REPORT

Security Report 2023

March 2023

KEYSIGHT

Table of Contents

Introduction

Welcome to the fifth edition of this security report issued by Keysight Technologies. This report combines lessons learned in 2022 along with predictions for 2023. Both the data and the predictions are based upon research conducted by Keysight's Application and Threat Intelligence (ATI) Research Center.

The purpose of this report is to help strengthen global cybersecurity. Effective cybersecurity needs to be a collaborative function by security experts. This report is one way of sharing what Keysight has learned over the past year with the international community of security practitioners. We hope it will help security teams think about their security architecture vulnerabilities and how they can better prepare for future attacks.

There were three trends that characterized cybercrime for most of 2022:

- Malware as a service became more prevalent
- Ransomware continued in full force with attacks on healthcare leading the way[1]
- Threat actors continue to leverage old vulnerabilities in campaigns

In this report, we will explore these three trends from the perspective of our research data along with published MITRE Corporation information. We then suggest three areas of focus for enterprises in 2023 to help protect themselves.

Specifically, this report will cover the following areas:

- 2022 – A year in review
- CISA alerts for vulnerabilities in 2022
- Android malware with focus on polymorphism
- Top vulnerabilities disclosed in 2022
- Our view of potential 2023 threats
- Some suggestions for actions that can be taken

2022 – A Year in Review

In this report, we will highlight some of the threats we followed along with strategies for mitigation and educational takeaways. We hope all readers learn something new and come away with actionable intelligence for their organization.

[1] Mathew J. Schwartz, "Healthcare Most Hit by Ransomware Last Year, FBI Finds," Data Breach Today, February 27, 2023.

Top MITRE ATT&CK techniques

We will begin with a review of the MITRE ATT&CK® tactics and techniques (TTPs) that we have captured from the analysis of threat actors and families of malware. For anyone that wants a refresher of MITRE ATT&CK TTPs, we have provided a primer in Appendix A of this document to help you out.

These techniques are related to sandbox detonations and research the Keysight ATI team conducted in our threat intelligence analysis lab to generate content for our products to help improve our customers' security posture. Keysight's threat intelligence system is continually being optimized by the security engineering team through the collection of malware based on the most relevant threat actors and families of malware in use. As new samples are collected, they are sent through an automated set of analysis tools that have been built up over the past decade.

For these attacks, we will analyze the MITRE ATT&CK tactics and techniques used on the endpoint side during malware executions after a compromise. The attack can be an information stealer like RedLineStealer, Lokibot, or Raccoon, a remote access tool (RAT) such as Agent Tesla or Remcos, or ransomware like LockBit and Conti.

Malware

It's essential to understand how MITRE TTPs are applied to malware families. Keysight has dedicated efforts to continuously identify and track malware families along with their command and control (C&C) infrastructure.

We can start with a cross-correlation of the United States Cybersecurity and Infrastructure Security Agency (CISA) top malware strains article. While the 2022 top malware attacks haven't been published yet, we can use the top 2021 attacks as a starting point[2]. If we compare our findings with the top CISA malware families, we'll find that some of them are still very active (see below) even after more than five years. In our threat intelligence system, we've observed the following top malware families:

- Lokibot (top 5 CISA)
- Redline and NanoCore (top 7 CISA)
- Agent Tesla (top 1 CISA)

Lokibot[3] – This information stealer has been around for a long time. It was first reported as far back as 2015, usually distributed as an attachment in email spam campaigns. Keysight has been tracking Lokibot for the past three years. Looking at the data from the past year, we've noticed the following MITRE ATT&CK TTPs in approximately 75% of the monitored Lokibot executions.

[2] https://www.cisa.gov/uscert/sites/default/files/publications/aa22-216a-2021-top-malware-strains.pdf
[3] https://attack.mitre.org/versions/v11/software/S0447/

The top MITRE techniques used with the Lokibot attack are listed in Table 1.

Table 1. Top MITRE techniques used with Lokibot malware

Tactic	Tactic name	Technique	Technique name
TA0007	Discovery	T1033	System Owner/User Discovery
TA0002	Execution	T1106	Native API
TA0007	Discovery	T1083	File and Directory Discovery
TA0007	Discovery	T1082	System Information Discovery
TA0007	Discovery	T1497	Virtualization/Sandbox Evasion
TA0006	Credential Access	T1552	Unsecured Credentials
TA0006	Credential Access	T1003	OS Credential Dumping
TA0002	Execution	T1569	System Services
TA0009	Collection	T1005	Data from Local System
TA0006	Credential Access	T1555	Credentials from Password Stores
TA0005	Defense Evasion	T1070	Indicator Removal on Host
TA0005	Defense Evasion	T1564	Hide Artifacts
TA0005	Defense Evasion	T1045	Obfuscated Files or Information: Software Packing

Looking at the C&C servers used by Lokibot operators, we can see the geolocation distribution of C&C servers used by the Lokibot malware. See Figure 1. One item of interest, related to the network traffic, is that throughout these past years, Lokibot hasn't changed a lot — notably the User-Agent in the HTTP connections "Mozilla/4.08 (Charon; Inferno)".

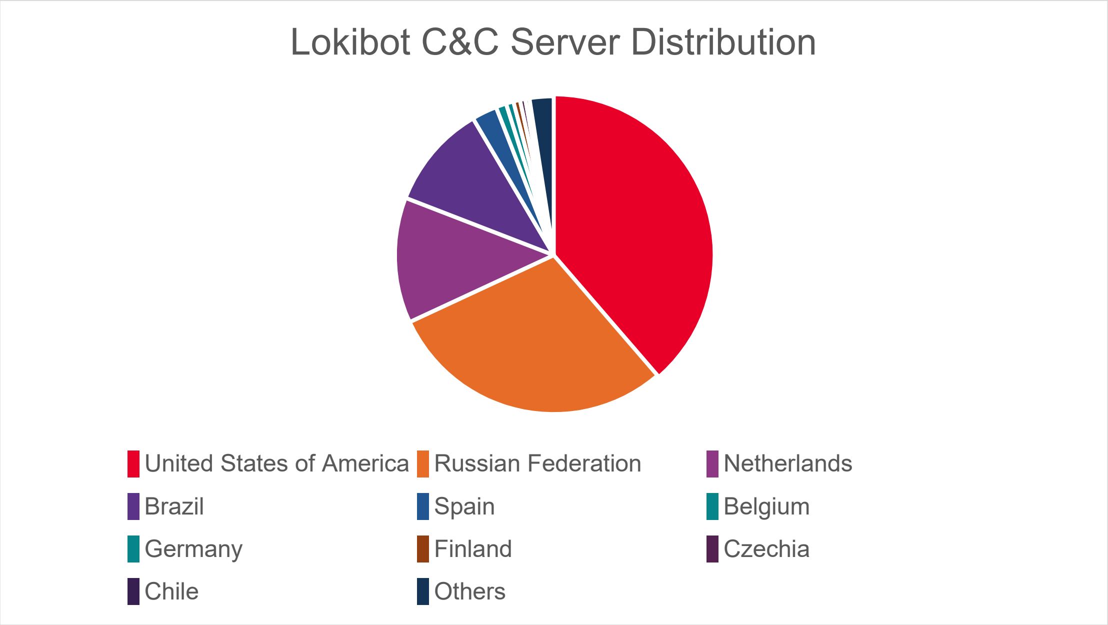


Figure 1. Lokibot malware C&C server geographic location

Redline – While not in the CISA top 2021 malware families, we've observed high activity throughout 2022 from Redline. Other security researchers have seen this as well[4]. Redline's primary function is to be an infostealer — harvesting credentials and targeting a wide variety of cryptocurrency wallets from the victim system. Late 2022 showed a different approach in how it's being distributed — abusing Google Ads by impersonating various software projects and tools.[5]

The top MITRE techniques used with the Redline attack are listed in Table 2.

Table 2. Top MITRE techniques used with Redline malware

Tactic	Tactic name	Technique	Technique name
TA0007	Discovery	T1012	Query Registry
TA0007	Discovery	T1082	System Information Discovery
TA0007	Discovery	T1033	System Owner/User Discovery
TA0007	Discovery	T1083	File and Directory Discovery
TA0007	Discovery	T1497	Virtualization/Sandbox Evasion
TA0002	Execution	T1106	Native API
TA0002	Execution	T1047	Windows® Management Instrumentation
TA0006	Credential Access	T1555	Credentials from Password Stores
TA0007	Discovery	T1057	Process Discovery

Looking at the number of C&C servers detected, we can see that the malware actors have preferred using infrastructure in the Russian Federation (more than double than the next two countries combined) for hosting Redline C&C servers. See Figure 2. While the earlier versions of the malware would use SOAP over HTTP for communications, Redline has transitioned towards sending data in SOAP carried over NET.TCP.

[4] https://info.spamhaus.com/hubfs/Botnet%20Reports/2022%20Q3%20Botnet%20Threat%20Update.pdf
[5] Bill Toulas, "Hackers abuse Google Ads to spread malware in legit software", Bleeping Computer, December 22, 2022.

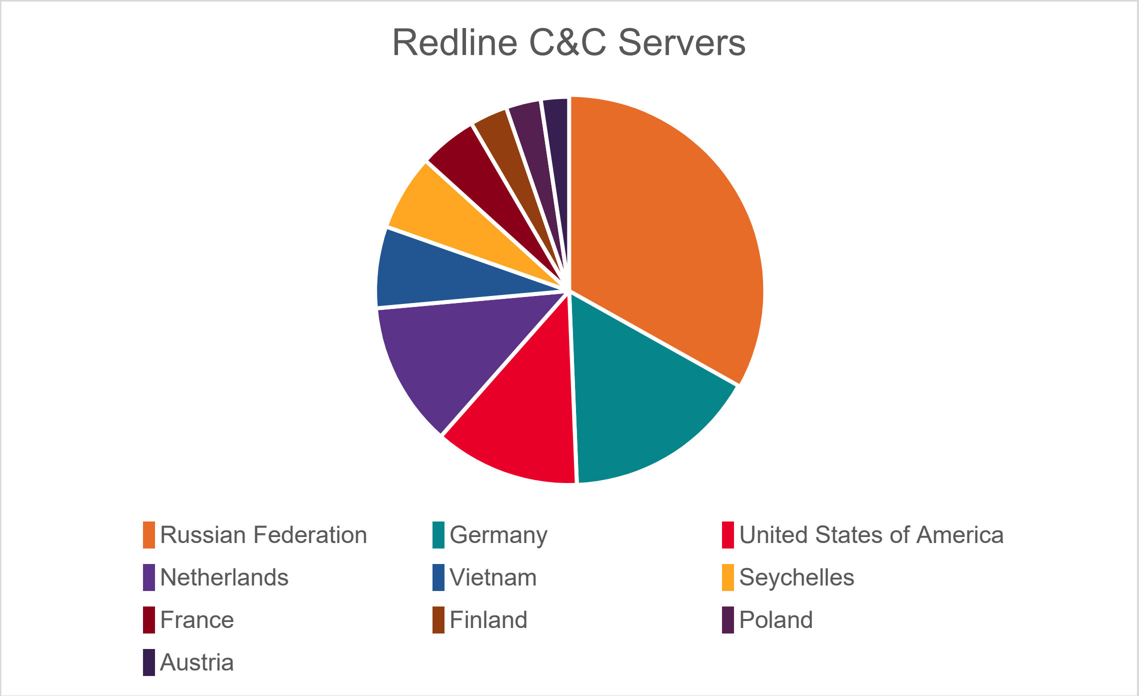


Figure 2. Redline malware C&C server geographic location

NanoCore[6] – This is a remote access Trojan (i.e. RAT) distributed mainly through malspam campaigns, with multiple updates in terms of functionality over time. Spamphaus reported an increase of over 264% in NanoCore activity[7] in the 3rd quarter of 2022. Although there have been changes on the endpoint side, we've noticed that the C&C communication hasn't changed — a custom TCP protocol that uses DES encryption with a hardcoded key.

The top MITRE techniques used with the NanoCore attack are listed in Table 3.

Table 3. Top MITRE techniques used with NanoCore malware

Tactic	Tactic name	Technique	Technique name
TA0007	Discovery	T1033	System Owner/User Discovery
TA0007	Discovery	T1083	File and Directory Discovery
TA0007	Discovery	T1497	Virtualization/Sandbox Evasion
TA0007	Discovery	T1082	System Information Discovery
TA0007	Discovery	T1012	Query Registry
TA0007	Discovery	T1057	Process Discovery
TA0003	Persistence	T1053	Scheduled Task/Job
TA0005	Defense evasion	T1027	Obfuscated Files or Information
TA0003	Persistence	T1547	Boot or Logon Autostart Execution
TA0005	Execution	T1055	Process Injection

[6] https://attack.mitre.org/software/S0336/
[7] https://info.spamhaus.com/hubfs/Botnet%20Reports/2022%20Q3%20Botnet%20Threat%20Update.pdf

Agent Tesla[8] – This is another infostealer that has been active for quite some time. It is often used to get an initial foothold into a network. It is commonly packaged as part of a malware as a service solution in the cyber underworld and uses process injection via hollowing to evade security controls. For data exfiltration, although it also has both SMTP and FTP capabilities for its C&C connections, we've noticed that Agent Tesla tends to favor SMTP for C&C connections.

