FEBRUARY 2021

Global Threat Landscape Report

A Semiannual Report by FortiGuard Labs

Table of Contents

2H 2020 **Introduction and Key Findings**

The world rarely comes to a consensus on anything, but pretty much everybody agrees that putting 2020 behind us was a good thing. In many ways, we'd also prefer to move rather than revisiting the cyber threat landscape of the past year. But like it or not, the echoes of 2020 continue to reverberate into 2021 in both the physical and digital worlds, and we ignore that fact to our peril. Thus, we're going back into the second half of 2020 (2H 2020) so we can move forward into a better, more secure future. Please join us.

The SolarWinds of Change

There's a good chance that SolarWinds is the "Target breach" equivalent of supply chain cybersecurity. Target wasn't the first retail hack, but it was the first that most security people could talk to their families about. Similarly, supply chain attacks have a long history, but SolarWinds seems to have blown the discussion to new heights. Get the scoop and full scope of the campaign across our sensors.

Don't Be So APT To Forget

The SolarWinds breach might have stolen the spotlight in 2H 2020, but plenty of other advanced persistent threat (APT) groups continued unabated in their illicit activities in the shadows. We expose the most active groups, what they're up to, and where they focused operations to close out 2020.

An SOS for IoT and CMS

Internet-of-Things (IoT) devices and content management systems (CMS) continue to be at the front lines in the battle for the internet. Nine of the top 10 exploits target technologies falling into one of these categories. They might not be your most critical assets, but there's a good chance they're network neighbors to your critical assets. Be a good neighbor and keep them on a tight leash.

The Trials of Home Pwnership

Sticking with the battle theme, the elevated interest in IoT devices may be a type of flanking maneuver. The barriers between home and corporate offices have eroded in 2020, meaning that "pwning" a home puts adversaries one step closer to pwning their own business. Put them out of business anticipating and thwarting their plans using intel shared in this report.

Relationships Built on (Un)Trust

The work-from-home (WFH) transition has been tough on many, but a positive outcome is that it could be the final nail in the coffin of trust-based security. A disappearing perimeter puts ever-growing pressure to move security monitoring and enforcement to every device. Human relationships might be built on trust, but it's increasingly apparent that distrust builds healthier IT relationships.

Hunting Game for Big Gain

It seems we do a "Rise of Ransomware" story in every edition, yet here we are again. Ransomware activity jumped 7x from the start of the half to the end, earning another headlining act. The continued evolution of Ransomware-as-a-Service (RaaS), an emphasis on "Big Game Hunting" (big ransoms for big targets), and the threat of disclosing compromised data if demands weren't met created a market for massive growth that cyber criminals turned into big profits.

Exploits of Epidemic Proportions

COVID made "flatten the curve" a household phrase in 2020, but did you know the concept also applies to vulnerability exploits? Our final story tracks the spread of 1,500 exploits over the last two years to shed light on how fast and how far they propagate in the wild. What's the likelihood you'll be exposed? Keep reading to find out!

Top Threats During 2H 2020

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 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 2020.

The MITRE ATT&CK framework is an increasingly popular lens for analyzing cyber threats by classifying 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 FortiGate intrusion prevention system (IPS) sensors provide excellent visibility into this type of activity around the world. We'll use additional sensors to expand that visibility deeper into ATT&CK later in this report, but let's get things started with the top 10 most-probed technologies over the second half of 2020.

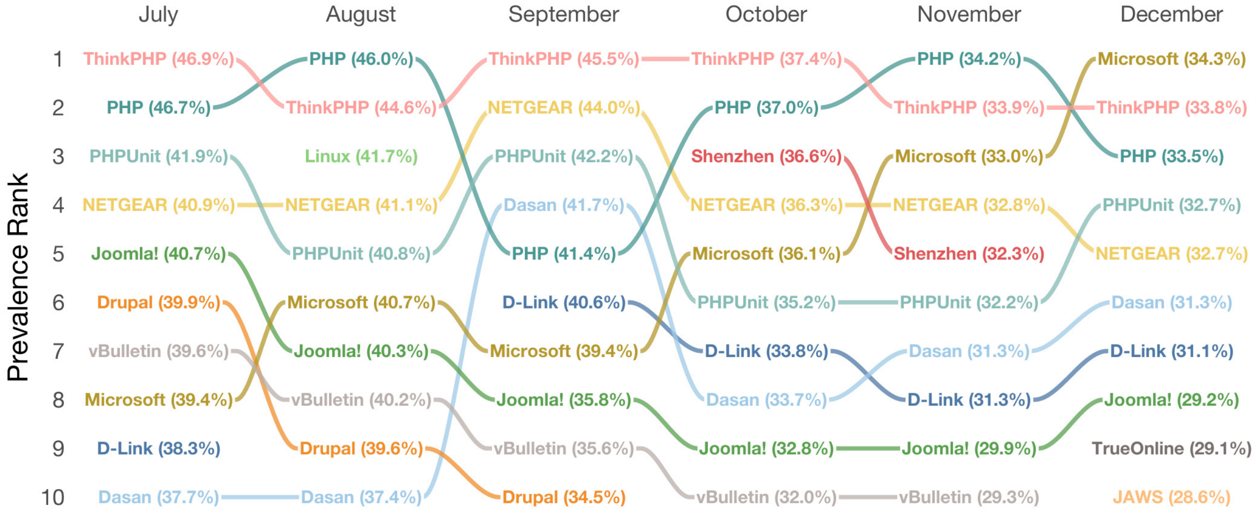


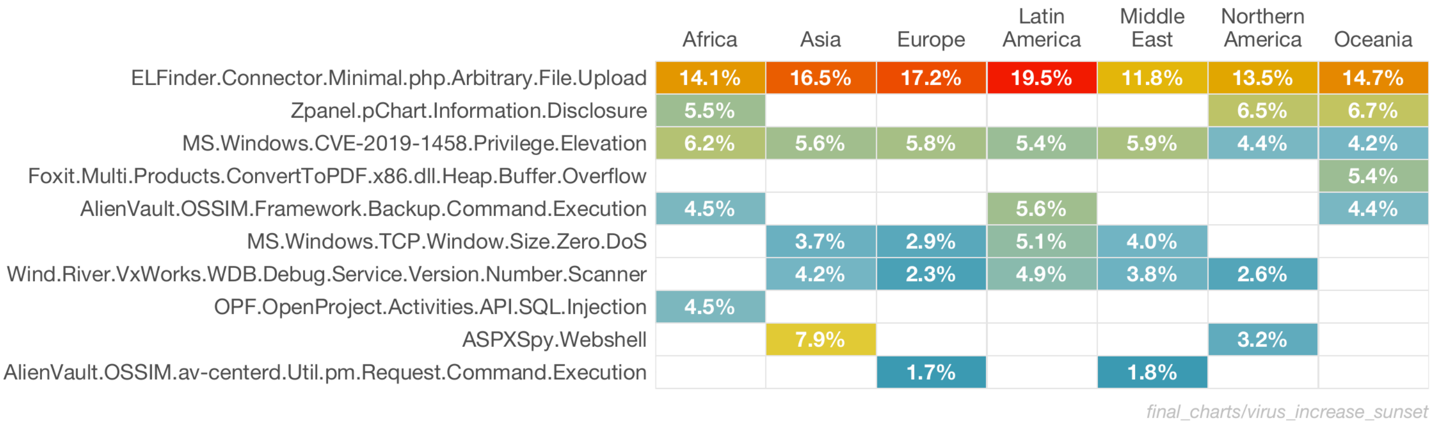
Figure 1: Most prevalent IPS detections by technology during 2H 2020.

