

QUARTERLY

Threat Landscape Report



Table of Contents

Introduction and Overview	3
Q4 Chart Toppers	4
Featured Q4 Updates	8
Exploratory Analysis: Who's Spamming Whom?	13
Reference	15

Q4 2019 Introduction and Overview

Concern over cyber threats keeping you up at night? Wondering which ones warrant your prompt attention and which ones can wait until later? We all have such questions and even the most informed among us could use some extra intel to help answer them from time to time. And that's exactly why we publish this Threat Landscape Report to detail the threats and trends analyzed by our researchers. Here's a glimpse of what you can look forward to in this edition:



Chart Toppers

Which threats registered the highest levels of activity last quarter? Which ones are old news and which constitute something new you should be watching out for? We tackle these burning questions by peering into the billions of exploit, malware, and botnet events observed across our sensors.



A WIFICAM Whodunit

Everyone loves a good “Whodunit” and threat researchers are no exception. Exploit detections surged this quarter for a seemingly mundane networked camera, prompting us to wonder what was going on and who was behind it. This is no open and shut case; it's full of intrigue and plot twists that you won't want to miss!

vBulletin

Latest Stresses for CMS

We've talked a lot about vulnerabilities in content management systems (CMS) in the past, but the fact that they comprise four of the top five intrusion prevention system (IPS) detection targets in Q4 leads us to do it again. We focus on the latest platform climbing the exploit charts, vBulletin.



Start Spreadin' the Blues

In a potentially dangerous development, the EternalBlue Downloader gained the ability to exploit BlueKeep, a critical vulnerability in Microsoft's Remote Desktop Protocol (RDP). If that sounds eerily familiar, you probably remember the EternalBlue exploit that caused havoc in the WannaCry and NotPetya ransomware outbreaks. Experts fear this latest “Blue” is similarly primed for widescale attacks.



The Death of Ransomware

Not “death” as in going away forever; we don't see cyber criminals abandoning the ransomware cash cow anytime soon. We're referring here to the “Deathransom” malware that emerged last quarter. It seemed to do everything ... except the one thing ransomware should do—encrypt files. This prompted some to label it a hoax. We examine how real it is and whether it lives up to its name.



A Not So Charming Kitten

Charming Kitten (aka APT35) is a cutely named threat group with a not-so-cute disposition. Active since at least 2014, their latest scratching post is a series of attacks on targeted email accounts associated with a U.S. presidential election campaign. This suggests the Iranian threat actor is sharpening its claws for the election-disruption business.



Who's Spamming Whom?

Our exploratory analysis for this quarter digs into data from our FortiMail email gateways. Have you ever wondered which countries produce the most spam and where they ship it? If so, this spam dish should delight your palate.

Q4 Chart Toppers

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.

Exploit Detections

Exploit detection trends reveal what adversaries do to recon and compromise vulnerable systems. Triggering one of the many threats detected this quarter doesn't mean the attack succeeded, but it does provide good intelligence on which types of vulnerabilities and systems are actively in the cross hairs. Top platforms and technologies targeted by exploit activity in the fourth quarter of 2019 are plotted in Figure 1 according to prevalence (horizontal axis) and volume (vertical axis).

Prominent in the upper left-hand corner, attempts to exploit a vulnerability (CVE-2019-12678) in the Session Initiation Protocol (SIP) inspection module of Adaptive Security Appliances ranked highest on the volume scale. Successful exploitation results in a denial-of-service condition, which helps explain how this exploit achieved such high volume despite its moderate prevalence.

The HTTP.Server detection grouping includes several signatures, but one indicating detection of an overly long HTTP Authorization value was responsible for the bulk of volume. Successful attacks may allow a remote attacker to execute arbitrary code within the context of the web server, crash the affected application, or deny services to legitimate users.

Continuing our journey down and to the right arrives an exploit targeting multiple vulnerabilities found in several wireless camera models (WIFICAM). There are some aspects to this activity that we thought worthy of a standalone analysis, and you can read more about it in the "Featured Q4 Updates" section below.

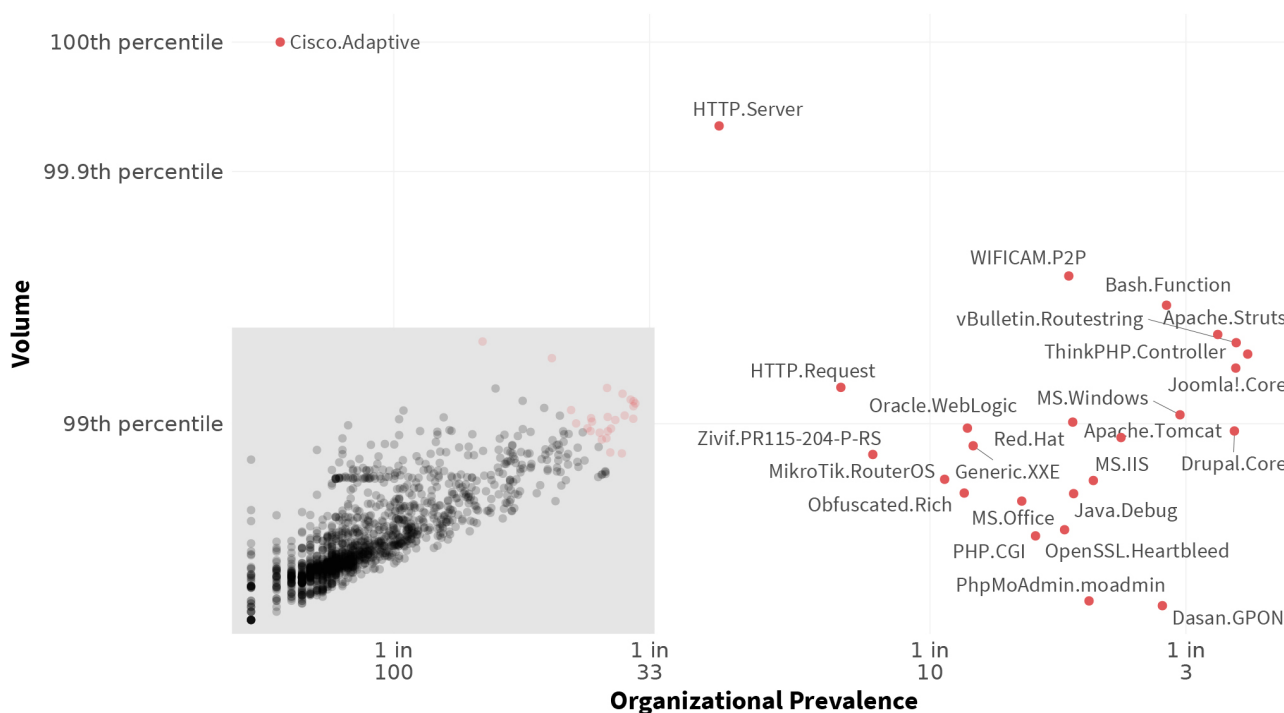


Figure 1: Top 25 technologies targeted by exploit activity in Q4 2019 by global prevalence and volume.

