FEBRUARY 2022

Global Threat Landscape Report

A Semiannual Report by FortiGuard Labs

TABLE OF CONTENTS

Overview and Key Highlights

With any new year, there's always a temptation to leave the past behind and press on to new and hopefully better times ahead. But as the saying goes, "Those who don't learn history are doomed to repeat it." We want to help you to avoid that doom as we look back on the cyber threat landscape during the latter half of 2021 through our global array of sensors monitored by FortiGuard Labs. Here's what we learned:

Sizing up Log4j

Despite emerging in the second week of December, exploitation activity escalated quickly enough to make it the most prevalent IPS detection of the entire half! But how does it compare to other headliner vulnerabilities of the past? In less than a month, the Log4j RCE managed nearly 50x the activity of 2021's other darling, ProxyLogon, measured by peak 10-day average volume.

ELF on a Shelf

Threat actors are moving Linux-based malware closer and closer to the top shelf in their collection of nefarious tools. Detections of ELF files (binary format for Linux) doubled during 2021 and the rate of new signatures created for our AV sensors quadrupled! This doesn't look like a friendly holiday tradition.

Ransomware Changed Stride

After a 10.7x increase over the prior 12 months, ransomware prevalence across our sensors remained at an elevated level over the latter half of 2021. But while overall detections might not be spiking as they did in the past, the sophistication, agressiveness, and impact of this threat charged on.

More Pangs for Exchange

Exploits targeting a set of four vulnerabilities in Microsoft Exchange Server hit many organizations where it hurts in the first half of the year. Unfortunately, the pain didn't stop in the latter half, with several more "Proxies" emerging to erase any chance of relief.

Baby Got Hack

A remote access flaw in a popular baby monitor attracted the interest of more than just concerned parents. It rose high in the ranks of new exploits and served as the latest reminder that the myriad of connected things in our homes—even those we rely on for the safety of our most vulnerable family members—come with a risk.

On the ATT&CK

Understanding adversaries' goals is crucial to defending against the flood of changing techniques they may use. By focusing on a handful of techniques, you can effectively shut down malware's methods of choice for getting in and making itself at home. Check out the technique breakdowns by region and industry to see if you've got your bases covered!

Top Threats During 2H 2021

The findings in this report represent the collective intelligence of FortiGuard Labs, drawn from a vast array of network sensors collecting billions of threat events each day observed in live production environments around the world. According to independent research, Fortinet has the largest security device footprint in the industry. This unique vantage offers excellent views of the cyber threat landscape from multiple perspectives that we're glad to share with you. We'll start things off by examining the threats that hit the top of the charts (or surged up them) during 2H 2021.

IPS Detections

IPS activity captured by the FortiGuard Intrusion Prevention System (IPS) sensors running on our FortiGate firewalls provides unrivaled visibility into how threat actors find vulnerabilities, exploit their targets, and build malicious infrastructure. In the parlance of the popular MITRE ATT&CK framework, these detections correspond to the Reconnaissance, Resource Development, and Initial Access techniques. Figure 1 presents the top monthly targets of exploit activity over the second half of 2021.

Figure 1 demands that we begin at the end of the year with a little-known remote code execution (RCE) vulnerability that affects a popular Java library called Log4j2 (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105). The sarcasm should be evident there, because literally everyone in the cybersecurity industry is aware of the Log4j 0-Day exploit; more than a few lost a lot of sleep and logged a lot of overtime because of it.

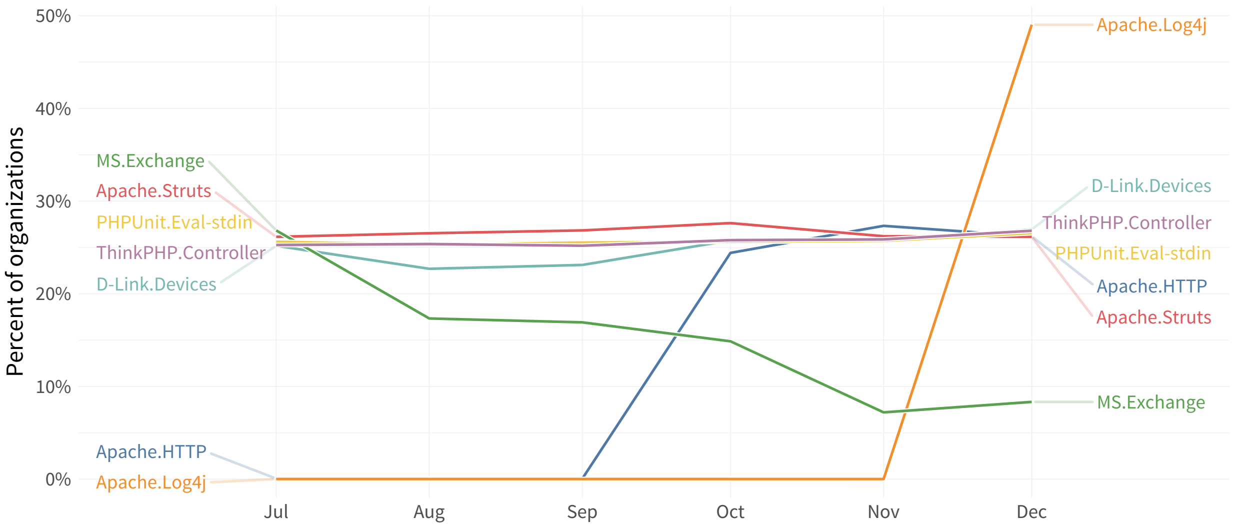


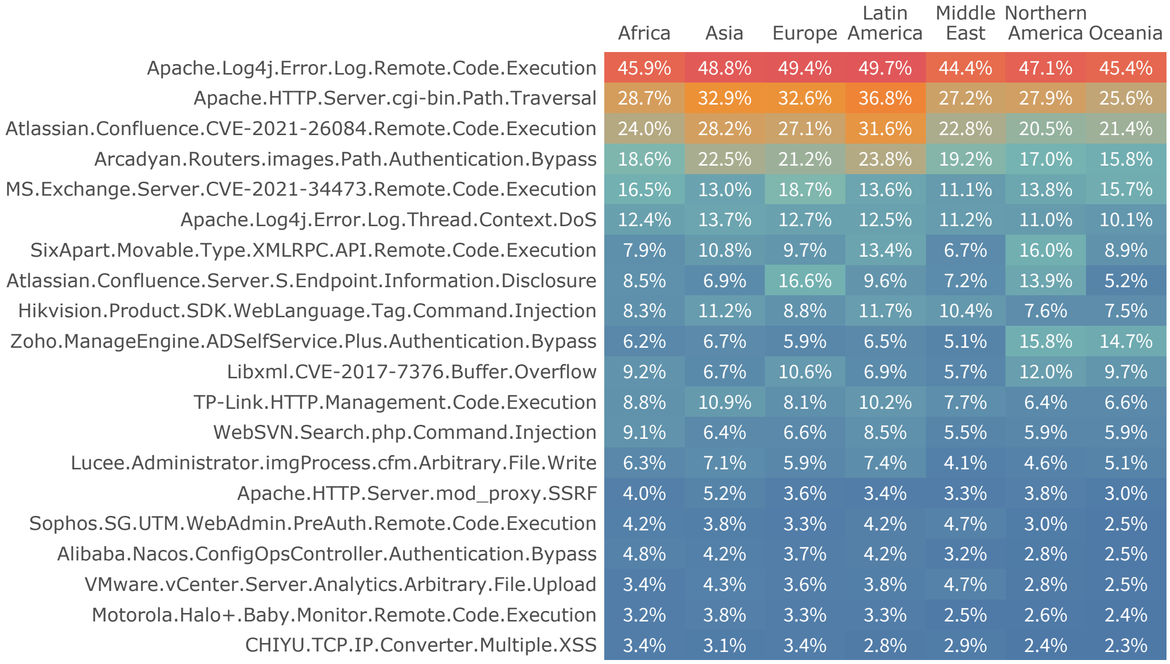
Figure 1: Prevalence of top IPS detections by technology during 2H 2021.