Regardless of the month, the listing of top exploit detections can pretty much be summed up in two acronyms: CMS (content management systems) and IoT (Internet of Things). CMS like ThinkPHP, Joomla, Drupal, and vBulletin have long supplied cyber criminals with soft targets that make for easy access into enterprise environments. Since they're top of mind for attackers, they should be top of mind for defenders as well.

IoT devices also fall in that category of soft/attractive targets. In our 1H 2020 report, we spotlighted a marked increase in detected attempts to exploit vulnerabilities in consumer networking and other connected devices. We speculated this trend may parallel the transition to remote work in the wake of the COVID-19 pandemic. It's possible that attackers are seeking to subvert the less-than-enterprise-grade security inherent to many of these devices since they're now effectively part of the corporate perimeter. That means employees may be accessing corporate resources from a compromised environment—a security model to which many organizations are unaccustomed.

The targeting of emerging edge environments like the home office and the cloud was one of our Cyber Threat Predictions for 2021. This trend could be the final nail in the coffin of trust-based security. A continually expanding and eroding perimeter puts ever-growing importance on moving deep security monitoring and enforcement to every device—trusted or otherwise. Human relationships might be built on trust, but it's increasingly apparent that zero trust builds healthier IT relationships. Learn how Fortinet implements Zero Trust Access for more comprehensive visibility and control of all devices across every part of the network.

Tracking the extreme front-runners of exploitation activity in the wild is certainly useful, but keeping tabs on the up-and-comers is likely more relevant to readers of a report like this. Figure 2 picks up that banner by presenting the IPS detections exhibiting the biggest gains during the latter half of 2020. More specifically, Figure 2 lists the top 5 "gainers" for each global region in terms of the proportion of organizations reporting detections.



	Africa	Asia	Europe	Latin America	Middle East	Northern America	Oceania
ELFinder.Connector.Minimal.php.Arbitrary.File.Upload	14.1%	16.5%	17.2%	19.5%	11.8%	13.5%	14.7%
Zpanel.pChart.Information.Disclosure	5.5%					6.5%	6.7%
MS.Windows.CVE-2019-1458.Privilege.Elevation	6.2%	5.6%	5.8%	5.4%	5.9%	4.4%	4.2%
Foxit.Multi.Products.ConvertToPDF.x86.dll.Heap.Buffer.Overflow							5.4%
AlienVault.OSSIM.Framework.Backup.Command.Execution	4.5%			5.6%			4.4%
MS.Windows.TCP.Window.Size.Zero.DoS		3.7%	2.9%	5.1%	4.0%		
Wind.River.VxWorks.WDB.Debug.Service.Version.Number.Scanner		4.2%	2.3%	4.9%	3.8%	2.6%	
OPF.OpenProject.Activities.API.SQL.Injection	4.5%						
ASPXSpy.Webshell		7.9%				3.2%	
AlienVault.OSSIM.av-centerd.Util.pm.Request.Command.Execution			1.7%		1.8%		

final_charts/virus_increase_sunset

Figure 2: IPS detections with the largest growth in prevalence in each region during 2H 2020.

The values at each intersection indicate the prevalence in the second half of 2020. So, for instance, exploits against the ELFinder arbitrary file upload bug surged to 12% to 20% of organizations, depending on region. That may not seem like much, but it actually places this exploit among some elite company (less than 1% of exploits reach that level of prevalence). Factors fueling its growth include: 1) it's a WordPress plugin (see CMS trend from Figure 1) with approximately 700,000 deployments around the world and 2) it's easily exploitable by remote attackers, earning it a perfect 10 from CVSS.

Another notable global gainer is a privilege escalation vulnerability affecting multiple Windows Server and Desktop versions. CVE-2019-1458 achieved notoriety after being used extensively over the last year by North Korean threat actors in the WizardOpium operation and NetWalker ransomware. It doesn't have the scale of some of the other exploits in Figures 1 and 2, but the fact that it's associated with such high-profile campaigns certainly justifies updating those Windows systems.

We've added some links below from our Threat Encyclopedia to help you get started researching other gainers that grab your attention in Figure 2. The context provided there should be useful in understanding the associated vulnerability and determining your organization's exposure to it. Many entries also include recommended actions from the vendor of the affected device. And if you're a Fortinet customer, you'll also find additional information such as product coverage, defaults taken by those products, etc. Happy hunting!

- Zpanel.pChart.Information.Disclosure
- Foxit.Multi.Products.ConvertToPDF.x86.dll.Heap.Buffer.Overflow
- AlienVault.OSSIM.Framework.Backup.Command.Execution
- MS.Windows.TCP.Window.Size.Zero.DoS
- Wind.River.VxWorks.WDB.Debug.Service.Version.Number.Scanner
- OPF.OpenProject.Activities.API.SQL.Injection
- ASPXSpy.Webshell
- AlienVault.OSSIM.av-centerd.Util.pm.Request.Command.Execution

Continuing our progression through the ATT&CK framework brings us to the Execution phase, where attackers attempt to deploy and run malicious code on a target system. Thus, samples detected by our various anti-malware solutions offer insight into popular techniques for establishing a foothold within corporate environments. Figure 3 ranks the most prevalent malware delivery vectors from July through December 2020.

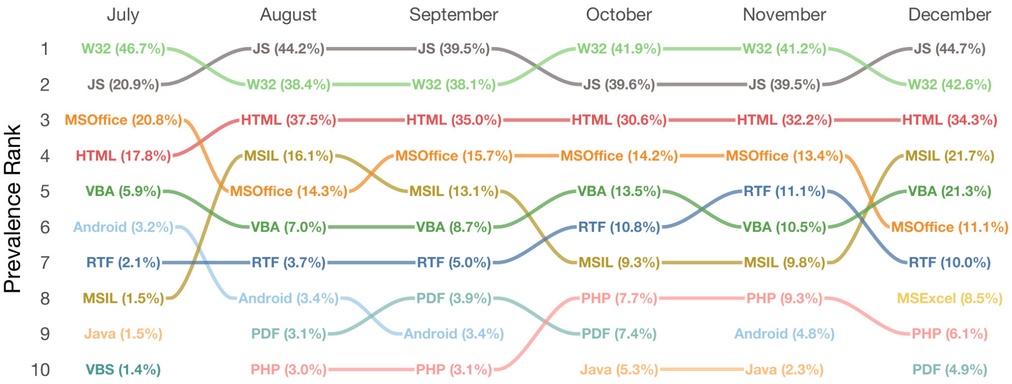


Figure 3: Most prevalent malware categories by month during 2H 2020.

