
FORTINET
QUARTERLY THREAT LANDSCAPE REPORT
Q3 2018

TABLE OF CONTENTS

Q3 2018 **INTRODUCTION AND KEY FINDINGS**

Thank you for checking back in with us for the Q3 2018 edition of our quarterly review of the cyber-threat landscape. We know we aren't the only threat report vying for your attention, so we're mindful of making sure your time with us is well-spent. In fact, let's get started.

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. According to IDC, Fortinet is the No. 1 most adopted network security solution, having deployed 4.2 million devices.[1] This provides a unique perspective on the threat landscape that we distill into this report. The rest of the report digs into and adds context around those key findings.

This report is similar in structure to its predecessors. We set the stage for our data-driven analysis with some noteworthy events pulled from Q3 headlines. Data analysis starts with some IT infrastructure trends, focusing this time on web encryption and cloud applications. We then move into the trio of threat datasets that comprise the bulk of this report—exploits, malware, and botnets. While those categories remain the same, we've created some brand new ways of visualizing them that we hope you'll find interesting and useful.

Another new innovation we're very excited to introduce this quarter is the Fortinet Threat Landscape Index. There's a detailed explanation of what it is and how it was developed in the report, but suffice it to say it will help answer that recurring question of "Is it getting worse out there?"

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.

Q3 2018 BY THE NUMBERS:

Exploits

- Exploit Index rose 2%
- 7,925 unique exploits detected
- 1,114 detections per firm
- 65.4% of firms saw severe exploits
- IoT exploits increased in prevalence
- 20 zero days found by FortiGuard Labs

Malware

- Malware Index rose 4%
- 34,148 unique variants detected
- 21 unique daily detections per firm
- 4 variants spread to ≥10% of firms
- 19% saw cryptojacking malware
- 26% reported mobile malware

Botnets

- Botnet Index rose 2%
- 257 unique botnets detected
- 10.2 infection days per firm
- 3.2% of firms saw ≥10 bots
- 58% of infections lasted 1 day
- 4% of infections lasted >1 week

LONG-TERM TRENDS WE'RE TRACKING:

- Economic dynamics driving the development of ransomware, cryptojacking, and other crimeware
- Evolution of rapid malware development through code reuse, agile approaches, and other methods
- Continued rise of destructive threats and the changing impact on business risk and resiliency
- Evolution of attacks targeting critical infrastructure and IoT devices

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

HIGHLIGHTS FROM THE HEADLINES

This report analyzes threat data culled from millions of Fortinet devices across the Internet, but what's happening in the dataset is not disconnected from what's happening in the headlines. With that in mind, we offer a selection of cyber storylines that caught our attention last quarter.

There were several indictments related to major breaches over the past years:

- 12 Russian intelligence officers were indicted by the U.S. Department of Justice for their role in expansive cyber operations against the Democratic Party leading up to the 2016 Presidential election. This activity is old news by now, but indictments ratchet things up several notches above accusations.

- Park Jin Hyok of North Korea was indicted by the U.S. Department of Justice for his alleged involvement in the 2014 hack of Sony Pictures, the 2016 theft of $81 million from Bangladesh Central Bank, as well as the 2017 WannaCry ransomware attacks.
- The U.S. Department of Justice announced the indictment and extradition of Andrei Tyurin, the Russian hacker accused of stealing data from over 80 million JPMorgan Chase customers in 2014.

Other notable events from the quarter include:

- A bombshell Bloomberg story asserted that Chinese spies had exploited the technology supply chain of 30 companies, including Amazon and Apple, and managed to insert tiny rogue microchips into servers during the manufacturing process. The report was publicly denied by Amazon and questioned by some in the security community. But Bloomberg continues to stand by its story. Either way, it's a significant, plausible event prompting important international dialogue regarding supply chain threats.

- Facebook announced they had discovered a security breach that compromised over 50 million user accounts. The scope escalated when it was subsequently announced the flaw in question also affected third-party apps linked to a user's Facebook account.

- SingHealth, Singapore's largest healthcare institution, reported an attack compromising the personal information of 1.5 million patients and prescription details for 160,000 others. The country's Ministry of Health attributed the attack to state-sponsored actors.
- $31 million in cryptocurrency was stolen from South Korean crypto exchange Bithumb. Bitcoin prices dropped directly after the announcement of the breach.

- We've seen a glut of accidental data leaks lately, with two notables this quarter: 1) Comcast Xfinity quickly patched a bug in a login page that leaked partial Social Security numbers and addresses of over 26 million customers; 2) A Government Payment Service Inc. website flaw exposed personal and payment records of more than 14 million customers dating back at least six years.

- Gemalto generated headlines by announcing 1 billion records were breached from India's Aadhaar database (U.S. SSN equivalent). But their retraction of and apology for that announcement wasn't as well-covered (it didn't happen).

INTRODUCING THE FORTINET THREAT LANDSCAPE INDEX

Our goal with this report has always been to track the ever-shifting contours of the cyber-threat landscape and communicate what we're seeing to our readers. For the most part, your feedback suggests we've done that well over the years. But one thing we've found challenging is providing a clear and concise answer to the seemingly simple, yet deceptively difficult question of "Is it getting better or worse out there?" We're happy to say that we now have a way to answer that question. It's called the Fortinet Threat Landscape Index (TLI).

Generally speaking, the TLI is based on the premise that if organizations are seeing more threats more frequently, then things are getting worse. If the opposite is true, then the cyber landscape is less threatening. Perhaps most importantly, it shows the rate and reasons for those changes. This is conceptually consistent with the measures of prevalence and volume regularly featured in the report for specific threats (see the Sources and Measures section for definitions).

Here's a summary of how it works: For each week, we iteratively sample 1,000 firms at random and determine the total number of unique threats observed by each and the total volume or frequency of those threats across all firms in the sample. Then we aggregate the iterated samples with an arithmetic mean of the log and equalize them across our two measurements in order to compute the combined distance from zero. We then scale the output to a starting point of 1,000 for the first week this quarter. Without further adieu, here's what the Fortinet TLI looks like for Q3 2018:

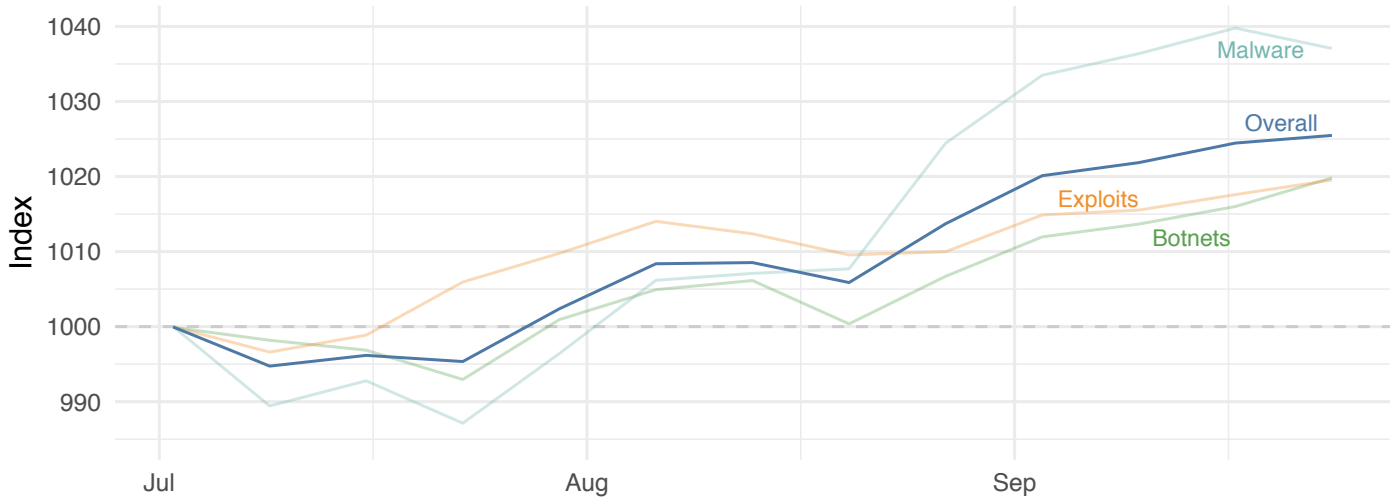


FIGURE 1: FORTINET THREAT LANDSCAPE INDEX (OVERALL) WITH INDIVIDUAL INDICES SHOWN FOR EXPLOITS, MALWARE, AND BOTNETS.

The overall composite TLI is represented by the bold line, with the individual indices for exploits, malware, and botnets broken out for comparison. After an initial dip, the TLI rose steadily over the quarter to close roughly 2.5% higher than it began. With regard to the question that spawned this, "Things got a little worse in Q3," overall, organizations reported a widening variety of threats at increasing rates over the course of the quarter. It can further be deduced from Figure 1 that malware was a larger contributing factor to that rise than exploits or botnets. How and why is that? Well, that's what the rest of this report is all about—read on!


INFRASTRUCTURE
TRENDS
FORTINET

INFRASTRUCTURE TRENDS

We regularly stress the relationship between an organization's IT infrastructure and the external threat environment. Not only does this directly impact the attack surface but also a host of other risk-relevant factors as well. Figure 2 presents statistics over the past 2.5 years on web traffic encryption and the usage of SaaS and IaaS applications among firms in our sample.

