FORTINET

QUARTERLY Threat Landscape Report

Q4 2018

Table of Contents

Q4 2018 **Introduction and Key Findings**

The fourth quarter. For some, it signifies a mad rush to make annual sales targets. For others, it's a time to step back from the madness and spend some time with family and friends. Still others carry on as usual, unswayed by the changing of the seasons or years.

What about cyber-threat actors? According to the Fortinet Threat Landscape Index, nefarious activity across the internet subsided toward the end of the year. At the same time, the Index hit an all-time high during Q4, indicative of the constant ebbs and flows of cyber-threat activity.

What were the major drivers of those movements in Q4? Below, you'll see a summary of statistics culled from billions of threat events observed by Fortinet devices in live production environments around the world. The rest of the report digs into and adds context around those key findings.

Q4 2018 by the Numbers:

Exploits

- Exploit Index declined slightly (-0.3%)
- 8,309 unique exploits detected (+5%)
- 1,218 exploits detected per firm (+10%)
- 54% saw severe exploits (-11%)
- IoT exploit prevalence fell 5%
- 15 zero days found by FortiGuard Labs

Malware

- Malware Index fell 4.3%
- 33,653 unique variants (-1.5%)
- 6,405 different families (0%)
- 13.7 variants per firm (+0.5%)
- 6 variants spread to ≥10% of firms
- 18% saw cryptojacking malware (-1%)

Botnets

- Botnet Index fell 1.5%
- 261 unique botnets detected (+2%)
- 11.69 infection days per firm (+15%)
- 555 average volume per day/firm (+7%)
- 3% of firms saw ≥10 bots (0%)
- 4.3% of infections last >1 week (0%)

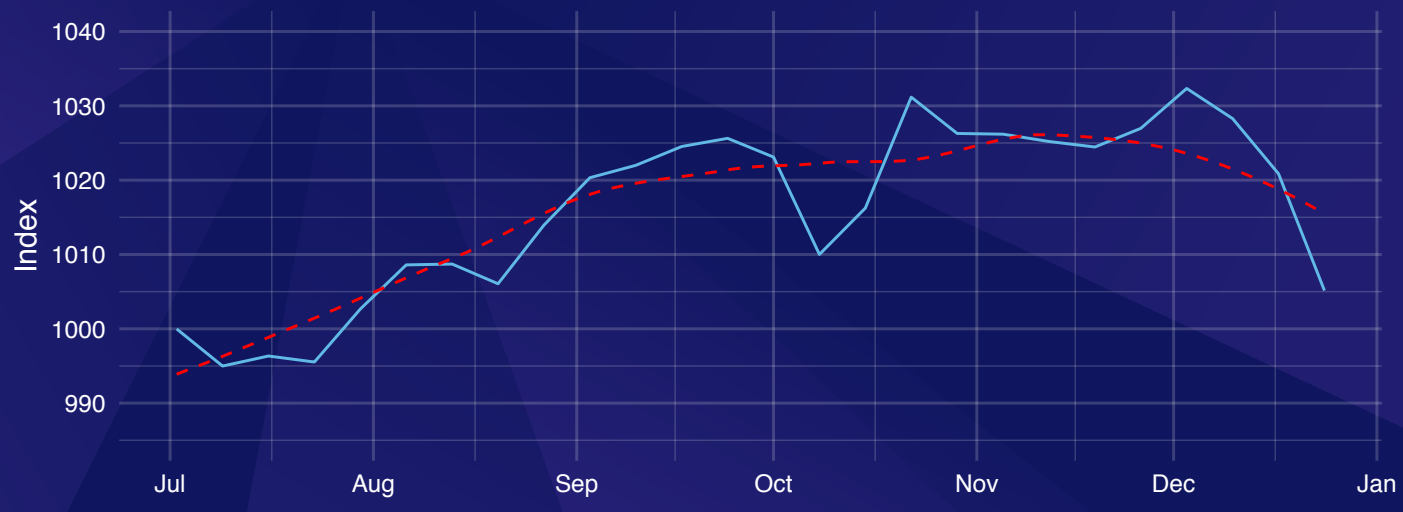


Figure 1: Fortinet Threat Landscape Index (Overall)

Share your thoughts with us and others along the way on Twitter, Facebook, and LinkedIn. Connect with our FortiGuard Labs team at @FortiGuardLabs or with the hashtag #FortiResearch. You can also find us at @Fortinet and @FortinetPartner for the latest business and cybersecurity insights.

Highlights from the Headlines in Q4 2018

This report primarily analyzes threat data from millions of Fortinet devices across the internet. But what's happening in the dataset is at least somewhat related to what is happening in the headlines. Here are some of those stories we tracked in Q4 2018:

October 6

Iceland hit with what officials claim is the country's largest cyberattack ever. A very elaborate phishing campaign mimicking the police service targeted citizens.

October 8

News emerges about the first of two bugs in the Google+ API that together affected 50M+ users and sped up its shutdown timetable. It kicked off a rough quarter for social platforms.

October 24

Cathay Pacific Airways announced that a hacker stole the personal and payment details of almost 10M passengers. It is the largest data breach reported by an airliner.

November 12

For two hours, traffic destined for Google's Cloud Platform was routed to Russia and China instead. All reports point to a goof rather than a coup, but the incident is yet another reminder of the internet's fragility.

November 28

The U.S. Department of Justice indicts two Iranians for perpetrating the destructive ransomware attacks against the city of Atlanta in 2018 and Hollywood Presbyterian Hospital in 2016.

November 30

Marriott discloses a massive data breach affecting 500M guests of various Starwood properties. It is the largest data breach reported by a hotel and the second largest ever.

December 13

Italian oil and gas company, Saipem, was hit by a new version of the Shamoon malware that wiped data from roughly 10% of its systems.

December 14

Capping off a very public year of privacy woes at Facebook, a software bug exposed the private photos of users to third-party app developers without permission.

December 20

IBM and HPE named targets of a Chinese espionage campaign, Cloud Hopper. U.S. and British officials report the aim was to infect the systems of these and other large service providers to access hosted client data.

Exploit Trends

FORTINET

Exploit Trends

Exploit trends reveal what adversaries do to identify and compromise vulnerable systems. Triggering one of the many threats detected this quarter doesn't mean the attack succeeded or even that the vulnerabilities existed in the environment. Because exploit activity tends to be rather noisy, we focus analysis on critical and high-severity detections for this section.

QUICK STATS:

- Exploit Index declined slightly (-0.3%)
- **8,309** unique exploits detected (+5%)
- **1,218** exploits detected per firm (+10%)
- **54%** saw severe exploits (-11%)
- IoT exploit prevalence fell **5%**
- **15** zero days found by FortiGuard Labs

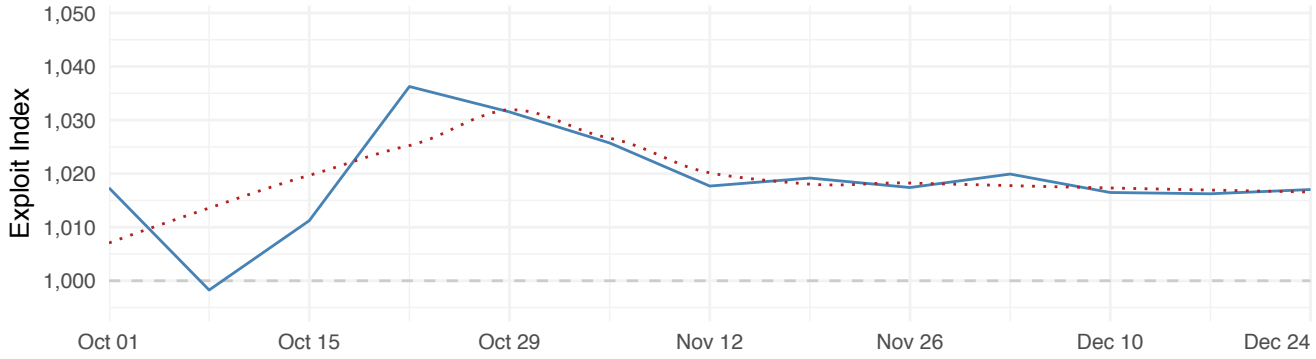


Figure 2: Fortinet Exploit Index for Q4 2018

After a dramatic start to Q4, the Exploit Index settled into a remarkably steady-as-she-goes latter half of the quarter. It ended a scant three points down from where it closed in Q3, but still up from its midyear opening of 1,000. A series of concurrent events conspired to form the peak of 1,036 during the week of October 22, and the primary culprits are called out in Figure 3.

