FORTINET

QUARTERLY

Threat Landscape Report

Q3 2019

Table of Contents

Q3 2019 **Introduction and Overview**

For many of us, the summer months bring not just a change in the weather, but a change of pace as well. Time off school, family vacations, slowdowns at work ... we're all familiar with our version of that routine. But what's the summer routine for cyber-threat actors? Do things heat up or cool down? Is it a time to sow, to reap, or to rest? Thankfully, there's no need to speculate—we kept an eye on summer antics across the threat landscape. Here are some highlights:

The Fortinet Threat Landscape Index

This summary measure of how bad it is out there remained relatively stable during Q3. We saw fluctuations but no major swings.

Attackers might be going old school

We detected an abnormally high number of attempts to inject and execute code onto a range of devices this quarter. It's an old trick, but perhaps attackers are eyeing some new treats?

What a tangled web we weave, which they practice to deceive

Attackers appeared to double down on their efforts to exploit core web infrastructure and content management systems (CMS).

Urgent/11 caused a river of concern

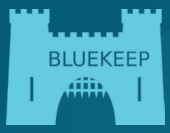
Multiple vulnerabilities were disclosed in Wind River VxWorks, a trusted real-time operating system deployed on more than 2 billion embedded devices. See why we think that concern is warranted.

Ransomware-as-a-Service (RaaS) ran ahead

The authors behind the GandCrab ransomware proved RaaS is a lucrative business model. Others are looking to emulate that success, resulting in new ransomware running on RaaS in Q3.

Criminals made bank on banking Trojans

In a troubling development for enterprise organizations, cyber criminals are increasingly using banking Trojans to drop other payloads and additional banking malware on infected systems to maximize their opportunities for financial gain.



Many are still choosing the blue pill

The BlueKeep vulnerability and the older EternalBlue exploit targeting core Microsoft protocols remained potent last quarter, indicating many vulnerable targets still exist in large numbers.

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 be able to share each quarter.

Threat Landscape Index

The Fortinet Threat Landscape Index (TLI) was developed to provide an ongoing barometer of overall malicious activity across the internet. Generally speaking, the TLI is based on the premise that the cyber landscape gets more threatening as more of our sensors detect a wider variety of threats at a higher volume. Movement in the opposite direction indicates improving conditions. Perhaps most importantly, it shows trends over time and helps identify what's driving them.

Figure 1 tracks the last year of the overall index as well as the subindices for exploits, malware, and botnets. The gray lines fluctuate up and down each week, but the orange trend line stays remarkably stable during the period shown. Q3 of 2019 closed about 1% lower than Q2 and never set any records for weekly highs.

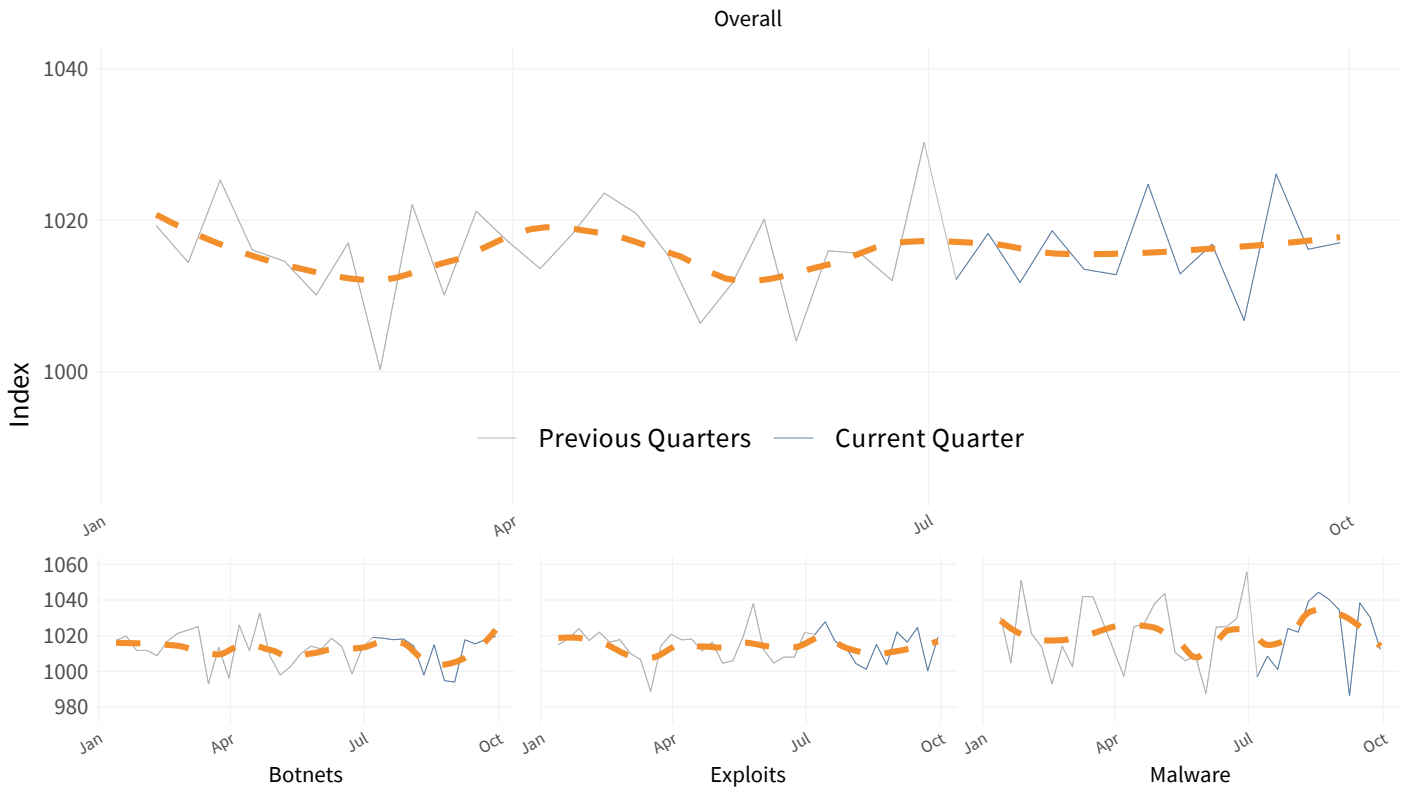


Figure 1: Fortinet Threat Landscape Index (top) and subindices for botnets, exploits, and malware.

While a flat threat index won't grab media attention, it's actually kind of refreshing to see some data that doesn't point to imminent Cybergeddon. That, of course, doesn't mean we should let our guard down. There are plenty of bad actors out there that will be more than happy to take advantage of any opening we give them. Let's see what openings they're looking to exploit.

