AUGUST 2021

Global Threat Landscape Report

A Semiannual Report by FortiGuard Labs

TABLE OF CONTENTS

Overview and Key Highlights

In the cybersecurity world, every year gets a "Year of" designation based on industry consensus. We're only halfway done at this point, but it seems to us that 2021 is building a good case to become known as the "Year of the Outbreak." Yes, 2020 probably earned that moniker among those outside the field; maybe it takes a year for physical realities to go virtual. Regardless, the first six months of 2021 have seen wide-scale attacks that spread to envelop numerous organizations and countless individuals become a regular occurrence. We've studied the aftermath and summarized developments that we hope keep you one step ahead of whatever breaks out next.

The ProxyLogon Feeding Frenzy

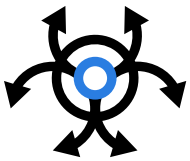
A China-based threat group named 'Hafnium' purportedly attacked tens of thousands of organizations via four vulnerabilities in Microsoft Exchange Server months before patches were available. Smelling blood in the water, other groups began targeting those same bugs in earnest. It's no surprise, therefore, that our sensors picked up a huge surge in related activity that you can read more about in our first Featured Story.

Ransomware Takes an Ominous Turn

Last year sure seemed like a doozy, but we're clocking another 10.7x increase in ransomware over the last 12 months! And not only has it gotten more prevalent, but it's somehow gotten even nastier. Attacks that crippled the supply chains of companies like Colonial Pipeline and JBS feel like harbingers of ransomware gangs leveling up and impacting daily life more than ever before. Get our thoughts on what this means and where it's headed.

OT Not Under IT's Shadow Anymore

Operational Technology (OT) may not get the same attention as IT, but its connection to our physical world means it can impact lives long after we close our laptops at the end of the day. We've had numerous reminders of that connection so far in 2021 through ransomware and other attacks aimed at industrial environments. We analyze detected exploits targeting industrial control systems (ICS) and demonstrate that OT sits higher on the attacker radar than you might think.



The Emotet Takedown and Other Law Enforcement Actions

Cybersecurity is a long game and few actions have an immediate and lasting effect. That's why we have to savor the small victories that propel us forward to fight another day. The coordinated takedown of Emotet, one of the most prolific malware schemes in recent history, as well as actions to disrupt the Egregor, NetWalker, and Cl0p ransomware operations represent wins by global governments and law enforcement to curb cybercrime. We're glad to participate in such actions and you can read our take here.

Top Threats During 1H 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,[1] 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 eager to share with you. We'll start things off by highlighting threats that topped the charts during the first six months of 2021.

IPS Detections

MITRE ATT&CK is an increasingly popular framework for studying adversary tactics, techniques, and procedures (TTPs). The first three groupings of TTPs in ATT&CK span reconnaissance, resource development, and initial access. They essentially describe how threat actors find vulnerabilities, build malicious infrastructure, and exploit their targets. Our FortiGuard Intrusion Prevention System (IPS) sensors running on our FortiGate firewalls provide excellent visibility into this type of activity around the world because they're often positioned to be the first point of contact with an adversary probing for exposures.

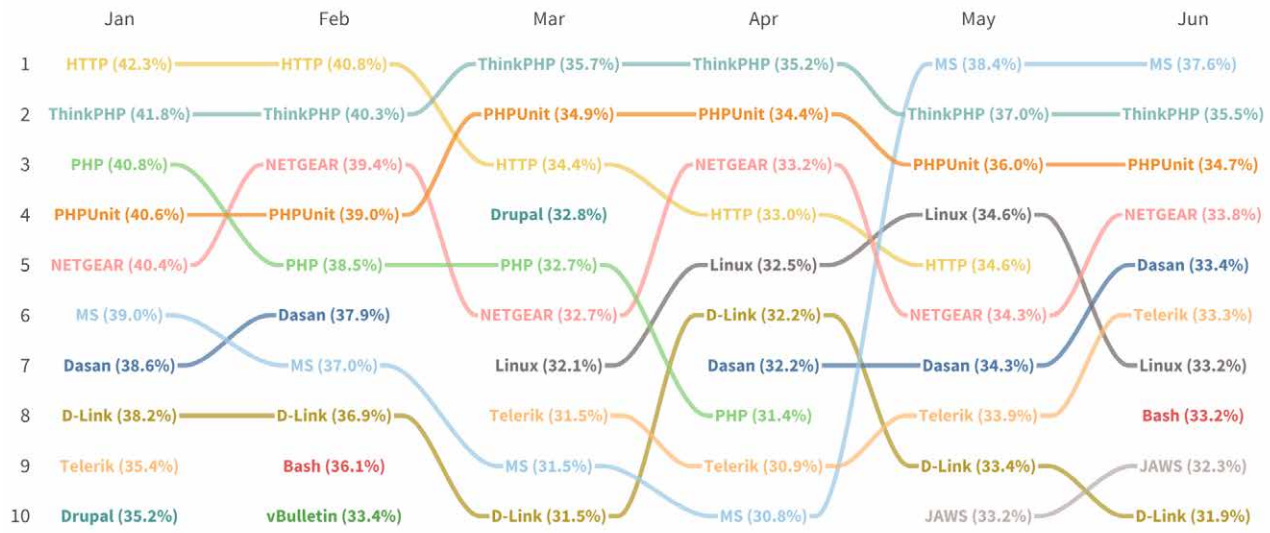


Figure 1: Prevalence of top IPS detections by technology during 1H 2021.

Figure 1 presents the top technologies targeted by exploit attempts during the first half of 2021. Overall the IPS detections shown reflect several general trends we've seen for some time now: web servers, content management systems (CMS), and Internet of Things (IoT) devices. We'll unpack that a bit more in the paragraphs that follow. The HTTP signature header claiming the #1 spot for January and February is admittedly vague, but it encompasses a long list of exploits targeting web servers. To give a few concrete examples, the IPS triggers racking up the highest volume were HTTP.Server.Authorization.Buffer.Overflow and HTTP.URI.Java.Code.Injection, while HTTP.Header.SQL.Injection and HTTP.URI.SQL.injection were detected by the largest number of organizations.

Sticking with the theme of exploits targeting web and other enterprise servers, Microsoft (MS) and Linux make regular appearances in Figure 1. That's not a huge surprise given the wide usage of those platforms. The primary signature behind the rise of Linux-based detections starting in March relates to a vulnerability allowing a remote attacker to trigger a kernel panic in systems, thereby impacting availability. Microsoft's climb to the top in May and June ties back to a long list of signatures, but one of the most prevalent ones detects attempts to exploit a remote code execution vulnerability in Microsoft Exchange Server. We'll circle back to that in one of our Featured Stories.

Exploits targeting ThinkPHP, a PHP-based CMS, fluctuate between the top two spots each month over the half. Several other CMS (Drupal, vBulletin) and related development frameworks (PHPUnit) enter the monthly top 10 at various points as well. CMS are notorious targets for opportunistic cybercriminals because they so often instantiate the proverbial low-hanging fruit. They're designed to make it easier to manage web content–a feature that becomes a liability in the wrong hands. If your organization uses them, diligently applying security fixes to CMS and plugins is a must.

Top IPS detections reveal several examples of highly-targeted network and IoT devices, including those from Netgear, D-Link, Dasan, and JAWS. Most of these are small business or consumer-grade technologies, pointing to a trend we called out in our Cyber Threat Predictions for 2021 white paper. The shift to remote and home-based work has brought devices populating those environments into the crosshairs of cyber threat actors. Part of this attraction is that such devices store a wealth of information about users and their online activities, which attackers can leverage for fraud and social engineering schemes.