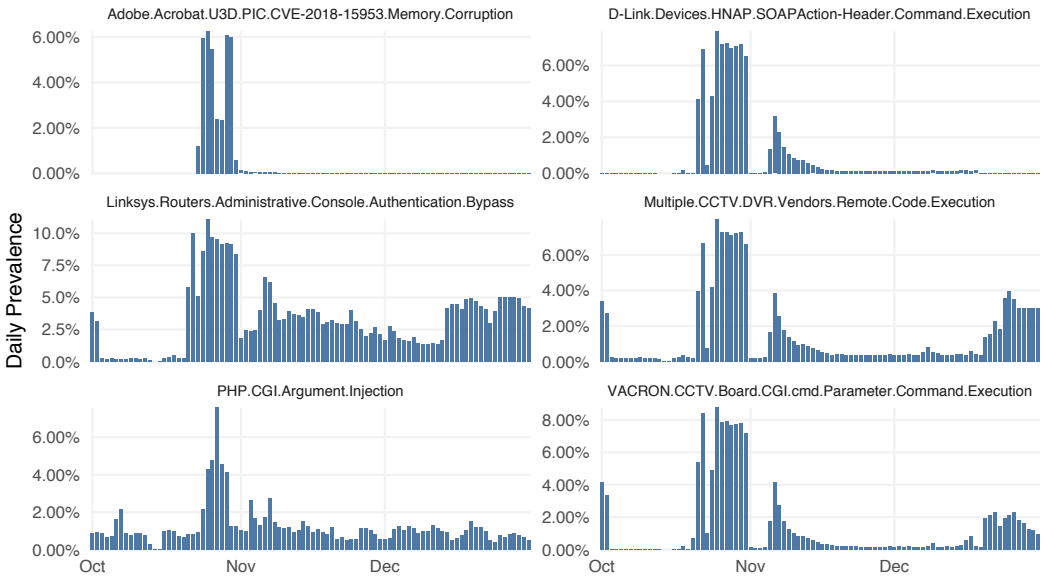


Figure 3: Most Prevalent Exploits During Week of October 22

While a couple exploits break the mold, a common thread readily emerges among the signatures in Figure 3. Four of the six target various types of IoT devices. This focus wasn't limited to a week in October, however, as we will elaborate momentarily.

Widening the scope of analysis to the entire quarter, the 12 exploits with the highest average prevalence across regions are shown in Figure 4. The top of the list is a Who's Who of repeat offenders, and they show little variation across regions.

Demonstrating that the internet never forgets, the Apache Struts exploit (associated with CVE-2017-5638) has been a top detection since its role in the infamous Equifax breach back in 2017. More recently, attackers have been using this exploit as a way to implement cryptojacking functions on compromised machines. The No. 2 exploit in Figure 4 designates an attempt to use a known buffer overflow vulnerability (CVE-2017-7269) in Microsoft IIS. It's been around for a while, but first rose to prominence in the spring of 2018, when it was utilized in mass attacks after the Shadow Broker leaks.

Scanning further down the list finds several exploits related to various types of IoT devices. This is somewhat curious, given that the overall prevalence of IoT detections declined by 5% over the quarter. But the fact that half of the top 12 global exploits in Figure 4 target these devices is a testimony to how widespread and persistent these threats have become. So much so, in fact, that they earned their own time under the spotlight in Figure 5.

	Europe	Northern America	Oceania	Latin America	Africa	Asia	Middle East
Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	29.08%	28.96%	26.28%	28.5%	22.50%	30.2%	25.72%
MS.IIS.WebDAV.PROPFIND.ScStoragePathFromUrl.Buffer.Overflow	25.81%	26.03%	22.91%	25.4%	20.00%	26.2%	22.44%
Avtech.Devices.HTTP.Request.Parsing.Multiple.Vulnerabilities	24.34%	24.47%	21.66%	23.5%	18.98%	25.5%	20.72%
Linksys.Routers.Administrative.Console.Authentication.Bypass	24.06%	23.29%	19.89%	24.4%	16.99%	23.2%	19.85%
D-Link.DSL-2750B.CLI.OS.Command.Injection	23.33%	23.16%	20.44%	21.6%	17.50%	23.2%	19.64%
Oracle.WebLogic.Server.wls-wsat.Component.Code.Injection	23.09%	21.38%	19.77%	21.9%	16.78%	22.9%	19.57%
MS.IE.COM.Object.Instantiation.Buffer.Overflow	23.88%	21.83%	19.83%	20.5%	17.12%	18.5%	20.15%
VACRON.CCTV.Board.CGI.cmd.Parameter.Command.Execution	21.88%	21.23%	18.47%	21.4%	15.05%	21.3%	18.09%
PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	22.16%	20.38%	18.84%	20.3%	14.14%	20.8%	17.81%
Multiple.CCTV.DVR.Vendors.Remote.Code.Execution	20.49%	20.05%	17.54%	19.1%	14.65%	21.2%	16.94%
JAWS.DVR.CCTV.Shell.Unauthenticated.Command.Execution	20.97%	19.95%	17.57%	19.8%	14.51%	20.7%	16.66%
PHP.CGI.Argument.Injection	20.16%	19.98%	17.51%	18.0%	13.58%	21.0%	15.89%

Figure 4. Most Prevalent Exploit Detections By Region

Still on Figure 4 for a moment, the AVTECH signature denotes an exploitation of various vulnerabilities in cameras from that vendor. It reached its highest position ever, having been seen by almost 40% of all sensors on October 12. We previously detailed this exploit's role in the Hide 'N Seek botnet. The signature associated with Linksys routers exploits an authentication bypass vulnerability in those devices, often used to spread the Moon malware. Linksys provides an article detailing steps to help mitigate this vulnerability here. Rounding out the top five, the D-Link signature detects exploitation of an OS command injection vulnerability present in D-Link DSL-2750B routers. There is no known patch for this vulnerability.

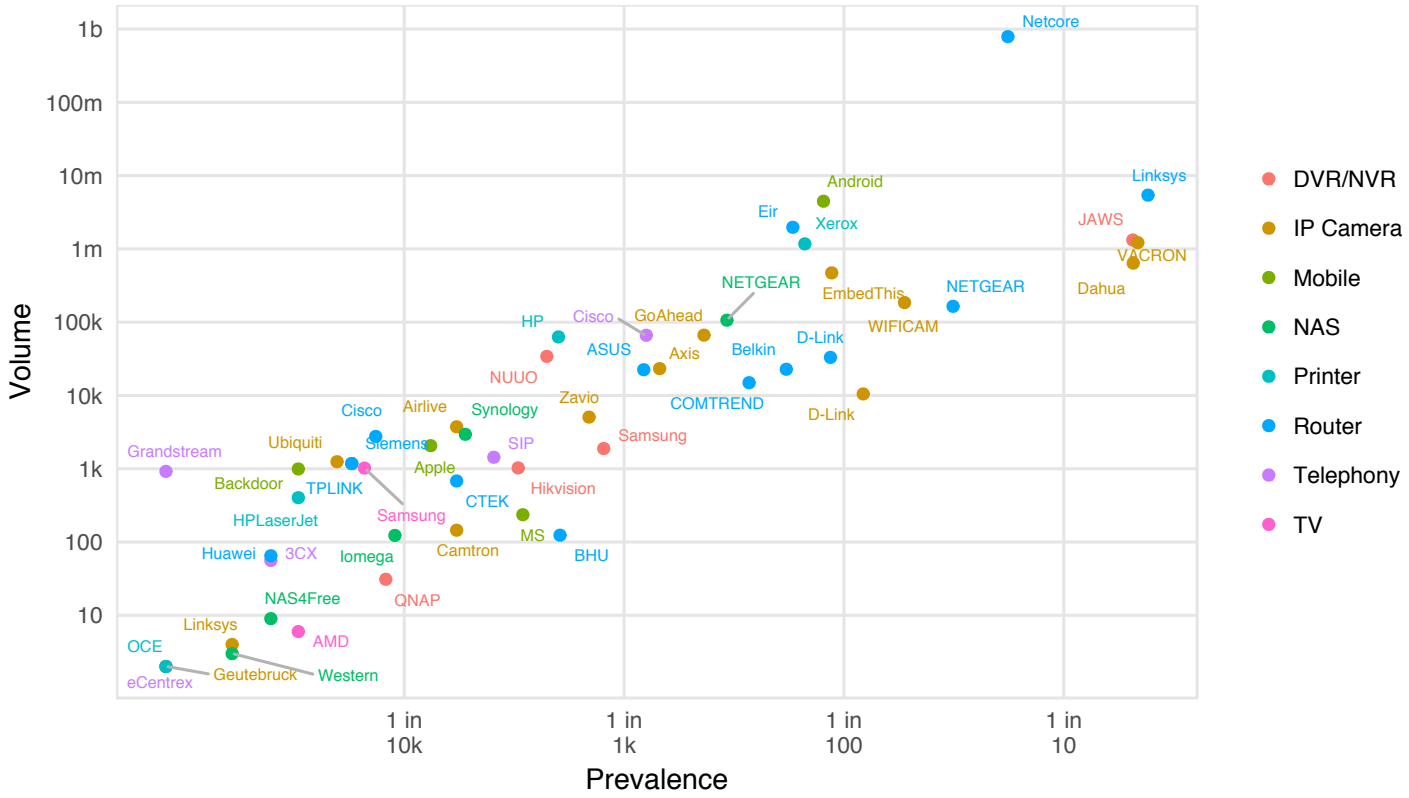


Figure 5: Prevalence and Volume of IoT Exploits By Device Category

OK: now back to Figure 5. Rather than individual detections, this chart focuses only on the prefix of the signature corresponding to the manufacturer of IoT devices. This view makes it very easy to see that exploits against Netcore devices are far and away the most voluminous, whereas Linksys, JAWS, VACRON, and Dahua are detected by the highest proportion of firms. Our main takeaway from Figure 5 is not a list of vendors to avoid, but rather a working assumption that any internet-facing device will be attacked, regardless of who makes it. Implement and operate accordingly.