The top MITRE techniques used with the Agent Tesla attack are listed in Table 4.

Table 4. Top MITRE techniques used with Agent Tesla malware

Tactic	Tactic name	Technique	Technique name
TA0005	Execution	T1047	Windows Management Instrumentation
TA0007	Discovery	T1033	System Owner/User Discovery
TA0007	Discovery	T1012	Query Registry
TA0007	Discovery	T1082	System Information Discovery
TA0007	Discovery	T1057	Process Discovery
TA0007	Discovery	T1016	System Network Configuration Discovery
TA0007	Discovery	T1083	File and Directory Discovery
TA0007	Discovery	T1497	Virtualization/Sandbox Evasion
TA0007	Discovery	T1124	System Time Discovery
TA0006	Credential access	T1003	Unsecured Credentials
TA0006	Credential access	T1555	Credentials from Password Stores
TA0005	Defense Evasion	T1055	Process Injection

Key takeaways for malware in 2022:

2022 has been a year of increased activity in the realm of infostealers and RATs, with Redline taking the lead in this sector. While for most malware families from these categories, understanding the network protocol for communication and generating signatures to block them isn't a difficult endeavor, it's clear from the increased activity and usage of these tools — that this problem hasn't been solved.

Another key aspect while looking at these malware families, is the observation that the Discovery tactic is prevalent. Malware actors are spending more and more effort in understanding and grabbing as much information as possible about the environment that they're running their software in before moving to other phases of the execution.

Network / C&C servers

If we look at the top 10 countries hosting C&C servers, we can identify some interesting trends. See Figures 3 and 4. While the top 4 countries are essentially the same (just changing positions between

[8] https://attack.mitre.org/software/S0331/

them) from previous years, we can see a big increase in the number of C&Cs identified in Russia — an increase of almost 300% in 2022 vs 2021, followed by a 190% increase in the USA. Whether this is related to the war in Ukraine or not is difficult to tell. However, the increase is difficult to ignore.

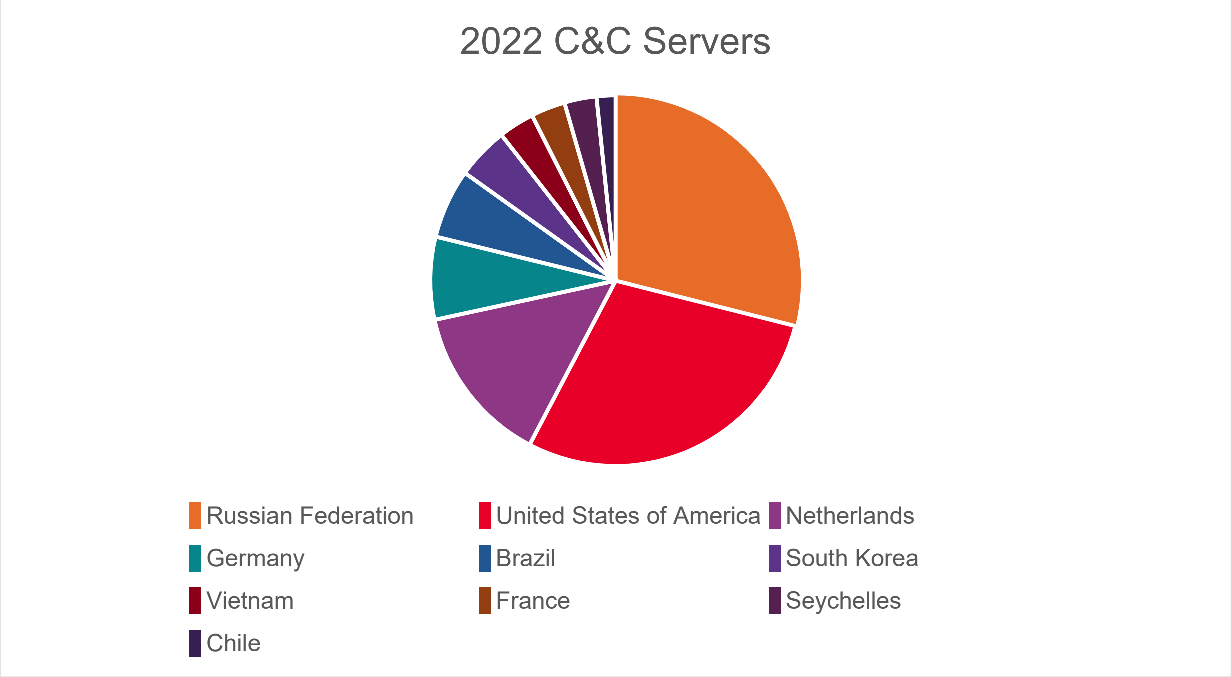


Figure 3. Top malware C&C server geographic location for 2022

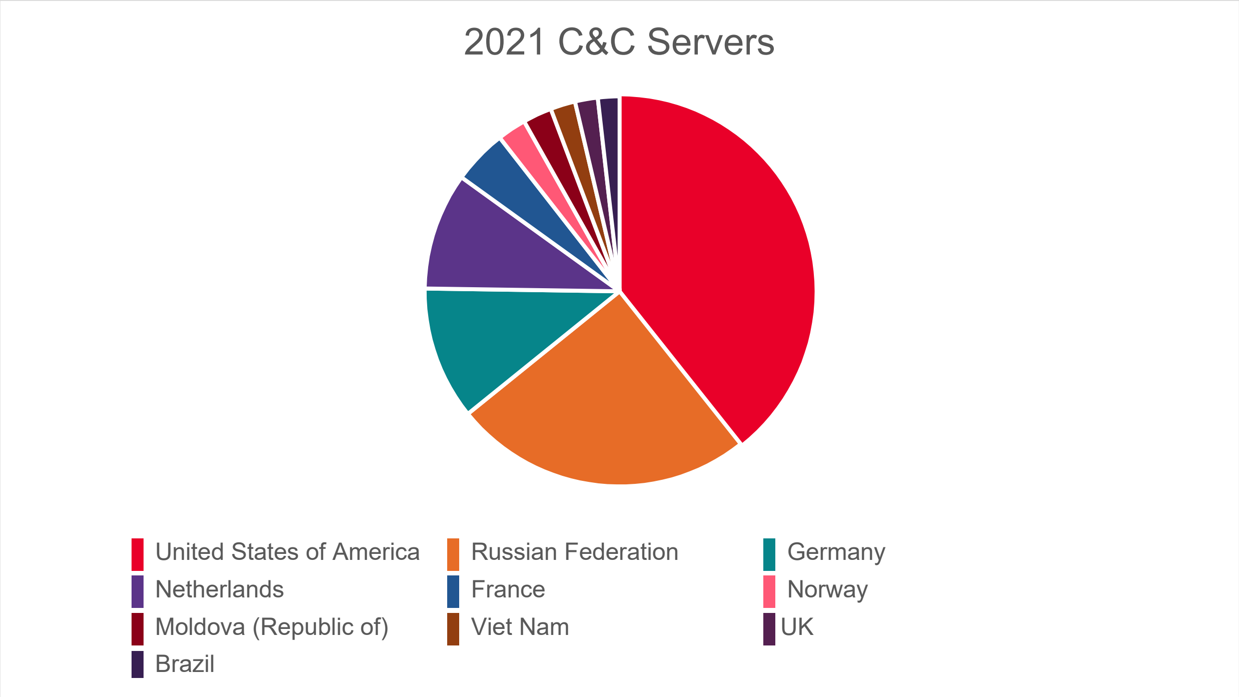


Figure 4. Top malware C&C server geographic location for 2021

CISA Alerts for Vulnerabilities in 2022

In this section we will be analyzing the vulnerabilities which were mentioned multiple times in CISA alerts, excluding the known exploited vulnerabilities (KEV) binding operation directives. The CISA released a total of 35 alerts in 2022. This included 21 alerts that had some vulnerabilities mentioned in the form of CVEs. In total, there were 93 unique CVEs mentioned in these alerts, which were mainly distributed amongst the vendors shown in Figure 5.

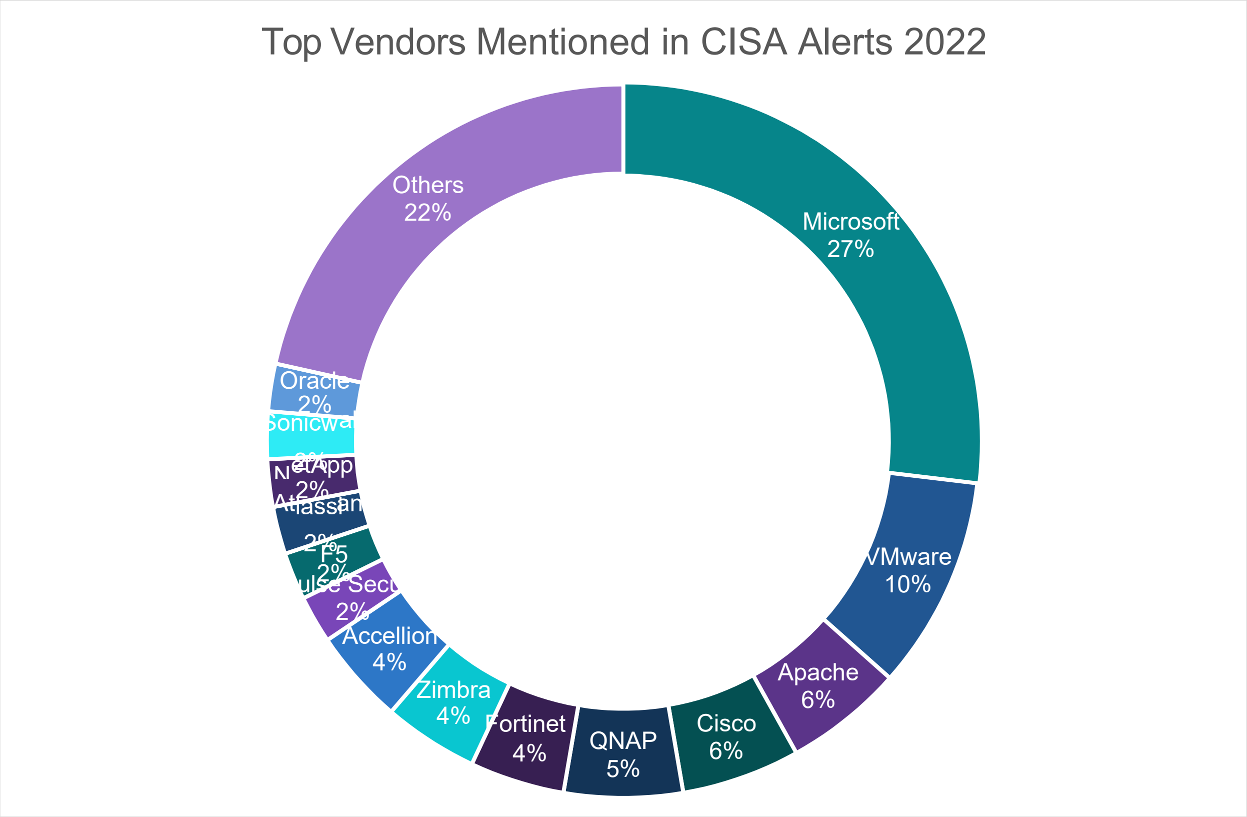


Figure 5. Top vendors mentioned in 2022 CISA alerts

Let’s look at some of the vulnerabilities in detail.

Log4J

The vulnerability which was mentioned the most amongst the alerts was the CVE-2021-44228 Log4J vulnerability. This vulnerability was disclosed in December of 2021, and it took the cyber world by storm. We released a blog post to cover this vulnerability when we first saw it in 2021.

