August 2023

Global Threat Landscape Report

A Semiannual Report by FortiGuard Labs

FORTINET

Table of Contents

Executive Summary 3

1H 2023 at a Glance 3

Let's Rewind: Five-Year Threat Trends 5

Penetrating the Red Zone 6

From Exploit Prediction to Outbreak 8

Global ATT&CK Heatmap 9

Technique Insights from Endpoint Telemetry 11

Protecting Your Enterprise from Evolving Threats 12

Conclusion and Final Outlook 14

Executive Summary

The threat landscape and organizations' attack surfaces are constantly transforming. And the ability of cybercriminals to quickly design and adapt their techniques to exploit this evolving environment continues to pose significant risks to businesses of all sizes, regardless of industry or geography.

As we examine activity in the first half of 2023, we see cybercrime organizations and nation-state cyber-offensive groups swiftly adopting new technologies. Notably, some of these actors operate much like traditional enterprises, complete with well-defined responsibilities, deliverables, and objectives. This organizational structure, combined with deep pockets resulting from past exploits or nation-state sponsors, facilitates their offensive stance, allowing them to experiment with and incorporate game-changing technologies, such as new generative AI, that make their attacks more complex and harder to detect.

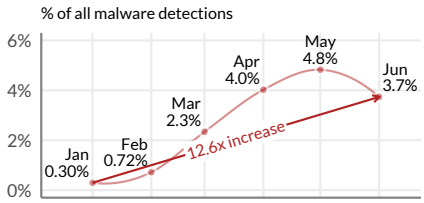
A significant uptick in the sophistication of malicious actors is especially evident in the cybersecurity domain, where threats have escalated in frequency and complexity. This is characterized by a rise in highly targeted attacks across various sectors, including intricate ransomware campaigns, substantial data breaches, and a notable shift in MITRE ATT&CK tactics, as observed through our global, AI-enhanced detection capabilities.

1H 2023 at a Glance

APT Groups

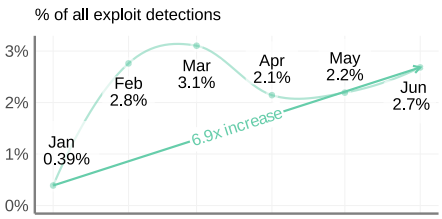
Activity was detected for 41 of 138 (30%) APT groups identified by MITRE. These attacks are more focused and planned and also occur in quick "waves," so seeing a third of all categorized APT groups being active is concerning.

Ransomware



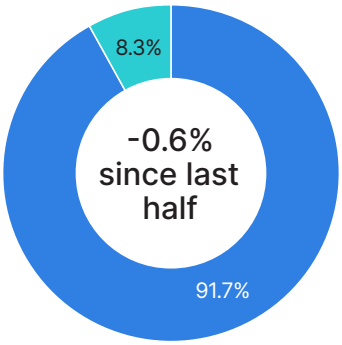
The ransomware rollercoaster continued, ending 1H 2023 13x higher than it began. Fewer organizations are successfully detecting ransomware than in the past (13% versus 22%), reaffirming that ransomware is also becoming more sophisticated and targeted.

ICS and OT Attacks



Attacks targeting industrial control systems (ICS) and operational technologies (OT) didn't occur at high volume but trended up over the first half of 2023. Half of organizations saw ICS or OT exploits, with energy and utilities ranking among the top targets.

Into the Red Zone



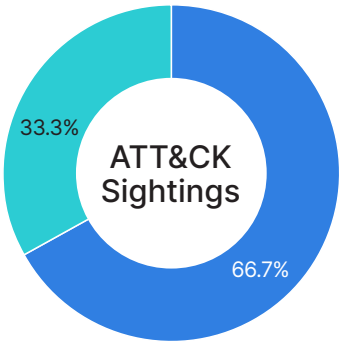
The percent of all endpoint vulnerabilities targeted by attackers remained relatively steady (around 8%) in 1H 2023 compared to the previous period.

Time-to-Exploitation

327x

Our analysis shows that the top most exploitable vulnerabilities, as identified by EPSS, are 327 times more likely to be attacked within a week than others on your radar.

ATT&CK Sightings



Using our detection technologies, we observed activity for two-thirds of all known MITRE ATT&CK techniques over the first half of 2023.

In 1H 2023, we observed significant activity among advanced persistent threat (APT) groups, a rise in ransomware frequency and complexity, increased botnet activity, a shift in MITRE ATT&CK techniques used by attackers, and more.

However, despite the changing threat landscape, it's not all bad news for defenders. In this report, we'll also look closely at vulnerabilities and offer advice on prioritizing your patching and remediation efforts. And because so much of the threat landscape activity we're seeing is familiar, there are plenty of opportunities to implement strategies to effectively defend against bad actors. Lastly, we'll cover numerous actionable steps you can take today, such as leveraging threat intelligence to better safeguard your organization.

A third of all categorized APT groups were active in 1H 2023

It's worth taking a moment to spotlight the threat actors behind these trends we're analyzing. As part of their efforts to support the ATT&CK framework, MITRE tracks 138 cyberthreat groups.[1] Monitoring the collective activity of these groups is an essential component of mapping and analyzing the threat landscape. From January through June 2023, we observed activity attributed to 41 of these groups (30%). Of those, Turla, StrongPity, Winnti, OceanLotus, and WildNeutron were the most active based on malware genetic code analysis.

Turla is possibly one of the most-proficient threat groups in existence. They have operated under numerous aliases (Snake, Venomous Bear, and Blur Python, to name a few) for nearly two decades. Turla has been linked to more than 45 high-profile attacks, impacting government agencies, media, energy sector organizations, and embassies worldwide. They've had success in breaching organizations and flying under the radar for years, even in highly monitored environments, and given the escalation of the Russian-Ukrainian conflict, we were not surprised to see increased activity from this particular group.

However, there's some good news: Over the past six months, APT group activity impacted only a small subset of all organizations, indicating that APT activity is still highly targeted, at least for the time being. This makes sense as they won't waste their cyber weapons on spraying attacks.

