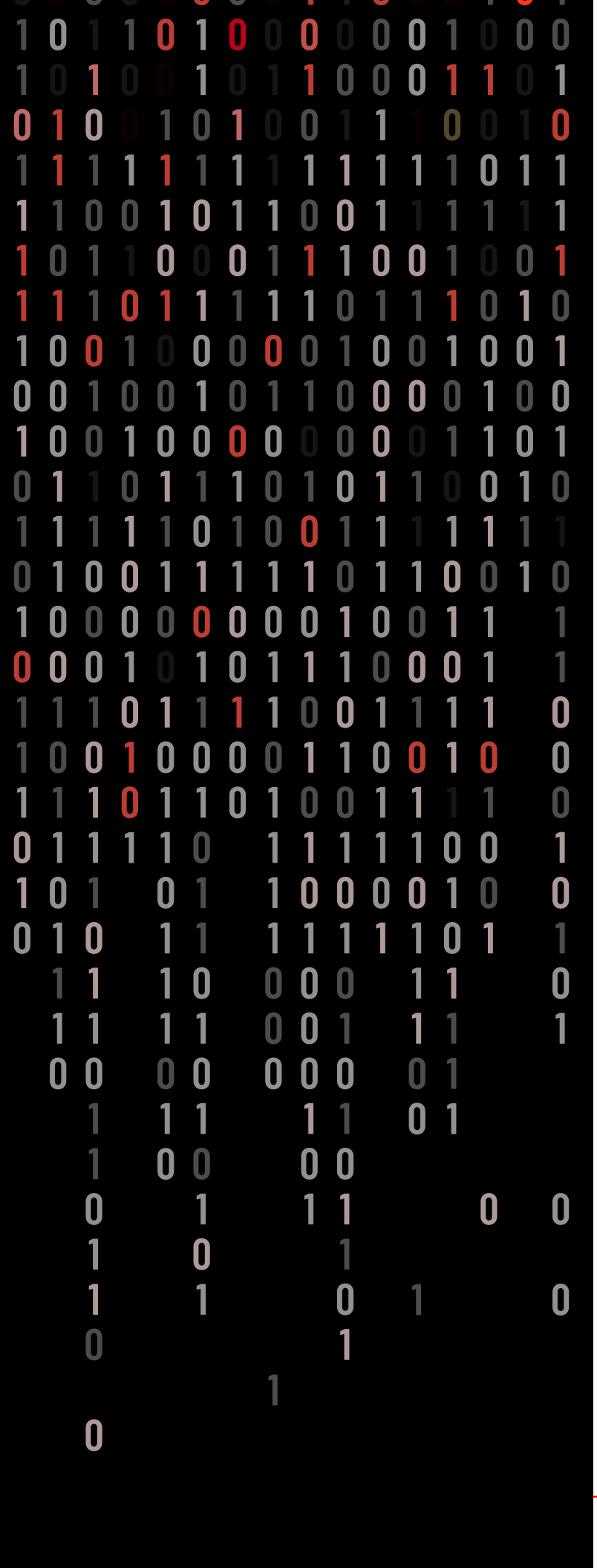
INTERNET SECURITY REPORT

Q4 2023

WatchGuard



CONTENTS

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

INTRODUCTION

"The sea is dangerous and its storms terrible, but these obstacles have never been sufficient reason to remain ashore... Unlike the mediocre, intrepid spirits seek victory over those things that seem impossible... It is with an iron will that they embark on the most daring of all endeavors... to meet the shadowy future without fear and conquer the unknown."

~Ferdinand Magellen, great explorer and cartographer

Exploration of the unknown, especially when mapping your findings to benefit those who come after, is among the most courageous missions one can undertake. When embarking into mysterious new realms, you never know what new threats and dangers you might confront. Setting out into that enigmatic territory to both find and map out those dangers so others can avoid them is a boon to society, which is why famous explorers and cartographers like Ferdinand Magellan, Christopher Columbus, Francis Drake, and James Cook have always fascinated and impressed me (despite some of their misdeeds as well).

While not nearly as impressive as exploring uncharted land, our quarterly Internet Security Report (ISR) intends to act as your map to the ever-changing cyber threat landscape. Our security products act as constant explorers, fearlessly seeking victory over the shadowy landscape of the Internet by hunting for threats. When we find them, we map out and share that threat intelligence for all our other explorers to see, providing a map that keeps everyone safe. In this report, we package up and share our analysis and "maps" from our brave explorers' online travels during the previous quarter, acting as cyberattack cartographers sharing a first glimpse of our completed map.

As the landscape changes, we continue to update our map, and provide analysis and forecast of what we expect might alter in the future, not only to give you a guide to what was already discovered, but a general expectation of what new dangers you might prepare for. We hope both the short- and long-term patterns we chart in our online travels will help guide you with a clear path through any cyber obstacles.

Fancy metaphors aside, every quarter we aggregate cyber threat telemetry from tens of thousands of WatchGuard network appliances and millions of endpoint products whose owners have opted to share this data with us. These valuable records provide insight into the top malware, network attacks, malicious websites, computer attack vectors, and threat actor tactics that were exploited against our customers on the Internet. The good news is our security products defended against these assaults, and what's more, the additional telemetry allows us to create a map of the most common threats folks face online.

We analyze all this data to identify various threat patterns, such as the most common or widespread malware, or the most prominent endpoint attack vectors, and much more! We do this to provide you a map of what cybercriminals have been trying to do against unsuspecting victims recently and to try to predict how those miscreants will evolve their attacks in the future. Most importantly, once we identify these threats and patterns, we provide a "map" of the best defense strategies to help you avoid them in your future Internet travels. Here are just a few examples of what our ISR cyber threat map shares with you this quarter:

Here are just a few examples of what our ISR cyber threat map shares with you this quarter:

08 **Network malware and attack trends**

Fireboxes offer up to three different network-based anti-malware services and an Intrusion Prevention Service (IPS) that block hundreds of thousands of network and malware attacks every day. This section highlights the most prominent and widespread malware and network exploits our products saw during the quarter. Highlights from this quarter include a huge increase in malware overall, though a slight decline in zero-day malware seen over encrypted connections. We also saw a few different JavaScript-based variants delivering the DarkGate trojan and bot client. Network attack volume decreased by 10 percent quarter over quarter (QoQ). ProxyLogon, a fancy name for a critical, pre-authentication flaw in Exchange server found being exploited in the wild during 2022, continues to remain high on our list of top attacks, falling as the second-most targeted attack this quarter.

29 **Top malicious domains**

Using data from our DNSWatch service, we share trends about the malicious web links your users click. We prevent your users from reaching these domains, thus protecting your organization, but we still report on the most popular malicious domains they accidentally clicked on. This quarter, we share the top phishing, malware, and compromised sites blocked, and highlight new domains we saw. For instance, we detail some new malvertising domains, a malicious domain used in millions of WordPress attacks, and the return of some malicious SharePoint subdomains.

