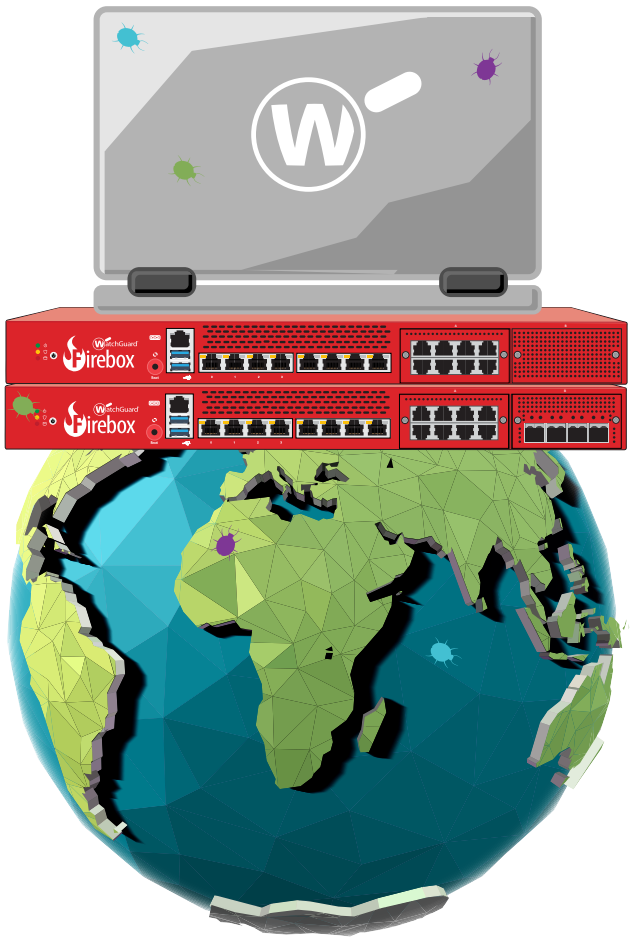

# Internet Security Report

QUARTER 3, 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.





**03 Introduction**

**04 Executive Summary**

**05 Firebox Feed Statistics**

**07 Malware Trends**

**08** Quarter-Over-Quarter Malware Analysis

09 Mac Scareware Makes the Top Ten

10 Razy Learns New Cryptomining Tricks

12 Old Cisco Exploits Return

14 Geographic Threats by Region

15 Zero Day vs. Known Malware

**16 Network Attack Trends**

17 New Network Attacks

19 Interesting Network Attacks Not on the Top 10

20 Quarter-Over-Quarter Attack Analysis

21 Battlegrounds: The Web

22 Geographic Attack Distribution

**23 Firebox Feed: Defense Learnings**

**24 Top Security Incidents: Facebook Breach**

25 Web Authentication

25 The Attack

26 The Response

27 Lessons Learned

**28 WatchGuard Threat Lab Research**

29 **Analyzing the Security Posture of the Top Websites**

30 Top 100,000 Website SSL/TLS Security

32 Top Sites Still Using Revoked Symantec Certificates

33 Top Websites Graded

**34 Conclusion & Defense Highlights**

36 Everyone needs Multi-factor Authentication (MFA)

36 Install an endpoint security suite on remote Mac computers

36 Train users on social media best practices and help them harden their accounts

37 Layer anti-malware services with IntelligentAV

**38 About WatchGuard**

# Introduction

Any savvy business executive knows you can't make very good decisions if you don't have good data. Imagine your sales are up 20%. That's great, but why? Is a particular product doing better than average in a particular region? Did something happen in that region that prompted the change? Unless you have the additional data to measure these changes, you may never find out the root cause, which means you may not repeat the success. The same goes for negative trends as well. If your service renewals drop one quarter, but you don't have the information to help you find out why, they may continue to drop precipitously for many quarters to come.

Like the skilled business executive striving to leverage data to grow revenue and increase profits, security professionals can use data to increase their protections. If you know what type of attacks hackers prefer in your region, you can cater your security policies to defend against them. If you know the most common malware seen around the world, you can make sure your users are aware of it and your anti-malware service is updated to catch it. If you understand which threats bypass which defenses, you can ensure you have the additional layers needed to catch them. In other words, having the right trend data can help you adjust your defenses to attackers' latest changes, making you a better security practitioner.

The goal of our quarterly Internet Security Report (ISR) is to supply the valuable threat data security professionals need to stay at the top of their game. The WatchGuard Threat Lab team records, measures, and analyzes real threats that our products see affecting small to midsize businesses (SMB's), and distributed enterprises around the world, and we share that valuable security information in this convenient and free report. After looking at each quarter's security trends, we inform you which threats you need to look out for and share tips on how you might avoid becoming the next victim in a headline-grabbing breach.

Specifically, our report includes the top malware and network attacks seen by tens of thousands of Firebox® appliances around the world. We share new research on a variety of topics; from the latest Internet of Things vulnerability our team found, to how secure the top websites on the Internet are. We also share deeper technical insights about information security topics you may have seen in the news.

As always, we don't analyze this data just to gossip about what the black hats are up to, but to turn it into actionable defense strategies you can incorporate into your protections to keep your business safe. The most successful business executives tend to have an impressive store of data backing their successful decisions. Let our quarterly report act as your data store and guide you to being the respected security leader at your organization.

## The report for Q3 2018 includes:


### *Quarterly Firebox Feed Trends*

In this regular section, we analyze threat intelligence from over 40,000 WatchGuard Fireboxes. This section includes the top global malware and network attacks from the quarter, some quarter-over-quarter and year-over-year analysis, and a few regional trends as well. Of course, we also share a few tips that can keep you safe from the latest threats.


### *The Facebook "View As" Breach*

During Q3, a chain of small vulnerabilities combined together to expose a critical Facebook issue that attackers exploited to make off with the personal information from 50 million accounts. In this section of the report, we share the technical details that allowed these flaws to expose your Facebook accounts to hackers.


### *Q3 Research: Grading the Security of the Alexa Top 100,000.*

For this quarter's research project, the Threat Lab team analyzed the security posture of the most popular websites on the Internet using three different methods. Learn which sites use bad certificates, which sites allow weak encryption protocols, and what you can do to avoid the less secure websites on the Internet.


### *Many Tips to Protect Your Network*

While hacks can be interesting, we do this to learn how to best defend ourselves, not to promote hacks. Throughout our report, we share security advice relating to the different trends we saw during the quarter, we also end many sections and conclude the report with three top tips you can follow to keep your business protected from the latest threats.

If you don't know what's happening in the threat landscape, it's hard to know what you should do to keep yourself safe. However, as soon as you have the data to expose what the bad guys are up to, it becomes trivially easy to find the right path and avoid those miscreants entirely. We hope this report provides you with the data you need to make the right decisions for your company.

# Executive Summary

This quarter, we saw Facebook leak data from 50 million accounts through a chain of vulnerabilities, the rise of an old trojan with new cryptomining capabilities, Mac scareware that made our global top ten list and a record low of network attacks in general. Keep in mind, we know about these trends because WatchGuard security services blocked them, so Firebox owners who properly configure the Total Security Suite have little to worry about. That said, not all our readers own Fireboxes, so this report will share how you might bolster your existing defenses to avoid the latest attacks.

Here are the highlights from the Q3 2018 ISR report:

- **Razy evolves into a cryptominer.** Last quarter, a two-year old code injector named Razy became the second most common malware, and now includes cryptomining capabilities. This means cryptominers continue to grow as a top threat, with this one variant making up about 4% of all the malware blocked by our Gateway AntiVirus (GAV) service.
- **macOS scareware makes the top ten list.** Those who think Macs are invulnerable to malware are sadly deluded. That said, we rarely do see Mac malware in the wild in significant volume, and it has never made our top ten list… that is until now. In Q3, a Mac-based scareware threat reached 6th place in our list. Read the malware section to learn more.
- **Mimikatz returns as the top malware in Q3,** now growing to 36.1% of the top ten malware. We have seen this credential-stealer many times before, and it remains popular as ever; still focusing on the U.S.
- **Overall malware is up 34% QoQ.** Our Firebox's' GAV service blocked 14.3 million malware variants during Q3, which is a 34% increase over Q2, but a 36% decrease YoY. In general, malware volume seems to be slowly recovering from a big unexpected decline during Q2.
- **Zero day malware dropped to 28.9%.** We compare how much malware evades our basic signature protection (GAV), and requires more advanced malware services to catch. This quarter, that number drop to less than 1/3 of all malware. That said, few businesses can survive missing three of every ten threats.
- **Network attacks declined again, with less than one million hits worldwide.** We've hit another record low. In Q2, IPS barely caught one million exploits. This quarter, we caught less than 900,000. While it's great news that attacks are down, we find this an unusual turn of events.
- **Cross-site scripting (XSS) accounts for 39.3% of the top ten exploits.** It appears attackers targeted web applications in Q3, with generic XSS attacks as the top exploit.
- **6.8% of the top 100K websites use insecure SSL protocols.** We researched the SSL/TLS habits of Alexa's top 100,000 sites, and found many sites to be lacking. Read our research section to learn more.
- **20.9% of the top 100K websites do not use web encryption at all.** This leaves them fully open to data interception or man-in-the-middle (MitM) attacks.
- In Q3 2018, WatchGuard Fireboxes **blocked over 17,917,916 malware variants** (445 per device) and **851,554 network attacks** (21 per device).

Read on to learn more about these trends and other threat and security insights from last quarter.


# Firebox Feed Statistics

# Firebox Feed Statistics

## *What Is the Firebox Feed?*

WatchGuard Firebox owners all over the world can opt in to sending anonymized data about detected threats back to the WatchGuard Threat Lab for analysis. We call this threat intelligence feed the Firebox Feed. Every quarter, we summarize our observations from the Firebox Feed and report on the latest threat trends that are likely to affect our customers and the industry as a whole.

We do not collect any private or sensitive data in the Firebox Feed and, as always, we encourage our customers and partners to opt in whenever possible to help us obtain the most accurate data possible.

We constantly develop the Firebox Feed to capture the most useful threat intelligence. Currently, it 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.

Throughout this section of the report, we analyze the most prolific malware and exploit trends that we saw in Q3 and provide actionable defensive tips for keeping your networks safe.

During Q3 2018, the Firebox Feed included threats captured from 40,265 Firebox appliances deployed across the world. While this is the highest participation by count that we have seen yet, it still only accounts for around 10% of the active Fireboxes deployed on customer networks. If you're a customer or partner and want to help improve these results, see the panel to the right to learn how to participate.


## 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 Fireboxes in the field. If you want to improve this number, follow these three steps.

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

# Malware Trends

Malware today continues to evolve, evade and steal. Whether it is a virus, trojan, adware, ransomware or any other malware variation, the goal of most malware campaigns is to harvest as much value from a computer's data and resources as possible. Cryptominers show a clear example of this resource harvesting. This quarter, cryptominers retained their place in our top malware list, with threats like the Razy trojan adding cryptomining capabilities. Cryptominers become more sophisticated every day, often evading detection by limiting the resource they steal from a computer to stay under the victim's radar. We hope to help you understand more about this variation of Razy and other malware throughout this section.

Coming up, we share the most common malware the Firebox Feed saw during Q3 2018, and we compare those trends to both last quarter and the same quarter last year. We also provide a glimpse of malware trends by region. We hope this analysis provides insights and patterns that help you better protect your network and devices.

Let's start with the overall malware highlights from this quarter.

**Malware data in this report comes from two Firebox services:**

- The basic Gateway AntiVirus 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.

**Q3 2018 Overall Malware Trends:**

- **40,265 Fireboxes** reported to the Firebox Feed in Q3. A 1% increase quarter-on-quarter (QoQ) and **34.6% increase year-over-year (YoY)**. We are pleased to see the number of reporting boxes continue to grow and ask customers to continue opting in to this data sharing.
- GAV services worked significantly harder this quarter compared to last, blocking **14,343,015 malware variants; a 34% increase QoQ, yet 36% decrease YoY.**
- **APT Blocker** contributed more this quarter as well, **blocking 3,574,901 additional threats**. This represents a **13% increase QoQ** and, more significantly, a **14% increase YoY**.
- However, despite the growth in APT Blocker hits, the comparably larger increase in GAV detection **lowered our zero day malware percentage to 28.9%**. That is a **22.7% decrease from Q2 (37.4%)**, but a **4% increase YoY**.
- To summarize, we saw a **23% QoQ increase in malware overall**.

The **Firebox Feed** recorded threat data from

**40,265**

participating Fireboxes

a **34.6%** increase year over year.

**Our GAV service blocked**

**14,343,015**

malware variants

a **34%** increase quarter over quarter

**APT Blocker stopped an additional**

**3,574,901**

additional threats

**13%** increase QoQ

## Quarter-Over-Quarter Malware Analysis

As you can see, Mimikatz continued as the top malware last quarter (Q3). Between this and the continued news around password database breaches, we believe two-factor authentication (2FA) is all but required for all organizations, including small and midsize businesses (SMBs). Since we've covered Mimikatz in past reports, we won't cover it here. However, you can learn more about Mimikatz in our **Q2 2017 report**.