The ransomware rollercoaster continues

While ransomware has existed for decades, in recent years, we've witnessed threat actors using more-sophisticated and complex strains to infiltrate networks, largely thanks to the rise of Ransomware-as-a-Service (RaaS) operations.[2] And as ransomware activity remains rampant, business leaders around the globe are becoming more concerned about this threat. In a recent survey conducted by Fortinet, of the 78% of leaders who claimed their enterprises were prepared for an attack, half still fell victim to them.[3]

Ransomware shows no signs of slowing, with ransomware activity ending 13 times higher than at the start of 2023 as a proportion of all malware detections. Nearly a quarter (22%) of firms detected ransomware activity on their respective networks five years ago. That's now down to 13% as we examine the first half of 2023. Unfortunately, this apparent decrease in activity doesn't indicate that ransomware activity is subsiding. Instead, it's a sign that ransomware distribution has become more concentrated as ransomware gangs advance their business models by carrying out more targeted attacks using quickly adaptable and sophisticated playbooks.

The following image shows information on the most-prevalent malware families observed via our telemetry in the first half of 2023. It shares the top families for each category across cryptominers, infostealers, ransomware, and Remote Access Trojans (RATs).

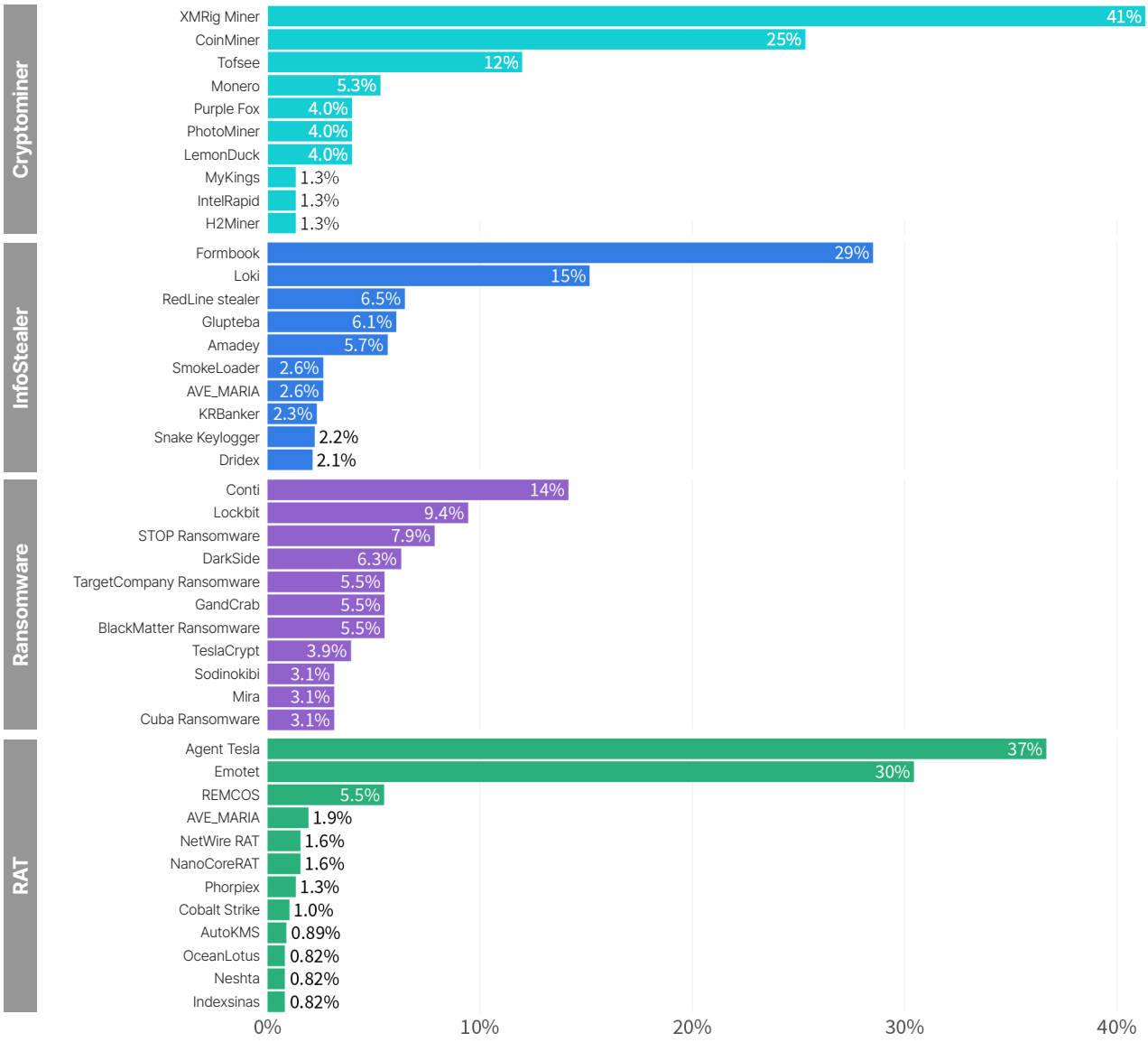


Figure 1: Top malware families by type

Wipers are waning… for now

One category of ransomware not listed above is wiper malware.[4] Wipers are aptly named because this destructive attack technique "wipes" data off infected systems. We observed a surge in wiper use in early 2022, mainly in conjunction with the Russian-Ukrainian conflict.[5] And while that increase persisted through the rest of the year, it slowed over the first half of 2023.

While we've often observed wipers being used primarily by nation-state actors during times of war, we've also seen cybercriminals use this type of malware to target organizations in specific sectors, including technology, manufacturing, government, telecommunications, and healthcare.

Let's Rewind: Five-Year Threat Trends

As security practitioners, many of us tend to assume that everything always gets worse when it comes to cybersecurity.

But is that assumption fact or fiction? It's important to take a step back occasionally to examine longer-term trends, which can give us needed perspective on the current state of the threat landscape. Let's rewind and look at five-year trends regarding exploits, malware, and botnets.

Exploit variants on the rise

The count of unique exploit detections is up 68% over the past five years. This indicates that we have more ways to detect malicious attacks today than we have previously. Additionally, it demonstrates that attackers are multiplying and diversifying their exploits. But at the same time, we observed a 75% drop in exploitation attempts per organization and a 10% dip in severe exploits.

While this drop in exploitation attempts may initially sound promising, it is another indication that attackers are carrying out more targeted attacks. Cyber weapons can also become weary if used too often, as detection capabilities will eventually pick up, rendering the payload useless over time.

Exploits

10,042 **unique exploit detections**
- +68% over last 5 years

54 **exploit detections per organization**
- -75% over last 5 years

69% **of organizations saw severe attacks**
- -10% over last 5 years

Increased malware activity driven by organized cybercrime

Malware families and variants have exploded over the past five years, up 135% and 175%, respectively. Arguably more noteworthy is that the number of malware families that have infiltrated at least 10% of global organizations (a critical prevalence threshold) has doubled. That's undoubtedly the result of an increasing number of cybercriminal and nation-state groups, as well as the expansion of operations of those that are currently active.