Even more worrisome to corporate security programs, however, is the potential for attacks launched from a remote worker's home network. Think about how many devices lie between an employee working from home and the enterprise applications and data needed to do their job. Now think about all the things attackers could do if they compromise those devices. You can be sure that attackers are thinking about it too.

For the most part, the exploits represented in Figure 1 aren't the newest kids on the block. It generally takes a while to rise to the tip of the top. But what about the up-and-comers? Lest we neglect those, Figure 2 alters the algorithm to focus on "Rookie of the Year" candidate exploits for which we've developed IPS signatures within the last year. It also adds the twist of comparing detected activity across sectors.

	Aerospace & Defense	Agriculture	Automotive	Banking/Finance/Insurance	Construction	Consulting	Education	Energy & Utilities	Environmental	Food & Beverage	Government	Healthcare	Legal	Manufacturing	Media/Communications	MSSP	Nonprofit	Retail/Hospitality	Technology	Telco/Carrier	Transportation & Logistics
vBulletin.tabbedcontainer.Template.Remote.PHP.Code.Execution	21%	26%	20%	24%	19%	20%	39%	23%	21%	20%	36%	23%	17%	22%	29%	32%	21%	21%	27%	40%	26%
MS.Exchange.Server.ProxyRequestHandler.Remote.Code.Execution	16%	18%	15%	19%	14%	14%	23%	19%	16%	16%	24%	17%	15%	17%	20%	25%	14%	14%	20%	28%	20%
F5.BIG.IP.TMM.URI.Normalization.Buffer.Overflow	14%	19%	14%	16%	12%	13%	30%	17%	15%	13%	26%	16%	12%	15%	21%	27%	15%	14%	20%	31%	18%
Netis.WF2419.Router.Remote.Command.Execution	15%	18%	14%	16%	13%	13%	28%	15%	13%	13%	24%	16%	11%	16%	18%	21%	15%	14%	18%	26%	18%
Tenda.AC15.AC1900.Authenticated.Remote.Command.Injection	13%	17%	13%	15%	12%	13%	28%	14%	13%	12%	24%	15%	11%	14%	19%	23%	14%	13%	18%	28%	17%
Oracle.WebLogic.Fusion.Middleware.Authentication.Bypass	12%	13%	10%	15%	9%	11%	25%	12%	13%	11%	24%	13%	8%	11%	15%	22%	11%	11%	16%	26%	14%
F5.iControl.REST.Interface.Remote.Command.Execution	10%	8%	6%	11%	5%	7%	18%	8%	9%	6%	18%	10%	6%	7%	10%	16%	8%	7%	12%	22%	9%
F5.BIG.IP.Traffic.Management.User.Interface.Directory.Traversal	8%	7%	5%	11%	4%	5%	14%	8%	5%	5%	16%	8%	5%	6%	10%	15%	7%	7%	11%	19%	8%
MobileIron.MDM.Unauthenticated.Remote.Code.Execution	6%	6%	5%	11%	4%	6%	12%	7%	7%	5%	16%	8%	3%	5%	9%	15%	6%	5%	10%	18%	7%
Spring.Boot.Actuator.Unauthorized.Access	3%	5%	4%	8%	3%	4%	14%	5%	4%	3%	15%	6%	2%	4%	8%	12%	6%	4%	9%	17%	5%
Nette.Framework.Callback.Parameter.Remote.Code.Execution	6%	5%	4%	6%	3%	5%	9%	6%	5%	3%	11%	5%	4%	4%	7%	10%	5%	3%	7%	13%	6%
Cisco.ASA.Web.Interface.Directory.Traversal	4%	4%	3%	9%	2%	3%	8%	4%	4%	3%	11%	5%	3%	3%	6%	10%	4%	4%	7%	14%	4%
Cisco.HyperFlex.HX.storfs-asup.Handling.Command.Injection	5%	6%	4%	5%	3%	3%	8%	4%	3%	3%	8%	5%	4%	4%	6%	12%	4%	4%	6%	14%	5%
VMware.vRealize.Operations.SSRF	3%	3%	2%	6%	1%	3%	6%	4%	4%	2%	10%	4%	2%	2%	5%	10%	3%	3%	6%	11%	4%
CraftCMS.SEOmatic.Template.Remote.Code.Injection	3%	4%	3%	5%	2%	3%	9%	2%	3%	2%	11%	4%	2%	2%	5%	8%	4%	3%	6%	10%	3%
Apache.Flink.JobManager.Arbitrary.Path.Traversal	3%	4%	2%	4%	2%	3%	8%	3%	3%	2%	11%	3%	1%	3%	4%	7%	3%	2%	6%	10%	3%
Apache.Struts.OGNL.BeanMap.Remote.Code.Execution	3%	4%	2%	4%	2%	3%	8%	3%	3%	3%	11%	4%	2%	2%	4%	7%	2%	2%	5%	10%	4%
FreePBX.Remote.Admin.Authentication.Bypass	2%	3%	2%	3%	2%	3%	9%	3%	3%	2%	6%	3%	2%	3%	5%	9%	3%	2%	5%	11%	4%
Citrix.XenMobile.Server.sbFileName.Arbitrary.Path.Traversal	2%	4%	2%	5%	2%	3%	7%	2%	2%	2%	11%	3%	2%	2%	5%	6%	3%	2%	5%	10%	3%

Figure 2: Prevalence of new (<12 months) IPS detections during 1H 2021.

We know that the IPS.Signature.Naming.Schema might not be the most intuitive parlance, but they do make it easy to search and find anything listed in Figure 2 using our Threat Encyclopedia. This chart is tailormade to answer the very important question of "what new exploits are other organizations like mine detecting?" Explore that question at your leisure, and we'll keep our comments to a few high-level observations.

Figure 2 makes it very clear that certain sectors see higher levels of activity, regardless of the specific exploit in question. Education, Government, Managed Security Service Providers (MSSPs), and Telecommunications are visibly "hotter" across the board, often doubling or tripling the prevalence exhibited in other sectors. Organizations in these sectors tend to have a high number of devices and represent numerous subsidiaries (i.e., government sub-agencies or customers of MSSPs/Telcos). And some of them–most notably educational institutions–traditionally have looser control over the security and usage of those devices.

Beyond those, the sectors that attract more exploit attention–like financial institutions, media companies, and tech firms–align with expectations. Agriculture, however, may seem out of place to some. But if you consider how tech-dependent agriculture has become, these findings become more intuitive. A modern farm or other type of agricultural facility can have a huge number of IoT devices deployed, each with their own connections and exposures. Cybercriminals are equal opportunity exploiters.

Malware Detections

Samples detected by our various anti-malware solutions offer insight into popular techniques for establishing a foothold within corporate environments. Within the context of ATT&CK, this activity correlates with the Execution phase in which attackers attempt to deploy and run malicious code on a target system.

We've chosen to group malware into families rather than specific variants in Figure 3. Our purpose in doing this is to group the numerous, often short-lived variants by their similarities so that we don't lose the big picture among the details. Figure 4 drops down to the detailed view when presenting new strains spreading around the globe.

