MANDIANT®

NOW PART OF Google Cloud

M-TRENDS 2023

MANDIANT SPECIAL REPORT

Table of Contents

Introduction

The lines separating the real world and the cyber realm have never been hazier. We're seeing Russia engage in information operations in an attempt to influence the narrative surrounding their invasion of Ukraine, and attempt to disrupt critical infrastructure through both physical and cyber attacks. We're seeing the invasion have an influence on the broader cybercrime ecosystem, notably in Europe, where actors are choosing sides or shutting down operations altogether. And we're seeing actors engage in cybercrime to fund espionage to support the North Korean regime, targeting information on topics ranging from nuclear to COVID-19.

Every day Mandiant responders are investigating and analyzing the latest attacks and threats, and understanding how best to respond to and mitigate them. We pass these learnings on to our customers through our various services, helping them to stay ahead of a constantly evolving threat landscape.

In releasing our annual M-Trends report, we aim to provide some of that same critical intelligence to the greater security community. M-Trends 2023 continues our tradition of offering details on the evolving cyber landscape, mitigation recommendations, and a wide variety of security incident-related metrics.

Let's start with answering one of the biggest questions from our "By the Numbers" section. The answer is yes, attacks are being detected faster than ever before. From January 1, 2022, to December 31, 2022, the global median dwell time is now 16 days, down from 21 days in our M-Trends 2022 report. This may demonstrate an improved ability to detect attacks, but we also credit ransomware attacks to be a driving factor in reducing dwell time. Intrusions involving ransomware had a median dwell time of 9 days in 2022, compared to 5 days reported in M-Trends 2022.

The topics of M-Trends 2023 include:

By the Numbers: Organizations were notified of breaches by external entities in 63% of incidents compared to 47% in M-Trends 2022, which brings the global detection rates closer to what defenders experienced in 2014. We have many more signature metrics on targeted industries, attack types, threat groups, and malware use, along with new breakdowns based on trends and observations.

The Invasion of Ukraine: Russia's invasion of Ukraine has consumed almost every aspect of Russia's international relationships, and has evolved as nearly the sole driver of cyber threat activity from Russia in 2022. We cover operations dating back to before the physical invasion in February, including use of destructive and disruptive attacks, and information operations.

North Korean Financial Operations: For years, North Korea has reportedly conducted various illicit financial activities to fund the regime. The explosive growth of cryptocurrency is converging with aggressive and flexible North Korean cyber capabilities, making it natural that at least some North Korean threat groups would expand operations into this sector.

Shifting Focus and Uncommon Techniques: In 2022, Mandiant investigated a series of high-profile intrusions that were successful and impactful to the targeted organizations despite significant deviations from common threat actor behaviors, underscoring the threat posed to organizations by persistent adversaries willing to eschew the unspoken rules of engagement.

M-Trends 2023 additionally contains a red team case study, tales of threat actors and vulnerabilities from our Campaign and Global Events team, and details from our APT42 graduation.

M-Trends builds on our dedication to continue 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

Data from Mandiant Investigations

The metrics reported in M-Trends 2023 are based on Mandiant Consulting investigations of targeted attack activity conducted between January 1, 2022 and December 31, 2022. Note that this edition of M-Trends returns to a 12-month period compared to the 15-month period reported in M-Trends 2022.

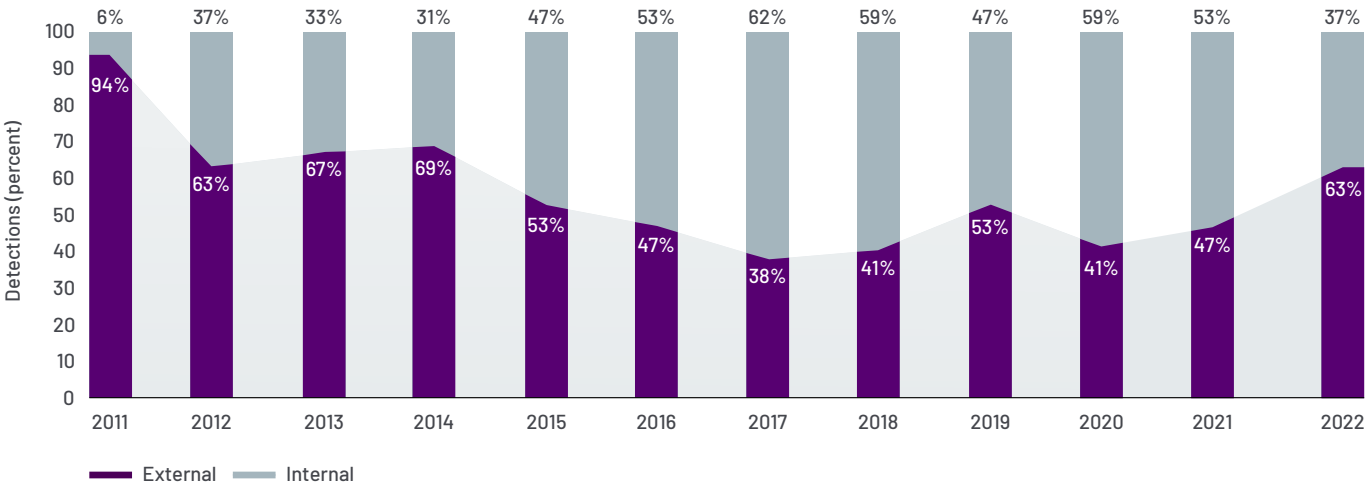
Internal detection is when an organization independently discovers it has been compromised.

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

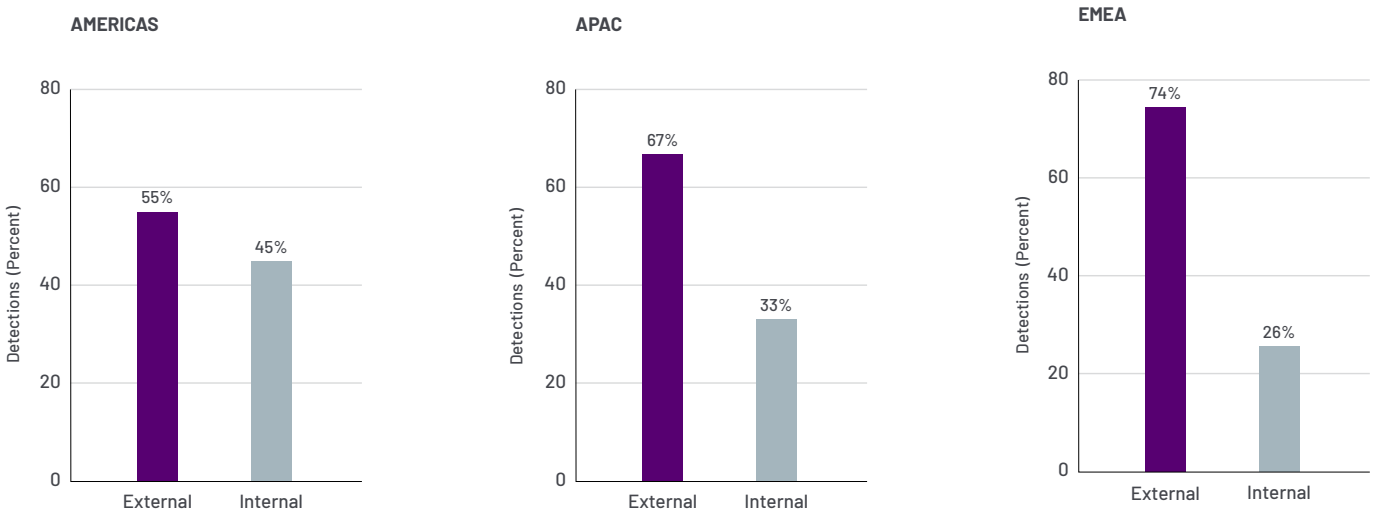
Detection by Source

In 2022, Mandiant observed a general increase in the number of organizations that were alerted by an external entity of historic or ongoing compromise. Organizations were notified of breaches by external entities in 63% of incidents. This continues the trend observed in 2021 and brings the global detection rates closer to what defenders experienced in 2014. The increase in external notification observed in 2022 is likely impacted by Mandiant's investigative support of cyber threat activity which targeted Ukraine and an increase in proactive notification efforts. Proactive notifications from security partners enable organizations to launch response efforts more effectively. Analysis of Mandiant's efforts in Ukraine are highlighted in The Invasion of Ukraine: Cyber Operations During Wartime.

Detection by Source, 2011-2022



Detection by Source by Region, 2022



Historically, Mandiant has observed relatively stable detection rates for organizations headquartered in the Americas. However, in 2022, organizations were notified by an external entity in 55% of incidents, compared to 40% of incidents last year. This is the highest percentage of external notifications the Americas has seen over the past six years. While organizations in the Americas continue to improve detection capabilities, external notifications from trusted security partners remain the primary way organizations are made aware of incidents.

In 2022, 33% of the incidents Mandiant experts responded to in the Asia Pacific (APAC) region were originally identified by internal entities. However, over the past six years, Mandiant has observed a trend towards greater external notifications in the APAC region. This year's 9-percentage point increase in internal detections when compared to 2021 demonstrates the strong variability Mandiant has observed in detection source in the APAC region.

Organizations in Europe, the Middle East and Africa (EMEA) were alerted of an intrusion by an external entity in 74% of investigations in 2022 compared to 62% in 2021. This marked increase in external notifications could be explained by Mandiant's investigative support to Ukraine and is likely an outlier from the general trend. Mandiant continues to see a shift to more external notifications in the EMEA region over the past six years, however because of extenuating circumstances in 2022, this trend may stabilize in the future.

Detection by Source by Region, 2017–2022

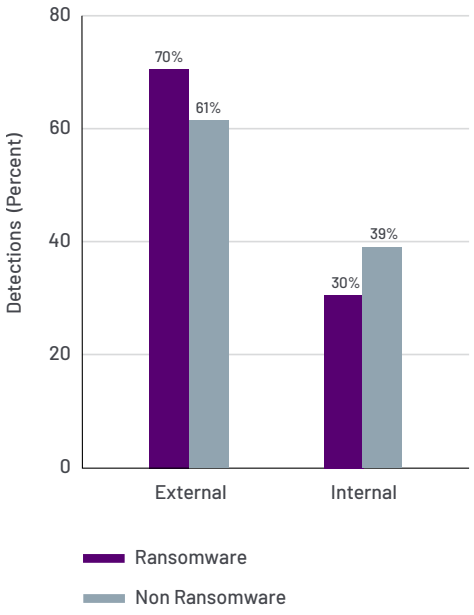
A **ransomware related intrusion** provides access for, or is associated with, a malicious actor that has the primary goal of encrypting data with the intention of extracting payment from the target in order to avoid further or undo the malicious action.

In 2022, external notifications were more prevalent as a notification source regardless of the investigation type. In intrusions related to ransomware, organizations were notified by an external entity in 70% of investigations. Organizations were predominantly notified by adversaries due to a fully executed ransomware event with 67% of investigations (8% of all investigations) detected due to a ransom note. Notifications from external partners comprise the remaining 33% of ransomware related investigations (4% of all investigations).

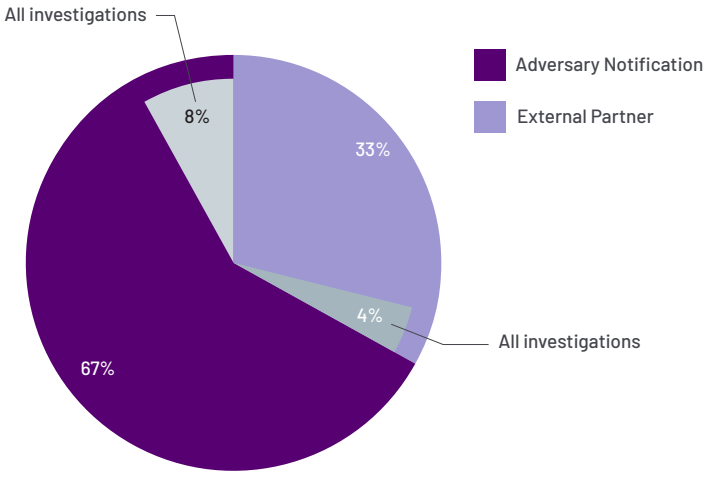
Similarly, organizations were notified by external entities of non-ransomware related intrusions more often than the organization was able to identify similar intrusions internally. However, Mandiant observed organizations in 2022 identify non-ransomware intrusions internally more often than ransomware intrusions. This may be due to increased visibility allowing organizations to detect intrusions earlier in the Targeted Attack Life Cycle. While non-ransomware operations often prioritize avoiding detection mechanisms, the longer operations cycles provides more detection opportunities when compared to the relatively short cycle employed by ransomware operators.

Mandiant continues to see positive collaboration between organizations and external partners that perform compromise notifications. These external parties provide effective information that aids an organization's ability to identify intrusions more quickly, regardless of the investigation type.

Detection by Source, by Investigation Type, 2022



Ransomware Investigations— External Notification Source



Dwell Time

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

Change in Median Dwell Time

21 → **16**

Days in 2021 Days in 2022

Global Dwell Time

Global median dwell time continued to improve year over year, with organizations detecting incidents in just over two weeks in 2022. This is the shortest global median dwell time from all M-Trends reporting periods.

Notable improvement in global median dwell time where an external entity was the notification source may indicate that organizations respond to external notifications more quickly. This reflects a growing recognition of the critical role partnerships and information exchange play in building a resilient cybersecurity ecosystem. As security partners are improving the critical information contained within external notifications, the improvement of information sharing will enable organizations to act more effectively than if left to identify similar intrusions on their own.

Defenders continue to detect events faster than external entities notify. The global median dwell time for internally detected incidents in 2022 returned to similar timeframes defenders saw in 2020. In 2022, the global median dwell time for intrusions detected internally was 13 days. The global median dwell time was 18 days in 2021 and 12 days in 2020.

Similarly, Mandiant experts observed another significant decrease in the global median dwell time for investigations with an external notification source in 2022, down 32% compared to 2021. External notifications allowed for organizations to initiate response to intrusions within a median of 19 days of the initial compromise.

Improvements in global median dwell time in 2022, regardless of detection source, enabled organizations to respond to incidents faster than ever before.

Global Median Dwell Time, 2011-2022

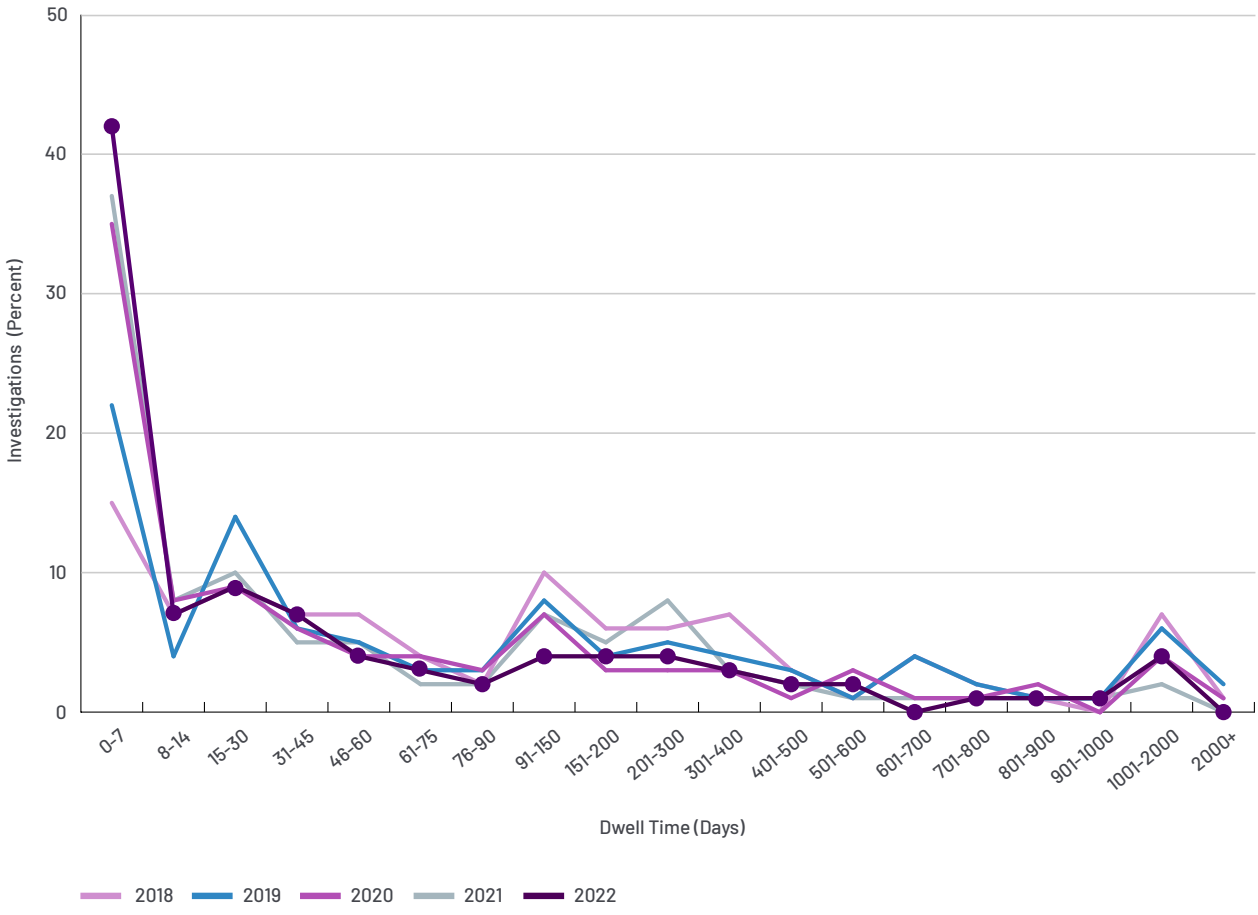
	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
All	416	243	229	205	146	99	101	78	56	24	21	16
External	–	–	–	–	320	107	186	184	141	73	28	19
Internal	–	–	–	–	56	80	57.5	50.5	30	12	18	13

Global Dwell Time Distribution

Global dwell time distribution continues to improve. 42% of intrusions were detected within a week or less, compared to 37% of intrusions in the last reporting period. Compared to previous years, Mandiant saw more evenly dispersed dwell times across investigations in 2022. Continuing trends from the last M-Trends reporting period, this could indicate that detection is becoming more streamlined and detection abilities have improved to highlight actions in the environment during the initial infection or the reconnaissance phases of the Targeted Attack Lifecycle.

However, as Mandiant continues to see a wider distribution for non-ransomware related investigations, organizations are still facing intrusions that go undetected for extensive periods of time. Variance in the detection capabilities of impacted organizations and the types of intrusions they face are likely contributors to this distribution spread.

Global Dwell Time Distribution, 2018-2022



Change in Global Investigations Involving Ransomware

23% → **18%**

in 2021 in 2022

Change in Global Median Dwell Time – Ransomware

5 → **9**

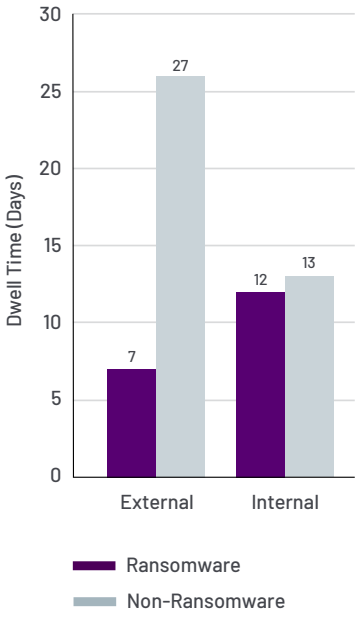
Days in 2021 Days in 2022

Change in Global Median Dwell Time—Non-Ransomware

36 → **17**

Days in 2021 Days in 2022

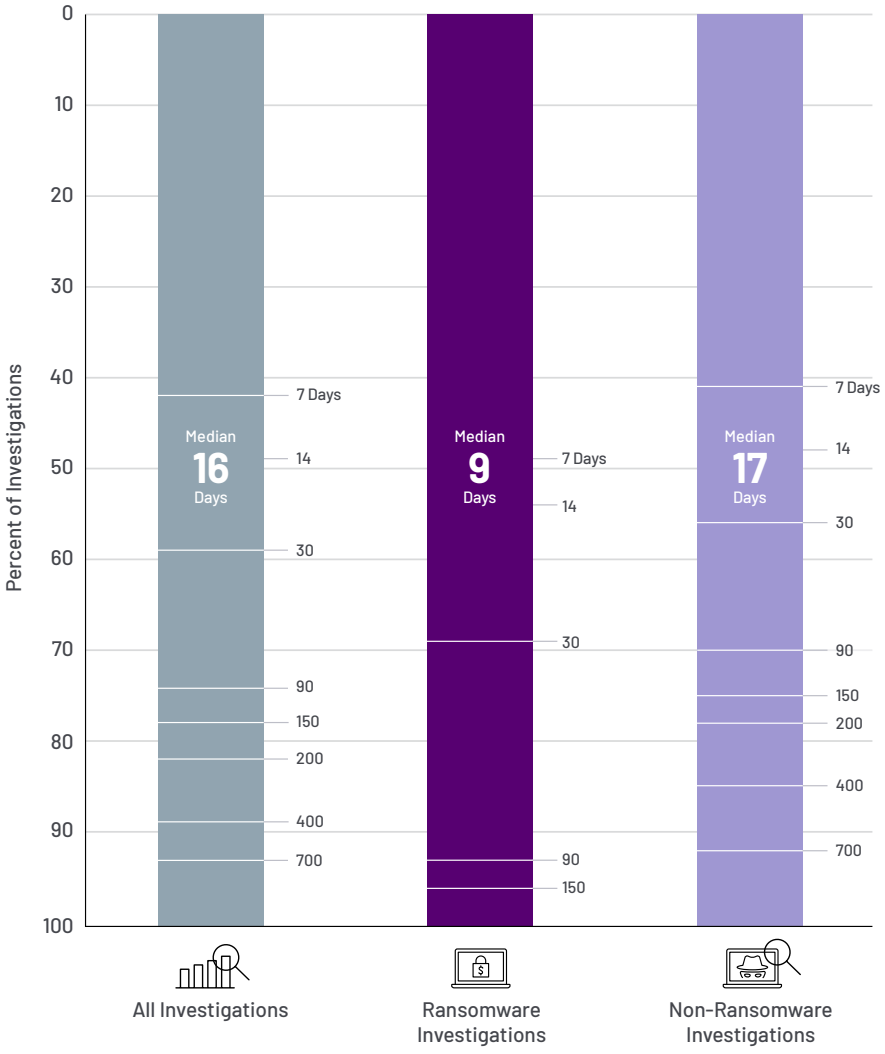
Global Median Dwell Time by Detection Source



Investigations Involving Ransomware

Mandiant experts note a decrease in the percentage of global intrusions involving ransomware between 2021 and 2022. In 2022, 18% of intrusions involved ransomware compared to 23% in 2021. Ransomware attacks continue to be a driving factor in a reduced dwell time. Intrusions involving ransomware had a median dwell time of 9 days in 2022, compared to 5 days in 2021. Mandiant observed that in instances where external entities are making the notification, the global median dwell time for intrusions involving ransomware was 7 days compared to 12 days when an organization detected the intrusion internally. Mandiant observed that adversaries leveraging ransomware remained undetected for longer periods of time in 2022 compared to 2021.

Global Dwell Time by Investigation Type, 2022



Americas

Change in Americas Median Dwell Time

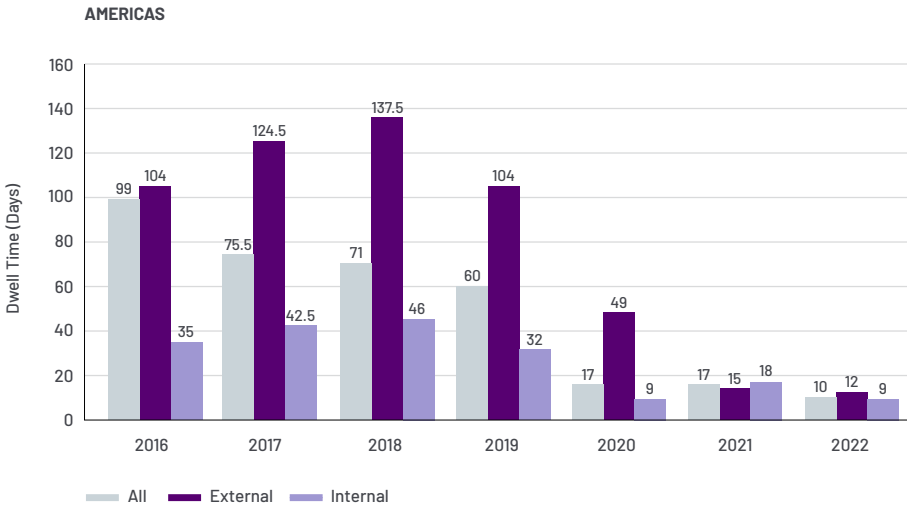
17 → **10**

Days in 2021 Days in 2022

Americas Median Dwell Time

The median dwell time for intrusions investigated in the Americas decreased by a full week in 2022 to 10 days compared to 17 days in 2021 and 2020. Mandiant observed consistent median dwell times for all detection types in the Americas, with internal detections decreasing to 9 days and external detections at its lowest with 12 days. Organizations in the Americas demonstrated another year of improvement for detecting adversaries faster than previous years, quicker than the previously smallest timeframe of 17 days observed in 2021.

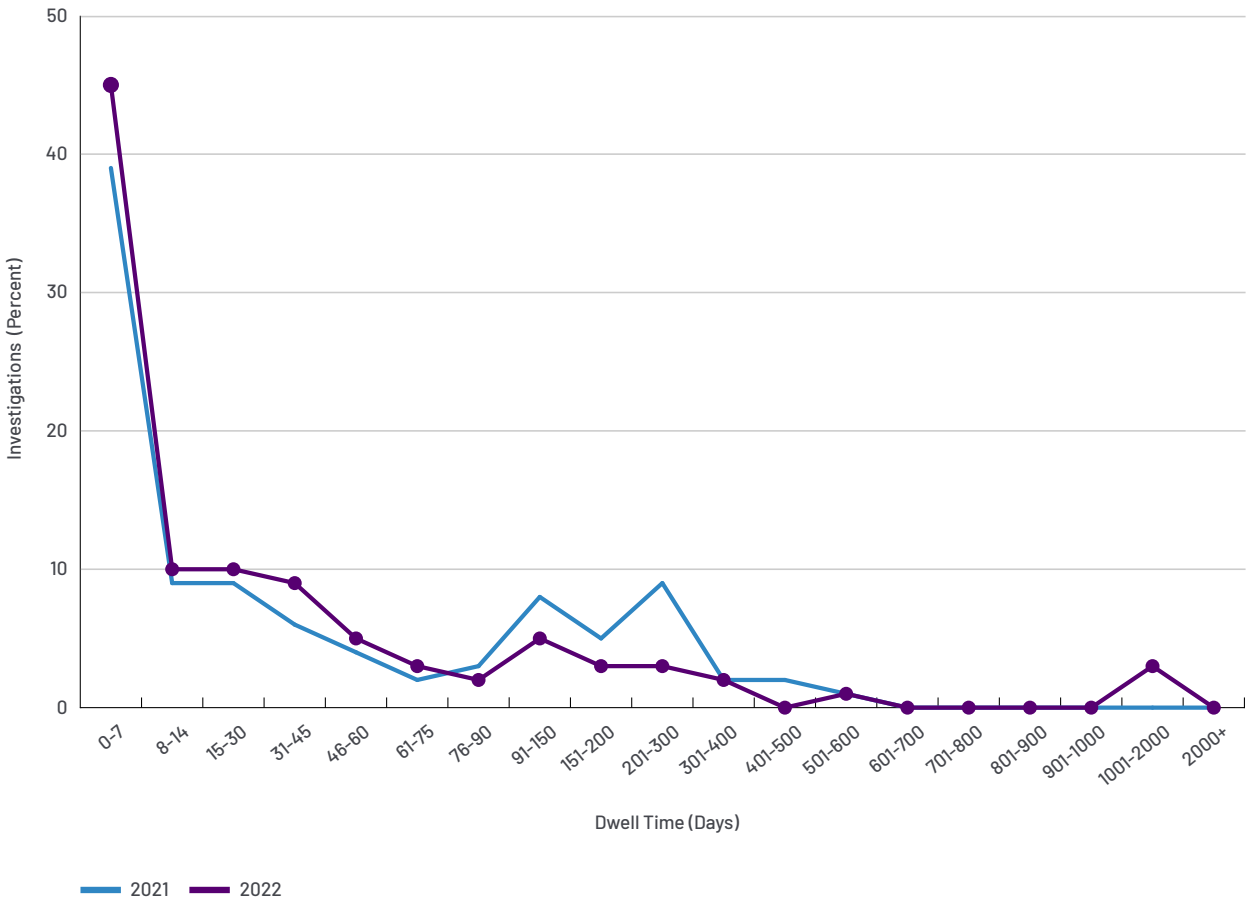
Americas Median Dwell Time, 2016-2022



Americas Dwell Time Distribution

In the Americas, 64% of intrusions were detected in 30 days or less and 70% of these intrusions (45% of total intrusions in the Americas) were detected in less than one week. In 2022, more than half of the intrusions in the Americas were detected in less than two weeks. However, Mandiant observed a small uptick in intrusions that go undetected for longer periods of time, with 7% of total intrusions in the Americas remaining undetected for more than a year. This is an increase from 4% observed in the reporting period of M-Trends 2022. This shows that while organizations in the Americas were able to detect most intrusions within two weeks, due to detection improvements, they identified intrusions by adversaries that would have otherwise remained undetected for longer.