Given the holiday shopping season, FortiGuard researchers closely monitored exploits against Magento, the second-largest ecommerce platform in the world. We recently discovered a cross-site scripting (XSS) vulnerability in the platform and released detection signatures for this in early October. We saw limited activity for this newer signature, but detected a significant increase in exploitation attempts for an older 2015 remote code execution vulnerability.

Mini-Focus: **Open Source Malware Development**

The open source movement in cybersecurity has been and will continue to be very beneficial to defenders. The ability to share code allows blue teams to test defenses, researchers to analyze exploits, and instructors to use realistic examples when teaching concepts. Many security tools are openly shared as well to help deal with the security problem we all face today. Some good examples of sharing sites for malware that are cropping up on GitHub are:

Windows Open Source Ransomware: This ransomware kit showcases communications over the Tor protocol. In no way are we saying the author has any malicious intent. In fact, without the author's contributions, many security professionals would have a difficult time understanding how ransomware can be simple for malicious actors to create. The proof of concept is detected by many AV programs, but this could still be a starting point for someone with malicious intentions.

Hidden Tear Ransomware: Hidden Tear is a great proof of concept for both ransomware and encryption technologies security professionals can use. The project itself includes a descriptor to unlock all encrypted files. Tools such as these are essential in the learning process for security professionals but are being used by script kiddies to infect victims and demand payment to unlock their files.

Android Backdoor Malware: Android backdoor is a shell script that makes it easy to add a backdoor to any APK file. Obviously there many steps from getting an unsigned application from a malicious attacker to a potential victim, and the tool itself was a proof of concept to showcase Android vulnerabilities.

Retired Malware Remote Admin Trojan—Quasar: It's possible there may be individuals using Quasar RAT as a legitimate administration tool in lieu of commercial paid products. However, we have seen the remote administration tool being deployed in stealth mode, and recently security organizations found the tool was used to distribute malware.

Despite these benefits, there is also a dark or bad side. Because these resources are available to anyone, attackers new and old are using them for nefarious activities, which is contributing to the growth of malware threats.

Some of these freely available malware tools can be weaponized very easily. If a newbie wants to get into cyber crime and hold computers hostage for a ransom, they can use one of the proof-of-concept ransomwares and all they need to do is make a few updates, such as changing the wallet address on where to send the payment, and they are ready to start attacking.

Other more experienced attackers can and will combine the open source code with an evasion tool like the Veil-Framework—which is also open source—to repackage the code in an attempt to circumvent anti-malware. Of course, having this malicious code available for an attacker can give them a head start on modifying and testing new versions with additional capabilities. A great example of this is when the Mirai IoT botnet source code was released in 2016. Since then, we've seen an explosion of variants and related activity.

Malware Trends

FORTINET

Malware Trends

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.

QUICK STATS:

- Malware Index fell **4.3%**
- **33,653** unique variants (-1.5%)
- **6,405** different families (0%)
- **13.7** variants per firm (+0.5%)
- **6** variants spread to ≥10% of firms
- **18%** saw cryptojacking malware (-1%)

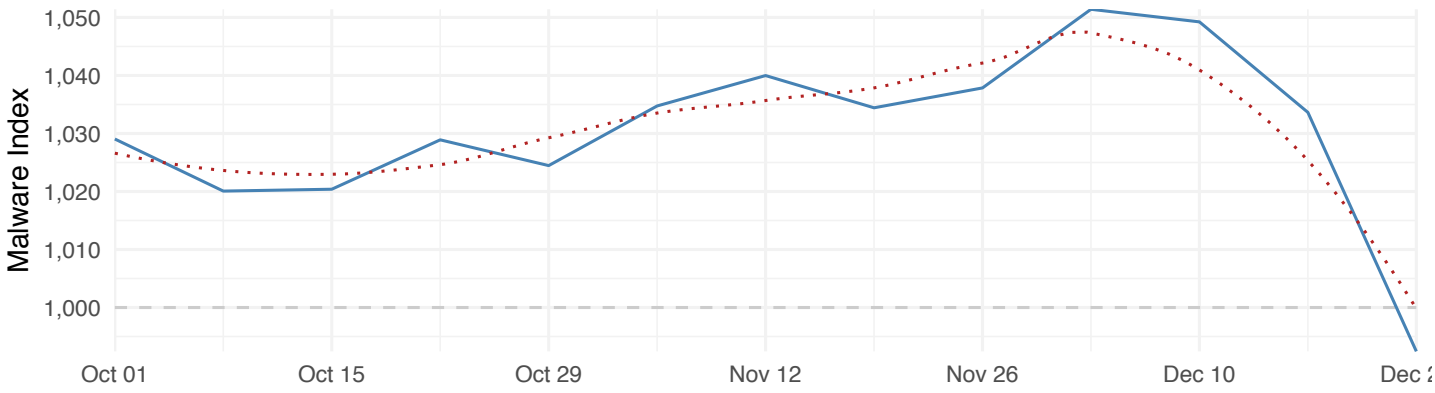


Figure 6: Fortinet Malware Index for Q4 2018

The Malware Index for Q4 serves as a good illustration of why we made the overall Threat Landscape Index a composite score. This allows us to view the behavior of these different types of threats independently. With respect to malware, that behavior is very distinct from what we observed previously for exploits. It dives off in mid-December and is the only one of the three subindices that closed out the year below its starting point of 1,000.

What's behind that downturn in malware? Well, oddly enough, you are. Well, not "you" in particular, but "you" as a representative of people working in firms around the world who relish time away from the office to be with friends and family during the end-of-year holidays. It may seem strange that corporate vacations would have an effect on malware prevalence, but think about it this way: with fewer employees around to click on harmful attachments, visit fraudulent websites, and download malicious files, what would you expect to happen? Keep in mind as well that even cyber criminals enjoy some R&R during the holidays.

Data from our web filtering team corroborates this explanation. Figure 7 charts the web filtering volume for the quarter by category. The trend is somewhat visually dampened by the use of a log scale, but it can be seen that all categories hit lower levels in December.

Let's unpack malware trends further by examining the most prevalent variants across the globe in Q4 2018. Figure 8 gives the relevant statistics. Two generic detections, one for adware and one for the cryptocurrency mining service Coinhive, sit atop the list. The regional differences aren't striking, but it is interesting to note that the highest value roughly doubles the lowest for each of these.

