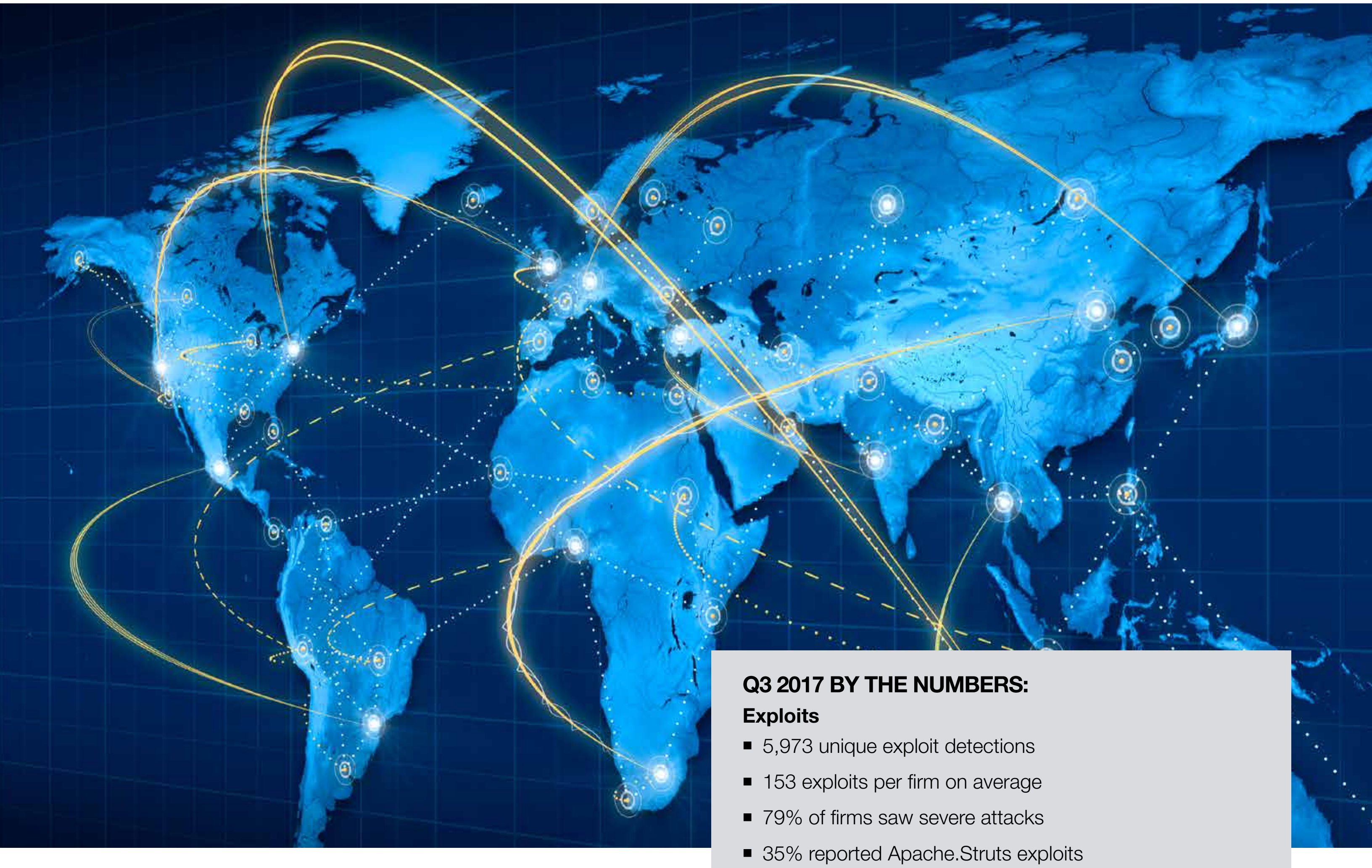
FORTINET®

THREAT LANDSCAPE REPORT

Q3 2017

TABLE OF CONTENTS

INTRODUCTION



The third quarter of the year should be filled with family vacations and the back-to-school hubbub. Q3 2017 felt like that for a couple of months, but then the security industry went into a hubbub of a very different sort. Credit bureau Equifax reported a massive data breach that exposed the personal information of approximately 145 million consumers.

That number in itself isn't unprecedented, but the public and congressional outcry that followed may well be. In a congressional hearing on the matter, one U.S. senator called the incident "staggering," adding "this whole industry should be completely transformed." The impetus, likelihood, and extent of such a transformation is yet unclear, but what is clear is that Equifax fell victim to the same basic problems we point out quarter after quarter in this report. In fact, the exact application exploit used by attackers to breach Equifax was featured in our last report as the most prevalent among 6,000+ unique detections recorded that quarter. And it's #1 again this time.

Q3 2017 BY THE NUMBERS:

Exploits

- 5,973 unique exploit detections
- 153 exploits per firm on average
- 79% of firms saw severe attacks
- 35% reported Apache.Struts exploits

Malware

- 14,904 unique variants
- 2,646 different families
- 25% reported mobile malware
- 22% detected ransomware

Botnets

- 245 unique botnets detected
- 518 daily botnet comms per firm
- 1.9 active botnets per firm
- 3% of firms saw ≥10 botnets

Far from attempting to blame and shame Equifax (or anyone else), we're simply stating the facts: ordinary threats will harm even the most extraordinary security programs if they're caught off guard. We hope the facts shared in this report will help guard your organization against such a fate.

Q3 2017 **HIGHLIGHTS AND KEY FINDINGS**

STRUTTING THEIR STUFF. Three exploits against the Apache Struts framework made the top 10 list and another was among the major movers for the quarter. It's an example of how attackers swarm when they catch scent of a widespread, vulnerable target.

GROWING PAINS. It's not just an '80s TV show or a joint affliction. Both infrastructure usage and threat trends tend to increase and diversify as organizations grow larger. That's not terribly surprising, but it's one more piece of evidence demonstrating security is not a one-size-fits-all solution. Make sure your security program fits well now and grows with you.

MIDSIZE WITH LARGE-SIZE PROBLEMS. Midsize firms saw higher rates of botnet infections, a trend we doubt is limited to this quarter. It may be they represent a good "bang for the buck" from the adversary's standpoint, with a large attack surface, lots of data, and yet a fraction of the resources of their larger brethren.

A NEW GAZE AT ZERO DAYS. We have a new addition to our report this quarter—zero-day vulnerabilities found by our team of expert researchers. We've identified 185 zero days to date this year and 503 since 2006. We announced eight in Q3 once the patch was released to fix the vulnerability.

SCADA SCATTER. In addition to high-volume attacks like those against Apache Struts, we offer a view of threats flying below the radar too. For example, you should definitely check out our scatter plot of top exploit detections against SCADA systems if your firm uses industrial control systems.

LOCKYING IT UP. After a hiatus during the first half of the year, the Locky ransomware ramped up in a big way this quarter with three new campaigns. Roughly 10% of firms reported it, which may not seem like much until you realize that percentage spans tens of thousands of organizations in our data. All told, 22% detected some type of ransomware in Q3.

DROPPIN' DOWN THE BEAT. The most common functionality among top malware families is downloading, uploading, and dropping malware onto infected systems. This technique helps slip malicious payloads through legacy defenses by wrapping them in dynamic packaging.

PEER-TO-FEAR APPS. We showed last time that firms using a lot of P2P and proxy apps report 7x to 9x as many threats as those that don't use any at all. This round we extend that to study exactly which types of malware and botnets organizations that use these apps should fear most.

SOURCES AND MEASURES

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 July 1 through September 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 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[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] 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.

INFRASTRUCTURE TRENDS

INFRASTRUCTURE TRENDS

As anyone who's studied cyber threats for any length of time knows, application exploits, malware vectors, botnet infections, and the like are a reflection of the attack surface across the organizations they target. The adversaries behind those threats monitor trends such as encryption, application usage, and cloud adoption very closely, and it behooves defenders to do the same. With that in mind, we present infrastructure trends for Q3 2017 in Figure 1.