Americas Dwell Time Distribution, 2021-2022



Change in Americas Investigations Involving Ransomware

22% → **22%**

in 2021 in 2022

Change in Americas Median Dwell Time – Ransomware

5 → **5**

Days in 2021 Days in 2022

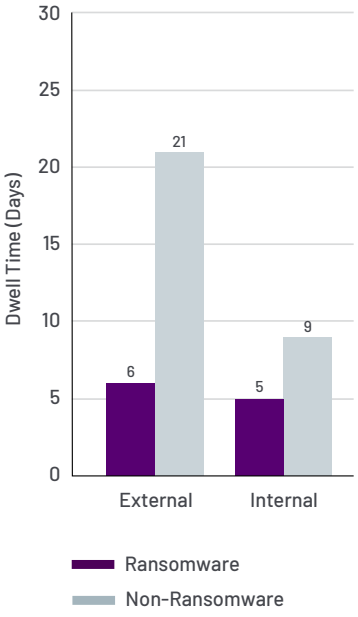
Change in Americas Median Dwell Time – Non-Ransomware

17 → **12**

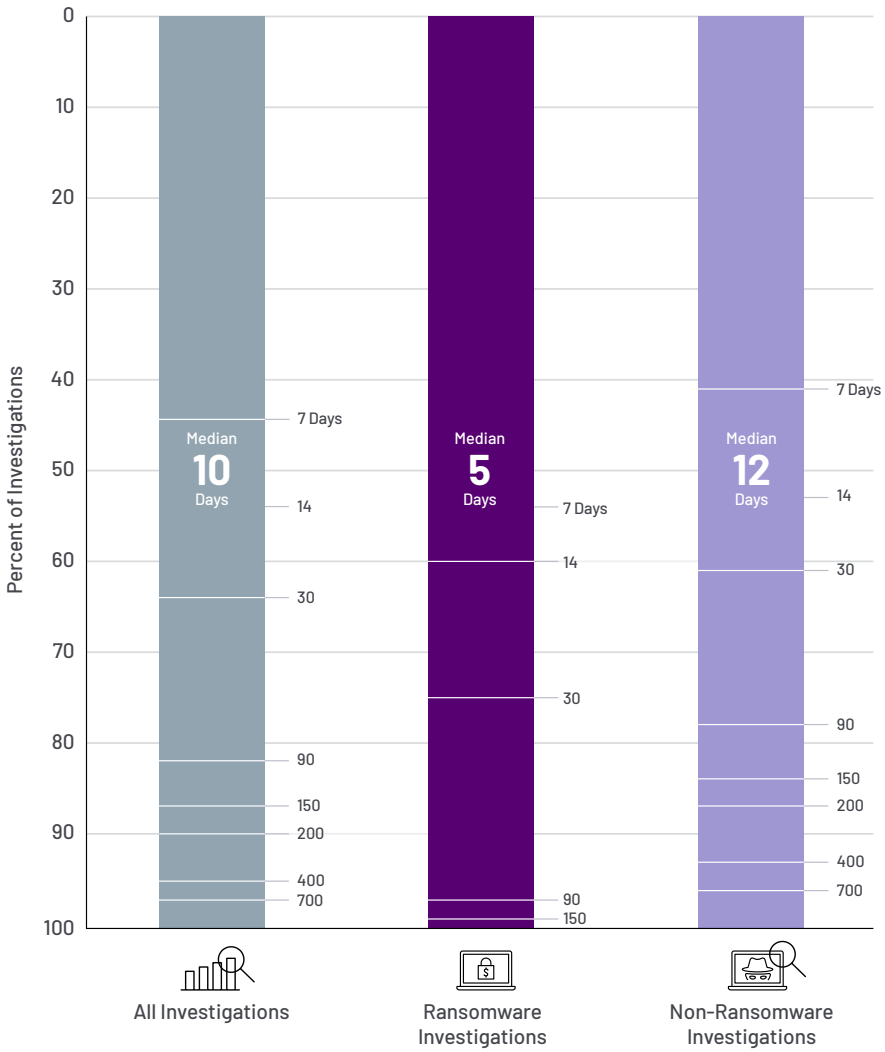
Days in 2021 Days in 2022

Although the percentage of intrusions involving ransomware has decreased globally, Mandiant observed a consistent percentage of investigations in the Americas involving ransomware compared to last year. Similarly, ransomware dwell time continues to remain the same in the Americas region. Mandiant noted that these investigations have similar median dwell times regardless of internal or external detection source, with five days median dwell time for internally notified investigations, and six days when external entities make the notification. Mandiant continues to observe improvements in external notifications for non-ransomware related intrusions. In 2022 organizations in the Americas detected intrusions that did not relate to ransomware in 12 days, compared to 17 days in 2021.

Americas Median Dwell Time by Detection Source



Americas Dwell Time Investigation by Type, 2022



APAC

Change in APAC Median Dwell Time

21 → **33**

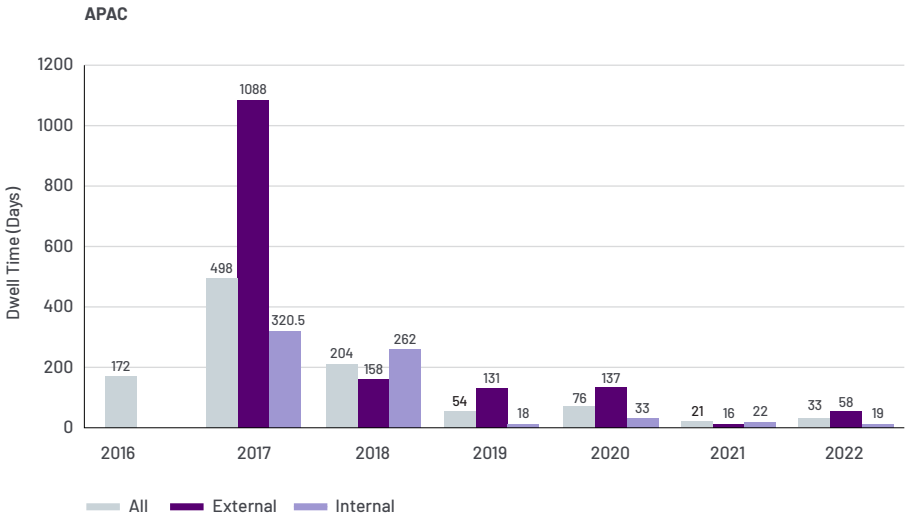
Days in 2021 Days in 2022

APAC Median Dwell Time

Overall, median dwell time in APAC increased compared to the last M-Trends reporting period. However, organizations in APAC are still detecting intrusions more quickly than in previous years, with a median dwell time of 19 days for intrusions identified internally compared to 22 days in 2021. Organizations in APAC have consistently improved internal detection capabilities over the past three years.

Notifications from external entities resulted in a median dwell time of 58 days in 2022 compared to 16 days in 2021. While this represents an increase in median dwell time, it is still a 58% decrease compared to external notification median dwell time in 2020 which was 137 days. The increase to 58 days is likely a result of the median dwell time numbers normalizing from an abnormally short period of time observed in 2021.

APAC Median Dwell Time, 2016-2022

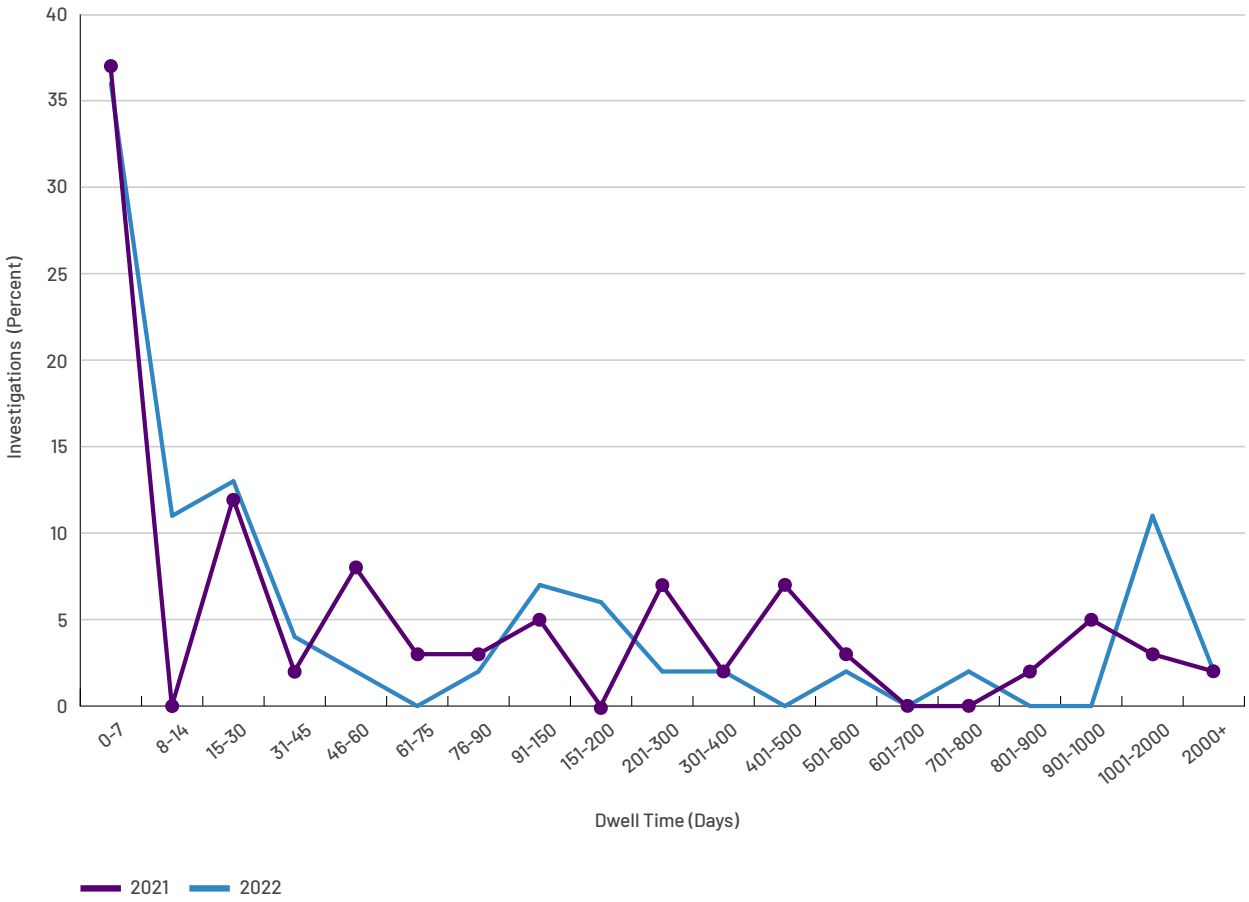


APAC Dwell Time Distribution

APAC dwell time distribution continues to show variability. Dwell time distribution shows 48% of APAC investigations had dwell times of 30 days or less with 76% of these intrusions (37% of all APAC intrusions) detected in one week or less. On the other side of the dwell time distribution, APAC organizations had a wider distribution of intrusions go undetected for longer periods of time, with 30% of investigations remaining undetected for a year or longer compared to 20% of investigations in 2021.

Cyber security continues to mature in APAC with ongoing detection capability improvements. This allows organizations to identify intrusions that would have otherwise gone long undetected, resulting in a wider distribution of intrusions.

APAC Dwell Time Distribution, 2021-2022



Change in APAC Investigations Involving Ransomware

38% → **32%**

in 2021 in 2022

Change in APAC Median Dwell Time – Ransomware

9 → **18**

Days in 2021 Days in 2022

Change in APAC Median Dwell Time – Non-Ransomware

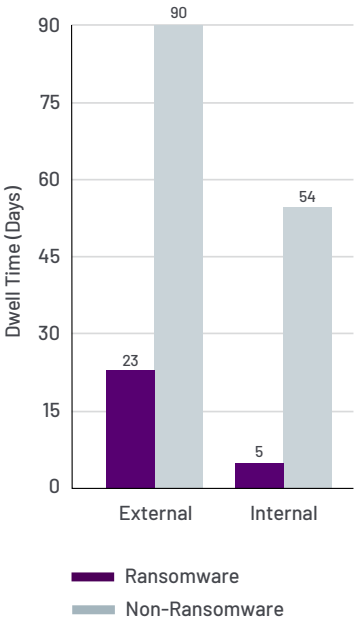
38 → **60**

Days in 2021 Days in 2022

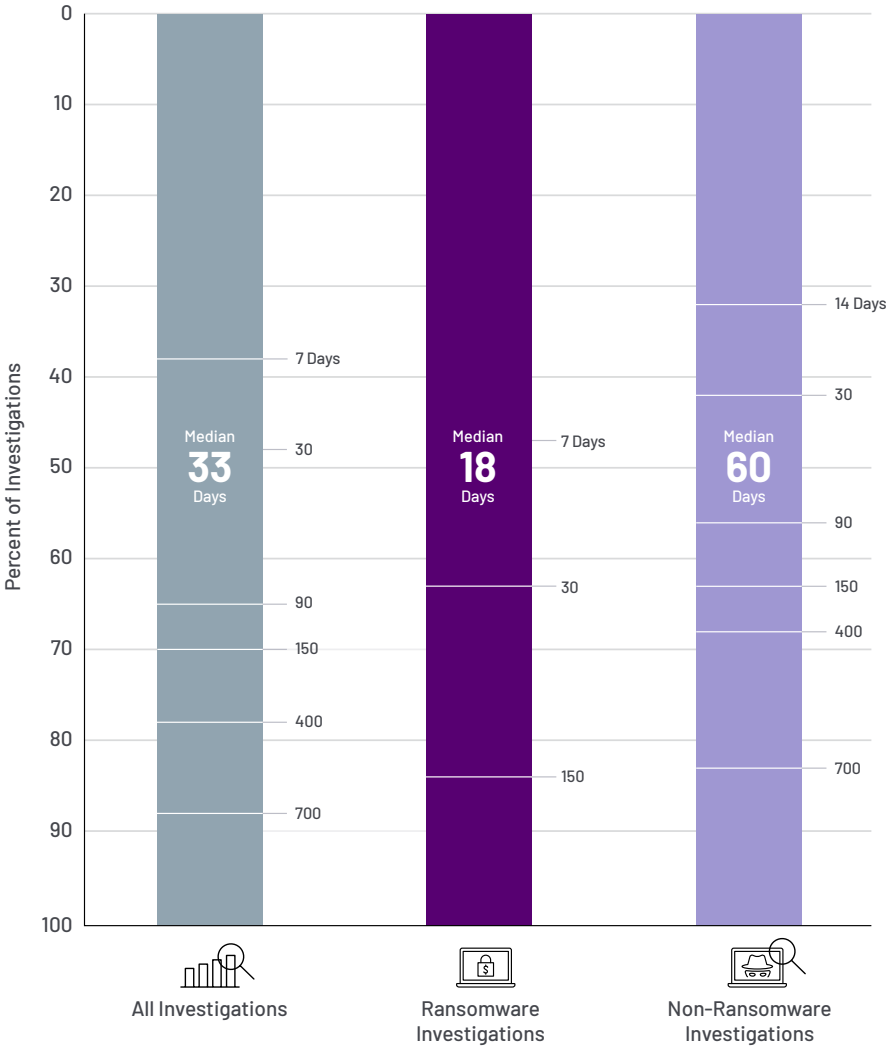
Similar to the observed decrease in global investigations involving ransomware, APAC saw a 6-percentage point decrease in ransomware investigations, with 32% in 2022 compared to 38% in 2021. This number is still almost double the percentage of investigations from 2020 (12.5%) and 2019 (18%).

The median dwell time for ransomware investigations in APAC was 18 days compared to 60 days for non-ransomware investigations. Organizations in APAC are quicker to detect incidents internally than externally, regardless of the type of investigation. However, the timeframe observed with relation to ransomware median dwell time does significantly impact dwell time as a whole.

APAC Median Dwell Time by Detection Source



APAC Dwell Time by Investigation Type, 2022



EMEA

Change in EMEA Median Dwell Time

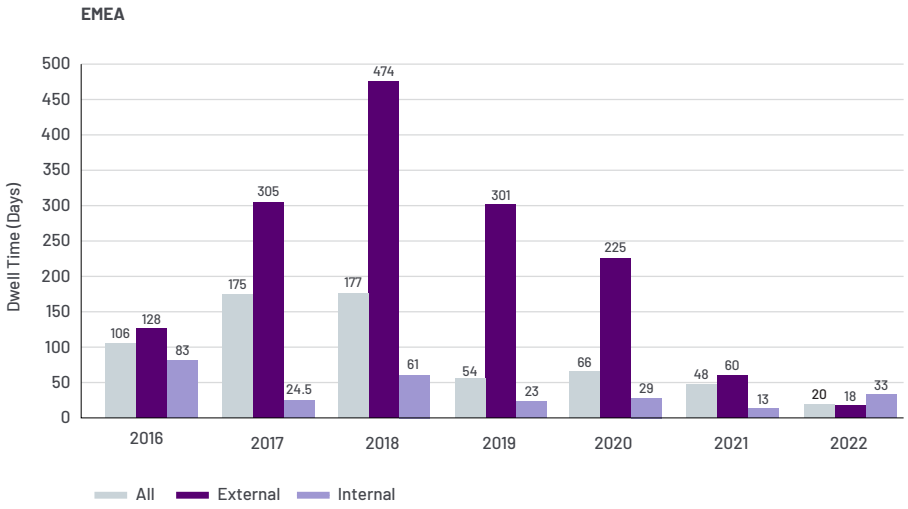
48 → **20**

Days in 2021 Days in 2022

EMEA Median Dwell Time

Organizations in EMEA detected incidents 58% faster in 2022 compared to 2021, with the overall median dwell time now less than three weeks. Looking closer at detection sources, median dwell time for intrusions that were detected by an internal source increased from 13 days seen in 2021 to 33 days in 2022. External notification sources decreased from 60 days seen in 2021 to 18 days in 2022. This large change may be influenced by Mandiant's work in Ukraine, which makes up a notable portion EMEA investigations in 2022. However, even outside of this work, the general trend shows that median dwell time continues to decrease year over year.

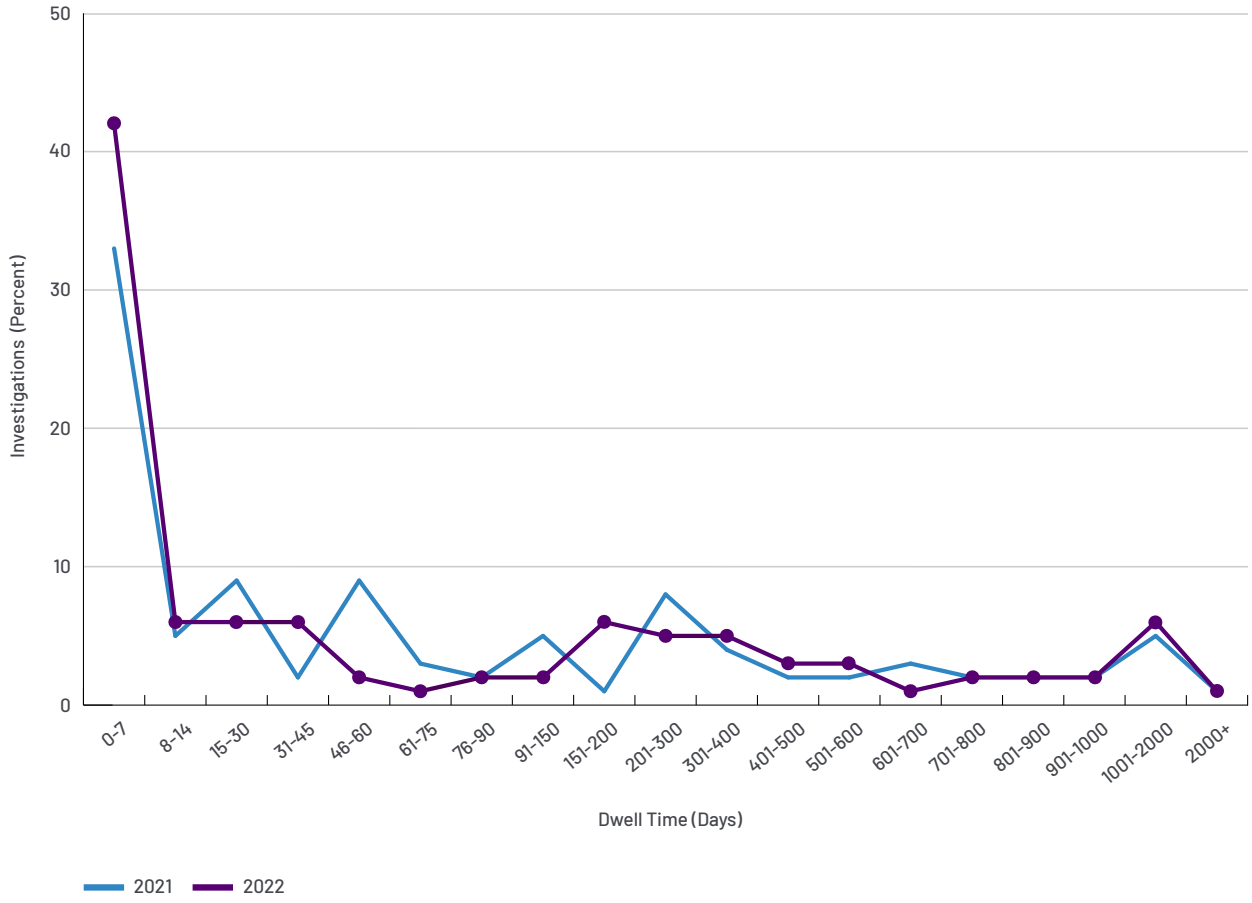
EMEA Median Dwell Time, 2016-2022



EMEA Dwell Time Distribution

Dwell time distribution in EMEA showed that 54% of intrusions investigated by Mandiant were identified within 30 days, with 76% of those intrusions (42% of total EMEA investigations) identified within a week. Organizations in EMEA showed improvement detecting a majority of incidents more quickly. However, the general distribution of intrusions remains consistent with 2021 with 23% of intrusions being identified after a year of initial intrusion.

EMEA Dwell Time Distribution, 2021-2022



Change in EMEA Investigations Involving Ransomware

17% → **7%**

in 2021 in 2022

Change in EMEA Median Dwell Time – Ransomware

4 → **33**

Days in 2021 Days in 2022

Change in EMEA Median Dwell Time – Non-Ransomware

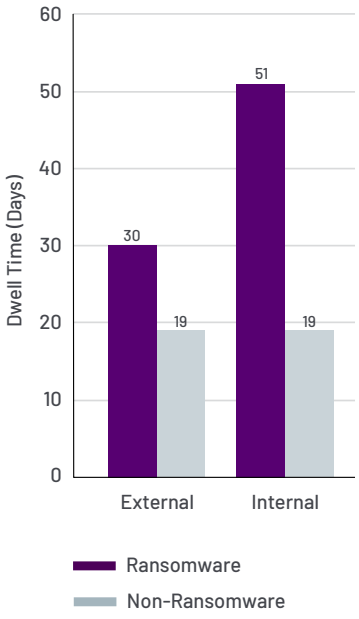
60 → **19**

Days in 2021 Days in 2022

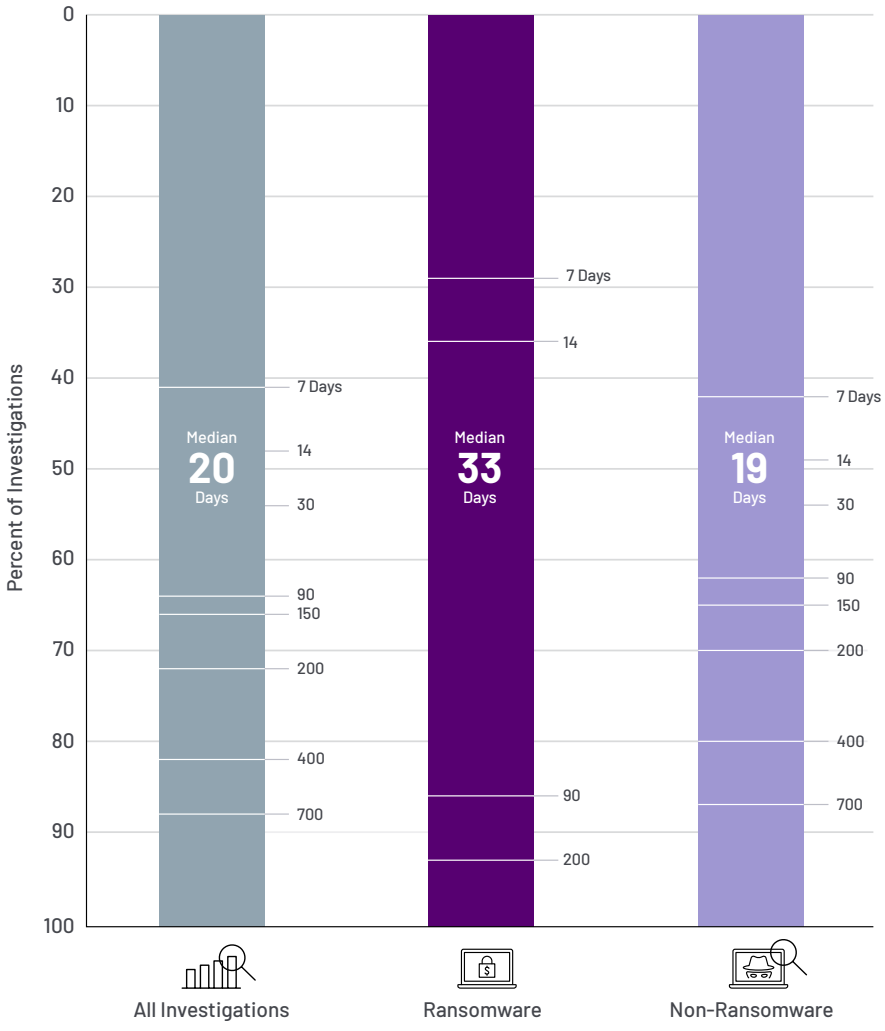
In 2022, Mandiant saw a 10-percentage point decline in EMEA investigations related to ransomware. Additionally, Mandiant noted an increase in the median dwell time for ransomware specific investigations in EMEA to 33 days in 2022, up from just four days in 2021. This means that, in 2022, adversaries leveraging ransomware against organizations in EMEA spent 89% longer in compromised environments before being detected. However, the median dwell time for ransomware related investigations in EMEA in 2021 was exceptionally short, making it unsurprising that this metric reverted in 2022. Organizations were notified by an external entity of a ransomware event faster than they were able to detect the event internally in 2022. Organizations in EMEA were notified by an external entity within 30 days of ransomware related intrusions however, when similar intrusions were identified internally, adversaries remained undetected for 51 days.

Mandiant did see a significant improvement in non-ransomware dwell time. Organizations in EMEA detected non-ransomware intrusions nearly two thirds quicker, with the median dwell time at 19 days in 2022 compared to 60 days in 2021.

EMEA Median Dwell Time by Detection Source



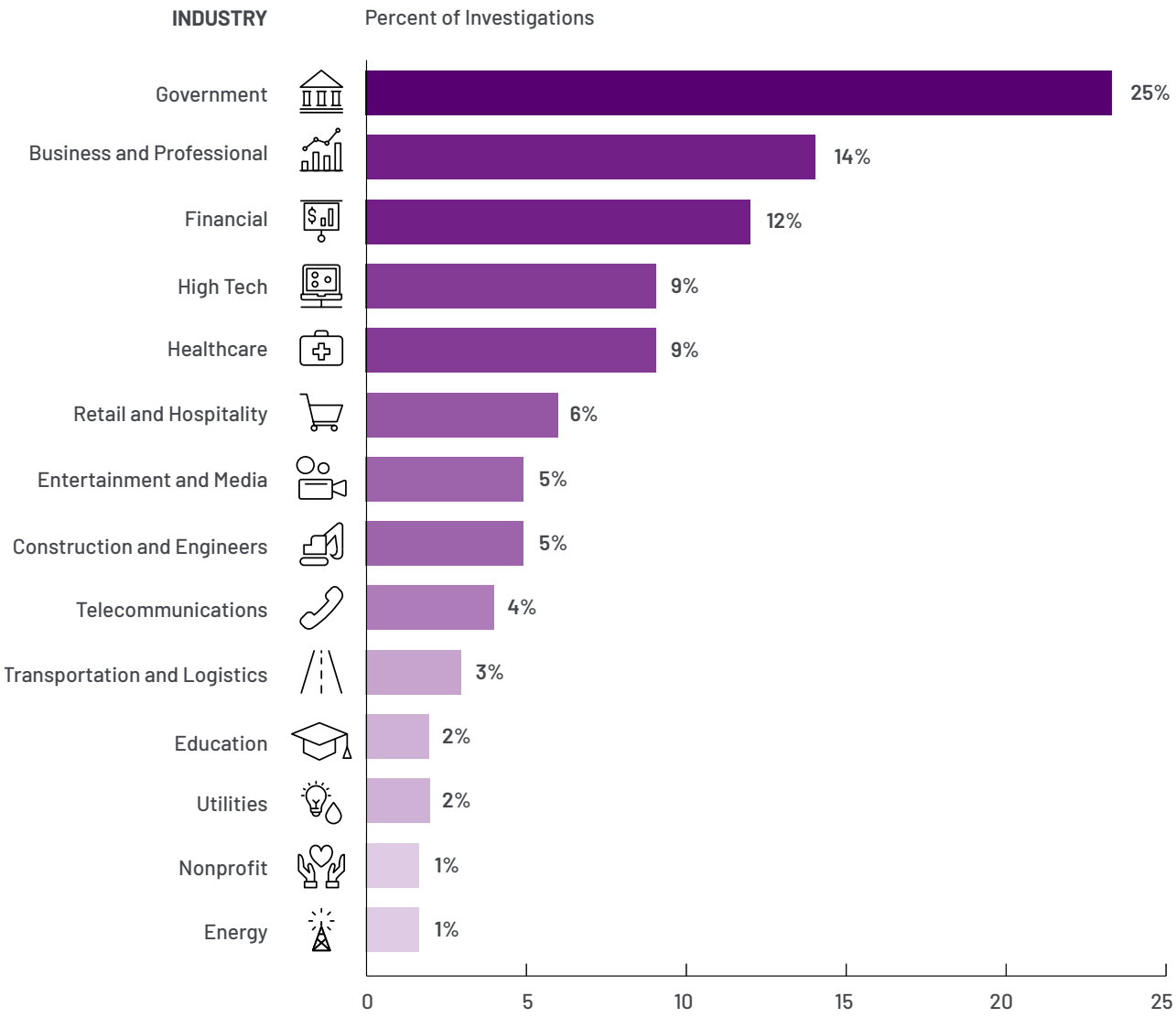
EMEA Dwell Time Investigation by Type, 2022



Industry Targeting

Of the intrusions investigated by Mandiant in 2022, response efforts for government related organizations captured a quarter of all investigations. Compared to 9% in 2021, this primarily reflects the extensive work Mandiant has done in support of Ukraine. The next four most targeted industries from 2022 are consistent with what Mandiant experts observed in 2021. Mandiant observed business/professional services, financial, high tech and healthcare industries to be favored by adversaries. These industries remain attractive targets for both financially and espionage motivated actors.