	Q1 2016	Q2 2016	Q3 2016	Q4 2016	Q1 2017	Q2 2017	Q3 2017	Q4 2017	Q1 2018	Q2 2018	Q3 2018
HTTPS ratio	52.5%	49.8%	52.4%	50.8%	54.9%	57.3%	55.4%	58.5%	61.7%	65.7%	72.2%
SaaS apps	33	35	35	36	33	28	32	37	32	34	38
IaaS apps	26	22	23	27	29	25	26	28	23	25	32

FIGURE 2: QUARTERLY MEDIAN VALUES FOR HTTPS RATIO, SAAS USAGE, AND IAAS USAGE.

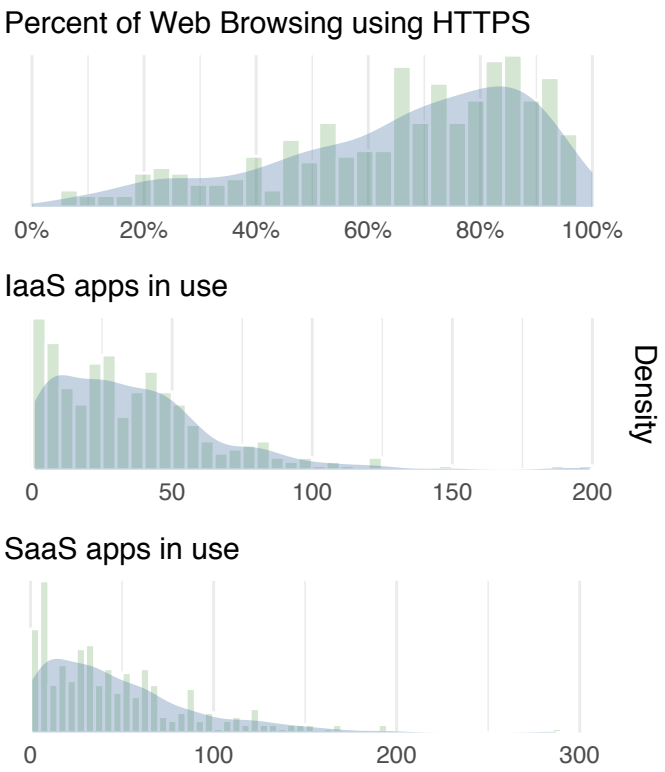


FIGURE 3: DISTRIBUTION OF HTTPS RATIO, SAAS USAGE, AND IAAS USAGE ACROSS FIRMS.

Q3 2018 marks the first time that all three of these measures are at their highest point. And there's probably good reason for that. As firms migrate sensitive applications and data to the cloud, their need to secure those communication channels increases as well.

The fact that the HTTPS ratio has risen 20% over the period shown in Figure 2 is a net positive for security for firms and the Internet at large. However, higher encryption rates can present challenges to threat monitoring and detection. Organizations cannot afford to turn a blind eye toward threats that might use encrypted communications for cover.

Cloud applications are another double-edged sword. Done right, they can boost resiliency, lower cost, and reduce risk. Done wrong, they can negate or even reverse those benefits. Want to know if you're doing it right? We're glad to help with that.

While the trio of all-time highs is interesting, Figure 3 reminds us that the median value doesn't tell the whole story. The distributions show that some firms encrypt all web traffic while others encrypt none. And the long tails for SaaS and IaaS usage speak to a wide variation in cloud adoption.

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 rose **2%**
- **7,925** unique detections
- **1,114** detections per firm
- **65.4%** saw severe exploits
- IoT exploits increased in prevalence
- **20 zero days** found by FortiGuard Labs

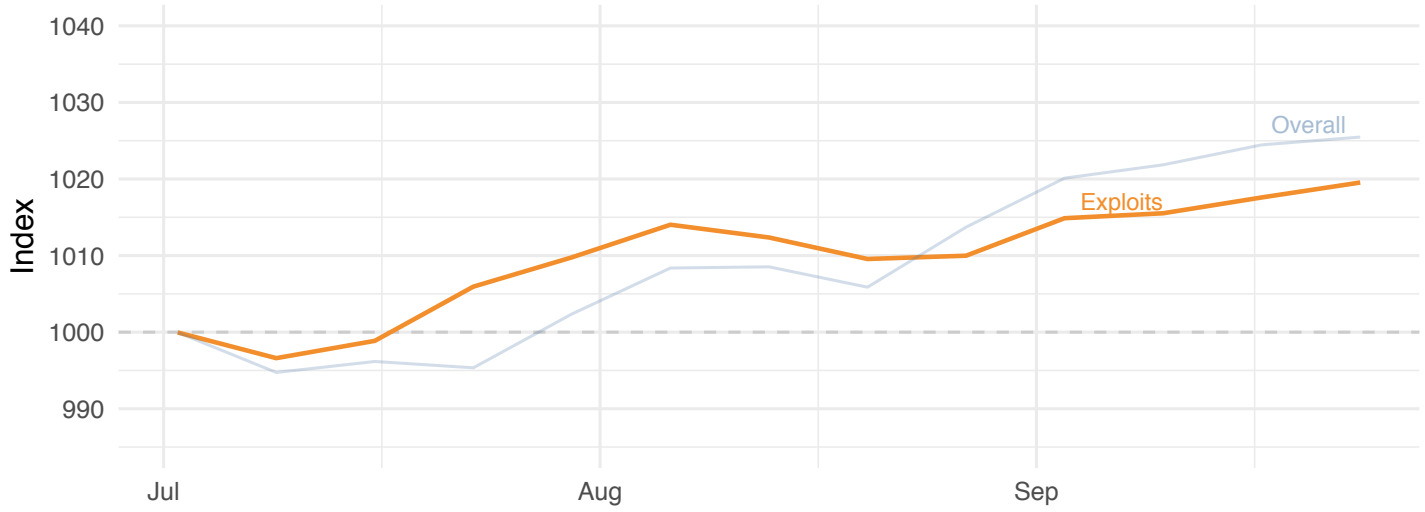


FIGURE 4: FORTINET EXPLOIT INDEX FOR Q3 2018.

The Exploit Index rose about 2%, but tracked below the overall TLI for the last month. Let's unpack what's driving that trend by examining the most prevalent exploits and vulnerabilities observed during the quarter.

We've seen the first few items on the list in Figure 5 before. The No. 1 ranked Apache Struts exploit has been a top detection since its role in the infamous Equifax breach a year ago. A related new development this quarter is that the Mirai and Gafgyt botnets—which historically target IoT devices—added this exploit (as well as the one targeting SonicWall GMS) to their arsenal. More on that to follow.

The buffer overflow bug in the WebDAV service in Microsoft IIS 6.0 was reportedly first exploited about midway through 2016. It remained low on our radar until a surge in activity during April of this year. This prompted us to take a closer look in this blog post. The scoop is that it's being used to distribute multiple cryptojacking malware variants. There's no patch for CVE-2017-7269, so those concerned should follow Microsoft's advice and upgrade to IIS version 7.0.

An exploit against a 2012 arbitrary code execution vulnerability in PHP takes us even further back in time. It's still popular with attackers due to the combo of low effort and high reward when successfully exploited.

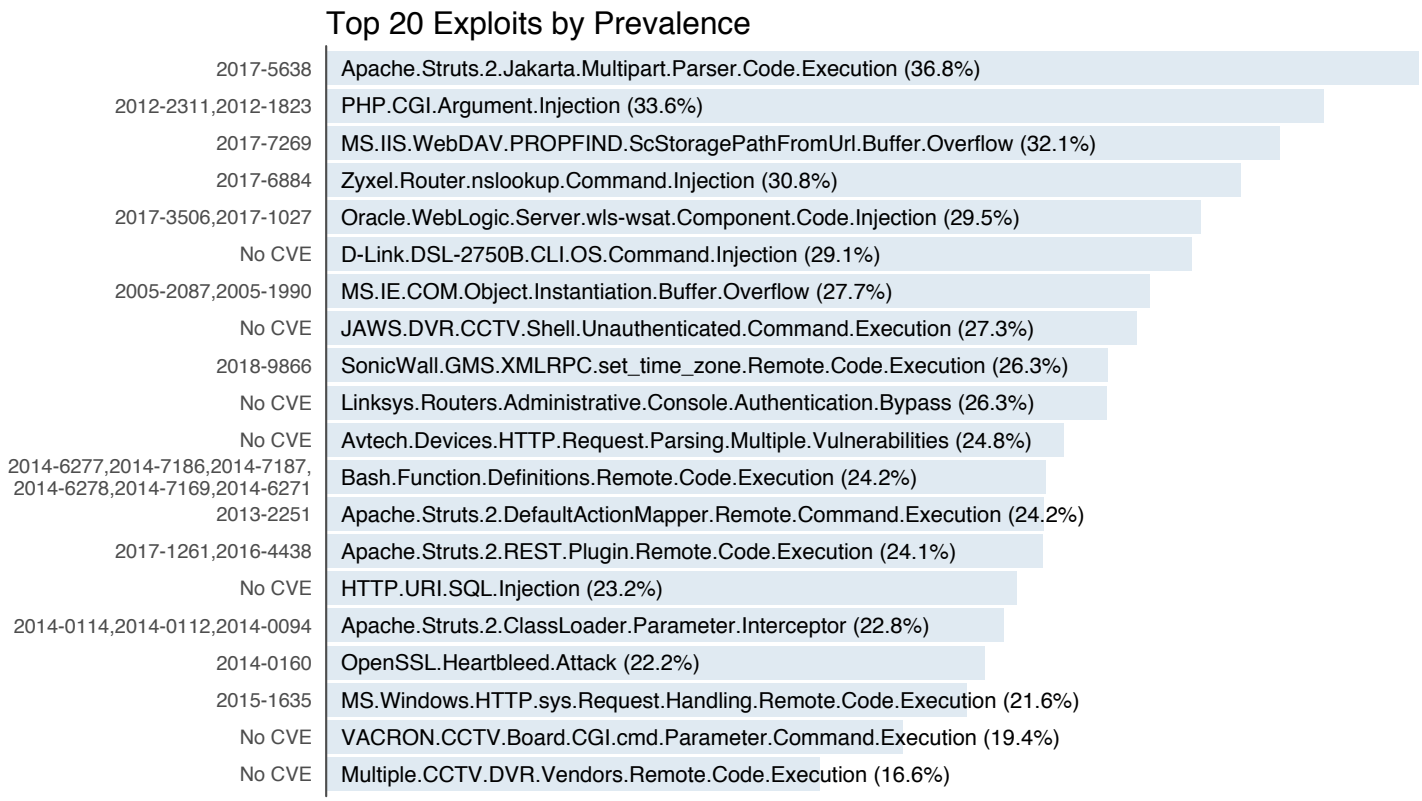


FIGURE 5: MOST PREVALENT EXPLOIT DETECTIONS AND ASSOCIATED CVES.