As these adversaries become increasingly selective, precise, and destructive, they represent a progressively escalating threat, necessitating an unending battle against them. Leveraging the most recent and significant technological advancements from the past few years, these foes have rapidly evolved to become more capable, versatile, and covert.

Botnets become more persistent

Most modern malware families have established botnets for command and control (C2) communications. Given the growth in malware families and variants, it makes sense that botnet activity would increase as well. Today, there are more active botnets (+27%) and a higher incidence rate of botnet infection among organizations (+126%).

The real kicker for botnet trends observed in the 1H 2023, though, is the significant increase in the total number of "active days"—the time measured between when botnet activity was first detected by sensors and when the botnet ceased C2 communications. Over the last six months, that averaged 83 of 183 days (the last day we measured), nearly half the period. This represents a more than 1,000-fold increase from measurements taken at the beginning of 2018, indicating that botnets have become more persistent over the past five years. The overall increase in the availability of vulnerabilities and exploits to incorporate into the "botnet weapons belt" makes this a concern, as they are quick to adapt and increase the range of devices they can automatically breach and control.

Penetrating the Red Zone

We introduced the "Red Zone" in our 2H 2022 Global Threat Landscape Report to better understand how likely (or unlikely) it is that threat actors will exploit a specific vulnerability.[6]

While several factors influence the relationship between Common Vulnerabilities and Exposures (CVEs) on endpoints and CVEs targeted by attackers, such as vulnerability management practices among organizations or developments in adversary tooling, this provides a valuable snapshot of the state of the attack surface that security leaders can use to prioritize their patching efforts.

In the second half of 2022, the red zone hovered around 9%, meaning that about 1,500 CVEs, out of more than 16,500 we observed, were under attack. But for the first half of 2023, this proportion of CVEs under attack dropped to 8.3%. Interestingly, about the same number of CVEs appeared in attacks, while the share of CVEs observed on endpoints grew. While this doesn't necessarily indicate that organizations are gaining ground in the fight against new vulnerabilities, at least the percentage of vulnerabilities under attack appears to be slightly lower than in the past.

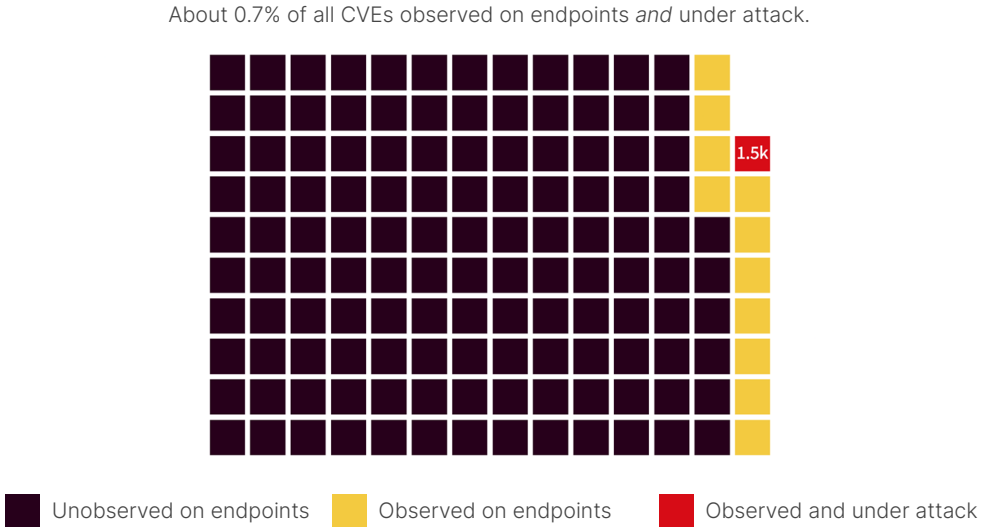


Figure 2: All CVEs by presence on endpoints and among attacks

We also know that the share of vulnerabilities under attack can vary widely by platform, as much as 11%, as shown below. Another noteworthy distinction among platforms is the share of all CVEs that appeared on endpoints, shown in yellow. Consider Microsoft and Adobe, where over half of the related vulnerabilities were observed, compared to 12% for Apple platforms or 20% for Linux. It's worth noting that these charts normalize all platforms. For example, one square for Adobe represents a different absolute number of vulnerabilities from Linux.

What's clear is that organizations continue to struggle with closing vulnerabilities as quickly as they're released, and cybercriminals are quick to exploit that reality. So, it's vital to have a sound strategy when prioritizing which vulnerabilities to patch and to protect systems in the interim, deploy methods such as virtual patching until patches can be deployed. While each platform should be considered during that prioritization process, that only scratches the surface in anticipating which open vulnerabilities will likely be targeted by attackers in the near future.

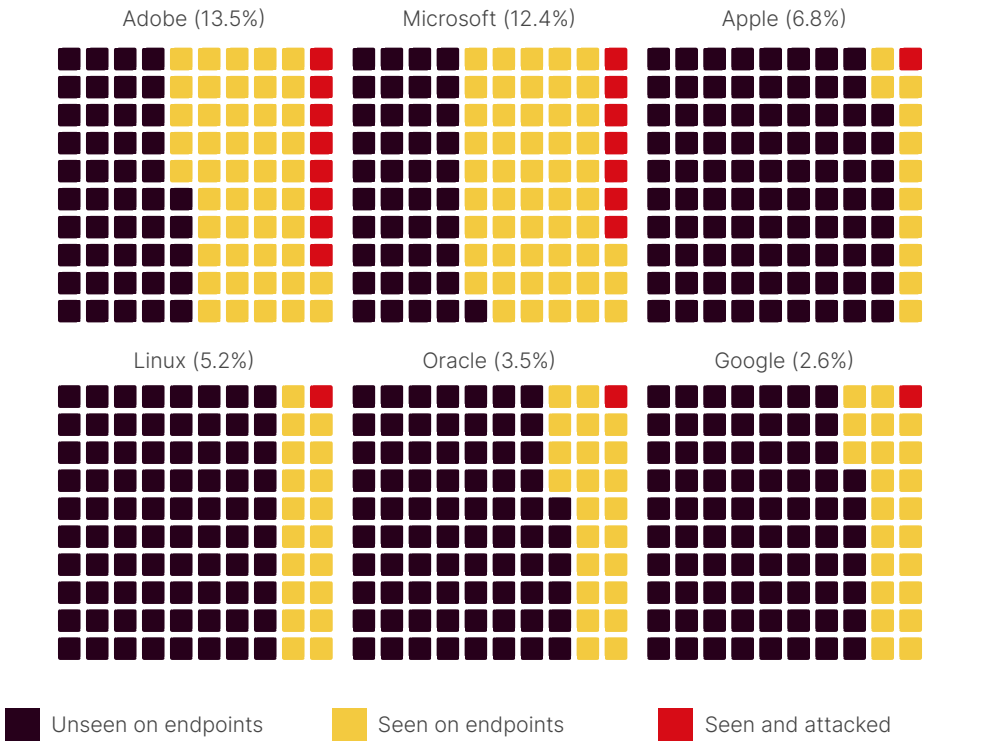


Figure 3: CVEs for multiple platforms by presence on endpoints and among attacks

The good news is that defenders already have something more powerful at their disposal, the Exploit Prediction Scoring System (EPSS), covered in the next section.[7]