Chart Toppers

Figure 2 identifies the most prevalent types of exploits observed by our IPS sensors, and things look a bit different this quarter. Namely, we detected an elevated level of attempts to inject and execute code/commands on target systems. That's nothing new, but it does seem to be reaching new heights.

We believe this trend may indicate threat actors are changing their tactics on exploiting systems. Simply put, attackers want more bang for their buck and this provides a mechanism to achieve that goal. Attacking vulnerable services was in vogue years ago before companies started shoring up their publicly exposed services. Phishing attacks then became the main delivery vehicle to implant code onto target systems. But it's possible that attackers could be going back to (or reincorporating) some of these "old-school" tactics. Attackers love to focus their efforts where/when defenders aren't watching. Could this be a sign organizations are letting their guard down on exposed services?

The specific vendors and devices targeted by these exploits aren't shown in Figure 2 (though you'll find them in the last section of this report), but a couple of trends are worth calling out anyway. A command injection vulnerability in JAWS MVPower digital video recorders rose out of the depths to devour IPS log space across all regions. Beyond that, many of the top exploit detections appear to be targeting web infrastructure and content management systems (CMS). So if the guard does have to slip somewhere, it's probably best not to let it be there.

Figure 3's regional breakdown of common malware observed over the quarter reveals a surprising predominance of one particular variant from the Framer family. The prevalence was so unusually extreme, in fact, that our initial reaction was that it must be a false positive. Once our researchers dug into these detections, that assumption proved partially correct ... but they also discovered the whole truth runs deeper than that.

	Europe	Northern America	Oceania	Latin America	Africa	Asia	Middle East
Code.Execution	50.5%	45.8%	48.4%	56.9%	50.5%	58.0%	52.2%
Command.Injection	44.8%	38.3%	41.4%	47.9%	42.7%	44.1%	42.3%
Command.Execution	41.5%	38.9%	38.3%	49.1%	39.9%	47.0%	39.5%
Buffer.Overflow	35.6%	33.9%	34.5%	40.7%	39.3%	41.8%	36.4%
Code.Injection	35.6%	33.5%	33.1%	42.4%	34.5%	38.1%	33.6%
SQL.Injection	35.9%	33.3%	32.3%	41.1%	33.9%	40.2%	32.9%
Information.Disclosure	34.6%	32.5%	31.9%	37.1%	34.0%	37.3%	31.3%
Multiple.Vulnerabilities	30.1%	27.0%	29.0%	35.2%	29.6%	35.1%	28.4%
Script.Injection	25.9%	25.0%	29.7%	32.2%	25.1%	32.8%	26.5%
Argument.Injection	26.8%	25.3%	23.3%	28.6%	24.8%	28.2%	22.5%

Figure 2: Most prevalent categories of exploit attempts detected in Q3 2019.

	Europe	Northern America	Oceania	Latin America	Africa	Asia	Middle East
HTML/Framer.INF!tr	35.1%	53.0%	40.5%	46.4%	44.1%	42.1%	43.5%
JS/Agent.OAY!tr	10.6%	18.2%	12.5%	13.9%	12.6%	16.5%	12.5%
HTML/ScrInject.OCKK!tr	9.7%	31.1%	15.1%	15.2%	14.4%	11.5%	10.8%
HTML/Download.7031!tr	11.4%	13.6%	11.4%	13.8%	13.4%	10.8%	11.7%
Riskware/InstallCore	7.1%	5.2%	7.1%	12.7%	16.3%	12.5%	12.4%
W32/InnoMod.AYH	6.4%	7.0%	9.8%	10.4%	12.5%	10.9%	8.1%
W32/Injector.EHDJ!tr	9.2%	2.3%	6.0%	5.9%	11.7%	11.1%	13.2%
MSOffice/CVE_2017_11882.B!exploit	9.7%	2.7%	6.8%	4.8%	7.9%	9.4%	12.1%
HTML/Phish.EMW!tr	8.0%	3.2%	7.7%	4.6%	8.2%	10.7%	10.9%
JS/Agent.OCQ!tr	8.9%	7.1%	10.2%	10.9%	5.9%	6.0%	7.7%

Figure 3: Most prevalent malware variants detected in Q3 2019.

The *HTML/Framer.INF!tr* signature detects webpages that use frames to connect to specific domains. These webpages contain a specific key that Adblock Plus, an open-source browser extension for content filtering and ad blocking, recognizes. This key is actually used to whitelist certain legitimate advertisement domains, such as Google AdSense. This allows Adblock to recognize them as safe and okay to be displayed to the public.

No harm, no foul so far. However, malware and malvertisement authors learned about this key and have begun using it for their own purposes. They include it in webpages so their domains circumvent the Adblock Plus browser extension. These domains may serve their own malicious advertisements, or in one example we found, may host a phishing page.

At the end of the day, there is no exploit here. It is a simple design flaw that attackers have been abusing for years to support their illicit schemes. And we have no way of producing a reliable signature because of the way Adblock is designed. But it serves as a good reminder that a) adversaries are crafty, b) they're perfectly happy to suborn legitimate features, and c) it's good to follow anomalies down the rabbit hole when possible.

If IPS and malware detections indicate what attackers are trying and spreading, botnet traffic reveals where they're succeeding. Communication with command and control (C2) infrastructure is often step one once a beachhead has been established in the network and is rarely a good sign (though still much better than missing that sign entirely). Figure 4 lists the most prevalent botnets we observed in Q3.

More so than any other type of threat, the top botnets tend to carry over with little change from quarter to quarter and region to region. That's an interesting window into modern cyber crime and suggests the control infrastructure is more permanent than particular tools or capabilities. But it also means we've already discussed these botnets numerous times in the past.

	Europe	Northern America	Oceania	Latin America	Africa	Asia	Middle East
Gh0st	71.4%	77.0%	81.4%	56.2%	57.2%	52.0%	53.3%
Bladabindi	69.4%	75.1%	79.4%	54.4%	57.3%	49.9%	51.8%
WINNTI	60.5%	65.2%	67.2%	46.3%	47.8%	37.7%	44.8%
Mirai	40.7%	27.3%	26.2%	42.6%	22.6%	23.2%	31.3%
Ganiw	28.3%	29.9%	33.0%	20.9%	20.9%	21.0%	20.5%
Pushdo	23.5%	26.7%	22.5%	19.3%	14.6%	15.7%	15.8%
Zeroaccess	11.1%	12.8%	9.8%	14.5%	12.8%	14.5%	9.8%
Xtreme	8.2%	7.3%	10.0%	10.4%	8.5%	10.0%	7.7%
Andromeda	2.5%	1.4%	4.1%	19.0%	27.4%	25.5%	26.6%
Sality	3.1%	3.1%	3.5%	7.6%	12.3%	14.4%	17.6%

Figure 4: Most prevalent botnets detected in Q3 2019.

