FORTINET®

THREAT LANDSCAPE REPORT

Q4 2017

TABLE OF CONTENTS

Q4 2017 **INTRODUCTION AND KEY FINDINGS**

In many ways, the fourth quarter of 2017 was a montage of what played out before our eyes throughout the year. No one theme or threat stole the show such that everything else disappears into the background with time

Reaper breathed new life into threats targeting the Internet of Things (IoT). Key Reinstallation Attacks (KRACK) against WPA2 protocol pushed the word "nonce" out of the cryptographer's lexicon and into the mainstream. Ransomware added some sinister-sounding monikers like "Asasin" and "Bad Rabbit." Cryptocurrencies surged then crashed in value, and cryptomining attacks surged and crashed systems. The Andromeda takedown warmed our hearts, but FALLCHILL reversed that feeling.

Thank you for joining us once again as we process the past quarter together so we're all better prepared for those ahead. As always, we begin with some highlights and then dive into the details as seen by our global array of sensors.

Q4 2017 BY THE NUMBERS:

Exploits

- 5,988 unique detections (+0.3%)
- 274 detections per firm (+82%)
- 2% saw severe exploits (-7%)

Malware

- 17,671 unique variants (+19%)
- 3,317 different families (+27%)
- 22% detected ransomware (0%)

Botnets

- 259 unique botnets detected (+2%)
- 513 daily botnet comms per firm (-1%)
- 3.3% saw ≥10 botnets (+0.3%)

THAT'S SO TYPICAL. Readers of this report will recognize the "Infrastructure Trends" we show quarter after quarter in Figure 1. A common question that arises is how typical those stats are of all organizations. If you have that same question, we've added Figure 2 just for you.

STILL STRUTTING THEIR STUFF. Multiple exploits against the Apache Struts framework that made so much headway and so many headlines last quarter are still doing their thing. It's a continuing example of how attackers swarm when they catch scent of a widespread, vulnerable target.

SOME "THINGS" BREWING IN THE IoT. The arrival of the Reaper attacks and quadrupling of exploit activity against devices like Wi-Fi cameras in Q4 have our hackles raised about what's next. We share why and what we're watching for in the months to come.

SAY CHEESE. We all know human families come in many different forms. We present portraits of common malware families in Figure 11 that show it's no different for these threats.

RANSOMWARE TO THE TOP. Ransomware has been a common thread in these reports but this is the first time two different strains have led the pack. Locky was a lock-in for the most prevalent malware variant in Q4 and GlobeImposter proved itself no imposter by taking the No. 2 spot.

CRYPTOMINING MAL-WHERE? If you're not familiar with cryptomining malware (also sometimes called cryptojacking), you'll definitely want to check out our Mini Focus on that topic. We discuss the dramatic increase in these attacks and reveal where it's happening the most.

THAT FALLCHILL IN THE AIR. Our analysts monitored FALLCHILL threat activity closely in Q4 after the U.S. Department of Homeland Security, FBI, and US-CERT released indicators and research tying it to a North Korean APT group. FALLCHILL targets victims in the aerospace, telecommunications, and finance industries.

A LITTLE REGIONAL FLAVOR. In our Exploratory Analysis section this quarter, we seek to find the threats that exhibit the highest amount of variation across regions of the globe. What's on the menu in your neck of the woods? Read to find out!

SOURCES AND MEASURES

FORTINET

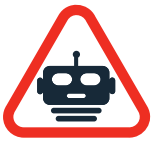
SOURCES AND MEASURES

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 October 1 through December 31, 2017. According to independent research, 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

FORTINET

INFRASTRUCTURE TRENDS

As has become our tradition, we begin this exploration of the Q4 2017 threat landscape not with threats, but rather with some trends about infrastructure and application usage. When looking at any landscape, we typically focus on what's at the top—trees, hills, water, and so forth—but we don't often think about what lies beneath all that. When it comes to the cyber threat landscape, the infrastructure statistics in Figure 1 offer us that underlying view of it all.

Why is such a view needed? Remember from our previous reports that strong correlations exist between infrastructure usage and threat frequency. For example, 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! That alone is sufficient justification to monitor these trends closely.

	Q1 2016	Q2 2016	Q3 2016	Q4 2016	Q1 2017	Q2 2017	Q3 2017	Q4 2017
Daily bandwidth	6.3G	7.7G	7.3G	8.5G	8.5G	6.4G	8.9G	10.6G
HTTPS ratio	52.5%	49.8%	52.4%	50.8%	54.9%	57.3%	55.4%	58.5%
Daily Total Apps	216	215	211	211	195	187	195	202
SaaS apps	33	35	35	36	33	28	32	37
IaaS apps	26	22	23	27	29	25	26	28
RAS apps	4	4	4	4	4	4	4	4
Proxy apps	4	4	4	5	4	4	4	3
P2P apps	1	2	2	1	1	1	1	1
Social apps	14	19	17	17	14	13	14	15
Streaming apps	17	24	21	20	16	14	15	15
Gaming apps	2	3	3	3	2	2	2	2
Daily website visits	600	590	571	595	502	411	404	364

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 a "typical" infrastructure profile and how that changes over time.

Comparing Q4 2016 to Q4 2017, we see both give and take. Firms appear to be using more bandwidth and encrypting more web traffic but visiting fewer sites and using fewer applications. The "more" part of that statement probably won't shock anyone, but the "fewer" part may prompt some head scratching. Several possible explanations exist for declining apps and website visits, but consolidation in the enterprise software market, migrations to cloud application suites, and the use of mobile devices for personal web browsing are high on the list from our perspective. Among applications, cloud apps are the only category that shows an increase (barely).

Figure 1 is useful for keeping an eye on trends at a macro scale, but as mentioned above, these statistics represent a diverse array of organizations. Obviously, not all firms visit exactly 364 websites or use 37 SaaS apps. The density plots[3] in Figure 2 are more conducive to getting a sense for how these measures vary across organizations in the CTAP program.

[3] We've removed the y-axis in these density plots because they aren't very meaningful to the purpose, which is to study how the distributions fell across the x-axis. The height of the bars/distribution basically means "a larger proportion of firms reported that x-axis value" and are comparable within each distribution.

Going back to the examples of website visits and RAS usage, Figure 2 reminds us why measures of centrality like median and mean can sometimes be misleading. Yes, many orgs visit hundreds of websites a day, but some show values of 22x the median! How productive they are while browsing 8,000 websites a day is a question we won't attempt to answer in this report (but who knows...maybe they use a pay-per-click business model). A similar pattern can be seen for SaaS applications; quite a few organizations use two or three times the median number (37) and a handful use hundreds of them.