Rounding out the old-yet-still-lively category, probes for the Heartbleed vulnerability increased this quarter even though the exploit is now four years old. The vulnerability gives attackers the ability to read system memory as long as the systems contain unpatched versions of OpenSSL. Staying on top of security hygiene is the best way to avoid waking these sleeping giants.

INTERNET OF THINGS EXPLOITS

Beyond the aforementioned exploits, Figure 5 takes on a decidedly IoT theme—perhaps more so than any previous quarter. To expand and emphasize the scale of attacks recorded against IoT and consumer devices, we created Figure 6. It is comprised of six separate charts that plot the volume and prevalence of exploits targeting various manufacturers of IoT device categories.

The figure makes it possible to compare the categories to each other (i.e., the variety, volume, and prevalence of router exploits are higher than the printer category) as well as the devices within each category. Within the router category, for instance, the volume of attacks against Netcore devices was two orders of magnitude higher than any other manufacturer, but a much larger proportion of firms (one in eight) reported Linksys exploits.

We find it interesting that, while some manufacturers appear in multiple categories, no manufacturer leads in more than one. In fact, Linksys lies on opposing sides of the grid for routers and IP cameras. It's quite possible this correlates with relative market share for manufacturers in different device categories. With those observations in mind, we'll let you explore Figure 6 at your own leisure.

For insight into how botnets coordinate all these IoT attacks, see the "Evolution of IoT Botnets" Mini Focus in the Botnet Trends section.

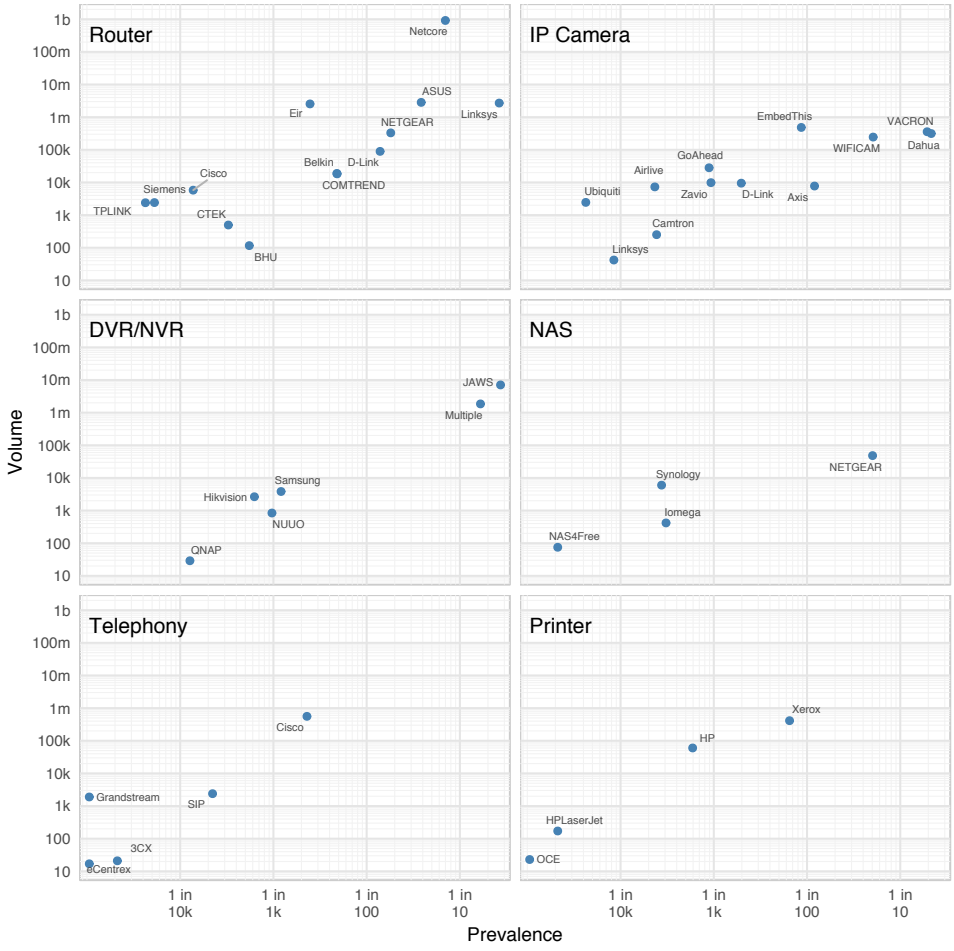


FIGURE 6: PREVALENCE AND VOLUME OF IOT EXPLOITS BY DEVICE CATEGORY.

ICS AND SCADA EXPLOITS

On the opposite end of the spectrum from consumer tech lie exploits against industrial technologies. The scope of these attacks is understandably smaller than for the more widespread consumer devices, but their potential impact is much greater. ICS and SCADA technologies have become high-value targets for hackers looking to disrupt business operations, collect ransom, or compromise a rival nation's critical infrastructure. As evidence of that, a recent Forrester study found that nearly 60% of firms using SCADA or ICS experienced a breach in those systems in the past year. For organizations working to protect such systems, we offer Figure 7. It shows which ICS/SCADA products drew the most fire over the last quarter.

The positioning seen in Figure 7 appears very similar to previous quarters. Unlike consumer devices, industrial technologies are built and deployed for the long term, meaning the ICS/SCADA attack surface doesn't change overnight. Schneider typically leads in attack prevalence every quarter, with Siemens and Advantech vying for second and third place. Exploit attempts against VIPA PLCs are reported by far fewer firms, but the volume among the subset that do is very high.

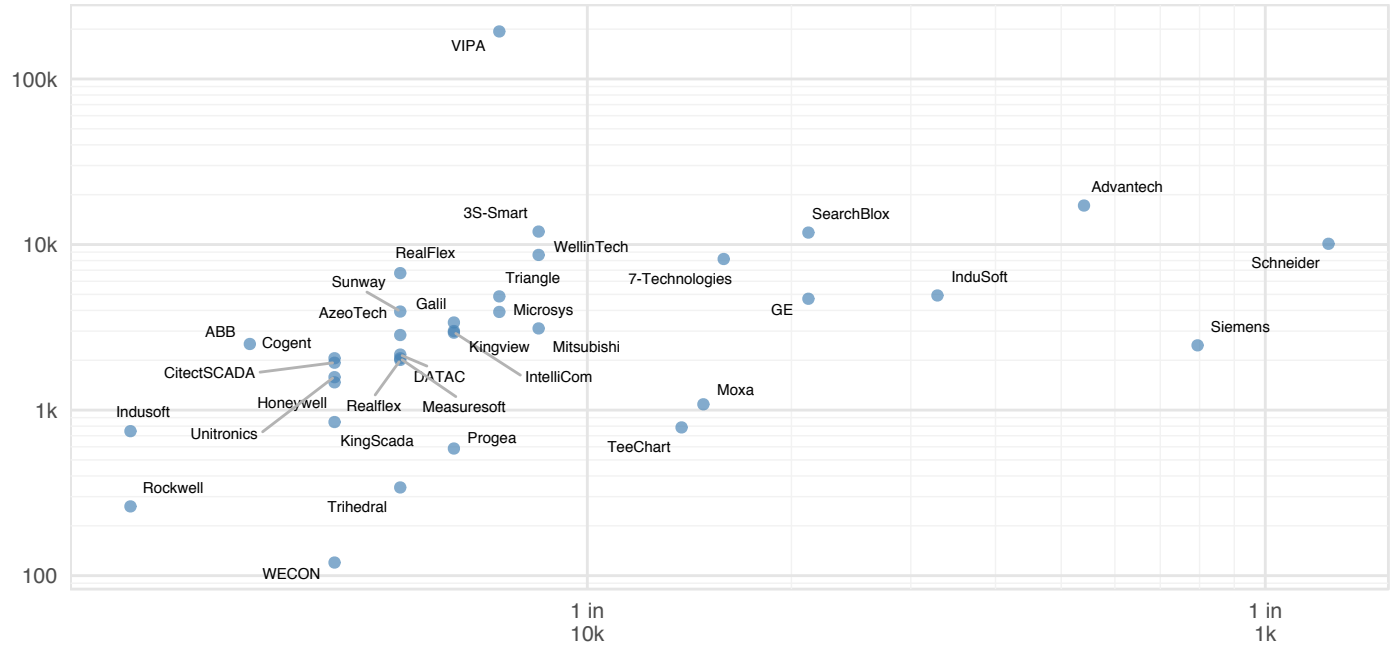


FIGURE 7: PREVALENCE AND VOLUME OF ICS/SCADA EXPLOITS.