The cluster on the right of Figure 1 represents the most widespread IPS detections in terms of the proportion of firms reporting them. Four of the five most prevalent exploits target vulnerabilities in popular CMSes like ThinkPHP, Joomla, Drupal, and vBulletin. We've covered those first three multiple times in prior reports, and at the risk of downplaying their importance (we're not; they're persistent for a reason), we've chosen to spotlight the latter this quarter. You'll find more on vBulletin in our section of featured updates.

Black hats and red teams have been scanning for Apache Struts vulnerabilities in earnest since the Equifax breach more than two years ago. If that's still exposed in your environment, well then you should stop reading now and get that vulnerability locked down.

That covers the top five of the most widespread exploits in Q4, but we understand many of you will want to continue further down the list. We offer Figure 2 to make that exploration easier and more informative. It has the added bonus of enabling comparisons of detection prevalence among regions.

We encourage readers to find the region(s) relevant to them at the top of the chart and scan down the list of threats. You'll notice that, for the most part, the top five or so threats are consistent across regions, which reflects the opportunistic nature of, for instance, scanning for ThinkPHP vulnerabilities across a wide IP range. But things begin to shift around lower down the figure. While still not indicative of targeted attacks, such variation stems from technology adoption, system configuration, security posture, and a range of other details.

	Africa	Asia	Europe	Latin America	Middle East	Northern America	Oceania
ThinkPHP.Controller	34.6%	42.5%	39.1%	43.2%	35.3%	37.6%	40.0%
vBulletin.Routestring	33.2%	37.5%	38.8%	42.5%	33.9%	35.3%	38.2%
Joomla!.Core	32.7%	41.0%	37.9%	41.2%	32.7%	35.0%	36.9%
Drupal.Core	33.1%	40.2%	37.6%	40.5%	33.3%	34.8%	37.9%
Apache.Struts	29.4%	44.5%	32.1%	36.4%	31.2%	30.7%	39.8%
MS.Windows	28.9%	32.6%	26.5%	31.3%	28.8%	29.0%	30.8%
Dasan.GPON	24.7%	25.2%	30.9%	30.6%	25.4%	23.7%	29.3%
Bash.Function	15.9%	27.9%	28.8%	36.6%	19.4%	28.8%	22.5%
Apache.Tomcat	19.9%	33.8%	20.0%	24.2%	20.2%	18.2%	28.6%
MS.IIS	18.1%	21.8%	21.1%	20.9%	16.6%	20.0%	20.5%
PhpMoAdmin.moadmin	16.6%	20.0%	20.1%	19.6%	14.1%	23.6%	18.1%
Java.Debug	18.3%	22.1%	15.9%	19.3%	17.7%	19.5%	15.5%
Red.Hat	15.6%	25.7%	16.5%	23.2%	17.3%	13.7%	23.8%
WIFICAM.P2P	13.2%	21.3%	17.6%	19.2%	13.6%	19.5%	16.7%
OpenSSL.Heartbleed	18.4%	19.1%	20.1%	13.0%	13.0%	19.7%	17.7%
Plone.Zope	14.2%	19.4%	16.7%	17.8%	13.2%	19.1%	16.3%
Alcatel-Lucent.OmniPCX	12.9%	19.3%	17.2%	17.5%	13.1%	19.5%	17.1%
AWStats.Configdir	13.7%	18.6%	17.4%	18.2%	13.0%	19.3%	16.4%
MS.Office	20.3%	19.5%	18.7%	11.5%	14.6%	8.2%	14.1%
PHP.CGI	16.1%	15.2%	16.3%	15.5%	10.7%	18.8%	14.7%

Figure 2: Top 25 IPS detections in Q4 2019 by regional prevalence.

Malware Detections

Studying malware trends is beneficial because they reflect adversary intent and capability. Similar to exploits, malware detections by our sensors do not always indicate actual infections, but rather the weaponization of code and/or attempted delivery to target victims and systems. Detections can occur at the network, application, and host level on an array of devices.

Figure 3 lists malware variants that registered the highest average volume per organization across the globe in Q4 2019. The ever-iterating nature of malware results in file names that are mostly meaningless to anyone other than malware researchers or those responsible for maintaining anti-malware products. For those of you not in one of those groups, our [Threat Encyclopedia](#) will help you make some sense of it all.

Without getting too deep into malware-naming gibberish, Figure 3 does contain some high-level takeaways. For instance, note the prefixes across the variants, which tell us about their language or platform. The fact that we see Windows, Visual Basic, HTML, JavaScript, Adware, etc., reminds us that attackers design malware to target a wide variety of systems through a wide variety of vectors. Malware is an innovative and rapidly evolving threat, and we all do well to remember that.

It's also apparent from the chart that malware isn't evenly distributed around the world. The mind naturally attributes that to regional targeting by threat actors, but while that's certainly a factor, technology adoption, user behavior, national and corporate policies, culture, and even random chance shape those trends as well. The HTML/ScrInject.OCKK!tr variant serves as a good example. We haven't seen use of this Trojan by any known campaigns to target organizations or individuals in Latin America, but detections still shot up over the quarter (Q3 showed the heaviest volume in Northern America).

	Africa	Asia	Europe	Latin America	Middle East	Northern America	Oceania
W32/FlyAgent.K!tr.bdr	11.8	45.1	20	17.7	12.6	9.2	15
VBA/Agent.QAP!tr.dldr	32.7	24.5	17.4	16.5	13.5	3.1	9.1
W32/Injector.EHDJ!tr	22.1	20.9	4.9	3.7	13.3	4.9	5.3
W32/Wintri!tr	32.4	83.6	4.7	6.4	6.9	5.7	1.6
HTML/ScrInject.OCKK!tr	9.7	5.3	20.7	163.8	16	81.4	1.6
VBA/Agent.NVE!tr.dldr	31.7	12.6	10.7	19.1	1.7	4.8	5.6
W32/Frauder.ALT!tr.bdr	31.6	4.6	3.3	9.5	4.2	2.3	5.8
JS/ProxyChanger.ES!tr	44	33.7	2.9	6.1	9.4	3.2	0.5
VBA/Agent.136E!tr.dldr	3.4	14.9	3	6.5	6.6	2.9	2.6
VBA/Agent.IP!tr.dldr	5.9	5.2	3.6	7	3.4	1.4	2.7
Adware/AdblockPlus	11.9	5.5	1.9	3.6	2.8	3.5	1
VBA/Agent.D5CD!tr	5	9.1	19	9.1	1.3	3.5	2.8
VBA/Agent.F36A!tr.dldr	11.3	8.3	3.4	3.6	2.5	1.1	3
MSOffice/CVE_2017_11882.C!exploit	6.8	10	2.3	12.5	5.1	1.2	0.7
W32/Glupteba.B!tr	13.6	48.1	0.6	8.3	21.9	1	0.6
W32/CrypterX.1A93!tr	9.9	59.7	0.6	13.1	31.2	0.3	4.2
W32/Banker!tr.pws	4.1	10.1	2.3	4.5	5	0.8	3.8
MSOffice/CVE_2017_11882.B!exploit	7	10	3.2	2.3	4.1	0.9	1.1
W32/SillyFDC.A!worm	8.2	3.4	2.3	6.5	4.8	1.1	0.7
HTML/Framer.INF!tr	9.1	3.9	1.1	2	2.1	2.4	1.5

Figure 3: Top 25 malware variants in Q4 2019 by regional volume per organization.