Global Industries Targeted, 2022



Targeted Attacks

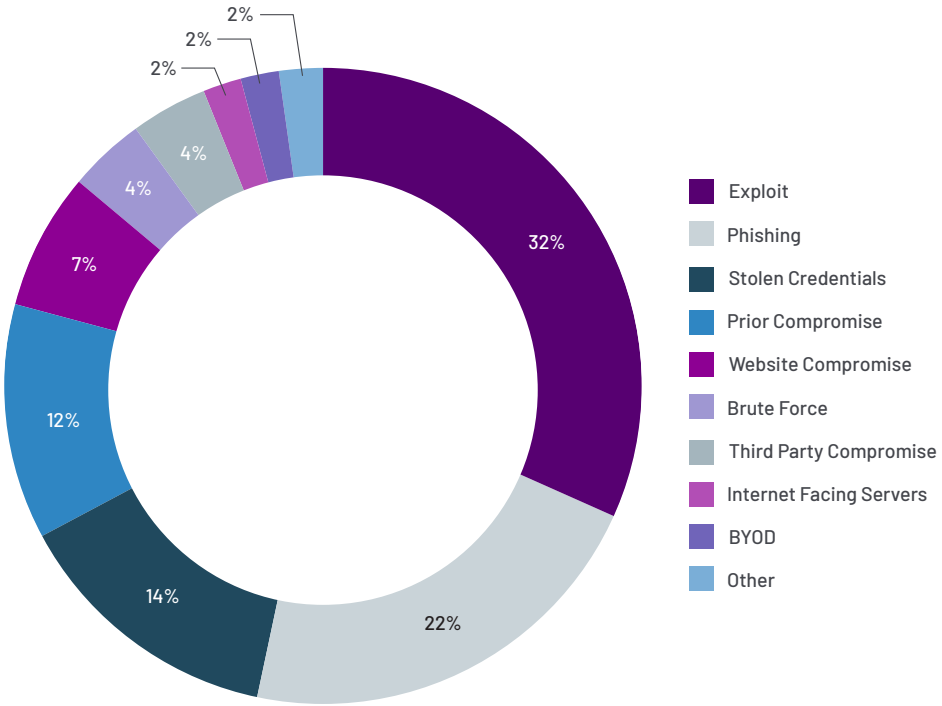
Initial Infection Vector

Exploits continued to be the most leveraged initial infection vector used by adversaries in Mandiant investigations conducted in 2022. In intrusions where the initial infection vector was identified, 32% of intrusions began with an exploit. While this was a decrease from the 37% of intrusions identified in the reporting period of M-Trends 2022, exploits remained a critical tool for adversaries to use against their targets.

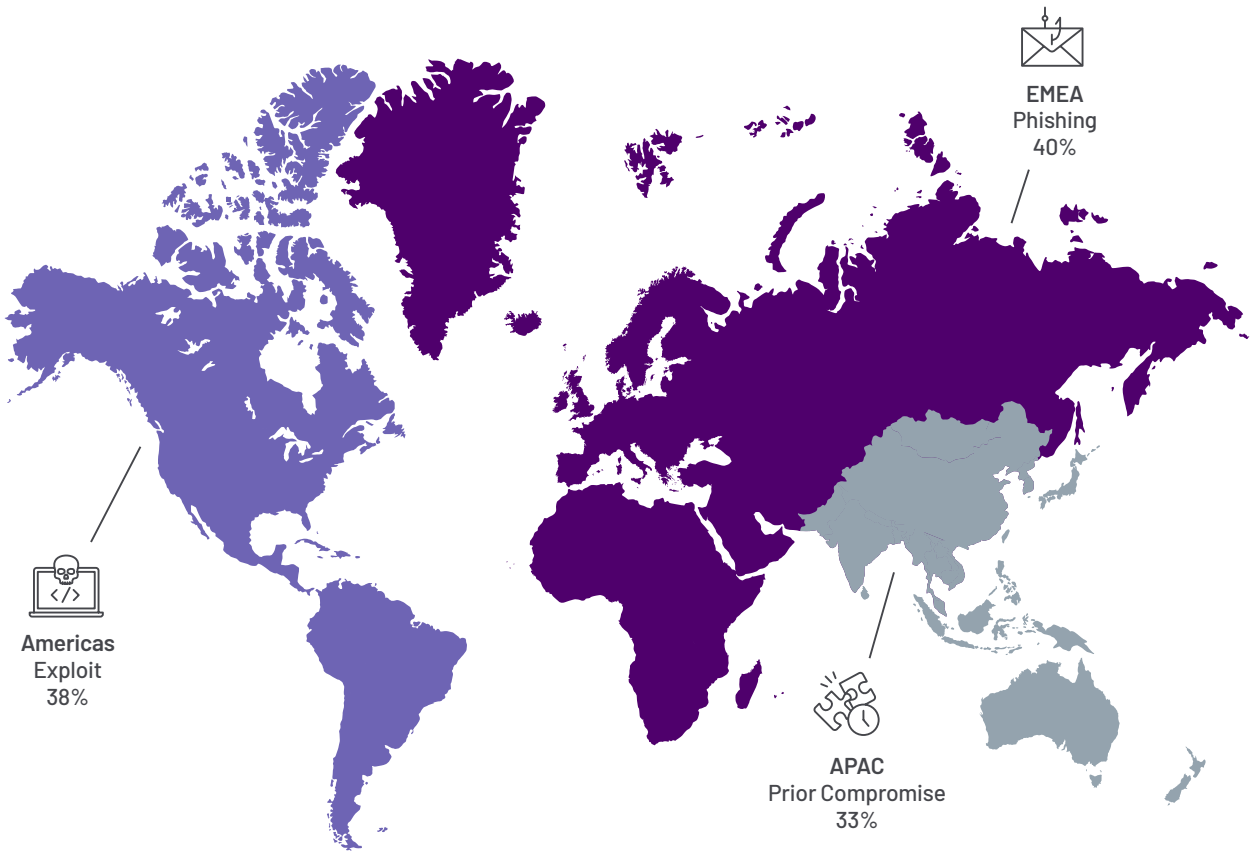
In 2022, phishing returned to the second most utilized vector for initial infection observed in intrusions, representing 22% of intrusions where the initial infection vector was identified. This was an increase from 12% of intrusions seen in 2021. Phishing continues to be a lucrative and mainstay vector for adversaries year over year.

Adversaries leveraged stolen credentials more often in 2022 than 2021 in investigations where the initial infection vector was identified, at 14% and 9% respectively. Mandiant investigations uncovered an increased prevalence in both the use of widespread information stealer malware and credential purchasing in 2022 when compared to previous years. In many cases, investigations identified that credentials were likely stolen outside of the organization's environment and then used against the organization, potentially due to reused passwords or use of personal accounts on corporate devices.

Initial Infection Vector (when identified)

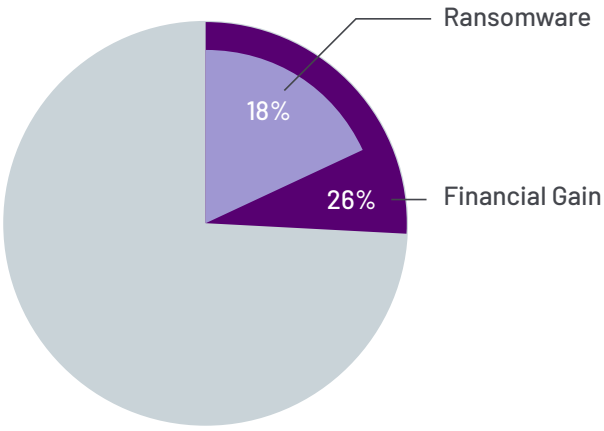


Most Prevalent Initial Intrusion Vector by Region



Regionally, adversaries made use of various vectors to gain access to targeted organizations and complete their missions. In the Americas, in intrusions where initial infection vectors were identified, the use of exploits remained the most leveraged vector at 38% of investigations. Adversaries targeting organizations in APAC used access from a prior compromise to perform their intrusions more often than other vectors by more than 10-percentage points. In EMEA, phishing was leveraged by adversaries in 40% of investigations where an intrusion vector was identified. This variety of vectors used across regions likely indicates that adversaries are not leveraging the same attack paths to accomplish their missions. Adversaries continue to leverage the intrusion vector that is the most effective to gain access to their targets that reside in each region.

Adversary Operations



Financial Gain

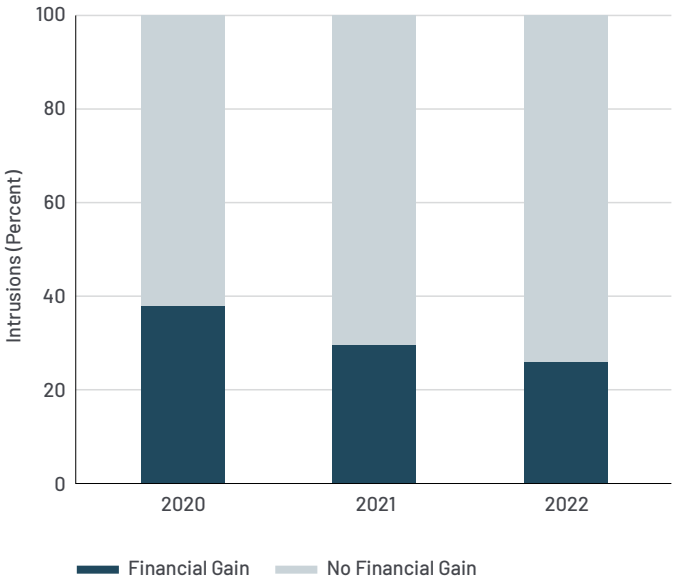
30% → **26%**

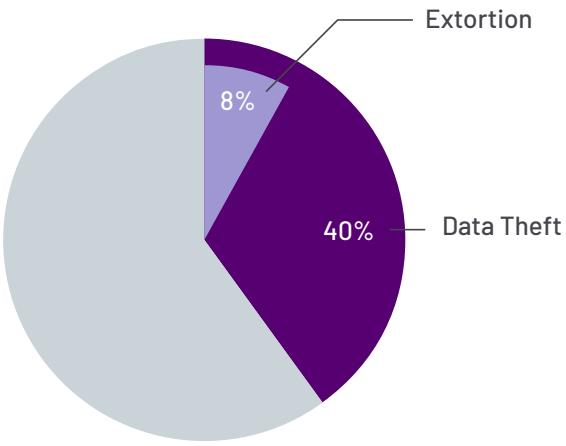
in 2021 in 2022

Mandiant investigations where an adversary was identified seeking financial gain decreased in 2022. However, financially motivated intrusions still comprised over a quarter of intrusions investigated by Mandiant. Of Mandiant investigations in 2022, 26% of intrusions surfaced adversaries seeking monetary gain through extortion, ransomware, sold access, illicit transfers, or payment card theft.

Compared to the reporting period of M-Trends 2022, ransomware related investigations conducted by Mandiant decreased by 5-percentage points. In 2022, 18% of all Mandiant investigations were related to ransomware. This represents the smallest percentage of Mandiant investigations related to ransomware since prior to 2020.

Financial Gain, 2020-2022





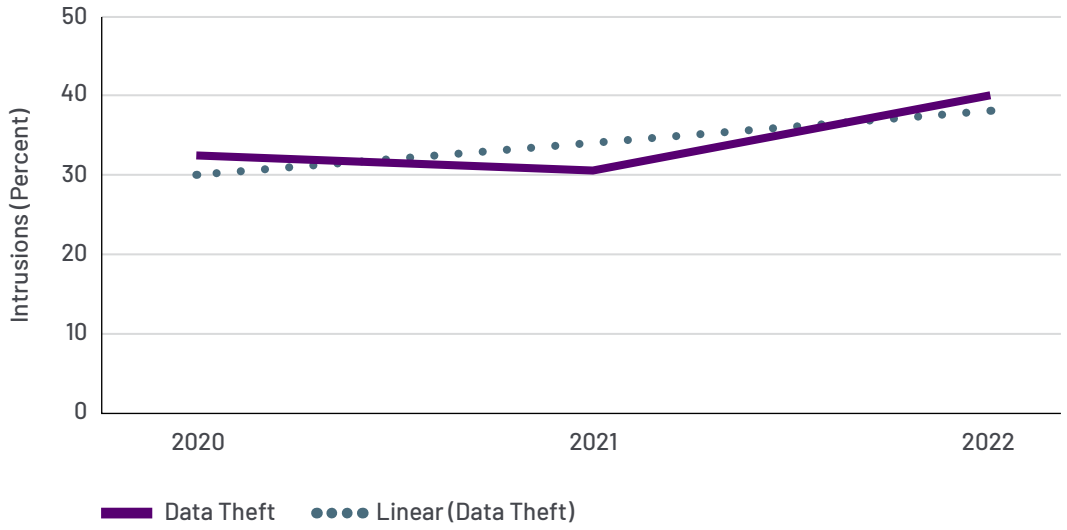
Data Theft

29% → **40%**

in 2021 in 2022

Mandiant experts identified that in 40% of intrusions in 2022, adversaries prioritized data theft. Mandiant defenders have observed threat actors attempting to steal, or successfully completing data theft operations, more often in 2022 compared to previous years. In 19% of those intrusions (8% of all intrusions) the data stolen was used by the threat actor during negotiations for payment. Mandiant continues to observe threat actors performing data theft operations for numerous goals. However, adversaries were observed prioritizing data theft that likely indicates intellectual property theft or espionage related end goals in 22% of investigations. The continued increase of observed data theft likely indicates that organizations are improving their ability to detect data theft operations, allowing investigators to conduct more complete investigations.

Data Theft Observed, 2020-2022



Compromised Architecture

4% → **6%**

in 2021 in 2022

Modus Operandi

Mandiant experts continue to see a small uptick in the occurrence of opportunistic compromise being leveraged as a source of targeted attack activity. Campaigns of broad scale non-targeted activity have, in some cases, translated into targeted attack activity as access to compromised environments is sold to targeted threat actors or critical information gathered during the attack is leveraged to accomplish the goals of targeted attackers.

In 2022, Mandiant experts identified this activity in 6% of intrusions compared to 4% in 2021 and 3% in 2020. As the use of exploits continues to rise, it is no surprise that use of compromised architecture is also increasing. As proof of concept (POC) code is made available for newly identified exploits, the ability to automate compromise increases. This shorter cycle from POC to widespread attack allows actors to gain quick wins which in turn provide necessary infrastructure for additional non-targeted attacks.

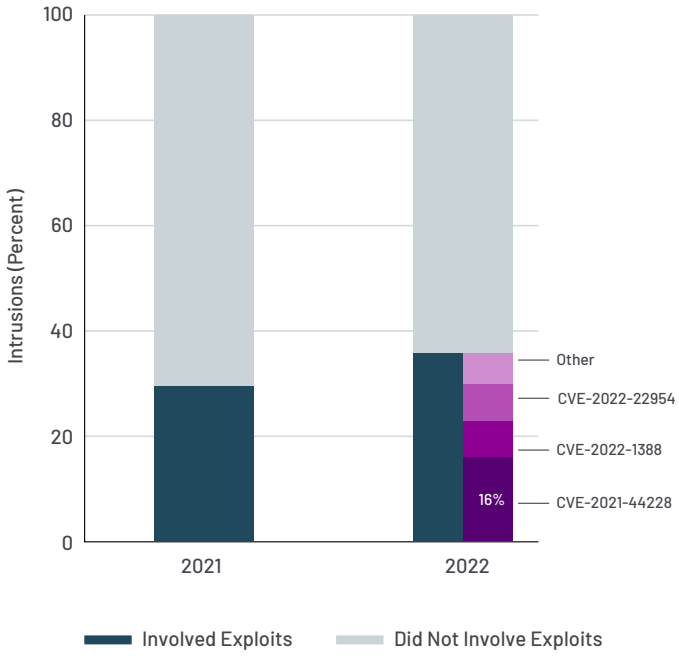
Of the Mandiant investigations where compromised architecture was observed, roughly 60% of the intrusions resulted in some type of crypto-mining activity. In the remaining nearly 40% of these intrusions, the architecture was leveraged for actions, including ongoing spam and/or phishing operations, as well as to further the distribution of botnets. Similar to previous years, intrusions related to insider threats made up 1% of Mandiant investigations in 2022.

Exploit Activity in 2022

Adversaries are still making use of exploits to conduct their operations. Mandiant observed evidence of successful exploit activity of at least one exploit against a vulnerability in 36% of investigations in 2022 compared to 30% of investigations from 2021. Mandiant continues to observe adversaries leveraging exploits to initiate and continue intrusions. Perimeter devices that are accessible via the internet - including firewalls, virtualization solutions and virtual private network devices - remain a highly sought after target for attackers.

Across all investigations where a vulnerability was targeted, abuse of the Log4j[1] vulnerability represented 16% of investigations. The second and third most notable vulnerabilities identified were related to F5 Big-IP[2] and VMware Workspace ONE Access and Identity Manager[3].

Exploit Activity When Identified



Multiple Threat Groups Identified (per environment)

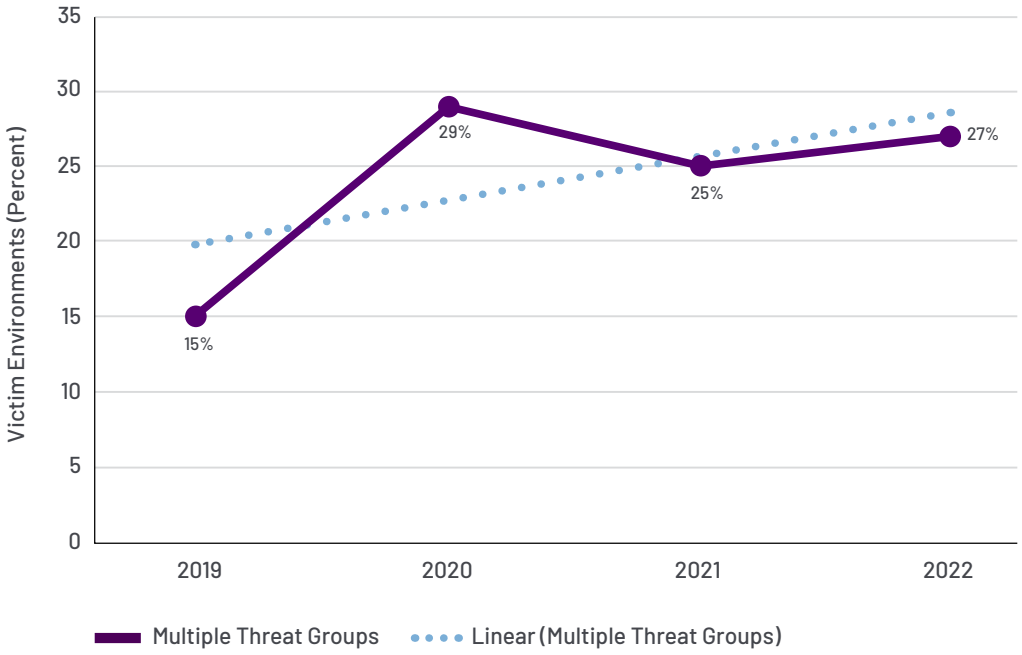
25% → **27%**

in 2021 in 2022

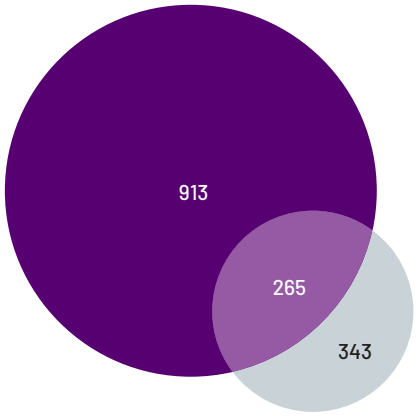
Environment

In more than a quarter of investigations, Mandiant experts identified multiple threat groups within the same environment. During these investigations, Mandiant observed threat groups working together to accomplish a central goal as well as instances where the target environment was enticing to multiple threat actors independently. The percentage of investigations where multiple threat actors were identified in 2022 increased to a similar percentage that was observed in 2020. This trend remains volatile, however Mandiant has observed a general rise in multiple threat groups identified in the same environment over the past four years.

Multiple Threat Groups Identified



Threat Groups



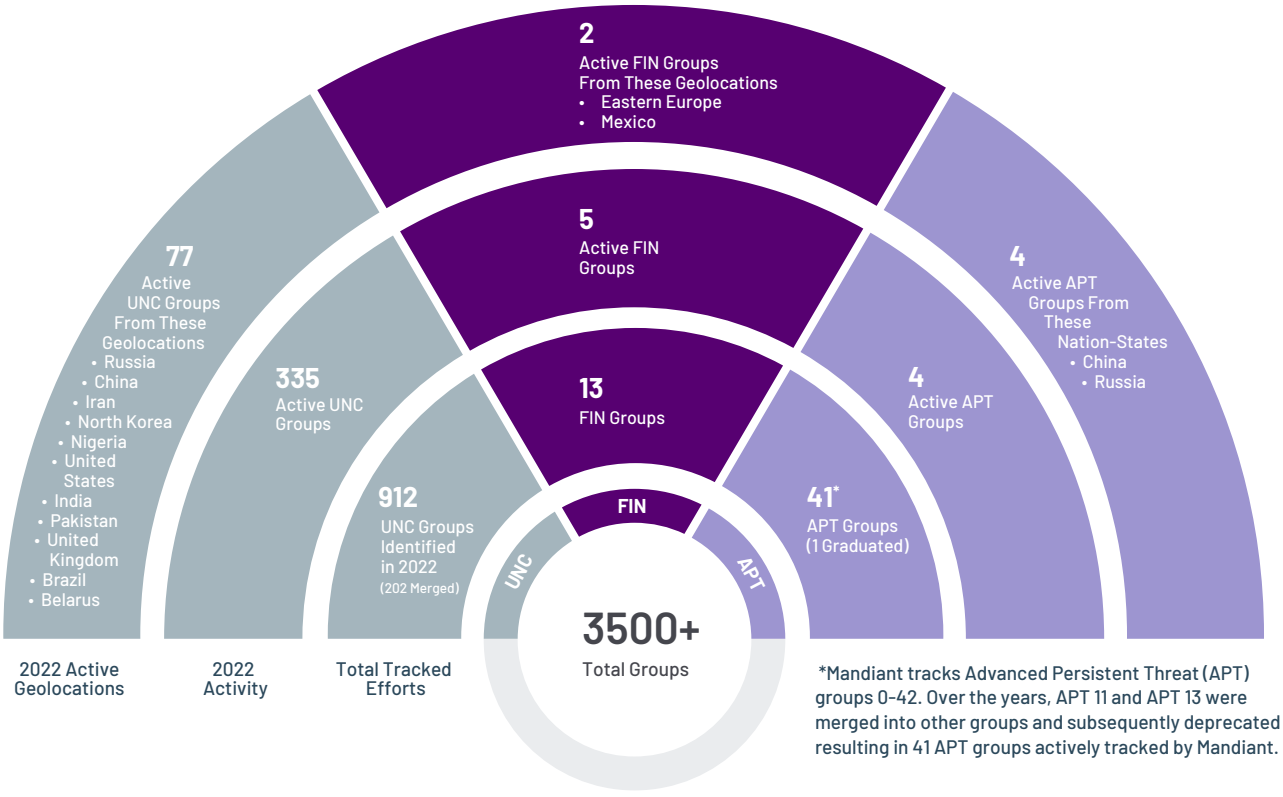
Newly Tracked Threat Groups

Newly Tracked and Observed Threat Groups

Observed Threat Groups

Mandiant tracks more than 3500 threat groups, including 900+ newly tracked threat groups in this M-Trends reporting period. Of the newly tracked groups, 265 threat groups were first identified during Mandiant investigations in 2022. Mandiant identified a total of 343 unique threat groups across all intrusions in 2022. Organizations faced intrusions by four named Advanced Persistent Threat (APT) groups. This includes government sponsored groups from China and Russia, five named financially motivated threat (FIN) groups, and 335 uncategorized threat (UNC) groups. Overall, organizations are still facing and responding to well-established threat groups while also contending with newly attributed groups.

Threat Groups 2022



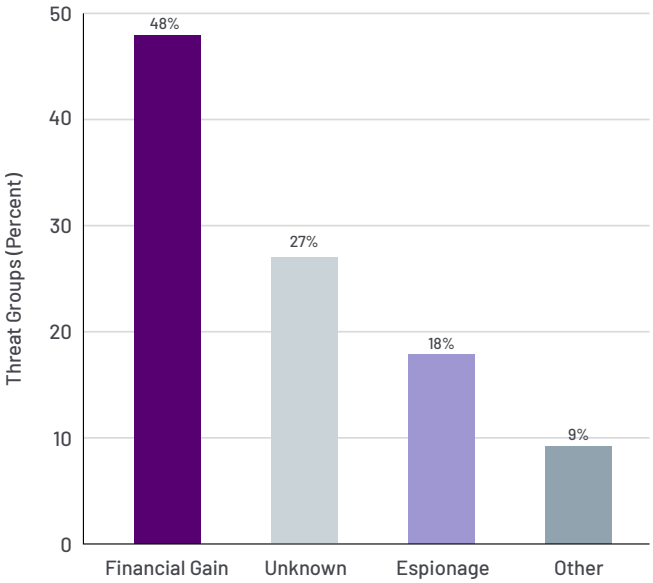
*Mandiant tracks Advanced Persistent Threat (APT) groups 0-42. Over the years, APT 11 and APT 13 were merged into other groups and subsequently deprecated resulting in 41 APT groups actively tracked by Mandiant.

Destructive Operations – The threat group's assessed goal is to destroy or damage a target's infrastructure, such as DDoS or a destructive ICS attack.

Hacktivism – The threat group's assessed goal is defamation, to obtain press, and/or to influence policy.

Nuisance – The threat group's assessed goal is to obtain access and propagate through the victim environment such as botnets and spam.

Observed Threat Groups by Goal, 2022

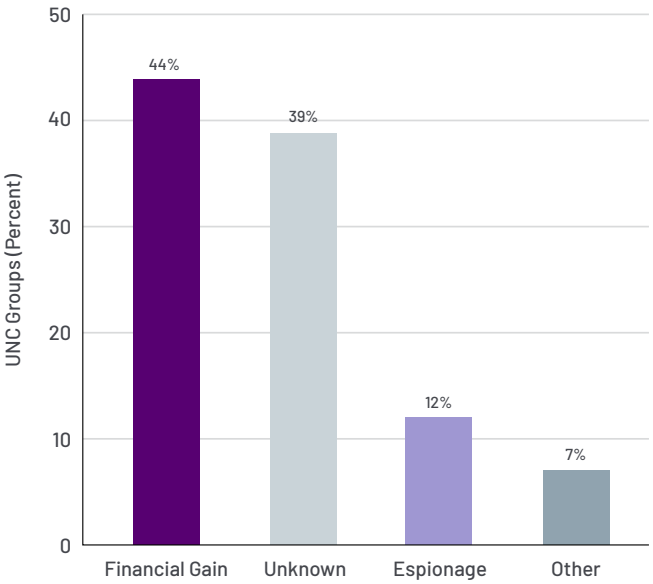


These threat groups are clusters of cyber activity that include artifacts such as adversary infrastructure, tools, and tradecraft. When a threat grouping is first created, Mandiant assesses a primary goal for the group. As our knowledge of a threat grouping becomes sufficiently mature, in-depth research aids in assigning a formal designation based on established Mandiant naming conventions.

Of all threat groups observed in 2022, Mandiant assessed that 48% of these threat groups to have financially motivated operations, 18% with espionage related motivations and 9% with other motivations like, destructive operations, hacktivism, and being a nuisance. In the remaining 27% of threat groups, the motivation was not able to be assessed. This is often because the adversary was detected before they were able to complete their mission or direct evidence was not uncovered to establish a credible goal.

Of the active groups in 2022, 335 of the threat groups, which Mandiant tracks as uncategorized (UNC) groups, were observed in intrusions. Mandiant assesses that 44% of these threat groups were motivated by financial gain and 12% were motivated by espionage related actions. Notably, these UNC groups can have more than one motivation. In order to continuously refine our understanding of these threat groups and their activity, Mandiant continuously analyzes adversary actions from frontline investigations in order to generate and integrate actionable intelligence across all Mandiant products and services. Through this work, as well as analysis of public reporting, information sharing and other research, Mandiant continues to expand its threat actor knowledge base through continuous clustering and merging.