Two malware variants, Exploit.RTF-ObfsStrm.Gen and Application Coinminer were just knocked out of the top 10, ending up in spots 11 and 12. In Q2, they were 10 and 9 respectively. W97M/Downloader – a generic rule to catch malicious Word documents – returned to the top 10 list for the first time in over a year. The last time we saw this threat was in Q2 of 2017.

As we have seen in previous years there has been an increase in malware from Q2 to Q3. We can contribute most of this increase to two new malware variants, Razy and MAC.OSX.AMCleaner. Razy used to be a code injector in 2016 but has evolved to add cryptomining capabilities as well. A code injector is malware that exploits vulnerabilities in software to add malicious code to the software. Since most programs don't have the correct privileges to directly add code to another program, using a code injector bypasses this defense. With Razy's newfound cryptomining features, this makes the second quarter to see cryptominers in the top 10 malware list.

Received mostly by email, MAC.OSX.AMCleaner is very much like FakeAlert and tries to trick you into buying unneeded services. As the name suggests, this is malware meant for OS X or macOS systems. We describe Razy and MAC.OSX.AMCleaner in more detail later in this report.

Attackers are continuing to use Office exploits to backdoor systems this quarter. We see about the same number of office exploits in the top 10 as we saw in Q2. Patching the Office suite is your best bet to prevent this type of malware.

**Below you'll find the top 10 malware variants blocked by WatchGuard's Gateway AntiVirus service during Q3 2018.**

| COUNT | THREAT NAME | CATEGORY |
|---|---|---|
| 1,344,351 | Mimikatz | Password Stealer |
| 575,155 | Razy | Cryptominer/ Win Code Injection |
| 464,414 | Win32/Heim.D | Win Code Injection |
| 433,450 | Win32/Heur | Generic Win32 |
| 327,044 | Exploit.CVE-2017-11882 | Office Exploit |
| 198,295 | MAC.OSX.AMCleaner | Dropper |
| 136,079 | FakeAlert | Dropper |
| 132,098 | W97M/Downloader | Office Exploit |
| 113,591 | Win32/Heri | Win Code Injection |
| 109,438 | Exploit.CVE-2017-0199 | Office Exploit |

***Top 10 Malware Variants***

| Threat Name | 2017 Q3 | 2018 Q2 | 2018 Q1 |
|---|---|---|---|
| Mimikatz | ✔ | ✔ | ✔ |
| Razy | | | ✔ |
| Win32/Heim.D | ✔ | ✔ | ✔ |
| Win32/Heur | ✔ | ✔ | ✔ |
| Exploit.CVE-2017-11882 | | ✔ | ✔ |
| MAC.OSX.AMCleaner | | | ✔ |
| FakeAlert | ✔ | ✔ | ✔ |
| W97M/Downloader | | | ✔ |
| Win32/Heri | | ✔ | ✔ |
| Exploit.CVE-2017-0199 | | ✔ | ✔ |

## Mac Malware Makes the Top Ten (MAC.OSX.AMCleanerCA)

MAC.OSX.AMCleanerCA is **scareware**, the same type of malware as FakeAlert but meant for OS X. This immediately piqued our interest as OS X isn't traditionally as popular a target for malware, at least in as large of volumes as Windows and Linux systems. During Q3, we saw this Mac scareware affect many countries all over the world.

Through our investigations, we found a few variations of this particular threat. In one variation the malware opens an HTML page that is stored in its contents. In another, it is a full application that shows false scan results. In both instances, the malware prompts you to purchase a fake malware cleaning service. If you follow the link to buy the cleaner, it takes you to a malicious domain and prompts you to download and install the bogus cleaning software.

When you run the malicious installer, it's actually signed with a valid Apple-issued certificate. This valid certificate allows the malware to bypass macOS protections like Gatekeeper, and helps trick the victim it's safe to run the software. Though digital signatures are a good way to help software manufacturers prove the authenticity and legitimacy of their software, they are not panaceas. We have repeatedly seen sophisticated attackers steal legitimate digital certificates or infiltrate the software supply chain in order to sign their own malware with legitimate signatures. If you are at all suspicious of certain software, don't let a valid-seeming certificate convince you it's ok.

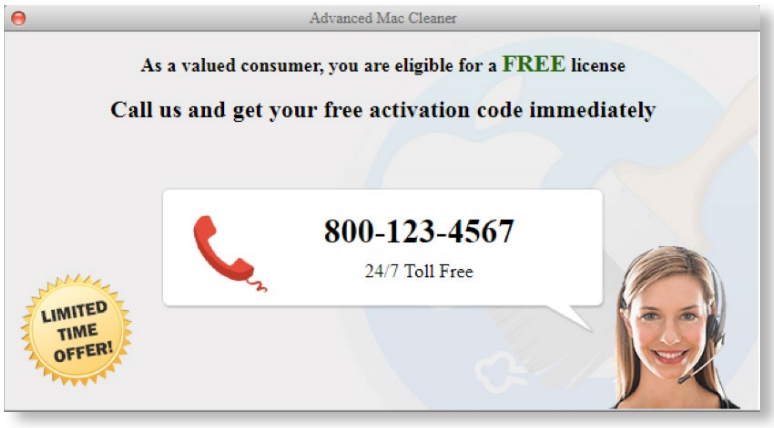



*Figure 1: Advanced Mac Cleaner Activation Window*

Once installed, the victim will get pop-ups sharing a phone number to get a free activation code. A close look at the number should tip you off that it is unusual (1, 2, 3, 4, 5, 6, 7). Unsurprisingly, we were unable to learn anything interesting about this number. Nonetheless, we found the same phone number used in all the different variants of this malware we analyzed. We tried calling the number despite its unusual nature, and it kept ringing. During some attempts, the number we called from was blocked.

There is a good chance that this threat is more along the lines of greyware, rather than truly malicious software. There is a class of malware that doesn't necessarily hide on your computer or steal information, but is really just worthless software that some unethical, but technically legitimate, company might trick you into paying for. This type of greyware often comes from sophisticated enterprises with the financial backing to buy a phone numbers like this.


*Figure 2: Advanced Mac Cleaner Discount Window*

## Malware Delivery Trends:

According to our Firebox Feed, most malware gets delivered over the web (HTTP and HTTPS). Specifically, 81% of all malware came through web ports (80 and 443) in Q3, which is a 5% increase over last quarter. However, we suspect technology evolutions may contribute to these web-skewed results.

Nowadays, many IT organizations have outsourced their email servers to the Cloud or have adopted web-based email solutions. If your email server is not behind your Firebox, we may not recognize email-based malware in the same way. Rather, email attachments could show up as "web traffic" if delivered through a webmail client. That said, we also see some attackers switching to malicious links in email rather than direct attachments.

In the end, though web-based malware is increasing, we believe the modern adoption of external, Cloud- and web-based email servers does skew this malware deliver statistic. Email-based malware attacks using simple attachments are not going away any time soon. If you do manage an internal email server, be sure to use our SMTP malware protections.

## Razy Learns New Cryptomining Tricks

With its most recent evolutions, the latest versions of Razy malware are often simply called BitCoinMiner by some malware detection engines. On first seeing this variant in our top ten, we originally assumed this was just a typical variation of the Razy malware, which has existed for many years. However, we quickly learned it has been updated to become a cryptominer.

To analyze this new variant, we ran it in our test sandbox environment. On initial inspection, the executable is obviously a Portable Executable (PE) format file targeting Windows systems. When first run, we see the malicious executable call out to an HTTP-based command and control (C2) channel. Though the malicious website seemed active during our initial testing, any attempts to access it from a normal web browser failed with an unauthorized message. Before we could complete our testing, the malicious C2 site went down, though we are unsure if it's permanently gone or otherwise.

The communications we did see were in a format similar to HTTP, but slightly different. The requests didn't follow all HTTP standards. The C2 site itself is previously known to control other cryptominers like the **RiskTool.AndroidOS.Miner**. This piqued our interest again, so we monitored the malware's traffic to see if we could understand what it sent and received.

The malware sends a JSON request to the C2 server. It looks to be a login request with a simple username and password of "x." The format of this JSON request format is similar to many cryptomining request formats.

```
{"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"x","pass":"x","agent":"Chrome",
"algo":["cn/1","cn/0","cn/xtl","cn"]}}
```

The malicious server replies to this request with the information the cryptominer needed to start mining. This includes the blob. The long hash fallowing "blob" is the data that needs to be processed. This can be found in the fallowing code.

```
{"jsonrpc":"2.0","id":1,"error":null,"result":{"id":"15b9fa21-caad-435c-8693-ddc2d61edf6a","
job":{"blob":"0709c4be9dde052d0393ff2df8dc0ab225e8d25277aa79105280d4282eaf8699f7502e6f8ebe34
000000f82cc8eaedef4f1736e5418b3f989f0f74ef0b2e0712cca9a01d3d41a2875787e503","job id":
"5UUIo8jT6Nf79pcgMU56fZmcr2pf80","target":"e2361a00","algo":"cn/1","variant":1},"extensions"
:["algo","nic ehash"]},"status":"OK"}aa79105280d4282eaf8699f7502e6f8ebe34000000f82cc8eaedef4f
1736e5418b3f989f0f74ef0b2e0712cca9a01d 3d 41a2875787e503","job_id":"5UUIo8jT6Nf79pcgMU56fZmcr2p/
f80","target":"e2361a00","algo":"cn/1","variant":1},"extensions":["algo","nicehash"]},
"status":"OK"}
```

The client responds with a confirmation of the data and a status "OK."

```
{"id":93,"jsonrpc":"2.0","method":"submit","params":{"id":"15b9fa21-caad-435c-8693-
ddc2d61edf6a",
"job_id":"5UUIo8jT6Nf79pcgMU56fZmcr2p/f80","nonce":"fb0900f8","result":"e1f0fe6c06a49d367fbc5e17ee27a74
867ba9cf4bd0dcd126d20ac4fccde1300","algo":"cn/1"}}
```

```
{"id":93,"jsonrpc":"2.0","error":null,"result":{"status":"OK"}}
```

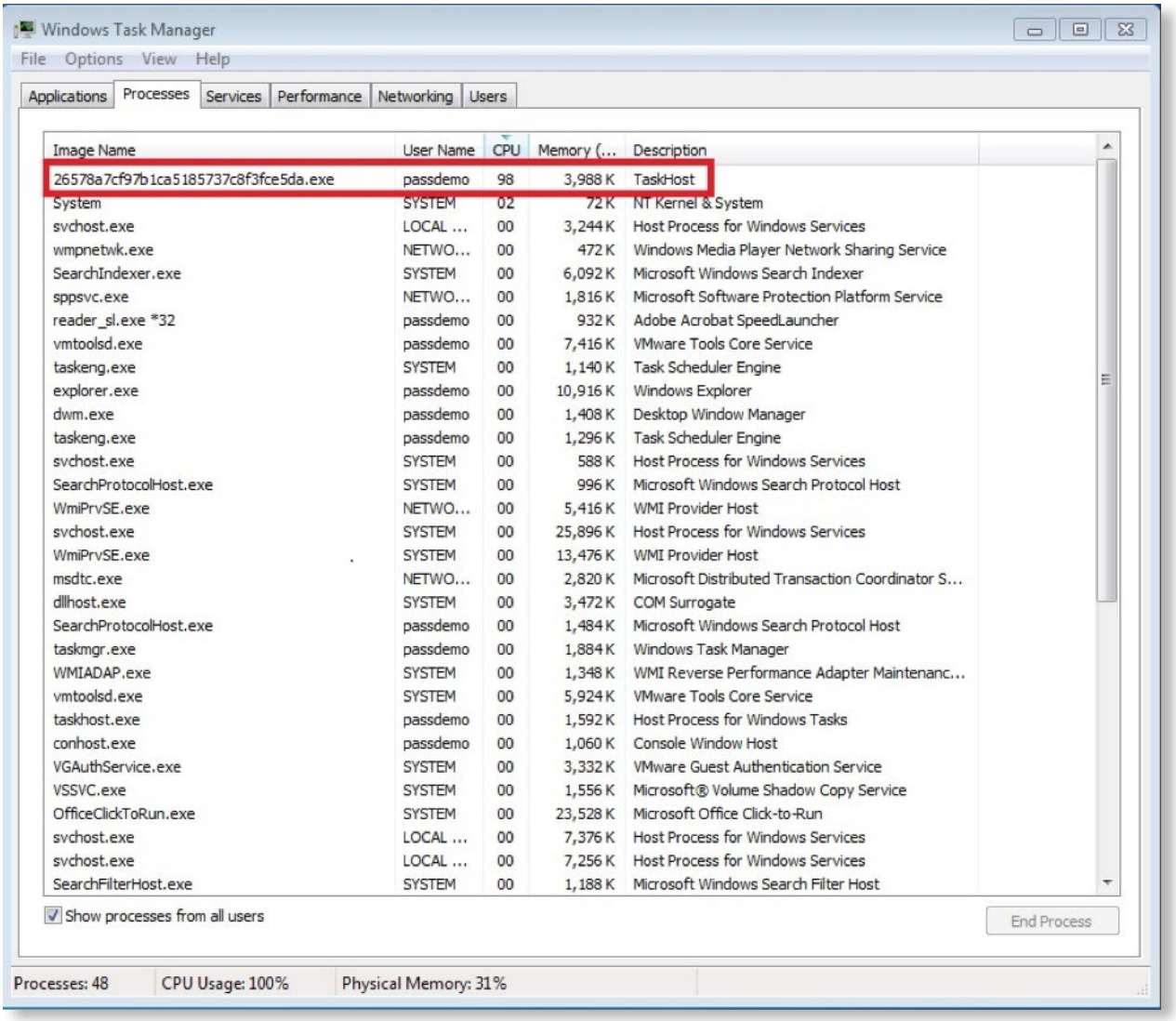



***Figure 3: Razy CPU usage***

The cryptominer then started mining and quickly took 98% of the CPU as can be seen in "Figure 3: Razy CPU usage." Nothing could be done in the test environment at this point. We didn't provide a lot of resources for the test environment so perhaps the cryptominer malware wouldn't crash a faster computer. Nonetheless, cryptomining malware can obviously have a significant effect on your computer's resource.

