AUGUST 2020

# Global Threat Landscape Report

## A Semiannual Report by FortiGuard Labs

1H 2020

# Table of Contents

**Overview and Key Findings** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3

**Top Threats During 1H 2020** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4

Vulnerabilities and Exploits . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4

Malware Detections. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 6

Botnet Activity . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8

**Featured Threats and Trends** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 10

Exploiting a Global Pandemic . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 10

From the DVR to the DMZ. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 11

OT Threats, Past and Present . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 12

Ransomware Spreads Its Wings . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 13

The Age of Exploitation . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 15

# 1H 2020 **Overview and Key Findings**

Years down the road when we all reflect back on 2020, it's unlikely that cybersecurity will displace the COVID-19 pandemic at the top of our collective memories. It's an unprecedented series of events and we'll be dealing with the aftermath for a long time to come. But that doesn't change the fact that the first six months of 2020 also saw significant developments across the cyber threat landscape. Some trends relate to those aforementioned events, while others have their own drivers. We're here to distill it all down so you enter the latter half of the year more prepared for whatever comes next.

### The Rona Was Rampant

The coronavirus spread quickly but it's possible cyber criminals moved even quicker in distributing all manner of pandemic-themed lures and scams. We hit the high points so you don't fall for their next scheme spawned from whatever global event we face next.

### Battle for the Browser

Speaking of lures, web-based malware used in phishing and other campaigns outranked other delivery vectors early this year. We also noted a drop in corporate web traffic due to people surfing from home rather than the office. The combination of those two trends means firms need to button up those browsers.

### The Perimeter Gets Personal

Let's do one more in the work-from-home (WFH) theme. Exploit attempts against several consumer-grade routers and IoT devices made our top IPS detections. We hate making spurious connections but can't help but wonder if this also stems from criminals trying to take advantage of "The New Normal" of the network perimeter extending to the home.

### Ransomware Not Running Away

An attack on a well-known manufacturer in June that interfered with their operations and caused temporary production interruptions at several of the company's facilities capped another six months of ransomware activity targeted at enterprise organizations.

### OT Threats After Stuxnet

June marked the 10th anniversary of Stuxnet, which forever changed the way we view operational technology (OT) security. A lot has happened since then and the Ramsay espionage framework is the latest example of threat actors looking to infiltrate air-gapped industrial environments. Learn how to keep them out.

### The Age of Exploitation

So far, 2020 is on pace to shatter the record for the total number of disclosed vulnerabilities. But 2020 also has the lowest ratio ever recorded for vulnerabilities with active exploits in the wild. Will a lower percentage of a higher number mean more or less work for vulnerability management teams? Read on to find out.

# Top Threats During 1H 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 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.

## Vulnerabilities and Exploits

IPS activity captured by our sensors reveal how adversaries recon and attempt to compromise vulnerable systems. Triggering one of these detection signatures doesn't mean the attack succeeded, but it does provide good intelligence on which types of vulnerabilities and systems are actively in the crosshairs. Top platforms and technologies targeted by exploit activity in the first half of 2020 are plotted month over month in Figure 1. We've taken the liberty of highlighting those that show the greatest movement, with discussion following below.

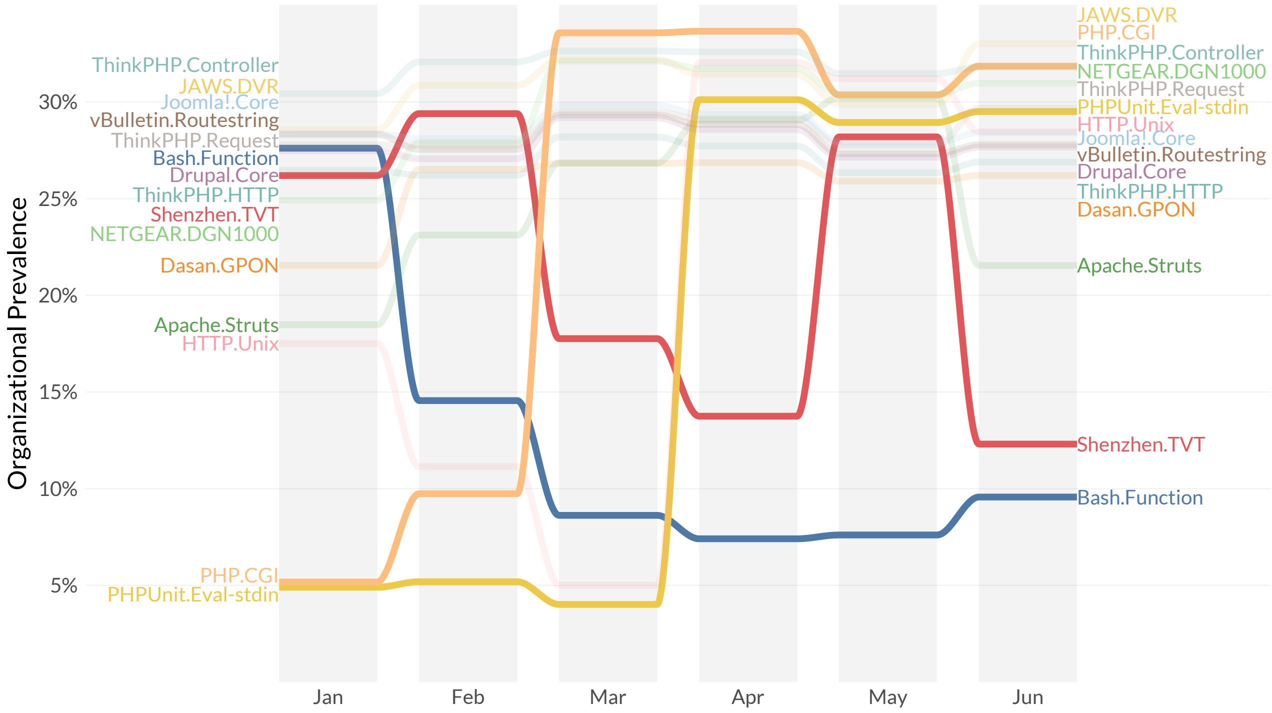


Figure 1: Most prevalent IPS detections by month during 1H 2020.

Let's review the composition of the top detections before getting into the monthly shifts. With one exception (Shenzhen), the list of technologies on the left and right of the figure looks very similar to our prior reports. The seemingly constant presence of content management systems (CMS) like ThinkPHP, Joomla, Drupal, and vBulletin at the top of our charts serves as a reminder that these platforms receive a ton of flak from cyber artillery. We can't stress enough that if your organization uses these tools, they must be diligently maintained.

Setting aside the oft-discussed Apache Struts flaw tied to the Equifax breach of 2017, several other technologies fall in the network device category. We have a featured story on such devices later in this report, so we'll leave it at that for now. Shenzhen, however, is worth calling out here because of its newbie status among the IPS elite. First discovered in 2018, it rocketed from nearly nowhere late last year to a peak as the second most prevalent detection during a week in February. This activity ties back to a single exploit targeting a remote code execution vulnerability in Shenzhen TVT DVR and OEM. The exploit contains indicators that may reflect an association with Lizard Squad, a group known for DDoS attacks against online gaming services. It's yet another example of criminals looking to build massive botnets of consumer IoT devices for assorted schemes.

Beyond listing the top targets, we chose this type of chart to highlight a few of the rather large shifts that occurred. A remote code execution (RCE) vulnerability in Bash was the major mover in January, with the first of several drops before settling into last place among the top-tier detections by the end of June. It should be noted that this vulnerability is basically the infamous Shellshock RCE that was discovered in 2014 and was considered to be worse than Heartbleed. February saw a major surge in detections related to an old argument injection vulnerability in PHP CGI. Another PHP-related detection surged in March, this time targeting another RCE flaw in PHPUnit. Shenzhen was once again a huge upstart in April and then a big downer in May.

Now let's adjust our search to focus on exploits that weren't necessarily global chart toppers, but did achieve a measure of regional fame. These are featured in Figure 2. Zivif, TrueOnline, and Allegro offer additional examples of attempts to recon vulnerable IoT devices. It's not always intuitive why certain exploits gain traction in a certain region, and TrueOnline, an ISP in Thailand, is a good case in point.