We also observed several malware variants outside the top 25 that we feel deserve mention. Dexphot is one example of those. This polymorphic malware (malware that rapidly changes its form/features) was first discovered in October 2018 and since then has been observed deploying files that change form repeatedly over the course of a single day. Dexphot's payload is a cryptominer that runs solely in memory and is hard to trace. This, combined with its polymorphic nature and its capability to utilize monitoring and re-infection techniques, makes the malware extremely persistent. Microsoft described Dexphot as exemplifying the sophistication and complexity that is present in even the most mundane malware tools these days.

Another example was a tandem of malicious JavaScript files targeting Magento's ecommerce platform and CMS that spiked in mid-November. The Magecart cyber-crime conglomerate was very active in Q4, placing digital credit-card skimmers on compromised ecommerce sites. One particular group operating under the Magecart umbrella is known to deploy skimmers via JavaScript libraries used for things like tracking visitors, serving ads, and site analytics, so these detections raised our hackles.

Also on the naughty list, Trickbot returned for the holiday season to spread fake emails about end-of-year bonuses and payroll issues. Inside of these emails is a link to a malicious Google Drive doc containing Trickbot. Trickbot has undergone several code modifications in recent months, expanding its targets to mobile devices and online banking users in Japan.

The "2019 Holiday Gift Everyone Wants But Nobody Needs" award goes to Ai.type, an Android app that allows for keyboard customization and has had 40 million downloads. The app was discovered to be signing up users for various paid services without the victims' knowledge, prompting Google to remove the app from their store. So far, 14 million suspicious transactions have been traced back to Ai.type, totaling more than \$18 million. Too bad that's not eligible for regifting.

Botnet Detections

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 malicious hosts, and such traffic in a corporate environment indicates something went wrong. That makes this dataset valuable from a “learning from our mistakes” perspective.

The most active botnets for Q4 2019 feature the usual suspects we’ve grown accustomed to seeing. From a pure newsworthiness standpoint, there’s little to note among these top botnets. We’ve been writing [analyses](#), [blogs](#), etc., on most of these for years now. But that fact is the real story here—why do these botnets have such staying power, despite even coordinated takedown operations?

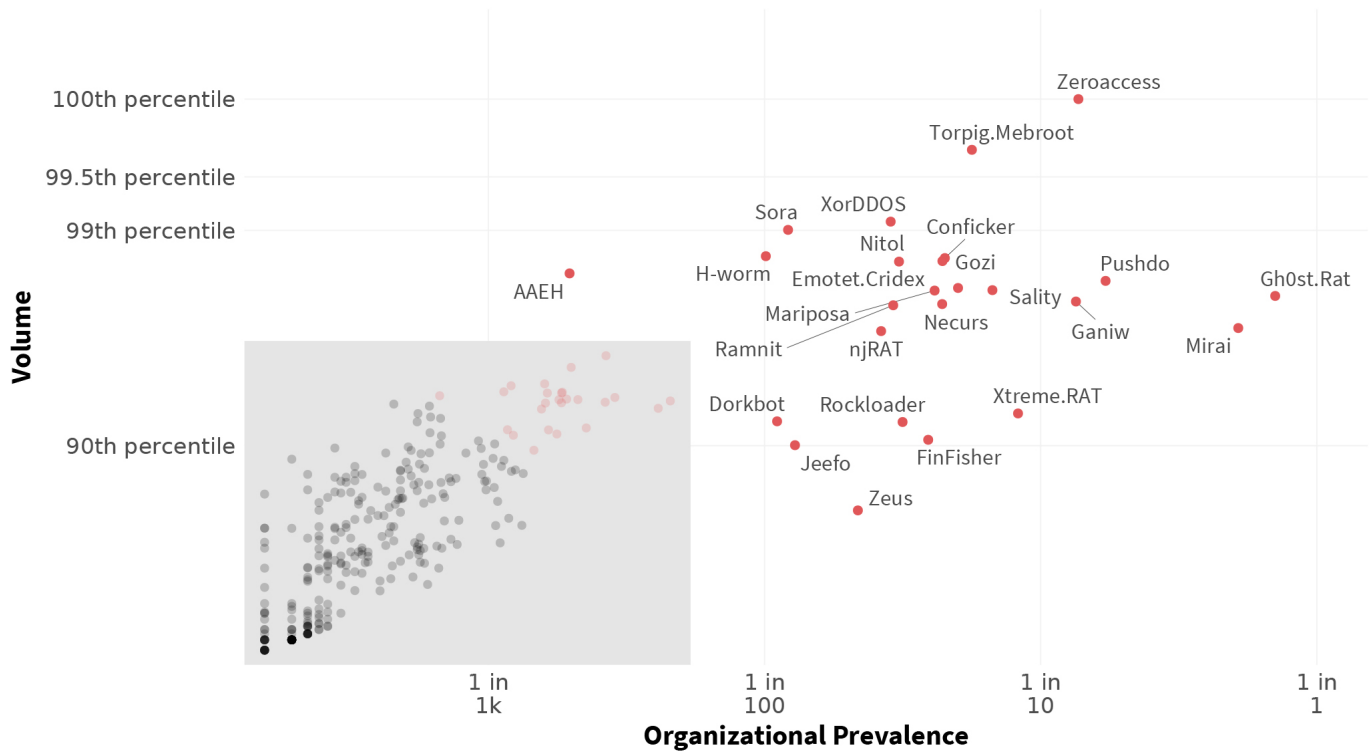


Figure 4: Top 25 botnet detections in Q4 2019 by global prevalence and volume.

While botnets and malware are intricately related (malware infections being the seed from which a botnet grows), their life expectancy is very different. Malware is made to change, resulting in a constant emergence of slightly modified variants to evade detection or add features. Botnets, on the other hand, are made to survive and adapt. Taking down botnets is often like fighting the proverbial hydra—chop off a control node and another rises to take over. Manage to knock out all the controllers and you’re still left with an army of infected hosts trying to call home.

The ZeroAccess botnet offers a good example. It’s pretty remarkable that a botnet born in mid-2011 continues to register the highest volume (though not the highest prevalence) across our sensors. Once it takes root on a system, it uses the host to download additional malware, mine cryptocurrency, engage in click fraud, and other sundry schemes at the behest of criminals running or renting it at the time. And due to rootkit techniques enabling it to remain hidden on infected systems, it can carry out these functions for a long, long time. Gh0st RAT, Mirai, and the rest of the botnet leaderboard all have similar stories.

To our mind, the real story here, however, is more about hygiene than hype. We’d love to fill these pages with cutting-edge analysis of brand-new, sophisticated botnets, but the reality is that out-of-date systems running unpatched hardware/software on inadequately monitored, flat networks are the larger threat to internet security. That might be the same ‘ol story, but until those things change, the story depicted in Figure 4 won’t change either.

