FORTINET

THREAT LANDSCAPE REPORT

Q2 2018

TABLE OF CONTENTS

Introduction and Key Findings 3

Infrastructure Trends 4

Exploit Trends 6

Mini Focus: Vulns Gone Wild 9

Malware Trends 10

Mini Focus: A Gander at GandCrab 14

Botnet Trends. 15

Mini Focus: Botnet Epidemiology 19

Conclusions and Recommendations 20

Sources and Measures 23

Q2 2018 **INTRODUCTION AND KEY FINDINGS**

It's that time again—our quarterly trek into the wilds of the cyber-threat landscape. We're glad to be your hosts on this adventure, and appreciate you coming along with us.

As the highlights to the right suggest, a lot has happened since our last outing. No single breach, event, or even theme dominated the cyber zeitgeist in Q2 2018. It featured a healthy dose of international intrigue, major disruptions, global infections, innovative malware, clever heists, and more.

Sound overwhelming? Don't despair—we're here to help. We start the journey with a quick view of application usage trends across industries. From there, we head into myriad vulnerabilities and exploits that affect those applications we use every day. Malware is the next stop on our tour, where we will see a range of threat actor capabilities on display from commoditized crimeware to custom-developed espionage kits. We then turn our attention to botnets, which—quite literally—connect all of the above together into a vast web of malicious control. Our final stop will be some recommendations from our experts on actions you can take in light of everything we've seen and learned this quarter.

Share your thoughts with us and others along the way using #FortiResearch on Twitter/ LinkedIn/Facebook.

HIGHLIGHTS FROM THE HEADLINES:

U.K. and U.S. agencies issued a joint alert on Russian-sponsored cyberattacks involving millions of devices.

All government services for the island of Sint Maarten were taken offline for a week by a cyberattack.

Details emerged around a targeted campaign using VPNFilter malware affecting a range of IT and OT devices.

A flaw was discovered in the website for the Panera Bread chain of restaurants, which may affect 37 million customers.

Meltdown and Spectre Variants 3a and 4 were discovered, extending the rash of side-channel vulnerabilities.

A Banco de Chile wiper attack was used as a smokescreen for a $10 million SWIFT heist.

In a win for the good guys, Operation WireWire led to the arrest of 74 criminals involved with global business email compromise schemes.

Q2 2018 BY THE NUMBERS:

Exploits

- 7,230 unique detections
- 811 detections per firm
- 96% saw severe exploits
- 30 zero days found by FortiGuard Labs
- 5.7% of CVEs exploited in wild

Malware

- 23,945 unique variants
- 4,856 different families
- 13 unique daily detections per firm
- 6 variants spread to ≥10% of firms
- 23.3% saw cryptojacking malware

Botnets

- 265 unique botnets detected
- 7.6 infection days per firm
- 1.8 active botnets per firm
- 10% of botnets hit >1.1% of firms
- 5% of botnets infections last >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

INFRASTRUCTURE TRENDS

FORTINET

INFRASTRUCTURE TRENDS

This is the “Threat Landscape Report,” but it is good to remind ourselves that what’s happening across the external threat environment is very much a reflection of what’s happening within our own internal environments. Because of this, we periodically include a view of infrastructure trends before digging into threat-centric updates.

	Construction	Education	Financial Svcs	Government	Healthcare	Manufacturing	Retail/Hospitality	Services	Technology	Transportation
HTTPS ratio	62.2%	65.7%	69%	64.3%	67.3%	65.7%	69.4%	63.4%	66.1%	62.6%
Daily Total apps	182	352	194	255	190	199	181	174	159	196
SaaS apps	26	51	32	70	42	44	26	35	19	31
IaaS apps	21	29	25	38	31	33	24	21	15	21
RAS apps	4	5	4	6	5	4	4	3	3	4
Proxy apps	4	11	3	6	4	5	4	3	2	4
P2P apps	<1	4	<1	2	1	1	1	1	<1	1
Social apps	14	26	14	18	14	15	14	14	11	14
Streaming apps	12	33	12	20	14	15	10	12	9	14
Gaming apps	2	12	2	4	1	2	2	2	1	2
Daily malicious websites	<1	2	1	2	1	<1	1	<1	<1	1

FIGURE 1: APPLICATION USAGE STATISTICS FOR TOP INDUSTRIES. NUMBERS REPRESENT THE MEDIAN VALUE.

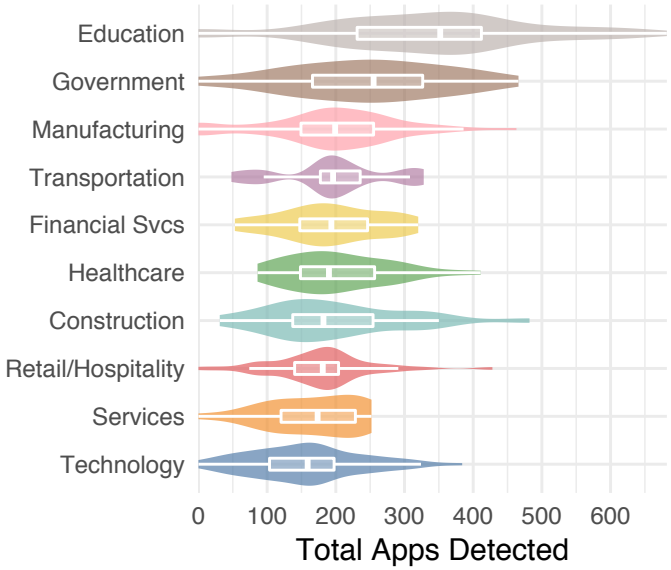


FIGURE 2: VARIATION IN APPLICATION COUNT ACROSS INDUSTRIES.

In this edition, we’ve elected to present usage statistics for various types of applications broken out by industry. Figure 1 compares the median value (number of apps in most cases) for each item, but it should be noted that a wide variation exists among organizations in the same industry. Figure 2 illustrates this well; the median app count (middle line in the box plot) differs, but overall distributions for firms within industries overlap considerably. Some technology organizations (smallest median) use more apps than some in the education sector (largest median).

We can’t definitively determine from the data why differences seen in Figures 1 and 2 exist, but we suspect, for instance, that students, labs, instructional technology, and less-stringent usage policies have a lot to do with the higher across-the-board counts for educational institutions. Tech and construction firms run comparatively sparse application environments, which undoubtedly has a lot to do with business models and company size.

The number of observations and possible explanations from Figures 1 and 2 are nearly limitless, so we will simply offer it up for consideration as you see fit. But if you do want to swap theories, we’ve no doubt that your friendly Fortinet representative will lend a willing ear.