From Exploit Prediction to Outbreak

Since its inception, Fortinet has been a core contributor to exploitation activity data in support of the EPSS. The Exploit Prediction Scoring System leverages numerous data sources to predict the likelihood that a vulnerability will be exploited in the wild. The Exploit Prediction Scoring System is led by a special interest group at FIRST.org, where Fortinet is a member company.

Vulnerability management teams use EPSS to help prioritize their remediation efforts. But EPSS can also support intelligence efforts to track the progression of vulnerabilities from initial disclosure to the outbreak of an exploitation in the wild. It's that use case we want to explore here. If EPSS data is incorporated into your threat intelligence process, it can be used effectively as an early warning system.

Let's look at an example. On May 31, an SQL injection vulnerability was announced in the MOVEit Transfer web application that could allow an unauthenticated attacker to change or delete elements in the database engine used.[8] The cybersecurity community quickly recognized this vulnerability as one to watch, and FortiGuard Labs released a Threat Signal to spread awareness and an IPS signature to monitor for exploitation activity.[9]

Once the CVE was published, EPSS was able to predict a very high chance of exploitation in the next 30 days. Spoiler alert: It didn't take that long. Our sensors recorded attacker attempts to exploit the MOVEit vulnerability on June 5, just five days after the vulnerability was first identified, and we released a signature that same day. In this case, EPSS provided independent validation of what our analysts anticipated and helped us stay ahead of this emerging threat during its fast ramp-up period.

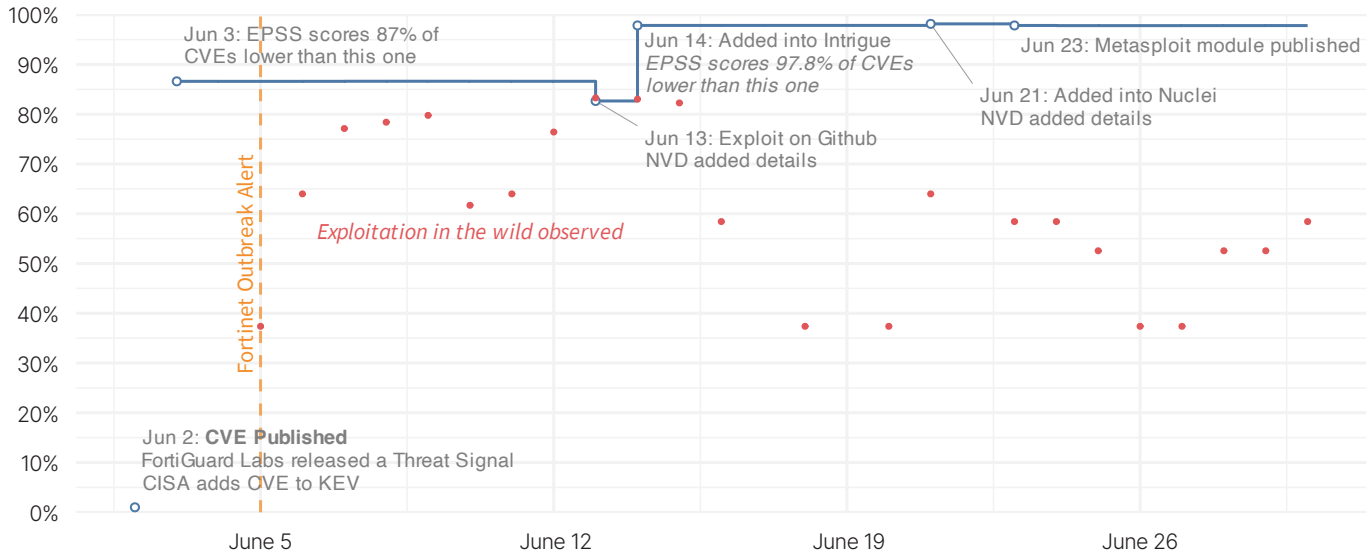


Figure 4: Evolution of EPSS and exploitation for the MOVEit vulnerability

The MOVEit example prompts an interesting line of questions. How long does it typically take for a vulnerability to move from initial release to exploitation in the wild? Do CVEs with a high EPSS score get exploited faster than those with lower scores? If so, can we predict the mean time-to-exploitation for any given vulnerability using EPSS?

Let's see if we can answer those questions. To do that, we analyzed six years of data spanning more than 11,000 published vulnerabilities for which our sensors detected exploitation. For each CVE, we determined the time from publication to the first observation of exploitation and the corresponding EPSS score. The resulting analysis is captured in the chart below:

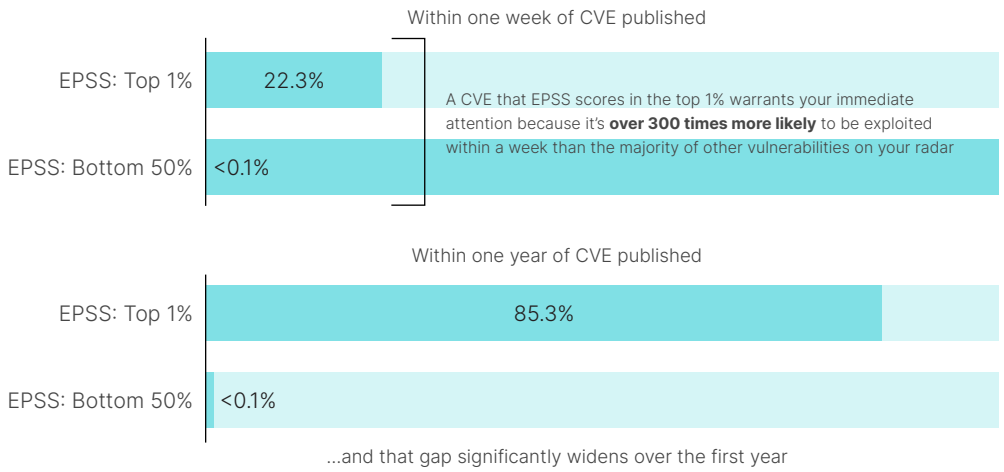


Figure 5: Exploitation rate of vulnerabilities with different EPSS scores

In short, we learned that EPSS matters when predicting which vulnerabilities might be exploited and how quickly that exploitation will occur. Within seven days of publication, 22% of vulnerabilities with the highest EPSS scores (top 1%) saw exploitation activity, compared to just 0.07% of those in the bottom half of EPSS scores. After a full year, 85% of the highest-ranking EPSS CVEs recorded exploitation, while the lower half remained largely ignored by attackers.