32 **Endpoint malware trends**

Network-based malware detection tends to see more different types of malware (like droppers and stagers) than endpoint-based detection since real malware payloads don't tend to surface until later stages of an attack. In our endpoint section, we look at malware trends from an endpoint perspective, using data from our WatchGuard EPDR and AD360 products. Among other things, we share the most popular vectors that malware arrives from and information about the growth or decline of various malware types and families. This quarter, we continued to watch malware detection on endpoint decline by about 12 percent, which is great news. We even saw the unique new instances of malware decline as well. It's hard to guess whether this is due to fewer attacks or more malware being blocked at the perimeter, but we don't complain when malware slows down. From a geographic perspective, interestingly we see more malware in a few South American, African, and Southeast Asia countries than anywhere else. In general, Glupteba and Conficker are the two most prominent threats hitting endpoints, and malicious scripts, such as PowerShell, present the most common infection vectors. The endpoint section contains additional detail on all this and much more.

52 **Best defense strategies for the latest attack patterns**

We map out the top dangers in the cyber threat landscape for you do have a guide to avoid and protect yourself from them. By recognizing the most prevalent attack patterns, we can identify defense you can enable or adjust to avoid them. As we share our findings through this report, we also share how you can defend yourself. W summarize these defense tips throughout many sections of the report, and in our conclusion at the end.

EXECUTIVE SUMMARY

During Q4, perimeter-based malware volume is up, but network attacks are down.

Network malware detections increased overall. Raw malware detection is up almost a whopping 80 percent and the sophisticated and evasive threats stopped by our behavioral detection service, APT Blocker, increased about 37%.

Unlike Q3, network attacks decreased during Q4, dropping about 10 percent. That said, unique detections – a measure of the variety of different network attacks – increased during the quarter about 16 percent. ProxyLogon – a critical Microsoft Exchange vulnerability that could lead to remote code execution – remained high on our top network attack list and grew in volume, even though it dropped down one level on the top 10. You should have patched this critical flaw during 2020 or 2021, but if you haven't it's probably already too late for you.

Compared to network-based malware detection, endpoint malware detections continues to drop QoQ. Older threats remain high on our top 10 list, but happily our products block those old threats easily. Malicious scripts continue to remain the most popular way for malware payloads to arrive at victim computers, but Windows-based files linger as a significant second vector of attack.

Below, you'll find a bulleted summary of some of our top findings this quarter:

- **Total network-based malware detections were up a huge ~80%** with malware detection from the APT Blocker service up 37%, which suggests sophisticated and evasive malware continues to grow. This is further reinforced by an enormous 196% increase in malware detected by machine-learning methods.
- Our "per Firebox" malware results for various network malware detection services:
  - **Average total malware detections per Firebox: 2,416** (~80% increase)
  - **Average malware detections by GAV per Firebox: 520** (2.6% increase)
  - **Average malware detections by IAV per Firebox: 1,404** (196% increase)
  - **Average malware detections by APT Blocker per Firebox: 492** (~37% increase)
- We extrapolate that if all the Fireboxes reporting to us had all malware detection services enabled, we would have had **193,280,000 malware detections during Q4 2023.** Note, that number only represents the Fireboxes that have opted into sharing data with us, it would be significantly higher if it included all active Fireboxes in the world.
- **Malware hiding behind encryption (TLS) increased to 55% in Q4.** This is not as high as it has been in the past, but still shows that you will miss more than half of malware over a network unless you decrypt HTTPS web traffic.
- **Zero-day malware accounts for 60% of all malware during Q4.** As a reminder, we define zero-day malware as malware that evades signature-based protection, only detected by machine-learning malware models or behavioral analysis. Meanwhile, zero-day malware detected over TLS decreased 10 points to 60%.
- **Two top 5 malware variants redirect to DarkGate network.** Among the top 5 most-widespread malware detections were JS.Agent.USF and Trojan.GenericKD.67408266. Both variants redirect users to malicious links, and both malware loaders attempt to load DarkGate malware on the victim's computer.
- **Network attacks decreased 10 percent quarter over quarter (QoQ).** However, unique network attacks, which shows the variety of different network exploits attackers use, rose nearly 16 percent.
- **ProxyLogon remains as one of the top exploited attacks during the quarter.** As a reminder, this was a critical, remote code execution vulnerability against Microsoft Exchange servers that you should have patched long ago. While it dropped to the number two spot on our top 10, it seems to have increased a bit in volume.
- **Four of the five most-widespread network vulnerabilities target Microsoft-related software**, and included named vulnerabilities like ProxyLogon, ProxyShell, and ProxyNotShell**.**
- **Our endpoint protection products blocked 108 unique malware variants per 100k machines.** This represents a continued decline over Q3. Simply put, we are seeing less malware hit endpoints lately. However, that could make sense with the increase in network-based malware detection. Any malware you catch at the perimeter saves the endpoint.
- **Endpoint ransomware attacks decreased about 19.7%.** Ransomware will likely remain a top malware payload for a while, but it has plateaued recently. Its decrease is likely due to many takedown efforts by the authorities. Unfortunately, we do expect to see these variants eventually return despite their takedowns.

- **Cyberattack commoditization continues, trending toward "victim-as-a-service" offerings.** Glupteba and GuLoader were once again counted among the top 10 most prevalent endpoint malware in Q4, making a return as two of the most prolific variants analyzed during the quarter. Glupteba is worth noting as a particularly formidable and sophisticated adversary, due in part to its prevalence targeting victims on a global scale. A multi-faceted malware-as-a-service (MaaS), Glupteba's malicious capabilities include downloading additional malware, masquerading as a botnet, stealing sensitive information, and mining cryptocurrency with tremendous stealth.
- **Malicious Scripts remains as the most prevalent malware delivery vector.** Watch out for malicious PowerShell and JavaScript!
- **Malicious SharePoint subdomains return as a top malicious link.** We also have seen a rise in malvertising links and malicious domains placed on compromised WordPress sites.

Those are just the highlights from this quarter's report. You'll find more fascinating details and additional information throughout this report, including many defense strategies and security tips. We hope you enjoy this "map" of quarterly cyber threats.

FIREBOX FEED STATS

WHAT IS THE FIREBOX FEED?

Each quarter, the WatchGuard Threat Lab collects and analyzes anonymized data from Firebox customers that have opted in to share threat intelligence with us. This threat intelligence is made up of security events that the Firebox security services identify and block including malware and network attacks. By analyzing these events, we can identify the underlying attack trends targeting small and midmarket organizations around the world.

In this section, we review the high-level trends and dive into the specific top threats that either generate the most alerts by volume or impact the most unique networks. Our analysis includes information about the malware families and security vulnerabilities threat actors are targeting and tips administrators can take away to defend their networks.