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:

- 7,230 unique detections
- 811 detections per firm
- 96% saw severe exploits
- Microsoft is #1 exploit target
- Schneider Electric is #1 ICS target
- 30 zero days found by FortiGuard Labs

There are many different ways to study exploits within our dataset. We often show the top signatures, which has the benefit of specificity but the challenge of readability. After all, not everyone speaks the native language of our FortiGuard IPS sensors. As a compromise, we sometimes show different categorizations or abstractions of exploits. Figure 3 gives two such examples based on the prefix of the signature, which corresponds to the targeted technology or service. The left column lists the most widely exploited technologies overall, while the right filters that down exclusively to industrial control systems (ICS).

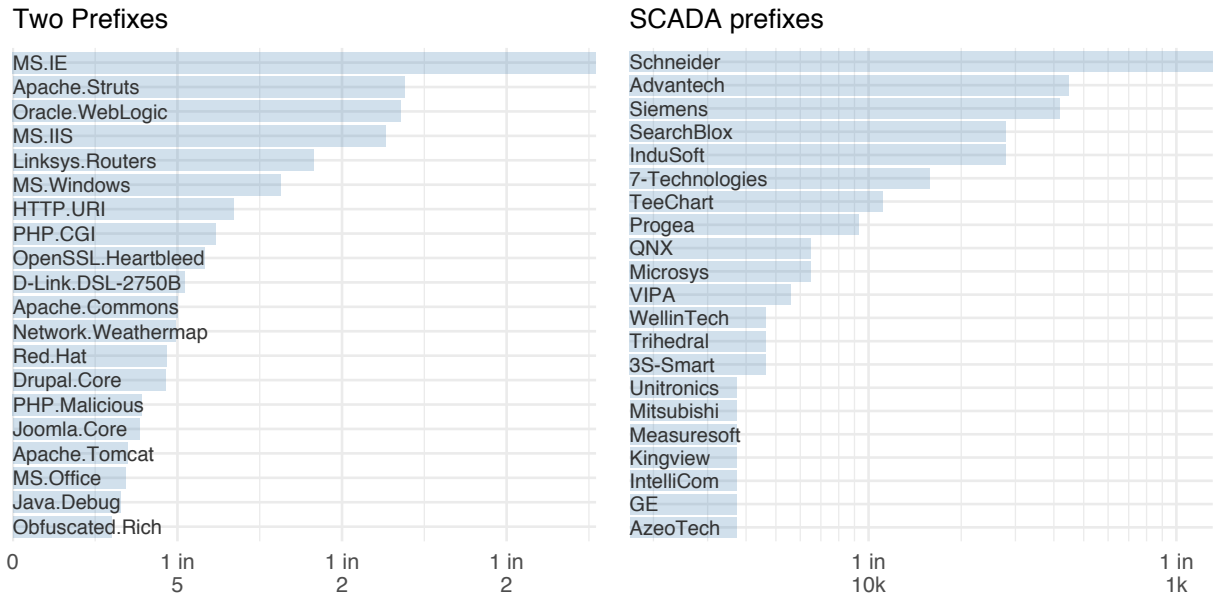


FIGURE 3: TOP TECHNOLOGIES TARGETED BY EXPLOITS.

The first column in Figure 3 is like an "Internet's Most Wanted" board of notorious exploits. There are no noteworthy new developments related to Apache Struts (of Equifax fame) and Heartbleed—and they're covered extensively in prior reports—so we'll skip the commentary on those for now. Their presence in this list is a sufficient reminder that criminals are still actively trolling for an unwary catch.

The Oracle exploit relates to CVE-2017-3506, a flaw in the Oracle WebLogic Server component of Oracle Fusion Middleware. It allows an unauthenticated attacker with network access via HTTP to compromise the server, resulting in unauthorized access to or modification of critical data. We've observed this being leveraged to run cryptojacking malware of late.

Content management platform, Drupal, shot up the list last quarter on the back of the so-called "Drupalgeddon 2" vulnerability. It enables remote code execution on vulnerable systems due to insufficient input validation when parsing a crafted HTTP request. Once working exploit code was developed, the popularity of Drupal and ease of exploitation combined to make this irresistible to attackers. As a result, we registered a thousandfold increase in detections over a 24-hour period in early May. Many of these attacks targeted Internet of Things (IoT) devices and served as the base point for various cryptocurrency mining operations.

WAIT—DID YOU SAY CRYPTOJACKING WITH IoT DEVICES?

Yes. That is now a "Thing." Criminals apparently aren't satisfied with the supply of vulnerable servers and PCs to mine their favorite cryptocurrency, and so have turned to another rich source of computational horsepower—IoT devices.

Media devices are an especially hot commodity due to their use of powerful GPUs to decode and transcode content in high-resolution formats. Attackers take advantage of this by loading malware that can mine continually because the devices remain on and connected. Making matters worse, the interface for many of these devices acts as a modified web browser, with all the vulnerabilities that come with it. We've already caught several of these in our honeypots and expect this to become a trend in the near future.

The inclusion of exploits targeting Linksys and D-Link points to the ongoing "link" between malicious activity and IoT devices. This is no longer hot news, but it's not fake news either. Criminals have not abandoned their plans of amassing armies of compromised things around the world for sundry illicit schemes. FortiGuard Labs is doing its part to fight back, with one of the exploits bumping D-Link up the list, being an unauthenticated buffer overflow vulnerability found by our researchers in 2017. The patch was released in March of this year, just before the exploit jumped into our top five detections in April.

Moving over to the right side of Figure 3, we find a record of the most-attacked SCADA manufacturers. Before perusing the names on the list, take notice of the scale at the bottom. The prevalence values are far, far lower than those for general exploits. However, those values simply reflect the fact that far fewer organizations run SCADA systems in their environment than, for instance, Apache web servers. Those that do understand those small numbers are a really big deal.

Returning to the list itself, Schneider Electric sits on top with a comfortable lead. The most prevalent exploit attempt by far for the quarter involved backdoor access in Schneider's Quantum Ethernet Module due to a default factory account with a hard-coded password. Remote attackers can obtain access to the device with this account through FTP access.

Attempts to exploit a buffer overflow vulnerability in Siemens Automation License Manager fall next on the list, which was followed closely by another overflow condition in Advantech WebAccess. Both result from improper sanitization of inputs and allow execution of arbitrary code. Definitely not something you want happening in your operational technology environment.

REMEMBERING THE GOOD "O" DAYS

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 Q2 2018, our researchers disclosed 30 vulnerabilities affecting a range of products. Vendors for those products are listed below, along with a count of vulnerabilities found and a link to vulnerabilities we've discovered for each vendor.