Keep in mind, more sophisticated cryptominers often hide their resource usage better than the one tested. In some cases, smart cryptominers could hide on your computer much longer unless detected by anti-malware software. However, this particular one was quite noisy, and would likely cause visible slowdowns on your machine.

## Old Cisco Exploits Return

While looking through the top 50 malware from Q3 2018, we noticed an interesting malicious Perl script that was relatively common despite being an older exploit. The script is essentially a compilation of older Cisco exploits that attackers can launch against various Cisco devices. In fact, it turned out to be a well-known exploit script that ships with **Kali**, a popular Linux penetration testing distribution.

Due to the way Kali is packaged and compressed, downloading the distro alone will not trigger our GAV alarms for this malicious script. Attackers – or penetration testers – actually have to launch the script against Cisco devices to trigger this signature. So even though this script comes with a well-known hacking distro, attackers still have to be using the malicious script for it to show up in our Firebox Feed.

Since this script consists of older exploits, and has been publicly available for a while, you can read more about these threats in **Cisco's response about this issue**. Nonetheless, we still took some time to analyze the script for ourselves. Much of the script is repeated to set up the exploit. The only differences are the ports used, addresses, and the actual exploit being sent. Here is a detailed analysis from a few interesting parts of the script.

Many of the exploits in the script trigger buffer overflow flaws in the server used for web management. Attacker can exploit these flaws to remotely execute code or commands. A buffer overflow attack works by adding more data to a memory location than expected. Extra code that doesn't fit into a limited memory segment ends up overwriting other memory locations, which it should not have access to. Smart attackers extend this memory overwrite all the way to a special memory location that decides what to execute next, called the stack pointer or register. From there, the attacker can run any code with full web server privileges. The buffer overflow exploits in this script are numbered. The attacker chooses which to run from a list of available exploits.

One option is the "Cisco IOS Router Denial of Service (DOS) Vulnerability." This sends a crafted GET request to exploit an old IOS DoS vulnerability, which can prevent victims from reaching the Cisco's device's web interface. Let's take a close look at that part of the script.

The script sets up variables to use later. These variables identify the server address that was provided by the user who ran the code.

```
my $serv = $host;
```

Many scripting programs like Perl allow you to import data from other libraries of data. These are called modules. This uses the Perl module "Socket." Using this module in Perl allows the script access to the network stack for communication. It also sets up variables for the ports and protocols it will use.

```
 my $sockd = IO::Socket::INET->new (

       Proto=>"tcp",
       PeerAddr=>$serv,
       PeerPort=>"http(80)",);
       unless ($sockd){die "No http server detected on $serv ...\n\n"};

 $sockd->autoflush(1);
```

The following part of the script sends a specially crafted GET request to trigger the DoS vulnerability.

```
print $sockd "GET /\%\% HTTP/1.0\n\n";

 -close $sockd;

 print "Packet sent ...\n";
```

This code forces the script to wait a bit, and then test if the exploit worked, reporting whether or not it was successful.

```
sleep(1);

print("Now checking server's status ...\n");
sleep(2);
my $sockd2 = IO::Socket::INET->new (

       Proto=>"tcp",
       PeerAddr=>$serv,
       PeerPort=>"http(80)",);

unless ($sockd2){die "Vulnerability successful exploited. Target server is down ...\n\n"};
print("Vulnerability unsuccessful exploited. Target server is still up ...\n\n");
close($sockd2);
exit(1);
```

Next, let's look at a more critical exploit in the script that allows attackers to remotely execute code, called "Cisco Catalyst 3500 XL Remote Arbitrary Command Vulnerability." Older Cisco Catalyst switch firmware suffered from a **code execution vulnerability** that allowed anonymous, unauthenticated attackers to execute any command by requesting the /exec location from Cisco device's Web UI server. One way attackers might exploit this issue is by launching the "show" command to see the device's configuration file, which often included all the device's user passwords. Let's take a look at this exploit script.

Again, the script starts by setting up variables it uses throughout the script.

```
my $serv = $host;
my $port = 80;
my $k = "";
```

When first run, the script prompts the attacker to enter the command they want to execute using the WebUI. By default, the script is set to "show" the local configuration file, which often contains user passwords and other important and sensitive configuration info.

```
print "Enter a file to read [ /show/config/cr set as default ] : ";
$k = <STDIN>;
chomp ($k);
if ($k eq "")
```

Next, the script crafts (but doesn't yet send) the malicious GET request to exploit this code execution flaw based on whatever command the attacker inputted in the previous step.

```
{$vuln = "GET /exec/show/config/cr HTTP/1.0\n\n";}
else
{$vuln = "GET /exec$k HTTP/1.0\n\n";}
```

Again, the script imports the default Socket module used for network communications. And then it sends the malicious GET request to the victim Cisco device.

The script includes many other older exploits against Cisco devices, all of which are similar to the two examples above.

As mentioned before, this is an old exploit script, dating back to 2004. Nonetheless, it seems some attackers or pen-testers are still downloading it and attempting to use these exploits against various targets on the Internet. These hits could be generated by malicious cyber criminals just opportunistically trying to find unpatched victims, or it could be automated vulnerability testing platforms or penetration testers checking for unpatched devices. In either case, you should keep your Cisco gear patched and up to date. If you have an older Cisco device, then we recommend upgrading the device. If you have an older Cisco device, we recommend upgrading it. If this is no longer possible, disable any direct network access to the device except by authorized users.

## Geographic Threats by Region

In previous reports, this section detailed the geographic breakdown of just the top 10 malware. This quarter, we're switching things up to show the breakdown of all malware in order to show an important trend. For the second time ever, the Asia-Pacific (APAC) region saw the highest volume of malware overall. Europe, the Middle East and Africa (EMEA) dropped to second place and the Americas (AMER) fell in last. The APAC region has seen a sharp rises in malware over the last three quarters. If we see similar numbers next quarter, then we'll suspect this trend to be a little more permanent.

The AMER (Americas) saw more malware than last quarter but still received the least amount during Q3. This seems unusual, as it typically ranked second place the first few years we created this report.

The newcomer **Razy** primarily targeting APAC, with 91% of its hits falling in that region. India and Thailand were the worst hit by Razy. In any case, this Razy campaign clearly is targeting one region.

***Table 1: Geographic Threats by Region***

| Region | Hits | Percent |
|---|---|---|
| APAC | 8,185,332 | 45.7% |
| EMEA | 5,706,942 | 31.8% |
| AMER | 4,025,642 | 22.5% |

**MAC.OSX.AMCleanerCA**, on the other hand, affected all regions fairly evenly. We saw 37.2% of its hits in APAC, 38.9% in EMEA, and 23.8% in the AMERs.

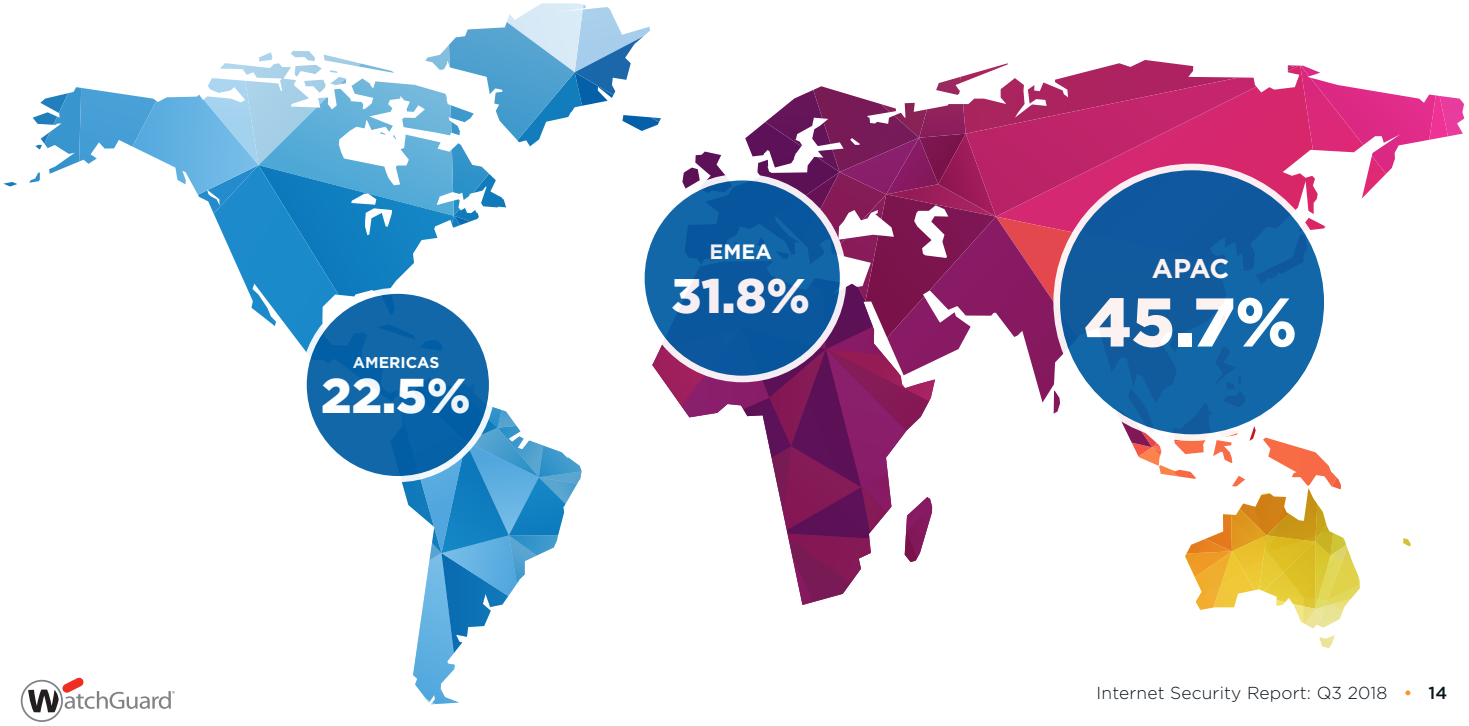
Not to be left out, 98% of **W97M/Downloader** hits were in AMER. Like Razy, this threat seemed to primarily focus on one region, and we have seen past malicious Word attacks also largely fall in the AMERs, with just a sprinkling in China.

India continues to receive a large number of hits from the **Win32/Heur** malware. This is a continuation from previous quarters, but this doesn't mean other regions can ignore it as everyone is affected to some extent by this malware. Granted, this is such a generic, **heuristically based signature** that it could match just about any malware.

Italy received the largest number of FakeAlert hits with Japan closely following. These two countries make up almost all of the **FakeAlert** hits, which is interesting. This seems to be a new trend with **FakeAlert** switching off between Italy and Japan for the most hits.

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. If you want an up-to-date picture of threats for your specific country or region, be sure to check out **https://secplicity.org/Threat-Landscape** where you can filter the public Firebox Feed data by date and country.

## Malware Detection by Region



## Zero Day vs. Known Malware

Signature-based malware detection is decent at catching the high-volume, well-known malware "noise" on the Internet, but it often misses newly packaged variants the day they come out. More specifically, cyber criminals actively use automated techniques to create new malware variants that evade pattern-based detection. In the malware cat-and-mouse game, malware authors only have to bypass our detection once to win. Meanwhile, we, as users, have to get it right all the time to stay infection-free.

Advanced malware detection systems like APT Blocker don't just use signatures to identify malware. Rather, they run suspicious files in a fully emulated sandbox environment to analyze behavior and identify the intent of the files and processes. This makes them more capable of weeding out brand new malware without having to know about a pattern they've seen before. In other words, they can catch completely new malware that has never been seen before, which we call "zero day malware." Since our Firebox runs both signature-based (GAV) and advanced (APT Blocker) malware protection services, we can give you the ratio of malware that legacy antivirus technologies catch, in comparison to what you need more advanced techniques to block.