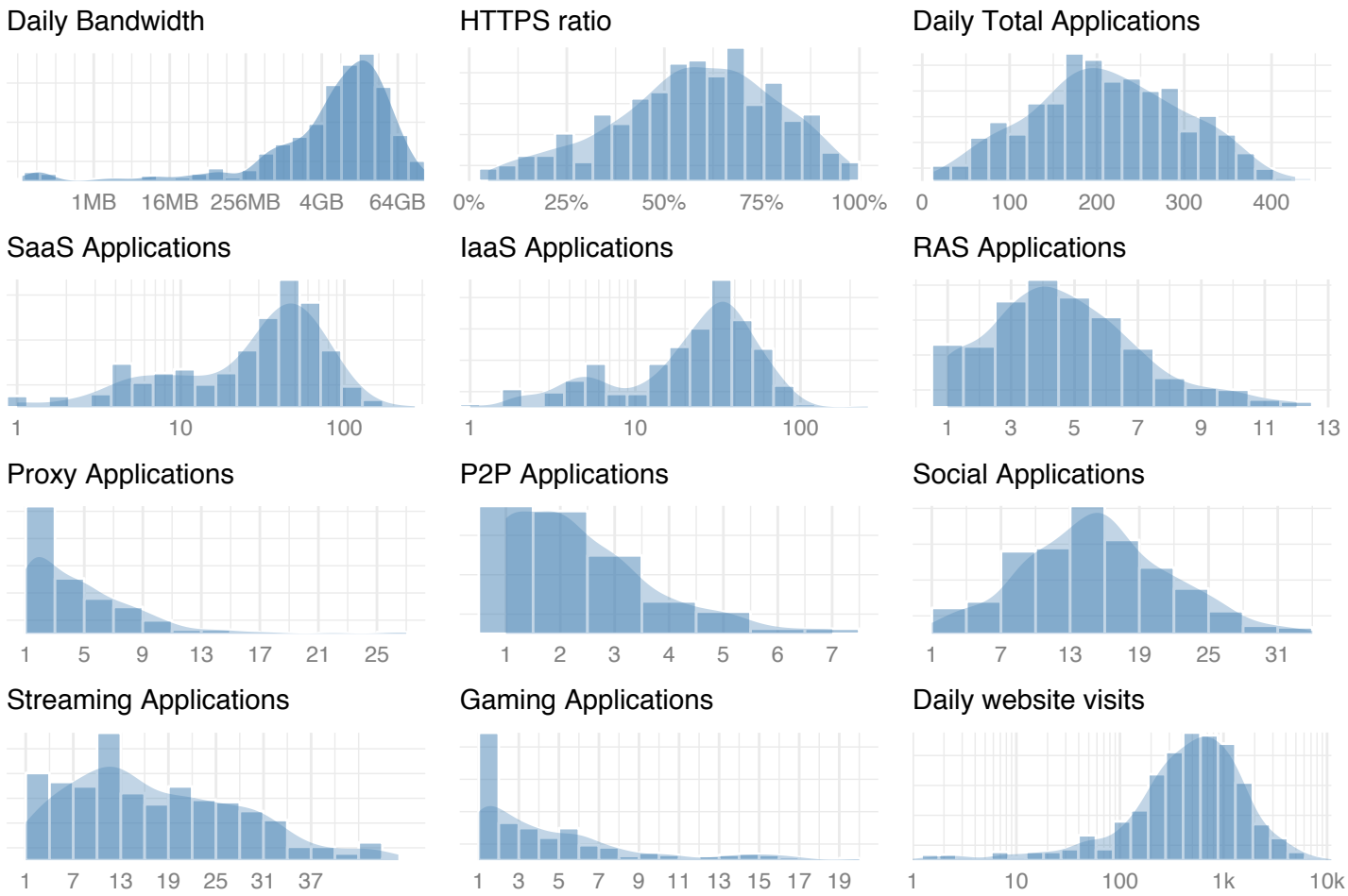


FIGURE 2. VARIATION OF INFRASTRUCTURE USAGE STATISTICS ACROSS FIRMS.

We have a special interest in keeping tabs on the HTTPS ratio. Figure 1 shows it's trending up and Figure 2 demonstrates that some firms encrypt nearly everything and some encrypt very little. That's important because, while helpful to maintaining privacy, higher encryption rates can present 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.

THREAT LANDSCAPE TRENDS

FORTINET

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:

- 5,988 unique detections (+0.3%)
- 274 detections per firm (+82%)
- 72% saw severe exploits (-7%)
- 37% still seeing exploit attempts targeting Apache Struts vulnerability (+2%)
- 33% recorded exploits of Wi-Fi camera devices (up 4x)

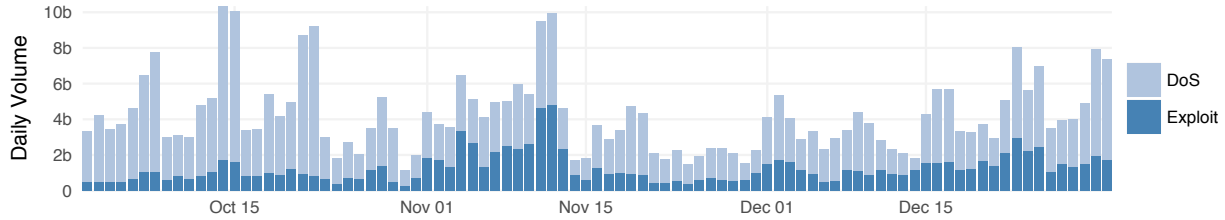


FIGURE 3. QUARTERLY APPLICATION EXPLOIT ACTIVITY.

The last day of Q3 posted the highest exploit volume for that quarter (~6B), which was a rather ominous sign heading into Q4. While several days met or exceeded that amount, Q4 turned out to be more of a return to "normal" after a summer hiatus than a major escalation in activity. That said, there was a lot of activity to go around and Figure 4 breaks that down for us.

In terms of the most prevalent detections, we see many of the usual suspects in Figure 4. Exploits targeting flaws in the Apache Struts framework remain high on the list after jumping in popularity among attackers in Q3 due to Struts' role in the Equifax breach.

If anything takes home the prize for the Q4 exploit-a-thon, it would have to be IoT-based attacks. Exploits against the GoAhead WIFICAM, MVPower DVR, Netcore/Netis devices, and Ubiquiti Networks airOS equipment all widened their spread across our sensors in Q4 and made the top 20. Notice none of these detections is associated with a known/named CVE, one of the many troubling aspects of the myriad vulnerable devices in the IoT.

WIFICAM detections, in particular, shot up the list. Eight percent of firms registered them in Q3 but Q4 brought 4x that amount. That's nowhere near the 25x surge in IoT detections we observed following the release of the Mirai botnet code in Q4 of 2016, but we can't help but sense some "things" stirring in the air.

In our last report, we featured attacks against industrial control systems (ICS), which are generally much more under the radar than those targeting more widespread applications. For instance, the most prevalent ICS-related detection according to our sensors in Q3 was reported by nearly 1 in 100 firms (no other ICS exploit crossed the 1 in 1,000 threshold). Since then, FortiGuard has seen a steady uptick in ICS exploit activity and our intelligence operations suggest these under-the-radar attacks might be climbing higher on attackers' radar.

Case in point is the recent revelations around the Triton (aka Trisis) attack. Triton is very sophisticated in nature and designed to target Triconex safety instrumental systems (SIS). SIS are designed to protect assets and ensure a safe and stable environment within a plant. Distributed Control Systems (DCS) allow the plant's operator to control industrial processes within their environment. Due to controlling costs and ease of use, plants are moving towards integrating DCS and SIS machines, making these systems a tempting target of attack.

Fortunately, in the case of Triton, plant operators discovered the attack when safety mechanisms put the SIS into failsafe mode as a precautionary measure. The discovery is nevertheless concerning because Triton looks to be designed to cause physical damage. Scenarios for achieving this include hijacking the SIS to terminate processes, run in an unsafe state, and manipulate other DCS controls. To cover its tracks, Triton will overwrite the malware itself with garbage data to thwart forensic analysis. Needless to say, FortiGuard researchers remain vigilant about this and other ICS threats.

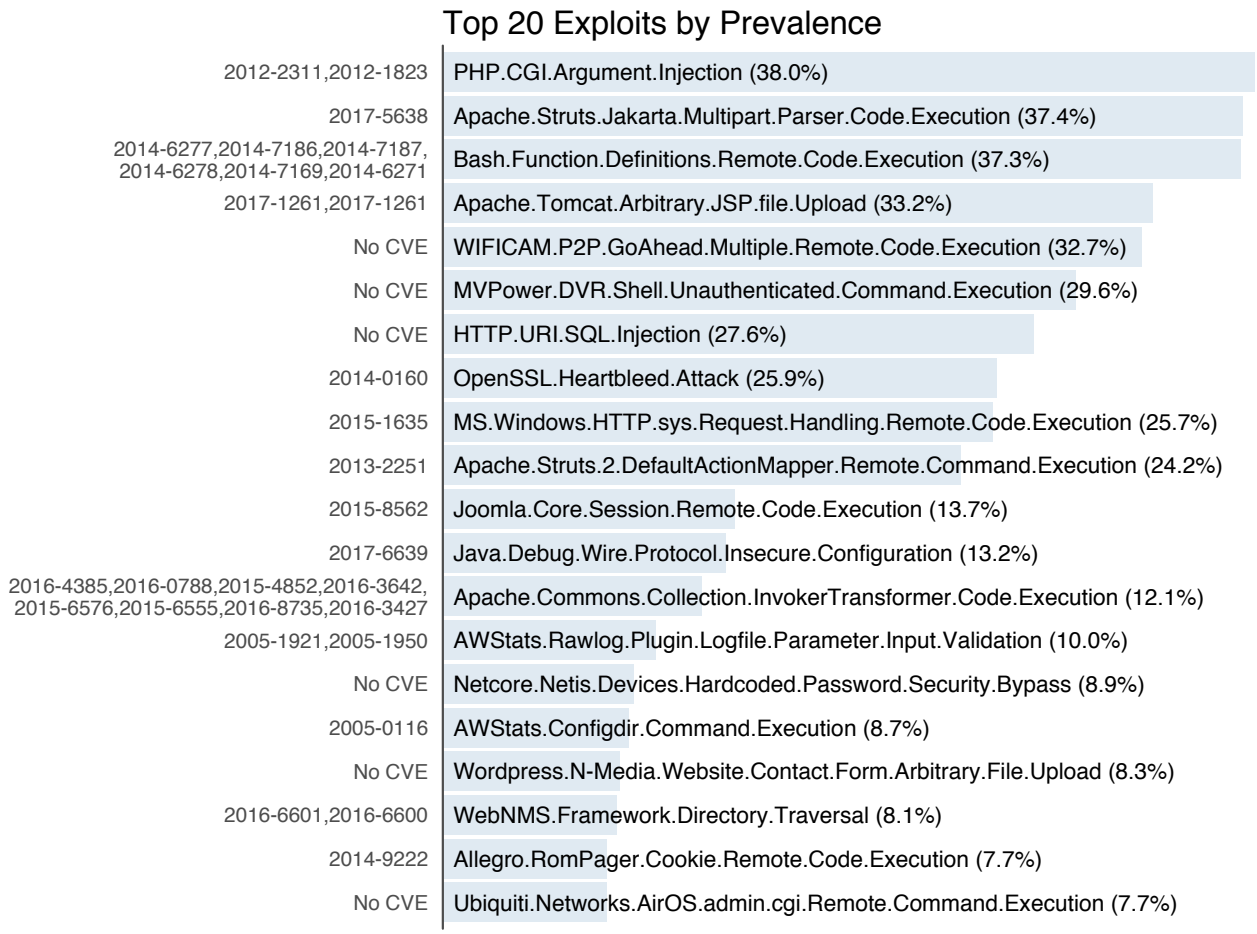


FIGURE 4. TOP EXPLOIT DETECTIONS BY PREVALENCE AND ASSOCIATED CVEs.