Vendor	Vulns	Vendor	Vulns
Adobe	2	Joomla	1
Box	1	Microsoft	5
Cisco	3	Naver	2
CrashPlan	1	Recon Instruments	1
D-Link	2	Shenzhen Lingan Intelligent Technology	1
FooLabs	2	Smarter	1
Foxit Software	1	Telesquare	1
Free Software Foundation	1	Tresorit	1
Golden Frog	1	Zabbix	1
Google	1	Zimbra	1

FIGURE 4: VENDORS ASSOCIATED WITH ZERO-DAY VULNERABILITIES DISCOVERED BY FORTIGUARD LABS IN Q2 2018.

MINI FOCUS: **VULNS GONE WILD**

Another interesting way to study exploits is through the vulnerabilities they target. We track this important association in our Threat Encyclopedia. Joining these two bits of information enables us to measure which *known* vulnerabilities are being attacked in the wild at any given time.

Of the 103,786 vulnerabilities published on the CVE List since it began, 5,898 (5.7%) were exploited in the wild during Q2 2018, according to our global sensors.

On that topic, Kenna Security and the Cyentia Institute recently published a report stating that roughly 2% of all published CVEs have been exploited in the wild. Some suggested that estimate was on the low side, so we wanted to duplicate their analysis using our dataset of exploit detections. Of the 103,786[1] vulnerabilities published on the CVE List[2] since it began, 5,898 (5.7%) were exploited in the wild during Q2 2018, according to our global sensors.[3]

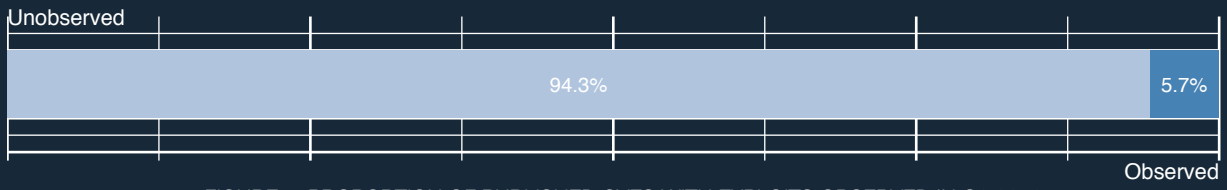


FIGURE 5: PROPORTION OF PUBLISHED CVES WITH EXPLOITS OBSERVED IN Q2 2018.

While our statistic is nearly 3x higher than that of the Kenna-Cyentia report—and likely understated due to being only a quarter's worth of observations—it agrees with the overall conclusion that a small minority of published vulnerabilities are exploited in the wild. That is important because it dramatically affects remediation decisions and how we make them. If the vast majority won't be exploited, then "fixing everything" is not only impossible but extremely inefficient. Knowledge of what is actually exploited, then, becomes very valuable.

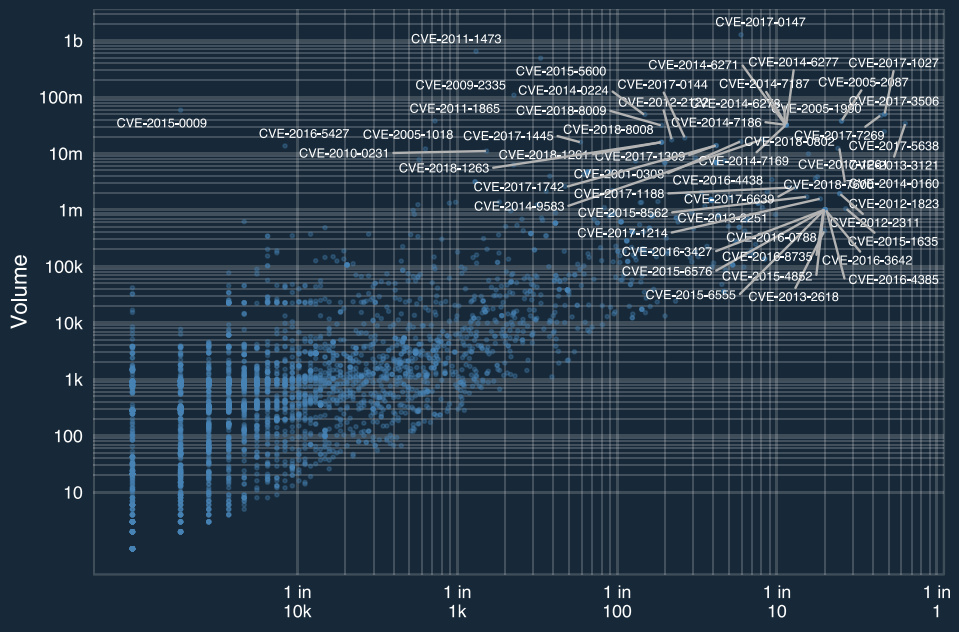


FIGURE 6: VULNERABILITIES EXPLOITED IN THE WILD DURING Q2 2018.

Since we consider it our job to share valuable information, Figure 6 plots CVEs based on the prevalence and volume of related exploit detections. If you think of all those dots as a "should I remediate that?" decision, you get a sense for the scale of the challenge. Even more so when you consider that Figure 6 includes only a subset of the subset for which we observed exploit attempts in Q2. Most CVEs in the upper right relate to exploits discussed earlier, but feel free to head over to the CVE List search page to look up anything that catches your attention.

[1] This number includes CVE List entries with a status of "Published" or "Disputed," which mirrors the methodology used by Kenna Security.

[2] We are aware that the CVE List is not a comprehensive listing of all known vulnerabilities. We have based our analysis on CVEs because they are publicly available and because this mirrors the methodology used by Kenna Security.

[3] In case you're curious, only 4 out of 4,122 CVEs published in Q2 were exploited in Q2 (0.1%).

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:

- 23,945 unique variants
- 4,856 different families
- 13 unique daily detections per firm
- 6 variants spread to ≥10% of firms
- 23.3% saw cryptojacking malware

After The Great Cryptojacking "Gold Rush" of late 2017 and early 2018, the malware landscape looks to have settled back into more familiar form during Q2. Cryptojacking activity continued to increase globally, but not relative to the growing volume of malware overall. As with any market, such fluctuations may be attributable to the forces of supply and demand.

