FORTINET

THREAT LANDSCAPE REPORT

Q2 2017

TABLE OF CONTENTS

INTRODUCTION

Q2 2017 began normally enough, but then a Mayday call in the form of the WannaCry ransomware sounded across the world to ensure the quarter would be anything but normal.

WannaCry lit up our sensors in mid-May at a peak rate near 25 million hits a day for the DoublePulsar tool used as the primary vector of attack. The EternalBlue exploit leveraged by the worm spiked to over 7 million attempts picked up by FortiGuard sensors before trailing off after the "kill switch" was flipped. But as its name implies, EternalBlue wasn't done; it was resurrected by NotPetya in late June along with another SMB vulnerability coined EternalRomance. Its love fizzled by Q2's close and we hope it won't be rekindled. We've laid out all the key events in one visualization (Figure 12) for you, along with some key lessons.

While WannaCry and NotPetya were generating headaches and headlines, the rest of the cyber criminal world kept at its old ways. That story may have been lost in the din, but we've preserved it for posterity within the numbers and narratives recounted in these pages. We also have some very interesting exploratory analysis to share, which measures how a firm's infrastructure and application usage contributes to malware and botnet infections.

We'll start with some of the highlights from our Q2 collections and get into the details after that.

Q2 2017 by the Numbers

Exploits

- 184 billion exploit detections
- 1.8 billion average daily volume
- 6,298 unique exploit detections
- 69% of firms saw severe exploits

Malware

- 62 million malware detections
- 677,000 average daily volume
- 16,582 variants in 2,534 families
- 18% of firms saw mobile malware

Botnets

- 2.9 billion botnet detections
- 32 million average daily volume
- 243 unique botnets detected
- 993 daily communications per firm

KEY FINDINGS

MORE ENCRYPTED RECORDS. We saw a second straight record high for encrypted communications on the web. The percentage of HTTPS traffic increased its majority hold over HTTP to 57%. We pay close attention to this trend because threats are known to use encrypted comms for cover.

DON'T GIVE ME SaaS. Continuing a downward trend for 2017, the number of SaaS applications detected per firm hit its lowest mark ever in Q2. That's probably due to consolidation of software/subscriptions as well as growing usage of cloud access security brokers (CASBs).

A LIBERAL EDUCATION. Education institutions posted the highest marks for infrastructure and application usage in almost every category. The energy sector exhibited the most conservative approach, with all others falling somewhere in between.

OLDIES BUT GOODIES. A full 90% of organizations recorded exploits for vulnerabilities that were three or more years old. Even 10+ years after a flaw's release, 60% of firms still see related attacks.

WEEKEND WARRIORS. Nearly 44% of all exploit attempts occurred on either Saturday or Sunday, and the average daily volume on weekends was twice that of weekdays. Is nothing sacred?!

WHERE THE WILD THINGS ARE? The overall volume of exploits targeting the Internet of Things (IoT) was consistent with last quarter and we saw no major movements among any of the common device categories. The height of activity was Q4 2016—will Q3 return to those wilder days?

THAT'S SUCH A DOWNER. The most common functionality among top malware families is downloading/uploading files, followed by dropping other malware onto the infected system. This technique helps slip innocuous files through now in order to deliver malicious payloads later.

NOTHING BUT BOTNETS. The majority of firms detected only one or two types of botnets active in their environment. Good on them. But about 3% of firms were infested with 10 or more unique active botnets! Don't be them.

CLOUDY WITH A SLIGHT CHANCE OF PAIN. Chances are low that cloud applications will contribute to your next malware or botnet infection. Our analysis found no correlation between cloud application usage and increased threat event frequency.

WHEN SHARING ISN'T CARING. Firms that use a lot of P2P and proxy apps report seven to nine times as many botnets and malware as those that don't use any P2P or proxy apps. How many are running in your environment right now? Are you sure?

SOURCES AND MEASURES

FORTINET

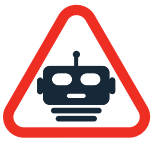
SOURCES AND MEASURES

The findings in this report represent the collective intelligence of FortiGuard Labs, drawn from Fortinet's vast array of network devices/sensors within production environments. This comprises billions of threat events and incidents observed in live production environments around the world from April 1 through June 30, 2017. According to independent research[1], 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 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[2] 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.**

1. Source: IDC Worldwide Security Appliances Tracker, April 2017 (based on annual unit shipments)
2. The phrase "of reporting organizations" is an important distinction. We can only measure prevalence among organizations reporting threat activity. So, for instance, a prevalence of 50% for a given botnet doesn't mean it impacted half of all firms in the world. It means half the firms reporting back botnet detections observed that botnet. That denominator usually represents tens of thousands of firms.

INFRASTRUCTURE TRENDS

FORTINET

INFRASTRUCTURE TRENDS

As we embark on this expedition into the wilds of the Q2 2017 threat landscape, we find it prudent to first get our bearings. And a great way to do that is by reviewing trends associated with the underlying infrastructure those threats so often target. As our usage and configuration of applications, networks, devices, and controls evolve, exploits, malware, botnets, and the actors behind them adapt as well. This never-ending cycle between attackers and defenders, though exhausting, is important to keep in the forefront of our view.

According to Figure 1, the median ratio of HTTPS to HTTP traffic hit a high mark in Q1 2017. Figure 2 reveals the distribution around that median value and reminds us that some firms encrypt nearly everything and some encrypt very little. That's important because, while helpful to maintaining privacy, this trend presents challenges to threat monitoring and detection. Organizations—especially those with higher HTTPS ratios—cannot afford to turn a blind eye toward threats that might be lurking within encrypted communications.

(median values shown)	Q2 2016	Q3 2016	Q4 2016	Q1 2017	Q2 2017
Daily bandwidth	**7.7G**	**7.3G**	**8.5G**	**8.5G**	**6.4G**
HTTPS ratio	**49.8%**	**52.4%**	**50.8%**	**54.9%**	**57.3%**
Total apps	**215**	**211**	**211**	**195**	**187**
SaaS apps	**35**	**35**	**36**	**33**	**28**
IaaS apps	**22**	**23**	**27**	**29**	**25**
Streaming apps	**24**	**21**	**20**	**16**	**14**
Social apps	**19**	**17**	**17**	**14**	**13**
RAS apps	**4**	**4**	**4**	**4**	**4**
Proxy apps	**4**	**4**	**5**	**4**	**4**
Gaming apps	**3**	**3**	**3**	**2**	**2**
P2P apps	**2**	**2**	**1**	**1**	**1**
Daily website visits	**590**	**571**	**595**	**502**	**411**
Daily malicious website visits	**3**	**3**	**3**	**2**	**1**

FIGURE 1. QUARTERLY INFRASTRUCTURE TRENDS. NUMBERS REPRESENT THE MEDIAN VALUE PER FIRM

The statistics shown in Figure 1 were derived from a voluntary threat assessment program that usually lasts about a week. The numbers differ dramatically across participants, which is understandable given the mix of sectors, sizes, business models, regions, and other factors. Even so, we get a snapshot of what a "typical" organization looks like in terms of infrastructure trends and how that profile changes over time.

It's difficult to discern any meaningful pattern for daily bandwidth usage. After seeing steady growth for a year, it stalled last quarter and then dove back down to early 2016 levels. This is one of those measures that's probably highly dependent on which types of firms happen to be in the assessment program at any given time.

SaaS and IaaS applications show a modest drop, but the overall trend line is pretty flat. If those numbers continue to decline, it may indicate increased enlistment of CASBs or other visibility mechanisms to better control cloud usage.

The ratio of HTTPS to HTTP traffic, on the other hand, raised the bar to set another record in Q2.

Figure 2 creates a distribution around that ratio and shows that some firms encrypt the entirety of their web traffic while others let it all out in the open for the world to see. We pay close attention to this trend because threats are known to use encrypted communications for cover, introducing some unique challenges for detection and other tasks like load balancing. Many network devices simply can't keep up as HTTPS traffic increases, resulting in bottlenecks or passing through of potentially malicious traffic.

