

# Internet Security Report

QUARTER 3, 2019



# 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 Overall Malware Trends
- 09 Most-Widespread Malware
- 10 New Malware Hits
- 12 Quarter-over-Quarter Trends
- 13 Year-over-Year Trends
- 13 Geographic Attack Distribution
- 14 Zero Day vs Known Malware

### 15 Network Attack Trends

- 17 Top 10 Network Attacks Review
- 18 Top 10 Network Attack Percentage Overall
- 20 Geographic Attack Distribution

### 22 DNS Analysis

- 22 Top Malware Domains
- 23 Top Compromised Websites
- 24 Top Phishing Domains
- 25 Firebox Feed: Defense Learnings

## 26 Top Security Incidents

### 27 Kazakhstan Forced HTTPS Decryption

- 28 HTTPS Encryption and Decryption
- 29 Other National Programs
- 29 What About the Office?
- 31 Important Takeaways

## 32 Conclusion and Defense Highlights

## 35 About WatchGuard

# Introduction

If you believe one of the most [popular TV shows in the world](#), [CSI: Crime Scene Investigation](#), forensic analysts prefer scrutinizing crime scenes in the dark, using just a flashlight. This particular cliché TV trope came up while a friend and co-worker of mine discussed our love of procedure forensic crime dramas like CSI (and its spin-offs), [NCIS](#), and [The Killing](#) (I recommend [the original Danish one](#), too). We wondered, “do cops or forensic investigators really search crime scenes in the dark with just a flashlight, even when normal lights are available?”

To be honest, I don't know how legitimate that particular Hollywood crime show trope is but you can find at least one [law enforcement official defend it online](#). Specifically, that official points out that a flashlight can help illuminate hidden evidence in two ways. First, it provides oblique lighting, which creates harsh shadows and helps anomalies stand out. Second, it greatly focuses the viewer's field of view (FOV), forcing them to really concentrate on the area they're examining.

WatchGuard's Threat Lab team are like forensic cyber investigators who shine our analytical flashlight into the threat landscape in order to uncover hidden digital cyber crime trends. Our quarterly Internet Security Report includes detailed threat intelligence about the top and most-widespread malware, the most common network attacks seen in the wild, and the top domains targeting your users. While the report includes raw numbers and high-volume trends, the true value lies in our experts' additional analysis and insight. Like the flashlight focusing criminal investigators on that one small detail that solves a case, our analysts highlight the important veiled findings from our oceans of data so that you know how to focus your defenses to defeat the latest threats.

**There's a lot you can learn just by “turning on the lights” of our Firebox Feed data and taking in the high-level trends. However, the best findings come from the flashlight WatchGuard's Threat Lab expertly shines into the nooks and crannies of this data. Let us be your cyber crime scene investigators this quarter and solve the case of how to stay breach-free going forward.**



## The Q3 report covers:

### Q3's Firebox Feed results.

The bulk of our report comes from threat intelligence data that tens of thousands of Fireboxes share with us, called the Firebox Feed. This feed includes historical data about the top malware, both by volume and percentage of victims affected. It also includes network attack statistics based on our intrusion prevention service and our DNS security service. We also highlight interesting regional trends, when relevant, and give you advice for protecting yourself from the latest threats. Our flashlight exposes the most relevant threat details from each quarter, so you don't have to find them yourself.



### Top Story: Kazakhstan HTTPS MitM

Secure web traffic, or HTTPS, is supposed to be protected from prying eyes. However, there are certificate configurations you or a business can make to allow third parties to access your HTTPS traffic, usually to help secure it. Unfortunately, governments can use those same techniques to spy on their citizens' traffic, which is exactly what happened in Kazakhstan during Q3. In this section, we detail how the Kazakh government intercepted the entire country's HTTPS traffic and discuss what implications that could have to Internet security going forward.



### Defense Strategies and Tips

Throughout this report, we'll shine light onto the latest attack techniques, new malware strategies, and the most malicious sites your employees click on. These scary trends could convince even the biggest cyber junkie to avoid the Internet. However, you don't have to go to that extreme. Once you understand the latest attack strategies, it's easy to guard against them. Throughout the report, we'll share insights and defense tactics that will protect you from these evolving threats. Remember, if we saw it in our report, we blocked it.

# Executive Summary

This quarter the team saw significant increases in both malware and network attacks. Beyond the raw volume, we discovered cyber criminals targeting Apache Struts – specifically reusing the vulnerability responsible from the Equifax breach. We also noted that zero day malware rose to an all-time high – just a smidge under 50% of all malware. This means that almost half of the malware our customers encountered during Q3 could sneak right past legacy AV detection. Finally, we analyzed how one government hijacked the secure web connections of all its users to potentially spy on them, and what ramifications that might have on Internet politics and policy.

## Additional Q3 2019 Internet Security Report highlights include:

- **Two Apache Struts exploits made our top 10 network attacks in Q3.** Notably, this includes the specific one **used during the Equifax breach**. If you haven't patched yet, you should immediately.
- **Total Malware rose 30%** during Q3 2019. Meanwhile, **zero day malware accounted for just under 50% of all malware**, which is higher than ever before.
- **Gateway AntiVirus blocked 23,009,403 malware variants, a 4% increase QoQ** and a **60% increase YoY**. Win32/Heri, a generic rule used to detect different trojan families, represented a disproportionately large amount of hits.
- **Network attacks rose 8% QoQ**, continuing the increase in intrusion prevention service (IPS) numbers for a second quarter in a row. The amount of unique attacks remained relatively stable at 345.
- **A large majority of attacks targeted the Americas (AMER)** with 60% of hits affecting that region. Specifically, Brazil was targeted with a high volume of attacks.
- **Mimikatz was finally dethroned** after over a year as the number one malware, dropping to number three. However, a new credential threat, Windows Credential Editor (WCE), made the list showing that authentication still is a target.
- DNSWatch found a **legitimate image-sharing site abused to spread malware**. By not validating files beyond extension, the site makes it easy for attackers to store renamed malicious executables.
- We also found attackers **abusing user-controlled SharePoint subdomains to host malware**.
- For three weeks in August, the **government of Kazakhstan** used a forced CA certificate to **man-in-the-middle (MitM) all their citizens' Internet traffic**.
- The **Europe and Middle East (EMEA) region received the majority of the most-widespread malware**, which is malware that affects the most individual victims.
- In Q3 2019, WatchGuard **Fireboxes blocked 22,619,836 malware variants** (798 per device) across all three anti-malware engines and **2,398,986 network attacks** (65 per device).

With the big highlights out of the way, it's time to take out our flashlights and focus on the hidden details in the Q3 cyber crime scene. Keep reading to learn what important defensive takeaways we can glean from attackers' latest tactics.

```
... = modifier_ob.modifiers.new("...")
... mirror object to mirror_ob
... mirror_mod.mirror_object = mirror_ob

... operation == "MIRROR_X":
... mirror_mod.use_x = True
... mirror_mod.use_y = False
... mirror_mod.use_z = False
... operation == "MIRROR_Y":
... mirror_mod.use_x = False
... mirror_mod.use_y = True
... mirror_mod.use_z = False
... operation == "MIRROR_Z":
... mirror_mod.use_x = False
... mirror_mod.use_y = False
... mirror_mod.use_z = True

... selection at the end -add back the deselected
... mirror_ob.select= 1
... mirror_ob.select=1
... context.scene.objects.active = modifier_ob
... "selected" + str(modifier_ob) # modifier
... mirror_ob.select = 0
```



```
... context.scene.objects[one.name].select = 1
... print("please select exactly two objects,")
... OPERATOR CLASSES -----
... context.scene.objects.Operator):
... on & mirror to the selected object""
... context.mirror_mirror_x"
... context):
... object is not None
```

```
... context.scene.objects[one.name].select = 1
... print("please select exactly two objects,")
... OPERATOR CLASSES -----
... context.scene.objects.Operator):
... on & mirror to the selected object""
... context.mirror_mirror_x"
... context):
... object is not None
```

# 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.

The data we receive from Fireboxes as part of the Firebox Feed does not contain any private or sensitive information. We always encourage our customers and partners to opt in whenever possible to help us obtain the most accurate data.

The Firebox Feed contains five different detection services:

- Malware our Gateway AntiVirus (GAV) service prevents.
- Malware detected by our IntelligentAV (IAV) machine-learning engine.
- Advanced malware detected by our behavioral analysis service, APT Blocker.
- Network exploits our Intrusion Prevention Service (IPS) blocks.
- Connections to malicious domains blocked by DNSWatch.

In Q3 2019, the Firebox Feed included threats captured from 36,794 Firebox appliances across the globe. This number still accounts for around 10% of the active Firebox appliances deployed on customer networks. If you are a customer or partner and want to help improve these results, please 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.




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

# Malware Trends





Malware increased all around in Q3 2019 when compared to Q2. This includes payloads detected by the three WatchGuard anti-malware services, Gateway AntiVirus (GAV), IntelligentAV (IAV), and Advanced Persistent Threat Blocker (APT Blocker). Most drastically, the amount of zero day malware (threats that evade signature-based detection) rose to just a fraction under 50%! Additionally, eight of the top 10 threats carried over from previous quarters with two new attacks debuting on the list. We also saw more penetration testing tools showing up on the top 10. Anti-malware services often block these types of tools as “greyware” since it’s hard to tell whether good or bad guys are using them.

In this section, we take a look at the top 10 attacks by volume, explore the most-widespread attacks, and review new malware variants in detail. We’ll also compare quarter-over-quarter (QoQ) and year-over-year (YoY) statistics. Lastly, we’ll review geographic attack distributions and also discuss zero day trends.

