M-TRENDS 2022

MANDIANT SPECIAL REPORT

EXECUTIVE SUMMARY

Recent cyber events are a stark reminder that our work as defenders is never done. Critical vulnerabilities such as "Log4Shell" highlight the dangers of the unknown and the complexity of patching. The supply chain is as attractive a target as ever, providing a potential entry point into multiple vendors. And we must remain vigilant about protecting our industrial control systems, especially given that 1 in 7 multifaceted extortion attacks leak critical operational technology information.

Mandiant responders are on the frontlines every day, investigating and analyzing the latest attacks and threats, and understanding how best to respond to and mitigate them. Everything we learn is passed on to our customers through our various services, giving them a much-needed advantage in a constantly evolving threat landscape.

Every year the *M-Trends* report provides some of that same critical intelligence to the greater security community. *M-Trends 2022* continues that tradition, offering details on the evolving cyber landscape, mitigation recommendations, and a wide variety of security incident-related metrics.

Let's start with a win for defenders: the global median dwell time has continued its decline in 2021. For intrusions investigated between October 1, 2020 through December 31, 2021, the median number of days between compromise and detection was 21 days (down from 24 days in 2020). Although this may demonstrate improved visibility and response, the pervasiveness of ransomware has helped drive this number down.

Ransomware and multifaceted extortion continue to be concerning. We highlight an increase in targeting of virtualization infrastructure and offer mitigations. We also provide guidance on ransomware preparedness (via red teaming) and recovery operations.

Other topics covered in *M-Trends 2022* include:

By the Numbers The global median dwell time for intrusions identified by external third parties and disclosed to the victims dropped to 28 days from 73 days in 2020, a stellar improvement. In less desirable news, when the initial infection vector was identified, supply chain compromise accounted for 17% of intrusions in 2021 compared to less than 1% in 2020. Other signature metrics include detection by source, industry targeting, threat groups, malware and attacker techniques.

Recently Graduated Threat Groups A detailed analysis of two financially motivated groups we graduated in 2021: FIN12 and FIN13. We also highlight two noteworthy uncategorized groups: UNC2891 and UNC1151.

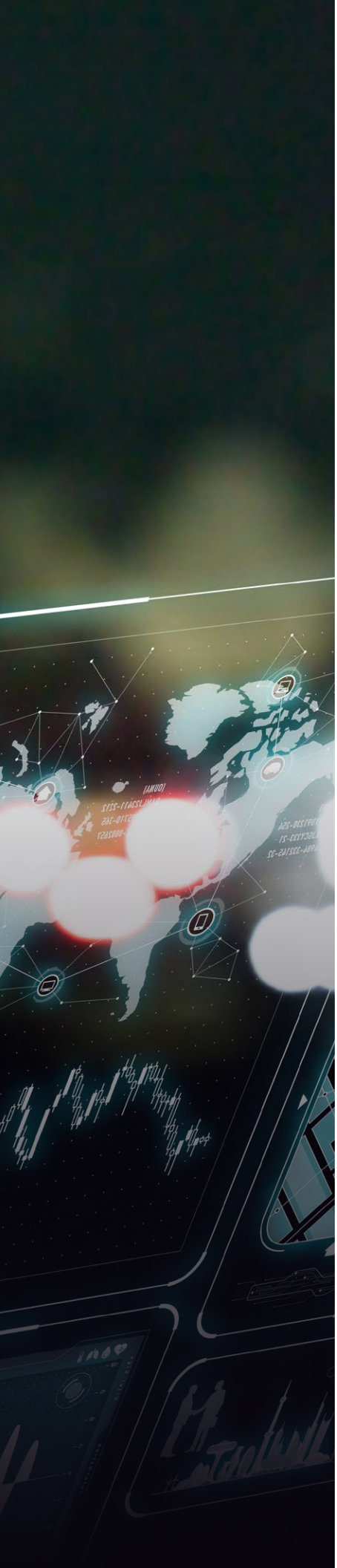
Microsoft Exchange Case Study Our observations responding to more than 20 incidents involving exploitation of on-premises Microsoft Exchange servers. In one testament to dedicated investigation and analysis, the deployment of cryptocurrency coinminers by one financially-motivated threat group led to the discovery of two nation-state actors in the same environments.

China Cyber Operations We review China's realignment and retooling, explore reemerging espionage activity and highlight actors such as APT10 and APT41.

Misconfiguration Mitigations We observed various compromises due to misconfigurations when using on-premises Active Directory with Azure Active Directory to achieve a single integrated identity solution.

M-Trends 2022 builds on our transparency to continue providing critical knowledge to those tasked with defending organizations. The information in this report has been sanitized to protect identities of victims and their data.

BY THE NUMBERS



DATA FROM MANDIANT INVESTIGATIONS

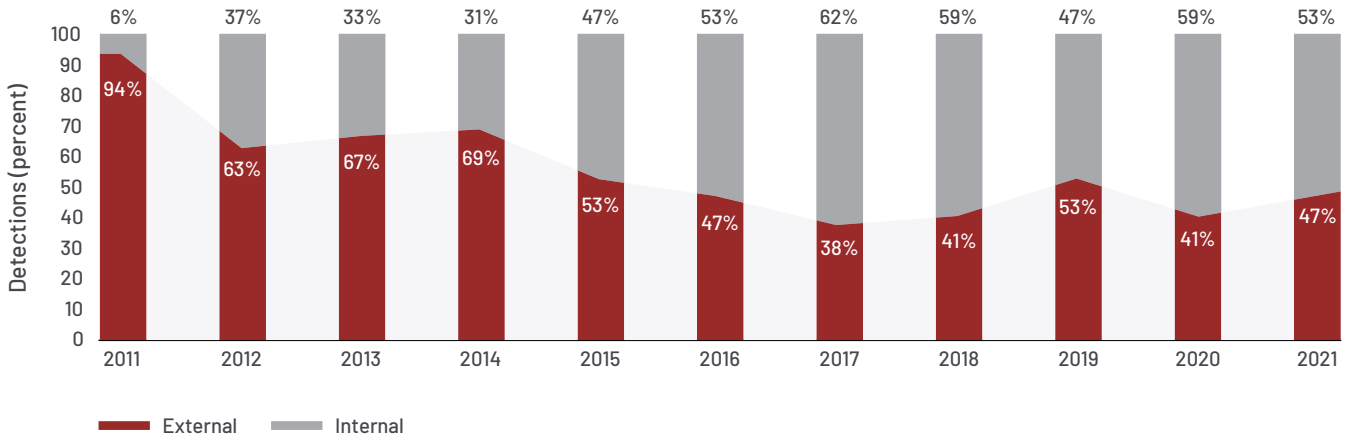
The metrics reported in *M-Trends 2022* are based on Mandiant investigations of targeted attack activity conducted between October 1, 2020 and December 31, 2021.

This edition of *M-Trends* covers a 15-month period compared to a 12-month period in previous editions.

Detection by Source

Across the board, there was an increase in external notification of intrusions in 2021 compared to 2020. However, awareness of most intrusions continues to come about through internal detections. The percentage of intrusions detected internally has maintained a gradual upwards trend with moderate fluctuation over the last six years.

Detection by Source, 2011-2021

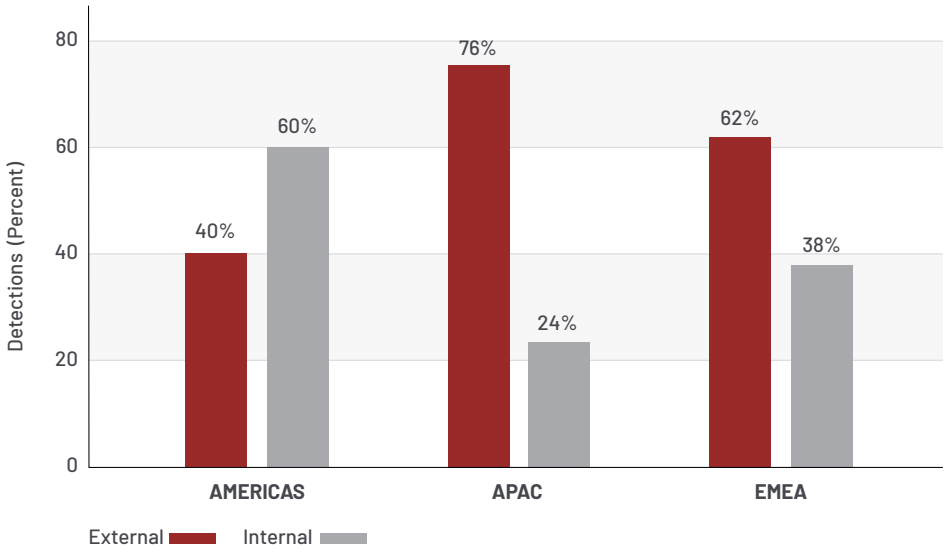


In APAC and EMEA, the majority of intrusions in 2021 were identified externally—a reversal of what was observed in 2020. The detection by source for Americas held steady with most intrusions continuing to be detected internally.

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

External notification is when an outside entity informs an organization it has been compromised. This includes when a compromised organization is first notified of an incident by an attacker via an extortion note.

Detection by Source by Region, 2021

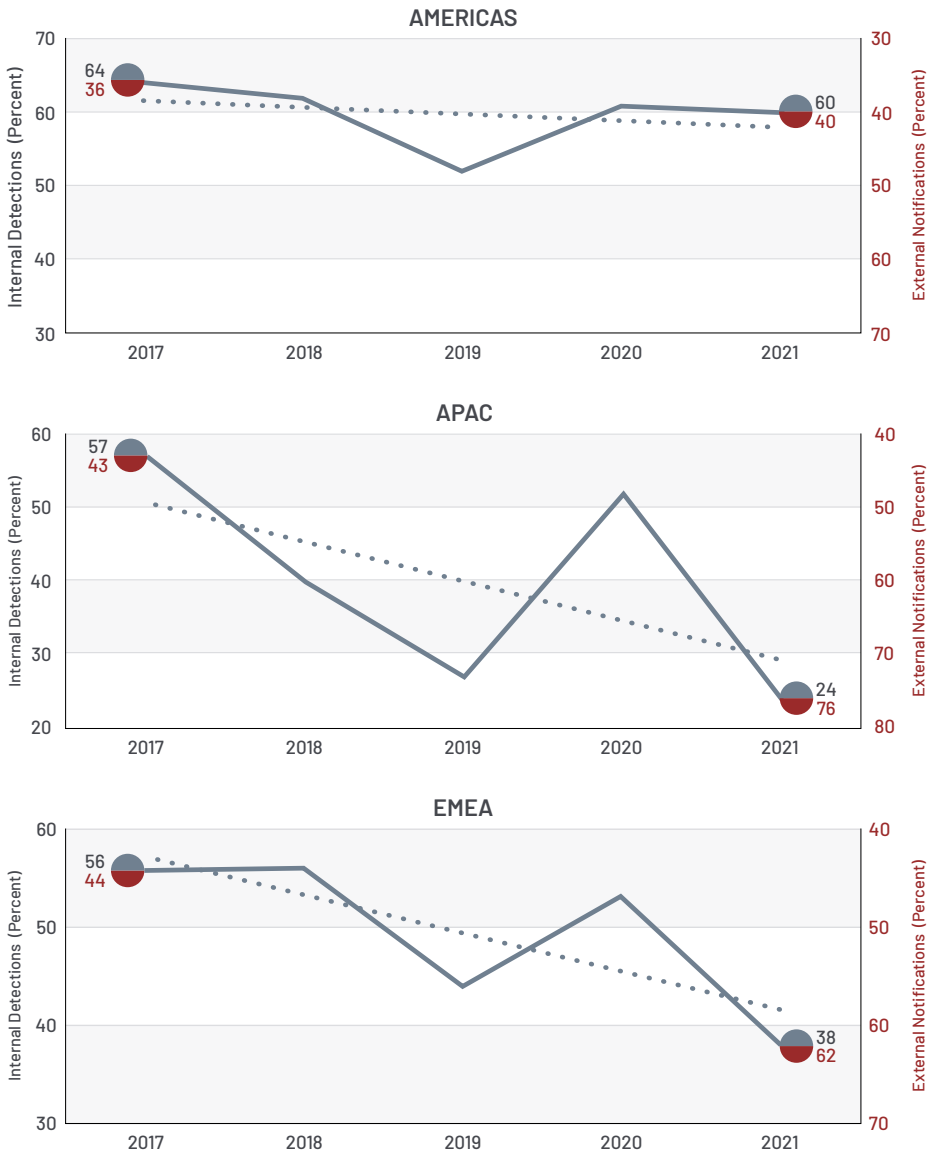


In Americas, organizations detected intrusions internally in 60% of cases in 2021 compared to 61% of cases in 2020. There is relative stability in detection by source trends for Americas from 2017 to 2021.

Organizations in APAC were notified by an external entity in 76% of intrusions in 2021 compared to 48% of intrusions in 2020. Observations for 2021 are in line with observations for APAC from 2019. Mandiant experts have seen relatively large shifts in detection by source metrics for APAC over the past five years.

In EMEA, organizations were notified of an incident by an external entity in 62% of intrusions in 2021 compared to 47% of intrusions in 2020. Similar to APAC, when analyzing the five-year trend, there remains variability in detection by source in EMEA. The variability observed for both APAC and EMEA can be explained in part by continued maturity of organizations' security programs as well as external entities' notification ability in these regions.

Detection by Source by Region, 2017–2021



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.

Dwell Time

The global median dwell time continued to improve in 2021 with organizations now detecting intrusions in three weeks. The global median dwell time for organizations that learned about their security incident through an external third party notification improved markedly in 2021. Not only are external entities doing more notifications of intrusions to organizations compared to 2020, they are also notifying them more quickly, resulting in shorter dwell times. The median dwell time for internally detected intrusions lengthened in 2021 compared to 2020 but remained shorter than median dwell time for external notifications.

Change in Median Dwell Time

24 → **21**

DAYS IN 2020 **DAYS IN 2021**

Global Dwell Time

The global median dwell time for 2021 was 21 days compared to 24 days in 2020. This 13% improvement in global median dwell time was comprised of noteworthy changes in relation to source of detection. The global median dwell time for incidents which were identified externally dropped from 73 to 28 days. Conversely, incidents which were identified internally saw a lengthening of global median dwell time from 12 to 18 days.

There were significant improvements to global median dwell time when an external entity was the notification source. External entities are now detecting intrusions and notifying organizations in less than a month—62% faster compared to 2020. This speaks to improved detection capabilities of external entities in addition to more established communications and outreach programs.

