: Asynchronous Procedure Call	0.9%
		T1055.001: Dynamic-link Library Injection	0.8%
		T1055.002: Portable Executable Injection	0.4%
		T1055.012: Process Hollowing	0.4%
T1053 Scheduled Task/Job	18%	T1053.003: Cron	1.7%
T1134: Access Token Manipulation	13.7%	T1134.001: Token Impersonation/Theft	4.9%
		T1134.004: Parent PID Spoofing	0.6%
T1547: Boot or Logon Autostart Execution	9.6%	T1547.001: Registry Run Keys/Startup Folder	7.1%
		T1547.009: Shortcut Modification	2.6%
		T1547.004: Winlogon Helper DLL	0.4%
		T1547.011: Plist Modification	0.2%
T1546: Event Triggered Execution	3.4%	T1546.003: Windows Management Instrumentation Event Subscription	2.8%
		T1546.008: Accessibility Features	0.4%
		T1546.010: AppInit DLLs	0.2%
		T1546.015: Component Object Model Hijacking	0.2%
T1484: Domain Policy Modification	1.5%	T1484.001: Group Policy Modification	1.5%
T1037: Boot or Logon Initialization Scripts	0.9%	T1037.004: RC Scripts	0.6%
T1548: Abuse Elevation Control Mechanism	0.8%	T1548.002: Bypass User Account Control	0.8%
T1068: Exploitation for Privilege Escalation	0.6%		

Internal Reconnaissance

Discovery

T1083: File and Directory Discovery	38.6%		
T1082: System Information Discovery	37.1%		
T1033: System Owner/User Discovery	31.7%		
T1087: Account Discovery	28.1%	T1087.002: Domain Account	15.0%
		T1087.001: Local Account	10.5%
		T1087.004: Cloud Account	0.8%
T1012: Query Registry	24.8%		
T1016: System Network Configuration Discovery	23.5%	T1016.001: Internet Connection Discovery	5.3%
T1622: Debugger Evasion	21.8%		
T1057: Process Discovery	18.9%		
T1003: OS Credential Dumping	16.9%	T1003.003: NTDS	7.1%
		T1003.001: LSASS Memory	5.4%
		T1003.002: Security Account Manager	3.0%
		T1003.008: /etc/passwd and /etc/shadow	2.4%
		T1003.006: DCSync	0.4%
		T1003.004: LSA Secrets	0.2%
T1518: Software Discovery	16.3%	T1518.001: Security Software Discovery	1.3%
T1614: System Location Discovery	15.9%	T1614.001: System Language Discovery	9.6%
T1069: Permission Groups Discovery	14.8%	T1069.002: Domain Groups	11.1%
		T1069.001: Local Groups	1.3%
		T1069.003: Cloud Groups	1.1%
T1482: Domain Trust Discovery	12.6%		
T1497: Virtualization/Sandbox Evasion	12.2%	T1497.001: System Checks	10.1%
T1007: System Service Discovery	11.4%		
T1552: Unsecured Credentials	8.8%	T1552.002: Credentials in Registry	2.4%
		T1552.004: Private Keys	1.7%
		T1552.001: Credentials In Files	1.3%
		T1552.003: Bash History	0.9%
		T1552.006: Group Policy Preferences	0.8%
T1049: System Network Connections Discovery	8.1%		
T1056: Input Capture	8.1%	T1056.001: Keylogging	7.5%
		T1056.002: GUI Input Capture	0.6%
		T1056.003: Web Portal Capture	0.2%
T1110: Brute Force	7.3%	T1110.001: Password Guessing	2.8%
		T1110.003: Password Spraying	1.1%
		T1110.004: Credential Stuffing	0.8%
T1010: Application Window Discovery	7.1%		

T1135: Network Share Discovery	6.8%		
T1555: Credentials from Password Stores	5.4%	T1555.003: Credentials from Web Browsers	3.2%
		T1555.004: Windows Credential Manager	2.8%
		T1555.006: Cloud Secrets Management Stores	0.9%
		T1555.005: Password Managers	0.8%
		T1555.001: Keychain	0.2%
T1046: Network Service Discovery	3.4%		
T1111: Multi-Factor Authentication Interception	3.2%		
T1558: Steal or Forge Kerberos Tickets	3.2%	T1558.003: Kerberoasting	1.7%
T1018: Remote System Discovery	2.8%		
T1556: Modify Authentication Process	1.7%	T1556.006: Multi-Factor Authentication	1.1%
		T1556.002: Password Filter DLL	0.2%
		T1556.003: Pluggable Authentication Modules	0.2%
T1580: Cloud Infrastructure Discovery	1.5%		
T1124: System Time Discovery	1.3%		
T1619: Cloud Storage Object Discovery	1.3%		
T1040: Network Sniffing	0.8%		
T1615: Group Policy Discovery	0.8%		
T1187: Forced Authentication	0.8%		
T1539: Steal Web Session Cookie	0.8%		
T1526: Cloud Service Discovery	0.6%		
T1120: Peripheral Device Discovery	0.4%		
T1201: Password Policy Discovery	0.4%		
T1538: Cloud Service Dashboard	0.4%		
T1649: Steal or Forge Authentication Certificates	0.4%		
T1217: Browser Bookmark Discovery	0.2%		
T1557: Adversary-in-the-Middle	0.2%	T1557.001: LLMNR/NBT-NS Poisoning and SMB Relay	0.2%
T1621: Multi-Factor Authentication Request Generation	0.2%		

Lateral Movement

Lateral Movement

T1021: Remote Services	37.3%	T1021.001: Remote Desktop Protocol	28.3%
		T1021.004: SSH	10.3%
		T1021.002: SMB/Windows Admin Shares	10.1%
		T1021.006: Windows Remote Management	1.3%
		T1021.005: VNC	0.8%
T1570: Lateral Tool Transfer	2.3%		
T1563: Remote Service Session Hijacking	2.1%	T1563.002: RDP Hijacking	0.4%
T1550: Use Alternate Authentication Material	1.7%	T1550.001: Application Access Token	1.1%
		T1550.002: Pass the Hash	0.6%
		T1550.004: Web Session Cookie	0.2%
T1534: Internal Spearphishing	0.6%		
T1091: Replication Through Removable Media	0.6%		
T1072: Software Deployment Tools	0.2%		
T1080: Taint Shared Content	0.2%		

Maintain Presence

Persistence

T1027: Obfuscated Files or Information	46.5%	T1027.009: Embedded Payloads	9.6%
		T1027.002: Software Packing	8.6%
		T1027.010: Command Obfuscation	3.9%
		T1027.004: Compile After Delivery	1.3%
		T1027.005: Indicator Removal fromTools	0.4%
		T1027.001: Binary Padding	0.2%
		T1027.003: Steganography	0.2%
		T1027.008: Stripped Payloads	0.2%
T1070: Indicator Removal	35.1%	T1070.004: File Deletion	26.6%
		T1070.009: Clear Persistence	9.0%
		T1070.006: Timestomp	7.1%
		T1070.001: Clear Windows Event Logs	5.6%
		T1070.007: Clear Network Connection History and Configurations	3.4%
		T1070.005: Network Share Connection Removal	1.1%
		T1070.003: Clear Command History	0.6%
		T1070.002: Clear Linux or Mac System Logs	0.4%
		T1070.008: Clear Mailbox Data	0.2%
T1140: Deobfuscate/Decode Files or Information	31.5%		
T1543: Create or Modify System Process	28.3%	T1543.003: Windows Service	16.7%
		T1543.002: Systemd Service	0.9%
		T1543.004: Launch Daemon	0.4%
		T1543.001: Launch Agent	0.2%
T1112: Modify Registry	26.5%		
T1564: Hide Artifacts	19.5%	T1564.003: Hidden Window	14.8%
		T1564.001: Hidden Files and Directories	4.7%
		T1564.008: Email Hiding Rules	2.1%
		T1546.008: Accessibility Features	0.4%
		T1564.011: Ignore Process Interrupts	0.2%
T1562: Impair Defenses	18.6%	T1562.001: Disable or Modify Tools	13.3%
		T1562.004: Disable or Modify System Firewall	7.9%
		T1562.002: Disable Windows Event Logging	4.3%
		T1562.010: Downgrade Attack	0.9%
		T1562.003: Impair Command History Logging	0.9%
		T1562.009: Safe Mode Boot	0.2%
T1053: Scheduled Task/Job	18.0%		

T1218: System Binary Proxy Execution	16.1%	T1218.011: Rundll32	12.9%
		T1218.010: Regsvr32	1.7%
		T1218.005: Mshta	1.3%
		T1218.007: Msiexec	0.9%
		T1218.014: MMC	0.4%
		T1218.001: Compiled HTML File	0.2%
T1036: Masquerading	11.8%	T1036.001: Invalid Code Signature	6.8%
		T1036.008: Masquerade File Type	0.8%
		T1036.005: Match Legitimate Name or Location	0.8%
		T1036.003: Rename System Utilities	0.2%
T1547: Boot or Logon Autostart Execution	9.6%	T1547.001: Registry Run Keys / Startup Folder	7.1%
		T1547.009: Shortcut Modification	2.6%
		T1547.004: Winlogon Helper DLL	0.4%
		T1547.011: Plist Modification	0.2%
T1202: Indirect Command Execution	8.6%		
T1620: Reflective Code Loading	8.6%		
T1222: File and Directory Permissions Modification	7.9%	T1222.002: Linux and Mac File and Directory Permissions Modification	4.1%
		T1222.001: Windows File and Directory Permissions Modification	1.1%
T1546: Event Triggered Execution	3.4%	T1546.003: Windows Management Instrumentation Event Subscription	2.8%
		T1564.010: Process Argument Spoofing	0.2%
		T1546.010: AppInit DLLs	0.2%
		T1546.015: Component Object Model Hijacking	0.2%
T1556: Modify Authentication Process	1.7%	T1556.006: Multi-Factor Authentication	1.1%
		T1556.002: Password Filter DLL	0.2%
		T1556.003: Pluggable Authentication Modules	0.2%
T1037: Boot or Logon Initialization Scripts	0.9%	T1037.004: RC Scripts	0.6%
T1006: Direct Volume Access	0.8%		
T1553: Subvert Trust Controls	0.8%	T1553.002: Code Signing	0.6%
		T1553.005: Mark-of-the-Web Bypass	0.2%
T1578: Modify Cloud Compute Infrastructure	0.6%	T1578.002: Create Cloud Instance	0.6%
		T1578.005: Modify Cloud Compute Configurations	0.2%
T1207: Rogue Domain Controller	0.4%		
T1014: Rootkit	0.4%		
T1480: Execution Guardrails	0.2%		
T1601: Modify System Image	0.2%	T1601.001: Patch System Image	0.2%
T1647: Plist File Modification	0.2%		
T1127: Trusted Developer Utilities Proxy Execution	0.2%	T1127.001: MSBuild	0.2%
T1220: XSL Script Processing	0.2%		