**WatchGuard Fireboxes with Total Security offer a multi-layered anti-malware pipeline, which leverages three types of malware detection. The services include:**

- Gateway AntiVirus (GAV) uses signatures, heuristics and other methods as the first line of defense to block malware. 
- When advanced malware bypasses signature detection, **IntelligentAV (IAV)** comes into play, using machine learning to immediately identify never-before-seen malware. 
- **APT Blocker** analyzes files in a full sandbox environment to catch zero day malware before it reaches your network. 

The order of our anti-malware services follows the list above. GAV followed by IAV, then APT Blocker. If IAV is not available, APT Blocker analyses the file after GAV. IAV requires a large amount of memory, thus only runs on our rack-mounted Fireboxes. This affects the data we see in IAV as Fireboxes with IAV enabled are normally found in larger set-ups.

 <p><b>The Firebox Feed</b> recorded threat data from <b>36,794</b> participating Fireboxes a <b>11%</b> drop in the number of Fireboxes reporting last quarter</p>	 <p><b>Our GAV service</b> blocked <b>23,009,403</b> malware variants a <b>4% increase</b> quarter over quarter (QoQ)</p>	 <p><b>APT Blocker</b> detected <b>6,125,572</b> additional threats QoQ we saw a <b>18%</b> increase. YoY we saw an increase by <b>70%</b></p>	 <p><b>IntelligentAV</b> blocked <b>220,088</b> malware hits <b>52%</b> QoQ decrease.</p>
---	--	---	--

## Q3 2019 Overall Malware Trends:

- **GAV blocked 23,009,403** malware variants, a **4% increase QoQ** and a **60% increase YoY**. Win32/Heri, a generic rule used to detect different trojan families, accounted for a disproportionately large number of these hits.
- **APT Blocker** detections increased **18% QoQ** and over **70% YoY**.
- IAV detected **7.14% of malware** on devices that support it, while APT Blocker detected **22.6% of malware** on those same devices.
- **Penetration testing tools** continue to trend up in our top 10 list. This could be either good guys testing - or threat actors nefariously abusing these open source tools.











Top 10 Gateway AntiVirus Malware Detections				
COUNT		THREAT NAME	CATEGORY	LAST SEEN
6,287,518		Win32/Heri	Win Code Injection	Q2 2019
2,439,830		Win32/Heim.D	Win Code Injection	Q2 2019
1,130,834		Mimikatz	Password Stealer	Q2 2019
1,110,231		Boxter	PowerSploit Script	NEW
743,161		Trojan.GenericKD (SBD)	Generic Win32	Q2 2019
516,512		CVE-2017-11882	Office Exploit	Q2 2019
503,861		RTF-ObfsObjDat	Office Exploit	Q2 2019
443,460		Application.Hacktool.JQ	Password Stealer	NEW
284,137		Win32/Heur	Generic Win32	Q2 2019
234,834		Backdoor.Small.DT	Web Shell	Q2 2019

Figure 1: Top 10 Gateway AntiVirus Malware Detections



## Most-Widespread Malware

Two malware samples overlapped both our top 10 and most-widespread malware lists. These threats deserve closer attention as they represent high-volume attacks that also touch the most victims.

Malware Name	Top 3 Countries by %			EMEA %	APAC %	AMER %
<b>CVE-2017-11882</b>	Greece 6.5%	Belgium 4.9%	Netherlands 4.6%	53.3%	27.2%	19.5%
<b>RTF-ObfsObjDat</b>	Greece 6.7%	Germany 4.7%	Portugal 4.5%	50.7%	31.3%	18.0%
<b>RTF-ObfsStrm</b>	Germany 6.6%	Greece 5.9%	Spain 5.3%	58.9%	25.3%	15.7%
<b>SpamMalware-RAR</b>	Hong Kong 7.5%	Greece 6.8%	Italy 5.3%	52.7%	29.4%	17.8%
<b>Trojan.Cryxos</b>	United States 33.5%	Canada 22.6%	France 15.1%	8.2%	15.2%	76.6%

Figure 2: Top 5 Most-Widespread Malware Detections

First, CVE-2017-11882 is the Common Vulnerabilities and Exposures (CVE) reference number for a [memory corruption vulnerability affecting Microsoft Word](#). The flaw specifically resides in Word's [Equation Editor](#) and allows an attacker to execute arbitrary code when your users open a maliciously crafted Word, RTF, or other format Office document. This Word-based malware first debuted on our top 10 during Q2 2018.

The second sample, RTF-ObfsObjDat, is a generic signature that catches a range of RTF document malware. In fact, it can [even](#) catch malicious RTF documents that exploit the same CVE mentioned above. It too has appeared in our previous reports, both on the most-widespread malware list in Q4 2018 and on our top 10 list during Q2 2019.

Note that both of the samples that overlap our high-volume and wide-range lists arrive as documents. This suggests threat actors are focusing on document-based attacks lately, likely because the average user falls for them more regularly. Make sure your users recognize the danger of any unsolicited documents they encounter online, whether through email or the web.

Transitioning to the most-widespread list in general, we found the regional distribution interesting in that four of the five threats prominently affected the Europe/Middle East (EMEA) and Asia Pacific (APAC) region. Meanwhile the Americas (AMER) region was least affected by those same four threats. However, this trend flipped for the fifth sample, Trojan.Cryxos, which affected AMER the most and EMEA the least. APAC remained in the middle for all five threats.

In the end, three of the five most wide-spread malware samples affect Microsoft Office products and arrive as document-based threats. The other two are trojans. All five typically arrive via malicious email, which is why we suggest you emphasize user training to help your employees identify phishing and other malicious emails. Obviously, anti-malware services like WatchGuard's GAV, IAV, and APT Blocker can usually prevent this type of malware from reaching your inboxes. Nonetheless, you should still make sure your users know how to avoid any that might sneak through your defenses.

## New Malware on Our Top 10

We saw two new malware variants (or more specifically, [greyware](#)) make our top 10 this quarter. Both are penetration testing (pen-test) tools included with [Kali Linux](#), and sometimes other [security OS distributions](#). This rise in pen-test tool detection could indicate either good or bad news. On one hand, it may suggest that more businesses conducted penetration tests to improve their security posture during Q3, which would be a great sign. However, criminal hackers often use these freely available, open source attack tools nefariously. Without more data, it's impossible for us to know if these detections are of the good or bad variety.

In either case, we recommend businesses regularly pen-test their infrastructure to help audit and improve their security. While we don't discourage IT organizations from learning these pen-test tools themselves, realize that a skilled security professional can often find things automated tools miss. Don't hire just any company or individual to do this but look for experienced security auditors with proven history.

Let's take a closer look at the two pen-test tools that made our top 10 this quarter.

### Boxter

Boxter is a PowerShell trojan used to further download and install other potentially unwanted programs onto a victim's PC without their consent.

Since there were four variants of this attack, we combined their total hits. Cyber criminals are increasingly abusing legitimate tools like PowerShell to carry out their attacks; a technique often called [fileless malware](#) or "[living off the land](#)." We highlighted one example in detail in our Q2 2019 report, where we walked through how attackers used PowerShell (and other tools) to compromise several Managed Service Providers (MSPs).

```
PS C:\> Get-ChildItem 'MediaCenter:\Music' -rec |
>> where < -not $_.PSIsContainer -and $_.Extension -match 'wma|mp3' > |
>> Measure-Object -property length -sum -min -max -ave
>>
Count          : 1307
Average        : 5491276.09563887
Sum            : 7177097857
Maximum       : 22905267
Minimum       : 3235
Property      : Length

PS C:\> Get-WmiObject CIM_BIOSElement | select biosv*, man*, ser* | Format-List
BIOSVersion   : <TOSCPPL - 6040000, Ver 1.00PARTIBL>
Manufacturer  : TOSHIBA
SerialNumber   : M821116H

PS C:\> <[umiSearcher]@'
>> SELECT * FROM CIM_Job
>> WHERE Priority > 1
>> '().get()' | Format-Custom
>>
class ManagementObject#root\cimv2\Win32_PrintJob
```

Figure 3: PowerShell (Source: Microsoft)

## Hacktool.JQ

Mimikatz is no longer the only authentication attack tool in our top 10 list. Hacktool.JQ, also known as Windows Credentials Editor (WCE), offers many features similar to Mimikatz. Attackers and penetration testers alike use it to perform [pass-the-hash attacks](#), obtain NT/LM password hashes from memory, and even list logon sessions and modify associated credentials. This tool also supports dumping Kerberos tickets and reusing/reloading the tickets on other systems to authenticate against other systems and services.

As an aside, Kerberos is a more secure authentication option compared to Windows' legacy NTLM. For a comparison between NTLM and Kerberos, read [this](#) Microsoft post. We highly recommend you use Kerberos authentication today and try to end-of-life any servers that still use NTLM.

If you'd like to learn more about this WCE, [check out its official FAQ](#).

```
C:\test\neu>wce -w
WCE v1.3beta (Windows Credentials Editor) - (c) 2010,2011,2012 Amplia Security -
by Hernan Ochoa (hernan@ampliasecurity.com)
Use -h for help.

Secure_User\WIN-LOANLOTDQLU:CvM*901D0?#<Fg["MNoP43!Ta$cv2%
George\WIN-LOANLOTDQLU:George
Fred\WIN-LOANLOTDQLU:
WIN-LOANLOTDQLU$\WORKGROUP:
C:\test\neu>
```

Figure 4: Windows Credentials Editor (Source: darknet.org.uk)

## Quarter-over-Quarter Trends

The following table shows the QoQ volume changes for reoccurring threats on our top 10. As previously mentioned, eight of the top 10 threats returned from Q2. Mimikatz detections dropped from its number one spot in previous quarters. Meanwhile, Win32/Heri (a rule that generically catches a trojan family) detections increased the most at 363%! Finally, Win32/Heim.D, a threat containing code injection capabilities, experienced a slightly less impressive 118% increase.