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

2,416

Average detections per Firebox increased by a whopping **80%**

Basic Gateway AntiVirus (GAV) service

520

Basic malware detections increased slightly by **3%**

APT Blocker (APT)

492

APT hits increased by **36%**

IntelligentAV (IAV)

1,404

IAV hits jumped by **196%**

GAV with TLS

290

TLS detection by GAV increased **166%**

APT Blocker with TLS

288

Encrypted evasive malware dropped **51%**

TLS malware

55%

Malware over encrypted connections increased **7%**

MALWARE TRENDS

We receive threat intelligence telemetry data from Fireboxes whose administrators have opted to share it with us. Part of this data includes anonymized malware detections from Firebox proxies. This data allows us to identify trends in malware over time. For example, we have not seen great changes in the amount of malware our Gateway AntiVirus (GAV) has detected over the last few quarters, but we do see significant increases in the amount of malware detected over encrypted connections. By analyzing these historical malware trends, we can make recommendations on how you can prepare your network to protect against new threats in the future.

During this quarter, we will try to provide more details on the types of malware that traverse encrypted connections. New to this report, we added additional details on widespread malware over encrypted connections. In the past, we didn't have enough reporting data to make a complete analysis, but this quarter we have included our 2023 top widespread encrypted malware table. Since most malware arrives over encrypted connections, we believe this new table best represents the malware your average network sees in the wild.

In Q4, malware spikes like the Linux.Lucifer botnet came back for the third quarter in a row. We also saw malicious redirect scripts from JS.Agent.USF in both our Widespread Malware table and our new 2023 Top Widespread Encrypted Malware table. Additionally, we saw a different variant JS.Agent.UUQ in the top 10 malware table. Later, we will cover how this JavaScript threat works and detail its final payload, called DarkGate.

Starting with a high-level overview, we saw an increase in malware overall during Q4. The evasive malware detected by APT Blocker and IntelligentAV, basic malware detected by GAV, and encrypted malware captured by all malware services via our HTTPS proxy all increased last quarter. The only exception was that evasive malware detected over encrypted connections dropped. Most of these increases come from the Americas (AMER) and, to a lesser extent, Asis-Pacific (APAC) regions. Let's start by looking at the totals in the table to the left.

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

In the past, our top 10 malware list only included malware detected by our signature-based Gateway AntiVirus (GAV) service. We did this because our more advanced and proactive anti-malware services, IntelligentAV (IAV) and APT Blocker (APT), cannot name the malware they detect. Since both those services use either machine learning or behavioral detection to automatically catch new malware, they don't attach malware family names to their results the way a human malware analyst would.

However, our team identified a process that allows us to take the hashes of the malware IAV detects and run them against public malware databases to attach them to known malware families. So now we can pair the malware that both GAV and IAV detects together. This is why our new Top 10 Malware Detections table replaces the Top 10 Gateway AntiVirus table and combines detections from both services. The malware families shown in this table represent most of the reported detections Fireboxes saw globally overall.

In Q4, we didn't see any new malware family's surface on our top 10, but the botnet Linux.XORDDoS.AT and the Coinminer Linux.Lucifer topped our list with the most volume. Though not new to our top 10, the variant Linux.Generic.319779 was last on our top 10 list. This is a generic linux "dropper" that downloads additional payload. During Q4, we saw this script download the Gafgyt malware, which attackers can use for distributed denial-of-service attacks (DDOS). **Reports** show that Gafgyt copied code from the Miria botnet malware.

Other interesting detections from the top 10 include Logan.581. This threat installs a password stealer using Office exploits and primarily targeted Italy during Q4. Zusy.512780 and Heur.RP.Cu2@babWB3ij both mostly targeted China. Finally, JS.Agent.UUQ proxies and redirects web traffic to popular crypto exchanges that contain the words, "binance", "huobi", or "okx" in their URL. The malware sends this proxied traffic to a server controlled by the malware creator.

Threat Name	Malware Category	Count	Last Seen
Linux.XORDDoS.AT	Dropper	724,298	Q3 2023
Linux.Generic.314124(Linux.Lucifer)	Dropper	578,904	Q3 2023
Zusy.512780	Win Code Injection	93,192	Q3 2023
Heur.RP.Cu2@babWB3ij	Win Code Injection	87,829	Q1 2021
Logan.581	Password Stealer	83,980	Q3 2023
Heur.LShot.1	Dropper	59,100	Q1 2021
JS.Agent.UUQ	Dropper	59,055	Q1 2023
RTF-ObfsObjDat.Gen	Office Exploit	53,503	Q1 2023
Fugrafa.12219	Dropper	48,526	Q3 2022
Linux.Generic.319779 (Gafgyt)	Dropper	42,249	Q3 2023

Figure 1. Top 10 Malware Detections

Top 5 Encrypted Malware Detections

While the top malware detections table represents the highest volume of malware Fireboxes detected, we don't believe it accurately represents the most common malware since web traffic is mostly encrypted today (95% according to Google). While our Fireboxes have an HTTPS proxy that allows you to scan encrypted web sessions, only one in five Fireboxes do so. We believe if more Fireboxes were configured to scan encrypted connections, most of our malware detection volume would occur there, and the variants detected in these encrypted sessions probably represent the most common malware on the internet.

As previously shown, this quarter Fireboxes that scan encrypted connection detected 55% of malware over that connection. In other words, most Fireboxes miss more than half of malware detections because they they aren't configured to scan encrypted connections.

Threat Name	Malware Category	Hits
Heur.LShot.1	Win Code Injection	59,100
Logan.749	Password Stealer	9,216
Tedy.392826	Win Code Injection	6,238
Furtiu.2.41AAAEB8.Gen	Win Code Injection	5,479
PoweCod.B.D569C97E	Win Code Injection	3,925

Figure 2. Top 5 TLS Malware

Looking at the top 5 TLS Malware table we see the same Heur.LShot.1 in the Top 10 Malware table that targeted the United States. It injects code to gain RDP access to its victim's system. With RDP access it may load ransomware or other malicious software. Skipping to Furtiu.2.41AAAEB8.Gen, we couldn't find a sample but we know the malware family exploits the MSCOMCTL.OCX RCE Vulnerability tagged as **CVE-2012-0158**. It leverages that vulnerability to inject malicious code and likely download additional malicious payloads. Finally, PoweCod.B identifies suspicious PowerShell code that can open multiple command windows to do any number of malicious things. This script also uses basic Base64 encoding to obfuscate its malicious code.

Top 5 Widespread Malware Detections

Our top 10 list covers the most malware detections by volume, but what if we look at the data from a different perspective. Specifically, how many Fireboxes detected a malware variant. This slightly different view of the same data identifies the most widespread malware variants. We also look at what countries and regions were affected the most by each threat.