Mandiant experts observed a 50% increase in global median dwell time for internally detected intrusions. The global median dwell time for internally detected intrusions rose from 12 days in 2020 to 18 days in 2021. While median dwell time for internal detections was slower compared to 2020, internal detections were still 36% faster than external notifications.

Global Median Dwell Time, 2011-2021

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

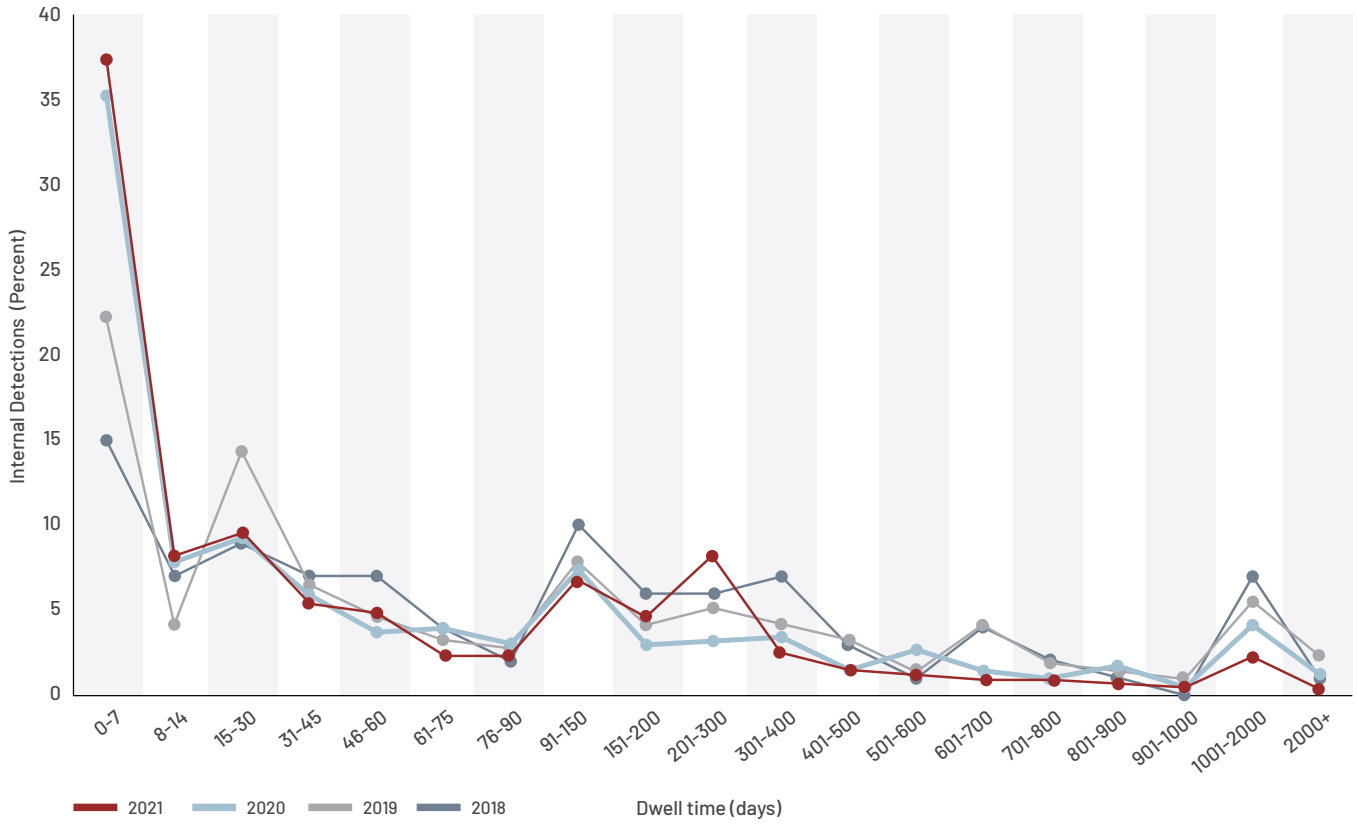
Global Dwell Time Distribution

Global dwell time distribution continues to improve at both ends of the spectrum. In 2021, 55% of investigations had dwell times of 30 days or fewer with 67% of these (37% of total intrusions) being discovered in one week or less.

Mandiant experts observed a spike in dwell times between 90 and 300 days with 20% of investigations falling into this range. This could indicate intrusions going undetected until more impactful actions occur in the environment following initial infection and reconnaissance phases of the targeted attack lifecycle. This may also highlight a disparity between organizational detection capabilities and the types of attacks organizations face.

Fewer intrusions are going undetected for extensive periods of time. Only 8% of intrusions investigated in 2021 had a dwell time of more than a year and half of these (4% of total intrusions) had dwell times greater than 700 days.

Global Dwell Time Distribution, 2018–2021



Change in Investigations Involving Ransomware

25% IN 2020 → **23%** IN 2021

No Change in Global Median Dwell Time: Ransomware

5 DAYS IN 2020 → **5** DAYS IN 2021

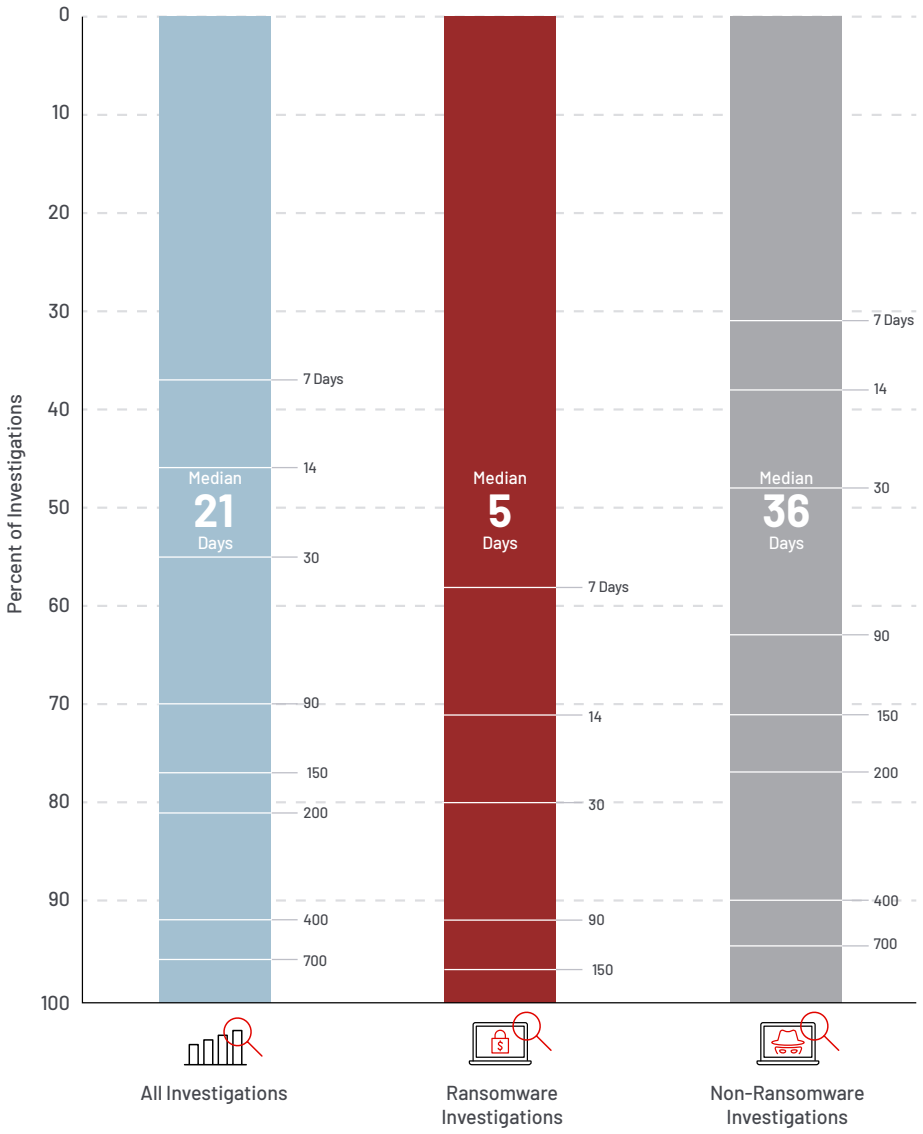
Change in Global Median Dwell Time: Non-ransomware

45 DAYS IN 2020 → **36** DAYS IN 2021

Investigations involving Ransomware

Mandiant experts observed that the percentage of intrusions involving multifaceted extortion and ransomware was relatively stable from 2020 to 2021. In 2021, 23% of intrusions involved ransomware compared to 25% in 2020. These types of attacks continue to be a driving force of reduced median dwell times. Ransomware-related intrusions had a median dwell time of 5 days compared to 36 days for non-ransomware intrusions, making dwell times for ransomware intrusions one-seventh the duration of non-ransomware. While median dwell time for ransomware-related intrusions in 2021 remained the same as 2020, Mandiant experts noted a 20% reduction in median dwell time for non-ransomware intrusions year over year.

Global Dwell Time by Investigation Type, 2021



AMERICAS

No Change in Median Dwell Time

17 → **17**

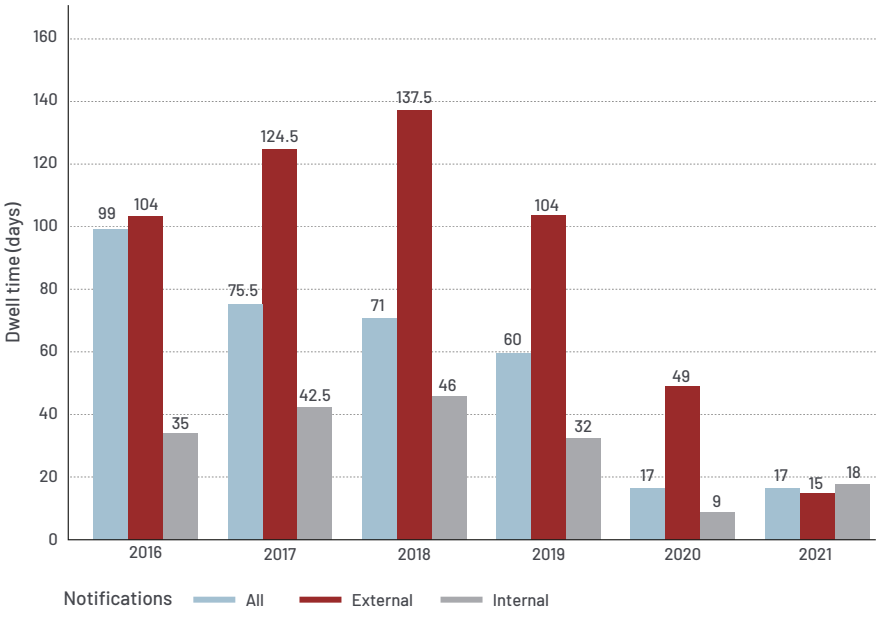
DAYS IN 2020 **DAYS IN 2021**

Americas Median Dwell Time

The median dwell time for intrusions investigated in Americas remained constant at 17 days in 2021 compared to 2020. When considering detection source, there was a 9-percentage point increase in median dwell time for intrusions detected internally, increasing from 9 days in 2020 to 18 days in 2021. While median dwell time for internal detection did lengthen in 2021 compared to 2020, the six-year trend continues towards faster internal detections. Americas median dwell time for internal detections in 2020 demonstrated a major improvement, making it unsurprising this metric reverted some in 2021.

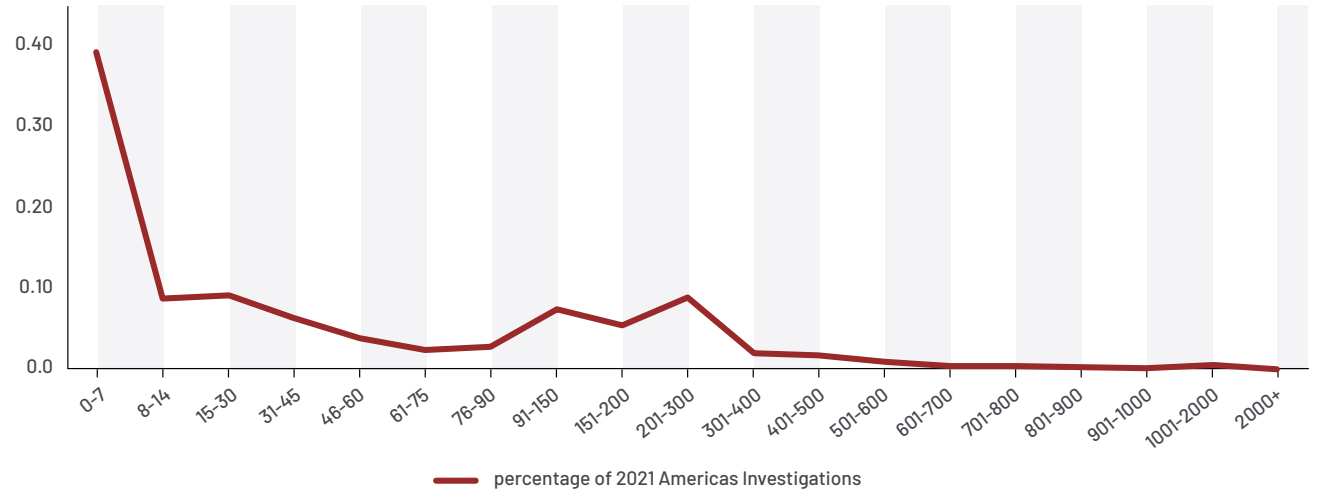
Intrusions with an external notification source had a median dwell time of 49 days in 2020 compared to only 15 days in 2021. External entities notified organizations in Americas 69% faster in 2021 compared to 2020.

Americas Median Dwell Time, 2016–2021



In Americas 57% of intrusions were detected in fewer than 30 days in 2021, and 68% of these intrusions (39% of total Americas intrusions) were detected in less than one week. Not only are nearly half of intrusions being detected in two weeks or less, but also fewer intrusions are going undetected for extended periods of time. Mandiant experts observed a spike in intrusions with dwell times between 90 and 300 days, accounting for 22% of intrusions in Americas. Further, only 4% of intrusions in Americas had dwell times longer than one year.