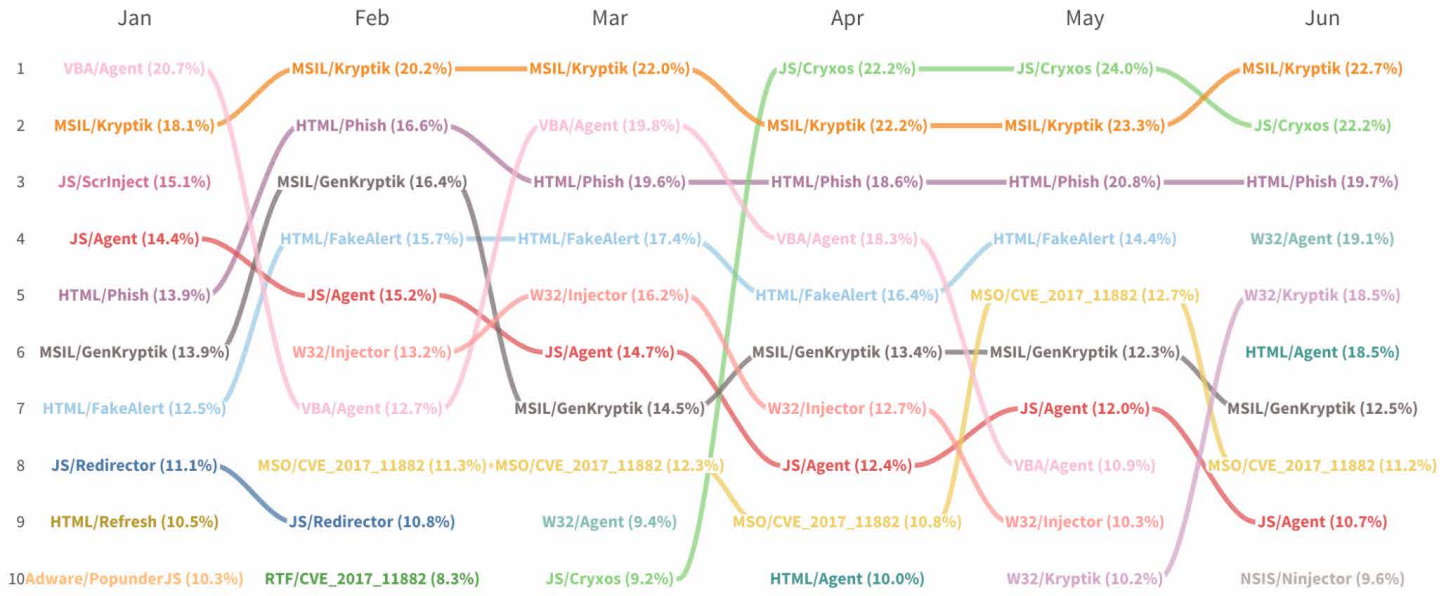


Figure 3: Prevalence of top malware detections by family during 1H 2021.

From a vector perspective, the families and variants in both charts can be largely grouped into two broad distribution mechanisms: Microsoft platforms and web browsers. The first of those groups (Microsoft platforms) includes malware in the form of 32-bit Windows executables (W32), malicious Office or Visual Basic (VBA) files, and that use a .NET or Microsoft Intermediate Language (MSIL) packer. Malware families exploiting web browsers often get assigned the HTML or Javascript (JS) prefix. This encompasses malware-laced 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 peoples' craving for news/information during the COVID-19 pandemic and the concurrent transition to working from home outside corporate web filters.

Ranking the prevalence of top malware detections by malware families shows a rise in deceptive social engineering javascript-based malvertising and scareware (e.g., Cryxos). Such schemes are commonly associated with fake notifications purporting to be the Microsoft tech support team. In a typical scenario, users receive some type of message (e.g., a browser pop-up) stating their device has been infected or hacked. The user is then urged to contact (and pay) support staff and/or grant remote access for help in fixing the issue. Overall, more than one in four organizations detected malvertising or scareware attempts during the first half of 2021.

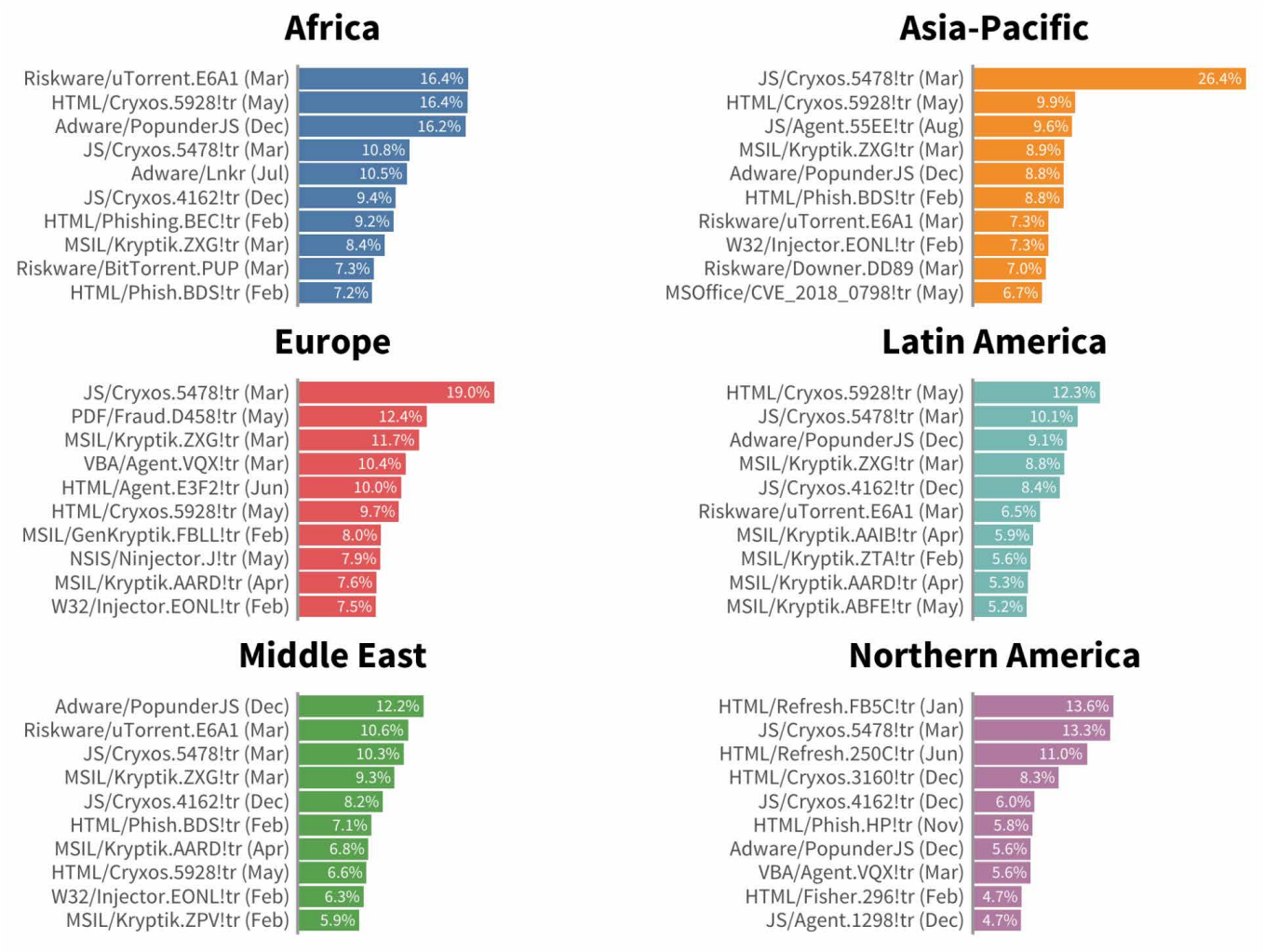


Figure 4: Prevalence of new (<12 months) malware variants by region during 1H 2021.