Featured Q4 Updates

A WIFICAM Whodunit

The Wireless IP Camera or WIFICAM is a web camera that is produced and sold in bulk to various buyer companies. These buyers add software and branding to the camera before selling it to the public. Interestingly, the HTTP interface for the cameras is provided by a server based on a heavily modified rendition of the GoAhead web server service. This modification resulted in multiple vulnerabilities unique to WIFICAM as well as various vulnerabilities that GoAhead already suffers from (for example, the Remote Code Execution Vulnerability CVE-2019-5096 and an arbitrary file content disclosure vulnerability).

Although these cameras contain software unique to each seller, the vulnerabilities within WIFICAMs impact all models regardless of the company reselling it. Among these vulnerabilities are vulnerable backdoor accounts (CVE-2017-8224), Apple certificates and private RSA keys (CVE-2017-8222), Authentication bypass (CVE-2017-8225), Authenticated remote code execution, access to the camera streams without authentication (CVE-2017-8223), and a vulnerability within the cCloud functionality these cameras utilize by default (CVE-2017-8821). Around 185,000 of these cameras are known to be vulnerable. Despite these vulnerabilities being well known for more than two years, there is no patch yet available.

In 2018, [Fortinet researchers discovered](#) that Satori, a Mirai-based IoT botnet, had implemented an exploit chain for the explicit purpose of assimilating WIFICAMs and other devices sharing the custom GoAhead server configuration. Previously this exploit chain had been associated with the Persirai botnet where it had been used to great effect to enslave countless similar IP cameras. The continued absence of a patch, the multiple vulnerabilities present for these cameras, as well as the documented efforts of multiple IoT botnets to incorporate these devices all contribute to this exploit having the third-highest volume among all IPS detections in Q4.

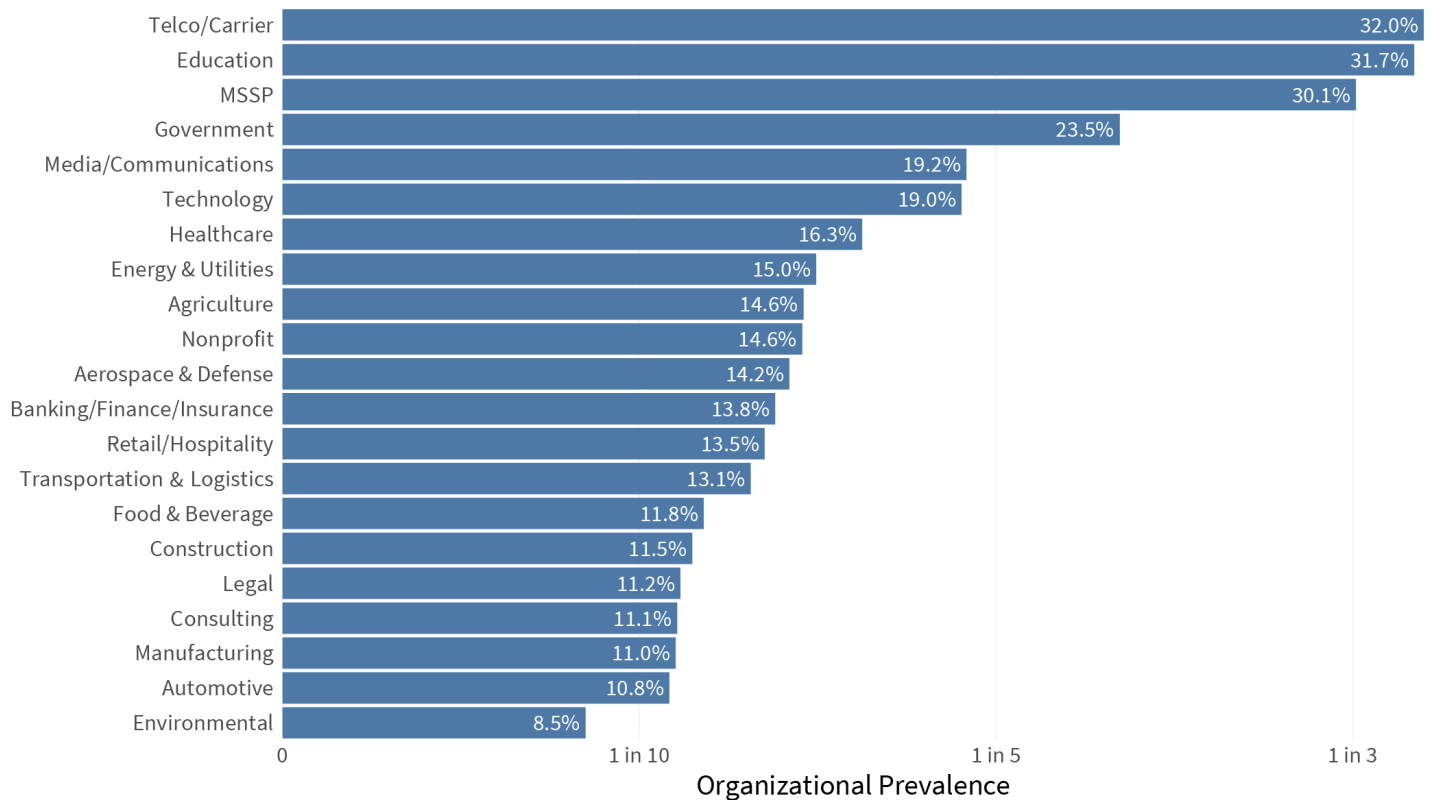


Figure 5: Prevalence of WIFICAM exploit detections across industries.

Looking at the profile of companies reporting exploit activity targeting WIFICAM vulnerabilities adds another layer of intrigue to this story. While certainly not definitive proof, the top five industries depicted in Figure 5 do fit the pattern one might expect from an espionage campaign. Then again, widespread infections of consumer devices on telco and university networks also fit the classic pattern for building a large botnet.

Whatever's going on, it spotlights the difficulties of supply chain security. Is something nefarious occurring here or is this simply one more example of unintended consequences of buggy third-party code development/reuse? The sad truth is that for the vast majority of products, most end-users simply can't know for certain.

Latest Stresses for CMS

In Q4, attackers targeted vulnerabilities in CMS more so than almost any other platform or technology. A flaw in one of these platforms, vBulletin, was especially noteworthy for how widely it was targeted for exploit activity. vBulletin is an extremely popular forum management platform that organizations like Sony, Zynga, EA, and tens of thousands of others use for managing online comments and building community websites.

When an anonymous security researcher last September disclosed an unauthenticated remote code execution flaw in versions 5.0.0 through 5.5.4 of the software—along with Google Dorks for finding vulnerable systems—attempts to exploit the issue were swift and widespread. Numerous vendors reported efforts to exploit the flaw just hours after it was disclosed and before vBulletin had a patch for it. The prevalence of vBulletin detections in Q4 was high across the board. In countries with good sensor coverage, we detected vBulletin-related activity in one-third or more firms. In some regions it even approached as many as two-thirds of all organizations.

vBulletin released a patch for the flaw (CVE-2019-16759) two days after it was disclosed last September. But the ease of exploitation and the severity of the vulnerability made it one of the biggest threats we encountered in Q4. Once exploited, the flaw allows attackers to take control of the host system and use their access to drop malware, install backdoors, execute shell commands, and to try and move laterally within the network. The exploits that are publicly available allow even attackers with relatively low-level skills to take complete control of hosts running vulnerable versions of vBulletin. Organizations that have not yet secured their vBulletin platform run the very real risk of giving attackers a foothold on their network.