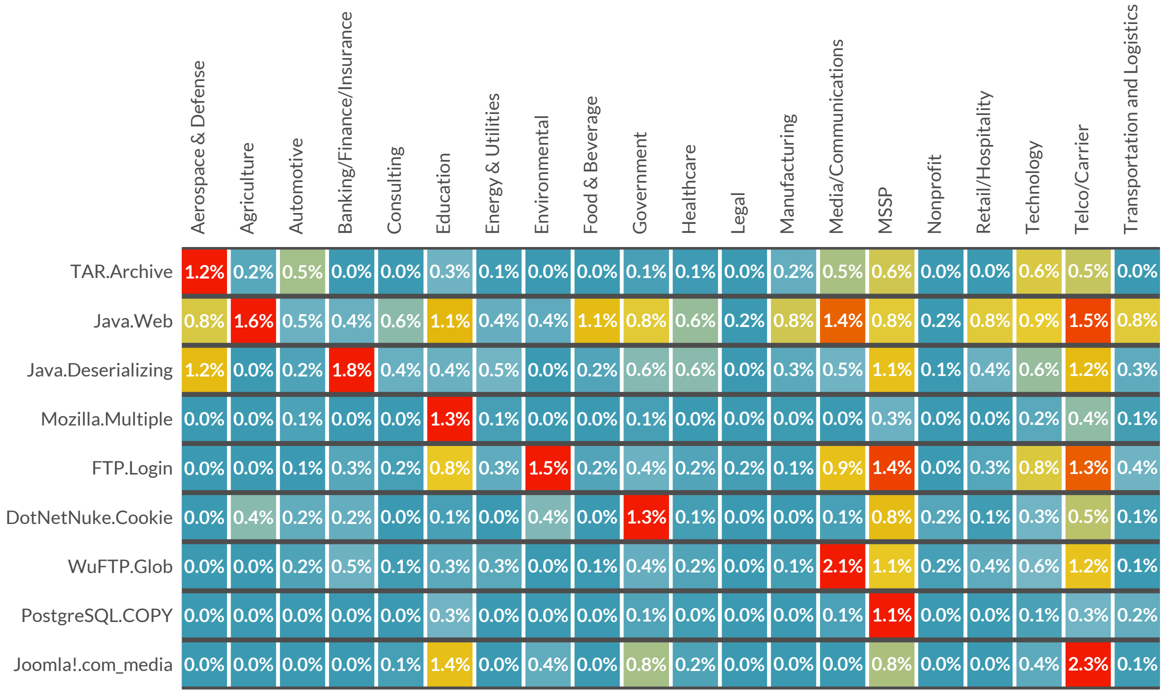
| | Africa | Asia | Europe | Latin America | Middle East | Northern America | Oceania |
|---|---|---|---|---|---|---|---|
| Sun.Java | 5.6% | 1.6% | 0.9% | 0.9% | 1.3% | 1.0% | 0.6% |
| Zivif.PR115-204-P-RS | 4.2% | 32.7% | 11.1% | 12.4% | 15.2% | 4.6% | 23.1% |
| Adobe.Reader | 8.2% | 5.2% | 10.5% | 6.7% | 4.5% | 6.1% | 9.0% |
| TrueOnline.ZyXEL | 3.7% | 0.4% | 10.8% | 15.4% | 4.8% | 1.8% | 0.4% |
| Allegro.RomPager | 4.4% | 3.2% | 2.9% | 2.2% | 6.7% | 3.6% | 3.7% |
| SonicWall.GMS | 0.3% | 0.3% | 1.1% | 0.4% | 2.4% | 9.4% | 0.5% |
| Pulse.Secure | 3.8% | 2.7% | 8.8% | 5.8% | 2.1% | 10.5% | 11.4% |

Figure 2: Regionally prevalent IPS detections during 1H 2020 (percent of organizations).

The vulnerability in view affects a modified version of a ZyXEL router that TrueOnline distributes to its (presumably Thai) customers. That begs the question of why the prevalence of detections in Latin America is so much higher than in Asia. The answer is fairly simple. The router's firmware contains a language package, enabling international distribution. When ISPs were migrating from ADSL to VDSL circa 2016, ZyXEL routers became widely distributed across Latam countries. Current activity reflects that history.

Switching gears again, we'll take a look at IPS detections that exhibited unusually high prevalence within certain industries. We'll call out a few high-level observations based on Figure 3 and leave it to you to review the details for your sector. We note that some of these (e.g., TAR-Archive and FTP.Login) are fairly easy to exploit and look like criminals hoping to take advantage of security slip-ups.

DotNetNuke is a CMS based on .NET According to their website, the U.S. Department of Defense runs hundreds of public websites on DotNetNuke. That probably has something to do with the elevated rate of detections for the public sector. The bump for PostgreSQL exploits observed for MSSPs may indicate databases unintentionally left accessible to the internet. A Shodan search reveals hundreds of thousands of PostgreSQL databases, many of which are hosted in Amazon Web Services (AWS). Is your MSSP exposing your sensitive data?



| | Aerospace & Defense | Agriculture | Automotive | Banking/Finance/Insurance | Consulting | Education | Energy & Utilities | Environmental | Food & Beverage | Government | Healthcare | Legal | Manufacturing | Media/Communications | MSSP | Nonprofit | Retail/Hospitality | Technology | Telco/Carrier | Transportation and Logistics |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| TAR.Archive | 1.2% | 0.2% | 0.5% | 0.0% | 0.0% | 0.3% | 0.1% | 0.0% | 0.0% | 0.1% | 0.1% | 0.0% | 0.2% | 0.5% | 0.6% | 0.0% | 0.0% | 0.6% | 0.5% | 0.0% |
| Java.Web | 0.8% | 1.6% | 0.5% | 0.4% | 0.6% | 1.1% | 0.4% | 0.4% | 1.1% | 0.8% | 0.6% | 0.2% | 0.8% | 1.4% | 0.8% | 0.2% | 0.8% | 0.9% | 1.5% | 0.8% |
| Java.Deserializing | 1.2% | 0.0% | 0.2% | 1.8% | 0.4% | 0.4% | 0.5% | 0.0% | 0.2% | 0.6% | 0.6% | 0.0% | 0.3% | 0.5% | 1.1% | 0.1% | 0.4% | 0.6% | 1.2% | 0.3% |
| Mozilla.Multiple | 0.0% | 0.0% | 0.1% | 0.0% | 0.0% | 1.3% | 0.1% | 0.0% | 0.0% | 0.1% | 0.0% | 0.0% | 0.0% | 0.0% | 0.3% | 0.0% | 0.0% | 0.2% | 0.4% | 0.1% |
| FTP.Login | 0.0% | 0.0% | 0.1% | 0.3% | 0.2% | 0.8% | 0.3% | 1.5% | 0.2% | 0.4% | 0.2% | 0.2% | 0.1% | 0.9% | 1.4% | 0.0% | 0.3% | 0.8% | 1.3% | 0.4% |
| DotNetNuke.Cookie | 0.0% | 0.4% | 0.2% | 0.2% | 0.0% | 0.1% | 0.0% | 0.4% | 0.0% | 1.3% | 0.1% | 0.0% | 0.0% | 0.1% | 0.8% | 0.2% | 0.1% | 0.3% | 0.5% | 0.1% |
| WuFTP.Glob | 0.0% | 0.0% | 0.2% | 0.5% | 0.1% | 0.3% | 0.3% | 0.0% | 0.1% | 0.4% | 0.2% | 0.0% | 0.1% | 2.1% | 1.1% | 0.2% | 0.4% | 0.6% | 1.2% | 0.1% |
| PostgreSQL.COPY | 0.0% | 0.0% | 0.0% | 0.0% | 0.0% | 0.3% | 0.0% | 0.0% | 0.0% | 0.1% | 0.0% | 0.0% | 0.0% | 0.1% | 1.1% | 0.0% | 0.0% | 0.1% | 0.3% | 0.2% |
| Joomla!.com_media | 0.0% | 0.0% | 0.0% | 0.0% | 0.1% | 1.4% | 0.0% | 0.4% | 0.0% | 0.8% | 0.2% | 0.0% | 0.0% | 0.0% | 0.8% | 0.0% | 0.0% | 0.4% | 2.3% | 0.1% |

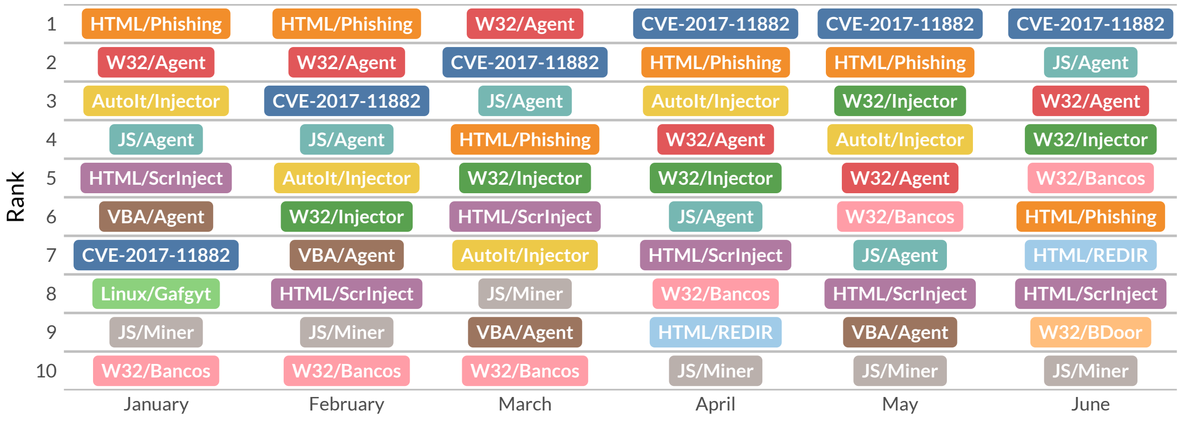
Figure 3: Industry-focused IPS detections during 1H 2020 (percent of organizations).