Observed Threat Groups by Goal, 2022



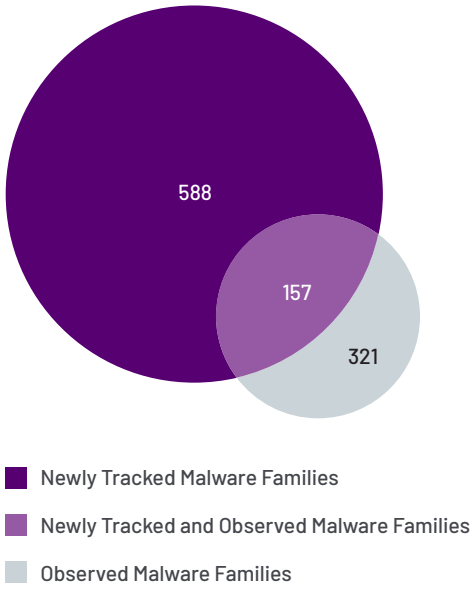
In 2022, Mandiant graduated one group to a named threat group, APT42, and merged 202 threat groups into other threat groups based on extensive research into activity overlaps. For details on how Mandiant defines and references UNC groups and merges, please see "How Mandiant Tracks Uncategorized Threat Actors."[4]

Malware

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

In 2022, Mandiant began tracking 588 new malware families to increase its knowledge base of malware. Compared to the 700+ newly tracked malware reported in the reporting period for M-Trends 2022 which covers 15 months, Mandiant's newly tracked malware equates to roughly 49 new malware families identified each month in 2022, compared to 45 new families a month in 2021. This may indicate that adversaries are continuing to expand their toolsets at a similar rate compared to previous years.

Of these new malware families, 157 families were observed in intrusions investigated by Mandiant. This represents a little less than half of the total number of malware families, 321, seen in Mandiant investigations. This indicates that while adversaries continue to deploy new tools, previously observed malware families still make up a significant portion of their arsenal.



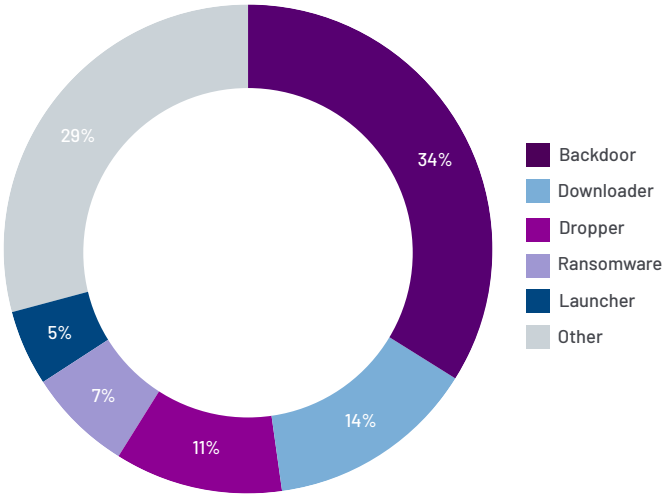
A **malware category** describes a malware family's primary purpose. Each malware family is assigned only one category that best describes its primary purpose, regardless of functionality for more than one category.

New Malware Families by Category

Of the 588 newly tracked malware families, the top five categories consisted of backdoors (34%), downloaders (14%), droppers (11%), ransomware (7%) and launchers (5%). These categories of malware remain consistent over the years and backdoors continue to represent slightly over one third of the newly tracked malware families. Newly tracked credential stealers fell out of the top five categories tracked by Mandiant in 2022. Considering that stolen credentials appeared for the first time in the most frequently seen intrusion vectors, this seems to suggest that threat actors are leveraging previously created credential stealers to obtain stolen credentials.

Malware Category	Primary Purpose
Backdoor	A program whose primary purpose is to allow a threat actor to interactively issue commands to the system on which it is installed.
Credential Stealer	A utility whose primary purpose is to access, copy or steal authentication credentials.
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 victim in order to avoid or undo the malicious action.
Tunneler	A program that proxies or tunnels network traffic.
Other	Includes all other malware categories such as utilities, keyloggers, point-of-sale (POS), tunnelers and data miners.

Newly Tracked Malware Families by Category, 2022

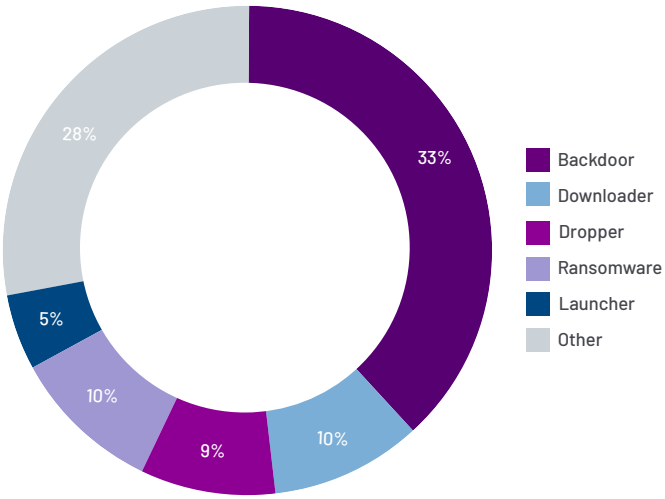


An **observed malware family** is a malware family identified during an investigation by Mandiant experts

Observed Malware Families by Category

Mandiant experts observed 321 unique malware families in intrusions over the course of 2022. Backdoors remain a mainstay for threat groups, with threat actors using malware with backdoor capabilities in 33% of Mandiant investigations. Comparatively to 2021, this is a 7-percentage point decrease, however malware families with backdoor capabilities are still observed in vastly more investigations than the next most seen capability type. The next categories show a small variance in order compared to 2021, with downloaders (10%), ransomware (10%), droppers (9%) and launchers (5%) to round out the top five.

Observed Malware Families by Category, 2022



Backdoors

40% → **33%**

in 2021 in 2022

Ransomware

10% → **10%**

in 2021 in 2022

Launcher

4% → **5%**

in 2021 in 2022

Other

22% → **28%**

in 2021 in 2022

Downloaders

7% → **10%**

in 2021 in 2022

Dropper

12% → **9%**

in 2021 in 2022

Tunneler

4% → **5%**

in 2021 in 2022

Usage of unique ransomware families in investigations between 2021 and 2022 remained relatively stable. While the percentage of ransomware intrusions has decreased, adversaries are still leveraging similar percentages of distinct ransomware malware families to carry out their missions for financial gain.

The use of unique downloaders increased 3-percentage points in 2022 from the 7% of investigations observed in 2021. Meanwhile, the use of unique droppers decreased by the same amount, from 12% observed in 2021 to 9% observed in 2022. The use of unique malware that provide tunneling capabilities which increased from 4% could likely also be a contributing factor to the decrease in unique droppers and backdoors across missions.

Notably, credential stealers fall off the top five observed malware families by category list in 2022, despite the use of stolen credentials appearing in the initial infection vector top five. However, Mandiant observed an explosion of credential and information stealer type malware, such as REDLINESTEALER, VIDAR and RECORDSTEALER to name a few delivered through abuse of search engine optimization (SEO) and malicious advertisements. Mandiant also observed that the usage of other types of malware may indicate that adversaries are becoming more flexible with tooling to accomplish missions.

RECORDSTEALER, aka Raccoon Stealer V2 (Sekoia), Record Stealer (AhnLab), and RecordBreaker (Proofpoint), is a credential stealer written in C with the capability to obtain sensitive data from common web browsers, crypto wallets and be configured as a downloader.

REDLINESTEALER, aka RedLine (Minerva Labs and Proofpoint), and Redlinestealer (Fortinet), is a credential stealer malware that is capable of stealing credentials from web browsers, files, FTP applications and cryptocurrency wallets. It also collects extensive system survey information such as the basic hardware specifications, desktop screenshot, username, OS, language, geographic location, installed software, process listing and Global IP address. The malware can download and launch additional payloads or launch a hidden command shell for the attacker. Redline Stealer has been advertised for sale on hacking forums.

VIDAR, aka Mosaicloader (Bitdefender), is a data miner written in C++ that targets data from multiple web browsers, cryptocurrency wallets, chat software, the Authy two-factor authentication utility, and various other applications. Collected data is compressed and uploaded to a remote server using HTTP. VIDAR appears to be based on a similar data miner named ARKEI.

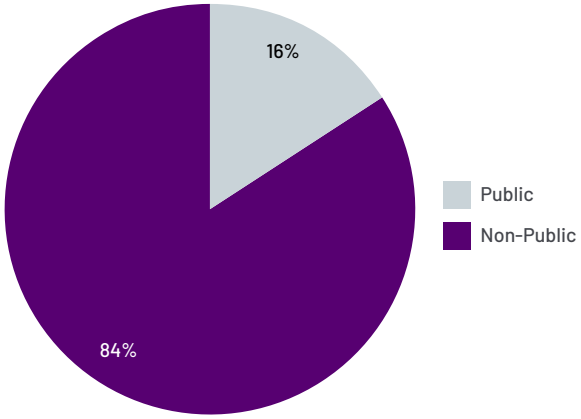
A **publicly available tool** or **code family** is readily obtainable without restriction. This includes tools that are freely available on the Internet, as well as tools that are sold or purchased, as long as they can be purchased by any buyer.

A **non-public tool** or **code 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.

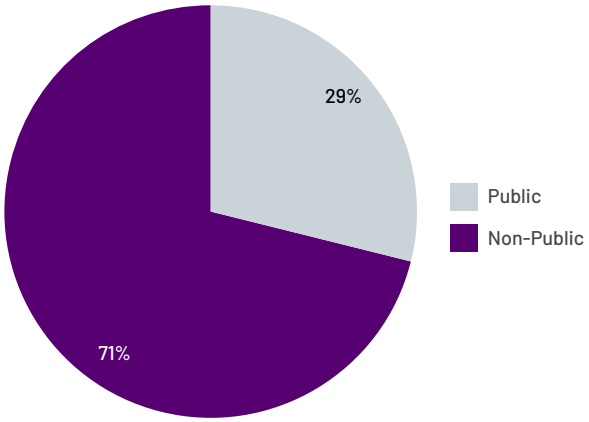
Malware by Availability

Availability of both newly tracked and observed malware families remains consistent year over year. In both categories, malware families were more often privately developed or had restricted availability. Mandiant noted that 29% of malware families used during an intrusion were publicly available, which is a 1-percentage point increase from 28% in 2021. While adversaries continue to make use of a wide variety of non-publicly available malware and develop malware to achieve their goals per target environment, many adversaries continue to use the same publicly available malware families (e.g. BEACON).

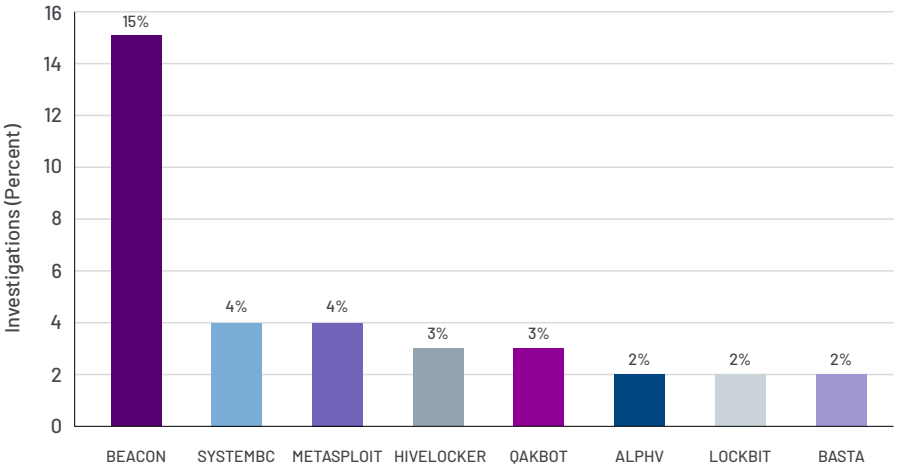
Newly Tracked Malware Families by Availability, 2022



Observed Malware Families by Availability, 2022



Most Frequently Seen Malware Families, 2022



Consistent with previous years, the most common malware family identified by Mandiant in investigations was BEACON. BEACON was identified at 15% of all intrusions investigated by Mandiant and remains by far the most seen in investigations across regions. It has been used by a wide variety of threat groups tracked by Mandiant including state backed threat groups attributed to China, Russia and Iran, as well as financially motivated threat groups including FIN6, FIN7, FIN9, FIN11 and FIN12, and over 700 hundred UNC groups. This ubiquity is likely due to the common availability of BEACON combined with the malware's high customizability and ease of use.

While the overall usage of BEACON in 2022 is still the most notable, it is more than a 10-percentage point decrease in usage compared to 2021, which makes it the smallest percentage of observed BEACON activity in recent years. Use of BEACON across intrusions was captured in 28% of all of intrusions in 2021 and 24% in 2020.

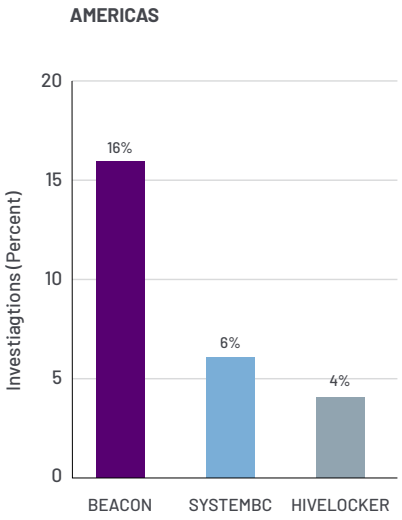
The second and third most common malware families observed were SYSTEMBC and METASPLOIT. These malware families provide adversaries similar capabilities to BEACON, however with various limited capabilities. The use of malware that acts as a tunneler increased in 2022. This likely reflects the increased usage of malware like SYSTEMBC which is used heavily by actors who deploy ransomware. In 2022, Mandiant observed four distinct ransomware families emerge as a formidable threat to organizations. Mandiant observed that ransomware families such as HIVELOCKER, ALPHAV, LOCKBIT and BASTA, make up a majority of ransomware related intrusions.

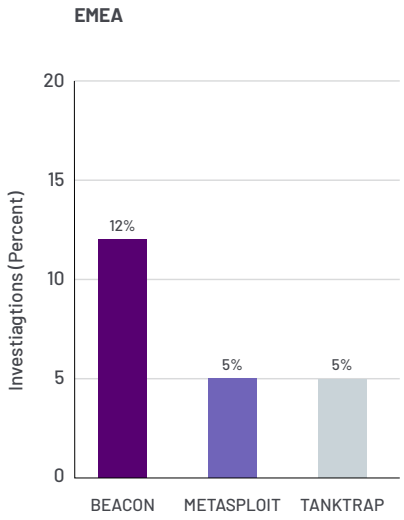
While intrusions related to ransomware decreased, Mandiant also observed a general decrease in the volume of organizations added to data leak sharing sites related to ransomware families tracked in 2022 compared to that of 2021. Of the most prevalent and destructive ransomware families, Mandiant observed a nearly 10% decrease in organizations added to ransomware data leak sites related to ransomware families such as LOCKBIT, ALPHV, BASTA, CONTI and HIVELOCKER.

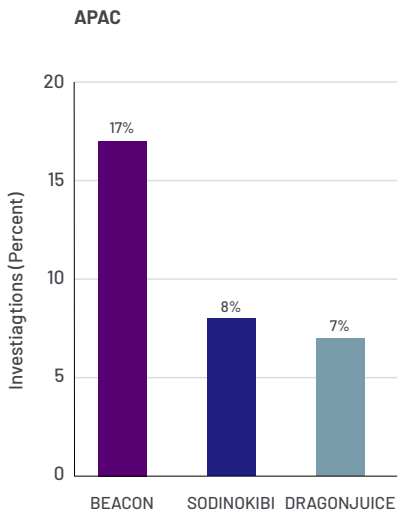
In 2022, Mandiant observed the LOCKBIT data leak sharing sites captured the most change compared to posts in 2021. Mandiant also assesses that with the CONTI group disruption in early 2022, former affiliates began using other ransomware families such as BASTA, ROYALLOCKER and HIVELOCKER to carry out their operations. This likely explains the wider assortment of ransomware families in use in 2022 compared to 2021.

Regional Breakdown

While BEACON was the most frequently seen malware family across all regions, the next most popular malware families varied regionally. In the Americas, SYSTEMBC and the cross-platform HIVELOCKER ransomware were seen most frequently after BEACON. In APAC, SODINOKIBI ransomware and the reconnaissance tool DRAGONJUICE were most common. In EMEA, METASPLOIT and the PowerShell utility TANKTRAP rounded out the top three. Over the years, Mandiant has observed increasing regional variation in common malware families as adversaries progressively specialize in their missions.







Malware Definitions

BEACON is a backdoor that is commercially available as part of the Cobalt Strike software platform and commonly used for penetration testing network environments. The malware supports several capabilities, such as injecting and executing arbitrary code, uploading and downloading files and executing shell commands. 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 750 UNC groups.

SYSTEMBC is 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 SYSTEMBC used by FIN12 and as more than 20 UNC groups with goals related to financial gain.

METASPLOIT is a penetration testing platform that enables users to find, exploit, and validate vulnerabilities. Mandiant has seen METASPLOIT used by APT28, APT35, APT40, APT41, FIN6, FIN7, FIN11, FIN12, FIN13 and 152 UNC groups with end goals ranging from espionage and financial gain to penetration testing.

HIVELOCKER is a ransomware family that has impacted Windows and Linux operating systems. It was originally written in GoLang, however was rewritten in Rust in early 2022. It can encrypt both logical drives and remote network shares. On execution, the ransomware will parse command-line arguments that specify its behavior, such as processes to terminate and services to stop prior to encryption. HIVELOCKER can skip files based on file size, filename, or file extension specified in a command line argument during the encryption process. Mandiant tracks more than 15 UNC groups associate with the distribution or usage of HIVELOCKER ransomware.

QAKBOT is a backdoor written in C/C++ that implements a plug-in framework to extend its capabilities via embedded and downloaded plugins that provide capabilities such as keylogging, file transfer, and file execution. QAKBOT also targets credentials by intercepting browser activity, injecting malicious code into browser sessions, and extracting credentials stored by browsers, email clients, and FTP clients. QAKBOT is capable of propagating to other systems on a network via SMB and setting up port forwarding on a connected router via the UPnP protocol. Mandiant has seen QAKBOT used by more than 20 UNC groups including distribution clusters that have provided access for the usage of BASTA ransomware.

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

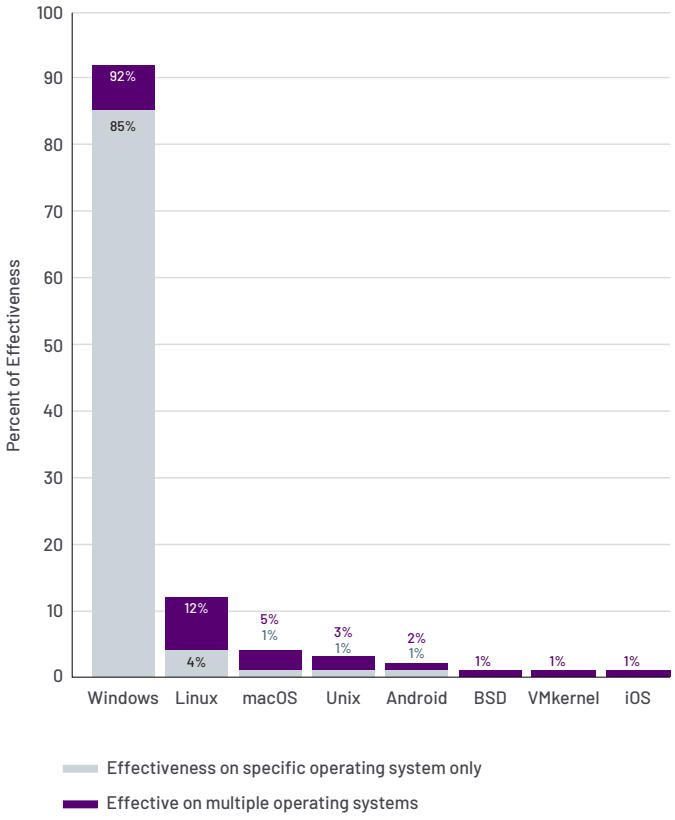
Operating System Effectiveness

In line with previous M-Trends reports, malware effective on Windows was by far the most common newly tracked and observed malware, with 92% of the newly identified malware families and 93% of observed malware able to run on Windows. Compared to 2021, Mandiant observed relatively stable usage of newly tracked malware effective on the Linux platform in 2022 with a slight decrease in observed malware, 15% of observed malware was effective on Linux, compared to 18% in 2021.

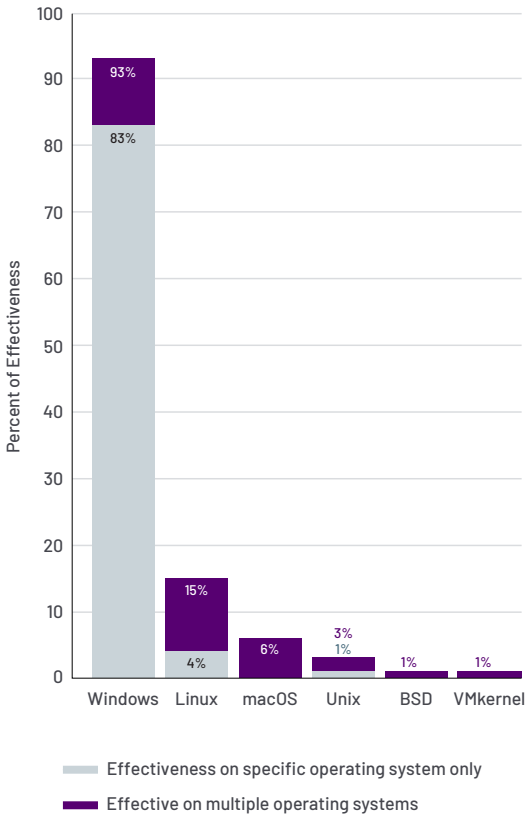
Similarly, compared to previous years, Mandiant has observed adversaries making use of malware families that are effective on one or more operating systems more often than leveraging malware that is designed to focus on one operating system. In instances where malware is effective on only one operating system, it will likely target the Windows OS.

This year marks the first time Mandiant highlights malware effective on the VMWare created operating system, VMkernel. While the general volume of malware effective on this operating system is not significant, this is notable for defenders due to the prevalence of VMWare architecture, specifically ESXi hosts. These types of operating systems do not have significant capability for Endpoint Detection and Response (EDR) tool monitoring. As a result, monitoring and investigations into the platform can be challenging for defenders.

Operating System Effectiveness of Newly Tracked Malware Families, 2022



Operating System Effectiveness of Observed Malware Families, 2022



Threat Techniques

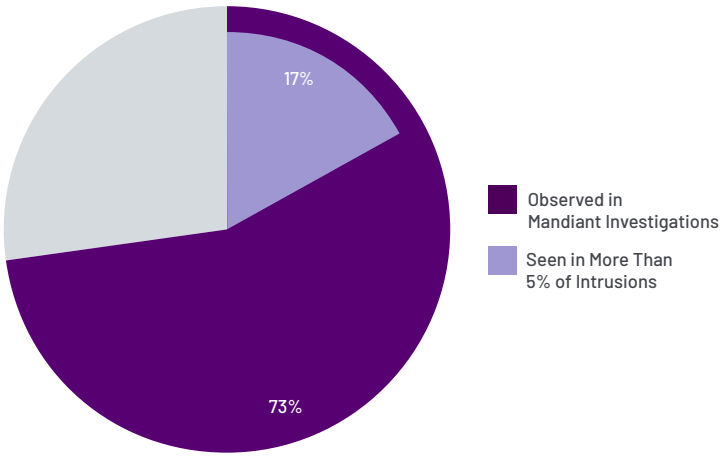
MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, government and the cyber security product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

Mandiant continues to support the community by mapping its findings to the MITRE ATT&CK framework. Organizations should prioritize which security measures to implement based on the likelihood of a specific technique being used during an intrusion. Mandiant has mapped an additional 150 Mandiant techniques to the updated MITRE ATT&CK framework, bringing the total to 2300+ Mandiant techniques and subsequent findings associated with the ATT&CK framework. In 2022, the MITRE ATT&CK Framework was updated to version 12 resulting in ATT&CK for Enterprise now containing 193 techniques and 401 sub-techniques.

Mandiant provides metrics around most observed techniques used by observed adversaries as a resource to organizations as they make decisions on how to further improve their detection capabilities. Prioritizing the detection of the most leveraged techniques can help organizations build a solid foundation on the way to creating a stronger security ecosystem.

Mandiant observed 73% of MITRE ATT&CK techniques in investigations in 2022 compared to 70% of techniques during the last M-Trends reporting period. In 2022, 71% of the techniques observed (17% of all techniques) were seen in more than 5% of intrusions, compared to 43% of techniques observed (30% of all techniques) in 2021. This convergence in the techniques commonly used by adversaries underscores the defensive value from prioritizing implementation of security measures to protect against the most commonly used techniques. Only a small number of techniques had high prevalence, with just 4.3% of observed techniques (1% of all techniques) seen in over 30% of intrusions. Notably, the highest frequency techniques remain consistent with what Mandiant observed in 2021, indicating enduring defender value from efforts to detect and mitigate their use.

MITRE ATT&CK Techniques Used Most Frequently, 2022



In half of the investigations conducted by Mandiant in 2022, adversaries leveraged a command or scripting interpreter to further intrusions (T1059) with 65% of those cases (one third of all intrusions) involving the use of PowerShell (T1059.001). Mandiant also continues to observe frequent use of web protocols (T1071.001) and Remote Desktop (T1021.001) across intrusions, indicating that adversaries continue to depend heavily on the organization's existing technologies in their operations. These sub-techniques have been in the top five for the past three years. However, this could indicate that detection for these techniques has continued to improve and other evidence sources have been prioritized to capture evidence of additional techniques.