Rolling up malware into delivery formats like those shown in Figure 3 yields useful insight into all the various ways adversaries attempt to get their code running on target systems. If you're hoping for a listing of specific variants, stay tuned—we're headed there next. For now, though, it's worth noting how and where malware is targeting us, broadly speaking. On that topic, Figure 3 reveals a few common themes.

The first vector through which malware authors try to get us is Microsoft platforms. That's certainly nothing new, but the presence of 32-bit Windows executables (W32), MS Office products, Visual Basic (VBA), and the Microsoft Intermediate Language (MSIL) must be acknowledged.

From Figure 3, we can also see that they're trying to leverage the documents we constantly create and consume during the typical workday. This includes some of the aforementioned MS Office applications, plus RTF and PDF documents. Again, not new information. But it's always good to have a reminder that we can't let ourselves be lulled into trusting common file formats and attachments. That's especially true when there's a great deal of these exploits leveraging vulnerabilities that don't depend on user interaction or macros to trigger.

Web browsers are another battlefront based on the results in Figure 3. The HTML category includes malware-laden phishing sites and scripts that inject code or redirect users to malicious sites. Such threats inevitably rise during times of social unrest and global issues. This well-known fact becomes more concerning in light of the recent WFH trend. Employees who typically benefit from web filtering services when browsing from the corporate network now find themselves more exposed when doing so outside that protective filter. It's a scary world out there—don't leave them to fend for themselves!

Now on to particular malware variants picked up by our sensors around the world. Figure 4 compares the percentage of organizations detecting the top strains in each region. Not surprisingly, we observe many variations of the broad categories described above. You can find more details on anything listed that catches your eye using our Threat Encyclopedia.

	Africa	Asia	Europe	Latin America	Middle East	Northern America	Oceania
JS/ScrInject.B!tr	28.0%	15.0%	14.5%	19.1%	21.0%	16.0%	19.1%
JS/Agent.BI!tr	18.9%	8.1%	12.4%	13.1%	11.5%	11.6%	14.4%
MSOffice/CVE_2017_11882.C!exploit	12.3%	12.6%	13.1%	6.7%	12.5%	4.1%	7.5%
HTML/ScrInject.B!tr	14.9%	9.1%	7.4%	5.3%	10.2%	4.3%	8.0%
MSOffice/CVE_2017_11882.B!exploit	8.4%	10.0%	9.9%	5.5%	10.5%	3.3%	6.4%
W32/Agent.OAY!tr	6.8%	12.9%	7.6%	7.2%	5.6%	7.7%	6.6%
MSIL/GenKryptik.EWCI!tr	8.1%	7.7%	8.7%	5.2%	9.2%	3.3%	5.9%
JS/Redirector.IF!tr	7.1%	5.1%	9.2%	4.8%	5.4%	6.9%	9.8%
MSIL/Kryptik.SHS!tr	7.3%	7.6%	6.7%	4.9%	6.9%	2.7%	6.2%
VBA/Agent.SNH!tr.dldr	8.2%	5.0%	8.9%	7.9%	3.4%	3.0%	8.8%
JS/Script.INF!tr	4.8%	4.3%	3.8%	4.8%	6.8%	13.6%	11.4%
JS/Miner.BP!tr	8.8%	5.5%	5.9%	6.9%	5.1%	5.0%	2.9%
VBA/Agent.LXMF!tr	3.8%	4.5%	8.8%	4.5%	3.8%	5.0%	6.7%
RTF/CVE_2017_11882.BX!exploit	4.6%	7.0%	6.7%	4.7%	7.7%	1.8%	4.9%
JS/Agent.79EE!tr	6.9%	9.7%	3.4%	6.5%	4.0%	2.8%	3.2%

Figure 4: Most prevalent malware by region during 2H 2020.

Due to the length and format of the signature name, the three variants of malware exploiting CVE-2017-11882 stick out like a sore thumb. According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA), this is one of the top 10 vulnerabilities exploited by state-affiliated threat actors. The Cobalt group, Loki, Ursnif, Zbot, and Fareit/Pony are a sampling of the threat actors and malware known to exploit CVE-2017-11882. It's also been used in several COVID-themed campaigns. All that to say, keep those malware defenses tuned to snuff out this one.

While IPS and malware trends usually show the pre-compromise side of cyber threats, botnets give a view of post-compromise activity. In ATT&CK parlance, botnet traffic is most indicative of Command and Control (C2) activity, whereby infected systems communicate with remote malicious hosts for further instructions. Figure 5 tracks the prevalence of the most common botnets month over month in 2020. Note that the percentages in Figure 5 are based on organizations detecting botnets, which was about 1% of all firms. Thus, you can read it like "About 75% of the 1% of firms reporting any botnet in December detected Mirai."

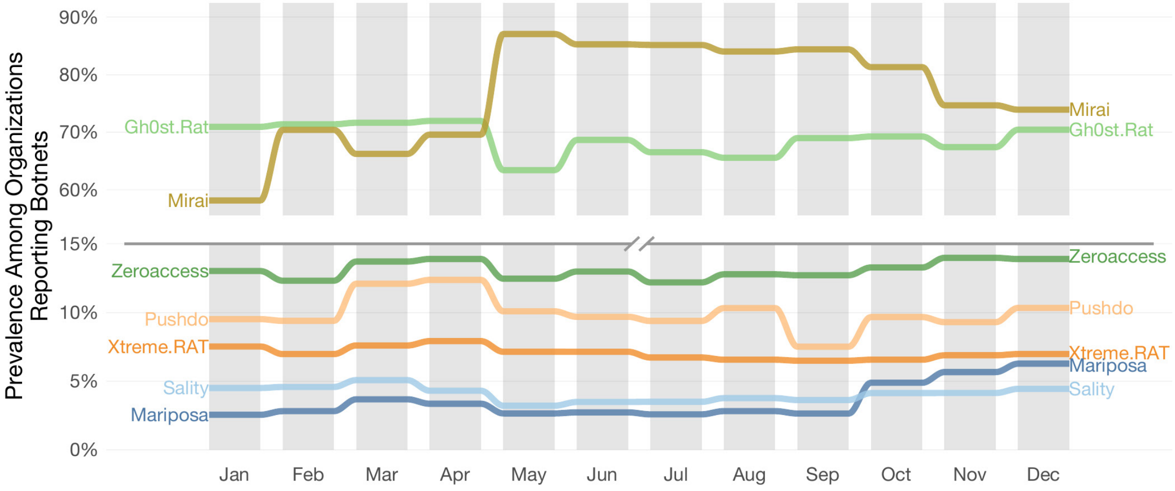


Figure 5: Most prevalent botnet detections by month during 2020.