In general, education institutions, media companies, MSSPs, and telcos have more hotspots than other industries. If your company falls into one of those groups, ensure defenses are ready to thwart a wider range of threats. On the other hand, notice how legal firms and nonprofits show a cool blue all the way down. That indicates we didn't detect any particular threats that were abnormally prevalent or unique to those industries. That doesn't mean those industries aren't in the crosshairs; it just means they weren't the target of many novel exploit attempts during the first part of the year. You'll see in the next section that they don't get off so easily when it comes to malware.

## Malware Detections

Malware trends reflect adversary intent and capability. Similar to IPS detections, malware picked up by our sensors does not always indicate confirmed infections, but rather the weaponization and/or distribution of malicious code. Detections can occur at the network, application, and host level on an array of devices.

Figure 4 ranks the most prevalent malware for each of the first six months of 2020. Similar to how we truncated IPS detections to focus on technologies, we've chosen to group malware into families, or categories, rather than specific variants. Our purpose in doing this is to group the numerous, often short-lived variants by their similarities so that we don't miss the malware forest for the trees.



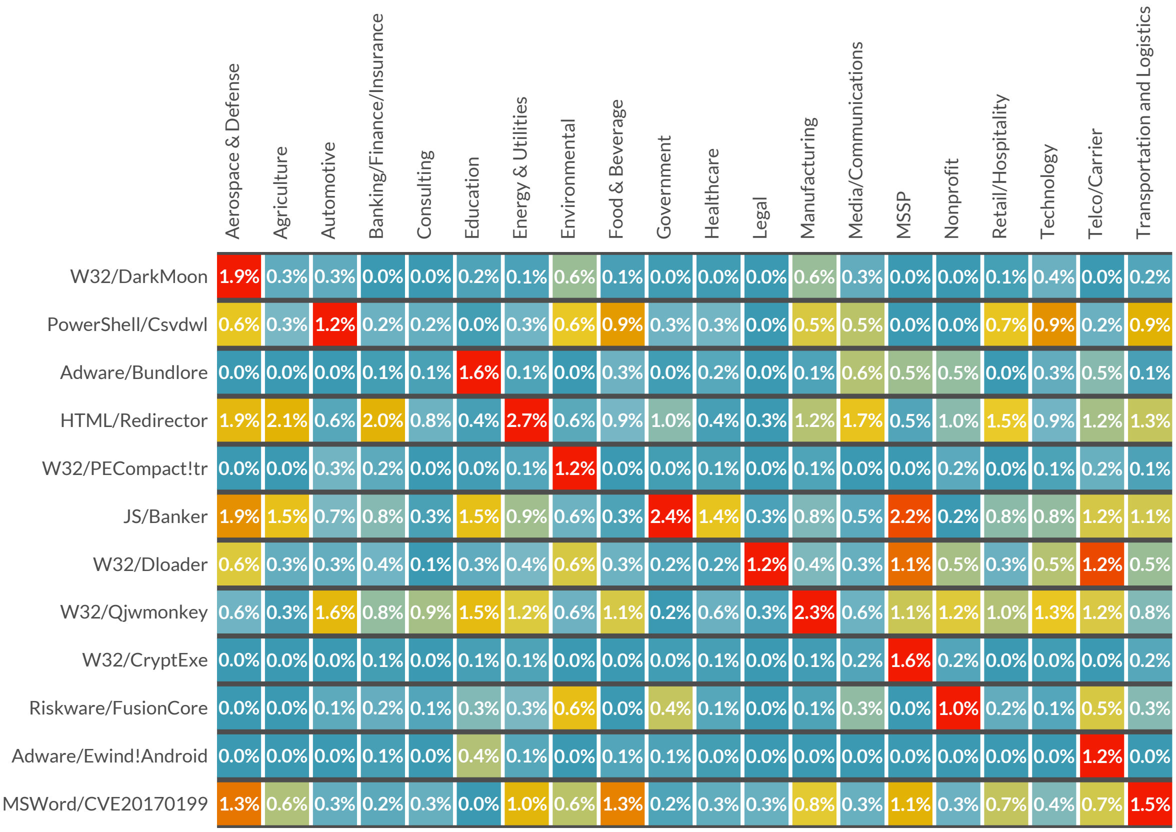
| Rank | January | February | March | April | May | June |
|---|---|---|---|---|---|---|
| 1 | HTML/Phishing | HTML/Phishing | W32/Agent | CVE-2017-11882 | CVE-2017-11882 | CVE-2017-11882 |
| 2 | W32/Agent | W32/Agent | CVE-2017-11882 | HTML/Phishing | HTML/Phishing | JS/Agent |
| 3 | AutoIt/Injector | CVE-2017-11882 | JS/Agent | AutoIt/Injector | W32/Injector | W32/Agent |
| 4 | JS/Agent | JS/Agent | HTML/Phishing | W32/Agent | AutoIt/Injector | W32/Injector |
| 5 | HTML/ScrInject | AutoIt/Injector | W32/Injector | W32/Injector | W32/Agent | W32/Bancos |
| 6 | VBA/Agent | W32/Injector | HTML/ScrInject | JS/Agent | W32/Bancos | HTML/Phishing |
| 7 | CVE-2017-11882 | VBA/Agent | AutoIt/Injector | HTML/ScrInject | JS/Agent | HTML/REDIR |
| 8 | Linux/Gafgyt | HTML/ScrInject | JS/Miner | W32/Bancos | HTML/ScrInject | HTML/ScrInject |
| 9 | JS/Miner | JS/Miner | VBA/Agent | HTML/REDIR | VBA/Agent | W32/BDoor |
| 10 | W32/Bancos | W32/Bancos | W32/Bancos | JS/Miner | JS/Miner | JS/Miner |

Figure 4: Most prevalent malware categories by month during 1H 2020.

One area of that forest that bears mention here is the HTML/Phishing family that includes all variants of web-based phishing lures and scams. They sit firmly atop the list in January and February and only drop out of the top five in June. Together with its HTML cousins of /ScrInject (browser script injection attacks) and /REDIR (browser redirection schemes), this demonstrates strong interest from cyber criminals to get us where we're often most vulnerable and gullible—browsing the web. Web-based malware often obfuscates and/or bypasses conventional AV products, upping the chance of successful infection. That's even more concerning because we noted a marked drop in corporate web traffic due to people surfing from home rather than the office. Savvy defenders should note that the browser was a prime delivery vector for malware in the first half of 2020 and act accordingly to ensure consistent controls for remote systems.

The other part of the forest we'd like to spotlight from Figure 5 is malware that exploits CVE-2017-11882. This bug has been public for a few years now (the bug itself is much, much older), but it steadily climbed in prevalence over the first half of 2020 and held the #1 spot for four straight months. And we weren't the only ones to note the increase. On April 1 (not a joke), the U.S. Secret Service (USSS) posted an alert about fraudulent COVID-19 emails using malicious attachments. A representative of the USSS's Criminal Investigative Division told CSO Magazine that the malware spreaders were seeking to exploit CVE-2017-11882 for multiple campaigns. One that seems particularly mean purports to come from the U.S. Department of Health and Human Services (HHS) and informs the recipient that they've contracted COVID-19. Another targets medical equipment manufacturers with a (malware-laden) document sent via email asking them to provide equipment.