Of those listed in Figure 4, WINNTI is the botnet most worthy of mention regarding its Q3 activity. Fellow Cyber Threat Alliance member, Lastline, published research attributing the surge in global WINNTI detections to nonmalicious "HELO" scans looking for infected hosts rather than actual attacks. While that's good news in this case, it's another example (along with the Framer malware detections discussed previously) of the broader challenge of distinguishing malicious from benign traffic in active networks. Such distractions make it even harder to keep our collective guard up. We hope this report helps improve that signal-to-noise ratio.

Featured Q3 Updates

Urgent/11 vulnerabilities put 200 million devices at risk

Many organizations, including healthcare and industrial firms, were left scrambling last quarter after multiple vulnerabilities were disclosed in Wind River VxWorks, a trusted real-time operating system deployed on more than 2 billion embedded devices. The vulnerabilities, collectively dubbed Urgent/11, gave attackers a way to take complete control of embedded devices and use them to steal data, execute denial-of-service attacks, and other malicious actions. The flaws evoked widespread concern because they impacted some 200 million devices including mission-critical ones such as those used in SCADA and industrial settings, for patient monitoring, such as MRI machines, and even enterprise firewalls and printers.

Fortinet observed sustained and substantial scanning activity for multiple VxWorks bugs targeting thousands of organizations in Q3 2019. The relative volume and prevalence of detections tied to these vulnerabilities can be seen in Figure 5. We haven't featured a chart like this before, so some explanation may be needed. For each vulnerability listed in Figure 5, the arrows indicate the percentile ranking of related IPS detections. For example, the volume of triggers for the *VxWorks.WDB.Agent.Debut.Service.Code.Execution* detection exceeded ~95% of all detections we observed for the quarter. Exploit volume for the *Wind.River.VxWorks.Large.DHCP.Packet.Handling.Heap.Overflow* was much lower and somewhere near the 5th percentile.

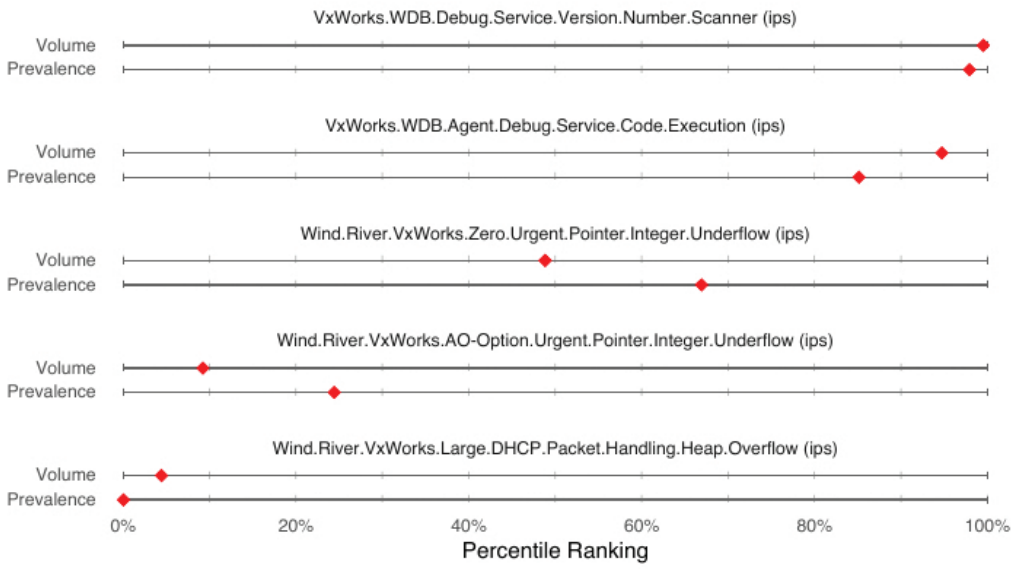


Figure 5: Ranking of exploit activity targeting multiple vulnerabilities in Wind River VxWorks.

Armis, the company that first reported Urgent/11, later updated its advisory to disclose six other real-time operating systems that were vulnerable as well because they used the same VxWorks TCP/IP stack. The six operating systems were identified as: ThreadX by Microsoft, INTEGRITY from Green Hills, Operating System Embedded by Enea, ITRON from TRON Forum, Nucleus RTOS from Mentor, and ZebOS from IP Infusion. The Armis report prompted an advisory from the FDA warning medical device manufacturers of the threat.

Takeaway: The level of activity across the Wind River VxWorks vulnerabilities underscores the need for organizations to ensure their vulnerability management program is holistic in scope. It may be tempting to relegate nontraditional infrastructure to the back burner, but the scope of deployment and mission of these systems demand attention. Patches for these vulnerabilities are available and we strongly recommend deploying them.

Banking malware evolving to leverage predecessors' success

In a troubling development for enterprise organizations, cyber criminals are increasingly using banking Trojans to drop other payloads and additional banking malware on infected systems to maximize their opportunities for financial gain. The constantly evolving Emotet provided an example of that trend when—after months of relative quiet—we spotted a sudden surge in spamming activity related to the banking malware.