That sense of an impending storm was heightened with the recent arrival of the IoT-based Reaper attacks.[4] Reaper bears some similarities to Mirai, such as using parts of Mirai's codebase to infect IoT systems, but it also exhibits some significant evolutionary advances. For example, samples analyzed by FortiGuard Labs revealed that it has been armed with exploits covering nine different vulnerabilities spanning a variety of IoT vendors and devices (e.g., GoAhead's WIFICAM mentioned above). Mirai, on the other hand, focused exclusively on password cracking to amass its army of commandeered devices. Figure 5 plots exploit volume associated with Reaper over the quarter, and it captures an early October jump from 50,000 to 2.7 million over a few days before dropping back to normal.

Reaper is also especially concerning because it is built around a Lua engine combined with additional Lua scripts in order to run its attacks. Lua is an embedded programming language designed to enable scripts to run. So, even though the current Reaper threats we have seen to date appear to be benign, its flexible Lua-based framework means its code can be easily updated to include more malicious attack options. Needless to say, we're watching weather patterns closely to see how this all develops.

[4] https://blog.fortinet.com/2017/11/16/reaper-the-next-evolution-of-iot-botnets.

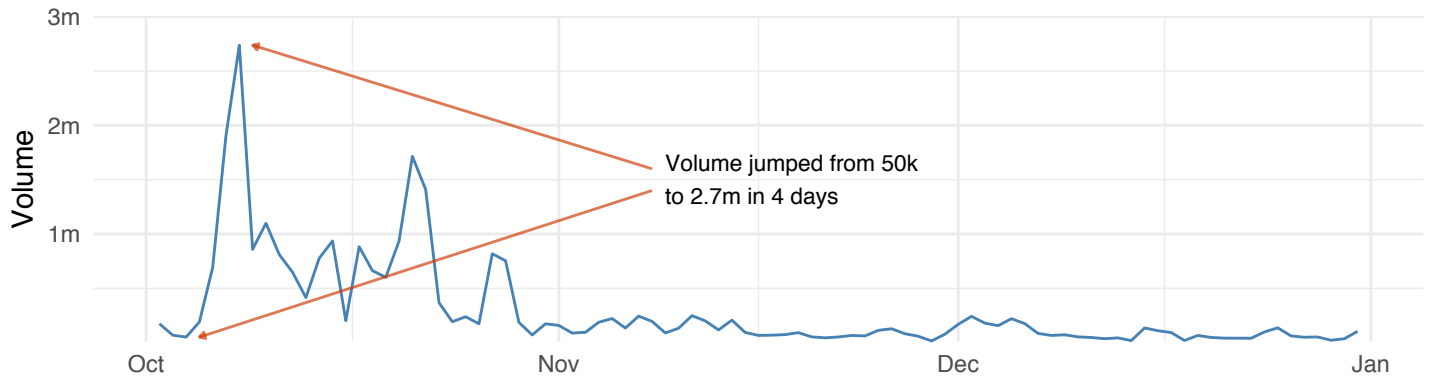


FIGURE 5: IOT EXPLOIT VOLUME ASSOCIATED WITH REAPER BOTNET.

Getting back to Figure 4, the detection signature names make it a bit difficult to get a "big picture" view of the exploit landscape. To help with that, we've trimmed detections down to just the final suffix (e.g., ".Injection"). This essentially categorizes thousands of exploits into a manageable number of (mostly) recognizable labels. We then plot those according to prevalence (x-axis), volume (y-axis), and intensity (dot size) in Figure 6.

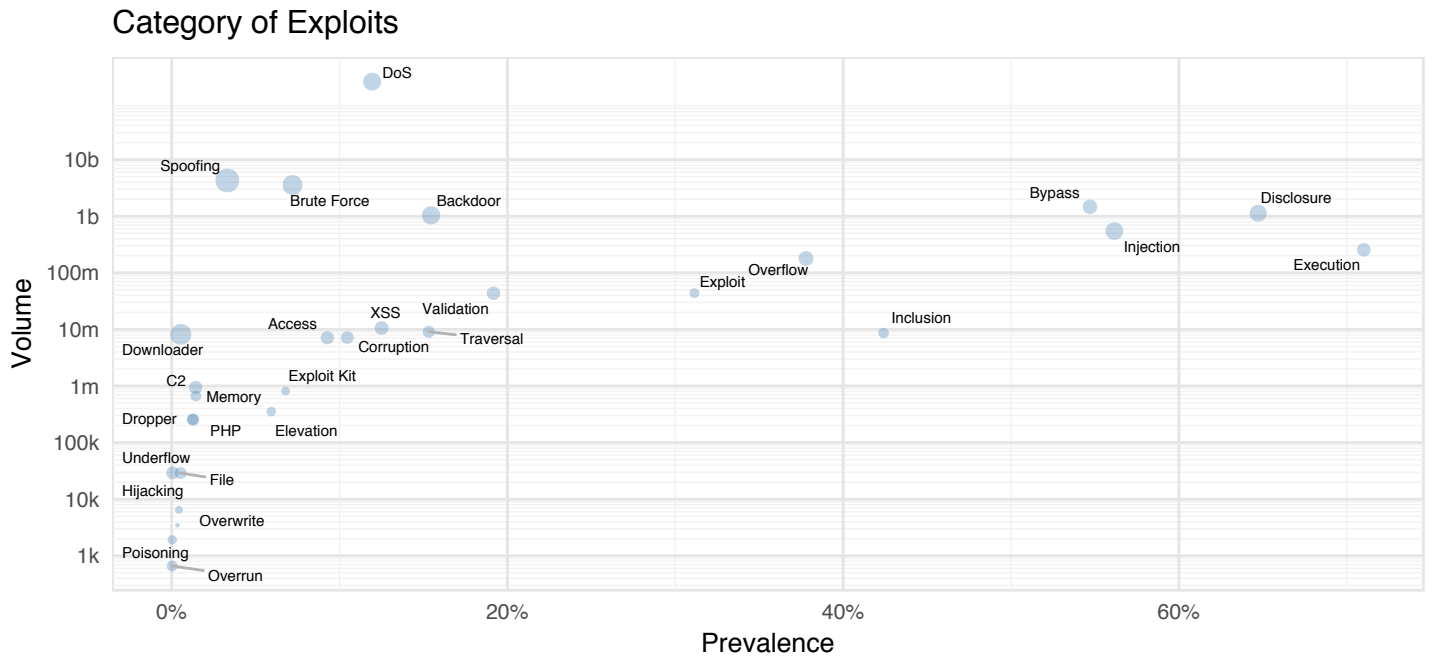


FIGURE 6: EXPLOIT CATEGORIES PLOTTED BY PREVALENCE (X) AND VOLUME (Y).

It's not too surprising to see that DoS exploits stand orders of magnitude above the competition on the y-axis; they are, by definition, high-volume attacks. Execution attacks, which allow an attacker to run arbitrary code or commands on the host system, rule the x-axis and are reported by more firms than any other category of exploit. Spoofing attacks as a group look to rank highest on the intensity scale. Beyond that, you're free to explore Figure 6 as you like. If interested in a particular category—exploit kits, for instance—you can find numerous examples using our Threat Encyclopedia.[5]

[5] https://fortiguard.com/encyclopedia

MINI FOCUS: **EXPLOIT KITS**

Speaking of exploit kits, they represent a special breed of threats that our FortiGuard Labs keeps close tabs on. As the name implies, exploit kits are toolkits used by malicious actors to attack all sorts of system vulnerabilities. Figure 7 narrows the aperture of Figure 6 to focus on the top exploit kits detected by our sensors in Q4. We've analyzed several of these in detail before, and even have a special section on our blog[6] for exploit kits.