Americas Dwell Time Distribution, 2021



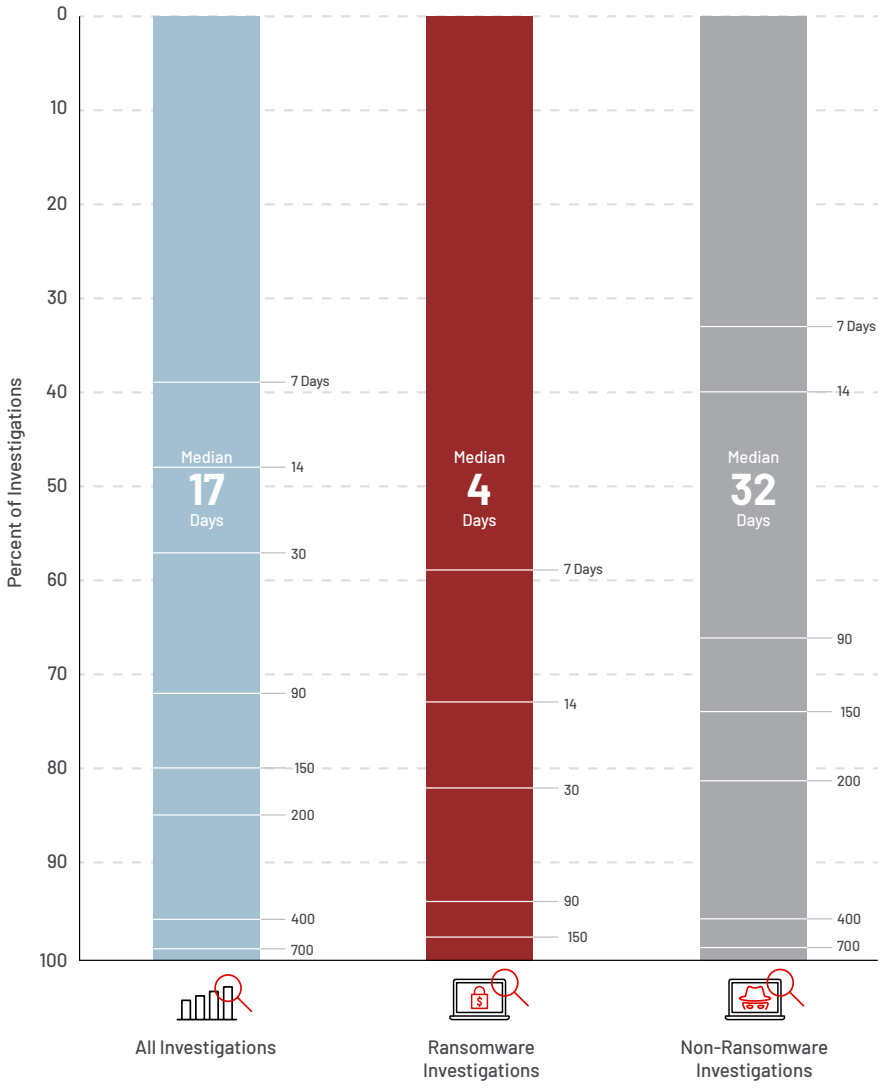
Change in Investigations Involving Ransomware

27.5% → **22%**

IN 2020 **IN 2021**

In 2021, 22% of intrusions in Americas were related to ransomware—a 5.5-percentage point decrease compared to 2020. Even though there were fewer ransomware-related intrusions in Americas, these intrusions continue to impact the median dwell time. Ransomware intrusions in Americas had a median dwell time of 4 days compared to 32 days for non-ransomware intrusions.

Americas Dwell Time by Investigation Type, 2021



APAC

Change in Median Dwell Time

76 → **21**

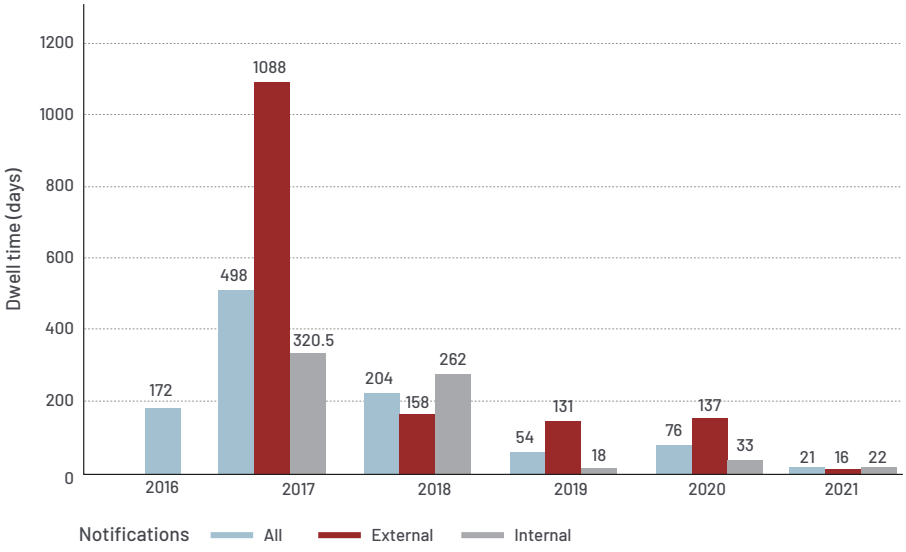
DAYS IN 2020 **DAYS IN 2021**

APAC Median Dwell Time

All median dwell time metrics improved in APAC in 2021. The median dwell time for intrusions in APAC was just 21 days in 2021 compared to 76 days in 2020, a 72% improvement in median dwell time year over year.

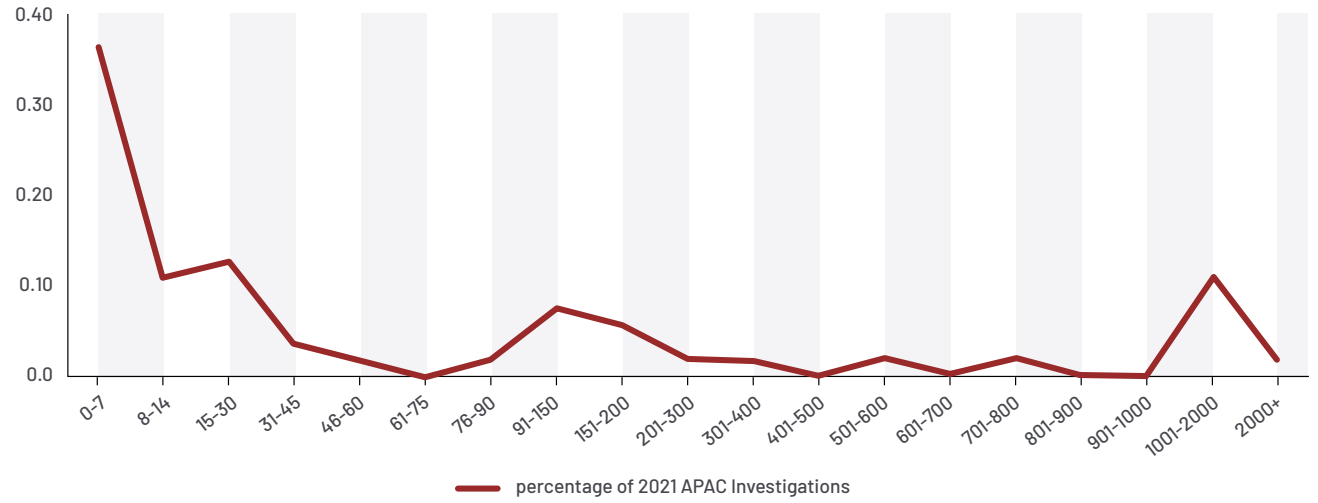
In APAC, organizations are detecting intrusions quicker and external entities are notifying organizations of intrusions faster. Intrusions in APAC that were detected internally had a median dwell time of 22 days in 2021 compared to 33 days in 2020. The median dwell time for intrusions with an external notification source was 16 days in 2021 compared to 137 days in 2020—an 88% reduction.

APAC Median Dwell Time, 2016–2021



The dwell time distribution for APAC reveals 60% of intrusions had dwell times of 30 days or fewer with 60% of these (36% of all APAC intrusions) detected in one week or less. At the other end of the spectrum, similar to observations from previous years, dwell time distribution in APAC continues to show that several intrusions go undetected for extended periods of time. Mandiant experts observed that 13% of intrusions in APAC in 2021 had dwell times that exceeded three years. Organizations in APAC have impressive detection capabilities. However, intrusions that go undetected initially can remain undetected, resulting in extensive dwell times when they are ultimately detected.

APAC Dwell Time Distribution, 2021

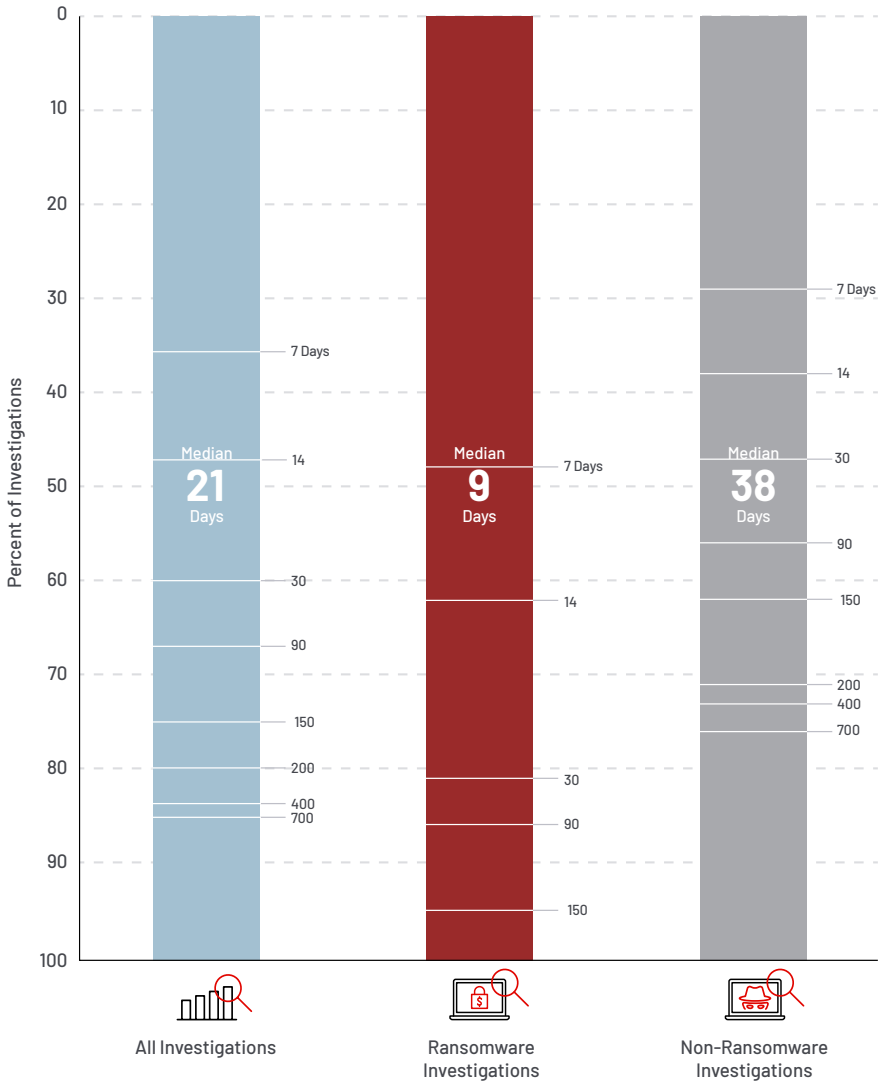


Change in Investigations Involving Ransomware

12.5% → **38%**
IN 2020 **IN 2021**

Ransomware was more prevalent in APAC in 2021 compared to previous years. Ransomware-related intrusions accounted for 38% of intrusions investigated in APAC in 2021 compared to 12.5% of intrusions in 2020 and 18% of intrusions in 2019. Median dwell time in APAC for ransomware-related intrusions was 9 days compared to 38 days for non-ransomware intrusions.

APAC Dwell Time by Investigation Type, 2021



EMEA

Change in Median Dwell Time

66 → **48**

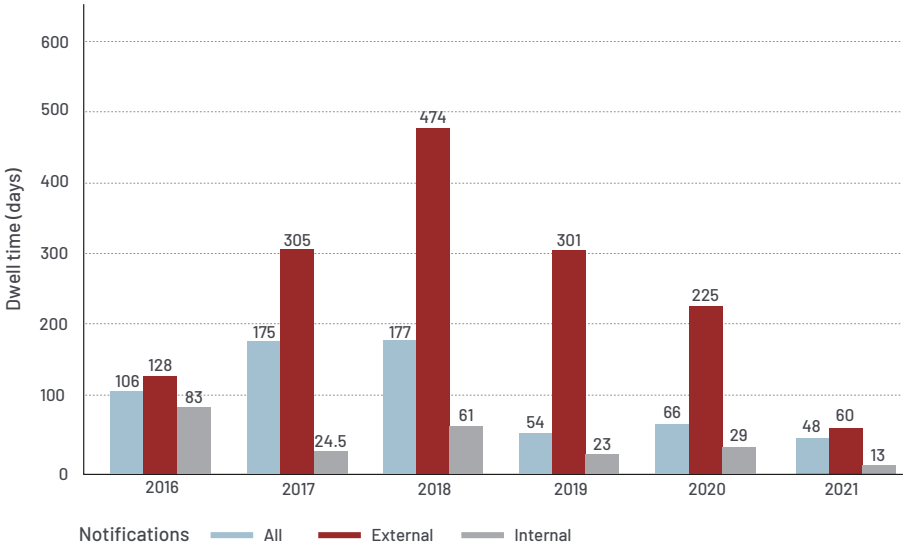
DAYS IN 2020 **DAYS IN 2021**

EMEA Median Dwell Time

In 2021, EMEA showed improvement in median dwell times across the board with the shortest dwell times ever observed for EMEA in all categories. The median dwell time for intrusions investigated in EMEA was just 48 days in 2021 compared to 66 days in 2020 and 54 days in 2019.