Figure 1 draws its results from a voluntary threat assessment program that typically runs about a week and includes organizations of mixed demographics, a fact that undoubtedly affects the counts you see here. Even so, we still get a reasonable sense for what a "typical" organization looks like and how infrastructure usage is changing over time. We showed last quarter how "typical" differs across industry lines, and we do the same based on firm size later in this section. But let's not get ahead of ourselves.

(median values shown)	**Q3 2016**	**Q4 2016**	**Q1 2017**	**Q2 2017**	**Q3 2017**
Daily bandwidth	7.3G	8.5G	8.5G	6.4G	8.9G
HTTPS percentage	52.4%	50.8%	54.9%	57.3%	55.4%
Total apps	211	211	195	187	195
SaaS apps	35	36	33	28	32
IaaS apps	23	27	29	25	26
Streaming apps	21	20	16	14	15
Social apps	17	17	14	13	14
RAS apps	4	4	4	4	4
Proxy apps	4	5	4	4	4
Gaming apps	3	3	2	2	2
P2P apps	2	1	1	1	1
Daily website visits	571	595	502	411	404

FIGURE 1. QUARTERLY INFRASTRUCTURE TRENDS. VALUES REPRESENT THE MEDIAN PER ORGANIZATION.

Taking it from the top of Figure 1, the ratio of HTTPS vs. HTTP traffic is slightly off last quarter's high mark, but the overall upward trend remains. This represents a net positive for Internet privacy but can be challenging when it comes to detecting threats that may use encrypted communications for cover. We have shown in previous reports that such environments aren't rare; many firms encrypt the majority of their traffic, while others encrypt very little.

The median number of applications used per firm seems to be flat or trending slightly down in most categories. There are many possible reasons for this, including changing demographics of companies in the assessment program, paring down and/or consolidation among apps, and perhaps even stricter policies against historically risky apps like peer-to-peer (P2P) software.

Figure 2 compares infrastructure statistics among three groups based on the number of employees within the organization. For a refresher on box plots, read this, but you can keep things simple by knowing the dark line in the middle of the colored boxes corresponds to the median—which can be compared to overall stats from Figure 1. Your immediate reaction may be something like "So, bigger firms use more apps and do more stuff on the web—so what?" It's true there's nothing terribly unexpected here, but it does remind us that more stuff used equals more stuff to protect. As networks grow larger and more complex, this very often becomes the proverbial Achilles heel of growing organizations.

If you are responsible for a firm going through such growing pains, there are ways of keeping your attack surface in check. Regardless of size, it's good practice to limit applications to those necessary for business use. Even among those, restricting who can use them and how they can/should be used will help keep things from getting out of hand too quickly. Monitoring those applications—whether on-premises or in the cloud—becomes more important as usage and users increase.

A couple of points from Figure 2 bear mentioning because they buck the "bigger = more" trend. The first is HTTPS ratio. Smaller firms look to encrypt a bit more of their traffic on average than their larger brethren. They may find it easier to do so for various reasons, including a greater freedom to adopt newer applications without being bound by legacy technology. The second nonconformist is cloud applications, specifically IaaS. This likely reflects midsize firms seeking the cost and scalability advantages of cloud environments over on-premises appliances. Larger organizations, on the other hand, are often heavily invested in hardware that needs to be used and generally more predisposed to keeping their applications and data in-house when possible.

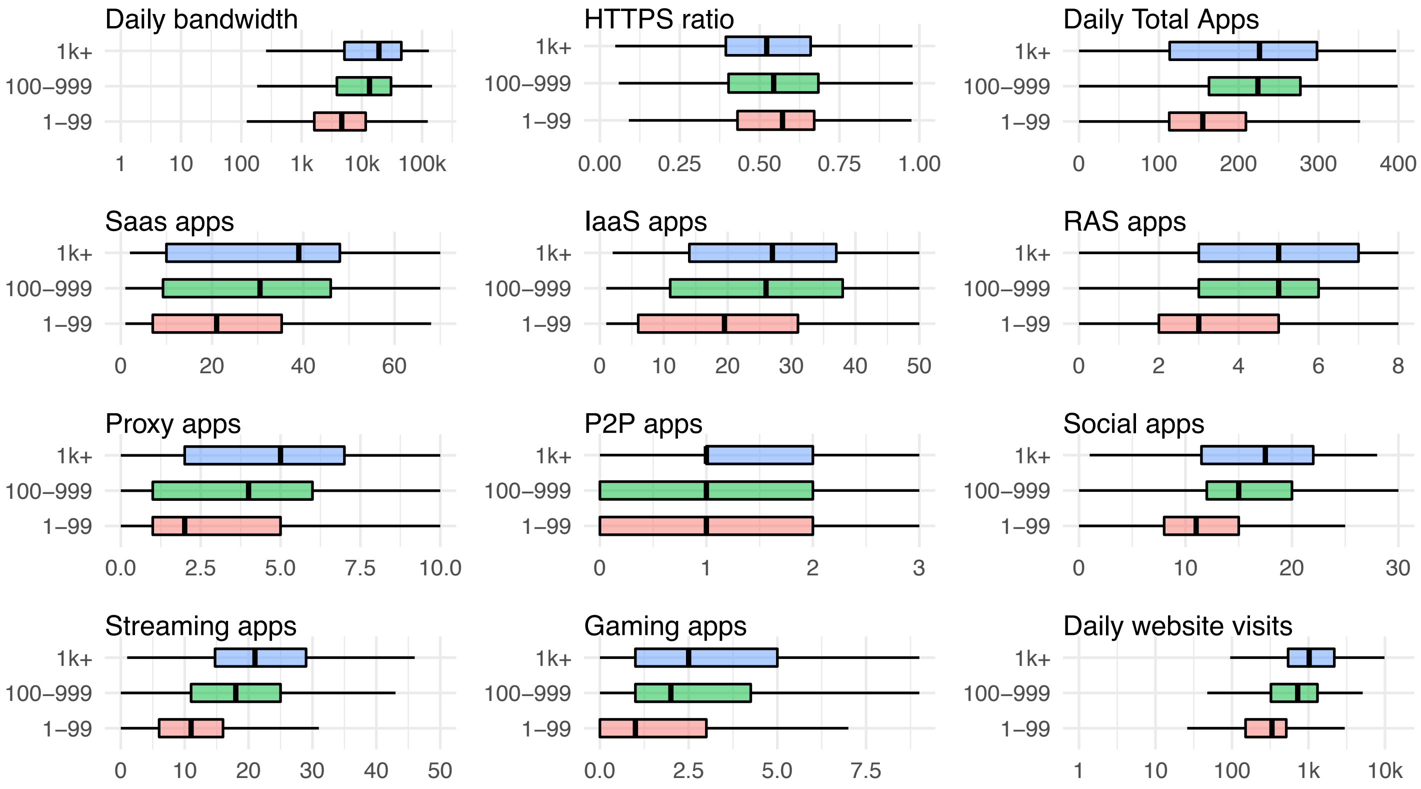


FIGURE 2. COMPARISON OF INFRASTRUCTURE USAGE STATISTICS BY FIRM SIZE.

THREAT LANDSCAPE TRENDS

THREAT LANDSCAPE TRENDS

EXPLOIT TRENDS

Exploit trends grant a view into adversary attempts to identify and compromise vulnerable systems. Triggering one of the multibillion detections recorded this quarter doesn't mean the attack succeeded or even that the targeted vulnerabilities existed in the environment. Because exploit activity tends to be rather noisy, we've restricted our analysis to only critical and high-severity detections for this section.