As a future aside, we have recently added a third malware detection technology to our suite of protection called IntelligentAV (IAV). IAV uses modern machine-learning and artificial intelligence models to help detect, and even predict, if a new file might be malware based on millions and millions of malware and file samples it's analyzed before. This additional layer of defense further improves our Firebox's ability to find new malware without waiting for human researchers to catch up. We just released IAV last quarter, so it has not shown up in our Firebox Feed results yet. However, we do plan to share our IAV results in future reports, when more Fireboxes have upgraded to it, and started using it for the full quarter.

Q3 quarter did see a QoQ increase in the volume of zero day malware detections with APT Blocker. However, it also saw a corresponding and larger increase in GAV detections, which ultimately reduced the overall percentage of zero day malware last quarter to about 29%.

Nonetheless, that's still close to one-third of all malware. Without advanced malware protection, our customers would have missed 3,574,901 pieces of malware. If you are not yet using our APT Blocker or IntelligentAV services, we highly recommend you start.

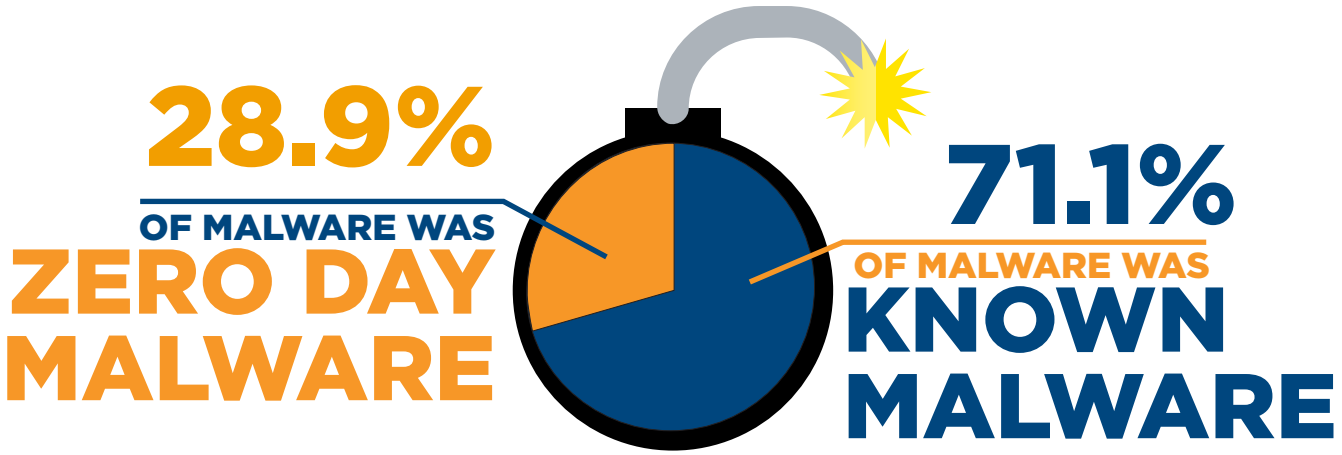



*Figure 4: Known vs. Zero Day Malware*

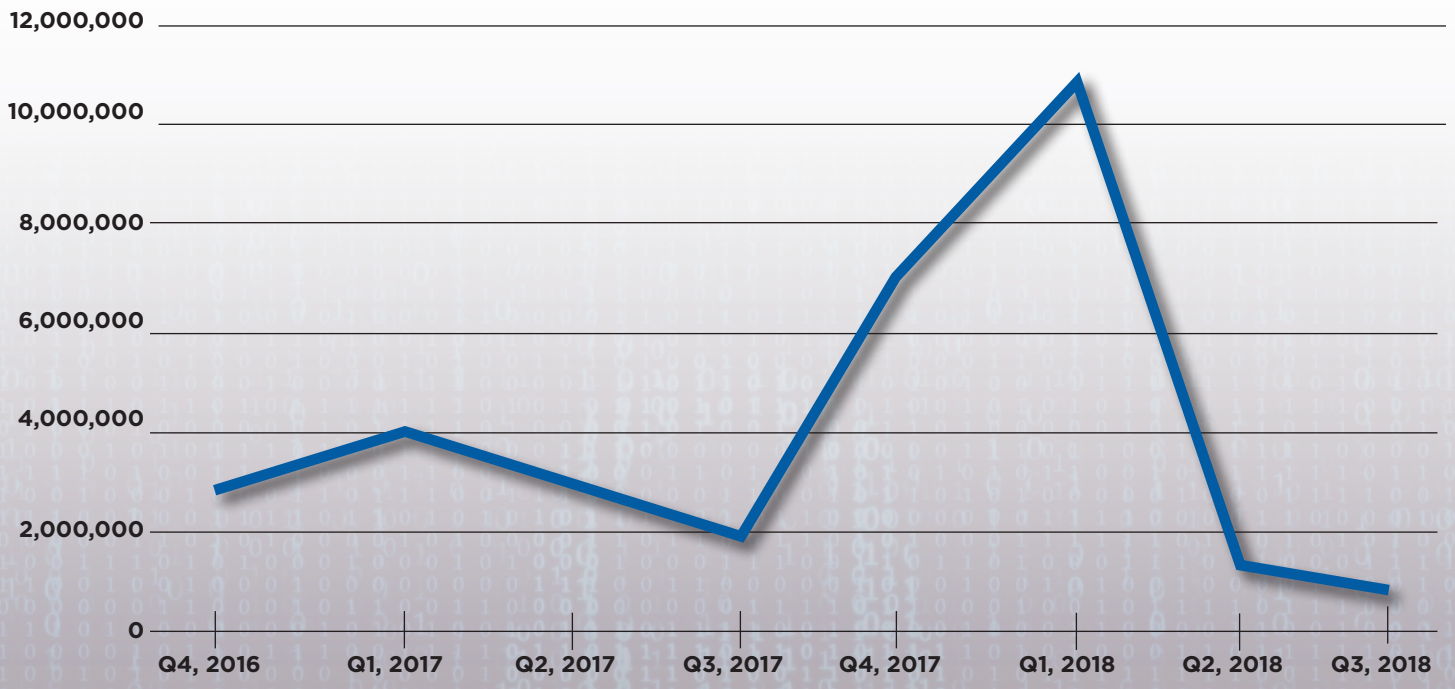
# Network Attack Trends

Not only did Q2 set an all-time record low for network attacks detected by WatchGuard's Intrusion Prevention Service (IPS), Q3 broke that record as well! In Q3, our IPS service only detected **851,554 network attacks**, which is good in terms of a low number of attacks, and unusually low compared to previous quarters. Breaking down the attacks by device, each Firebox blocked **roughly 21 network attacks**, down from 26 per device last quarter.

Bear in mind that network attacks are exploits for vulnerabilities in server or client software used over the network. This includes the ever-popular Microsoft Office products and varying desktop and server applications that are available both for free and at a cost. It's partially up to white hat hackers and penetration testers, but mainly the software vendor's internal quality assurance assessment teams, to find software security vulnerabilities and resolve them before the bad guys exploit them. Once security researchers or software authors find a vulnerability, security vendors can create signatures to identify and block attempted exploits against that flaw. We add these signatures to WatchGuard's IPS service to detect and prevent future attempts of this attack, even if the victim system is unpatched.

In the upcoming section, we cover some new attacks that have never previously appeared in our report's top 10 network attack list, briefly touch on the full top 10 attacks, perform a quarter-over-quarter analysis, and cover a few other highlights that stood out this quarter. Note that you can find more details about the referenced signatures at WatchGuard's IPS Security portal using the **signature ID look up tool**.

## Quarterly Trend of All IPS Hits



## New Network Attacks


There were three new attacks in the top 10 this quarter, two classified as access control flaws and another as a buffer overflow vulnerability. **Adobe's Flash Player and AIR** run-time system (**signature ID 1130948**) took 2nd place with 88,941 detections. The **WEB URI Handler buffer overflow attack** (**signature ID 1054968**) took 6th place with 31,449 hits. Finally, **GNU Bash Remote Code Execution – 6** (**signature ID 1130029**) took 8th place with 27,815 hits. Let's take a closer look at each of these three new attacks:

- **Adobe's Flash Player & AIR services**: This signature catches a four-year-old vulnerability affecting two different Adobe software packages, Flash Player and AIR. Flash player is a media player and plug-in to view Adobe Flash and Shockwave multimedia content, and Air is a cross-platform runtime system to create desktop and mobile applications. If you have updated either of these products in the past four years, these attacks won't affect you, otherwise see **Adobe's alert** for more information about the affected versions.

  The vulnerability has to do with how the affected applications read the "track" tag in an MP3 file's ID3 metadata. If the track tag contains a zero-length string, the application instead reads the value out of uninitialized memory. Uninitialized memory can be treated as garbage values and lead to unpredictable program behavior, as the call to this location wasn't intended by the original developer. Attackers can often leverage these sorts of memory corruption issues to execute arbitrary code. In other words, if an attacker can trick you into viewing multimedia content containing a specially crafted MP3 file, he could exploit this vulnerability to execute code on your computer, doing anything from installing malware to creating a backdoor connection over the Internet.

- **WEB URI Handler Buffer Overflow – OPTIONS:** This vulnerability affects the WebDAV implementation in older versions of Sun Java System Web Server's (SJWS) webservd 7.0 Update 7. It's possible for an attacker to send an HTTP Options request with an overly long path to trigger a buffer overflow on the server. This can either cause the server to crash or allow an attacker to execute arbitrary code.

  Stack-based overflows are a bit complex. They occur when a program writes to a memory address on the program's call stack outside its intended data structure. This usually happens when a program doesn't verify the size of data from user input before storing it in a variable. In a computer program, a call stack refers to the location in memory that contains a computer program's subroutines (think of subroutines as specific instructions and tasks that make the program what it is). A stack consists of the local stack data (variables) and the program's execution instructions (subroutines). If data being saved to the stack, perhaps from a malicious request, is larger than its storage location on the stack (this is where the failure to verify the size of the input leads to an overflow in memory allocation), it can overwrite the program's instructions and allow an attacker to take over the application.

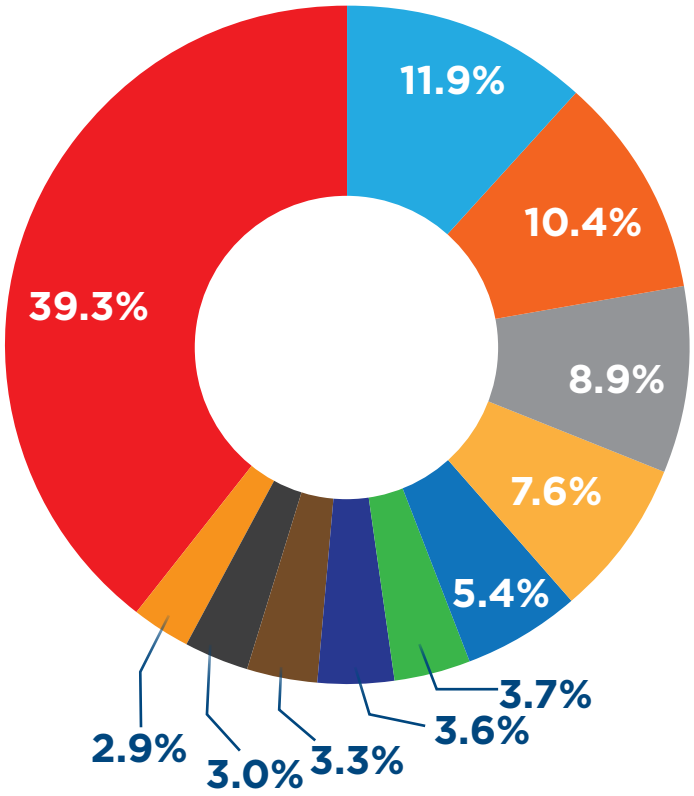
- **WEB GNU Bash Remote Code Execution – 6 (Shellshock):** This is the Shellshock vulnerability from 2014 that you may have heard of. Most Linux, Unix and Mac OS systems use GNU Bash as their command-line terminal also known as the "**shell.**" In 2014, researchers found that you could use environment variables (variables that persist in the operating system outside of individual applications) to store malicious code and then trick applications into executing that code. This was a serious issue when it was discovered because attackers could exploit the vulnerability using Internet-facing applications like web servers and SSH servers.

  This is the worst of these three attacks as it can lead to OS Command Injection attacks. Any service using a bash shell to perform tasks is prone to this exploit; examples of services include CGI-based web servers, OpenSSH servers, or DHCP clients. Following the principal of least privilege can help to mitigate the more nefarious commands.