That means that a CVE that EPSS scores in the top 1% warrants your immediate attention because it's over 300 times more likely to be exploited within a week than most other vulnerabilities on your radar. If you aren't doing so already, pull those EPSS scores daily and prioritize your patching efforts accordingly.[10]

Global ATT&CK Heatmap

After approximately six months of continual data processing leveraging our global network of over 10 million sensors, we compiled a list of the most commonly observed hashes in the wild. Our state-of-the-art sensors employ machine learning (ML) techniques to transform raw data into an enriched dataset that examines network traffic for potential threats. We then use our portfolio of Fortinet products and solutions to analyze detected malicious payloads, observing and identifying subtle behavior indicative of their underlying intent. The insights generated through this process are crucial for cybersecurity defenders worldwide, enabling laser-focused red team engagements and effective threat hunting activities.

MITRE offers us a better understanding of the operations of threat actors. Both easy-to-follow and actionable, ATT&CK enables defenders to categorize threat actor behaviors in a manner that is both systematic and repeatable, ultimately helping security teams to better identify potential attacks and accurately assess organizational risk.

Please note that this report represents only "a piece of the pie." Different security solutions have their own unique capabilities and roles when it comes to detecting specific techniques. This analysis is based on data from FortiSandbox sandboxing and FortiEDR endpoint detection and response solutions.

Let's examine data first. These techniques can best be interpreted as attack capability.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Replication Through Removable Media: 60%	Exploitation for Client Execution: 24%	Hijack Execution Flow: 30%	Process Injection: 34%	Obfuscated Files/Info: 19%	OS Credential Dumping: 42%	System Info Discovery: 21%	Replication Through Removable Media: 63%	Data from Local System: 29%	Application Layer Protocol: 40%	Exfiltration Over Alternative Protocol: 100%	System Shutdown/ Reboot: 56%
Phishing: 28%	WMI: 22%	Boot/Logon Autostart Execution: 20%	Hijack Execution Flow: 21%	Masquerading: 15%	Input Capture: 40%	File & Directory Discovery: 15%	Taint Shared Content: 25%	Input Capture: 23%	Non-Application Layer Protocol: 22%	Automated Exfiltration: 0.02%	Data Manipulation: 30%
Drive-by Compromise: 5%	Command & Scripting Interpreter: 19%	Create/Modify System Process: 19%	Boot/Logon Autostart Execution: 14%	Virtualiz./ Sandbox Evasion: 15%	Unsecured Credentials: 17%	Software Discovery: 13%	Remote Services: 4%	Email Collection: 21%	Ingress Tool Transfer: 19%		Data Encrypted for Impact: 5%
Exploit Public-Facing Application: 4%	Shared Modules: 13%	Scheduled Task/Job: 18%	Create/Modify System Process: 13%	Impair Defenses: 13%	Credentials from Password Stores: 0.6%	Virtualiz./ Sandbox Evasion: 11%	Use Alternate Authentication Material: 4%	Automated Collection: 15%	Encrypted Channel: 12%		Inhibit System Recovery: 3%
External Remote Services: 2%	Scheduled Task/Job: 10%	Office Application Startup: 11%	Scheduled Task/Job: 13%	Process Injection: 9%	Steal Web Session Cookie: 0.1%	Process Discovery: 9%	Lateral Tool Transfer: 2%	Archive Collected Data: 4%	Non-Standard Port: 4%		Service Stop: 3%
Valid Accounts: 1%	Native API: 6%	Event Triggered Execution: 0.3%	Access Token Manipulation: 4%	Indicator Removal on Host: 7%	Network Sniffing: 0.09%	Remote System Discovery: 8%	Exploitation of Remote Services: 1%	Clipboard Data: 3%	Proxy: 2%		Endpoint Denial of Service: 1%
	System Services: 5%	Browser Extensions: 0.3%	Event Triggered Execution: 0.3%	Hijack Execution Flow: 6%	Adversary in the Middle: 0.01%	Query Registry: 7%	Software Deployment Tools: 1%	Browser Session Hijacking: 3%	Web Service: 0.7%		Resource Hijacking: 0.7%
	Inter-Process Comm.: 0.5%	Pre-OS Boot: 0.2%	Abuse Elevation Control Mechanism: 0.07%	Hide Artifacts: 4%	Forge Web Credentials: 0.007%	System Network Configuration Discovery: 6%		Screen Capture: 0.7%	Remote Access Software: 0.07%		Data Destruction: 0.7%
	User Execution: 0.06%	Boot/Logon Initialization Scripts: 0.09%	Boot/Logon Initialization Scripts: 0.07%	Deobfuscate/ Decode Files/Info: 3%	Modify Authentication Process: 0.0006%	Application Window Discovery: 5%		Video Capture: 0.4%	Data Obfuscation: 0.02%		Defacement: 0.08%
	Software Deployment Tools: 0.005%	Create Account: 0.03%	Valid Accounts: 0.02%	Modify Registry: 3%	Brute Force: 0.0003%	System Owner/User Discovery: 1%		Data from Info Repositories: 0.3%	Data Encoding: 0.02%		Account Access Removal: 0.05%

Figure 6: ATT&CK techniques in cloud data by tactic

As you can see, detections gleaned from data provide thorough visibility across the ATT&CK framework. The columns above highlight the top 10 most-detected techniques for each tactic. Subtechniques listed in each category column have been rolled up to their parent technique for the sake of the visual. Let's explore how these techniques have been deployed over the past six months and discuss ways to counter them.