In our 1H 2020 report, we observed a sharp uptick in activity tied to the Mirai botnet. We observed that this trend could suggest cyber criminals are looking for a backdoor into the corporate perimeter by exploiting consumer networks and devices used by WFH employees in the wake of the COVID-19 pandemic. Mirai's continued reign among botnets, along with the predominance of IoT-related IPS detections presented back in Figure 1, suggests this trend continued over the remainder of 2020.

That said, the prevalence of Mirai detections began declining after the peak in May. We hesitate to read too much from those tea leaves, but an optimistic inference is that it could foreshadow a return to the "Old Normal" of a post-peak COVID world we're (hopefully) entering in 2021. That would be a welcome change, because the "New Normal" is getting pretty old.

Featured Stories From 2H 2020

The SolarWinds Breach That Shook the Industry

News broke last quarter about nation-state attackers hiding a backdoor called SUNBURST/Solorigate in legitimate updates of SolarWinds' Orion network management software and distributing it to numerous organizations worldwide. The revelation shook the industry and exposed troubling weaknesses in enterprise defenses against advanced threats targeting the digital supply chain. Victims of the campaign included several U.S. government agencies and even leading technology companies such as Microsoft and security vendor FireEye. Beyond those directly affected, the event should be a wake-up call that enterprise defenses can be undermined by weak links in the (often long) chain of partners and suppliers.

To pull off the attack, the adversary broke into SolarWinds' build system and inserted the backdoor into a digitally signed component of the Orion network management framework. The malware lay dormant for two weeks before retrieving commands for collecting and transferring specific data, conducting reconnaissance and halting systems services and other malicious actions. On systems of specific interest, the adversaries—believed to be Russia-based—used the backdoor to deploy additional malware including customized versions of the Cobalt Strike Beacon post-compromise attack kit for lateral movement.

Analysis of the attack revealed the threat actors had gone to extraordinary lengths to maintain operational secrecy around the initial compromise of SolarWinds, the distribution of the malware, the deployment of the second-stage payload, and in C2 communications. By hiding the malware in a trusted network management tool from a trusted vendor, the attackers managed to gain highly privileged access on the networks of some of the largest organizations in the world.

The malware utilized the legitimate Orion Improvement Program protocol and stored its results within Orion plugin files to avoid detection. The threat actors used a limited set of malware tools to carry out their malicious activities. Stolen credentials provided the means for remote access. Operational security measures took the form of C2 servers with IP addresses located within the victims' country. By gaining access to the victim's Security Assertion Markup Language (SAML) token signing certificate, attackers were able to forge tokens for infiltrating resources across on-premises and cloud environments.

The campaign exposed several weaknesses in industry defenses against advanced persistent threat (APT) actors. Most anti-malware and endpoint detection and response tools failed to spot the initial backdoor or malicious activity until signatures were developed and indicators of compromise (IOCs) released after the breach was discovered. That's not necessarily a knock against them; that's simply how they function. Likewise, SolarWinds wasn't aware of the poisoned updates it was distributing to customers worldwide for several months.

By customizing the second-stage payload for individual victims, the attackers showed how threat actors can bypass indicator-based detection mechanisms. By using a previously known technique called "Golden SAML" for forging SAML authentication tokens, they demonstrated how adversaries can maintain virtually undetectable persistent access on compromised networks.

As the attack unfolded, we saw a flurry of information being shared from victim and security vendor organizations, including Microsoft and FireEye. FortiGuard Labs monitored this emerging intelligence closely, using it to create IOCs to detect related activity going forward. Predictably, we observed a **huge** increase in connections matching those IOCs. When all was said and done, FortiGuard Labs detected over 300,000 requests to infrastructure associated with SolarWinds!

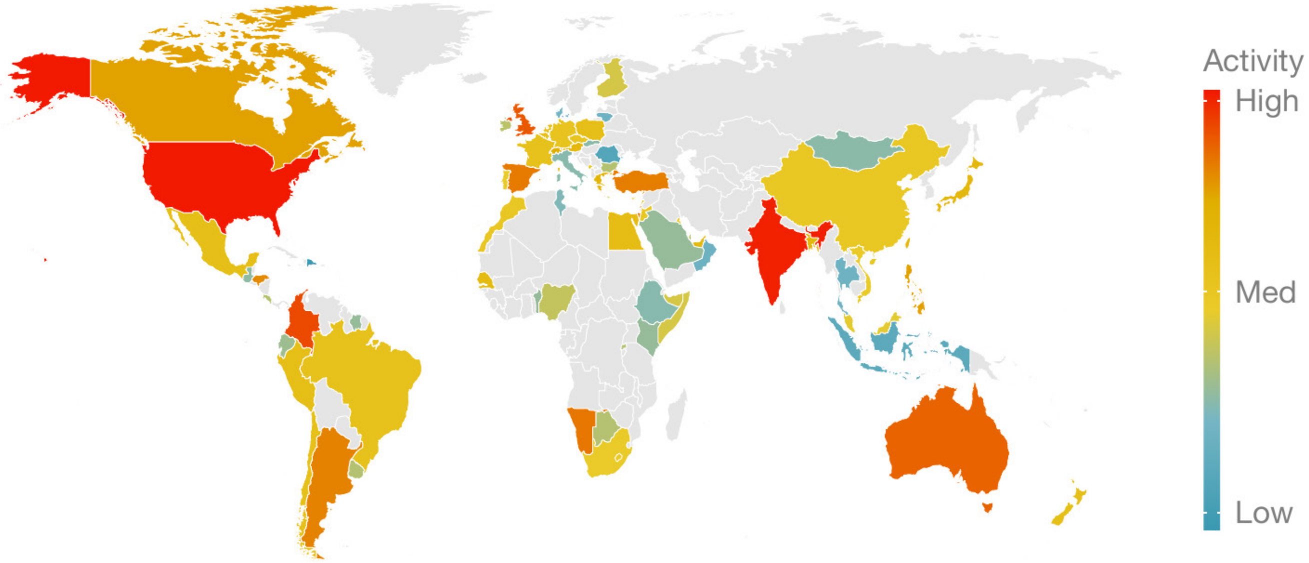


Figure 6: Detected communications with internet infrastructure associated with SUNBURST during December 2020.

Not only did we uncover a plethora of activity as intelligence emerged, but our ongoing tracking of the extent of the SolarWinds campaign revealed it to be truly global in nature. As seen in Figure 6, the "Five Eyes" exhibited particularly high rates of traffic matching malicious IOCs. Evidence of possible "spillover" or opportunistic targets further emphasizes the scope of modern supply chain attacks—except most notably in Russia.