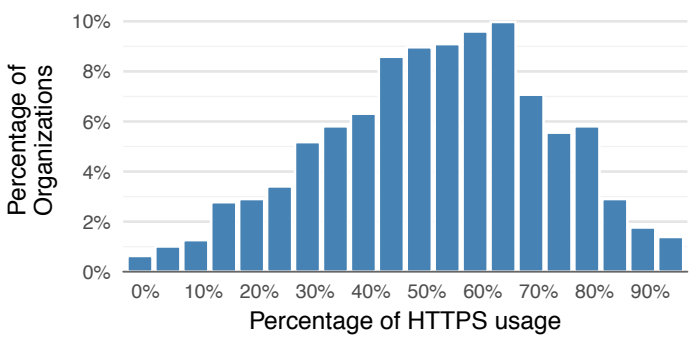


FIGURE 2. DISTRIBUTION OF HTTPS TRAFFIC PROPORTION ACROSS FIRMS

INFRASTRUCTURE TRENDS BY INDUSTRY

In last quarter's report, we asked the question "which industries share closely related profiles when it comes to infrastructure usage?" We used cluster analysis to compare industries along the set of infrastructure elements listed in Figure 1 above. We learned that "infrastructure profiles" do indeed exist, and we discovered some counterintuitive pairings among the industries. We did not, however, dig too deeply into exactly what makes them similar or different. And that's where we'd like to resume our digging for this quarter.

	Construction	Education	Energy & Utilities	Finance/Insurance	Government	Healthcare	Manufacturing	Retail/Hospitality	Services	Technology
Daily bandwidth	9,310	8,997	3,698	3,549	7,872	7,315	6,744	6,681	4,938	4,603
HTTPS ratio	58.0%	59.9%	55.7%	58.8%	57.5%	58.3%	56.1%	53.2%	58.6%	53.5%
Daily Total Apps	190	292	166	161	212	201	192	174	163	170
SaaS apps	38	62	18	21	40	33	26	27	25	26
IaaS apps	31	36	20	21	30	29	26	24	22	20
RAS apps	4	4	3	4	4	4	4	4	3	4
Proxy apps	4	10	4	3	4	4	4	3	3	4
P2P apps	1	3	1	<1	1	1	1	1	1	1
Social apps	13	21	11	11	16	12	13	12	12	12
Streaming apps	15	29	12	14	17	17	14	13	12	13
Gaming apps	1	9	1	1	2	2	2	1	1	2
Daily website visits	410	1,010	227	315	526	528	499	357	304	352
Daily malicious websites	1	4	<1	<1	2	<1	2	1	1	<1

FIGURE 3. INFRASTRUCTURE USAGE STATISTICS FOR TOP INDUSTRIES. NUMBERS REPRESENT THE MEDIAN VALUE

Figure 3 presents the infrastructure and app usage statistics from Figure 1 broken out across the top 10 industries. Several things stand out, but let's start with the elephant in the room—education. The education sector leads in nearly every measure of infrastructure usage. And not just by a tiny margin. To be fair, educational institutions aren't exactly known for their pristine networks and rigid policies due to a need to support openness and a curious student body, but it's still a tad shocking to see it laid out like this. It may seem obvious, but the student population is a key differentiating factor here. If we included the personal computers and applications of banking customers in with that sector's statistics, the results would undoubtedly look much, much different than they do here.

Shockingly, the energy and utilities sector (see what we did there?) stands on the opposite end of the spectrum from EDUs. It generally shows the lowest usage levels across the infrastructure elements. This is likely partly due to more stringent policies and partly due to the nontraditional technology environments in which many of them operate.

Outside education and energy, sectors range from more conservative usage (e.g., financial) to more liberal (e.g., government) and in between (e.g., healthcare). External pressures (from both adversaries and regulators) surely shape what we see here—and will continue to do so.

Some elements such as HTTPS ratios and remote access service (RAS) applications are remarkably consistent across industries. Keep in mind these are median values, which tend to dampen extremes—especially for smaller numbers like we see for RAS apps. Even so, there's a good deal of variation apparent in the figure too. We find the varying usage of cloud applications (SaaS and IaaS) particularly interesting. It will be fun to watch these adoption rates over time as each industry weighs the pros and cons of migrating workloads to the cloud.

It's time for us to continue our journey into the Q2 threat landscape, but fans of infrastructure statistics have no reason to fret. We'll be retreading this ground in the Exploratory Analysis section at the end of this report.

THREAT LANDSCAPE TRENDS

FORTINET

EXPLOIT TRENDS

Exploit trends grant a view into adversary attempts to identify and compromise vulnerable systems. Triggering one of the 184 billion signatures observed this quarter doesn't mean the attack succeeded or that the targeted vulnerabilities were present in the environment. Thus, exploit detections tend to be rather noisy. We've elected to improve the signal-to-noise ratio by restricting our analysis to critical and high-severity events for this section.

QUICK STATS

- 184 billion total exploit detections
- 1.8 billion average daily attack volume
- 6,298 unique exploit detections
- Exploit volume per firm averaged 2.5 million, with a median of 456
- 69% of firms saw severe attacks

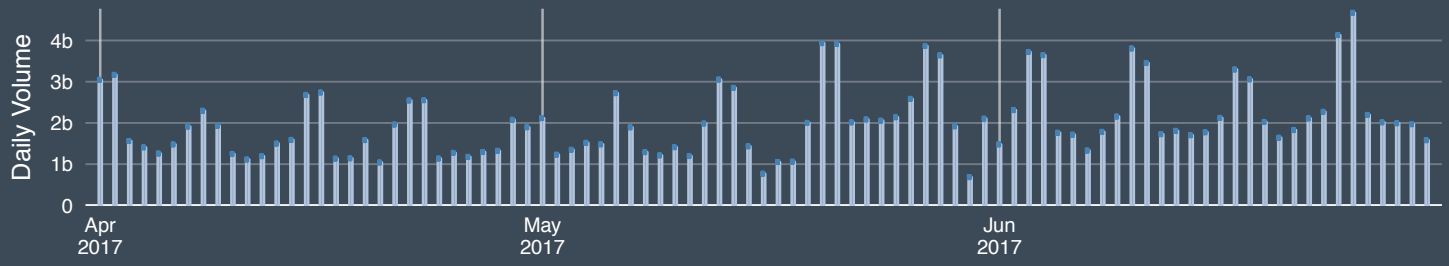


FIGURE 4. QUARTERLY APPLICATION EXPLOIT ACTIVITY

Looking for a single chart that plots all 6,300 unique exploits generating 184 billion sensor detections over the course of Q2 2017? Well then, Figure 5 is your eureka moment. Prevalence is shown along the x-axis, volume on the y-axis, and intensity determines the size of the dot (larger = greater). Note that axes are presented on a log scale, so jumps between grid lines are actually much larger than they appear. Ignoring the IPS signature names for now, we can discern that the bulk of them are observed by fewer than one in 100 firms and at a volume less than 100K. Generally speaking, as volume increases, so too does prevalence. And exploits with the highest intensity tend to fall along the upper half of the volume axis.

To allow closer examination, exploits reported by more than one in 10 firms or at a volume higher than 10 million bear a label in Figure 5. We've seen most of these before. A cadre of brute force exploits targeting Telnet, FTP, WordPress, SSH, POP3, RDP, and MySQL occupies the top middle section of the chart. The far right appears dominated by code/command execution and injection attacks against SQL servers, ASUS routers, PHP applications, Microsoft's HTTP protocol stack, Bash (Shellshock), Apache Struts, and Joomla, among others. So, brute force attacks soak up bandwidth and code execution/injection attacks affect a lot of organizations. Not exactly an earth-shattering revelation, but an interesting data-driven observation nonetheless.

Prior to WannaCry and NotPetya, network worms took a hiatus over the last decade plus. SQL Slammer apparently never got that memo because it's been pummeling the Internet since 2003. Let's hope we're not talking about WannaCry and NotPetya in our Q2 2030 report.