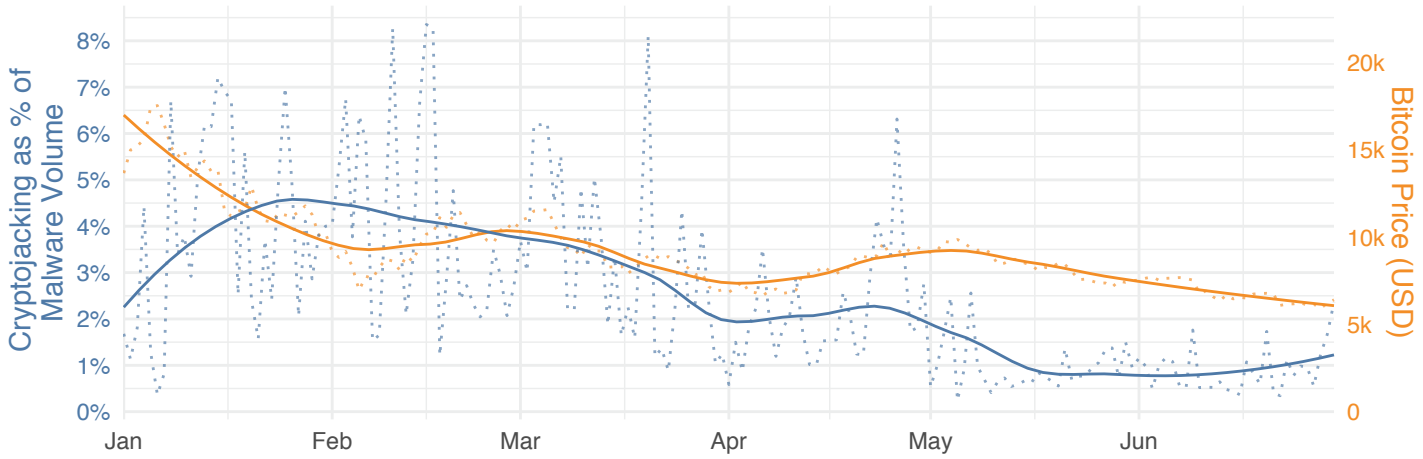


FIGURE 7: CRYPTOJACKING MALWARE VOLUME (BLUE) AND BITCOIN PRICE (ORANGE).

To test that hypothesis, Figure 7 compares the relative volume of cryptojacking malware with the price of bitcoin for the first six months of 2018. If you thought the price of bitcoin was volatile, check out that dashed blue line for cryptojacking! The smoothed trend lines, however, show a similar declining behavior over time[4]. We also compared the price of another popular cryptocurrency, Monero, and found it nearly identical to the pattern exhibited by bitcoin.[5] Thus, we infer a moderate positive correlation between the market price of cryptocurrencies and malware designed to illicitly mine those currencies.

With that out of the way, we'll widen the aperture to examine the broader malware landscape. Figure 8 captures that picture for us, plotting the most active malware families over the quarter based on prevalence and volume.

[4] Pearson's correlation coefficient for the two trend lines is 0.4.

[5] Pearson's correlation coefficient for pricing fluctuations in bitcoin and Monero is 0.95.

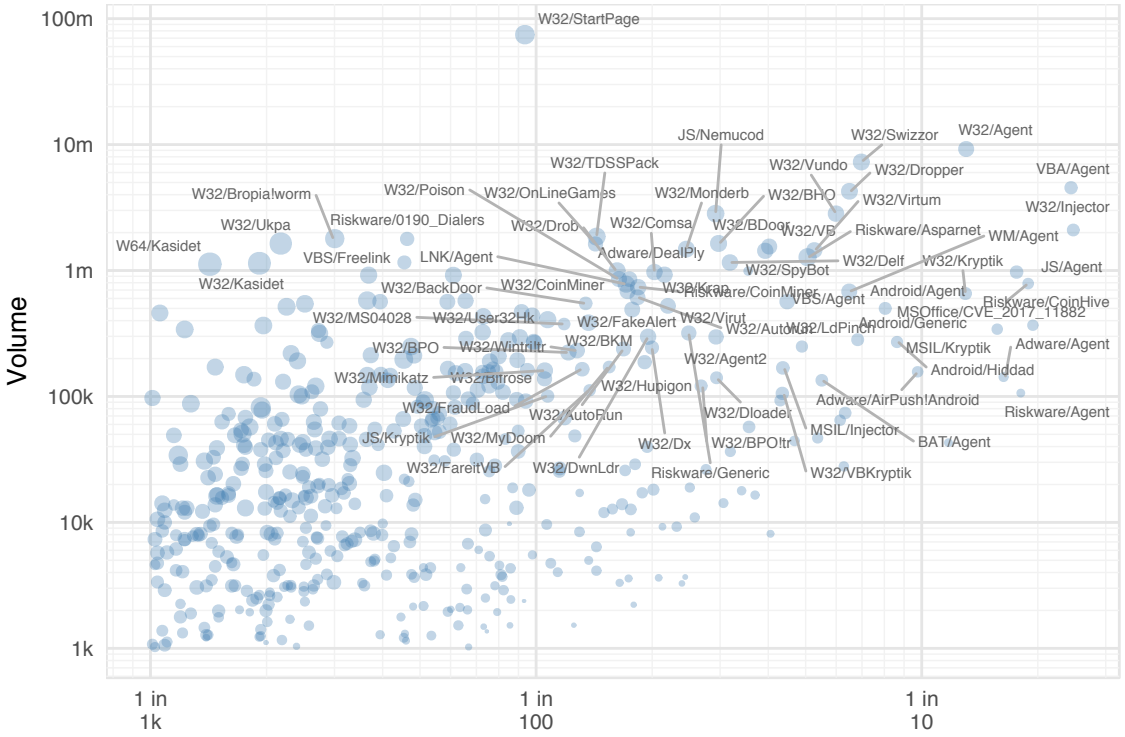


FIGURE 8: TOP MALWARE FAMILIES IN Q2 2018.

Far above the throng on the volume scale in Figure 8 stands W32/StartPage. The most boisterous member of that family over the quarter was a generic detection for a Trojan covering a range of malicious behaviors. Most samples falling under this detection are Browser Helper Objects (BHOs), many of which are designed to alter the user's browser start page.

MALWARE IN THE AGE OF AGILE DEVELOPMENT

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 that was recently analyzed by FortiGuard Labs.

We noticed that when a <8hex-chars>.lock file in the system's COMMON APPDATA folder is present, the files will not be locked. This usually occurs after the malware determines the keyboard layout is in the Russian language, along with other techniques to determine computers in Russian-speaking countries. We speculate in our blog that adding this file could be a temporary solution. Based on our analysis, industry researchers created a tool that prevents files from being encrypted by the ransomware. Unfortunately, GandCrab 4.1.2 was released a day or two later, rendering the lock file useless. If only we could infiltrate their scrums...

If there was such a thing as a "Hardest Working Malware Family" award for Q2, it would have to go to W32/Injector. It nabbed four of the top five malware variant spots during the week ending May 11, and captured the lead position on the prevalence scale for the entire quarter. Most of the offending variants in that family relate to Loki and Fareit, a class of information-stealing Trojans capable of harvesting credentials from browsers, FTP clients, and email clients as well as bitcoin wallets. Our sensors picked up samples of these infostealers all over the world, as evidenced in Figure 9. Raw detection volume was highest in India and Singapore, but Israel and Indonesia led proportionally.