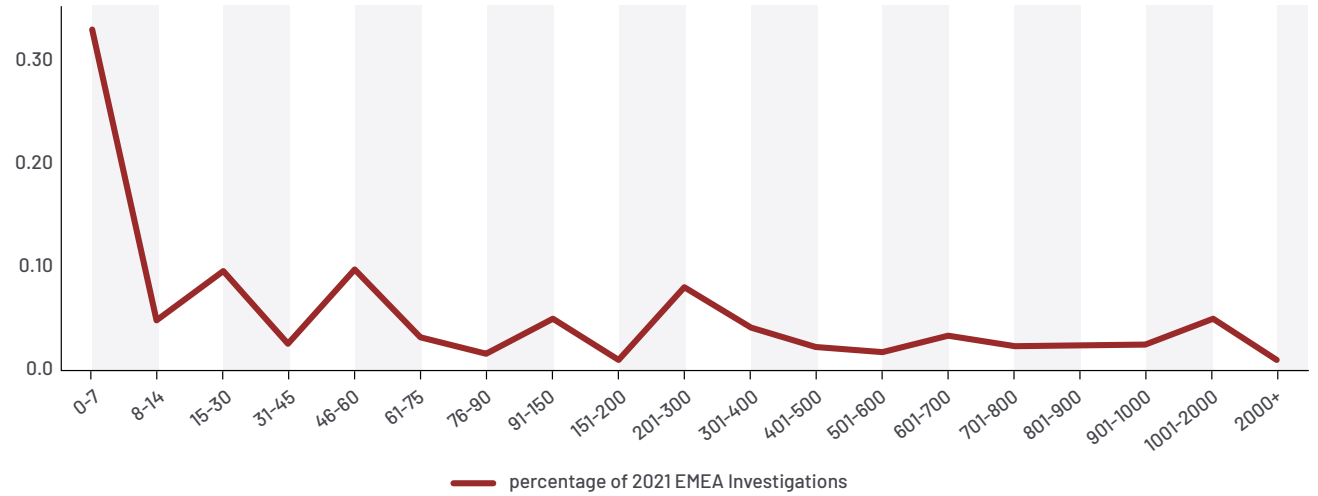
For intrusions detected internally in EMEA, the median dwell time improved from 29 days in 2020 to 13 days in 2021. Similarly, median dwell time for EMEA intrusions involving external notifications dropped from 225 days in 2020 to 60 days in 2021.

EMEA Median Dwell Time, 2016–2021



When examining dwell time distribution, 47% of intrusions in EMEA were detected within 30 days; 70% of these intrusions (33% of all EMEA intrusions) were detected within one week. EMEA also showed improvement in the percentage of intrusions with extended dwell times. In 2021, 5.5% of intrusions in EMEA had dwell times longer than three years, which is a 2.5-percentage point improvement over 2020.

EMEA Dwell Time Distribution, 2021

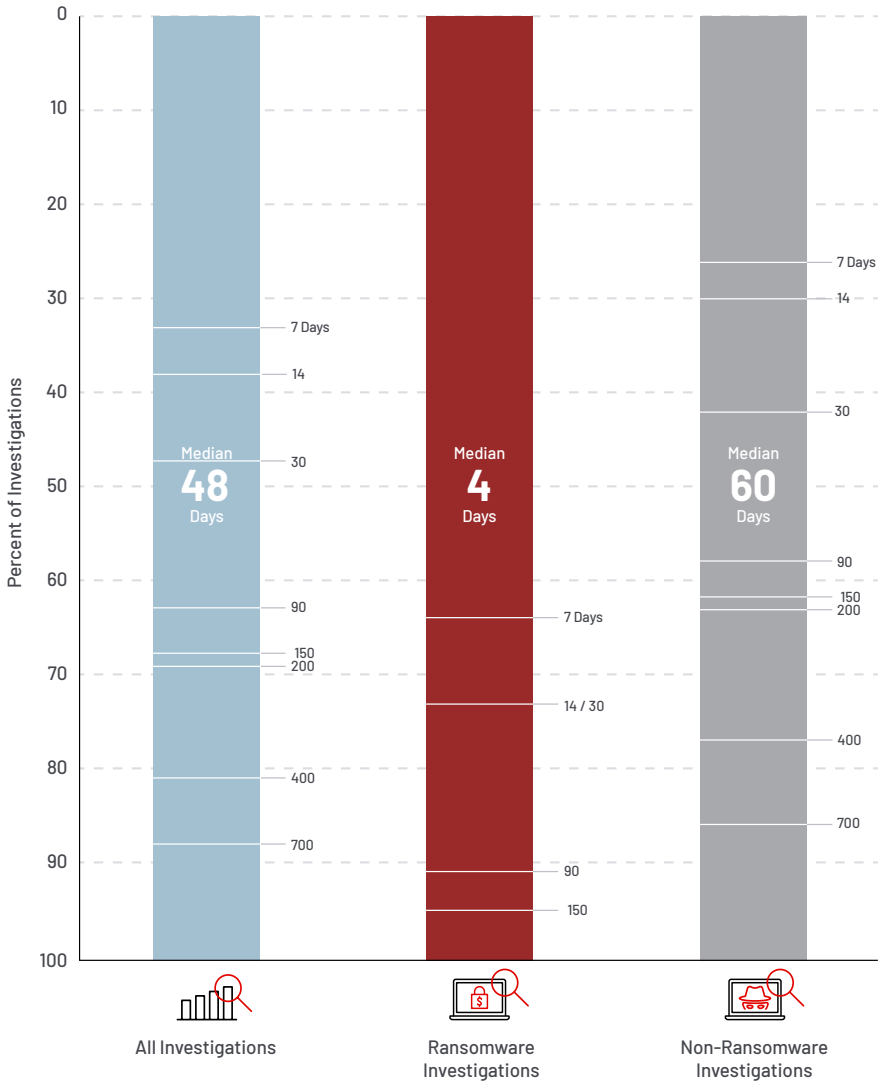


Change in Investigations Involving Ransomware

22% IN 2020 → **17%** IN 2021

In 2021, fewer investigations in EMEA were ransomware related—17% compared to 22% in 2020. However, the quick nature of ransomware intrusions contributed to the overall improvement of the median dwell time in EMEA. Mandiant experts observed that the 2021 median dwell time in EMEA for ransomware-related intrusions was only 4 days compared to 60 days for non-ransomware intrusions.

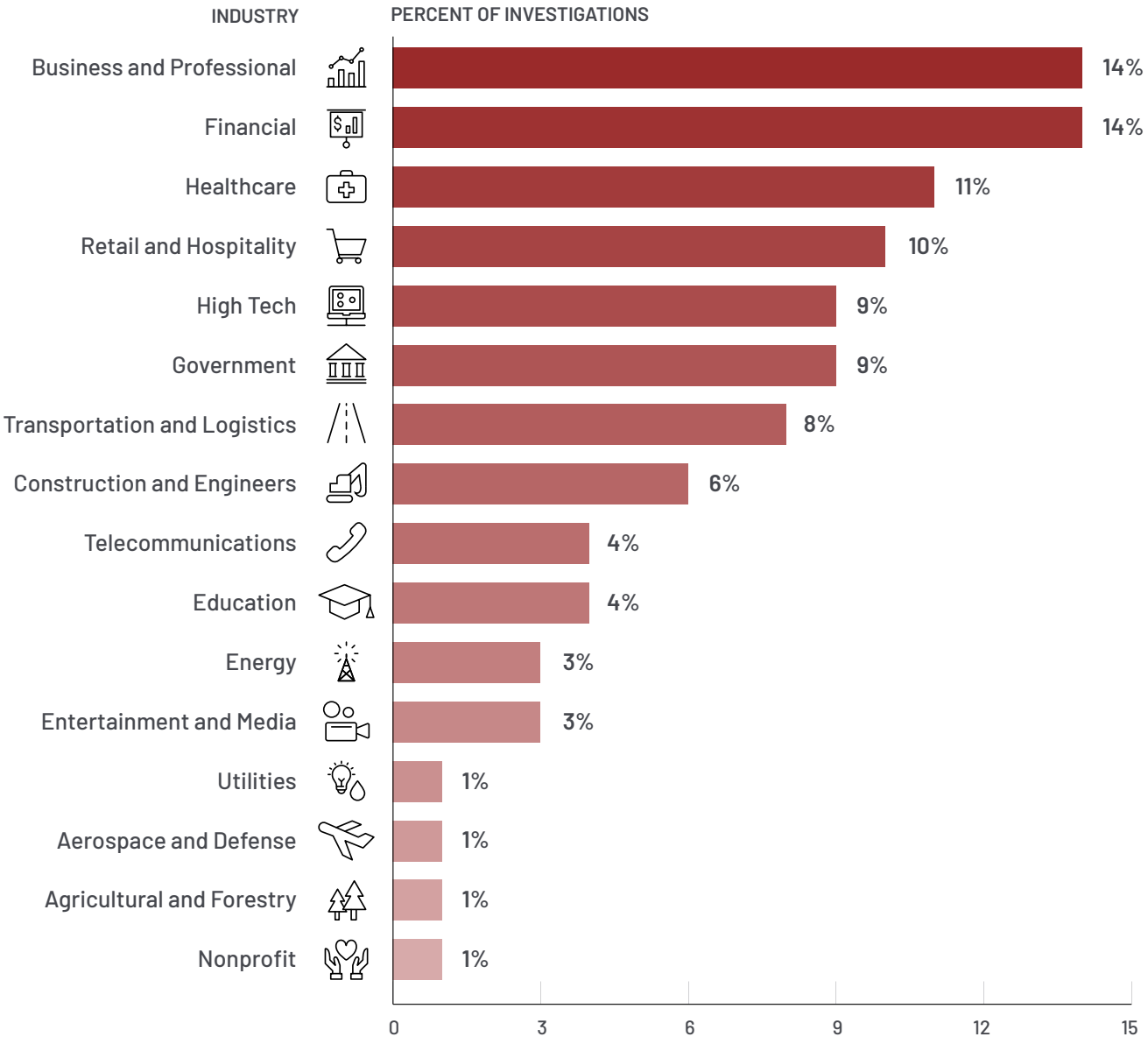
EMEA Dwell Time by Investigation Type, 2021



Industry Targeting

Mandiant continues to see consistent industry targeting by adversaries. In 2021 business/professional services and financial were the top targeted industries across the globe. Retail and hospitality, healthcare and high tech round out the top five industries favored by adversaries. Mandiant continues to see these same industries targeted across the globe every year.

Global Industries Targeted, 2021



Targeted Attacks

Initial Infection Vector

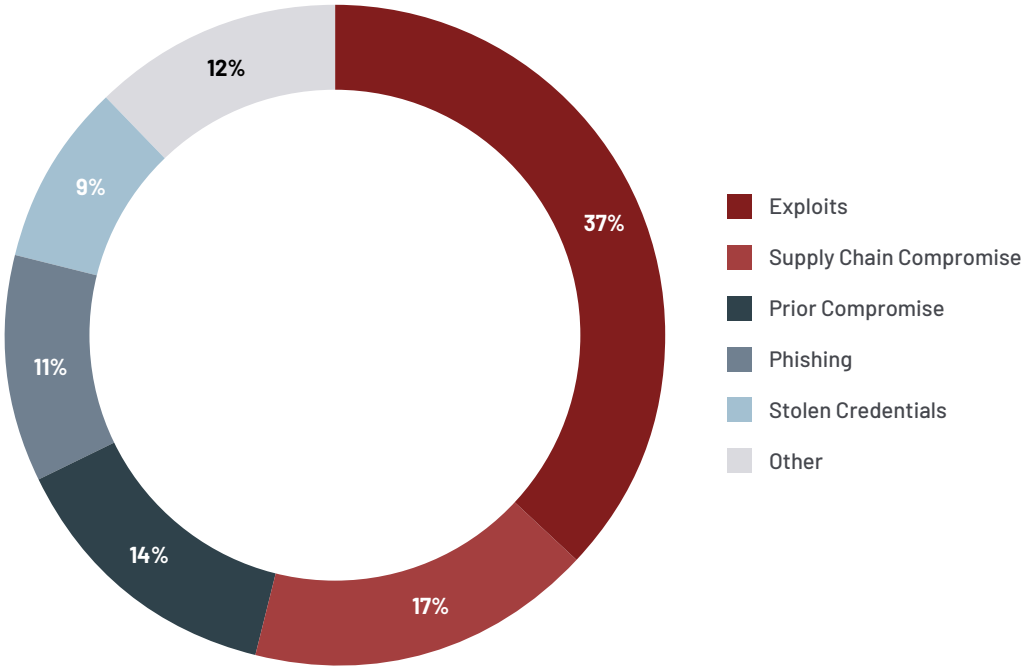
Exploits remained the most frequently identified initial infection vector in 2021. In intrusions where the initial infector vector was identified, 37% started with an exploit—an 8-percentage point increase over 2020.

Supply chain compromise was the second most prevalent initial infection vector identified in 2021. When the initial infection vector was identified, supply chain compromise accounted for 17% of intrusions in 2021 compared to less than 1% in 2020. Further, 86% of supply chain compromise intrusions in 2021 were related to the SolarWinds breach and SUNBURST.[1]

In 2021, Mandiant experts observed an uptick in intrusions with an initial infection vector due to a prior compromise. These intrusions include handoffs from one group to another and prior malware infections. Prior compromises accounted for 14% of intrusions where the initial infection vector was identified.

Mandiant experts observed far fewer intrusions initiated via phishing in 2021. When the initial compromise was identified, phishing was the vector in only 11% of intrusions in 2021 compared to 23% in 2020. This speaks to organizations' ability to better detect and block phishing emails as well as enhanced security training of employees to recognize and report phishing attempts.

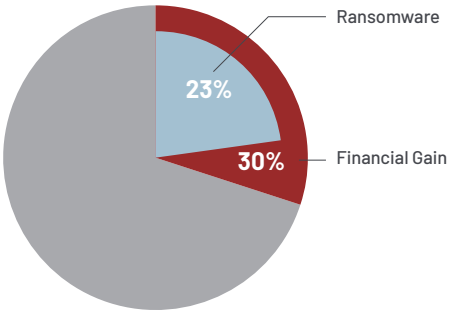
Initial Infection Vector, 2021 *(When Identified)*



1. Mandiant (December 13, 2021). Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor.

Adversary Operations

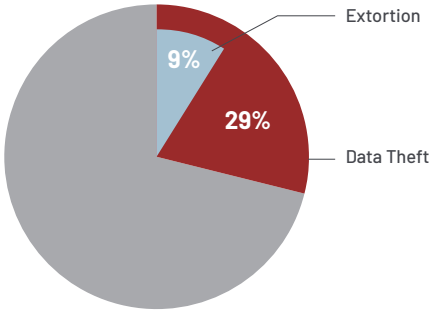
Financial Gain



38% IN 2020 → **30%** IN 2021

Financially motivated intrusions continue to be a mainstay in 2021, with adversaries seeking monetary gain in 3 out of 10 intrusions through methods such as extortion, ransom, payment card theft and illicit transfers. The percentage of financially motivated intrusions dropped to 30% in 2021 compared to the 38% of intrusions observed in 2020. Mandiant experts observed a 2-percentage point decrease specifically in ransomware-related incidents in 2021. Another likely contributing factor for decreased financial gain operations in 2021 was an increase in law enforcement action taken against financially motivated actors leading to arrests, takedown of servers and seizure of extorted funds.