Mission Completion

Collection

T1213: Data from Information Repositories	16.7%	T1213.002: Sharepoint	8.4%
		T1213.001: Confluence	0.4%
		T1213.003: Code Repositories	0.2%
T1560: Archive Collected Data	14.6%	T1560.001: Archive via Utility	7.5%
		T1560.002: Archive via Library	0.8%
T1056: Input Capture	8.1%	T1056.001: Keylogging	7.5%
		T1056.002: GUI Input Capture	0.6%
		T1056.003: Web Portal Capture	0.2%
T1074: Data Staged	5.4%	T1074.001: Local Data Staging	4.7%
		T1074.002: Remote Data Staging	0.4%
T1115: Clipboard Data	5.3%		
T1113: Screen Capture	4.7%		
T1125: Video Capture	3.9%		
T1114: Email Collection	2.4%	T1114.002: Remote Email Collection	0.6%
		T1114.001: Local Email Collection	0.2%
T1039: Data from Network Shared Device	1.7%		
T1005: Data from Local System	0.8%		
T1530: Data from Cloud Storage	0.6%		
T1602: Data from Configuration Repository	0.4%	T1602.002: Network Device Configuration Dump	0.4%
T1119: Automated Collection	0.2%		
T1123: Audio Capture	0.2%		
T1557: Adversary-in-the-Middle	0.2%	T1557.001: LLMNR/NBT-NS Poisoning and SMB Relay	0.2%

Exfiltration

T1567: Exfiltration Over Web service	5.6%	T1567.002: Exfiltration to Cloud Storage	2.4%
		T1567.003: Exfiltration to Text Storage Sites	0.2%
T1041: Exfiltration Over C2 Channel	3.6%		
T1020: Automated Exfiltration	1.1%		
T1052: Exfiltration Over Physical Medium	0.2%	T1052.001: Exfiltration over USB	0.2%

Impact

T1486: Data Encrypted for Impact	25.5%		
T1489: Service Stop	15.9%		
T1657: Financial Theft	7.9%		
T1529: System Shutdown/Reboot	6.9%		
T1490: Inhibit System Recovery	5.8%		
T1485: Data Destruction	2.8%		
T1496: Resource Hijacking	2.3%		
T1565: Data Manipulation	2.3%	T1565.001: Stored Data Manipulation	2.3%
T1531: Account Access Removal	1.7%		
T1491: Defacement	1.1%	T1491.002: External Defacement	0.2%
T1561: Disk Wipe	0.6%	T1561.001: Disk Content Wipe	0.4%
T1498: Network Denial of Service	0.2%	T1498.001: Direct Network Flood	0.2%
T1499: Endpoint Denial of Service	0.2%		

Articles

Chinese Espionage Operations Targeting The Visibility Gap

Endpoint detection and response (EDR) platforms have become commonplace among companies seeking to expand the visibility into endpoint activity necessary to provide a baseline of security monitoring. This increase in visibility has forced attackers to evolve in order to maintain operational efficacy. While some attackers have invested in EDR bypass techniques, others have, instead, chosen to focus on areas of the corporate environment where in-depth visibility remains uncommon. While EDR agents have become a standard part of security deployments, many specialized appliances that either segment or host assets critical to the organization often lack similar levels of visibility. These systems have become a new preferred safe haven for attackers as it enables them to maintain long-term persistence with lower risk of detection due to the gap in visibility.

Common examples of devices that rarely support EDR deployment are firewalls, email filtering products, virtualization platforms, and virtual private network (VPN) solutions. To further complicate matters, the platforms on which these appliances are built may be proprietary or otherwise locked down, such that forensic analysis efforts are hindered. Exploits for these devices are exceedingly valuable to attackers, primarily because they typically require no user interaction to succeed, which helps to minimize the chance of detection. If an attacker possesses an exploit for a zero-day vulnerability on these devices, they are often able to gain access to a target environment and remain undetected for an extended period of time. Furthermore, the attacker can use the exploit to gain access to additional targets or reestablish access to the same target if it is disrupted.

Zero-day: Vulnerabilities disclosed before patches are made available.

N-day: Vulnerabilities first exploited after patches were made available.

Mandiant observed a range of attackers targeting devices that matched this profile in 2023. Sandworm[24] continued to leverage access via compromised network edge infrastructure to enable their wartime operations in Ukraine. The financially motivated group FIN11[25] exploited a zero-day in MOVEit Transfer software to steal data as part of their data theft extortion operations. In the past year alone, Mandiant has investigated several high-profile cases of suspected Chinese espionage operations leveraging zero-day and n-day vulnerabilities to target systems where visibility has been difficult to instrument.

Custom Malware for Edge Devices

Security and networking devices that sit at the logical perimeter of a network and host services on the internet are often referred to as “edge devices.” Mandiant has observed a trend in which China-nexus attackers have gained access to edge devices via exploitation of vulnerabilities, particularly zero-days, and subsequently deployed custom malware ecosystems. These malware ecosystems have typically consisted of several distinct code families that attackers operate in unison, and are usually custom developed or tailored for the target edge device and underlying operating system. Developing malware for these managed appliances is a non-trivial task. Vendors typically do not enable direct access to the operating system or filesystem for appliance device owners or users. In order to operationalize attacks within this class of platform, attackers must maintain a resource intensive malware development lifecycle that, by necessity, maintains flexibility and a high degree of technical acumen. While this process requires a substantial investment, it also produces clear results when leveraged successfully by attackers.

Remaining Undetected

In general, custom malware may go undetected for long periods of time since there is unlikely to be specific detections in place for the malware. This is particularly true for edge devices, where network defenders may have little to no means for monitoring and detection of malware activity. Malware authors may also take special care to ensure that the malware hinders forensic investigation by circumventing or clearing logging systems in place on the device. Even after the malware has been discovered and exposed by the security community, it is often a non-trivial task for a device owner to identify if they have been impacted, since off-the-shelf security products typically will not support edge devices. Furthermore, it is sometimes the case that exploitation attempts of zero-day vulnerabilities leave little or no reliable evidence behind. This is often exacerbated by the fact that the attack may have occurred months or even years prior to detection. Additionally, there are often challenges with traditional forensic techniques as these devices are typically kept under tight control by manufacturers, adding to the already complex nature of investigating these types of compromises.

Example: BOLDMOVE

BOLDMOVE is a backdoor used by suspected Chinese espionage groups that has both Windows and Linux variants containing a core set of features. Mandiant identified a custom variant of the Linux version of BOLDMOVE, which contained an extended set of features to remain undetected on Fortinet devices. This variant of BOLDMOVE disabled the `miglogd` and `syslogd` logging daemons on the appliance, and contained a command to patch memory address space for these logging functions.These customizations of the BOLDMOVE backdoor are suspected to have enabled the attacker to remain undetected for a longer period of time than they would have otherwise been able to through traditional means.

Reduced Complexity, Increased Reliability

Edge devices such as email security gateway appliances and VPNs are typically high-availability devices that run for months or years at a time without being rebooted. As such, many of these devices are put through rigorous testing regimes by the manufacturer during development to ensure their stability. China-nexus malware developers take advantage of the built-in functionality included in these systems, which benefits them in several ways. In general, leveraging native capabilities will enable attackers to reduce the overall complexity of the malware by instead weaponizing existing features within that have been rigorously tested by the organization. For example, for devices that use proprietary software components such as custom file formats or configuration files, attackers may be able to leverage built-in functions to parse or process these files rather than developing their own implementation. This concept is analogous to living-off-the-land, and is particularly effective on edge devices since these native device operations are likely not being monitored by network defenders and, as such, may go unnoticed.

> **Living off the land:** Attacker use of legitimate, pre-installed tools and software within a target environment, notably to evade detection.

Example: THINCRUST

During an UNC3886 compromise, Mandiant discovered a backdoor deployed to FortiAnalyzer and FortiManager devices named THINCRUST, which disguised its command and control (C2) communications as legitimate API calls to the devices. UNC3886, a suspected Chinese espionage group, appended the Python-based backdoor code into legitimate web framework files that were responsible for providing the API interface for the appliance. This gave UNC3886 the ability to harness the native API implementation to access and send commands to THINCRUST by simply interacting with a new endpoint URL, which they had added. By leveraging existing capabilities built into the appliance, UNC3886 was able to simplify their malware while maintaining the reliability necessary for continued operations.

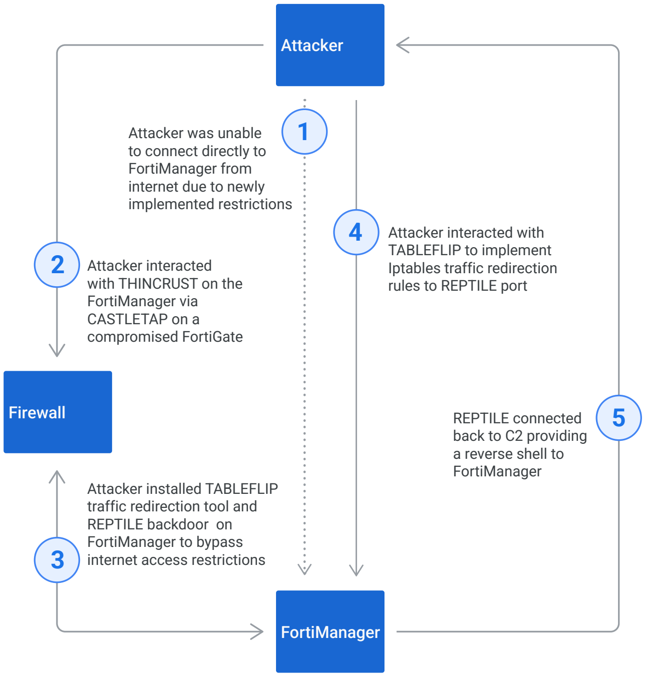
Tailored Capabilities and Smaller Footprint

Custom malware for edge devices may only include the capabilities required to achieve the attacker's mission objectives. Malware used to exploit vulnerabilities may never be used again once the vulnerabilities are discovered and patched, as the cost to maintain and repurpose the code often outweighs the benefits. By developing relatively simple malware that serves only to provide the attackers with the desired functionality on the target device, attackers are able to achieve their goals while minimizing their overall footprint. In the same vein, the requirement for complex obfuscation is likely lessened since the primary objective of the attacker is to remain undetected entirely, rather than hinder the analysis of the malware once it has been discovered. By the time the malware is discovered, the vulnerability and campaign would have already been exposed, and the attacker's operations typically come to a close.

Example: TABLEFLIP

After losing access to a FortiManager device during one incident due to access control lists change, UNC3886 adapted to the situation by deploying a network traffic redirection utility named TABLEFLIP. TABLEFLIP passively listens on all active interfaces for specialized command packets that contain an XOR encoded IP address and port to redirect traffic to using iptables commands. UNC3886 deployed TABLEFLIP alongside the publicly available REPTILE rootkit to act as a reverse shell, and successfully gained access back to the FortiManager device. The ability to produce purpose-built malware in response to changes in an ongoing operation places defenders at a disadvantage when facing capable and agile attackers with nation-state backing.

Activity after internet access restrictions implemented to FortiManager


Attacker
1
Attacker was unable to connect directly to FortiManager from internet due to newly implemented restrictions
2
Attacker interacted with THINCRUST on the FortiManager via CASTLETAP on a compromised FortiGate
Firewall
3
Attacker installed TABLEFLIP traffic redirection tool and REPTILE backdoor on FortiManager to bypass internet access restrictions
4
Attacker interacted with TABLEFLIP to implement Iptables traffic redirection rules to REPTILE port
5
REPTILE connected back to C2 providing a reverse shell to FortiManager
FortiManager

Attribution Challenges

Custom malware developed for edge devices may stifle attribution for cyber threat intelligence analysts. These malware families, and potentially the entire ecosystem, could be almost entirely unique when compared to existing malware because of the target operating system and tailored capabilities. As such, they may not contain code or other overlaps analysts traditionally find between related malware families that contribute to the technical attribution analysis.