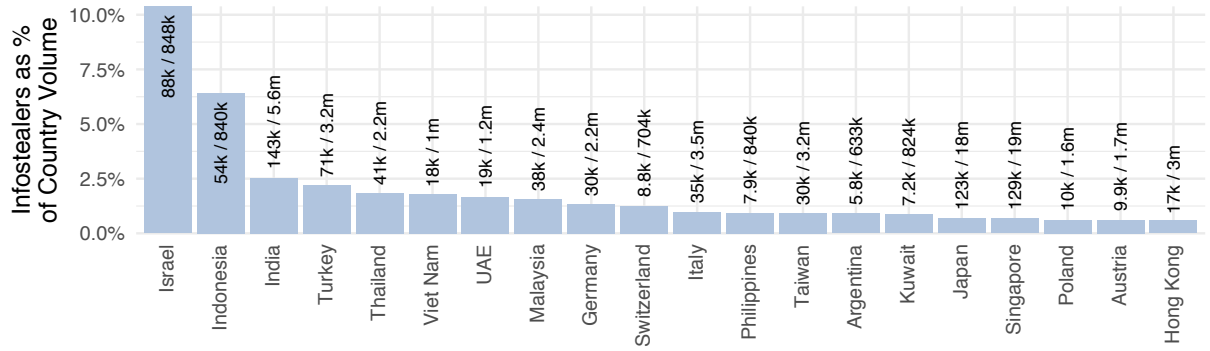


FIGURE 9: RELATIVE VOLUME OF LOKI AND FAREIT INFOSTEALERS BY COUNTRY.

While on the topic of Loki and Fareit, we'll go ahead and address another prominent family in Figure 8, MSOffice/CVE_2017_11882. The .B!exploit variant is the most widespread and has been serving as a downloader of Loki for over a year now. We observed the *.A!exploit variant*—which is still quite prevalent—distributing a recent variant of Remcos RAT (version "2.0.4 Pro"). Like most RATs, it is able to control the victim's PC after infection.

If you scan the upper right corner of Figure 8, one word stands out—"Agent." The W32/Agent, VBA/Agent, and JS/Agent all feature prominently among leading malware families. Another cousin, PowerShell/Agent, is not labeled but did make our list of "major movers" for the quarter. ELF/Agent is also not shown, but encompasses samples associated with the VPNFilter botnet (see coverage in the Botnet Trends section). "Agent" families are generic detections in our FortiGuard devices, covering a wide range of threats, but an overarching theme emerged among leading X/Agent samples observed in Q2—PowerShell.

PowerShell is a sort of "Dr. Jekyll and Mr. Hyde" of administrative tools. By day, it is a legitimate command-line shell and scripting language popularly used by whitehats everywhere to automate administration of operating systems, processes, and applications. By night, however, it is often wielded by those who seek to corrupt its power for less-honorable purposes. It is very common for evil macros to call PowerShell in order to download additional malicious files to the system. But it doesn't stop there; PowerShell is increasingly used by adversaries to escalate privileges and move laterally inside networks. The Thrip ATP Campaign—for which we received updated intelligence through our partnership with the Cyber Threat Alliance—offers an excellent example for those who want to see the darker side of PowerShell in action.

Speaking of Thrip, the threat actor offers a good segue back into some of the non-PowerShell variants in the extended Agent family. Several W32/Agent samples tie back to Thrip, as well as Sofacy (aka APT28, Fancy Bear), Hacking Team (aka Grey Heron), and Hidden Cobra (aka Lazarus Group). The MuddyWater APT group makes heavy use of MS Word documents containing malicious macros and VBScripts, several of which are currently detected as VBA/Agent variants. Like we said, Agent is quite the diverse family. Most of these are fairly low-level threats, but that is expected for targeted attacks.

MINI FOCUS: **A GANDER AT GANDCRAB**

Many samples detected under the W32/Kryptik malware family back in Figure 8 relate to the GandCrab ransomware. Over the last several months, it has risen through the ransomware ranks to become one of the most—if not the most—impactful threats of its type. Major reasons for its success tie back to its innovative development, collection, and distribution methods.