Despite emerging in the second week of December, exploitation activity escalated quickly enough to make it the most prevalent IPS detection of the half! These detections were logged by nearly 50% of organizations running FortiGuard IPS. To put that in perspective, the next highest on the list—another Apache exploit (CVE-2021-42013, CVE-2021-41773)—was detected by 31% of organizations. There's a dedicated story on Log4j later in this report, so we'll keep it at that for now.

We see another RCE vulnerability, the infamous "ProxyLogon" that affected Microsoft Exchange Server (CVE-2021-26855), atop the list back toward the beginning of the half (see our 1H 2021 report on "The ProxyLogon Feeding Frenzy"). A slew of additional Exchange vulnerabilities dropped in 2021 with nifty names like ProxyShell, ProxyToken, and ProxyOracle, and their exploitations ramped up over the latter half of the year. They also warrant a story of their own in this report, so be sure to check that out if you're curious which came out on top.

Beyond those headliners, we see entries from familiar consumer-grade networking and Internet-of-Things (IoT) devices (e.g., Dasan, D-Link). Just because they're familiar doesn't mean they're unimportant, mind you. The lines between personal and corporate networks are blurred with so many working from home, and threat actors are looking to exploit that trend. It's a big reason why "Attacks on the Edge" made our top 5 threats to watch in 2022.

In addition to the most common IPS detections overall, we wanted to keep an eye on potential up-and-comers. Figure 2 facilitates that by listing the most prevalent exploits of the last six months that had no activity in the six months prior. With the exception of the code execution flaw in TP-Link.HTTP, all were created since July 2021. The chart also compares the prevalence of those chart climbers across regions. We've already discussed several of the exploits from Figure 2, so we'll highlight a few that only appear here.



	Africa	Asia	Europe	Latin America	Middle East	Northern America	Oceania
Apache.Log4j.Error.Log.Remote.Code.Execution	45.9%	48.8%	49.4%	49.7%	44.4%	47.1%	45.4%
Apache.HTTP.Server.cgi-bin.Path.Traversal	28.7%	32.9%	32.6%	36.8%	27.2%	27.9%	25.6%
Atlassian.Confluence.CVE-2021-26084.Remote.Code.Execution	24.0%	28.2%	27.1%	31.6%	22.8%	20.5%	21.4%
Arcadyan.Routers.images.Path.Authentication.Bypass	18.6%	22.5%	21.2%	23.8%	19.2%	17.0%	15.8%
MS.Exchange.Server.CVE-2021-34473.Remote.Code.Execution	16.5%	13.0%	18.7%	13.6%	11.1%	13.8%	15.7%
Apache.Log4j.Error.Log.Thread.Context.DoS	12.4%	13.7%	12.7%	12.5%	11.2%	11.0%	10.1%
SixApart.Movable.Type.XMLRPC.API.Remote.Code.Execution	7.9%	10.8%	9.7%	13.4%	6.7%	16.0%	8.9%
Atlassian.Confluence.Server.S.Endpoint.Information.Disclosure	8.5%	6.9%	16.6%	9.6%	7.2%	13.9%	5.2%
Hikvision.Product.SDK.WebLanguage.Tag.Command.Injection	8.3%	11.2%	8.8%	11.7%	10.4%	7.6%	7.5%
Zoho.ManageEngine.ADSelfService.Plus.Authentication.Bypass	6.2%	6.7%	5.9%	6.5%	5.1%	15.8%	14.7%
Libxml.CVE-2017-7376.Buffer.Overflow	9.2%	6.7%	10.6%	6.9%	5.7%	12.0%	9.7%
TP-Link.HTTP.Management.Code.Execution	8.8%	10.9%	8.1%	10.2%	7.7%	6.4%	6.6%
WebSVN.Search.php.Command.Injection	9.1%	6.4%	6.6%	8.5%	5.5%	5.9%	5.9%
Lucee.Administrator.imgProcess.cfm.Arbitrary.File.Write	6.3%	7.1%	5.9%	7.4%	4.1%	4.6%	5.1%
Apache.HTTP.Server.mod_proxy.SSRF	4.0%	5.2%	3.6%	3.4%	3.3%	3.8%	3.0%
Sophos.SG.UTM.WebAdmin.PreAuth.Remote.Code.Execution	4.2%	3.8%	3.3%	4.2%	4.7%	3.0%	2.5%
Alibaba.Nacos.ConfigOpsController.Authentication.Bypass	4.8%	4.2%	3.7%	4.2%	3.2%	2.8%	2.5%
VMware.vCenter.Server.Analytics.Arbitrary.File.Upload	3.4%	4.3%	3.6%	3.8%	4.7%	2.8%	2.5%
Motorola.Halo+.Baby.Monitor.Remote.Code.Execution	3.2%	3.8%	3.3%	3.3%	2.5%	2.6%	2.4%
CHIYU.TCP.IP.Converter.Multiple.XSS	3.4%	3.1%	3.4%	2.8%	2.9%	2.4%	2.3%

Figure 2: Prevalence of new and fastest-growing IPS detections by region (% of organizations).

Let's start with a vulnerability in Atlassian's popular web-based wiki, Confluence. A new OGNL injection vulnerability associated with CVE-2021-26084 was the prime offender. Attackers jumped to attention soon after the bug was announced, and it wasn't long before threat actor Atom Silo targeted vulnerable Confluence servers to deliver ransomware. The Cybersecurity and Infrastructure Security Agency (CISA) thought it important enough to release an advisory urging prompt remediation.

Zoho ManageEngine ServiceDesk Plus (CVE-2021-40539) also bears mention. According to a joint advisory from CISA and the Federal Bureau of Investigation (FBI), successful exploitation allows an attacker to upload executable files and place webshells for post-exploitation activities, such as compromising administrator credentials, conducting lateral movement, and exfiltrating registry hives and Active Directory files. Per Figure 2, exploitation activity was highest in North America and Oceania (mainly Australia). The same agencies had previously released an advisory in September on another Zoho vulnerability (CVE-2021-44077). This Threat Signal gives our assessment and protections for it.

A trio of new VMware vulnerabilities (CVE-2021-21985, CVE-2021-21980, CVE-2021-22005) pushed the virtualization platform into the ranks of the up-and-comers for the second half of 2021. Exploits targeting the first CVE racked up the most detections and VMware concurred that it was critical, urging customers to make patching it a top priority. Activity was fairly evenly distributed around the world but reached the highest points in the Middle East and Asia.

And last but not least, exploit activity targeting Motorola Halo+ video baby monitors (CVE-2021-3577) caught our attention. We don't recall a baby monitor making this high up the list before. Hackers invading our *cribs* (homes) is nothing new … but literal cribs?! That's not right on a whole new level. We look into this new level of privacy invasion further in the "Baby Got Hack" featured story.