# Top Network Threats Seen During Q3 2018

| Name | Threat Category | Affected Products | WatchGuard Signature ID | CVE Number | Count |
|---|---|---|---|---|---|
| **WEB Cross-site Scripting -36** | Access Control | Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device | 1133451 | CVE-2011-1965 | 330,385 |
| **FILE Adobe Flash Player And AIR Multiple Vulnerabilities (CVE-2014-0552)** | Access Control | Windows | 1130948 | CVE-2009-0183 | 138014 |
| **WEB Brute Force Login -1.1021** | Web Attacks | Linux, FreeBSD, Solaris, Other Unix, Network Device, Others | 1133407 | CVE-2016-7231 | 63714 |
| **WEB Nginx ngx_http_parse_chunked Buffer Overflow -1 (CVE-2013-2028)** | Buffer Overflow | Windows, Linux, FreeBSD, Solaris, Other Unix, Mac OS | 1057664 | N/A | 55614 |
| **WEB Ruby on Rails Where Hash SQL Injection (CVE-2012-2695)** | Web Attacks | Windows, Linux, FreeBSD, Solaris, Mac OS | 1056282 | NA | 41533 |
| **WEB URI Handler Buffer Overflow - OPTIONS** | Buffer Overflow | Windows, Linux, FreeBSD, Solaris, Other Unix, Others | 1054968 | CVE-2016-3078 | 37013 |
| **WEB PHP ZipArchive getFromIndex and getFromName Integer Overflow (CVE-2016-3078)** | Buffer Overflow | Windows, Linux, FreeBSD, Other Unix | 1132891 | CVE-2011-2133 | 35311 |
| **WEB GNU Bash Remote Code Execution -6 (CVE-2014-6271, Shellshock)** | Access Control | Linux, FreeBSD, Solaris, Other Unix, Mac OS | 1130029 | CVE-2006-4704 | 29655 |
| **EXPLOIT Adobe Shockwave Director PAMI Chunk Parsing Memory Corruption (CVE-2010-2872)** | Access Control | Windows | 1054264 | CVE-2010-2872 | 27557 |
| **WEB-CLIENT WScript.Shell Remote Code Execution -1 (Ransomware Attack Vector)** | Access Control | Windows | 1110895 | CVE-2016-3316 | 23729 |

# Top 10 Network Attack Percentage Overall




- 11.9% WEB Cross-Site Scripting-36
- 10.4% File Adobe Flash Player and AIR Multiple Vilnerabilities (CVE-2014-0552)
- 8.9% WEB Brute Force Login-1.1021
- 7.6% WEB Nginx ngx_http_parse_chuncked Buffer Overflow-1 (CVE-2013-2028)
- 5.4% WEB Ruby on Rails Where Hash SQL Injection (CVE-2012-2695)
- 3.7% WEB URI Handler Buffer Overflow- OPTIONS
- 3.6% WEB PHP ZipArchive getFromIndex and getFromName Integer Overflow (CVE-2016-3078)
- 3.3% WEB GNU Bash Remote Code Execution - 6 (CVE-2014-6271, Shellshock)
- 3% EXPLOIT Adobe Shockwave Director PAMI Chunk Parsing Memory Corruption (CVE-2010-2872)
- 2.9% WEB-CLIENT WScript.Shell Remote Code Execution - 1 (Ransomware Attack Vector)
- 39.3% Other Attacks

## Interesting Network Attacks Not on the Top 10

In order to keep things interesting and provide additional beneficial information to our readers, we decided to start reviewing network attacks outside of just the top 10. Looking at the top 50 attacks overall, we selected a few that stood out as worthy of specific mention.

- **WEB Remote File Inclusion /etc/passwd**:

  **Signature ID 1054837** can allow remote attackers access to the system password file on servers running vulnerable versions of ManageEngine's OpManager, Applications Manager and IT360 applications. Those applications' failure to sanitize user-supplied input can lead to unauthorized access to and the modification of data, obtaining sensitive information, or exploiting other underlying vulnerabilities in the database.

  The affected servlet called "FailOverHelperServlet" had quite a few vulnerabilities at the time. Arbitrary file download was one example, as well as listing all files in a directory and even blind SQL injections attacks.

You can read more detail **here**.

- **WEB Directory Traversal (boot.ini) -1**

  Signature ID 1110000 allows remote attackers to escape the given directory storing the 3Com Network Supervisor software and potentially access any file on that computer system. Many network services allow administrators to limit which files a remote visitor can access by designating a 'root' directory. The root directory becomes the top-most directory available for that networked application, and the application should isolate visitors to the files and nested folders within that directory. However, this vulnerability allows attackers to escape the "root" directory by simply using the command line sequence (../) used to move up one folder. By repeating this command sequence in a malicious URL, an attacker can exit an application's root directory and gain access to any directory or file on the vulnerable server. This gives the attacker unauthorized access to many sensitive files on your computer, such as the system's password file.

  This vulnerability is exploited by the lack of properly restraining "../" sequences, which are shortcuts used to move between folders via the command line. Thus, repeating this sequence properly will allow the compromised software to exit the root directory of that application, leading to accessing the computer system itself. This gives way to potentially accessing other sensitive information on that same server but not within the directory structure initially designated to the software.

  This product is used in network monitoring and considering its privileges, chances are an attacker could exploit this flaw to gain administrative access to the vulnerable system or at least read protected files. Refer to **this** for further reading around this vulnerability.

- **WEB Microsoft ASP.NET Error Handling Denial Of Service -2**

  **Signature ID 1054702**. This is a denial of service (DoS) vulnerability in an old version of the .NET Framework from 2009. The flaw can only be exploited against IIS 7.0 server that have configured ASP.NET in "integrated mode." In short, by sending a specially crafted web request, an attacker could cause your web server to become unresponsive until you reboot the system or restart the application pool.

Read more about this on **Microsoft's bulletin**.

## Quarter-Over-Quarter Attack Analysis

In our Q2 report, two network attacks we had never seen before made the top 10 list, and they remained there during Q3.

1. Previously, **WEB PHP ZipArchive getFromIndex and getFromName Integer Overflow** (signature ID 1132891) took 6th place with 37,013 hits but this quarter went down to 7th with 30,427 hits.
2. **EXPLOIT Adobe Shockwave Director PAMI Chunk Parsing Memory Corruption** (signature ID 1054264) remained at the same spot (9th) on the top ten, though with slightly less volume than the previous quarter.

If you want to learn more about these two vulnerabilities you can review the **Q2 2018 Internet Security Report**.

Out of the top 10 IPS hits, half of them are new (mentioned in the previous section) or have only occurred this quarter and last (the two mentioned just above). The other five attacks have appeared at least four other times, if not more, and go back quite some time. We'll skip those details as we've covered them before.

Overall, the top 10 network attacks only made up about 60.7% of all attacks with the remaining 39.3% being spread across the other exploits. This dropped from the previous quarter, where the top 10 network attacks accounted for 75.7% of all attacks.

Here's a highlighted summary of the top 10 and their occurrences over the past quarters:

## Top Network Threats and Their Occurrences Over the Past Quarters

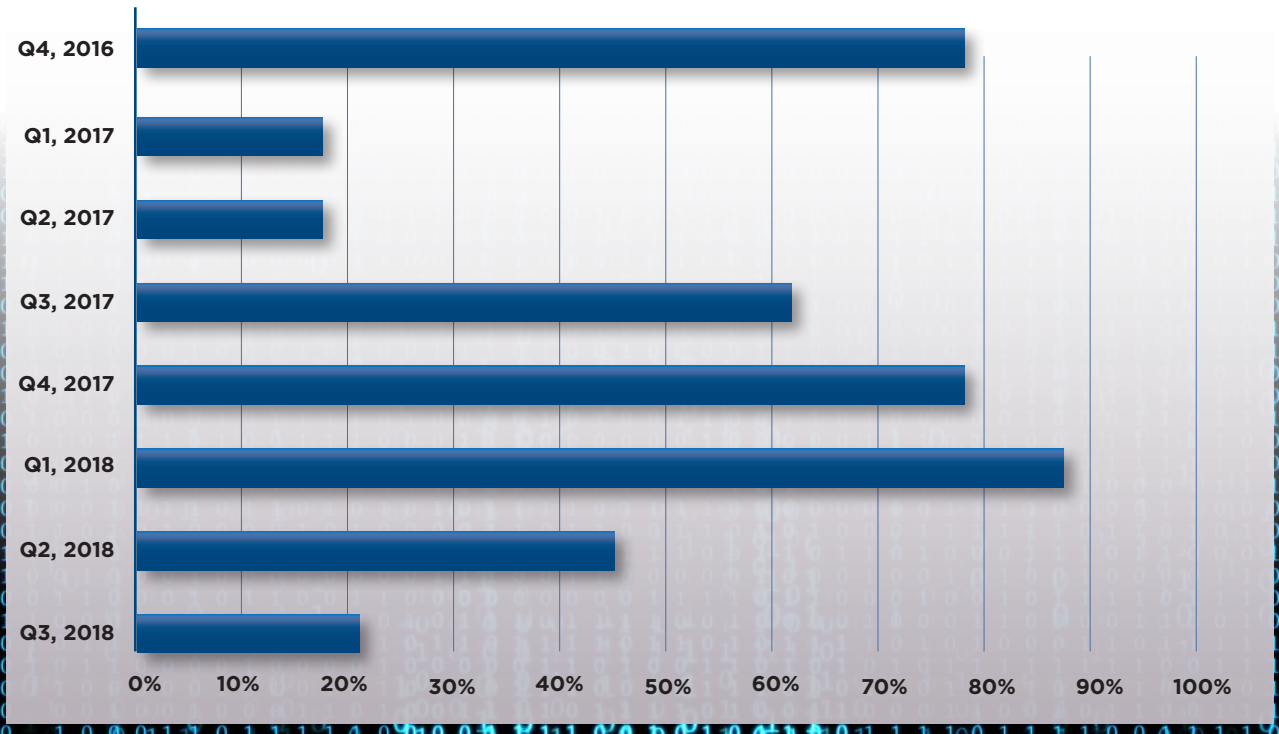
| Name | New to ISR | Total Number of Occurrences | First Appeared |
|---|---|---|---|
| **WEB Cross-site Scripting -36** | No | 6 | Q1, 2017 |
| **FILE Adobe Flash Player And AIR Multiple Vulnerabilities (CVE-2014-0552)** | Yes | 1 | Q3, 2018 |
| **WEB Brute Force Login -1.1021** | No | 5 | Q1, 2017 |
| **WEB Nginx ngx_http_parse_chunked Buffer Overflow -1 (CVE-2013-2028)** | No | 6 | Q4, 2016 |
| **WEB Ruby on Rails Where Hash SQL Injection (CVE-2012-2695)** | No | 5 | Q2, 2017 |
| **WEB URI Handler Buffer Overflow - OPTIONS** | Yes | 1 | Q3, 2018 |
| **WEB PHP ZipArchive getFromIndex and getFromName Integer Overflow (CVE-2016-3078)** | No | 2 | Q2, 2018 |
| **WEB GNU Bash Remote Code Execution -6 (CVE-2014-6271, Shellshock)** | No | 1 | Q3, 2018 |
| **EXPLOIT Adobe Shockwave Director PAMI Chunk Parsing Memory Corruption (CVE-2010-2872)** | No | 2 | Q2, 2018 |
| **WEB-CLIENT WScript.Shell Remote Code Execution -1 (Ransomware Attack Vector)** | No | 5 | Q4, 2016 |

## Battlegrounds: The Web

Web attacks continue to dominate the top 10 hits this quarter, but the total percentage for the top two web attacks wasn't as high as previous reports. In Q2's report, we pointed out that 4 out of 7 reports attributed over 50% of all IPS hits to the top two web-based attacks, with a 5th cutting it close. This quarter, only 20.8% of attacks belonged to the top two web attacks, causing this even split between the number of reports with the top two web attacks being over 50% of total attacks and not. This causes the tally to be split 50/50 over all eight reports (including this).

This quarter isn't the lowest in terms of percentages of the top two web attacks but it's the 6th ranking. Attackers are still trying to brute force login pages, so we advise you to use solid login practices. Here's a graph showing this for easier interpretation.


### Top Two Web Attacks, Historically



## Geographic Attack Distribution

Seven of the top attacks were prevalent in all regions; the Americas (AMER), Europe/ the Middle East/and Africa (EMEA), and the Asia Pacific (APAC). Here are a few regional trends:

- EMEA was not affected by the WScript.Shell attack (WEB-CLIENT WScript.Shell Remote Code Execution -1 **signature ID 1110895**).
- Likewise, AMER wasn't affected by the ZipArchive attack (WEB PHP ZipArchive getFromIndex and getFromName Integer Overflow / **signature ID 1132891**).
- Neither the ZipArchve attack (**signature ID 1132891**) nor the URI Handler Buffer Overflow (WEB URI Handler Buffer Overflow / **signature ID 1054968**) affected the APAC region.

The top 10 accounted for 516,573 of the total 851,554 network attacks, or 60.7%. Of the top 10, EMEA had the most network attacks (344,016 hits), distantly followed by AMER (156,829 – or less than half of EMEA's). APAC trailed with only 15,728 hits.

In our Q2 report, EMEA had about the same percentage of top 10 network attacks as this time, but AMER and APAC split the remaining attacks pretty evenly. In Q3, however, APAC dropped to 3%, making the AMERs a closer 2nd to EMEA. This suggests that fewer attackers or penetration testers launched attacks last quarter in Asia Pacific.