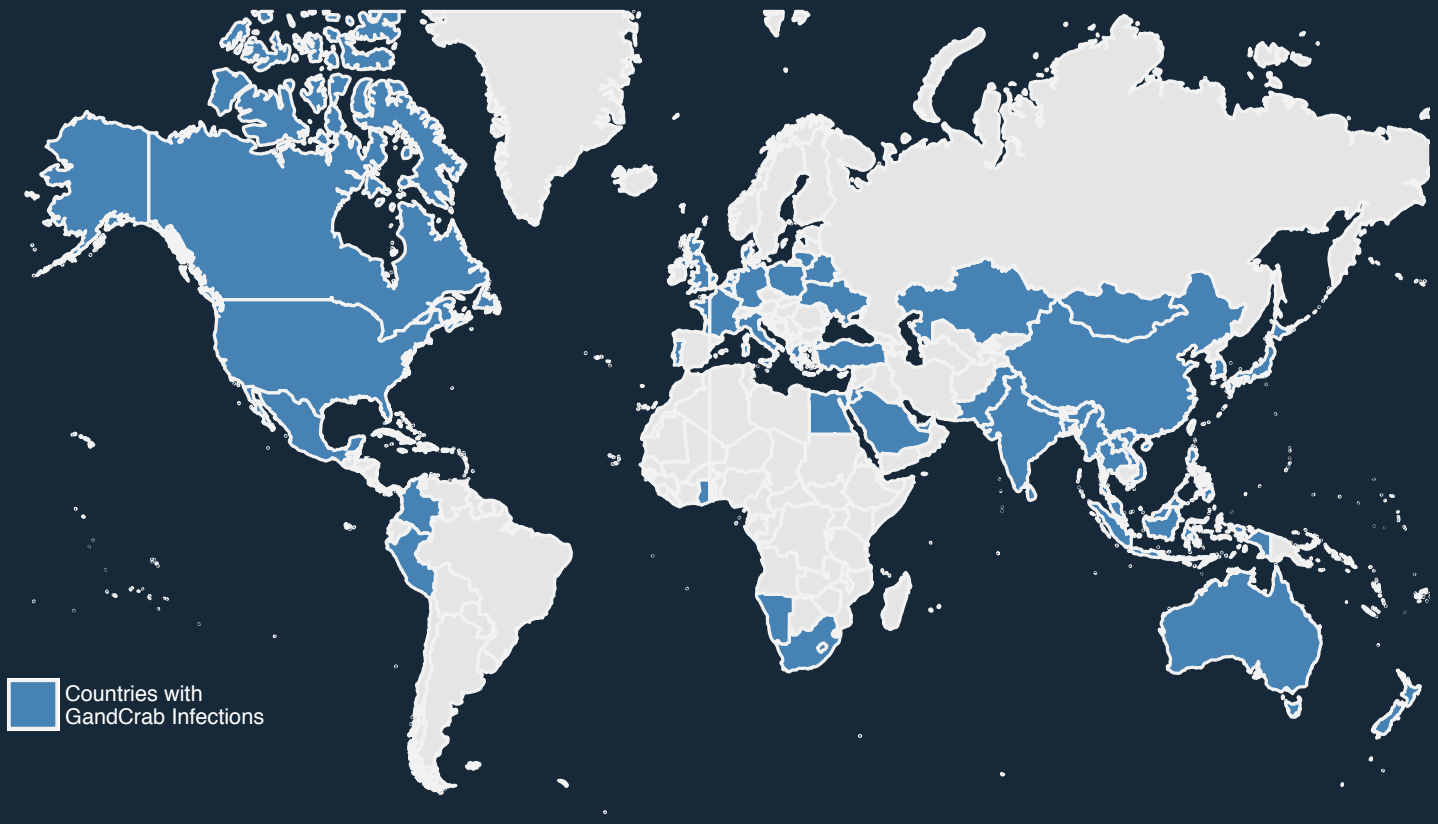
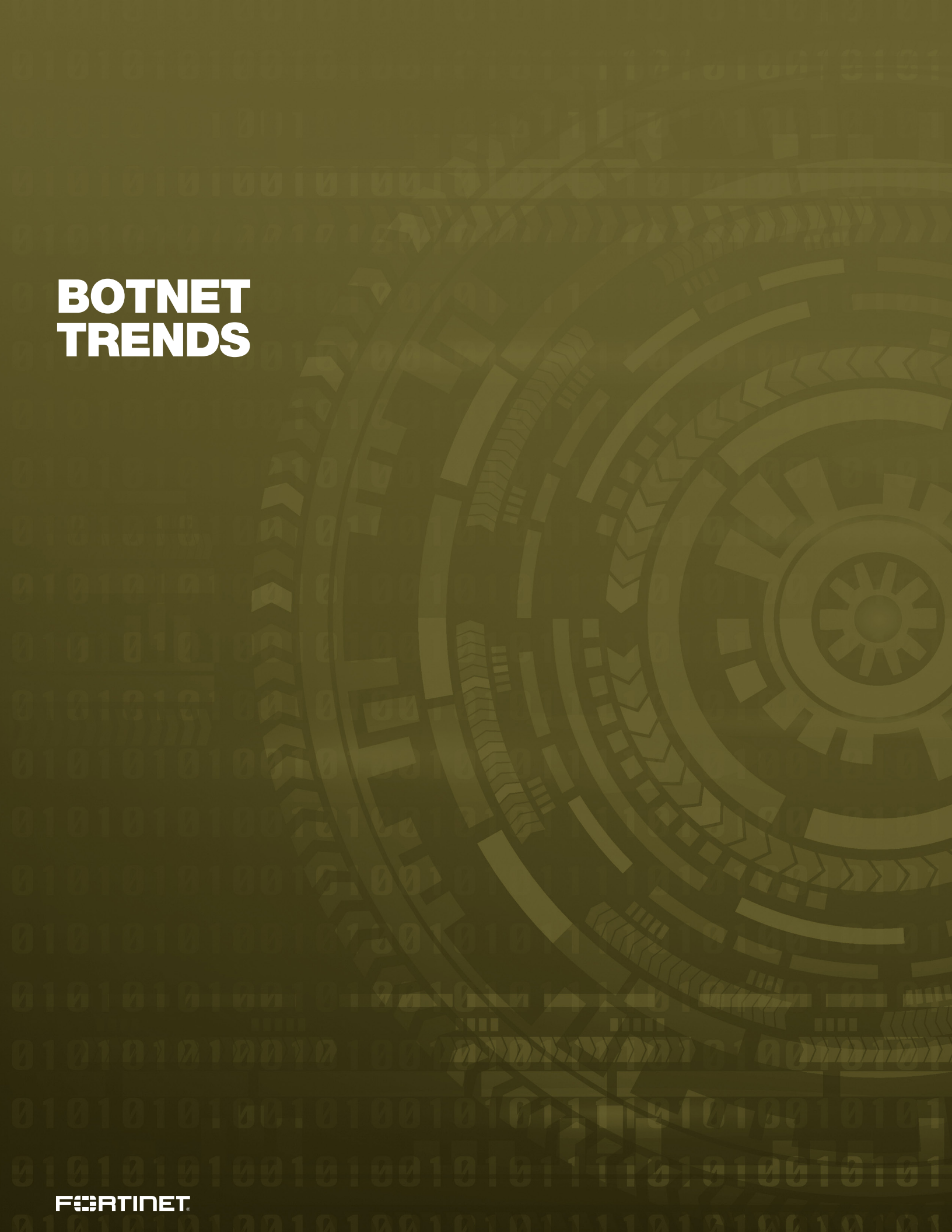


FIGURE 10: GLOBAL DISTRIBUTION OF GANDCRAB.

The actors behind GandCrab are 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.

GandCrab 2.x versions were most prevalent during Q2, but by the quarter's close v3 was in the wild and the v4 series would follow in early July. This is definitely a threat we are actively tracking, and you can keep up with what we're learning about GandCrab from our blog.

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:

- 265 unique botnets detected
- 7.6 infection days per firm
- 1.8 active botnets per firm
- 10% of botnets hit >1.1% of firms
- 57% of botnet infections last 1 day
- 5% of botnet infections last >1 week

Botnet activity for Q2 is plotted in Figure 11 according to overall prevalence and volume. The leaders' quadrant in the top right shows the same cast of characters from previous quarters. This is not terribly surprising, as the number of active botnets observed (265) is far lower than, for instance, malware variants this quarter (23,945). Good botnets are custom built to last.