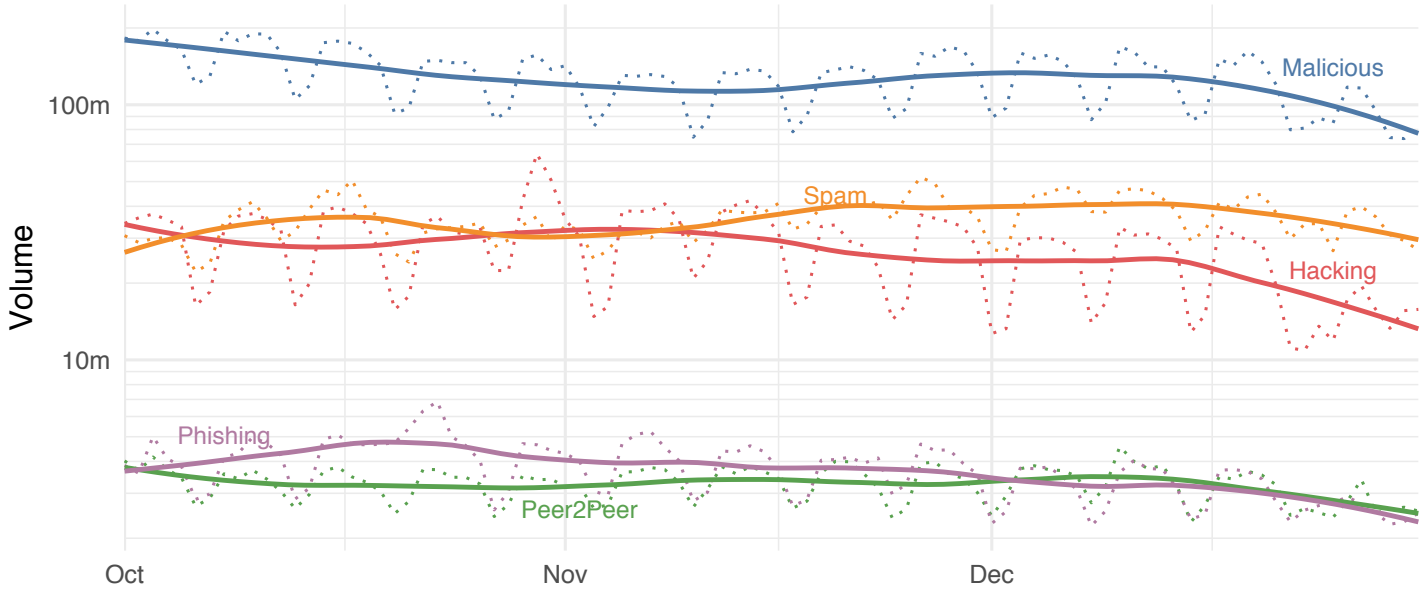


Figure 7: Categories of Websites Detected By Web Filtering Service

Regional variation grows even more apparent beyond the two leading malware detections. They represent a wide variety of functionality, and W32/Agent.AJFK!tr is a case in point. It is a detection for a generic Trojan that has been known to log keystrokes, initiate command-control (C2) functionality, and download/drop additional files.

	Europe	Northern America	Oceania	Latin America	Africa	Asia	Middle East
Adware/Agent	24.5%	27.5%	25.6%	18.3%	18.1%	14.7%	15.1%
Riskware/CoinHive	13.9%	9.5%	14.0%	19.7%	16.5%	14.6%	18.4%
W32/Agent.AJFK!tr	17.2%	5.8%	12.6%	12.6%	15.0%	17.6%	25.3%
Android/Agent.FJ!tr	14.8%	17.7%	20.9%	10.5%	12.9%	7.7%	10.4%
MSOffice/CVE_2017_11882.A!exploit	15.3%	5.3%	11.2%	7.9%	10.4%	14.1%	21.3%
W32/Kryptik.GLZZ!tr	12.5%	3.7%	9.3%	8.6%	10.2%	12.9%	18.1%
W32/Agent.HTL!tr.rkit	9.7%	8.1%	6.6%	7.5%	8.9%	10.8%	10.2%
VBA/Agent.IOV!tr.dldr	10.0%	3.1%	7.1%	5.4%	6.7%	10.4%	12.5%
MSOffice/CVE_2017_11882.B!exploit	10.9%	3.0%	7.0%	4.6%	5.9%	9.5%	13.6%
VBA/Agent.LWI!tr.dldr	10.2%	7.9%	3.6%	16.1%	5.3%	4.9%	5.6%
Riskware/InstallCore_Gen	4.4%	4.5%	3.0%	9.6%	7.9%	7.6%	8.2%
W32/DwnLdr.HQY!tr	6.7%	4.9%	3.9%	7.3%	4.9%	5.3%	6.0%

Figure 8: Most Prevalent Malware Variants By Region

The Android/Agent.FJ!tr variant has ties to FakeSpy, a malware discovered in June 2018. As described in this blog post from early in Q4, FortiGuard Labs encountered malicious traffic to a C2 server in China. The connection was established by a domain that closely resembled one of Japan's well-known express post delivery services. Our analysis showed that the website making the connection is fake and spreading an Android malware. Though the sample code is based on FakeSpy, this particular variant contains new features.

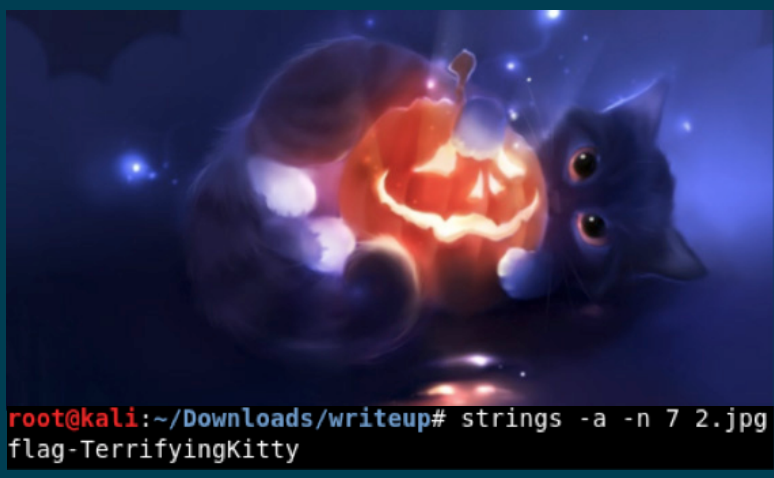
Coming in at No. 5 for the quarter, MSOffice/CVE_2017_11882.A!exploit indicates an exploitation of a remote code execution vulnerability within Microsoft Office. This FortiGuard Encyclopedia entry shows some example screenshots of associated malicious documents, and this blog post details an attack using this malware. It is also one of the many malicious indicators associated with the nation-state threat actor dubbed "Gorgon" that was the focus of a Hot Bulletin we shared with customers earlier this summer based on intelligence shared through our membership in the Cyber Threat Alliance. The B! variant has the same functionality except that it calls out to a malicious domain instead of triggering the exploit used in the A! variant (list of known domains shown in this Encyclopedia entry).

As a reminder that "important" does not necessarily equate to "frequent," we detected activity from malware associated with the GreyEnergy APT group in a mere handful of devices in Poland and Ukraine. The group focuses on stealing of data instead of destruction, allowing it to keep its stealth qualities. Because of its modularity, attacks are able to be fine-tuned depending on the target. It distributes via spear phishing and compromised web servers.

Mini-Focus: **Steganography for Fun and Profit**

As long as communication has existed, humans have wanted to keep those communications secret. Cryptography is the most well known of the ancient clandestine arts, but steganography has a long and storied history as well. Steganography is the technique of hiding something (a message, picture, content, etc.) within something else, often in plain sight.

In the more recent world of cybersecurity, steganography is commonly integrated into Capture the Flag (CTF) competitions. A recent example comes from the 2018 Hacktober.org CTF event, where the flag "TerrifyingKitty" was embedded in the image. If you'd like to see more, the solution write-up for the event is chock full of spooky stego threads.



Steganography can be used for more than fun and games, however. Cyber-threat actors have been known to incorporate this technique into various aspects of their schemes and wares. Examples include the Sundown Exploit Kit and the Vawtrak and Gatak/Stegoloader malware families. Due to its nature, steganography isn't generally used in high-frequency threats, but it's worth noting that the Vawtrak botnet did make our list of "bursty" botnets in Q4 2018 (see Figure 12 in the Botnet Trends section). The chart below showing the daily prevalence of the Vawtrak malware exemplifies this; it never exceeds a dozen firms on any given day.

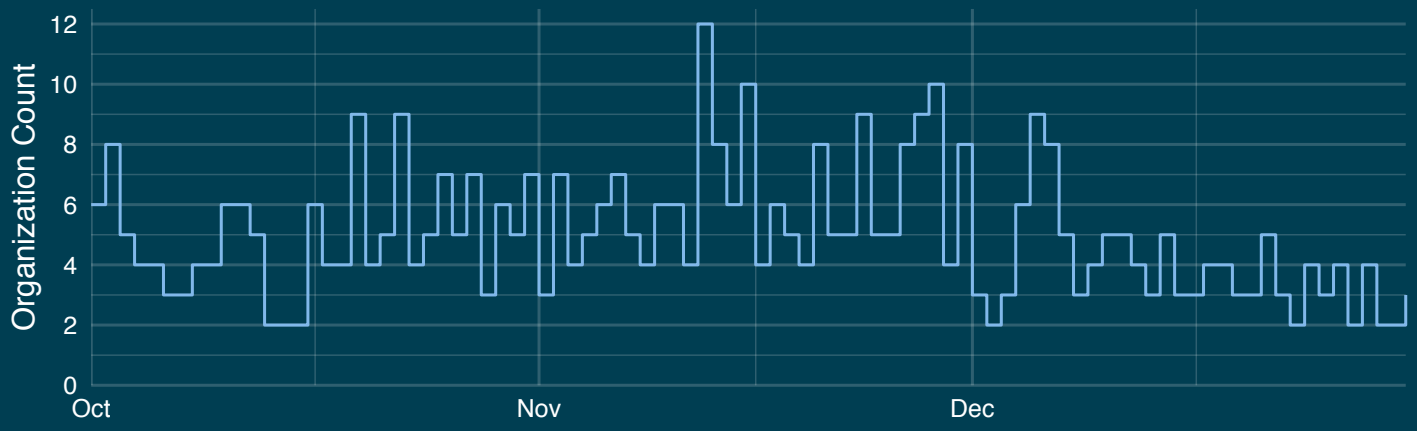


Figure 9: Daily Number of Firms Reporting Vawtrak Malware

During the quarter, external researchers observed malware samples using steganography to conceal malicious payloads in memes passed along on social media. We found the meme twist intriguing, and so FortiGuard Labs did some reversing on the code to see what it was doing under the covers (that's a stego joke, not colloquialism). This and just about every other malware starts by attempting to contact a C2 host, which has been taken down. But that's where it gets interesting. The samples then look for images in the associated Twitter feed, download those images, and look for hidden commands within the images. It does this by searching for image tags with modified values containing commands like /print (screen capture), /processes (write list of running processes), and /docs (write list of files from various locations). Clever, huh?