Malvertising is not a new tactic, nor is the most dangerous form/function of malware. The remote work trend has undoubtedly contributed to malvertising's rise up the charts. With so many working outside the traditionally-more-secure confines of the corporate perimeter and also deprived of the convenience of being present with IT staff in the office, workers are more on their own than ever before. This is yet one more example of how cybercriminals are adapting existing tools to exploit changing conditions.

Observed Malware TTPs

In addition to listing the malware samples detected over the last six months, we wanted to go one step further to study the specific functionality inherent to those samples. The best way to do that is to detonate the malware and observe what it's actually attempting to do. And that's exactly what we did to create Figure 5.

Figure 5 depicts several ATT&CK TTPs associated with the malware analyzed by our FortiSandbox Cloud service. Think of it as a laundry list of all the nasty things malware samples would have done if they had successfully executed payloads in the target environment. They seek to escalate privileges, evade defenses, begin moving laterally across internal systems, establish command and control, exfiltrate compromised data, and accomplish whatever impact they're trying to achieve.

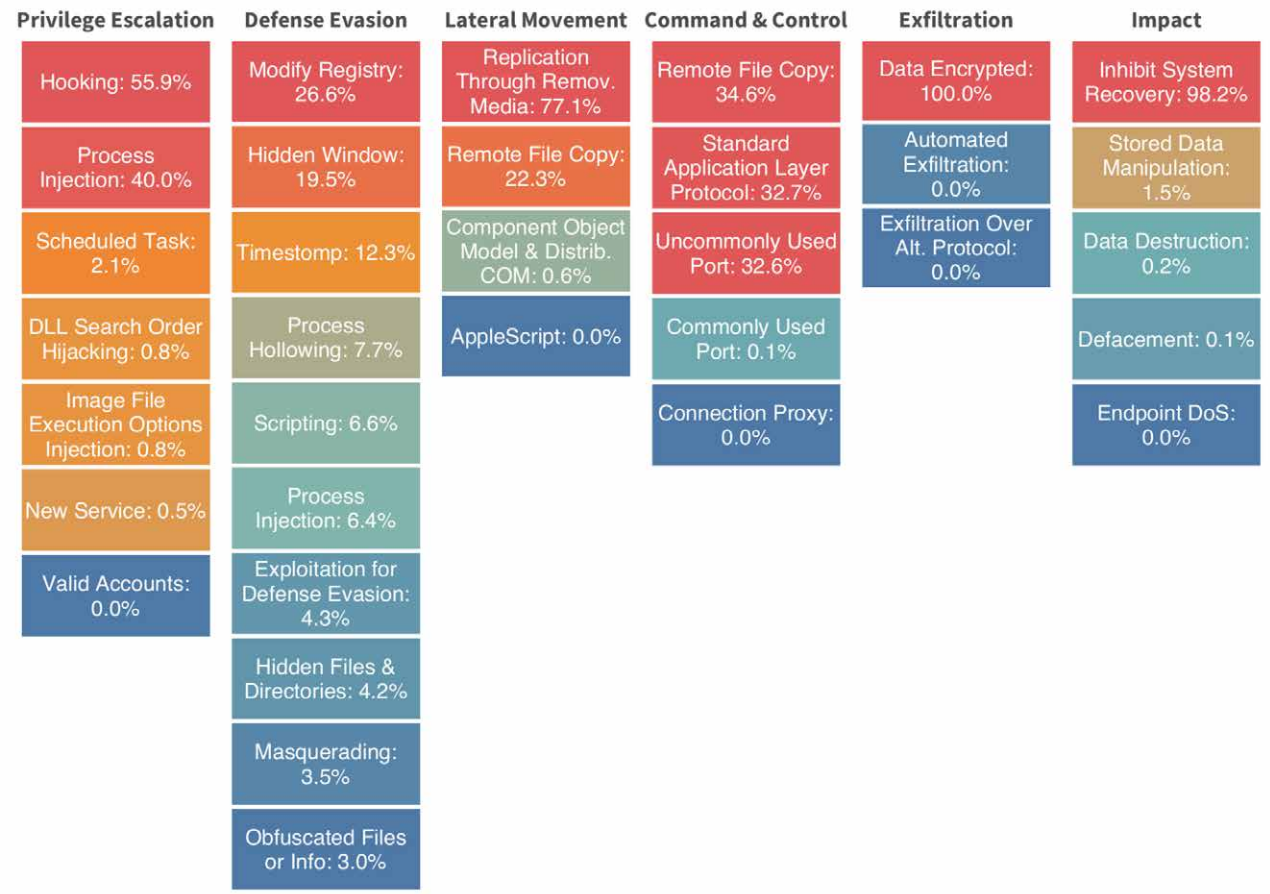


Figure 5: Relative frequency of malware TTPs observed by Fortinet in 1H 2021.

The percentages shown in the chart are based on the frequency of each technique within the top-level tactic. So, 55% of observed privilege escalation functionality leveraged hooking, 40% utilized process injection, and so on. From that, it's obvious there is a heavy focus on Defense Evasion and Privilege Escalation tactics. None of these techniques are novel but some require deep instrumentation at the kernel level to understand how the malicious process interacts with and requests resources from the core of the operating system. Making sure there's an inspection point between these interactions is paramount to intercepting advanced threats that would likely slip past through traditional defenses (as happens in attacks such as ProxyLogon).

We've seen APT actors becoming increasingly fond of using zero days to infiltrate networks. Thus, the ability to observe this functionality—before it actually impacts a production system—and trigger mitigation through fabric integration is more critical than ever to interrupt their ability to progress through stages of the kill chain. Doing that successfully is a lot easier when you know which specific techniques threat actors use most often and can use that intel to build a threat-informed defense.

Speaking of building a threat-informed defense, FortiGuard Labs is proud to be a leading contributor to MITRE's aptly-named Center for Threat-Informed Defense through projects like the Sightings Ecosystem. It's one of the many ways we're collaborating with industry partners to help keep you more informed and more secure.

Botnet Detections

While IPS and malware trends reveal what's happening "left of boom" (pre-compromise), botnets grant insight to malicious activities that occur during the all-important "right of boom" (post-compromise) phase. In terms of ATT&CK, this is most closely associated with techniques falling under the Command and Control tactic, whereby infected systems communicate with remote malicious hosts. Figure 6 presents the top bots of 1H 2021.

Before we discuss specific bots tracked in Figure 6, let's cover how to interpret it. The height of the colored streams correlates with the number of organizations detecting activity associated with each botnet. Every botnet detection that's NOT among those labeled here is represented by the relatively thin "Everything Else" band at the bottom. That points to the existence of a Pareto principle among botnets, whereby 80% of activity ties back to the top 10 botnets. This is why dismantling major botnets can be an effective strategy against cyber threats. We'll discuss one such operation to takedown the Emotet botnet in one of our Featured Stories.