Looking further back across all of 2017, RIG deserves mention as the top exploit kit.

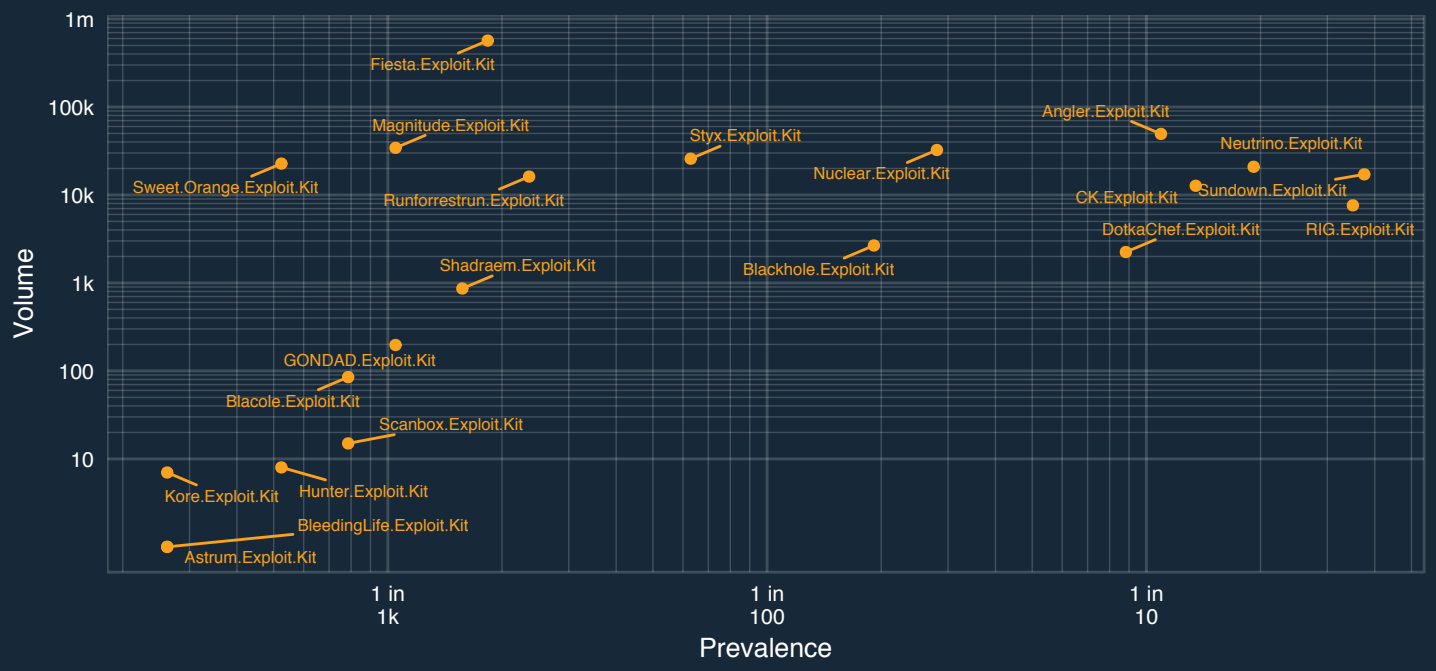


FIGURE 7: EXPLOIT KITS PLOTTED BY PREVALENCE (X) AND VOLUME (Y).

To our mind, the most noteworthy exploit kit from Figure 7 is Sundown. It was reported by more organizations than any other in Q4 and rose to become the top trigger across our sensors in early December. Sundown borrows many capabilities from other kits, but adds a unique twist in its use of steganography to conceal harvested information within ordinary PNG files. It's been known to distribute ransomware payloads such as CryLocker.

Looking further back across all of 2017, RIG deserves mention as the top exploit kit. RIG is interesting due to the number of ways it attacks a system, including exploits in a variety of plugins and applications such as VBScript, Flash, and JavaScript. There are also multiple options for presenting or pushing infected websites to unsuspecting visitors. The kit usually takes the simple approach of luring visitors to a site through spam emails, phishing campaigns, and similar means. RIG mostly targeted the healthcare, technology and banking industries.

[6] https://blog.fortinet.com/tag/exploit-kit

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:

- 17,671 unique variants (+19%)
- 3,317 different families (+27%)
- 14% reported mobile malware (-11%)
- 22% detected ransomware (0%)
- 9 families spread to ≥1/10 firms (-40%)

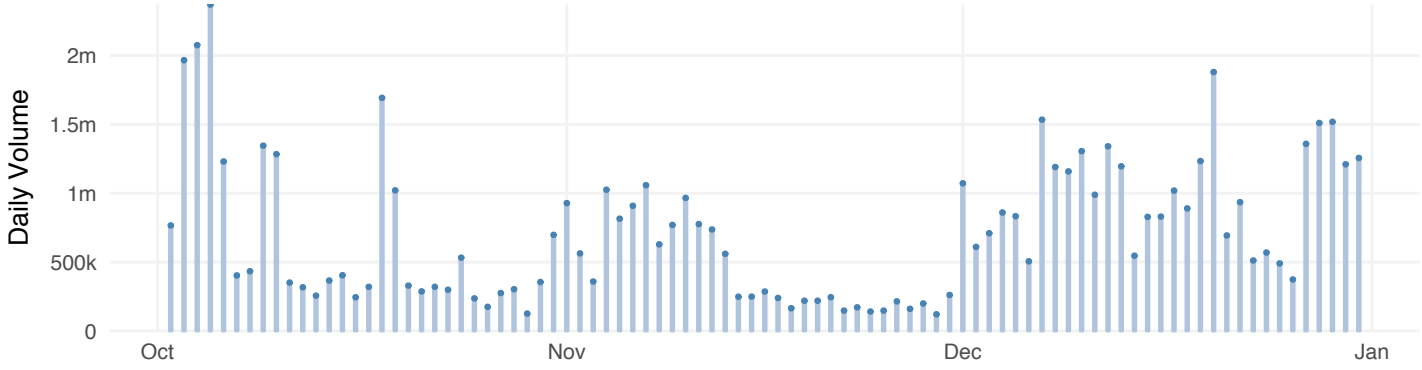


FIGURE 8. QUARTERLY MALWARE DETECTION VOLUME.

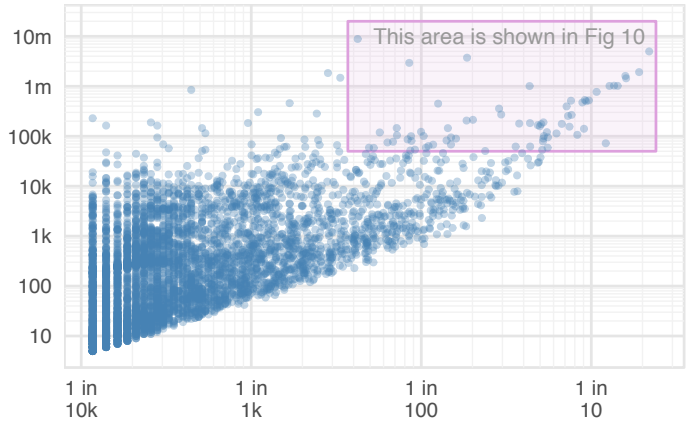


FIGURE 9: ALL MALWARE VARIANTS PLOTTED BY PREVALENCE (X) AND VOLUME (Y).

In past reports, we've presented malware according to families as a way to emphasize higher-level trends and manage the continual deluge of new variants. But sometimes it's nice to let the deluge wash over you for a fresh perspective, which is what we've done here. Figure 9 plots all 17,600+ malware variants reported in Q4 by prevalence (x-axis) and volume (y-axis).

The shape of Figure 9 is quite fascinating. Notice the imaginary boundary formed along the bottom of the conglomeration that no dots (variants) seem to cross. It's almost like it's impossible for malware to spread to more firms without increasing in volume. That may not be a revelation on its own, but the variants along that bottom line are interesting in that they appear to achieve maximum effect (prevalence) for minimum effort (volume). If those at the bottom represent the most efficient strains of malware, those on the top (especially to the left) could be considered the most wasteful.

Our commentary will center on the upper right tip of the variants in Figure 9, so Figure 10 conveniently zooms in on that section of the chart to make things more readable. In so doing, however, we want to caution against ignoring the huge mass of malware below that tip. Remember the fate of the Titanic; don't let threats lurking below the surface sink your ship.

Coming back to Figure 10, several malware variants bear mention. VBS/Locky.D!tr.dldr is a new strain of Locky that emerged in October using the ".asasin" extension for encrypted files. This latest spam variant includes forged header information designed to trick recipients into believing that the email is from a shipping company, such as DHL or FedEx. We strongly recommend not accepting that package. As with previous Locky variants, once the ransomware has finished encrypting the computer, it removes the downloaded executable and then displays a note that provides information on how to pay the ransom.