Reoccurring Threat	Percentage Increase/Decrease	Q3 Hits	Q2 Hits
<b>Win32/Heri</b>	<b>+363.87%</b>	6,287,518	1,355,429
<b>Win32/Heim.D</b>	<b>+118.43%</b>	2,439,830	1,116,985
<b>Mimikatz</b>	<b>-48.15%</b>	1,130,834	2,180,937
<b>Trojan.GenericKD (SBD)</b>	<b>+51.85%</b>	743,161	489,400
<b>CVE-2017-11882</b>	<b>-47.24%</b>	516,512	978,996
<b>RTF-ObfsObjDat</b>	<b>+191.37%</b>	503,861	172,927
<b>Win32/Heur</b>	<b>-50.14%</b>	284,137	569,964
<b>Backdoor.Small.DT</b>	<b>-36.19%</b>	234,834	368,067

Figure 5: Quarter-over-Quarter Trends

## Year-over-Year Trends

In contrast, only five malware variants carried over from our top ten last year. Win32/Heri saw a shocking 5,435% increase YoY and Win32.Heim.D jumped 425%. Mimikatz, however, declined, dropping nearly 16% YoY.

Reoccurring Threat	Percentage Increase/Decrease	Q3 2019 Hits	Q3 2018 Hits
<b>Win32/Heri</b>	<b>+5,435.22%</b>	6,287,518	113,591
<b>Win32/Heim.D</b>	<b>+425.36%</b>	2,439,830	464,414
<b>Mimikatz</b>	<b>-15.88%</b>	1,130,834	1,344,351
<b>CVE-2017-11882</b>	<b>+57.93%</b>	516,512	327,044
<b>Win32/Heur</b>	<b>-34.44%</b>	284,137	433,450

Figure 6: Year-over-Year Trends

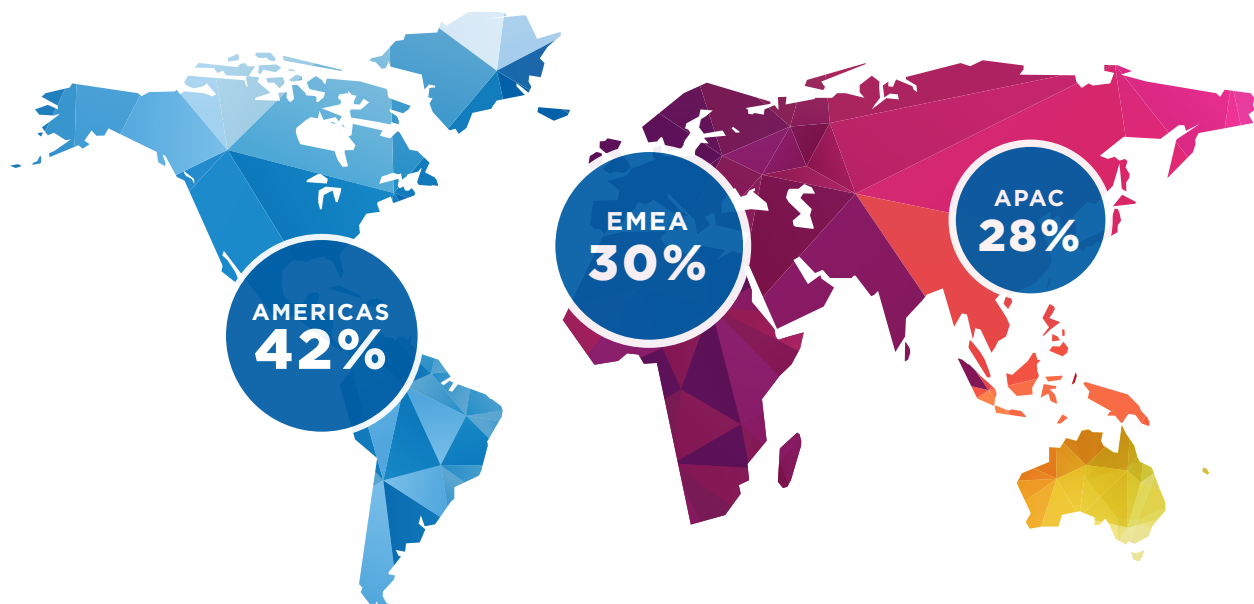
## Geographic Attack Distribution

On a geographical level, the AMER region saw the most malware volume claiming 42% of the total. EMEA came second with 30%, whereas APAC was a close third at 28%. This is quite a change from Q2, where AMER came last in malware volume and EMEA and APAC nearly tied for first.

Other interesting Q3 regional observations include:

- Four of the top 50 attacks only targeted EMEA (two Linux trojans and two Bitcoin miners)
- A “pen-test” tool called Shellter only targeted APAC

## Network Attacks by Region



## Zero Day vs Known Malware

Zero day malware refers to malware that wasn't detected by traditional signature-based solutions, such as GAV. IAV and APT Blocker offer protections against these zero day attacks. One important thing to keep in mind is that all devices support APT Blocker but not all devices support IAV.

From an overall perspective, Q3 experienced a drastic uptick in zero day malware, reaching nearly 50% of detections. This number includes threats detected by both IAV and APT Blocker, regardless if the devices support IAV or not. Previously, our zero day malware percentage stabilized around 38%. However, in Q3 it grew to just under 50%, which means that nearly half of Q3 malware bypassed traditional signature-based solutions. In today's threat landscape, it is evident we must stack security layers to better protect our networks from ever-evolving threats. Services like IAV and APT Blocker provide just that, offering more proactive machine-learning and behavioral analytics-based anti-malware layers to your security stack.

Interestingly, if we narrow the field of focus to just devices supporting IAV, our zero day percentage changes. For that subset of devices, IAV blocked 7.14% of malware and APT Blocker blocked 22.56%. GAV blocked the remaining 70% of malware attacks. This is quite a distinct contrast from the full picture, considering zero day malware accounted for nearly half of all attacks.