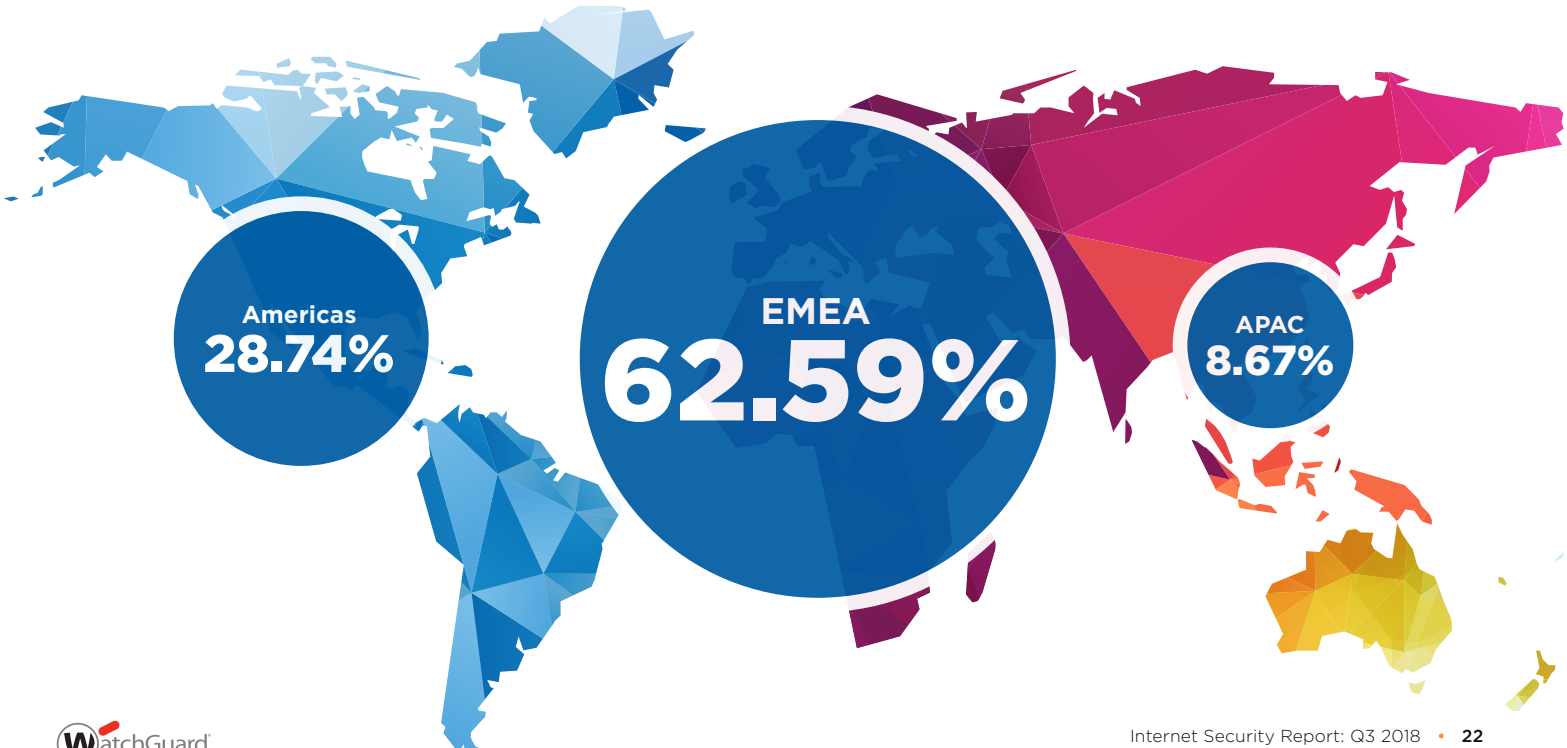
Moving out of just the top 10 network attacks. EMEA took the lead with a total of 62.59% of all network attacks, or 532,989 hits. The AMER region followed distantly at 28.74%, or 244,761 hits. APAC trailed last with only 8.67%, or just 73,804 attacks.

## Other Interesting Regional Trends:

Many of the attacks primarily affected EMEA, which makes sense given that the overall attack numbers fell in that region. Here are a few highlights:

- Though present in all regions to some extent, the Adobe Flash Player and AIR (**signature ID 1130948**) attack by far favored EMEA, with 85% falling in that region.
- 98.6% of URI Handler Buffer Overflow – OPTIONS (**signature ID 1054968**) was found in EMEA. AMER received the remaining trickle, with no hits in APAC.
- Lastly, the WEB GNU Bash (**signature ID 1130029**) exploit targeted EMEA 99.9% of the time. While there were a handful of hits in AMER and APAC, they were too few to be of any consequence.

## Total IPS Hits in Precentage by Region



# Firebox Feed: Defense Learnings

In conclusion, despite the sometimes lower volumes, malware and network attacks continue to evolve and are not going anywhere. As malware and threats advance, so must our diligence in staying abreast of those changes, and adjusting our defenses accordingly. In our Q1 2018 report, we warned you to watch out for an increase in cryptocurrency miners. Alas, we have seen that was valid advice as they grew in Q2 and continued to rise last quarter as well. Further, password stealers remain in prominence, so you should consider them a top concern. Lastly, just because you use a Mac doesn't mean that you're safe from malware. Threat actors try to get whatever they can regardless of the type of victim. As Macbooks and Apple devices continue to gain marketshare, you should expect to see more malware targeting them. With those takeaways in mind, here are a few tips to protect your environment from these threats.


## Remain vigilant against cryptominers

With attackers releasing more and more sophisticated cryptominers, pay close attention to your computer's resource usage. If you notice sluggish performance or hear your computer's fans kick into overdrive, look at your system's Task Manager or simply close your web browser and other program windows to see if you can identify the process responsible for hogging resources. Remember, attackers can embed web-based Cryptominers into web sites, and those only run when they're corresponding windows are open. Closing them should release your systems resources. That said, do know that many malicious cryptojackers use various tricks to hide their windows, so checking Task Manager is an important step to finding the offending process.

For web-based cryptominers, you can also install third-party plug-ins, such as NoCoin. Plug-ins like NoCoin can often detect and block web-based miners from starting in the first place.

Finally, if you are a WatchGuard Firebox customer, all three of our antimalware services can block cryptominers, whether web-based or otherwise. Gateway Antivirus, Intelligent AV, and APT blocker all have the ability to catch traditional malware that include cryptomining features, and two of those services can also catch the malicious javascript used to launch web-based cryptojackers. The reason we are ability to report the increase in cryptomining malware comes from the fact that we actively block it from affecting our customers. If you have our Total Security Suite (TSS), make sure you've enable all our antimalware services.


## Macs DO get malware.

This quarter, we saw 'MAC.OSX.AMCleaner' as a top threat, which goes to show that malware can indeed infect Mac users. As described earlier, this threat malware tries to convince you to buy fake malware cleaning products, which in turn forward you to malicious domains. This more sophisticated variant even uses a valid Apple-issued certificate with a valid fingerprint to helping it bypass MacOS protections. Don't trust fake alerts and if you're in doubt, get a second opinion from an IT technician. Furthermore, if you haven't installed any Mac security software due to the impression that they are invulnerable to attacks, it's time you change that opinion. You do need to install antimalware and security software on your Mac (though WatchGuard's Firebox can protect you when you remain inside the office network).


## Don't download just anything you see online.

With more malware and network attacks being delivered via the web, don't just download anything you see—even if you feel the software comes from a trusted provider. Taking the simple step of submiting new files to Virus Total (a free service that scans the file using tens of antimalware products) is a great idea. Don't forget that hackers can hide malware in many types of files, not just executables. Potentially malicious downloads can include all Microsoft Office documents, Adobe Flash or shockwave files, and even image formats as well. If you download any type of file from the outside source, it's worth scanning using tools like VirusTotal.

That said, if your computer sits behind a properly configured Firebox with TSS, it does scan those files before they reach your computer using three different scanning methods. It certainly doesn't hurt to triple-check them using additional services like VirusTotal, but having Total Security alone will protect you much more than the average legacy antivirus product.

# Top Security Incidents

# Top Security Incidents

## Facebook Breach

It has been a pretty rough year for Facebook. Back in March, a whistleblower from the research firm Cambridge Analytica revealed that they had harvested information from over 50 million Facebook profiles, which they then used for targeted political advertisements. In response, the United States Congress forced Facebook's CEO Mark Zuckerberg to testify, while their CTO met a similar fate in front of the British parliament.

Facebook spent much of the year attempting to repair their reputation, touting their renewed focus on user privacy. In late September though, Gizmodo journalist Kashmir Hill published an article on Facebook's use of "shadow contact information" for targeted advertisements. As a practical demonstration, Hill successfully targeted an advertisement at Alan Mislove, a professor at Northeastern University, using his landline telephone number, something he never shared with Facebook.

Just a few days later, Facebook notified the public that nearly 50 million users had fallen victim to a breach that enabled full account access. An attacker managed to exploit several bugs, which when chained together, gave them total control of targeted accounts. To Facebook's credit, they quickly shut down the vulnerable module and forced potentially affected users to re-authenticate.

Over a few days, Facebook released more details about the attack. From their disclosures, we can build a reasonably accurate picture of how the attacker managed to breach one of the largest companies in the world.

## Web Authentication

When you submit login credentials to a website it validates those credentials against its back-end database and generates, then sends, your browser an authentication token, usually in the form of a session cookie. This token acts as a nametag for your browser on the website. Any time you interact with the website, like updating your address or adding a product to your shopping cart, your browser includes your nametag (authentication token) with the request. On the back end, the server confirms the token is still valid and then associates the action with your account. If someone were to steal your nametag, they could perform actions on the website pretending to be you as long as the cookie remains valid.

## The Attack

Prior to them disabling it in response to the breach, Facebook had a feature called "view as," which allowed users to view their profile as it looked from another user's perspective. This was designed to allow users to confirm their privacy settings and

ensure certain parts of their profile were hidden from specific audiences. Facebook understandably designed this feature to be view-only, meaning you can't create any posts while in the "view as" mode.

During their investigation of the breach, Facebook discovered that the "view as" mode wasn't entirely view-only. On your birthday, Facebook adds a special post box that allows your friends to wish you a happy birthday by either posting a message, a picture, or a video. While using the "view as" mode to view your own profile on your birthday, the option to post a happy birthday video was not properly disabled. This was the start of a series of bugs that allowed an attacker (or multiple attackers) to compromise almost 50 million accounts.

Normally, when you upload a video to Facebook, it uses your existing authentication token that you received when you last logged in to your account. As long as your token is still valid, meaning you haven't logged out or it hasn't expired, Facebook accepts the video upload and ties it to your account. This wasn't the case with the faulty birthday video uploader though.

During July 2017, Facebook introduced a new version of its video uploader. This new version didn't use your existing authentication token when uploading a video but instead generated a new one. This on its own isn't a security issue. Web applications often re-generate authentication tokens as you navigate around and interact with them to avoid prematurely kicking you out of your session, and forcing you to log back in. You've probably seen this in action if you've ever left your bank account open in a browser tab, and returned to find a pop up asking if you would like to continue your session. Generating this new authentication token only became a critical security issue when combined with Facebook's "view as" feature.

The third, and most critical flaw in this chain of exploits, was who Facebook generated the authentication token for. Facebook, and the attacker, found that when you use the "view as" feature to view your profile on your birthday as someone else, the video uploader generates an authentication token for that other person. Facebook includes that authentication token as part of the page's HTML, which means the attacker could intercept and save it. The attacker could, and did, use that token to obtain full access to the account they used in the "view as" feature.

An attacker could trivially write a script to programmatically exploit these flaws. Once they obtained access to an account, they would only have to change the user's birthday to the current date, then use the "view as" feature to load the video upload form as each of that user's friends, steal their authentication tokens, and repeat the process with the new batch of compromised accounts. This is likely how the attacker was able to compromise 50 million accounts so quickly.

## The Response

Facebook responded to the attack by immediately disabling the "view as" feature, pending a full security audit. They identified the nearly 50 million accounts affected by the attack and revoked all authentication tokens. These users were forced to re-authenticate the next time they logged in to Facebook or the Facebook Messenger app. They also revoked tokens for another 40 million accounts that were the subject of a "view as" lookup in the last year. In a separate response, Facebook confirmed that any third-party account linked to a Facebook login could have been accessed as well, though they saw no evidence of it actually happening.

# Lessons Learned

Facebook's rough year gives us the opportunity to discuss security and privacy in the information age. There is no putting the genie back in the bottle when it comes to our society's adoption, and reliance, on social media platforms. There are however, lessons we can learn from Facebook's latest breach.

1

## Convenience vs. Security

Facebook, Google and other service providers often provide options to link accounts with third-party services instead of creating unique accounts. Using your existing Facebook session to order a pizza adds convenience but comes with potential security risk. In this breach, the attacker could have used the stolen authentication tokens to access any linked accounts as well. Always consider the tradeoff between security and convenience when deciding whether to link an account or to create a unique account on any given service.