As can be seen from the graph in Figure 6, our honeypots observed a steep rise in exploitation attempts for this vulnerability from December of 2021 onwards. It continued to be popular for most of the first half of 2022. During the March 2022 time period, advanced persistent threat (APT) groups like DeepPanda had launched a campaign targeting the VMware Horizon servers for the Log4J vulnerability.[9]

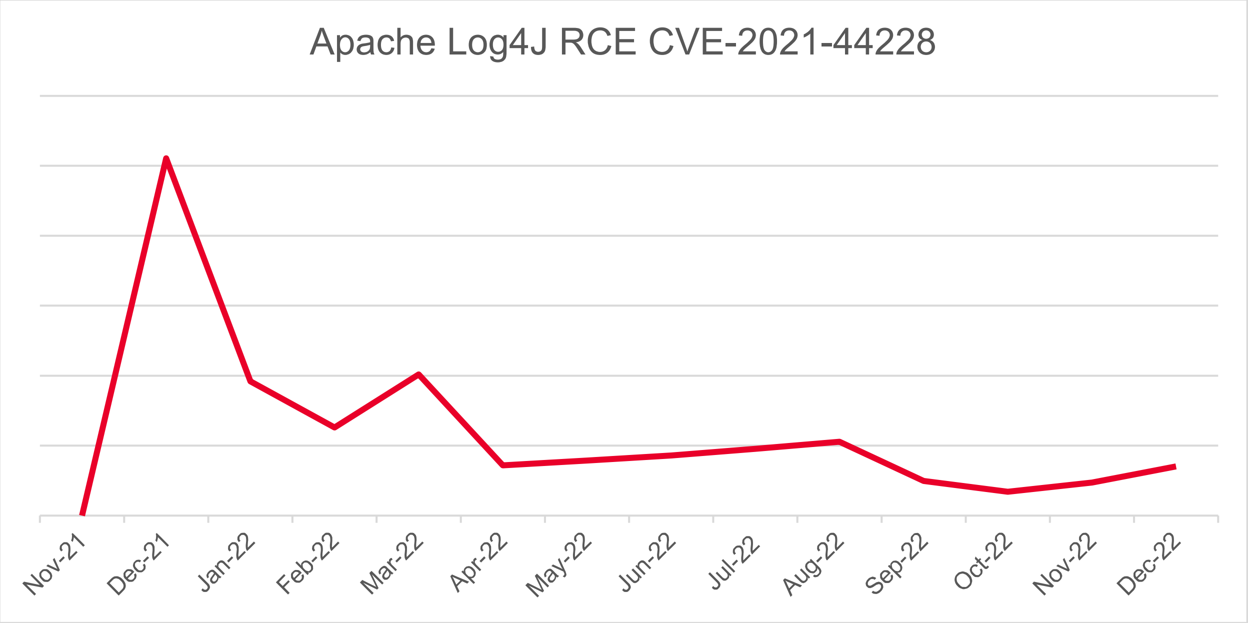


Figure 6. Apache Log4J exploits plotted versus time in 2022

This vulnerability was, and is still being actively exploited, and it remains the most popular vulnerability of 2022. The vulnerability in Log4J was seen being used by various APT threat actors like Lazarus Group and Hafnium.

[9] Rotem Sde-Or and Eliran Voronovitch blog, “New Milestones for Deep Panda: Log4Shell and Digitally Signed Fire Chili Rootkits,” March 30, 2022, Fortinet Inc.

Microsoft Exchange Server and Active Directory related vulnerabilities

There is a second set of popular vulnerabilities with CISA alerts that can be grouped into the following three categories:

- NetLogon Privilege Escalation Vulnerability
- ProxyShell Vulnerabilities
- ProxyLogon and HAFNIUM exploited vulnerabilities

NetLogon Privilege Escalation Vulnerability

The NetLogon vulnerability is also known as ZeroLogon and is tracked with CVE-2020-1472. This vulnerability works by escalating privileges in a domain controller until it can completely take control of the domain. It was one of the most popular vulnerabilities of 2020. However, it continues to be one of the most actively exploited vulnerabilities in 2022 and into 2023. CISA issued their latest alert for the vulnerability in December of 2022, with their alert for the Cuba Ransomware.

To read more about the technical details for this vulnerability and how you can better track this vulnerability, please refer to this blog written by our team.

ProxyShell Vulnerabilities

ProxyShell vulnerabilities were first discussed at Black Hat 2021. Attackers continued to leverage the vulnerability throughout 2022. There are three different CVEs that cover this type of vulnerability: CVE-2021-34473 (Exchange EwsAutodiscoverProxyRequestHandler SSRF), CVE-2021-34523 (Elevation of Privilege on Exchange PowerShell Backend), and CVE-2021-31207 (Exchange MailboxExportRequest Arbitrary File Write). When the three CVEs are chained together, they result in the exploitation of the ProxyShell vulnerability.

Figure 7 shows a flow-chart of how these vulnerabilities are intertwined together to finally get a reverse shell back to the attacker.

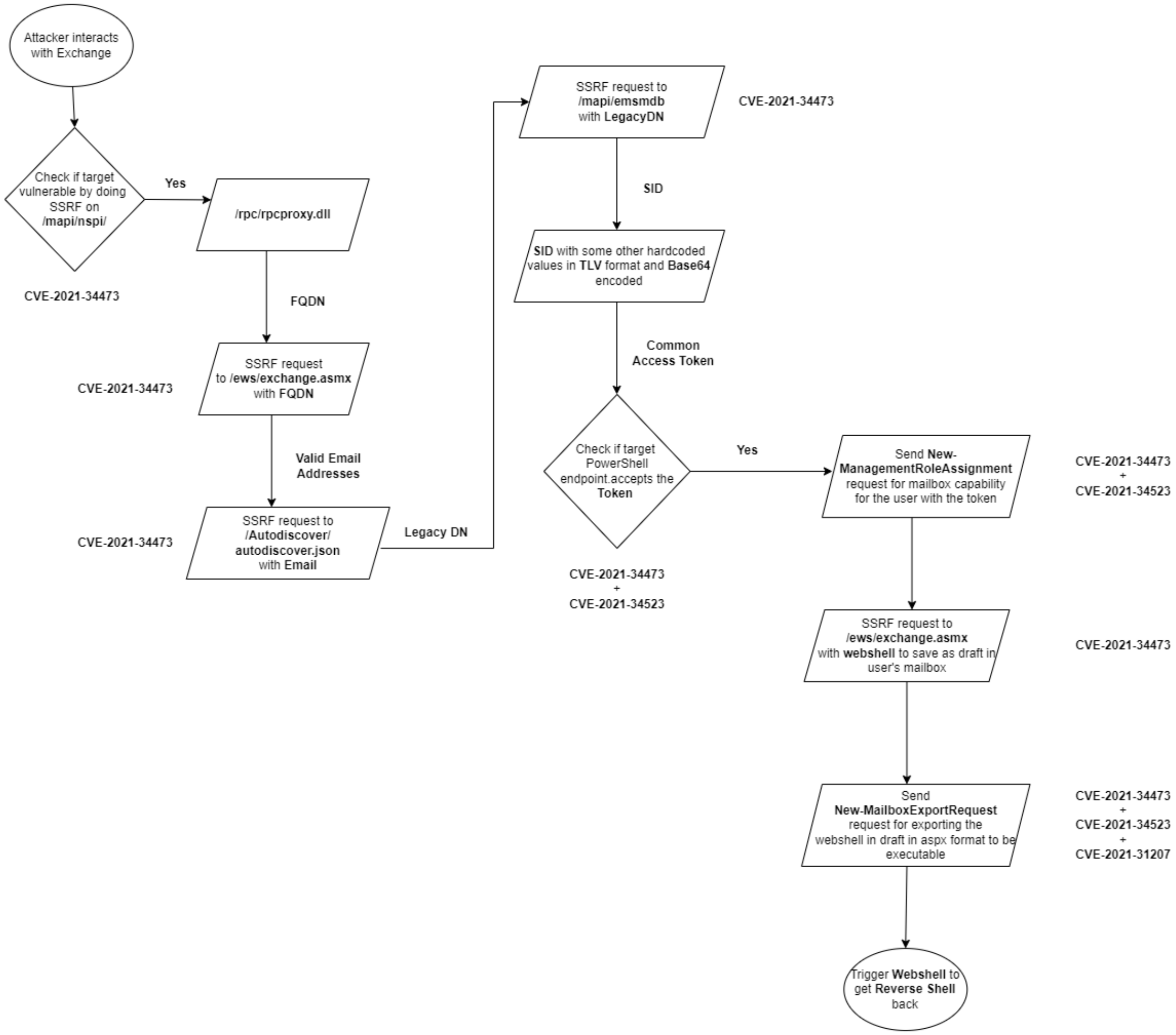

Attacker interacts with Exchange
Check if target vulnerable by doing SSRF on /mapi/nspi/
Yes
CVE-2021-34473
/rpc/rpcproxy.dll
FQDN
SSRF request to /ews/exchange.asmx with FQDN
CVE-2021-34473
Valid Email Addresses
SSRF request to /Autodiscover/ autodiscover.json with Email
CVE-2021-34473
Legacy DN
SSRF request to /mapi/emsmdb with LegacyDN
CVE-2021-34473
SID
SID with some other hardcoded values in TLV format and Base64 encoded
Common Access Token
Check if target PowerShell endpoint.accepts the Token
CVE-2021-34473 + CVE-2021-34523
Yes
Send New-ManagementRoleAssignment request for mailbox capability for the user with the token
CVE-2021-34473 + CVE-2021-34523
SSRF request to /ews/exchange.asmx with webshell to save as draft in user's mailbox
CVE-2021-34473
Send New-MailboxExportRequest request for exporting the webshell in draft in aspx format to be executable
CVE-2021-34473 + CVE-2021-34523 + CVE-2021-31207
Trigger Webshell to get Reverse Shell back

Figure 7. Reverse engineering flowchart example of a security exploit

To know more about the inner workings of this vulnerability please refer to an in-depth article which Keysight published in August 2022 — ProxyShell: Deep Dive into the Exchange Vulnerabilities.

ProxyLogon and HAFNIUM exploited vulnerabilities

The major components of this vulnerability include the following:

- CVE-2021-26855, also known as ProxyLogon, is a server-side request forgery (SSRF) vulnerability in Microsoft Exchange which allows the attacker to send arbitrary HTTP requests and authenticate as the Exchange server.
- CVE-2021-26857, which is an insecure deserialization vulnerability in the Unified Messaging Service, can allow for executing remote code as a SYSTEM User. However, this vulnerability requires administrative privileges.

- CVE-2021-26858 and CVE-2021-27065 are post authentication file write vulnerabilities which allow the attackers to write arbitrary files, in turn allowing them to drop web shells to get control of the server.

CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065 are all post authentication vulnerabilities that utilize the ProxyLogon vulnerability to authenticate first. The ProxyLogon vulnerability has been discussed in our blog — A look at the ProxyLogon Microsoft Exchange vulnerability (CVE-2021-26855).

Networking related vulnerabilities

Another set of common 2022 vulnerabilities affect network vulnerabilities. Here are three popular exploits:

- Pulse Secure VPN
- Citrix ADC
- Fortinet FortiOS vulnerability

Pulse Secure VPN

Amongst the virtual private network (VPN) vulnerabilities that were exploited in 2022, Pulse Secure SSL VPN Information Disclosure (or CVE-2019-11510) remained popular with various threat actors. The mass exploitation of this CVE in 2020 resulted in CISA releasing two separate alerts AA20-010A and AA20-107A to highlight this vulnerability.

In 2022, this CVE saw continuous exploitation by threat actors including the Peoples Republic of China State-Sponsored Cyber Actors (Alert AA22-279A) and Russian State-Sponsored Cyber Actors (Alert AA22-011A).

Citrix ADC

The Citrix Application Delivery Controlled Directory Traversal vulnerability which is tracked with CVE-2019-19781. The mass exploitation of this CVE in 2020 resulted in CISA releasing two separate alerts AA20-031A to detect the exploitation of this vulnerability and AA20-020A just for highlighting and helping in mitigating this vulnerability.

In 2022, this CVE saw continuous exploitation by threat actors, including Peoples Republic of China State-Sponsored Cyber Actors (Alert AA22-158A) and Russian State-Sponsored Cyber Actors (Alert AA22-011A).

The Keysight honeypots confirm exploitation attempts against this CVE in both 2021 and 2022. As Figure 8 shows, there was constant activity all year long with a burst for CVE 2019-19781 from February to May of 2021.

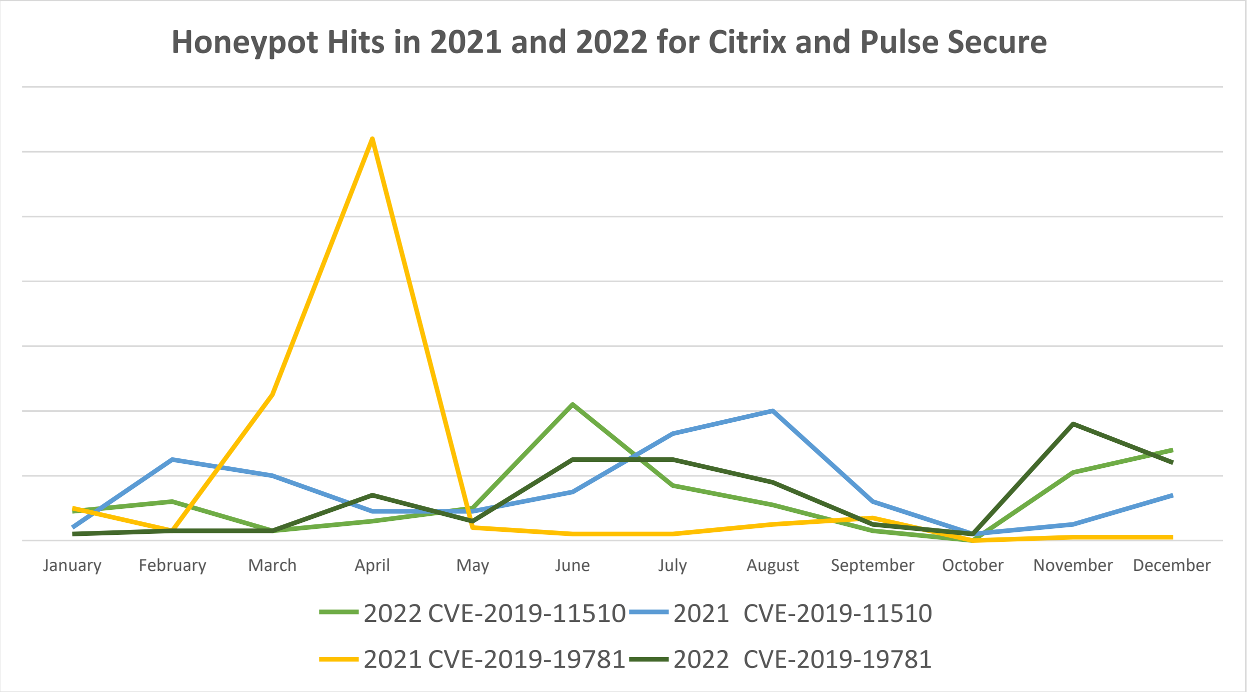


Figure 8. Citrix and Pulse Secure honey pot hits plotted versus time

Fortinet FortiOS Vulnerability

CVE-2018-13379 is a critical vulnerability in Fortinet FortiOS that was first disclosed in 2019. The mass exploitation of this CVE in 2020 resulted in the CISA releasing five separate alerts. including AA20-133A mentioning the top 10 routinely exploited vulnerabilities in May 2020.