Data Theft

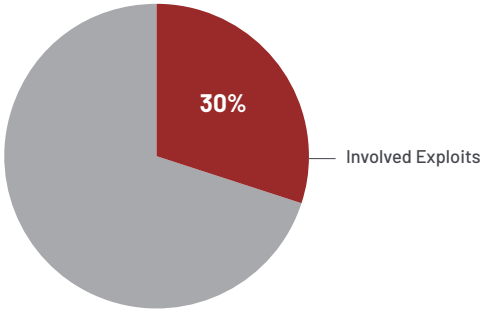


32% IN 2020 → **29%** IN 2021

Threat actors continue to prioritize data theft as a primary mission objective. In 2021, Mandiant identified data theft in 29% of intrusions. In 32% of intrusions involving data theft (9% of all intrusions) the stolen data was specifically targeted for use as the threat actor's leverage during negotiations for payment. In 12% of intrusions involving data theft (4% of all intrusions) the data theft likely supported intellectual property or espionage end goals.

Compromised Architecture and Insider Threat

In 2021 Mandiant experts observed a slight uptick in compromises that likely served only to compromise architecture for further attacks. In 2021, this activity was identified in 4% of intrusions, a 1-percentage point increase compared to 2020. Likewise, insider threat continues to be rare with only 1% of intrusions investigated by Mandiant related to insider threat. These metrics have remained relatively stable over years of reporting.



Exploit Activity

Adversaries frequently leveraged exploits in 2021 with 30% of all intrusions involving exploit activity. In 2021, major vulnerabilities were discovered in products such as Microsoft Exchange[2,3], SonicWall's Email Security (ES) product[4], Pulse Secure VPN appliances[5] and Apache's Log4j 2 utility[6] among others. Adversaries exploited these vulnerabilities to initiate and further intrusions. Mandiant experts even observed adversaries leverage vulnerabilities to deploy ransomware.[7]

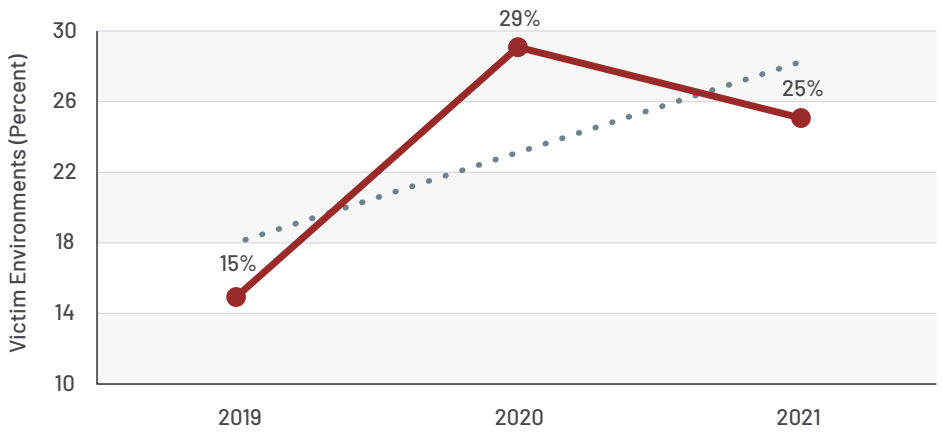
Change in Multiple Threat Groups Identified (per environment)

29% IN 2020 → **25%** IN 2021

Environment

In 2021, Mandiant experts identified that a quarter of victim environments had more than one distinct threat group. These environments included investigations with threat groups working together and attractive target environments enticing multiple threat actors independently. While the percentage of victim environments with multiple threat groups decreased in 2021 compared to 2020, the three-year trend demonstrates likely continued growth.

Multiple Threat Groups Identified, 2019-2021

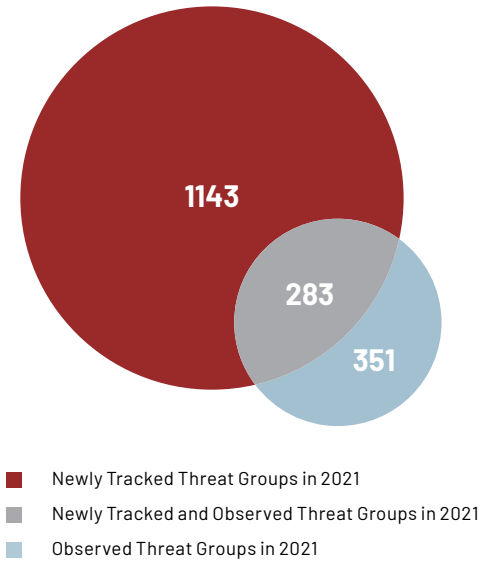


2. Mandiant (March 4, 2021). Detection and Response to Exploitation of Microsoft Exchange Zero-Day Vulnerabilities.
3. Mandiant (November 17, 2021). ProxyNoShell: A Change in Tactics Exploiting ProxyShell Vulnerabilities.
4. Mandiant (April 20, 2021). Zero-Day Exploits in SonicWall Email Security Lead to Enterprise Compromise.
5. Mandiant (April 20, 2021). Check Your Pulse: Suspected APT Actors Leverage Authentication Bypass Techniques and Pulse Secure Zero-Day
6. Mandiant (December 15, 2021). Log4Shell Initial Exploitation and Mitigation Recommendations.
7. Mandiant (February 23, 2021). (Ex)Change of Pace: UNC2596 Observed Leveraging Vulnerabilities to Deploy Cuba Ransomware.

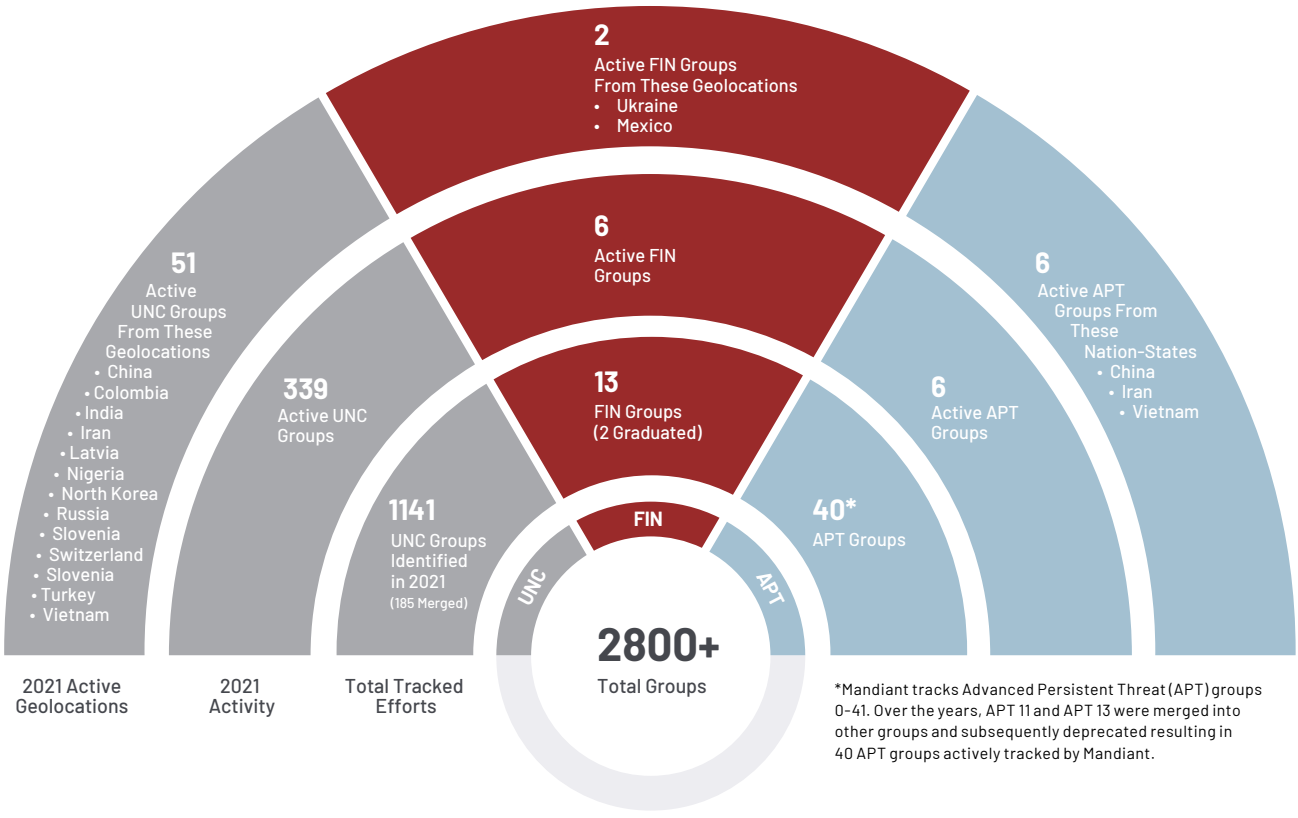
Threat Groups

Mandiant experts currently track more than 2,800 threat groups, which include 1100+ newly tracked threat groups for this ***M-Trends*** reporting period. Mandiant continues to expand its extensive threat actor knowledgebase through clustering and attributing adversary activity observed not only during frontline investigations, but also from analysis of public reporting, information sharing and other research.

In 2021, Mandiant experts graduated two groups to named threat groups, FIN12[8] and FIN13.[9] Additionally, Mandiant merged 185 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."[10]



Threat Groups 2021



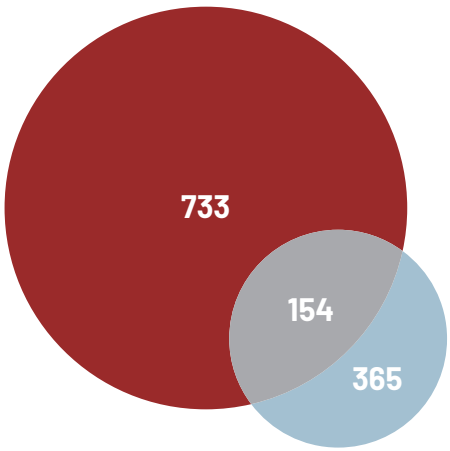
8. Mandiant (October 7, 2021). FIN12: The Prolific Ransomware Intrusion Threat Actor That Has Aggressively Pursued Healthcare Targets
9. Mandiant (December 7, 2021). FIN13: A Cybercriminal Threat Actor Focused on Mexico
10. Mandiant (December 17, 2020). DebUNCing Attribution: How Mandiant Tracks Uncategorized Threat Actors

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.

Malware

Mandiant continuously expands its body of knowledge on malware based on insights gained from the frontlines of cyber incidents, public reporting and various other research avenues. In 2021, Mandiant began tracking over 700 new malware families. This number continues to grow in line with previous trends with no indication of slowing down.

In 2021, Mandiant experts observed adversaries use 365 distinct malware families during investigations of compromised environments. This number continues to grow in line with the number of observed malware families compared to previous years. Of the 365 malware families observed by Mandiant experts during intrusions, 154 were malware families which Mandiant began tracking in 2021.



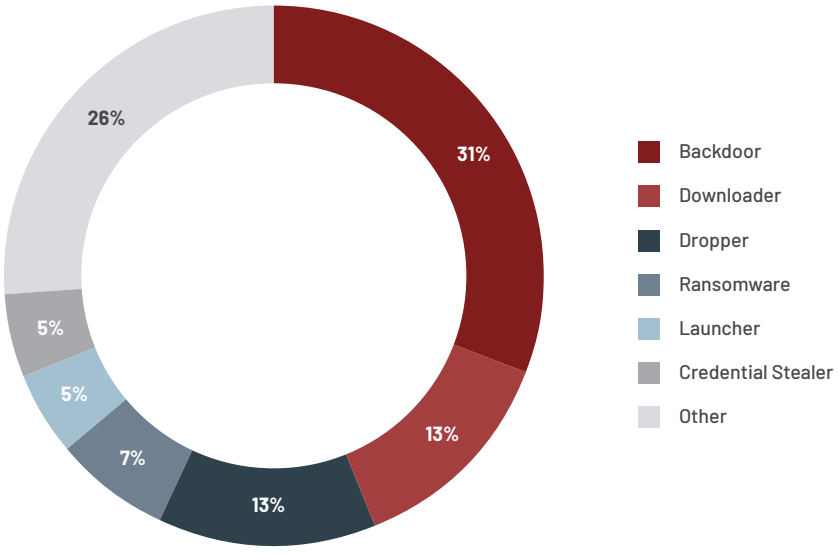
Malware Families by Category

Of the 733 newly tracked malware families in 2021, the top five categories were backdoors (31%), downloaders (13%), droppers (13%), ransomware (7%), launchers (5%) and credential stealers (5%). These categories remain consistent with previous years.

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.

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.
Other	Includes all other malware categories such as utilities, keyloggers, point-of-sale (POS), tunnelers and data miners.

Newly Tracked Malware Families by Category, 2021



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

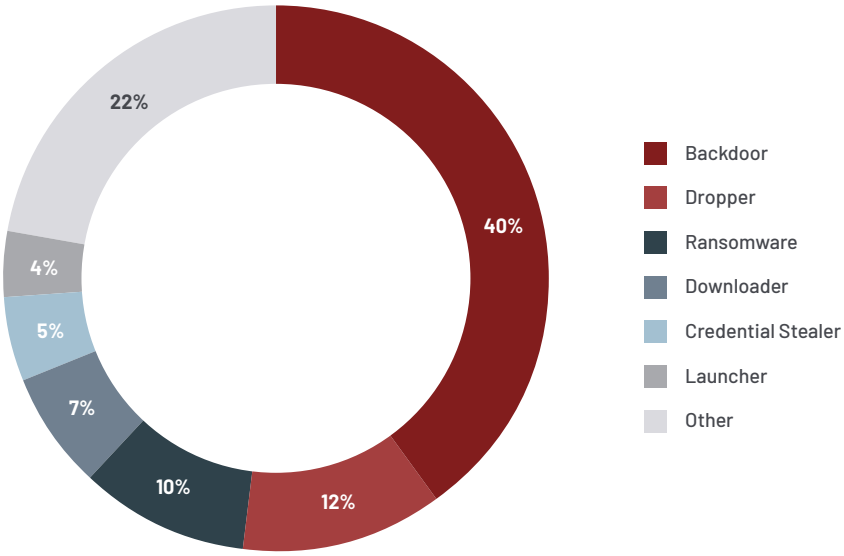
Observed Malware Families by Category

Backdoors continue to be preferred by adversaries and consistently comprise the largest malware family category observed during Mandiant investigations over the years. Of the 365 malware families observed in 2021, the top categories were backdoors (40%), droppers (12%), ransomware (10%), downloaders (7%), credential stealers (5%) and launchers (4%).

