FURTINET

August 2022

Global Threat Landscape Report

A Semiannual Report by FortiGuard Labs

TABLE OF CONTENTS

Overview and Key Highlights

Another half-year through unprecedented times has passed. But as unique as these times may feel, we continue to see familiar exploits, names, and attacks taking up space. To help you and your business feel confident in your ability to protect yourself against the threats that continue to come our way, this report looks back on the cyber threat landscape of the first half of 2022 using our global array of sensors monitored by FortiGuard Labs. Here's what we learned:

Ransomware Roundup:

Over the past six months, we have seen 10,666 ransomware variants across our platform, compared to just 5,400 in the previous six months. That's almost **2x growth** in ransomware variants in half a year.

Wipers Widening:

1H-2022 saw a surge of wipers (malware designed to delete data) deployed in parallel with the Russia-Ukraine war. However, those wipers didn't just stay in one place - their proliferation worldwide proves there are truly no borders when it comes to cybercriminal activity.

OT Vulnerabilities:

Operational Technology (OT) products are increasingly targeted and demonstrate higher risk due to today's shift from air-gapped environments to the interconnected world. We look at which OT vendors have the highest volume of vulnerabilities.

Log4j Lingers:

This vulnerability found in Apache servers made itself known in late 2021, and while exploits targeting it may not have reached the peaks that were predicted, that doesn't mean it's any less of a threat. Cyberespionage groups, like APT41, exploited this vulnerability to gain access to US government systems in the first half of 2022, showing we are far from being "done" with it. Generally, vulnerabilities as ubiquitous as this that are easily exploitable with public proof of concept exploits tend to linger for years.

HTML & JavaScript are the most popular delivery mechanisms, but don't count Linux out:

HTML & JS are the pack leaders here, although LNK also placed high in the first half of 2022. While most Linux-based malware attacks these days are cryptomining-related, attackers also leverage Linux for staging, automated authentication attacks, and persistence after an identified vulnerability has been exploited.

Top Threats During 1H- 2022

The findings in this report represent the collective intelligence of FortiGuard Labs, drawn from a vast array of sensors collecting hundreds of billions of threat events each day observed in live production environments worldwide. Independent research shows Fortinet has the industry's most extensive security device footprint. We'll start things off by examining the threats that hit the top of the charts (or surged up them) during 1H 2022.

0-day Heyday

2022 is on pace to be another record year for 0-day vulnerabilities. In the first six months of the year, we discovered 72 0-days in products from numerous vendors, including those providing software to critical infrastructure sectors. From the beginning of 2020 to June 2022, the average number of 0-days we have published every six months has consistently kept rising. Others tracking 0-day activity have reported similar trends. Google's Project Zero has similarly marked a steady increase in the number of 0-days year over year.

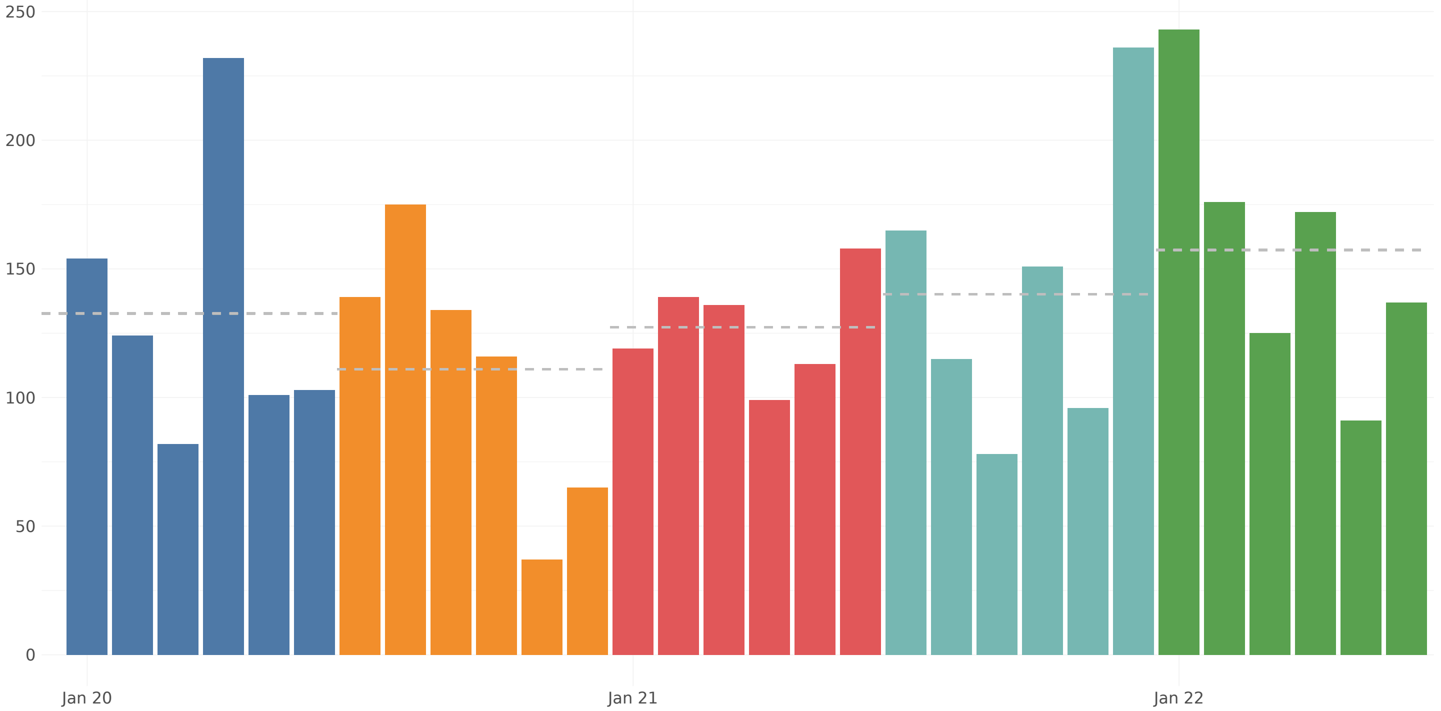


Figure 1 - Monthly counts of published 0-dayvGoogle'se's's Project Zero

Some researchers have attributed this increase to improved detection capabilities among security researchers and heightened attacker interest in finding flaws that haven't been detected yet. In many instances, the 0-days that Google identified in 2021 were similar to previous vulnerabilities and fell within popular and well-known vulnerability classes. More than two-thirds of the flaws were tied to memory corruption issues, and the rest primarily stemmed from logic and design flaws.

But regardless, the trend spells trouble for organizations because 0-days, by definition, are vulnerabilities that attackers have already exploited – or at least know about – before a patch is made available. 0-day bugs, especially in widely used products, give attackers a way to compromise enterprise networks and remain hidden until the vulnerability is discovered, which can sometimes take months.

The first half of 2022 served up several examples of such vulnerabilities. One was “MSDT Follina,” a remote code execution vulnerability in the Microsoft Support Diagnostic Tool (CVE-2022-30190). It gave attackers a trivially easy way to compromise systems via Office documents. Security researchers reported several threat actors – including nation-state-based groups – exploiting the flaw in data-theft campaigns and dropping ransomware such as Qakbot on target networks.

CVE-2022-24521, Microsoft Windows’ Common Log File System (CLFS) driver, was another major 0-day bug in H1, 2022. Microsoft issued a fix for the vulnerability in April after researchers from the US National Security Administration (NSA). Another 0-days that garnered attention in 1H, 2022 was CVE-2022-26134, an unauthenticated code execution vulnerability in Atlassian’s Confluence Server and Data Center technology. Attackers exploited this vulnerability to drop web shells, ransomware, and cryptominers on vulnerable systems. And CVE-2022-26925, a spoofing vulnerability in Microsoft Local Security Authority (LSA) function, gave threat actors a way to force domain controllers to authenticate to them.

Twenty-four of the 72 0-days we discovered in the first half of 2022 were memory corruption vulnerabilities in Siemens’ PADS Standard/Plus Viewer design flow technology. Five of them were rated as being of critical severity, and four as important. The FortiGuard Zero Day program is crucial because we’re trying to discover this before the bad actors can inflict any damage.

There is little one can do to prevent zero-day vulnerability attacks on their network. The efforts must be focused on proper visibility, instrumentation of devices, zero trust access, and quick responses to the incident. One of the only things you can do to prevent zero-day attacks is to deploy anti-exploit technologies on your devices, which can be implemented by FortiClient.