2

## Social Media Privacy

We have now seen several instances in the last year alone of privacy compromises via social media. This latest breach proves that you can't even rely on built-in privacy-restriction tools to always limit access to your personal information. Regardless of the account or service provider, you should always consider the assumption that anything you put on the Internet will eventually become public.

3

## Chaining Vulnerabilities

Many attacks, this one included, are the result of chaining multiple vulnerabilities together. By finding ways to combine multiple flaws in an application or system, attackers can often elevate seemingly minor bugs into critical flaws. If you maintain a system or application and receive a bug report, always consider how other features may interact and open up new issues.

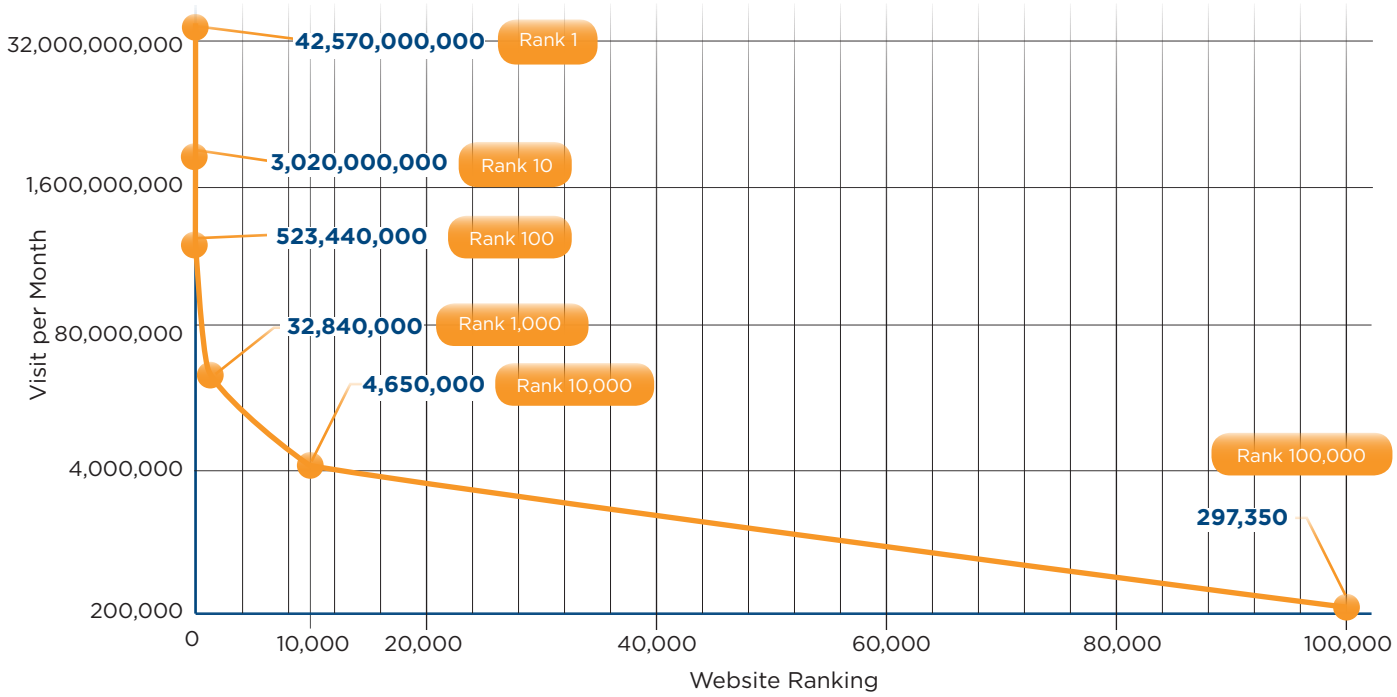

# WatchGuard Threat Lab Research

# Analyzing the Security Posture of the Top Websites

With the release of TLS 1.3 and the deprecation of TLS 1.0 and TLS 1.1 for PCI compliance in June, we wanted to find out just how secure the average website is today. Last quarter, we launched a research project to probe the general security posture of the Alexa top 100,000 websites. In this test, we analyzed two things; whether or not the top sites used secure, up-to-date versions of SSL/TLS, and whether or not the top sites use recently revoked Symantec certificates. We then graded the sites tested as a whole.

With over one billion websites on the Internet, testing each one is not realistically possible. We suspected the top websites make up most of the Internets users' page visits. To prove this, we used the Alexa top 100,000 results and results from similarweb.com. Alexa compiles a list of the top one million websites in order of the most visited. Similarweb.com also compiles the top websites by the most visited and provides estimated visits per month for the most popular websites. The chart below shows how much we visit the very top websites compared to websites ranked closer to 100,000. Assuming this holds true for the ranking of all websites, investigating just the top 100,000 websites provides a good compromise between available time and getting accurate results.

## Visits per month for top 100,000 websites



# Top 100,000 Website SSL/TLS Security

SSL and TLS are protocols used for secure web traffic. These protocols allow you to both validate that you're at the right site when visiting a domain and allow your computer to encrypt all your communications to that domain. Over time, the SSL/TLS protocols have had to evolve with new standards due to security weaknesses and vulnerabilities. Websites that support older SSL/TLS protocols are even more dangerous than sites that don't support TLS at all because they can fool the user into thinking the connection is secure when it really isn't. This quarter, we wanted to see how the top 100,000 sites fared against the latest SSL/TLS security standards.

In general, the SSL protocol (including SSLv2 and SSLv3) is no longer considered secure because of fundamental flaws that attacks like **POODLE** can exploit. The industry will soon deprecate TLS 1.0 and TLS 1.1 because of similar security concerns. In some cases, just leaving one of these legacy protocols enabled on a web server can leave your visitors vulnerable to various security issues that may allow attackers to intercept their data, such is the case with the **DROWN** vulnerability.

Though the Internet Engineering Task Force (IETF) still considers TLS 1.2 secure, they recently ratified TLS 1.3, which adds several security improvements. As part of our test, we analyzed which SSL/TLS protocols the top 100 thousand websites supported, giving us some insight into each website's security. For instance, if a site still supports SSLv2 and SSLv3, it suggests less security diligence from that web administrator. Below we share the results from our testing and analysis.

### Highest Protocol Supported for Websites That Still Support SSLv2 or SSLv3

| NUMBER OF SITES | HIGHEST SUPPORTED PROTOCOL |
|---|---|
| 0 | SSL2 |
| 5 | SSL3 |
| 2,221 | TLS 1 |
| 53 | TLS 1.1 |
| 59,580 | TLS 1.2 |
| 17,345 | TLS 1.3 |
| 20,911 | No encryption supported |

*We found 24 of the websites we tested accept SSLv2 but not SSLv3, yet still accept more recent protocols like TLS1.x. When testing just the sites that support SSLv2 and SSLv3 we found all but 5 support a higher protocol.*

Overall, 79,089 of the top 100 thousand website used HTTPS and responded to some version of SSL/TLS. That leaves 20,911 websites that still use unencrypted HTTP, which falls right around the global average of HTTPS usage per Google's **HTTPS Transparency Report**. We didn't add HTTP sites in our statistics because the sites are not trying to be secure and are clearly shown to not be secure. A distinct difference from the sense of security given by HTTPS sites.

**From the 79,089 HTTPS uses:**
5,383 or 6.8% still accept SSLv2 or SSLv3, deprecated and insecure protocols.

- 4,474 or 5.7% support SSLv3
- 909 or 1.1% accept SSLv2

In our opinion, there is no good reason for these sites to support SSLv2 or v3. Luckily, many of these sites will still accept a more secure protocol when offered. However, retaining support for older SSL protocols can allow hackers to force downgrade attacks.

Surprisingly, more websites support TLS 1.0 as their highest protocol rather than the more secure TLS 1.1. We find this disappointing and believe it indicates a lack of willingness or vigilance to increase security. Granted, we've seen this sort of secure apathy before. Unfortunately, some website administrators only consider security after receiving outside pressure.

On the other end of the spectrum, two websites, kinogo-2018.net and moovie.cc, only support the most secure TLS 1.3, and won't downgrade to a less-secure protocol. This shows that these site owners prioritize their site's security and their visitors' privacy, which is ironic since the one of the sites is currently categorized as compromised by our WebBlocker. Websites that are compromised indicate a malicious user has manipulated the site. Also, somewhat ironic is the site seems to trade in pirated movies.

We wish we could say that the websites that use older protocols are just placeholders or at least don't send and receive any user information. Unfortunately, this is not the case.

Of the 909 sites that support SSLv2, 349 respond to the weakest SSLv2 cipher suite (SSL_CK_DES_192_EDE3_CBC_WITH_MD). When we reviewed these sites to determine if they might have sensitive user data like a login, banking info, or other personally identifiable information (PII), we found 12 sites of interest. For example, we were surprised to find a website run by the Massachusetts State Lottery Commission – a government committee – still supporting SSLv2. Masslottery.com, as you might guess, provides information and records from the Massachusetts State Lottery. We couldn't find any user inputs, which is good, but there was a location that told visitors where to send payments. An attacker could exploit the weak SSL protocol to launch a man-in-the-middle (MitM) attack and manipulate a visitor's payment address. In any case, we did not expect a website run by the U.S. government to use SSLv2. Below are a few more examples of surprising sites using SSLv2.

- Tkj.jp is a magazine and shopping website from Japan. It sells products such as magazines, clothing and purses to users around the world. This site eventually directs visitors to www.worldshopping.global to input their credit card information. Unfortunately, www.worldshopping.global also supports SSLv2. It is our opinion that this set-up shows a lack of concern for customer security.
- Ugamsolutions.com advertises themselves as a global leader in data and analytics. They are located in India but have an English website with phone numbers in the United States, United Kingdom, Australia, and India. The site accepts job applications and resume. Using a MitM attack, hackers could compromise this website's connections to steal personal information, such as resumes, from visitors without them knowing.
- Exist.ru is a Russian site where it appears visitors can purchase vehicle parts. The login portal for Exist.ru directs you to connect.exist.group. This domain also uses SSLv2. Attackers could easily exploit this flaw to redirect the purchases and potentially steal credit card information.
- Simplysportsware.com is a sports gambling site that requires payment after a trial period.
- Tallentex.com is another site based in India,

## Vulnerable Websites

What information could be transferred over the vulnerable connection

| Website | Credit Card Info | Identification Number | Username & Password | Work History/ Resume | Home Address | Phone Number | Birthdate | Email Address | Name |
|---|---|---|---|---|---|---|---|---|---|
| masslottery.com | | | | | | | | | |
| tkj.jp | ✓ | | | | ✓ | ✓ | | ✓ | ✓ |
| ugamsolutions.com | | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| exist.ru | ? | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ |
| simplysportsware.com | ? | | ✓ | | | | | ✓ | ✓ |
| tallentex.com | | ✓ | ✓ | | | ✓ | ✓ | ✓ | ✓ |
| iranian.cards | | | | | | ✓ | | ✓ | ✓ |
| edjoin.org | | | ✓ | | | ✓ | | ✓ | ✓ |
| wisestep.com | | | ✓ | ? | | | | ✓ | ✓ |
| destoon.com | | | ✓ | | | ✓ | | ✓ | ✓ |
| vns6489.com | ? | | ✓ | | | | | | |
| okmart.com.tw | ? | ✓ | ✓ | | | ✓ | ✓ | ✓ | ✓ |

*exist.ru, okmart.com.tw, and vns6489.com either prevent access to the site based on the location or require a country ID number before making purchases.*
*simplysportsware.com says it will charge after a few weeks but we have yet to see the end of the trail period.*

this time for a technical school. The student registration form on the website requires a name, birthdate, phone number, and a kind of country ID. Other locations such as the Associate (careers) page require similar information. All of these forms still support SSLv2.

- Iranian.cards is a credit card sales site. They require your name, email, and phone number for support. Login and application forms do use a more secure protocol but a finance company that still uses SSLv2 as a security method at any location shouldn't exist today.

While its entirely up to web administrators to keep their websites secure, a little user vigilance can help you avoid the more dangerous parts of the web. As you can see, some websites use more secure encryption standards than others so don't let your guard down on the web. If a website uses a deprecated encryption standard, it could indicate they have poor security in their back end as well. We recommend avoiding inputting any private information on sites that support outdated protocols. To prevent this, we recommend disabling the use of SSL. Disabling all protocols but TLS 1.2 and TLS 1.3 would be best but sometimes this will prevent some websites from working. If you are using Windows you can change this in the **Internet Options**. You can also test which SSL/TLS protocols are supported on the website by checking the site at **https://www.ssllabs.com/ssltest/analyze.html**. TLS 1.2 should be supported on the site but if TLS 1.3 is supported this is even better. SSLv2 and SSLv3 should not be supported on the site.