Malware Detections

Samples picked up by our various anti-malware solutions offer insight into popular adversary tools for establishing a foothold, escalating privileges, and moving laterally within corporate environments. Malware is truly the multi-tool of choice among actors of all types as they can use multiple techniques in the ATT&CK Matrix from Execution through Impact.

Figure 3 presents the top "Rookie of the Half" candidates in each region. Malware signatures appearing in this chart were created some time during 2021 and are among each region's ten most prevalent detections across devices during the last six months of 2021.

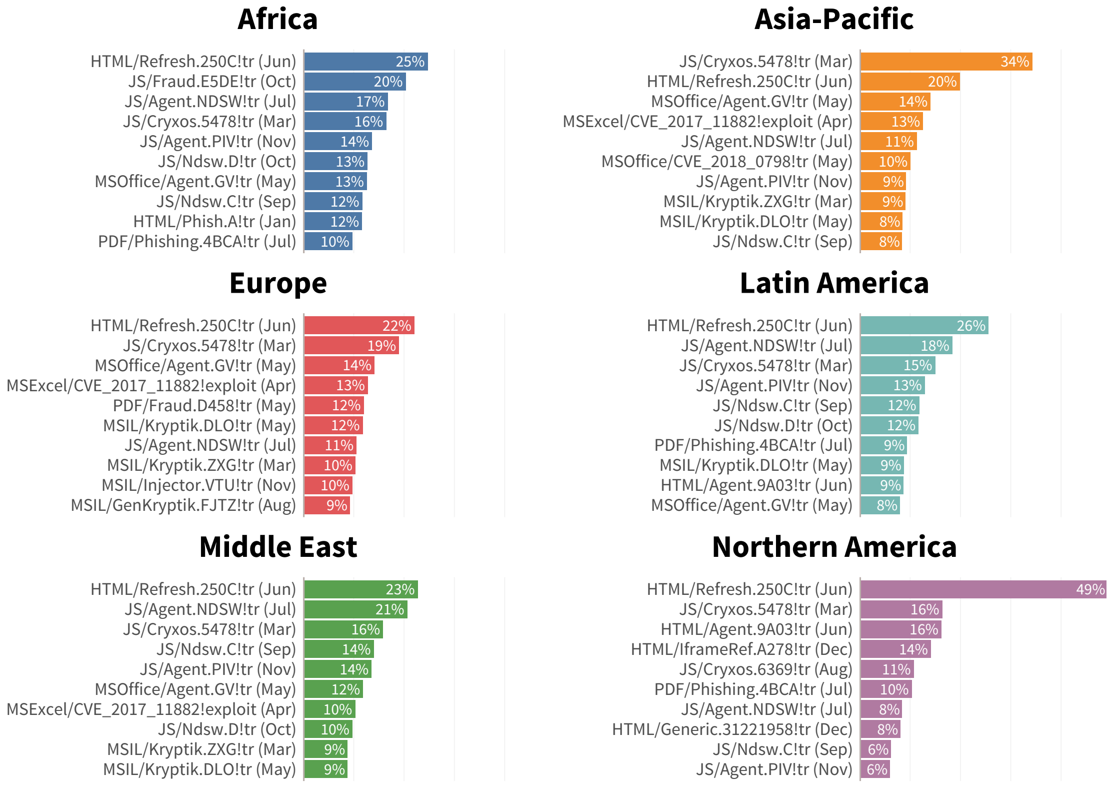


Figure 3: Prevalence of recent malware variants by region during 2H 2021 (% of organizations).

Detections vary across regions, of course, but can be largely grouped into three broad distribution mechanisms: Microsoft Office executables (MSExcel/, MSOffice/), PDF files, and browser scripts (HTML/, JS/). Files packed with the Microsoft Intermediate Language (MSIL) are another common target.

We find it noteworthy that various forms of browser-based malware occupy the top spots in all regions. This often takes the form of phishing lures and scripts that inject code or redirect users to malicious sites. Such techniques have risen in popularity of late as a way to exploit people's desire for the latest news about COVID-19, politics, sports, or any headline du jour. And since many are browsing from their home networks these days, there are fewer layers of protection between such malware and would-be victims (e.g., no corporate web filters).

ELF on a Shelf

Keep in mind, however, that not all important threats reside at the top of the current charts. Some lesser or low-lying threats have the potential to cause bigger problems and are thus worthy of watching. One such trend we're keeping an eye on is malware designed to exploit Linux systems, often in the form of Executable and Linkable Format (ELF) binaries. Linux runs the back-end systems of many networks and container-based solutions for IoT devices and mission-critical applications, and it's becoming a more popular target for attackers.

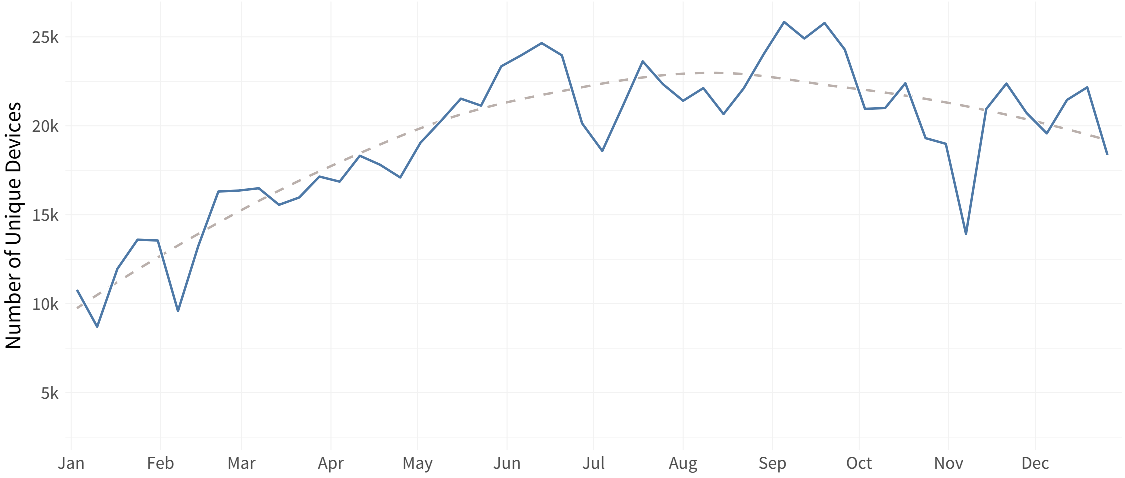


Figure 4: Number of unique devices detecting ELF files targeting Linux systems during 2021.

As can be seen in Figure 4, the prevalence of ELF and other Linux malware detections across our sensors doubled during 2021. And the rate of new Linux malware signatures distributed to our AV sensors in Q4 of 2021 quadrupled that of Q1. That's not exactly a meteoric rise, but it's not something to ignore either. Such growth in variants and spread suggests that Linux malware is moving up in the cyber adversary arsenal.

The most common ELF variant has ties to Muhstik, a Linux malware that turns infected machines into bots and is known to exploit vulnerabilities for propagation. One notable Muhstik exploit is the aforementioned Confluence flaw that saturated our IPS sensors. See our analysis of that malware for more information.

We also observed botnet activity associated with a new variant of the RedXOR malware, which targets Linux systems for data exfiltration and leapt into our top 10 list in October. A malicious implementation of the Beacon feature of Cobalt Strike called Vermilion Strike can target Linux systems with remote access capabilities. Log4j is another example of a recent attack where we are seeing Linux binaries being used to capitalize on the opportunity.