In 2022, this CVE saw continuous exploitation by threat actors including Peoples Republic of China State-Sponsored Cyber Actors (Alert AA22-196A) and it was also mentioned in Alert AA22-225A, which talks about the top routinely exploited vulnerabilities.

The Keysight honeypot saw continuous exploitation of this vulnerability throughout 2021 and 2022. However, as we can see from Figure 9, the exploitation of this vulnerability increased from July of 2022 onwards.

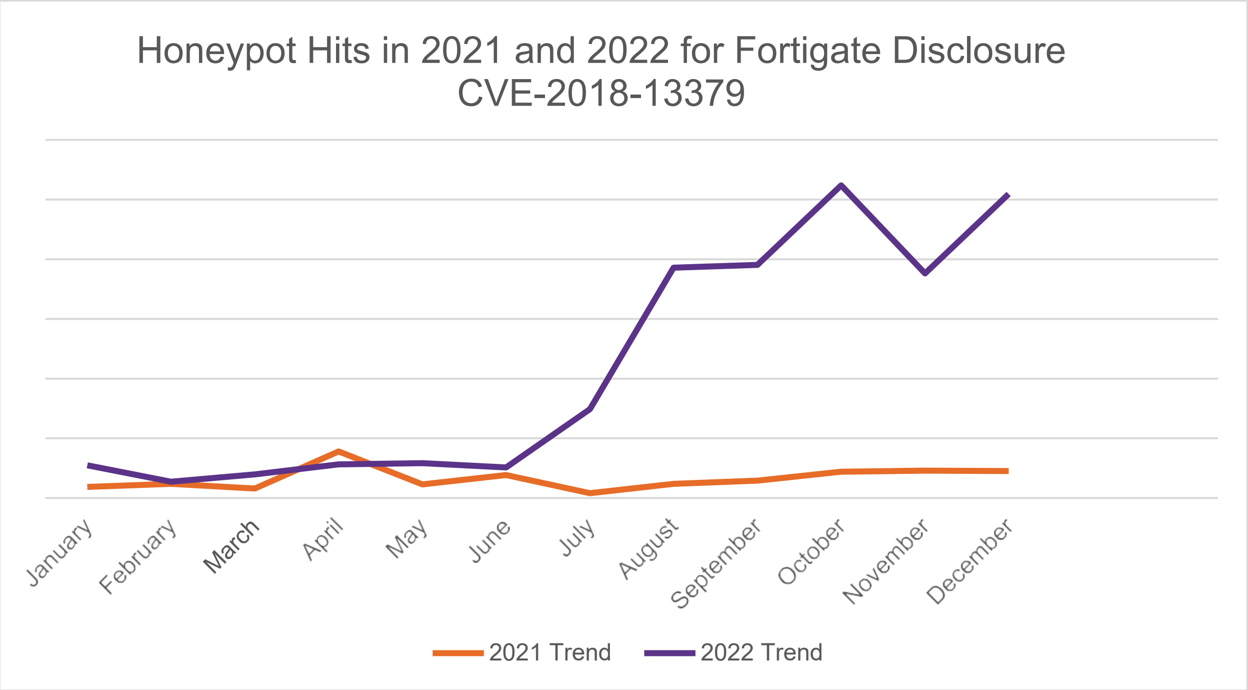


Figure 9. FortiGate CVE-2018-13379 honeypot hits plotted versus time

Key takeaways

There are three key takeaways regarding CVEs and CISA alerts. CVEs from 2021 were mentioned most in the CISA alerts from 2022. This was followed by CVEs from 2019, 2022 and 2020 in that order. We also see that vulnerabilities from 2017 and 2018 are still being mentioned in these alerts, signaling that those vulnerabilities are still being actively exploited.

A second key takeaway is that while threat actors use the latest vulnerabilities, they still rely on old major vulnerabilities. One example is Log4J. Even though it was announced in 2021, Log4J still remained the most popular vulnerability amongst attackers in 2022.

A third takeaway is that the sheer number of CVEs generated in 2022 was only 1/3 of the number in 2021. In looking at Figure 10 though, the real issue is that the numbers of CVEs generated in 2021 and referenced in CISA alerts was an excessive amount (48%). The year 2022 had 15% of the total used CVEs and 2020 had about 12%.

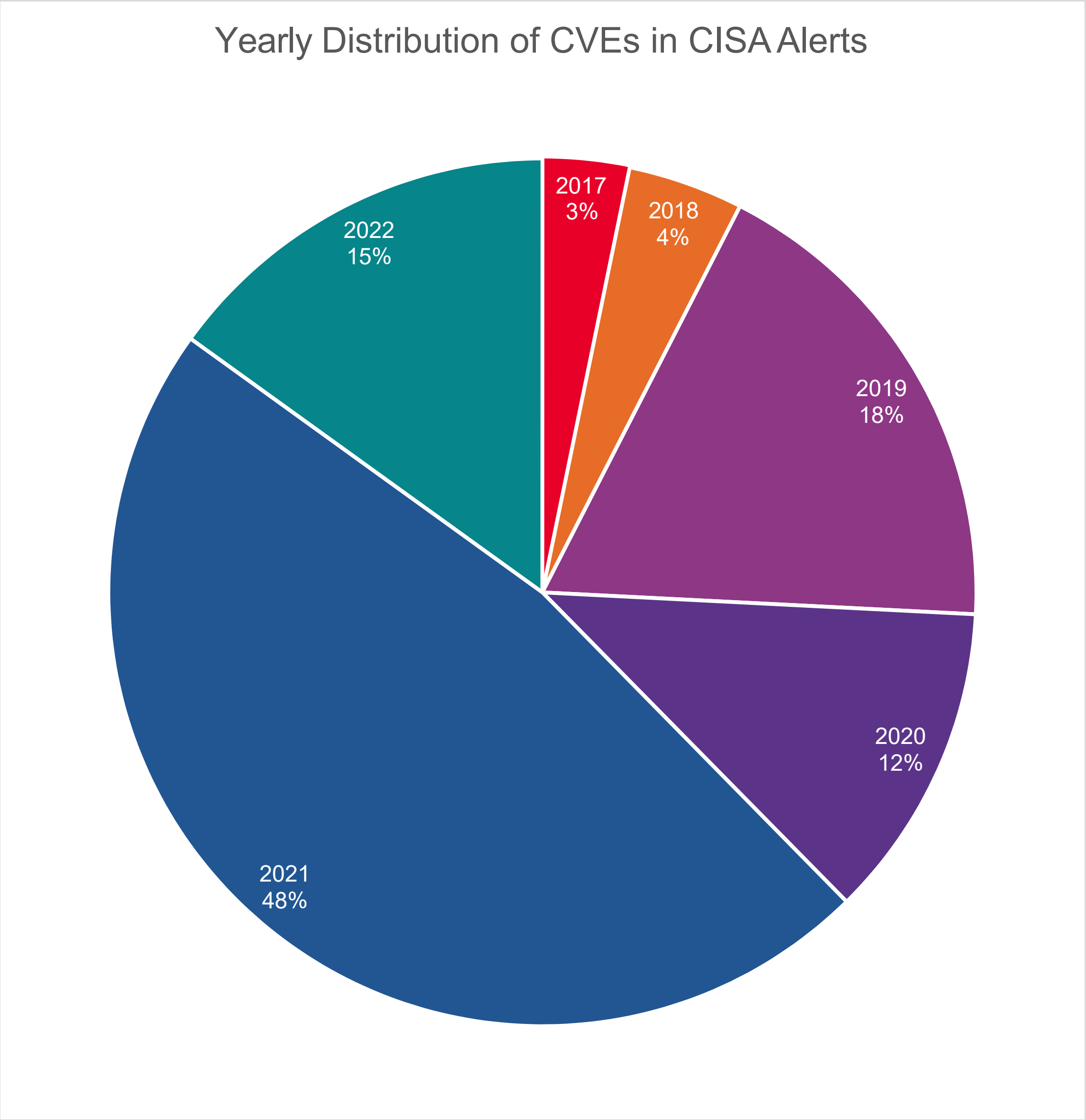


Figure 10. Distribution of CISA alerts per year

Android Malware with Focus on Polymorphism

Smartphones have become an indispensable part of our daily lives and are now commonly used to store a wealth of sensitive personal information. This includes financial data, confidential documents, and login credentials. Android, with 2.8 billion active users (global market share of 75 percent), is undeniably the most popular OS for smartphones. This has made Android smartphones a high value, lucrative target for threat actors. A multitude of new variants of android malware pop up every day. As we can see from Figure 11 below, during the months of November through December of 2022 there were around 3.2 million Android APK malware attacks submitted to the virus total count, making it the 5th popular malware file type. Many of these attacks make it to the app store. Given the ineffectiveness of mobile security solutions, it’s high time that we focus on Android malware.

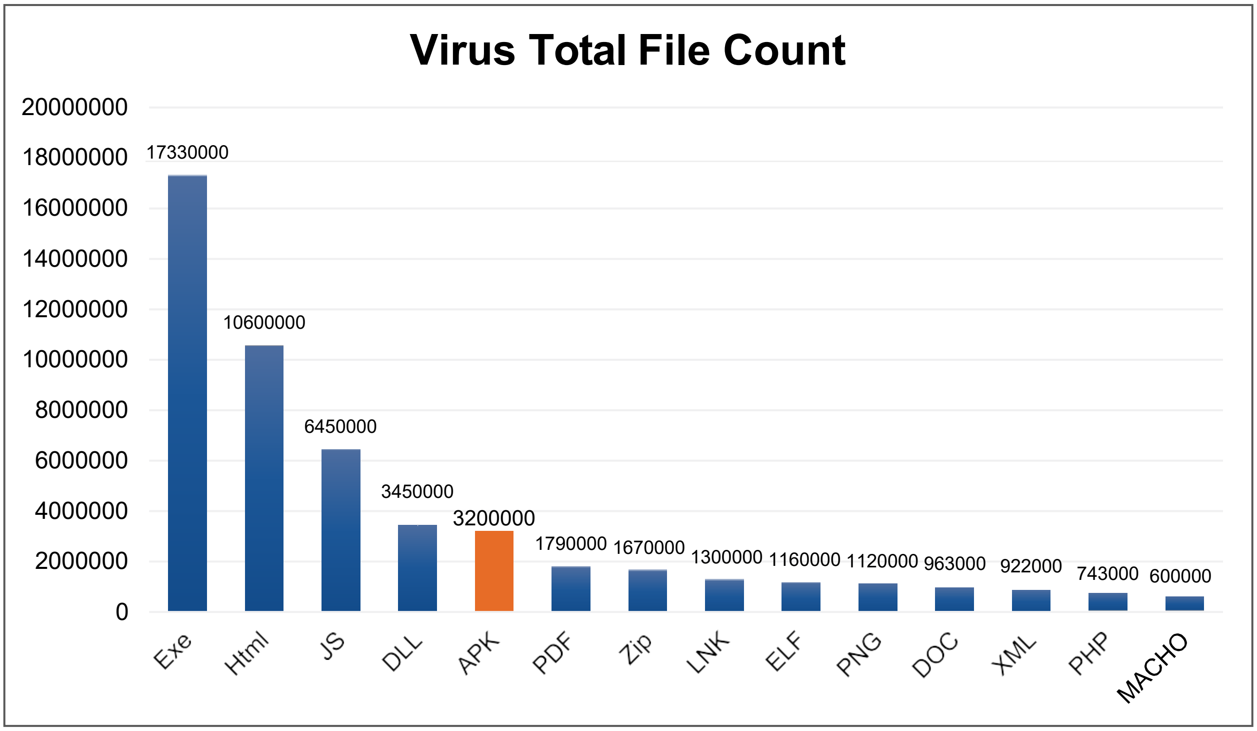


Figure 11. Total virus file types submitted from Nov-Dec 2022

Android malware highlights for 2022

In early 2022, **Pegasus** made some news after it successfully used zero-click exploits to infect the phones of Finnish officials. However, the officials stated that the information communicated via mobile devices was not highly sensitive.[10]

In addition, new spyware (**Hermit)** was detected. The spyware is similar to Pegasus. It is an advanced malware variant that has been used on victims in Kazakhstan, Syria, and Italy, and is known to spread through smishing tactics.[11]

[10] https://threatpost.com/nso-group-pegasus-spyware-finnish-diplomats/178113/
[11] https://techcrunch.com/2022/06/17/hermit-spyware-government/

Another malware highlight was **Flubot**, which the international law enforcement agencies from multiple countries were able to take down. It was the fastest growing Android malware and is known to steal sensitive financial credentials and spread rapidly by sending phishing messages (smishing) to the victim's contacts.[12]

Banking trojans were widespread in 2022, with various families targeting different countries. For instance, MaliBot targeted Spain and Italy. It is believed to be filling the market gap left by the takedown of Flubot. Drinik (which masquerades as an official tax management tool) and the malware Sova primarily targeted India. In addition, Godfather (a variant of Anubis) was used to target 400 online banking sites and cryptocurrency exchanges.