Figure 5 follows the method used by Figure 3 to identify malware families that exhibit unusually high prevalence within certain industries. Scanning the columns, it's apparent that no industry is blue all the way down. Every sector has at least one malware hot(ter) spot and some of them have several.



| | Aerospace & Defense | Agriculture | Automotive | Banking/Finance/Insurance | Consulting | Education | Energy & Utilities | Environmental | Food & Beverage | Government | Healthcare | Legal | Manufacturing | Media/Communications | MSSP | Nonprofit | Retail/Hospitality | Technology | Telco/Carrier | Transportation and Logistics |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| W32/DarkMoon | 1.9% | 0.3% | 0.3% | 0.0% | 0.0% | 0.2% | 0.1% | 0.6% | 0.1% | 0.0% | 0.0% | 0.0% | 0.6% | 0.3% | 0.0% | 0.0% | 0.1% | 0.4% | 0.0% | 0.2% |
| PowerShell/Csvdwl | 0.6% | 0.3% | 1.2% | 0.2% | 0.2% | 0.0% | 0.3% | 0.6% | 0.9% | 0.3% | 0.3% | 0.0% | 0.5% | 0.5% | 0.0% | 0.0% | 0.7% | 0.9% | 0.2% | 0.9% |
| Adware/Bundlore | 0.0% | 0.0% | 0.0% | 0.1% | 0.1% | 1.6% | 0.1% | 0.0% | 0.3% | 0.0% | 0.2% | 0.0% | 0.1% | 0.6% | 0.5% | 0.5% | 0.0% | 0.3% | 0.5% | 0.1% |
| HTML/Redirector | 1.9% | 2.1% | 0.6% | 2.0% | 0.8% | 0.4% | 2.7% | 0.6% | 0.9% | 1.0% | 0.4% | 0.3% | 1.2% | 1.7% | 0.5% | 1.0% | 1.5% | 0.9% | 1.2% | 1.3% |
| W32/PECompact!tr | 0.0% | 0.0% | 0.3% | 0.2% | 0.0% | 0.0% | 0.1% | 1.2% | 0.0% | 0.0% | 0.1% | 0.0% | 0.1% | 0.0% | 0.0% | 0.2% | 0.0% | 0.1% | 0.2% | 0.1% |
| JS/Banker | 1.9% | 1.5% | 0.7% | 0.8% | 0.3% | 1.5% | 0.9% | 0.6% | 0.3% | 2.4% | 1.4% | 0.3% | 0.8% | 0.5% | 2.2% | 0.2% | 0.8% | 0.8% | 1.2% | 1.1% |
| W32/Dloader | 0.6% | 0.3% | 0.3% | 0.4% | 0.1% | 0.3% | 0.4% | 0.6% | 0.3% | 0.2% | 0.2% | 1.2% | 0.4% | 0.3% | 1.1% | 0.5% | 0.3% | 0.5% | 1.2% | 0.5% |
| W32/Qjwmonkey | 0.6% | 0.3% | 1.6% | 0.8% | 0.9% | 1.5% | 1.2% | 0.6% | 1.1% | 0.2% | 0.6% | 0.3% | 2.3% | 0.6% | 1.1% | 1.2% | 1.0% | 1.3% | 1.2% | 0.8% |
| W32/CryptExe | 0.0% | 0.0% | 0.0% | 0.1% | 0.0% | 0.1% | 0.1% | 0.0% | 0.0% | 0.0% | 0.1% | 0.0% | 0.1% | 0.2% | 1.6% | 0.2% | 0.0% | 0.0% | 0.0% | 0.2% |
| Riskware/FusionCore | 0.0% | 0.0% | 0.1% | 0.2% | 0.1% | 0.3% | 0.3% | 0.6% | 0.0% | 0.4% | 0.1% | 0.0% | 0.1% | 0.3% | 0.0% | 1.0% | 0.2% | 0.1% | 0.5% | 0.3% |
| Adware/Ewind!Android | 0.0% | 0.0% | 0.0% | 0.1% | 0.0% | 0.4% | 0.1% | 0.0% | 0.1% | 0.1% | 0.0% | 0.0% | 0.0% | 0.0% | 0.0% | 0.0% | 0.0% | 0.0% | 1.2% | 0.0% |
| MSWord/CVE20170199 | 1.3% | 0.6% | 0.3% | 0.2% | 0.3% | 0.0% | 1.0% | 0.6% | 1.3% | 0.2% | 0.3% | 0.3% | 0.8% | 0.3% | 1.1% | 0.3% | 0.7% | 0.4% | 0.7% | 1.5% |

Figure 5: Industry-focused malware detections during 1H 2020 (percent of organizations).

We realize malware names aren't always clear—our threat encyclopedia should help with that—but some are intuitive. Telcos see more malware on Android devices, for instance. Adware roams the halls of academia. JS/Banker steals from government agencies and MSSPs more often than banks. PowerShell in the automotive industry raises an eyebrow. We could go on, but we'll leave you to explore your sector as desired and transition on to our discussion of botnets. Hopefully these details help you focus security efforts on threats that matter most to your organization.

## Botnet Activity

Whereas exploit and malware trends usually show the pre-compromise side of attacks, botnets give a post-compromise viewpoint. Once infected, systems often communicate with remote hosts, making this traffic an important part of monitoring the full scope of malicious activity.

One lesson botnet data imparts every time we examine it is that pervasive and persistent control is a prized commodity among cyber criminals. A side effect of this is that activity for the top bots is remarkably consistent. Figure 6 illustrates this perfectly. The month-by-month rankings for prevalence are far more consistent than seen for IPS and malware detections. We've studied botnet persistence in prior reports and saw that enterprise security teams will typically identify botnet traffic and snuff out infected systems within a reasonable time frame. But botnets infecting small businesses and millions of consumer devices tend to stick around for quite a while. And that's a lot of what we see here.

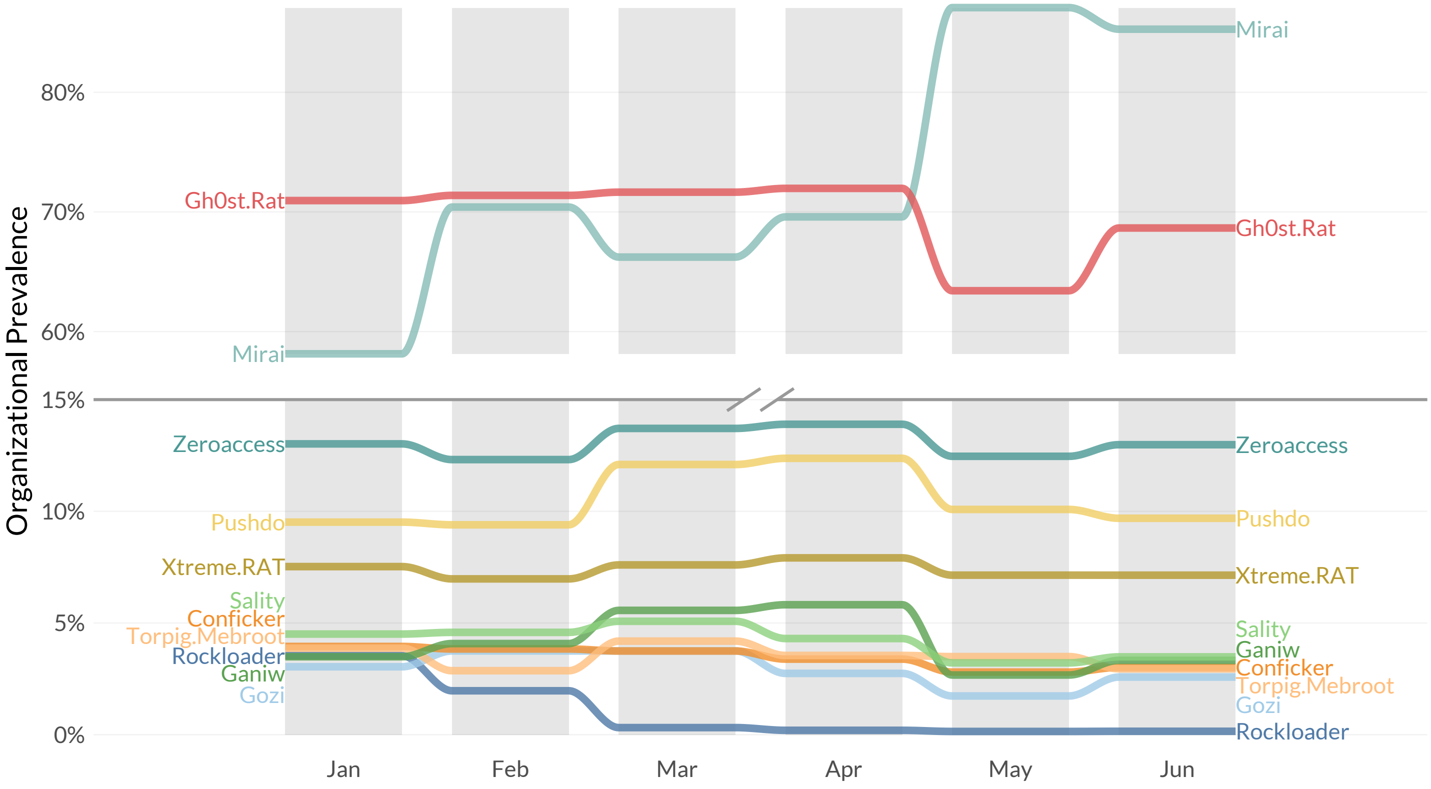
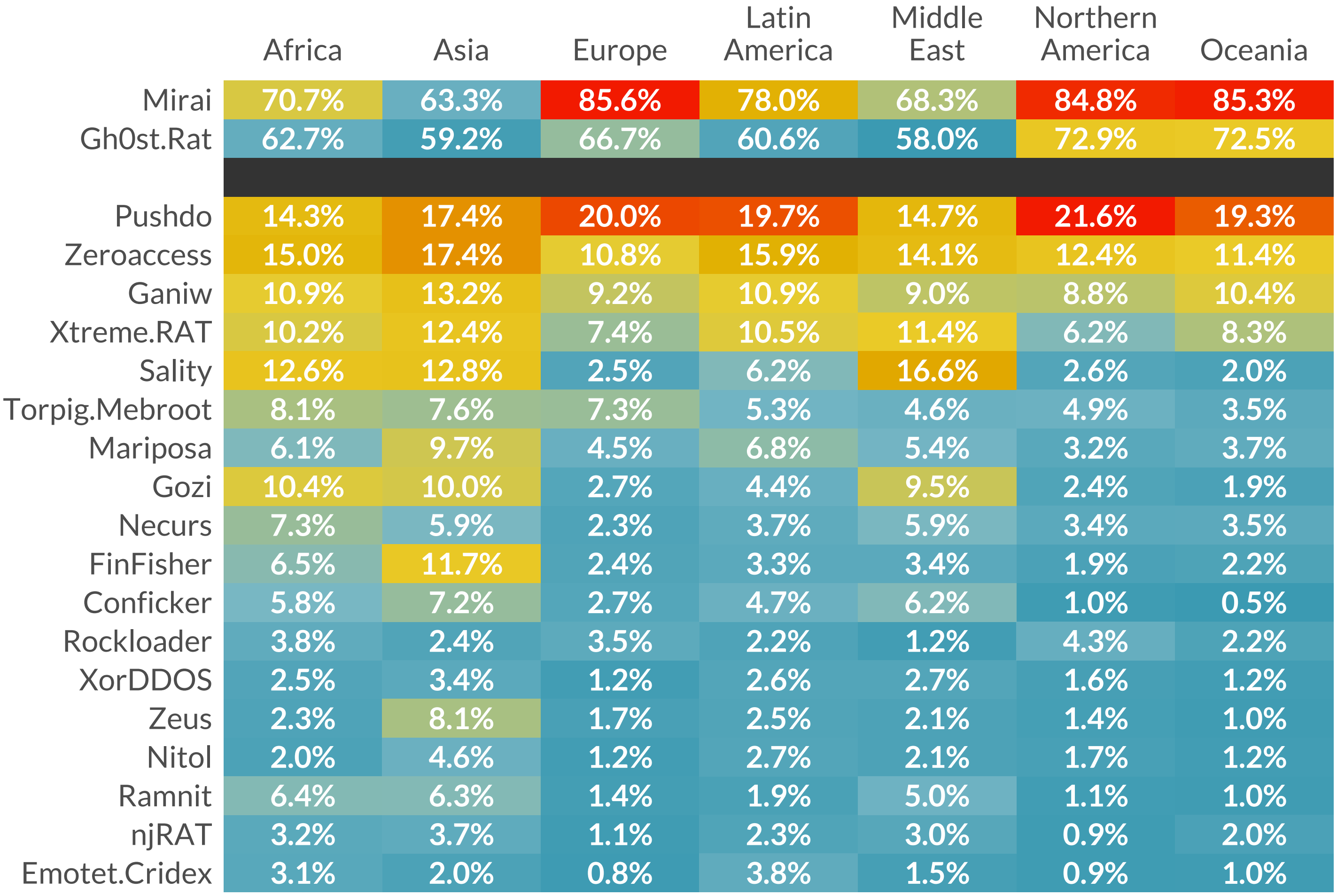