Now that Microsoft is actively integrating Windows Subsystem for Linux (WSL) into Windows 11, it's inevitable that malware will follow. WSL is a compatibility layer that is used for running Linux binary executables natively on Windows. All that to say—there's ample evidence and plenty of reasons why continued increase in Linux attacks made our list of predictions for 2022.

Botnet Detections

Whereas IPS and malware trends usually show the pre-compromise side of cyber threats, botnets give a view of post-compromise activity. Once infected, systems often attempt to communicate with remote hosts, making this traffic an important part of monitoring the full scope of malicious activity. In ATT&CK parlance, botnet traffic is most indicative of Command and Control (C2) TTPs.

One recurring lesson from this data is that the most successful botnets are remarkably consistent over time. Those most prevalent across our sensors tend to remain the same over time, in large part because persistent control is a prized commodity among cybercriminals and much work goes into preserving their investment in their malicious infrastructures.

For that reason, we've decided to base Figure 5 on the volume of botnet traffic detected rather than the prevalence-oriented view we typically use. The top 10 botnets are shown such that the thickness of the colored streams corresponds to total volume of C2 communications. The volume of activity clearly expands and contracts, both overall and for individual botnets. Two large swells of C2 activity associated with the Warzone remote access trojan (RAT) and the RedLine Stealer malware are easy to spot.

Before we dig into those, however, let's note that C2 activity is so top heavy that all botnets outside the top 10 fit within the comparatively thin "Everything Else" band at the bottom! Most of those seen here are familiar names. We (and many others) have given plenty of airtime to perennial top bots like Mirai (#1 based on prevalence across devices), ZeroAccess, and Pushdo over the years. Let's acknowledge their remarkable staying power (particularly in consumer and small business networks) and move on to the notable upstarts of 2H 2021.

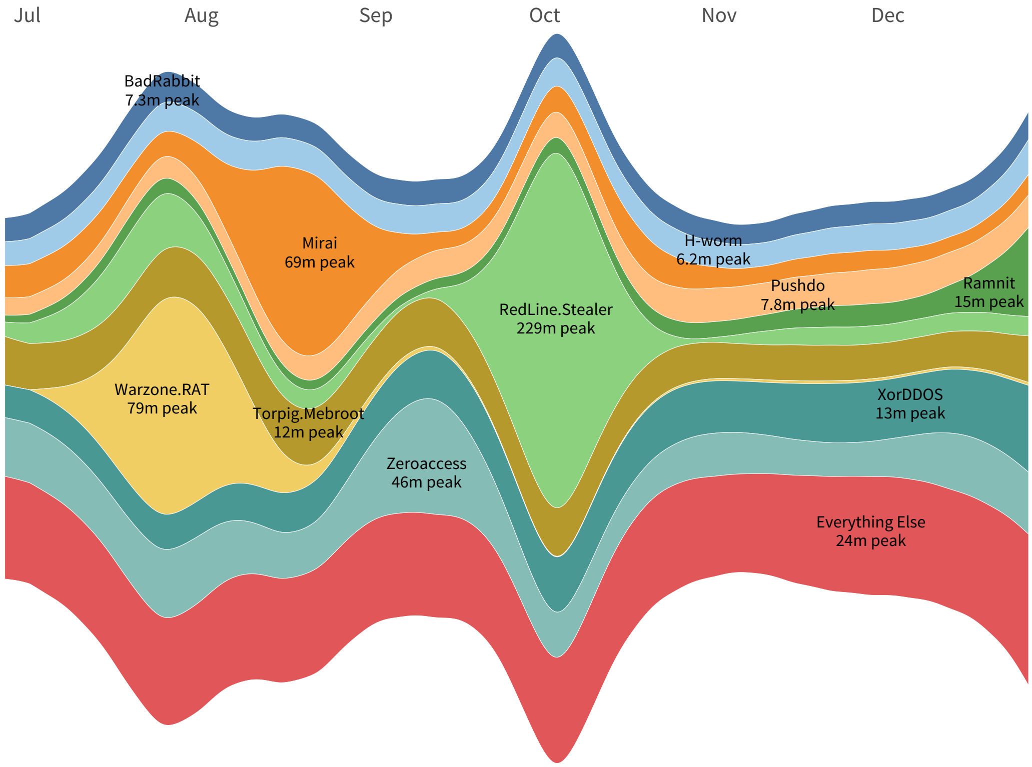


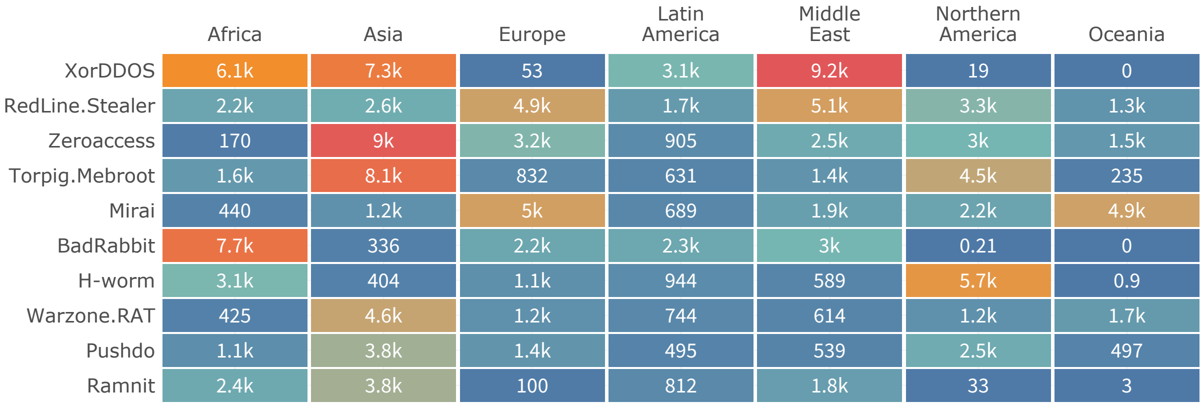
Figure 5: Weekly volume of top botnet detections during 2H 2021 (total detections).

Warzone RAT might be more aptly named "BargainZone RAT" due to its reputation as a low-cost, high-functionality Malware-as-a-Service tool. Blackberry's description of the RAT as "the choice for aspiring miscreants on a budget" captures it quite well. In an era of commoditization in cybercrime markets, Warzone has carved out a successful business model. The large swelling of botnet activity stemming from Warzone RAT infections in Figure 5 is a testament to that success.

The cause of the late July surge in the Warzone RAT botnet appears to be a spear-phishing campaign that targeted the manufacturing firms in the Asia-Pacific region. That checks out with our data as well, where related activity in Asia is four times that of any other region (see Figure 6). Fortinet Open Fabric Ecosystem member, Anomali, reports that the TTPs identified in this campaign align with the Aggah threat group.

The RedLine Stealer malware has been around since at least early 2020, with cybercriminals using it to nab credentials from infected systems. Information harvested by RedLine Stealer is sold on the darknet marketplace for as low as 10 US dollars per set of user credentials. The malware emerged just as COVID-19 infections spread around the world, and the RedLine Stealer developers preyed on the ensuing fear and uncertainty as bait for its own spread.