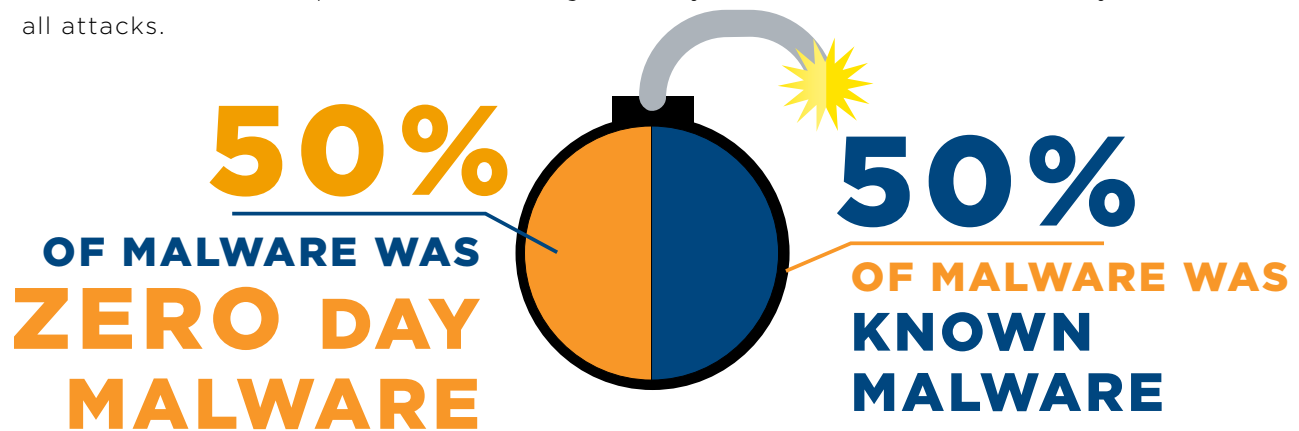


Figure 7: Zero Day vs Known Malware

# Network Attack Trends

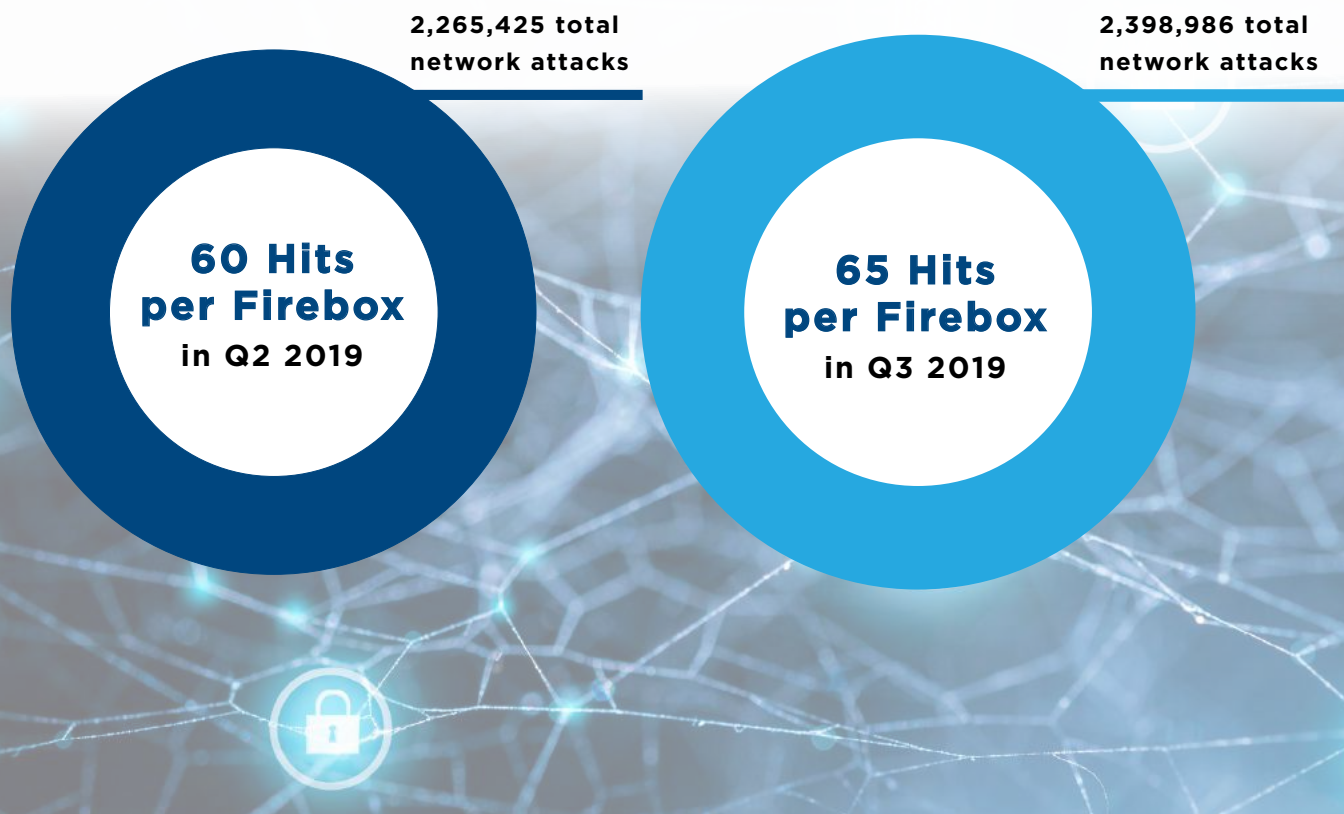
In this section, we look at the types of network attacks our Firebox customers encountered the most in Q3 2019. While we still see plenty of traditional network attacks showing up in the top 10 list, all IPS engines must constantly update to block new, inventive attacks. The Firebox appliance's IPS engine carefully reviews network traffic and compares it to known network-based attacks, allowing it to block threats based on signatures and network rules.

We tend to see many of the same reoccurring network attacks in our top 10 list every quarter, and Q3 was no different. However, this quarter we identify unique trends in certain network attacks we haven't identified previously.

Since last year, we've seen relatively consistent network attack volume. In fact, between Q2 2018 and Q1 2019 the network attack volume didn't change significantly. However, since Q2 2019 we've seen a steady rise and that's continued this quarter.

In past years, we've seen slight dips in network attack volume from Q2 to Q3 in general. In Q3 2019, however, there was a QoQ rise in network attacks. That said, the number of unique network attacks (a measure of the variety of exploits attackers launch at victims) didn't change much, only dropping by 3 to 345 unique signatures.

With over 2,398,986 total hits, each Firebox blocked 65 network attacks on average during Q3 2019 – more than an 8% increase per Firebox from Q2 2019.



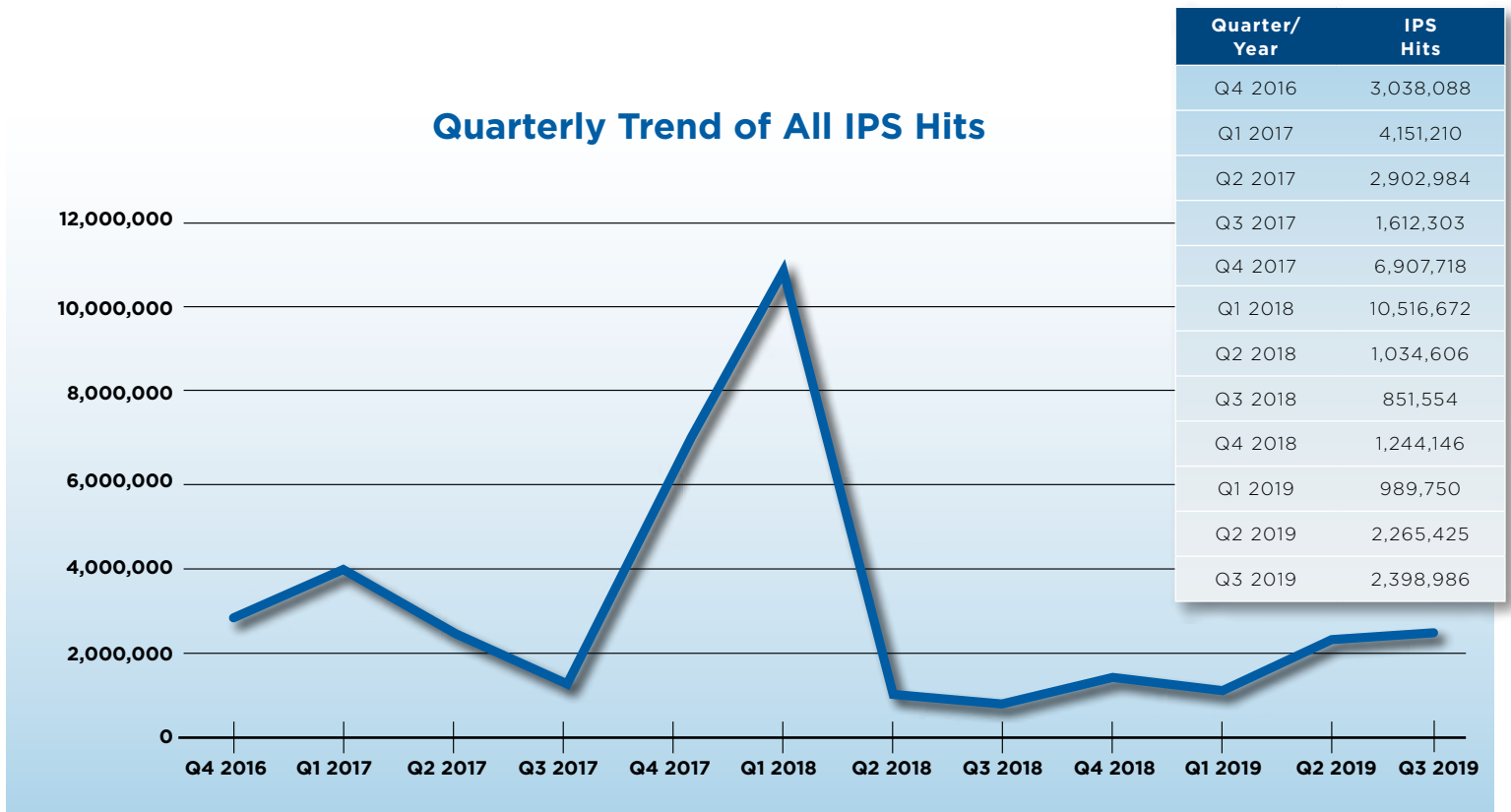


Figure 8: Quarterly Trends of All IPS Hits

### Unique IPS Signatures

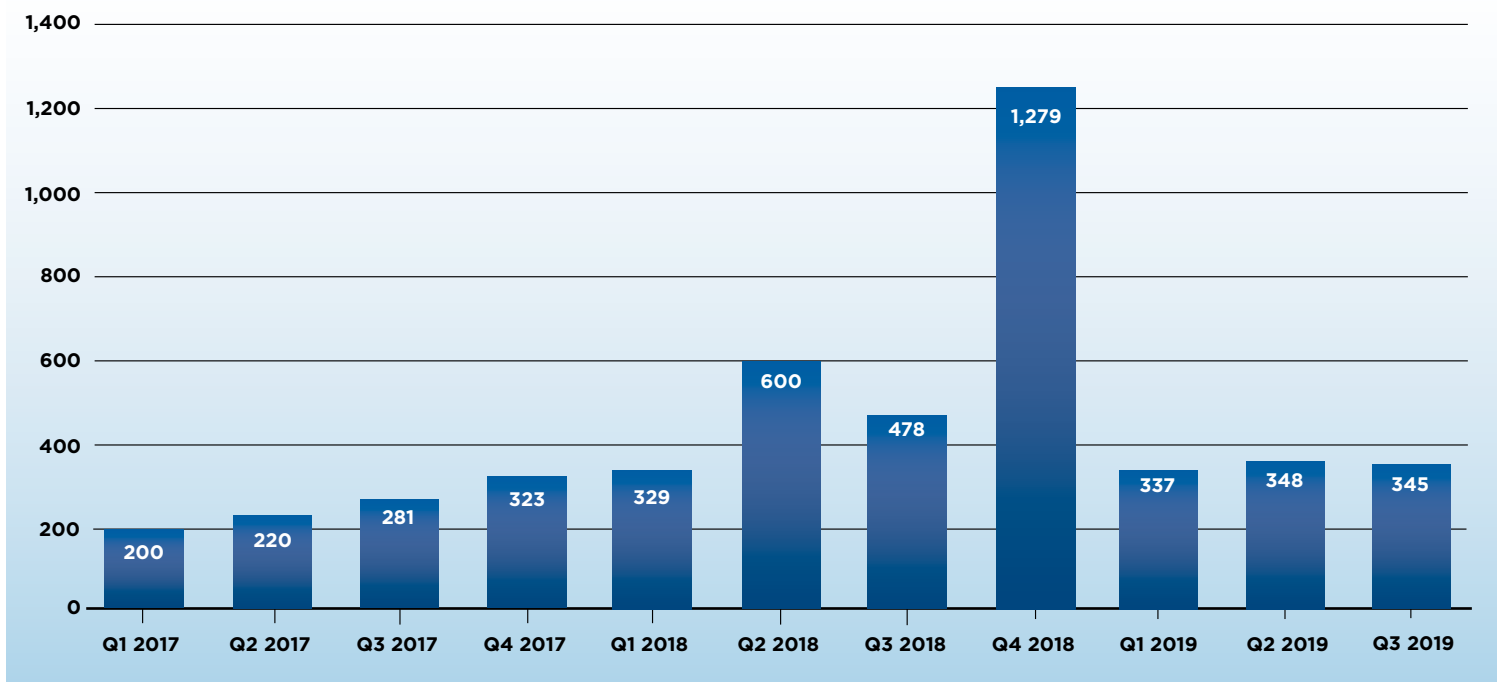


Figure 9: Unique IPS Signatures



## Top 10 Network Attacks Review

Let's take a look at the top 10 most popular network attacks in Q3. There were three new network attacks this quarter, Apache Struts 2 Remote Code Execution (which attackers used in the [Equifax](#) breach), Apache Struts Dynamic Method Invocation, and Generic JavaScript Remote Code Execution. We'll describe these network attacks in detail soon, but for now let's take a look at the rest of the top 10.