Top 10 Most Frequently Seen Techniques

1.	T1059: Command and Scripting Interpreter	**50.9%**
2.	T1027: Obfuscated Files or Information	**43.5%**
3.	T1071: Application Layer Protocol	**33.1%**
4.	T1082: System Information Discovery	**31.6%**
5.	T1070: Indicator Removal	**31.5%**
6.	T1083: File and Directory Discovery	**29.5%**
7.	T1140: Deobfuscate/Decode Files or Information	**27.3%**
8.	T1021: Remote Services	**26.4%**
9.	T1105: Ingress Tool Transfer	**24.9%**
10.	T1543: Create or Modify System Process	**24.7%**

Top 5 Most Frequently Seen Sub-Techniques

1.	T1059.001: PowerShell	**33.2%**
2.	T1070.004: File Deletion	**25.2%**
3.	T1071.001: Web Protocols	**24.3%**
4.	T1569.002: Service Execution	**21.8%**
5.	T1021.001: Remote Desktop Protocol	**20.3%**

MITRE ATT&CK Techniques Related to Mandiant Targeted Attack Lifecycle, 2022

Mandiant's Targeted Attack Lifecycle is the predictable sequence of events cyber attackers use to carry out their attacks. For more information: https://www.mandiant.com/resources/targeted-attack-lifecycle

Initial Reconnaissance

Reconnaissance

T1595: Active scanning	**1.3%**	T1595.002: Vulnerability Scanning	**0.5%**
		T1595.001: Scanning IP Blocks	**0.5%**
		T1595.003: Wordlist Scanning	**0.2%**

Resource Development

T1608: Stage Capabilities	**8.8%**	T1608.003: Install Digital Certificate	**6.0%**
		T1608.005: Link Target	**2.7%**
		T1608.002: Upload Tool	**0.5%**
		T1608.004: Drive-by Target	**0.2%**
		T1608.001: Upload Malware	**0.2%**
T1583: Acquire Infrastructure	**7.5%**	T1583.003: Virtual Private Server	**7.5%**
T1584: Compromise Infrastructure	**3.5%**		
T1587: Develop Capabilities	**2.6%**	T1587.003: Digital Certificates	**1.3%**
		T1587.002: Code Signing Certificates	**1.3%**
T1588: Obtain Capabilities	**2.2%**	T1588.003: Code Signing Certificates	**1.6%**
		T1588.004: Digital Certificates	**0.5%**
T1585: Establish Accounts	**0.2%**	T1585.002: Email Accounts	**0.2%**

Initial Compromise

Initial Access

T1190: Exploit Public-Facing Application	**21.2%**		
T1566: Phishing	**16.5%**	T1566.001: Spearphishing Attachment	**8.2%**
		T1566.002: Spearphishing Link	**3.7%**
		T1566.003: Spearphishing via Service	**0.2%**
T1133: External Remote Services	**12.6%**		
T1078: Valid Accounts	**9.3%**		
T1189: Drive-by Compromise	**4.6%**		
T1199: Trusted Relationship	**2.4%**		
T1091: Replication Through Removable Media	**1.5%**		
T1200: Hardware Additions	**0.4%**		
T1195: Supply Chain Compromise	**0.2%**	T1195.002: Compromise Software Supply Chain	**0.2%**

Establish Foothold

Persistence

T1543: Create or Modify System Process	**24.9%**	T1543.003: Windows Service	**13.6%**
		T1543.002: Systemd Service	**0.9%**
T1053: Scheduled Task/Job	**18.3%**	T1053.005: Scheduled Task	**12.8%**
		T1053.003: Cron	**0.9%**
T1098: Account Manipulation	**14.1%**	T1098.005: Device Registration	**1.5%**
		T1098.004: SSH Authorized Keys	**1.1%**
		T1098.001: Additional Cloud Credentials	**0.7%**
		T1098.002: Additional Email Delegate Permissions	**0.5%**
T1133: External Remote Services	**12.6%**		
T1505: Server Software Component	**11.9%**	T1505.003: Web Shell	**11.7%**
		T1505.004: IIS Components	**0.2%**
T1547: Boot or Logon Autostart Execution	**10.8%**	T1547.009: Shortcut Modification	**3.1%**
		T1547.004: Winlogon Helper DLL	**0.7%**
T1136: Create Account	**9.2%**	T1136.001: Local Account	**3.8%**
		T1136.003: Cloud Account	**0.7%**
		T1136.002: Domain Account	**0.7%**
T1574: Hijack Execution Flow	**8.2%**	T1574.001: Registry Run Keys/Startup Folder	**7.7%**
		T1574.011: Services Registry Permissions Weakness	**6.0%**
		T1574.002: DLL Side-Loading	**1.8%**
		T1574.008: Path Interception by Search Order Hijacking	**0.9%**
		T1574.010: Services File Permissions Weakness	**0.2%**
		T1574.005: Executable Installer File Permissions Weakness	**0.2%**
		T1574.001: DLL Search Order Hijacking	**0.2%**
T1546: Event Triggered Execution	**4.8%**	T1546.003: Windows Management Instrumentation Event Subscription	**2.4%**
		T1546.008: Accessibility Features	**1.3%**
		T1546.012: Image File Execution Options Injection	**0.4%**
		T1546.002: Screensaver	**0.4%**
		T1546.010: AppInit DLLs	**0.4%**
		T1546.004: Unix Shell Configuration Modification	**0.4%**
		T1546.007: Netsh Helper DLL	**0.2%**
		T1546.001: Change Default File Association	**0.2%**
T1037: Boot or Logon Initialization Scripts	**1.1%**	T1037.001: Logon Scrips (Windows)	**0.4%**
		T1037.004: RC Scripts	**0.2%**
T1542: Pre-OS Boot	**0.2%**	T1542.002: Component Firmware	**0.2%**
T1176: Browser Extensions	**0.2%**		
T1137: Office Application Startup	**0.2%**	T1137.006: Add-ins	**0.2%**

Escalate Privileges

Privilege Escalation

T1543: Create or Modify System Process	**24.9%**	T1543.003: Windows Service	**13.6%**
		T1543.002: Systemd Service	**0.9%**
T1055: Process Injection	**23.1%**	T1055.003: Thread Execution Hijacking	**1.5%**
		T1055.001: Dynamic-link Library Injection	**0.7%**
		T1055.002: Portable Executable Injection	**0.5%**
		T1055.004: Asynchronous Procedure Call	**0.5%**
		T1055.012: Process Hollowing	**0.5%**
T1134: Access Token Manipulation	**16.3%**	T1134.001: Token Impersonation/Theft	**8.1%**
		T1134.004: Parent PID Spoofing	**0.4%**
		T1134.002: Create Process with Token	**0.4%**
T1547: Boot or Logon Autostart Execution	**10.8%**	T1547.001: Registry Run Keys/Startup Folder	**7.7%**
		T1547.009: Shortcut Modification	**3.1%**
		T1547.004: Winlogon Helper DLL	**0.7%**
T1078: Valid Accounts	**9.3%**		
T1574: Hijack Execution Flow	**8.2%**	T1574.011: Services Registry Permissions Weakness	**6.0%**
		T1574.002: DLL Side-Loading	**1.8%**
		T1574.008: Path Interception by Search Order Hijacking	**0.9%**
		T1574.010: Services File Permissions Weakness	**0.2%**
		T1574.005: Executable Installer File Permissions Weakness	**0.2%**
		T1574.001: DLL Search Order Hijacking	**0.2%**
T1546: Event Triggered Execution	**4.8%**	T1546.003: Windows Management Instrumentation Event Subscription	**2.4%**
		T1546.008: Accessibility Features	**1.3%**
		T1546.012: Image File Execution Options Injection	**0.4%**
		T1546.002: Screensaver	**0.4%**
		T1546.010: AppInit DLLs	**0.4%**
		T1546.004: Unix Shell Configuration Modification	**0.4%**
		T1546.007: Netsh Helper DLL	**0.2%**
		T1546.001: Change Default File Association	**0.2%**
T1548: Abuse Elevation Control Mechanism	**2.7%**	T1548.002: Bypass User Account Control	**1.8%**
		T1548.003: Sudo and Sudo Caching	**0.5%**
		T1548.001: Setuid and Setgid	**0.4%**
T1484: Domain Policy Modification	**2.0%**	T1484.001: Group Policy Modification	**2.0%**
T1037: Boot or Logon Initialization Scripts	**1.1%**	T1037.001: Logon Scrips (Windows)	**0.4%**
		T1037.004: RC Scripts	**0.2%**
T1086: Exploitation for Privilege Escalation	**0.2%**		

Internal Reconnaissance

Discovery

T1082: System Information Discovery	**31.3%**		
T1083: File and Directory Discovery	**29.3%**		
T1033: System Owner/ User Discovery	**22.5%**		
T1012: Query Registry	**22.3%**		
T1622: Debugger Evasion	**21.1%**		
T1057: Process Discovery	**20.7%**		
T1087: Account Discovery	**18.3%**	T1087.002: Domain Account	**5.5%**
		T1087.002: Local Account	**5.1%**
		T1087.004: Cloud Account	**0.9%**
		T1087.003: Email Account	**0.4%**
T1016: System Network Configuration Discovery	**15.8%**	T1016.001: Internet Connection Discovery	**1.1%**
T1518: Software Discovery	**15.4%**		
T1497: Virtualization/Sandbox Evasion	**13.7%**	T1497.001: System Checks	**10.1%**
		T1497.003: Time Based Evasion	**0.2%**
T1007: System Service Discovery	**10.4%**		
T1135: Network Share Discovery	**9.7%**		
T1069: Permission Groups Discovery	**9.3%**	T1069.002: Domain Groups	**6.0%**
		T1069.001: Local Groups	**1.8%**
		T1069.003: Cloud Groups	**0.9%**
T1010: Application Window Discovery	**8.4%**		
T1049: System Network Connections Discovery	**8.2%**		
T1482: Domain Trust Discovery	**6.8%**		
T1614: System Location Discovery	**5.9%**	T1614.001: System Language Discovery	**5.7%**
T1046: Network Service Discovery	**2.7%**		
T1580: Cloud Infrastructure Discovery	**1.5%**		
T1018: Remote System Discovery	**1.3%**		
T1538: Cloud Service Dashboard	**0.9%**		
T1615: Group Policy Discovery	**0.9%**		
T1040: Network Sniffing	**0.5%**		
T1201: Password Policy Discovery	**0.4%**		
T1124: System Time Discovery	**0.4%**		
T1120: Peripheral Device Discovery	**0.2%**		

Lateral Movement

Lateral Movement

T1021: Remote Services	**26.4%**	T1021.001: Remote Desktop Protocol	**20.3%**
		T1021.002: SMB/Windows Admin Shares	**6.6%**
		T1021.004: SSH	**6.4%**
		T1021.005: VNC	**1.3%**
		T1021.006: Windows Remote Management	**0.2%**
T1091: Replication Through Removable Media	**1.5%**		
T1570: Lateral Tool Transfer	**1.5%**	T1550.002: Pass the Hash	**0.5%**
		T1550.001: Application Access Token	**0.2%**
		T1550.003: Pass the Ticket	**0.2%**
T1550: Use Alternate Authentication Material	**1.1%**	T1550.002: Pass the Hash	**0.7%**
		T1550.001: Application Access Token	**0.4%**
T1534: Internal Spearphishing	**0.9%**		
T1563: Remote Service Session Hijacking	**0.2%**		

Maintain Presence

Persistence

T1543: Create or Modify System Process	**24.9%**	T1543.003: Windows Service	**13.6%**
		T1543.002: Systemd Service	**0.9%**
T1053: Schedule Task/Job	**18.3%**	T1053.005: Scheduled Task	**12.8%**
		T1053.003: Cron	**0.9%**
T1098: Account Manipulation	**14.1%**	T1098.005: Device Registration	**1.5%**
		T1098.004: SSH Authorized Keys	**1.1%**
		T1098.001: Additional Cloud Credentials	**0.7%**
		T1098.002: Additional Email Delegate Permissions	**0.5%**
T1133: External Remote Services	**12.6%**		
T1505: Server Software Component	**11.9%**	T1505.003: Web Shell	**11.7%**
		T1505.004: IIS Components	**0.2%**
T1547: Boot or Logon Autostart Execution	**10.8%**	T1547.001: Registry Run Keys/Startup Folder	**7.7%**
		T1547.009: Shortcut Modification	**3.1%**
		T1547.004: Winlogon Helper DLL	**0.7%**
T1136: Create Account	**9.2%**	T1136.001: Local Account	**3.8%**
		T1136.003: Cloud Account	**0.7%**
		T1136.002: Domain Account	**0.7%**
T1574: Hijack Execution Flow	**8.2%**	T1574.011: Services Registry Permissions Weakness	**6.0%**
		T1574.002: DLL Side-Loading	**1.8%**
		T1574.008: Path Interception by Search Order Hijacking	**0.9%**
		T1574.010: Services File Permissions Weaknes	**0.2%**
		T1574.005: Executable Installer File Permissions Weakness	**0.2%**
		T1574.001: DLL Search Order Hijacking	**0.2%**
T1546: Event Triggered Execution	**4.8%**	T1546.003: Windows Management Instrumentation Event Subscription	**2.4%**
		T1546.008: Accessibility Features	**1.3%**
		T1546.012: Image File Execution Options Injection	**0.4%**
		T1546.002: Screensaver	**0.4%**
		T1546.010: AppInit DLLs	**0.4%**
		T1546.004: Unix Shell Configuration Modification	**0.4%**
		T1546.007: Netsh Helper DLL	**0.2%**
		T1546.001: Change Default File Association	**0.2%**
T1037: Boot or Logon Initialization Scripts	**1.1%**	T1037.001: Logon Scrips (Windows)	**0.4%**
		T1037.004: RC Scripts	**0.2%**
T1542: Pre-OS Boot	**0.2%**	T1542.002: Component Firmware	**0.2%**
T1176: Browser Extensions	**0.2%**		
T1137: Office Application Startup	**0.2%**	T1137.006: Add-ins	**0.2%**

Mission Completion

Collection

T1560: Archive Collected Data	**17.2%**	T1560.001: Archive via Utility	**7.3%**
		T1560.002: Archive via Library	**0.5%**
T1213: Data from Information Repositories	**10.4%**	T1213.002: Sharepoint	**3.5%**
		T1213.003: Code Repositories	**1.6%**
		T1213.001: Confluence	**0.9%**
T1056: Input Capture	**6.8%**	T1056.001: Keylogging	**6.6%**
		T1056.003: Web Portal Capture	**0.2%**
T1113: Screen Capture	**5.1%**		
T1115: Clipboard Data	**4.9%**		
T1114: Email Collection	**3.8%**	T1114.002: Remote Email Collection	**1.5%**
		T1114.001: Local Email Collection	**0.5%**
		T1114.003: Email Forwarding Rule	**0.4%**
T1074: Data Staged	**3.8%**	T1074.001: Local Data Staging	**3.1%**
		T1074.002: Remote Data Staging	**0.4%**
T1039: Data from Network Shared Device	**2.9%**		
T1005: Data from Local System	**1.1%**		
T1602: Data from Configuration Repository	**0.7%**	T1602.002: Network Device Configuration Dump	**0.7%**
T1119: Automated Collection	**0.4%**		
T1530: Data from Cloud Storage	**0.4%**		
T1125: Video Capture	**0.2%**		
T1557: Adversary-in-the-Middle	**0.2%**	T1557.002: ARP Cache Poisoning	**0.2%**

Exfiltration

T1567: Exfiltration Over Web Service	**4.4%**	T1567.002: Exfiltration to Cloud Storage	**2.4%**
T1020: Automated Exfiltration	**1.3%**		
T1041: Exfiltration Over C2 Channel	**0.7%**		
T1030: Data Transfer Size Limits	**0.2%**		

Impact

T1486: Data Encrypted for Impact	**18.3%**		
T1489: Service Stop	**13.0%**		
T1529: System Shutdown/Reboot	**7.5%**		
T1496: Resource Hijacking	**5.3%**		
T1490: Inhibit System Recovery	**5.1%**		
T1565: Data Manipulation	**2.0%**	T1565.001: Stored Data Manipulation	**2.0%**
T1485: Data Destruction	**1.8%**		
T1561: Disk Wipe	**0.7%**	T1561.001: Disk Content Wipe	**0.4%**
		T1561.002: Disk Structure Wipe	**0.2%**
T1531: Account Access Removal	**0.7%**		
T1491: Defacement	**0.7%**	T1491.002: External Defacement	**0.4%**
T1498: Network Denial of Service	**0.4%**	T1498.001: Direct Network Flood	**0.4%**
T1499: Endpoint Denial of Service	**0.2%**	T1491.001: Internal Defacement	**0.2%**

Additional Malware Definitions

ALPHV, aka BlackCat (internet) and Noberus (Symantec), is 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.

BASTA, aka Basta Ransomware, is a ransomware written in C++ that encrypts local files. The malware uses .basta as the extension for encrypted files.

DRAGONJUICE is a comprehensive, modular, cross-platform, customizable scanning tool based on the "Ladon" project.

LOCKBIT is 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.

ROYALLOCKER is a privately managed windows-based ransomware capable of encrypting local files, disabling running processes and deleting shadow copies. The ransomware is also capable of encrypting VMDK disk formats.

SODINOKIBI, aka Revil (Internet), Sodin (Internet), and Trickgate (Check Point) is ransomware written in C that encrypts files stored locally and on network shares. It can delete files from specified directories, backup files, and volume shadow copies. SODINOKIBI may be configured to send basic system information to a remote server via HTTP. System information includes the current username, hostname, domain name, and locale.

TANKTRAP is a utility written in PowerShell that utilizes Windows group policy to spread and launch a wiper. TANKTRAP has been observed being used with NEARMISS, SDELETE, PARTYTICKET, and CADDYWIPER.

The Invasion of Ukraine: Cyber Operations During Wartime

Russia began amassing troops along its border with Ukraine in the fall of 2021, prompting warnings from U.S. and European officials of the threat of a Russian invasion. Mandiant identified extensive cyber espionage, disruptive and destructive cyber attacks, and information operations leading up to and since Russia's invasion of Ukraine on February 24, 2022.

The Kremlin's escalating attempts to bring Ukraine into the Russian sphere of influence culminated with Russia's invasion and created unprecedented circumstances for cyber threat activity. The invasion of Ukraine represents one of the first instances in which a major cyber power has conducted disruptive attacks, espionage, and information operations concurrently with widespread, kinetic military operations. Mandiant has never observed threat actor activity that matches the volume of attacks, variety of threat actors, and coordination of effort as was seen during the first months following the invasion by Russia. The invasion has also caused temporary disruption to the Russian-speaking cybercrime ecosystem, in some cases splitting criminal groups along political lines, and it has seemingly triggered the biggest revival in international hacktivism since 2015.

The evolution of Russian cyber operations during the conflict can be loosely mapped to five main phases:

- **Strategic Cyber Espionage and Pre-Positioning (prior to February 2022)**
- **Initial Destructive Cyber Operations and Military Invasion (February 2022 – April 2022)**
- **Sustained Targeting and Attacks (May 2022 – July 2022)**
- **Maintaining Footholds for Strategic Advantage (August 2022 – September 2022)**
- **Renewed Campaign of Disruptive Attacks (October 2022 – December 2022)**

Mandiant also observed Chinese, Belarusian, and Iranian threat groups targeting Ukraine in each of these phases. We believe that the intrusions by Chinese and Iranian groups were aimed at gathering intelligence for their governments, while the Belarusian group both collected intelligence and used the intrusions to enable information operations.

Across all phases of the invasion, Mandiant has supported dozens of organizations in Ukraine with incident response, remediation, intelligence, managed services, cyber defense, and general advisory, and we continue to respond to incidents across Ukraine in 2023. While Mandiant conducted engagements across nearly every sector of Ukrainian industry, our investigations overwhelmingly supported Ukrainian National Government organizations.

Mandiant also identified related information operations conducted throughout each of these phases, including those leveraging traditional cyber threat activity.

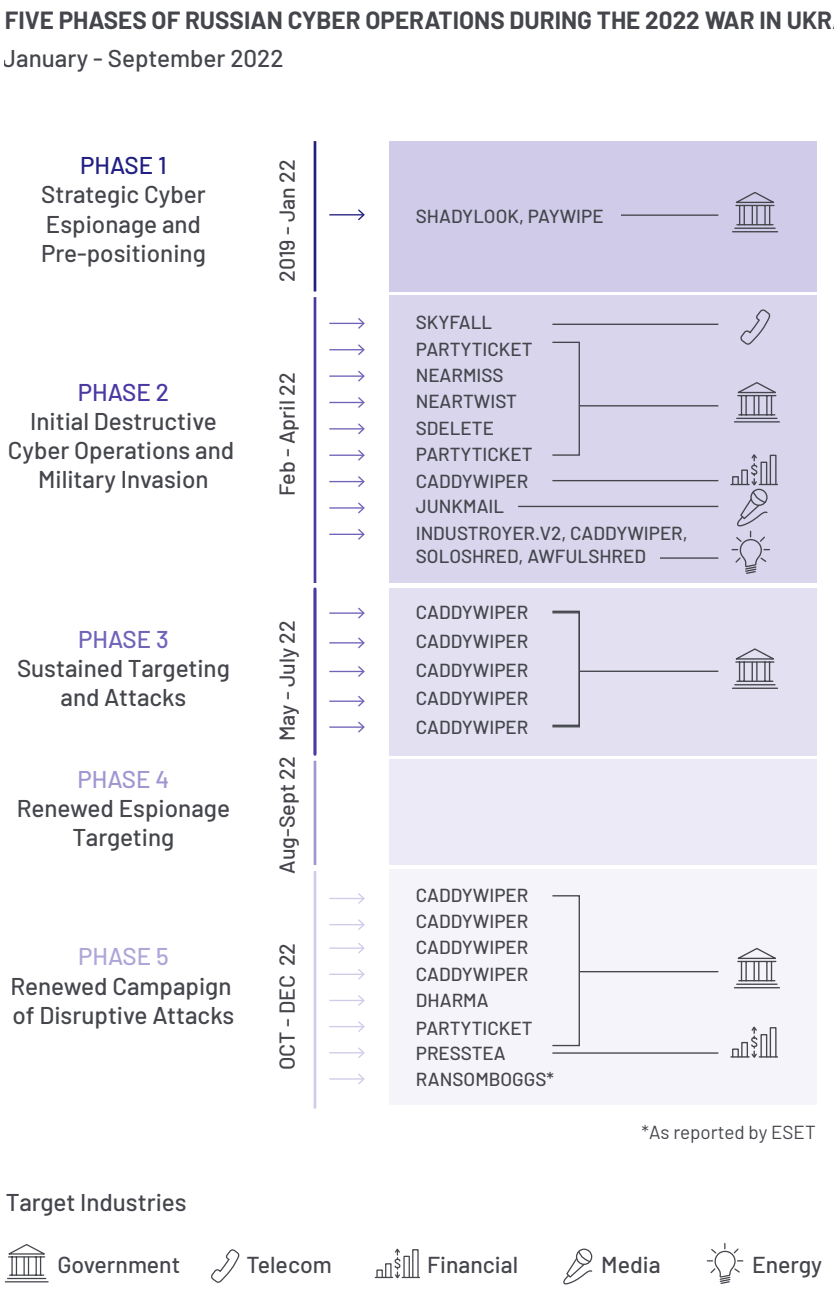


Figure 1. Phases of Russian Cyber Operations in Ukraine observed in 2022.

Strategic Cyber Espionage and Pre-Positioning Prior to Invasion

Intrusion Activity

Mandiant observed multiple threat groups conducting intrusion campaigns in the timeframe leading up to the invasion. Most notably, we observed activity by UNC2589 and APT28 prior to the invasion of Ukraine.

UNC2589

UNC2589, which Mandiant suspects operates on behalf of Russian government interests, conducted extensive espionage collection in Ukraine, particularly in late 2021 and early 2022 preceding the Russian invasion. Notably, we assess UNC2589 conducted the January 14, 2022, disruptive attacks on Ukrainian entities with PAYWIPE (aka WHISPERGATE). This may have been a preliminary but premature strike that Russian military doctrine characterizes as "preparing the information sphere" for armed conflict in an attempt to shake Ukrainians' trust in their government and fracture support for a strong defense against Russian aggression. Additional UNC2589 operations in January and February 2022 targeted Ukrainian critical infrastructure supporting that aim as well, however, distributed denial-of-service (DDoS) attacks were also conducted against financial institutions.

APT28 and Other GRU Clusters

Mandiant identified multiple instances where Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU)-related clusters relied on opportunistic access from historical compromises for current, persistent accesses once the war began. In late February 2022, APT28, a threat group sponsored by the GRU, reactivated a dormant 2019 EMPIRE infection to move laterally within the environment and use the SDELETE utility to delete files and directories from the infected systems. In another case, APT28 targeted VPNs to gain access and deploy the FREETOW dropper to multiple victims in April 2021. In at least one case, upon gaining a foothold, the attacker laid dormant until conducting a series of wiper attacks in February and March 2022 during Phase II of the war. APT28 has been the most active Russian cluster of activity in Ukraine since the war began and has prioritized disruptive cyber attacks over espionage operations in Ukraine.

Initial Destructive Cyber Operations and Military Invasion

(February 2022–April 2022)

Mandiant observed more destructive cyber attacks in Ukraine during the first four months of 2022 than in the previous eight years. Ukrainian organizations were impacted by threat actors using six unique wipers during the first few phases of the war. These destructive cyber attacks were timed to coincide with, and likely support, Russia's invasion of Ukraine on February 24, 2022, and did not target organizations directly related to or supporting the war effort. While the destructive cyber attacks did initially achieve significant widespread disruption in some Ukrainian networks, they were likely not as impactful as previous Russian cyber attacks targeting Ukraine. In comparison, Russia had launched successful cyber attacks targeting power grid disruptions in 2015 and 2016 that interrupted power for hundreds of thousands of Ukrainians for hours, and the 2017 NOTPETYA attacks disrupted operations throughout Ukraine and beyond.

APT28 Wiper Attacks and GRU Living on the Edge

Mandiant observed APT28 targeting multiple Ukrainian entities with disruptive and espionage operations similar to the efforts undertaken at the outset of war. APT28's wartime operations have deviated from historical APT28 activity. The group has demonstrated a preference toward compromising edge infrastructure to conduct a variety of operations, a technique we call "Living on the Edge." APT28 has also used a variety of disruptive and espionage malware over a short period of time, and leveraged several recently published exploits during wartime, including Follina, the PROXYSHELL exploitation chain, and several Exchange vulnerabilities.

"Living on the Edge" has become a key part of GRU operations during wartime. Since the outset of the war in Ukraine, the GRU has attempted to conduct successive and almost constant campaigns of cyber espionage and disruption aimed against key services and organizations within Ukraine. This balance of access to and action against targeted organizations relies on the compromise of edge infrastructure such as routers and other internet connected devices. Where destructive actions necessitate the loss of direct access to endpoints, compromised edge devices allow for continued re-entry to the network. Compromise of these routers can also be harder for defenders to detect as most EDR technologies do not cover these types of devices.

Renewed Russian Interest in Industrial Control Systems Capabilities

Between February and April 2022, the software company ESET reported on a suspected Russian threat actor targeting a Ukrainian electric utility in an operation that resulted in the deployment of multiple wiper malware families. The attack also involved a variant of the Industrial Control Systems (ICS)-oriented disruption framework INDUSTROYER.V2, of which a previous version had been leveraged during a similar attack in December 2016 to cause power outages in Ukraine. While it is unclear if this operation was effective in its impact to the utility's electric transmission and distribution operations, the event reinforced the notion that Russia has a reusable capability to affect electric energy systems.

Reemergence of Hacktivist Personas and Cyber-Enabled Information Operations

Mandiant observed a significant increase in hacktivism after the invasion of Ukraine, including activity emanating from Russian-backed groups. The Russian intelligence services have an extensive history of using false hacktivist personas to support information operations, along with disruptive and destructive cyber activity. In particular, Mandiant has focused on analyzing a set of self-proclaimed hacktivist groups—XakNet Team, Infoccentr, and CyberArmyofRussia_Reborn—all of which likely at least coordinate their operations with GRU-sponsored APT28. Mandiant has directly observed the deployment of wipers used by APT28 on the networks of multiple Ukrainian organizations, and the subsequent leaks of data on Telegram by threat actors claiming to be hacktivists, likely originating from those entities within 24 hours. We identified at least 16 data leaks from these groups, four of which coincided with wiping attacks by APT28.

On the Telegram channels, the threat actors claimed to have targeted victims with traditional hacktivist activity such as DDoS attacks, website defacements, and hack-and-leak operations. Such activity serves two possible influence objectives that benefit Russia in the invasion of Ukraine. The groups promote Russian interests abroad through their threat activity, and they promote the idea of average Russians supporting the government to domestic audiences through their claims to be patriotic volunteers. Both efforts have been amplified by the Russian media, on social media platforms, and elsewhere online.

During this phase Mandiant also observed an increase in hacktivist activity by the KillNet collective. KillNet claimed activity against Poland, Lithuania, and other NATO countries, which seemed to align with priorities of the Russian government. However, Mandiant has not yet uncovered direct evidence linking KillNet to Russian Intelligence.

Use of Physical Access to Enable Cyber Operations

During an investigation into activity targeting a Ukrainian government organization's network, Mandiant uncovered evidence the compromise occurred after Russian military units physically accessed the network in early 2022. The actor, which Mandiant tracks as UNC3762, used this physical access to conduct network reconnaissance, harvest credentials, and move laterally using remote desktop and web shells. UNC3762 also exploited the PROXYSHELL vulnerability chain (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207), deployed THRESHGO malware, and stole data from the environment.

Sustained Targeting and Attacks

(May 2022–July 2022)

After the initial waves of destructive attacks, the pace and variety of cyber operations targeting Ukraine shifted. Mandiant observed continued attempts to deploy wiper malware, but these attacks appeared less coordinated than the initial wave in February 2022. These attacks often occurred more quickly after the attacker gained or re-gained access, often via compromised edge infrastructure. In many instances, Ukrainian defenders were able to identify and mitigate attempted attacks before any disruption occurred. Mandiant also saw attempts at access and collection operations between waves of disruptive activity, demonstrating Russia's requirement for continued access to previously wiped entities.

Continued Intrusions and Operational Tempo

Throughout this phase of the war, Russian cyber actors continued to attempt to either re-gain access to multiple victim environments via compromised edge infrastructure or to maintain persistence on networks despite ongoing mitigation, often via GRE tunnels. This pattern was demonstrative of cyclical collection and disruptive operations undertaken by Russia-aligned threat actors. GRU clusters maintained their high operational tempo by adopting newly published exploits while also working to standardize their destructive operations. Between waves of disruptive activity, one phishing campaign leveraging a compromised legitimate mail server attempted to exploit the Follina vulnerability to enable APT28 access and collection operations using the EARLYBLOOM and DARKCRYSTALRAT backdoors. The GRU also shifted away from using multiple different wipers to relying heavily on CADDYWIPER and variants thereof to wipe organizations in quick-turnaround operations. This high operational tempo led to operators making several mistakes. In one instance a threat actor attempted to deploy the PARTYTICKET payload using the arguments for NEARMISS. They were able to adjust and successfully deploy NEARMISS, but the error caused a delay and potentially impaired their effectiveness.

GRU intrusion operations maintained several themes between their operations at the outset of the war, and those that have occurred during this sustained targeting phase. Overall, GRU continued to target and leverage edge infrastructure to gain access to strategic targets. Once within an environment, GRU clusters leveraged IMPACKET and publicly available backdoors to maintain a foothold. Mandiant also observed another GRU cluster, UNC3810, demonstrate proficiency at targeting and operating on Linux systems. UNC3810 has largely leveraged proxying tooling such as GoGetter and Chisel to maintain access and move laterally within target environments.

Maintaining Footholds for Strategic Advantage

(August 2022–September 2022)

Through the end of the previous phase, we had not observed any direct evidence of activity associated with suspected FSB-cyber threat actors Turla or Temp.Isotope. However, between August and September, GRU clusters stepped away from disruptive activity targeting Ukraine and clusters associated with the FSB—Russia's Federal Security Service—began to emerge. While one GRU-associated cluster, UNC3810, remained active in an espionage capacity, Mandiant observed activity from the Russia nexus threat group TEMP.Armageddon targeting four distinct government entities in Ukraine. Though we primarily observed GRU clusters at the helm of cyber operations against Ukraine since the inception of the war, TEMP.Armageddon—a Russia-nexus threat actor that collects information on Ukrainian national security and law enforcement entities in support of Russia's national interest, focusing exclusively on Ukrainian targets—has targeted Ukrainian and other European organizations throughout with evolving tooling and techniques. The breadth of operations observed from TEMP.Armageddon is consistent with the prolific campaigns the group undertook in years past.