Example: SEASPRAY and WHIRLPOOL

SEASPRAY is a launcher written in Lua that UNC4841 injected into legitimate Barracuda Email Security Gateway (ESG) modules. SEASPRAY registers an event handler for incoming emails, and launches an external binary, which Mandiant tracks as WHIRLPOOL, when certain markers are present. WHIRLPOOL is a simple TLS reverse shell utility that receives a C2 IP address and port to connect to from SEASPRAY at runtime. Because SEASPRAY was a relatively simple implementation that consisted of a few lines of code that were specific to the Barracuda ESG appliances, it did not offer much value in terms of attribution. Similarly, WHIRLPOOL was a simple and generic TLS reverse shell that did not contain any embedded C2 server information that could be analyzed. Usage of such malware on edge devices presented significant challenges for analysts performing attribution analysis.

In-Depth Knowledge of Edge Devices

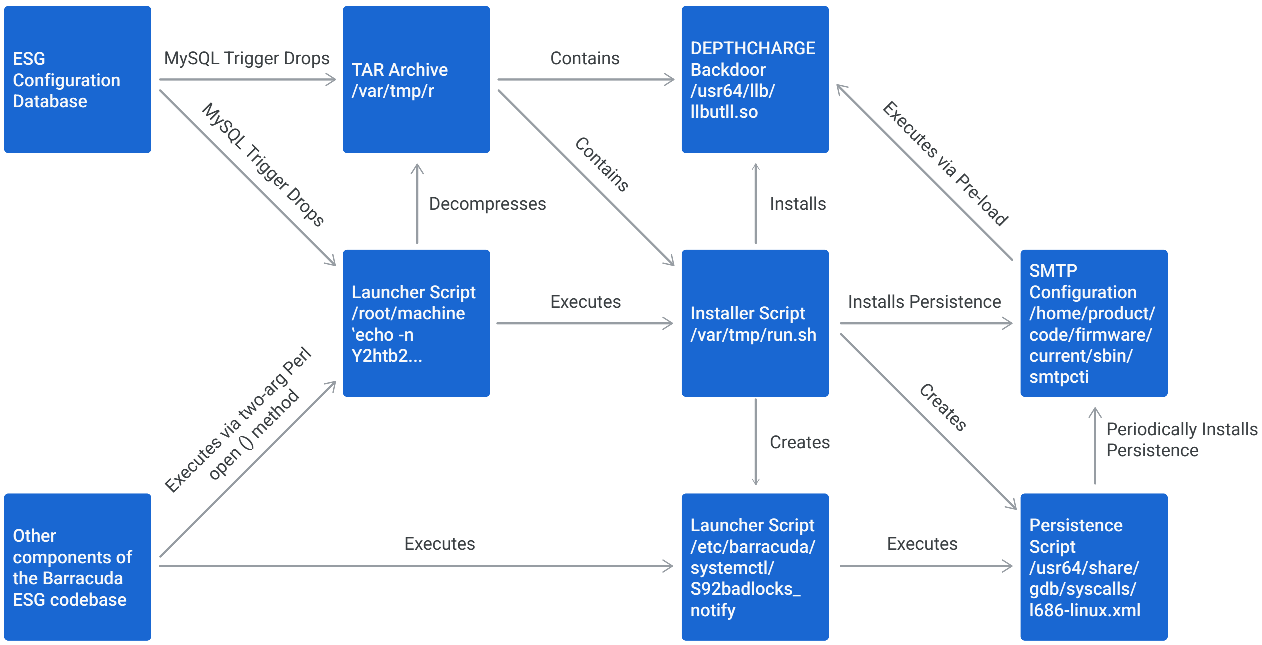
Mandiant has observed several instances where China-nexus attackers demonstrated a high level of in-depth knowledge when targeting edge devices. The degree of knowledge spanned not only the malware used during the attack, but also the zero-day vulnerabilities used to gain access to these devices.

Example: DEPTHCHARGE

DEPTHCHARGE is a passive backdoor that Mandiant observed UNC4841 begin to deploy about one week after Barracuda's initial public notification of the ESG zero-day campaign. This was followed by more rapid deployment to what Mandiant assessed were high-value targets, once Barracuda announced plans to replace affected devices. The timing of the accelerated deployment suggests that UNC4841 may have anticipated this, and was prepared for remediation efforts with tooling and tactics, techniques and procedures (TTPs) designed to enable them to continue operations in the face of attempts to disrupt their access to target networks.

Several aspects of DEPTHCHARGE and its execution chain demonstrated an intimate knowledge of the Barracuda ESG device and its software components. Most notable was that the attacker had identified a method for malware persistence inside the configuration database for the appliance, which would result in it being present in exported backup configurations. This meant that device owners looking to set up a clean device would unknowingly export backup configurations containing DEPTHCHARGE persistence, and in-turn infect their clean appliances when attempting to restore their configuration.

Perhaps an even more intricate display of UNC4841's knowledge of the inner workings of the appliance was the method through which DEPTHCHARGE achieved command execution from a trigger inside the MySQL configuration database after it had been imported. UNC4841 understood that completely separate components of the ESG's codebase accessed files using the two-argument form of Perl's open() function, and that they could craft a special filename that would result in commands being executed on the appliance. By having the MySQL trigger drop a file that induces this command execution, UNC4841 was able to chain these techniques together to have DEPTHCHARGE dropped and executed upon import of a backup configuration on a new appliance. This effectively enabled UNC4841 to survive through a complete device replacement in the small number of cases where this occurred.

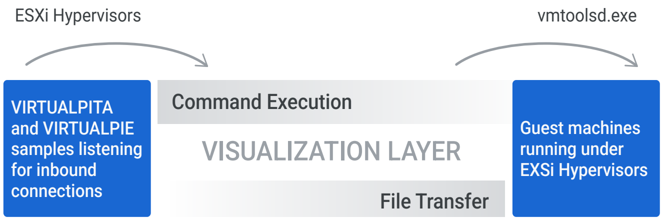

ESG Configuration Database
MySQL Trigger Drops
TAR Archive /var/tmp/r
MySQL Trigger Drops
Contains
DEPTHCHARGE Backdoor /usr64/llb/llbutll.so
Contains
Executes via Pre-load
Decompresses
Installs
Launcher Script /root/machine 'echo -n Y2htb2...
Executes
Installer Script /var/tmp/run.sh
Installs Persistence
SMTP Configuration /home/product/code/firmware/current/sbin/smtpcti
Executes via two-arg Perl open () method
Creates
Creates
Periodically Installs Persistence
Other components of the Barracuda ESG codebase
Executes
Launcher Script /etc/barracuda/systemctl/S92badlocks_notify
Executes
Persistence Script /usr64/share/gdb/syscalls/l686-linux.xml

Custom Malware for Hypervisors

As cloud computing has grown in popularity over the years, hypervisors have subsequently become commonplace within modern infrastructures. However, while instrumenting endpoint visibility on the guest virtual machines is relatively easy, instrumenting visibility on the hypervisor itself can present substantial challenges. As with network edge devices, Type 1 hypervisors commonly run on operating systems versions that are rarely supported by EDR vendors. Not surprisingly, given the low visibility yet excessively high target value of a hypervisor, Mandiant has observed China-nexus attackers targeting hypervisors as well.

Hypervisor technologies, such as VMware's ESXi, use Virtual Machine Communication Interface (VMCI) sockets to facilitate communication between the bare-metal host and the guest operating systems. Mandiant has observed attackers leverage VMCI sockets for lateral movement and continued persistence within targeted environments. UNC3886 utilized backdoors such as VIRTUALPITA, and took advantage of VMCI-based channels to communicate from the ESXi host to the guest virtual machines (VM). Since the traffic over the virtualized layer is localized to the bare metal machine, there are no security mechanisms restricting any guest VM or ESXi host from initiating a connection with the other, essentially bypassing any network segmentation. Additionally, traffic cannot be monitored outside of the guest VMs and ESXi hosts present in the virtualized environment. While the client/server communication socket has connection-oriented and connectionless variants very similar to TCP and UDP, it is invisible to commonly used networking tools such as tcpdump, netstat, nmap, and Wireshark without custom configurations, as it belongs to a different socket address family.

UNC3886 used a novel persistence technique to deploy the VIRTUALPITA backdoor using vSphere Installation Bundles ("VIBs"). Mandiant had not previously observed this technique for deploying malware or persistence, which suggests UNC3886 spent significant resources to understand the inner workings of VMware technologies, especially the VMCI sockets for circumventing security restrictions. Furthermore, VIRTUALPITA was used to pass arbitrary commands to guest VMs without being logged on the host. These commands then get executed on the guest VM with the vmtoolsd.exe process where they are then observed in the Windows event logs. VIRTUALPITA also sets the HISTFILE to 0, which would remove any terminal history on the host system, leaving behind little forensics evidence.


ESXi Hypervisors
vmtoolsd.exe
VIRTUALPITA and VIRTUALPIE samples listening for inbound connections
Command Execution
VISUALIZATION LAYER
File Transfer
Guest machines running under EXSi Hypervisors

Recommendations

The most critical strategy for protecting against such attacks is maintaining proper patch management to mitigate the risk of exploitation of known vulnerabilities. Applying the most recent patch is the best way to limit any unexpected tampering or modification of the appliance. For zero-day vulnerabilities, where exploitation is unlikely to be detected, a defense-in-depth approach provides the best chances of surfacing evidence of the malicious activity further in the attack lifecycle.

If an organization has identified that they were operating vulnerable devices and may have been compromised, Mandiant recommends performing an investigation and hunting activities within their networks. An investigation may include, but is not limited to, the following:

- Scanning potentially impacted devices with publicly available tools such as IOC scanners to identify evidence of compromise.
- Sweeping the entire environment for known IOCs.
- Reviewing network logs for signs of data theft and lateral movement.
- Reviewing network logs for abnormal logins or internal traffic from edge devices.
- Capturing a forensic image of the impacted appliance and conducting a forensic analysis.
- Applying any malware signatures (e.g. YARA rules) to appliance images to assist forensic investigators.

Organizations should also consider implementation of security controls detailed in architecture hardening guidance provided by security vendors. Mandiant has previously provided such documentation for the Barracuda ESG event.[26]

Outlook

Despite the amount of resourcing required, Chinese espionage groups are almost certainly going to continue investing in the acquisition of zero-day exploits and platform-specific tooling. Mandiant expects that we will continue to see targeting of edge devices and platforms that traditionally lack EDR and other security solutions due to the challenges associated with discovery and investigation of compromise. Exploitation of these devices will continue to be an attractive initial access vector for Chinese espionage groups to remain undetected and maintain persistence into target environments.

It is also likely that we will continue to see the deployment of custom malware ecosystems by Chinese espionage groups that are tailored for the device and operation at hand. This approach provides several advantages such as the increased ability to remain undetected, reduced complexity and increased reliability, and a reduced malware footprint. Additionally, it presents challenges to technical attribution being performed by threat intelligence analysts.

Organizations must remain vigilant and ensure that they’re not only monitoring their networks at the operating system layer, but also continue to patch, maintain and, where possible, monitor the appliances that are running the underlying infrastructure of their networks.

Attacker Operations Involving Zero-Days Vary Depending on Motivation

In the ever-evolving landscape of cybersecurity, zero-day exploits remain a potent weapon in the hands of attackers. These vulnerabilities, unknown to software vendors, can provide attackers with a stealthy means to gain unauthorized access to systems and sensitive data.