Organizational Prevalence (countries with more than 10 customers)

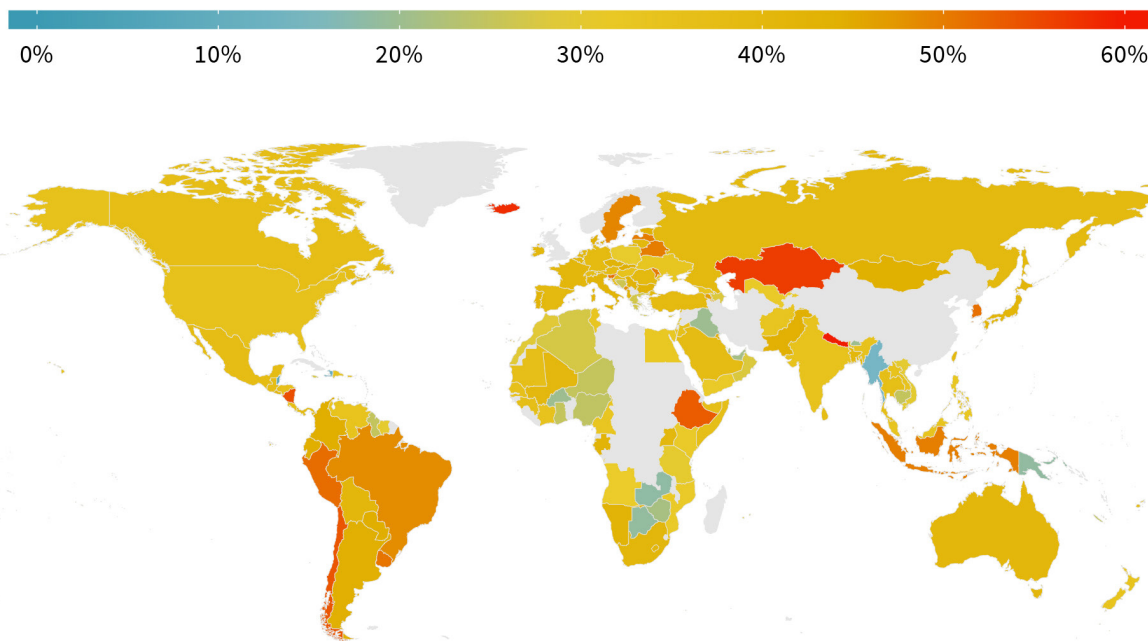


Figure 6: Global prevalence of vBulletin exploit detections.

Speaking of CMS-related threats, we'll also mention another WordPress vulnerability that resurfaced in Q4, this time in the form of an arbitrary file upload vulnerability (CVE-2012-3574) from several years ago. The vulnerability, in the MM Forms Community plugin versions 2.2.5 and 2.2.6, results from insufficient sanitization and verification of files uploaded to the platform. It allows for unauthenticated attackers to execute arbitrary code on systems running vulnerable versions of the software. We observed increased activity for the signature in Q4 2019 with most of it coming from Belarus and Spain—another reminder that old vulnerabilities and exploits never really die.

The WordPress vulnerability is another example of website operators being put at risk by vulnerable WordPress plugins. Recent months have witnessed the emergence of similar vulnerabilities in WordPress plugins. Examples include authentication bypass bugs reported in January in WordPress plugins InfiniteWP Client and WP Time Capsule, another in November in the Jetpack WP plugin: one reported in October 2019 in the Rich Reviews plugin and bugs disclosed last August in multiple NicDark plugins including Components For WP, ND-Bakery Page Builder, ND-Donations, ND-Booking, ND-Travel Management, ND-Learning Courses, etc.

The big-picture message here is that while CMS might make building and managing websites easy, they don't make managing website security any easier. That takes sustained vigilance and work.

Start Spreadin' the Blues

In the constant pressure to keep ahead of new threats, organizations can sometimes forget that older exploits and vulnerabilities really have no expiration date. Threat actors will continue to use them as long as they work. A case in point is EternalBlue, an NSA-developed exploit (CVE-2017-0144) targeting Microsoft's implementation of the SMB protocol. A group calling itself the Shadow Brokers leaked the exploit in 2017. Since then EternalBlue has been used in numerous campaigns including, most notably, the WannaCry and NotPetya ransomware attacks of 2017. The malware has been adapted to exploit common and/or major vulnerabilities. These include the adoption of SMB and SQL brute-force attacks, a Windows RDP flaw (CVE-2019-0708), and also an LNK file vulnerability (CVE-2017-8464).

In a potentially dangerous development, last quarter the EternalBlue Downloader Trojan gained the ability to exploit BlueKeep, a critical vulnerability in Microsoft's Remote Desktop Protocol (RDP). If a victim device is determined to be vulnerable to BlueKeep, the downloader will report back to a C2 server, which then provides the necessary tools to carry out the attack.

For those needing a refresher, BlueKeep (CVE-2019-0708) is a remote code execution vulnerability that impacts all Windows versions. The flaw, disclosed last May, allows an unauthenticated user to connect to a vulnerable system over RDP and execute arbitrary code on it. Microsoft, the NSA, and numerous others have warned of the flaw being "wormable," allowing malware to spread like wildfire in the same manner as WannaCry and NotPetya.

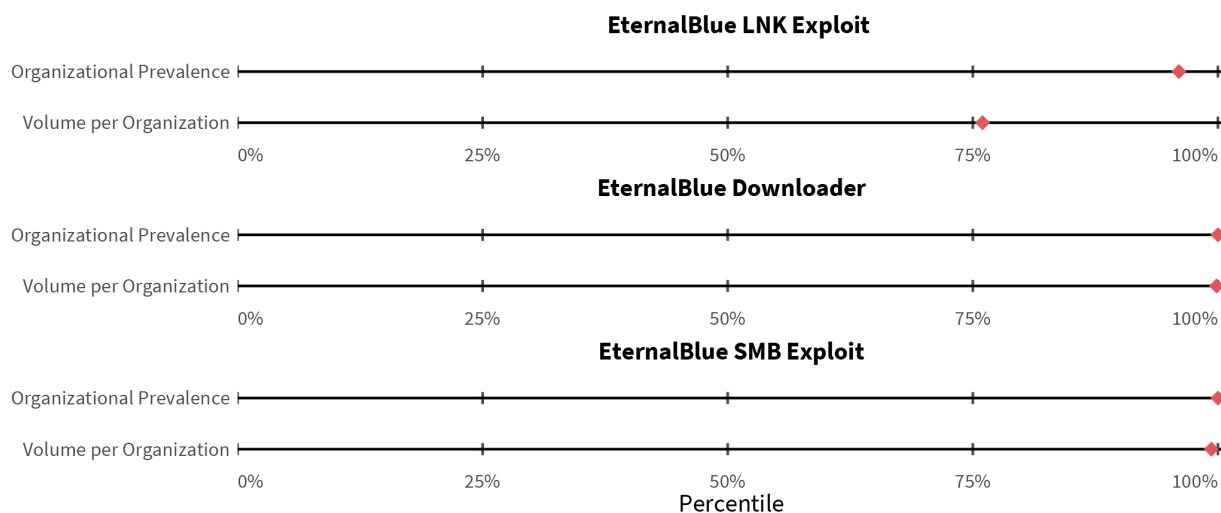


Figure 7: Ranking of prevalence and volume of detections for EternalBlue downloader and EternalBlue exploits (CVE-2017-0144 and CVE-2017-8464).