OTHER EXPLOITS ON OUR RADAR IN Q3 2018

Aside from the top exploits discussed above, here's a quick summary of other developments we monitored during the quarter:

- A zero-day local privilege escalation vulnerability was found in the Advanced Local Procedure Call (ALPC) interface of Microsoft Windows task scheduler, which can allow a local user to obtain SYSTEM privileges. Exploits are now in the wild.
- Foreshadow (also known as Intel L1 Terminal Fault) (CVE-2018-3615) and Foreshadow-NG (CVE-2018-3620, CVE- 2018-3646) are a new breed of speculative execution attacks disclosed in Q3 affecting Intel's Software Guard Extensions (SGX) technology, which is supposed to protect systems from unauthorized access and limits access to ring 3 (least privileged). There are no reports of active exploitation at this time.
- Researchers announced a variant of the Spectre side-channel attack, dubbed "NetSpectre." What makes this new attack vector unique from the previous versions over the past few months is that this disclosure shows that a network-based side-channel attack is possible. There are no reports of active exploitation at this time.

SPOTLIGHT ON ZERO-DAY RESEARCH

Fortinet's team of dedicated expert researchers and analysts examine many third-party products and software applications daily, looking for weaknesses and exploitable vulnerabilities. When a vulnerability is found, the FortiGuard Labs teams work together to create protective measures that can be delivered to our customers and notify the software/product vendor of the vulnerability. Learn more.

During Q3 2018, our researchers disclosed 20 vulnerabilities affecting a range of products:

- Adobe Photoshop CC PCT File Memory Corruption Vulnerability (CVE-2018-12811)
- Adobe Photoshop CC TGA File Memory Corruption Vulnerability (CVE-2018-12810)
- AirVPN for Windows DLL PreLoading Vulnerability
- AnyDesk for Windows DLL PreLoading Vulnerability (CVE-2018-13102)
- Asus Routers Persistent Cross-Site Scripting Vulnerability (CVE-2018-13154)
- Cisco WebEx Network Recording Player Memory Corruption Vulnerability (CVE-2018-0380)
- Cisco WebEx Network Recording Player Memory Corruption Vulnerability II (CVE-2018-0380)
- Cisco WebEx Network Recording Player Remote Code Execution Vulnerability (CVE-2018-0379)
- Cisco WebEx Player Memory Corruption Vulnerability I (CVE-2018-0380)
- Cisco WebEx Player Memory Corruption Vulnerability II (CVE-2018-0380)
- Dell EMC Isilon OneFS and IsilonSD Edge Remote Kernel Crash Vulnerability (CVE-2018-11071)
- Easy Hosting Control Panel Multiple Cross-Site Scripting Vulnerabilities (CVE-2018-13124)
- Easy Hosting Control Panel SQL Injection Vulnerability (CVE-2018-13125)
- Jenkins Config File Provider Plugin Cross-Site Scripting Vulnerability
- Jenkins Metadata Plugin Cross-Site Scripting Vulnerability
- Microsoft Windows JET Database Engine Buffer Overflow Vulnerability (CVE-2018-8392)
- Nextcloud Insufficient Input Validation Vulnerability (CVE-2018-3776)
- Sony SmartTV Vulnerabilities
- Symantec Norton Power Eraser DLL Preloading Vulnerability (CVE-2018-5238)
- TorGuard VPN for Windows DLL PreLoading Vulnerability

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 levels on an array of devices.

QUICK STATS:

- Malware Index rose **4%**
- **34,148** unique variants
- **6,405** different families
- **21** unique daily detections per firm
- **4** variants spread to ≥10% of firms
- **19.31%** saw cryptojacking malware
- **26%** reported mobile malware

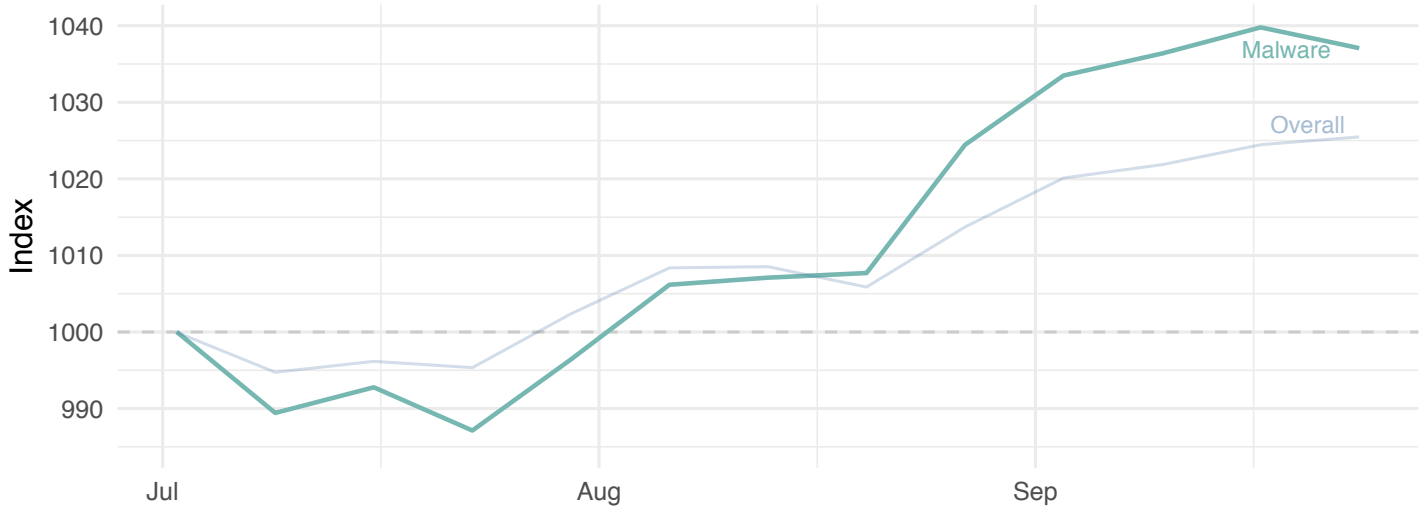


FIGURE 8: FORTINET MALWARE INDEX FOR Q3 2018.

As mentioned previously, the Malware Index in Q3 2018 outpaced the overall TLI and the indices for exploits and botnets. It peaked in mid-September at 4% above the starting point. A major driver for that was 10,000 additional variants that flooded the landscape (not all of which were new; some just didn't make an appearance in Q2) and a near doubling of malware detections per firm. Looks like malware season is in full swing—might want to get that vaccine!

To help you peruse and ponder all this malware, we did something a little different this quarter. Rather than a single chart of top malware, we show separate charts for the major platforms or categories in Figure 9. Within each of those, we then plot malware families according to prevalence and volume. Because they're all the rage with the criminals lately, cryptojacking strains are shown in red—but let's not get too far ahead of ourselves.

There are many things that could be said about Figure 9, so we'll stick to some high-level observations. The first of those is obvious—malware developers offer good support for multiple platforms. The Agent family is a good example of this, appearing in all nine plots (and usually toward the upper right). That makes sense in light of that family's role as a generic downloader or dropper for numerous other types and strains of malware.

Another takeaway from Figure 9 is that volume, variety, and prevalence of malware differs across platforms. For instance, the Win32 grid appears extremely dense from the bottom left to the upper right. The Linux plot, on the other hand, is comparatively sparse and devoid of any high-prevalence, high-volume malware. These results should not be overinterpreted, but it does say something about what platforms criminals are targeting as well as the adoption and susceptibility of those platforms.