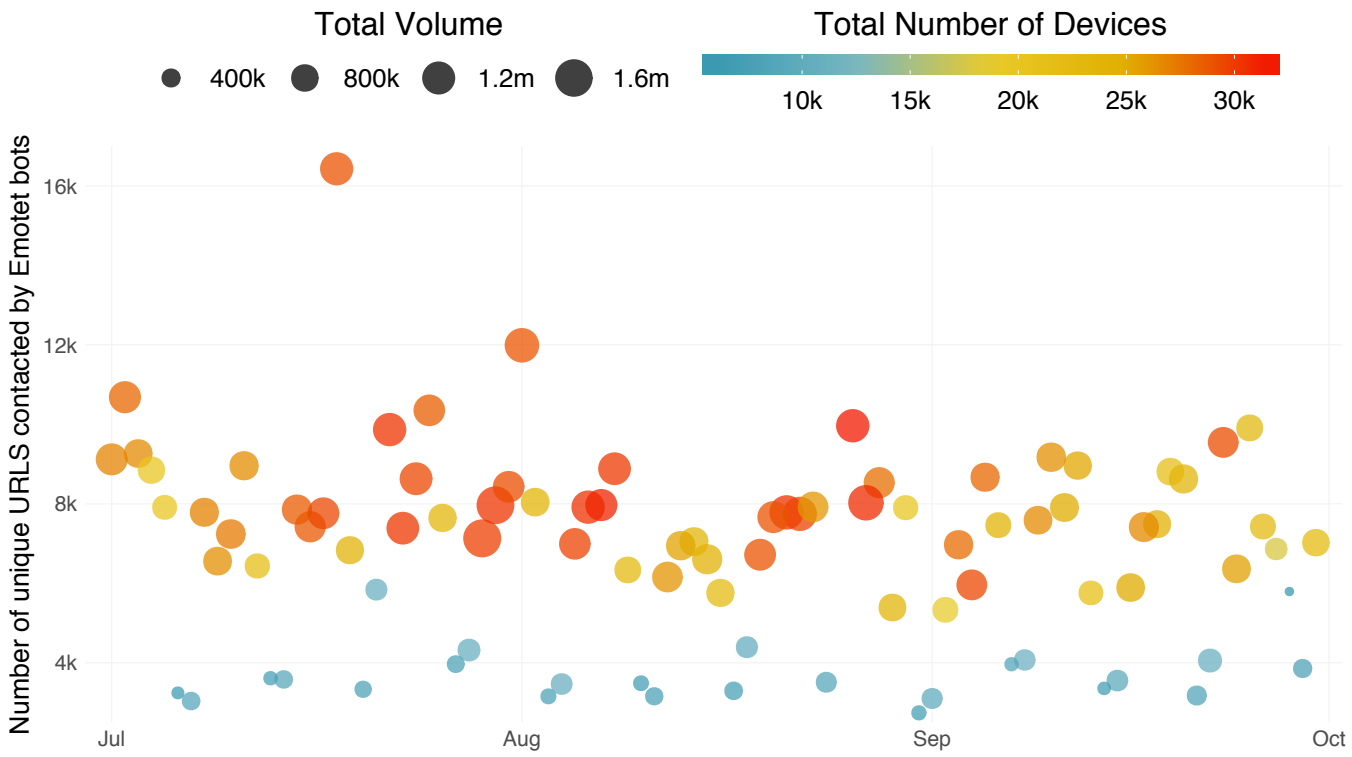


Figure 6: Communications to domains associated with Emotet detected by FortiGuard Web Filter service.

The spike in activity had to do with Emotet being used in a spear-phishing campaign to distribute TrickBot, a dangerous piece of malware that has been targeting the financial services industry since at least 2016. Like Emotet, TrickBot primarily spreads via email, though both banking Trojans can also propagate via SMB file shares using the EternalBlue exploit, mentioned in the next section.

Emotet began life as a fairly basic banking malware in 2014 and has gone through multiple iterations since then. Initially, the malware was delivered as a malicious JavaScript file but later versions have used macro-enabled documents, PDF files, and weblinks to fetch malicious payloads from a C2 server. The banking Trojan's operators no longer simply maintain the malware; they are also actively distributing malware for other attack groups, particularly in Eastern Europe.

Recently, attackers have begun using Emotet as a payload delivery mechanism for ransomware, information stealers, and other banking Trojans including TrickBot, IcedID, and Zeus Panda.

In one reported campaign earlier this year, attackers slammed targeted organizations with an especially potent combination of Emotet, TrickBot, and Ryuk ransomware. Emotet was used to download TrickBot, which then stole credentials and other data from the compromised network and finally helped deliver Ryuk on targeted systems.

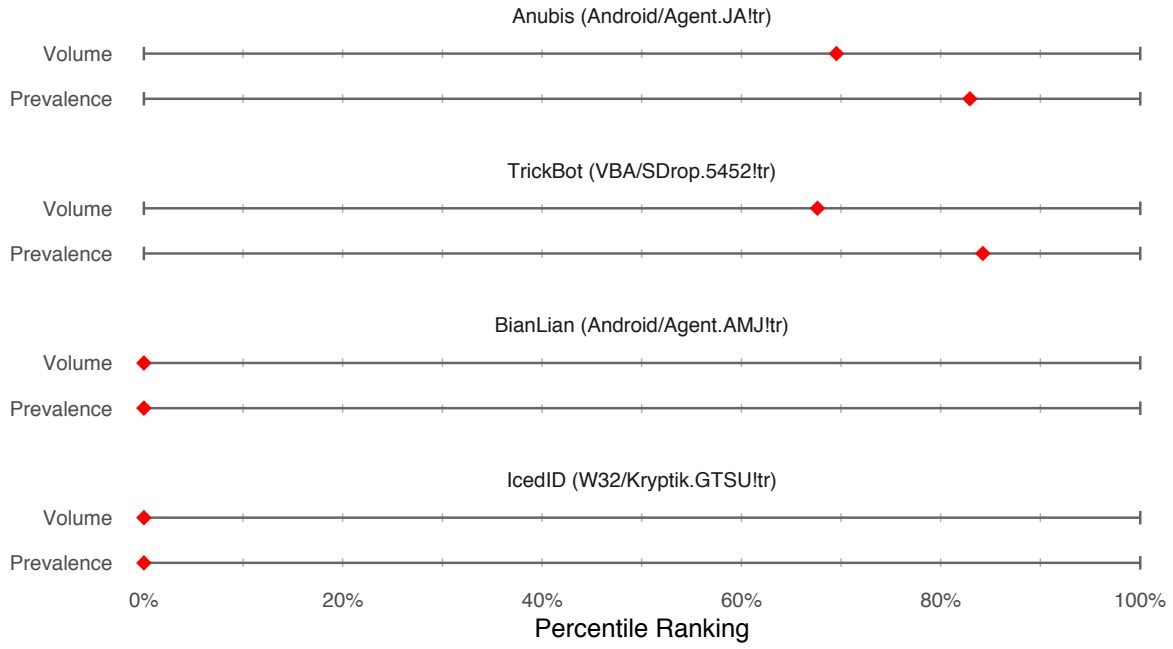


Figure 7: Ranking of detections for several banking malware samples analyzed in Q3.

TrickBot and IcedID were two other banking malware families for which we observed activity last quarter. TrickBot, like Emotet, started off as a banking Trojan designed to steal online banking information. But over the years it has assumed multiple roles. We discovered a targeted attack in VirusTotal in early September involving a TrickBot variant with a spamming module for harvesting a victim's address book and using the addresses to self-propagate to other systems in order to steal data. Another sample we collected last year had a new module for stealing credentials, autofill data, browser histories, and other information from an infected host. That particular variant was spread via an Excel file with malicious VBS code. There have also been reports about TrickBot being used to drop Emotet and possibly other banking malware and ransomware.

IcedID is a relatively new banking Trojan that in many ways epitomizes the changes going on in the banking malware space. The malware was first discovered in 2017 and has earned a reputation for constantly evolving and becoming more sophisticated with each iteration, especially with respect to its evasion capabilities. The malware injects itself into web browsers and can act as a proxy to inspect and manipulate traffic. It steals information—such as the credentials to a user's online bank account—and sends the information to an attacker-controlled remote server.