Similar to newly tracked malware families, 22% of observed malware families in 2021 were comprised of the "other" malware family category. Compared to previous years, this number remains stable as adversaries create and use a variety of different tools to achieve their missions.

Mandiant observed a rise in the variety of ransomware malware families used by adversaries, growing the observed population from 8% in 2020 to 10% in 2021.

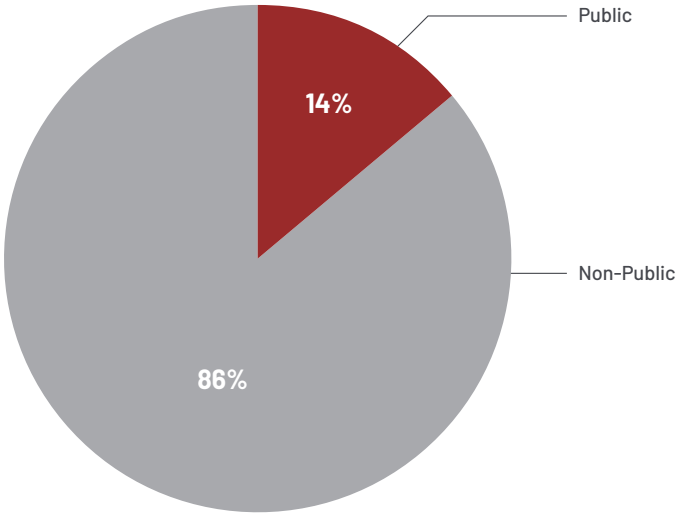
Observed Malware Families by Category, 2021



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.

Newly Tracked Malware Families by Availability, 2021

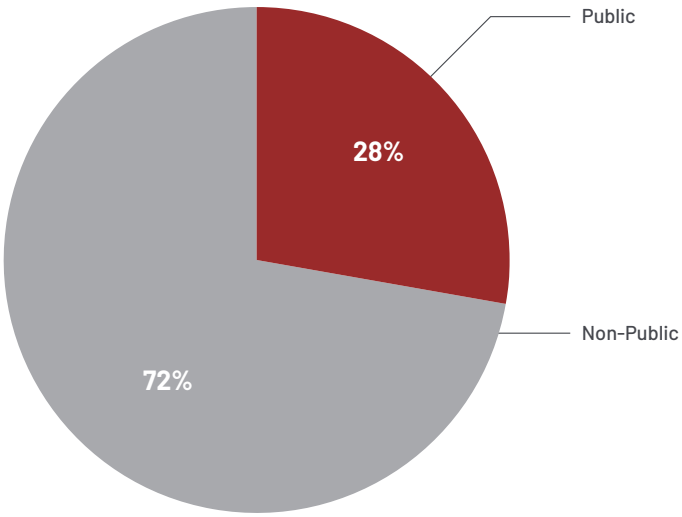
Mandiant experts observed that 86% of newly tracked malware families were non-public whereas 14% were publicly available. The majority of new malware families tracked continue the trend of availability being restricted or likely privately developed.



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.

Observed Malware Families by Availability, 2021

Similar to availability for newly tracked malware families, Mandiant experts observed 72% of malware families used by adversaries during an intrusion in 2021 were non-public and 28% were publicly available. Adversaries use both publicly and non-publicly available malware to accomplish missions across intrusions. While many adversaries often use the same publicly available malware families such as BEACON, Mandiant continues see adversaries innovate and adapt to be effective in victim environments.



Change in the use of BEACON

24% → **28%**

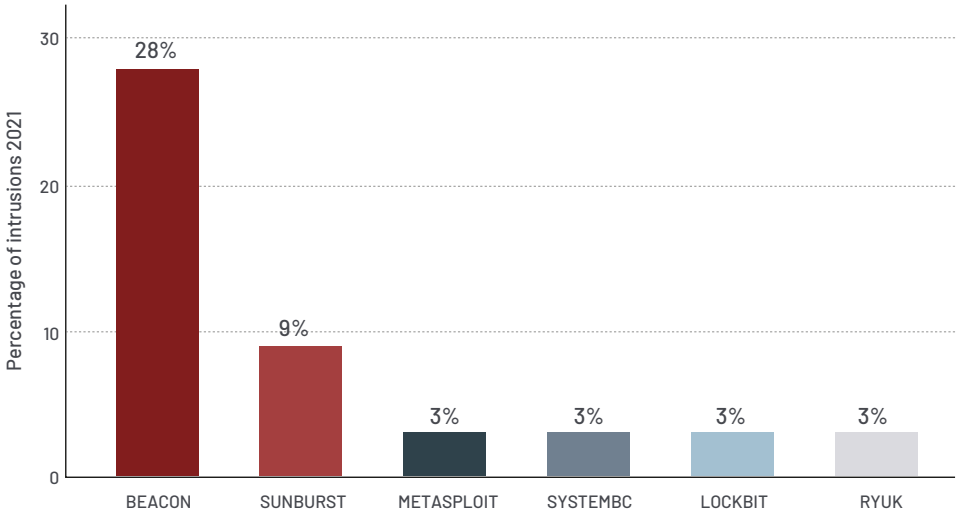
OF INTRUSIONS IN 2020 **OF INTRUSIONS IN 2021**

Most Frequently Seen Malware Families

The malware families seen most frequently during intrusions investigated by Mandiant experts were BEACON, SUNBURST, METASPLOIT, SYSTEMBC, LOCKBIT and RYUK. BEACON was once again the most prevalent malware family observed in 2021—three times more often than the second most frequently seen malware family. Further, use of BEACON across intrusions increased from 24% of intrusions in 2020 to 28% in 2021. BEACON remains by far the favorite malware family among adversaries and Mandiant expects its use will likely increase in the years to come.

SUNBURST[12] was observed in 9% of all intrusions investigated by Mandiant in 2021. SUNBURST was delivered at scale to victim environments across the globe through a malicious update, resulting in widespread compromised access. This metric is in line with the observed relationship between the second most prevalent initial infection vector, supply chain compromises and the use of SUNBURST in intrusions.

Most Frequently Seen Malware Families, 2021



RYUK and LOCKBIT were the most used ransomware families during intrusions investigated by Mandiant in 2021. Notably, newly graduated FIN12[13] leveraged RYUK, BEACON, SYSTEMBC and METASPLOIT to carry out some of the most prolific intrusions seen throughout 2021. Ransomware families continue to contribute to the malware family collection every year.

Adversaries continue to use a variety of malware to carry out missions. In 2021, Mandiant observed just 3.8% of malware families being used in 10 or more intrusions while 81% of malware families were observed in only one or two intrusions. Over the years, Mandiant has observed adversary toolsets become more diverse as adversaries continue to evolve. This diversification is demonstrated by a continuation of limited retooling across intrusions.

12. Mandiant (December 13, 2020). FIN12: Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor
13. Mandiant (October 7, 2021). FIN12: The Prolific Ransomware Intrusion Threat Actor That Has Aggressively Pursued Healthcare Targets

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 nearly 650 UNC groups.

SUNBURST is a .NET-based backdoor that initially communicates via DNS. SUNBURST generates the domain of the initial remote server using a domain generation algorithm. The DNS response returns a CNAME record containing the domain of the C2 server used for subsequent communication via HTTP. Supported backdoor commands include file download and execution, file management, registry manipulation, and process termination. SUNBURST can also disable targeted services to avoid detection and upload basic system information that includes the system's IP address, DHCP configuration, and domain information. Mandiant has observed UNC2452 leverage SUNBURST.[14]

METASPLOIT is a penetration testing platform that enables users to find, exploit, and validate vulnerabilities. Mandiant has seen METASPLOIT used by APT40, APT41, FIN6, FIN7, FIN11, FIN12, FIN13 and 40 UNC groups with end goals ranging from espionage and financial gain to penetration testing.

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 many as 10 UNC groups with goals related to financial gain.

LOCKBIT is ransomware written in C that encrypts files stored locally and on network shares. LOCKBIT can also identify additional systems on a network and propagate via SMB. Prior to encrypting files, LOCKBIT clears event logs, deletes volume shadow copies and terminates processes and services that may impact its ability to encrypt files. LOCKBIT has been observed using the file extension ".lockbit" for encrypted files. Mandiant as seen LOCKBIT used by more than 10 UNC groups with goals relating to financial gain and espionage.

RYUK is ransomware written in C that encrypts files stored on local drives and network shares. It also deletes backup files and volume shadow copies. Some RYUK variants can propagate to other systems on a network. Mandiant has seen RYUK used by FIN6, FIN12 and 10 financially motivated UNC groups.

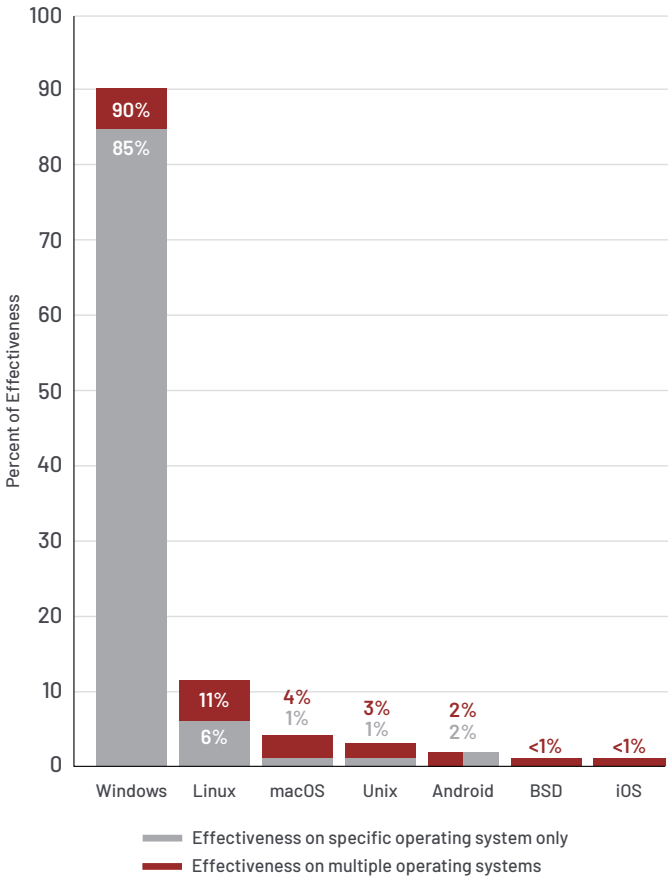
14. For more information, please visit the SolarWinds Breach Resource Center

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

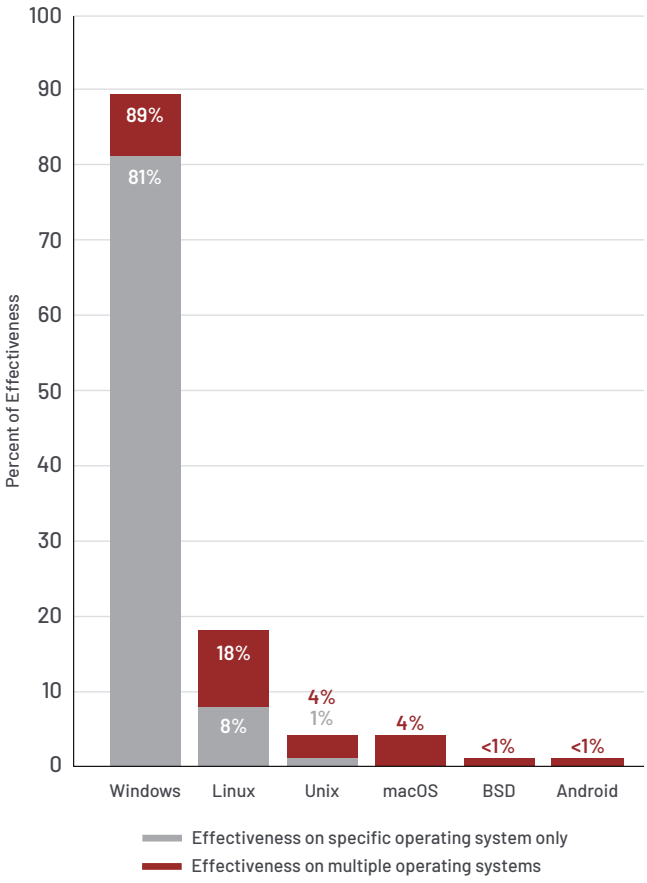
Operating System Effectiveness

Previous trends in operation system effectiveness continued in 2021 as newly tracked as well as observed malware families were predominately effective on Windows. However, malware families impacting Linux became more prevalent in 2021. Newly tracked malware families effective on Linux increased to 11% in 2021 compared to 8% in 2020. Further, observed malware families effective on Linux increased to 18% in 2021 from 13% in 2020. The increase in effectiveness on Linux in both newly tracked and observed malware families shows adversaries' ability and willingness to develop and target different operating system environments. In intrusions investigated by Mandiant, adversaries continue to target operating systems with the same relative attention.

Operating System Effectiveness of Newly Tracked Malware Families, 2021



Operating System Effectiveness of Observed Malware Families, 2021



Threat Techniques

Mandiant remains committed to supporting community and industry efforts by mapping its findings to the MITRE ATT&CK framework. In 2021, MITRE released versions 9 and 10 of ATT&CK, which focused on advancement of MITRE's coverage of Linux, macOS and container techniques. Mandiant mapped 300+ additional Mandiant techniques to the MITRE ATT&CK framework in 2021, bringing the total to 2100+ Mandiant techniques and subsequent findings associated with MITRE ATT&CK.