In 2023, we tracked a combined total of 97 unique zero-day vulnerabilities exploited in-the-wild, surpassing the volume tracked in 2022 by nearly 56%. People's Republic of China (PRC) cyber espionage groups were the most prolific attackers to exploit zero-days in 2023, and demonstrated a focus on stealth in their zero-day exploitation campaigns. The state-sponsored groups tracked by Mandiant primarily utilize zero-days for intelligence gathering and strategic advantage.

Zero-day: Vulnerabilities disclosed before patches are made available.

Another consistent component of cyber espionage exploitation has been the rise of commercial commercial surveillance vendors selling what are often turnkey or off-the-shelf capabilities. In many instances, these vendors offer not just the technical expertise to build an exploit chain, but also the subsequent tools necessary to identify and exfiltrate data from the targeted victim. The growth of these capabilities suggests internal expertise is no longer required to exploit zero-day vulnerabilities. This expands the access to zero-day exploits for attackers, even if they lack the technical sophistication to conduct zero-day research.

At the same time, financially motivated attackers have continued to embrace zero-days, aiming to infiltrate systems and steal valuable data for financial gain. During 2023, financially motivated attackers and espionage groups appear to represent roughly the same proportion of total zero-days exploited as they had in the previous two years. FIN11, a financially motivated group active since at least 2016, exploited two zero-days in 2023 in widespread campaigns. FIN11's investment in developing zero-days demonstrates their continued sophistication. Zero-day vulnerability research is a time and resource intensive process, and FIN11's exploitation of multiple zero-day vulnerabilities indicates the group has consistent access to both. Notably, FIN11 has frequently targeted file transfer applications, which can provide quick and efficient access to large amounts of sensitive data without the need for lateral movement within a victim network.

The diverse motivations of attackers translate into distinct approaches to the utilization of zero-day exploits. Espionage groups prioritizing stealth and long-term access may employ zero-days sparingly, and meticulously craft exploits to minimize detection. Financially motivated attackers, on the other hand, often prioritize speed and efficiency, potentially sacrificing stealth for quicker returns and wider exploitation.

Two case studies, derived from frontline Mandiant engagements, exemplify the varying behavior of attackers when driven by distinct objectives. The financially motivated campaign that exploited Progress Software's MOVEit Transfer demonstrates the adaptability and speed of financially motivated attackers. In contrast, the espionage-driven campaign that targeted the Barracuda Email Security Gateway (ESG) highlights the persistence and sophistication of state-sponsored groups. These case studies exemplify the varied tactics, techniques, and procedures (TTPs) of two groups that have distinctly different objectives, but prosecute those objectives with similar ingenuity and adaptability.

Cybercrime Campaign Case Study: MOVEit

In May 2023, Mandiant observed the exploitation of CVE-2023-34362,[27] a zero-day vulnerability in Progress's managed file transfer solution MOVEit Transfer. This vulnerability, affecting all MOVEit Transfer versions prior to May 31, 2023, allowed attackers to gain unauthorized access to MOVEit Transfer's database, potentially leading to data breaches and financial losses. To exploit CVE-2023-34362, the attacker had to send a specially crafted request to a vulnerable server, which injected malicious SQL statements into application queries on the vulnerable systems. After gaining access to a vulnerable application's database, the attacker could perform additional actions to gain elevated privileges and execute arbitrary code, including accessing, modifying or deleting data within the database. Mandiant investigated 31 attacks related to this vulnerability, providing valuable insights into the TTPs employed by FIN11, to which we've attributed all exploitation. Mandiant's analysis revealed a pattern of automated attacks, during which FIN11 appeared to focus on speed and efficiency of exploitation. FIN11's approach to campaigns has evolved to become more sophisticated, and pose greater risks to targeted organizations.

FIN11's Attack Campaign

FIN11 emerged as the key player exploiting the MOVEit Transfer zero-day. Mandiant's investigations revealed that FIN11 began testing the vulnerability as early as April 2022. However, public reporting indicates testing might have begun even earlier. Testing likely continued until a reliable exploit and means for data exfiltration was developed.

Beginning in May 2023, FIN11's attack methodology primarily involved the deployment of web-based backdoors, data enumeration, and data theft. Upon gaining initial access, FIN11 deployed a web-based backdoor, which Mandiant tracks as LEMURLOOT, on compromised systems. These backdoors masqueraded as legitimate software components, and provided functionality for the enumeration and theft of data. FIN11 executed commands through LEMURLOOT to enumerate files and folders, retrieve configuration information, and create or delete a user with a hard-coded name.

Impact and Remediation

Nearly 2,600 organizations across various sectors and industries were targeted by FIN11 during this campaign. The scale of the attacks further indicates that FIN11 relied on automated methods, as it would be impractical for them to engage in hands-on-keyboard intrusions on such a broad scale. Based on data posted on the FIN11 data leak site , FIN11 stole terabytes of potentially sensitive data during their campaign.

Mandiant did not identify evidence of lateral movement during any of the investigations related to FIN11's use of the MOVEit Transfer vulnerability. It is likely that FIN11's primary objective was the immediate theft of data rather than establishing long-term persistence or compromising additional systems within the target networks. Access to file transfer appliances likely provided FIN11 with sufficient access to sensitive data they could use to extort victims without needing to move laterally in the network.

Remediation efforts surrounding FIN11's targeting of MOVEit Transfer appliances involved applying a sequence of patches released by Progress Software. Organizations were urged to prioritize patching and to implement robust cybersecurity measures to safeguard against similar attacks.

Espionage Campaign Case Study: Barracuda

PRC cyber espionage groups conducted multiple high-profile zero-day exploitation campaigns in 2023. One of the most notable, and likely the most widespread, was a campaign targeting Barracuda ESG appliances.[28] UNC4841, a cluster of Chinese cyber espionage activity, targeted Barracuda ESGs through a remote command injection vulnerability (CVE-2023-2868), which was publicly disclosed in May 2023. However, Mandiant investigations identified evidence of exploitation dating back to at least October 2022. UNC4841 exploited ESG appliances by taking advantage of a flaw in the parsing logic for processing of TAR files. By formatting TAR files in a particular way, UNC4841 was able to trigger a remote command injection attack that enabled them to execute system commands. UNC4841 carefully crafted their attack strategy, employing emails cleverly designed to appear as low quality spam, and including malicious TAR archive attachments. The filenames included in the TAR archive email attachments contained malicious commands, which were leveraged to establish a foothold on vulnerable appliances. After gaining access, UNC4841 deployed a wide range of second-stage backdoors specifically tailored to Barracuda ESGs to establish long-term access, enabling them to conduct their espionage activities undetected for more than eight months.

Stealing Sensitive Data with Precision

With long-term access firmly established, UNC4841 focused on quietly stealing sensitive data from targeted organizations. Their tactics centered on harvesting email from the ESG's temporary mail storage component, which enabled them to conduct broad email collection on compromised appliances. UNC4841 also targeted email collection through shell scripts, which targeted specific email domains and users deemed to be of strategic importance to China. Additionally, Mandiant observed UNC4841 targeting email being sent to Barracuda appliances for collection as they may originate from sources of particular intelligence value. The staging file naming conventions utilized by UNC4841 throughout the campaign were indicative of a large-scale espionage operation. UNC4841 primarily staged data in the /mail/tmp/ directory and utilized a consistent file naming convention containing three letters corresponding to the victim organization followed by a number.

Targeting Trends

UNC4841's targeting patterns evolved over the campaign, which lasted longer than eight months. While initially focusing on government organizations, as the campaign progressed, UNC4841 expanded their reach to include organizations in the information technology sector, as well as a wide range of others. After the public notification of the vulnerability, UNC4841 prioritized government agencies and high-tech organizations for deployment of specific malware families. UNC4841 deployed a series of backdoors across organizations in the post notification period in order to maintain access and continue operation.

Mitigating the Threat

On May 31, 2023, Barracuda strongly advised organizations to replace all compromised ESGs immediately regardless of patch level. This incident underscores the importance of proactive cybersecurity measures, including prompt vulnerability patching, regular security audits, and continuous monitoring of networks for attempted lateral movement or suspicious activity stemming from edge appliances. While defenders cannot anticipate a zero-day, these measures can help expose other security flaws that could allow an attacker to more easily move throughout a network or escalate privileges. Limiting the damage and breadth of an attack from undisclosed vulnerabilities helps limit the risks organizations face as attackers evolve.

A Comparative Analysis: Lessons Learned and the Evolving Threat Landscape

The campaigns targeting MOVEit Transfer and Barracuda ESG vulnerabilities highlight the evolving threat landscape, and the stark differences between how financially motivated and espionage-driven attackers operationalize the use of zero-day exploits. FIN11 prioritized a fast and efficient approach to its exploitation of MOVEit, targeting a large number of organizations for brief but efficient access to sensitive data.

Feature	Financially Motivated	Espionage
Quantity vs Quality of Victims	Vastly more victims (reportedly over 2,600)	Relatively few victims (~5% of vulnerable appliances)
Approach to Weaponization of CVE	Quick monetization	Sustained intelligence gathering
Impact	Loss of PII, potential exposure of trade secrets, impact on personal privacy and business operations	Implications to national security, targeted attacks on government organizations
Response/Containment	Requires minimizing data exfiltration and preventing ransomware deployment	Requires thorough understanding of the compromise, attacker tactics, and malware detection

Meanwhile, UNC4841 exhibited a more meticulous and targeted approach during its Barracuda ESG exploitation, seeking long-term, surreptitious access to sensitive data for intelligence purposes.

The means through which various attackers have historically acquired and leveraged zero-day exploits should inform the decision-making and prioritization for organizations that may become future targets. While there is no reliable way to defend against zero-day exploits, organizations can mitigate risk by working to protect and segregate critical systems, while also ensuring they have the visibility needed for continued monitoring of suspicious activity.

Organizations traditionally prioritize patching by risk scores, with a higher risk score often getting patched prior to those with lower risk scores. However, evidence of active exploitation of a vulnerability should escalate patching priority,[29] and affected organizations should launch an immediate investigation into impact.

Organizations that have an existing incident response plan and broad environmental monitoring are often better prepared to assess the potential impact of a vulnerability on their environment. Layering network segmentation and logging with advanced endpoint detection and response solutions provides organizations with an efficient means through which investigations can be started and brought to a swift close.

Similarly, thoroughly evaluating the security practices and network requirements for vendors prior to deploying hardware or software into the environment allows defenders to build a quality baseline of what should be considered “normal” use. Vendor vetting also allows for the creation of comprehensive detection mechanisms as the definition of non-standard use is clarified. Any detections for non-standard use within the context of a vendor’s product should be prioritized and investigated to ensure the legitimacy of the actions on which the detection fired. A blending of policy, threat intelligence, and active monitoring can act as an early warning system for attackers leveraging zero-day vulnerabilities.

Conclusion

Zero-day exploitation is no longer a niche capability accessible to only a handful of attackers, and Mandiant anticipates that the growth we have seen across the last few years will continue. The rise of zero-day exploitation by ransomware and data theft extortion groups, continued state-sponsored exploitation, and the growth of turnkey or off-the-shelf capabilities that can be purchased from commercial commercial surveillance vendors will continue to drive the identification of zero-day vulnerabilities and exploits that target them. By understanding the motivations and TTPs of attackers, organizations can build defensive strategies that prioritize the types of threats that are most likely to impact their environments. Strengthening cybersecurity posture, adopting robust vulnerability management practices, and fostering a culture of security awareness are key steps in safeguarding against zero-days. The MOVEit and Barracuda campaigns offer a stark reminder that cyber threats are not merely a nuisance, but a threat that demands our attention and action. Defenders must adopt a proactive approach to cybersecurity, recognizing that zero-day vulnerabilities are a reality and that preparation reduces their impact.