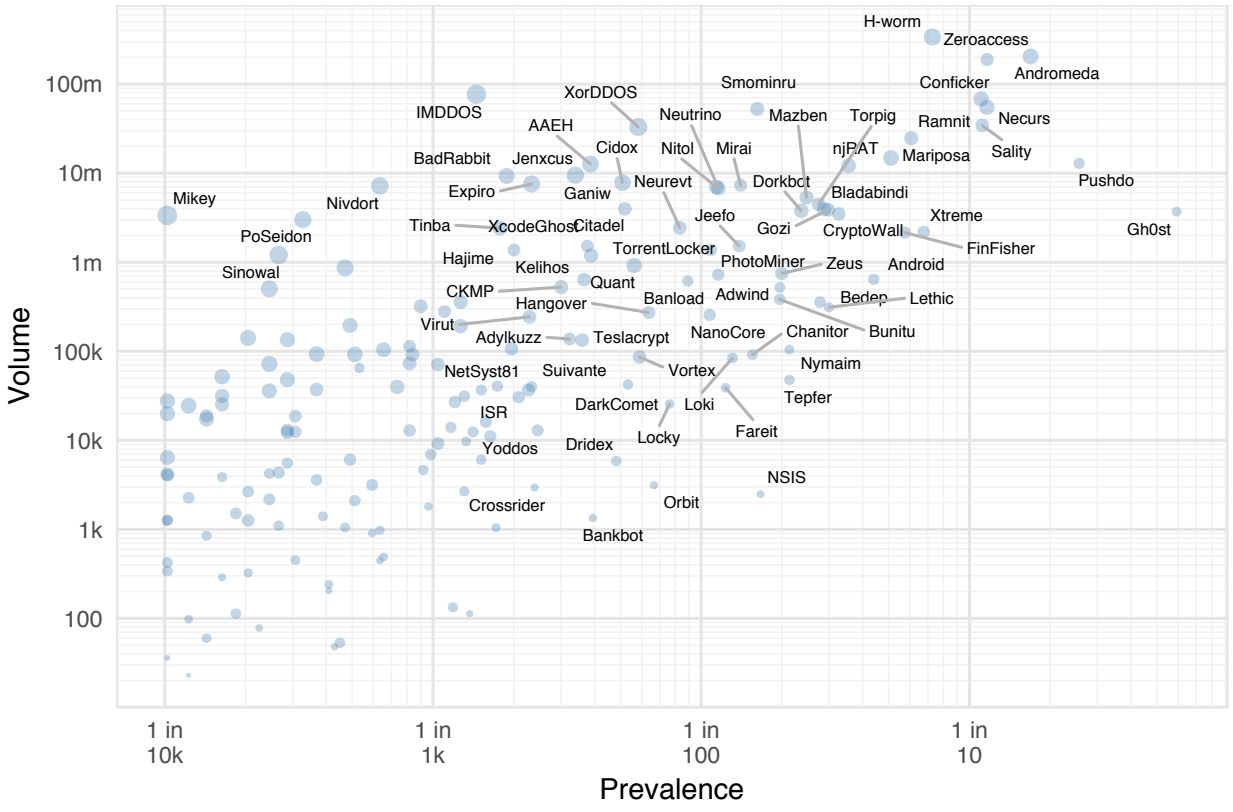


FIGURE 11: TOP BOTNETS FOR Q2 2018.

Smominru is a notable addition to the upper end of the volume axis in Figure 11. It caught our notice back in February, when it was being spread via the infamous EternalBlue exploit (CVE-2017-0144). Smominru is a Monero mining malware/botnet that targets the Windows platform. It contacts C&C servers via HTTP requests and allows remote attackers to issue commands to download and install additional files.

OLDIES 'BOT GOODIES

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 many hosts are still infected.
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. **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.
6. **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.
7. **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.

On the other end of the volume axis, BankBot would not garner much attention based on its overall standing alone. But a new member of the BankBot family—Anubis—was on the move in Q2. As the name suggests, BankBot is a family of banking Trojans targeting Android devices that surfaced in the second half of 2016. The main goal of this malware is to steal credentials from the victim's device. This new Anubis variant introduces several innovations to the family, as it is capable of performing ransomware, keylogger, RAT functions, SMS interception, lock screen, and call forwarding. In the recent campaign, we identified new C&C hosts joining the botnet containing suspicious names such as locker, keylogger, and ratgate.

Another botnet deserving a callout is Loki. Like BankBot, it is easily lost in the herd (it's near the intersection of the 1/100 prevalence and 100K volume gridlines in Figure 11). This information-stealing botnet tied to the malware of the same name was among the top gainers in Q2 and crossed 1% on the prevalence scale. That feat might not seem remarkable in its own right, but it's actually relatively uncommon among botnets. Loki's relationship to the surge in infostealers we discussed in the Malware Trends section makes it even more noteworthy.

The Mirai botnet doesn't fall on the bleeding edge of Figure 11, but it undoubtedly warrants mention for its edgy behavior in Q2. Since the release of the source code two years ago, Mirai variants land on our radar with increasing regularity. Some of those made significant modifications, such as adding the capability to turn infected devices into swarms of malware proxies and cryptominers. Others integrated Mirai code with multiple exploits targeting known and unknown vulnerabilities. A new variant discovered by FortiGuard Labs, which we dub WICKED, adds at least three exploits to its arsenal to target unpatched IoT devices. You can read more about WICKED on our blog.

	Africa	Asia	Europe	Latin America	Middle East	Northern America	Oceania	Overall
Andromeda	26.5%	24.3%	3.3%	20.3%	24.1%	10.8%	7.5%	14.2%
H-worm	13.8%	7.4%	2.0%	15.1%	8.4%	4.6%	3.1%	5.9%
Ramnit	10.07%	9.83%	1.50%	3.79%	8.53%	3.24%	2.97%	4.95%
Lethic	4.69%	4.49%	0.62%	3.27%	3.53%	1.64%	1.95%	2.42%
Mazben	3.28%	3.67%	0.65%	2.19%	2.89%	1.50%	0.68%	1.97%
Dorkbot	3.19%	4.11%	0.52%	1.92%	2.18%	1.05%	1.78%	1.87%
Nymaim	0.81%	4.39%	0.93%	0.38%	0.50%	0.91%	3.06%	1.66%
NSIS	2.47%	1.85%	1.16%	3.45%	1.16%	0.48%	0.59%	1.27%
Jeefo	1.66%	2.11%	0.35%	1.29%	1.99%	0.72%	0.59%	1.11%
Loki	1.70%	1.59%	1.16%	0.65%	2.20%	0.50%	0.34%	1.01%
Fareit	1.70%	1.49%	0.88%	0.93%	2.68%	0.37%	0.34%	0.95%
Neutrino	1.70%	1.28%	0.32%	2.05%	1.07%	0.73%	0.25%	0.90%
PhotoMiner	5.05%	1.96%	0.19%	0.11%	0.21%	0.60%	1.36%	0.93%
Nitol	0.61%	2.31%	0.36%	0.50%	0.85%	0.48%	0.34%	0.90%
NanoCore	1.33%	1.81%	0.46%	0.25%	1.35%	0.51%	0.59%	0.84%

FIGURE 12: BOTNETS WITH HIGHEST VARIATION IN PREVALENCE ACROSS REGIONS.

A final botnet that must be highlighted before moving on is VPNFilter, another threat that deserves a hat tip to our partnership in the Cyber Threat Alliance. This is an advanced nation-state-sponsored attack that targets SCADA/ICS environments by monitoring Modbus SCADA protocols. What makes this VPNFilter particularly dangerous is that it not only performs data exfiltration but can also render devices completely inoperable, either individually or as a group. Activity from the campaign was initially seen in Ukraine, but data indicates devices in over 100 countries are being scanned. More updates on VPNFilter are available on our blog.