As research continued, we found Hiddad and other android malware were found to be present on Play Store with millions of downloads.

Polymorphic Android malware

Whenever we examined new Android malware variants, we observed that there were multiple hashes for a single type of malware. These are variations of the original malware that may have slight modifications, such as a new user interface in the foreground, but typically carry out the same harmful actions in the background as the original — see Figures 12 and 13. These variations are referred to as Polymorphic malware. For example, the Schoolyard Bully malware has over 150 different variations, as seen here.

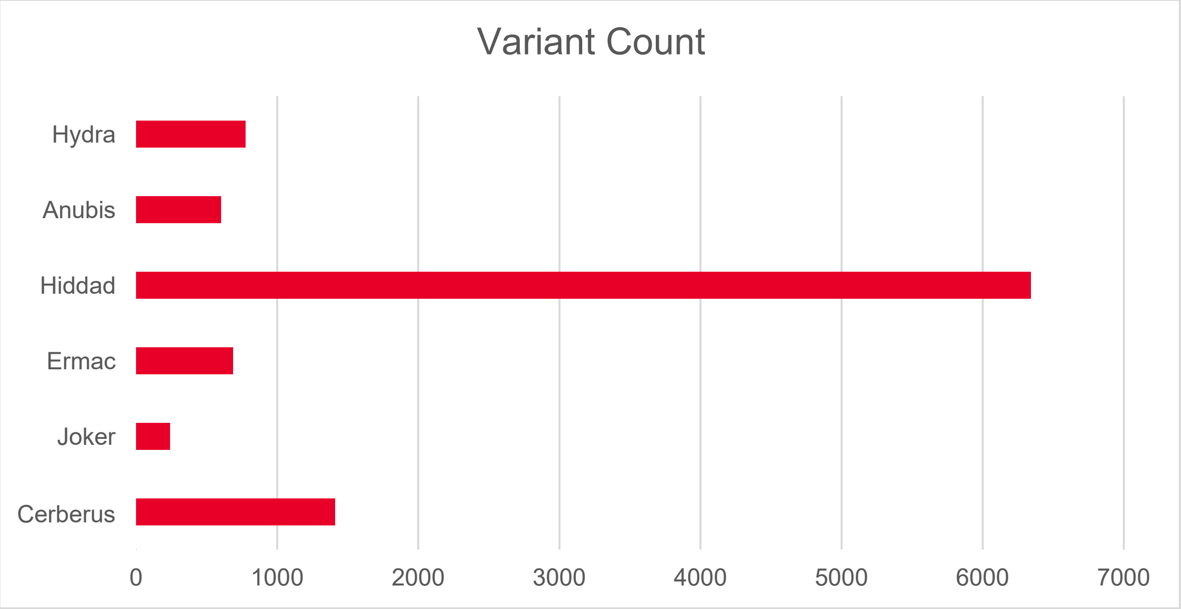


Figure 12. Virus total variants of Android malware families Nov-Dec 2022

[12] https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones

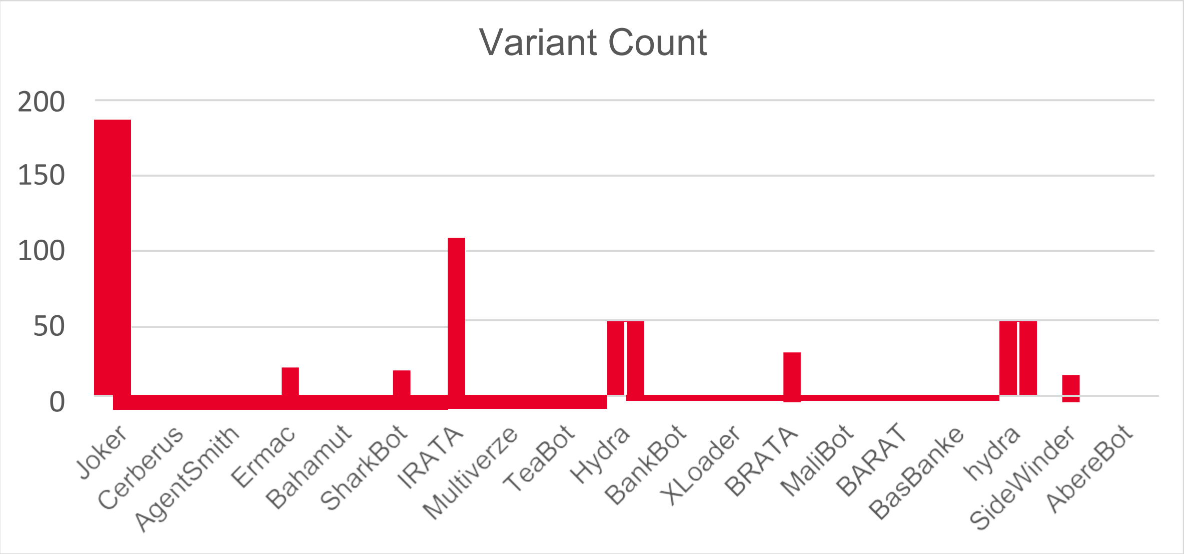
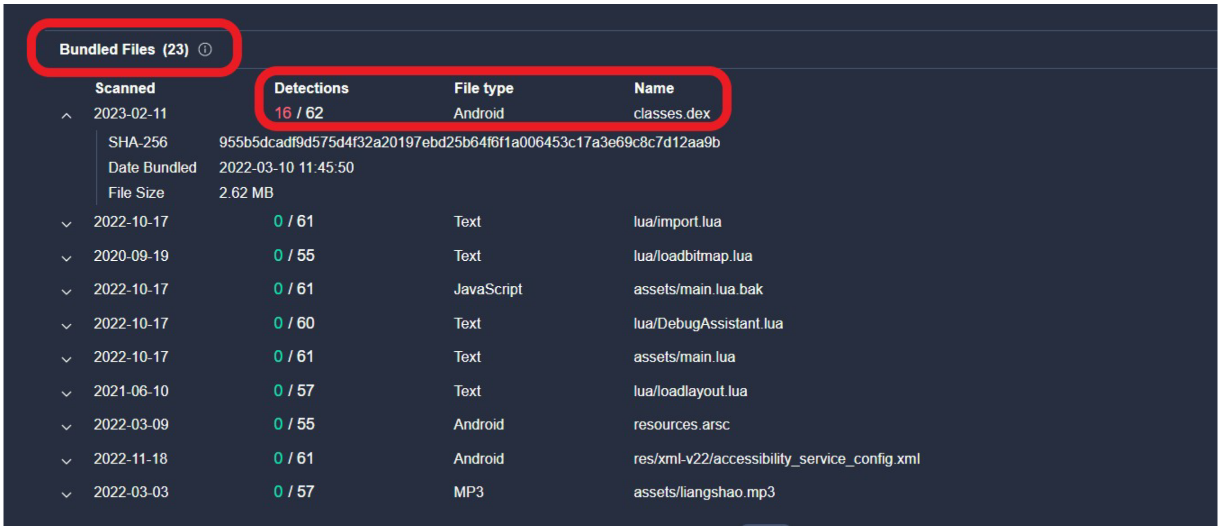


Figure 13. MalwareBazaar variants of Android Malware families Jan-Dec 2022

The charts shown above provide the variant counts in VirusTotal and MalwareBazaar, which have been correctly identified as polymorphic versions of a particular family. It is suspected that there are plenty of others that have not been categorized.

Cyber attackers work hard to create variations like these to evade various detection methods. Keysight analyzed the ease of bypassing these mechanisms and found it to be straightforward. Some security measures rely on simple static analysis methods, such as comparing the hash of the entire file, which can easily be circumvented by decompiling and recompiling the APK file which gives a new hash every time. Some solutions may be slightly more advanced, using techniques like unzipping the Android APK and checking the hash of the classes.dex file (as shown in Figure 14 below), which holds the compiled logic of an Android APP in Dalvik Executable format. However, even this method can be bypassed by simply adding some redundant code to the source.



Bundled Files (23)

Scanned	Detections	File type	Name
2023-02-11	16 / 62	Android	classes.dex
SHA-256	955b5dcadf9d575d4f32a20197ebd25b64f6f1a006453c17a3e69c8c7d12aa9b		
Date Bundled	2022-03-10 11:45:50		
File Size	2.62 MB		
2022-10-17	0 / 61	Text	lua/import.lua
2020-09-19	0 / 55	Text	lua/loadbitmap.lua
2022-10-17	0 / 61	JavaScript	assets/main.lua.bak
2022-10-17	0 / 60	Text	lua/DebugAssistant.lua
2022-10-17	0 / 61	Text	assets/main.lua
2021-06-10	0 / 57	Text	lua/loadlayout.lua
2022-03-09	0 / 55	Android	resources.arsc
2022-11-18	0 / 61	Android	res/xml-v22/accessibility_service_config.xml
2022-03-03	0 / 57	MP3	assets/liangshao.mp3

Figure 14. Security measure example

Key takeaways

There are two clear takeaways in this area. First, new Android malware variants appear every day. So, it is important to exercise caution when downloading apps, whether from unknown sources or even the official App Store. Also avoid clicking on unknown links as they can be attempts of smishing attacks.

Second, security vendors should avoid relying solely on static analysis methods, such as hash databases, and instead incorporate dynamic analysis in their approach. Keysight has recently started to create polymorphic Android malware, which can be used to test the resilience of security solutions against new variants. More information can be found in this blog post.

Top Vulnerabilities Disclosed in 2022

In this section, we will be looking at top vulnerabilities that had been disclosed in the year 2022, i.e. CVEs which have the CVE ID beginning with 2022 and were exploited in the wild. We will be referring to the CISA KEV catalog which contains vulnerabilities that have been seen in the wild and used as a frequent attack vector by malicious cyber actors. The present catalog can be found at here.

At Keysight, we also have a network of honeypots deployed to catch and monitor various cyber threats. Our honeypot data helps to paint a picture about the exploitation trends for vulnerabilities that we have seen and can tell us if, and when, an attacker tried to probe for certain vulnerabilities.

In 2022, CISA made its first entry to the KEV catalog on January 10, 2022 and its final entry on December 29. During this period, they added 557 new entries of which 93 had a CVE identification beginning with 2022. This is illustrated in Figure 15.

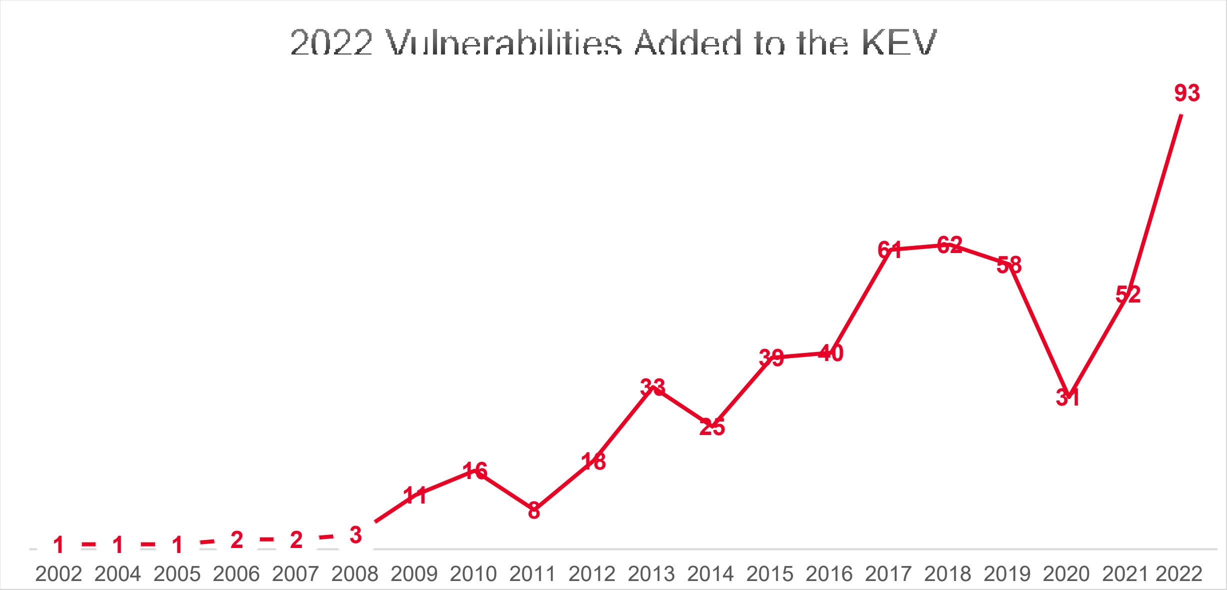


Figure 15. Number of vulnerabilities added to the KEV over time

In the following sections, we will be reviewing the top vulnerabilities that were disclosed in 2022. The vulnerabilities are categorized according to their attack surface.