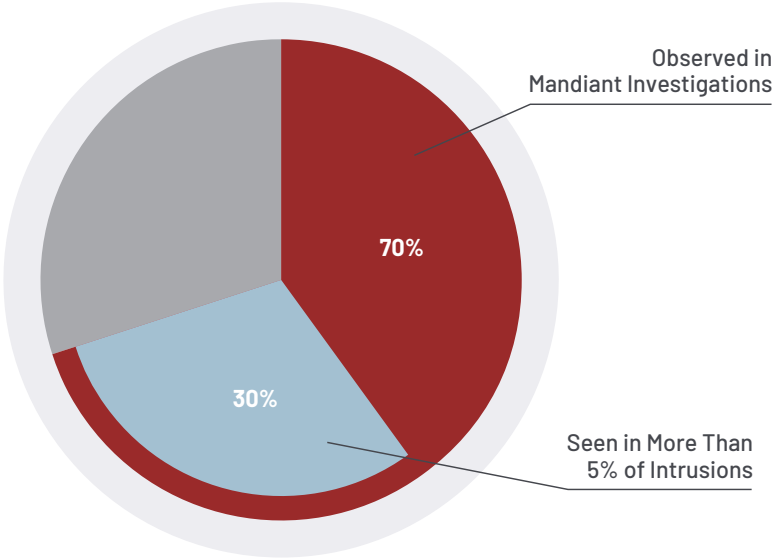
Organizations must prioritize which security measures to implement and the likelihood of specific techniques being used during an intrusion should impact this decision-making process. Examining the prevalence of technique usage during recent intrusions, can better equip organizations to make intelligent security decisions.

Mandiant experts observed adversaries use 70% of MITRE ATT&CK techniques and 46% of sub-techniques during an intrusion in 2021. Compared to 2020, this represents an 11% increase in techniques observed and a 92% increase in sub-techniques observed. While this is representative of adversaries using a wider variety of techniques to further intrusions, Mandiant experts believe this increase is due in part to more robust classification and systematic categorization of threat data that was implemented in 2021.

In 2021, 43% of techniques observed (30% of all techniques) were seen in more than 5% of intrusions compared to 37% of techniques observed in 2020 (23% of all techniques in 2020). Mandiant experts recommend prioritizing implementation of security measures to protect against the most commonly used techniques over techniques with a lower prevalence.

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.

MITRE ATT&CK Techniques Used Most Frequently, 2021



In 2021, Mandiant observed that more than half of the intrusions used obfuscation, such as encryption or encoding, on files or information to make detection and subsequent analysis more difficult (T1027).

Adversaries also continue to use a command or scripting interpreter to further intrusions (T1059) and 65% of those cases (29% of all intrusions) involved the use of PowerShell (T1059.001).

In 37% of investigations the adversary communicated using application layer protocols (T1071) with 87% of those (32% of all investigations) specifically using web protocols such as HTTP and HTTPS.

Mandiant experts observed adversaries perform discovery actions for system information (T1082) in 32% of investigations and file or directory information (T1083) also in 32% of investigations. Similarly, in 32% of investigations adversaries removed indicators on a host (T1070) with 85% of these (27% of all investigations) involving file deletions.

Similar to 2020, adversaries demonstrated a willingness to take advantage of what is available in a victim's environment to further intrusions in 2021. This is particularly evident in how frequently adversaries used web protocols, PowerShell, system services and Remote Desktop. Organizations must balance convenience and accessibility of common technologies with security of environments.

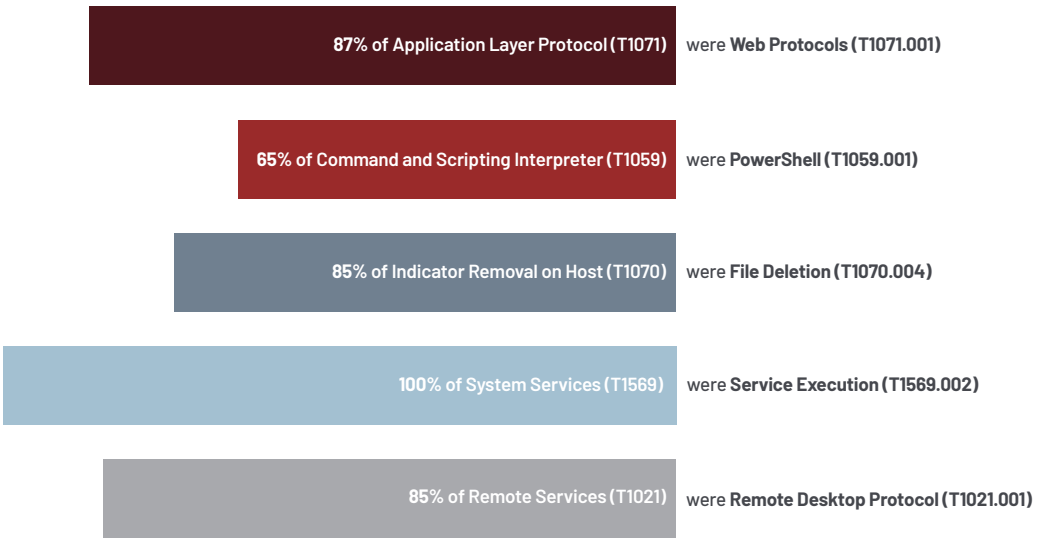
Top 10 Most Frequently Seen Techniques

1.	T1027: Obfuscated Files or Information	51.4%
2.	T1059: Command and Scripting Interpreter	44.9%
3.	T1071: Application Layer Protocol	36.8%
4.	T1082: System Information Discovery	31.8%
5.	T1083: File and Directory Discovery	31.7%
6.	T1070: Indicator Removal on Host	31.7%
7.	T1055: Process Injection	28.5%
8.	T1021: Remote Services	27.4%
9.	T1497: Virtualization/Sandbox Evasion	26.9%
10.	T1105: Ingress Tool Transfer	26.5%
	T1569: System Services	26.5%

Top 5 Most Frequently Seen Sub-Techniques

1.	T1071.001: Web Protocols	32.0%
2.	T1059.001: PowerShell	29.4%
3.	T1070.004: File Deletion	27.1%
4.	T1569.003: Service Execution	26.5%
5.	T1021.001: Remote Desktop Protocol	23.4%

Frequently Targeted Technologies, 2021



MITRE ATT&CK TECHNIQUES RELATED TO MANDIANT TARGETED ATTACK LIFECYCLE, 2021

Targeted Attack Lifecycle

MITRE ATT&CK Framework

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

The Mandiant 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

Active scanning	0.8%	T1595.002: Vulnerability Scanning	0.5%
		T1595.001: Scanning IP Blocks	0.3%

Resource Development

T1588: Obtain Capabilities	16.0%	T1588.003: Code Signing Certificates	15.5%
		T1588.004: Digital Certificates	0.5%
T1608: Stage Capabilities	12.9%	T1608.003: Install Digital Certificate	9.2%
		T1608.005: Link Target	3.5%
		T1608.004: Drive-by Target	0.2%
		T1608.001: Upload Malware	0.2%
		T1608.002: Upload Tool	0.2%
T1583: Acquire Infrastructure	9.4%	T1583.003: Virtual Private Server	9.4%
T1584: Compromise Infrastructure	3.4%		
T1587: Develop Capabilities	1.7%	T1587.003: Digital Certificates	0.9%
		T1587.002: Code Signing Certificates	0.8%

Initial Compromise

Initial Access

T1190: Exploit Public-Facing Application	25.8%		
T1195: Supply Chain Compromise	11.1%	T1195.002: Compromise Software Supply Chain	11.1%
T1133: External Remote Services	8.8%		
T1566: Phishing	8.6%	T1566.001: Spearphishing Attachment	4.3%
		T1566.002: Spearphishing Link	3.5%
T1078: Valid Accounts	6.3%		
T1189: Drive-by Compromise	4.3%		
T1199: Trusted Relationship	0.6%		

Targeted Attack Lifecycle

MITRE ATT&CK Framework

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

Establish Foothold

Persistence

T1053: Scheduled Task/Job	15.8%	T1053.005: Scheduled Task	13.5%
		T1053.003: Cron	0.5%
		T1053.001: At (Linux)	0.2%
T1505: Server Software Component	14.0%	T1505.003: Web Shell	14.0%
		T1505.004: IIS Components	0.5%
T1543: Create or Modify System Process	13.1%	T1543.003: Windows Service	12.8%
		T1543.002: Systemd Service	0.5%
T1133: External Remote Services	8.8%		
T1098: Account Manipulation	8.3%	T1098.001: Additional Cloud Credentials	0.6%
		T1098.002: Exchange Email Delegate Permissions	0.6%
		T1098.004: SSH Authorized Keys	0.6%
T1547: Boot or Logon Autostart Execution	6.9%	T1547.001: Registry Run Keys / Startup Folder	5.5%
		T1547.009: Shortcut Modification	1.4%
		T1547.004: Winlogon Helper DLL	0.6%
		T1547.006: Kernel Modules and Extensions	0.2%
T1136: Create Account	6.3%	T1136.001: Local Account	1.5%
		T1136.002: Domain Account	0.8%
		T1136.003: Cloud Account	0.5%
T1574: Hijack Execution Flow	4.2%	Lore T1574.011: Services Registry Permissions Weakness	3.4%
		T1574.002: DLL Side-Loading	0.9%
		T1574.001: DLL Search Order Hijacking	0.3%
		T1574.008: Path Interception by Search Order Hijacking	0.2%
T1546: Event Triggered Execution	2.8%	T1546.003: Windows Management Instrumentation Event Subscription	1.4%
		T1546.008: Accessibility Features	0.9%
		T1546.007: Netsh Helper DLL	0.3%
		T1546.010: AppInit DLLs	0.2%
		T1546.001: Change Default File Association	0.2%
		T1546.015: Component Object Model Hijacking	0.2%
		T1546.012: Image File Execution Options Injection	0.2%
		T1546.002: Screensaver	0.2%
T1197: BITS Jobs	0.8%		
T1037: Boot or Logon Initialization Scripts	0.5%	T1037.001: Logon Script (Windows)	0.2%
		T1037.003: Network Logon Script	0.2%
		T1037.004: RC Scripts	0.2%
T1556: Modify Authentication Process	0.3%	T1556.003: Pluggable Authentication Modules	0.3%
T1554: Compromise Client Software Binary	0.2%		

Targeted Attack Lifecycle

MITRE ATT&CK Framework

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

Escalate Privileges

Privilege Escalation

T1055: Process Injection	28.5%	T1055.003: Thread Execution Hijacking	2.8%
		T1055.001: Dynamic-link Library Injection	1.1%
		T1055.004: Asynchronous Procedure Call	0.9%
		T1055.012: Process Hollowing	0.8%
		T1055.002: Portable Executable Injection	0.2%
T1053: Scheduled Task/Job	15.8%	T1053.005: Scheduled Task	13.5%
		T1053.003: Cron	0.5%
		T1053.001: At (Linux)	0.2%
T1543: Create or Modify System Process	13.1%	T1543.003: Windows Service	12.8%
		T1543.002: Systemd Service	0.5%
T1134: Access Token Manipulation	12.2%	T1134.001: Token Impersonation/Theft	6.3%
		T1134.002: Create Process with Token	0.2%
T1547: Boot or Logon Autostart Execution	6.9%	T1547.001: Registry Run Keys / Startup Folder	5.5%
		T1547.009: Shortcut Modification	1.4%
		T1547.004: Winlogon Helper DLL	0.6%
		T1547.006: Kernel Modules and Extensions	0.2%
T1078: Valid Accounts	6.3%		
T1574: Hijack Execution Flow	4.2%	T1574.011: Services Registry Permissions Weakness	3.4%
		T1574.002: DLL Side-Loading	0.9%
		T1574.001: DLL Search Order Hijacking	0.3%
		T1574.008: Path Interception by Search Order Hijacking	0.2%
T1546: Event Triggered Execution	2.8%	T1546.003: Windows Management Instrumentation Event Subscription	1.4%
		T1546.008: Accessibility Features	0.9%
		T1546.007: Netsh Helper DLL	0.3%
		T1546.010: AppInit DLLs	0.2%
		T1546.001: Change Default File Association	0.2%
		T1546.015: Component Object Model Hijacking	0.2%
		T1546.012: Image File Execution Options Injection	0.2%
		T1546.002: Screensaver	0.2%
T1548: Abuse Elevation Control Mechanism	2.2%	T1548.002: Bypass User Account Control	2.0%
		T1548.001: Setuid and Setgid	0.2%
T1484: Domain Policy Modification	0.8%	T1484.001: Group Policy Modification	0.8%
T1037: Boot or Logon Initialization Scripts	0.5%	T1037.001: Logon Script (Windows)	0.2%
		T1037.003: Network Logon Script	0.2%
		T1037.004: RC Scripts	0.2%
T1068: Exploitation for Privilege Escalation	0.3%		

Targeted Attack Lifecycle

MITRE ATT&CK Framework

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

Internal Reconnaissance

Discovery

T1082: System Information Discovery	31.8%		
T1083: File and Directory Discovery	31.7%		
T1497: Virtualization/Sandbox Evasion	26.9%	T1497.001: System Checks	17.7%
		T1497.003: Time Based Evasion	3.4%
T1012: Query Registry	21.1%		
T1033: System Owner/User Discovery	19.1%		
T1057: Process Discovery	18.9%		
T1016: System Network Configuration Discovery	16.9%	T1016.001: Internet Connection Discovery	0.6%
T1518: Software Discovery	16.8%	T1518.001: Security Software Discovery	0.3%
T1087: Account Discovery	13.7%	T1087.002: Domain Account	2.3%
		T1087.001: Local Account	1.4%
		T1087.004: Cloud Account	0.2%
		T1087.003: Email Account	0.2%
T1482: Domain Trust Discovery	8.2%		
T1069: Permission Groups Discovery	8.2%	T1069.002: Domain Groups	2.0%
		T1069.001: Local Groups	1.1%
		T1069.003: Cloud Groups	0.2%
T1007: System Service Discovery	8.0%		
T1010: Application Window Discovery	6.5%		
T1135: Network Share Discovery	6.2%		
T1049: System Network Connections Discovery	6.2%		
T1614: System Location Discovery	3.8%	T1614.001: System Language Discovery	3.8%
T1018: Remote System Discovery	2.6%		
T1046: Network Service Scanning	2.0%		
T1580: Cloud Infrastructure Discovery	0.8%		
T1124: System Time Discovery	0.6%		
T1040: Network Sniffing	0.3%		
T1201: Password Policy Discovery	0.3%		
T1538: Cloud Service Dashboard	0.2%		
T1526: Cloud Service Discovery	0.2%		
T1619: Cloud Storage Object Discovery	0.2%		
T1120: Peripheral Device Discovery	0.2%		

Targeted Attack Lifecycle

MITRE ATT&CK Framework

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

Lateral Movement

Lateral Movement

T1021: Remote Services	27.4%	T1021.001: Remote Desktop Protocol	23.4%
		T1021.004: SSH	4.8%
		T1021.002: SMB/Windows Admin Shares	4.0%
		T1021.005: VNC	0.5%
		T1021.006: Windows Remote Management	0.2%
T1550: Use Alternate Authentication Material	0.8%	T1550.002: Pass the Hash	0.5%
		T1550.001: Application Access Token	0.2%
		T1550.003: Pass the Ticket	0.2%
T1570: Lateral Tool Transfer	0.6%		
T1534: Internal Spearphishing	0.5%		