QUICK STATS:

- 5,973 unique exploit detections
- 153 exploit detections per firm
- 79% of firms saw severe attacks
- Top exploit against Apache.Struts reported by 35% of firms

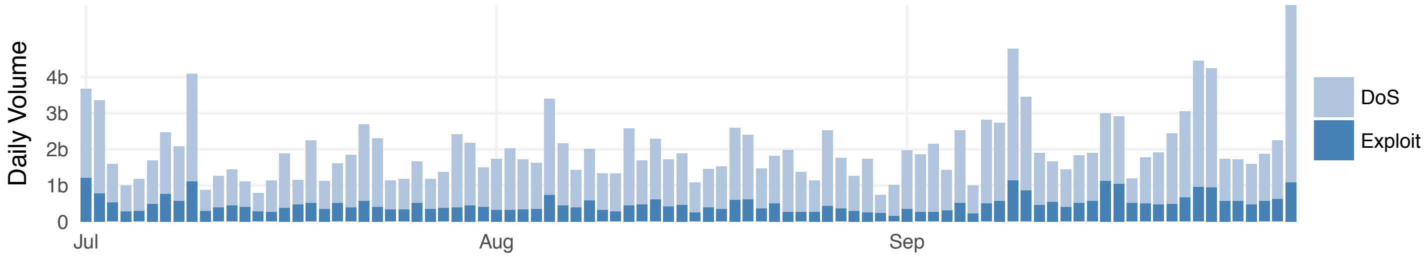


FIGURE 3. QUARTERLY APPLICATION EXPLOIT ACTIVITY.

Exploit volume over Q3 was fairly steady, picking up slightly toward the end of the quarter with a few noticeable spikes. Investigating the spikes in September prompted us to distinguish denial of service (DoS) activity from other types of exploits in Figure 3, the former being primarily responsible for the spikes, obviously. The main offenders were low-severity detections, which reinforces our decision to filter such background noise from the subsequent charts.

Figure 4 lists the 20 most-prevalent exploits in Q3 2017 as well as the most-targeted vulnerabilities (CVEs) by volume. Many of them are repeat offenders quarter after quarter, and they have gotten plenty of airtime in previous reports. As a high-level observation, they generally fall into the command/code execution, code injection, DoS, buffer overflow, or brute force categories. Knowing what kind of vulnerabilities attackers probe for most often can be helpful in deciding which ones deserve priority for patching efforts. We hope Figure 4 helps you ask some pointed questions like "Have we seen these alerts?" and "Do our scans detect these vulnerabilities?"

The current poster child for patching priority is CVE-2017-5638 and its corresponding detection signature *Apache.Struts.Jakarta.Multipart.Parser.Code.Execution* (top detection in Figure 4). If that sounds curiously familiar, then you either read the introduction of this report or you've probably been paying attention to the news lately. That exploit targets a flaw in the Apache Struts framework that attackers leveraged to nab approximately 145 million records from credit bureau Equifax.

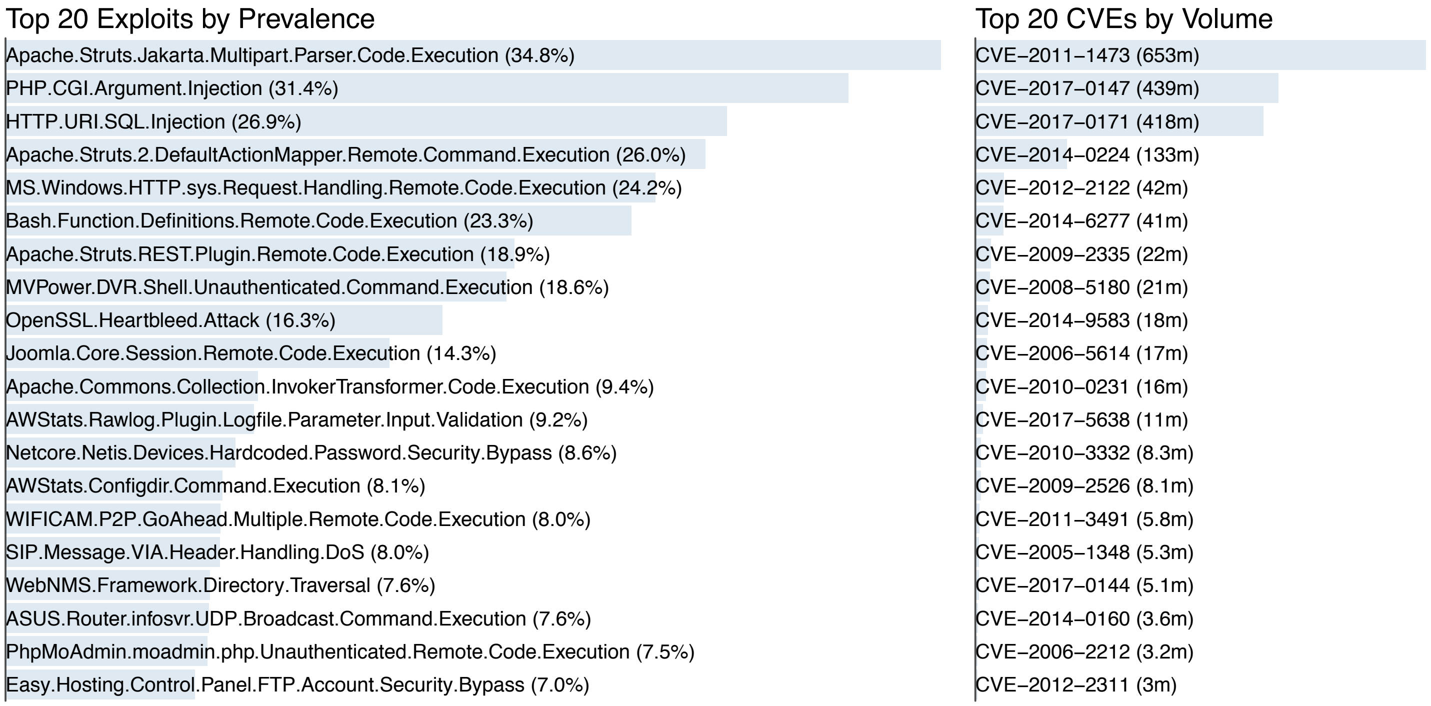


FIGURE 4. TOP EXPLOIT DETECTIONS BY PREVALENCE AND TOP CVEs BY VOLUME.

Thankfully, you needn't wait for an Equifax-like event to motivate action. For instance, perhaps you read our March 17 Weekly Threat Brief in which we stated this critical vulnerability was among our top detections for the week following its release. Or perhaps its appearance as the most prevalent exploit in this Threat Landscape Report for two quarters running got your attention. The point is, data like this can help you see and avoid disaster—use it!

Exploit detection signature	**CVE (if applicable)**
FlashChat.Arbitrary.File.Upload	N/A; Unpatched
Apache.Tomcat.Remote.Exploit.Account.Scanner	N/A; Unpatched
WordPress.WP.EasyChart.Unrestricted.File.Upload	CVE-2014-9308
MS.IE.CAttrArray.Object.Handling.Code.Execution	CVE-2015-2452

FIGURE 5. EXPLOITS WITH LARGEST GROWTH IN PREVALENCE FOR Q3 2017.

Apart from *THE* Apache exploit, two others against the popular Struts framework took top spots in Figure 4, and another against Apache Tomcat made the list of major movers in Figure 5. We shouldn't be too surprised by this; Apache is one of the most popular server platforms on the web. Add Figure 5 to your set of diagnostics from Figure 4.

Since the Apache Struts framework seems to be a theme among exploit activity this quarter, we'll devote a little more page space to it before we switch topics. Figure 6 shows daily fluctuations (light gray lines) and trend (dark colored lines) for the three Apache Struts exploits listed in Figure 4. The uptick after Equifax's breach announcement is quite pronounced, demonstrating that attackers exhibit shark-like qualities when they smell blood in the water.