Evolution of Phishing Amid Shifting Security Controls

In 2022, Microsoft moved to block by default the execution of macros in Office documents. This change effectively impeded attackers' ability to leverage this technique for code execution following initial access. Since then, Mandiant has observed attackers moving to adopt new methods of initial access involving expanded payload selection, and highly effective social engineering tactics. To circumvent security controls, attackers have begun to experiment with a variety of payload types, including LNK files and weaponized Microsoft Office documents. Attackers also sought to move out of the traditional bounds of targeting, and began to engage on platforms beyond email such as social media, SMS messaging, and other common communications platforms. Mandiant also observed attackers exploit trusted relationships and communications through techniques such as conversation hijacking, and by simply masquerading as internal users. These contemporary phishing techniques challenge traditional security paradigms that have focused on user education, email gateway filtering, and multi-factor authentication (MFA). When targeting users in 2023, attackers leveraged multiple types of phishing payloads and techniques that fell outside of historical norms. Mandiant observed attackers leveraging code obfuscation, remote payload hosting, placing dropper scripts within archive files, and bypassing email filtering controls.

Malware Delivery: Old, Borrowed, and New Techniques

When targeting users in 2023, attackers leveraged multiple types of phishing payloads and techniques that fell outside of historical norms. Mandiant observed attackers leveraging code obfuscation, remote payload hosting, placing dropper scripts within archive files, and bypassing email filtering controls.

Compressed Archive Files

Compressed archives such as the ZIP and RAR file formats can be used as a container for malicious dropper files, and provide password-based encryption capabilities that can circumvent automated detection. Email security and firewall technologies can decompress specific archive file formats to perform content inspection and policy enforcement during file transfer. However, sandbox analysis of unencrypted archives may not occur rapidly enough to prevent the delivery of a malicious file to an end user. Similarly, archive files that are encrypted using password protection, in effect, bypass automated file scanning. Following Microsoft's move to disable macros by default in 2022, Mandiant observed multiple threat groups shift towards the inclusion of compressed archives as a means to bypass initial detection.

UNC2500 moved away from macro-enabled Office documents to other file types, including OneNote and LNK files, contained within password-protected ZIP archives. These files were commonly delivered as attachments to emails or downloaded from OneDrive links, Google Drive URLs, and compromised websites. UNC2500 phishing distribution campaigns have led to the deployment of multiple backdoor types following initial compromise, and have provided access for multiple attackers as a precursor to ransomware operations. Beginning in September 2023, the LNK files weaponized by UNC2500 contained commands that leveraged the built-in cURL utility to download and execute a Visual Basic script hosted at a malicious URL leading to the deployment of various backdoors.

Another threat group, UNC4814, sent spear-phishing emails to government and critical infrastructure targets in Ukraine between April and May 2023. These emails included attachments that contained an obfuscated JavaScript downloader. UNC4814 targeted organizations with a lure referencing a convention hosted by the PAX organization based in the Netherlands. Launching the obfuscated JavaScript downloader resulted in the execution of a PowerShell command, which installed a downloader.

Microsoft Office Documents

When Microsoft announced their intent to block VBA Macros, Mandiant observed malware distribution methods shift to new delivery mechanisms within the ecosystem of Microsoft applications. Beginning in late January 2023, UNC2633 leveraged malicious OneNote files to distribute QAKBOT malware. These OneNote files would drop and execute a Windows Script File to run additional malicious commands. In February, Mandiant also observed FIN6 use CV-themed OneNote lures to distribute a payload consisting of a downloader embedded in LNK files.

Despite Microsoft blocking office macros by default, Mandiant continued to observe attackers leverage Office documents to target users in 2023. Continued use of malicious macros may reflect that some organizations maintain policies that keep macros enabled due to reliance on macros for legitimate business purposes. Since at least February 2023, the Russia-nexus attacker Turla, tracked by Mandiant as UNC638, has likely targeted Ukrainian military personnel using spear-phishing emails containing Excel documents. The spreadsheets attached to the emails contained embedded macros to install a .net backdoor on targeted machines. In April 2023, UNC1151 targeted Ukrainian government entities with a RAR archive containing an Excel spreadsheet with a malicious macro that dropped an embedded .net downloader payload.

Hyperlinks in Email Body and Attachments

Mandiant has observed attackers leverage a notable technique in their attempts to bypass email security solutions. Instead of including a malicious attachment, which may be defeated by scanning, attackers have started to include hyperlinks to second-stage payloads. In some cases the hyperlinks are included in innocuous attachments, whereas, in others, the links are included in the message bodies. Email security solutions vary in how far they will follow hyperlinks and the depth of the scanning performed.

Beginning in February 2023, Mandiant observed APT29 conduct multiple phishing campaigns against diplomatic entities using hyperlinks to host second-stage payloads. In one particular phishing campaign, APT29 attached a PDF masquerading as a wine-tasting event invite, which contained a malicious embedded URL. In a separate instance targeting diplomatic entities, APT29 embedded the URL directly in the email body. Once a targeted user clicked on a URL within the phishing email or PDF, an HTML dropper attachment, which Mandiant tracks as ROOTSAW, would be downloaded to disk. ROOTSAW leverages HTML smuggling in order to launch JavaScript to decode and further execute embedded malware within the attachment. Beginning in October 2023, Mandiant observed FIN6 also leveraging this technique through social media phishing messages containing a resume or job-themed PDF. Once a targeted user opened the PDF, the user was presented with a fake error message, which included a URL to an attacker-controlled domain.

Social Engineering: Leveraging Alternative Platforms

As new technologies are created and deployed to defend against email-based phishing, attackers have undertaken a natural process of identifying, trialing, and ultimately leveraging new platforms to deliver lures to targets. Attackers have employed a variety of methods to move user interaction and exploitation away from email and perimeter network monitoring, where detections are most heavily focused. Notably, they focused on areas where visibility is considerably less common, including infiltrating target environment communication and messaging platforms, connecting over social media, and phishing mobile devices.

Communication and Messaging Platforms

Mandiant observed multiple attackers attempting to send phishing messages to Microsoft Teams users by leveraging compromised internal accounts and external accounts. In April 2023, UNC3944 used compromised internal O365 accounts to target other internal users over Microsoft Teams. The attackers pretended to be members of the organization’s Human Resources department in order to persuade targeted users to access a spoofed O365 login page hosted on a domain that included the name of the organization. The attacker provided guidance to the users on how to access the login form, and provide their MFA code. Once the attacker was authenticated as the compromised users, they registered new MFA methods or updated the user’s phone number used to receive MFA SMS codes.

In September 2023, UNC5051 used an external O365 tenant account to target users with a Microsoft Teams chat request that contained a malicious URL. Once accessed, the user was prompted to download a ZIP archive stored on an attacker-controlled SharePoint site. The ZIP archive contained a LNK dropper masquerading as a PDF file that, when executed, launched a Visual Basic script downloader that used the built-in Windows cURL utility to download and execute a pre-compiled AutoIT script leading to installation of the DARKGATE backdoor. Mandiant has identified multiple threat clusters incorporating the DARKGATE backdoor into their operations, including those that have provided initial access for ransomware intrusions.

Social Media

Social media platforms provide attackers with additional data collection and phishing opportunities against users of target organizations. LinkedIn is a particularly popular choice for attackers, which they use to target employees of specific companies. Due to LinkedIn’s status as a business-oriented platform and the visibility it provides into employee names, job titles, and responsibilities, attackers were able to build more plausible lures for phishing campaigns.

In 2023, Mandiant identified multiple attackers adopting fake LinkedIn personas and engaging with users of target organizations over private messages. Beginning in May 2023, UNC2970 used the LinkedIn platform to conduct spear-phishing operations using varied payload types, including container files, to compromise employees of target organizations. Post-compromise activity included the execution of backdoors, and the targeted theft of information in support of suspected espionage operations. In late June 2023, UNC4962 targeted users through LinkedIn private messaging using themes related to corporate development projects and job roles. Message recipients were directed to download a ZIP archive, hosted on cloud storage services, that contained a Visual Basic script payload. That payload executed a Windows Installer (MSI) package, and resulted in the execution of the DARKGATE backdoor. In October 2023, FIN6 also used the LinkedIn platform to send a URL to HR recruiters of a target organization, which prompted them to download a PDF file hosted on a fake resume site. FIN6 restricted access to the URL using filtering requirements, including specific User-Agent strings and geofencing. Users who met the criteria were served a ZIP archive containing a malicious LNK file, which, in turn, led to the instantiation of both a downloader and a backdoor.

> **Geofencing:** Virtual boundaries around specific geographic locations that attackers will use to only target individuals in certain regions.

QR Code Phishing (“Quishing”)

Quick Response codes (QR codes) are a type of barcode containing encoded data, such as URLs, that can be scanned with mobile devices. Web browser usage on mobile devices is not commonly collected or monitored, which makes it difficult to determine when users interact with a phishing website. By encoding a malicious URL in a QR code image and embedding it within a phishing email, attackers can circumvent email security scanning that relies on detecting hyperlinks within the email message body. Users may also find it challenging to confirm the authenticity of a URL or web page when viewing it through a mobile device browser compared to a desktop browser client. In 2023, attackers included QR codes in phishing emails by embedding them within an attached PDF or image file, and prompting the email recipient to scan the barcode to retrieve information such as an invoice or a document.

Since September 2023, Mandiant has observed UNC5103 leveraging QR codes to direct phishing email recipients to websites masquerading as the State Taxation Administration (STA) of the People’s Republic of China. The attacker attached a Microsoft Word document to the phishing email that, when opened, would display a malicious QR code with instructions to begin a tax refund application. Users who visited the spoofed STA website from a mobile device were prompted to provide personal information, including name, personal identification number, and bank account information.

Between September and October 2023, UNC5092 used compromised third-party email accounts to send phishing emails with an image file containing a QR code. The QR code contained an encoded URL that directed the user’s mobile device browser to a spoofed Microsoft login page for credential theft. Mandiant subsequently observed UNC5092 conducting session token theft via adversary-in-the-middle attacks to obtain additional authentication information. UNC5092 leveraged the obtained cloud access to conduct a wide variety of activities, including registering external devices to enable MFA, accessing corporate email accounts to scrutinize data, creating new email inbox rules, acquiring files from SharePoint, and sending fraudulent fund transfer phishing emails to internal users.

SMS Phishing (“Smishing”)

attackers can target users through SMS phishing (smishing), which is a technique that takes advantage of the internet-connected nature of mobile devices to load web content such as spoofed login pages for credential theft. In 2023, Mandiant responded to multiple incidents involving SMS phishing.

In one October 2023 instance, a attacker, masquerading as Helpdesk members of a third-party financial institution, sent SMS messages that directed recipients to a spoofed web page from their corporate systems. Users who accessed the malicious web page were prompted to install AnyDesk remote access software on their corporate systems. Once the attacker gained remote access to targeted systems, they navigated to multiple web pages related to the users’ third-party financial institution account with the intent of registering new mobile application access, and stealing money through funds transfers.

Mandiant has also observed UNC3944 use SMS phishing campaigns against employees of targeted organizations to obtain credentials in order to gain and escalate access to the environments. Starting in mid-2023, Mandiant identified UNC3944 leveraging a new phishing kit that delivers phishing pages designed to appear as if they belong to the targeted organization, and using registered domains that include the targeted organization name in combination with “-sso” or “servicenow” in the domain. Follow-on access by UNC3944 has typically involved targeting of cloud resources to establish a foothold for data theft and monetization, but in 2023 this attacker shifted tactics to include data extortion and ransomware.