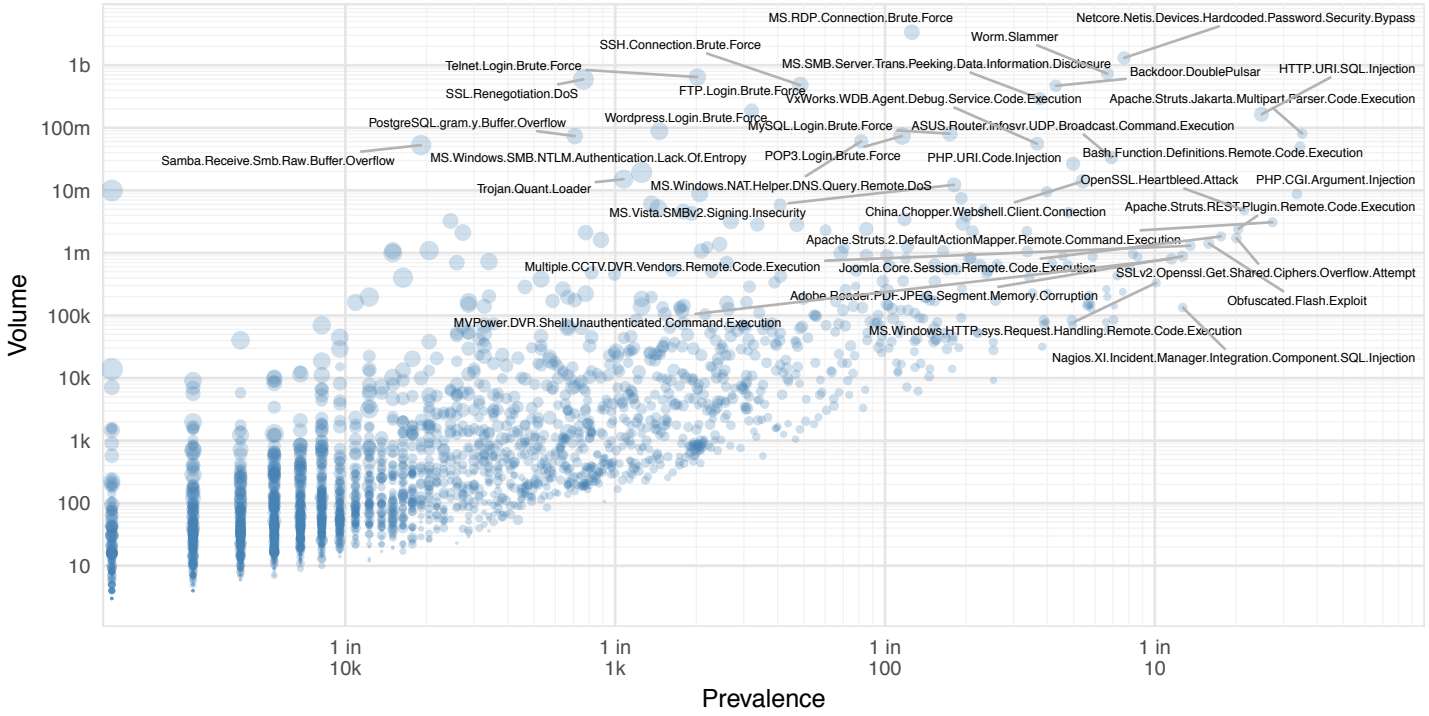


FIGURE 5. ALL Q2 EXPLOITS PLOTTED BY PREVALENCE, VOLUME, AND SEVERITY

The *Netcore.Netis*, *Multiple.CCTV.DVR*, and *ASUS.Router* signatures are associated with scans for vulnerable IoT devices to join in massive DDoS attacks. Overall volume of IoT-targeted exploit activity was consistent with last quarter and we saw no major movements among any of the common device categories.

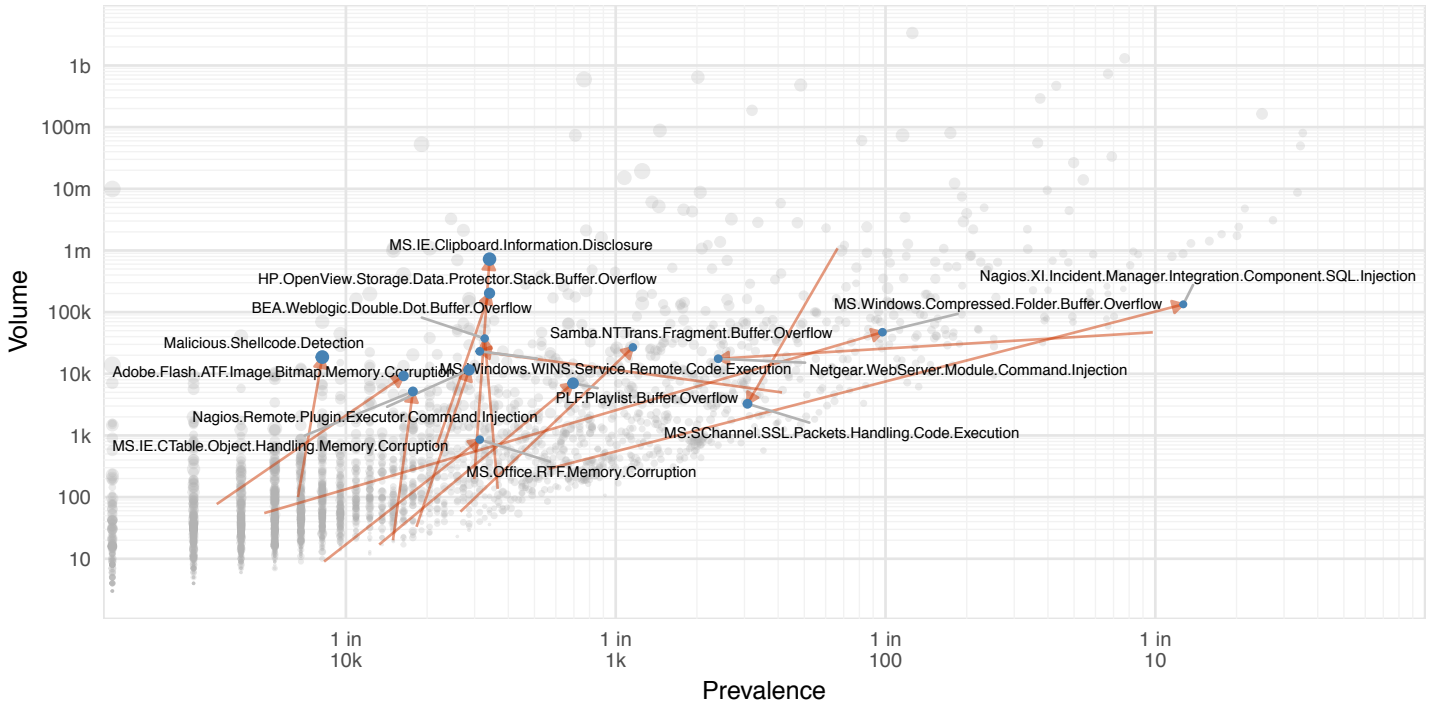


FIGURE 6. MAJOR MOVERS AMONG Q2 EXPLOITS. ARROW SHOWS Q1 TO Q2 MOVEMENT

Speaking of movements, Figure 6 shares the same layout as Figure 5 but focuses instead on exploits that were the biggest movers over the quarter. We determined this by comparing the x-y position of each exploit in Q1 and Q2. Those that traveled the furthest on the coordinate grid are designated with a label and an arrow tracking their movement. Some of those arrows are quite long, jumping four orders of magnitude in volume, prevalence, or both.

For the most part, there's no larger trend or hidden story behind these movers, which we view as a reminder of the automated and arbitrary nature of exploit activity. Nagios XI certainly isn't the most pervasive software on the Internet and we highly doubt adoption jumped four orders of magnitude in Q2 to invite more attention. But when it costs the criminal nearly nothing to kick off an automated scan for tens of thousands of vulnerabilities before calling it a day, why not try?

Exploit Severity, Longevity, and Periodicity

Figure 7 depicts the percentage of firms that detected exploits in Q2 against vulnerabilities that have been released over the past 15+ years. It attempts to answer the question "what percentage of firms saw an exploit from each year?" The exploits are color-coded according to severity rating.