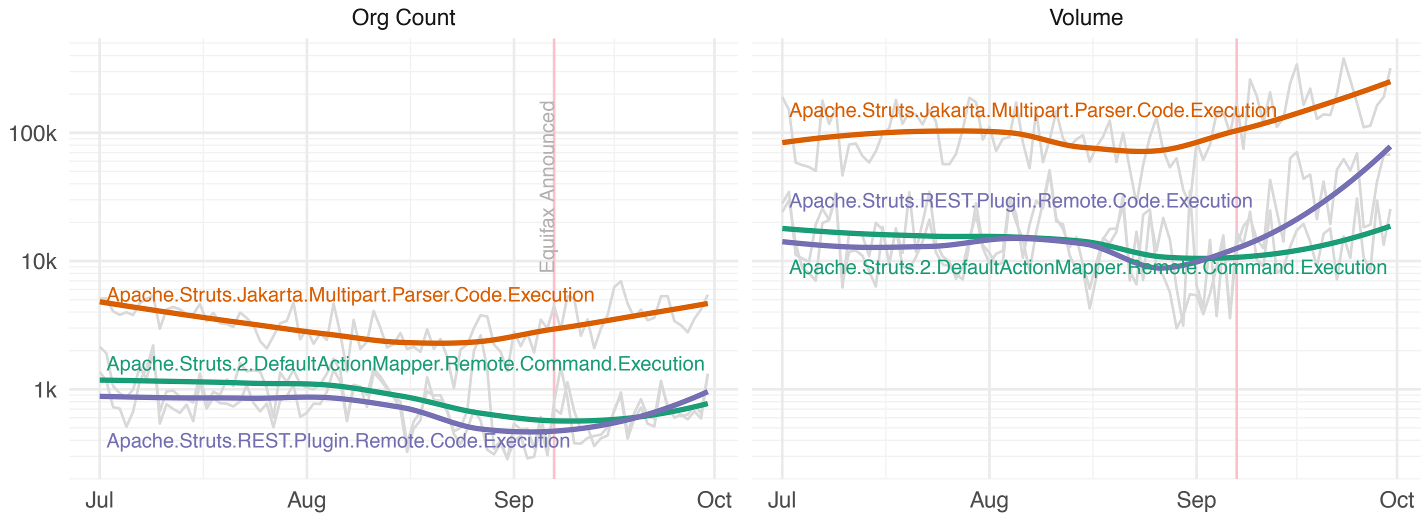


FIGURE 6. TOP EXPLOITS AGAINST APACHE STRUTS IN Q3 2017 BY PREVALENCE AND VOLUME.

EXPLOITS AGAINST SCADA SYSTEMS

While we tend to highlight prominent threats in this report like those against Apache Struts recently, it's good to remember that many relevant threats may fly below the radar and/or have severe consequences that spill over beyond the organization in which they occur. Take, for example, exploits listed in Figure 7, which target various types of supervisory control and data access (SCADA) systems. Only one crosses the 1/1,000 threshold on the prevalence axis and none were observed by more than 1% of reporting firms. Similarly, volume measures are orders of magnitude below leaders in that metric. Does that mean such exploits can be safely ignored if/when you see them? Well, if your organization doesn't use SCADA systems, perhaps. If it does, however, consider Figure 6 a critical expansion pack to your patch prioritization. Enterprise network intrusions and outages are bad, but breaches into SCADA environments put the physical infrastructure on which many lives depend at risk.

The detection nomenclature is fairly intuitive, so the best way to use Figure 7 is to look for products used by your organization. You can find more information on these exploits from our Threat Encyclopedia and/or the manufacturer's website.

Those interested in more general information about securing SCADA environments can start with this "SCADA Security 101" post from our blog. Beyond that, the North American Electric Reliability Corporation (NERC), Electricity Information Sharing and Analysis Center (E-ISAC), and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) are great resources for any organization responsible for the security of industrial control systems of all types.

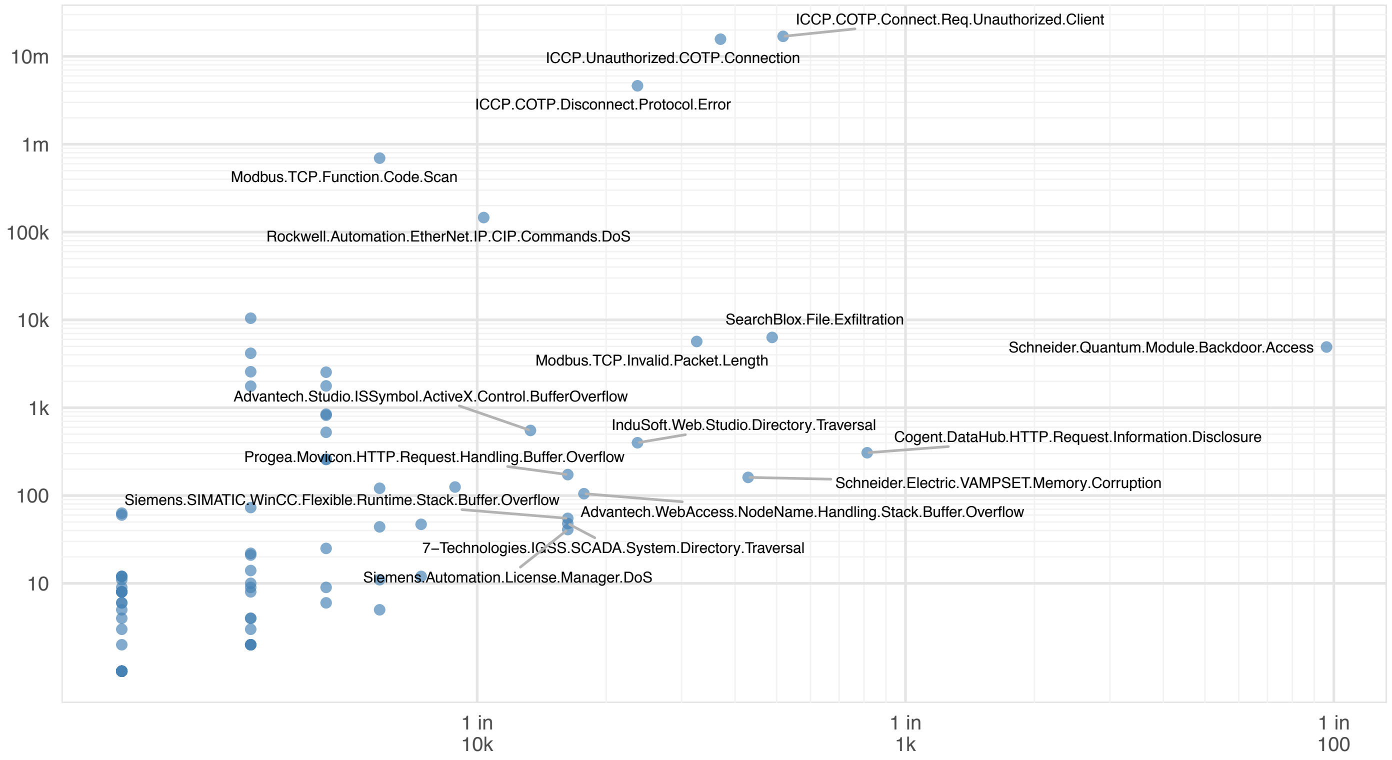


FIGURE 7. ALL Q3 2017 SCADA EXPLOITS PLOTTED BY PREVALENCE (X) AND VOLUME (Y).

MINI FOCUS: **ZERO-DAY RESEARCH**

Here at Fortinet we have a dedicated team of expert researchers and analysts that examine many third-party products and software applications daily, looking for weaknesses and exploitable vulnerabilities. And as the Quick Stats to the right suggest, we manage to find no shortage of them.

Quick Stats:
8 zero days announced in Q3 2017
63 zero days discovered in Q3 2017
185 zero days discovered YTD 2017
503 zero days discovered since 2006

Because we follow responsible disclosure, we will notify the vendor upon discovering a zero day before we announce it publicly. This allows the vendor time to create a patch, which could take a few months or longer due to the complexity of some vulnerabilities. But don't worry—our FortiGuard Labs team simultaneously creates a zero-day IPS signature to protect our customers from the vulnerability even if it hasn't been publicly announced. For those customers using our IPS service, you may see from time to time signatures that will end in the ".0day" extension. This means that the vulnerability is still in an unpatched state and we do not want to identify the product via the signature as we normally do.

Below is a list of zero-day vulnerabilities that were announced in Q3 2017 by FortiGuard Labs. Our risk levels are aligned with the standard CVSS scoring. To find out more information about the vulnerability, please visit our Zero Day web link https://fortiguard.com/zeroday).