Botnet Trends

FORTINET

Botnet Trends

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.

QUICK STATS:

- Botnet Index fell **1.5%**
- **261** unique botnets detected (+2%)
- **11.69** infection days per firm (+15%)
- **555** average volume per day/firm (+7%)
- **3%** of firms saw ≥10 bots (0%)
- **59%** of infections last ≤1 day (-1%)
- **4.3%** of infections last >1 week (0%)

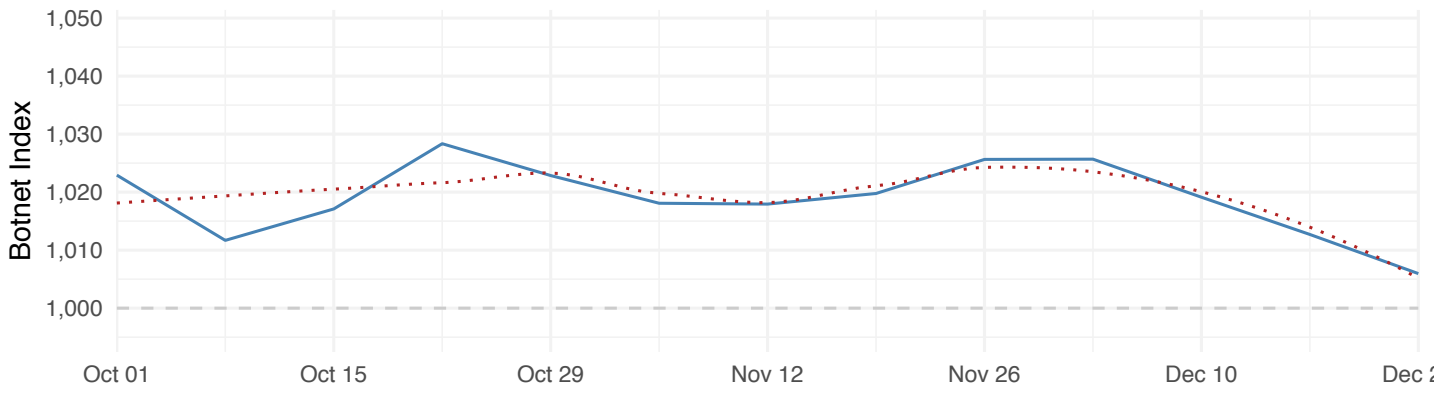


Figure 10: Fortinet Botnet Index for Q4 2018

The Botnet Index for Q4 appears to blend behaviors from the previous two threat categories. The fall and rise in October echoes what we see for exploits, and the December decline mimics that of malware. Overall, it closed 1.5% below where it opened the quarter. We scoured the data for interesting stories behind the (modest) peaks in the Botnet Index, but there wasn't much to tell. Every peak had the exact same botnets in the exact same order by volume of communications: ZeroAccess, Andromeda, H-Worm, Emotet, Conficker. None of these are new, and we (and others) have covered them extensively before, so let's move on.

	Europe	Northern America	Oceania	Latin America	Africa	Asia	Middle East
Gh0st	68.4%	70.4%	78.4%	43.5%	44.2%	43.1%	41.0%
Pushdo	26.7%	32.3%	24.5%	19.5%	16.1%	15.9%	16.7%
Zeroaccess	10.8%	11.9%	9.1%	12.1%	11.4%	12.4%	8.6%
Andromeda	3.6%	2.7%	5.5%	23.5%	30.9%	29.0%	33.1%
Sality	4.0%	5.8%	4.2%	9.6%	15.1%	17.4%	21.4%
Xtreme	7.3%	6.5%	6.0%	8.0%	7.8%	6.9%	6.2%
Necurs	2.9%	3.9%	3.7%	8.7%	11.3%	11.3%	9.1%
Mariposa	4.7%	2.7%	3.7%	10.8%	6.7%	9.5%	6.8%
Conficker	5.2%	1.8%	1.4%	8.8%	9.5%	11.1%	7.2%
CryptoWall	2.2%	3.9%	2.7%	7.2%	14.1%	6.5%	6.5%
FinFisher	3.5%	3.8%	3.8%	5.4%	5.5%	11.5%	4.3%
Torpig	7.1%	5.6%	3.7%	3.3%	3.7%	3.6%	3.9%

Figure 11: Most Prevalent Botnets By Region

Following similar charts in the previous sections, Figure 11 displays a global view of botnet prevalence for the quarter. In it we see another lineup of sinister-sounding threats, with Gh0st chief among them. It was reported by more organizations in every region by a wide margin—even managing to quadruple the runner-up in Oceania. It's far from new, but has a timeless laundry list of useful features, allowing an attacker to take full control of the infected system, log keystrokes, spy on live webcam and microphone feeds, download and upload files, etc.

The stark contrast among regions for the Andromeda botnet is rather shocking at first glance, with the Middle East posting 12X the prevalence of North America. But when you remember that it was the target of a major law enforcement takedown in late 2017, things come into proper perspective. This likely reflects a large number of forgotten and/or neglected hosts in those Andromeda-plagued regions rather than some kind of targeted campaign.

Allow us to offer one final visual perspective on botnet activity in Q4. Last quarter, we introduced a technique to measure the "burstiness" of botnets—sudden activity changes during the quarter that may indicate malicious campaigns. You can read more about the method used in this analysis here if you care to know the details. More extreme bursts are designated by more intense color shading in Figure 12. This highlights that some botnets exhibit a slow burn all quarter (long lighter lines), some appear cyclical (repeating blips), while still others flare up and then die out (longer intense dashes). None of these correlated with major events or noteworthy campaigns, but we do believe this analysis offers a useful way to keep tabs on botnet activity.