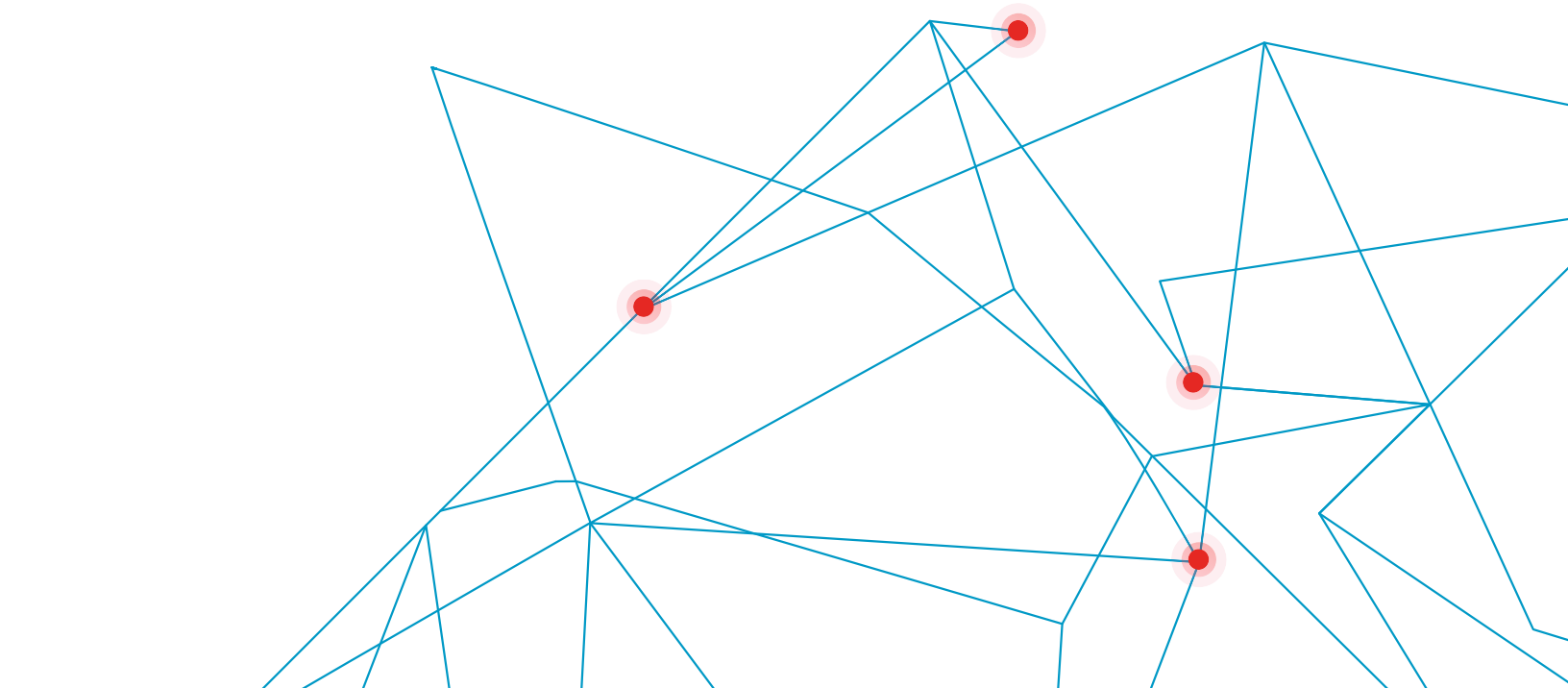
In addition to TEMP.Armageddon targeting of Ukrainian government entities, Mandiant identified suspected Turla activity in August and September. Turla is a Russia-based cyber espionage actor active since 2006 that is known to target diplomatic, government, and defense entities. Mandiant identified a compromise dating back to a late 2021 compromise at a Ukrainian government agency that aligns with Turla's tactics, techniques and procedures.

Renewed Tempo of Disruptive Attacks

(October 2022–December 2022)

The most recent phase of operations was characterized by a resurgence in disruptive cyber attacks in Ukraine. Though some of the attacks appeared similar to disruptive attacks seen in previous phases, this new wave of disruptive attacks appeared to deviate from the historical norm. Earlier attempts relied on quick-turnaround operations using CADDYWIPER variants, but the attacks undertaken in October to December saw GRU clusters deploying ransomware variants on targeted networks. This shift is consistent with Microsoft's reporting on the Prestige (PRESSTEA) ransomware deployment by IRIDIUM in Poland. Though the cycle of access and action appears to have continued during this phase, GRU's shift to using ransomware may be a sign they are undergoing tooling shifts and don't have the resources to rely on writing or modifying custom malware.

During this phase, Mandiant also observed GRU disruptive operations against the Ukrainian energy sector that coincided with the broader Russian kinetic campaign targeting Ukrainian energy infrastructure. While it is possible that cyber operations are supporting the kinetic campaign, we do not have sufficient insight to confirm it.



Information Operations Surrounding Russia's Invasion of Ukraine

Russia's war against Ukraine has generated a disproportionate amount of disinformation on the topic. Mandiant observed disinformation campaigns ranging from cyber-enabled information operations to campaigns leveraging coordinated and inauthentic networks of accounts to promote fabricated content across online media. Mandiant has identified multiple Russia-aligned information operations linked to known actors promoting a narrative related to the conflict, including the Belarus-linked Ghostwriter campaign, the Secondary Infektion campaign, and activity reportedly linked to individuals affiliated with Russia's Internet Research Agency.

Russia's disinformation campaigns appear to serve the dual purposes of tactically responding to or shaping events on the ground, and strategically influencing the shifting geopolitical landscape. The narratives being promoted seek to demoralize Ukrainians and foment internal unrest, isolate Ukraine from its allies, and bolster positive perceptions of Russia. While much of the disinformation activity has targeted audiences in Ukraine and Europe, Mandiant has identified information operations promoting messaging aimed at Russian domestic audiences, further underscoring Russia's need to sell the war to its own people.

Mandiant anticipates that such operations, including those involving cyber threat activity and potentially other disruptive and destructive attacks, will continue as the conflict progresses. Meanwhile, Mandiant has also observed pro-PRC and pro-Iran campaigns leveraging the Russian invasion opportunistically to further progress long-held strategic objectives. Though some of these operations have promoted narratives that appear to be aligned with Russian interests, they also demonstrate how events of global significance have the power to attract third-party actors. Mandiant expects this dynamic to continue and is actively monitoring for expansions in their scope of information operations activity surrounding the conflict.

Takeaways

Russia's invasion of Ukraine has demonstrated the potential overlap of cyber operations and kinetic warfare as a new de facto standard. The war has consumed almost every aspect of Russia's international relationships and has evolved as nearly the sole driver of cyber threat activity from Russia in 2022. While Russian threat actors are responsible for the vast majority of the espionage campaigns and all of the disruptive or destructive operations that Mandiant has investigated, Chinese and Iranian state sponsored groups have also been active in the region, highlighting how states will use cyber to gain information on intelligence priorities.

The tactical and strategic choices by Russian actors demonstrate both the versatility of cyber operations and the tradeoffs. Russia's use of a pre-existing compromise to conduct a wiper operation shows how an intrusion that was started for espionage purposes can be used for an attack if the geopolitical situation changes, and demonstrates the imperative for defenders to identify and fully remediate intrusions. The tactical choice by Russian actors to focus on edge devices also allowed flexibility and enabled the actors to potentially continue to collect information following a disruptive event. These devices are difficult for defenders to monitor, but they should be promptly patched, and any suspicious traffic originating with them should be thoroughly investigated.

Any armed conflict brings with it the possibility of disruptive actions aimed at the populations and governments. Governments and private sector organizations both play an important role in the functioning of a country. Preparations to defend against and recover from these types of attacks should be standard as even countries not directly impacted by hostilities may be targeted if they are perceived to be supporting one of the sides.

North Korea's Financial Operations Continue to Evolve

Alongside their traditional intelligence collection missions, in 2022 DPRK operators showed more interest in stealing—and using—crypto, with their activity expanding to new parts of the digital asset ecosystem as the regime looks to mitigate the economic impact of sanctions.

Since at least 2016, threat actors associated with the Democratic People's Republic of Korea (DPRK) have expanded cyber operations beyond traditional espionage collection and disruptive attacks to leverage their capability for financially motivated campaigns and intrusions. Historically, North Korean threat actors have targeted financial entities, investment services, eCommerce, cryptocurrency users and exchanges, and transaction processing organizations throughout the globe. These activities have included compromises into traditional financial entities—most famously targeting the central bank of Bangladesh—and the burgeoning cryptocurrency and digital asset sector. In 2022, Mandiant observed North Korean threat actors continuing to evolve their targeting as part of an effort to identify alternative revenue streams and mitigate the impact of sanctions.

While these groups appear to continue to take advantage of various financial targets, Mandiant has observed an increasing and evolving focus on the cryptocurrency ecosystem in 2022. Threat actors leveraged creative means through which the North Korean regime and their own operations could be funded. Notably, over the past year Mandiant also observed a shift away from targeting fewer, larger organizations toward targeting a larger number of smaller entities for modest financial gains. Media reports have highlighted how North Korean operators stole approximately $1.7 billion in cryptocurrency in 2022, eclipsing the $428 million stolen in 2021. Additionally, the regime allegedly has $170 million in unlaundered cryptocurrency holdings, which are potentially being stored as reserves. The United nations (UN) suggests these illicit funds are being used to finance the country's missile programs.

NFTs, Bridges, Ransomware and More: North Korean Cybercrime in 2022

Early Mandiant analysis of North Korean crypto-focused operations highlighted their centering around targeting cryptocurrency exchanges, and was predominantly driven by TEMP.Hermit and clusters suspected of being linked to APT38. Since then, the number of suspected DPRK groups involved in thefts of cryptocurrency, and the nature of their targets, has continued to expand. North Korean threat actors have targeted interdisciplinary aspects of cryptocurrencies, including Non-Fungible Tokens (NFTs), cross-blockchain connection mechanisms, and even online games.

In one broad, months-long cryptocurrency phishing campaign by suspected North Korea-nexus UNC4469, thousands of smart contracts were used to deliver malicious NFTs to over a million unsuspecting users. UNC4469 leveraged malicious, mass NFT airdrops to user wallets, phishing pages, and social media platforms with themes designed to socially engineer the victim into connecting their wallets. Once the wallets were connected, UNC4469 was able to collect and transfer assets, including NFTs, to UNC4469-controlled wallets. Assets stolen from phishing victims were quickly sold, and the funds moved through various blockchains to launder the funds and obscure their trail. The automation, duration, and volume of activity spanning multiple blockchains indicates an ongoing sophisticated and mature operation.

Alongside NFTs, "bridges" are another part of the cryptocurrency ecosystem that has grown in usage in recent years. Bridges facilitate movement of assets between different blockchains without the need to use a cryptocurrency exchange. Bridges can accumulate value as they become more widely used, making them attractive targets. This was demonstrated in 2022 with the $100 million compromise of Harmony's Horizon Bridge by actors, which the FBI attributed to North Korea[5].

Online games with cryptocurrency and blockchains as a central feature have gained popularity with the rise of cryptocurrency, and thus have also gained the interest of North Korean groups. In April 2022 the U.S. Department of the Treasury alleged that North Korea-based threat actors were responsible for a $600 million theft from a digital ledger used by players of the online game Axie Infinity. The U.S. Government managed to seize $30 million in cryptocurrency related to the heist, which it attributed to the "Lazarus" cybercrime gang. The North Korean actor TEMP. Hermit has demonstrated a history of targeting cryptocurrency services, and many of these incidents are publicly attributed to Lazarus.

NOTABLE NORTH KOREAN THREAT ACTIVITY TARGETING CRYPTOCURRENCIES IN 2022

		SUSPECTED GROUP	MALWARE FAMILY USED
2022	January	UNC1130	COINTOSS
		UNC1130	N/A
	March	TEMP.HERMIT	N/A
		N/A	N/A
	April	N/A	N/A
	May	N/A	N/A
	June	UNC1069	LONEJOGGER
	July		
	Aug	UNC1130	LOGCABIN
	Fall	UNC1758	AppleJeus

Separately, Mandiant investigated open source reports of multiple suspected DPRK efforts to gain employment at cryptocurrency-focused organizations in April and May 2022. The accounts seem consistent with a May 2022 U.S. government advisory on North Korean IT workers posing as non-North Korean nationals to gain employment in areas where they would have an opportunity to generate revenue for DPRK programs.

While the scale and nature of these operations suggests they exist primarily to facilitate funding for the North Korean regime's nuclear program ambitions, some activity observed by Mandiant suggests they may also function to support further cyber operations for the actors themselves. For example, Mandiant has observed UNC1130, an activity cluster that aligns with the publicly reported Kimsuky activity set, uses targeted financial data and stolen cryptocurrency to procure infrastructure and equipment. UNC1130 operators employed various online personas to purchase infrastructure, hardware, and code signing certificates from multiple vendors. In at least some of the identified purchases, the threat actors used U.S.-based addresses. The purchases were funded via PayPal, American Express credit cards, and cryptocurrencies that may have been derived from previous operations. Mandiant previously observed payments from DPRK-controlled wallets to cryptocurrency payment processors.

Finally, in late 2022, sensitive and open source reporting suggests that some clusters related to the threat group publicly tracked as Andariel are involved in utilizing ransomware in campaigns impacting global organizations. Analysis of these activities, including those of UNC4131 and UNC4369, indicate their goals seem financially motivated with the self-funding of further operations at least a partial goal. In comparison to other money-making schemes, the activities undertaken by UNC4131 and UNC4369 are limited in volume.

Not Just Money: Continued Intelligence Collection Operations in Context

North Korean-associated threat clusters operate with a dual mandate today. Even with their growing focus on financially motivated activity, Mandiant has continued to witness DPRK campaigns and operations of a traditional espionage nature. In 2022, Mandiant observed compromises impacting government, aerospace and defense, education, legal, media, pharmaceutical, and technology sectors, as well as other organizations in South Korea, Japan, and the United States. These operations demonstrate continued reconnaissance and social engineering efforts to tailor spear phishing campaigns to access strategic information.

In early 2022, North Korean espionage groups conducted credential theft operations targeting academics, journalists, political figures, bloggers, and other private sector individuals, primarily in South Korea. Mandiant observed targets were consistent with similar activity ongoing since mid-2021, though they reflect an increase in private sector victims and decrease in targeting against religious organizations compared to prior months. Analysis of malware distribution data, lure document language, and lure content suggests entities in South Korea and Japan were targeted by a campaign of phishing emails themed around software development. One of the documents mentioned a Japanese tech company that sells security equipment, including security cameras.

Analysis of the email contents, spoofed entities, and targets indicate UNC1130 is continuing to carry out strategic intelligence collection and credential harvesting campaigns. These are most likely intended to inform North Korean leadership on geopolitical events and issues ranging from interest in DPRK weapons testing by various countries to potential responses to perceived DPRK activities.

Mandiant observed another North Korean threat actor, UNC2970, sending messages to targets in the media industry via LinkedIn messages. Once contact was established, the medium was changed to a text messaging service. A weaponized job description lure document was then sent to the victims, enabling initial access. Upon gaining access to the target environments, UNC2970 leveraged various malware families to perform traditional espionage operations.

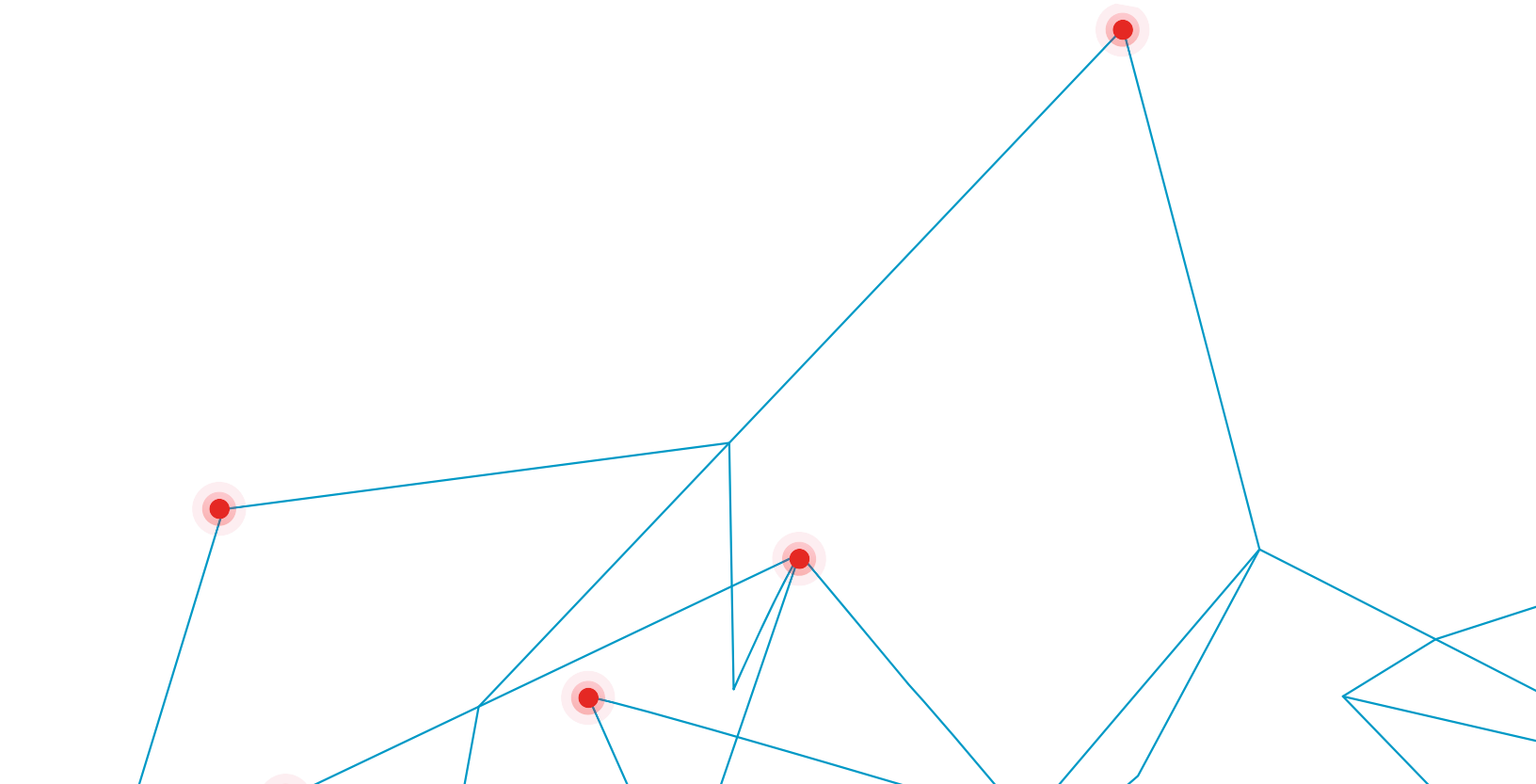
While traditional cyber espionage remains a priority for North Korea, the need for funding manifested more heavily in 2022 with a concerted determination to make financial gain a priority. North Korea's targeting of Western interests will likely continue commensurate with national priorities such as the regime's nuclear ambitions, and regionally focused geopolitical events.

Conclusion

For years, North Korea has reportedly conducted various illicit financial activities to fund the regime. The explosive growth of cryptocurrency is converging with aggressive and flexible North Korean cyber capabilities, making it natural that at least some North Korean threat groups would expand operations into this sector. DPRK actors such as APT38, TEMP.Hermit and UNC1130 have demonstrated a continued willingness to explore new ways to exploit the growing crypto ecosystem, and Mandiant's analysis of DPRK activity trends in 2022 reinforces that. With the lucrative success DPRK operations have had in providing funding for cyber activity and supporting the regime, these focused efforts will likely continue unabated throughout 2023. Many of the DPRK threat groups Mandiant tracks have moved into cryptocurrency targeting or usage in some form. This expansion of potential targets provides opportunities for network defenders in other sectors to gain valuable insight into North Korean tactics, techniques, and procedures.

Efforts of North Korean personnel to gain employment without revealing their true nationality fulfills strategic needs for the regime while introducing immense risk to targeted organizations. In addition to funding the regime, these personnel can exfiltrate sensitive and proprietary information, introduce vulnerabilities, or facilitate cyber intrusions. Attempts at employment can also telegraph DPRK interests to network defenders, providing a window of preparation.

Mandiant graduated UNC1130 to APT43 in March 2023. The full APT43 report is available at https://www.mandiant.com/resources/blog/apt43-north-korea-cybercrime-espionage



Shifting Focus and Uncommon Techniques Brought Threat Actors Success in 2022

In 2022, Mandiant investigated a series of high-profile intrusions that were successful and impactful to the targeted organizations despite significant deviations from common threat actor behaviors. While the threat actors demonstrated relatively less technical sophistication than the government sponsored and criminal threat actors Mandiant regularly investigates, the impacts to the targeted organizations were disproportionate. These incidents underscored the threat posed to organizations by persistent adversaries willing to eschew the unspoken rules of engagement. Mandiant observed threat actors leverage data available in underground cybercrime markets, clever social engineering schemes, and even bribes to carry out intrusions and account takeovers. Furthermore, these adversaries demonstrated a willingness to get personal with their targets, bullying and threatening many of them.

In early 2022, a group of cyber criminals made headlines when they began to target major international corporations in highly publicized, and often sensationalized, intrusions. The group, which Mandiant tracks as UNC3661 and is publicly referred to as "Lapsus," conducted a wide range of malicious activity inside targeted organizations. UNC3661 initially targeted organizations in South America, but shortly expanded scope to include global organizations. Intrusions undertaken by UNC3661 resulted in stolen source code, intellectual property, and, in multiple instances, significant reputational damage.

Despite the damage and scope of the intrusions, UNC3661's motives were not limited to financial gain. In fact, their actions during intrusions spoke broadly to a desire for notoriety, rather than being optimized to increase profits. UNC3661 often demanded corporations release intellectual property as open source and, rather than choosing targets for their financial potential, would often conduct polls in Telegram chats to determine which organization to target next.

More recently, Mandiant encountered another group, tracked as UNC3944, that demonstrated characteristics similar to UNC3661. UNC3944 is a financially motivated threat cluster, active since at least May 2022, that commonly gains initial network access using stolen credentials obtained from SMS phishing operations. On rare occasions actors affiliated with UNC3944 have engaged in interactive social engineering operations, actively threatened individuals, and attempted to bribe individuals to obtain system access.

A common theme for both threat clusters is the oversized impact of their intrusions without relying on zero-days, custom malware, or new tools. It is important organizations understand the potential ramifications of this new, more outspoken threat, and adjust both protections and expectations accordingly.

Initial Intrusions

Both UNC3661 and UNC3944 relied on a combination of stolen credentials and clever social engineering to gain initial access to targeted environments. While Mandiant has not confirmed additional initial attack vectors, UNC3661 has solicited VPN credentials from insiders, and open source reporting has suggested they obtain these credentials through phishing email campaigns. UNC3661 also used stolen cookies to gain access to the network of a targeted organization. In an interview with a reporter, the threat actor stated they had purchased these stolen cookies from the underground marketplace Genesis Market.

Mandiant observed UNC3661 authenticate to an organization's VPN infrastructure using stolen or illicit credentials, as well as manage social engineering campaigns to enroll new devices in multi-factor authentication (MFA) platforms. UNC3944 leveraged valid credentials for authentication as well; however, when presented with MFA restrictions, they would socially engineer helpdesk operators to enable Subscriber Identity Module (SIM) swapping attacks and enroll new phones. SIM swapping allows for the transfer of an existing phone's service to a new phone. Threat groups can intercept MFA verification messages by using SIM card swapping to hijack SMS messages.

Getting Around and Getting Out

Once implanted inside an organization's network, both UNC3661 and UNC3944 preferred to use tools available on the various endpoints on which they had gained access. This operating model, sometimes referred to as 'Living off the Land', removes the chance an attacker will be detected while transporting tools or malware into the environment. Similarly, detection opportunities are further obfuscated as the actions a threat actor takes during reconnaissance or lateral movement blend in with activity already common to the environment. In some cases, however, simple tools already present in the environment were insufficient and Mandiant observed both UN3944 and UNC3661 leverage more complex tooling.

UNC3944 would often rely on virtual machines (VM) to drive toward their mission objectives post-compromise. In one instance, the threat group installed VMware on a Citrix desktop after exploiting MFA gaps, and subsequently used the VM to perform broad-scale internal reconnaissance activity within the compromised network. Mandiant also identified evidence that UNC3944 gained access to an organization's Azure portal and created VMs configured to accept Remote Desktop Protocol (RDP) connections from external attacker-controlled IP addresses. By remotely connecting to the Azure VMs, the attacker abused access control policies, which allowed for ingress into the customer network from the Azure tenant. UNC3944's use of VMs also provided partial anti-forensic capabilities. In cases where UNC3944 deleted the VM, they created evidence that had to be gathered from secondary observations from within the network.

UNC3944 also took great care to ensure that, even when they were removed from the networks, they were able to regain access through a variety of techniques. While they commonly avoided the use of persistent backdoors, the efforts undertaken to regain access were nonetheless effective. For instance, UNC3944 was able to abuse various password reset services such as ServiceNow and ManageEngine to reset passwords to accounts that had been remediated. Instead of risking detection in a new attack, leveraging the assumption that an account had been successfully reset and secured during remediation paid dividends for UNC3944's continued access to targeted environments.

In comparison, UNC3661 would leverage common malware such as Mimikatz or Impacket to aid in harvesting credentials if needed. Mandiant identified evidence demonstrating the use of both tools by UNC3661 to access an organization's ntds.dit file, as well as perform DCSync operations. Mandiant also observed UNC3661 exploit CVE-2022-21919 using a public utility Mandiant tracks as DOUBLEJUMP to escalate privileges within an environment. CVE-2022-21919 is a vulnerability in the Windows User Profile Service that, when exploited, allows for the execution of a malicious DLL under the NT AUTHORITY\SYSTEM user context.

While UNC3661 was, at times, able to leverage operating system weaknesses and vulnerabilities to escalate privileges, the use of stolen credentials that already had elevated rights was a favored technique for the group. The majority of lateral movement observed by Mandiant with respect to UNC3661 occurred over RDP using valid credentials, and the threat group has demonstrated an ability to zero in on stores of credential data otherwise thought secure by the environments' owners. Mandiant observed UNC3661 access internal data, messaging platforms, and management systems, which they subjected to a rigorous search for plaintext credentials and access tokens.

A common theme between both groups was the targeting of endpoint detection and response (EDR) capabilities in the environments they compromised. Both UNC3661 and UNC3944 took active steps to remove EDR tooling where possible to limit visibility into their activities. Mandiant observed UNC3661 use ProcessHacker to gain the privileges necessary to disable EDR services on endpoints, though they would also resort to simply uninstalling the services when needed. UNC3944 was observed leveraging unsophisticated yet effective custom malware to disable EDR services on endpoints in order to deter detection and inhibit remediation activities.

Making Things Personal

Over the years there has been a surprising trend towards an implicit professionalism in cybercrime. Ransomware operators learned early on that poor customer service affected their bottom line when it came to negotiating extortion demands and coordinating decryption. Threat groups that operate in the realm of cyber espionage rarely, if ever, interact with the employees of the organizations they target beyond social engineering or spear phishing efforts. UNC3661 and UNC3944, on the other hand, went to extreme lengths to harass and, in some cases, intimidate members of the organizations they compromised. Often, these outbursts coincided with remediation activities that saw the attackers progress rolled back, but just as often this tactic was deployed in service of extortion demands. In one case, UNC3944 targeted individual employees of an organization by changing their titles in the Global Address List and, in another, spammed obscene messages to employees using a variety of internal tools. UNC3661 went as far as joining the teleconference calls held by the employees of the compromised organizations to push for capitulation to extortion demands. UNC3661 would also brazenly inform members of the security and operations team of destructive actions taken within the environment using the same communications platforms.

While the evolution of cybercrime from ransomware to multifaceted extortion operations has seen an increase in direct interaction with the members of targeted organizations, the interactions undertaken by groups such as UNC3661 and UNC3944 bear a different flavor altogether. The activities put on display by these groups speak more to a confluence of financial motivation and a desire for notoriety.

Lessons Learned

The common thread between Lapsus and UNC3944 is simple; both groups realized the value in targeting credentials and accounts rather than endpoints. Despite the lack of maturity and sophistication on display, both groups were able to gain access to large entities with mature security organizations. Both groups ignored the idea of establishing a foothold on network, instead focusing on targeting the accesses and accounts of legitimate individual users.

Beyond the targeting of credentials rather than endpoints, there is another, more sinister thread that binds these actors together. UNC3944 and UNC3661 have both purposefully targeted executives and privileged administrators during intrusions with personal intent to threaten, coerce, or otherwise motivate these high priority employees to pay a ransom or submit to the actors' demands. This intentional willingness to target individual people with threats and other malicious activity constitutes an evolution of the attack surface; individual people and their families are now considered fair game for malicious actors in their efforts to monetize their intrusions. In response to this evolutionary leap, defenders should expand their definition of "attack surface," and consider that providing protection for their employees may become a necessary part of protecting your organization from malicious actors.

In the near term, organizations will have to contend with threat actors that find new ways to steal identities from users through a combination of social engineering and commodity information stealers alongside information gathering operations targeting their internal data stores. As MFA grew more commonplace, attackers sought novel means to bypass MFA without relying on malware. The same is to be expected of Identity and Access Management (IAM) systems in the near term as attackers and researchers alike explore the capabilities supplied by such platforms.

Notably, actions taken by government and law enforcement to disrupt and deter ransomware operations may result in additional actors shifting their focus to data theft and extortion operations. Recent steps taken to recover ransomware payments, issue indictments and make arrests, as well as the dramatic downturn in crypto markets, may remove some incentive in cybercrime's use of ransomware. While other groups may be more sophisticated than UNC3661 and UNC3944, their notoriety and effectiveness is likely to inspire follow-on attacks that leverage many of the same tactics. As organizations prepare and work to position their security teams and infrastructure, keeping an eye toward protecting against unsophisticated yet persistent attackers should be part of their design goals.