Exploits (IPS)

The Cybersecurity & Infrastructure Security Agency’s (CISA) Known Exploit Vulnerability (KEV) resource has started emphasizing the risk of vulnerability exploitations and how important it is for organizations to not only work to recognize where they may be vulnerable but also to create and execute a plan to mitigate those vulnerabilities as they are often used to gain initial access to critical systems. Exploits show us what criminals are probing and generally focused on, so it’s incredibly important to keep our fingers on the pulse here and implement granular segmentation to prevent secondary downloads and lateral movement.

We look at IPS triggers captured by FortiGuard Intrusion Prevention System (IPS) sensors to find exploit activity. These provide unrivaled visibility into how threat actors find vulnerabilities, exploit their targets, and build a malicious infrastructure. In the parlance of the popular MITRE ATT&CK framework, these detections correspond to the Reconnaissance, Resource Development, and Initial Access techniques. FTNT introduced FortiRecon in Q1 to help CISOs get an outside-in view of their organization and alert on any vulnerability or Brand reputation exposure.

So, let’s take a moment to look at the top 20 exploits for this half of 2022.

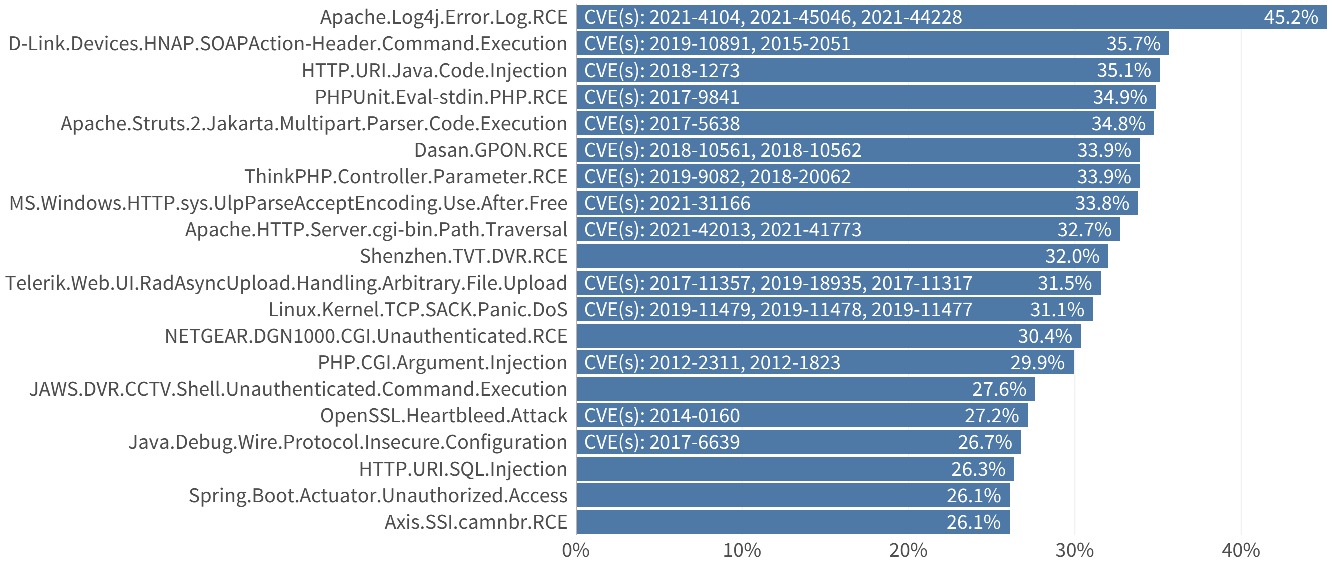


Figure 2 – Prevalence of top IPS detections for 2022-H1

We might all be tired of hearing about Log4j, but our fatigue didn't slow it down. Even the Cyber Safety Review Board wrote a review of the initial 2021 Log4j event, saying, "The Log4j event is not over. Log4j remains deeply embedded in systems, and even within the short period available for our review, community stakeholders have identified new compromises, new threat actors, and new learnings." A lot of the exploit activity targeting the Apache Log4j vulnerability in 2022 involved VMWare Horizon systems, prompting the US-CERT to issue a warning.

Although the number of exploits was lower than first expected, several attacks have used this vulnerability throughout the first half of this year. In March 2022, vulnerabilities in the Animal Health Emergency Diagnostic System (USAHERDS) made it possible for a cyberespionage campaign by APT41 to gain access to multiple US government systems. So, what is USAHERDS used for? It's a tool that helps states track and trace animal diseases through livestock populations. Healthcare is another industry that illustrates how prolonged and impactful the Log4j vulnerability is and will continue to be. Since the vulnerability is found in so many fundamental systems, it can be extremely difficult to update one system without breaking other parts of the system in the process. Cybercriminals will exploit anything and everything that can get them the initial access to the data or action they desire to achieve. We'll most likely continue to see Log4j on our "top" charts for a long time. This is an excellent testament to the importance of vulnerability assessments and active and virtual patching.

Vulnerabilities at the Endpoints

This section provides deeper insight into what happens at the endpoint, leading to more information, visibility, and control around a particular device.

What do we mean when we talk about endpoints? Any device or application connected to your network is considered an endpoint. Our endpoint data reports primarily on workstations. So, when we look at trends around endpoint vulnerabilities and how to secure them, we start to unravel a rather complex matrix of applications, programs, and devices that all live and operate on one network.

Before we dive into looking at vendors with the most-targeted endpoint vulnerabilities, it's important to note that in this sample, we detected roughly 15.3k CVEs of the 180k+ CVEs published by the FIRST Exploit Prediction Scoring System (EPSS). We're an active part of FIRST EPSS, a "data-driven effort for estimating the likelihood (probability) that a software vulnerability will be exploited in the wild."

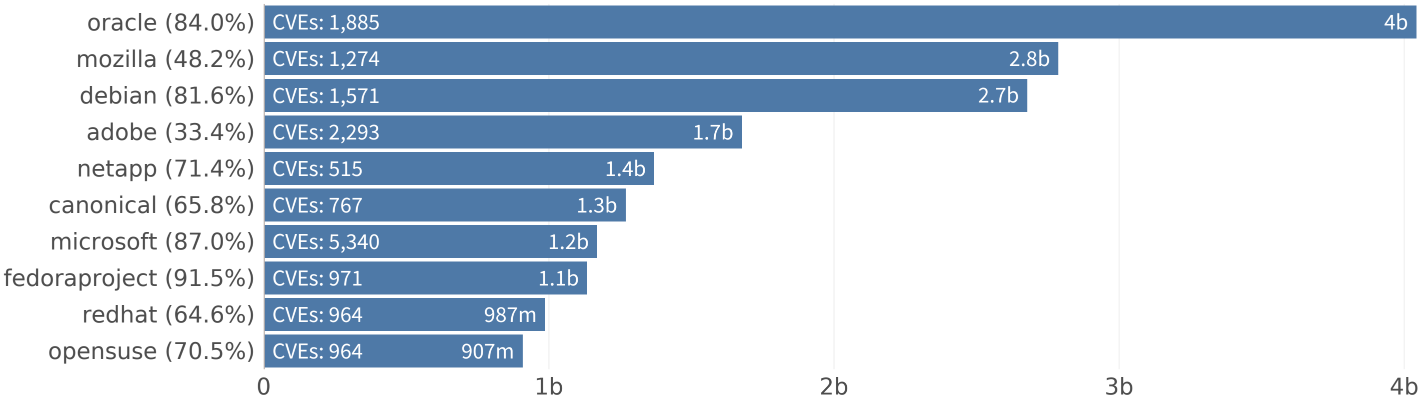


Figure 3 – Volume of endpoint vulnerabilities by vendor in 2022-H1

As mentioned above, this visualization is just a slice of all the activity. The top three platforms of endpoint vulnerabilities by volume that we observed are Oracle (predominantly related to JRE and JDK with a sprinkling of MySQL), Mozilla, and Debian. But you can also see each vendor's prevalence across devices in parenthesis. Many of these vendors have endpoint vulnerabilities centered around unauthorized users gaining access to a system.

People see new IPS data all the time, and one of the first big questions they always ask is, "why does this matter?" They ask the same question when they see new vulnerability information. This question is usually answered when a criminal successfully finds their way into a vulnerable system.