Detection	Detection	Product	Vulnerability	Risk
July Announcements				
FG-VD-17-107	Multi-byte Character Filtering Cross-Site Scripting Vulnerability II	Joomla	CVE-2017-7985	High
FG-VD-17-108	Core Line Feed Character Cross-Site Scripting Vulnerability I	Joomla	CVE-2017-7985	High
FG-VD-17-109	Core Line Feed Character Cross-Site Scripting Vulnerability II	Joomla	CVE-2017-7985	High
July Announcements				
FG-VD-17-142	Embedded Open Type Font File Handling Memory Corruption	Microsoft	CVE-2017-8691	High
FG-VD-16-062	AVG Self-protection Bypass by disabling AV update	AVG	N/A	Med
FG-VD-17-018	Bitdefender AVC3 Driver Local Privilege Escalation	Bitdefender	N/A	High
July Announcements				
FG-VD-17-019	Bitdefender Kernel Driver Self-Protection Bypass	Bitdefender	N/A	Med
FG-VD-16-043	Cisco Web Security Appliance Cross-Site Scripting Vulnerability	Cisco	N/A	Med

FIGURE 8. ZERO-DAY VULNERABILITIES ANNOUNCED BY FORTIGUARD LABS DURING Q3 2017.

Note that Figure 8 includes three vulnerabilities affecting AV software. Attackers usually try to evade AV software to remain undetected, but will sometimes attempt to exploit a weakness in the software itself to gain control. An example of this would be the DoubleAgent attack that was discovered earlier this year. Take this as a reminder that although AV software is there to protect you from malware, it can also be a target. Ensure you are vigilant with patching these technology controls, especially since they usually run at higher system privileges.

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:

- 14,904 unique variants
- 2,646 different families
- 25% reported mobile malware
- 22% detected ransomware
- 15 families spread to ≥1/10 firms

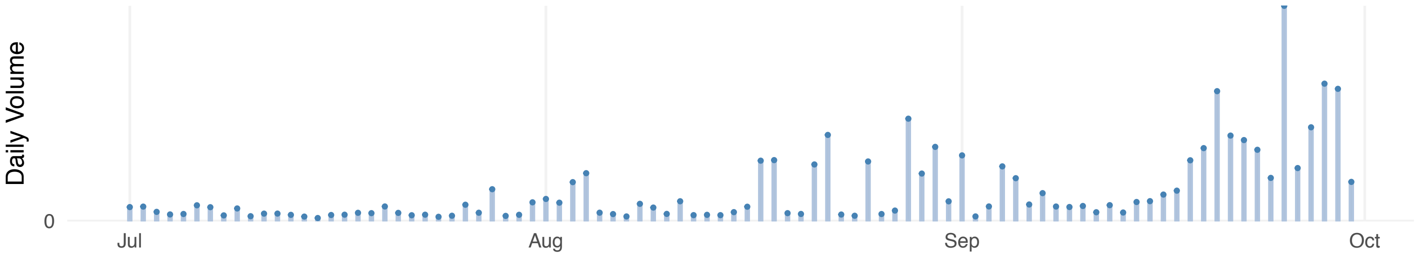


FIGURE 9. QUARTERLY MALWARE DETECTION VOLUME.

Malware distributors take vacations too. That's the immediate takeaway from Figure 9, which shows a long lull over the summer followed by some sporadic activity in late August that transitions into full swing by mid-September. We can't help but wonder where they go—the ***Mal***dives, perhaps?

Figure 10 plots every unique malware family detected (2,600+) by our sensors in Q3. The x-axis corresponds to prevalence, volume is on the y-axis, and intensity determines the size of the dot (larger = greater). Notice that axes are shown on a logarithmic scale, making transitions between grid lines much larger than they appear. Malware detected by at least 1/10 firms or above a volume of 100K bears a label. We present malware in higher-order families here to emphasize broader trends, but those wanting more variant-level information can check out our Weekly Threat Briefs and our Security Blog.

As was the case with exploits, we've seen most malware from Figure 10 repeatedly in previous reports. The most common functionality among those in the upper right quadrant is downloading, uploading, and dropping files or other malware onto infected systems. The Agent and Nemucod families are prime examples of this behavior. Malware strains that establish remote access connections, capture user input, and gather system information litter the pack as well (e.g., W32/Backdoor and W32/PECompact). As an interesting observation, our archives show Q3 marks the first time we've seen four mobile malware (Android) families gain label-worthy status. All told, roughly one in four firms detected mobile malware.

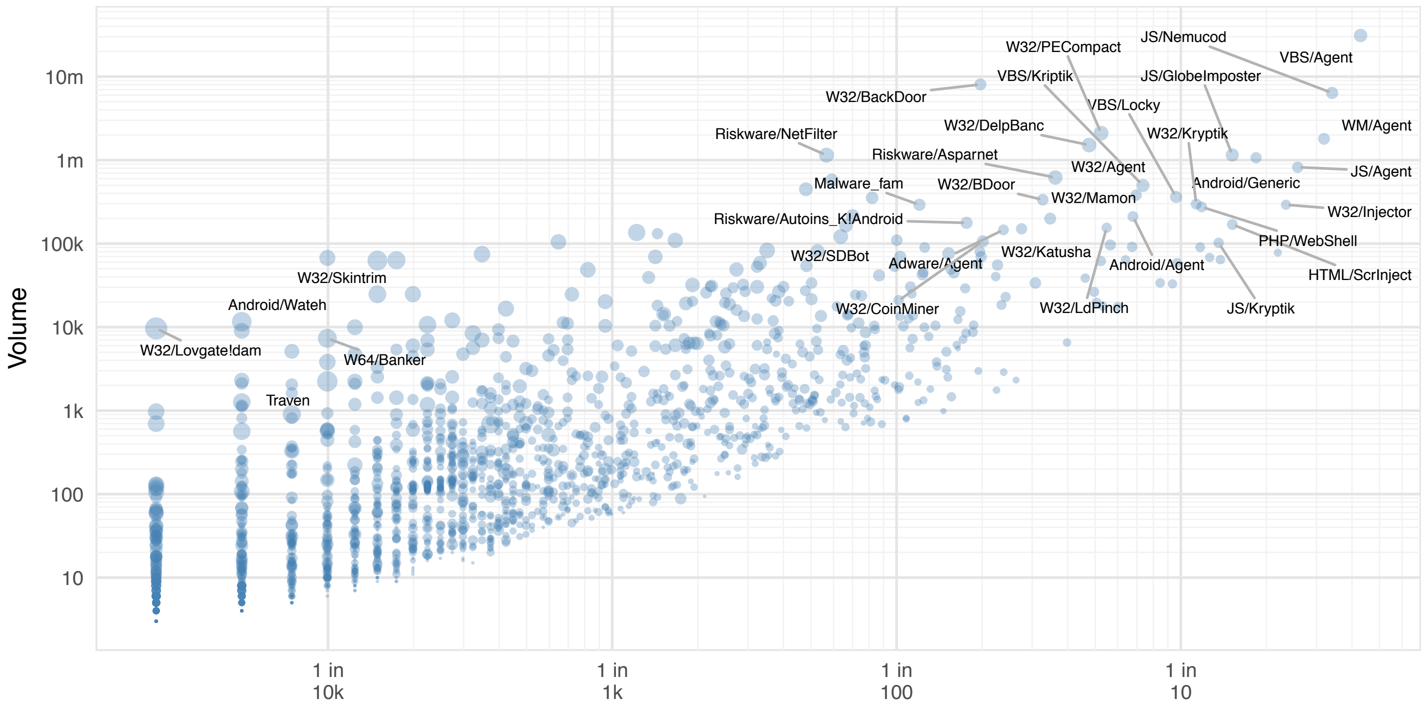


FIGURE 10. ALL Q3 2017 MALWARE FAMILIES PLOTTED BY PREVALENCE (X), VOLUME (Y), AND SEVERITY (DOT SIZE).

One newcomer breaching the 1 in 10 firms barrier is the JS/GlobeImposter ransomware family. Our sensors began picking up variants from this family in late July, and our research team posted their analysis soon thereafter. GlobeImposter isn't terribly remarkable as ransomware goes, but is noteworthy due to its rapid rise and widespread nature. Other major movers over the quarter can be found in Figure 11.