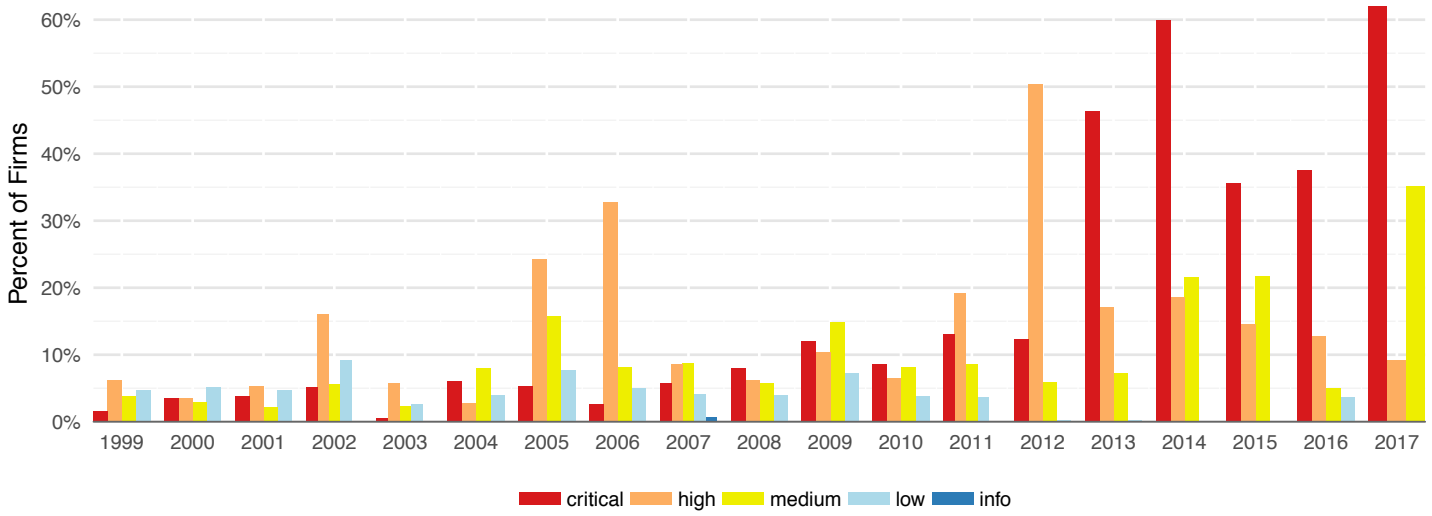


FIGURE 7. PREVALENCE OF VULNERABILITIES TARGETED BY EXPLOITS. GROUPED BY CVE RELEASE YEAR AND COLORED BY SEVERITY RATING

All told, more than two-thirds of firms experienced high or critical exploits in Q2 2017. Compared to previous quarters, activity in Q2 appears to involve a higher proportion of critical-severity exploits targeting more recent CVEs. Even so, we're once again reminded that attackers show no sign of discrimination against elderly vulnerabilities. A full 90% of organizations recorded exploits for vulnerabilities that were at least three years old. Even at 10 or more years out from a CVE's release, the majority of firms (~60%) still see related attacks.

Sharp eyes may perceive the quarterly volume chart leading off this section appears very cyclical. We suspected those peaks might correspond to weekends, and ran a quick check. Nearly 44% of all IDS detections fired on either Saturday or Sunday, and the average daily volume on weekends was twice that of weekdays. As if we needed another reason to loathe cyber criminals—they're after our data AND our weekends! Let's don't let them take either.

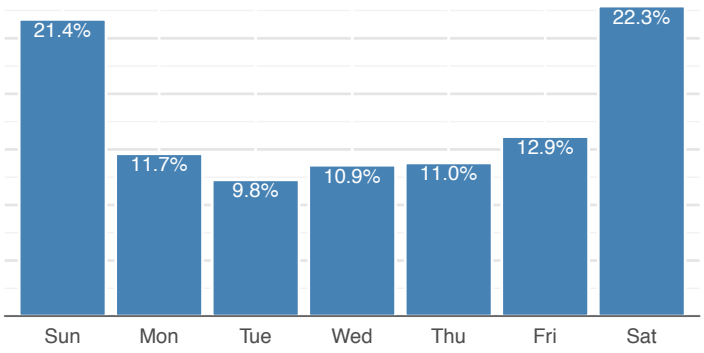


FIGURE 8. EXPLOIT VOLUME BY DAY OF WEEK.

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

- 62 million malware detections
- 677,000 average daily volume
- 16,582 total malware variants
- 2,534 different malware families
- 18% of firms saw mobile malware

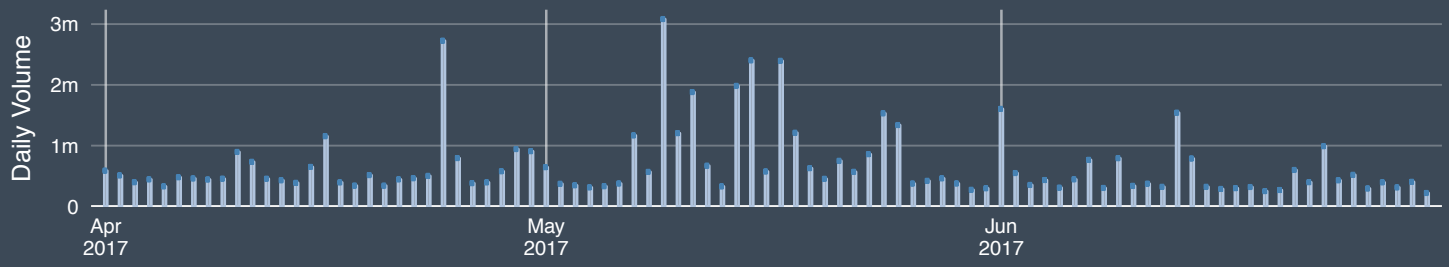


FIGURE 9. QUARTERLY MALWARE DETECTION VOLUME

Figure 10 mimics the layout of Figure 5 from the previous section on exploits and is interpreted in the same way. We present malware according to higher-order families rather than particular variants because we think it suits the purpose of studying overall trends.

Those wanting more granular information on the enormous number of variants within those families can check out our Weekly Threat Briefs as well as our Security Blog.

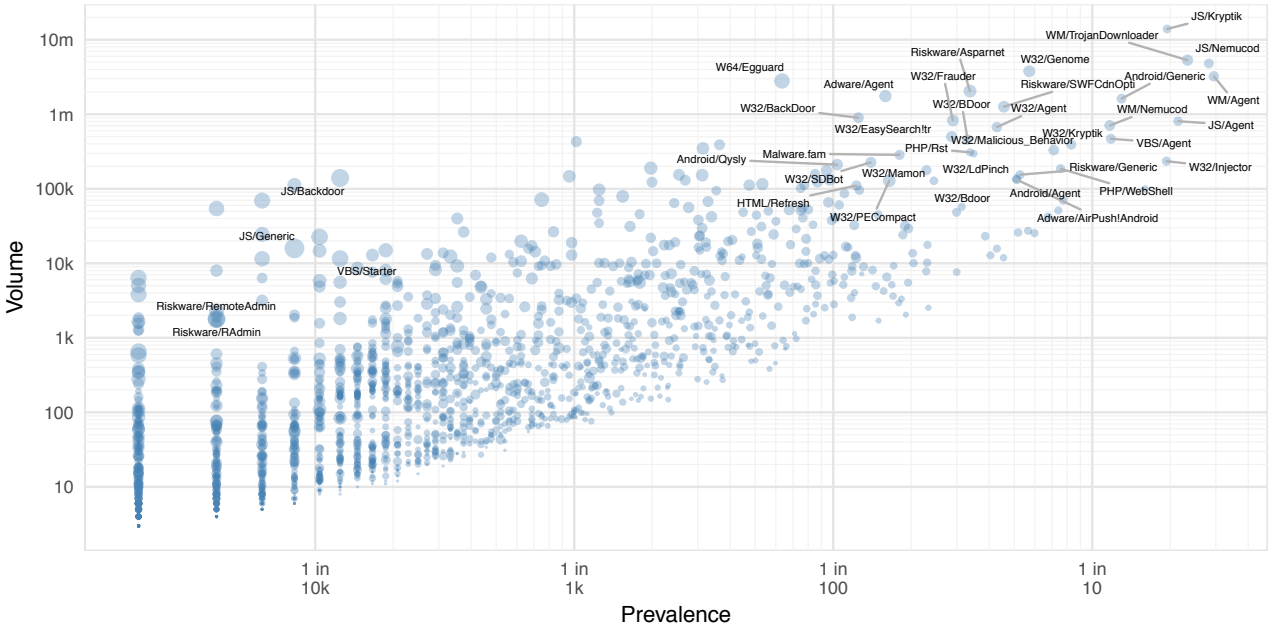


FIGURE 10. ALL Q2 MALWARE FAMILIES PLOTTED BY PREVALENCE, VOLUME, AND SEVERITY

In the upper right of Figure 10, malware families detected by at least one in 100 firms and/or at a volume of 100K or more are labeled. The most common functionality among these is downloading/uploading files, followed by dropping other malware onto the infected system. Downloaders and droppers are a rather interesting breed of malware because they often don't have a malicious payload within their codebase. They discreetly deliver weapons to the target, but don't pull the trigger themselves. *JS/Nemucod* is the poster child for such functionality, having established a notorious record of spreading ransomware and other trojans.