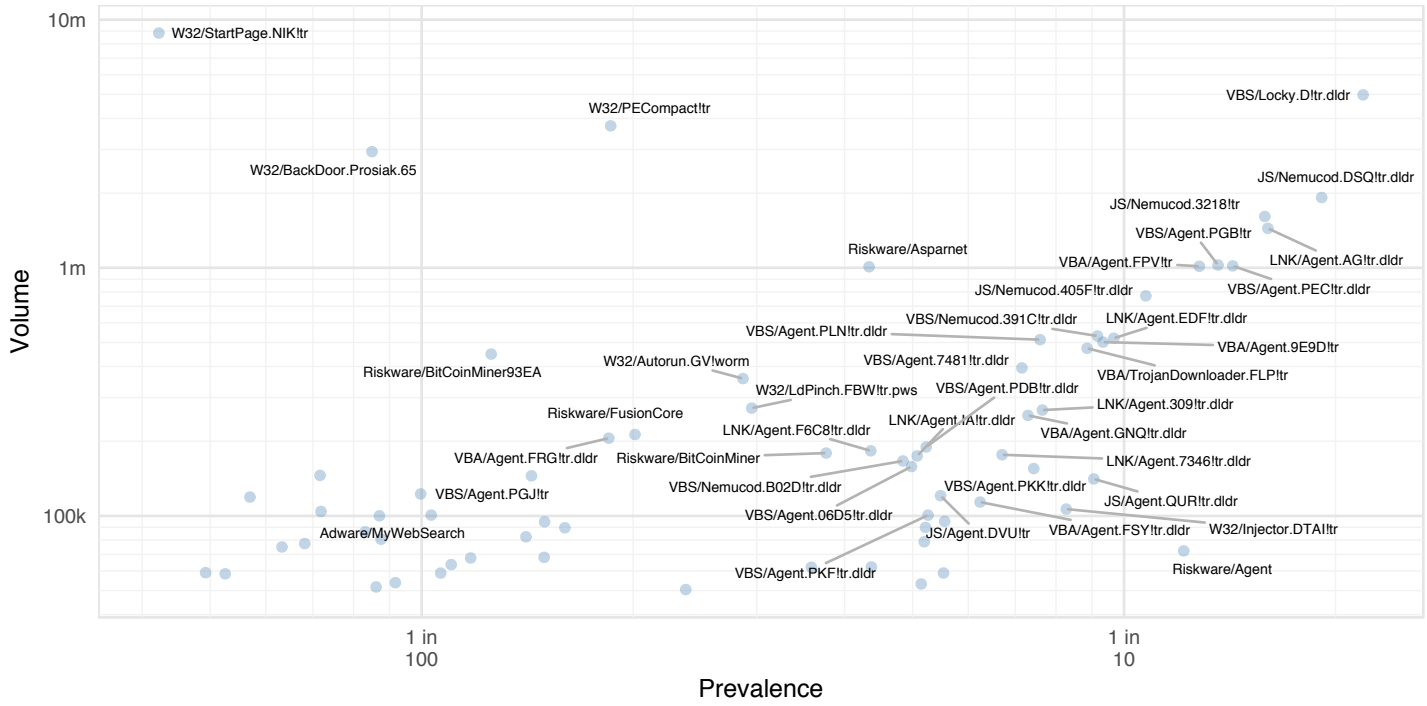


FIGURE 10: TOP MALWARE VARIANTS PLOTTED BY PREVALENCE (X) AND VOLUME (Y).

While we're on the topic of paying ransoms, we've noticed that criminals have begun to accept payment in cryptocurrencies other than bitcoin. For instance, we recently discovered (and wrote about[7]) a variety of ransomware that only accepts Monero. As in markets above ground, competition seems to be developing around cryptocurrencies within the internet's underground. We are actively following this trend and will report on it in our weekly Threat Briefs[8] and future versions of this quarterly report.

[7] https://blog.fortinet.com/2018/01/22/spritecoin-another-new-cryptocurrency-or-not

[8] https://fortiguard.com/resources/threat-brief

JS/Nemucod.DSQ!tr.dldr is associated with a late December surge of the GlobeImposter malware. This variant of GlobeImposter appends a "..doc" [ex: taxreturn.xls..doc] extension to files it encrypts. Once the encryption routine runs, it leaves an HTML file on the desktop (Read___ME.html), which provides instructions to the victim on how to decrypt their machine. The TOR URL presents the victim a professional customer support ticketing page, which may enable the criminals behind the scheme to keep track of their new "customers."

We could keep going on about interesting Q4 malware for several more pages, but we will refrain and refer you to our Threat Encyclopedia[9] for that. Instead, we'll call your attention to how well-represented the Nemucod and Agent families are among the leading malware variants in Figure 10. And that brings up an interesting point about malware families and tactics.

To leave you with a better view of what's going on in some of these leading crimeware families, we present Figure 11. It highlights individual variants (red) within four families of interest against a backdrop of all other 17,600+ malware variants (blue-gray). Immediately apparent is the marked difference between a "liberal" family like Agent vs. the relative "conservatism" of Locky. It's also clear that variants within families cover the spectrum in both volume and prevalence.

Much of this can be explained by the purpose of the malware. Nemucod and Agent, for instance, are designed to deliver payloads like Locky to the intended target and so must iterate variants often to increase their chances of bypassing anti-malware defenses.

The BitCoinMiner family is not as well known as the others in Figure 11, but a couple of its members did manage to strike their way into the leader's quadrant for the first time in Q4. This family is representative of the growing number of cryptomining malware in the wild, along with CoinHive, CoinMiner, JSEcoin, and MineMyTraffic. Cryptomining, aka cryptojacking, was such a strong trend in late 2017 that we "dig" deeper into it in the Mini Focus below.

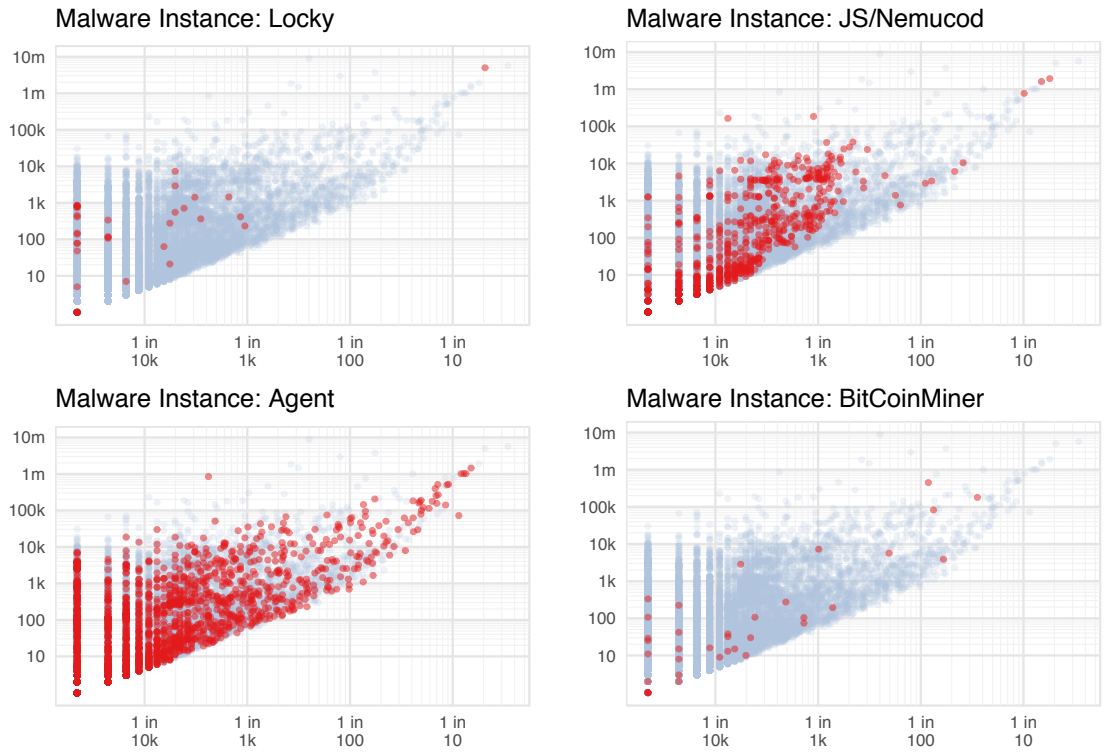


FIGURE 11: SELECTED MALWARE "FAMILY PORTRAITS" SHOWING INDIVIDUAL VARIANTS IN RED PLOTTED BY PREVALENCE (X) AND VOLUME (Y).