In the Initial Access phase, the most-prevalent technique observed is replication via removable media.[11] While it's not the number-one entry point into corporate networks, the majority of malicious payloads we analyzed could spread via this method. This technique saw an uptick in usage when it was picked up by Raspberry Robin, which we covered in our previous report.[12] Since then, Microsoft has uncovered numerous other uses of this worm, with Raspberry Robin growing into one of the largest malware distribution platforms. From the FortiGuard Labs perspective, this worm has spread so widely mainly because of its simple tactic of masquerading a .LNK file as a folder, which most individuals are likely to open. This malware family has been named by the Cybersecurity and Infrastructure Security Agency (CISA) as one of the most active droppers in existence, being used to deliver IcedID, TrueBot, and Bumblebee malware.[13]

In the Execution phase, we noted a surge in Exploitation for User Execution.[14] This trend implies that attacks are decreasingly dependent on users inadvertently triggering a payload or enabling macros. An example is a specific vulnerability exploited in Microsoft Word, like the increasingly prevalent Follina vulnerability (CVE-2022-30190) detailed in several of our recent blog posts.[15] We also observed this trend in threats stopped by FortiEDR. Many are now less reliant on user interaction to achieve code execution. One way to safeguard your organization from this technique is to shrink your attack surface by regularly patching vulnerabilities.

For the Persistence phase, we continue to see high instances of DLL Sideloading (under Hijack Execution Flow).[16] The 3CX attack employed this technique to achieve both Defense Evasion and Persistence, which we analyzed in this recent blog post.[17] This technique is particularly troublesome because it enables attackers to sidestep protective measures like application control and other limitations on software execution. To protect your organization's network from this technique, ensure that software isn't vulnerable to DLL Sideloading in the first place, as there is not much you can do otherwise to avoid running unintended code. While malicious payloads within the network will get flagged eventually, that will only occur after they've been loaded into memory.

The top three techniques under Defense Evasion are no great surprise: Obfuscated Files and Information, Masquerading, and Virtualization/Sandbox Evasion.[18, 19, 20] Even unique pieces of malware demonstrate various forms of obfuscation, from API calls to strings in memory. Given the widespread implementation of sandbox solutions on-premises and as Software-as-a-Service (SaaS) offerings, mastering these techniques has become essential for any threat actor.

OS Credential Dumping and Input Capture lead the pack under Credential Access.[21, 22] Since its release, we have observed multiple threat actors leveraging Mimikatz for related functionality. Furthermore, its integration into various post-exploitation frameworks, such as Cobalt Strike, Metasploit, and Sliver (and its ability to use Reflective Loading T1620 via PowerShell) make it a helpful tool, even among fileless attacks.

The Discovery and Lateral Movement phases exhibit a symbiotic relationship; increased asset discovery leads to heightened lateral movement within compromised environments. One of the most effective defense strategies against this is ensuring proper visibility and control over network traffic, as a wide variety of techniques occur during these phases and can be detected with appropriate controls.

From Collection to Impact, little has changed. Adversaries use the same techniques to collect and aggregate sensitive data, then exfiltrate over a protocol different from the command and control channel. About 22% of attacks use connectionless protocols, such as UDP or ICMP, to communicate with their C2 servers. While it's an unusual choice due to the increased complexity of establishing and maintaining a connection and a lack of error correction, this technique can fly under the radar because these protocols aren't closely monitored.

Technique Insights from Endpoint Telemetry

Looking at our FortiEDR data gives us another perspective regarding attacks and the initial access techniques that cybercriminals use. In the majority of cases, organizations using EDR capabilities also use some form of sandboxing, so it's safe to say that the threats that are stopped by an EDR tool are most likely those that would have managed to bypass "traditional" sandboxing technology (an excellent example of the need for defense-in-depth). Understanding how these threats operate can give defenders more focused intelligence for their threat hunting activities.

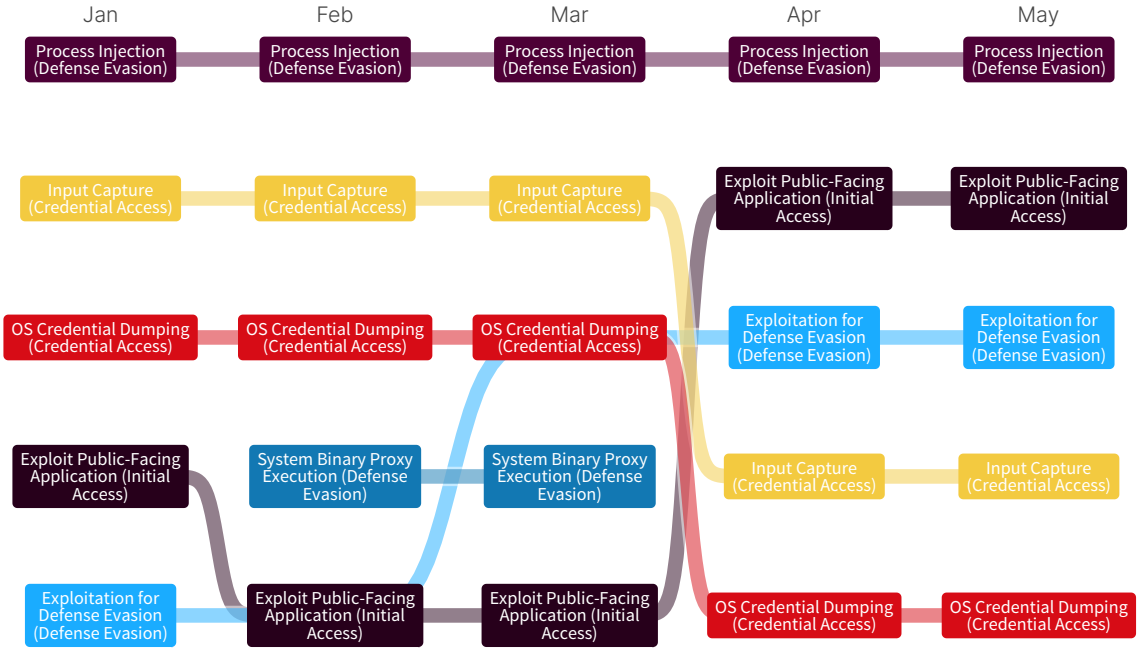


Figure 7: Top ATT&CK techniques detected by FortiEDR by month

Above are the five most active techniques per month. Some of the same techniques seen and stopped by sandboxing technology get used in other events once execution is achieved inside a machine in an organization. The most active techniques we observed during 1H 2023 include:

- Process Injection
- Input Capture
- OS Credential Dumping
- Exploit Public-Facing Application
- Exploit For Defense Evasion

Process Injection is the leader across all months.[23] With a dozen possible process injection types that have already been categorized, this technique is undoubtedly used and abused by attackers for both defense evasion and privilege escalation.