Figure 5 attests to the virulence of RedLine Stealer, as related botnet traffic surged in late September through early October. Figure 6 makes it clear that activity was highest in the Middle East and Europe. One might interpret Figure 5 to suggest that RedLine Stealer was a temporary outbreak that's now contained. But like the virus they take advantage of, RedLine's developers regularly morph the malware to find new victims. In fact, FortiGuard Labs recently discovered a new variant in the form of a COVID-themed file, "Omicron Stats.exe." It won't be the last.



	Africa	Asia	Europe	Latin America	Middle East	Northern America	Oceania
XorDDOS	6.1k	7.3k	53	3.1k	9.2k	19	0
RedLine.Stealer	2.2k	2.6k	4.9k	1.7k	5.1k	3.3k	1.3k
Zeroaccess	170	9k	3.2k	905	2.5k	3k	1.5k
Torpig.Mebroot	1.6k	8.1k	832	631	1.4k	4.5k	235
Mirai	440	1.2k	5k	689	1.9k	2.2k	4.9k
BadRabbit	7.7k	336	2.2k	2.3k	3k	0.21	0
H-worm	3.1k	404	1.1k	944	589	5.7k	0.9
Warzone.RAT	425	4.6k	1.2k	744	614	1.2k	1.7k
Pushdo	1.1k	3.8k	1.4k	495	539	2.5k	497
Ramnit	2.4k	3.8k	100	812	1.8k	33	3

Figure 6: Most active botnets by region during 2H 2021 (volume per org).

We'll close with a botnet that *didn't* make it into the previous figures—Emotet. In our last report, we discussed the coordinated effort by global law enforcement agencies to dismantle the botnet and the resulting decline in activity. Ten months after the takedown, Emotet proved to be only mostly-dead instead of dead-dead, experiencing some semblance of resurrection in the latter half of the year. The good news is that Emotet activity is well below what it once was and not nearly as rampant globally. For example, two-thirds of detections were limited to the region of Latin America, where activity was 25x higher than in Europe and North America. We'll call mostly-dead a win for the time being.

Featured Stories

Sizing up Log4j

Few vulnerabilities in recent years garnered as much attention or sparked so much concern industrywide as CVE-2021-44228, a critical remote code execution (RCE) vulnerability disclosed in December in the Apache Log4j Java-based logging framework. The flaw impacted nearly every environment with a Java application, was trivially easy to exploit, and gave attackers a way to gain complete control of vulnerable systems. Too often it was also excruciatingly hard to find because dependencies on Log4j could sometimes be buried multiple layers deep in applications.

On December 9, the Apache Foundation disclosed CVE-2021-44228, or 'Log4Shell' as it became known colloquially. Within days it became the most prevalent IPS detection during 2H 2021 as attackers—including several state-backed threat actors and organized criminal groups—began scanning the internet for vulnerable systems. Several security vendors reported observing threat actors—including operators of cryptominers, ransomware tools, and botnets like Mirai—integrating exploits for the Log4j vulnerability into their attack kits. Figure 7 shows the cumulative volume of activity around Log4j's first days, supplying the context needed to appreciate just how much attention it got from attackers. In just 21 days, the Log4j RCE had reached 1.4x the cumulative volume that the infamous Struts flaw (CVE-2017-5638) achieved in one year.

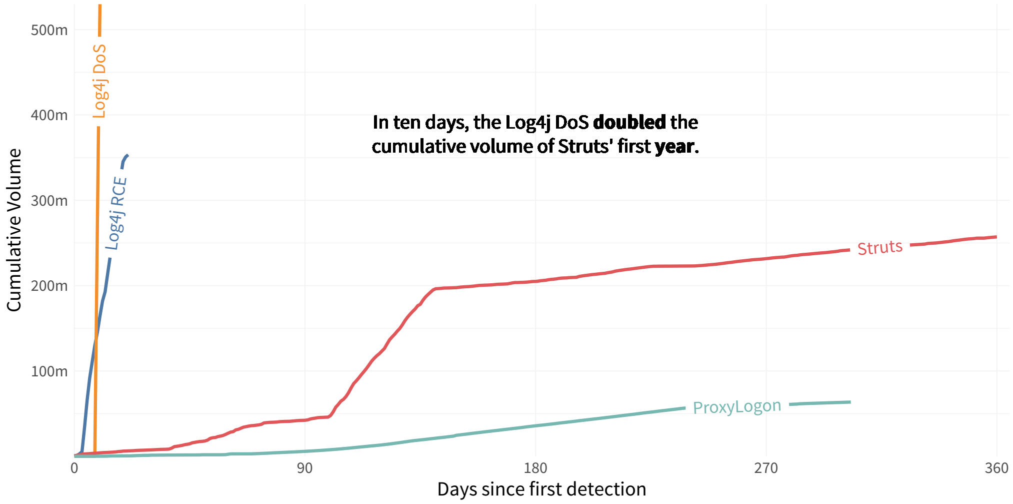


Figure 7: Comparing Log4j's cumulative volume to historic high-profile vulnerabilities.

The activity prompted concerns about widespread attacks on everything from internet-facing servers to back-end systems, network components, SCADA systems, and cloud applications. Fears were fueled by reports of exploit activity targeting the flaw occurring at least one week before the vulnerability was disclosed and a patch for it became available. In the week following the Log4Shell disclosure, the Apache Foundation reported two other bugs in the logging framework: CVE-2021-45046 and CVE-2021-45105. The flaws turned out to be not as critical as Log4Shell, but they forced organizations to update their Log4j versions three times in a single week.

Despite the wide concerns, there were no reports of major compromises involving the flaw in the month after it was discovered. Many described that as likely resulting from the defensive measures that organizations rushed to implement in the immediate aftermath of bug disclosure. Others postulate that attackers exploited the bug to breach networks and are waiting for the right time to strike. One such case from the recent past was the 2017 breach at Equifax via a vulnerability (CVE-2017-5638) in Apache Struts. The breach—which exposed data belonging to nearly 150 million individuals—happened several months after the flaw was disclosed and long after most of the initial malicious activity targeting the flaw had quieted.

The Apache Struts vulnerability was one of several flaws in recent years to evoke levels of concern similar to Log4Shell. The 'ProxyLogon' flaw (CVE-2021-26855) in Exchange Server disclosed last March is the most recent example. The authentication bypass vulnerability gave attackers a way to impersonate users and access on-premises Exchange servers and email accounts. Attackers chained the flaw with three other vulnerabilities in Exchange Server (CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065) to compromise tens of thousands of servers before Microsoft issued a patch for them. Concerns over the flaw prompted the FBI to take the unprecedented measure of removing webshells from infected systems without the owners' permission.

Only time will tell if we've witnessed the birth of the entry point into the next "mega-breach," but with history as our teacher, perhaps defenders will have adequate time and the motivation to snuff it out before it gets started.

More Pangs for Exchange

Microsoft's Exchange Server technology remained a major pain point for enterprises in 2H 2021, just as it had been in the year's first half. Exploits targeting Exchange Server vulnerabilities ranked third by volume in the second half of 2021, behind those targeting the Log4j flaw and another in Apache Struts. In July, we observed more exploits targeting Exchange Server than any other technology (see Figure 1). Much of the malicious activity in the second half was tied to several separate Exchange Server flaws dubbed 'ProxyShell', 'ProxyToken,' and 'ProxyOracle.'