Microsoft products

CVE-2022-30190 aka Follina

Follina is a remote code execution vulnerability in the Microsoft Support Diagnostic Tool (MSDT). It is caused when MSDT is called using the URL protocol. The vulnerability is due to the MSDT tool executing arbitrary code. A remote unauthenticated attacker can trick the victim into downloading a malicious HTML file served up by the attacker which might execute arbitrary code on the victim's machine. This vulnerability can also be exploited by invoking any web request command in PowerShell.

At the time of writing, this CVE has been associated with 28 malware families including Remcos, Redline Stealer, Snake, Emotet as well as nine threat actors including Turla, APT28, APT15, and TA570. This vulnerability was also part of the 2022 0day "In the wild" Exploit report from Google's Project Zero. CVE-2022-30190 is the top high-profile vulnerability of 2022. It was added to the KEV catalog on June 14, 2022.

To provide a better coverage for this vulnerability, Keysight released a strike and we have also provided a campaign around this vulnerability with the Follina Turian June 2022 campaign.

CVE-2022-41082 / CVE-2022-41040 aka ProxyNotShell

These vulnerabilities were commonly dubbed as "ProxyNotShell" which were 0-day vulnerabilities in Microsoft Exchange Server. CVE-2022-41040 is a server-side request forgery (SSRF) vulnerability which allows an authenticated attacker to trigger CVE-2022-41082. This CVE allows for remote code execution when the Exchange PowerShell is accessible. These CVEs were added to the KEV on September 30 and have been linked to multiple malware families including LockBit and others.

Java Web applications

CVE-2022-22965 aka Spring4Shell

Spring4Shell is a remote code execution vulnerability in Spring Cloud Foundation. The vulnerability is due to inadequate validation of parameters used for data binding, allowing for manipulation of the ClassLoader. A remote attacker could exploit this vulnerability by providing a crafted parameter in an HTTP request. Successful exploitation could lead to ClassLoader manipulation, which may lead to execution of arbitrary code under the security context of the container of the target application.

This CVE has been associated with Mirai and ZeroBot malware families and was added to the KEV catalog on April 4. To provide better coverage for this vulnerability, Keysight released a strike which exploits this vulnerability, and which also works in a one-arm mode against a real server. This vulnerability was disclosed March 31, 2022 and our honeypots saw active exploitation attempts against this CVE from April onwards.

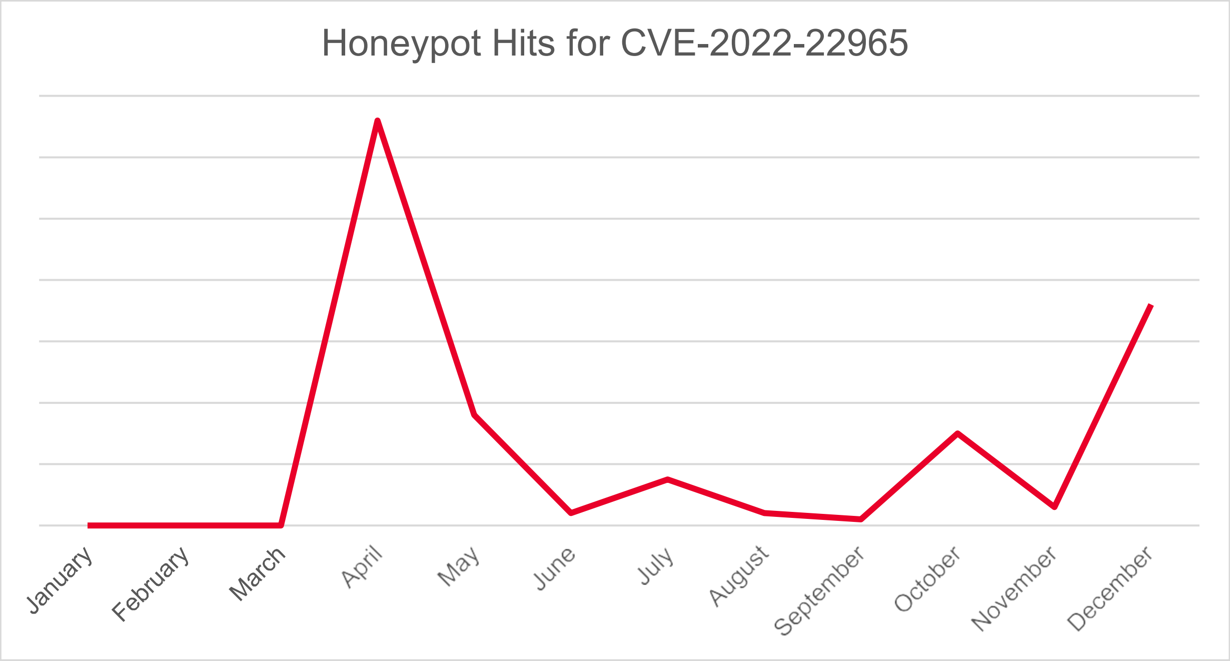


Figure 16. Honeypot hits for CVE-2022-22965 during 2022

CVE-2022-26134 - Atlassian Confluence OGNL Injection

CVE-2022-26134 is an ONGL injection vulnerability in the Atlassian Confluence Server and Data Center. The vulnerability is due to improper validation of the URL in an HTTP request. A successful attack may result in arbitrary code execution in the security context of the server process.

This CVE has been associated with 17 known malware families and frameworks including: Mirai, Cobalt Strike, Cerber, Kinsing, Monero Miner, etc. and has been linked to threat actors including Hezb and BRONZE STARLIGHT. This CVE was added to the KEV catalog on June 2, 2022 — on the same day Atlassian shared a security advisory detailing about this vulnerability. As Figure 17 shows, Keysight honeypots saw active exploitation attempts against this CVE from July onwards.

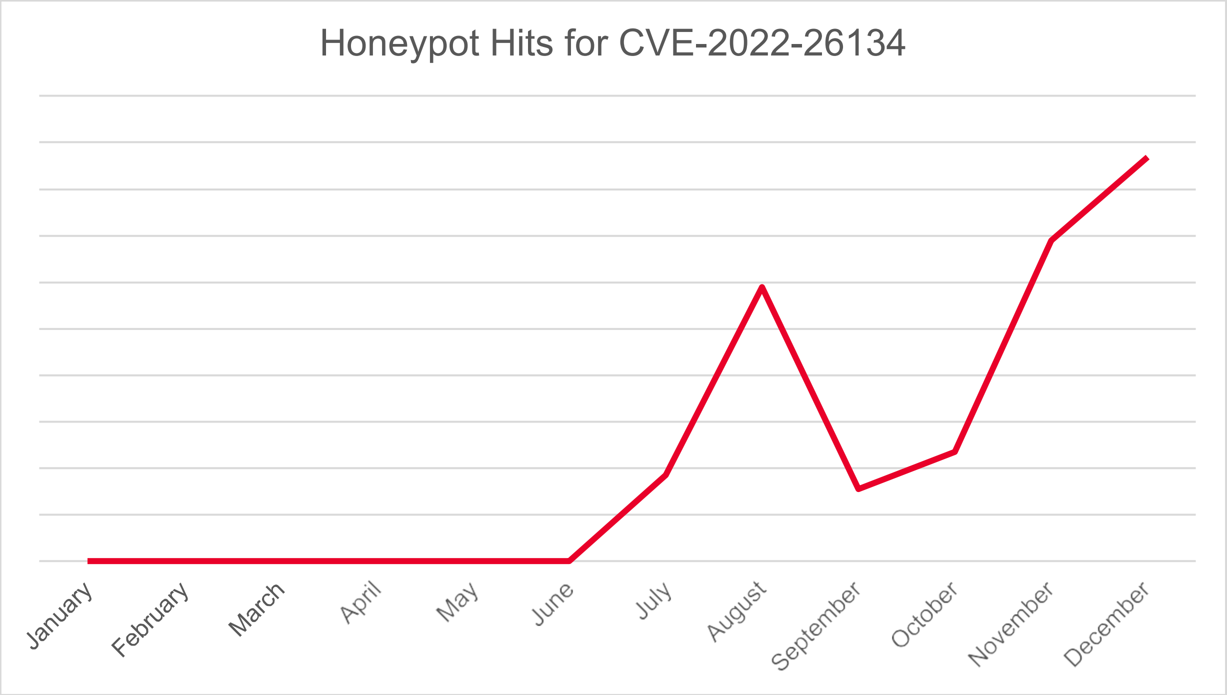


Figure 17. Honeypot hits for CVE-2022-26134 during 2022

Network security solutions

The following list of vulnerabilities relates to network and equipment-based CVEs discovered in 2022.

CVE-2022-1388 F5 BIG-IP RCE

CVE-2022-1388 is an authentication bypass vulnerability in the F5 BIG-IP product. The vulnerability is due to improper handling of requests sent to the management port. A remote, unauthenticated attacker could exploit this by sending a maliciously crafted request to the management port. A successful attack may result in remote code execution in the security context of ROOT.

This CVE was added to the KEV catalog on May 10, 2022 and has been associated with Kaiji, EnemyBot, and Chaos malware families. To provide better coverage for this vulnerability, Keysight released a strike which exploits this vulnerability and also works in a one-arm mode against a real server.

CVE-2022-40684 Fortinet Authentication Bypass

CVE-2022-40684 is an authentication bypass vulnerability in multiple Fortinet products, including FortiOS, Forti Proxy, and FortiSwitchManager. The vulnerability is due to errors in handling certain HTTP headers within user requests. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target server. A successful exploitation could result in an attacker bypassing authentication and executing commands as an admin user on the target system.

This CVE was added to the KEV catalog on October 11 and has been associated with the OilRig threat actor. To provide a better coverage for this vulnerability, Keysight released a strike which exploits this vulnerability. Our honeypots saw active exploitation attempts against this CVE from December of 2022 and onwards.

CVE-2022-30525 Zyxel Firewall CGI Command Injection

CVE-2022-30525 is a command injection vulnerability within the Zyxel firewall product. The vulnerability is due to improper input validation in the CGI component. A remote, unauthenticated attacker could exploit this by sending a maliciously crafted request to the CGI component. A successful attack could result in remote code execution in the security context of the Unix persona ”nobody user.”

This CVE was added to the KEV catalog on May 16, 2022 and has been associated with Chaos and ZeroBot malware. To provide a better coverage for this vulnerability, Keysight released a strike which exploits this vulnerability. Our honeypots saw active exploitation attempts against this CVE from July 2022 and onwards.

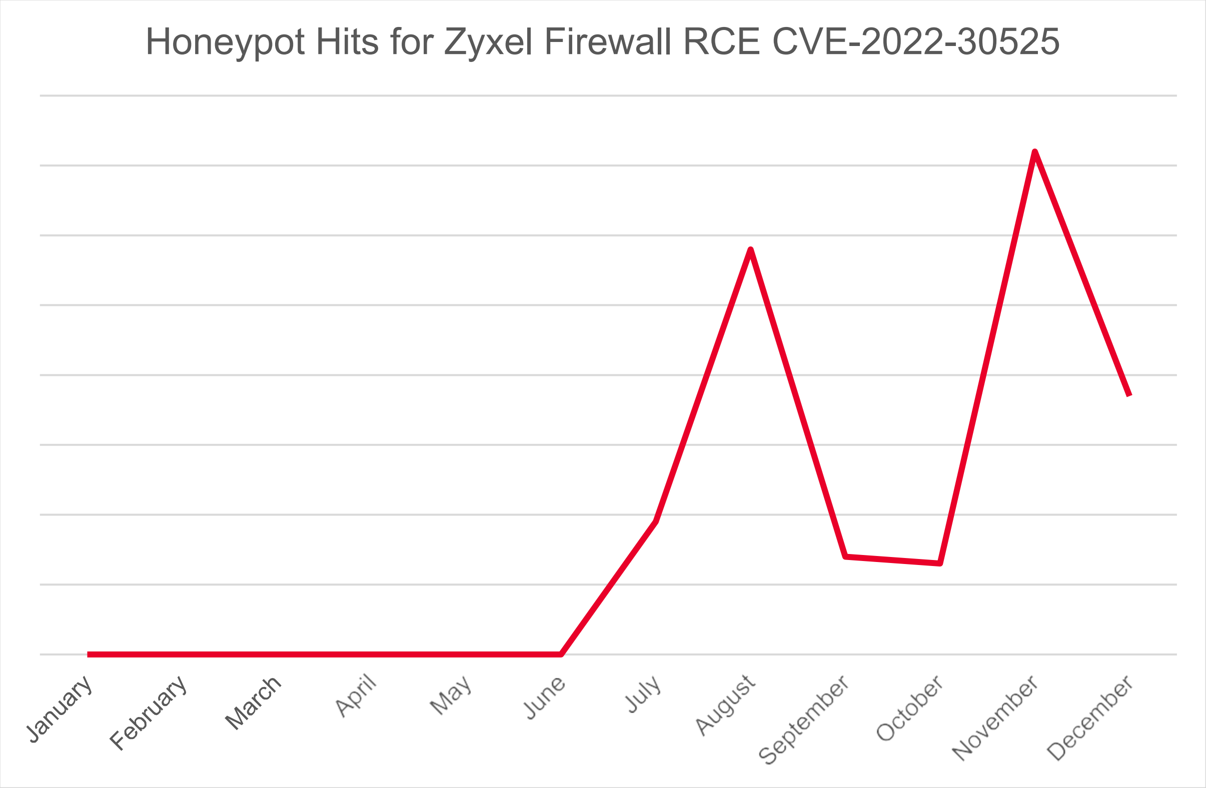


Figure 18. Honeypot hits for CVE-2022-30525 during 2022

Web browsers

The following list of vulnerabilities relates to Internet browser-based CVEs discovered in 2022.