Signature	Type	Name	Affected OS	Count	CVE Number
<a href="#">1059160</a>	Web Attacks	WEB SQL injection attempt -33	Windows, Linux, FreeBSD, Solaris, Other Unix	548,443	N/A
<a href="#">1133451</a>	Access Control	WEB Cross-site Scripting -36	Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device	258,941	CVE-2011-2133
<a href="#">1133407</a>	Web Attacks	WEB Brute Force Login -1.1021	Linux, FreeBSD, Solaris, Other Unix, Network Device, Others	141,960	N/A
<a href="#">1130029</a>	Access Control	WEB GNU Bash Remote Code Execution -6 (CVE-2014-6271, Shellshock)	Linux, FreeBSD, Solaris, Other Unix, Mac OS	123,712	CVE-2014-6271
<a href="#">1133959</a>	Web Attacks	WEB Apache Struts Dynamic Method Invocation Remote Code Execution -4.2	Windows, Linux, FreeBSD, Other Unix, Mac OS	110,232	CVE-2017-9791
<a href="#">1133529</a>	Access Control	WEB Apache Struts 2 Remote Code Execution -1.2 (CVE-2017-5638)	Windows, Linux, FreeBSD, Solaris, Other Unix	107,603	CVE-2017-5638
<a href="#">1054841</a>	Web Attacks	WEB SQL injection attempt -7	Windows, Linux, FreeBSD, Solaris, Other Unix	99,370	CVE-2010-0112
<a href="#">1133223</a>	Web Attacks	FILE Microsoft Office Memory Corruption Vulnerability (CVE-2016-7231)	Windows	93,513	CVE-2016-7231
<a href="#">1054837</a>	Web Attacks	WEB Remote File Inclusion / etc/passwd	Windows, Linux, FreeBSD, Solaris, Other Unix	88,720	CVE-2014-7863
<a href="#">1055175</a>	Web Attacks	WEB-CLIENT Generic Javascript Remote Code Execution -1	Windows, Linux, Other Unix	81,799	CVE-2011-2140

Figure 10: Top 10 Network Attacks in Q3, 2019

## Top 10 Network Attack Percentage Overall

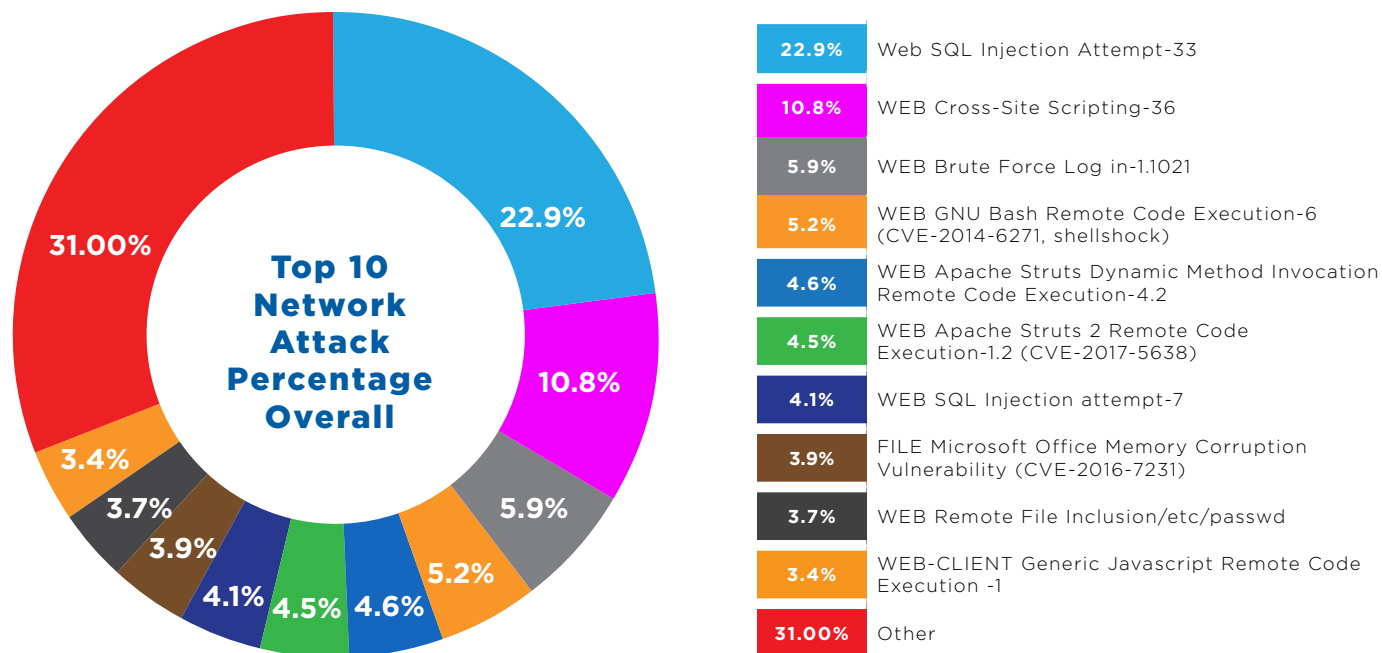


Figure 11: Percentage Makeup of Top 10 Attacks vs All

## New Network Attacks

### Apache Struts 2 Remote Code Execution

This exploit is best known as the network attack used in the Equifax breach. It affects servers running an unpatched version of Apache (a popular web server), which also have Struts (a Java web app framework) installed. By sending a specially crafted HTTP request with a malicious Content-Type header, an attacker can execute arbitrary code on vulnerable Apache Struts servers. Once the server receives the malicious request, it responds with an error. Object Graph Navigation Language (OGNL), part of Struts, redirects the error in the request to copy a command written into the request. By producing the error, the request tags the error with a command that is then executed with the error.

While this becomes a long and complex command, anyone able to install python or make a custom HTTP request could exploit this and obtain shell access to a vulnerable system. [As seen in the example we found here](#), you only need a few lines of code to make it work.

```
requests.get("https://target", headers={"Connection": "close", "Accept": "*/*", "User-Agent": "Mozilla/5.0", "Content-Type": "%{(#_='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmd='dir').(#iswin=@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=@org.apache.struts2.ServletActionContext@getResponse().getOutputStream()).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}"})
```

Everything after the “Content-Type” header declaration is the actual exploit. This particular example just executes the ‘dir’ command to list the folders on the system, but you can run any command you like including a reverse shell by replacing ‘dir’ with something more complex. With a 10 of 10 for severity in the [National Vulnerability Database](#) and the national attention the Equifax breach got from this vulnerability, we hope web admins have already upgraded their servers. If you’ve patched, this attack won’t work (and if you have a Firebox with IPS, it will block the attempt). However, vulnerable servers won’t last long while connected to the Internet. Even if you have internal servers not exposed to the Internet, we recommend you patch this flaw since hackers might use this vulnerability for lateral movement, to further exploit a compromised network. To resolve this vulnerability, [upgrade to Struts 2.3.31 or 2.5.10](#) or higher. But Struts 2.3.31 and Struts 2.3.32 have another vulnerability we talk about next.

### **WEB Apache Struts Dynamic Method Invocation Remote Code Execution**

In Q3, we saw another Apache Struts vulnerability make our top 10. While examining the logs, we didn’t find any similarities in the affected devices or the attacker of the previous new network attack. This attack, like the previous one, exploits the Struts module by sending OGNL expressions to run a command, but unlike the previous exploit, it uses the Struts 1 plugin for Struts 2. This vulnerability affects Struts 2.3.1 to 2.3.32, but the server must also use raw messages instead of keys when accepting content types. This just means the server should only accept preapproved input.

We also saw a third Apache vulnerability, ‘WEB Apache Struts Wildcard Matching OGNL Code Execution’ or [CVE-2013-2134](#) in our most-widespread network attacks, as well as further down in the top 50 network attacks by volume. If you’d like to know more about this vulnerability, read [Apache’s write-up on it](#). Due to traffic flow patterns in the data we reviewed on this network attack, we suspect a compromised computer, possibly part of a botnet, caused this issue. We don’t know why we saw so many attacks on Apache Struts but hope the press from Equifax has caused web admins to upgrade already. If you have not upgraded and you run Apache Struts before 2.3.32 or 2.5.10, be sure to update your web server immediately. It takes little knowledge of networking to run these exploits against a vulnerable server.

### **WEB-CLIENT Generic JavaScript Remote Code Execution**

This is more of a Flash Player vulnerability than a JavaScript one. A compromised or malicious web server may run a malicious flash file on your computer. You can learn a bit more about it from its Common Vulnerability and Exposures reference number ([CVE-2011-2140](#)). A memory corruption vulnerability allows an attacker to obtain code execution in Flash Player. If an attacker can trick one of your users into visiting a web page with a malicious flash file, simply visiting that page allows the attacker to run arbitrary code. Flash Player has suffered from many serious vulnerabilities over the years, to the point where most major web browsers have already disabled it. The CVE database tracking these flaws lists 894 critical vulnerabilities in Flash Player, all with severity scores of 9 or higher out of 10. In comparison, VMware only lists 48 critical vulnerabilities, despite being a much more complex application. HTML5, CSS3 and JavaScript (without Flash Player) have replaced most Flash implementations on the web, so outside of very specific use cases, you should consider removing Adobe Flash from your computer completely.