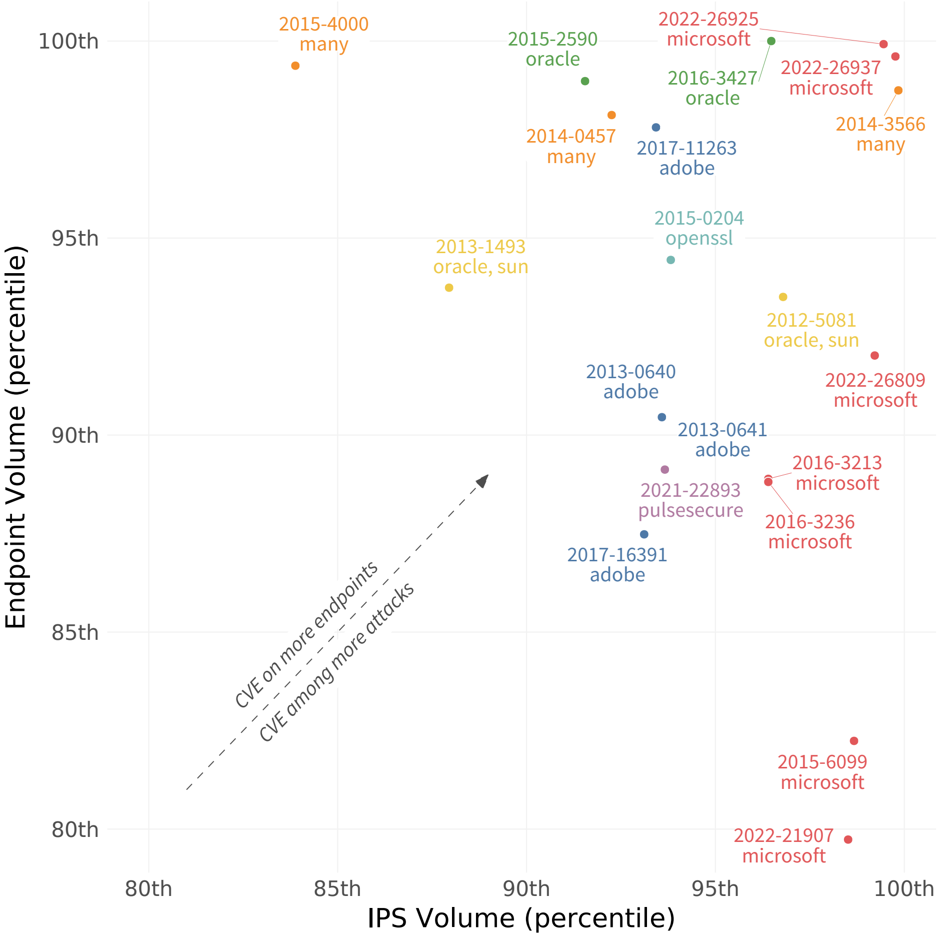


Figure 4 – Comparing CVEs by IPS activity and endpoint detections

Let's take a moment here to understand what we're explicitly talking about when it comes to endpoints and vulnerabilities. Not every exploit is related to a vulnerability (meaning no CVE was assigned), and not every vulnerability has a public PoC exploit. Vulnerability IDs are how we group volume measurements. However, it's not quite as simple as that. In some cases, one vulnerability ID can map to multiple CVEs, as is the case with a vulnerability ID created as an umbrella term that can catch different implementations of that vulnerability across multiple solutions. That being said, if you see something on the chart below that ranks high on IPS, there is a pretty good chance that it could be related to something on the top of IPS. So let's now dive a little deeper into why this matters.

Above, we see data from both the Endpoint and IPS, where a CVE can be mapped to BOTH data sets. So, what does that mean? Many endpoints have these vulnerabilities and many attackers are trying to exploit them, giving us a rough batting lineup of what we might see in the upcoming months.

Looking at those at the top right, CVE 2022-26925 is a spoofing vulnerability that places high in volume among other CVEs on both axes, and close to it is CVE 2022-26937, which is a Remote Code Execution vulnerability. CVE 2014-3566 may ring a bell for the old-timers in the crowd. It's the infamous SSLv3 vulnerability known as "POOD." While we can never truly predict what criminals will hit next (that crystal ball sure would be nice), this gives us a good indicator of where criminals are starting to sniff around and are getting warmer. Endpoint technology can help mitigate and effectively remediate infected units early in an attack. Endpoint vulnerabilities can be used for early access to the organization's infrastructure with the goal of moving laterally to a more profitable location. This is why coordinating endpoint, network, and cloud threat intelligence is so effective in preventing and responding to attacks across multiple stages and the reason for our Fabric Mesh architectural design.

Vulnerabilities in OT

Operational Technology (OT) products are highly targeted both for financial and political gain. In May 2022, we discovered and reported 24 0-days in Siemens products. This is in addition to the 56 vulnerabilities that impacted OT devices from 10 different vendors published by OT: ICEFALL earlier this year.

Many OT devices (hardware and software that help monitor and control physical devices) are considered insecure by design. What do we mean by insecure by design? Well, most OT devices are assumed to work on secure or private networks where trusted access is enabled by default (air-gaped). Designers often use this assumption when releasing new hardware or software because their goal is to make the system work more efficiently. But the design process is often function-oriented and lacks security. There have been too many instances where these designed-in vulnerabilities have been exploited for real-world attacks. As a result, we can no longer assume that any network is secure. This is why it's so important to keep OT in mind, especially when it comes to looking at vulnerabilities and 0-days.

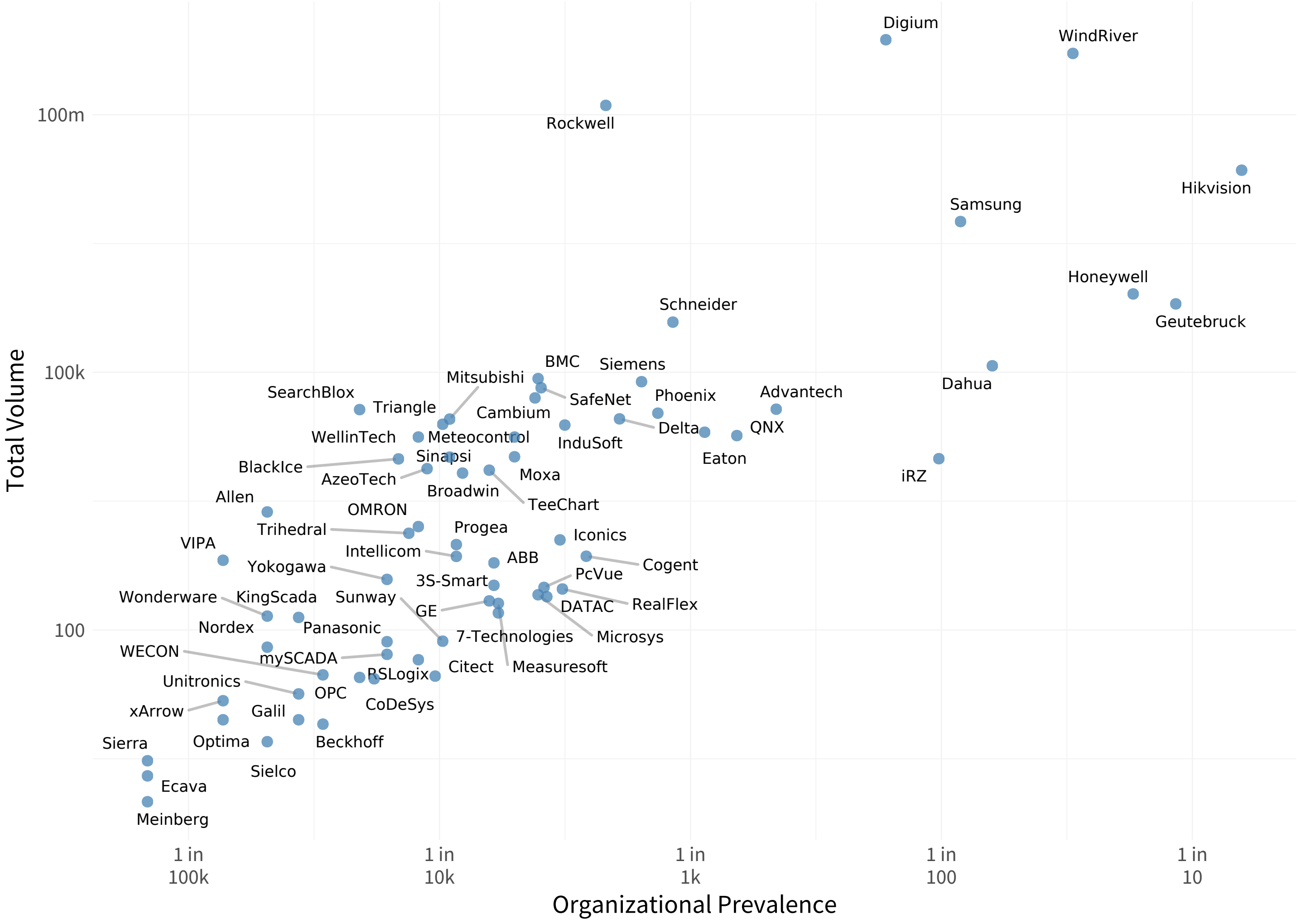


Figure 5 - Prevalence and volume of exploits targeting OT in 2022-H1

Looking at the visualization above, we see the prevalence of vulnerabilities found on OT devices. We can see that while most organizations tend to be pretty close to each other, there are some outliers, like Hikvision and Geutebruck. Taking a look through this visualization lets you scope out the OT your organization uses and take note of areas that might need an extra layer of security, both through visibility into OT-specific protocols and OT-specific vulnerabilities and patching.