At the bottom of our list, we saw Trojan.Zmutzy.1305, a trojan that attempts to load malware on a victim's computer, which we'll cover in more detail later in this section. We also saw JS.Agent.USF, which also showed up in our encrypted most-widespread malware table. We'll describe that more in that section.

Top 5 Most-Widespread Malware	Top 3 Countries by %			EMEA %	APAC %	AMER %
Exploit.RTF-ObfsObj-Dat.Gen	Germany - 31.32%	Hong Kong - 27.97%	Greece - 26.27%	19.83%	7.74%	5.27%
Exploit.MathType-Obfs.Gen	Greece - 25.58%	Germany - 25.49%	Belgium - 18.24%	16.55%	5.55%	5.39%
JS.Agent.USF	India - 57.81%	Mexico - 16.74%	United Kingdom - 15.24%	5.68%	7.95%	10.11%
Exploit.CVE-2018-0802.Gen	Hong Kong - 14.69%	Turkey - 14.57%	Poland - 12.3%	8.42%	3.71%	2.21%
Trojan.Zmutzy.1305	Hong Kong - 13.29%	Greece - 13.13%	Germany - 11.63%	7.71%	3.98%	2.78%

Figure 3. Most-Widespread Malware table

As we mentioned earlier, in this report we debut our newly created Top 5 Widespread Encrypted Malware table. This table covers the entire year of 2023 to provide the most accurate representation of what malware families targeted the widest ranges of victims over encrypted web connections. While the percentages vary quarter to quarter, on average 74 percent of malware arrived over encrypted connections during all of 2023. As we have stated, since most web traffic is encrypted, we believe that only the Fireboxes scanning encrypt traffic with our HTTPS proxy see the most common malware spreading online. That is why we believe this list likely best represents the most common malware found on the Internet. We have also noticed other research groups with similar results in their top malware lists, which we believe confirms our analysis. Let's get into it.

Cryxos.12423 contains JavaScript that normally runs on compromised WordPress pages to load malvertisments and coinminers. We saw that in AMER and EMEA just a few countries were targeted, and the rest of the region spared, for the most part. We also saw the APAC region hit the hardest with this malware.

Next up, JS.Agent.USF identifies a redirect script used to transfer users to a malicious link. As mentioned earlier, we also saw this variant in our Most-Widespread Malware table. Interestingly, after deeper analysis we found the malware GenericKD.67408266 also redirects users to a similar malicious link as JS.Agnet.USF. Both "loader" variants attempt to load additional malware called DarkGate onto the victim's computer. We cover these malware variants, and PDF.Spam.Heur.1 more in detail later.

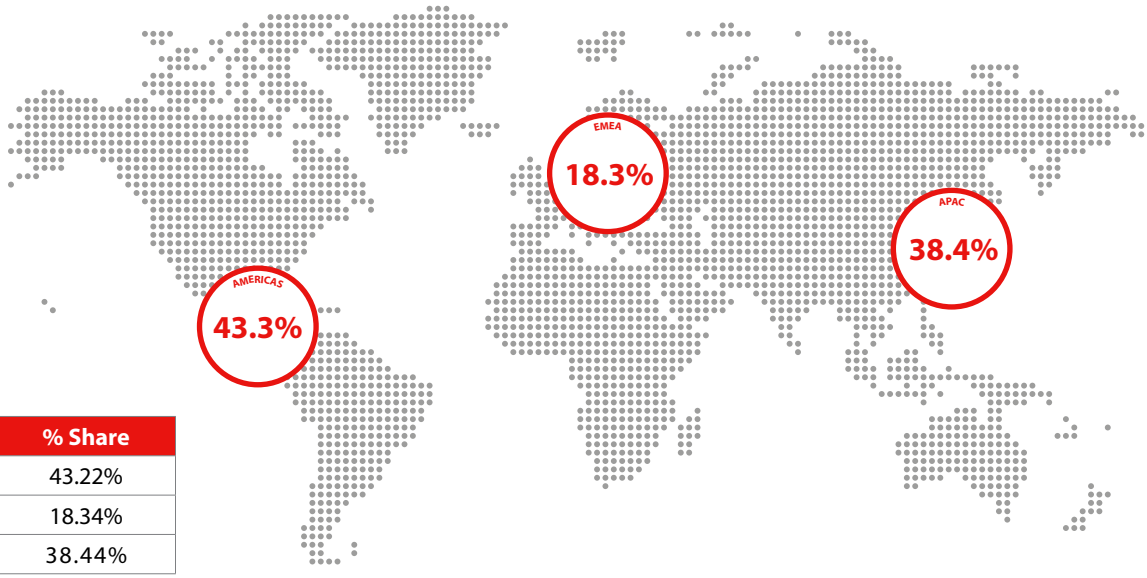
Finally, JS.Agent.FQ also redirects victims. This time to shady sites, including Chinese-hosted gambling sites.

Malware Name	Top 3 Countries by %			EMEA %	APAC %	AMER %
Cryxos.12423	Brazil - 31.9%	Portugal - 29.08%	France - 25.74%	12.26%	22.03%	13.22%
JS.Agent.USF	Australia - 19.79%	Canada - 19.53%	United States of America - 16.98%	7.84%	18.98%	15.57%
JS.Agent.FQ	Brazil - 15.24%	United Kingdom - 11.3%	Portugal - 9.93%	7.40%	7.46%	6.81%
PDF.Spam.Heur.1	United Kingdom - 12.09%	United States of America - 7.82%	Canada - 7.69%	4.63%	4.41%	7.46%
GenericKD.67408266	Turkey - 15.69%	Australia - 8.33%	United Kingdom - 5.02%	3.74%	12.88%	2.43%

Figure 4. Most-Widespread Malware

Geographic Threats by Region

To better understand the Top 10 Malware table and the Top 5 Encrypted Malware, it's interesting to add regional context to see where attackers are targeting most of their malware. Since we don't want our company's regional sales trends to poison our results, we weigh our results by the number of Fireboxes in each region to level the playing field. This allows us to find what region sees the most malware without worrying about one region having more detections simply because more Fireboxes report to us in that region.



Region	% Share
AMER	43.22%
EMEA	18.34%
APAC	38.44%

Figure 5. Geographic Threats by Region

In Q4, Americas (AMER)-based Fireboxes saw an unusually high percentage of detections (43.22%). This represents an 11 percent increase from Q3 2023. The Asia-Pacific (APAC) region received 38.4 percent of malware, which was a 6 percent increase QoQ. Finally, Europe, the Middle East, and Africa (EMEA) suffered the remaining 18.3 percent of malware, which was a 17 percent drop over the previous quarter. Without additional data, it's hard for us to understand why attackers target regions differently each quarter, but we still find it interesting to follow these changes. Malware evolves all the time and so do its targets locations.