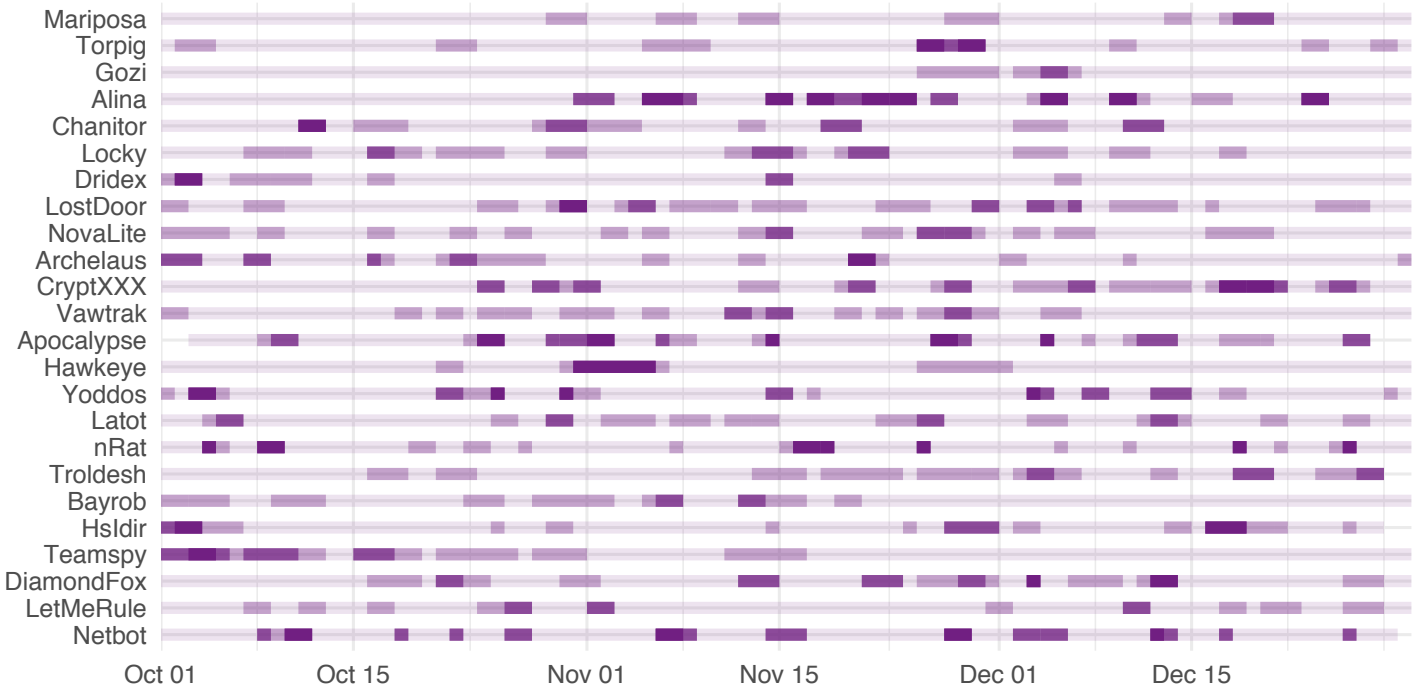


Figure 12: Activity Bursts Among Top Botnets in Q4 2018

A few botnets in Figure 12 are worth a brief mention. We issued a brief to customers in Q3 on Gozi in relation to a variant of the Ursnif banking Trojan borrowing from its codebase. Gozi was mostly quiet and steady this quarter, except for a few sputters in late November and early December.

Alina is a point-of-sale malware that caught our attention last quarter when it showed a similar behavior pattern. We analyzed samples, and they appear largely the same as the original source code leaked years ago. We find no obvious explanation for its newfound vigor, but we will continue to keep tabs on it.

We mentioned the Vawtrak malware in the previous section in connection to threats that use steganography to conceal malicious payloads. The botnet related to that malware shows irregular, mostly mild, bursts throughout the quarter. Insofar as we can determine, this activity does not tie to any particular events.

Hawkeye is another one that may be settling into a pattern. It's had one major burst in about the middle of each of the last two quarters. Hawkeye was used in attacks last year to steal payments that victim companies made to suppliers in a heist that netted nearly $80 million for the criminals behind it. The initial attack is seen as a mass email spray coupled with automated information gathering. These sprays are what appear to be registering in our analysis.

One botnet that did not make it into any charts, but did top our list of "major movers" for the quarter, is TrickBot. From humble beginnings at a volume of 10 (nope; we didn't forget an extra zero or two), it surged to an impressive 3.5M. TrickBot was also the leading gainer on the prevalence scale, crossing the botnet "Mendoza Line" of 1/1,000 firms. It might be an old dog (we published some deep analysis on it back in 2016), but that hasn't kept it from learning some new tricks (you knew we were going there, didn't you). Its new trick comes in the form of a pwgrab module recently added to samples of TrickBot malware we collected. Our analysis reveals the module attempts to steal credentials, autofill data, and history from browsers other applications.

2018 Year in Review

FORTINET

2018 Year in Review

Time is a strange thing and our perception of it stranger still. This becomes especially apparent when reflecting back on key events over longer periods of time, as we often do when heading into a new year. Our industry is quite fond of looking back and predicting forward, possibly due to the public nature of many security failures and our need to prevent them in the future.

Thus, we thought it a fitting addition to this Q4 2018 review to reflect back across the entire year, adding our perspective to that of others in our industry. We've chosen to focus these reflections on several key trends as seen through our global telemetry, which may look a bit different than other annual roundups out there. But hey—you don't read this report just to see us parrot what everyone else is saying, right?

Meltdown and Spectre

Our first stop on the trip down memory lane probably WILL be on everyone else's list, but it can't be helped. Almost as soon as 2018 began, a tandem of side-channel attacks dubbed Meltdown and Spectre were announced that exploit vulnerabilities found in most microprocessors, allowing rogue processes to read kernel memory without authorization. As if that weren't scary enough, more CPU vulnerabilities emerged to haunt us: RizenFall, MasterKey, Fallout, and Chimera.

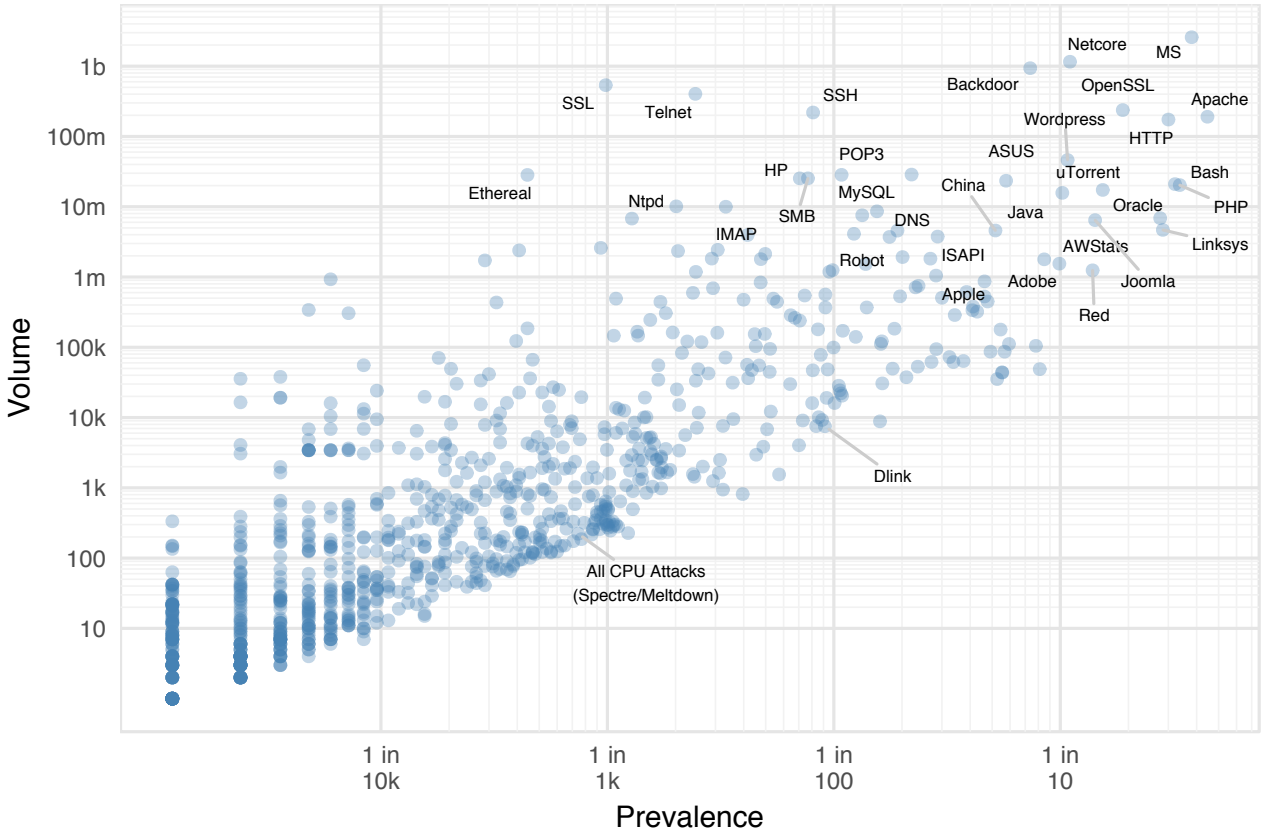


Figure 13: Volume and Prevalence of Exploit Targets Following Release of Spectre and Meltdown Vulnerabilities in Q1 2018

Things that scare us, however, don't necessarily pose the most harm. Such was the case in 2018 with Meltdown, Spectre, and their ilk. The potential for exploitation represented by these attacks is mind-boggling, but most of us are far more likely to fall victim to exploits of a more mundane nature. Figure 13 proves this point well. All of the CPU exploits put together were observed by fewer than 1 in 3,000 organizations, while 1 in 6 detected attacks targeting Apache. We can't afford to turn a blind eye towards the next security "Meltdown" in 2019, but neither can we lose focus on what matters most right now.

Zero-Day Research

At least part of the reason Meltdown and Spectre garnered so much attention was that they caught many by surprise. We don't like surprises in this profession, which is why our experts in FortiGuard Labs spend so much time looking for unknown exploitable vulnerabilities in hardware and software. When they uncover zero-day vulnerabilities, the Labs work together with the product vendor to create protective measures that can be delivered to our customers.

We're proud to say those efforts are paying off. In five short years, we've increased the number of zero days found and responsibly facilitated by our researchers by tenfold. All in all, we've helped keep over 650 vulnerabilities from surprising the community before a fix has been prepared.