Malware Delivery Mechanisms

Once threat actors find an exploitable vulnerability, their next step is often to deliver malware so they can get whatever they are after. There are many methods and vectors for delivering malware, often undetected, into systems - basically making a "hacker's choice" when thinking about what platforms they'll use. So let's take a moment to look at the most prevalent malware delivery mechanisms over the past six months.

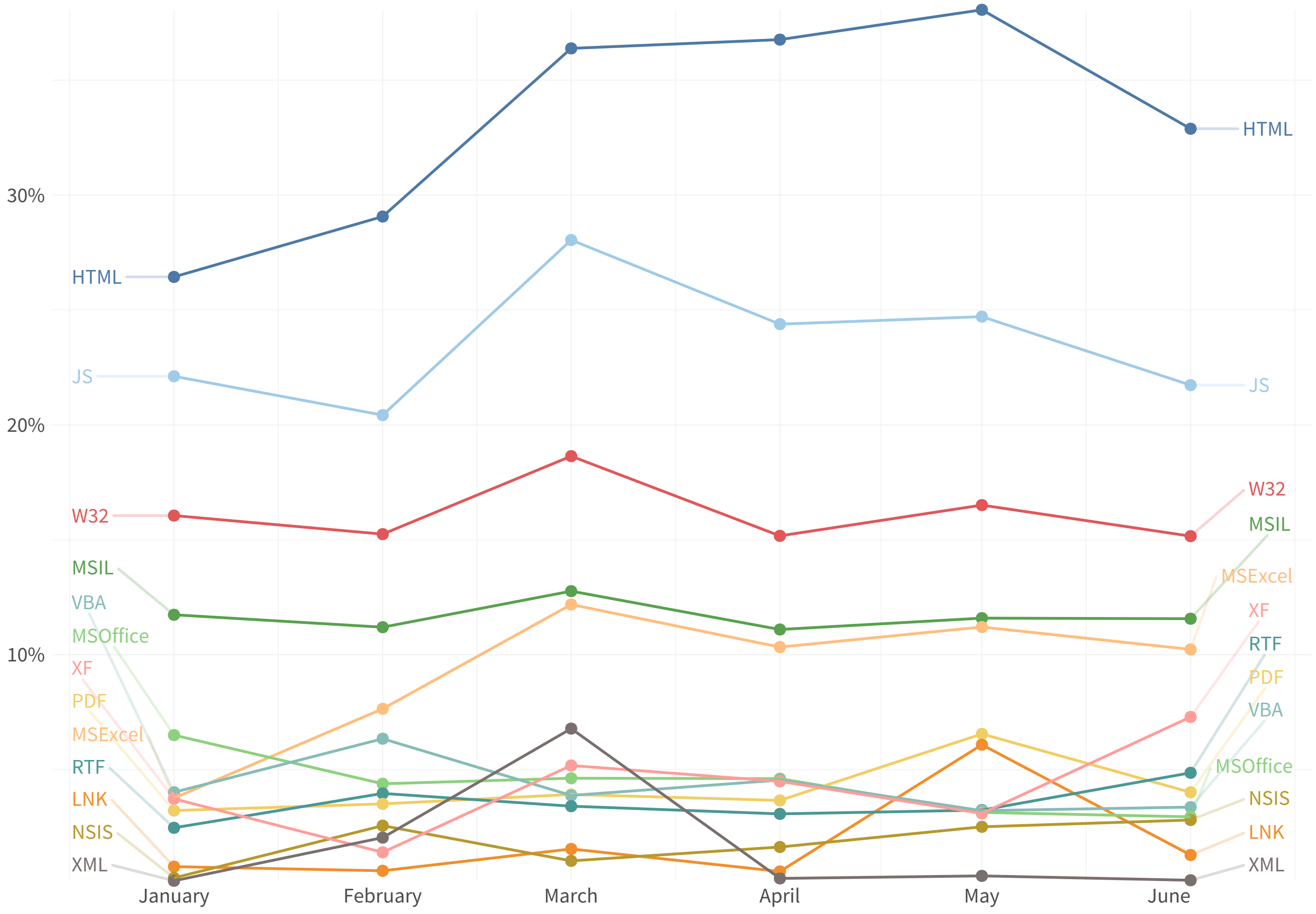


Figure 6 - Monthly prevalence of malware delivery mechanisms in 2022-H1

HTML is the most prevalent way to deliver malware, with an almost 10% difference between it and JS. This isn't super surprising. However, it looks like every platform typically remained pretty consistent - apart from XML, which saw a slight jump in March and then a plunge back in April. This is expected since malware developers typically specialize in and use one malware delivery platform.

So, now that we understand what platforms are being used to deliver malware, let's look into the top variants for each leading platform.

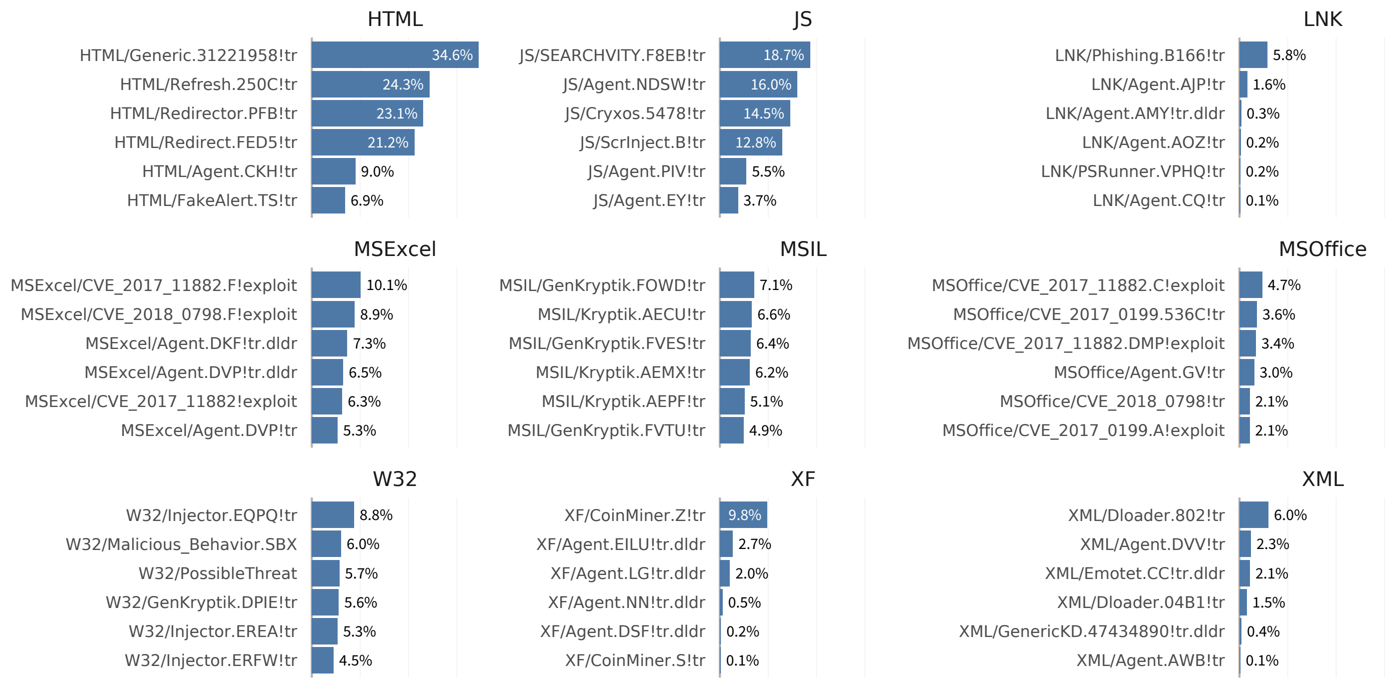


Figure 7 - Top malware variants by major platform in 2022-H1

HTML & JS are the pack leaders here, although LNK also places high. There is now a malicious framework for deploying malware with LNK extensions, making it easier to carry out this type of attack. LNK is a Shell item that points to and opens another application, folder, or file. eXcelForumla, or XF, is an Excel formula virus that works by infecting excel spreadsheets. In this instance, CoinMiner was identified by FortiGuard Labs as a trojan that "performs activities without the user's knowledge. These activities commonly include establishing remote access connections, capturing keyboard input, collecting system information, downloading/uploading files, dropping other malware into the infected system, performing denial-of-service (DoS) attacks, and running/terminating processes."