Initially, the authors of IcedID used other banking Trojans such as Emotet and Ursnif (aka Gozi) to distribute their malware. Later they added TrickBot to the mix as well. But like its more recent counterparts, IcedID can do more than just steal information for enabling financial theft from banks, payment card providers, and other services. Our investigation of some IcedID samples in June showed that the malware in turn can deliver a TrickBot payload—and presumably other payloads if needed. Since the malware first surfaced, some researchers have observed growing behavioral similarities between IcedID and TrickBot, hinting at a collaboration between the two groups behind them.

Takeaway: Malware is a complicated ecosystem to say the least. With so many interrelated and ever-evolving variants emerging constantly, it's easy to lose sight of what's happening in the bigger picture. But one thing we can count on is that cyber criminals will always seek easy money and malware is a tool to that end. As with legitimate business models, the easiest way to make money is to leverage existing investments and successes. That's the bigger picture of what we see here: Use successful malware to expand business opportunities. Don't buy in.

EternalBlue, BlueKeep still at it and delivering a one-two punch

The BlueKeep vulnerability in Microsoft's Remote Desktop Protocol (RDP) service and the older EternalBlue exploit targeting a flaw in Microsoft Server Message Block (SMB) protocol continued to remain potent threats last quarter. They served as useful reminders to enterprises of the need for timely patching.

In September, Rapid7's Metasploit Project released a public exploit for BlueKeep that essentially gave attackers a tool for leveraging the flaw to take remote control of Windows systems. The exploit sparked concerns about attackers exploiting BlueKeep to launch a WannaCry or NotPetya-like mass attack. The exploit is one of many that are thought to have become available for BlueKeep since Microsoft patched the vulnerability back in May.

BlueKeep (CVE-2019-0708) is a vulnerability affecting Windows XP, Vista 7, Server 2003, and Server 2008. The flaw allows an unauthenticated user to connect to a vulnerable Windows system via RDP and take complete control of the system. The flaw is considered especially dangerous because it is "wormable"—meaning malware can spread autonomously from system to system in the same manner that WannaCry did in 2017. Microsoft, the United States Department of Homeland Security, and the NSA are among the many that have warned about the severity of the risk, but a substantial number of organizations are believed to remain unpatched against BlueKeep.

Fortinet detected significant activity for the BlueKeep signature in the U.S., Taiwan, and India last quarter. The activity indicates that attackers are actively looking for vulnerable systems with exposed RDP services. Companies that don't patch or mitigate the issue are not only exposing themselves, but others to the threat as well.

Meanwhile, Gh0stCringe RAT, another threat that surfaced in Q3, showed that attackers are continuing to target systems that are vulnerable to the EternalBlue exploit (MS17-010).

The NSA is believed to have developed EternalBlue for offensive cyber-intelligence purposes. An outfit called the Shadow Brokers leaked the tool publicly as part of a massive data dump in 2017. The exploit targets a security vulnerability in the Server Message Block 1.0 (SMBv1) server in multiple Windows versions. It allows attackers to take complete remote control of a vulnerable system and execute code of their choice on it. Microsoft issued a patch for EternalBlue and multiple related exploits soon after the details were leaked in 2017. As with BlueKeep however, hundreds of thousands of systems—a majority located in the U.S.—are thought to still be vulnerable to the EternalBlue exploit.

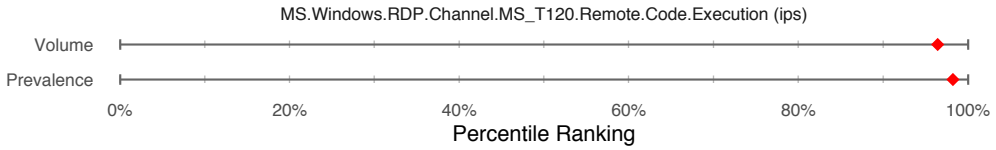


Figure 8: Ranking of exploit activity targeting BlueKeep vulnerability (CVE-2019-0708).

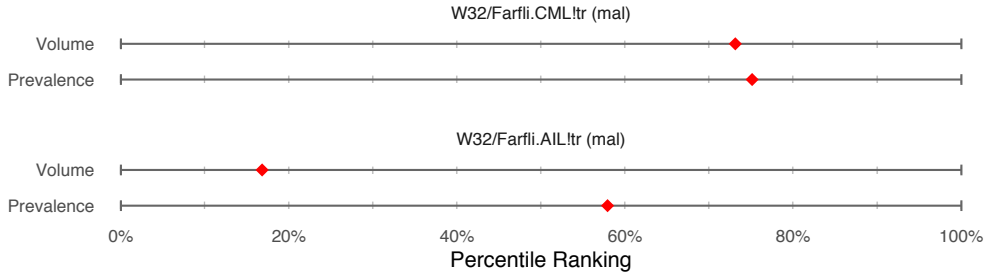


Figure 9: Ranking of detections for two common variants of the Gh0stCringe RAT.

These attributes make it very attractive to criminals as a dropper to deliver a range of exploits to target systems, including BlueKeep. Gh0stCringe is a nasty Remote Access Trojan that exploits EternalBlue to infiltrate systems and leave them open to remote attacks. The malware is similar to Gh0st, a RAT that just so happens to occupy the top spot among botnets in Q3 (see Figure 4). It is spyware that enables attackers to log keystrokes, remotely control webcams, download files, and execute other malicious actions. Just as with Gh0st, the new Gh0stCringe RAT also encrypts all communication between an infected host and the C2 server, though the actual encryption protocol itself is slightly different. One tactic that Gh0stCringe uses to evade forensics is to uninstall itself completely from an infected file and to also wipe all event logs associated with it. The majority of Gh0stCringe activity during the third quarter was focused on Chinese targets.

Gh0st and Gh0stCringe are just two examples of malware currently targeting EternalBlue. There are several others. Banking Trojans Emotet and TrickBot, for instance, have exploited and continue to exploit the vulnerability to spread laterally within an infected network. Smominru, a Monero mining malware and botnet that we have been tracking since 2017, also continues to infect thousands of enterprise Windows systems in the U.S. and elsewhere via the EternalBlue exploit.

Takeaway: The continued activity surrounding BlueKeep and EternalBlue shows how unpatched vulnerabilities—regardless of age—can heighten exposure. It's usually bad form to introduce new stats in a "takeaway," but here's one anyway: In Q3 of 2019, we saw more attempts targeting vulnerabilities from 2007 than from 2018 and 2019 combined. Every year in between equals 2018/19 levels. The point is that attackers (and their tools) don't ignore old vulnerabilities and neither should you.