Detection and Mitigation

When user credentials are successfully compromised through alternative platform phishing such as involving SMS or QR codes, the initial discovery of compromise can often involve cloud security alerts for risky sign-in events, mailbox rule creation, suspicious MFA device registration, or internal and external users reporting suspicious emails originating from a compromised user account within the organization. Detection strategies may include generating alerts for the aforementioned activity. Platform logs may also record messages or URLs transmitted between users that could be proactively analyzed for suspicious content. For example, the Microsoft 365 audit log can record URLs sent over Microsoft Teams under the MessageURLs field within the MessageCreatedHasLink Operation. Common mitigation approaches to reduce the threat of alternative platform phishing include specifying which Microsoft 365 organizations are trusted and allowed to chat with internal users over Microsoft Teams, deploying phishing-resistant MFA methods, and other recommendations detailed within Microsoft security guides.[30]

Detection Opportunity	Detection Name	Pseudocode	Description	MITRE

File downloads—Web Proxy	File Download—Executable	Logsource = Web Proxy
		Eventtype = file download
		Filetype = [exe, lnk, vb, …]
			Alert when anomalous, executable file extensions are observed being downloaded.	T1566.002

File downloads—Web Proxy	File Download—Container contains Executable	Logsource = Web Proxy
		Eventtype = file download
		Filetype = [zip, rar…]
		Archive_Contents = [exe, vb, com, bat, js, …]
			Even when password protected, many archives still expose a directory of their contents. Some tools may include archive contents in their log event metadata. Alert when an archive contains executable files.	T1566.002

File downloads—Web Proxy	File Download from External Cloud Storage	Logsource = Web Proxy
		Eventtype = file download
		Sourcedomain = [*.onedrive.com, drive.google.com, *.sharepoint.com, …]
			If your organization rarely interacts with other organizations through cloud storage, alert to use of external org's cloud storage. Mark as informational downloads from approved domains.	T1566.002

File write—Endpoint	Creation of suspicious LNK file	Logsource = endpoint
		Eventtype = file creation
		Filetype = lnk
		Contents contain (cscript or wscript or cmd or powershell or curl or wget or bitsadmin or …)
			Look for the creation of LNK files that would be used to execute scripting environments or launch tools that download contents from the internet. Some endpoint detection and response tools and Sysmon can provide this insight.	T1566.002

File write—Endpoint	Creation of WSF files	Logsource = endpoint Eventtype = file creation
		Filetype = wsf
			WSF files may be rare in your environment. If so, alert to the creation of any such files.	T1059

Continued

Detection Opportunity	Detection Name	Pseudocode	Description	MITRE

File write—Endpoint	Creation of office files that may include macros	Logsource = endpoint
		Eventtype = file creation
		Filetype = [doc, docm, xls, xlsm, …]
			Most organizations no longer use the antiquated office document format. Alert when these file types are written to disk. Also alert when macro specific document types are written.	T1566.001

Email Security Gateway	Email contains office files that may include macros	Logsource = email
		Eventtype = email
		Attachment=true
		Filetype = [doc, docm, xls, clsm, …]
			Most organizations no longer use the antiquated office document format. Macro oriented attachments should be blocked, otherwise alert and investigate.	T1566.001

Endpoint Execution	Use of cURL on non power user endpoint	Logsource = endpoint
		Eventtype = process start
		Filename = curl.exe
		NOT user = [list of power users…]
			Alert to highly anomalous use of cURL on Windows endpoints in the organization.	T1204.002

Endpoint Execution	Use of MSI packages	Logsource = endpoint
		Eventtype = process start
		Filename = *.msi
			Alert to execution of MSI files.	T1204.002

Teams Messages	Suspicious link sent between Teams users	Logsource = M365
		Eventtype = MessageCreatedHasLink
		MessageURL contains [strings similar to org's domain]
			Alert to urls sent over teams that are likely referencing a lookalike domain in order to capture more accounts.	T1534

Network Connection	Network traffic to a lookalike domain	Logsource = [dns, webproxy] domain contains [strings similar to org's domain]	Alert to dns queries or web traffic to domains with suspicious strings. E.g. ex4mple[.]com instead of example.com.	T1583.001

MFA Changes	Change or addition to user's MFA	Logsource = MFA
		Eventtype = [change phone, add phone]
			Changes to a user's phone number in their MFA profile should be rare. Alert and verify with the user.	T1098.005

Conclusion

Attackers have advanced the effectiveness of their techniques beyond the scope of what is covered by traditional anti-phishing guidance. User awareness concepts such as "only interact with emails from trusted senders" are no longer effective against attackers' use of compromised third-party accounts, conversation hijacking, internal phishing, and interactive social engineering. User devices outside the visibility of organizations are also being targeted, which drives the need for implementing stricter technical controls for authentication, and the detection of suspicious access. Often, an infection chain can involve more than one attacker, with separate groups responsible for the initial phishing access and control of a backdoor, and only a brief overlap in operations. Having a comprehensive detection and threat hunting strategy focused on behavioral indicators across all stages of the intrusion lifecycle can lead to faster identification of novel initial access methods. Early detection of intrusion activity and rapid system containment are critical to limiting impact from security incidents.

How Attackers Leverage AiTM to Overcome MFA

Mandiant has observed an increase in compromises against cloud-based identities configured with multi-factor authentication (MFA). As the adoption of MFA becomes commonplace across organizations, attackers are becoming proficient in methodologies capable of overcoming weaknesses in widely-adopted MFA methods. Most notable is the increasing adoption of web proxy or adversary-in-the-middle (AiTM) phishing pages, which are capable of rendering most MFA implementations ineffective by stealing sensitive login session tokens.

Common MFA Methods

MFA solutions often provide a variety of mechanisms for the management and approval of authentication requests. While mechanisms exist that are resistant to AiTM phishing, they often require additional infrastructure and overhead. However, the most commonly employed MFA mechanisms are the ones that are susceptible to attackers leveraging AiTM phishing.

MFA Type	Description
Push notification	Phone call or mobile application based prompt that only requires a user to accept a phone app push notification or press a key on their mobile device. Push notifications often lack context about the resource being accessed and can enable MFA fatigue attacks, in which users are sent repeated requests until the prompt is approved.
One-time password (OTP) / Time-based one-time password (TOTP)	Code from a SMS or email message, or a time-bound code generated by a mobile application or hardware device that is input along with a username and password during or following authentication. SIM swapping and credential harvesting webforms are common methods of stealing these codes, but they are also susceptible to exposure from seed theft or takeover of an account with access to cloud-synced TOTP codes.
Push notification with number matching verification	A push notification prompt generated on a user's mobile device that can only be accepted upon inputting a code generated by the logon portal. This addresses abuse mechanisms associated with MFA fatigue as well as TOTP code and seed theft.
Certificate-based authentication (CBA)	Authentication requiring X.509 certificate to be installed on devices. Resistant to AiTM phishing attacks.
Hardware keys	Physical devices compatible with the FIDO2 or U2F standard, which use public-key cryptography with supported cloud authentication services. This standard requires the server requesting a key to match the server tied to that key, therefore making it resistant to AiTM phishing attacks.

Credential Harvesting Evolved: Adversary-in-the-Middle

Attackers often leverage credential harvesting forms, or phishing pages, as a means to obtain logon credentials from their targets. These websites, which are designed to resemble popular login portals, can forward to an attacker credentials and MFA codes submitted by the targeted user. During an investigation into a business email compromise, Mandiant observed an attacker operating a credential harvesting form that forwarded credentials and time-based MFA codes to a private Telegram channel. This instant notification of stolen credentials provided the attacker an opportunity to successfully log in prior to the MFA code expiring, granting initial access into the targeted account.

AiTM phishing pages go beyond typical credential harvesting forms, and use infrastructure designed to overcome commonly implemented MFA methods. Unlike traditional credential harvesting forms, AiTM pages behave as a reverse web proxy between the targeted user and the legitimate logon portal. AiTM pages not only intercept credentials and MFA codes, but more critically, the post-authentication session token issued by the logon portal. These tokens can be used by an attacker to bypass security controls that are only evaluated on the initial sign-in.

Compared to traditional credential harvesting forms, the relative complexity of setting up AiTM phishing infrastructure may have kept its adoption by attackers limited in the past. However, in 2023, Mandiant observed a marked increase of AiTM phishing pages in use by attackers. The acceleration of AiTM usage amongst attackers has likely been aided by the availability of phishing-as-a-service offerings in the cybercriminal underground. Such offerings can provide less technically sophisticated attackers access to regularly maintained phishing infrastructure through which they can launch complex campaigns.

Detection and Mitigation

While AiTM phishing represents an evolution of attacker capabilities in the face of stronger controls such as MFA, compromises through AiTM phishing pages and the ensuing use of stolen session tokens provides defenders with detection opportunities. Since AiTM phishing pages are designed to intercept and forward a targeted user’s login information to a cloud authentication service, authentication logs will record the IP address associated with this phishing infrastructure as the user’s source IP address. The attacker’s IP address and associated User-Agent string, which may differ from the initial AiTM logon, will also be recorded when authenticating with a stolen token. Defenders should continue to monitor for anomalies, such as geographically infeasible or unexpected source IP addresses, and logins originating from data centers.

In nearly all of Mandiant’s investigations involving compromised cloud accounts, attackers were observed enrolling their own MFA methods shortly upon gaining initial access. Typically, this was done by interacting with a self-service security portal. While this activity isn’t exclusive to AiTM attacks and session token theft, it’s still worth highlighting as an effective detection opportunity, especially if paired with other logon anomalies. A regular review of new MFA registrations, as well as auditing accounts with multiple MFA methods configured, can reveal events worth further investigation.

To best defend against AiTM attacks, organizations should pursue a combination of AiTM-resistant MFA methods and access policies. Most cloud authentication services support access policies that can block logons based on organization-defined locations, device management status, or an assessment of risk based on the account’s historical logon properties. When implementing these access policies, it is important to understand which can be applied continuously throughout the logon session. Typically, most access policies are only applied at the initial token issuance stage, which will not offer protection against the use of previously stolen tokens.

Detection Opportunity	MITRE ATT&CK	Rule Logic
Okta - Detect AiTM Phishing using FastPass	T1078 T1556	eventType = "auth_via_mfa" AND result=FAILURE AND reason="FastPass declined phishing attempt"
Azure - Change of Authentication Method	T1098 T1556	LoggedByService="Authentication Methods" AND Category="UserManagement" AND OperationName="User registered security info"
M365 - Detects disabling of Multi Factor Authentication	T1556	LogSource = M365 Audit logs AND Operation="*Disable Strong Authentication.*"
Device Registration without MFA	T1078.004	Logsource = Azure sign in logs AND resourceDisplayName = “Device Registration Service” AND status = “Success” AND NOT authenticationRequirement = “multifactorAuthentication”
Attempt to reset Okta MFA factors for user	T1098	Logsource = Okta System events AND action = “user.mfa.factor.reset_all”

Conclusion

As AiTM phishing pages continue to grow in prevalence, many organizations today still rely on security controls that do not offer token theft protection. Furthermore, mitigating token theft and stolen token usage does not presently fit into a single, one-size-fits-all solution. Organizations can better protect against AiTM token theft by implementing phishing-resistant MFA methods and effective access policies, and reduce the risk of stolen token use with policies that are continuously evaluated during a logon session. If these controls are paired with effective anomaly-based detection methodologies, organizations can greatly reduce the risk of phishing attacks and an attacker’s dwell time.