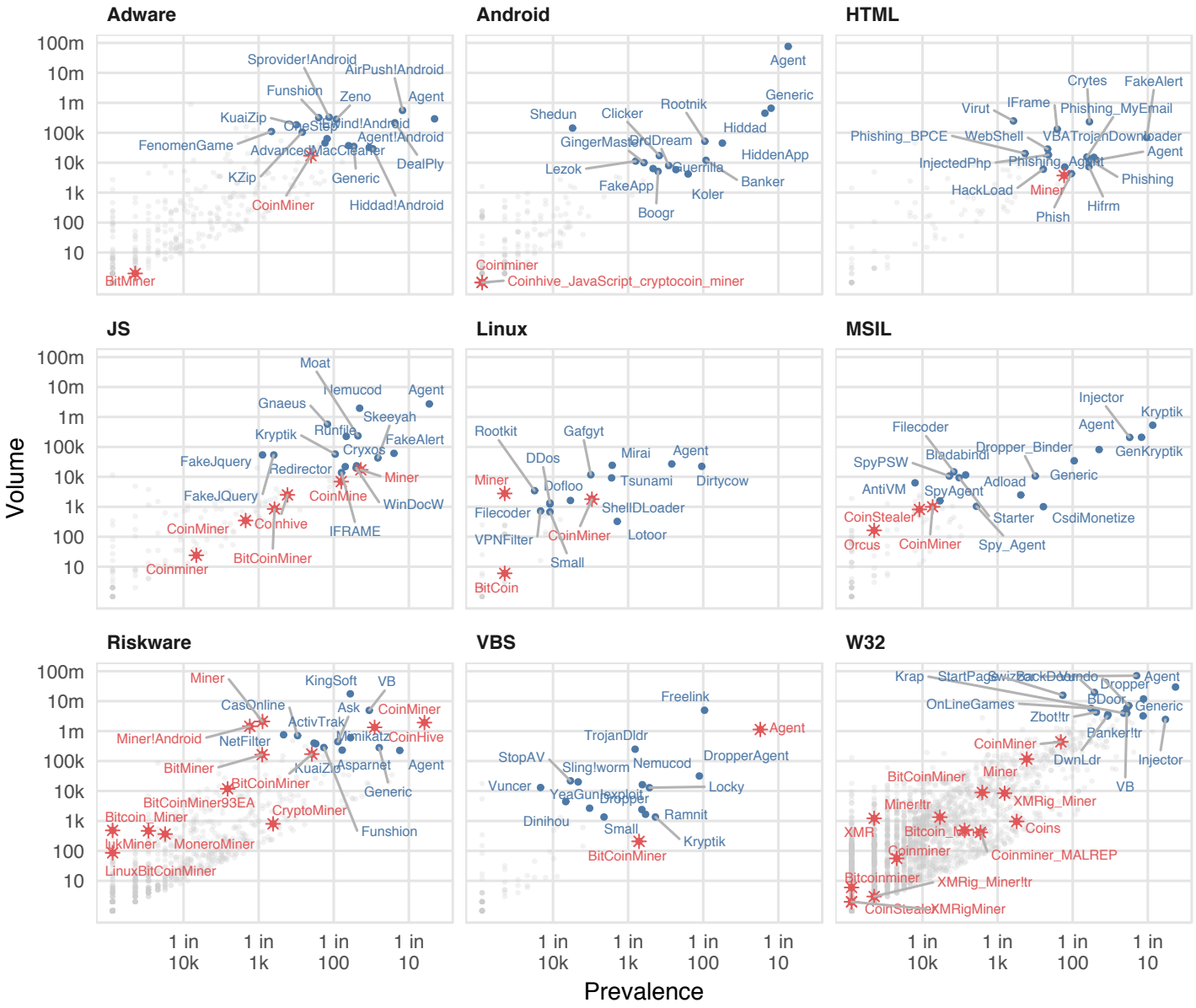


FIGURE 9: PREVALENCE AND VOLUME OF MALWARE FAMILIES BY PLATFORM.

CRYPTOJACKING

We will make one more observation regarding Figure 9, and then let you derive your own. As mentioned before, strains of cryptojacking malware are colored red. We did that to emphasize its wide and growing attack surface. Not only can a cryptojacking representative be seen in every grid but it also makes the leaders' quadrant in a few of them. We explore a potential outcome of that rise in the Mini Focus at the end of this section.

Fortinet released the first signature for a JavaScript-based cryptojacking malware in 2006. Since then, we've tracked its spread across many platforms and architectures. Figure 10 makes it easy to see that this trend is accelerating in recent years, with 2018 posting a 38% jump in the number of platforms affected by cryptojacking.

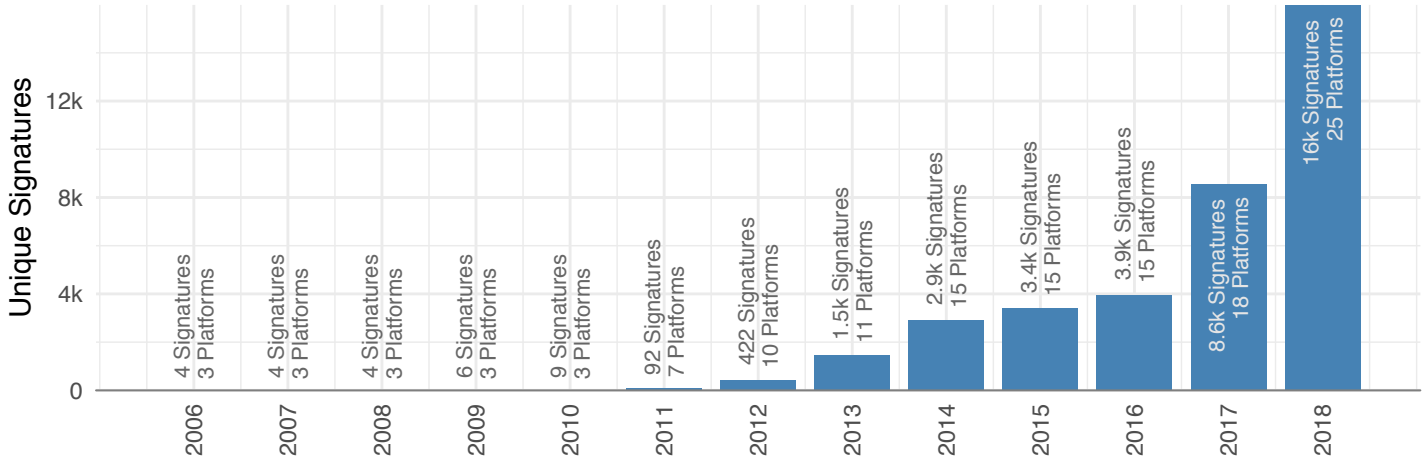


FIGURE 10: GROWTH IN CRYPTOJACKING SIGNATURES AND PLATFORMS OVER TIME.

MOBILE MALWARE

Mobile malware was on the move in Q3, with Android variants ranking in the top five of our Weekly Threat Briefs several times. Referring back to Figure 9, it can be determined that the Agent family in the Android panel sits higher on the volume scale than any other family for any other platform. We don't recall that occurring before.

The variant behind much of that activity (Android/Agent.FJ!tr) has ties to FakeSpy, a malware discovered by Trend Micro researchers in June 2018. As described in this blog post, FortiGuard Labs recently 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.

Figure 11 communicates the scale of mobile malware across the threat landscape. It's definitely come into its own over the past several years. Nearly all of these target Android devices, so we colored iOS variants red to make them easier to spot. Though other factors are certainly involved, the chart offers a thought-provoking comparison of open vs. closed operation systems.

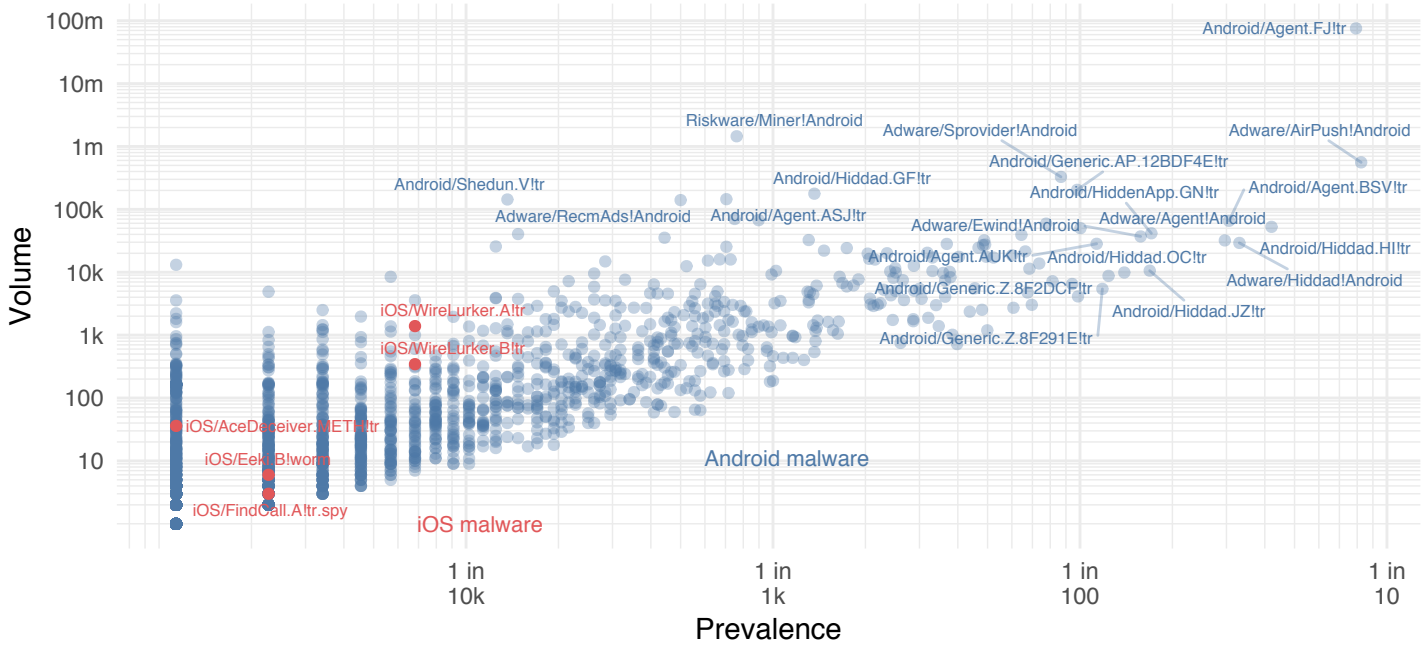


FIGURE 11: PREVALENCE AND VOLUME OF MOBILE MALWARE VARIANTS.

OTHER MALWARE ON OUR RADAR IN Q3 2018

Aside from the top malware discussed above, here's a quick summary of other developments we monitored during the quarter:

- VPNFilter is a multistage attack that was first discovered by Cisco/Talos attacking various IoT devices and routers in Ukraine. The threat continues to evolve. The actors behind VPNFilter added seven additional modules in Q3 that perform various rogue activities, effectively expanding the potential attack surface.
- The website for the popular remote administration tool Ammyy Admin was compromised and began bundling infostealer malware with each download. We detected (and blocked) that unwanted parasite in several hundred firms.
- The Ursnif banking Trojan is one of the most prolific in recent history. Our researchers uncovered a new Ursnif campaign that included highly targeted spear-phishing emails mimicking businesses relevant and local to the victim. The actors behind the campaign have clearly done their homework, and we'll keep doing ours as well.