Figure 6: Most prevalent botnet detections during 1H 2020 (not split vertical axis).

The first two botnets in Figure 6, Mirai and Gh0st, predominate the chart and did so for the latter part of 2019 as well. Driven by apparent growing interest by attackers targeting old and new vulnerabilities in consumer IoT products, Mirai surged into first place among botnets by early May. This trend is noteworthy because it could suggest cyber criminals are seeking to gain a foothold in enterprise networks by exploiting devices that WFH employees might be using to connect to the enterprise network. In a sense, the corporate network perimeter has extended to the home—and that's not a very comforting thought.

Gh0st, an old malware-botnet crime family, was also leveraged for campaigns targeting WFH users and applications. Gh0st is a remote access botnet that allows an attacker to take full control of the infected system, log keystrokes, provide live webcam and microphone feeds, download and upload files, and other nefarious activities.

To better highlight variation that does exist among botnets, Figure 7 expands the list of chart-toppers from Figure 6 and compares them across regions. Mirai and Gh0st are still omnipresent, but it's apparent that their activity is not uniform around the world. The proportion of organizations that detected traffic related to one of Mirai's many variants, for example, is more than 20% higher in Europe than Asia. But Europe lands in third place for Gh0st activity.



| | Africa | Asia | Europe | Latin America | Middle East | Northern America | Oceania |
|---|---|---|---|---|---|---|---|
| Mirai | 70.7% | 63.3% | 85.6% | 78.0% | 68.3% | 84.8% | 85.3% |
| Gh0st.Rat | 62.7% | 59.2% | 66.7% | 60.6% | 58.0% | 72.9% | 72.5% |
| | | | | | | | |
| Pushdo | 14.3% | 17.4% | 20.0% | 19.7% | 14.7% | 21.6% | 19.3% |
| Zeroaccess | 15.0% | 17.4% | 10.8% | 15.9% | 14.1% | 12.4% | 11.4% |
| Ganiw | 10.9% | 13.2% | 9.2% | 10.9% | 9.0% | 8.8% | 10.4% |
| Xtreme.RAT | 10.2% | 12.4% | 7.4% | 10.5% | 11.4% | 6.2% | 8.3% |
| Sality | 12.6% | 12.8% | 2.5% | 6.2% | 16.6% | 2.6% | 2.0% |
| Torpig.Mebroot | 8.1% | 7.6% | 7.3% | 5.3% | 4.6% | 4.9% | 3.5% |
| Mariposa | 6.1% | 9.7% | 4.5% | 6.8% | 5.4% | 3.2% | 3.7% |
| Gozi | 10.4% | 10.0% | 2.7% | 4.4% | 9.5% | 2.4% | 1.9% |
| Necurs | 7.3% | 5.9% | 2.3% | 3.7% | 5.9% | 3.4% | 3.5% |
| FinFisher | 6.5% | 11.7% | 2.4% | 3.3% | 3.4% | 1.9% | 2.2% |
| Conficker | 5.8% | 7.2% | 2.7% | 4.7% | 6.2% | 1.0% | 0.5% |
| Rockloader | 3.8% | 2.4% | 3.5% | 2.2% | 1.2% | 4.3% | 2.2% |
| XorDDOS | 2.5% | 3.4% | 1.2% | 2.6% | 2.7% | 1.6% | 1.2% |
| Zeus | 2.3% | 8.1% | 1.7% | 2.5% | 2.1% | 1.4% | 1.0% |
| Nitol | 2.0% | 4.6% | 1.2% | 2.7% | 2.1% | 1.7% | 1.2% |
| Ramnit | 6.4% | 6.3% | 1.4% | 1.9% | 5.0% | 1.1% | 1.0% |
| njRAT | 3.2% | 3.7% | 1.1% | 2.3% | 3.0% | 0.9% | 2.0% |
| Emotet.Cridex | 3.1% | 2.0% | 0.8% | 3.8% | 1.5% | 0.9% | 1.0% |

Figure 7: Most prevalent botnets by region during 1H 2020 (percent of organizations).

As you move down Figure 7, some even stronger regional differences emerge. Gozi pops in Africa and FinFisher is particularly active in Asia. Emotet.Cridex is the only botnet shown that leads in Latin America. Sality jumps among organizations in the Middle East, and North America owns the Pushdo crown. Curiously, Oceania doesn't take the #1 spot for any of the botnets shown here (though it's a very close second for Mirai). Myriad factors account for such differences, including targeting, infrastructure, technology adoption, security configurations, and user behavior.

# Featured Threats and Trends

## Exploiting a Global Pandemic

Security researchers and other vendors have written a lot already on the enormous impact that COVID-19 has had on cybersecurity. We've done so ourselves here, here, here, here, here, and more. Even so, it would be remiss of us to ignore the topic for that reason, especially in a report summing up threat activity in the first half of 2020.

Predictably, cyber criminals of all shades—from opportunistic phishers to scheming nation-state actors—found some way to exploit the pandemic for their benefit. Organizations around the world were suddenly confronted with a situation where they had to support a majority of employees working from home. For attackers, the shift presented an unprecedented opportunity to break into enterprise networks by targeting weakly protected home networks, consumer devices, VPN connections, and video communication and collaboration tools.