Ransomware-as-a-Service appears to be gaining ground

The cyber criminals behind the prolific GandCrab ransomware strain reportedly made more than $2 billion in less than two years before "retiring" this May. Much of those illegitimate gains came from their use of a Ransomware-as-a-Service (RaaS) model to distribute the malware. By establishing a network of affiliate partners, GandCrab's authors were able to spread their ransomware widely and scale earnings dramatically in the process.

Last quarter, we observed at least two other significant ransomware families—Sodinokibi and Nemty—being deployed in a similar manner, suggesting the Ransomware-as-a-Service model is gaining ground. Sodinokibi (aka Sodin, REvil) surfaced shortly before GandCrab's authors supposedly retired and quickly became one of the biggest ransomware threats in Q3. It was used in multiple targeted attacks on major organizations including nearly two dozen local governments in Texas.

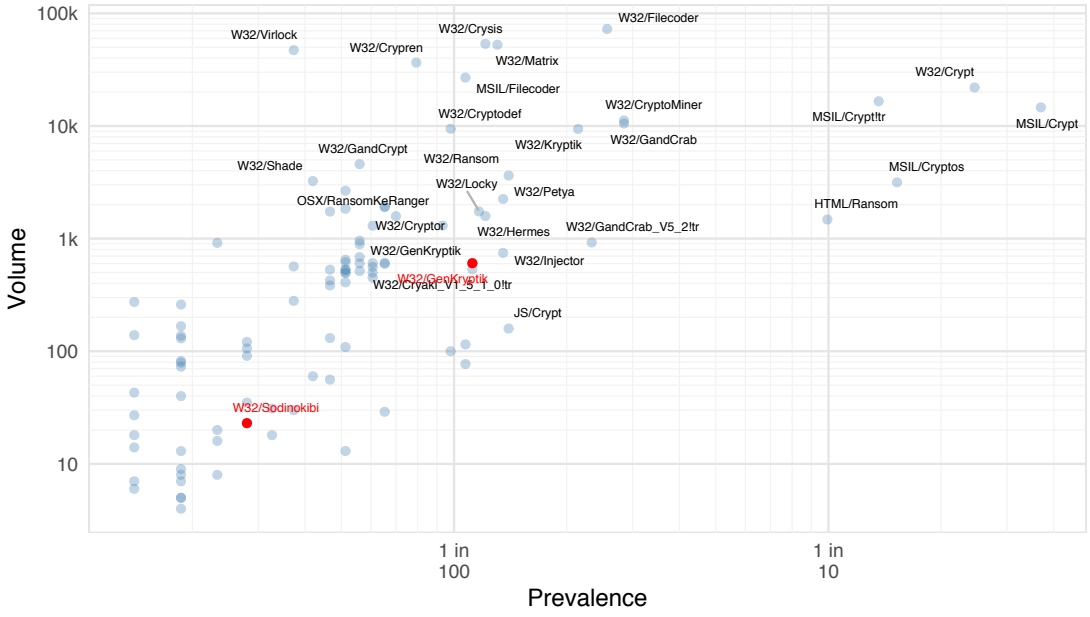


Figure 10: Prevalence and volume of Sodinokibi detections in the context of other ransomware.

Attackers used a variety of tactics to distribute Sodinokibi including phishing, exploit kits, and software vulnerabilities such as a deserialization flaw in Oracle WebLogic that was disclosed early this year (CVE-2019-2725). Toward the latter part of the quarter, we observed attackers also taking advantage of a former Windows Zero-Day privilege escalation bug (CVE-2018-8453) to distribute the ransomware. We believe Sodinokibi is unique among ransomware strains in exploiting a remote code execution vulnerability such as this to infect systems.

Our analysis showed Sodinokibi to have sophisticated capabilities for evading AV detection. In that regard, it is similar to many other modern malware tools that incorporate multiple anti-analysis techniques including those for detecting sandboxes and emulators and for disabling security controls. The biggest clue that Sodinokibi is being distributed via an RaaS model is a "skeleton key" embedded in the code. The universal decryption key allows Sodinokibi's authors to unlock any file regardless of the keys that were originally used to encrypt it.

Because of certain code similarities, some researchers have theorized that the authors of GandCrab also created Sodinokibi. However, the fact that we observed Sodinokibi operating alongside GandCrab calls that theory at least somewhat into question.

Nemty is another ransomware strain with links to GandCrab that surfaced last quarter. We came across the file-encrypting malware when investigating Sodinokibi. During our analysis of Nemty we found an artifact embedded in its binary that GandCrab's authors had also used before their retirement announcement. We observed Nemty being distributed in a similar fashion to Sodinokibi. There were also some reports about the malware being distributed via vulnerable or compromised Remote Desktop Protocol (RDP) services. We found what looked like an affiliate ID hard coded into the malware code that suggested the malware is being sold on an RaaS basis just like Sodinokibi and GandCrab. Our analysis of Nemty revealed several irregularities and inefficiencies in its code that hinted the malware is still in its early stages of development.

Sodinokibi and Nemty are the latest evidence that ransomware continues to be a clear and present danger to enterprise organizations. The recent success that many ransomware purveyors have had in extorting sizable ransoms from business victims has encouraged others to join the fray. Many threat actors have eschewed mass-volume spray-and-pray attacks for more carefully planned, targeted ones aimed at maximizing disruption.

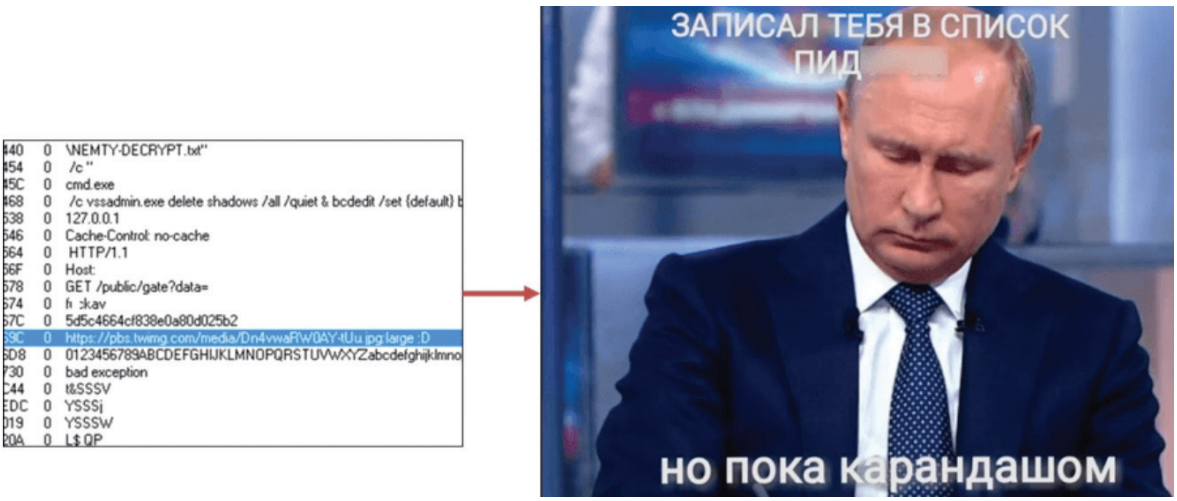


Figure 11: Screenshot of Nemty binary with embedded link to an image very similar to one used by GandCrab.