Though some have described the group behind the SolarWinds campaign as a highly sophisticated Russian government-backed operation, multiple security vendors who have analyzed the campaign have so far been unable to—or have refused to—publicly attribute the attacks to any specific country. FireEye, one of the many victims of the campaign, has described the group as previously unknown and is currently tracking it as "UNC2452." Meanwhile, Volexity has noted that evidence suggests the SolarWinds attack was carried out by a group that it has been tracking known as "Dark Halo."

Regardless of the sponsor-country, many security researchers have described UNC2452/Dark Halo and its campaign as one of the most significant and sophisticated attacks they have observed in more than a decade. So, where do we go from here? The good news for Fortinet customers is that FortiGuard Labs researchers are diligently updating our Security Fabric components with the latest intelligence to detect and mitigate threats associated with this campaign.

Beyond that, the first step is creating a supply chain risk management plan to establish policies and procedures for dependencies and exposures. This plan should document key risks throughout the system development life cycle, including design, manufacturing, production, distribution, acquisition, installation, operations, maintenance, and decommissioning. At a more tactical level, we encourage all organizations to update antivirus and IPS signatures and ensure all known SolarWinds vulnerabilities have been remediated.

It's also a good opportunity to impress upon security leadership the importance of maintaining situational awareness through timely threat intelligence so they can quickly reprioritize strategy and defenses when the situation calls. There's no guarantee for preventing whatever the next SolarWinds-like campaign might be, but putting intelligence to work for you as quickly as it emerges is the next best thing to stopping it altogether.

Beyond SolarWinds: An APT Roundup

The actors behind SolarWinds might have been the headliner of 2020's second half, but a cast of supporting actors joined the stage as well. We'll round them up so you're better equipped to knock them down.

APT groups continued to exploit the COVID-19 crisis in a variety of ways in the second half of 2020. The most common among them included attacks focused on gathering personal information in bulk, stealing intellectual property, and nabbing intelligence aligned with the APT group's national priorities. This was noted by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) in an advisory back in May. The second half also witnessed an increase in APT activity targeting organizations involved in COVID-19-related work including vaccine research and development of domestic and international healthcare policies around the pandemic. Targeted organizations included government agencies, pharmaceutical firms, universities, and medical research firms.

Some of the groups that we tracked in the latter half of 2020 were involved in other activities. One of them was BeagleBoyz, a relatively new North Korean APT actor that was observed robbing banks via an ATM cash-out scheme that U.S. law enforcement dubbed FASTCash 2.0. The group, whose typical modus operandi is social engineering, spear phishing, and watering hole attacks, is believed to be linked to activity associated with North Korea's notorious Lazarus/HIDDEN COBRA APT. U.S. authorities estimate the BeagleBoyz have attempted to steal $2 billion from financial institutions around the world.

The Lazarus Group itself meanwhile was observed last August targeting organizations in the cryptocurrency vertical. The campaign involved the attackers sending a phishing document to LinkedIn accounts of certain people at targeted organizations. The document purported to be a job advertisement for a blockchain company but contained a lure that led to malware being distributed on the targeted environment.

Meanwhile, MUMMY SPIDER, the APT group that spawned the prolific Emotet Trojan, resurfaced in the second half of last year with yet another version of their malware. The new version, distributed via email, was designed for harvesting email addresses, spamming, stealing account credentials, and spreading across local networks. FortiGuard Labs observed a steady thrum of activity related to MUMMY SPIDER and the new Emotet version through 2H 2020. Perhaps that's part of what motivated a consortium led by Europol to disrupt the Emotet botnet in late 2020.

In August, Russia's well-known Fancy Bear (aka Sofacy/APT28 group) was observed distributing a particularly nasty piece of Linux-based malware dubbed Drovorub on target systems. The multi-component malware is believed to have been developed for use by the Russian military intelligence apparatus. It allowed attackers a way to take full remote control of compromised systems and/or direct them via attacker-controlled infrastructure or hosts.

Outside those highlighted above, many other APTs closed out 2020 with their usual (and sometimes unusual) antics. Figure 7 shows an activity trendline and country-level breakdown of connections to IOCs linked to the APT groups listed via intelligence collected by FortiGuard Labs. The list includes the six most active APTs (Turla, Fancy Bear, Lazarus, MuddyWater, TA505, OilRig) plus two additional groups that showed elevated activity during the latter half of 2020 (Kimsuky, Promethium).

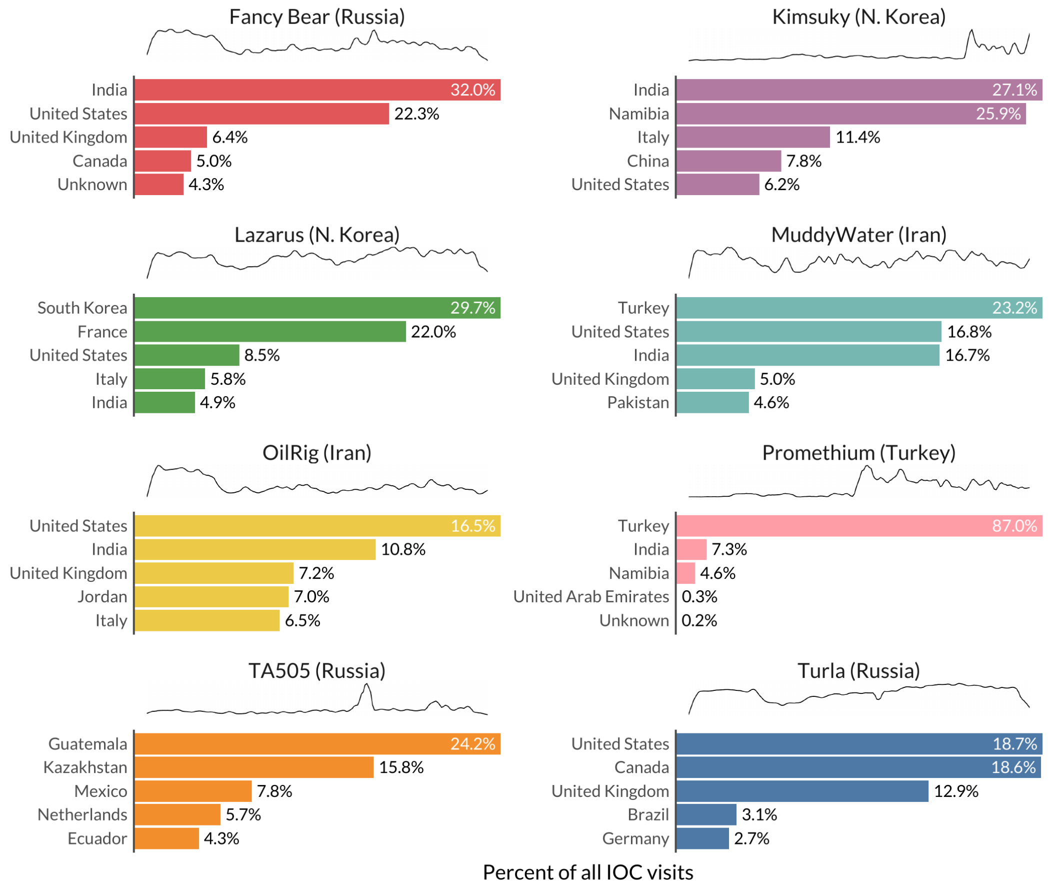


Figure 7: Origin of detected connections to IOCs associated with select APT groups in 2H 2020.