Standouts from Figure 11 include W32/DelpBanc (Trojan detection exhibiting varying behavior), HTML/ScrInject (remote access Trojan), and VBS/Locky (ransomware). W32/DelpBanc jumped an impressive six orders of magnitude in volume and four along the prevalence axis. Let's hope it stops to catch its breath in Q4.

Speaking of taking a breather, the infamous Locky ransomware seems to have been doing just that over much of 2017. But it re-entered the game this quarter with a vengeance, showed off some new skills, and was reported by about 1 in 10 organizations. The early August Diablo6 campaign spread via waves of attachment-laden spam messages pushed by the Necurs botnet. Within a week, Locky launched another campaign dubbed Lukitus, which was several times larger than Diablo6, according to our sensors. In both campaigns, opening the attachment downloads and executes the Locky ransomware, beginning the irreversible encryption process on the victim's computer. Some new malicious domains facilitated the spread and a few Windows registry hacks aided persistence.

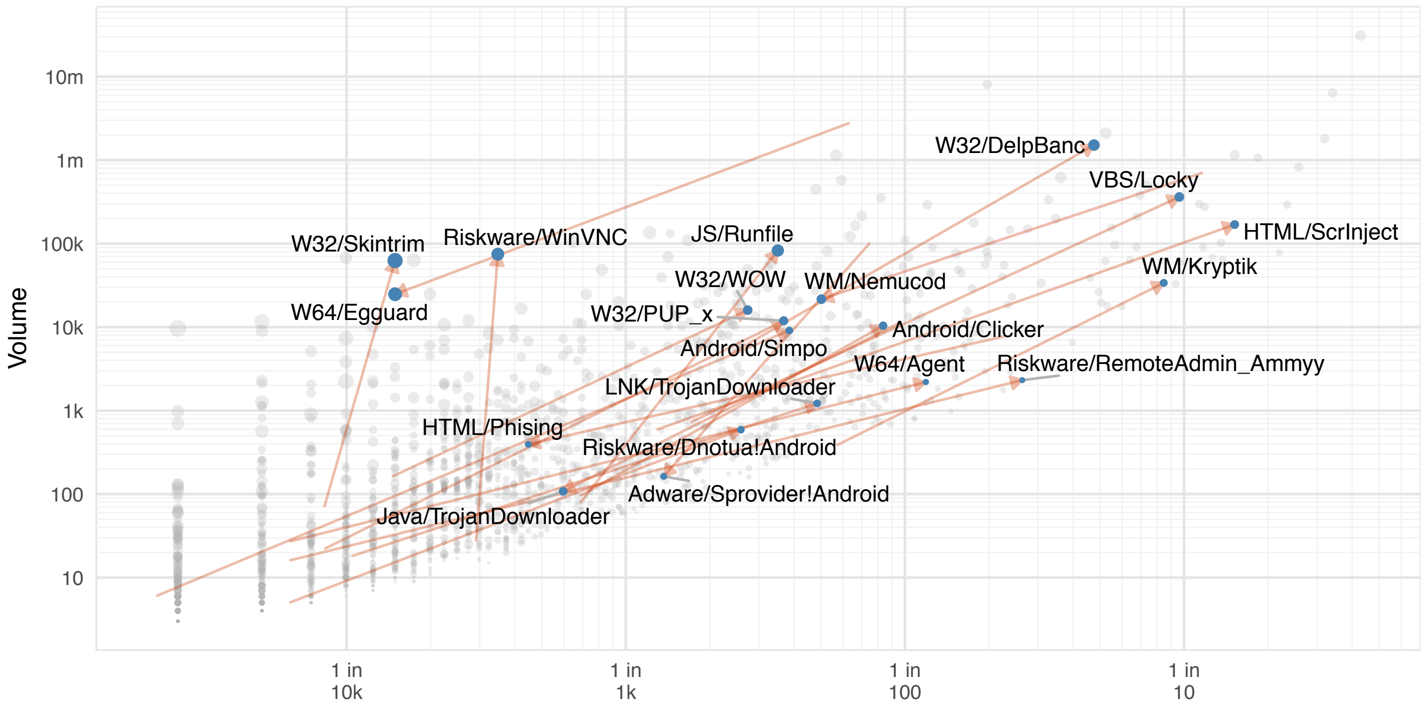


FIGURE 11. MAJOR MOVERS AMONG Q3 2017 MALWARE. ARROW SHOWS Q2 TO Q3 MOVEMENT.

The third week of September brought with it yet another Locky variant, this time breaking the traditional mythology naming convention. The Ykcol campaign (Locky spelled backwards) retained the same basic functionality as the previous two waves, but was thoughtful enough to adjust the ransom price down from 1 BTC to 0.5 BTC, reflecting the increasing value of bitcoin.

That's a wrap for Q3 malware in this section, but stay tuned. We pick up this topic again in the Exploratory Analysis section and study how using risky applications affects the prevalence and volume of malware and botnets in your network.

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:

- 518 daily botnet comms per firm
- 245 unique botnets detected
- 3.5 infection days per firm
- 1.9 active botnets per firm
- 3% of firms saw ≥10 botnets

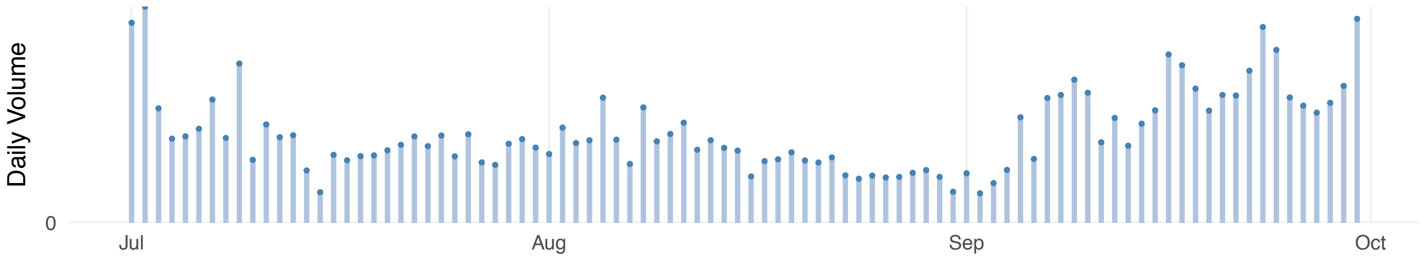


FIGURE 12. QUARTERLY BOTNET DETECTION VOLUME.

Overall botnet activity was down in Q3, due mainly to the dip apparent in Figure 12 that ran from mid-July through August. That does follow a gradual decline over Q2, so we're looking at a moderate drawback for the year so far. We're far from declaring victory over the bot herders, but we'll count our blessings as they come.

In terms of botnets that were most active over Q3, Figure 13 appears amazingly similar to Q2. Gh0st, Pushdo, Andromeda, Necurs, and Conficker remain the most prevalent—in the exact same order, no less. Add in Zeroaccess, H-worm, and IMDDOS and you also have a curtain call of the highest-volume botnets in both of the last two quarters.

Given such similar quarterly results, one might conclude there must be a large number of persistent botnet infections among firms reporting in to our dataset. In other words, we're seeing the same results because the same firms remain infected with the same botnets. But a glance at Figure 14 contradicts that conclusion because we see, for instance, that Gh0st and Pushdo are still spreading to quite a few new organizations each week.