Targeted Attack Lifecycle

MITRE ATT&CK Framework

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

Maintain Presence

Persistence

T1053: Scheduled Task/Job	15.8%	T1053.005: Scheduled Task	13.5%
		T1053.003: Cron	0.5%
		T1053.001: At (Linux)	0.2%
T1505: Server Software Component	14.0%	T1505.003: Web Shell	14.0%
		T1505.004: IIS Components	0.5%
T1543: Create or Modify System Process	13.1%	T1543.003: Windows Service	12.8%
		T1543.002: Systemd Service	0.5%
T1133: External Remote Services	8.8%		
T1098: Account Manipulation	8.3%	T1098.001: Additional Cloud Credentials	0.6%
		T1098.002: Exchange Email Delegate Permissions	0.6%
		T1098.004: SSH Authorized Keys	0.6%
T1547: Boot or Logon Autostart Execution	6.9%	T1547.001: Registry Run Keys / Startup Folder	5.5%
		T1547.009: Shortcut Modification	1.4%
		T1547.004: Winlogon Helper DLL	0.6%
		T1547.006: Kernel Modules and Extensions	0.2%
T1136: Create Account	6.3%	T1136.001: Local Account	1.5%
		T1136.002: Domain Account	0.8%
		T1136.003: Cloud Account	0.5%
T1574: Hijack Execution Flow	4.2%	T1574.011: Services Registry Permissions Weakness	3.4%
		T1574.002: DLL Side-Loading	0.9%
		T1574.001: DLL Search Order Hijacking	0.3%
		T1574.008: Path Interception by Search Order Hijacking	0.2%
T1546: Event Triggered Execution	2.8%	T1546.003: Windows Management Instrumentation Event Subscription	1.4%
		T1546.008: Accessibility Features	0.9%
		T1546.007: Netsh Helper DLL	0.3%
		T1546.010: AppInit DLLs	0.2%
		T1546.001: Change Default File Association	0.2%
		T1546.015: Component Object Model Hijacking	0.2%
		T1546.012: Image File Execution Options Injection	0.2%
		T1546.002: Screensaver	0.2%
T1197: BITS Jobs	0.8%		
T1037: Boot or Logon Initialization Scripts	0.5%	T1037.001: Logon Script (Windows)	0.2%
		T1037.003: Network Logon Script	0.2%
		T1037.004: RC Scripts	0.2%
T1556: Modify Authentication Process	0.3%	T1556.003: Pluggable Authentication Modules	0.3%
T1554: Compromise Client Software Binary	0.2%		

Targeted Attack Lifecycle

MITRE ATT&CK Framework

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

Mission Completion

Collection

T1560: Archive Collected Data	13.8%	T1560.001: Archive via Utility	4.0%
		T1560.002: Archive via Library	1.1%
T1056: Input Capture	7.5%	T1056.001: Keylogging	7.5%
T1213: Data from Information Repositories	6.9%	T1213.003: Code Repositories	1.1%
		T1213.002: Sharepoint	1.1%
		T1213.001: Confluence	0.3%
T1074: Data Staged	4.6%	T1074.001: Local Data Staging	3.8%
		T1074.002: Remote Data Staging	1.5%
T1115: Clipboard Data	4.3%		
T1113: Screen Capture	3.8%		
T1114: Email Collection	2.0%	T1114.002: Remote Email Collection	1.1%
		T1114.001: Local Email Collection	0.3%
		T1114.003: Email Forwarding Rule	0.2%
T1039: Data from Network Shared Drive	1.1%		
T1530: Data from Cloud Storage Object	0.9%		
T1005: Data from Local System	0.5%		
T1119: Automated Collection	0.2%		
T1602: Data from Configuration Repository	0.2%	T1602.002: Network Device Configuration Dump	0.2%

Exfiltration

T1567: Exfiltration Over Web Service	3.1%	T1567.002: Exfiltration to Cloud Storage	0.9%
		T1567.001: Exfiltration to Code Repository	0.2%
T1020: Automated Exfiltration	1.1%		
T1041: Exfiltration Over C2 Channel	0.6%		
T1030: Data Transfer Size Limits	0.2%		
T1048: Exfiltration Over Alternative Protocol	0.2%		

Impact

T1486: Data Encrypted for Impact	22.6%		
T1489: Service Stop	11.5%		
T1529: System Shutdown/Reboot	4.9%		
T1490: Inhibit System Recovery	3.2%		
T1496: Resource Hijacking	3.2%		
T1485: Data Destruction	2.8%		
T1565: Data Manipulation	0.5%	T1565.001: Stored Data Manipulation	0.5%
T1531: Account Access Removal	0.3%		
T1491: Defacement	0.2%	T1491.002: External Defacement	0.2%
T1561: Disk Wipe	0.2%	T1561.002: Disk Structure Wipe	0.2%

Targeted Attack Lifecycle

MITRE ATT&CK Framework

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

Across the Lifecycle

Credential Access

T1003: OS Credential Dumping	9.8%	T1003.001: LSASS Memory	4.3%
		T1003.003: NTDS	3.7%
		T1003.002: Security Account Manager	1.4%
		T1003.008: /etc/passwd and /etc/shadow	1.2%
		T1003.006: DCSync	0.8%
		T1003.004: LSA Secrets	0.2%
T1056: Input Capture	7.5%	T1056.001: Keylogging	7.5%
T1552: Unsecured Credentials	4.0%	T1552.004: Private Keys	1.4%
		T1552.002: Credentials in Registry	1.1%
		T1552.001: Credentials In Files	0.6%
		T1552.006: Group Policy Preferences	0.6%
		T1552.003: Bash History	0.5%
		T1552.005: Cloud Instance Metadata API	0.3%
T1558: Steal or Forge Kerberos Tickets	2.5%	T1558.003: Kerberoasting	2.0%
		T1558.004: AS-REP Roasting	0.3%
		T1558.001: Golden Ticket	0.2%
T1555: Credentials from Password Stores	2.0%	T1555.003: Credentials from Web Browsers	1.4%
		T1555.005: Password Managers	0.5%
		T1555.004: Windows Credential Manager	0.2%
T1110: Brute Force	3.7%	T1110.001: Password Guessing	1.2%
		T1110.003: Password Spraying	0.9%
		T1110.004: Credential Stuffing	0.5%
T1111: Two-Factor Authentication Interception	1.1%		
T1539: Steal Web Session Cookie	0.8%		
T1187: Forced Authentication	0.5%		
T1556: Modify Authentication Process	0.3%	T1556.003: Pluggable Authentication Modules	0.3%
T1040: Network Sniffing	0.3%		
T1606: Forge Web Credentials	0.2%	T1606.001: Web Cookies	0.2%

Command and Control

T1071: Application Layer Protocol	36.8%	T1071.001: Web Protocols	32.0%
		T1071.004: DNS	8.2%
		T1071.002: File Transfer Protocols	0.3%
T1105: Ingress Tool Transfer	26.5%		
T1573: Encrypted Channel	14.3%	T1573.002: Asymmetric Cryptography	13.7%
		T1573.001: Symmetric Cryptography	0.6%
T1095: Non-Application Layer Protocol	12.8%		
T1090: Proxy	6.2%	T1090.003: Multi-hop Proxy	3.5%
		T1090.004: Domain Fronting	0.8%
		T1090.001: Internal Proxy	0.2%
T1572: Protocol Tunneling	4.5%		
T1568: Dynamic Resolution	3.4%	T1568.002: Domain Generation Algorithms	3.4%
T1219: Remote Access Software	1.4%		
T1102: Web Service	1.1%	T1102.001: Dead Drop Resolver	0.2%
T1132: Data Encoding	0.8%	T1132.001: Standard Encoding	0.8%
T1001: Data Obfuscation	0.5%	T1001.002: Steganography	0.2%
T1008: Fallback Channels	0.2%		

Targeted Attack Lifecycle

MITRE ATT&CK Framework

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

Defense Evasion

T1027: Obfuscated Files or Information	51.4%	T1027.005: Indicator Removal from Tools	9.8%
		T1027.002: Software Packing	5.4%
		T1027.003: Steganography	3.4%
		T1027.004: Compile After Delivery	0.5%
T1070: Indicator Removal on Host	31.7%	T1070.004: File Deletion	27.1%
		T1070.006: Timestomp	6.5%
		T1070.001: Clear Windows Event Logs	3.7%
		T1070.005: Network Share Connection Removal	1.7%
		T1070.002: Clear Linux or Mac System Logs	0.5%
		T1070.003: Clear Command History	0.3%
T1055: Process Injection	28.5%	T1055.003: Thread Execution Hijacking	2.8%
		T1055.001: Dynamic-link Library Injection	1.1%
		T1055.004: Asynchronous Procedure Call	0.9%
		T1055.012: Process Hollowing	0.8%
		T1055.002: Portable Executable Injection	0.2%
T1497: Virtualization/Sandbox Evasion	26.9%	T1497.001: System Checks	17.7%
		T1497.003: Time Based Evasion	3.4%
T1140: Deobfuscate/Decode Files or Information	23.5%		
T1112: Modify Registry	22.3%		
T1564: Hide Artifacts	20.2%	T1564.003: Hidden Window	18.9%
		T1564.008: Email Hiding Rules	0.9%
		T1564.004: NTFS File Attributes	0.3%
T1553: Subvert Trust Controls	15.5%	T1553.002: Code Signing	15.5%
T1620: Reflective Code Loading	13.5%		
T1562: Impair Defenses	13.4%	T1562.001: Disable or Modify Tools	9.1%
		T1562.004: Disable or Modify System Firewall	5.7%
		T1562.003: Impair Command History Logging	0.5%
		T1562.008: Disable Cloud Logs	0.3%
		T1562.007: Disable or Modify Cloud Firewall	0.2%
T1134: Access Token Manipulation	12.2%	T1134.001: Token Impersonation/Theft	6.3%
		T1134.002: Create Process with Token	0.2%
T1202: Indirect Command Execution	8.2%		
T1078: Valid Accounts	6.3%		
T1218: Signed Binary Proxy Execution	5.4%	T1218.011: Rundll32	3.4%
		T1218.005: Mshta	0.6%
		T1218.010: Regsvr32	0.6%
		T1218.007: Msiexec	0.5%
		T1218.002: Control Panel	0.3%
		T1218.003: CMSTP	0.2%

Targeted Attack Lifecycle

MITRE ATT&CK Framework

20.00%	100.00%
10.00%	19.99%
5.00%	9.99%
2.00%	4.99%
0.00%	1.99%

T1574: Hijack Execution Flow	4.2%	T1574.011: Services Registry Permissions Weakness	3.4%
		T1574.002: DLL Side-Loading	0.9%
		T1574.001: DLL Search Order Hijacking	0.3%
		T1574.008: Path Interception by Search Order Hijacking	0.2%
T1480: Execution Guardrails	3.7%	T1480.001: Environmental Keying	0.2%
T1036: Masquerading	3.2%	T1036.005: Match Legitimate Name or Location	0.6%
		T1036.007: Double File Extension	0.3%
		T1036.003: Rename System Utilities	0.3%
T1548: Abuse Elevation Control Mechanism	2.2%	T1548.002: Bypass User Account Control	2.0%
		T1548.001: Setuid and Setgid	0.2%
T1222: File and Directory Permissions Modification	1.7%	T1222.001: Windows File and Directory Permissions Modification	0.6%
		T1222.002: Linux and Mac File and Directory Permissions Modification	0.5%
T1197: BITS Jobs	0.8%		
T1484: Domain Policy Modification	0.8%	T1484.001: Group Policy Modification	0.8%
T1550: Use Alternate Authentication Material	0.8%	T1550.002: Pass the Hash	0.5%
		T1550.001: Application Access Token	0.2%
		T1550.003: Pass the Ticket	0.2%
T1127: Trusted Developer Utilities Proxy Execution	0.5%	T1127.001: MSBuild	0.5%
T1556: Modify Authentication Process	0.3%	T1556.003: Pluggable Authentication Modules	0.3%
T1578: Modify Cloud Compute Infrastructure	0.3%	T1578.002: Create Cloud Instance	0.3%
		T1578.003: Delete Cloud Instance	0.2%
T1014: Rootkit	0.3%		

Execution

T1059: Command and Scripting Interpreter	44.9%	T1059.001: PowerShell	29.4%
		T1059.003: Windows Command Shell	11.2%
		T1059.005: Visual Basic	4.0%
		T1059.006: Python	3.4%
		T1059.007: JavaScript	1.8%
		T1059.004: Unix Shell	1.5%
T1569: System Services	26.5%	T1569.002: Service Execution	26.5%
T1053: Scheduled Task/Job	15.8%	T1053.005: Scheduled Task	13.5%
		T1053.003: Cron	0.5%
		T1053.001: At (Linux)	0.2%
T1204: User Execution	5.8%	T1204.001: Malicious Link	3.4%
		T1204.002: Malicious File	2.5%
T1047: Windows Management Instrumentation	4.0%		
T1203: Exploitation for Client Execution	2.0%		
T1559: Inter-Process Communication	0.8%	T1559.001: Component Object Model	0.5%
T1129: Shared Modules	0.6%		

CONCLUSION

The cyber threat landscape is vast and deep and regularly influenced by the world around us. When the COVID-19 pandemic began, we observed an uptick in targeting of healthcare and research and development. Now, at the time of publishing *M-Trends 2022*, the situation unfolding in Ukraine shows how tightly the geopolitical and cyber worlds are intertwined.

Our mission at Mandiant is to ensure every organization is secure from cyber threats and confident in their readiness. The annual *M-Trends* report represents significant effort towards advancing that mission with the use of data and learnings from our incident response engagements.

The global median dwell time is now 21 days, down from 24 days last year, which is a downward trend we like to see. A trend we don't like to see is the continued use of ransomware and multifaceted extortion. With low risks and barrier to entry and high rewards, we see this as an ongoing threat posing a risk to every organization.

Preparation is vital not just for ransomware but all types of attacks, whether through red teaming, tabletop exercises, training or other techniques. Sound fundamentals, such as vulnerability and patch management, least privilege and hardening also play a role in building strong defenses. Our case study involving coinminers illustrates the value of logging and following up on alerts, since the investigation eventually led to even more significant threats.

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.

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

Since 2004, Mandiant® has been a trusted partner to security-conscious organizations. Today, industry-leading Mandiant threat intelligence and expertise drive dynamic solutions that help organizations develop more effective programs and instill confidence in their cyber readiness.

MANDIANT