MINI FOCUS: **IS CRYPTOJACKING JACKING UP YOUR DEFENSES?**

When we look back at 2018, cryptojacking will almost certainly be in the running for "Threat of the Year" recognition. But because cryptojacking doesn't attempt to steal data, wipe the system, or deliver some other malicious payload, not everyone views it as a critical threat to their organization. We're all for prioritization of threats based on risk to the business, but what many don't realize is that cryptojacking malware often compromises the defenses of systems under its sway. Below are some examples of this malicious activity.[2]

- PowerGhost alters preferences for system scans and updates and disables Windows Defender through the registry. It has also been observed downloading a DDoS tool.
- PyRoMine creates a backdoor account called "Default" so attackers can gain remote access with admin privileges. It enables RDP and opens up the RDP port in the Windows Firewall. It also disables services, deletes net users, and kills processes.
- Adylkuzz has functionality to change firewall rules and kill processes like the Microsoft Management Console. It also stops and deletes the Event Log Management service.
- RubyMiner clears out all cron jobs and schedules a cron job for itself. Because of this, scripts or programs—including those with security functionality—could be wiped out.
- The Jenkins miner is perhaps the most interesting. It downloads and runs a Linux binary that remains a mystery since no one was able to obtain a copy. It could be a different miner or it could be a random Linux rootkit to hide itself. Speaking of hiding, Jenkins can fake its process name to appear as "/usr/sbin/sshd" in the list of running processes.

Beyond these examples, we see a strong correlation between cryptojacking and other types of malware in our dataset. Figure 12 shows that firms reporting cryptojacking also have a larger number of other types of malware (and/or vice versa). Notice that both the peak and the tail of the reddish distribution (those with cryptojacking) exhibit significantly higher values.

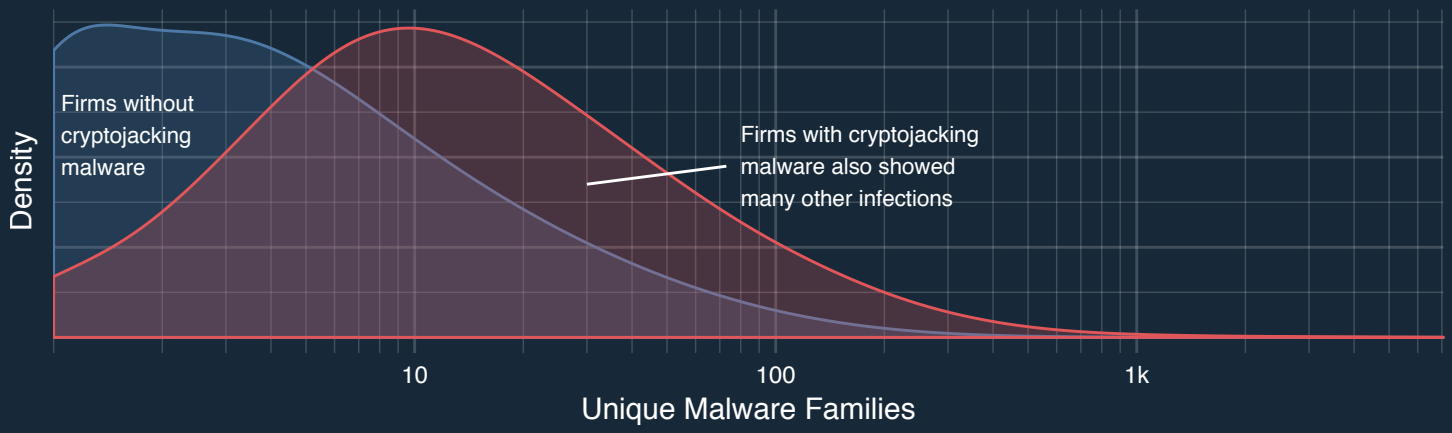


FIGURE 12: COMPARISON OF THE NUMBER OF MALWARE FAMILIES BETWEEN FIRMS THAT REPORTED CRYPTOJACKING MALWARE AND THOSE THAT DID NOT.

We attempted to establish a definitive causal relationship, and while those tests showed statistically significant results, they fell short of the burden of proof needed for a guilty conviction. We'll let you know if we find the evidence to lock cryptojacking up for good.

[2] We offer a tip of the hat to the Cyber Threat Alliance for their Joint Analysis report on cryptomining released in Q3. Some of these examples come from that report.

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.

The Botnet Index for the quarter trended up, but not quite as much as the overall TLI. Botnets differ from exploits and malware in that the most prevalent botnets remain relatively static from quarter to quarter. In fact, the top seven botnets from Q2 are the exact same for Q3, with one minor change in ordering (Sality moved from No. 7 to No. 5). That kind of consistency is fairly remarkable when you think about the dynamic nature of the cyber-threat landscape.

QUICK STATS:

- Botnet Index rose **2%**
- **257** unique botnets detected
- **10.2** infection days per firm
- **1.8** active botnets per firm
- **3.2%** of firms saw ≥10 bots
- **58%** of infections last 1 day
- **4%** of infections last >1 week

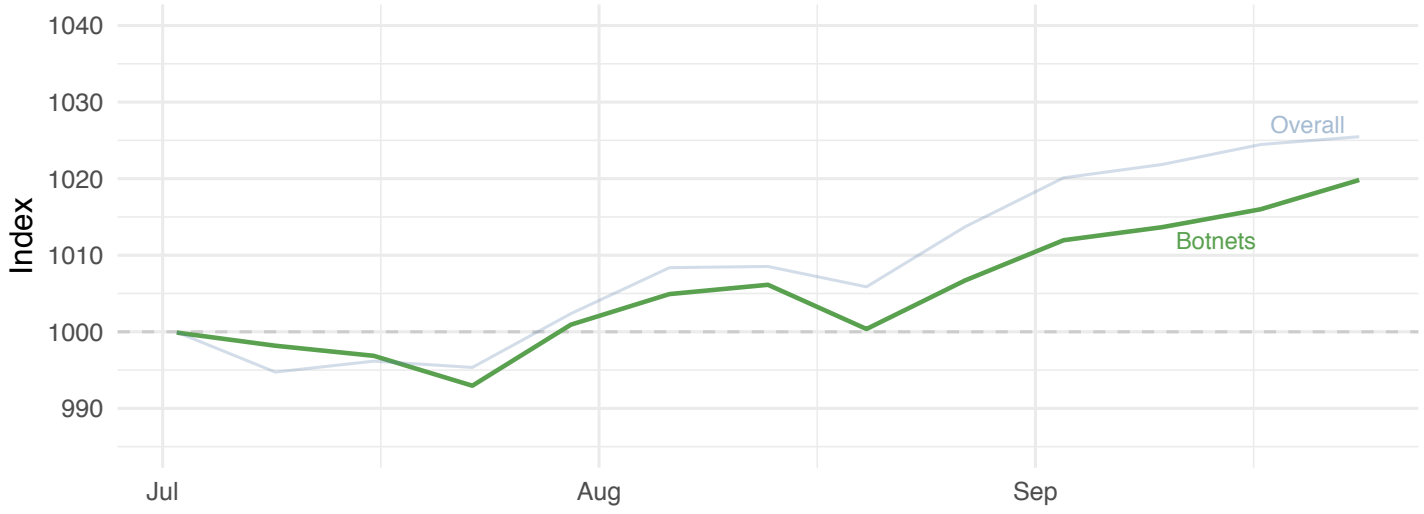


FIGURE 13: FORTINET BOTNET INDEX FOR Q3 2018.

TOP BOTS

These botnets are permanent fixtures at the top of our list every quarter. Rather than flattering them with novel commentary each time, we'll carry this summary forward and let you know if these old dogs learn any new tricks.

1. **Gh0st:** A remote access botnet that allows an attacker to take full control of the infected system, log keystrokes, provide live webcam and microphone feeds, download and upload files, and other nefarious activities.

2. **Pushdo:** This botnet saw heavy action early in its career supporting spam campaigns run by the Cutwail crime gang, but more recent activity commonly involves DDoS attacks against SSL-encrypted websites.

3. **Andromeda:** A modular botnet that installs components as needed on Windows machines, injects itself into trusted processes, and lies dormant until connection to a remote server is needed. It was the focus of a major law enforcement takedown in late 2017, but appears to still be going stronger than ever.

4. **Necurs:** A multitool of sorts among botnets, having built its name as a major distributor of ransomware, banking Trojans, and spam and financial fraud campaigns.

5. **Sality:** First spotted in 2003, this is one of the graybeards of active botnets. It's a P2P botnet used to download and install malware that will perform a wide range of secondary malicious actions.

6. **ZeroAccess:** A botnet associated with the P2P-spreading malware of the same name, it gives its masters control over affected systems and supports click fraud and cryptocurrency mining operations.

7. **Conficker:** Botnet associated with a mass-spreading worm that literally took the Internet by storm in 2008. Once infected, Conficker collects information from hosts, attacks websites, sends out spam, etc.