Among the groups shown in Figure 7, Fancy Bear and Lazarus already received some spotlight. So we'll shine it on a few others as we conclude this 2H 2020 APT roundup.

Turla (aka Venomous Bear, Waterbug) is a Russian-based group in operation for the greater part of two decades. They've been tied to espionage activities focused on government entities and embassies all over the world. We logged more connections to Turla-related infrastructure than any other APT group during this time period.

MuddyWater historically targets telecommunications, government services, and oil sectors in the Middle East, but is known to venture outside those circles as well. They've expanded operations and capabilities over the last year or so.

TA505 is a group originating from Russia traditionally associated with spam campaigns, banking Trojans (Dridex), and other financially motivated attacks. After two supposed members were indicted in late 2019, they resumed activities and malware distribution in 2020.

Promethium (aka StrongPity) has been active since ~2002 and is believed to operate out of Turkey. The group has a history of surveillance on political targets. We observed a surge of detections that peaked in July but remained elevated through the end of the year. Other sources have noted similar expansions during 2020.

Kimsuky is associated with the North Korean government that's been active over the last 10 years or more. Steady, low-level activity from July through October bumped up several notches beginning in November. It primarily focuses on South Korean targets, so the activity in India and Namibia is noteworthy.

OilRig purportedly hails from Iran and is known for attacking smaller/weaker members of large supply chains in order to get to their primary target. The group has been linked to attacks against organizations in the Middle East and abroad. In the second half of 2020, they entered the malware innovation game with a backdoor tool called RDAT.

Stories about the latest antics of cyber threat actors make for more than just interesting reading material. The better we know our adversaries and understand their TTPs, the better we're able to align effective defenses against them. We all know persistent adversaries will get in somehow, but successful organizations are able to find and flush them out quickly. Visibility into and focusing on the latest TTPs relevant to your organization's threat profile is a must. Ignorance is their ally, not ours.

The Runaway Ransomware Threat

Ransomware continued to plague organizations around the world in the second half of 2020 just as it has for the past several six-month periods. Our data showed a substantial increase in overall ransomware activity compared to 1H 2020. In fact, FortiGuard Labs analyzed the activity for all signatures that we have at one time or another classified as ransomware, which showed a sevenfold increase in ransomware activity in December compared to July 2020 (see Figure 8).

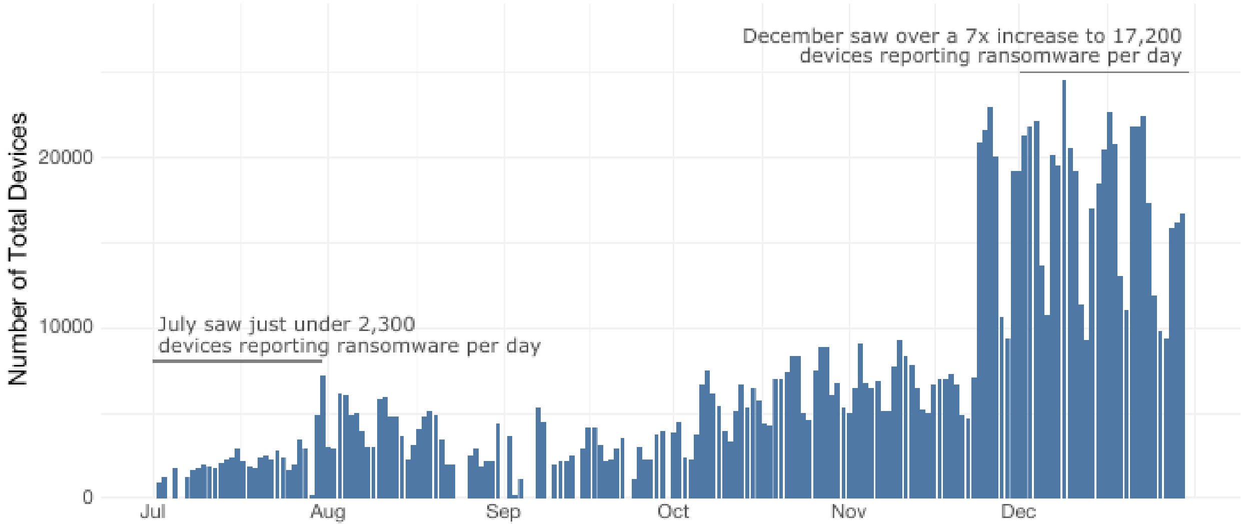


Figure 8: Daily number of devices detecting ransomware variants in 2H 2020.

Among the most active of the ransomware strains that we tracked in 2H 2020 were Egregor, Ryuk, Conti, Thanos, Ragnar, WastedLocker, Phobos/EKING, and BazarLoader. Each of these exhibited varying degrees of prevalence across Fortinet devices, but the common trend among them was an increase in activity over the period (see Figure 9).

For organizations following ransomware trends—which by now should be practically every single one—the increased activity over the last six-month period should come as little surprise. Threat actors have discovered that cryptolocking critical systems and demanding a ransom for the decryption key is a relatively easy way to extort money from organizations regardless of size or the industry to which they belong. This more targeted and sinister form of ransomware scheme has come to be known as "big game hunting." It's been all the rage with the ransomware gangs throughout 2020 and the larger paydays netted by such schemes virtually ensure the trend won't go away anytime soon.

Many adversaries took advantage of the disruptions caused by the COVID-19 pandemic to ramp up ransomware attacks against organizations in the healthcare sector in particular. In October, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Department of Health and Human Services, and the FBI issued a joint advisory warning U.S. hospitals and healthcare services of increased ransomware activity involving TrickBot and BazarLoader malware—both of which we tracked in 2H 2020. Other sectors that were also heavily targeted in ransomware attacks in 2H 2020 included professional services firms, consumer services companies, public sector organizations, and financial services firms.