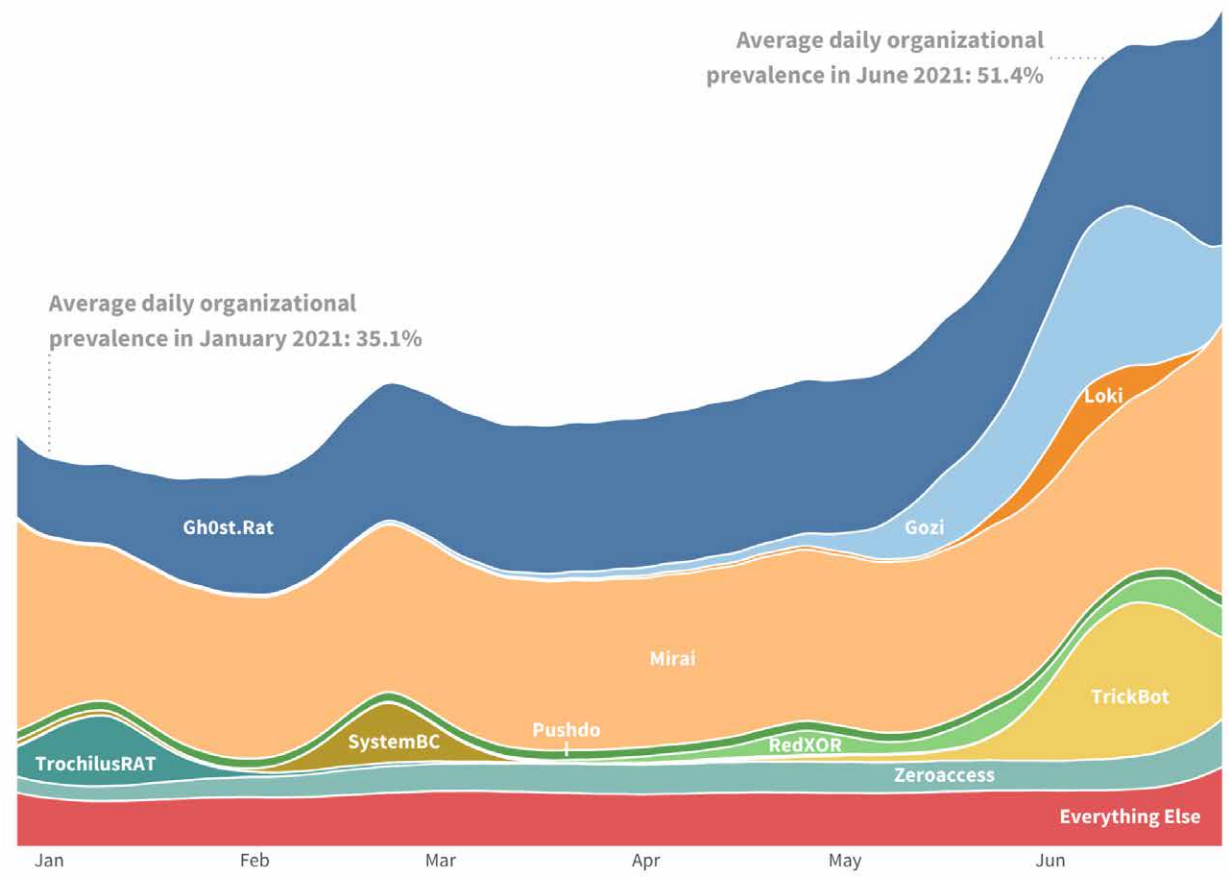


Figure 6: Prevalence of botnet detections during 1H 2021

You probably notice something else about Figure 6-a big jump in activity toward the end of the half. At the beginning of the year, 35% of organizations detected botnet activity of one sort or another. Fast forward six months, and that figure stands at 51%. Let's look into what's behind that surge (which is rather unusual for aggregate botnet activity, by the way).

Mirai is the thickest band and is therefore the most prevalent. It overtook Gh0st in early 2020 and has reigned supreme ever since. Mirai gained infamy several years ago after fueling massive IoT-based DDoS attacks. Since that time, Mirai has continued adding new cyberweapons to it's arsenal to retain its dominance (examples 1 and 2). We hate to sound like a broken record, but it's likely that Mirai's dominance at least partially stems from criminals seeking to exploit IoT devices used by (or proximate to) work-from-home employees.

Gh0st is also noticeably active across the period (and going back years). It's a remote access botnet that allows attackers to take full control of the infected system, log keystrokes, access live webcam and microphone feeds, download and upload files, and other nefarious activities.

In a very unusual twist, most of the remaining botnets depicted in Figure 6 were not among the top 10 prior to now. We tend to see the same old suspects every time, so it's refreshing to see some newcomers to the group. The prominent bump in prevalence toward the end of the half demonstrates those newcomers helped push overall botnet activity to new heights.

Communications with the Trochilus botnet bumped up early in the year, particularly in Oceania and Southeast Asia. In the past, the Trochilus remote access trojan (RAT) has been purportedly used by Chinese espionage groups in operations targeting that region (see Figure 7).

	Africa	Asia	Europe	Latin America	Middle East	Northern America	Oceania
TrickBot	50.0%	41.3%	66.8%	48.6%	40.9%	64.1%	66.4%
Gh0st.Rat	61.8%	61.4%	65.2%	61.4%	56.6%	71.9%	70.5%
TrochilusRAT	41.0%	38.7%	46.4%	42.5%	38.7%	51.5%	54.4%
Necurs	6.2%	4.0%	2.5%	2.9%	4.1%	3.8%	3.8%
Sality	12.9%	13.7%	3.0%	6.2%	18.2%	3.1%	3.3%
RedXOR	11.6%	12.3%	10.8%	20.5%	11.1%	7.9%	8.6%
Nymaim	0.4%	5.7%	0.3%	0.1%	0.1%	0.2%	0.4%

Figure 7: Prevalence of botnets exhibiting high regional variation in 1H 2021.

SystemBC, which jumped to #3 in February (Figure 6), is a RAT that's been popular of late in quite a few ransomware campaigns. One of the reasons for that popularity is that it provides persistent TLS-encrypted backdoor and C2 functionality to attackers. Ransomware operators have shifted their strategy away from email-initiated payloads to leveraging "access facilitators" (a nice-sounding name for cybercriminals that focus on gaining and selling initial access). SystemBC is one of the tools supporting that trend.

The large bump in TrickBot activity toward the end of the half in Figure 6 is largely responsible for the overall spike in botnet activity during June. TrickBot emerged on the cybercrime scene as a banking trojan but has since been developed into a sophisticated, modular, and multi-stage toolkit supporting a range of illicit activities. The Cybersecurity & Infrastructure Security Agency (CISA) released an alert in May detailing a surge of spear phishing campaigns using TrickBot. As a reminder that cybercriminals sometimes get their comeuppance, the original developer of TrickBot was arraigned on multiple charges in June.

The other big bump in June botnet activity (Figure 6) came from Loki. CISA issued a warning about a rise in detections of this information-stealing malware family in late 2020. There's no intelligence regarding new or specific campaigns driving this surge, but it's definitely on our radar based on these results. Speaking of things on our radar, let's take a look at the stories we chose to feature from the last 6 months.