You can learn more about FortiGuard's zero-day research here, including a complete list of affected products and a description of vulnerabilities.

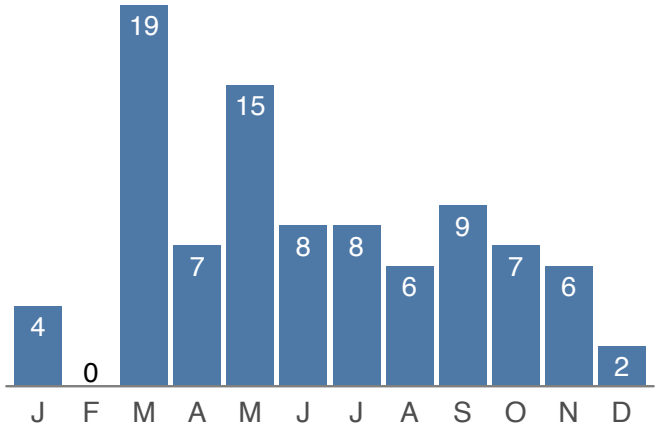


Figure 14: Zero Days Discovered by FortiGuard Labs

Ransomware and Destructive Malware

About a month after Meltdown and Spectre emerged, the world's attention converged on South Korea for the Winter Olympic Games. The spirit of global harmony wouldn't last long, however, when the Olympic Destroyer worm temporarily took down IT systems just before the opening ceremonies. The show went on, but the curtain didn't close on destructive malware in 2018.

March brought spring rains to Atlanta, Georgia, and with it, many pains inflicted by the SamSam ransomware when it disrupted municipal operations. The city spent millions on emergency efforts and the mayor went so far as to call it a "hostage situation."

We'd like to be able to say things settled down after Q1, but alas they did not. You'll find no shortage of examples of the effects of destructive malware over the year, including a hospital in Indiana that was forced to cancel surgeries when its network was seized by ransomware. It may seem odd to learn, then, that the overall prevalence of ransomware in 2018 fell substantially.

It is often said that following the money will find the criminal. As a tool made and used by criminals, malware is no exception. Destructive goals aside, many of the criminals behind major ransomware campaigns in 2018 eagerly embraced another method of monetizing malware—cryptojacking.

Cryptojacking Hit the Jackpot

Even with the aid of Figure 15, it is hard to understate the acceleration of cryptojacking (aka cryptomining) in 2018. Cryptojacking occurs when malware (typically via a script loaded into the web browser) hijacks a computer's resources to mine cryptocurrencies for a remote actor. 2018 will likely go down in the history books of the internet as the cryptojacking Gold Rush.

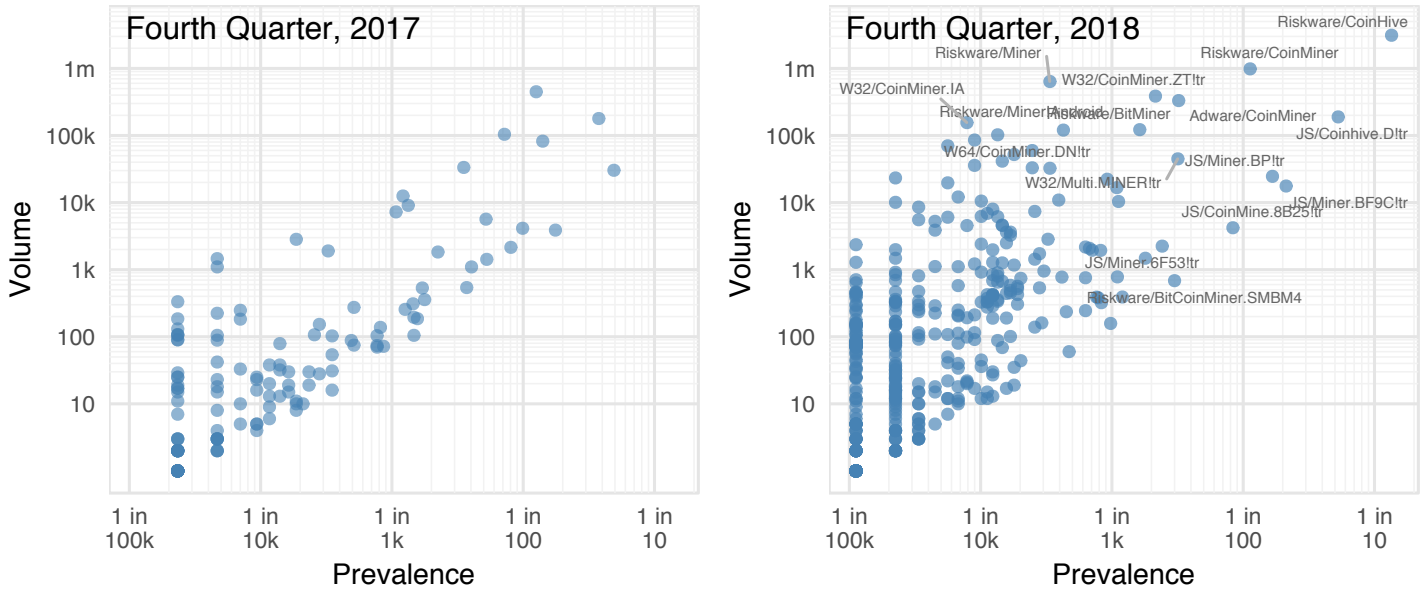


Figure 15: Growth in Cryptojacking Varieties and Prevalence from Q4 2017 to Q4 2018

Similar to the Great American Gold Rush of the late 1800s, a cottage industry seemed to spring up around cryptojacking. Tools of the trade evolved, the targeted platforms grew, new varieties blossomed, and quite a few struck it rich overnight. This led to a measurable explosion of new cryptojacking malware variants and the frequency at which they occur. As can be seen in Figure 15, Coinhive and CoinMiner led the throng of crypto prospectors flooding the market.

But "easy come, easy go," as they say. And in this case "they" appear to be right. Crashing cryptocurrency values later in the year seem to once again be tipping the scales of the cyber-crime economy.

Evolution of IoT Threats

Our Q3 report contained a section detailing the evolution of IoT botnets over the last few years. An important 2018 adaptation for IoT botnets was the ability to implant cryptojacking malware in infected IoT devices. Mining cryptocurrencies requires high CPU resources, and hordes of easily compromised and largely idle IoT devices offer that power through scale. Another development we saw coming was the merging of destructive tendencies with IoT botnets. We saw a bit of this kind of behavior with the Bricker bot. It might not sound terrible at first, but consider all the different types of IoT devices. Sure, it will be pretty bad when your internet-connected coffee maker bricks up, but what about a medical device or a component within the larger infrastructure of a hospital or power plant? Enter VPNFilter.

Intelligence on VPNFilter was shared via the Cyber Threat Alliance. This IoT malware was very similar to the BlackEnergy malware that was used against devices located in Ukraine. The VPNFilter malware targeted a variety of IoT devices, which were also primarily in Ukraine. Once the malware was installed, it could monitor SCADA protocols and steal website credentials. It also had a "kill switch" that would destroy the IoT device. In addition, since the malware on the device was basically monitoring traffic, it had the capability to inject malicious code back into the network session, allowing for crossover infection to an endpoint device. Yikes!

Malware Gets More Agile

Here's one thing we DIDN'T need in 2018—more efficient malware authors and faster release schedules. Yet we got both.

Malware authors have long relied on polymorphism to evade detection, but over time those systems have made improvements that make them more difficult to circumvent. Never ones to rest on their laurels, malware authors have turned to agile development to quickly counter the latest tactics of anti-malware products. A great example of this is the 4.0 version of GandCrab ransomware, which rose through the ranks over the year to become one of the most impactful threats of its type.

Major reasons for its success tie back to its innovative development, collection, and distribution methods. The actors behind GandCrab were the first group to accept Dash cryptocurrency. It also appears that they use the Agile development approach to beat competitors to market and deal with issues and bugs when they arise. Another unique aspect to GandCrab is its Ransomware-as-a-Service (RaaS) model, which is based on a profit-sharing (60/40) model between the developers and criminals wishing to utilize their services. And lastly, GandCrab uses .BIT, a top-level domain unrecognized by ICANN, which is served via the Namecoin cryptocurrency infrastructure and uses various name servers to help resolve DNS and redirect traffic to it.

Keeping an Eye on ICS

The reemergence of the Shamoon malware in a wave of attacks in the Middle East during December sent yet another signal of the renewed vigor among destructive attacks. The Shamoon malware doesn't target industrial control systems (ICS), but one of its most famous victims was the state-owned oil company, Saudi Aramco, in 2012. According to some,[1] overspending on ICS and underspending on IT is one of the factors that contributed to the scale and impact of the incident to the company. For many organizations, however, that budgetary focus—especially when it comes to security dollars—is reversed, leaving ICS exposed.