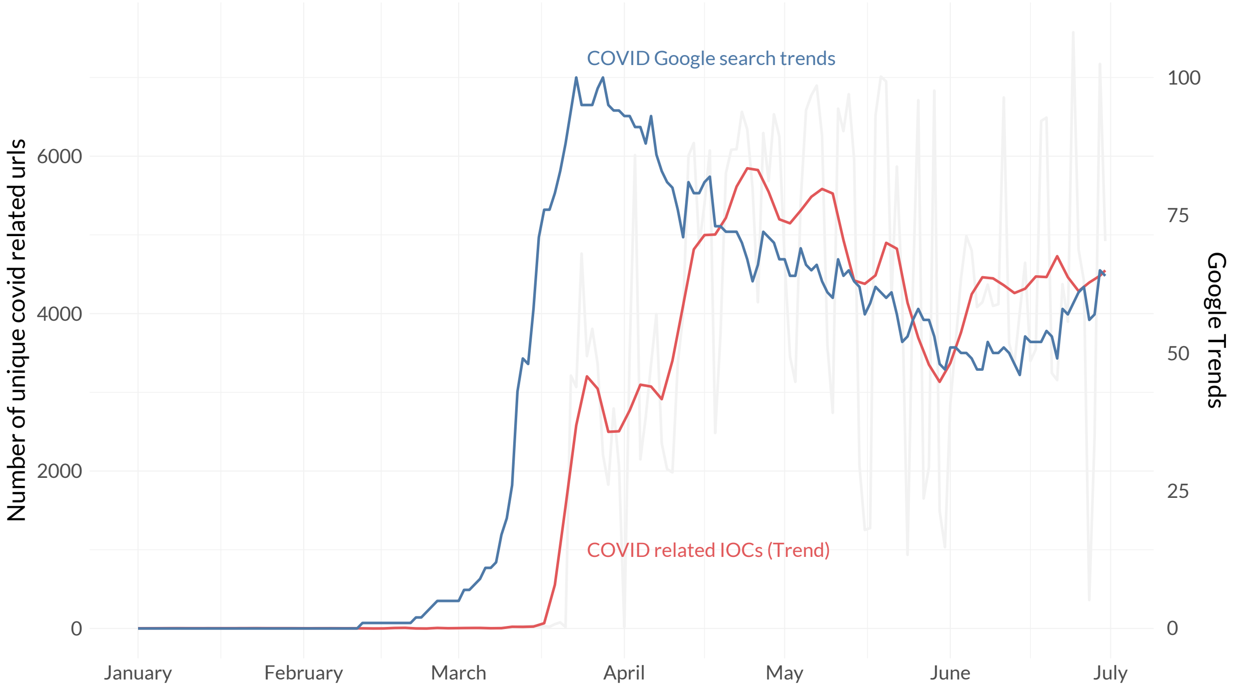


Figure 8: Comparison of COVID-related Google search trends and malicious COVID-themed URLs.

Indicators of threat activity began to emerge almost in lockstep with growing societal awareness of the scope and ramifications of the pandemic. Figure 8 illustrates this by comparing COVID-related Google search trends and COVID-themed malicious URLs picked up by our web filters. Many of the domains contained names such as "coronavirus," "vaccine," "chloroquine," and "remdesvir" and were created to harvest credentials or distribute malware and spam. It shows how quickly attackers move to take advantage of major news developments and events with broad social impact.

We also observed a sharp increase in malicious emails with documents purportedly containing pandemic-related guidance seemingly sent from trusted sources—such as the Centers for Disease Control and Prevention (CDC) and the World Health Organization (WHO). The operators of the Emotet banking Trojan were among the first to leverage the coronavirus scare to try and distribute their malware in this way.

Over the following weeks and months, we observed a widening range of malicious activity involving the use of COVID-19-related lures. This included phishing and business email compromise schemes, nation-state backed campaigns, and ransomware attacks. Some examples of the several threats we tracked include:

- the distribution of the AZORult information stealer via a website with a fake coronavirus infection-spread map;
- a phishing campaign targeting Ukrainian military and intelligence targets by the Gamaredon APT group;
- attacks against targets in mainland China by the Vietnam-affiliated APT32 group;
- targeted attacks against South Korean organizations by the North Korea-linked Kimsuky APT group.

Generally, organizations in the U.S., China, and Russia were the most frequent targets of coronavirus-themed attacks in the first half of 2020.

Ransomware hidden in COVID-19-themed messages, attachments, and documents was another threat. We tracked three ransomware samples that fell into this category in H1 2020 —NetWalker, Ransomware-GVZ, and CoViper. Of the three, CoViper was especially pernicious because it rewrote the computer's master boot record (MBR) before encrypting data. We have observed several attacks in the past where adversaries have used MBR wipers in combination with ransomware to effectively cripple the PC.

Toward the end of the first half of the year, there were also several reports of potentially state-backed threat groups attacking organizations involved in COVID-19-related research in the U.S. and other countries.

It's unclear how damaging—or not—the pandemic-related malicious activity in the first half of this year may have been ultimately. But for many organizations, the attacks highlighted the need for better approaches—including zero-trust models—for protecting their networks against threats posed by workers connecting from weakly protected home networks. It also emphasizes the importance that defenders keep an eye on the news to stay ahead of the threat du jour.

## From the DVR to the DMZ

The recent surge in remote work as a result of the COVID-19 pandemic has focused considerable attention on the security of routers, DVRs, and other internet-connected devices at home. One concern is that attackers can exploit the subpar security in these systems to try and gain a foothold on enterprise networks or on devices that WFH employees might be using to connect to the enterprise network. Another issue is that attackers can exploit these devices to quickly assemble massive botnets—in Mirai-like fashion—that can be used to launch DDoS attacks or distribute malware.

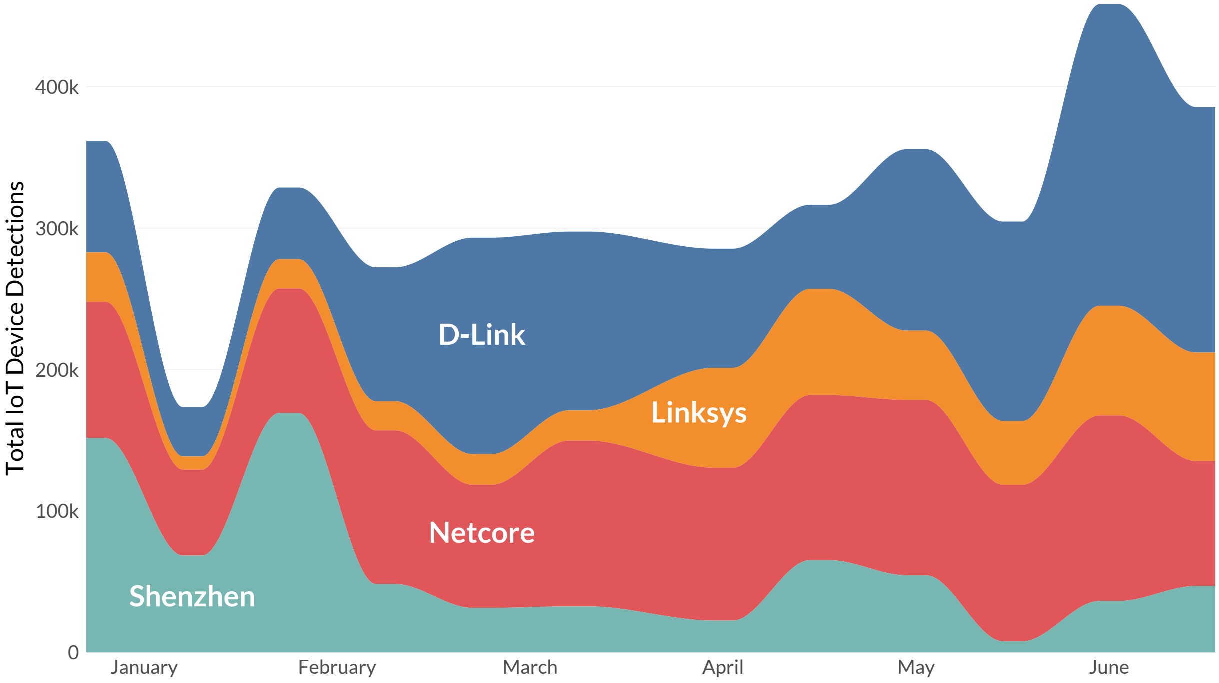


Figure 9: IPS detections targeting common network device brands during 1H 2020.