Featured Stories

The ProxyLogon Feeding Frenzy

A set of four vulnerabilities in Microsoft Exchange Server caused widespread concern in the first half of 2021 because of the number of systems impacted and the fact that attackers were actively exploiting the flaws before Microsoft issued patches for them on March 2. The flaws, which some referred to as ProxyLogon, posed a threat to organizations with Internet-facing Exchange servers that accepted untrusted connections from an external source. Some vendors have reported more than 30% of incidents detected in Spring 2021 as being tied to the Exchange server flaws.

The vulnerabilities were CVE-2021-26855, a Server-Side Request Forgery (SSRF) issue that could be used to bypass authentication; CVE-2021-26857, an insecure deserialization vulnerability that allowed attackers to elevate privileges to SYSTEM; and CVE-2021-26858 and CVE-2021-27065, two post-authentication arbitrary file-write vulnerabilities. When chained together, the four vulnerabilities give attackers a way to remotely execute malicious code on Exchange Servers and install backdoors.

A China-based advanced persistent threat (APT) group called 'Hafnium' is believed to have attacked at least 30,000 US-based organizations using the flaws before Microsoft's fixes for them became available. The first attacks against the flaws in fact were thought to have begun in January–more than two months before patch availability. Among those attacked were US-based think tanks, defense contractors, law firms, NGOs, and organizations conducting infectious disease research. After Microsoft disclosed the flaws, numerous other criminal groups, state-backed operators, and opportunistic hackers began targeting them in a virtual feeding frenzy. The attackers included at least one other China-based player called Barium (or APT41), a threat actor that Fortinet has previously linked to supply chain compromises and attacks on major software vendors.

The attacks prompted urgent advisories from CISA, Microsoft, and numerous other security vendors. Concerns over the threat were so great that in April the FBI conducted an unprecedented court-authorized operation to proactively remove malicious webshells that threat actors had installed on hundreds of US-based Exchange servers–without even notifying owners of these systems beforehand.

Fortinet tracked threat actors using a variety of malware tools against these vulnerabilities including Lemon Duck coinminer, BlackKingdom ransomware, Prometei botnet, and 'China Chopper', a lightweight webshell going back to at least 2012 that provides persistent backdoor access to a vulnerable system post-compromise. Fortinet's IPS detections for activity related to the Exchange Server vulnerabilities (see Figure 8) showed threat actors targeting the flaws in attacks worldwide but especially in Europe. Some have reported Turkey, USA, and Italy as being the three most-attacked countries. We observed a particularly high level of activity targeting CVE-2021-26855, the SSRF flaw that gave adversaries initial access to vulnerable Exchange servers.

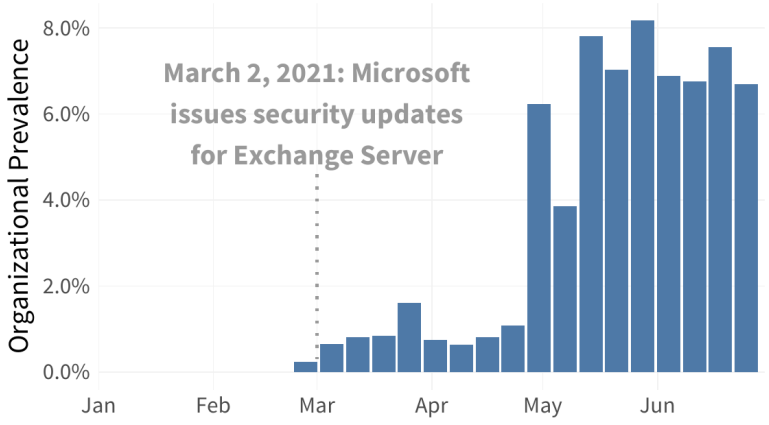


Figure 8: Exploitation activity targeting Exchange Server ProxyLogon vulnerabilities in 1H 2021.

For security teams the attacks were a reminder that vulnerabilities in widely used technologies—especially one as vital as email—continue to be a magnet for threat actors. In this instance, the vulnerabilities initially were exploited for cyber espionage purposes by a sophisticated state-backed APT. But once patches became available, adversaries quickly reverse-engineered them and began exploiting them for all sorts of other attacks once again highlighting the need for prompt patching and multi-layered defenses.

Ransomware Takes an Ominous Turn

Ransomware remained as ominous a threat for organizations worldwide during the first two quarters of this year as it has for the past several quarters. Though we did not observe as dramatic a surge in attacks as the 2H2020, ransomware levels remained high and increased steadily over the course of the year. Average weekly ransomware activity across our sensors in June 2021 was, in fact, 10.7x higher than levels set one year ago (Figure 9). Furthermore—and contrary to the general perception—ransomware presents a threat to a much broader range of industries than just healthcare, government, and the education sectors (Figure 10).

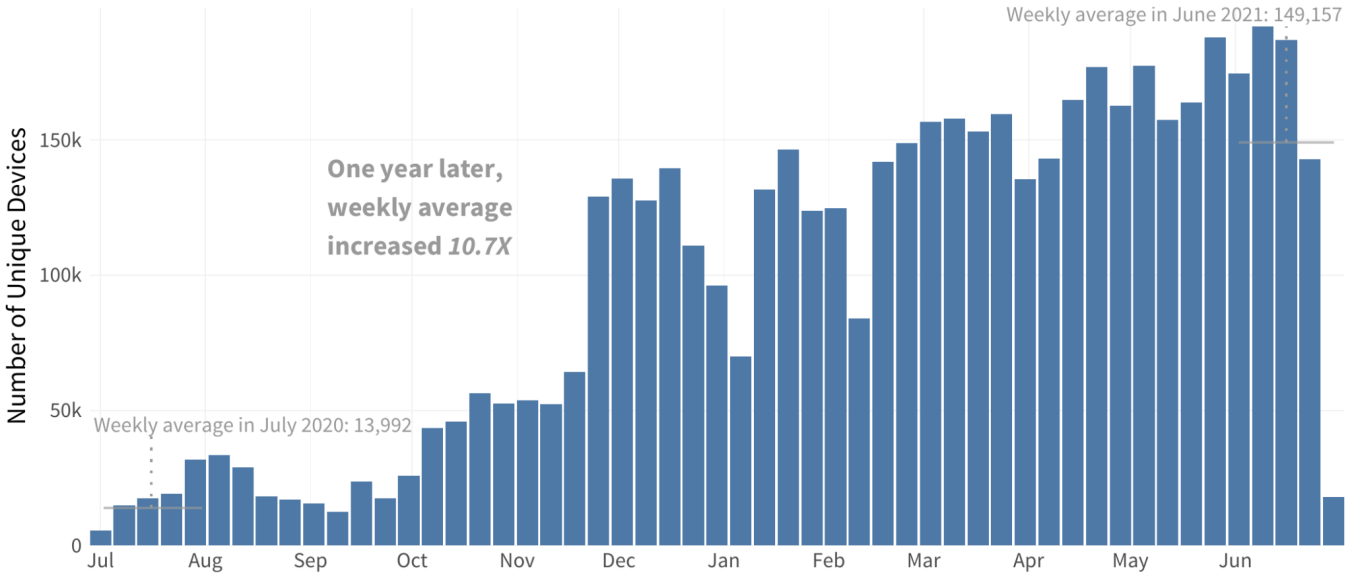


Figure 9: Growth in ransomware detections over last 12 months (Jul '20 - Jun '21).