ProxyShell is an exploit chain involving the use of three Exchange Server vulnerabilities (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) to remotely run malicious code on a vulnerable system. Microsoft patched the flaws as part of its monthly security updates for April and May 2021, but attackers continued to actively target the vulnerabilities throughout the year. In August the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and others warned about threat actors exploiting ProxyShell flaws to execute malicious code on internet-facing Exchange Servers.

In many of the attacks, threat actors dropped hidden webshells on compromised machines, likely for carrying out future attacks. In September we reported on a previously unknown threat actor leveraging ProxyShell to conduct active reconnaissance and to eventually establish persistence on vulnerable Exchange Servers. Fortinet's investigation uncovered a total of 22 DLLs in memory—many of them malicious—that were used as part of the attack chain. Another campaign involved a new threat actor, "Tortillas," exploiting ProxyShell to deploy a variant of the Babuk ransomware family. Some security vendors reported ProxyShell being exploited in business email compromise (BEC) attacks. At one point, more that 20,000 Exchange Servers in the U.S. alone were vulnerable to attack via ProxyShell vulnerabilities.

The ProxyToken flaw (CVE-2021-33766) disclosed last September was less severe than ProxyShell or ProxyLogon, but was another reminder of the target-rich environment that Exchange Server provides for threat actors. The security token bypass flaw gave attackers a way to create rules for forwarding emails from a target server to one they controlled, along with other ways to get it to disclose sensitive information.

Meanwhile, 'ProxyOracle' exposed yet another way for threat actors to attack Microsoft Exchange. The vulnerability consisted of two separate CVEs—a reflected cross-site scripting issue tracked as CVE-2021-31195 and a Padding Oracle attack tracked as CVE-2021-31196. Combined, the vulnerabilities gave threat actors a way to recover a user's password in plaintext just by getting them to visit a malicious link. Figure 8 shows us how tough a year it's been for Exchange Server, with a June peak of over 30% organizational prevalence for Proxy-related CVEs alone.

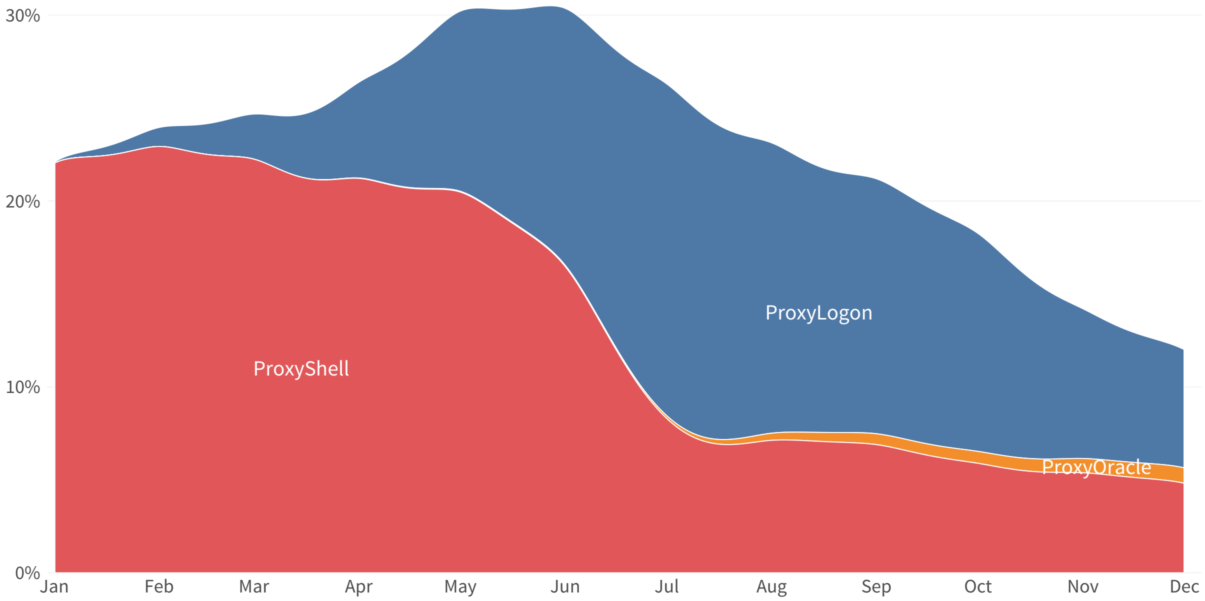


Figure 8: Monthly prevalence of IPS detections for Proxy-related CVEs during 2021.

Security researchers expect that attackers and hackers—of both the Black Hat and White Hat varieties—will continue to probe for and exploit weaknesses in Exchange Server simply because of its widespread use and the access it provides to email accounts and other sensitive data.

Ransomware Changed Stride

One of the headliner stats from our 1H 2021 report was a 10.7x increase in the number of sensors detecting ransomware variants over the 12 months prior. Upon closing the books for 2021, we were eager to see if that trend continued. Spoiler: it did not.

While we aren't seeing the spikes in ransomware activity like we have in previous reports, Figure 9 shows that ransomware prevalence across our sensors remained at an elevated level over the latter half of 2021. While the overall frequency of ransomware detections might be leveling off, the sophistication, aggressiveness, and impact of this threat rolled on relentlessly.

Threat actors continued to pound away at organizations (approximately 150,000 individual detections per week) with a variety of new and previously seen ransomware strains, often leaving a trail of destruction in their wake. Double extortion attacks, where ransomware actors steal data and use the threat of leaking it as additional leveraging for extorting ransoms, became the norm rather than the rarity it was a short while ago.

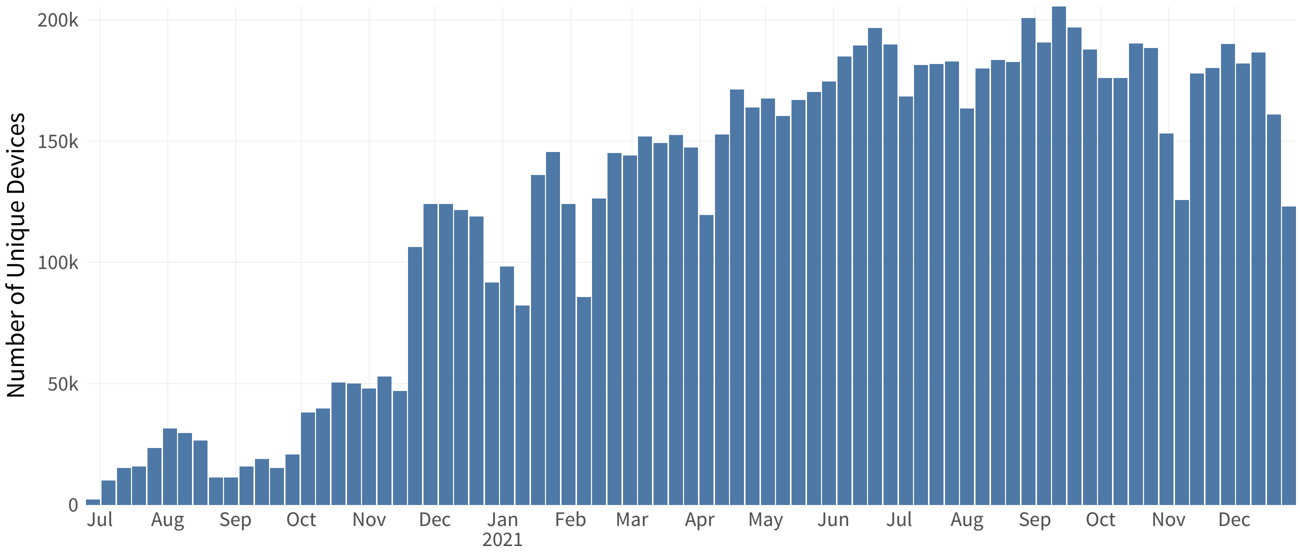


Figure 9: Weekly ransomware detections over last 18 months (Jul '20–Dec '21).