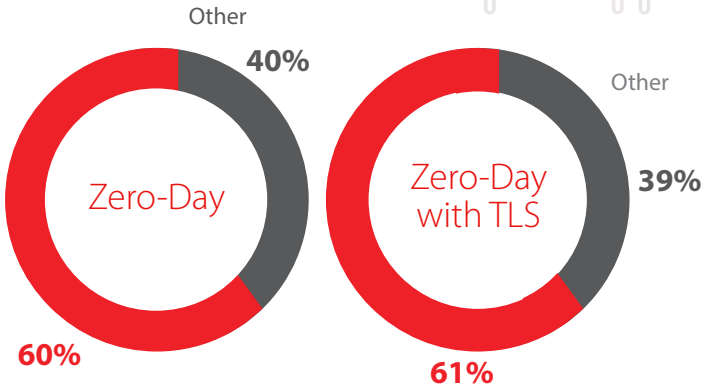


Figure 6. Zero-Day Malware

Catching Evasive Malware

Risky zero-day malware and other evasive malware often contain the latest malware like ransomware or new exploits. These types of malware tend to be harder to block as they contain techniques to bypass basic signature malware detection. APT Blocker and IAV don't just use signatures to detect malware but can identify a file as malware from the file structure and what the file does. APT Blocker does this by detonating unknown files in a sandbox and extracting the true intent of the file.

For this last quarter, zero-day malware detections jumped to 60% of all malware from 22% the previous quarter. For zero-day with TLS, this dropped 10% to 61%. These large variations show the unpredictability of malware in the wild. Perimeter defenses keep malware out of your network altogether so the attack surface, or the area that we expose to unknown threats, becomes as small as possible. This is why detecting zero-day malware at the perimeter is a key component to keeping unknown threats out.

Zero-day perimeter detection works well with host-based advance EPDR. While EPDR covers servers and workstations that have the service installed, you can't put EPDR on your printer. You also can't install EPDR on servers you don't know about. Layering these together provides the best protection for every host, server, printer, and IoT device in the office.

Individual Malware Sample Analysis

JS.Agent.USF and Trojan.GenericKD.67408266 - DarkGate

Even though our anti-malware services detect these malware variants with two different names, the threats they identify are virtually the same. Whichever the name, both are malicious JavaScript files that redirect its victims to malicious sites, which are designed to serve up an additional threat called DarkGate.

In most of the samples we analyzed, we saw JavaScript code that forces the victim's machine to a malicious php like the one seen in the URL below:

http://cdn.jsinit.directfwd[.]com/sk-jspark_init.php

This php page would appear to display a circular "loading" animation to the user, however behind the scenes it downloaded and ran Trojan.GenericKD.68092597.

At some point early 2023, the malicious link in these variants changed to a new URL seen below:

http://scoutnewresults.com/sk-jspark[.]php

Later in the year, we again saw the URL continue to change. This is not unusual for JavaScript threats like these. While the malicious JavaScript may not change much, the threat actors behind them may have to constantly change their malicious malware distribution URLs as authorities and hosting companies take down their old ones. So even though the URLs might change, often the additional malware payloads they are serving don't. They just must move from location to location to outrun the good guys.

Figure 7. DarkGate

In any case, since these URLs went down and changed so regularly, it is often hard for us to analyze the final malware payloads directly when these sites disappear. In this case, however, we found multiple reports indicating these URLs lead to the malware called DarkGate. Eventually, one sample we found contained a compressed file with the contents shown to the right.

The PNG image files shown don't have anything to do with the malware, but likely serve as some distraction or red herring against the actual threat, which really involve an .MSI file, Windbg.exe, the DLL, and BIN files. To summarize, those files are used to load the DarkGate malware, but we won't repeat a full analysis as others have already covered it in detail. To find more about how this malware and botnet loads see both the Splunk research **here** and eSentire research **here**.

PDF.Spam.Heur.1

The malware family PDF.Spam.Heur identify PDF files that link to malicious websites. These websites can host any malware family but most often contain credential stealers. When you open these malicious PDFs, they oftentimes present fake "are-you-human" challenges. However, if you click the link to complete these "I'm not a robot" challenges, it directs you to a malicious website.

Figure 8. pdf.spam.heur pdf

Hosting providers take these sites down within hours most of the time, but the groups who create them add new ones just as fast. In fact, to investigate a sample before it disappeared, we had to find one created the same day we inspected it.

In the active sample we found, the link in the PDF led to the website below.

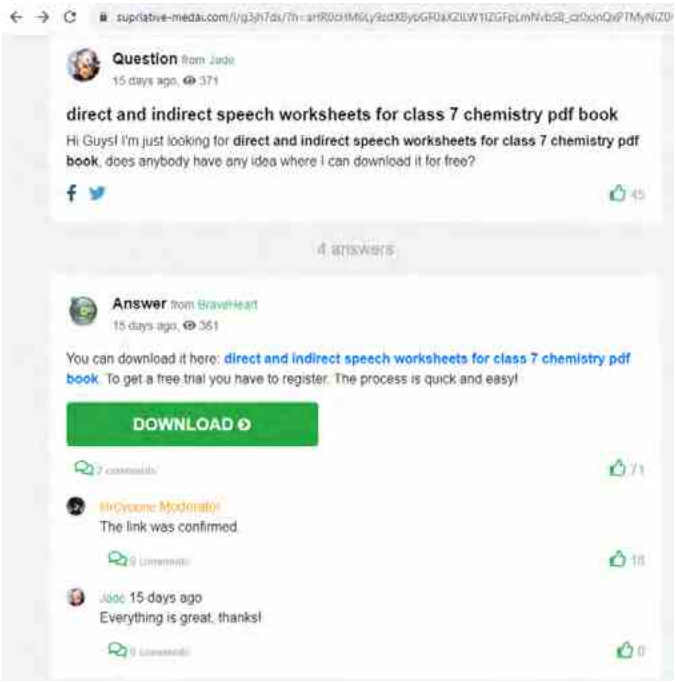


Figure 9. PDF.Spam.Heur Fake Comments

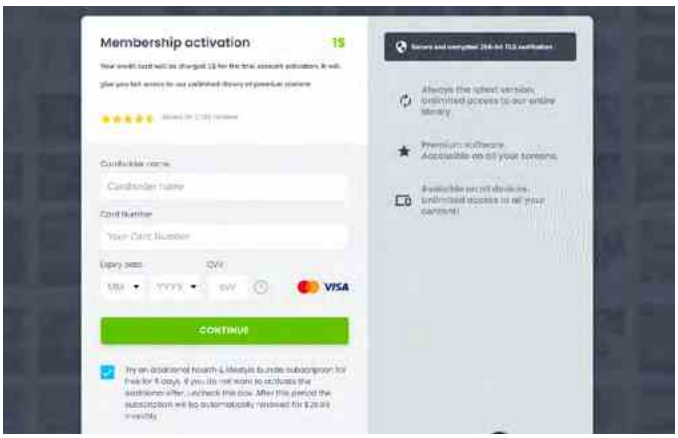


Figure 10. PDF.Spam.Heur.1 Payment Form

At first glance, it may look like a legitimate web forum. However, the comments are fake and every link leads to the "registration" page, which asks for your credit card information.