Because of this consistency among top botnets, we tend to focus on aspects other than total volume and prevalence in this section. You can review our analysis of botnet density, persistence, regional variation, etc., in previous reports. For this quarter, we decided to examine the "burstiness" of botnets—sudden activity changes during the quarter that may indicate campaigns or other malicious patterns. There's some interesting science behind this analysis, which you can read about here and here if you care to know the gritty details.

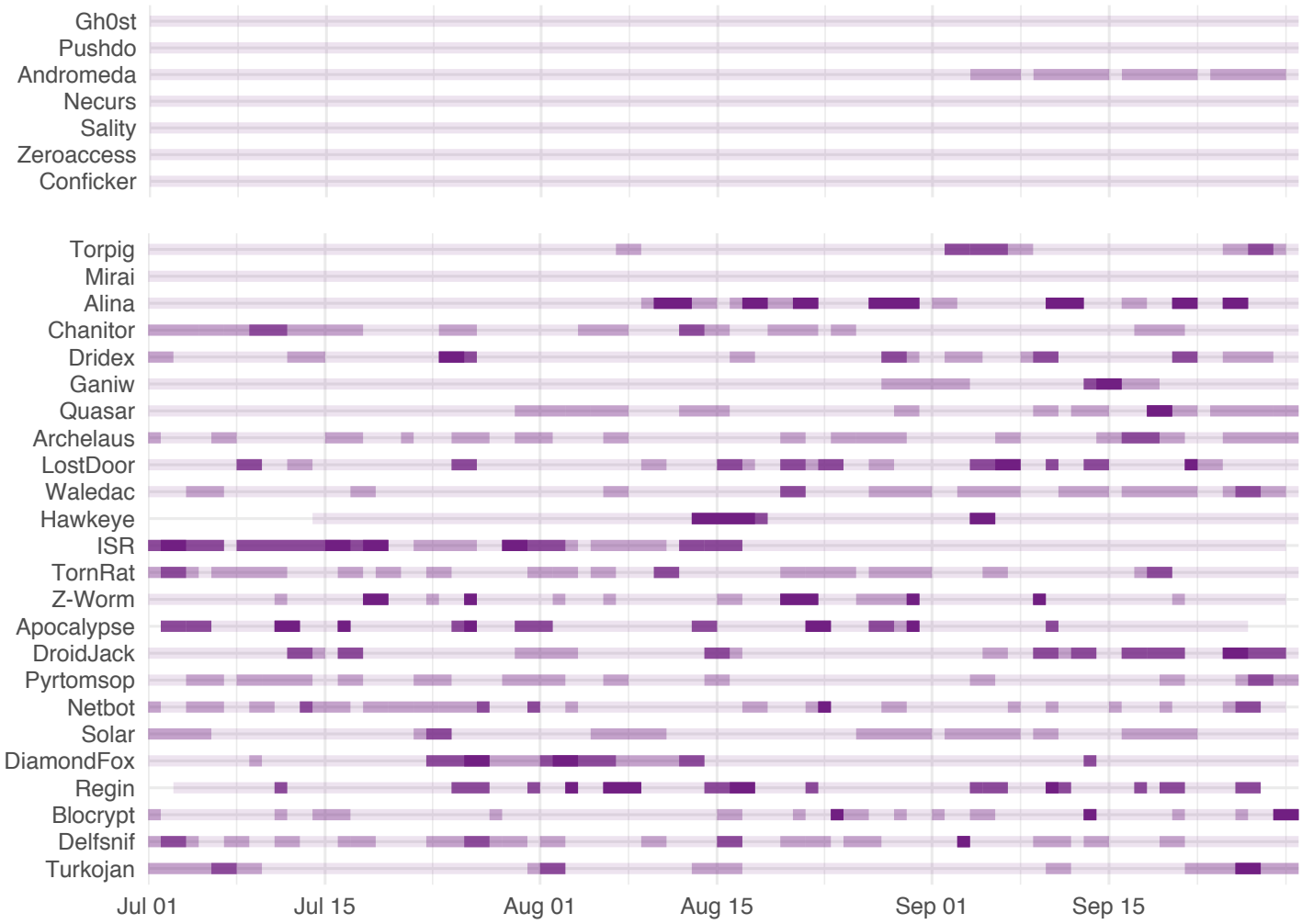


FIGURE 14: ACTIVITY BURSTS AMONG TOP BOTNETS IN Q3 2018.

The top of Figure 14 shows the daily activity for seven leading botnets described earlier along with two dozen of the most "bursty" botnets in order of decreasing overall prevalence. More intense bursts—defined as periods of uncharacteristic activity—are designated by more intense color shading. It's a lot to take in, but different behavior patterns soon become apparent. Some botnets are more persistent and burn constant all quarter (long lines of the lightest shading). Some have recurring or cyclical bursts (darker blips). Some flare up for a while and then die out (longer dashes). Overall, it seems to tell the story that attackers are constantly starting and stopping, pushing and pulling. And you wonder why SecOps staff are constantly frazzled.

BAD TRAFFIC ON THE WEEKEND?

Figure 14 highlights interesting patterns for individual botnets, but is not geared to show a view of activity across all botnets. When we create that view, it shows a clear cyclical pattern that includes regular dips in activity over the weekend.

So botnets kick it down a notch over the weekend—who cares? Well, you might when you view the chart below from our FortiGuard Labs Web Filtering team. That data shows the opposite trend—a spike in malicious traffic during weekends. Since botnets communicate with malicious hosts on the Internet, this may seem counterintuitive at first. But the y-axis labels in Figure 15 let us know we're looking at the proportional volume rather than absolute. The total botnet volume may drop for the weekend, but the relative volume of connections to malicious hosts increases. We point that out because a smaller weekend haystack may make it easier to find the needle hiding in it. Happy bot hunting!

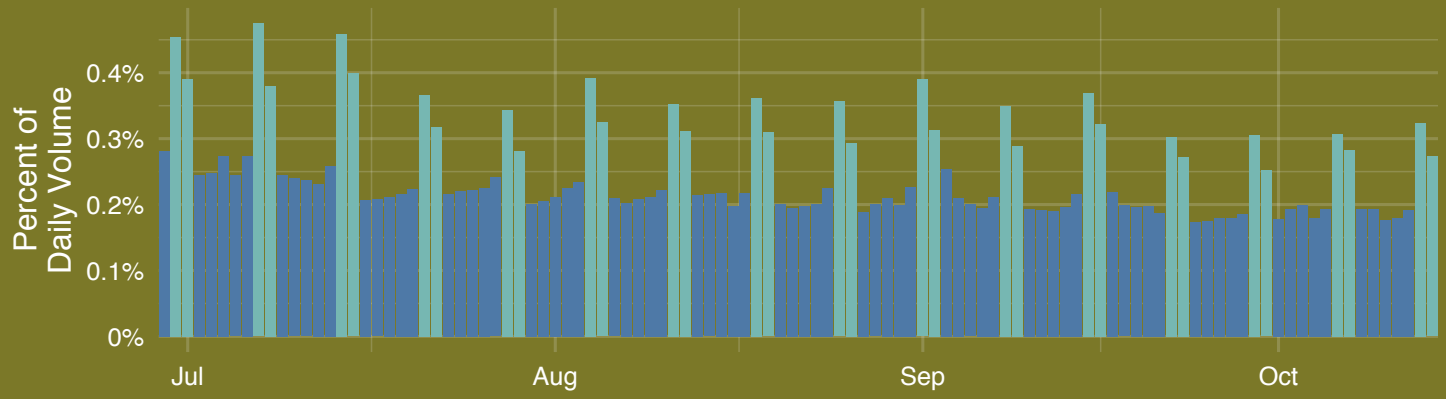


FIGURE 15: DAILY VOLUME OF TRAFFIC TO MALICIOUS WEBSITES IN Q3 2018.

There's no way we could cover every botnet in Figure 14, but we will call out a couple that caught our attention. We'll start with Alina, a relatively quiet botnet that developed quite an attitude about midway through the quarter. This caught the attention of researchers at FortiGuard Labs, who decided to do some reversing. Alina is a point-of-sale malware whose source code was leaked at least four years ago, and probably longer in underground forums. It has an optional rootkit option that hooks APIs in order to hide itself and can download/execute additional files as needed. Recent submissions of Alina to Virus Total appear largely the same as the original source code, so the exact cause of its "new life" is somewhat of a mystery.

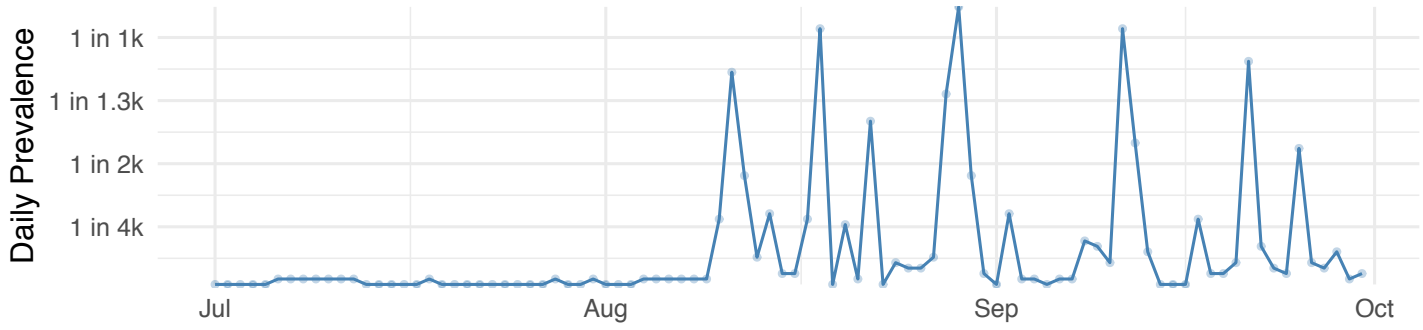


FIGURE 16: DAILY PREVALENCE OF ALINA BOTNET DETECTIONS IN Q3 2018.