Red Team Case Study

Mandiant red team engagements help organizations evaluate their security program's capabilities against real-world attack scenarios, and improve their security postures. Mandiant works with a wide range of clients, from financial institutions to manufacturers to global healthcare companies.

The scenario outlined in this article reflects a large utility company concerned about compromise of site-offices, enabling attackers to gain access to critical cloud and operational technology (OT) environment resources. They requested Mandiant to help them evaluate this risk by attempting to obtain Global Administrator access in Azure, and testing the effectiveness of its controls around the Software Development Life Cycle (SDLC).

Initial Compromise

Mandiant has observed threat actors leverage non-traditional social engineering channels, including targeting users through platforms such as WhatsApp and LinkedIn, as well as using SMS and voice phishing (vishing). Based on the customer's threat model, the red team targeted branch offices with a vishing campaign. Using a cloud-based service, they created a customized call center with a telephone number similar to the customer's own IT helpdesk number. This meant that the Caller ID of incoming calls from this number would look familiar, and any branch offices returning calls were less likely to think the number looked suspicious.

The red team called the reception desk at several branch offices to arrange an appointment for a "technician" to visit the site and install some new software. In reality, the "technician" would be a Mandiant employee, and the "software" was custom malware Mandiant created to allow remote access to the network while evading detection by defensive controls. Through the custom call center setup, incoming calls were routed to a pool of red team members. Subsequent calls appeared to be answered by different call agents, creating a convincing presentation to targets who called back to confirm or ask further questions.

Once a branch office confirmed the appointment, the red team tasked a consultant in that region to visit the office the same week. The consultant arrived at the site wearing a badge that had been fabricated based on images of employee badges the red team had gathered during open-source intelligence gathering (OSINT). Client staff at the regional office provided the red team operator unsupervised access to each workstation. The operator used this access to install Mandiant's custom command and control (C2) malware on each machine, ensuring the malware would restart if the device rebooted by performing a "COM Hijacking" attack. This persistence technique involves modifying the Windows registry to direct applications that leverage Microsoft's Component Object Model (COM) to load malicious code instead of legitimate binaries.

Lateral Movement to Azure

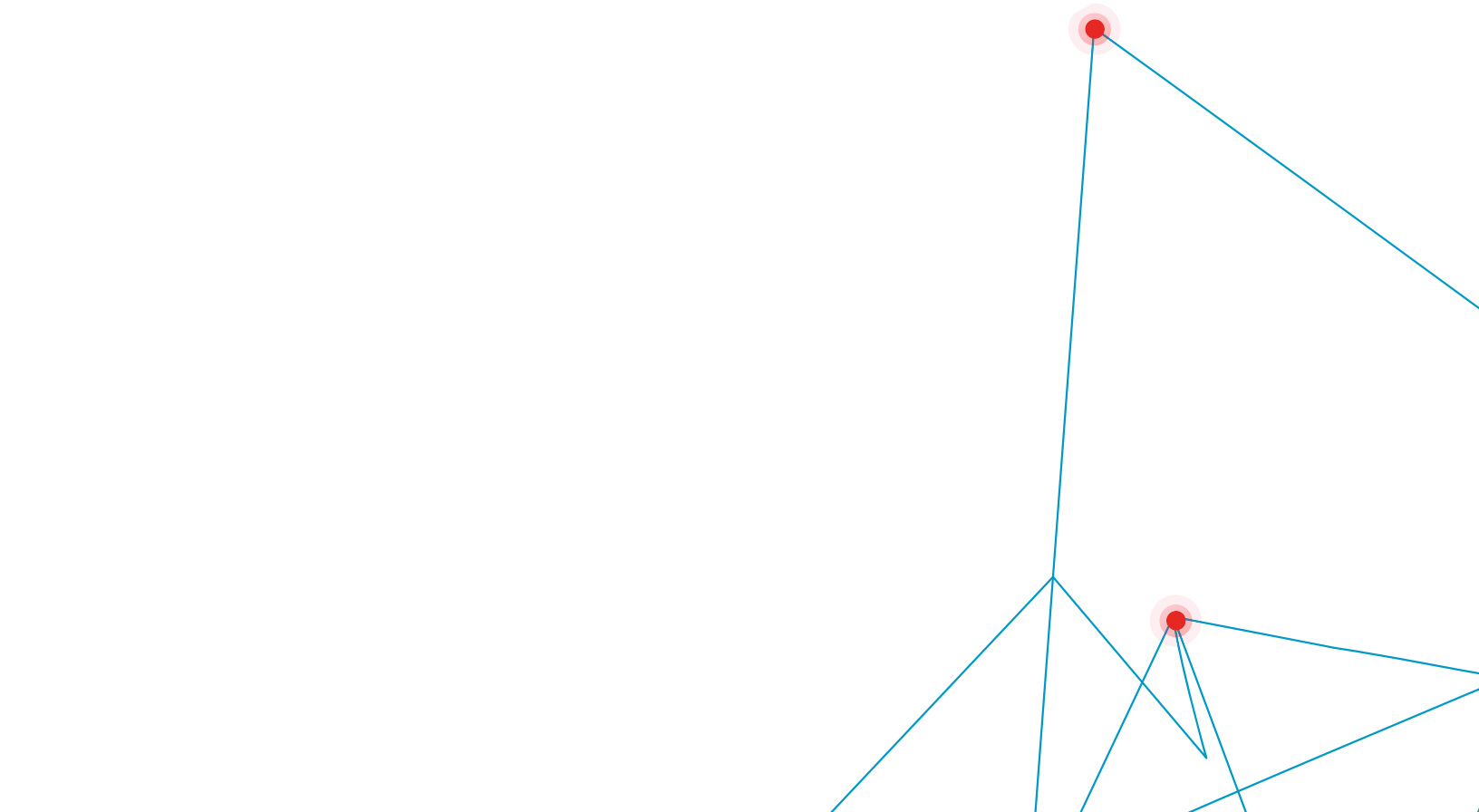
The red team had gained access to the client's internal network, but had not yet obtained credentials for any internal users that could allow them to move through the internal network. Mandiant queried the client's internal Domain Controller's Kerberos service and obtained a list of several thousand valid usernames. The list of usernames was then used in the password-spraying attack targeting the client's Azure cloud infrastructure. Password-spraying attacks differ from traditional brute-force password guessing attacks, in which an attacker tries thousands of passwords for each user account hoping to find valid credentials. In a password-spraying attack, an attacker instead attempts to log in using one common password across many user accounts. Mandiant performed the attack using an internal tool that uses the AWS API Gateway to make authentication attempts from non-attributable IP addresses that are rotated after every 25 attempts.

Password-spraying attacks are more difficult to detect than a brute force password attack. It is common to find environments that apply a policy to lock an account after a set number of failed attempts, but password-spraying attacks don't trigger the same lockouts. Since individual accounts are only tried once, one of the most common ways to identify password-spraying attacks is through statistical analysis of the number of failed authentications from a singular IP address. To avoid this means of detection, Mandiant configured a rolling pool of IP addresses from which requests would originate and changed source addresses after a set number of requests. Using this technique, Mandiant was able to identify multiple accounts that were using common passwords, including several hundred accounts that all used the same password. Historically, Mandiant has observed this phenomenon in organizations where a default password is configured for new accounts or after a password reset. Mandiant then uses the collected set of credentials to target common services, which may provide further insight or even access into the organization.

Services such as SharePoint and Outlook are often hosted in Azure and can be veritable treasure troves of sensitive data. While Mandiant did possess multiple sets of valid credentials, the client had configured multi-factor authentication (MFA) as a requirement to access the most used services. However, the Microsoft Graph API had not been configured with the same requirements. Using the Microsoft Graph API, Mandiant enumerated significantly more information regarding the organizational structure of the targeted environment, as well as the Conditional Access policies for the tenant. Mandiant's analysis of the Conditional Access policies revealed the existence of a set of accounts that were exempt from MFA. By targeting those accounts with further password-spraying attacks, Mandiant was able to collect additional sets of credentials, which allowed them to access a wider range of services without the need to attempt bypassing MFA.

Attacking a Password Manager Solution

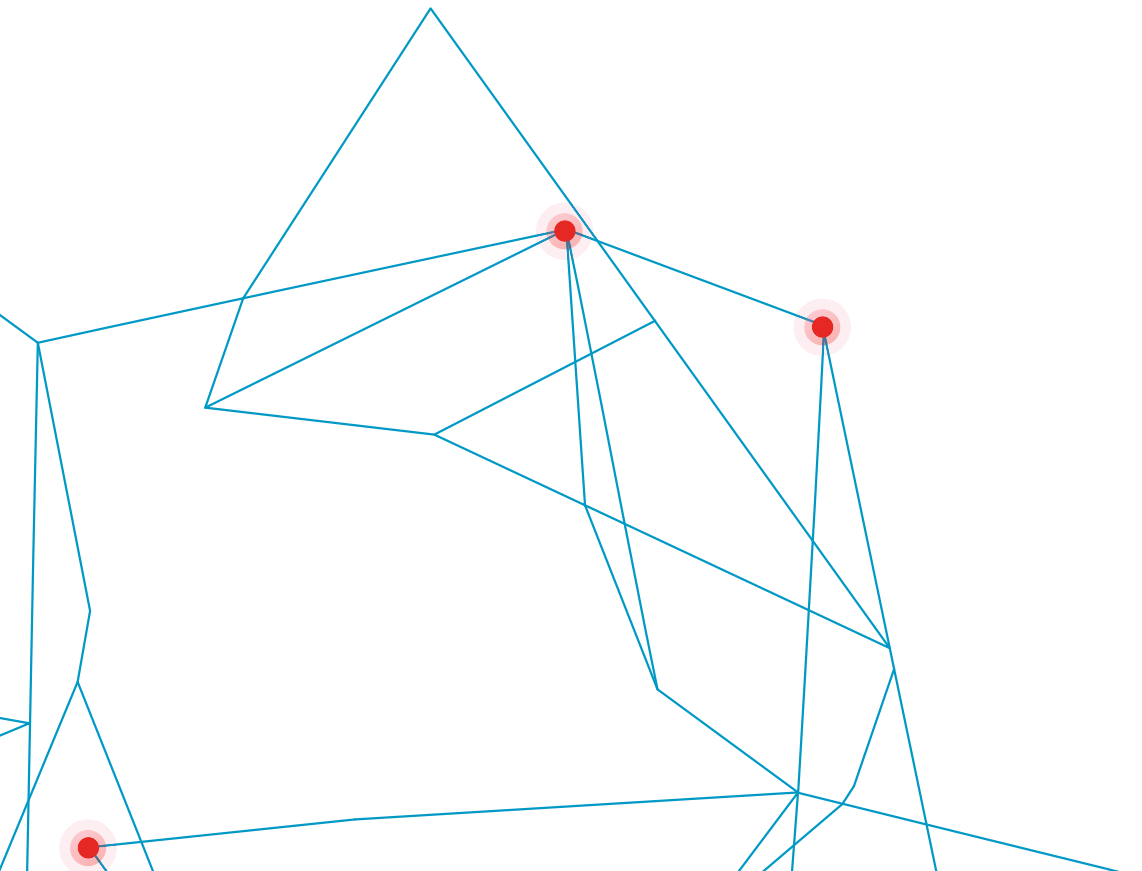
Mandiant now had access to almost a dozen endpoints at the branch office site, as well as access to Azure. On one of these endpoints, Mandiant identified an encrypted database file used by the popular password manager software KeePass. While the database was encrypted with a strong password, access to the KeePass configuration file was not secured. By modifying the configuration file, Mandiant leveraged a vulnerability in KeePass that allowed for the creation of malicious triggers in the KeePass client. Every time the KeePass password database was decrypted, the unencrypted passwords would be written to file. Once a user unlocked the database and the unencrypted passwords were written to file, Mandiant extracted the file, removed the triggers from KeePass, and deleted the file. Among the unencrypted passwords, Mandiant identified administrative credentials for several key systems within the client environment, including jump boxes used to access sensitive OT networks and internal servers. Mandiant used these credentials to move laterally and install malware on the associated machines. In one instance, a Domain Administrator was logged into one of these servers and Mandiant leveraged NanoDump to extract their credentials from memory without being detected. NanoDump is a sophisticated tool that implements functionality similar to the well-known Mimikatz utility, but includes advanced options and features that can help evade detection by antivirus (AV) and endpoint detection and response (EDR) solutions.



Gaining Visibility within Azure

While Mandiant possessed valid Domain Administrator credentials, conditional access policies that restricted administrative account access proved to be an obstacle. However, extensive internal domain reconnaissance revealed the presence of several built-in Microsoft On-Line (MSOL) accounts that were being used to synchronize the on-premises Active Directory with Azure Active Directory. If an attacker with sufficient privileges can gain access to a system performing synchronization it is possible to retrieve the MSOL account credentials in clear text. MSOL account permissions vary between deployment options, but often include the Global Reader role within Azure. With the Global Reader role, an account has visibility into all resources and properties within a tenant. Moreover, because MSOL is a service account, it is typically excluded from MFA enforcement with conditional access policies.

Mandiant used Domain Administrator credentials to obtain a session on a domain controller performing the synchronization. Using open source tooling which operated solely in-memory, Mandiant harvested the cleartext MSOL account password.



Privilege Escalation to Global Administrator Solution

The MSOL account to which Mandiant had access was the perfect position for privilege escalation within Azure due to its visibility into all resources within the cloud. Mandiant proxied browser traffic through a C2 implant to access the Azure Portal directly using the MSOL account credentials to gather valuable information regarding the tenant's application, user, and group hierarchies. Mandiant was able to confirm that, while the customer had implemented strong conditional access policies for all privileged accounts, the MSOL account was not restricted.

Mandiant identified that the Microsoft Office 365 application had the Global Administrator role within Azure. If Mandiant could identify an on-premises service account with the permission to add owners to the Microsoft Office 365 application, it could provide a path towards the Global Administrator role. A key condition to exploit this was the vulnerable user being an on-premises account rather than one that exists only in Azure AD. Mandiant's access to Domain Admin credentials allowed for the creation of what is commonly called a Silver Ticket for any synchronized on-premises account. A Silver Ticket allows an attacker to forge a Ticket Granting Service (TGS) ticket for a service that can be used in a pass-the-ticket attack. The machine hash of the system responsible for synchronization of AD and Azure AD is used to sign tickets for authentication to the Azure web portal. In this instance, Mandiant forged a ticket for an on-premise service account with permissions to add owners to the Microsoft Office 365 application. Once the Silver Ticket was loaded within a browser session with access to the Azure Portal, Mandiant add edits account as an owner of the Microsoft Office 365 application. With full ownership over a Service Principal (SP), a user within Azure can assume the identity of the service by creating certificates or credentials for the SP. Mandiant was able to impersonate the Microsoft Office 365 SP and obtain all privileges associated with the Global Administrator role.

Attacking the Software Development Life Cycle (SDLC)

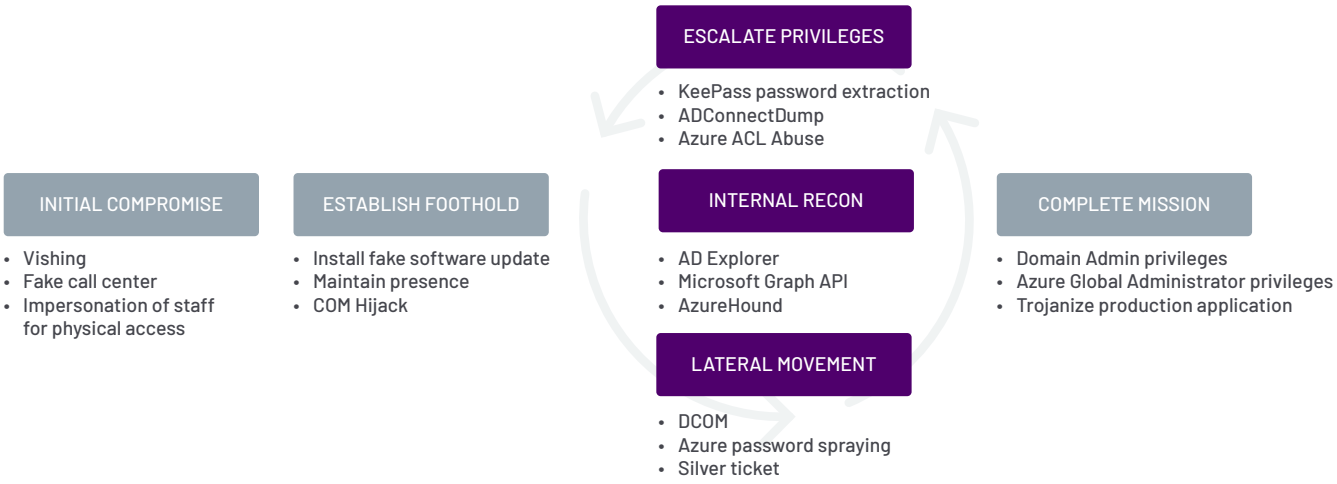
After gaining full Global Administrator access to the client's environment, Mandiant was ready to approach the ultimate objective of the engagement, which was to poison the SDLC of the client by injecting malicious code into an application. Many of the business processes within the client environment ran through custom applications. Mandiant targeted a JavaScript-based internal web application that would often be included in internal applications to produce a chat prompt with technical support personnel. The code for the chat prompt was hosted within Azure Blob storage, which allows for the storage of unstructured data such as text, images, audio visual components, and even binary large objects (BLOBs). This architecture provided the necessary means through which Mandiant could poison the Blob Storage container, which stored the JavaScript source code of the chat prompt.

Mandiant worked with the client to design a backdoor that would provide a realistic proof-of-concept demonstration without disruption to the applications on which the chat prompt was used. Malicious code injected into the JavaScript source would propagate to multiple internal applications, initiating a state change that met the parameters laid out by the client. A user visiting any of the dozens of impacted web applications within the client network would load the poisoned JavaScript code into their browser session. Extensive internal monitoring and change control systems allowed for early detection of the implanted code, and within 15 minutes the customer's security team had reverted the change and activated their incident response process.

Outcomes

The constantly evolving cybersecurity landscape continuously produces new challenges for defenders and attackers alike. Threat actors constantly innovate on their approach to social engineering, which, in turn, pushes security personnel to develop better protections and training for users. Hybrid on-premise networks connected to the cloud create unique challenges in security that require extensive planning and operational changes to address, while attackers operate without similar limitations and are guided only by their objectives. Similarly, multiple layers of identity management and application deployment create a new verticality to client environments that must be secured. It is not uncommon for misconfigurations to arise as the implementation and design phases of cloud service migrations meet the hard reality of business operations. Organizations should consider testing their cloud architecture deployments to promote resilience against motivated, agile adversaries.

Targeted Attack Lifecycle Mapping



2022 Campaigns and Global Events

Mandiant gains knowledge of threat actors during frontline investigations, analysis of public reporting, information sharing, and other research. In 2022, Mandiant Intelligence established the Campaign and Global Events (CGE) team to illuminate high-impact, multi-targeted intrusion activity and provide actionable threat intelligence to defenders. Each Campaign or Global Event profile includes indicators of compromise, notable adversary host commands, and in-depth analysis and context surrounding the tactics, techniques, and procedures (TTPs) used by the threat actors, complete with mappings to the MITRE ATT&CK framework. By providing this information overlaid with context and analysis, defenders are empowered to respond to these threats more effectively.

Campaigns—Threat Actors

Mandiant defenders responded to extremely impactful campaigns in 2022, ranging from state-sponsored espionage to financially motivated extortion. Mandiant defenders went head-to-head with multiple campaigns involving compromised USBs and other external devices that spread malware far and wide across targeted environments. The identification of these campaigns provided Mandiant services with actionable data to create new real-time detections, develop and expand existing threat hunting missions, and establish high-fidelity automatic containment guidelines to isolate affected systems at the outset of emerging threat activity. In 2022, among the notable campaigns tracked by the CGE team, APT29, BASTA ransomware operators, and threat groups leveraging USB-based malware provided illustrative examples of complex threat actor activity being distilled into actionable intelligence by this initiative.

APT29

APT29 is a cyber espionage threat group that has leveraged innovative TTPs against humanitarian groups, think tanks, defense, and diplomatic institutions in Europe and North America. Following the continued tensions between Russia and Ukraine in the beginning of 2022, Mandiant established the Ukraine Crisis Resource Center to monitor and prepare the wider community for a potential increase in Russian Cyber Activity. This Center provides customers and the community with valuable resources to proactively harden their environments against destructive attacks, highlights Russian information operations, and provides an overview of Russian cyber capabilities. Given historical campaigns against Ukrainian and western targets by Russia, Mandiant notified the community of suspected increases in retaliations from various Russian cyber threat groups. This notification included an outlook on various impacts to industries of high value for disruption such as the Energy, Financial and Transportation sectors, along with notable threat groups and each group's noteworthy techniques.

In 2022, Mandiant continued to track APT29 targeting organizations through non-traditional vectors in an attempt to remain undetected and achieve their mission objectives. In January 2022, approximately a month prior to Russia's invasion of Ukraine, APT29 initiated a phishing campaign targeting diplomatic entities primarily located in Europe. Over the ensuing months, APT29 continued to target multiple organizations within private industries with unique tactics, focusing heavily on obtaining email addresses. Mandiant launched two campaigns tracking specific APT29 activity.

Highlighted Activity

APT29 Conducts Phishing Campaign Targeting Multiple National Government Agencies

APT29 sent phishing emails designed to appear as administrative notices related to embassies that were relevant to the targeted organizations. The phishing emails utilized legitimate but co-opted email addresses to send emails containing malicious attachments. These attachments ultimately led to backdoors that used legitimate services for command and control (C2). Historically, APT29 made extensive use of a dropper that retrieved BEACON from a third-party cloud service. Mandiant observed an operational shift in February 2022 when APT29 began to deploy a simpler dropper that relied on co-opted infrastructure.

APT29 Targeting Organizations with QUIETEXIT Tunneler

A secondary campaign by APT29 targeted multiple organizations, where the group proxied their traffic through compromised video conferencing cameras (largely LifeSize TelePresence devices). APT29 deployed the QUIETEXIT tunneler to route traffic through compromised environments. QUIETEXIT is a modified version of the publicly available Dropbear software, which can provide an SSH reverse shell. APT29 meticulously targeted a specific subset of mailboxes, zeroing in on the executive teams and key employees involved in corporate development, mergers and acquisitions, large-scale business transactions, and IT security. The group utilized compromised usernames and passwords of privileged Exchange accounts to gain access and employed the use of "GetFolder" and "FindFolder" requests to enumerate mailboxes of interest. By using a "FindItem" query filter against targeted folders, APT29 was able to harvest all mailbox items created since their last data extraction.

Outlook

APT29 is a highly active and sophisticated threat group that has conducted numerous high-profile incidents globally. Most notably, the SolarWinds supply chain compromise that affected governments and corporations worldwide has been attributed to APT29 by Mandiant. Throughout 2022, alongside the ongoing Russian invasion of Ukraine, APT29 operations have concentrated on European diplomatic entities, almost certainly to meet ongoing Russian intelligence priorities concerning Western responses to the war and financial and military assistance provided to Ukraine. As the war moves into its second year and Western governments deepen their commitment to supporting Ukraine, Russia is likely to intensify these cyber espionage efforts to gather intelligence and shape Russia's posture in Ukraine and globally.

APT29 has continually refined and monitored their operations to maximize effectiveness and evade detection by minimizing C2 payload availability, using advanced endpoint detection mitigation techniques and, in some campaigns, using one-time encryption of payloads. APT29's evasion techniques will likely continue as they seek to avoid detection and accomplish their mission.

BASTA Ransomware

In mid-2022, Mandiant observed a significant shift in financially motivated activity from threat actors suspected to be based in Eastern Europe. In conjunction with increased public coverage and scrutiny of CONTI-affiliated actors, BASTA (aka BlackBasta) ransomware emerged onto the scene. CONTI operators developed a prolific crime syndicate that aggressively leveraged ransomware to extort victims. At the time, Mandiant suspected BASTA to be a rebrand by CONTI ransomware operators and affiliates, as a logical next step to avoid the increased scrutiny. Mandiant identified evidence to suggest at least one threat actor had incorporated BASTA ransomware into their operations as a direct replacement for CONTI ransomware. CONTI operations were officially shut down in late May 2022, shortly after the emergence of BASTA operations in April 2022. Mandiant created two campaigns to track active BASTA ransomware deployment efforts.

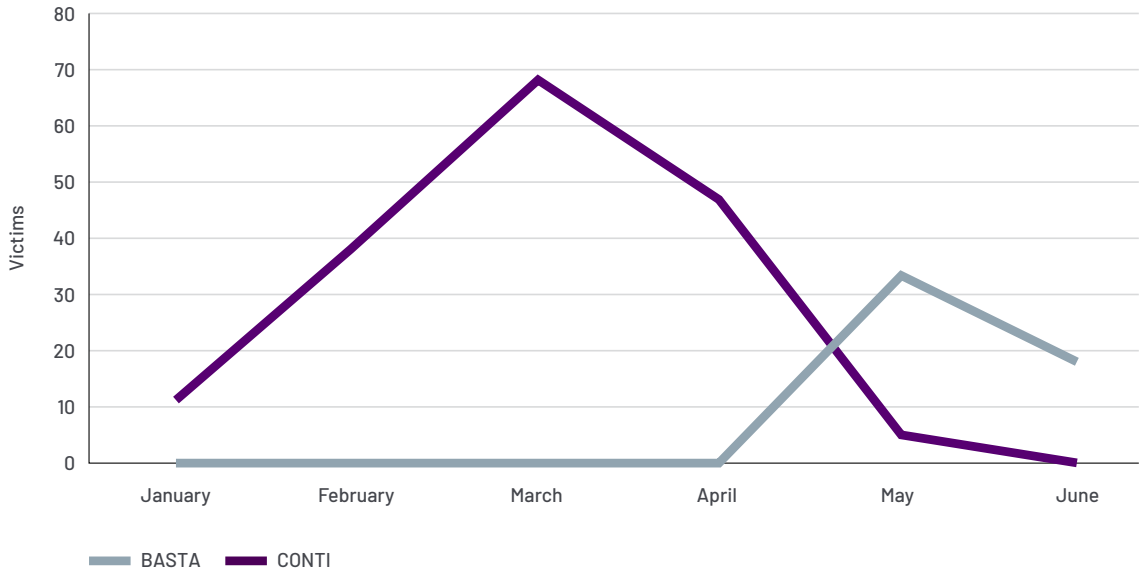


Figure 2. Victims added to CONTI and BASTA DLS sites (2022)

Highlighted Activity

Financially Motivated Actor Gains Access to Organizations through Third Party to Deploy BASTA Ransomware and Extort Victims

In June, Mandiant was made aware of a supply chain enabled compromise impacting credit unions in western Canada via infrastructure managed by a shared service provider. While gaining access via a third party is not novel, it is relatively rare for extortion operations. In some of these cases the actors responsible, which Mandiant tracks as UNC3973, used the SYSTEMBC tunneler for post-exploitation operations and attempted to deploy BASTA ransomware. Capitalizing on centralized access, UNC3973 utilized an unauthorized service account with domain administrator privileges shared between a compromised MSSP and targeted organizations to gain access to each environment. The attackers then employed a batch script that attempted to disable antivirus software and created a scheduled task to deploy SYSTEMBC, a tool used to proxy traffic through infected endpoints. However, the SYSTEMBC binary was detected and quarantined by the system's antivirus software. In a further attempt to ransom the network, the attackers created a Windows service to launch the BASTA ransomware. Fortunately, the system's endpoint antivirus software was able to detect and quarantine the malware regardless of attempted interference from UNC3973.

Suspected Financially Motivated Actor Obtains Access via QAKBOT to Deploy BASTA Ransomware

In October 2022, Mandiant responded to multiple intrusions where attackers deployed BASTA ransomware following a widespread QAKBOT phishing campaign. Mandiant observed the distribution threat cluster UNC2633 leverage QAKBOT to gain initial access to target environments. The QAKBOT compromises were then leveraged to provide a second threat cluster, UNC4393, with access to environments of interest. UNC4393 then proceeded to deploy various tools, including BEACON and the SYSTEMBC tunneler, before using Rclone to steal data from the environment and deploying BASTA ransomware. In some cases, UNC4393 has monetized their presence in an environment within just a few days of gaining access. This rapid pace is consistent with other threat clusters associated with CONTI. Historically, UNC2633 has also been a frequent collaborator with clusters Mandiant tracks within the CONTI ecosystem.

Outlook

Mandiant continues to cluster and track ransomware activity based on unique TTPs in order to evaluate the evolution of the criminal underground. While these two campaigns represent the use of BASTA ransomware, the components of the incidents shed light on how different actors complete missions using the same ransomware variants. As law enforcement efforts continue to stymie the criminal ecosystem, ransomware operators reinvent ways to maintain operational speed and consistency as they cycle through ransomware variants to carry out their missions.

USB-based Compromises leading to Financially Motivated and Espionage Related Threat Actor Activity

Throughout 2022, Mandiant observed several campaigns involving the use of infected USB drives and other external drives to spread malicious payloads. Responsible actors include a financially motivated group thought to be associated with the larger Evil Corp ecosystem, and espionage groups acting in accordance with Chinese nation-state interests. In response, Mandiant initiated multiple campaigns to track activity and threat clusters associated with the USB-based compromise.

Highlighted Activity

Actor of Unknown Motivation Distributes BIRDBAIT via Infected USB Drives

This campaign involves the execution of a worm propagated from USB-based storage media by a threat cluster Mandiant tracks as UNC3840. The worm creates and launches a shortcut file containing an embedded command that executes the Windows Standard Installer binary, Msiexec.exe, to download and execute a remotely hosted payload. Mandiant observed a malware chain that included the BIRDBAIT LNK downloader, DENSEDROP, and DENSELAUNCH. DENSEDROP, a highly obfuscated PE 32-bit in-memory dropper, ultimately launches DENSELAUNCH, a C++ Win32 DLL loader that writes arbitrary code into designated process memory space. Notably, in incidents where UNC3840 utilized the BIRDBAIT LNK downloader, C2 infrastructure generally resolved to IP addresses that appear to be compromised network attached storage (NAS) devices.