Next on the list of naughty behaviors from malware families in Figure 10 includes establishing remote access connections, capturing user input, and gathering system information. *W64/Egguard* and *JS/Backdoor* exemplify this functionality set, as do most of the families with the highest intensity scores.

A few Android families can also be seen amid the crowd in Figure 10. The ratio of all Android malware was 5% of total malware volume in Q2. This falls right in the middle of values recorded for the previous two quarters (8.7% and 1.7%). From a prevalence standpoint, slightly over 18% of organizations reported mobile malware in Q2, which is consistent with prior observations.

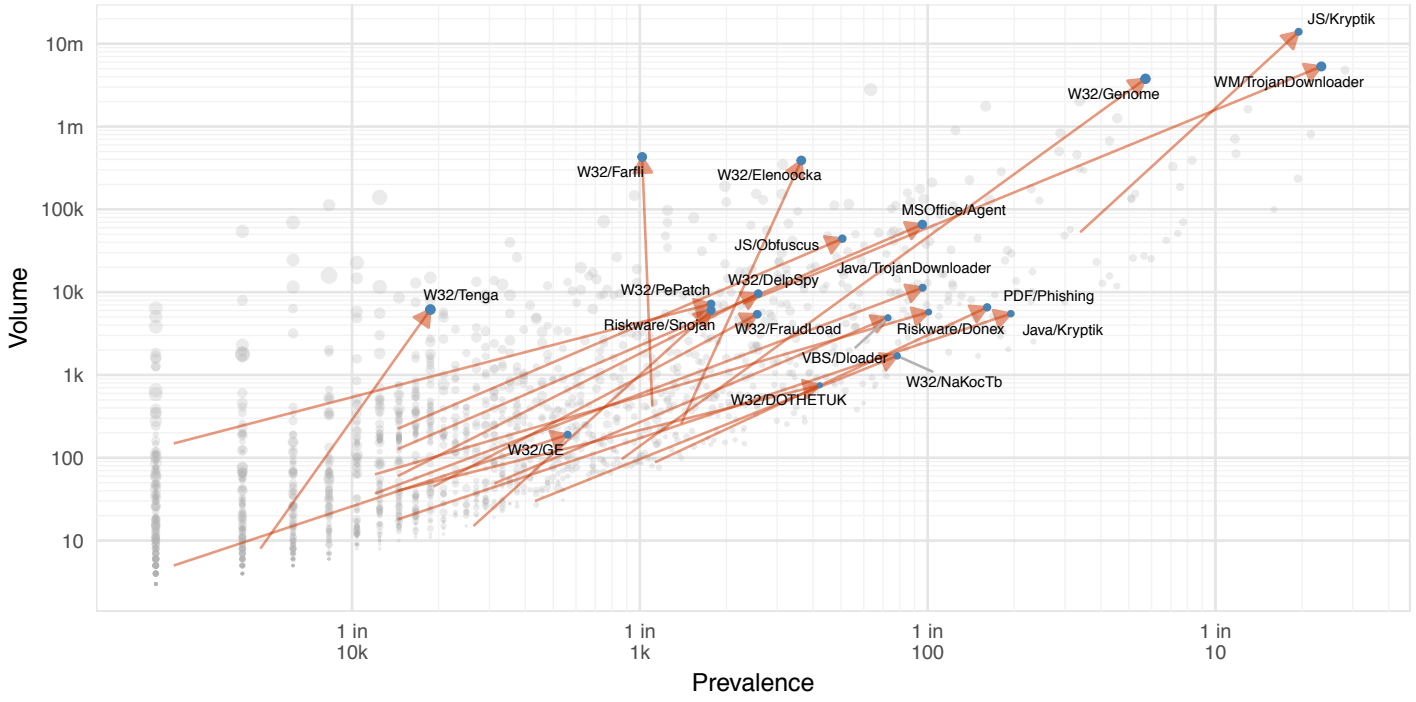


FIGURE 11. MAJOR MOVERS AMONG Q2 MALWARE. ARROW SHOWS Q1 TO Q2 MOVEMENT

The quarter's major movers for malware are featured in Figure 11 and tell a story similar to the preceding figure. *JS/Kryptik*, *W32/Genome*, and *WM/TrojanDownloader* each jumped several orders of magnitude to land in the top right corner and exhibit downloader/dropper functionality. A number of trojan-heavy families made a resurgence as well—*W32/Farfli*, *W32/Elenoocka*, *W32/FraudLoad*, and *W32/DelpSpy*, to name a few.

WannaCry and NotPetya Ransomware Worms

A Q2 2017 trend analysis of malware would simply not be complete without mention of the WannaCry and NotPetya ransomware worms. These events have been covered in detail by many sources, so we won't give a full debrief here (see our Security Blog for that). What we want to tell here is a tale of three exploits as witnessed by our sensors.

WannaCry and NotPetya are referred to as "ransomware worms" because they combine traditional ransomware and worm-like behaviors to maximize the scope and speed of spread. For these particular ransomware worms, that comes by way of exploiting three flaws leaked by the Shadow Brokers hacking group known as EternalBlue, EternalRomance, and DoublePulsar.

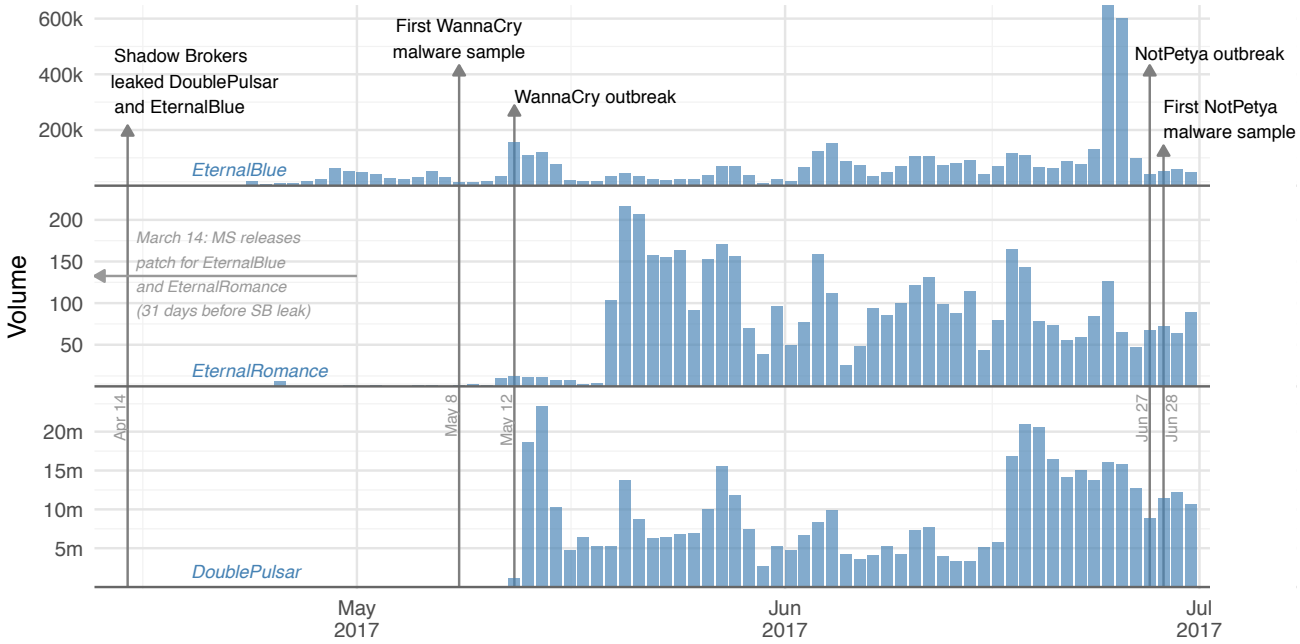


FIGURE 12. EVENT TIMELINE AND EXPLOIT ACTIVITY TARGETING VULNERABILITIES ASSOCIATED WITH THE WANNACRY AND NOTPETYA RANSOMWARE WORMS IN Q2 2017

The Shadow Brokers leak on April 14 marks the first event on the timeline in Q2. However, we've added a note regarding Microsoft's release of MS17-010 that patched the flaws targeted by DoublePulsar, EternalBlue, and EternalRomance. This will be important later.