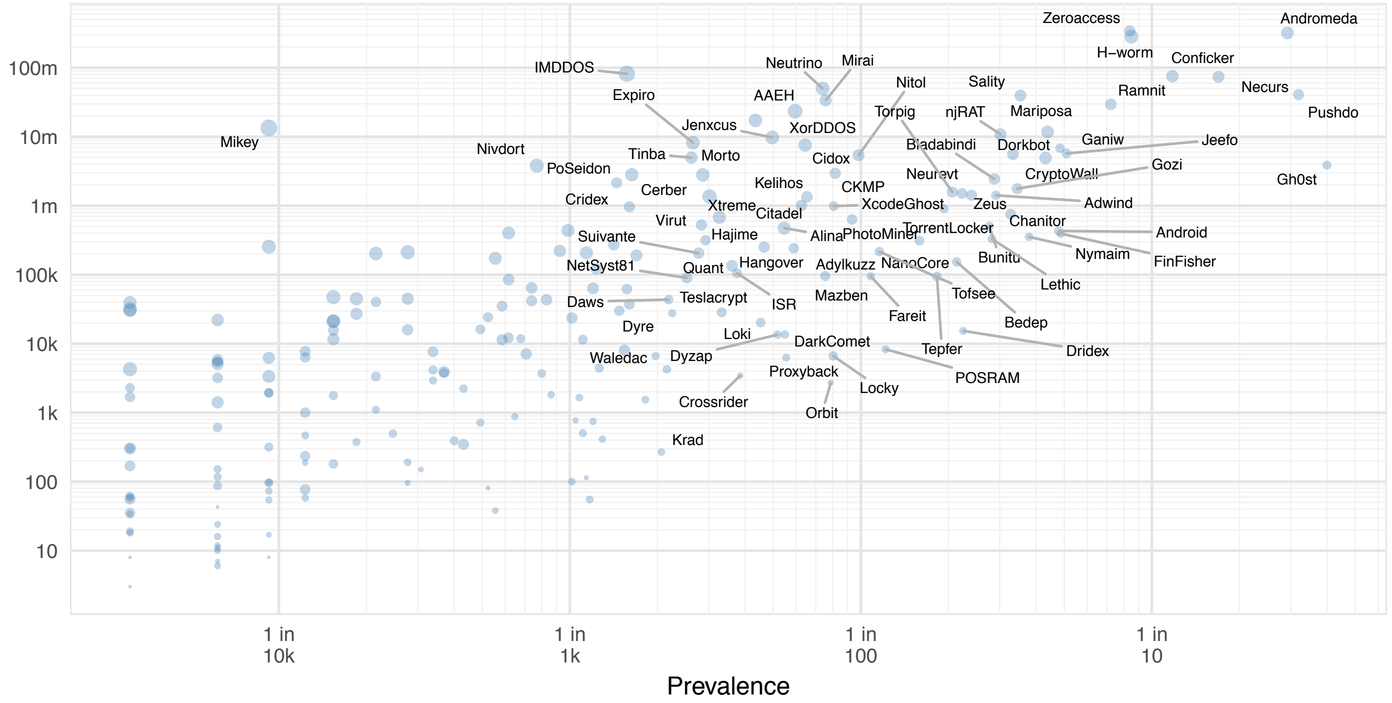


FIGURE 13. ALL Q3 2017 BOTNETS PLOTTED BY PREVALENCE (X), VOLUME (Y), AND SEVERITY (DOT SIZE).

That said, a little more data digging uncovered this interesting nugget: 75% of the organizations that reported Gh0st botnet infections in July also reported them in August, and 70% of those also reported September infections. But during those three months, firms typically detected Gh0st on four separate days (median = 4; mean = 11), which is rather counterintuitive given the previous finding.

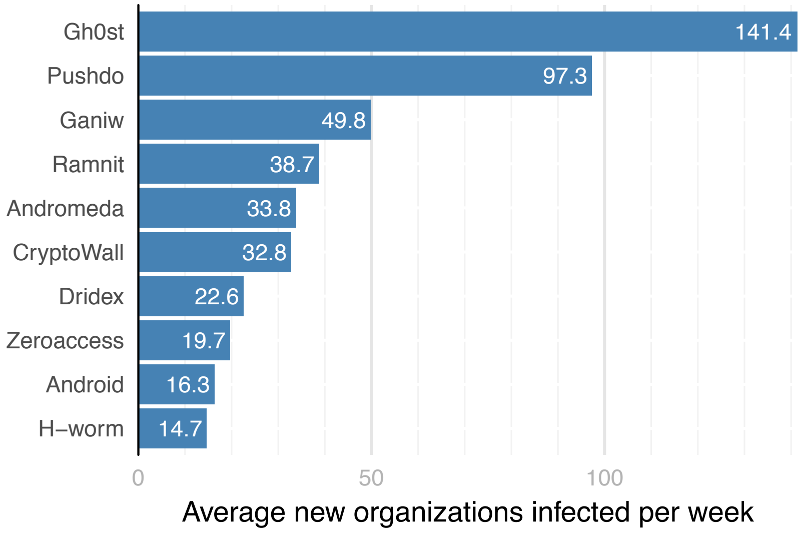


FIGURE 14. AVERAGE NUMBER OF NEW FIRMS REPORTING BOTNETS PER WEEK.

Our reading of these findings leads us to the notion of "periodic" vs. "persistent" infections. We imagine this plays out something like the famous arcade game Whack-a-Mole, where firms keep reactively squashing botnet infections as they pop up across the environment, but never eradicating whatever underlying issues cause them in the first place. We're using Gh0st as the example here because it was the most prevalent and fastest spreading over the quarter, but this general principle no doubt applies to other botnets in Figures 13 and 14.

Shifting gears but still heading in a similar direction, we were curious to see if botnet prevalence and type varied by organization size. Figure 15 borrows the same employee size buckets used in the Infrastructure Trends section and marks the percentage of firms in each group reporting the top botnets (colored bars form confidence intervals around those points). While Gh0st is still the most common across the groups, we do begin to see some variation among them. The Mariposa botnet, for example, was not observed within smaller firms. No larger organizations reported Neurevt infections.

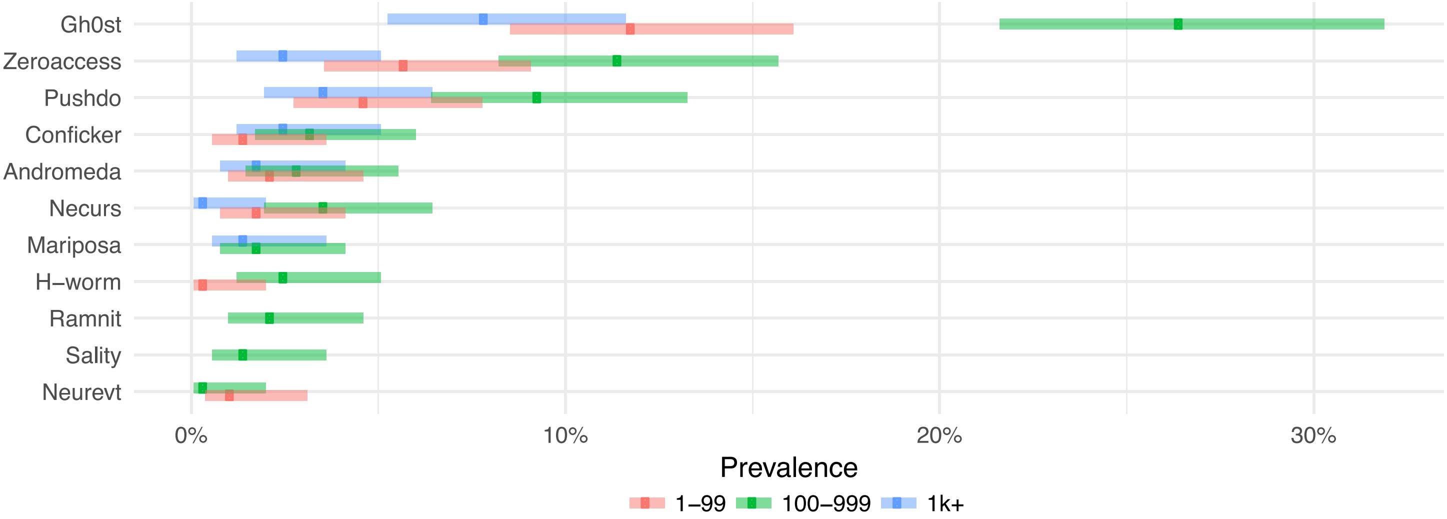


FIGURE 15. COMPARISON OF BOTNET PREVALENCE BY FIRM SIZE.

Perhaps most interesting is that midsize firms generally saw higher prevalence rates across the board. Overlapping confidence intervals notwithstanding, it may be that companies of this size represent a good "bang for the buck" for criminals. Smaller firms likely have less protection but also less (or less valuable) data. Larger firms certainly have the data, but also greater resources with which to protect it. Midsize firms typically have a large enough digital footprint to attract attention, enough valuable data to make them a worthwhile target, and yet not nearly the resources of their larger counterparts.