Cloud Intrusion Trends

As enterprise cloud adoption and the use of hybrid cloud/on-premises environments continues to grow, adversaries have followed similarly in their targeting. Attackers recognize the value of data stored in cloud environments, and the computing resources available that could enable future malicious operations. Mandiant continues to observe attackers of varying motivations pivot to cloud environments to target cloud-hosted data, and leverage cloud computing resources in their operations.

Targeting Identity and Access Management and Bypassing MFA Requirements

Historically, to gain initial access to cloud and hybrid environments, attackers have relied upon stolen credentials and access tokens that did not require multi-factor authentication (MFA). As security awareness and MFA adoption has increased in recent years, attackers have placed an increasing emphasis on social engineering. During targeted social engineering campaigns, attackers lure users into providing credentials and using innovative methods to circumvent MFA or exploit weaknesses in its implementation.

Mandiant has observed increased usage of adversary-in-the-Middle (AiTM) techniques to bypass MFA requirements by capturing session tokens. In an AiTM campaign, the targeted user's connection to the legitimate cloud service is proxied through an attacker controlled server. By doing so, the user's credentials and MFA method are relayed to the legitimate cloud service while the attacker can capture the access token returned to the user. There are a number of AiTM kits advertised by attackers that can help automate the construction of convincing landing pages that mimic the legitimate cloud service logon page. In the majority of business email compromise (BEC) cases Mandiant responded to in 2023, successfully targeted users had MFA configured, but it was circumvented by an AiTM phishing campaign.

Attackers are known to leverage social engineering to target users, and Mandiant continues to observe the effectiveness of these campaigns. An espionage-related investigation revealed the use of a heavily tailored spear-phishing email that impersonated an individual in the same industry as the target, and used legitimate content relevant to the user to build credibility. The email lured the targeted user to click a link and enter their credentials to access protected information. Once in possession of the username and password, the attacker triggered a MFA push notification, which the targeted user accepted.

Additionally, Mandiant observed attackers abuse the trusted role of help desk and technical support personnel. In one case, phishing messages purporting to be from technical support lured users into providing MFA approval for malicious signins to a cloud platform. In another case, the financially motivated attacker UNC3944 relied heavily on social engineering to obtain credentials of users with elevated privileges, leveraging SMS phishing and placing phone calls to the targeted organization's help desks to reset a user's password or associated MFA device.[31]

In 2023, we observed an increase in the use of targeted SIM swapping to gain access to accounts. In cases where this was effective, organizations sent time-based one-time password MFA codes via SMS messages. In other cases, organizations used SMS to verify ownership of an account before sending a password recovery link. Financially motivated attackers have been observed leveraging SIM swapping to receive both types of SMS codes to facilitate an account takeover. A financially-motivated threat cluster, UNC3786, routinely performed SIM swapping to compromise credentials and gain access to targeted organizations' Okta and/or Microsoft 365 accounts. In one UNC3786 intrusion, while performing a SIM swap, the attacker sent spam SMS messages to the targeted user's phone, likely in an attempt to distract the individual from notifications from their phone carrier related to the SIM swap. UNC3944 similarly leveraged SIM swapping to gain access to user credentials and SMS MFA codes.[32]

Mandiant continues to observe attackers perform password guessing attacks against cloud sign-in portals to identify accounts that do not have MFA configured. Often organizations will rely on users to self-enroll an MFA device. This means that if an account does not already have MFA, the first successful password authentication will immediately prompt to enroll an MFA device. We have seen espionage attackers perform these guessing attacks to find and take over dormant accounts without MFA that should have been disabled, or service accounts with no need for MFA.

Weak Credential Storage

In other cases, Mandiant observed attackers using credentials that were stored poorly to gain access to cloud environments. In one incident, default configurations on an Internet accessible server led to the discovery and compromise of clear text AWS credentials, which allowed the attacker to gain access to a target's AWS environment. In another case, an attacker leveraged account credentials believed to have been stolen during a previous incident, enabling the attacker to gain access to the targeted organization's cloud-hosted code repository, which did not require MFA. Mandiant also responded to an incident involving an attacker that accessed a targeted organization's AWS environment using a leaked AWS access key. The investigation revealed that the key likely originated from a Docker container, hosted on an EC2 instance and owned by the organization, that was exposed to the internet. Copies of the same key were also found in other public IP addressable resources not owned by the targeted organization.

Adversary Abuse of Cloud Services

After obtaining initial access to cloud environments, Mandiant observed adversaries abuse cloud native tools and services to maintain access, move laterally, and ultimately accomplish mission objectives such as stealing data. By limiting themselves to preinstalled tooling, attackers can decrease their operational profile, evade detection, and maintain presence in cloud environments for longer periods of time.

Mandiant has observed attackers using Azure Data Factory and AirByte to modify existing pipelines to steal data stored in various integrated platforms such as data warehouses, storage blobs, and SQL databases. Specifically, attackers have created pipeline jobs that export data from those data sources to an attacker-controlled SFTP server. The use of data factories provided the attackers with a stable and high-bandwidth platform to copy large volumes of data.[33]

In 2023, Mandiant observed a financially-motivated attacker, UNC3944, backdoor cloud identity providers (IDP) using techniques that were previously only observed in use by espionage groups. In multiple investigations, UNC3944 gained administrative access to Entra ID (formerly Azure AD) to configure a rogue federated identity provider, which allowed them to execute golden SAML attacks. The attacker could then authenticate to resources protected by Entra ID as any user in the organization without knowledge of their password or possession of their MFA device. In one investigation, Mandiant observed UNC3944 target an organization's Active Directory Federated Services (ADFS) server, and execute Mimikatz in an attempt to obtain the token signing certificate to conduct a golden SAML attack.

Mandiant also saw attackers target cloud compute instances to maintain stealthy persistence in target cloud environments. In multiple incidents the attackers created Azure Virtual Machines (VMs) and assigned them public IP addresses. These attacker-created VMs did not have the organization's mandated security and logging software installed on them. As such, the attackers gained unmonitored access to a trusted system inside of the organization's virtual network or virtual private cloud, which they then use to progress their intrusion.[34]

Cloud compute instances often have network connectivity to organization on-premises networks via virtual private network, and can provide an avenue for lateral movement. On multiple occasions UNC3944 moved laterally from Azure console access into an Azure-hosted VM using the Special Administration Console to connect to VMs via serial console. Attackers have employed malicious use of the Serial Console on Azure VMs to install third-party remote management software, which provided them with persistent access to the VM. This method of attack is unique in that it avoided many of the traditional detection methods employed within Azure, and provided the attacker with full administrative access to the VM.

Mandiant has also observed attackers target cloud infrastructure for the specific purposes of cryptomining based on their perceived significant processing power. In one incident, an attacker gained access to a targeted organization's Google Cloud Platform (GCP) project via a leaked service account key. After accessing the project, the attacker deployed more than 1,200 virtual machines with a startup script to execute a Monero cryptocurrency miner using the XMR-Stak miner.

Attackers also leveraged open-source offensive security toolsets to survey the environment in some cases. Tools such as Pacu, an open source AWS exploitation framework, and CloudFox, an open source command line tool that can enable the discovery of exploitable attack paths into cloud infrastructure, were seen in one case being leveraged to perform automated reconnaissance. ScoutSuite, a cloud security and auditing tool, was used in another case to access AWS API and Console to conduct operations, which included the deployment of a cryptocurrency dataminer in the AWS environment.

Recommendations

Mandiant continues to observe attackers targeting weakly implemented identity management practices and credential storage to obtain legitimate credentials and circumvent MFA. As attackers have developed new methods to bypass MFA, organizations need to implement changes to their authentication policies to maintain a strong security posture. Phishing-resistant MFA methods have gained widespread support by web browsers, operating systems, and cloud service providers. The two most commonly accepted phishing-resistant MFA methods are certificate-based authentication (CBA) and FIDO2 security keys. Organizations can limit a attacker's ability to circumvent MFA protections by phasing out legacy MFA methods such as SMS, phone calls, and TOTP codes in favor of these newer methods.

In CBA, users are provisioned a certificate identifying them and their device as well as a corresponding private key. The private key is used to prove the user's identity to the cloud service provider. The user is never prompted for the private key, and in fact they do not know it. Almost all end-user systems in use today contain a Trusted Platform Module (TPM), which is a separate chip that stores and manages cryptographic keys securely, including the private key used in CBA. The key material never leaves the hardware boundary of the TPM, so it cannot be stolen by malware on the device. When CBA is used, the connection is negotiated using mutual TLS authentication, which resists most phishing methods because the secret key is not known to the user, and they are never prompted for it. Techniques that use AiTM are also thwarted because when the attacker proxies a targeted user's login session they must terminate the TLS connection, which will break CBA.

FIDO2 security keys rely on a similar security model as CBA to be phishing resistant, with the major distinction being the portability of the keys. With a FIDO2 security key, often a USB device, the key material never leaves the hardware boundary of the physical key. Users do not know and are not prompted for the key's value. Each website configured for FIDO2 has a unique private key that is tied to a particular application. If a user visits a phishing website, the browser will refuse to prompt the user for their security key because the phishing domain does not match any configured keys.

Cloud service providers (CSP) provide many tools to organizations to help detect and prevent common cryptominer schemes. First, all CSPs support authentication methods that provide additional security features beyond access keys and API secrets. Organizations should audit their cloud accounts and establish a program to remove any access keys, especially "root" or "superuser" access keys, and move towards modern role-based programmatic access secrets. Additionally, budgeting alerts and limits are a great way to monitor cloud accounts for abnormal spending. This is often a high-fidelity signal of a cryptocurrency scheme that has hijacked a cloud account. Finally, consider using a "secure by default" design for any new cloud environments. Secure by default bakes in vendor best practices to reduce the attack surface.

Organizations should also consider implementing additional controls to restrict access to cloud resources to only trusted devices. Each CSP supports this in some form although the exact language may differ. This can be done by using mobile device management (MDM) technologies to maintain device state, and allow authentication only from enrolled devices. If organizations require access to resources using untrusted devices (for example, a hotel computer) they should put in place policies that restrict what can be accessed, and how. For example, users should not be able to access the cloud administration console from an untrusted device. Similarly, downloading documents on untrusted computers should be limited or restricted.

Artificial Intelligence in Red (and Purple) Team Operations

In 1955, John McCarthy, a luminary of the fields of both computer science and cognitive science, coined the term “artificial intelligence” to be “the science and engineering of making intelligent machines.” This research started as a way to make a machine behave or perform like a human, but, in the modern landscape, the meaning has evolved to encompass machines that can learn like a human. While the artificial intelligence (AI) systems imagined in popular science fiction are still quite far off, AI is currently in a period of massive growth, investment, and potential. What started as logic machines with massive decision trees has expanded to highly complex algorithms based on myriad statistics and large-scale compute power. Recently, the most topical of these algorithms are those that are designed to produce something; these systems are commonly referred to as generative AI (gen AI).

> **Targeted attack lifecycle:** The typical sequence of events taken by attackers when conducting targeted operations.

Gen AI has captured recent interest and achievements following the release of multiple gen AI tools. Gen AI now creates content on scales previously unseen, and is assisting with fields that diverge from the purely technical foundations of computer science. In cybersecurity, we have seen gen AI revolutionize the field of detection engineering, where neural networks and machine learning algorithms now form the heart of a variety of detection and response toolsets. However, an area where we have yet to see substantial adoption, yet has the potential to yield significant gains, is in the field of proactive security and red team assessments.