## Geographic Attack Distribution

While EMEA saw fewer weighted regional hits per box in Q3 2019, both AMER and APAC saw significantly more. AMER received 60% of the detections, meaning networks in the AMER region received more attacks than EMEA and APAC combined. EMEA saw 23% and APAC saw 17%.

Though comparing network attacks by volume helps us identify what services and applications cyber criminals target the most, it doesn't necessarily mean those high-volume attacks really affect the majority of victims. That's why we also track which attacks "touch" the most Fireboxes, regardless of volume. We cover these widespread attacks below. While the AMER region accounted for the majority of widespread network attacks, EMEA was actually the top recipient of the number one widespread attack, Web Cross-site Scripting -36. Outside that top hit though, AMER was the top recipient for every other widespread attack. APAC received a trivial share of widespread network attacks, always trailing by a large margin.

Name	CVE Number	Signature ID	EMEA %	AMER %	APAC %
<b>WEB Cross-site Scripting -36</b>	<b>CVE-2011-2133</b>	<a href="#">1133451</a>	36.1%	52.1%	11.8%
<b>WEB SQL injection attempt -33</b>	<b>N/A</b>	<a href="#">1059160</a>	47.2%	39.9%	12.9%
<b>WEB Cross-site Scripting -9</b>	<b>Multiple</b>	<a href="#">1055396</a>	45.8%	43.2%	11.0%
<b>WEB Directory Traversal -3</b>	<b>Multiple</b>	<a href="#">1052256</a>	42.2%	51.6%	6.3%
<b>WEB Apache Struts Wildcard Matching OGNL Code Execution -1</b>	<b>CVE-2013-2134</b>	<a href="#">1057877</a>	55.7%	39.0%	5.3%

Figure 12: Top 5 Most-Widespread Network Attacks

Name	Top 3 Countries by %		
<b>WEB Cross-site Scripting -36</b>	Venezuela - 7.3%	Brazil - 7.0%	Great Britain - 6.2%
<b>WEB SQL injection attempt -33</b>	Brazil - 6.7%	Great Britain - 6.4%	Switzerland - 6.1%
<b>WEB Cross-site Scripting -9</b>	Turkey - 12.6%	Brazil - 7.2%	Poland - 7.1%
<b>WEB Directory Traversal -3</b>	Brazil - 12.7%	Dominican Republic - 8.5%	Venezuela - 8.1%
<b>WEB Apache Struts Wildcard Matching OGNL Code Execution -1</b>	Brazil - 8.8%	Switzerland - 6.9%	Turkey - 6.7%

Figure 13: Top 5 Most-Widespread Network Attacks by Country

As mentioned in the malware section, the most-widespread malware list contained another Apache Struts flaw, WEB Apache Struts Wildcard Matching OGNL Code Execution. Despite the similar application target, we didn't find any correlation between victims, but note the larger trend - cyber criminals actively targeted Apache Struts in Q3.

Now that we have a few quarter's worth of data on widespread hits, we wanted to see if any new trends appeared across multiple quarters. We analyzed this widespread network attack data from Q4 2018 to Q2 2019. Unsurprisingly, Brazil, England, and Turkey showed up in most of the top five most widespread. Spain was the only other country to show in the widespread data by country over the time period.

Name	CVE Number	Signature ID	EMEA %	AMER %	APAC %
<b>WEB Cross-site Scripting -36</b>	<b>CVE-2011-2133</b>	<a href="#">1133451</a>	54.9%	35.4%	9.7%
<b>WEB SQL injection attempt -33</b>	N/A	<a href="#">1059160</a>	43.8%	44.5%	11.7%
<b>WEB Cross-site Scripting -9</b>	Multiple	<a href="#">1055396</a>	45.5%	44.0%	10.5%
<b>WEB Ruby on Rails Where Hash SQL Injection</b>	<b>CVE-2012-2695</b>	<a href="#">1056282</a>	53.3%	40.4%	6.4%
<b>WEB Apache Struts Wildcard Matching OGNL Code Execution -3</b>	<b>CVE-2013-2134</b>	<a href="#">1057983</a>	47.7%	48.3%	4.0%

Figure 14: Top 5 Most-Widespread Network Attacks by Region

When looking at this extended slice, we see the same cross-site scripting and SQL injection vulnerabilities from this quarter's widespread and top 10 lists also showing up historically as well. This further illustrates the continuing danger of these sorts of web application attacks. Make sure your web developers concentrate on security coding practices.

For the most part, EMEA accounted for the most widespread hits over time while APAC received very little (averaging less than 10% for each vulnerability). We have seen some users turn off their IPS to resolve access issues. We don't recommend this in any situation since it greatly lessens your network security. If you are getting many IPS hits, you should find the root cause of the error to ensure it's not malicious. Unusual IPS hits could be caused by networking issues, bad software, real attacks, or in some cases, even a false positive. Whatever you find, we highly recommend you not disable IPS completely; rather if you find a false positive, use our signature exception feature to simply ignore that one signature.

While doing this analysis, we found yet another interesting Apache Struts trend. The Apache Struts Wildcard Matching OGNL vulnerability also showed up in the top five for this time period even though it never registered in the QoQ views. Before this quarter we only saw 'WEB Apache Struts XSLTResult File Inclusion ([CVE-2016-3082](#))' in Q2 2019's widespread hits. Again, this trend data further supports that cyber criminals are actively targeting Apache Struts. From being almost nonexistent in our data just two quarters ago to multiple hits seen throughout this quarter and in the last year, we expect to see many more Apache Struts network attacks going forward. Again, if you run Apache Struts, ensure you have the latest patches since botnets and criminals now target these servers.

# DNS Analysis

In the Q1 2019 edition of this security report, we began presenting data from WatchGuard's DNSWatch service. DNSWatch works by intercepting Domain Name System (DNS) requests from protected systems and sending dangerous connections to a black hole instead of the original malicious destination. Because DNSWatch works on the DNS level, it detects and blocks threats independent of the application protocol for the connection. With our threat intelligence from DNSWatch, we're able to identify malicious domains used in all types of attacks ranging from botnet command and control to phishing attempts.

Last quarter, we expanded this section to include a look into specific threat categories, highlighting the top domains involving malware, compromised websites and phishing links. We continue that analysis this quarter with insights into those same malicious categories.

## Top Malware Domains

There were six new malware domains in Q3 that were not in the top 10 during Q2. Before we dive into them though, we should first point out an interesting returnee from the previous quarter. Last quarter, we wrote about the file share site my[.]mixtape[.]moe and how cyber criminals were using this site to host malware. Even though the website shuttered its doors because of the criminal activity it was drawn into by its users, we still saw a significant number of malware droppers attempting to grab payloads from it. This is a great example of the longevity of malware. Even once authors stop maintaining their payloads, they still have a lasting chance at causing damage to networks.

The final six domains in the top 10 malware domains list are all new to the report. Even though they were new, some of them have been around for quite a while. Both track[.]amishbrand[.]com and h1[.]ripway[.]com were added to our threat feeds in early/mid 2018 for hosting the **Cthonic** and **DiNGoes** malware families respectively. d3l4qa0kme17is[.]cloudfront[.]net was originally added two years ago after we found cyber criminals using it to host malware linked from PowerPoint files. The fact that we see these domains continuing to show up years after their creation is further testament to the longevity of malicious files.

## WARNING

All of the domains highlighted in this section have at one point hosted or continue to host malware. Do not visit any domain in this section or you risk infecting your system.

MALWARE
favourgrace[.]sytes[.]net
dc44qjwal3p07[.]cloudfront[.]net
d3i1asoswufp5k[.]cloudfront[.]net
my[.]mixtape[.]moe
orzdwjtvmein[.]in *
Track[.]amishbrand[.]com *
h1[.]ripway[.]com *
d3l4qa0kme17is[.]cloudfront[.]net *
agenciatoruja[.]com *
server2.aserdefa[.]ru *

\* New in Q3 2019

## Top Compromised Websites

There was only one new addition to the list of top compromised websites this quarter when compared to Q2 2019, `www12[.]Ozz0[.]com`. The root domain appears to be an Arabic photo-sharing platform where users can upload images and share links to others.

Unfortunately, the site's file type validation is minimal, checking only that the file extension is an accepted image type (e.g., .jpeg). Over the past six years, this domain has shown up time and time again hosting malicious payloads that attackers masked by changing the file extension. Many of the top malware threats we've highlighted over the years in this report have been "dropper" files, whose sole job is to scope out a system and go grab an appropriate malware payload. Malware droppers don't care what extension the malicious payload uses, which makes platforms like `Ozz0[.]com` perfect for distribution.

Changing the extension of a malicious executable has other benefits for attackers. Some anti-malware systems choose whether or not to scan a file based off of the extension instead of using a file type detection engine. If you're a WatchGuard customer, you're in luck. All Firebox proxy services support file type detection beyond just file extensions when determining whether to run a download through the three anti-malware engines.

COMPROMISED
<code>differentia[.]ru</code>
<code>disorderstatus[.]ru</code>
<code>update[.]intelliadmin[.]com</code>
<code>O[.]nextyourcontent[.]com</code>
<code>www[.]sharebutton[.]co</code>
<code>pm2bitcoin[.]com</code>
<code>query[.]network</code>
<code>rekoovers[.]ru</code>
<code>install[.]pdf-maker[.]com</code>
<code>www12[.]Ozz0[.]com</code> *

\* New in Q3 2019

## Top Phishing Domains

There were three new additions to the top phishing domains list this quarter when compared to Q2 2019. We added the first newcomer, help[.]fuzeqna[.]com, at the start of the quarter after finding a phishing campaign targeting a regional credit union hosted on it.