So far the simmering concerns about a BlueKeep-enabled malware pandemic have not quite borne out, although exploits for the flaw have now been available for several months. Besides a coin miner campaign last November, there have been few reports of attacks involving BlueKeep. However, that is little reason for complacency. A relatively high number of internet-accessible Windows systems remain unpatched and vulnerable to BlueKeep exploits. The recent addition of BlueKeep to the EternalBlue Downloader Trojan is another complicating factor. As with BlueKeep, hundreds of thousands of systems are believed to be still vulnerable to the EternalBlue exploit, although it's been more than two years since a patch for it became available.

Detections of the EternalBlue downloader (detected as JS/Kryptik.Q!tr) are fairly low-level at this time. Though, relatively speaking, it's still in the top 2% of IPS detections by prevalence. And the volume of BlueKeep detections within those organizations is pretty high, raising the possibility that cyber criminals are attempting to use BlueKeep in targeted attacks. The continuing—and evolving—threat actor interest in EternalBlue and BlueKeep is a reminder for organizations to ensure their systems are properly patched and secured against both threats.

The Death of Ransomware

There's really nothing remotely funny about ransomware these days, especially one that's named "DeathRansom." But when we first spotted the malware in the wild in Q4, the first thing that struck us was the fact that DeathRansom did a lot of things—except really encrypt file content. We discovered that victims only had to rename their files to restore their systems. This prompted some to initially consider DeathRansom to be something of a joke. Not anymore.

A new version of DeathRansom that Fortinet discovered in the wild is fully capable of encrypting files on target systems. The variant uses a combination of Curve25519 algorithm for the Elliptic Curve Diffie-Hellman (ECDH) key exchange scheme, Salsa20, RSA-2048, AES-256 ECB, and a block XOR algorithm for its encryption scheme. Our analysis leads us to strongly believe that there is a significant connection between DeathRansom and scat01, the operator of Vidar, an information-stealing malware campaign. We have spotted activity related to DeathRansom in a small handful of organizations across seven countries—Japan, Turkey, the U.K., Italy, Germany, Taiwan, and France. Overall though, detections for the malware so far have been very low-level.

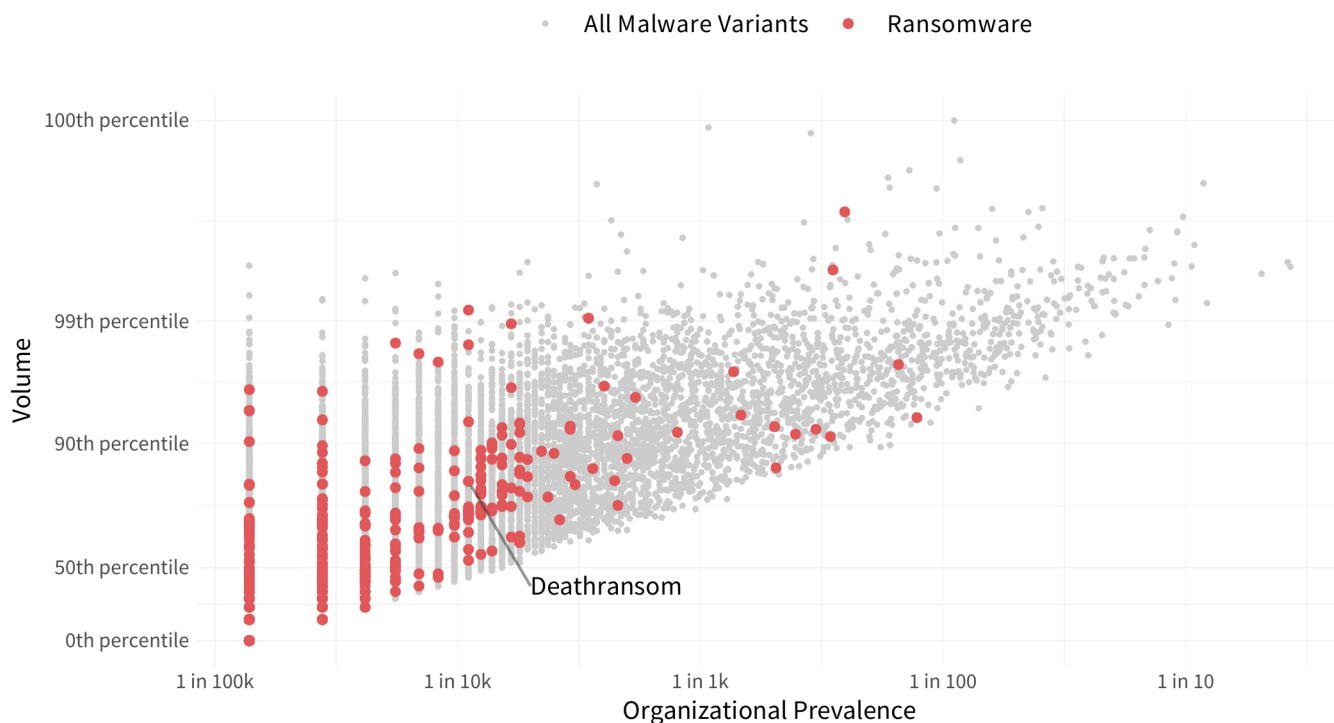


Figure 8: Prevalence and volume of ransomware strains in Q4 (in red) relative to all malware variants (gray).

This is not to say, however, that it will necessarily remain that way forever. One thing that threat actors have shown recently is that they have no intentions of letting up on ransomware attacks against business organizations. When we look at all malware variants and plot them by prevalence and volume, it is clear that ransomware isn't the most common form of malware. Overall, ransomware volumes have dropped significantly compared to two years ago. But that's mainly because attackers have switched from mass-volume spray-and-pray attacks to large-scale, targeted attacks on businesses. Another factor contributing to the growing attacks on businesses and enterprise organizations is the ready availability of Ransomware-as-a-Service (RaaS) offerings these days. Prolific ransomware variants such as Sodinokibi, Nemty, and GandCrab were all distributed via a RaaS model.

The FBI in October warned of a sharp increase in ransomware attacks targeting organizations in multiple sectors—especially state and local governments, healthcare organizations, transportation companies, and the industrial sector. The alert warned of attackers using email phishing campaigns, Remote Desktop Protocol vulnerabilities, and software vulnerabilities to infect corporate systems. Security researchers have also noted a recent increase in multiphased attacks, where threat actors first infiltrate an organization, scope it thoroughly for high-value systems, and only then deploy ransomware. The goal is to exert maximum pressure on organizations by encrypting core business and operational systems and all data backups as well. Hospitals and government agencies that have been impacted by ransomware attacks in recent months have spent days and even weeks recovering from them.