We hope no one will share their credit card details in a strange page like this but some victims must have, otherwise these threat actors wouldn't be trying this cheap phishing trick. This particular malicious PDF sample wasn't as dangerous as other SPF.spam.heur malware we've seen. Sometimes the PDF's malicious links might directly lead to ransomware loaders and other riskier malware. We found that many of these malicious PDF files contain multiple pages with random pictures in them. As always, don't open any unsolicited files, especially unexpected PDFs and if you do, avoid clicking on links inside them unless you know the file or link is safe.

Trojan.Zmutzy.1305 – Agent Tesla

Zmutzy.1305 is a trojan "loader" that downloads additional malware payloads. During this quarter, the samples we found usually downloaded Agent Tesla – an old but prolific remote access trojan (RAT) that often served up additional malware. We have covered Agent Tesla before so will analyze just its loader this time.

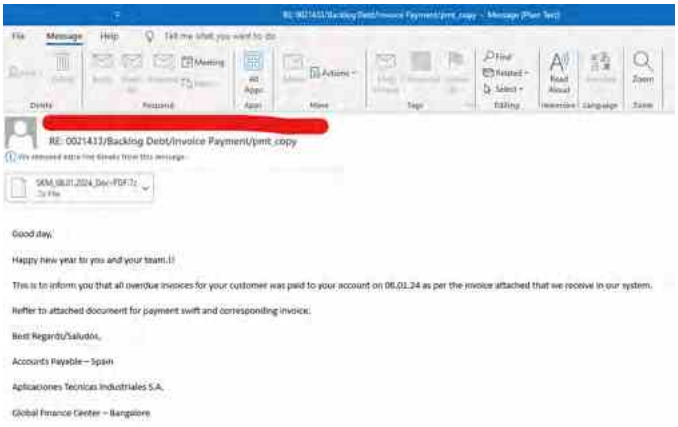


Figure 11. Zmutzy Email

Zmutzy begins as an extremely poorly written email; one that we feel is so bad you could barely believe it was written by a human. The email is chock-full of grammar issues, even starting on the 2nd line of the body, where its sentence ends with a period followed by two explanation marks. Besides the multiple grammar issues, the content of the email remains vague and unintelligible, and contains no personal reference to the victim to suggest it's really for them. With even marginal attention and skepticism, a user should never fall for such a horribly crafted lure. If you ever see an email like this, please do not interact with it or its attachments!

The attachment in the email contains a compressed archive .zip file and not the LZMA compression format as indicated in the extension ".7z." This was likely done to bypass email security controls that try to extract normal zip files, but only look at the file extension to establish the file type. If an email security solution had uncompressed this zip file, it may have blocked its malicious contents before it reached the victim's inbox.

Extracting the contents of this file reveals the actual malware, which was an executable (EXE) file masquerading as a PDF. If you protect your email server using a Firebox with an SMTP proxy, it can and will extract compressed files before scanning them with our anti-malware services. This is how our Fireboxes identified this file even though it arrived as a compressed file. It also won't be confused by a zip file pretending to a 7-zip file with a false extension.

Figure 12. Zmutzy Icon

As mentioned above, this portable executable (PE) file – which is easily identified by its extension – was made to look like a PDF. To analyze what this executable did, we ran it in our sandbox. We saw it generated some network traffic, making a call to an API located at ip-api[.]com/line/?fields=hosting. This API call returned the word "false." We suspect that the API call attempts to determine if the compromised device runs on a cloud-hosting environment. We suspect that if the API returned a true meaning, running on a cloud-hosted device, the malware installation would have changed in some way or maybe even halted. In some cases, malware makes checks to a victim's system to weed out undesirable targets. For instance, it may not want to target systems coming from IP ranges associated with authorities or security companies. Sometimes malware does system checks to see if it's running in virtual environments to weed out sandboxes. In other cases, malware may not want to infect operating systems with certain language settings, to avoid infecting victims in particular countries. In any case, this API may be some sort of system check when the threat actor has to avoid certain victims.

In the end, however, our sample received the false result, which seemed to allow the attack to continue and install the Agent Tesla malware. Once installed, the Agent Tesla variant is connected to its botnet Command and Control (C2) server. This variant used the chat program Telegram to send and receive botnet C2 commands.

Network Malware Summary

By analyzing the top malware by pure volume, most Fireboxes affected, by region, and within encrypted connections, we try to show you a complete picture of global threats in this section of the report. We hope you are better equipped to protect your network by knowing the type of threats targeting your region today. Hopefully, this quarters malware section reminder you a few things:

1. Most malware arrives over encrypted connections. If you haven't set your Firebox to decrypt and scan that traffic, you are missing it. You should correct that.
2. More than half of malware evades signature-based protections. If you are not using the advanced anti-malware services in our Total Security Suite of services, you will miss most of that malware.
3. Don't fall for stupid threat actors' horribly written email lures. If it is full of crappy grammar, and makes no sense in context to you, why would you ever interact with that email's attachment. If you must fall for malicious emails, at least don't fall for the stupid ones.
4. Don't rely on endpoint protection to save you. While it's critical you do use endpoint-based anti-malware and endpoint detection and response (EDR) solutions, some malware may have tricks to evade those tools. Any threats you can block at your perimeter will save you down the line.

NETWORK ATTACK TRENDS

WatchGuard's Intrusion Prevention Service is a network-based safeguard that uses a signature database to identify and stop known attacks. Many of the commonly triggered signatures we discuss in this section are for recent vulnerabilities. ProxyLogon, ProxyShell, and ProxyNotShell are three well-known ones – all Microsoft Exchange Server vulnerabilities. Here's a hint for much of the IPS section: Microsoft infrastructure is everywhere, and attackers want a piece of it! On the topic of Microsoft, there are also plenty of old and semi-old products that our top-detected signatures are connected to. That includes a Microsoft Internet Explorer memory corruption vulnerability, cross-site (XSS) scripting attack against Microsoft SharePoint Servers (and other companies' products), and IIS 6.0 and IIS 7.0 for different vulnerabilities.