In the first half of 2020 we saw plenty of evidence to suggest sustained attacker interest in exploiting old and new vulnerabilities in consumer-focused IoT products. We've already discussed the dramatic increase in malicious activity targeting the flaw in Shenzhen TVT DVRs, so we won't elaborate on that again here. Another vulnerability that elicited a lot of attacker interest in the first half of 2020 involved D-Link routers. The command execution flaw exists in multiple D-Link router models and gives attackers a way to take complete control of a vulnerable device. We observed most of the malicious activity targeting this vulnerability happening in May and June. Though the volume of attacks and the number of devices targeted was higher—around 160,000 at the peak—compared to the Shenzhen DVR flaw, this was substantial enough to suggest a high level of attacker interest.

The most sustained high-volume attack activity that we observed, though, impacted Netcore/Netis routers. From January through the end of June, threat actors kept relentlessly pounding away at a hard-coded password security bypass issue in Netcore/Netis routers. The backdoor vulnerability was first discovered in August 2014 and has since then been one of the top triggered IPS signatures we have tracked. During the peak of the attacks in May, we collected well over 60 million hits from this signature.

An authentication-bypass vulnerability in Linksys routers and another remote command execution flaw in Linksys E-Series routers were two other router flaws that received considerable attention from attackers in the first half of 2020.

Attackers have already successfully exploited some of these flaws to assemble dangerously large botnets. One example is Dark Nexus, an IoT botnet that emerged in the first half of this year, consisting of thousands of exploited ASUS and D-Link routers. Mozi, a peer-to-peer botnet that was also identified by researchers in the first half of 2020, is another botnet built from exploited routers and DVRs including D-Link devices with the command execution flaw referenced above.

The presence of such vulnerable devices on home networks significantly expands the attack surface for organizations with a large number of remote workers. Thus, organizations should evaluate options for achieving the same level of protection for WFH employees as they had in the office.

## OT Threats, Past and Present

On the opposite end of the spectrum from IT devices featured in the previous section are operational technologies (OT). The prevalence of threats targeting supervisory control and data acquisition (SCADA) systems and other types of industrial control systems (ICS) is understandably much less than IT, but that fact in no way diminishes their importance. Figure 10 provides a breakdown of exploit detections targeting ICS manufacturers and components.

If you're not responsible for managing OT, you might have missed an important anniversary this past June. 2020 marks 10 years since the discovery of Stuxnet, the malicious worm that made headlines by sabotaging industrial facilities critical to the nuclear program in Iran. Since that momentous event, there have been many instances of sophisticated cyberattacks on OT systems worldwide. This may be due in part to the fact that OT networks are now increasingly connected to the internet, making them more vulnerable to attack. That hypothesis is supported by our "State of Operational Technology and Cybersecurity Report" that found 74% of OT organizations had experienced a malware intrusion in the past 12 months!

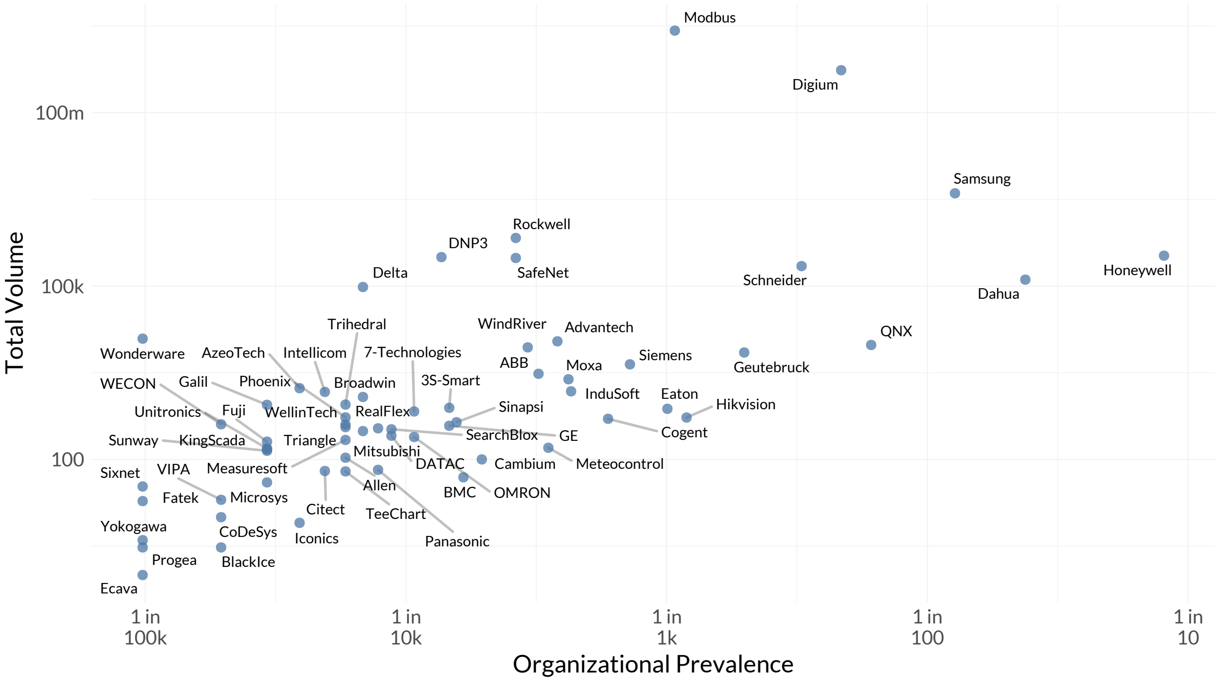


Figure 10: Prevalence and volume of IPS detections involving industrial systems.

In terms of more recent developments in the realm of OT threats, two in particular caught our attention in the first half of 2020. January saw a surge across our IPS sensors in the U.S., Brazil, and Germany of activity involving Modbus TCP servers and programmable logic controllers (PLCs) that could result in information leakage. This helped make Modbus-related detections the most voluminous of all OT systems featured in Figure 10. Note, however, that all triggers of this signature aren't necessarily malicious. But it's worth monitoring because an attacker infiltrating the SCADA network could certainly cause trouble by accessing the Modbus controller.

The second noteworthy development came in May when researchers uncovered Ramsay, an espionage framework designed for the collection and exfiltration of sensitive files within air-gapped or highly restricted networks. OT environments fit those characteristics, which is why we mention it here. It's not quite clear how long Ramsay has been active, but it's been tied to an older APT group, Darkhotel. As their name suggests, Darkhotel is more known for exploiting hotel Wi-Fi networks than industrial facilities, but we're more interested in Ramsay's potential than its progenitors.

Fortinet is one of the few security vendors committed to protecting and securing OT operations, especially those that are part of critical infrastructures. You can read more here about the unique challenges of securing operational technology environments and how we can help.

## Ransomware Spreads Its Wings

An attack on a well-known manufacturer in June that interfered with their operations and caused temporary production interruptions at several of the company's facilities capped another six months of ransomware activity targeted at enterprise organizations.

Security researchers identified the malware used in the attack as EKANS (which is sometimes referred to publicly as Snake), a ransomware sample with several features tailored to attack systems in ICS. Our analysis of the malware showed it to be heavily obfuscated, written in the GO programming language, and not very different from other ransomware tools except for its targeting of OT and ICS systems. The attack—and the use of EKANS—was troubling because it suggested that adversaries might be broadening the focus of ransomware attacks to OT environments as well.

Over the course of the first half of 2020 we analyzed activity specific to several other ransomware threats, including the COVID-19-themed ones mentioned in the previous section. One trend we observed was an increase in ransomware incidents where adversaries not only locked a victim organization's data but stole it as well and used the threat of widescale release as additional leverage to try and extort a ransom payment.

One example is DoppelPaymer, a ransomware used in attacks against a supplier of custom parts to the automotive and aerospace industries, a NASA contractor, and the city of Torrance, California. Our analysis showed Doppelpaymer to both encrypt files and offload them to a website where the data is published if the victim refuses to pay the demanded ransom.

The tactic was first observed being used in January when the operator of Maze ransomware published nearly 10GB of private research data belonging to Medical Diagnostic Laboratories after the latter refused to pay the Maze team a demanded ransom amount. Since then, the operators of Sodinokibi and DoppelPaymer have adopted the hybrid model as well. The trend significantly heightens the risks of organizations losing invaluable IP, trade secrets, and other sensitive data in future ransomware attacks.

Ransomware-as-a-Service (RaaS) continued to gain traction among cyber criminals in the first half of 2020 as well. One such threat we tracked was Phobos, a ransomware-type that exploits the Remote Desktop Protocol (RDP) attack vector to gain initial access to a network. We observed the malware to be capable of brute forcing credentials, using stolen credentials, or taking advantage of insecure connections on port 3389. The malware is being sold via a RaaS model, which has made it relatively easily available to even less sophisticated threat actors.

For organizations, malware like Phobos is another reminder to secure RDP servers. Poorly secured, internet-exposed RDP servers have long been favorite targets for criminals looking for a way to gain initial access to an enterprise network. Numerous underground forums and marketplaces sell relatively cheap access to previously hacked RDP servers so criminals in many cases don't even have to do any initial legwork of their own to break into one. Despite repeated warnings, hundreds of thousands of these systems remain accessible and vulnerable to attack over the internet.