Figure 12 offers a regional slant on botnets in Q2. Rather than simply listing the most common botnets regionally as we often do, we wanted to identify which ones showed the highest degree of regional variation. Long story short, we did this by calculating and then summing the differences between the overall (global) and regional prevalence values for each botnet.

Notice how certain regional differences and patterns bubble up using this method. Prevalence for the Andromeda botnet in Africa, Asia, and the Middle East is 8x that of Europe. That fact is even more interesting when one remembers that Andromeda was the target of a takedown operation in late 2017, which was led by a European law enforcement agency. It's clear that the process of cleaning up infected endpoints is not progressing at the same rate everywhere.

Aside from variation among specific botnets, notice how prevalence in Europe, North America, and Oceania usually (but not always) falls below other regions. This doesn't imply those regions are more immune to botnets, but it does suggest the general maturity of response and remediation capabilities may differ among them. As with the spread of diseases through human populations around the globe, there are many interrelated factors at play. And on that note, let's focus a bit on facts and figures about botnet epidemiology.

MINI FOCUS: **BOTNET EPIDEMIOLOGY**

Statements like the one we made earlier about it being relatively uncommon for the Loki botnet to have crossed the 1% line for prevalence are based upon baselines we've established over time. According to Figure 13, for instance, only the upper 10% of botnets ever spread beyond 1.1% of firms in our dataset. The median prevalence among all botnets is a perhaps surprisingly low 0.03% (1 in 3.5k firms).

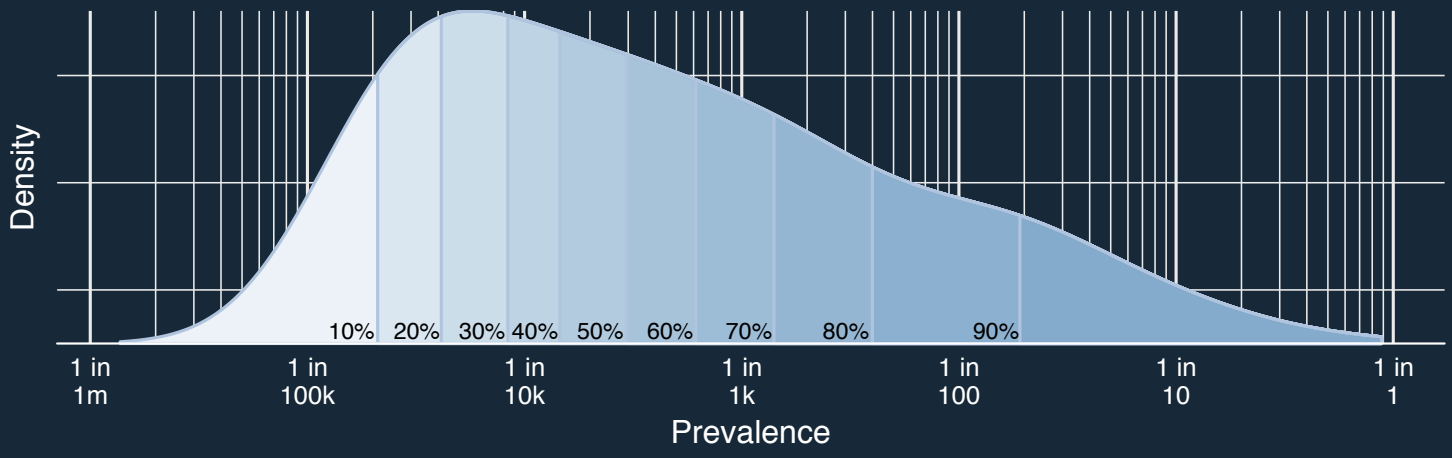


FIGURE 13: DISTRIBUTION OF BOTNET PREVALENCE.

What does one do with that statistic? Well, aside from impressing friends with your breadth of tech trivia during the next game night, data points like this are actually useful for developing an understanding of the threat landscape. In the field of epidemiology, for example, statistics relative to the spread of diseases, infection timelines, mortality rates, etc., are all important measures for researchers looking to combat those threats. We believe the same is true for threats in our field.

We've presented some of these statistics separately in past Threat Landscape Reports, but sometimes it helps to pull it all together for review. With that goal in mind, we present the table below summarizing interesting facts about botnet epidemiology.

A few stats on botnet epidemiology:		
50% of botnets infect less than 0.03% of firms. 15% of botnets infect at least 1% of firms.	45% of firms report no more than 1 botnet infection. 4% of firms report 10 or more infections.	57% of botnet infections last 1 day. 5% of botnet infections last more than 1 week.

CONCLUSIONS AND RECOMMENDATIONS

CONCLUSIONS AND RECOMMENDATIONS

We hope this brief excursion has given you some useful insights into the cyber-threat landscape in the second quarter of 2018. If you have questions about anything covered in this report, our experts are ready and willing to field them. Below you'll find a recap of findings along with some recommendations that should help make the information we've shared in these pages more actionable. Thank you for spending your valuable time with us again.

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

The more eyes you have looking at threats, the better off you'll be. This is why we co-founded the Cyber Threat Alliance, and the fruit of that partnership shows in this report. Security vendors sharing threat information amongst each other to make our respective customers more secure is a win for everyone involved. Be wary of intel providers who assert they know everything in isolation—they don't. Nobody does.

03

If you need more information—or want it faster—subscribe to our weekly Threat Briefs. If that's still not enough, consider our **Threat Intelligence Service**, which provides daily updates on important and trending threats.

04

Cryptojacking on IoT devices is a growing trend. 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

Most disclosed vulnerabilities are never exploited. But that doesn't at all imply you should ignore them. Much to the contrary, we know that many breaches exploit known vulnerabilities, making it even more important to leverage reports like this to help prioritize which ones warrant remediation now and which can be safely delayed.

06

The price of cryptocurrencies correlates moderately with cryptojacking. "Follow the money" is a tried-and-true strategy for understanding and uncovering criminal schemes. It shouldn't be a surprise that we're seeing a relationship between the rise in cryptojacking malware and the rise of cryptocurrencies. Thus, it's worth keeping tabs on that and other above-ground market factors that may indicate underground trends.

07

PowerShell is a tool for good, but can be used for evil. Because of that, organizations should make sure they track usage of PowerShell—and other administrative tools—so they can distinguish legitimate from malicious use. Larger enterprises may turn to User and Entity Behavior Analytics (UEBA) tools to help build a baseline for anomaly detection.

08

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.

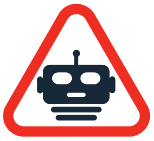
SOURCES AND MEASURES

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,[6] 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[7] 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.

[6] Source: IDC Worldwide Security Appliances Tracker, April 2017 (based on annual unit shipments)

[7] 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.

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

258263-0-A-EN August 02, 2018