[9] Curious about VBS/Agent.PEC!tr.dldr? Fantastic: https://fortiguard.com/encyclopedia/virus/7480252/vbs-agent-pec-tr-dldr

MINI FOCUS: **CRYPTOMINING MALWARE**

Have you noticed your computer's processor working harder than normal lately or the fan kicking on at odd times? If so, you might be an unwitting participant in the cryptocurrency market...but not in a way that's lining your virtual wallet. Your computer may be a mining tool for someone hoping to strike it rich in a scheme known as cryptojacking.

Cryptojacking involves loading a script into your web browser that forces your computer to mine cryptocurrencies without your knowledge. Nothing is installed or stored on your computer, but the cryptomining code does consume system resources. Given the escalating value of cryptocurrencies, cryptojacking is becoming quite popular among honest and dishonest profit seekers alike. Our blog has more background on this topic if you want it.

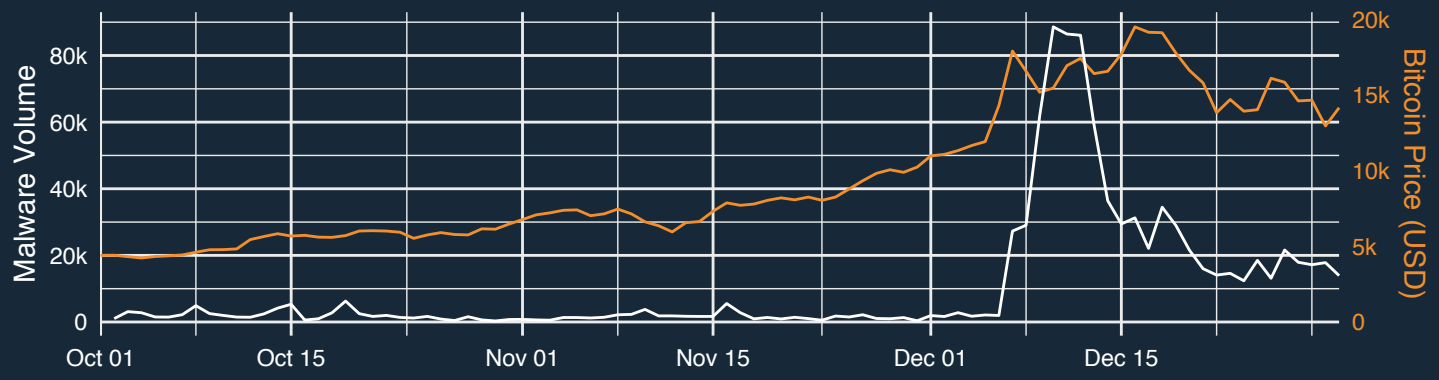


FIGURE 12: VOLUME OF CRYPTOMINING MALWARE (WHITE) AND BITCOIN PRICE (ORANGE).

Figure 12 charts the sharp increase in cryptomining malware detections toward the end of Q4. Because it illustrates the "Follow the Money" principle of criminal economics so well, we've also included the price of bitcoin. We suspect the future of cryptojacking and cryptocurrency will continue to be intertwined. Figure 13 compares the prevalence of these detections across regions and highlights elevated activity across sensors in the Middle East, Africa, and Latin America.

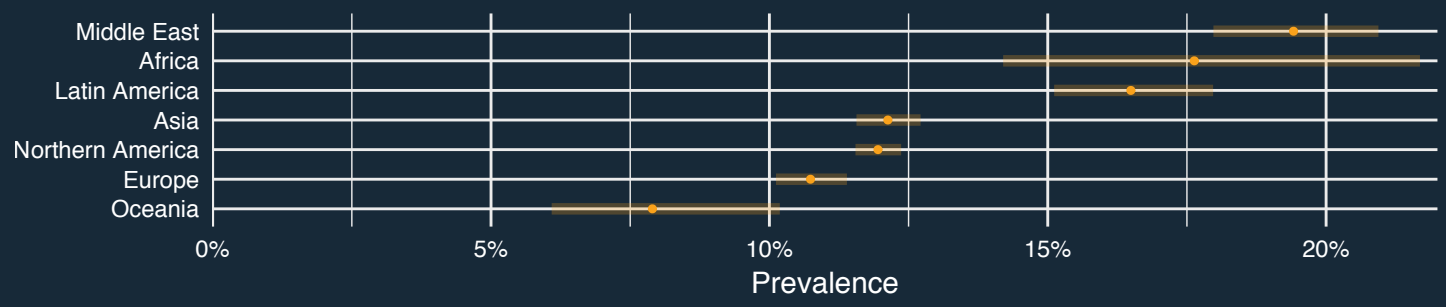


FIGURE 13: PREVALENCE OF CRYPTOMINING MALWARE ACROSS REGIONS.

Worried about being a victim of cryptojacking? Checking your CPU usage via the Task Manager (Windows) or Activity Monitor (Mac) is a good start. On the proactive side, plugins like AdBlock can prevent cryptomining scripts from being loaded into your browser. And as always, our FortiGuard team has your back and is actively watching out for new attacks and adding detections to keep your system from becoming someone else's pickaxe.

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:

- 513 daily botnet communications detected per firm (-1%)
- 259 unique botnets detected (+2%)
- 1.9 active botnets per firm (0%)
- 3.3% saw ≥10 botnets (+0.3%)

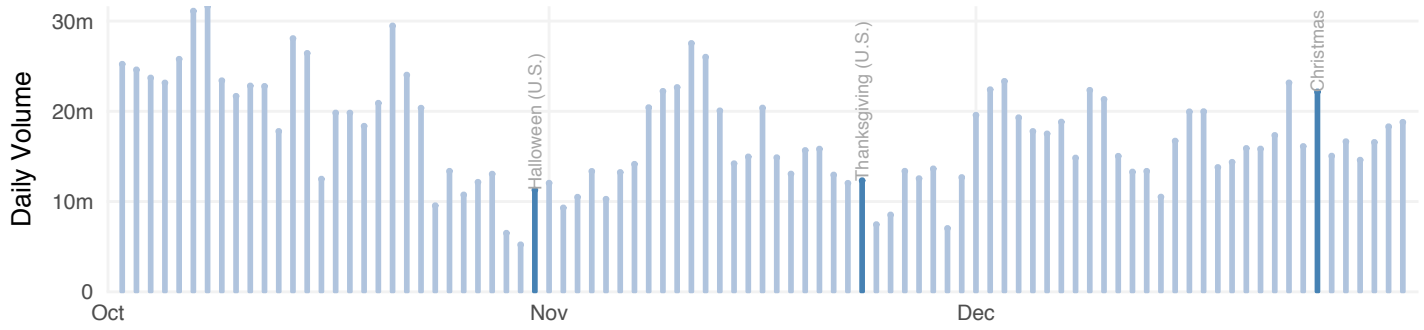


FIGURE 14: QUARTERLY BOTNET DETECTION VOLUME.

Overall botnet activity during Q4 remained remarkably steady, with the average number of daily communications per firm winding up a scant 1% off Q3 levels. Even key dates for the holiday season in much of the world show no significant difference from the ebbs and flows of the rest of the quarter. But these measures certainly do not mean Q4 was boring for botnets.

Most prevalent among botnets in Figure 15 for the third quarter in a row is Gh0st. The RAT behind it 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.

Necurs reliably follows Gh0st in the No. 2 spot for the fourth straight quarter (it was No. 1 in Q4 2016). It has become a multitool of sorts among botnets, having built its name as a major distributor of the Locky ransomware and Dridex trojan families. More recently though, Necurs seems to favor supporting large-scale spam campaigns centered on financial fraud.