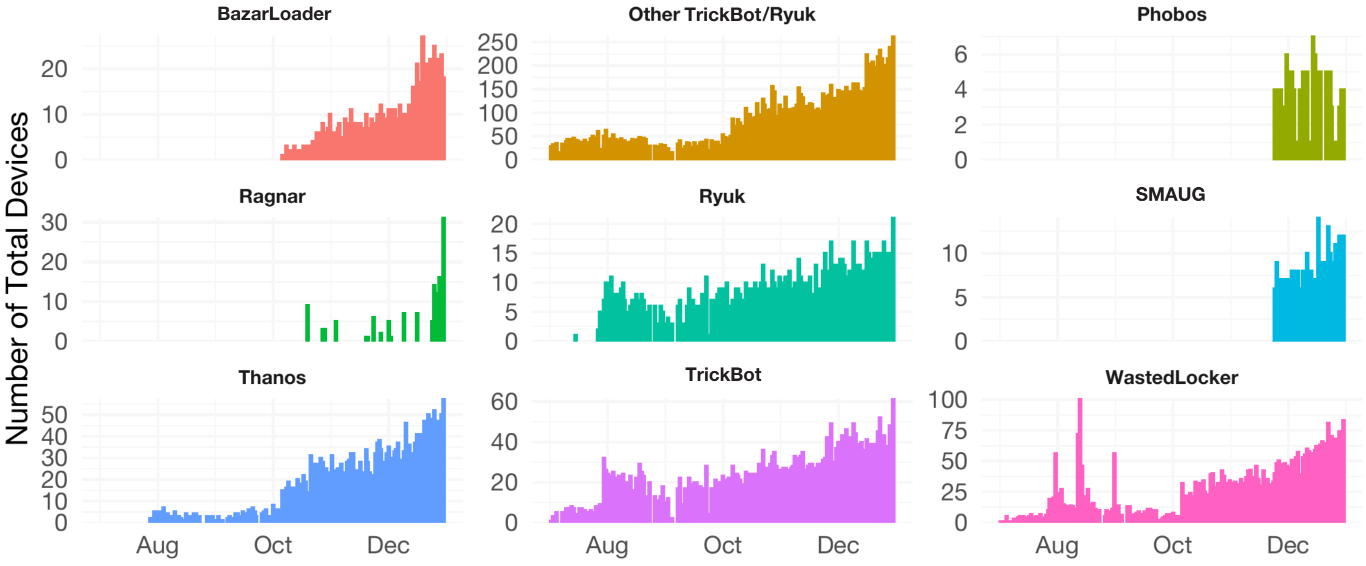


Figure 9: Daily detections of select ransomware strains of interest in 2H 2020.

Multiple trends characterized the ransomware activity that FortiGuard Labs and others observed in 2H 2020. One of the most troubling was the steady increase in ransomware attacks that involved data exfiltration and the subsequent threat to release the data if a ransom was not paid. The use of data theft as additional leverage in ransomware campaigns really only emerged as an adversary tactic in early 2020 but became part of a majority of attacks by the end of the year.

The operators of most major ransomware strains, including Sodinokibi, Ryuk, Egregor, and Conti, all deployed data exfiltration as part of their standard operations last year. Some reported incidents were attacker (sometimes false) claims of data theft to try and scare victims into paying a ransom. In many cases, when victims paid to get attackers to delete stolen data, the attackers reneged and instead leaked or sold the data to others anyway. For organizations, the trend means that robust data backups alone are no longer enough protection against ransomware demands.

A steady growth in Ransomware-as-a-Service (RaaS) options in underground markets also fueled a lot of the ransomware activity in the last six months of 2020. Such services made it easier for bad actors with little skills or resources to launch attacks. One threat actor we tracked offering RaaS was SMAUG, a service that offered threat actors ransomware strains that could be deployed across Windows, MacOS, and Linux platforms. Unlike many RaaS offerings that are restricted to vetted members, SMAUG surfaced in spring last year, and by the end of the year, it emerged as a fully public offering to bad actors willing to pay for the service. Other major players in the RaaS space included the operators of Phobos, Sodinokibi, Conti, and Egregor.

Don't want your organization to fund the latest ransomware money-making schemes? Deprive them of positive cash flow by keeping systems locked down and backed up. The major tactics used by ransomware are the same for many other threats: phishing emails, exploiting software vulnerabilities, and leveraging exposed services like Remote Desktop Protocol (RDP). Beyond shoring up technical controls, create or revisit corporate policies and procedures for handling ransom demands to avoid making tough decisions in the heat of the moment. Still looking for additional strategies for mitigating the ransomware threat? Here are 15 ways to take action now.

How Long Until We're Attacked?

If you have a role in defending enterprise assets from the horde of cyber threats that seek to exploit them, you've probably asked some variation of this question. And perhaps you've been frustrated by the lack of helpful answers. That frustration is understandable because knowing how long we have until exploits targeting the vulnerability du jour spread to our assets is something defenders need to know in order to prioritize remediation efforts and/or deploy compensating controls to minimize risk. In other words, should we fix this now or can we safely push this to work on other, more pressing, issues more likely to be exploited in the short term?

This is difficult to measure because so few organizations have data at the scale necessary to properly study it. Fortinet is one such organization, and FortiGuard Labs has been collaborating with others to help shine light on this topic. We contributed to developing the Exploit Prediction Scoring System (EPSS), an open model for predicting when vulnerabilities will be exploited. Fortinet data was also featured in a study by the Cyentia Institute and Kenna Security to measure remediation and exploitation timelines. We expand on these efforts here.

Figure 10 tracks the progression of over 1,500 exploits detected in the wild over the last two years. Each line represents an individual exploit, tracing the time from signature creation on the x-axis and the probability of detection by organizations on the y-axis. Thus, the path of each line measures the prevalence of exploitation at any given point of time. Most of the lines are grayed out so that we can focus on a few examples, but it should be obvious that the propagation of exploits in the wild varies dramatically. That means the answer to the question posed in the title of this section regarding the time-to-attack is "It depends on which exploit."