Ransomware has inflicted tens of billions of dollars in losses to organizations across sectors and poses arguably one of the biggest threats this year, especially for those that have not implemented a robust data backup and recovery program.

A Not So Charming Kitten

In Q4, Fortinet observed significant levels of activity across regions associated with Charming Kitten, an Iran-linked advanced persistent threat (APT) group with decidedly more sinister motives than its name might suggest.

Charming Kitten, like most APTs of its ilk, goes by a handful of other names including Phosphorus, APT35, and Ajax Security Team. The threat actor has been active since around 2014 and has been associated with numerous cyberespionage campaigns. Most recently though, it has been linked to a series of attacks on targeted email accounts associated with a U.S. presidential reelection campaign. Charming Kitten's intended targets have included government officials, journalists covering global politics, and prominent Iranian expats. The recent activity suggests that the Iranian threat actor has expanded into the election-disruption business—something incidentally that we expect to see more of from other groups this year as well.

In Q4, Charming Kitten was observed employing four new tactics against intended victims that were all designed to trick victims into parting with sensitive information:

- It began trying to collect Google credentials of targeted victims by using a phishing email that lured them to follow a link to Google Sites and download a malicious file.
- The group began sending SMS messages to targets with a fake alert about their email account security and urging them to click on a malicious link to verify their identities.
- The third tactic, once again, was a false alert, this time about a North Korean attack group purportedly compromising the target's account and urging recipients to click on a malicious link to secure their supposedly compromised account.
- The fourth new gambit involved the attackers impersonating account security teams at Facebook, Instagram, and other social networks to try and extract authentication credentials from the targeted victim.

It's worth noting here that with the Summer Olympics and the U.S. presidential campaign nearly upon us, there is a strong likelihood

Total attempted connections to Charming Kitten IOCs

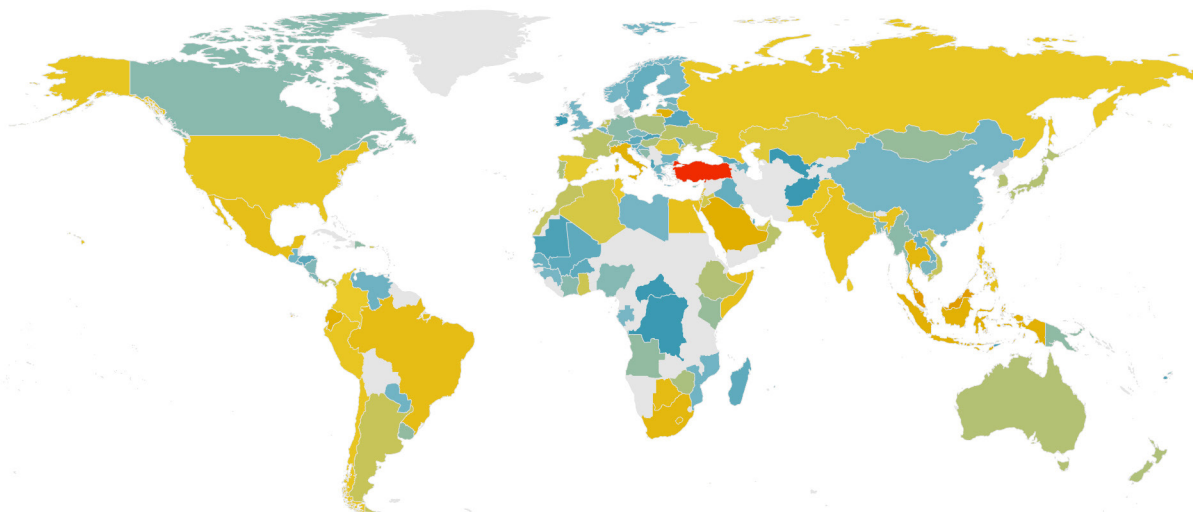


Figure 9: Global distribution of IOCs associated with Charming Kitten (aka APT35).

of more such campaigns from Charming Kitten and others, especially Russia-linked groups. Last October, Microsoft warned about a campaign by Russia’s notorious Fancy Bear/APT28 that targeted some 16 international sporting organizations and anti-doping organizations in countries across three continents. In previous attacks in 2016 and again in 2018, Fancy Bear is believed to have obtained and publicly leaked medical records and other data from anti-doping agencies. Even enterprise organizations that are not necessarily being targeted in these campaigns can become victims of collateral damage. For example, an attack designed to bring down a voter registration site or an anti-doping organization could disrupt services for everyone else that might be with the same ISP.

Another concern that security experts have expressed is the potential for false flag attacks, where threat actors aligned with one nation-state try to pin the blame for an attack on another actor to seed further confusion and mistrust. In Q4, National Cyber Security Centre (NCSC) and the U.S. National Security Agency (NSA) published a joint advisory describing how Russia-linked Turla Group has been systematically conducting attacks on targets in 35 countries using infrastructure belonging to Iran’s APT34 (aka Crambus/OilRig).

Exploratory Analysis: Who’s Spamming Whom?

This edition of our exploratory analysis section—in which we start with no agenda and see where the data leads—draws from our deployment of FortiMail email gateways. Spam is as old as email yet remains a big challenge for organizations and individuals alike. While most spam is just a nuisance, it’s also a conduit for malicious activity that must be taken seriously.

Spam analysis often takes the perspective of the recipient, but we were interested in studying the bidirectional flow of spam between nations. The visualization below traces country-to-country traffic flows collected by the FortiMail system. Countries are arranged in regional groupings with the size of each node corresponding to total spam volume registered for that country. The intensity of connecting lines traces traffic between countries, with deep red indicating the most voluminous flows.