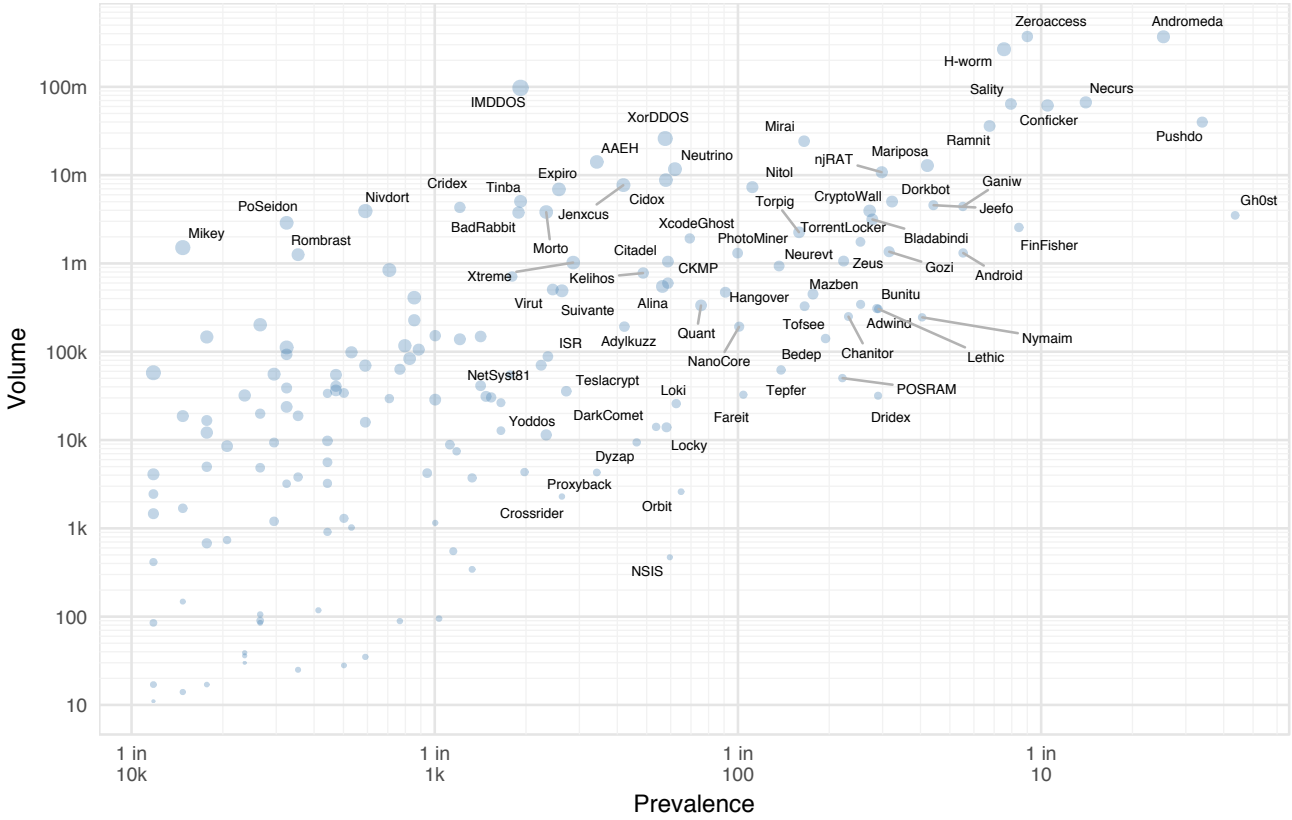


FIGURE 15: ALL BOTNETS PLOTTED BY PREVALENCE (X), VOLUME (Y), AND INTENSITY (DOT SIZE).

Andromeda rounds out the top three most prevalent botnets and it takes the highest volume crown as well. Andromeda is no stranger to the upper right pole position among botnets, having held that spot for several quarters now. But as the old saying goes, "what goes up must come down," and that's exactly what happened to Andromeda in Q4. Europol announced in December that a global coalition of law enforcement agencies had dismantled the botnet.

The takedown was accomplished by disabling more than 1,500 command and control domains, which housed servers that could direct the activities of systems connected to the botnet. Millions of systems tried to connect to those domains in the days after the takedown, a testament to the size of the botnet at the time of its demise. If you've ever wondered what the death throes of a botnet look like, Andromeda's final heartbeats are recorded in Figure 16.

FIGURE 16: TAKEDOWN OF THE ANDROMEDA BOTNET.

Figure 17 depicts botnets that racked up the largest shifts in prevalence during Q4. The Mirai botnet reasserted itself into the conversation with a new variant known as "Satori" or "Okiru." This particular one adds worm capabilities and targets Huawei HG532 home routers. It generated a lot of internet noise in December, but the good news is that it appears to have some code problems, preventing it from working properly. The source code was gifted to the world on December 25, so we'll continue to monitor and make sure it doesn't get out of hand. Those interested can find additional technical analysis on Okiru on our blog.

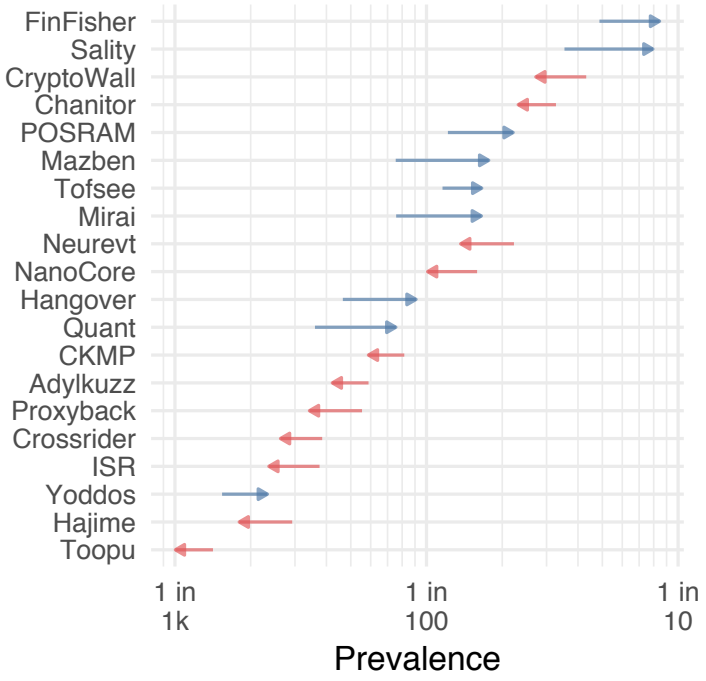


FIGURE 17: TOP MOVERS IN PREVALENCE AMONG Q4 2017 BOTNETS. ARROW SHOWS Q3 TO Q4 SHIFT.

Another botnet with an interesting Q4 story is FALLCHILL. In November, the U.S. Department of Homeland Security and the FBI identified a group of IP addresses associated with a Remote Administration Tool (RAT) known as FALLCHILL. A US-CERT alert issued around the same time attributes this activity to a North Korean threat group known as HIDDEN COBRA.

According to reports, HIDDEN COBRA actors have been using FALLCHILL to target victims in the aerospace, telecommunications, and finance industries. The malware is a fully functional RAT with multiple commands that threat actors can issue from a command and control server to a victim's compromised system via dual proxies. A significant number of network and system indicators of compromise (IOCs) associated with FALLCHILL have been independently verified by FortiGuard Labs. Deeper analysis of this activity is available on our blog.[10]

There's not much to share visually related to FALLCHILL activity, but that is often the case with targeted threats. The RAT only registered on a handful of sensors. Internal testing by FortiGuard Labs shows that all networks and devices being protected by FortiGate solutions running the latest updates are protected from this malware. Organizations that detect any of the IOCs associated with FALLCHILL should refer to the "Detection and Response" and "Mitigation Strategies" sections found in the US-CERT Technical Alert (TA17-318A[11]).

[10] https://blog.fortinet.com/2017/11/28/a-deep-dive-analysis-of-the-fallchill-remote-administration-tool

[11] https://www.us-cert.gov/ncas/alerts/TA17-318A

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 stats below suggest, we manage to find no shortage of them.

Quick Stats:
14 zero days discovered so far in 2018
38 zero days announced in Q4 2017
31 zero days discovered in Q4 2017
214 zero days discovered YTD 2017
526 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.

In early Q4, we discovered multiple Embedded Open Type (EOT) font vulnerabilities[12] in the Microsoft Windows font library by using a combination of open source fuzzing tools. The CVEs assigned to these vulnerabilities are CVE-2017-8691[13] and CVE-2017-11763[14]. An in-depth analysis[15] can be found on our blog, but the punchline is that these vulnerabilities can lead to issues ranging from mild out-of-bound reads to severe buffer overflows. The latter is certainly cause for concern and sufficient justification to ensure Microsoft Windows and Office products are up to date. Fortinet customers can use the corresponding IPS signatures to protect your environment:

- MS.Windows.Express.Compressed.Fonts.Remote.Code.Execution (CVE-2017-8691)
- MS.Windows.Graphics.EOT.File.Parsing.Code.Execution (CVE-2017-11763)

[12] https://www.fortiguard.com/zeroday/1984

[13] https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8691

[14] https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11763

[15] https://blog.fortinet.com/2017/10/19/a-14-day-journey-through-embedded-open-type-font-fuzzing

EXPLORATORY ANALYSIS

FORTINET

EXPLORATORY ANALYSIS

The word "landscape" used in the title of this report has become a fairly common way of referring to cyber threats that exist in the wild. But have you ever stopped to ponder why we as an industry have taken so readily to this term borrowed from the physical world? One reason is because it fits what we see around us. When you scan the horizon, it's not a homogenous plane extending in all directions; there are topological features that make one place different from others in countless ways. It is the same when we peer through our sensors across the internet.