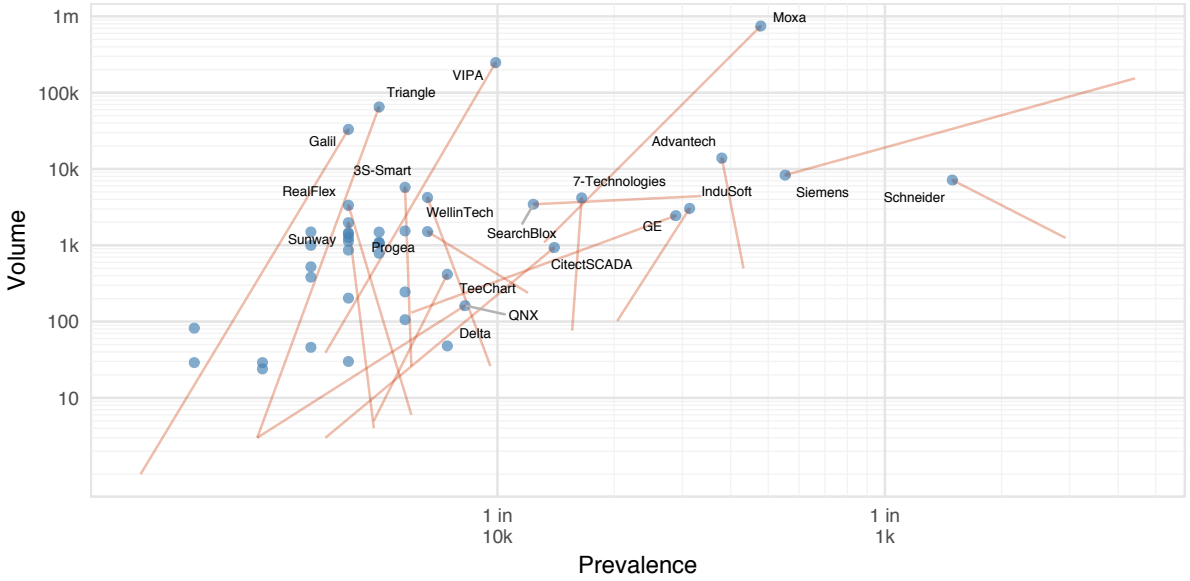


Figure 16: Change in Prevalence and Volume of ICS Exploits, Q1 > Q4 2018

Because of this tendency, we wanted to include Figure 16 in this Year in Review. The blue dot plots exploits targeting various ICS manufacturers according to their prevalence and volume in Q4 2018. The top 20 exploits are labeled. The red lines trace back to where each set of exploits was located on the coordinate plane in Q1 2018. So, we see the relative change in prevalence and frequency in these attacks for the year. It is noteworthy that most of them gain ground on both scales. We hope it offers a reminder to keep 2019 IT and OT investments in proper balance within your organization.

[1] Christina Kubecka (2015-08-03). "How to Implement IT Security after a Cyber Meltdown". Retrieved 2019-01-20.

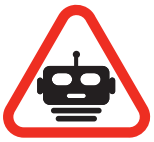
Sources and Measures

The findings in this report represent the collective intelligence of FortiGuard Labs, drawn from Fortinet's vast array of network devices/sensors collecting billions of threat events and incidents observed in live production environments around the world. According to independent research,[2] Fortinet has the largest security device footprint and accordingly we boast the largest sampling of threat data in the industry. All data was anonymized and contains no identifiable information on any entity represented in the sample.

As one might imagine, this intelligence offers excellent views of the cyber-threat landscape from many perspectives. This report focuses on three central and complementary aspects of that landscape, namely application exploits, malicious software (malware), and botnets.

Exploits
Application exploits described in this report were collected primarily via network IPS. This dataset offers a view into attacker reconnaissance activities to identify vulnerable systems and attempts to exploit those vulnerabilities.

Malware
Malware samples described in this report were collected via perimeter devices, sandboxes, or endpoints. For the most part, this dataset represents the weaponization or delivery stages of an attack rather than successful installation in target systems.



Botnets
Botnet activity described in this report was collected via network devices. This dataset represents command-and-control (C2) traffic between compromised internal systems and malicious external hosts.

In addition to these different aspects of the threat landscape, we use three measures to describe and interpret what the data tells us. You'll regularly see the terms volume, prevalence, and intensity used throughout this report, and our usage of these terms will always conform to the definitions provided here.

The figures in this report include a large number of threats. We provide brief descriptions on some, but you will undoubtedly desire more information than we're able to supply here. Consult the FortiGuard Labs Encyclopedia as needed while working your way through these pages.

VOLUME	Measure of overall frequency or proportion. The total number or percentage of observations of a threat event.
PREVALENCE	Measure of spread or pervasiveness across groups. The percentage of reporting organizations[3] that observed the threat event at least once.
INTENSITY	Measure of daily volume or frequency. The average number of observations of a threat event per organization per day.

[2] Source: IDC Worldwide Security Appliances Tracker, April 2018 (based on annual unit shipments)

[3] We can only measure prevalence among organizations reporting threat activity. A prevalence of 50% for a given botnet doesn't mean it impacted half of all firms in the world. It means half of the firms in our botnet dataset observed that particular botnet. That denominator usually represents tens of thousands of firms.

Conclusion and Recommendations

FORTINET

Conclusion and Recommendations

Time is an extremely precious and nonrenewable resource, so we appreciate you spending yours with us as we recapped the Q4 2018 cyber-threat landscape and highlighted key developments across the year. To help you turn this information into action, we provide the recommendations below, which tie back to our Year in Review section.

01

Vulnerabilities like Meltdown and Spectre are very concerning to security and privacy. One of the key challenges with addressing these vulnerabilities—besides the fact that the affected chips are already embedded in millions of devices running in home or production environments—is that developing a patch that resolves their exposed side-channel issues is extremely complicated. In fact, Intel had to pull one of the early patches because it led to a reboot issue on some devices. Which is why, in addition to establishing an aggressive and proactive patch-and-replace protocol, it is essential that organizations have layers of security in place designed to detect malicious activity and malware, and to protect vulnerable systems.

02

The above can also be said of any zero-day vulnerability. Test and deploy the patches when they become available, but do not make this the single line of defense. Proactively minimizing your externally visible and accessible attack surface will have the side benefit of buying you extra time when the next zero day becomes public. You won't be the first target picked up during the early reconnaissance runs looking for easy targets.

03

Innovation and destructive tendencies were on display among malware variants analyzed all year. This, combined with the cryptojacking trend, points to the continued transformation of cyber crime. To keep your organization ahead of the curve, check out this blog post for related recommendations.

04

We showed that cryptojacking jacked up more and more systems over the course of 2018. If you are worried that your systems might be among them, start by checking the Task Manager (Windows), Activity Monitor (Mac), and "top" on the Linux command line. Using these tools, you can also list all the processes running on your computer and then find/kill the culprit that's consuming resources. It may also be a good idea to help make sure employees' home networks are segmented from machines that connect to the enterprise network through VPNs. At a minimum, ensuring awareness on how to do this properly is part of your security training program.

05

Several exploits targeting IoT devices topped our charts this quarter and for the year. We recommend our Learn, Segment, and Protect approach to quell the storm. This starts with learning more about devices connected to networks, how they're configured, and how they authenticate. Once complete visibility is achieved, organizations can dynamically segment IoT devices into secured network zones with customized policies. Segments can then be linked together by an integrated, intelligent, and protective fabric across the network—especially at access points, cross-segment network traffic locations, and even into multi-cloud environments.

06

Defense against IoT botnets is challenging to say the least. Fortinet recommends pursuing options such as off-site storage of system backups, having redundant systems, keeping devices updated, segmenting networks between IoT devices and production network, monitoring traffic between these segments, and utilizing real-time threat intelligence.

07

Attacks against SCADA devices aren't the most common, but they could be the most critical. If your organization uses SCADA or other ICS, the first step is to fully assess business and operational risks associated with those technologies to define a risk-informed strategy. That should include defining the zones, conduits, boundaries, and security levels, which will be invaluable for limiting communications between OT and non-OT environments. Tips on securing OT networks can be found in this blog post.

08

A FortiGuard subscription detects threats discussed in this report. That may sound a little salesy or self-serving, but we'd be remiss if we didn't mention it for the sake of our customers. We consider it our duty to translate everything we learn through our threat and vulnerability research into the products and services we offer, and we want customers to have that peace of mind.

www.fortinet.com

356902-0-0-EN

Threat-Report-Q4-2018-021519-154pm