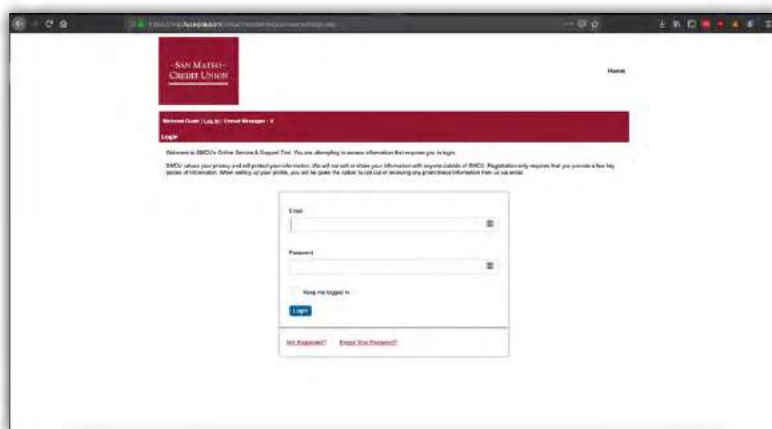


Figure 15: San Mateo Credit Union Website

The root domain does not appear to be optional and help[.]fuzeqna[.]com issues a 403 Access Denied response when a valid URL path is included. These signs point to the attackers using the domain as a purpose-built phishing platform vs it simply being a compromised website.

The next domain, nucor-my[.]sharepoint[.]com is another example of attackers abusing Cloud file-hosting to piggyback on the reputation of a trusted domain (sharepoint.com). In this instance, we added the domain to our blacklist in June of this year after discovering it hosting a fake file share that redirected to a compromised website.

We, and others in the industry, have always given advice that users should hover over email links to identify the actual destination domain before clicking. With modern phishing attacks though, you can no longer trust that the legitimacy of the domain is indicative of the content of that page. It's too easy for attackers to abuse Cloud hosting to host believable phishing pages.

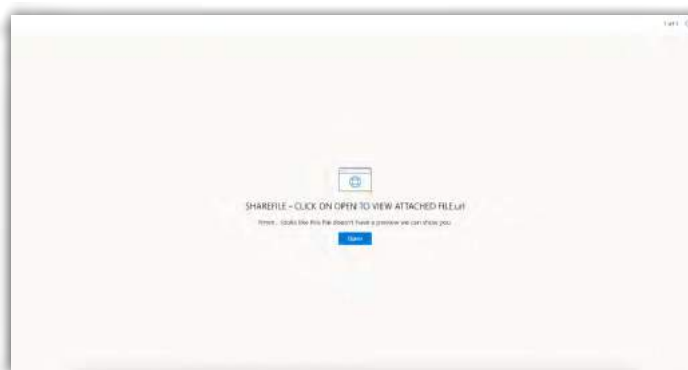


Figure 16: SharePoint Piggyback

Our DNSWatch trends show that cyber criminals continue evolving the methods they use to entice your users to malicious sites. Be sure to use a DNS-based filtering solution like DNSWatch to protect them when they do eventually click the wrong link.

PHISHING
paste[.]jee
usd383org-my[.]sharepoint[.]com
a[.]top4top[.]net
email[.]veromailer[.]com
help[.]fuzeqna[.]com *
uk[.]at[.]atwola[.]com
karrasconsulting[.]net
nucor-my[.]sharepoint[.]com *
link[.]medicanimal[.]com *
up[.]top4top[.]net

\* New in Q3 2019



# Firebox Feed: Defense Learnings

This quarter, we saw even more tools for pen-testers and cyber criminals appearing in our top malware feeds. This shows that attackers still prefer attacks that are easy to write and execute. Low-skill attacks and repeated known attacks from previous quarters also continued to plague customer networks because they run quickly and effectively through many defenses. Here are some tips for keeping your networks safe from the attacks we saw in Q3.

**1**

## Keep Your Web Apps Updated

Apache Struts vulnerabilities hit hard in Q3. After receiving almost no detections in previous quarters, this quarter it showed up in two of the top 10 by volume spots and one in the most-widespread list. One of the vulnerabilities that we detected this quarter was the one that attackers exploited in the Equifax data breach. If you maintain your own web app infrastructure, make sure you are keeping your services up to date with the latest security patches.

**2**

## Use Tools That Catch Code Injectors

The most malware detections from the Firebox Feed this quarter came from two code injection malware payloads, Win32/Heri and Win32/Heim.D. While it is easy to detect these specific threats, other code injector malware variants can be significantly stealthier. Make sure you are using tools that watch the behavior of good processes and detect malicious deviations.

**3**

## It Is Long Past Time to Phase Out Flash

Most major web browsers have already removed the plugin architecture required for Adobe Flash to function, but some users still run old versions that leave them vulnerable to attack. If you currently use Adobe Flash, it is long past time to migrate to a new tool that doesn't rely on an archaic and hyper-vulnerable framework.



# Top Security Incidents

# Top Security Incidents

## Kazakhstan Forced HTTPS Decryption

The top security incident this quarter didn't cause the most monetary damages or affect the most individuals. It didn't generate the most news or even last longer than half a day in the niche information technology headlines. We aren't covering this incident because of the tangible damages it caused, but because of the impact it will have as more nations converge on the same ultimatum.

On July 17, 2019, the government of Kazakhstan flipped the switch on a nationwide initiative to intercept and decrypt all HTTPS traffic inside its borders. At the same time, the government instructed Internet Service Providers (ISPs) to force their users to install a government-issued certificate on all devices. Users attempting to access the Internet were redirected to pages with instructions for installing the certificate, like the one to the right.

This decryption program lasted three weeks, until August 6th, when Kazakhstan's State Security Committee released a statement claiming the certificate rollout was only a test, one which had been completed. The President of Kazakhstan, Kassym-Jomart Tokayev followed up the statement with a tweet claiming he personally ordered the test to prove that protective measures "would not inconvenience Kazakh Internet users."

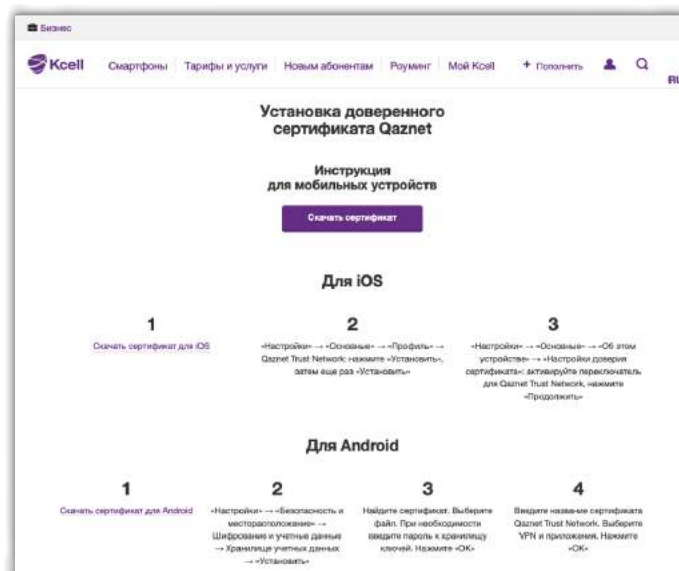


Figure 17: Kazakhstan Certificate

Whether this incident was a test or a full program that received too much backlash and had to be aborted doesn't matter. Either scenario highlights a massive privacy concern that could end up affecting Internet users across the world as nations continue to push towards backdoored encryption.

In the rest of this section, we'll cover how the Kazakh government managed to man-in-the-middle (MitM) HTTPS encryption within their borders, similar surveillance programs enacted in other nations, and security and privacy parallels with corporate HTTPS decryption.

## HTTPS Encryption and Decryption

When your web browser connects to a site protected by HTTPS encryption, a lot goes on behind the scenes before any content ever loads. First, your browser must authenticate the identity of the web server hosting the site and then agree on encryption protocols for the connection. Your browser uses a certificate, provided by the web server, for this authentication process.

For a detailed description of the certificate verification process, check out the [What Are Digital Certificates?](#) episode of [The 443 – Security Simplified Podcast](#). For a short description, Certificate Authorities (CAs) are special organizations in charge of verifying the identity and ownership of web domain names and servers before issuing a cryptographically signed certificate for that domain.

Your operating system, and even individual web-browsing software, maintains a list of trusted CAs. If your browser receives a certificate for a website signed by a CA in its trusted list, it builds an encrypted connection to the server and displays a lock in the address bar. If the certificate it receives is signed by a CA that isn't in its trusted list, the browser displays a prominent warning that the connection is not secure because the certificate could not be verified.

Operating system and browser manufacturers like Microsoft, Mozilla, Google and Apple

take care of maintaining these trusted CA certificate lists, adding new CAs that meet strict requirements and removing CAs that violate trust.

Because, in general, attackers (and governments) don't have access to a trusted CA certificate that already exists in your operating system or browser, they cannot man-in-the-middle your encrypted connections without triggering an untrusted certificate warning. This means the only way for them to covertly spy on your encrypted traffic is to have their own CA certificate added to that trusted list.

The government of Kazakhstan [originally tried back in December 2015](#) to have Mozilla add their government CA certificate to Firefox's trusted list. This request was swiftly shot down because the Kazakh government understandably failed to meet various Certificate Authority requirements including ensuring ownership of domains prior to issuing server certificates. This left the only alternative of having users install the certificate themselves.