We often do regional comparisons of threats in this report, and we will continue to do so in the future. But we wanted to offer a little twist on the standard way of doing that for this exploratory section. Rather than starting with a predetermined list of threats (e.g., the top 20 botnets globally) and then showing how they differ regionally, we wanted to start from scratch and identify which threats showed the highest degree of regional variation.

	Africa	Asia	Europe	Latin America	Middle East	Northern America	Oceania	Overall
Andromeda	45.7%	33.1%	8.1%	39.5%	43.8%	23.7%	17.6%	22.6%
Sality	13.6%	11.6%	3.3%	7.9%	11.7%	6.5%	4.3%	6.8%
H-worm	21.2%	7.5%	2.9%	17.6%	9.2%	7.1%	4.3%	6.4%
Ramnit	16.9%	10.6%	2.6%	5.2%	11.4%	5.2%	6.6%	5.8%
Android	1.01%	6.01%	5.42%	3.65%	1.43%	5.14%	6.38%	4.42%
Jeefo	10.86%	6.13%	1.56%	4.36%	7.15%	3.65%	1.72%	3.72%
Nymaim	3.79%	5.50%	3.93%	1.33%	1.92%	3.07%	6.72%	3.24%
Dorkbot	7.07%	5.53%	0.91%	2.99%	3.26%	2.21%	2.76%	2.66%
Gozi	5.56%	2.64%	1.63%	2.23%	2.07%	3.58%	0.69%	2.50%
Lethic	7.83%	4.45%	0.80%	3.46%	4.09%	2.14%	2.24%	2.43%
Dridex	0.25%	6.59%	0.36%	0.57%	0.59%	1.95%	2.07%	2.43%
Neurevt	3.03%	1.15%	0.49%	4.60%	1.23%	1.33%	0.52%	1.16%
Nitol	0.51%	2.31%	0.40%	0.71%	0.69%	0.64%	0.69%	0.92%
Fareit	1.26%	1.34%	0.46%	0.47%	2.52%	0.75%	0.17%	0.81%
NanoCore	0.76%	1.58%	0.80%	0.24%	1.87%	0.65%	0.34%	0.83%

FIGURE 18: BOTNETS WITH HIGHEST VARIATION IN PREVALENCE ACROSS REGIONS.

To do this, we filtered the botnet and malware datasets down to threats that were observed by at least 1% of firms (otherwise the numbers are so small that any difference is big by comparison). We then calculated the overall (global) prevalence of those threats as well as the prevalence within each of seven regions. Finally, we determined the total variation for each threat by calculating (and then summing) the differences between overall and regional prevalence values.

The results are presented in Figures 18 and 19, with threats exhibiting the highest variation at the top of the list. Using this method, the regional differences pop out nicely. Prevalence for the Andromeda botnet in Africa is twice the global value and over 5x that of Europe. On the other hand, the size of Europe's Android botnet problem is 5x Africa's. You win some, you lose some.

Other observations from Figures 18 and 19 abound. Botnet prevalence in Europe and Oceania usually (but not always) falls below other regions. Some (e.g., Adware/Ewind!Android malware) seem disproportionately common in a certain region (Africa) and quite rare elsewhere. Certain regions (e.g., Asia) stand on the high end of the spectrum for botnets, yet the low end for the malware (or vice versa). We could keep going, but we'll let you take it from here while we move on to the Conclusions and Recommendations.

	Africa	Asia	Europe	Latin America	Middle East	Northern America	Oceania	Overall
Adware/AirPush!Android	8.1%	2.7%	3.3%	10.9%	4.2%	5.3%	3%	5.2%
Riskware/CoinHive	6.8%	3.1%	4%	4.1%	9.5%	4.3%	3.4%	4.9%
Riskware/BitCoinMiner	4.3%	2.6%	3.3%	6.5%	3.8%	3.3%	1.6%	3.8%
Riskware/InstallCore_Gen	4%	2.3%	1.1%	2.2%	1.8%	2.1%	1.3%	2.2%
Riskware/FusionCore	6%	1.8%	1.2%	2.6%	1.9%	1.6%	1.8%	1.9%
Adware/DealPly	2.8%	1.8%	1%	1.8%	1.6%	1.6%	1.5%	1.8%
Adware/Agent	3.5%	3.3%	0.7%	0.5%	1.3%	1%	1.6%	1.7%
Riskware/Generic	0.3%	0.9%	0.1%	0.1%	0.2%	0.2%		0.4%
Riskware/Freemake	3.8%	1.5%	1.1%	1.8%	1.6%	1.5%	1.9%	1.7%
W32/Wintri!tr	1.3%	0.8%	1.4%	0.2%	0.9%	1.8%	0.9%	1.5%
Riskware/Donex		3.5%	0.2%	0.2%	0.3%	0.6%	1.3%	1.3%
Riskware/BitCoinMiner93EA	0.8%	0.8%	1.3%	2.7%	1.2%	1%	0.3%	1.2%
Riskware/DownloaderGuide	0.3%	0.3%	3.9%	0.1%	0.7%	0.6%		1.2%
Riskware/DriverPack	2.5%	1%	0.5%	1.2%	2.6%	0.9%	0.6%	1.1%
Adware/Ewind!Android	7.1%	1.1%	0.5%	1.3%	0.7%	0.9%	0.9%	1.1%

FIGURE 19: MALWARE WITH HIGHEST VARIATION IN PREVALENCE ACROSS REGIONS.

CONCLUSION AND RECOMMENDATIONS

CONCLUSION AND RECOMMENDATIONS

Thank you for spending another quarter with us as we explore the wilds of the threat landscape. 2017 was quite a tempest from the perspective of our global array of sensors, and the fourth quarter showed no sign of slacking off heading into 2018. We analyzed and discussed numerous challenges facing organizations conducting operations online today, and now it is time to offer some evidence-backed tips for meeting those challenges. We do that below, but as always, reach out to your Fortinet team members with any questions about the material covered in this report.

01

The exploit signatures and related CVEs from Figure 4 should provide some data and context to help answer questions like "Have we seen these alerts/ vulnerabilities?" You may also want to consider the most common exploit categories shown in Figure 6, since they broaden the aperture beyond exact signature matching. When practicing good "cyber hygiene," it's helpful to know where to scrub first and/or hardest.

02

Several exploits targeting IoT devices topped our charts this quarter. We recommend our Learn, Segment, and Protect[16] approach to quell the storm that seems to be brewing. This starts with *learning* more about devices connected to networks, how they're configured, and how they authenticate. Once complete visibility is achieved, organizations can dynamically *segment* IoT devices into secured network zones with customized policies. Segments can then be linked together by an integrated, intelligent, and protective fabric across the network—especially at access points, cross-segment network traffic locations, and even into multi-cloud environments.

03

The fallout from these escalating IoT attacks will most likely take the form of huge botnets comprised of hijacked devices that are used to launch large-scale DDoS attacks. The swarming effect we've seen in the past (e.g., Mirai-based attacks against Dyn) will get worse. Evaluating what your current DDoS defenses are able to handle now will help avoid troubles later if the swarm does come your way.

04

Our malware family portraits illustrate the incredibly prolific nature of this threat. This "proliferate to penetrate" strategy isn't new, but it's another reminder that single-point, signature-based AV simply cannot handle the volume, velocity, and variety of modern malware. Integrate malware defenses capable of detecting known and unknown threats at multiple layers throughout the environment.

[16] https://blog.fortinet.com/2017/11/07/3-must-haves-for-iot-security-learn-segment-protect

05

Several strains of ransomware led the throng of malware variants detected in Q4. It's a good reason to make sure the impact of an infection in your firm has minimum impact. That starts with good offline backups. Don't rely on shadow copy or online backups; they'll get encrypted too. Like it or not, the question of to pay or not to pay is something that deserves attention too. We generally don't recommend paying, but a situation may arise that forces you to at least consider it. Working out the policies and processes ahead of time will likely lead to a more clearheaded decision.

06

We showed that cryptojacking is jacking up more and more systems. If you are worried that your system might be one of them, start by checking the Task Manager (Windows), Activity Monitor (Mac), and "top" on the Linux command line. Using these tools, you can also list all the processes running on your computer and then find/kill the culprit that's consuming resources.

07

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

08

If threat actors do manage to establish a beachhead in your network, they will next begin a land-grabbing phase into other parts of the environment. An internal network segmentation strategy will help contain all kinds of threats, be they advanced adversaries or methodical malware.

09

Basic cybersecurity hygiene applies no matter where you sit in the real world. But the Exploratory Analysis section shows that regional differences among certain types of threats do exist. Assessing whether those differences warrant a change in security strategy or controls across regions is savvy practice in an increasingly interconnected world.

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

Feb 12, 2018