One attack in 2H 2021 on Kaseya's VSA remote monitoring and management technology attracted particular attention because of its widespread impact. A threat actor exploited an old vulnerability in VSA to deploy ransomware on systems belonging to some 50 to 60 of Kaseya's managed service provider customers who in turn infected their downstream customers. The exact number of organizations that were impacted by the attack on Kaseya remains unclear, but some have estimated the victims to number in the thousands from around the world. The incident was another troubling demonstration of the effectiveness of the breach-once-compromise-many nature of software supply chain attacks and prompted a reaction from U.S. officials that went all the way up to the White House. Many expect such attacks to increase in the future.

We observed a consistent level of malicious activity involving multiple ransomware strains in 2H 2021 including a new version of Phobos, Yanluowang, and BlackMatter, a ransomware family distributed in the wild via a Ransomware-as-a-Service model. BlackMatter surfaced soon after DarkSide—the group behind the crippling attack on Colonial Pipeline—went offline, and is believed to simply be a rebranding of the latter. The operators of BlackMatter professed they would not attack target organizations in the healthcare sector and other critical infrastructure sectors but did so anyway. A joint advisory from the FBI and CISA in October warned of BlackMatter ransomware being used in attacks against multiple U.S. critical infrastructure entities including two in the food and agriculture sector.

During the second half of 2021 we also observed a new variant of Phobos ransomware in the wild showing that the malware, which first surfaced in 2017, is still being actively updated and developed. Meanwhile Yanluowang, ransomware that surfaced around August last year, has been observed attacking several U.S. organizations, particularly those in the financial services, engineering, manufacturing, and IT services sectors. The operator of the malware previously used to distribute another ansomware family called ThiefLock. According to one security vendor, there is a likelihood that the operators of Yanluowang will adopt a Ransomware-as-a-Service model, which multiple threat actors could soon use to distribute the malware.

There were also multiple attacks targeting VMware ESXi hypervisor technology in the second half of 2021. Examples include an attack by the Hello Kitty ransomware group on video game company CD Projekt RED that resulted in the theft and subsequent leak of the company's source code and another attack on an unnamed organization that resulted in all of the company's VMs being taken offline very quickly. The attacks involved exploits of a couple of vulnerabilities in ESXi (CVE-2019-5544 and CVE-2020-3992). Both of these were older vulnerabilities that had patches available at the time the organizations were compromised.

Baby Got Hack

In September 2021, we noticed attacks attempting to exploit a remote code execution vulnerability in Motorola's Halo+ Baby Monitor. The attacks that followed allowed actors into one of the most intimate parts of people's homes via full access to the baby monitor's display device, camera, accompanying app, and data shared between the devices. This event, though uncomfortable in its own right, highlights the overarching topic of increasing the individual attack surface size and complexity due to the growing popularity and availability of IoT devices.

Don't get us wrong, we love a good smart gadget; IoT devices have revolutionized the way we humans interact with our environments. Yet, each new IoT device means one more connection to the internet and one more side-door for hackers to jiggle the handle of. With many IoT devices historically showing lackluster security performance, this is not good news for users.

That's right, baby monitors were not the only devices vulnerable to possible unauthorized access during the second half of 2021. In August 2021, millions of home routers were besieged by a malware attack. Included were Arcadyan routers, for which we observed attempted exploitations of an authentication bypass vulnerability. A couple months later in October, the FreakOut botnet was tracked infecting DVRs for Monero mining usage via a number of different available vulnerabilities including a remote code execution CVE in the Linux distribution ZeroShell.

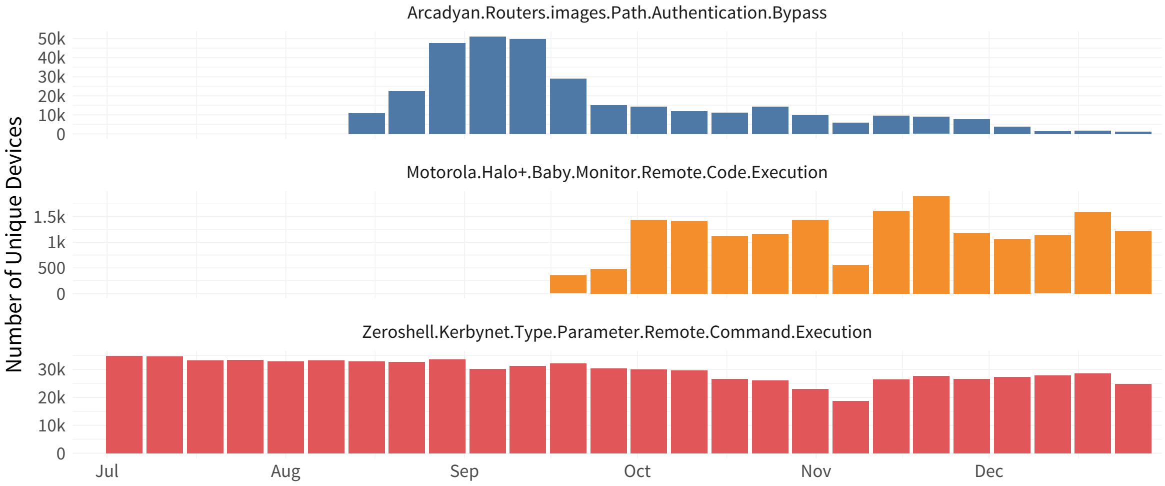


Figure 10: Weekly IPS detections for select IoT devices during 2H 2021.

The fact that baby monitors and so many other gadgets in our lives come with an internet connection these days is a big contributor to the record-breaking 20,000 vulnerabilities published to the CVE List in 2021. That record probably won't stand long. The volume of new vulnerabilities is such that CISA issued Binding Directive 22-01, requiring agencies to prioritize remediation of the subset of vulnerabilities most likely to be attacked.