Early in the campaign there was little evidence of significant follow-on activity after the deployment of DENSELAUNCH and DENSEDROP but the tracking of activity throughout 2022 led to the identification of additional malware families such as FRUITBIRD. It is likely that FRUITBIRD, which is launched by DENSEDROP after satisfying multiple environment checks, is being used to distribute additional payloads including malware, adware, and HOLA VPN installers. This activity suggests the threat actors behind UNC3840 may be utilizing their malware as a pay-per-install (PPI) service which could provide an intrusion vector for other threat actors.

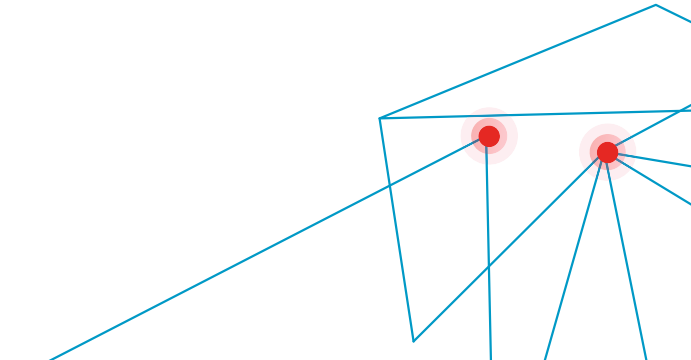
While Mandiant's insight into UNC3840 operations is limited, it is highly plausible that UNC3840 distributes payloads or provides services like pay-per-install access to multiple third parties. Mandiant's analysis of malware used by UNC3840 and other financially motivated threat actors has revealed potential overlaps with other tracked clusters. These overlaps include a packer that was leveraged in campaigns distributing URSNIF, and use of the LONGFALL crypter (also referred to as CryptOne), which has been used by various malware families including some associated with Evil Corp. Mandiant has observed a small number of cases where the FAKEUPDATES malware was deployed following UNC3840 infections. Threat actors that often use access provided by FAKEUPDATES also contain overlaps with Evil Corp.

The identification of Msiexec.exe processes launched with command line arguments which contained a URI proved to be an effective means of detecting the download of potentially malicious payloads. Mandiant identified activity which was later clustered under UNC3840 having occurred as early as September 2021.

Suspected Espionage Actor with China Nexus Spreading Malware via Infected USB Devices

Mandiant identified malicious activity tracked as UNC4191 targeting a range of public and private sector entities based primarily in Southeast Asia, but also in the U.S., Europe, and Oceania. The activity began in April 2022 and continued throughout the year, and leveraged infected USB devices as the initial intrusion vector for the campaign. In successful infections, malware deployment included the launchers MISTCLOAK and BLUEHAZE, the latter of which executes a copy of the ncat network utility to create a reverse shell to a hardcoded domain. Mandiant also identified evidence of the DARKDEW dropper, which is capable of collecting files from air-gapped systems and further propagating by infecting attached removable drives. Mandiant suspects this activity is indicative of Chinese operations intended to gain and maintain access to public and private entities in order to collect intelligence in support of China's strategic political and commercial interests. Based on malware similarities with the TWOPIPE dropper, there is some indication that UNC4191 activity is related to China-nexus operations associated with the actor tracked as UNC53. UNC53, also referred to as TEMP.Hex, is a prolific threat actor that targets public and private sector organizations on a global scale, and is suspected to be associated with China's Ministry of State Security.

Following the initial discovery of the UNC4191 campaign, Mandiant identified evidence of compromise leveraging MISTCLOAK, DARKDEW, and BLUEHAZE across multiple organizations. As analysts worked through the process of triaging impacted systems and notifying customers, Mandiant identified a pattern of targeting where the affected systems were physically located in the Philippines. This provided more context on regional targeting that Mandiant has observed to be consistent with various Chinese cyber espionage activities.



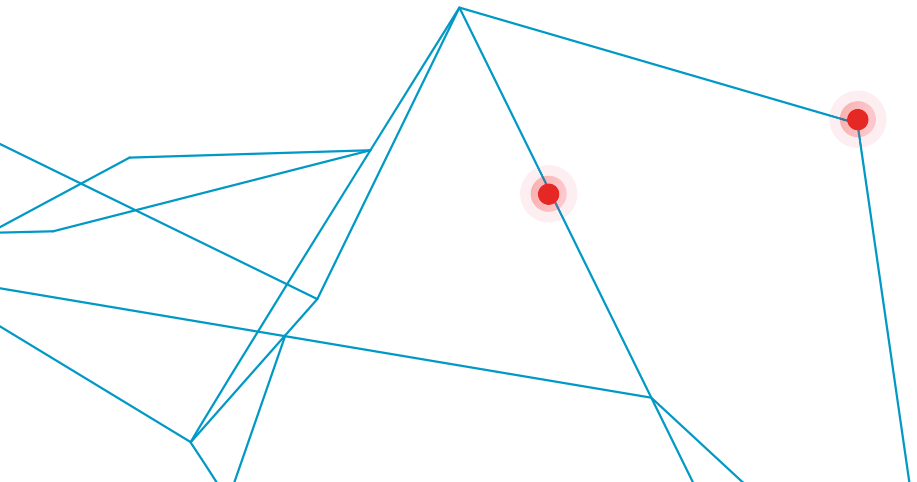
Suspected Espionage Group with a China Nexus Conducts USB Operations

Throughout 2022, Mandiant observed the suspected China-nexus actor UNC53 target a variety of industries across the globe. In some cases, UNC53 gained initial access to targeted environments through infected USB drives, leveraging legitimate binaries to side-load malicious DLLs and encrypted payloads that drop a SOGU variant. This activity is likely part of a long-term effort to gain access to and collect strategic data from multiple sectors around the globe, with activity involving this SOGU variant reaching as far back as 2020. Previously observed operations suspected to be linked to UNC53 also leveraged SOGU variants against multiple sectors in the Southeast Asia region in 2021.

Mandiant developed real-time detection signatures specific to these malware families as well as additional detections content focused on identifying malware replication through removable media. These efforts led to additional discoveries of USB-based compromise by UNC53 across multiple organizations along with deployment of SOGU, KORPLUG, and FLOOPYSTAMP. Mandiant's detection capability not only resulted in increased detection of UNC53 compromises, but also led to discovery of unrelated worm infections.

Outlook

Compromised removable devices are an effective technique for gaining access to a targeted environment and have resulted in impactful breaches. This initial intrusion vector and propagation mechanism has been leveraged by financially motivated threat actors and by threat actors tasked with intelligence collection for espionage purposes. Threat actors benefit from compromising systems that are a degree or two of separation from their intended target, such as hotel business offices and personal computers, that exist outside of an organization's technical controls and monitoring. Without strict technical controls on removable drive usage, this proximity provides threat actors with continual opportunities to gain access to an environment.



Global Events—Notable Vulnerabilities

Vulnerability disclosure has always been a vital pillar of the security community. As technology develops, spreads, and becomes embedded in the lives of people around the world, the identification and responsible disclosure of vulnerabilities within those technologies has served to protect people and their data. Public disclosure of vulnerabilities became more commonplace and led to the necessary conversations about maintenance and patching as a practice not only in the technology space, but within the general public. The need to assess potential impact, protect operations, and ultimately safeguard user data and experiences has over the years become more and more valuable. Unsurprisingly, threat actors of every type have learned similar lessons.

As new vulnerabilities are discovered, questions commonly arise around whether attackers are already using the vulnerability to further their goals. If data doesn't exist to support the idea that organizations are being successfully targeted using the vulnerability, it's often not for lack of trying on the attacker's part. Since the process of addressing newly released vulnerabilities is an exercise in cost-benefit analysis, a vulnerability that represents risk to the user is likely an unequal opportunity for threat actors. While operations teams must meet Service Level Agreements with respect to availability, threat actors are under no such limitation. Where Systems Administrators need time to test and validate patches, threat actors need only the barest coverage in proof-of-concept (PoC) code to start targeting those organizations.

This interplay of the need to react and the opportunity to attack gave rise to a process within Mandiant that we refer to as a "Global Event." Mandiant initiates a Global Event when the disclosed vulnerability represents a great enough threat, and malicious actors are observed attempting to exploit it in the wild. Of the over 20,000 vulnerabilities disclosed and published as CVEs in 2022, Mandiant initiated nine Global Events based on a variety of assessment criteria. Throughout 2022, Mandiant worked to track exploitation of and provide detections for several significant vulnerabilities, including Log4Shell, Follina, and a series of vulnerabilities impacting VMWare.

Log4Shell

On December 09, 2021, a vulnerability in the Java logging framework Log4j was publicized by the Lunasec team and dubbed Log4Shell. The vulnerability allowed for arbitrary Java code execution through malicious user input when processed via the Java Naming and Directory Interface (JNDI) features in Log4j. Apache, which owns the Log4j project, gave the vulnerability a 10, the highest possible rating, in the Common Vulnerability Scoring System (CVSS), and the vulnerability was published as CVE-2021-44228. Due to the vulnerability existing in Log4j since 2013 and the broad usage of Log4j as a logging framework, estimates of the potential impact appeared to be widespread and necessitated the immediate review of existing codebases in products and platforms around the world. Mandiant rated the risk associated with Log4Shell as Critical based on the public availability of PoC code as well as the trivial nature of the exploit, and anticipated exploitation of the vulnerability to begin and ramp up quickly in intensity and scope. Mandiant initiated a Global Event in response to Log4Shell on December 10, 2021, and, due to the extensive nature of compromises identified, continued the workflows well into 2022.

Predictions that the risk presented by Log4Shell would be global in nature were quickly proven to be accurate. Mandiant observed widespread scanning and exploitation attempts across a variety of customers by numerous distinct threat actors resulting in the deployment of a diverse set of malware. Few industry verticals, if any, were spared in the near constant scanning and subsequent exploitation attempts following the publication of PoC code. By the close of the Global Event workflows, over 1,000 IP addresses associated with attempted and successful exploitation of Log4Shell had been published to Mandiant's collection of indicators.

The ubiquitous presence of Log4j as a supporting library in larger applications further complicated efforts to secure environments. While vendors prioritized the identification and patching of vulnerable products, legacy products presented a substantial risk to both the continuity of business operations and the security of the environments in which they existed. Patches for legacy applications that use Log4j were often delayed or, in some cases, never provided. In the event that a legacy product could not be patched, organizations were reliant on significant mitigation efforts that required regular maintenance and review. Mandiant recommended mitigations in the form of isolation and monitoring for any instance of a vulnerable version of Log4j. As organizations performed initial scoping for the Log4Shell vulnerability, business critical products that could not be brought offline could, instead, have network ingress and egress restricted to limit risk while solutions or replacements were pursued. Restricting access to the application interfaces of impacted products aids in reducing the potential attack surface while limiting egress traffic prevents the Java service from accessing malicious class files used during exploitation. When paired with monitoring and filtering of both outbound DNS requests from and inbound HTTP requests to impacted products, organizations that could not patch in the near term would have what amounts to an early warning system for potential impact as exploitation attempts of Log4Shell began to intensify.

Exploitation of Log4Shell followed a pattern commonly seen with high criticality vulnerabilities in products with large scale deployments. Opportunistic attackers quickly targeted organizations through the vulnerability to earn easy wins and install cryptominers in wide scale attacks. However, in short order, actors leveraged the vulnerability in ransomware campaigns as a means of gaining an initial foothold into more rewarding targets. While Log4Shell impacted a large swath of Java-based platforms from Minecraft to Apple iCloud, services such as the mobile device management platform MobileIron stood out from the pack in terms of targeting. Mandiant observed groups such as UNC961 leveraging the Log4Shell vulnerability within HTTP header Cookie values within days of the publication of the vulnerability. UNC961, a financially motivated threat actor, is notable for its ability to capitalize on vulnerabilities that represent a broad opportunity for target selection, and favors web-based exploitation as a means of initial access. UNC961 crafted malicious requests to the MobileIron instances that would provide reverse-shell capabilities to the threat actor once the request was processed through Log4j. UNC961 took steps to hinder forensic analysis once successful exploitation had been achieved before seeking to establish persistence within the environment. UNC961 would also move from a simple reverse shell to a variant of the HOLEPUNCH tunneler capable of multiplexing connections back to command and control nodes.

Finally, cyber espionage groups wasted no time in exploiting critical services, which included using Log4j as a means to gain an initial foothold and progress toward their objectives. Mandiant observed APT41, a Chinese state-sponsored espionage group, target vulnerable MobileIron deployments in a similar fashion as UNC961. APT41 was observed targeting government entities, telecom companies, and financial organizations. Similarly, APT41's post-exploitation activity included anti-forensics techniques and pivoting from a simple reverse shell to a more feature-rich backdoor. While the methodologies of groups such as UNC961 and APT41 bear a resemblance in these instances, such distinction is driven primarily by the limitations of the environment and the quick turnaround time on Log4Shell PoC code.

In total, Mandiant published 1,632 indicators related to threat actor activity with Log4Shell during the Global Event.

Follina

In late March of 2022, Mandiant observed multiple suspected Chinese espionage clusters exploiting a zero-day vulnerability in the Microsoft Diagnostic Tool (MSDT) that allowed for the execution of arbitrary code. The vulnerability, published by Microsoft on May 30, 2022, was given the CVE identifier CVE-2022-30190 and came to be known as "Follina." While the vulnerability was given a 7.8 CVSS score, it requires the attacker to craft a special URL to call to MSDT, and for the user to open it on a vulnerable system, which influenced Mandiant's "Medium Risk" assessment. Following publication by Microsoft, Mandiant observed increased exploitation of Follina from government backed threat groups and financially motivated attackers.

The documents leveraged to deliver the Follina exploits during these operations were all likely delivered via spear phishing and, based on the document creation dates and sample submissions, operations exploiting the vulnerability began in late March or early April 2022. Despite a lack of widespread exploitation, Mandiant observed UNC3347, UNC3784, and UNC3819 leverage the Follina vulnerability to target organizations in India, Nepal, Belarus, Russia, and the Philippines. While these threat clusters are distinct, all three are associated with suspected Chinese cyber espionage activity. The distribution of a zero-day exploit to multiple Chinese threat groups, covering a broad geographic region, is consistent with the theory of a centralized digital quartermaster supporting Chinese cyber espionage. Similarly, the distribution of malware across multiple clusters presents a challenge to attribution, making it more difficult to differentiate specific Chinese threat group activity.

Both UNC3784 and APT28, Russian and suspected Chinese espionage groups, leveraged Follina in their attempts to target government organizations. In early June of 2022, APT28 compromised a government organization in EMEA using a password spraying attack, and used the compromised email account to send spear phishing emails to organizations in Ukraine. UNC3784 deployed backdoors and downloaders against government organizations in Southeast Asia.

While the elevated difficulty of exploitation may have restricted use of Follina to threat actors that selectively target organizations, Mandiant did observe instances where Follina was used for potential financial gain as well. A distribution threat cluster which Mandiant tracks as UNC2633 began to exploit Follina in early June of 2022 to deliver variants of the backdoor QAKBOT. UNC2633 has historically targeted broad selections of industries and is often observed as a precursor to ransomware operations. Mandiant also observed threat actors operating in underground forums advertising private exploits that would enable other threat actors to exploit Follina. The availability of exploit code implies additional actors may attempt to exploit Follina in future campaigns.

Mandiant published 84 indicators related to threat actor activity with Follina.

VMware Vulnerability Chaining

On May 18, 2022, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued an Emergency Directive[4] regarding threat actors chaining vulnerabilities in VMware products to gain privileged access to target systems. The vulnerabilities in question, CVE-2022-22954, CVE-2022-22960, CVE-2022-22972, and CVE-2022-22973, impact multiple VMware products and, when used together, may result in privilege escalation or remote code execution. In specific, CVE-2022-22954, which had been published on April 6, 2022, detailed a vulnerability that allows an attacker to perform server-side template injection on vulnerable instances of VMware's Workspace ONE Access product. Mandiant's analysis of CVE-2022-22954 provided a risk rating of High given the public availability of exploit code and confirmed exploitation of the vulnerability in the wild.

CISA's directive required federal agencies to mitigate the associated risks after reports of widespread exploitation, and led to speculation on potential impacts for both government entities and private organizations. Given the ubiquity of VMware, high concerns regarding the vulnerabilities and a need to triage potential exploitation attempts led to Mandiant's initiation of a Global Event on May 23, 2022. Mandiant observed evidence to indicate successful exploitation of CVE-2022-22954 as early as April 8, 2022, two days after the vulnerability was disclosed by VMware. Initial exploitation attempts appeared to successfully dump credentials from vulnerable VMware applications by accessing the /etc/shadow and /etc/passwd files.

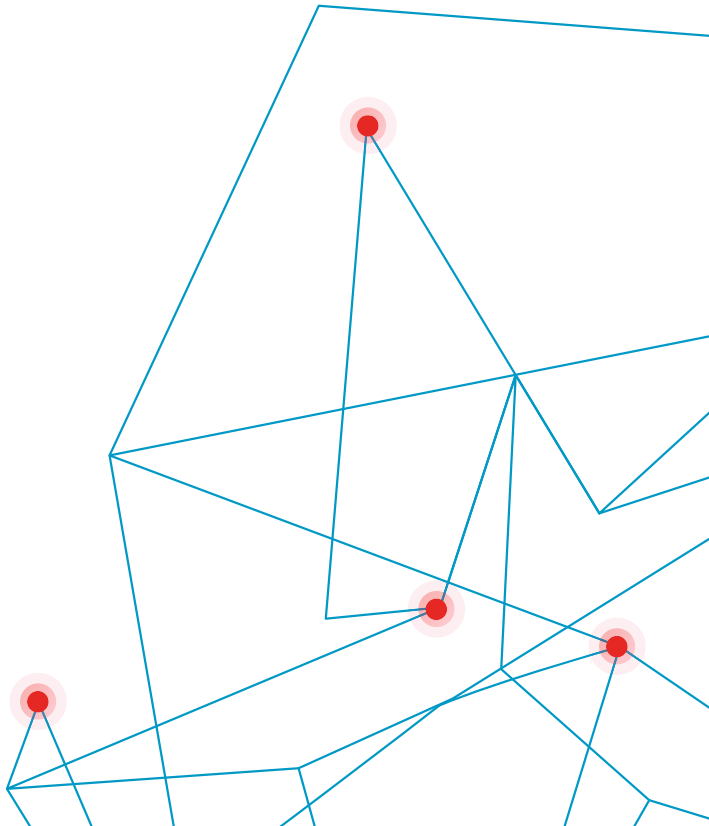
Mandiant observed financially motivated attackers and suspected Russian nexus attackers exploit CVE-2022-22954. The vulnerability was also exploited by UNC3905, a ransomware-as-a-service affiliate that has carried out data exfiltration against U.S.-based organizations. UNC961, which has provided access to targeted organizations on at least two occasions, targeted vulnerable VMware appliances and used the scripting language Perl to download second stage malware from attacker-controlled infrastructure on April 16, 2022. On the other end of the spectrum, threat clusters UNC3711 and suspected Russian threat actor UNC3810 exploited CVE-2022-22954 for what appears to be international operations. Both UNC3711 and UNC3810 were observed exploiting the vulnerability to deliver destructive malware to organizations in Ukraine as early as April 19, 2022.

During the Global Event, Mandiant published 67 IP addresses, seven URLs, and two file hashes associated with observed attacker activity to aid organizations in their attempts to triage potential exploitation attempts.

Conclusion

Every security organization understands there are simply too many threat actors and vulnerabilities to track, mitigate, or otherwise address while maintaining business operations. It is imperative that organizations use a data-driven approach to prioritize security efforts based on relative risk and on-the-ground intelligence. Mandiant's Campaigns and Global Events initiative seeks to centralize actionable indicators of threat actor activity to assist organizations in the identification of activity likely to impact multiple organizations. While Campaigns tracking threat actor efforts and Global Events tracking potential compromise of vulnerabilities differ slightly, the intention behind both is to enable the efficient identification of compromises impacting organizations.

Mandiant assembles cross-functional teams from threat intelligence, forensics, incident response services, and beyond to consolidate as much information as is available from the onset of an impactful set of intrusions that fall within the bounds of a Campaign or Global Event. Contributors to the Campaigns and Global Events are tasked with assessing the potential impact to organizations, collecting and assessing new intelligence, and developing and deploying new detections. The rapid provisioning of intelligence analysis to potential victims allows them to make better-informed decisions about how and when to implement security measures. Mandiant's Managed Defense service both contributes to and pulls threat intelligence from the aggregated Global Event data to safeguard customer networks directly, and in many cases, provides analysis before customers are impacted by a threat.



Notable and Recently Graduated Threat Groups

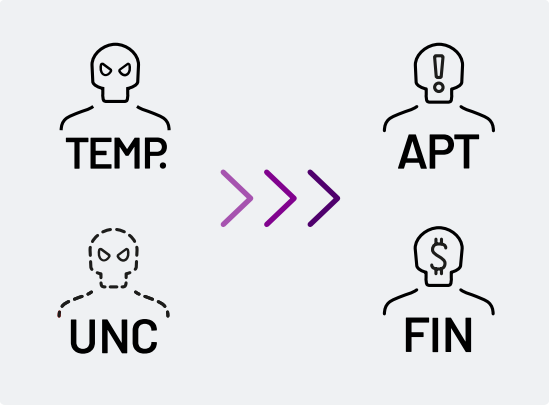
How a Threat Cluster Becomes an APT or FIN Group

Mandiant analysts review threat activity data from a variety of sources such as Mandiant incident response engagements, Managed Defense investigations, and security product telemetry to identify noteworthy clusters. When there is enough activity, but insufficient evidence to immediately attribute it to an existing threat actor or group, Mandiant creates an uncategorized (UNC) threat cluster to track the newly identified activity.

An UNC (previously referred to as TEMP) is a cluster of cyber activity that includes observable artifacts such as adversary infrastructure, tools, and tradecraft. UNCs are based on a defining, anchoring characteristic often discovered during a single incident. For example, a common anchor would be a malware sample that connects to an actor-controlled domain.

As our knowledge of a threat cluster matures, we may graduate it to an Advanced Persistent Threat (APT) group or financially motivated (FIN) group. APT groups are generally characterized by a focus on espionage operations, whereas FIN groups are characterized by criminal operations with a focus on monetization activities via methods such as ransomware deployment, payment card data theft, or business email compromise.

In 2022, Mandiant promoted one tracked threat cluster from "TEMP" designation to "APT" designation. In this report, we review APT42, an Iran-nexus espionage threat group.



APT42 Conducts Highly Targeted Surveillance Operations

In August 2022, Mandiant graduated UNC788 to APT42. Active since at least 2015, APT42 is a sophisticated cyber threat group that conducts espionage operations using highly targeted spear phishing and social engineering techniques. APT42 likely operates on behalf of the Islamic Revolutionary Guard Corps (IRGC) Intelligence Organization (IRGC-IO) based on targeting patterns that align with the organization's operational mandates and priorities, including defending the regime against internal and external threats, pursuing perceived domestic enemies, and confronting "revolutionary" ideas emanating from the West.

Global Targeting of Iranian Regime Opponents

APT42 operations largely focus on the Middle East region and primarily target organizations and individuals deemed opponents of the Iranian regime. APT42 has consistently targeted Western think tanks, researchers, journalists, current Western government officials, former Iranian government officials, and the Iranian diaspora abroad.

Some APT42-linked activity indicates the group alters its operational focus as Iran's priorities evolve. With the onset of the COVID-19 pandemic in March 2020, Mandiant observed a shift to include operations targeting the pharmaceutical sector. APT42 similarly shifted targeting to domestic and foreign-based opposition groups prior to the Iranian presidential election.

Building Trust and Rapport

APT42 often attempts to build rapport with their target by impersonating journalists or researchers and engaging the target in benign conversation for multiple days or weeks before sending a malicious link. In some cases, the group has infiltrated email accounts and then targeted colleagues, acquaintances, and relatives of initial victims. APT42 operations have also included credential harvesting to collect multi-factor authentication (MFA) codes to bypass authentication methods.

Between March and June of 2021, APT42 used a compromised email account belonging to a U.S.-based think tank employee to target Middle East researchers at other think tanks and academic organizations, U.S. government officials involved in Middle East and Iran policy, a former Iranian government official, and high-ranking members of an Iranian opposition group. APT42 posed as a well-known journalist requesting an interview and engaged the initial target for 37 days to gain their trust before finally directing them to a credential harvesting page.

In other instances, APT42 provided a Dropbox link to a PDF with an embedded URL-shortening link that led to a credential harvesting page. After sending an email from the compromised inbox, they attempted to cover their tracks by deleting the message from the victim's Sent folder. They also made careful attempts to access their targets' personal email accounts. APT42 bypassed multi-factor authentication by capturing SMS-based one-time passwords and setting up two-factor verification.

Surveillance Operations

APT42 also leverages mobile malware to conduct surveillance against individuals of interest. Targets include those connected to the Green Movement in Iran and other political targets.

APT42 has also targeted individuals who claimed to be able to provide tools to bypass government restrictions. During surveillance operations, APT42 has deployed VINETHORN and PINEFLOWER Android mobile malware to track victim locations, record phone conversations, access videos and images, and extract entire SMS inboxes.

Use of Custom Tools

APT42 operations are heavily focused on credential harvesting, but they also use several custom backdoors and tools. In September 2021, APT42 used a compromised European government email account to send a phishing email to nearly 150 email addresses associated with individuals or entities employed by or affiliated with civil society, government, or intergovernmental organizations around the world. The email purported to be related to the organizational chart of an embassy in Tehran and contained a link to a malicious macro document, which led to TAMECAT malware, a PowerShell toehold backdoor.

From January to March 22, APT42 leveraged various tactics, including hosting malicious Office documents on file-sharing platforms to deliver spear-phishing emails, and hosting malicious PowerShell code designed to retrieve payloads, including custom reconnaissance tools to collect system information and local account names.

Outlook

APT42 activity poses a threat to foreign policy officials, commentators, and journalists working on Iran-related projects particularly those in the United States, the United Kingdom, and Israel. Additionally, the group's surveillance activity highlights the real-world risk to individual targets, including Iranian dual-nationals, former government officials, and dissidents both inside Iran and those who previously left the country.

Given the long history of activity and imperviousness to infrastructure takedowns and media reports, we do not anticipate significant changes to APT42's operational tactics and mandate. Nevertheless, the group has displayed an ability to rapidly alter its operational focus as Iran's priorities change over time with evolving domestic and geopolitical conditions.

Conclusion

In M-Trends 2023, we have highlighted positive trends such as improved detection times, and more challenging ones such as the situation in Ukraine and the merging of the real and cyber worlds. But these are not the only observations and takeaways.

Overall, attackers are not giving up. In fact, we're seeing attackers cause bigger impacts with less skills. They're also more brazen, and willing to get much more aggressive and personal to achieve their goals. They will bully and threaten, and ignore the traditional cyber rules of engagement. It's not enough to just protect systems these days, employees need to be protected as well.

To ensure our customers are protected against the latest and most relevant tactics, techniques and procedures, we have adopted these same brazen tactics in our red team engagements. As shared in our case study, part of how we gained initial access was by showing up in person pretending to be a technician—a bold tactic. We're seeing increased focus on cyber hygiene, which is great, but organizations must continue to be vigilant in all forms of security.

Preparation is vital, but performing red team engagements isn't the only way to be ready. Organizations should consider tabletop exercises, training exercises, and other techniques. Sound fundamentals, such as vulnerability and exposure management, least privilege, and hardening also play a role in building strong defenses. Cloud considerations are also important. Our red team case study demonstrates just how challenging security can be in hybrid networks connected to the cloud.

Our mission at Mandiant is to ensure every organization is secure from cyber threats and confident in their readiness. Our Campaigns and Global Events article highlights how Mandiant shares valuable intelligence and indicators to help our clients and the community protect themselves from significant campaigns and vulnerabilities.

The annual M-Trends report, featuring data and learnings from our engagements, also plays a big part in advancing our mission.

At the heart of any cyber defense capability is the intelligence that drives it, and the best threat intelligence is gleaned directly from the frontlines. Mandiant will continue to share its frontline knowledge in M-Trends to improve our collective security awareness, understanding, and capabilities—and to ensure that organizations can stay relentless in their cyber security efforts.

Bibliography

1. "Apache Log4j Vulnerability Guidance". Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/news-events/news/apache-log4j-vulnerability-guidance

2. "Threat Actors Exploiting F5 BIG-IP CVE-2022-1388". Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-138a

3. "Threat Actors Chaining Unpatched VMware Vulnerabilities for Full System Control". Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-138b

4. Vanderlee, Kelli. "DebUNCing Attribution: How Mandiant Tracks Uncategorized Threat Actors". Mandiant, https://www.mandiant.com/resources/blog/how-mandiant-tracks-uncategorized-threat-actors

5. Franceschi-Bicchierai, Lorenzo. "FBI accuses North Korean government hackers of stealing $100M in Harmony bridge theft". TechCrunch, https://techcrunch.com/2023/01/24/north-korea-fbi-harmony-horizon-crypto/

Learn more at www.mandiant.com

Mandiant

11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant

Mandiant is a recognized leader in dynamic cyber defense, threat intelligence and incident response services. By scaling decades of frontline experience, Mandiant helps organizations to be confident in their readiness to defend against and respond to cyber threats. Mandiant is now part of Google Cloud.

MANDIANT
NOW PART OF Google Cloud