The data was rather ordinary this quarter. That is, no great big jumps in terms of total volume, per signature volume weight, or detections between regions when compared to previous quarters. Perhaps that's a good thing? It's important to note that the total detections volume significantly changed between Q1 2023 and the following quarter, when we adjusted our data to extend our definition of outlier data. This will be evident on several graphs in this section. In addition, we only had a handful of new signatures to discuss this quarter. The two new most-widespread signatures were related to ProxyShell and ProxyNotShell. The one new top 10 signature is a Microsoft Internet Explorer memory corruption vulnerability. This signature has been the number one most-widespread signature two quarters in a row. So, it is new to the top 10 but not the most-widespread list. Later in this section, we also discuss three new signatures among the top 50 signatures by volume. They are new in that they have not reached a significant volume to make it to the top 50 signatures.

Total Detections

470,338 detections this quarter.

- A nearly 10% decrease from last quarter.

Unique Signature Detections

451 Unique Detections

- 15.94% increase from last quarter.
- On average there has been little change in total unique signatures per quarter with only a 0.71% average change since Q4 2020.
- This is a 2.88% decrease between now and Q4 2022.

Average Detections per Firebox

87 detection average per Firebox among all regions.

- AMER: 92 detections per Firebox
- EMEA: 87 detections per Firebox
- APAC: 53 detections per Firebox

Other Highlights

The top 10 signatures represent nearly 60% of total volume.

- The top 3 are over 25% of total volume.

ProxyLogon is 8.37% of total volume this quarter. The highest since we began tracking it. It was only 0.60% percent of total volume in Q2, 2021.

The top 50 signatures represent 92.02% of total volume.

SQL injections attacks represent 21.37% of detections among the top 50.

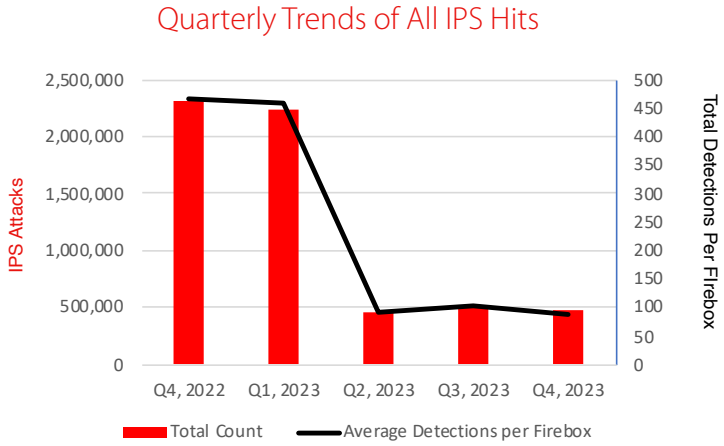


Figure 13: Average IPS Detection's per Firebox

Quarter/Year	Total Detections	Average Detections per Firebox
Q4, 2022	2,306,175	465
Q1, 2023	2,230,896	460
Q2, 2023	448,670	93
Q3, 2023	520,080	104
Q4, 2023	470,338	87

Figure 14. Average IPS Detections per Firebox

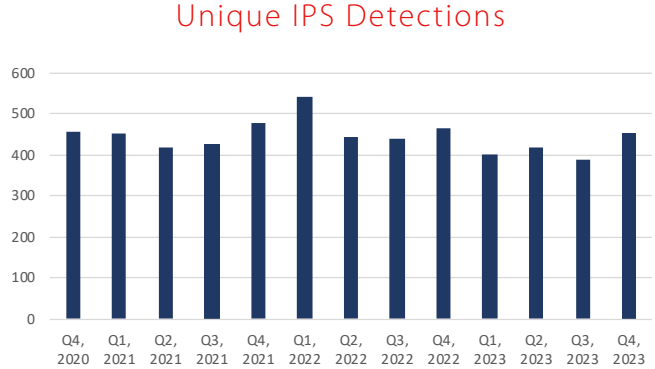


Figure 15. Unique IPS Signatures per Quarter

Top 10 Network Attacks Review

There wasn't a lot of change in the top 10 this quarter compared to Q3. This section will act more as a review for any returning ISR report readers. Unless you have a photographic memory, it won't hurt to read over the common threats again. Several have jumped places quite significantly or returned to the top 10 after one or more quarters away. Our one new signature in the top 10 is for a Microsoft Internet Explorer memory corruption vulnerability. While reaching the top 10 by total volume, it has been in first place among most-widespread signatures both this and last quarter. Several signatures worth noting are signature 1138800 (ProxyLogon) and signature 1056247 (Quagga network software).

Signature 1132793

This signature, in first place this quarter, rose from third place last quarter and sixth in Q2 2023 when it first reached the top 10. It is associated with a no longer maintained open-source learning management system (LMS) software. It has been several years since the software, ATutor, has been updated. Therefore, it has years of vulnerabilities piled up. Anyhow, this is obscure software. Likely this SQL injection attack is directed at a vast range of other software due to the broad nature of an SQL injection attack.

The detections per quarter have about doubled since Q2 2023. The aggregated data shows most of the traffic from the EMEA region with a fraction of it from AMER. Of the distribution among EMEA, a majority is from a few European countries and a small amount in the Middle East.

Signature 1138800

ProxyLogon, for which this signature is associated with, has been a top domain for the past two quarters. It has risen in the ranks among the top 10 since Q3, 2022. While the signature has dropped down to second place, it has reached new heights in terms of volume. It rose 0.17% from last year, to represent 8.37% of total traffic this quarter. Even if it doesn't hold first place, the vulnerability is much more consequential in terms of impact compared to our number one signature this quarter. Microsoft Exchange vulnerabilities will always be some of the most serious vulnerabilities organizations must encounter.

Quarter	Rank by Volume	% of Total Volume
Q4 2023	#2	8.37%
Q3 2023	#1	8.20%
Q2 2023	#1	2.10%
Q1 2023	#4	6.10%
Q4 2022	#4	5.54%
Q3 2022	#8	3.90%
Q2 2022	#14	1.80%
Q1 2022	#20	0.40%
Q4 2021	#26	0.30%
Q3 2021	#22	0.50%
Q2 2021	#20	0.60%

Figure 16. ProxyLogon History

Signature 1058470

We introduced this SQL injection attack signature in Q1 2023 when it was number one among all other signatures. It then fell from the top 10 in the previous two quarters, but remained a voluminous signature where it was in 16th place last quarter and 24th in Q2 2023. This affects two known software products. One is OpenEMR, an open-source medical practice management product. They had a list of vulnerabilities published in 2013, followed by several more in 2018. Unlike the open-source ATutor software mentioned earlier, this software remains actively managed and updated. The second affected software is Joomla!, an open-source content management system (CRM). Our presumption is that this is the main target as Joomla! is a widely used platform. But, as this is a SQL injection attack, it likely has a significant reach beyond the OpenEMR and Joomla!. Among the total connections, 60% of them were in EMEA and 40% in AMER.