## Top Sites Still Using Revoked Symantec Certificates

Over the past year, Symantec has fallen into disrepute among the industry that assigns digital certificates for breaking certificate assignment best practices. As a result, most web browser vendors have decided to revoke Symantec's digital certificates. On October 16th, Google released Chrome version 70 which revoked trust of Symantec-signed certificates. Firefox version 63, released on October 23rd, quickly followed suit with the same planned revocation. We wanted to see exactly how many sites were destined to fail HTTPS validation due to the continued use of revoked Symantec signatures.

We tested each of the top one million domains, both as the stand-alone domain and with "www," to see how many were still using Symantec-signed certificates. On Sep 9th, 2018 we found 2,568 of the top one million websites still used Symantec certificates. On Oct 11th, 764 of those websites had replaced their Symantec certificates to fix the issue, leaving 1,804 that would have issues soon if they didn't update their certificates.

Finally, on the Symantec D-day (when Chrome 70 released on Oct. 16th), 1,633 websites still used the now-revoked and untrusted Symantec certificates. Admittingly, that is only a meager 0.16% of the top one million sites, but these top sites receive millions of visits per month. 25 websites in the top 10,000 still had Symantec certificate issues on their domain or a subdomain.

### Domains that failed on Symantec D-Day

| Domain | Alexa Page Rank |
|---|---|
| hotstar.com | 98 |
| msi.com | 921 |
| iciba.com | 1763 |
| internetspeedtracker.com | 1974 |
| renren.com | 2024 |
| emirates.com | 2720 |
| endclothing.com | 3368 |
| wanfangdata.com.cn | 3389 |
| timewarnercable.com | 3911 |
| ufc.com | 4014 |
| rzd.ru | 4024 |
| caixin.com | 4271 |
| sbi.co.in | 4834 |
| jbhifi.com.au | 4980 |
| cimbclicks.com.my | 6107 |
| oppo.com | 6262 |
| wintalent.cn | 6988 |
| egypt.gov.eg | 7433 |
| qdaily.com | 8453 |
| platnosci.pl | 8696 |
| solidworks.com | 8739 |
| postupi.online | 8813 |
| porsche.com | 8857 |
| pbebank.com | 9127 |
| evga.com | 9540 |

## Top Websites Graded

We gave the top websites we analyzed a grade based on the combined results from our tests. The higher the security risk the more it affects the grade. Here are the results.

- **Deprecating Revoked Certifications: B**

  When pressed by the industry to remove bad certificates (as in the Symantec case), web administrators did fairly well. We only found 1,633 of the million tested sites continuing to use Symantec certificates after the Chrome release that revoked them. Not quite perfect, but still enough to get a B grade.

- **SSL/TLS Security: D**

  Some website admins are a little slower to respond when they are not in danger of having errors on their website. The good news, around 75% of websites that support encryption support TLS 1.2. The bad news, just under 7% of the top websites still support SSLv2 and SSLv3. Because of those holdouts, we're lowering the grade down to a D.

We hope this analysis gives you a decent idea of the security posture of the top websites people visit. While our tests cover only a small portion of the Internet as a whole, the majority of web traffic visits these sites regularly, and we believe you can extrapolate some of these trends to other sites as well. Though most of the top one 100 sites did OK, we did find a few laggards.

While website admins do update their security when pushed, many don't update to higher security standards like TLS 1.2 or TLS 1.3 when they become available. The websites that we tested failed in proactive security, though many sites did ok. This type of reactive maintenance is not good security practice. While the majority of sites have been using the latest security updates it is still possible that when visiting a HTTPS site, you are not completely safe. This minority of websites, that constantly change, is why we must stay vigilant at all times. User care and preparedness will again be the best protection against these sites and bad certificates. The OS and browser security updates should always be applied without delay to prevent any known vulnerable protocols from being used, as well as stop some intrusion attempts. As previously mentioned, your best defense against the use of bad certificates and lower security protocols is to update your browser and set your OS to only use TLS 1.0 and higher, or TLS 1.2 and higher if possible.

# Conclusion & Defense Highlights

# Conclusion & Defense Highlights

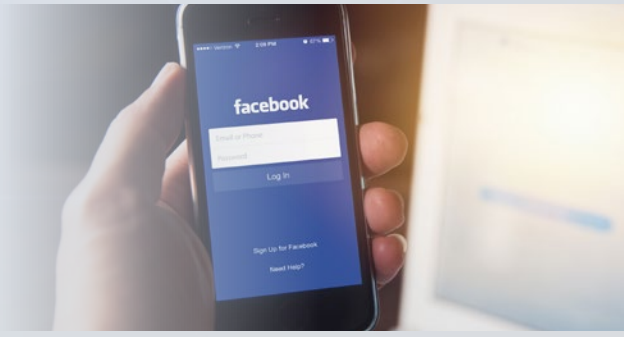
Last quarter saw a mix of good and bad news for defenders. On the positive side, network attacks dropped to a new record low, with fewer network exploits than we have ever seen during the history of our report. Meanwhile, on the negative side, malware has grown significantly in volume, and we expect to see it get even higher during Q4. While these seasonal volume changes can be interesting to security professionals, you shouldn't read too much into them. The fact remains that malware and network attacks will continue to plague Internet victims. Just because network attacks have dropped today, doesn't mean the next new zero day worm won't explode like wildfire tomorrow. You should not use the decrease in volume as an excuse to not use or invest in intrusion prevention (IPS) measures.

Despite cryptocurrencies' general drop in value, hackers continue to have great interest in it. Cryptominers remain a top malware threat, and likely will remain high on the list for the quarters to come. Luckily, even the more basic anti-malware services do a decent job of detecting these miners. If you use malware protection, you should remain fairly safe.

We saw a new trend in Q3 with Mac malware making our top ten list for the first time. Many Apple users still operate under the false impression that Macs somehow have better security than other computers. While Apple does take security seriously, and has some smart security features, the truth is macOS has had just as many critical vulnerabilities as any other operating system. Much of Apple's reputation for low malware infections likely has more to do with market share than any magical invulnerability. However, that market share has shifted, and attackers now see Apple equipment as a very attractive target. If you haven't installed security software on your Mac yet, perhaps our report will convince you to change your mind.

Also, don't forget that hackers are targeting authentication. As we mentioned in our previous report, authentication is the cornerstone of security. If an attacker can get one of your privileged credentials, they don't need software exploits or malware to compromise your network. They can bypass your security by exploiting that valid user account. Mimikatz – a well-known credential-stealing program – remained as the top threat in Q3. If you haven't deployed multi-factor authentication (MFA) across your business yet, we highly recommend it.

Finally, it's time you educate employees about the risks of social media. Social media hasn't just become a staple of personal life but has become critical to business as well. Unfortunately, its value to keeping us connected also benefits attackers who want to leverage our trust in our networks against us. Threat actors, from nation-states to cyber criminals, have realized how social networks can greatly increase their social engineering success and use these networks to learn exactly how to trick us into falling for their scams. You should help your employees to tighten their social network privacy settings and warn them not to share anything that they wouldn't share with the whole world.



**With those Q3 highlights in mind, here are a few high-level defense strategies against the top threats.**

## Everyone needs Multi-factor Authentication (MFA)

We've shared this tip in many reports, but SMBs still remains behind at adopting MFA. You'd have to be living in an igloo in the Arctic Circle to have missed the fact that the average user doesn't use passwords properly, and thus authentication remains weak. To solve this problem, the industry as a whole seems to be pivoting towards biometrics instead. While biometrics are great when it comes to usability, they aren't necessarily more secure than any other single factor of authentication. Security researchers and hackers have broken many biometric solutions, from fingerprint readers to the latest Apple FaceID technology. The only way you can really validate your users is by leveraging more than one factor of authentication. We don't care which two (or more) factors you combine. It could be a password and a certificate, a biometric and a device (like a mobile phone), or any other combination. However, we highly recommend you deploy MFA to all your employees as soon as you can. Otherwise, it's just a matter of time before some malicious actor leverages your own stolen user credentials against you.

## Install an endpoint security suite on remote Mac computers

Most organizations have perimeter security controls, such as WatchGuard's Firebox, protecting employee computers at the office. However, these same organizations realize that they need to install additional security software on roaming Windows devices that leave the network. However, many Apple users seem to have developed the delusion that Mac computers are more resilient to cyber attacks than any others. This is not true! Though Apple has made some smart secure design choices (secure boot, separating root privileges, built-in protections like GateKeeper), they have had many critical vulnerabilities in the past, and can get infected with malware like any other computing device. We believe the lower volume of Apple malware has more to do with market dynamics than it has with better security; and those dynamics are changing.

In any case, last quarter Mac malware made our top malware list for the first time, which proves that cyber criminals are targeting it. If you haven't already, we highly encourage you to install a security suite on your Mac machines. At the very least, it should include some sort of antivirus capability, but we also like ones that include more advanced firewalling, malicious URL filtering, and more.

## Train users on social media best practices and help them harden their accounts

Social media has become a core part of most businesses, if anything, for marketing alone. Many employees use their social media accounts both for personal and business use. Furthermore, even if your employees only keep their social media personal, it's still a great place for an attacker to gather data about them, which they can leverage in an attack targeting those employees at work. It's time you help them understand social media security best practices, which can benefit them both at home and at work.

When considering training, first and foremost teach them about the many privacy settings these networks offer that can help keep certain types of data more private. Second, teach them about the tradeoff between convenience and security. Sure, setting up your new WordPress blog using your Facebook account is much quicker, but do you really want an attack to have access to your Facebook if they have WordPress? Finally, remind them that even with privacy settings, and social networks' best intentions, these vendors make mistakes. Thing you post online, no matter how limited, have a chance of leaking to the whole world. As they share things on social media, they should consider if it's something they really would want the whole world to know about.

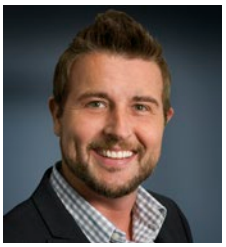
## Layer anti-malware services with IntelligentAV

One of the main points of our report is to show that malware and attacks change quarter by quarter. Malware, especially, evolves quickly with automated delivery services literally creating new variants for each victim in order to evade legacy antivirus solutions. This is immediately apparent in our quarterly "zero day malware" ratio. In Q3, approximately 29% of malware got past our basic, primarily signature-based anti-malware service (GAV). This is less than some quarters, but still almost one-third of all malware. Even a single malware miss can lead to a very bad day for IT administrators.

The only way you will defend against all of today's malware variants is to layer your malware solutions. With Total Security Suite, our Firebox layers three different malware detection engines into one extremely effective anti-malware solution. We use signature-based GAV to quickly catch the most common threats, but also employ both behavioral and machine-learning/AI-based solutions to detect the new malware that pattern-based AV misses. If you're a Firebox owner, we recommend Total Security to combine all these anti-malware options. Otherwise look for more advanced malware solutions from whichever vendor you prefer.

So that's it for another exciting quarter of cyber threat analysis. This quarter we learned that criminals are targeting Apple devices, malware authors continue to focus on cryptominers, and Facebook is still bleeding data. However, with these insights you can adjust your defenses and cyber security strategies to avoid being a victim of the latest threats. Like the executive that leverages data to find success, we hope our threat statistics help your cyber security programs succeed.

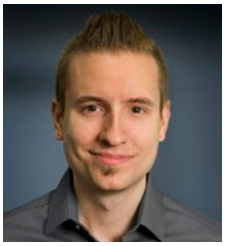
We hope you found the information in this report useful and return next time to see what changes in Q4. As always, we encourage you to leave any comments or feedback about this report at **SecurityReport@watchguard.com**. Thanks for reading. See you next time.



**Corey Nachreiner**

*Chief Technology Officer*

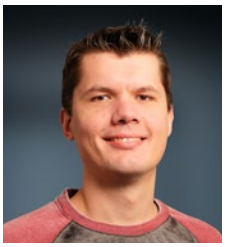
Recognized as a thought leader in IT security, Corey spearheads WatchGuard's technology vision and direction. Previously, he was the director of strategy and research at WatchGuard. Corey has operated at the frontline of cyber security for 16 years, and for nearly a decade has been evaluating and making 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.



**Emil Hozan**

*Jr. Security Threat Analyst*

Being a member of WatchGuard Technologies' Threat Lab as a Jr. Security Analyst, Emil hopes to bridge the technological rift between end users and the sophistication of technology. Taking complex situations and then analyzing and breaking them down, Emil enjoys diving deep into technical matters and summing up his findings in an easy-to-digest manner. He believes that being security-aware while online is only the tip of the iceberg and that what goes on in the background is just as important as being cautious. Emil is a technological enthusiast with many qualifications and years of experience in IT.

**Trevor Collins**

*Jr. Security Threat Analyst*

Trevor Collins is a Jr. Security Analyst at WatchGuard Technologies, specializing in network and wireless security. Trevor earned his security knowhow and several certifications through his past military experience in the United States Air Force. Trevor is a regular contributor to Secplicity.org where he provides easily understood data analysis and commentary to IT professionals. Trevor's experience with a wide range of network security vendors and technologies allows him to provide unique perspectives to the industry.

## 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, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by nearly 10,000 security resellers and service providers to protect more than 80,000 customers. WatchGuard'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. The company 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**.