Takeaway: By using an RaaS model, the authors of malware such as Sodinokibi and Nemty are significantly lowering the bar for launching such attacks. That lowered bar makes this particular form of cyber crime accessible and profitable for a larger pool of bad actors. Here's what we're doing to ruin that criminal business model, and some steps you can take to help.

Playbook Preview: Emotet Botnet

Rampant, Dangerous, and Devastating, Emotet is among the most alarming threats currently active today. At its initial discovery in 2014, Emotet was a simple banking Trojan. However, thanks to its modular nature, it has grown to incorporate botnet capabilities, obfuscation techniques, and other new features. Currently Emotet is active in a large-scale global campaign, indiscriminately targeting victims worldwide.

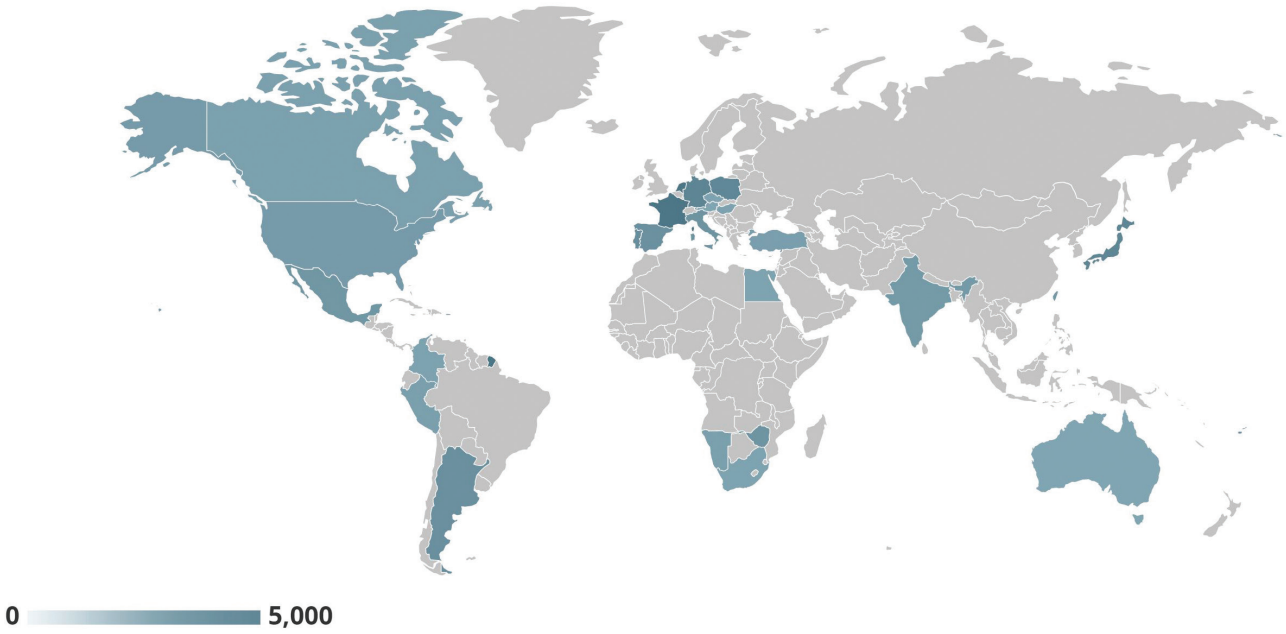


Figure 12: Geographic location of infrastructure known to be associated with Emotet.

Upon initial discovery in 2014, Emotet spread itself via malicious spam. These emails contained a link that would download two payloads: a configuration file that scans for predetermined banks and a DLL file that intercepts information from web browsers by injecting itself into processes. In order to avoid detection, Emotet continues to lean on its registry, as it has since its discovery. The advantages to this technique include longer time on target due to the encryption of exfiltrated data and requiring a far more complex search from victims in order to discover the infection.

Emotet associates with a bad crowd, being seen with the likes of the Carberp, Feodo, Cridex, and Bugat families. In recent years it has played a direct role in distributing IcedID, Zeus Panda Banker, TrickBot, and AZORult. This incorporation of a variety of threats and malware families has earned Emotet notoriety from a variety of organizational types, from law enforcement to threat researchers.

Underneath the success of the large-scale campaign Emotet is currently engaged in is an unknown team of threat actors. These threat actors are likely a dark mirror of a legitimate software company, operating precisely and in a well-disciplined manner. The vast quantities of attacks and continued updates to Emotet would not be possible without a highly skilled and dedicated group constantly directing and improving the virus.

Currently Emotet is spread largely through email, although other social engineering strategies have been observed. Emails sent for this purpose are from hijacked accounts previously used by individuals the target has already contacted. Not only will these attacks come in the form of new emails but also replies to preexisting email threads. It should be noted that this method can be somewhat obvious, with the target possibly noticing the sudden shift in conversation topic. Within these malicious emails is a zip file containing a malicious Word document. This document will download a payload via PowerShell. After the payload is deployed, Emotet will begin to search through the contents of files on local and remote computers. Insidiously, a second file connecting to a different C2 server, but identical otherwise, lies in wait. If the victim discovers the first file, then the second file will activate, ensuring a second chance at a successful attack.

The scale of Emotet's current campaign, as well as its capabilities, association with other major threats, and logistical support from its creators, makes it a threat with catastrophic potential. Its modular nature and constant updates ensure that it will be quite some time before Emotet becomes obsolete. We recently added Emotet to our Playbook Viewer, where you can find more information about their tactics and how to thwart them.

Exploratory Analysis: Organizational Threat Profiles

This report regularly presents threat statistics and trends in aggregate across our sensors. Obviously, we believe this to be helpful, or we wouldn't waste your time or ours with such analysis. But it may cause some to conclude that the top threats, like those shown in Figures 2 through 4, are the same for every individual organization. That is absolutely not the case, as we will demonstrate in this brief exploratory analysis of our IPS data.