Of note—and concern—this year were attacks on OT networks and organizations in sectors of critical importance. One example is an attack in May on Colonial Pipeline that resulted in a temporary but severe disruption of fuel supplies across large sections of the US East Coast. Colonial Pipeline paid $4.4 million to DarkSide, the Russian threat actor behind the attacks, to regain control of its pipeline. Another attack in May, this time on JBS, the world's largest meat processor, raised the specter of a similar disruption to meat supplies across the US. JBS paid $11 million to attackers to resolve the issue.

The two incidents elevated ransomware to the level of a national security concern and reportedly prompted the US Department of Justice to consider treating such attacks with the same priority as terrorist attacks. The level of attention that the attacks garnered at the highest levels of the US government spooked at least some ransomware operators—including DarkSide, Avaddon, and Ziggy—to announce they were ceasing operations.

In January Fortinet discovered a new ransomware variant called DarkWorld. The ransomware, written in .NET, was observed spawning 10 encryption threats and using the Rijndael encryption algorithm (AES) to lock victims' files. Most of the activity associated with this ransomware variant was from India, followed by Columbia, France, Chile, and the United States.

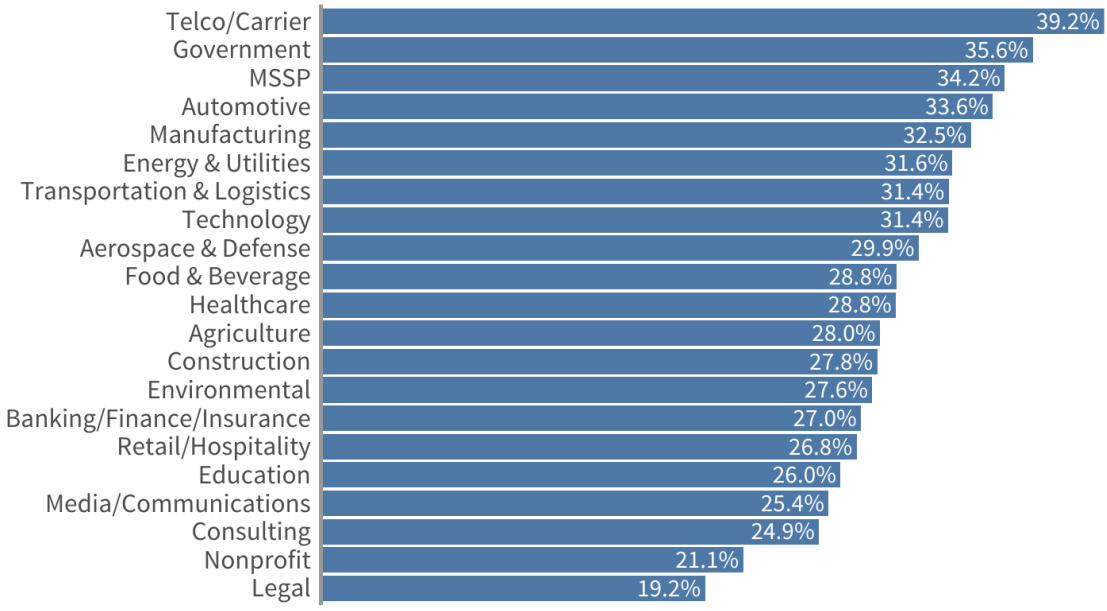


Figure 10: Prevalence of ransomware detections across sectors in 1H 2021.

Figure 10 demonstrates that ransomware is a threat common to all industries. That said, organizations in the telecommunications sector were the most heavily targeted followed by government, managed security service providers, automotive, and manufacturing sectors. The prevalence of ransomware in the healthcare and education sectors—generally considered the most heavily attacked—was noticeably lower than in all these sectors. For organizations the key takeaway is that ransomware is a clear and present danger regardless of industry or size.

OT Not Under IT's Shadow Anymore

Operational Technology (OT) may not get the same attention as IT, but its connection to our physical world means it can impact lives long after we close our laptops at the end of the day. Until recently, OT networks functioned as isolated, air-gapped environments, meaning cybersecurity was not a top priority. Exploits against supervisory control and data acquisition (SCADA) or industrial control systems (ICS) were viewed by many as a rare subset of highly-targeted attacks that most organizations needn't concern themselves with. But is that perception accurate in light of modern threats? Let's look at the evidence.

Figure 11 plots IPS detections according to their prevalence and volume. Gray dots represent the spectrum of prevalence and volume of attacks on IT (see Figure 1 for examples of technologies in the far upper-right) and red dots represent that of OT systems. While IT-related exploits are clearly more numerous and exhibit greater prevalence and volume, the relatively high level of exploitation targeting OT may surprise many. At the very least, what we see in Figure 11 shatters the perception that ICS exploits are an obscure niche of the cyber threat landscape.

This recalibration of perception is critical, given how new business demands and aging infrastructure are chipping away at the historical partitions separating OT and IT and leading to increased convergence of these networks. You can learn more about how to respond to the need for more flexible security infrastructure in March's Industry Perspective, focused on developments in industrial environments.