During a red team assessment, Mandiant experts evaluate the capabilities of a customer’s security programs by simulating real-world attack scenarios. Mandiant has observed that attacker usage of AI has largely been limited to the Initial Access stage of the Targeted Attack Lifecycle. Specifically, usage has been limited to social engineering and information operations. Mandiant’s Red Team has leveraged gen AI in similar fashion, seeing the greatest growth in adoption when leveraging AI to gain Initial Access to client environments.

Social Engineering Pretexts

One of the most prominent examples of gen AI usage within red team assessments is assisting with the process of generating content and media. Mandiant Red Team assessments will often include a social engineering portion, during which Mandiant is tasked with convincing clients to undertake malicious actions unknowingly. This is commonly done through text- or image-based channels, such as impersonation emails or websites. Mandiant consultants have used gen AI tooling to create initial drafts of malicious emails, as well as potential landing pages under the guise of communications that are more routine. When successful, these social engineering attempts result in Mandiant gaining access to a client network, which is often the first objective of the assessment.

However, success is not the only metric that is helpful when performing social engineering campaigns during red team assessments. By offloading the setup workflow to an AI system, Mandiant is able to gain overall increases in throughput. The faster a social engineering campaign can be set up and performed, the more potential campaigns can be completed. Instead of creating a template from scratch, for which tailoring details can be quite time consuming, gen AI can be leveraged to source social engineering pretexts more quickly.

Rapid Tool Development

Much like how gen AI can be leveraged for the creation of social engineering pretexts, gen AI has also proven to be helpful in software development across many areas of programming. Mandiant has found similar advances provided when AI is used to assist in the development of custom tooling during red team engagements. Gen AI is proving to be a capable resource when assisting with well-known algorithms and data structures, can generate code from a natural language-based description, and even integrates into popular developer environments. These capabilities and integrations provide significant value when Mandiant encounters uncommon or new applications and systems—a regular occurance during red team assessments.

In cases where environments do not fit the operational norm, Mandiant looks to operationalize as much tooling as possible to assist with achieving a variety of engagement objectives. In one scenario, Mandiant consultants used gen AI to help build a set of tools that would assist with the enumeration of accessible cloud environments to provide recommendations that improve the security posture of customer environments. Without gen AI, this process would have been much lengthier, forcing consultants to spend hours scouring related documentation as opposed to operating and delivering value. Tooling built during engagements often live on well past the close of the engagement, continuing to provide value well into the future when reused. By closing the time necessary for the initial research and creation, the value gained by repeated use increases as the tooling is formalized and adopted in future engagements.

Rapid Knowledge Acquisition

During purple team engagements, Mandiant looks to become familiar with a client's environment from the perspective of both attacker and defender. Logging, data storage, and detection stacks come in a variety of packages from off-the-shelf software to custom built detection stacks made of bespoke software. This often places a consultant in an environment where they may not be fully knowledgeable of the defensive toolkit that the customer relies on for day-to-day operations. As a result, Mandiant consultants must familiarize themselves not only with the products in use, but their potential responses to the attacks being tested.

> **Red Team:** Red teams plan and execute attacks against organizations for the purposes of identifying weaknesses.

> **Purple Team:** Purple teams foster communication and collaboration between red teams and defenders to improve incident response capabilities.

Recently, Mandiant has begun to leverage gen AI in a conversation capacity to enhance understandings of platforms and subsequently hone in on the security aspects of those platforms. Conversations with gen AIs are often iterative, with broad-stroke initial requests such as asking the AI to describe the common logging methods of a specific piece of software. This provides a launchpad for the conversation to turn to more detailed topics based on subsequent questions, which reference previous answers and public documentation. While this workflow requires vetting of answers and follow-on testing, the collaborative nature of the process provides a user with a framework and initial knowledge base off which they can work. Ultimately this has led to an ability to build a more accurate understanding of the technology stack deployed within a customer's environment, a better engagement workflow, and a better product.

Future adoption of AI for Red Teams

AI and large language model (LLM) development teams seek to ingrain a concept of appropriate values within a developed language model. This concept, called "AI Alignment", attempts to produce models that work to advance the designer's intended goals within the values defined, while denying requests which fall outside them. AI alignment helps provide guardrails, which limit the malicious use of an AI. While attackers have leveraged AI to become more efficient, shy of developing their own models, they have to operate within the bounds defined by the alignment or attempt to break the alignment. Google even operates their own AI-specific Red Team[35] to help find and address potential misuse of AI. However, Mandiant's red team assessments present a logical conundrum for AI alignment.

Mandiant's red team performs sanctioned malicious actions that customers have requested in order to help improve the overall security of their environments. The concept of AI Alignment places a ceiling on the level of AI adoption red teams can expect when the values encoded in the AI make it such that it will not provide answers. Conversely, red team engagements produce high-quality data, which helps drive better security outcomes for customers that can, in turn, be used to train AI models.

An exciting feature of LLMs is their ability to be fine-tuned or trained on what is known as domain specific knowledge. The majority of LLMs used by the public are generalist LLMs, meaning that the models are trained on a variety of data that covers a wide swath of different knowledge domains varying in both depth and breadth. Some LLMs are tuned for programming, whereas others might be targeted towards medical knowledge such as MedLM.[36] For the purposes of cybersecurity experts, there is Google's SecLM,[37] which is designed to provide actionable visibility into the latest threats. Tuning LLMs on specific knowledge domains requires vast amounts of specialized data within the target domain. Red teams, as professional organizations, generate and store a substantial amount of data, which could be used to train models tuned to help secure customer environments.

Resolving these logical and technical challenges will require a multi-pronged approach. Red teams will need to generate structured data on which models can be trained, and provide subject matter expertise to AI developers. Meanwhile, AI developers will have to find novel ways to pursue AI Alignment that leverages the legitimate use of malicious activity, and to properly secure access to the models that will be trained on that data. The combination of red team expertise and powerful AI leads could result in a future where red teams are considerably more effective, and organizations are better able to stay ahead of the risk posed by motivated attackers.

Conclusion

The continued decrease in global median dwell time is a positive trend to see, and a testament to the efforts of defenders to detect threats as quickly as possible. However, attackers are not giving up. In fact, they are focusing more of their efforts on evasion—notably through the increased use of zero-day vulnerabilities, and targeting of edge devices and other technologies outside the traditional lines of visibility. This is bound to be one of the more challenging trends facing defenders in 2024.

One of the ways organizations can test how quickly their security teams can defend against evasion tactics—as well as other threats discussed in M-Trends 2024 such as phishing and MFA bypasses—is by leveraging red team exercises. M-Trends 2024 highlights how Mandiant red and purple teams are using AI—as well as the latest attacker tactics, techniques and procedures—to enhance and improve the effectiveness of engagements, providing customers with a clear understanding about the effectiveness of their security controls. AI is a powerful tool, and organizations are increasingly using it in their security toolkit to identify threats faster, eliminate toil, and fill talent gaps. On the offensive end, attacker use of AI remains limited[38] for now, and is most notably being used for social engineering and information operations.

Preparation is vital, and should be comprehensive and layered. In addition to conducting red team and other exercises to test security teams, other best practices include involving Communications, Legal and other relevant teams in regular tabletop exercises that test incident response plans, and continually reviewing those incident response plans throughout the year.

Sound fundamentals, such as vulnerability and exposure management, least privilege, and hardening also play a role in building strong defenses. Organizations should focus on building a comprehensive security program that spans the entire enterprise, from cloud and on-premises, to IT/OT, and all assets. This program should be backed by strong detection and proactive hunting capabilities that are fueled by impactful threat intelligence.

The Mandiant mission is to help keep every organization secure from cyber threats and confident in their readiness. Our annual M-Trends report, featuring data and learnings from our engagements, plays a big part in advancing that mission. We will continue to share our frontline knowledge in M-Trends to improve our collective security awareness, understanding, and capabilities.

Bibliography

1. https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
2. https://cloud.google.com/blog/topics/threat-intelligence/separating-signal-noise-how-mandiant-intelligence-rates-vulnerabilities-intelligence
3. https://nvd.nist.gov/vuln/detail/CVE-2008-2463
4. https://nvd.nist.gov/vuln/detail/CVE-2017-0144
5. https://nvd.nist.gov/vuln/detail/CVE-2019-18935
6. https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-action-disrupt-illicit-revenue-generation
7. https://cloud.google.com/blog/topics/threat-intelligence/north-korea-cyber-structure-alignment-2023
8. https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/
9. https://cloud.google.com/blog/topics/threat-intelligence/unc3944-sms-phishing-sim-swapping-ransomware
10. https://cloud.google.com/blog/topics/threat-intelligence/apt29-evolving-diplomatic-phishing
11. https://cloud.google.com/blog/topics/threat-intelligence/unc4841-post-barracuda-zero-day-remediation
12. https://cloud.google.com/blog/topics/threat-intelligence/how-mandiant-tracks-uncategorized-threat-actors
13. https://cloud.google.com/blog/topics/threat-intelligence/apt43-north-korea-cybercrime-espionage
14. https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant
15. https://www.justice.gov/usao-nj/pr/russian-national-charged-conspiring-commit-lockbit-ransomware-attacks-against-us-and
16. https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation
17. https://cloud.google.com/blog/products/identity-security/attacker-visibility-threat-campaigns
18. https://cloud.google.com/blog/topics/threat-intelligence/zero-day-moveit-data-theft
19. https://www.progress.com/security/MOVEit-transfer-and-MOVEit-cloud-vulnerability
20. https://cloud.google.com/blog/products/identity-security/cloud-ciso-perspectives-late-june-2023
21. https://cloud.google.com/blog/topics/threat-intelligence/zero-day-moveit-data-theft
22. https://cloud.google.com/blog/topics/threat-intelligence/unc4841-post-barracuda-zero-day-remediation
23. https://www.fbi.gov/news/stories/fbi-partners-dismantle-qakbot-infrastructure-in-multinational-cyber-takedown
24. https://cloud.google.com/blog/topics/threat-intelligence/gru-disruptive-playbook
25. https://cloud.google.com/blog/topics/threat-intelligence/zero-day-moveit-data-theft
26. https://services.google.com/fh/files/misc/barracuda-esg-rpt-en.pdf
27. https://cloud.google.com/blog/topics/threat-intelligence/zero-day-moveit-data-theft
28. https://cloud.google.com/blog/topics/threat-intelligence/barracuda-esg-exploited-globally
29. https://cloud.google.com/blog/topics/threat-intelligence/putting-model-work-enabling-defenders-vulnerability-intelligence-intelligence-vulnerability-management-part-four
30. https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/
31. https://cloud.google.com/blog/topics/threat-intelligence/unc3944-sms-phishing-sim-swapping-ransomware
32. https://cloud.google.com/blog/topics/threat-intelligence/sim-swapping-abuse-azure-serial

33. https://cloud.google.com/blog/topics/threat-intelligence/unc3944-sms-phishing-sim-swapping-ransomware
34. https://cloud.google.com/blog/topics/threat-intelligence/unc3944-sms-phishing-sim-swapping-ransomware
35. https://blog.google/technology/safety-security/googles-ai-red-team-the-ethical-hackers-making-ai-safer/
36. https://cloud.google.com/blog/topics/healthcare-life-sciences/introducing-medlm-for-the-healthcare-industry
37. https://cloud.google.com/blog/products/ai-machine-learning/gemini-for-google-cloud-is-here
38. https://cloud.google.com/blog/topics/threat-intelligence/threat-actors-generative-ai-limited

Google Cloud

For more information, visit **cloud.google.com**.