Sodinokibi, Nemty, and DeathRansom were three other ransomware types that we observed being distributed via a RaaS model in H1 2020. An early version of DeathRansom that we analyzed did not actually encrypt files, however we found a more recent version that indeed does so.

Zooming out for a wider perspective, Figure 11 rebuts the fallacy of thinking "ransomware doesn't affect companies like mine." It reveals that no industry was spared from ransomware activity over the first six months of the year. The five most heavily targeted sectors were telcos, MSSP, education, government, and tech. Though healthcare is often associated with ransomware, it falls middle of the pack here.

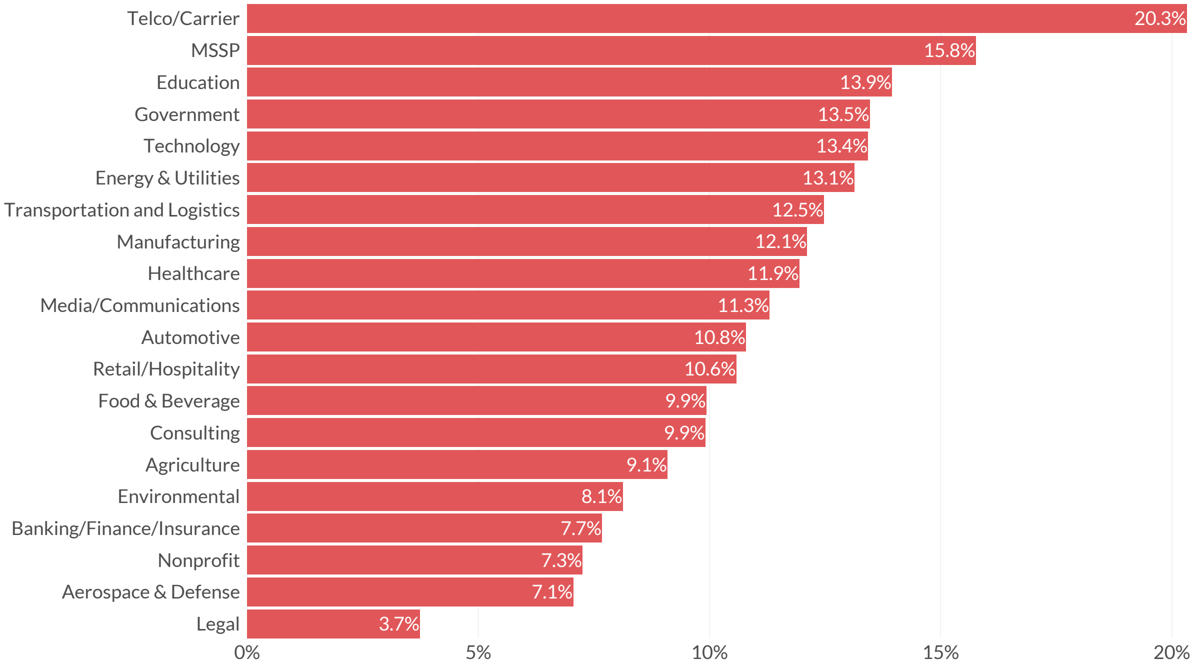


Figure 11: Percent of organizations detecting ransomware during 1H 2020.

The success cyber criminals have had in extracting sizable ransoms from some victims almost certainly means we'll see little letup in ransomware activity for the foreseeable future. In fact, the rise in hybrid attacks and the growing availability of RaaS suggests that things are only going to get worse before they get better. It's not hopeless; however, there are quite a few effective ways to combat ransomware for your organization.

## The Age of Exploitation

There's been a resurgence of interest of late in efforts to model and predict the exploitation of vulnerabilities. In part, this goes back to the long-standing defender's dilemma of not having enough time or resources to fix everything flagged by the latest vuln scan. Another, more recent driver is that the number of published vulnerabilities added to the CVE List has risen sharply over the last few years, mainly because MITRE expanded the set of organizations authorized to assign CVEs to vulnerabilities. Easier, more comprehensive tracking of CVEs is a good thing ... but it also means that list of things to fix only gets longer. And so prioritizing vulnerability remediation has become increasingly important.

One way of doing this is to prioritize vulnerabilities that have actually been exploited in the wild. The challenge with this, of course, is that knowing which CVEs have been exploited requires an expansive deployment of sensors to detect said exploitation. Thankfully, Fortinet has that covered.

The horizontal axis in Figure 12 shows the percentage of CVEs published each year for which we detected exploit activity during the first half of 2020. Overall, that ratio stands at 6%, but it's easy to see that more recent CVEs (reddish color) show lower rates of exploitation. So far, 2020 has the lowest exploitation rate (<1%) ever recorded in the 20+ year history of the CVE List! Part of that phenomenon ties back to the aforementioned increase in CVEs and part simply reflects the fact that exploit development and distribution takes time.

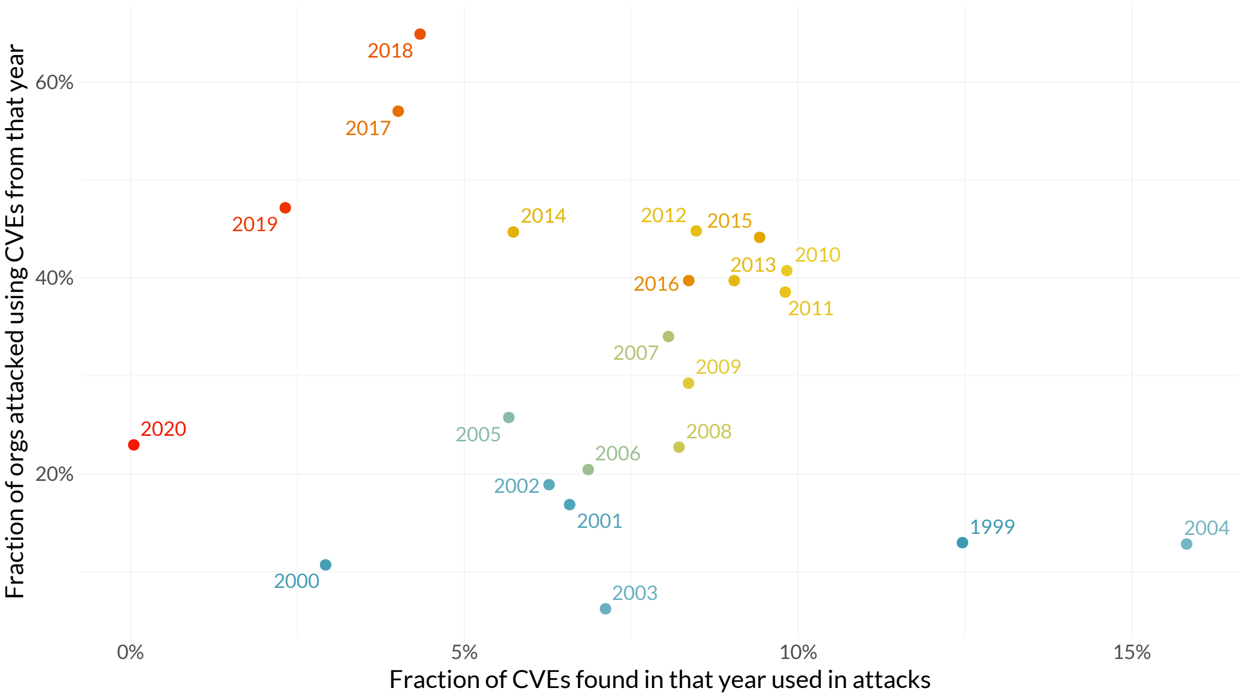


Figure 12: Percentage of CVEs with exploits detected (left) and percent of organizations detecting those exploits (right) by year.

The vertical axis in Figure 12 offers a different perspective. It reveals the percentage of organizations that detected exploit activity targeting CVEs published each year. From this, it's apparent that 2018 vulnerabilities claim the highest exploitation prevalence (65%), yet more than a quarter of firms registered attempts to exploit CVEs from 15 years earlier in 2005. There's a lesson there: Don't assume old vulnerabilities can't cause new problems. The general pattern here, though, is that newer vulnerabilities tend to garner more widespread exploitation (allowing for the time needed for at-scale exploits to be developed and distributed via legitimate and malicious hacking tools).

At the end of the day, all of this points to the fact that defenders increasingly contend with not only more vulnerabilities across their networks but also more vulnerabilities that are actively being exploited in the wild. We understand the challenge of keeping up and hope analysis like we've presented in this report makes it a little easier to do so. See you in our next edition, where we'll examine how the latter half of 2020 shaped the cyber threat landscape.

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

FORTINET®

www.fortinet.com