One platform you don't see in the data above is Linux. While certainly not among the most prevalent, that doesn't mean it can't make an impact. Most Linux-based malware attacks these days are cryptomining-related. In addition, the attackers leveraging this type of delivery mechanism often use it to stage attacks, automate authentication attacks, or have attacks persist after an identified vulnerability has been exploited. So let's take a quick moment to peek a little deeper into what threats are most prevalent on the Linux platform.

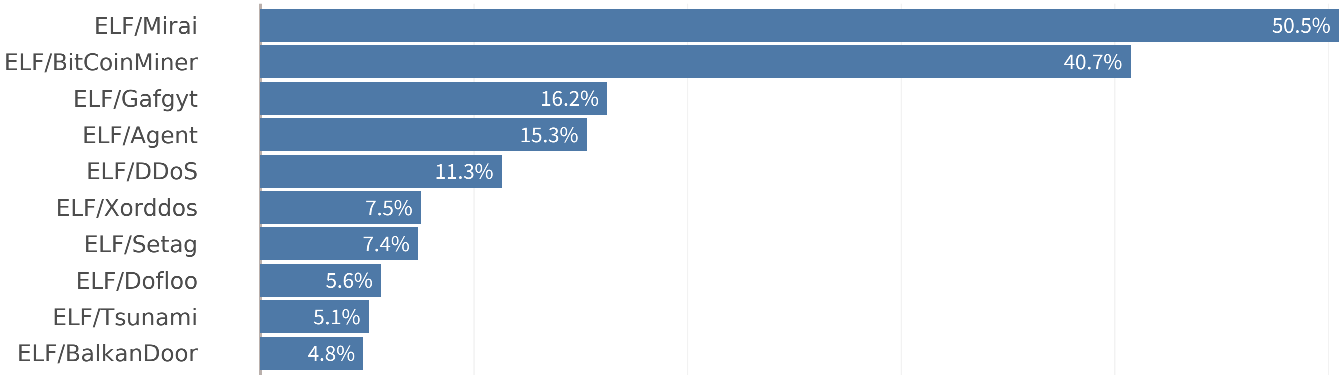


Figure 8 - Most prevalent ELF malware detections in 2022-H1

When we compare the volume of overall Linux activity with what we know about Linux-based malware attacks, it's no surprise to find Mirai topping the chart. Despite first appearing on the malware scene in 2016, this botnet continues to be heavily used, exploited, and updated six years later. Reflecting more recent trends, we also see BitCoinMiner as the next most prevalent ELF variety. A smattering of other threats follows, each with relatively low volume, including Agent, DDoS, and Tsunami. Low volume doesn't always mean low impact, however. So, let's look at other ELF detections that may have more insight into other things leveraging Linux.

While we can see that Miner samples are far and away the most common ELF detections, a few ransomware samples also utilize Linux – AvosLocker, Hive, and Vigorf. AvosLocker is a popular ransomware program typically sold and spread as Ransomware-as-a-service (RaaS) on the dark web. While AvosLocker was first spotted in July 2021, its ability to allow criminals to manipulate and target the malware as they see fit makes it hard for businesses and entities to address. Vigorf, another ransomware variant, found its momentum in March of 2022 and passed up both Hive (ransomware) and Miner malware in June in terms of count. Stealthworker, a Golang-based malware discovered in 2019 that relies on brute force, also continues to be seen, albeit in very small numbers.

Tactics and Techniques – TTPs

If you find yourself with malware on one of your systems, your SOC team can contain a compromised unit if they can detect and respond to it in near real-time. This typically involves recognizing malicious functionality. However, in the case of AvosLocker, even that might not even be good enough since AvosLocker is known for operating in "Safe Mode," making it very good at avoiding detection.

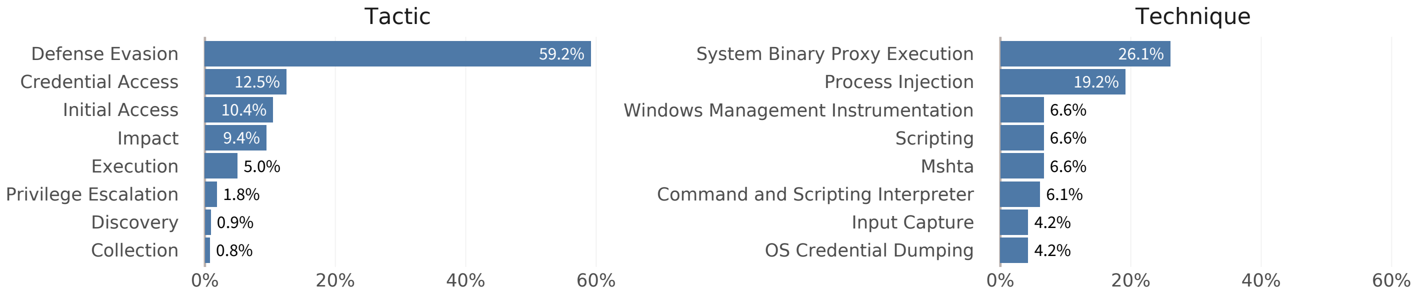
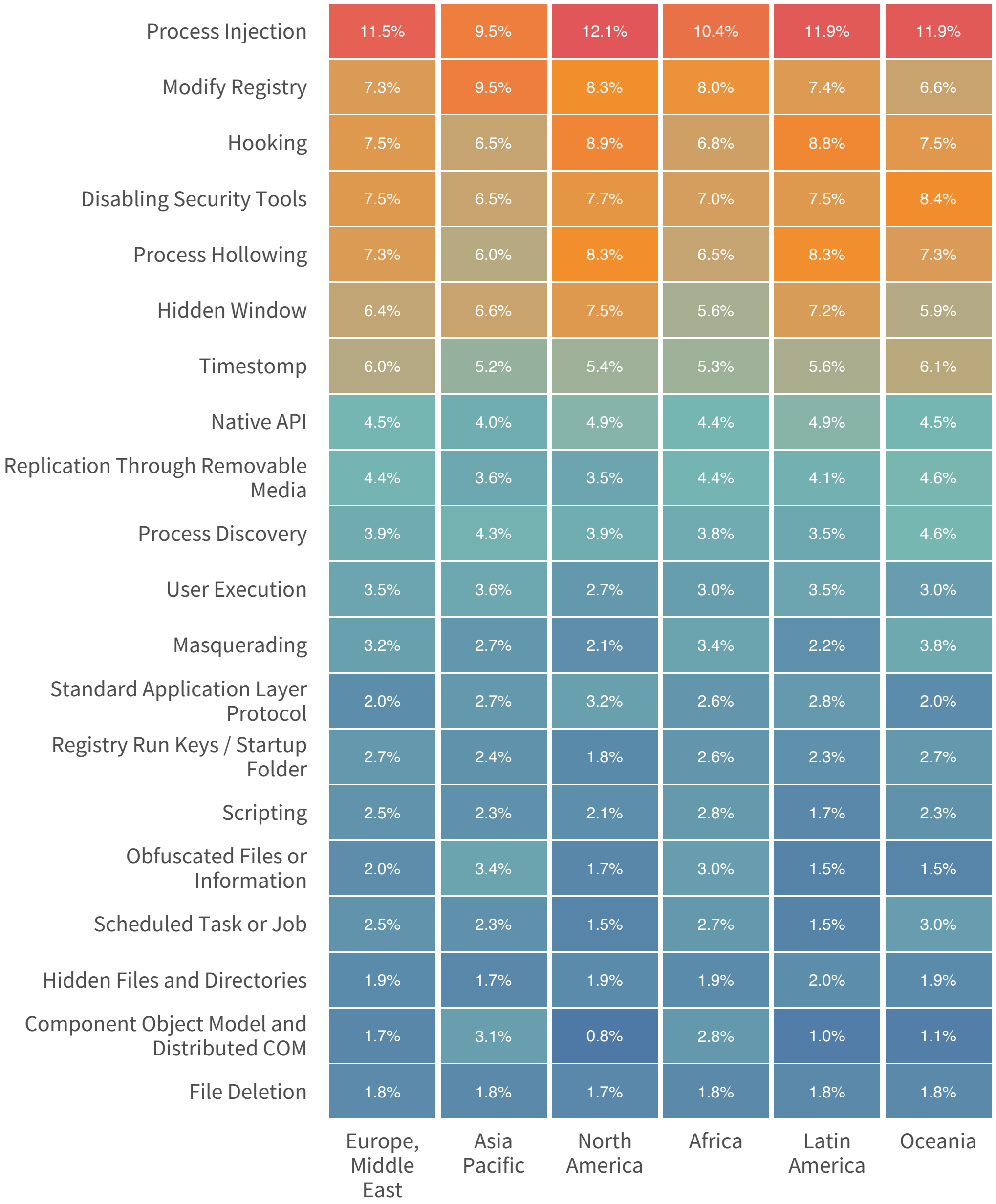