Following the leak, blips of activity can be seen for these exploits in April and early May. This is likely a combination of white and black hats probing the extent of vulnerable systems (for different reasons, of course). On March 8, our sensors picked up a handful of samples of a then unidentified malware later determined to be WannaCry. The WannaCry outbreak begins in full on May 12, easily apparent by the surge on the DoublePulsar and EternalBlue timelines. Activity settles down a bit after the sinkholing of the kill switch domain and as firms the world over scrambled to patch or otherwise remediate vulnerable systems.

Almost as if both bad and good guys read the writing on the wall, probes related to the other flaw, EternalRomance, began to roll across our sensors throughout May and June. A late June spike in EternalBlue exploits heralded the full brunt of the NotPetya outbreak right before the close of the quarter. We'd like to be able to say Q2 closed the curtain on ransomware worms, but we've seen this scene reenacted too many times for that.

The lesson? Act fast after critical patch releases and heed related intel about exploit life cycles.

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

- 2.9 billion botnet detections
- 32 million average daily volume
- 993 daily botnet comms per firm
- 243 unique botnets detected
- 2.7 unique active botnets per firm

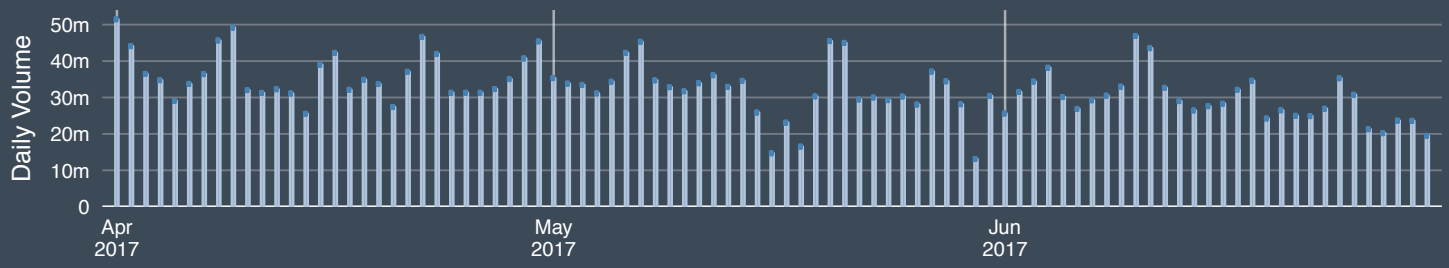


FIGURE 13. QUARTERLY BOTNET DETECTION VOLUME

The comparatively shorter botnet names in Figure 14 allow us to label any affecting more than one in 100 organizations and/or with a volume greater than 1 million. As you can see, quite a few fit that bill. We'll highlight some of them here, but feel free to use our Threat Encyclopedia to look up anything else that catches your attention. That's one of the benefits of complex data visualizations like this—we begin the story and you get to choose your own adventure after that.

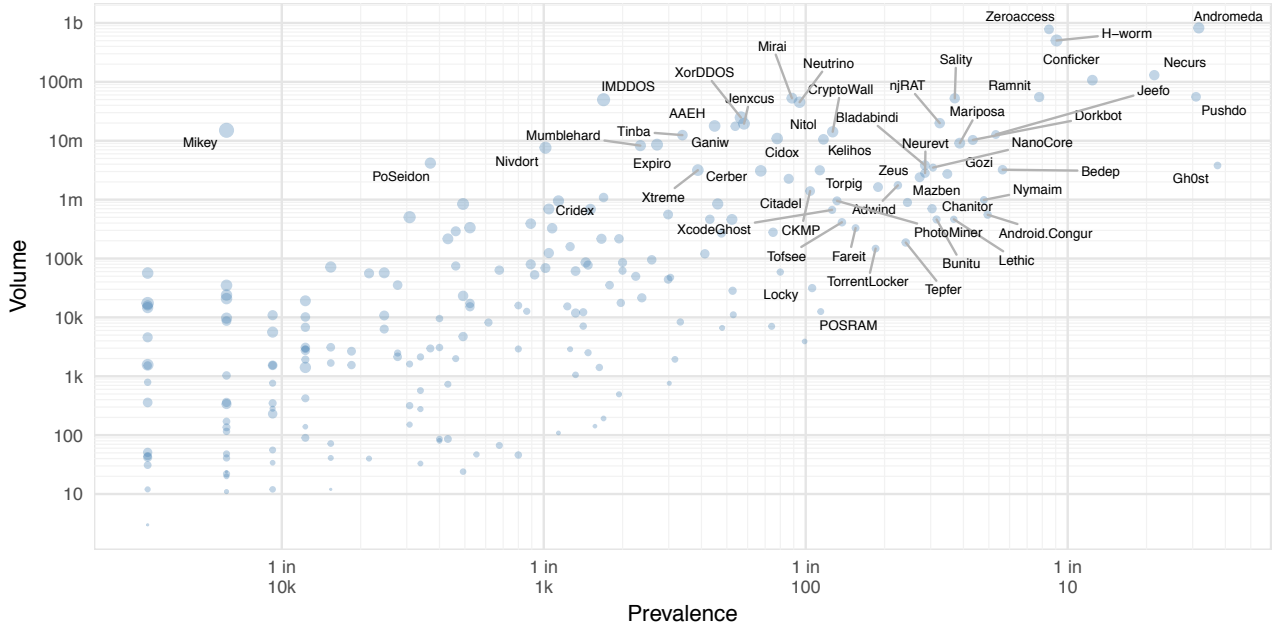


FIGURE 14. ALL Q2 BOTNETS PLOTTED BY PREVALENCE, VOLUME, AND SEVERITY

First off, notice that five different botnets were detected by at least one in 10 firms. We realize 10% isn't normally a sound bite-worthy stat, but it holds more weight when you consider that we're looking at a sample of tens of thousands of organizations here. There are also five botnets topping 100 million detections by volume. Let's start with the upper right block that met both of these conditions, where we see Andromeda, Necurs, and Conficker.

Andromeda boasted the fastest spread of any botnet in Q1, and it does not appear to have given up any of that hard-earned ground during Q2. It's 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. Necurs has become a sort of Swiss army knife of botnets. It built its name as the major distributor of the Locky ransomware and Dridex trojan families, and still jumps back into that role on occasion. Lately though, Necurs seems to favor supporting large-scale spam campaigns centered on financial fraud. Conficker is old in bot years, having been discovered in 2008, but is still going strong. Let's acknowledge its impressive staying power and just move on.