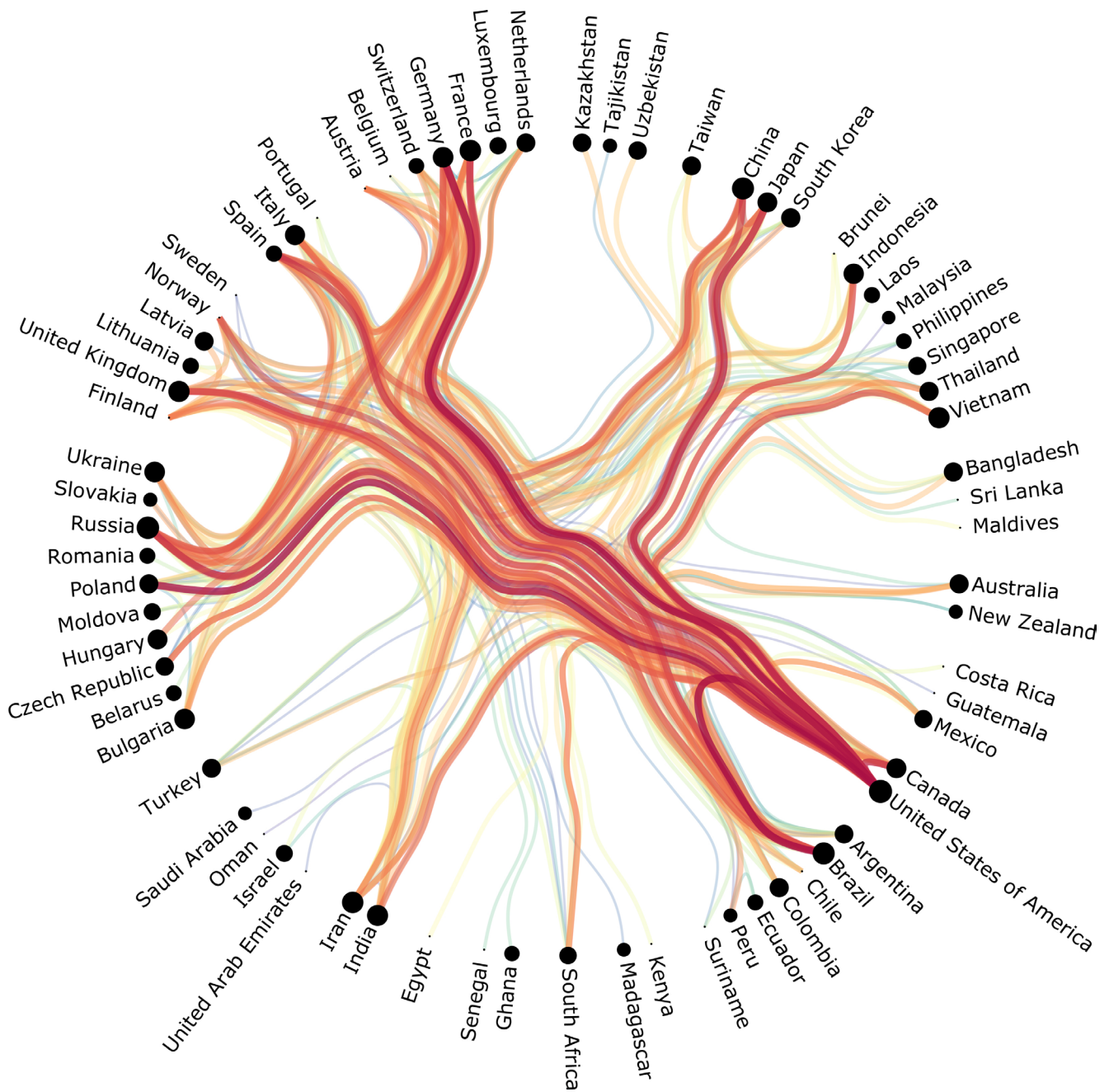


Figure 10: Volume of spam traffic flows between countries.

It's admittedly difficult to impossible to trace all the individual streams of spam in Figure 10, but that's not really the point of this particular visualization. Rather, it's meant to highlight broad patterns and flows. For instance, the heaviest "spam trade partners" of the United States include Poland, Russia, Germany, Japan, and Brazil.

With respect to trade partners, you might be wondering which countries or regions are net exporters vs. importers of spam. That aspect was difficult to integrate into Figure 10 without getting really messy, but Figure 11 has that covered. We've collapsed countries into larger regions here to conserve space and simplify the message.

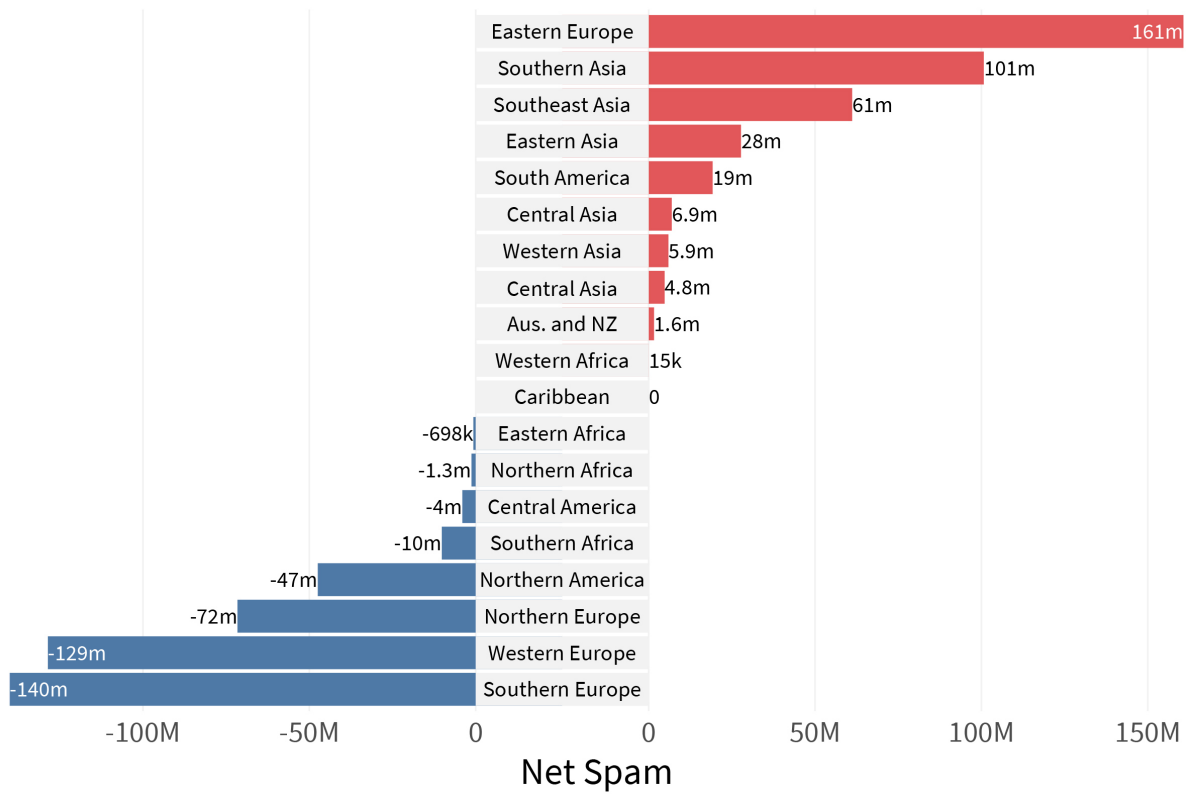


Figure 11: Net spam volume exported from world regions (total out – total in).

And that message is quite clear, outing Eastern Europe as the largest net producer of spam in the world (besides Hormel, of course). Most of the outbound-heavy spammers beyond that hail from Asian sub-regions. On the other side of the chart, the remaining European sub-regions lead those with net negative spam ratios (receive more than they send), followed by the Americas and Africa.

Speaking of Africa, we feel obliged to right a long-standing wrong. Nigeria (in Western Africa) is virtually synonymous on the internet with so-called 419 or “Nigerian Prince” scams. Based on this data, we probably owe the Nigerian Prince an apology. His region gets spammed just about as much as it spams others. Stereotypes thrive in ignorance, so let’s hope this data helps overcome that challenge! In fact, we hope all the data we’ve shared in this report helps you overcome many challenges of the current cyber-threat landscape.

Reference

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



www.fortinet.com

Copyright © 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.