Figure 9 - Top malware tactics and techniques in EDR data for 2022-H1

Looking at the top eight tactics and techniques from the past six months of EDR telemetry, defense evasion is the top tactic employed by malware developers. They are also the most likely to use system binary proxy execution to do so. Hiding malicious intentions is one of the essential things for malware developers to master, so it makes sense that they would try to mask their malware by using a legitimate certificate to hide commands to evade a business's defenses. Process injection, where the criminal works to inject code into a process to evade defenses, is the second most popular technique we've seen over the past six months.

By looking at detonated malware samples from the FortiSandbox Cloud, which includes data sent to it by various Fortinet solutions, we can also look for regional differences across techniques.



	Europe, Middle East	Asia Pacific	North America	Africa	Latin America	Oceania
Process Injection	11.5%	9.5%	12.1%	10.4%	11.9%	11.9%
Modify Registry	7.3%	9.5%	8.3%	8.0%	7.4%	6.6%
Hooking	7.5%	6.5%	8.9%	6.8%	8.8%	7.5%
Disabling Security Tools	7.5%	6.5%	7.7%	7.0%	7.5%	8.4%
Process Hollowing	7.3%	6.0%	8.3%	6.5%	8.3%	7.3%
Hidden Window	6.4%	6.6%	7.5%	5.6%	7.2%	5.9%
Timestomp	6.0%	5.2%	5.4%	5.3%	5.6%	6.1%
Native API	4.5%	4.0%	4.9%	4.4%	4.9%	4.5%
Replication Through Removable Media	4.4%	3.6%	3.5%	4.4%	4.1%	4.6%
Process Discovery	3.9%	4.3%	3.9%	3.8%	3.5%	4.6%
User Execution	3.5%	3.6%	2.7%	3.0%	3.5%	3.0%
Masquerading	3.2%	2.7%	2.1%	3.4%	2.2%	3.8%
Standard Application Layer Protocol	2.0%	2.7%	3.2%	2.6%	2.8%	2.0%
Registry Run Keys / Startup Folder	2.7%	2.4%	1.8%	2.6%	2.3%	2.7%
Scripting	2.5%	2.3%	2.1%	2.8%	1.7%	2.3%
Obfuscated Files or Information	2.0%	3.4%	1.7%	3.0%	1.5%	1.5%
Scheduled Task or Job	2.5%	2.3%	1.5%	2.7%	1.5%	3.0%
Hidden Files and Directories	1.9%	1.7%	1.9%	1.9%	2.0%	1.9%
Component Object Model and Distributed COM	1.7%	3.1%	0.8%	2.8%	1.0%	1.1%
File Deletion	1.8%	1.8%	1.7%	1.8%	1.8%	1.8%

Figure 10 - Prevalence of techniques by region in FortiSandbox Cloud data in 2022-H1

Defense Evasion with Process Injection had a moment in all regions where it was the most prevalent technique. Take a moment to look through the heat map to see what may be impacting your region the most.

Managing threats, tactics and techniques, and up-and-coming vulnerabilities might feel like treading water in the open ocean – you can't touch the bottom, and you don't know when the next boat will pass by. But the more we become aware of the surrounding landscape, the better prepared we can be when the next storm starts to brew.

Ransomware Roundup

Ransomware feels like it is spreading in prevalence, but sometimes that can be hard to quantify. Are we just hearing more stories about it? Or is it genuinely becoming more popular?

Well, the answer to that second question is most definitely yes.

Over the past six months, we have documented 10,666 ransomware variants across our platform, compared to just 5,400 in the previous six-month period. That's a nearly **2x growth** in variants in half a year.

So, what's behind it?

One of the biggest drivers is Ransomware-as-a-Service (RaaS). RaaS has become increasingly popular on the dark web, with developers utilizing different technologies to build subscription model services for their plug-and-play ransomware. This allows even novice cybercriminals to target people, businesses, and other organizations for a quick payday. That's right, just like your favorite subscription service lets you stream your favorite shows, order your favorite foods, or even visit your favorite places, RaaS gives criminals access to ransomware and other malicious software for a commission or monthly price.

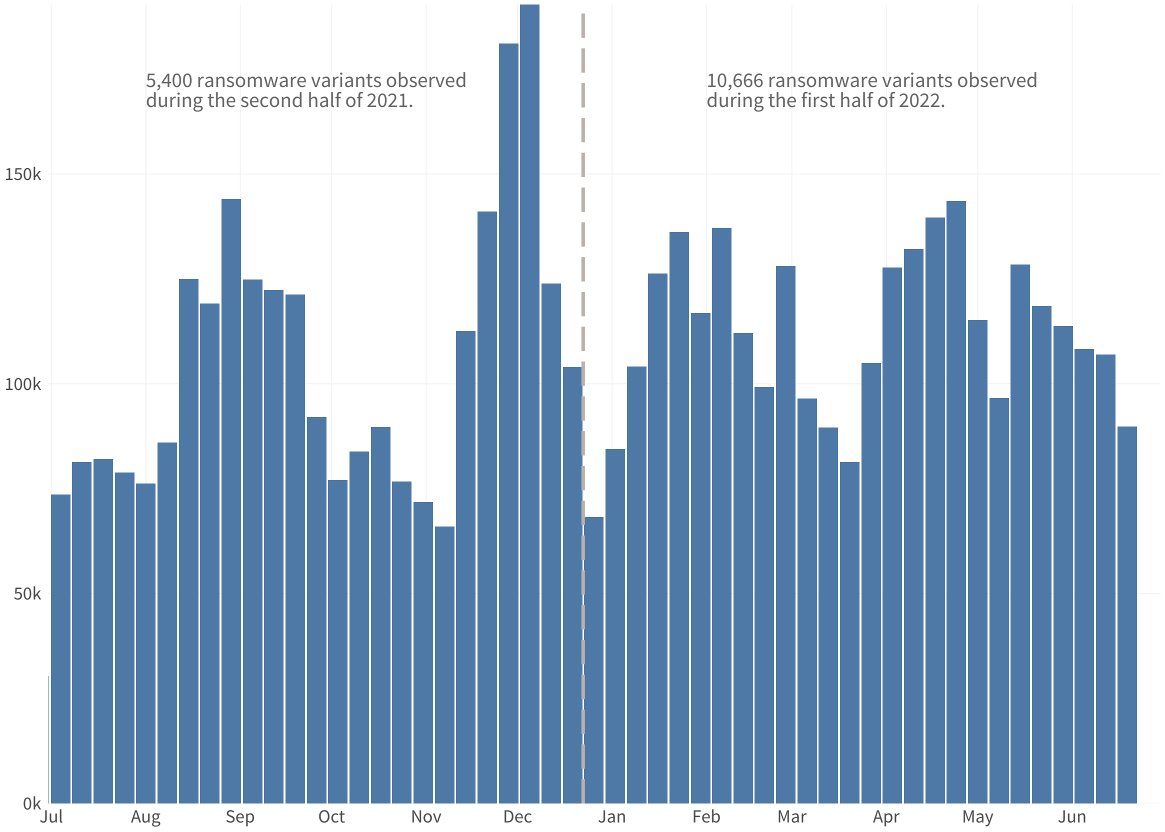
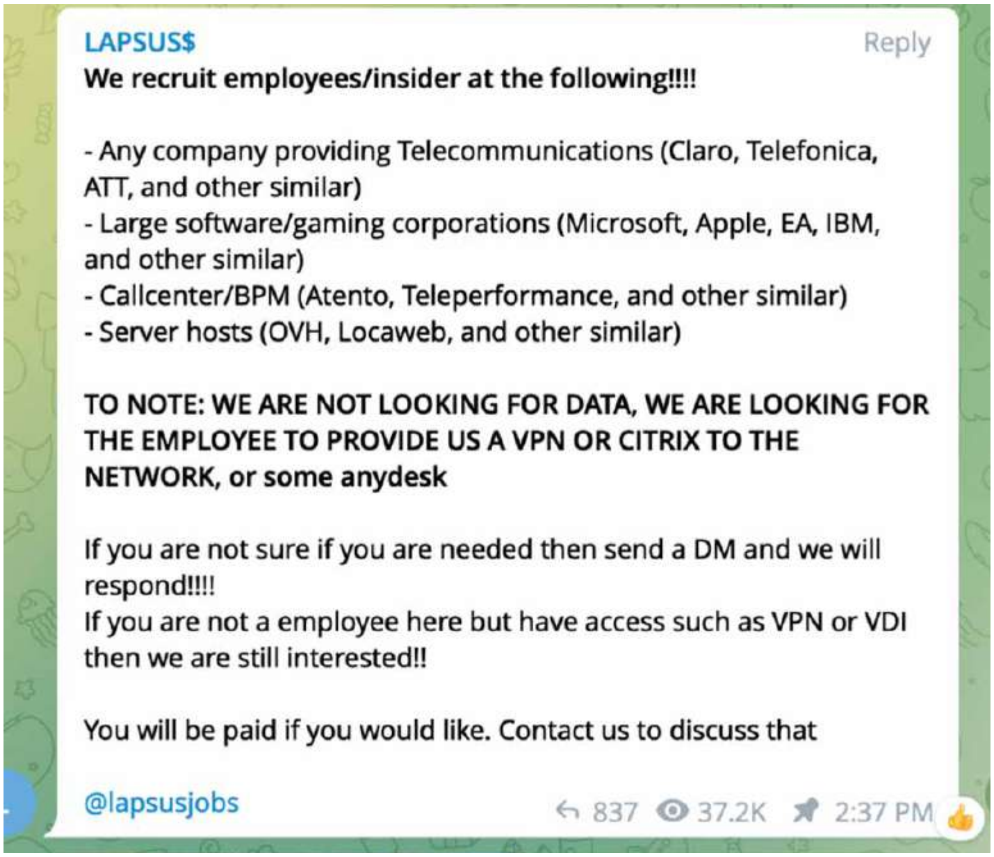