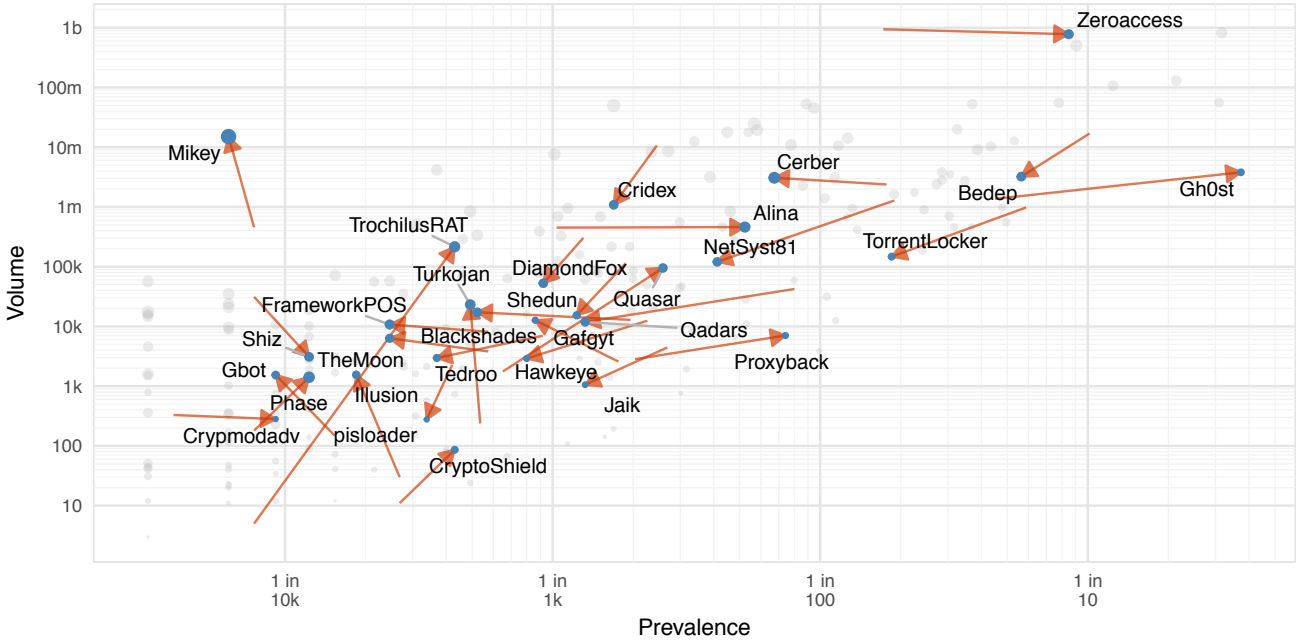


FIGURE 15. MAJOR MOVERS AMONG Q2 BOTNETS. ARROW SHOWS Q1 TO Q2 MOVEMENT

Just outside that block, Pushdo is another bot with a decade of deployment under its belt. It saw heavy action early in spam campaigns run by the Cutwail criminal gang, but more recent spikes in activity are DDoS related against SSL-encrypted websites. Though not graybeards like Conficker and Pushdo, ZeroAccess and H-Worm (aka Houdini Worm) aren't young either. Both give cyber criminals control of affected systems, but ZeroAccess favors siphoning data while H-Worm engages in click fraud and bitcoin mining. In addition to retaining its leadership on the volume axis, ZeroAccess made solid moves in Q2 along the prevalence scale. Other major movers can be found in Figure 15.

The Gh0st RAT botnet, another veteran, reinvigorated itself to hit 37% of the firms in our dataset. Once installed, Gh0st 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. Gh0st also has the ability to obfuscate client-server communications using a proprietary network protocol and comes bundled with intuitive graphical user interfaces that make it simple to use.

Another dirty RAT, Trochilus, was associated with an espionage campaign targeting firms in Myanmar a couple of years ago. We haven't seen much from it since and so eyebrows were raised when it jumped from a volume of less than 10 to over 100K and was reported by a number of firms in Asia, Europe, Africa, and the Americas. We will continue monitoring it with interest.

Botnet Infections and Infestations

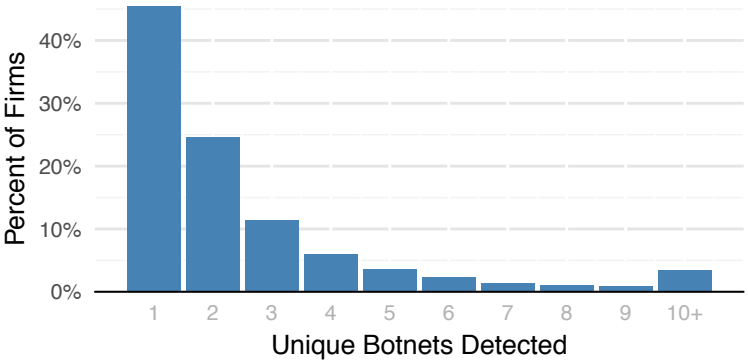


FIGURE 16. UNIQUE BOTNETS PER FIRM

At the beginning of this section, we give various stats like a total of 243 unique botnets were observed in Q2 and that organizations typically reported two to three of those over the span. But as with anything, "typical" doesn't cover everything. Figure 16 presents the distribution around that statement for unique botnets per firm.

According to the chart, roughly 45% of firms detected only one type of botnet active in their environment. Another 25% saw two unique botnets, 10% saw three, and so on. Way over to the right, about 3% of organizations reported 10 or more unique botnet infections—though "infestations" is probably the better term for that. So, where are infestations most common? We thought you might ask that, and Figure 17 serves as our prerecorded answer.

We need to caution that sample sizes are smaller here (we're unpacking that 3% from Figure 16), which means a lot of fuzziness around numbers. But as a proportion of firms within each sector, telcos experienced more infestations than anyone else. That almost certainly reflects more on their subscriber base than internal systems, and results for the education sector can be viewed in a similar light.

Some may be surprised to see healthcare in the bottom half of the list, but probably not so much to see the finance sector in relatively good standing. Industries at the very bottom often aren't as extensively IT-heavy across the user base as some of those towards the top, which may account for the low infestation rate.

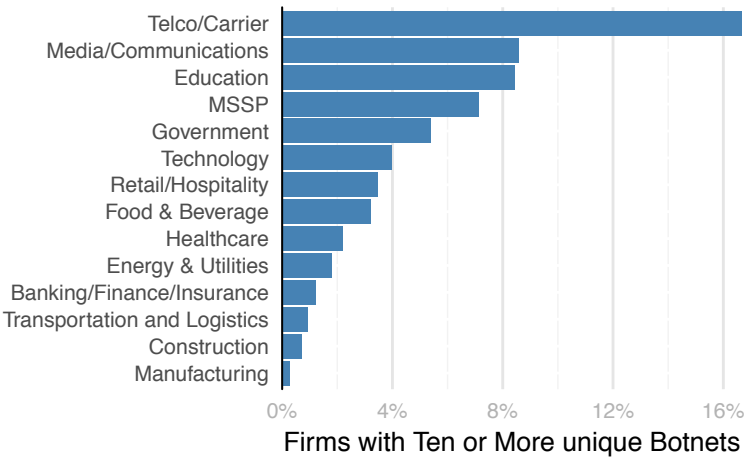


FIGURE 17. BOTNET INFESTATIONS BY SECTOR

EXPLORATORY ANALYSIS: INFRASTRUCTURE AND THREAT CORRELATIONS

FORTINET

EXPLORATORY ANALYSIS: INFRASTRUCTURE AND THREAT CORRELATIONS

In our Q1 2017 report, we presented the concept of using cluster analysis to profile firms and industries based on their shared infrastructure and threat characteristics. We noticed that certain sectors identified as having very distinct infrastructure profiles also appeared to have very distinct threat profiles. We ended that analysis with the following statement:

> *"We don't have sufficient space to explore where this falls on the spectrum of spurious correlation to direct causation, but we find the results compelling either way. Could it be that an organization's infrastructure usage has a stronger relationship to its threat profile than its industry?"*
>
> *– Fortinet Q1 2017 Threat Landscape Report, page 28*

Not ones to leave a question like that hanging out there for too long, we were eager to see what kind of answers we could pull from the data this quarter. The assessment program mentioned at the beginning of this report sets a perfect stage for this analysis. We are not only able to collect information regarding the infrastructure usage of participating firms (see list of elements in Figure 1) but also the number of threats they detect. Thus, we have the data necessary to search for interesting infrastructure-threat correlations.