At around the same time as the Mozilla request, [the government of Kazakhstan issued a declaration](#) requiring users to install the government-issued certificate no later than January 1st 2016. This attempt was eventually halted after the government was sued by multiple organizations over security concerns. Jump three and a half years later to this last July, and Kazakhstan restarted their

program, this time with more coordination and cooperation with local ISPs.

In late August, Google, Mozilla and Apple stepped in by manually blocking the Kazakhstan CA certificate in their web browsers, stating “It is not appropriate for this mechanism to be used to intercept traffic on the public Internet.” While this solved the issue with the particular Kazakh-issued certificate, it opened up another area of concern with private companies overruling a sovereign nation’s security programs.

## Other National Programs

Kazakhstan isn’t the first nation to enact a mass surveillance effort on its users’ Internet traffic. The Chinese government has long maintained the “Great Firewall of China” as a means to restrict the online content that its users have access to. This program works a bit differently than the one implemented in Kazakhstan. While the Chinese program likely inspects unencrypted traffic, as of yet it has not deployed certificates to enable inspection of encrypted HTTPS content. With that said, they still have the means to prevent their users from specific HTTPS websites.

Web browsers and web servers in general pass enough information during the encryption setup phase for someone watching the connection to identify the destination website. The certificate Subject Name field for example, usually contains the domain

name of the destination website while the **Server Name Indication** header during the encryption setup process usually contains the server domain name as well. This means that the Chinese Internet firewall can identify users going to unwanted domains and send a connection level “reset” command to prevent the connection from succeeding.

The United States isn’t exactly above mass Internet surveillance either, with the existence of the **PRISM program** leaked by Edward Snowden back in 2013. While PRISM also cannot decrypt HTTPS connections, it does enable the government to go directly to web application companies and request data from them.

In parallel to all of this, many national and international organizations are pushing towards backdoored encryption in the name of aiding law enforcement in catching criminals. The United States Attorney General has issued multiple statements demanding weekend encryption and Interpol is expected to release a statement against end-to-end encryption by early next year.

## What About the Office?

Man-in-the-middle attacks against HTTPS encryption do still have a place, specifically in the workplace. Attackers are increasingly using encryption to hide their malware and exploits from network-based detection tools. This means organizations must use HTTPS decryption in order to catch these threats before they reach vulnerable systems. In order to accomplish this, organizations must set up their own Certificate Authority and sign a “resigning” certificate for their network security appliance to use for inspecting HTTPS connections.

Decrypting HTTPS connections within your own company doesn't come without risk though. US CERT even went so far as to release an alert for the topic [\(TA17-075A\)](#) warning against insecure implementations. The alert's major concern involved HTTPS inspection that doesn't pass certificate warnings down to the client in the event of a broken chain. Specifically, there are some implementations that continue to re-encrypt connections without any warning when they encounter a website signed by a CA that they themselves don't trust. WatchGuard customers are safe from this risk as we maintain our own trusted CA list.



# Important Takeaways

The world seems to be moving towards a future where government agencies have the ability to decrypt and inspect what should be protected connections across the web. While this may enable them to catch more criminals that hide behind encryption, it comes with the tradeoff of putting everyday citizens at risk. No backdoor in encryption technology will remain out of the hands of cyber criminals for long. And government-sponsored HTTPS decryption will always run the risk of being abused for political gain. With that said, there does seem to be sufficient pushback from both citizens and private companies alike to keep the floodgates closed for now.

Meanwhile, here are three tips to protect the privacy of your encrypted web traffic.

**1**

## Don't Install Certificates from Untrusted Sources

Government agencies aren't the only people who might try to convince you into installing a certificate on your computer or mobile device. Threat actors commonly use phishing and other social engineering tactics to trick victims into installing malware and certificates and then use this access to steal sensitive information and inject ads or additional malware into decrypted HTTPS connections.

**2**

## Deploy HTTPS Inspection Securely

HTTPS inspection is still a very important tool for companies that control their own networks. When deploying HTTPS inspection though, make sure your solution validates certificate trust chains and passes down errors to the end user to keep them aware of any potential security compromise for the website they are visiting.

**3**

## Advocate for Encryption

Encryption protects everything from your bank transactions to your personal communications. Yes, criminals can use encryption to mask their activities as well but the risks of weakening encryption in the name of law enforcement are simply too high. If it is an important topic to you, be sure to reach out to your political representatives to inform their votes.



# Conclusion & Defense Highlights



# Conclusion & Defense Highlights

Now that our flashlights have illuminated the dark corners of last quarter's threat data, you have a much better idea of what attackers have been up to and how you might build a case to protect your organization. Let's finish with some executive-level tactics that can protect you during Q4 and beyond.

**Considering these trends, here's our security advice to survive next quarter:**



## **Patching Is Far Too Critical to Shirk**

You've heard it before and you will certainly hear it again, but you must patch any publicly exposed network services as soon as you can. This quarter we learned that threat actors are actively targeting the Apache Struts framework; reusing the same vulnerability responsible from the huge Equifax breach. By now, this vulnerability is very old. Most administrators likely patched it long ago. However, regardless of our best efforts, sometimes we still fall behind with patches, which is why attackers still target old vulnerabilities years after they're fixed. If you haven't patched any externally facing Apache Struts servers, do so immediately. Furthermore, by now you should have patched internal servers as well, even if Internet users technically can't reach them. Often, when attackers compromise networks using other tactics, they can then exploit unpatched internal flaws to assist in their lateral movement within your network. In short, make sure all your Apache Struts instance are up to date, and – as always – update other critical software as well.



## **Drop Flash Player**

Five to ten years ago, Flash Player was pretty much a necessity to everyone's web browsing experience. Back then, a lot of dynamic content and media simply wouldn't work without it. Things have changed. Few sites require Flash nowadays, and browser vendors are specifically and actively removing it from their products. Meanwhile, cyber criminals still target it. A Flash exploit prominently rose on our top 10 malware list during Q3. It makes perfect sense considering the plugin has suffered many vulnerabilities over the years (894 critically rated ones alone). At this point, we have no patience with patching Flash. Rather, we recommend you completely remove it. If you do absolutely have to keep it around then you should aggressively patch it on the second Tuesday of every month, when Adobe releases their monthly security updates.



## **Beware Baffling Certificates**

HTTPS, the standard we rely on to secure web connections, is dependent on a chain-of-trust maintained by certificate authorities (CAs) using digital certificates. When it works, it works well. However, if threat actors, spies, or governments can sneak or force special CA certificates onto your computer, they can completely hijack this chain-of-trust and gain access to your private communications. Attackers have attempted to break this trust chain for a long time, but more recently governments like Kazakhstan have gotten into the action – invading the privacy of all their citizens.

Meanwhile, we have legitimate reasons to sniff our own HTTPS traffic, too. As attackers hide more of their threats in secure web communication, our security controls need to scan this traffic to block those threats. Whether for nefarious government or attack purposes, or for added security, someone can only eavesdrop on your HTTPS traffic if they have installed a special CA certificate onto your computer. That's why you should pay particularly close attention whenever anyone is trying to add a certificate to your browser and computer's certificate store. In some cases, it might be a corporate certificate that you do need to accept to get some additional protection, but for the most part you should avoid installing any external CA certificates unless you know exactly what they are for.



## Proactive Anti-Malware Is Now a Prerequisite

In past reports, we've repeatedly described the difference between reactive, signature-based malware detection and the more advanced, proactive malware detection technologies, which use things like behavioral analysis, machine learning, and artificial intelligence to detect and block brand new malware without needing a human security analyst to examine it first. Our zero day malware statistic has always provided an important proof point on why you need advanced malware detection technology.

However, last quarter demonstrated that fact even more. With almost half of malware evading signature-based technologies, a business will not survive infection-free online for long without advanced malware protection. We highly recommend you implement such anti-malware technologies, if you haven't already. If you're a WatchGuard Firebox user, our Total Security Suite is your ticket to better protection. It includes IntelligentAV, APT Blocker, and Threat Detection and Response (TDR), which all block malware that signature-based solutions miss.



## Keep Ahead of Authentication Attacks with MFA

For the first quarter in over a year, Mimikatz - a popular credential-stealing tool - dropped in relevance during Q3, falling from its historical number one position to number three. That said, it still represents a high volume of malware. More importantly, we saw a new credential-stealing tool, Windows Credential Editor (WCE), appear on the top list as well. When you combine this new attack tool with the still relevant volume of Mimikatz, you clearly see that attackers still consider authentication one of the weak links in our security chain. Now that multi-factor authentication (MFA) offerings have become easier and inexpensive (with Cloud and mobile device options), we think every business should widely deploy it. At the very least, you must use MFA to protect your administrative and privileged accounts. However, our team believes every employee should start the day using MFA to log in to their computer. Keep in mind, solutions like AuthPoint provide access portals that make it much easier to use MFA every day, as one authentication then gets you into all your apps for the entire day.

Now that we've found and gathered all the threat evidence using our analytic flashlight (and other cyber [alternate light sources](#)), we have a good understanding of how hackers performed their cyber crimes during Q3. With that evidence, we can build an iron-clad case against their upcoming attacks and ensure their future crimes fail. We hope you found the information contained in this report useful and join us next time to learn what happened during the last quarter of 2019. As always, leave your comments or feedback about our report at [SecurityReport@watchguard.com](mailto:SecurityReport@watchguard.com). Keep your flashlights ready!



**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 19 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](http://www.secplicity.org).



**Marc Laliberte**  
*Sr. 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**  
*Information Security Analyst*

Trevor Collins is a Information. Security Analyst at WatchGuard Technologies, specializing in network and wireless security. Trevor earned his security know-how 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 midmarket businesses and distributed enterprises. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit [WatchGuard.com](http://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](http://www.secplicity.org).