The second and third most-used techniques across all months is Credential Access: Input Capture. Using these techniques, potential threat actors try intercepting user input to acquire credentials or amass data by looking for credentials in memory. During regular system interaction, users typically share their credentials across various endpoints, such as authentication portals or system prompt windows. The mechanisms deployed for capturing this input can often be indistinguishable to the user, such as through Credential API Hooking.

To finish, we have Exploitation for both Defense Evasion and Initial Access as the final most-used techniques, with almost the same number of triggers in the wild. Adversaries are keen to exploit vulnerabilities in software to gain a vantage point in the system so they can further carry out their nefarious actions. With the number of CVEs exploding over the last couple of years (we are on track to hit 30,000 CVEs this year, a 50% increase over the 20,000 CVEs reported in 2021), it's not like there is a shortage of vulnerabilities for attackers to add to their respective toolboxes. Coupled with the advent of AI LLMs (Large Language Models used to rapidly process large datasets to quickly pinpoint incoming threats and existing vulnerabilities), crafting an exploit for that low-hanging fruit is easier than ever, so we expect that these will continue to be the weapon of choice for cyberattackers.

Protecting Your Enterprise from Evolving Threats

Cybercriminals will never miss an opportunity to make a profit, and the rise of organized cybercrime like RaaS groups in recent years has made a quick payday even easier to achieve. Bad actors will constantly find new vulnerabilities to exploit and more-sophisticated attack techniques to infiltrate networks. However, the good news is that most of the tactics used by threat actors over the past few months are familiar to us, which means defenders have more opportunities than ever to thwart attacks before they happen.

As attackers continue to evolve their own operations, though, it's crucial to assess and enhance the cyber-defense strategies within your organization to stay ahead of potential threats. From using and sharing threat intelligence to implementing the right technologies, here are several steps you can take today to safeguard your enterprise's networks and data.

Share and utilize threat intelligence

To combat the ever-increasing sophistication and volume of cyberthreats, the practice of sharing and utilizing threat intelligence has emerged as a vital component of any organizational defense strategy. Fortinet is committed to doing its part to enable advancements in threat intelligence sharing.

Fortinet is a founding member of the Cyber Threat Alliance (CTA), an organization created in 2014 to enable threat intelligence sharing among competing cybersecurity vendors.[24] Fast-forward to today, and this organization has become vital to combating cybercrime effectively on a global scale. However, establishing trust and confidentiality, ensuring data standardization, and managing a high volume of information are just some obstacles that complicate effective intelligence sharing. The CTA has successfully tackled these challenges, uniting elite Cyber Threat Intelligence (CTI) teams worldwide and significantly enhancing the global perspective on cyberthreats.

Understand attack flows to identify patterns and indicators of compromise

Cyberattacks are becoming more sophisticated, frequent, and damaging, making it crucial for businesses to enhance their knowledge of their adversaries. Understanding the attack flow, from initial entry points to post-exploitation activities, is essential for developing effective cybersecurity strategies.

Attack flow refers to the sequence of steps an adversary takes to infiltrate a target system and achieve their objectives. It encompasses various stages, including reconnaissance, initial access, privilege escalation, lateral movement, data exfiltration, and persistence. Organizations can better identify vulnerabilities, implement appropriate security measures, and respond effectively to cyberthreats by understanding each stage.

Understanding the attack flow is crucial for several reasons. First, it allows organizations to visually understand the steps of an attack and their relationships and outcomes. By studying adversaries' tactics, techniques, and procedures (TTPs) at each stage, security teams can identify patterns and indicators of compromise (IOCs), enabling them to identify an attack in progress and take timely action.

Comprehending the attack flow also helps organizations allocate resources more effectively. By focusing on the most vulnerable stages of an attack, such as initial access or privilege escalation, businesses can prioritize security measures and investments to maximize their cybersecurity posture.

Lastly, understanding an attack flow enables organizations to enhance their incident response capabilities. By mapping out an attack's various stages and potential activities, security teams can develop playbooks and response plans tailored to each stage, ensuring a swift and effective response during a cyberattack.

The advantages of fully understanding attack flows are why Fortinet has participated as a research sponsor in both MITRE Engenuity's Center for Threat-Informed Defense (CTID) ATTACK Flow projects.[25] We believe that such advances in threat intelligence, in which we can identify and respond to threats based on their profile, will shift the economics of an attack to tip the scale in favor of the defenders.