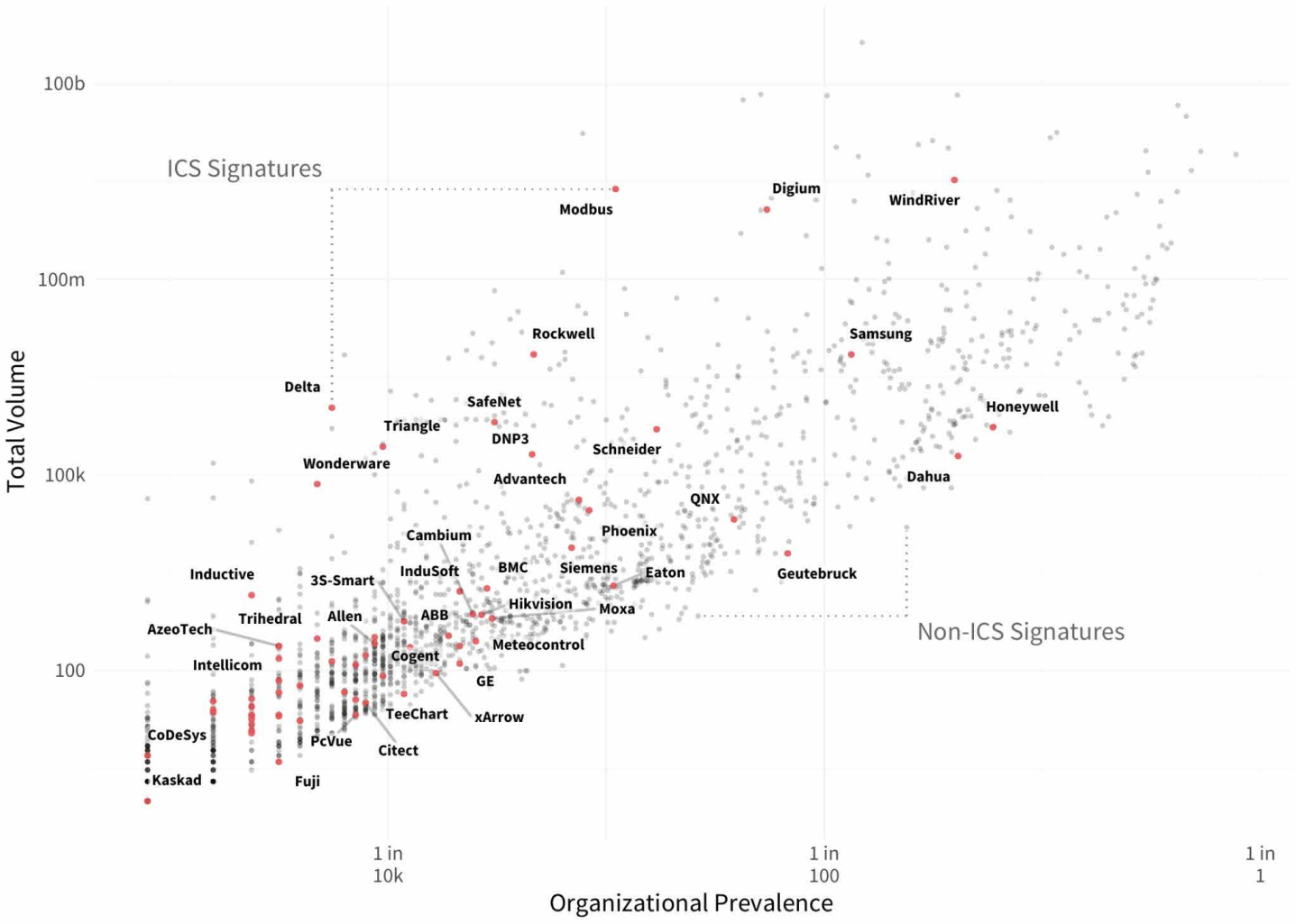


Figure 11: Prevalence and volume of exploits targeting OT (red) and IT (gray) in 1H 2021.

The placement of specific ICS in Figure 11 is remarkably consistent with what we observed from a similar chart a year ago. That points to steady interest from threat actors to identify OT vulnerabilities as well as the inclusion of said vulnerabilities into various exploit tools that lower the cost of attack. The result is that script kiddies are at least as likely to find your exposed OT as APT groups.

One notable exception to the steady drumbeat of ICS detections during the first half of the year was the increasing prevalence and volume of exploits targeting WindRiver VxWorks systems. VxWorks is purportedly the most widely-used real-time operating system (RTOS) in the world and therefore has a large potential attack surface. The RTOS has a history of high-profile vulnerabilities, including a slew of them identified by Rapid7 in 2010 and the more recent "Urgent/11" disclosed by Armis Labs in 2019.

Armis published an update to the Urgent/11 in mid-December of 2020, claiming that 97% of the OT devices impacted by URGENT/11 had not been patched. It's possible that this served to grab the attention of would-be attackers, resulting in a surge of reconnaissance activity probing for those vulnerabilities. That theory is supported by the fact that one of the most prevalent detections indicates attempted scans to ascertain the version number of VxWorks. While not particularly threatening in and of itself, that reconnaissance likely targets additional known flaws in the VxWorks TCP/IP stack, several of which have RCE potential.

The overall message here is that OT exploits are more common than you might think, indicate increasing interest from attackers, and therefore cannot be ignored. The best way to protect ICS, of course, is to find and fix vulnerabilities before they're attacked in the wild by malicious parties. To help with that, Fortiguard Labs are ramping up efforts to identify and disclose zero-days affecting ICS. In this half alone, we have submitted multiple vulnerability reports to Schneider Electric and are working together to protect our customer environments.

Emotet Takedown and Other Law Enforcement Actions

In January, law enforcement authorities from multiple countries including the US, Netherlands, United Kingdom and Germany took down the Emotet botnet infrastructure in a coordinated operation designed to disrupt arguably one of the most prolific malware operations in recent history. The operation involved the near-simultaneous taking over of several hundred servers worldwide that were being used as command-and-control servers and the redirecting of traffic from infected systems to infrastructure controlled by law enforcement.

The Emotet botnet was widely used to distribute a variety of malware including information stealers, Trojans, and ransomware. Groups that used the botnet included the operators of the prolific Ryuk and Qakbot ransomware families and the Trickbot banking Trojan. So, its takedown represented a big blow for the criminals using the botnet to distribute their malware.

Similar standalone and collaborative takedown operations in different countries resulted in the disruption of other major criminal ventures in the first half of 2021, most notably the Egregor, NetWalker and Cl0p ransomware operations. These operations represented a major step forward in efforts by governments and law enforcement to curb cybercrime. The law enforcement operations were bolstered by sanctions and indictments that the US government and its allies announced in recent months against various state-backed APT groups for attacks like the ones on SolarWinds, Colonial Pipeline and JBS. Also encouraging were the voluntary exits from the scene of some cybercrime groups such as DarkSide, Avaddon and Ziggy—and the refusal by some underground forums to deal in ransomware—in the aftermath of the Colonial Pipeline attacks. Their actions suggested that at least a few cybercrime groups are finally becoming more concerned about law enforcement action.

However, as laudable as the successes have been for the good guys, the impact of law enforcement action and voluntary exits are likely as always to be temporary. Fortinet's data, for instance, showed a slowdown but not an eradication of threat activity following the Emotet takedown (see Figure 12). Activity related to TrickBot and Ryuk variants persisted even after the Emotet botnet was taken offline, albeit at reduced volume. Other vendors also reported a temporary decline in malware detections in the immediate aftermath of the takedown followed by a gradual return to the usual volumes as threat actors turned to other sources for distributing malware.

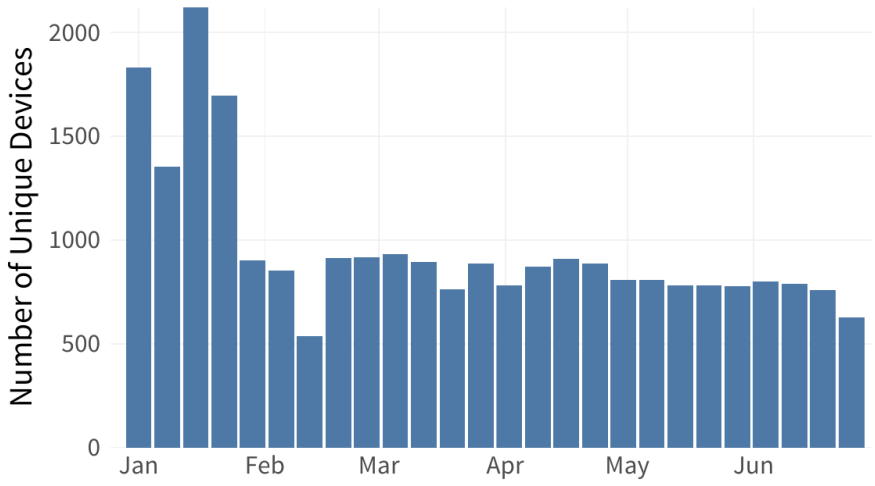


Figure 12: Detections of Emotet botnet communications in 1H 2021.

The data is another demonstration of just how hard it is to eradicate cyber threats and a reminder for organizations not to let news of law enforcement wins and voluntary cessation of malicious activity by some cybercrime groups be an excuse to let their guard down. Such actions are certainly worthwhile, but cleaning up the cybercrime ecosystem takes a lot of work by many organizations over a long period of time. This report is just one small part of how we're contributing to these efforts, and we hope it helps you better prepare for whatever the second half of 2021 has in store for us.

Did You Know...

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 are currently leading a project to map the cyber criminal ecosystem, better understand relations and business operations so we can create more tactical disruption efforts.

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.

[1] IDC Worldwide Security Appliance Tracker, April 2020 (based on annual unit shipments of Firewall, UTM, and VPN appliances)

August 20, 2021 10:54 AM

1221850-0-0-EN