Figure 11 - Weekly ransomware volume over the last 12 months

We're continually investing in ML-based analytics and other detection tactics for ransomware and other types of malware to keep ahead of the evolving threat landscape. After observing the 10.7X growth in average weekly devices from July 2020 to June 2021, activity appears to have stabilized at its elevated levels. A "new normal," if we dare say it.

Despite some significant law-enforcement successes, like the international effort to take down the RaaS operation REvil (also known as Sodinokibi), ransomware operators continue to be a significant threat to organizations, regardless of size or industry. However, while the REvil takedown sent ripples across the RaaS market, there have also been some notable ransomware campaigns that have stepped up to fill the void.

Lapsus$ first popped onto the extortion scene in December 2021 after it breached the Brazilian Health Ministry's computer systems. The group then quickly went after large companies, including LG, Microsoft, and T-Mobile, to name a few. According to Microsoft, Lapsus$ used social engineering techniques to facilitate account takeovers and infiltrate target systems. Microsoft also found instances where Lapsus$ gained access by recruiting and paying targeted company employees to allow them to take over their accounts.



LAPSUS$

We recruit employees/insider at the following!!!!

- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)

TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk

If you are not sure if you are needed then send a DM and we will respond!!!!
If you are not a employee here but have access such as VPN or VDI then we are still interested!!

You will be paid if you would like. Contact us to discuss that

@lapsusjobs

(source: Microsoft - https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction)

However, many noticed that the people behind Lapsus$ might be inexperienced, with whispers that it was just a bunch of kids since they would frequently brag about an attack as it was happening. On March 24th, UK law enforcement arrested seven people, ages 16 - 21, in connection with Lapsus$.

Conti, a RaaS group that has been around since 2020, used spearphishing campaigns with tailored emails that contained malicious attachments or malicious links to infiltrate a victim's network, according to CISA. Conti actors were also known for exploiting remote managing and monitoring software to help evade detection. In June 2022, Conti shut down its last two remaining TOR servers - breaking up the gang. However, it is expected that their operations will continue, just as smaller spin-off groups.

Ransomware, exploitation, and attacks on the supply chain will continue to dominate headlines due to their notoriety and disruptive nature, so we shouldn't expect them to disappear anytime soon.

A New Wave of Wipers

The war in Ukraine fueled a substantial increase in disk wiping malware used by threat actors. We identified at least seven major new wiper variants surfacing in the first six months of 2022 that were used in various targeted campaigns against government, military, and private organizations in Ukraine. The number is significant because that's almost as many wiper variants that have been publicly detected in total since 2012 when an attacker used the Shamoon wiper to brick tens of thousands of computers at Saudi Aramco and Qatar's RasGas operations.

Security researchers believe—but have not always been able to attribute with confidence—that groups aligned with Russian military goals were behind many of the wiper attacks in Ukraine during the first half of 2022. One example is CaddyWiper, a variant used to wipe data and partition information from drives on systems belonging to a limited number of Ukrainian organizations soon after the war began. Other examples include WhisperGate, a wiper that Microsoft discovered being used in attacks against Ukrainian entities in January 2022; HermeticWiper, a tool for triggering boot failures that SentinelLabs found being used in similar attacks; and IsaacWiper, a malware tool for overwriting data in disk drives as well as attached storage to make them inoperable. The three other wipers we observed in the first half of 2022 targeting Ukrainian companies and infrastructure were WhisperKill, DoubleZero, and AcidRain.