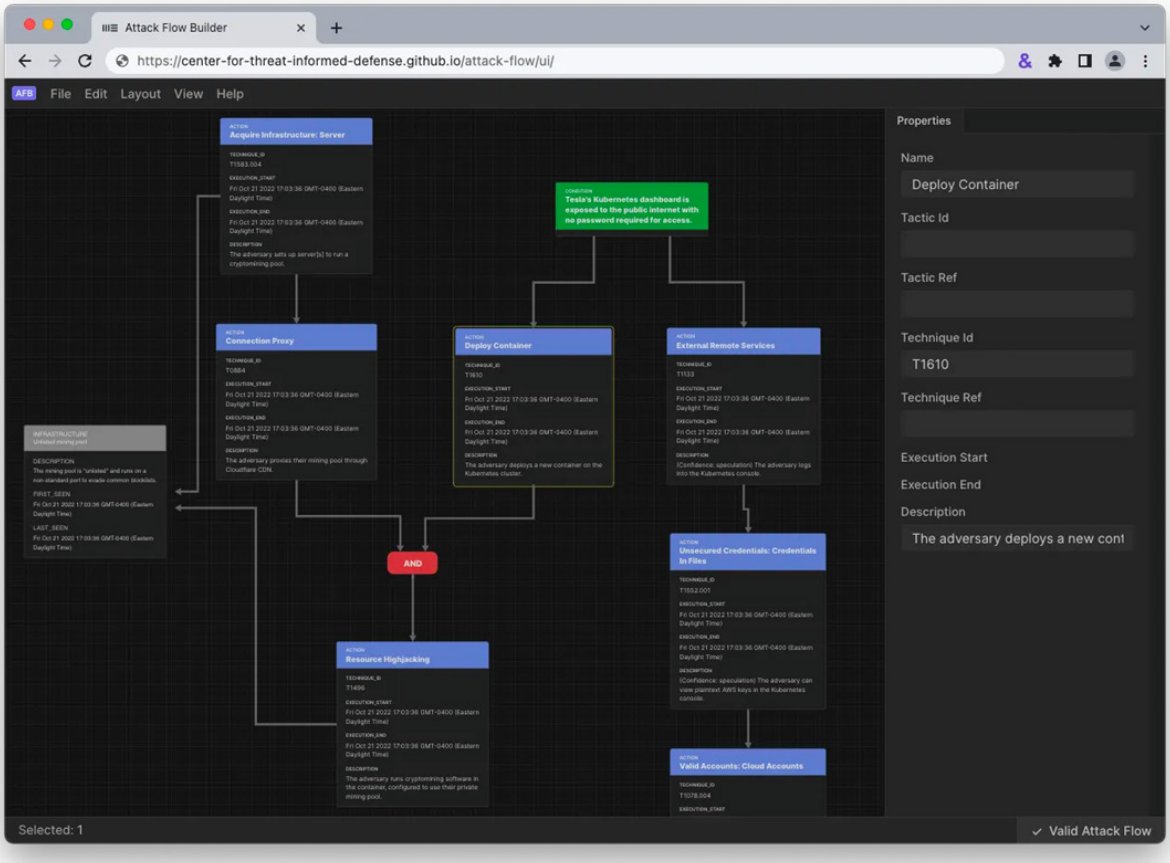


Figure 8: MITRE ATT&CK Flow Builder - Example Flow

We're also starting to incorporate standards in our reports, such as the Wintapix driver work published by two of our researchers.[26]

Shore up your technologies and processes

There's no time like now to implement new security technologies or reassess your current stack. Regardless of your chosen tools, you must ensure they can leverage AI, ML, deep learning (DL), and advanced analytics. These capabilities have become essential for processing the enormous volume of data organizations generate to identify risky or anomalous traffic that could indicate a threat or other risk.

Examining and adjusting your current processes is a must if you want to stay ahead of your adversaries. This includes redefining roles and responsibilities on your security team, building or updating playbooks, and conducting tabletop exercises to pressure-test your team's capabilities or identify process gaps that must be addressed.

Many organizations today are also turning to trusted vendors to act as an extension of their own security personnel. Our FortiGuard AI-Powered Security Services span a variety of powerful tools, like next-generation firewalls (NGFWs); network telemetry and analytics; endpoint detection and response (EDR); extended detection and response (XDR); digital risk protection (DRP); security information and event management (SIEM); inline sandboxing; deception; security orchestration, automation, and response (SOAR); and more. These solutions provide your organization with advanced threat detection and prevention capabilities that can help you quickly detect and respond to security incidents across the entire attack surface.

Conclusion and Final Outlook

We hope you enjoyed reading this report as much as we enjoyed creating it. We understand that cybersecurity can sometimes appear exceedingly complex. However, the field is invariably populated by inspired, enthusiastic individuals who work tirelessly to provide the community with innovative and streamlined approaches to enhance their security posture. The struggle against cybercrime and threats posed by nation-states is a constant challenge, and as an industry, we're fully prepared to confront and combat it.

The strengthening of partnerships sharing threat intelligence between the public and private sectors is crucial in fighting this cyber war. Threat intelligence must be immediately actionable through comprehensive playbooks, which can be a challenge without standards when it comes to sharing, tooling, and reporting. Yet shared threat intelligence is a key component of how we ensure frictionless, timely, and effective responses. We firmly believe that defenders today possess ample access to tools, knowledge, and support to begin altering the economics of an attack, all of which represent a powerful countermeasure against adversaries.

[1] "MITRE ATT&CK Matrix for Enterprise," MITRE, 2015–2023.

[2] Douglas Jose Pereira dos Santos, "2H 2022 Global Threat Landscape Report: Key Insights for CISOs," Fortinet, March 3, 2023.

[3] "2H 2022 Global Threat Landscape Report," Fortinet, March 3, 2023.

[4] Geri Revay, "The Year of the Wiper," Fortinet, January 24, 2023.

[5] Derek Manky, "The Latest Intel on Wipers," Fortinet, March 23, 2023.

[6] Douglas Jose Pereira dos Santos, "2H 2022 Global Threat Landscape Report: Key Insights for CISOs," Fortinet, March 3, 2023.

[7] "Exploit Prediction Scoring System," FIRST.org, 2015-2023.

[8] James Slaughter, Fred Gutierrez, and Shunichi Imano, "MOVEit Transfer Critical Vulnerability (CVE-2023-34362) Exploited as a 0-Day," Fortinet, June 8, 2023.

[9] "Threat Signal Report: MOVEit Transfer Critical Vulnerability (CVE-2023-34362)," FortiGuard Labs, June 2, 2023.

[10] "EPSS API," FIRST.org, 2015–2023.

[11] "Replication Through Removable Media," MITRE ATT&CK, May 31, 2017.

[12] "IPS Threat Encyclopedia: Raspberry.Robin.Worm," FortiGuard Labs, July 14, 2022.

[13] "Increased Truebot Activity Infects U.S. and Canada-Based Networks," Cybersecurity and Infrastructure Security Agency, July 6, 2023.

[14] "Exploitation for Client Execution," MITRE ATT&CK, April 18, 2018.

[15] Fortinet Follina Blog Posts, accessed July 27, 2023.

[16] "Hijack Execution Flow: DLL Side-Loading," MITRE ATT&CK, March 13, 2020.

[17] FortiGuard Labs, "3CX Desktop App Compromised (CVE-2023-29059)," Fortinet, March 30, 2023.

[18] "Obfuscated Files or Information," MITRE ATT&CK, May 31, 2017.

[19] "Masquerading," MITRE ATT&CK, May 31, 2017.

[20] "Virtualization/Sandbox Evasion," MITRE ATT&CK, April 17, 2019.

[21] "OS Credential Dumping," MITRE ATT&CK, May 31, 2017.

[22] "Input Capture," MITRE ATT&CK, May 31, 2017.

[23] "Process Injection," MITRE ATT&CK, May 31, 2017.

[24] Derek Manky, "Partnering to Disrupt Cybercrime," Fortinet, February 14, 2023.

[25] Douglas Jose Pereira dos Santos, "MITRE Attack Flow Gives CISOs Valuable Context for Better Risk Management," Fortinet, November 3, 2022.

[26] Geri Revay and Hossein Jazi, "WINTAPIX: A New Kernel Driver Targeting Countries in the Middle East," Fortinet, May 22, 2023.

August 7, 2023 11:15 AM

2278529-0-0-EN