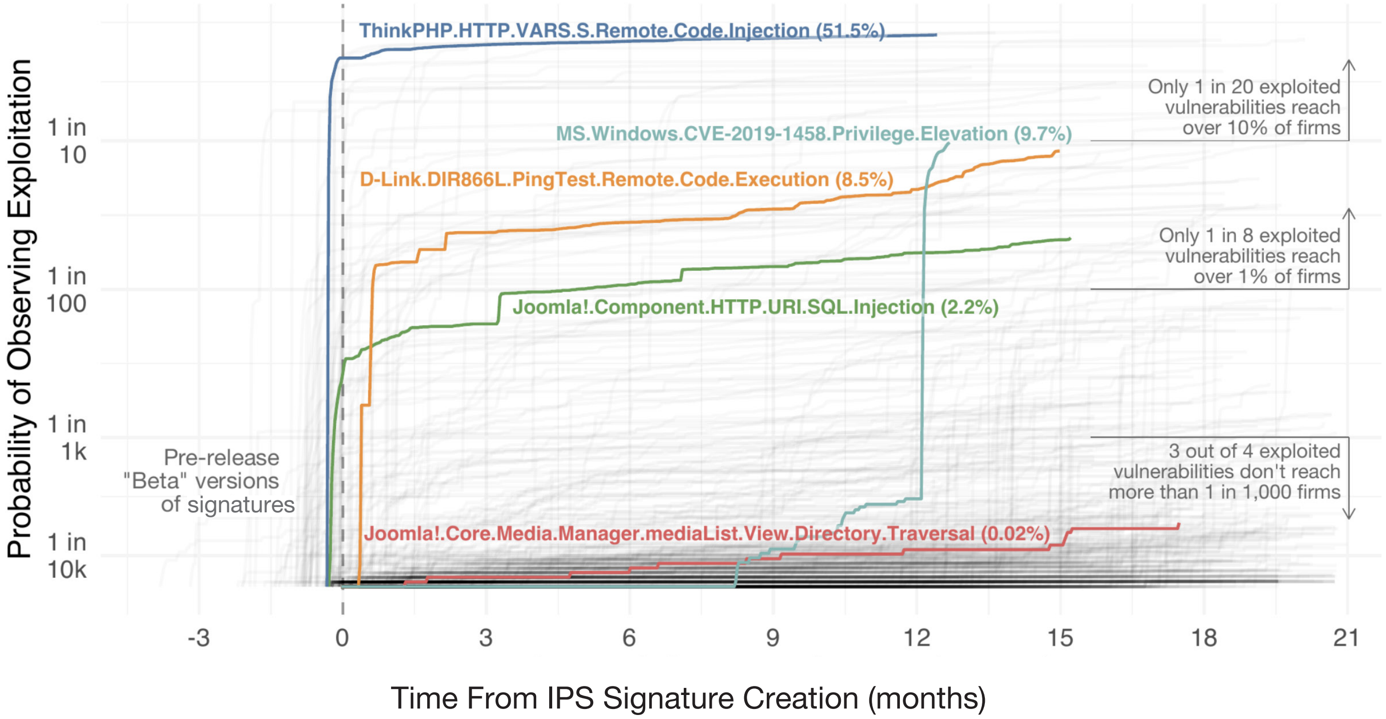
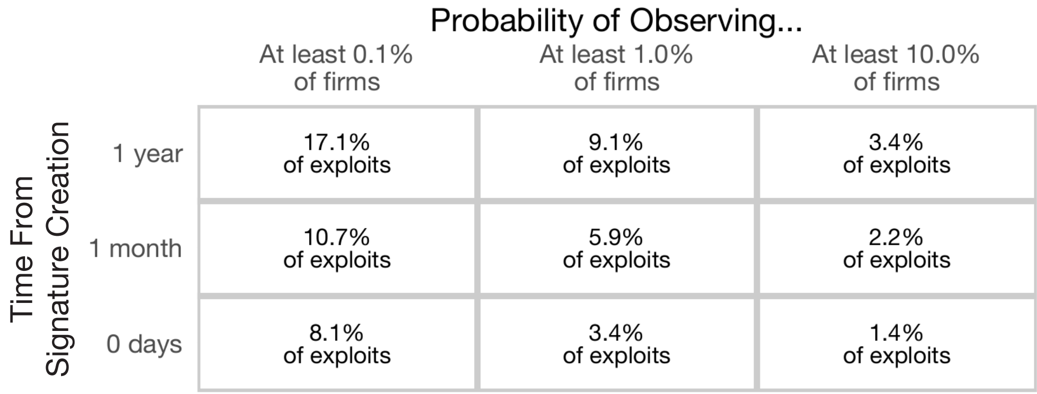


Figure 10: Rate and spread of over 1,500 vulnerability exploits in the wild.

We understand that's not a very satisfying answer, so let's see if we can dredge some useful statistics from the data in Figure 10. One big takeaway from all those jumbled propagation paths is that most exploits have a low probability of being used against organizations (y-axis). Looking at the most targeted technologies way back in Figure 1, one might conclude that exploits routinely hit one-third of organizations or more. But the reality shown here by our IPS detections is that very few vulnerabilities see widespread exploitation in the wild. Most lie in that dark morass of lines near the bottom. Among all exploits logged by our sensors over the last two years, only 5% were detected by more than 10% of organizations. Three out of four exploits didn't reach 1 in 1,000 firms.

Another important takeaway from Figure 10 is that the speed at which attacks spread in the wild differs greatly. Some, like those targeting the ThinkPHP code injection vulnerability, rocket across our sensors as soon as (and sometimes before) the production detection signature is deployed. Others, such as exploits against Joomla Media Manager, methodically crawl their way across a smaller population of organizations. And then you see exploits exhibiting behavior similar to the one against CVE-2019-1458, which begins crawling but shifts into rocket mode about 12 months into its exploitation life cycle.

But how (un)common are exploits that follow the anecdotal path of ThinkPHP or Joomla or CVE-2019-1458 or any of the other lines represented in Figure 10? Thankfully, we don't have to settle for an "it depends" answer to that question. Figure 11 gives us concrete statistics, and in so doing, provides the answer to our original question.



Probability of Observing...

Time From Signature Creation	At least 0.1% of firms	At least 1.0% of firms	At least 10.0% of firms
1 year	17.1% of exploits	9.1% of exploits	3.4% of exploits
1 month	10.7% of exploits	5.9% of exploits	2.2% of exploits
0 days	8.1% of exploits	3.4% of exploits	1.4% of exploits

Figure 11: Statistics on the rate and spread of over 1,500 vulnerability exploits in the wild.

All things being equal, if you pick a vulnerability at random, the data says there's about a 1 in 1,000 chance that any given organization will be attacked. Only 6% of exploits hit more than 1% of firms within the first month, and even after one year, 91% of exploits haven't crossed that 1% threshold. As logic suggests, it's even more rare that exploits reach 10% of the population in those time frames. Bottom line: Most exploits don't spread very far very fast.

It might offer some comfort to know the stats are on our side in terms of being singled out for attacks, but we don't typically manage to the middle, or average, scenario in cybersecurity. We manage to the extremes. Plus, the assumption leading off the last paragraph—all things being equal—may not be true for your organization. For whatever reason, it might be more likely that your organization routinely falls among that targeted (or unlucky) few. If that's the case, the statistics begin shifting against you.

The old adage of "better safe than sorry" applies well here. Unless you have reason to believe you won't see certain exploits, it's safer to assume you'll be on the leading edge of the curves depicted in Figure 10. Focus remediation efforts on vulnerabilities with known exploits, and among those, prioritize the ones propagating most quickly in the wild. Data routinely shows a small fraction of the multitude of vulnerabilities vying for your attention. That's why charts like Figures 1 and 2 are worth their weight in risk-mitigation gold.

We hope those charts and this entire edition of the Threat Landscape Report help you focus on the things that matter most and provide insight so you can act on them accordingly. We'll see you next time to digest and dissect the first half of 2021.

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

www.fortinet.com