Figure 13 identifies technologies targeted most widely by exploit attempts in Q3. We have shown similar views before, but the key difference here is that we compare the relative prevalence of those exploits among a sample of organizations. While commonalities do exist among firms (which are represented by rows), the chart makes it clear that each has a unique threat profile. Some report plagues of Microsoft exploits, Apache dominates others, and segments of different lengths and colors comprise them all.

Figure 13 is sufficient to make the point, but we can also apply this same technique to the categories of exploits detected. Figure 14 reinforces the notion that organizations deal with similar types of threats but in dissimilar ratios.

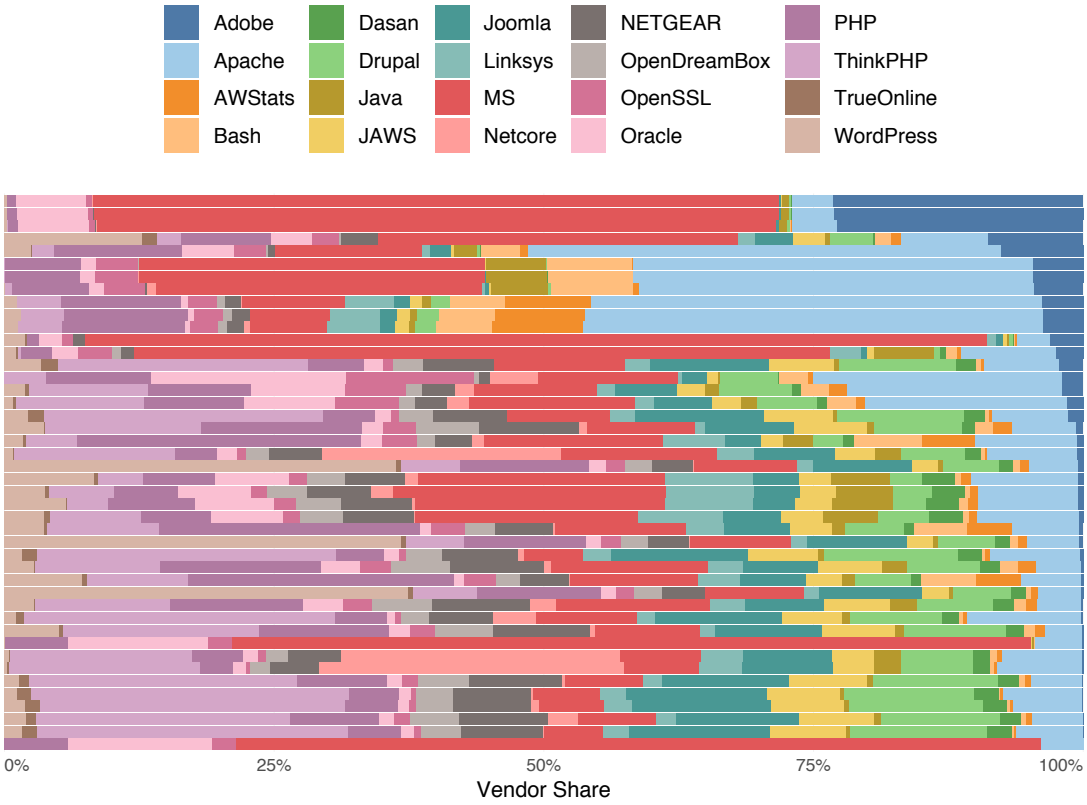


Figure 13: Comparison of top technologies targeted by exploits reported by a sample of organizations (shown as individual rows).

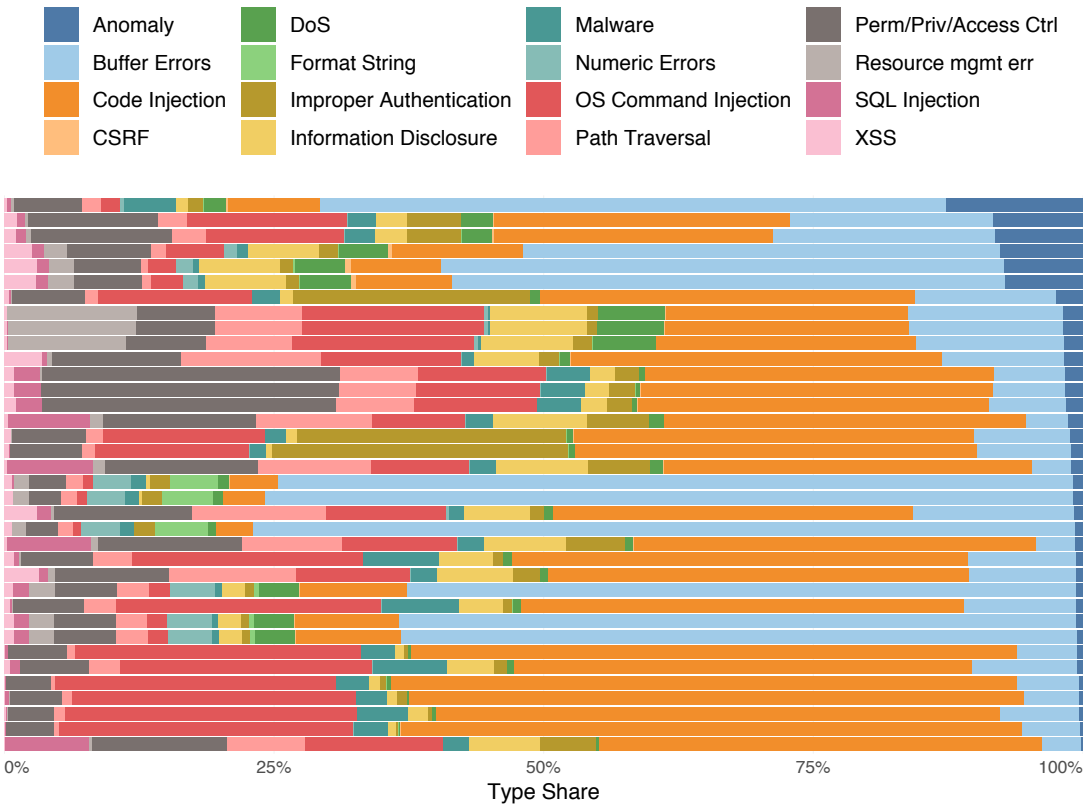


Figure 14: Comparison of top exploit categories reported by a sample of organizations (shown as individual rows).

The fact that each organization's profile is unique may not fundamentally alter your perspective. But it's a good reminder that having clear visibility into both surrounding areas and the immediate terrain is important to navigating the cyber-threat landscape. This report should help with the former and your friendly neighborhood Fortinet representative is standing by anytime you need help with the latter.

Reference

[1] IDC Worldwide Security Appliances Tracker, March 2019 (based on annual unit shipments)

www.fortinet.com

520097-0-0-EN