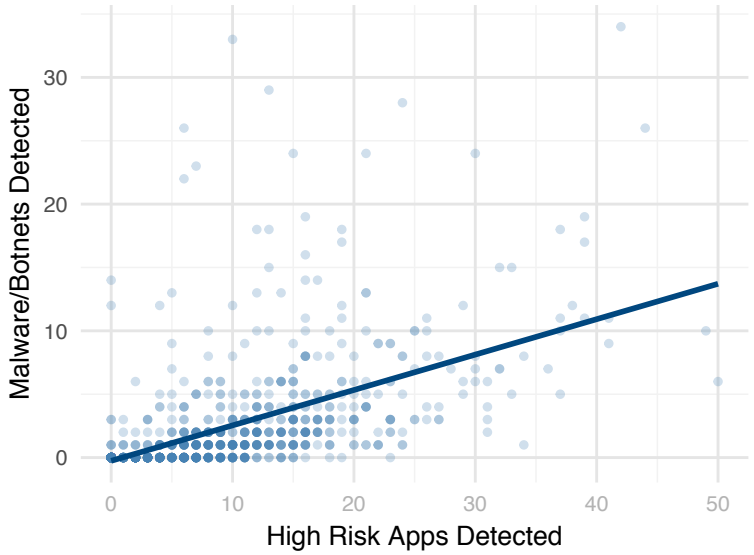


FIGURE 18. REGRESSION ANALYSIS OF HIGH-RISK APPS USED TO BOTNETS AND MALWARE INFECTIONS

To get this started, let's use the analytical equivalent of a backhoe to check whether there's any sign of gold in these hills. Running a regression analysis on the number of high-risk apps[3] used by the firm vs. the total number of malware and botnets detected finds a statistically significant positive correlation between these two variables. It's not a very strong relationship, as Figure 18 suggests, but it does give incentive to switch to a shovel and keep digging.

Testing for relationships between specific types of applications and detected threats highlights P2P and proxy applications as possible troublemakers. Equally interesting are some of those NOT on the naughty list. We saw no evidence at all that higher usage of cloud-based or social media applications leads to increased numbers of malware and botnet infections.

3. An app is designated "high risk" if it has an assigned risk rating of at least 4 out of 5. Don't get distracted by this for now; more specific examples will follow.

Let's follow the data's lead and probe deeper around P2P and proxy applications. We do this by separating firms into three groups: those that don't use any P2P or proxy apps (None), those that use some (Some), and those that use a lot of them (Lots). Figure 19 presents a series of violin plots that reveal the shape of the distribution of threat detections for each of those groups. If violin plots aren't your thing, read this explanation or just focus on the summary stats given in Figure 20, where there's a clear difference in the average number of malware and botnets observed for each of the three groups.

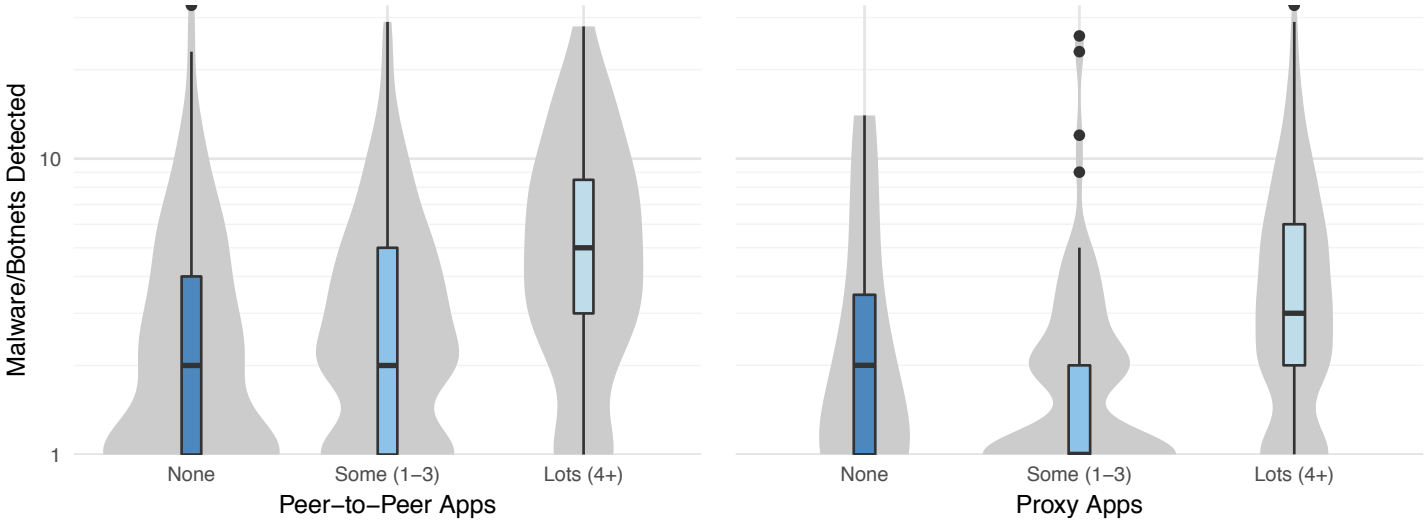


FIGURE 19. RESULTS OF ANALYSIS COMPARING THE NUMBER OF P2P AND PROXY APPS USED TO TOTAL NUMBER OF MALWARE AND BOTNET DETECTIONS

	Number of apps used			
Apps	**None**	**Some**	**All**	
P2P apps	**0.65**	**1.64**	**4.54**	**<- Mean # infections**
Proxy apps	**0.29**	**0.52**	**2.58**	

FIGURE 20. AVERAGE NUMBER OF DETECTIONS FOR P2P AND PROXY APPS AT VARYING USAGE LEVELS

This analysis leads us to some rather striking and important conclusions:

1. Organizations using a lot of P2P apps report 7x as many botnets and malware as those that don't use P2P apps.
2. Organizations using a lot of proxy apps report almost 9x as many botnets and malware as those that don't use proxy apps.

At this juncture, it's important to reiterate the warning that "correlation is not causation." We certainly have evidence that a relationship exists, but we cannot prove P2P and proxy apps cause malware and botnet infections. Perhaps firms that allow higher numbers of questionable apps like these also have generally poorer security practices, which are the real causal factor. Consonant findings like that start to smell a little more causal than spurious. At the very least, our findings here warrant a thoughtful reevaluation of software use policies and enforcement practices.

CONCLUSION AND RECOMMENDATIONS

CONCLUSION AND RECOMMENDATIONS

We threw a lot of numbers and information at you in the pages above. We'd like to close out this report by reiterating some of those findings and connecting them to practical things you can do in light of them to protect your organization. Your Fortinet representative will be glad to discuss strategies for implementing any of these recommendations. We also recommend reading our Security Blog for ongoing analysis of threats and mitigations. Thank you for reading.

01

From a headlines perspective, the WannaCry and NotPetya ransomware worms owned Q2 2017. They were far from silent across our sensors too. Ransomware is a lucrative criminal enterprise, and we don't see it going away anytime soon. See our ten-step program for ways to protect your organization against ransomware. Technical protections specific to WannaCry can be found here.

02

Network and device hygiene are perhaps the most neglected elements of security today. WannaCry targeted vulnerabilities that Microsoft patched two months previous. In spite of its worldwide impact, NotPetya successfully exploited the EXACT SAME vulnerability a month later. Pay close attention to critical patch releases and monitor intelligence sources for any signs of pre-attack reconnaissance and exploit development.

03

Even aside from WannaCry and NotPetya, nearly all organizations routinely recorded exploits against old vulnerabilities—years old, in fact. These "free pen tests" are bad news for legacy systems, complex environments, and lax patch management because they are relentless and unforgiving. Your efforts to identify and address exposed vulnerabilities must be equally dogged.

04

The ratio of encrypted web traffic continues to rise. While good for Internet privacy and security, this trend presents a challenge to many defensive tools that have poor visibility into encrypted communications. Assess whether this is a blind spot in your environment.

05

We presented views into threats that span the kill chain from pre-attack reconnaissance (exploits) to weaponization (malware) to post-compromise command and control (botnets). It stands to reason that a strong defensive fabric must cover that entire chain as well. Does yours?

06

It's not news that malware gets more evasive over time. Still, the fact that so many downloaders and droppers topped our charts is a good reminder that single-point, signature-based AV just doesn't cut it. Integrate malware defenses capable of detecting known and unknown threats at multiple layers throughout the environment.

07

Almost one in five organizations reported malware targeting mobile devices. Such devices present a challenge because they 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 the majority of firms in our sample 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

If threat actors do manage to establish a beachhead, they will next begin a land-grabbing phase into other parts of the network. An internal network segmentation strategy can help contain threats and minimize this lateral movement.

10

We found a strong link between malware/botnet infections and heavy usage of business-questionable software like P2P and proxy apps. It's a good excuse to review existing policies, update the software inventory, and scan for rogue applications.

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

August 15, 2017
108056 0 0 EN