CVE-2022-0609 UAF in Google Chrome

CVE-2022-0609 is a Use-After-Free (UAF) vulnerability within animation in the Google Chrome browser. This vulnerability allows a remote attacker to potentially exploit heap corruption via a crafted HTML page.

This CVE was added to the KEV catalog on February 15 and has been associated with AppleJeus malware in both Microsoft Windows and Apple Mac® focused malware families and was also actively exploited by the Lazarus Group.

Key takeaways

Going forward in 2023, the vulnerabilities disclosed in 2022 could be the ones that threat actors will exploit the most. This was the case from CISA data that shows that the top vulnerabilities from 2021 were the ones most exploited in 2022. Hence, it becomes critical that we are well protected against these vulnerabilities.

We also see a trend in the vendors that were added to the CISA KEV catalog in 2022. Approximately 43% of CVEs affected Microsoft products, followed by 14% targeted at Adobe, and then 13% targeted at Cisco. See Figure 19.

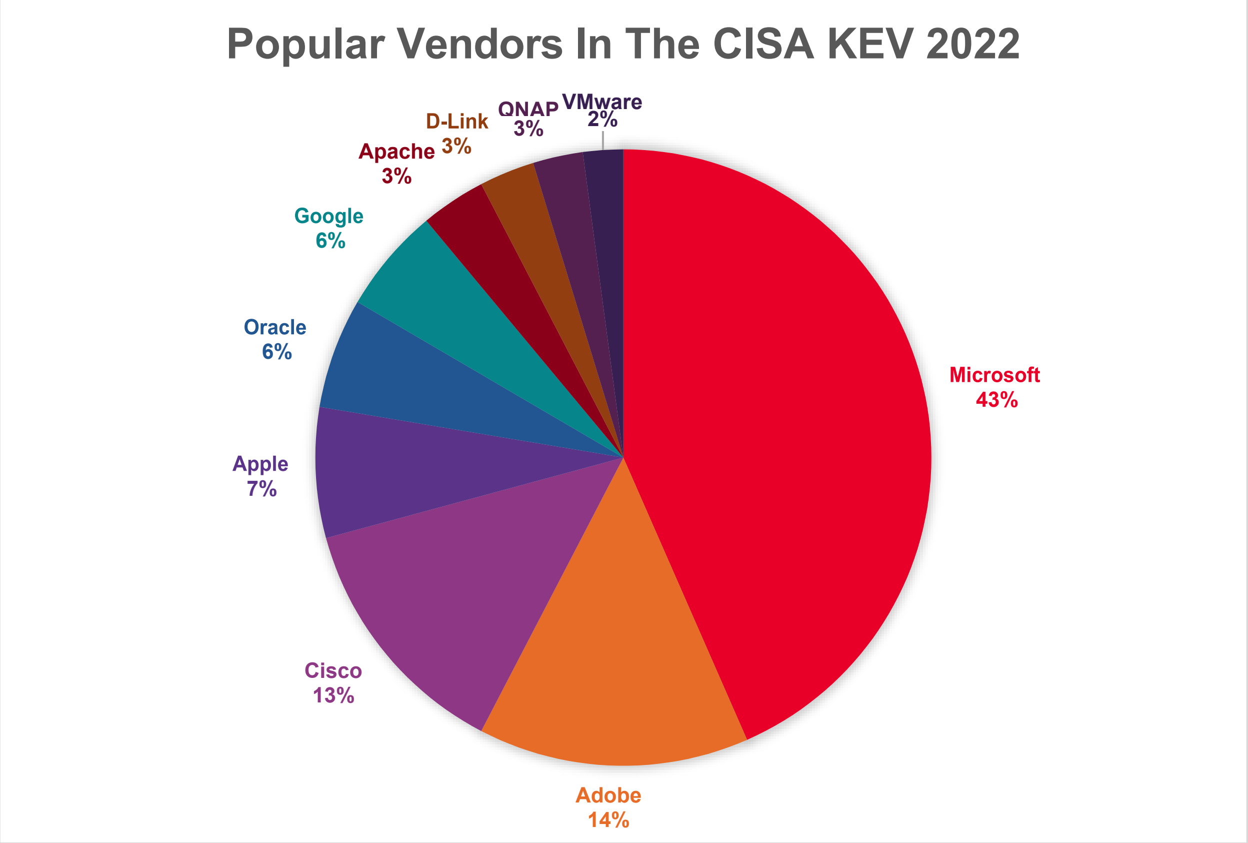


Figure 19. Vendors added to the CISA KEV catalog in 2022

Even older vulnerabilities from 2002, 2004, 2006 and 2009 were added to the catalog. Here are the CVEs that were added:

- CVE-2009-3129
- CVE-2009-1123
- CVE-2004-0210
- CVE-2002-0367
- CVE-2009-0563
- CVE-2009-0557
- CVE-2006-2492

All of these vulnerabilities affect Microsoft products, mainly Office® and Windows products.

Keysight's View of 2023 Threats

We expect that there will be three main target areas in 2023:

- Ransomware
- Internet of Things (IoT)
- Artificial Intelligence (AI)

Ransomware will continue its dirty work

Ransomware attack vectors will continue to be the most impactful security threat of the year for most enterprises. Threat actors have succeeded with successful deployments and monetizing the attacks.

The LockBit 3.0 builder was leaked on Twitter September 21, 2022 (although a copy of the builder was available as early as the beginning of September) for would-be attackers to play with and weaponize. This provided an excellent opportunity for malicious actors to leverage their ransomware easier than ever.

The leak correlates with Keysight's honeypot observation of a ransomware spike in September 2022, as shown in Figure 20 below.

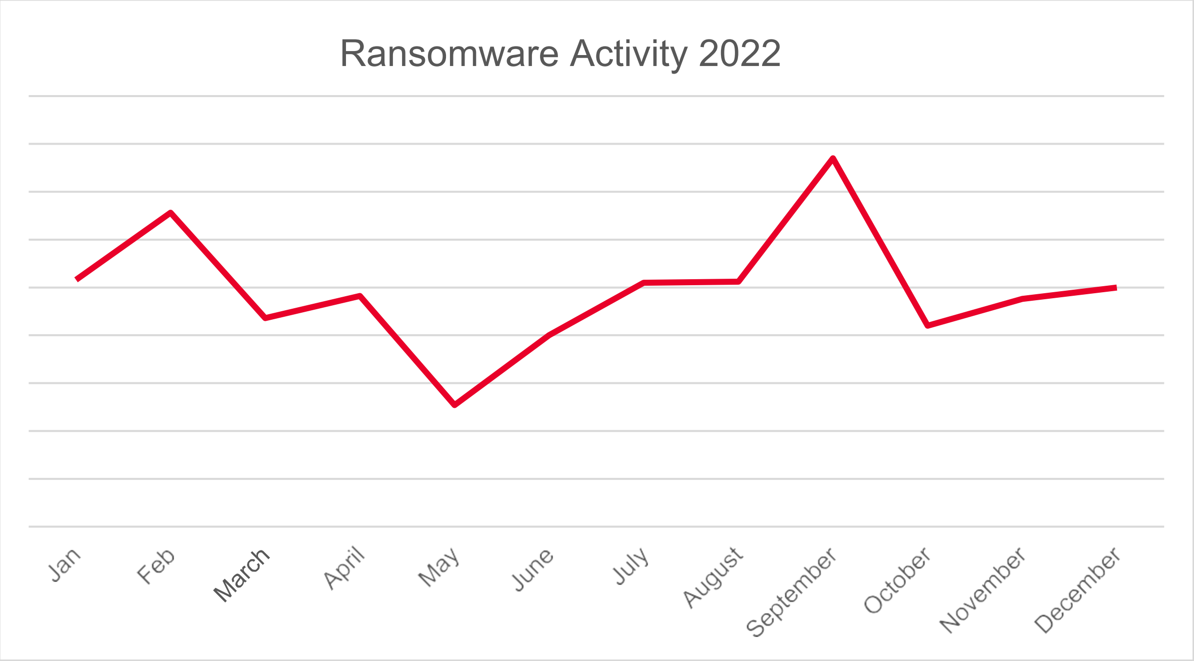


Figure 20. Ransomware activity across 2022

For 2023, we are predicting steady ransomware activity, but not necessarily tied to big groups. However, the leak of multiple ransomware builders and red-teaming tools (such as Brute Ratel and CobaltStrike in the past) will help threat actors to leverage new families of malware and campaigns.[13]

Additionally, we expect to see an increase in ransomware attacks targeting enterprise virtualization servers and data centers.

IoT security continues to be a challenge

IoT security has been a problem for several years. This will intensify over the next couple years as the immature Matter protocol is deployed. Matter is the new standard to interconnect IoT-enabled devices. The rise of this new protocol includes risks and a new opportunity for threats from attackers.

Indeed, based on our 20 years of experience in network protocol and security testing, Keysight predicts that Matter adoption will be an opportunity for new security breaches against common and sensitive assets. Replacing many protocols (Zigbee, Z-wave, etc.) with a unique new and less mature standard implementation will make room for new and unknown-vulnerabilities.

The fundamental areas of attack will be:

- denial of service (performance or vulnerability)
- compromise (vulnerability)
- espionage and data leak

It will take Matter a few, potentially painful, years to harden. During this time expect various threats and check for new CVEs that address the vulnerabilities.

The Dark Knight rises – artificial intelligence bots will increase malicious activity

OpenAI's ChatGPT and other AIs will be a challenge for security operators. At the end of 2022, ChatGPT generated much noise with its capability to write content like a human. Malicious actors already embrace this platform to enhance phishing attacks and multiply their realism through different languages. ChatGPT can even be used by novices, or script kiddies, for malicious purposes.

Since AI/ML is a very active and competitive market, the race is on to demonstrate capabilities. This competition will likely allow attackers to rely on these tools to enhance threat sophistication and evade current security controls. As an example, current phishing mitigation rules should be considered as deprecated, and the rule to check misspellings and lousy sentence structure to identify phishing attempts will be less effective due to tools like ChatGPT.

[13] Lawrence Abrams, LockBit ransomware goes 'Green,' uses new Conti-based encryptor, Bleeping Computer, February 1, 2023.

Conclusion

This report concludes with the following key takeaways:

1. Ransomware will be a constant threat that must be addressed ahead of time by IT security departments

2. AI is being weaponized by bad actors to improve their various threat vectors

3. You cannot defend against what you cannot see – you must deploy network visibility and breach and attack simulation technology

Ransomware security attack successes are an indicator of a weakness in most enterprise security architectures — along with the fact that humans (users through email phishing attacks) continue to be a weak link in the security chain. The first key conclusion from this report is that since ransomware will be a constant threat, IT security departments must address the threat ahead of time. This means having a prepared protocol ahead of time that describes how security engineers will need to react to a suspected ransomware threat.

For instance, are data backups being created? If so, how often? In addition, where are backups being stored so that a bad actor can't get to them? When should security engineers restore data to the network from those backups? Should a backup of the network be created of the infected, or suspicious, current network configuration and what are the handling procedures for that specific backup? These data storage concerns need to be documented and addressed long before an attack is recognized.

The general IT security response plan should also be validated and/or updated to specifically address ransomware issues. For instance, how should a potential attack be handled and mitigated? Here are a few example issues to address:

- Should the network be immediately shut down and who is authorized to make this type of decision?
- What isolation techniques can be deployed?
- How should ecommerce transactions and records be handled?
- How often should the network be investigated for a potential ransomware attack, i.e. how often should specific breach and attack (BAS) and threat hunting activities be performed?
- If there is a standby network available (either active load sharing, active / standby, or cold standby), when should this be engaged to isolate the security threat but still preserve business continuity?

A second conclusion is that since artificial intelligence is being weaponized by bad actors to improve their various threat vectors, you need to start preparing for this threat now. AI will probably be used to create autonomous attacks, especially when combined with the compute power of cloud computing networks.

In addition, AI lowers the skill level required for a would-be cybercriminal. Instead of engaging in proof of concepts (POC) to gain knowledge about systems, they can build malware attack scripts much easier using ChatGPT or some other AI system. These attacks will be created that are based on the cyber kill chain model; with each step being automated. Different evasions can also be created by AI solutions to create multiple malware variants with little time or effort required. This will make it much harder to stop an attacker.

In addition, AI will make it easier and faster to run spear phishing campaigns. The AI will be able to gather website and web link information that is tuned to individual people. This allows for better (more personalized) attacks designed to convince people to give up additional personal information and credentials.