It's highly unlikely these results represent hard and fast rules (any firm of any size can be infected with any botnet), but they do suggest that organizations may be more or less susceptible to certain types of threats based on demographic factors like employee size. And we've shown similar differences (and similarities) among industry sectors and geographic regions in prior reports.

EXPLORATORY ANALYSIS

EXPLORATORY ANALYSIS

Last time we explored the relationship between certain potentially risky applications and threats detected across the network. The major finding was that firms exhibiting high usage of P2P and proxy apps observed 7x to 9x as many botnets and malware as those that don't use those types of applications. We found this relationship compelling and important enough to warrant further exploration. This quarter, we'd like to pick up where we left off and look more deeply at what specific types of malware and botnets are associated with these risky apps.

Figure 16 compares malware and botnet volume and prevalence between firms that use (reddish dots) and don't use (blue dots) P2P and proxy apps. Faint lines with arrows are used to show the shift or difference in volume and prevalence between the two groups. For instance, notice how the Gh0st is far more prevalent among P2P/proxy users (the rightmost red dot) than non-users (the blue Gh0st in the lower middle section of the grid). If there is no line, it indicates the non-P2P/proxy user group didn't have that malware or botnet. Zeroaccess is an example of this; being a predominantly P2P-spreading malware, it has no blue counterpart.

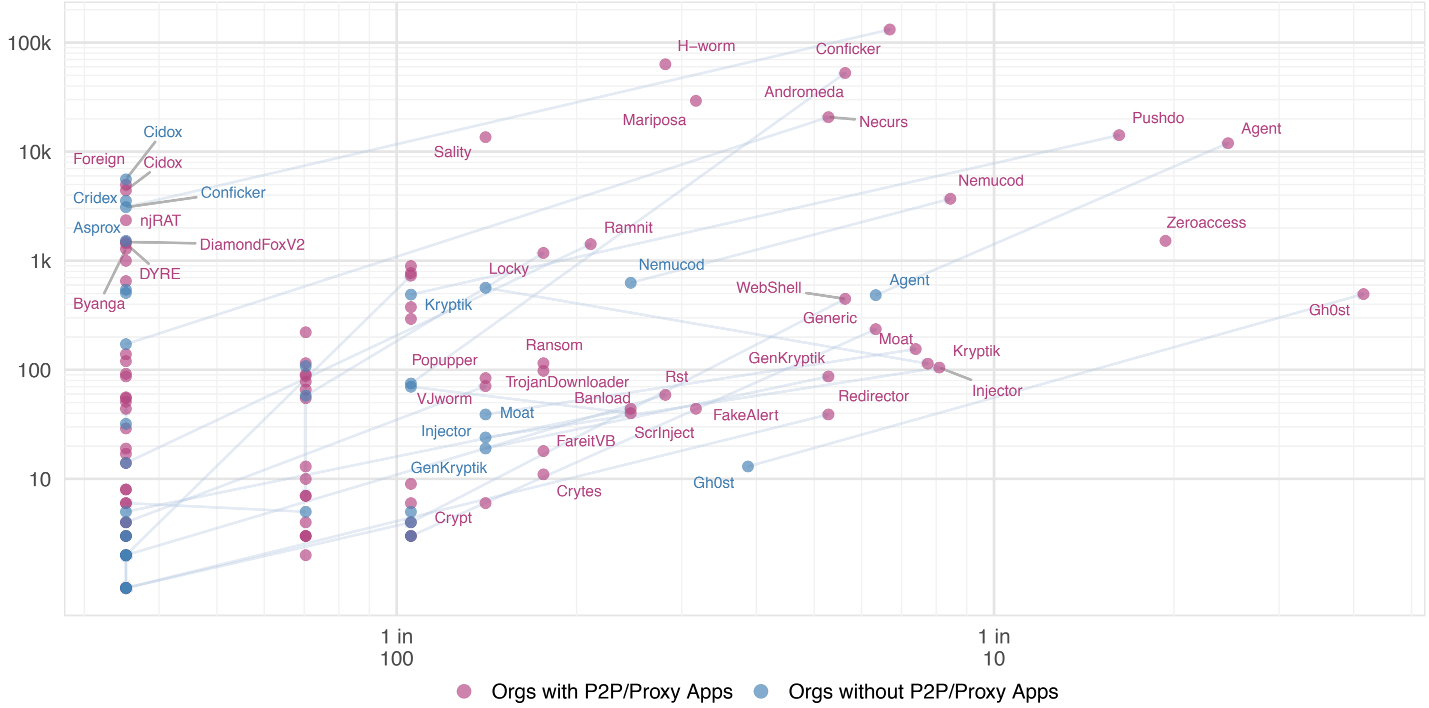


FIGURE 16. COMPARISON OF THREAT PREVALENCE (X) AND VOLUME (Y) BETWEEN FIRMS THAT USE (RED) AND DON'T USE (BLUE) P2P AND PROXY APPS.

You can think of Figure 16 as answering the question "If I'm going to allow P2P and proxy apps in my organization, what types and frequency of bad stuff are we likely to be exposed to?" In that sense, we find the plot quite thought-provoking. Notice how many more red threats there are than blue (you'll see threats you didn't before). Of those that do have a blue and red pair, the red usually moves up and to the right substantially (you'll see even more of what you saw before). Kinda forces you to ask whether the benefits are worth the cost, doesn't it? Well, it should. And maybe they are—only you can decide that. We just want to help you make an informed decision.

CONCLUSION AND RECOMMENDATIONS

CONCLUSION AND RECOMMENDATIONS

We appreciate you spending your valuable reading time with us again this quarter. Hopefully we've given you some useful perspectives on the global threat landscape that you can take back to your neck of the woods. To finish off all the statistics we shared in the previous pages, we'll leave you with some data-driven recommendations based on what we observed in Q3 2017. And as always, we're here if you have any questions related to this report or otherwise.

01

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 is a reminder that defenses should be spread along that chain as well. We recommend reviewing your current security posture to assess capabilities at each phase.

02

Whether it's WannaCry in Q2 or Apache Struts in Q3, long-known and yet still-unpatched vulnerabilities bite time and time again. Pay close attention to critical patch releases and monitor intelligence sources for signs of pre-attack activity and exploit development. We hope lists like we give in Figures 4 and 5 will aid you in this pursuit.

03

In addition to remaining vigilant of new threats and vulnerabilities in the wild, make sure not to lose sight of what's happening within your own environment. Network hygiene and device hygiene are perhaps the most neglected elements 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.

04

If your organization houses SCADA or other types of industrial control, the first step is to fully assess associated business and operational risks and to define an appropriate strategy commensurate with those risks. A major part of this will include defining the zones, conduits, boundaries, and security levels, which will be invaluable for limiting communications between SCADA and non-SCADA systems. Additional SCADA security basics can be found in our "SCADA Security 101" blog post, and you may also wish to learn more about our Industrial Security Service.

05

It's not news that malware gets more pervasive and evasive over time. But the fact that so many high-variant downloaders and droppers topped our charts again 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.

06

The Locky ransomware saw a resurgence this quarter, but our standard advice remains solid. The best defense against ransomware like Locky is deploying web-filtering techniques, using effective email security tools that include both antispam technology and the ability to detect and eliminate malicious email attachments, and above all, maintaining a current off-network backup of your critical data in case of infection.

07

One in four firms reported mobile malware in Q3. 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

Findings show that many organizations suffer recurring periodic botnet infections. Rather than just playing Whack-a-Mole across thousands of endpoints, mature your capability to detect and sever botnet communications at key chokepoints in your network through a combination of smart tools and good intel.

09

Midsize firms deal with more than their fair share of security problems. Right-size this situation by focusing hard on the basics. That includes taking inventory of authorized and unauthorized devices, limiting user privileges—especially administrators, limiting applications in your environment to only those with a business need, and keeping those applications and systems up to date and fully patched. Of course, larger enterprises would do well to follow these recommendations too.

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.

FORTINET®

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

Nov 17, 2017