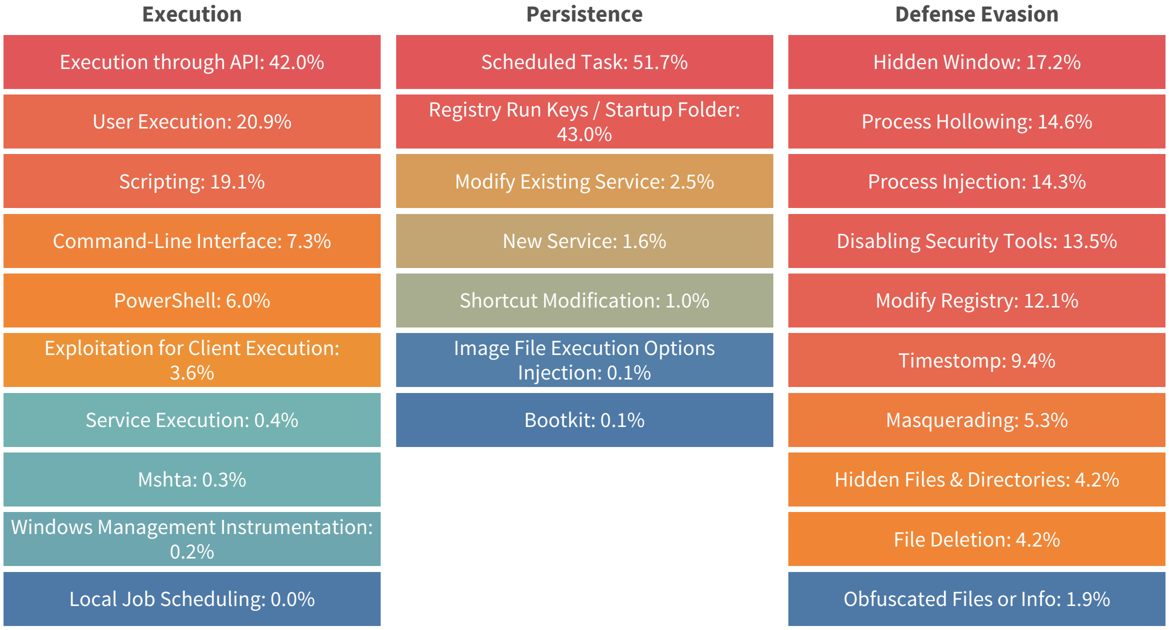
With the work-from-home wave sweeping through the workforce, these numerous and complex IoT-based points of entry to an individual's personal network are absorbed into their employer's attack surface. As with most cyberattacks, the primary concern with these kinds of attacks is not the initial unauthorized access to a device but rather the opportunity for attackers to move laterally through a network to other devices once inside. It's important for enterprises to not only implement good security practices on their end, but also to cultivate a culture of awareness and responsibility when it comes to cybersecurity that can be implemented in employees' professional lives and also roll over into their personal lives.

On the ATT&CK

Defenders and long-time readers of the Global Threat Landscape Report know that, by and large, individual malware strains come and go. Efforts such as MITRE's ATT&CK framework work to address the defender's reactive disadvantage by organizing adversaries' behaviors by their attack goals and the steps to achieve them (tactics and techniques, respectively). FortiGuard Labs is proud to work with MITRE on a variety of projects aimed at increasing the awareness and capabilities of defenders, particularly as a leading contributor to MITRE's Center for Threat-Informed Defense.

Understanding the functionality of specific, ephemeral malware in light of more enduring techniques gives defenders the context needed to protect from the next attack. But what about the popularity/prevalence of individual techniques? We used telemetry from detonated malware samples throughout the second half of 2021 in the FortiSandbox Cloud to find out what *might* have happened in a would-be victim's environment.

Figure 11 shows the prevalence of techniques for three tactics: Execution, Persistence, and Defense Evasion. Execution covers methods of attempting to run malicious code, and you can see that the top three techniques comprise 82% of the functionality for analyzed samples. We see an even more lopsided pattern for Persistence techniques where the top two techniques of obtaining a foothold represent nearly 95% of observed functionality.



Execution	Persistence	Defense Evasion
Execution through API: 42.0%	Scheduled Task: 51.7%	Hidden Window: 17.2%
User Execution: 20.9%	Registry Run Keys / Startup Folder: 43.0%	Process Hollowing: 14.6%
Scripting: 19.1%	Modify Existing Service: 2.5%	Process Injection: 14.3%
Command-Line Interface: 7.3%	New Service: 1.6%	Disabling Security Tools: 13.5%
PowerShell: 6.0%	Shortcut Modification: 1.0%	Modify Registry: 12.1%
Exploitation for Client Execution: 3.6%	Image File Execution Options Injection: 0.1%	Timestomp: 9.4%
Service Execution: 0.4%	Bootkit: 0.1%	Masquerading: 5.3%
Mshta: 0.3%		Hidden Files & Directories: 4.2%
Windows Management Instrumentation: 0.2%		File Deletion: 4.2%
Local Job Scheduling: 0.0%		Obfuscated Files or Info: 1.9%

Figure 11: Technique prevalence for select tactics during 2H 2021.

When contrasted with the variety of Defense Evasion techniques, stopping an adversary earlier seems to be the order of the day—i.e., before they've had an opportunity to make themselves at home and profile one's defensive capabilities.

Figure 12 reveals a similar concentration of techniques to Figure 11 when breaking out Persistence techniques by region, with the notable exception of samples observed in Asia. Threat hunters in this region might be well-advised to incorporate reviews of new or modified services into their standard operations.

	Africa	Asia	Europe	N. America	Oceania	S. America
Scheduled Task	55.9%	42.7%	56.5%	51.4%	55.8%	50.5%
Reg. Run Keys/Startup Folder	40.4%	44.7%	40.9%	44.6%	40.9%	46.4%
Modify Existing Service	1.9%	5.1%	1.7%	2.2%	3.2%	1.1%
New Service	0.1%	6.6%			0.2%	0.5%
Shortcut Modification	1.7%		0.5%	1.3%		1.5%
Other		1.0%	0.4%	0.5%		

Figure 12: Prevalence of Persistence techniques by region during 2H 2021.

Figure 13 confirms that Execution through API—where malware interacts directly with an application to compromise it—reigns supreme as the most common Execution technique for all industries. User Execution—where adversaries rely on specific actions to be taken by a victim—only comes close to the king in one vertical: Education. Few will raise their eyebrows at the notion of users in the Education vertical being a significant vector of infiltration, but it's interesting to see that attackers seem to believe that too when prioritizing malware functionality! And if User Execution—typically malware relying on clicked links or opened files—is hotter in Education (32%), it would appear cooler in Energy/Utilities, where malware is nearly twice as likely to interact with systems more directly via Scripting.

	Aero/Defense	Agriculture	Automotive	Banking/Fin/Ins	Construction	Consulting	Education	Energy/Utilities	Environmental	Food/Beverage	Government	Healthcare	Legal	Manufacturing	Media/Comms	MSSP	Nonprofit	Retail/Hosp.	Technology	Telco/Carrier	Transp./Logistics
Execution through API	42%	44%	42%	41%	43%	38%	38%	39%	38%	47%	41%	40%	44%	46%	45%	45%	47%	42%	42%	41%	38%
User Execution	25%	17%	24%	20%	22%	23%	32%	13%	22%	19%	22%	19%	18%	21%	20%	18%	18%	20%	22%	18%	23%
Scripting	18%	18%	18%	22%	20%	16%	15%	24%	18%	17%	18%	20%	21%	19%	19%	20%	19%	22%	18%	20%	20%
Other	15%	21%	16%	17%	15%	23%	16%	24%	21%	17%	18%	21%	17%	14%	15%	16%	16%	17%	18%	21%	20%

Figure 13: Prevalence of Execution techniques by industry during 2H 2021.

Ending on a High Note

Fortinet is a founding partner of The World Economic Forum's Centre for Cybersecurity (C4C), an independent and impartial global platform committed to fostering international dialogues and collaboration between the global cybersecurity community both in the public and private sectors. The Partnership against Cybercrime is part of the C4C Platform, and under that, FortiGuard Labs is currently leading a project to map the cybercriminal ecosystem and better understand relations and business operations so we can help disrupt activity such as described in this report.

Those wanting to know more about what can be done to raise the cost of conducting cybercrime and increase the risks for cybercriminals can read this report we co-authored that discusses the need to improve global capabilities for takedown operations and broader efforts to disrupt cybercrime.

www.fortinet.com

February 22, 2022 10:48 AM

1471550-0-0-EN