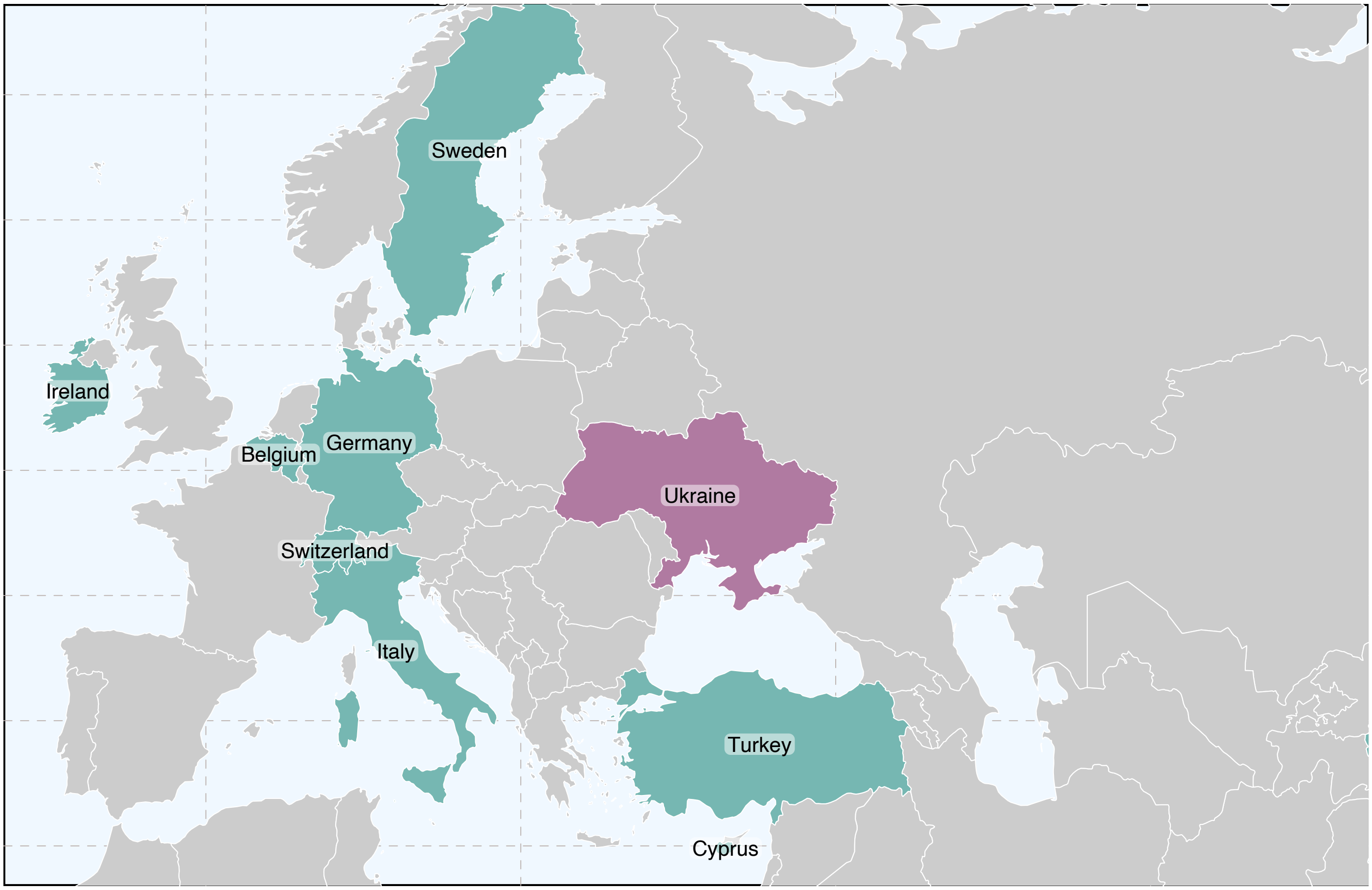


Figure 12 - Countries detecting wipers associated with the Russia-Ukraine war

One surprising aspect of these attacks is how many also spilled over to other countries, just as they have done during previous periods of conflict in the region. We have detected more wiper malware outside Ukraine than within the country since the war began in February 2022. The activity of these wipers was detected in 24 countries besides Ukraine during the year's first half. One example is AcidRain, a wiper used to target a Ukrainian satellite broadband service provider, but that also ended up being used in an attack that knocked nearly 6,000 wind turbines offline in Germany. Attacks like these demonstrate a capacity to jump boundaries, whether between countries or IT and OT.

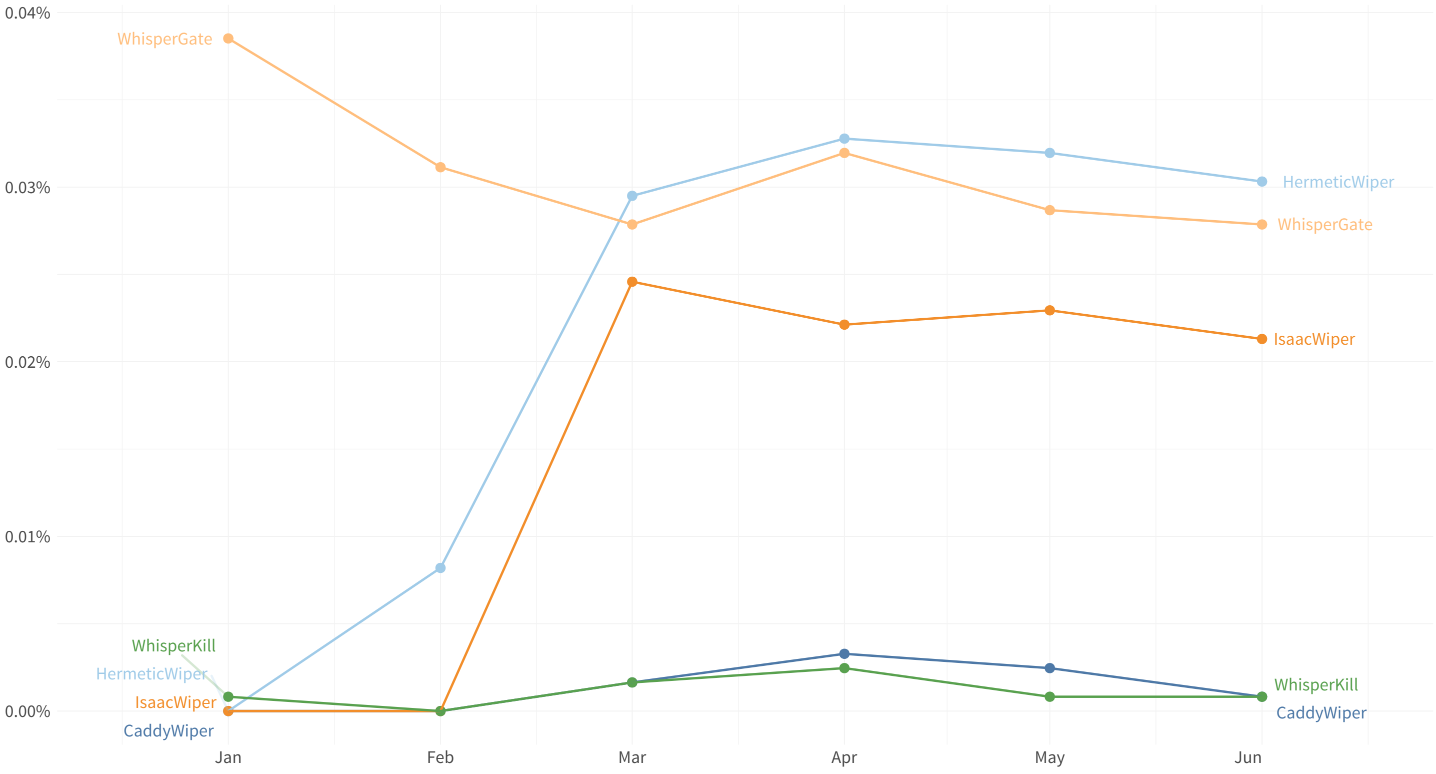


Figure 13 - Monthly prevalence of wipers associated with the Russia-Ukraine war

This sudden explosion in wiper malware spells trouble for enterprise security teams. Though the number of detections has been low so far, the nature of the malware and how threat actors use them makes this category particularly dangerous and something that security teams need to be vigilant about. Our analysis of wiper malware has shown that adversaries use it to support varied objectives, including attacks for financial gain, sabotage, destruction of evidence, and cyberwar.

In February, the US Cybersecurity and Infrastructure Security Agency (CISA) warned of the direct threat that wipers can present to daily operations and noted how the attacks in Ukraine could touch organizations in other countries. “Organizations should increase vigilance and evaluate their capabilities encompassing planning, preparation, detection, and response for wiper attacks,” the CISA warned.

The attacks in Ukraine have shown how this malware can be used to degrade and disrupt critical infrastructure capabilities and services to support broader kinetic warfare goals. But that is not the only threat. Shamoon showed how wipers can be used as weapons of cyber sabotage, and other variants, such as NotPetya and GermanWiper from 2017, showed how adversaries can use wipers as fake ransomware to try and extort money from victims.

Ending on a High Note

Cybercriminals will never let an opportunity go to waste. Whether it's a vulnerability, exploit, or even a war, someone is always trying to cause harm for profit. We want you and your business to feel confident in your ability to protect yourself against the growing volume and variety of threats that continue to come our way.

Fortinet continues to seek and develop technologies and products to address the needs at different layers of every security architecture. To keep you and your organization aware and prepared to respond to the ever-changing cyber threat landscape, here are some top-of-mind recommendations that Fortinet can help you with:

1. **Assessments, Training & Patching:** FortiRecon can be used to do external surface threat assessments, find and remediate security issues, and help you gain contextual insights on current and imminent threats. Our NSE Institute Training covers everything from cybersecurity basics to expert knowledge of all Fortinet solutions. For help with patching, this report has more than enough information to help you prioritize the patches needed to secure your environment.
2. **Endpoint security:** Fortinet has an extensive portfolio of technologies to help secure your endpoints, from vulnerability and patching to anti-exploit technologies. This can help address your need to detect and protect against zero-day vulnerability attacks.
3. **Centralized Data, Analysis, and Response:** Security is a big data problem, and finding the needle in the haystack is what catches the most advanced attacks. Detecting and correlating data from the endpoint, cloud, and network is paramount to stopping these attacks in their tracks.
4. **ZTNA:** Controlling access more granularly to application devices and networks is one of the most powerful things you can do to limit the extent of a breach in your enterprise environment.
5. **ML-Based Security Technology Adoption:** Machine learning is a game changer for all industries, including cybersecurity. For the past seven years, Fortinet has been working on implementing ML and AI in all products where it's deemed applicable. Machine learning has been woven into our products, including endpoint, cloud, and network-based solutions. This technology allows us to better capture the rapid changes in the threat landscape and help organizations triage and prioritize security incidents.

We hope the data and insights included in this report can help guide your security planning and strategy. We look forward to updating you with the latest insights into the threat landscape in our next edition!

August 15, 2022 9:32 AM

1471550-0-0-EN