To the delight of Marvel Comics fans, the HawkEye botnet forms a "bullseye" in the middle of the "bursty" section in Figure 14. This botnet was used in attacks last year to steal payments victim companies made to suppliers in a heist that netted nearly $80 million for the criminals behind it. The burst detected in Figure 16 and related spike in Figure 17 suggest a new spree in Q3. The initial attack is seen as a mass email spray coupled with automated information gathering. If something interesting is identified, the actors engage with the victim under the guise of a supplier to route payments to rogue bank accounts. Don't get caught in their crosshairs!

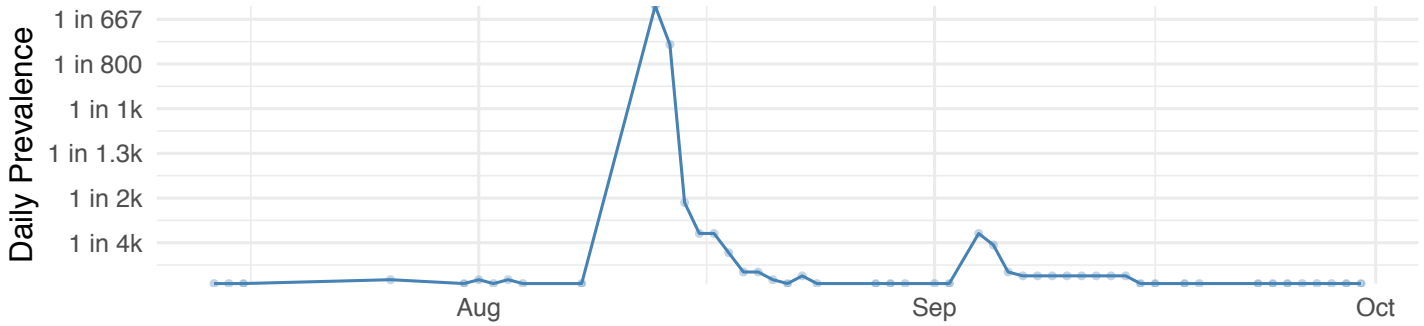


FIGURE 17: DAILY PREVALENCE OF HAWKEYE BOTNET DETECTIONS IN Q3 2018.

The Mirai and Gafgyt botnets also deserve mention, as both are back in action after receiving recent updates. These infamous botnets were discovered targeting multiple vulnerabilities in Apache Struts and Dell SonicWall network security appliances in Q3. It is unclear exactly why Mirai and Gafgyt, which traditionally focus on IoT and consumer devices, started targeting enterprise assets. Perhaps these new attack vectors are another zombie, which essentially adds more tools to the attackers' already cluttered tool belt.

OTHER BOTNETS ON OUR RADAR IN Q3 2018

Aside from the top botnets discussed above, here's a quick summary of other developments we monitored during the quarter:

- Bushido is another IoT botnet utilizing Mirai source code that brute forces common passwords on Telnet port 23 and receives commands from an IRC server, giving it a modular nature. The main functionality of Bushido is DDoS attacks. It will delete itself to stop analysis. Malware associated with this botnet was reported by 200+ organizations over the quarter, but fell largely silent after a mid-August spike.

MINI FOCUS: **THE EVOLUTION OF IoT BOTNETS**

IoT botnets rose to notoriety in September 2016 with the advent of Mirai and the 600,000 infected IoT devices under its control. Mirai's source code was released to the public the following month for unknown reasons. This has led to more powerful variants of Mirai such as Satori, JenX, OMG, and Wicked.

IoT botnets rose to notoriety in September 2016 with the advent of Mirai and the 600,000 infected IoT devices under its control.

Recent Developments

Mirai's main method of propagation was finding IoT devices and then brute forcing the target's login credentials. Over time this morphed into vulnerability exploitation of IoT devices. For example, Reaper targeted many IoT device vulnerabilities on vendors such as NETGEAR, GoAhead, Linksys, and AVTECH. It contained an LUA engine that leveraged scripts to run its exploits, making it very easy to swap exploits in and out. Nowadays it is common for IoT botnets to have multiple exploits for many IoT devices at its disposal.

Another new development in current botnets is the trend of decentralized command-and-control infrastructure via peer-to-peer (P2P) protocol communication. The exact P2P protocol used depends on the botnet, with some using existing protocols and others relying on custom-built protocols. The advantages of a decentralized command-and-control infrastructure are twofold: first, they make the botnet more resilient to takedown attempts, and second, they allow the botnets to spread far more rapidly.

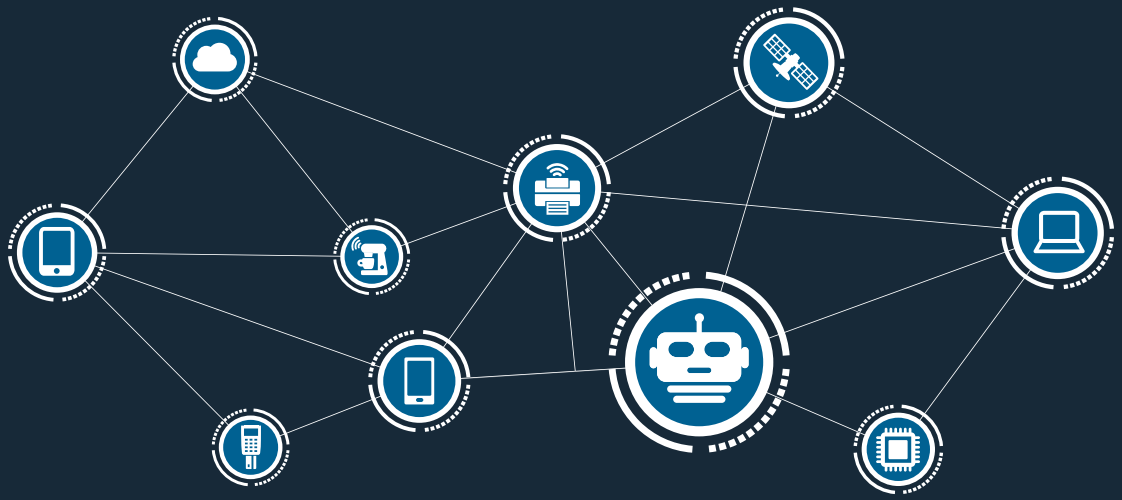
The previously mentioned variant OMG turns infected devices into proxy servers that can be rented to individuals looking for inconspicuousness via multiple proxies. IoT botnets have also begun to implant cryptojacking malware in infected IoT devices. Another risk posed by IoT botnets is the potential for infected devices to be rendered useless. This includes everything from smart TVs and coffee machines to medical devices.

An example of an IoT botnet targeting an entire country is VPNFilter and its attack on Ukraine. Devices infected with VPNFilter were laced with a kill switch that allowed the destruction of said device with a single command. Additionally, the capability for the botnet to spread via injecting malicious code into network sessions gave it the ability to infect endpoint devices.

Future Directions

IoT botnets will continue to evolve and grow. A possible avenue for this growth is the application of machine learning or data analytics to botnets, allowing it to refine itself by finding the most efficient exploits and the most vulnerable devices.

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.



SOURCES AND MEASURES

FORTINET

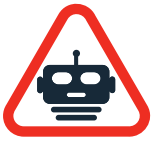
SOURCES AND MEASURES

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,[3] 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[4] 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.

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

[4] 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.

CONCLUSIONS AND RECOMMENDATIONS

FORTINET

CONCLUSIONS AND RECOMMENDATIONS

Thanks again for investing your valuable time with us again this quarter. Hopefully we've given you some useful perspectives on the global threat landscape that you can take action on in your local environment. To help with that, we'll leave you with some recommendations inspired by trends discussed in this report.

01

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.

02

If you want fuller and faster threat information than this quarterly report can supply, subscribe to our weekly Threat Briefs. It is essentially a weekly version of this report, with a more tactical focus.

03

The exploits and CVEs from Figure 5 should help answer questions like "Have we seen these alerts/vulnerabilities?" There are a lot of things that need fixing in every network, and having some direction on where to start can be a big help.

04

Several exploits targeting IoT devices topped our charts this quarter. We recommend our Learn, Segment, and Protect approach to quell the storm that seems to be brewing. 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.

05

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.

06

We showed that cryptojacking is jacking up more and more systems. If you are worried that your system might be one of 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.

07

One in four firms reported mobile malware last quarter. Unfortunately, such devices often don't have the level of control, visibility, and protection that traditional systems receive. Effective mobile security strategies must deal with this reality through mobile application controls and malware protections built into the network to cover any device anywhere.

08

Our data shows that firms typically have one or two different botnets active in their environment at any given time. Some, however, have 10 or more. And many of those frequently communicate with external hosts. Growing your capability to detect and sever those communications at key chokepoints in your network through a combination of smart tools and good intel is a solid investment.

09

In addition to remaining vigilant of new threats and vulnerabilities, don't lose sight of what's happening within your own environment. Basic cyber hygiene is perhaps the most neglected element of security today. Continually removing unnecessary services, stamping out vulnerabilities, and maintaining good order isn't the most fun or sexy part of security, but it is a critically important part.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

310149-0-0-EN November 2018