At the same time, one benefit from AI is that the security engineer can use the technology as well to automate BAS solutions and (potentially) threat hunting solutions. This empowers the engineer with a force multiplier and enables them to constantly look for signs of lateral movements, C&C, etc.

The third conclusion is that since you cannot defend against what you cannot see, you need to deploy network visibility technology immediately to expose security threats. The first step is to accurately capture and validate potentially suspicious packet data. Flow data and log data can, and should, also be used in threat analysis. However, both of these data sources have challenges. For instance, flow data provides only group and general data observations. While log data has more detail than flow data, specific malware threats can delete or corrupt log data and files — allowing certain threats to slip by unnoticed.

Packet data, however, doesn't lie. It is a consistent source of truth and needs to be utilized as such, even though it requires more work. Taps and packet brokers allow you to collect the packet data across your network, filter it to capture just the data you need, and then pass that data on to one or more security tools for data analysis.

In addition, your network will need continuous breach and attack testing. Annual penetration testing and quarterly cyber range red team/ blue team testing aren't good enough anymore. Not to say those activities should be eliminated, but additional proactive testing with a BAS solution should be included as well.

Good luck with your efforts. If you need help, Keysight Technologies is always available.

About the ATI Research Center

The Keysight ATI Research Center is an elite group of dedicated network security professionals. Its purpose is to stay current with ever-evolving changes that could impact the security of IT networks. The team then distils that knowledge into research which can be incorporated within Keysight solutions to keep up with continually evolving threats.

The ATI team is distributed across the world in locations like Singapore, California, Texas, Massachusetts, France, Romania, and India so that there is always a part of the team that is looking for new threats to analyze.

The ATI team also contributes to the larger security community. It is not just about us. Our team also shares what we learn with vendors that have been hacked, private agencies (e.g. www.mitre.org), government agencies (e.g. NIST and DARPA), and global security conferences like Black Hat and RSA. Keysight also promotes a summer security school in Bucharest, Romania to help train new security engineers.

The key goal for the ATI team is to assess and validate products that are meant to secure the enterprise. We do this by serving as a front line of defense to keep products from other vendors honest. Security alerts and incidents happen all over the globe and the team needs to be up around the clock. Dozens of engineers combine to form a single team that creates the intelligence and adds it to all product lines. In many cases, this lets the team go from discovery to product output within a twenty-four-hour period.

The exact input comes from many sources including:

- International exploit databases
- The “Dark Web”
- Scan of security news alerts and crowdsourcing
- Twitter handles of other security researchers
- Partner feeds
- Honeypots actively looking for attacks in the wild
- And independent research (testing and reverse engineering) by the ATI team

The team constantly polls multiple sources to get insights into vulnerabilities. This data is then normalized, correlated, and organized to get a clear direction on the threats, and how to prioritize them. Threats are investigated by team members and either validated or dismissed. The team validates everything to make sure that the content deployed in our products is 100% sure and correct. This gives the team the utmost confidence in our data and predictions.

The ATI team was established in 2005 as part of the BreakingPoint company. BreakingPoint was acquired by Ixia in 2012 and then Ixia was acquired by Keysight Technologies in 2017. The BreakingPoint solution is a security attack and traffic generator used by network equipment manufacturers, service providers, governments, and enterprises, to validate network and security resiliency while under load and attacks. This threat intelligence information is incorporated into Keysight security solutions.

The threat intelligence feed from the ATI team is unique. They set an incredibly high bar for threat intelligence so that customers can completely trust it. While others in the industry create automated intelligence platforms or open-source feeds, those solutions are not validated as thoroughly for accuracy as the Keysight solution. As an example, other intelligence information feeds can end up being focused on a specialized attack on a particular product (e.g. Cisco or Microsoft) instead of being related to the global picture of what is happening on the Internet.

Keysight is committed to making it as hard as possible for hackers to succeed.

Learn more at Keysight.com and getnetworkvisibility.com.

Appendix A – MITRE ATT&CK Review

As a review, we would like to have a short discussion related to two techniques that we would like to revisit:

- T1059: Command and Scripting Interpreter
  - From a defence point of view, blocking PowerShell (T1059.001), Windows Cmd (T1059.003), or JavaScript (T1059.007) is not as easy or straightforward. In many cases, you won't be allowed to disable or block them as they provide legitimate functionality for system administrators for troubleshooting and even forensic activities.
  - From the attack point of view, this technique can be used as an upstream method to leverage other functionalities covered in other MITRE ATT&CK techniques, such as registry key interaction (T1012 and T1112), download additional tools (T1105), establish C&C communication (TA0011), or to enforce information gathering (TA0007).
  - To provide some examples in this section, think about the following commands:
    - Based on CMD (T1059.003): dir (T1083), systeminfo (T1033), tasklist (T1057), ipconfig or nbstat (T1016)
    - Based on PowerShell (T1059.001): Get-ComputerInfo (T1082), GetCurrentProcess, (T1057), or Get-NetIPAddress (T1016)
- T1106: Native API
  - Unless you're dealing with very basic (bash or Windows batch) scripts, a security incident usually involves malicious binary delivery and execution. Using native operating system functions is a central part of any binary execution. Malicious actors abuse these legitimate functions provided by the operating system to enforce malicious activities. As an example, just by reviewing T1106 procedures on the MITRE ATT&CK page (note: as reminder a procedure is an implementation of the technique), you will figure out that the T1106 technique is used to leverage other MITRE ATT&CK techniques for execution or discovery. GetCurrentProcess, GetLogicalDrives, GetComputerName, and many others all have legitimate use cases. However, they have all been abused by malware for different purposes. To overcome this, monitoring low-level APIs should not be objective but, correlated with other information that can provide indicators of malicious behavior.

Aside from the examples provided above, there are many other publicly documented examples abusing native Microsoft Windows binaries as described in LOLBAS project or Windows APIs, such as MalAPI[14].

To conclude, as soon as you focus on endpoint execution, both techniques — T1059 and T1106 — essentially provide support for a multitude of functionalities employed by malicious actors, making them difficult to block. One should exercise caution when monitoring these techniques – and look for other TTPs before making a statement regarding maliciousness.

[14] https://malapi.io/

Top sample execution ATT&CK techniques

The focus will now be placed on which techniques are commonly used by malware as a downstream technique (the objective). The following table lists the top sample execution MITRE ATT&CK techniques we observed in our threat intelligence database:

Table 5. Top MITRE techniques for sample execution

Tactic	Tactic name	Technique	Technique name
TA0002	Execution	T1106	NativeAPI
TA0007	Discovery	T1083	File and System Discovery
TA0007	Discovery	T1497	Virtualization/Sandbox Evasion
TA0005	Defense Evasion	T1027	Obfuscated Files or Information
TA0007	Discovery	T1033	System Owner/User Discovery
TA0007	Discovery	T1082	System Information Discovery
TA0005	Defense Evasion	T1070	Indicator Removal
TA0007	Discovery	T1012	Query Registry
TA0007	Discovery	T1057	Process Discovery
TA0003	Persistence	T1053	Scheduled Task/Job
TA0002	Execution	T1129	Shared Modules (community signature)
TA0005	Defense Evasion	T1112	Modify Registry
TA0007	Discovery	T1016	System Network Configuration Discovery
TA0009	Collection	T1005	Data from Local System
TA0006	Credential Access	T1003	OS Credential Dumping
TA0006	Credential Access	T1552	Unsecured Credentials

Out of the list in Table 5, as far as Keysight can observe, discovery tactic TA0007[15] is a key and pivotal technique. Many of the attacks in the wild exploit this tactic as part of their attack. As for the rest of the techniques, why should you care about them? The main reason is that there is no debate that after any compromise, information gathering, system discovery, or network discovery is an essential activity before moving to more advanced phases in malware activity, such as lateral movement (the need to discover remote host) and data collection for exfiltration.

However, we should ask why those techniques are rarely exposed as top attacks? The first answer comes from MITRE itself, “This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.” Basically, these are common system features that non-malicious tools also utilize.

[15] https://attack.mitre.org/tactics/TA0007

The second reason is related to the number of assets to manage in a company. Even if your security information and event management (SIEM) solution includes rules to detect suspicious discovery API call[16], the fact to turn on all your endpoints as event log producers, they will flood your SIEM. This situation is not applicable from a technical, operational or financial point of view. Many SIEM vendors charge by the number of alerts, and this makes logging expensive.

The third circumstance is the cybersecurity market focus on endpoint detection and response (EDR) for endpoint and demonstration capabilities to stop malware at a relatively late step of its execution. We believe that these solutions are usually not designed to cover early steps, and the reason is mostly to prevent false positives. Instead, they must correlate early techniques such as discovery, collections, exploitation along with the other advanced techniques part of tactics — Execution [17] (TA0002), Persistence, Privilege Escalation, Evasion, Credential Access, etc.

The last aspect is tied to the previous one: the lack of easy-to-use tools to enforce tracking, mitigation and enforce security policy at endpoint level. Some security solutions can enforce security tracking, detection and block for unexpected and malicious access to your file servers, remote services (like Exchange, SharePoint, OneDrive, etc.) but with a focus on network activity.

Defensive goal

Monitoring/understanding what happens in this phase – is essential to stopping a threat campaign in the earliest stages and reducing malware time in your network. In general, at the beginning of the threat campaign or malware execution before further compromise

MITRE ATT&CK Discovery Tactic Mitigation

As mentioned in the MITRE ATT&CK framework, discovery techniques (like TA0007[18]) are not trivial to handle either in detection, or mitigation, as they are mainly based on native operating system scripts, libraries, tools, or API and can be very noisy.

However, some guidance can be drawn:

- First, manage your upstream techniques — T1059 (Command and Script) and T1106 (Native API). Then, maintain up to date system and security engines. Finally, enforce a strict security policy to limit user to its necessary rights.
- You should also consider enabling Windows Defender Attack Surface Reduction (ASR) to prevent malicious code execution (e.g., JavaScript, Macro, etc.) from potentially invoking a native API call, PowerShell or script, or command line.
- The MITRE ATT&K is an active framework permanently updating its content and doesn't pretend to be exhaustive. Focusing on T1059[19], the sub techniques list should be expanded with other missing

[16] https://www.elastic.co/guide/en/security/7.17/prebuilt-rule-0-16-2-powershell-suspicious-discovery-related-windows-api-functions.html
[17] https://attack.mitre.org/tactics/
[18] https://attack.mitre.org/tactics/TA0007
[19] https://attack.mitre.org/techniques/T1059/

commonly used programming languages such as Perl, Ruby, Java and more. Identify when and where these languages should be used legitimately in your organization and then monitor or prevent their usage in places where they should not happen.

- Windows Command Shell (T1059.003): You should prefer to use PowerShell and prevent the usage of cmd.exe. A lot of native Windows binaries can be abused for malicious purposes (as explained in the LolBas[20] project).

Some general recommendations:

- Disable command prompt usage and prefer PowerShell following guideline exposed in the next paragraph, or control cmd.exe usage (such as parameters)
- If you can't disable, restrict cmd.exe to authorized users and administrators only
- Track any attempt of Windows Command Shell to execute native Microsoft Windows binaries (see). It will allow you to detect suspicious and potential malicious activity

Some PowerShell-specific recommendations:

- PowerShell (T1059.001): when facing cyber threats, you might be tempted to disable or remove PowerShell. However, this powerful scripting language has more pros than cons and should remain enabled, as suggested in a joint publication by NSA, CISA, NCSC-UK and NCSC-ZL.
- Restrict PowerShell to authorized users and administrators only
- Allow signed scripts and register pre-approved PowerShell script for administrative tasks and limit others
- Enable logs to identify any PowerShell script execution and track if it was executed by a legitimate process/user
- Educate users — remind that PowerShell can be used by the sample (binary) as one step of the post-compromise because someone already executed it by double-clicking .exe file, enabled macro on documents, and so on
- Audit yourself and exercise your infrastructure and your team to adapt your processes by using existing red-teaming PowerShell frameworks such as PowerSploit, Empire, and so on

In general, discovery techniques are not trivial to manage. Many legitimate binaries are using Native API functions which might be recognized as suspicious activity, like the “Debugger Evasion”.

[20] https://lolbas-project.github.io/

In conclusion, you can attempt to reduce the attack surface of those techniques:

- Whitelisting
  - Restrict the usage of scripting and commands
  - For many discovery techniques, you should ask yourself which commands should be allowed on different assets. For instance, is it legitimate to see "ipconfig" on a secretary’s laptop and not executed by administrator? The common answer is, “Certainly not.”
  - The MITRE ATT&CK framework provides a list of procedures that you can use in combination with project-specific references to define your whitelist and blacklist of commands
- Correlation of rules for detection
  - For some discovery techniques (mainly related to collection), you must not look for individual indicators of compromise (IOCs) but a group of them and then link them to pre-authorized/whitelisted processes

For more information on Keysight Security and Visibility products and solutions, please contact us.

KEYSIGHT

Keysight enables innovators to push the boundaries of engineering by quickly solving design, emulation, and test challenges to create the best product experiences. Start your innovation journey at www.keysight.com.

Published in USA , July 21, 2023, 3122-1173.EN