Signature 1056773

This is another example of a signature whose volume can wildly bounce around quarter over quarter. It was first present in 10th place in Q1 2023, and moved up a spot in Q2 2023. It then dove to 33rd place last quarter and has now bounced back all the way to fourth place. As for what this signature is about, it is a buffer overflow attack resulting in attackers remotely executing arbitrary code. It targets Address Space Layout Randomization (ASLR), which is used to obfuscate the memory space and create an additional defensive layer to protect the memory stack. The known exploit is associated with a PoC against Windows 7 software from 2012. The attacker sends a malicious GET request to the vulnerable Simple Web Server 2.2-rc2, followed by a combination of memory manipulation and ASLR bypass, and ultimately a compromise of the system.

Signature 1055396

This signature encompasses numerous affected products. That's simply because it represents a generic cross-site (XSS) scripting attack. A successful XSS attack needs a vulnerable web-connected application, for which there seems to be an infinite number available. A simple Shodan scan for different web applications will demonstrate the realities of the Wild West of the web. To give context to the breadth of affected products, look at the list below, representing under half of the documented CVEs:

- Microsoft SharePoint Server 2007 12.0.0.6421 (and earlier versions) + SharePoint Services 3.0 SP1 and SP2, version
- Report Viewer Control in Microsoft Visual Studio 2005 SP1 and Report Viewer 2005 SP1
- Oracle GlassFish Server component in Oracle Sun Products Suite 2.1.1
- Joomla! before 1.7.0
- Microsoft SharePoint Foundation 2010 Gold and SP1
- Java Runtime Environment (JRE) in Oracle Java SE 7 update 4 and earlier and 6 update 32 and earlier, and the GlassFish Enterprise Server component in Oracle Sun Products Suite GlassFish Enterprise Server 3.1.1

- IBM Tivoli Endpoint Manager (TEM) 8 before 8.2 patch 3
- IPAM web interface before 3.0-HotFix1 in SolarWinds Orion Network Performance Monitor
- Symantec Web Gateway (SWG) appliance before 5.2
- D-Link DIR-100 4.03B07

Microsoft SharePoint Server, Oracle Java SE 7, and SolarWinds Orion Network Performance Monitor are all widely used products, as are most the other products listed. It is no surprise that this signature has been in the top 10 semi-regularly since Q4 2019. It is in fifth place this quarter, and when it was last in the top 10 in Q2 2023, it was the fourth most voluminous signature. Even when it doesn't make the top 10, it is usually close by, such as last quarter when it was in 11th place. Attackers will continue to compromise web apps and seek unsuspecting users who believe they are on a trusted site. Therefore, an array of defenses can go a long way toward protecting the end user, one of them being the Intrusion Prevention Service.

Signature 1054837

Here we have an even longer-term top 10 signature. It first appeared in 10th place in Q2 2017 and returned for a second time to become the top signature in Q4 2018 and continued as the top signature the following quarter. Since it reached the top spot, it has remained in the top 10 list except for a handful of quarters – such as last quarter when it was in 12th place. As the name "WEB Remote File Inclusion /etc/passwd" implies, Unix and Linux-based systems were the target as the /etc/passwd folder is where user login information is stored. The age of the vulnerability is evident as modern Linux systems have moved password hashes from etc/passwd to etc/shadow, which is only accessible by root. This change was enacted to prevent the ease of stealing hashes.

Much like XSS-related signature discussed before this, there is a long list of affected products due to the broad nature of the target; in this case, trying to access /etc/passwd in Linux systems, which are everywhere! Below is a list of some of the affected products:

- WordPress 2.1.1
- LotusCMS Fraise 3.0
- DreamBox DM800 1.6rc3, 1.5rc1
- Bitweaver 2.8.1
- VideoWhisper Live Streaming Integration plugin before 4.29.5 for WordPress
- McAfee Asset Manager 6.6
- ZOHO ManageEngine Applications Manager before 11.9 build 11912, OpManager 8 through 11.5 build 11400, and IT360 10.5 and earlier
- Elasticsearch before 1.6.1
- Schneider Electric's U.motion Builder software versions 1.2.1 and prior

The list encompasses a lot of different software all with the same directory structure. This signature was released in 2011, which shows, based on the old versions of some of these software products. Additionally, some of these products are no longer maintained, such as LotusCMS. Organizations who use outdated software aren't doing it because they want to. Often it is due to financial considerations. There's a cost to migrating to new software, and there's a cost to allocating enough working hours for operations staff to update and patch products. Therefore, the IT administrators must face reality handed to them and deal with building a fort around their outdated software. Hence, why there is an abundance of security vendors.

Signature 1059958

It was Q2 2022 when this signature reached 10th place, and has remained in the top 10 ever since. Last quarter it was the 2nd top signature, but often it has been between 3rd and 5th place. This directory traversal attack is connected to vulnerabilities in three separate IT management software's. Those are ZOHO ManageEngine Desktop Central (DC) v7 and up to v9 build 90054, Oracle Application Testing Suite within the Oracle Enterprise Manager Grid Control 12.4.0.2 and 12.5.0.2, and Trend Micro Control Manager. In each case to varying degrees, attackers could successfully acquire access to the host systems files and potentially exfiltrate files. The CVEs associated with these vulnerability discoveries range between 2014 to 2017.

Signature 1056247

Last quarter we talked in detail about this signature as it reached the top 10 for the first time. It is now only a few spots lower than last quarter. The term NOP in the signature name SHELLCODE NOP Sled refers to the No-Operations (NOP) instruction that is used to pad space in between other instructions in a memory stack. The Sled refers to where the memory will sled/slide down within a NOP instruction until it reaches the end. Attackers seeking to exploit a stack buffer overflow vulnerability and deliver a malicious payload will try to make their own luck by expanding NOP instruction. This is because the whereabouts of the NOP instruction will still be unknown to the attacker. It is much easier to land on a large NOP instruction and sled/slide to the return address, which will jump to the top of the buffer and execute the shellcode (the payload). This is the preferred method, whereas the other method is to hope to land on the small memory location hosting the shellcode instruction.

Detections for this signature are primarily associated with two products. One is Squid, a caching proxy. The Web Cache Communication Protocol (WCCP) has a 2005 vulnerability due to handling larger messages than the memory buffer was intended to handle. That can result in a denial-of-service (DoS) attack. The other is Quagga version 0.93 through 1.1.0 for, an open-source network routing software suit for Linux and Unix-like systems.

AMER and EMEA region have the bulk of total detections. In AMER the US represent 89.5% of detections while Chile is just under 10%, with the remainder spread among a few countries. Most of the EMEA detections are from France and Italy, followed by Germany and several other countries.

Even though this NOP Sled attack could affect other products, we chose to look further into Quagga. A quick search for Internet-facing Quagga instances on Shodan intrigued us – sending us down a short research side quest.

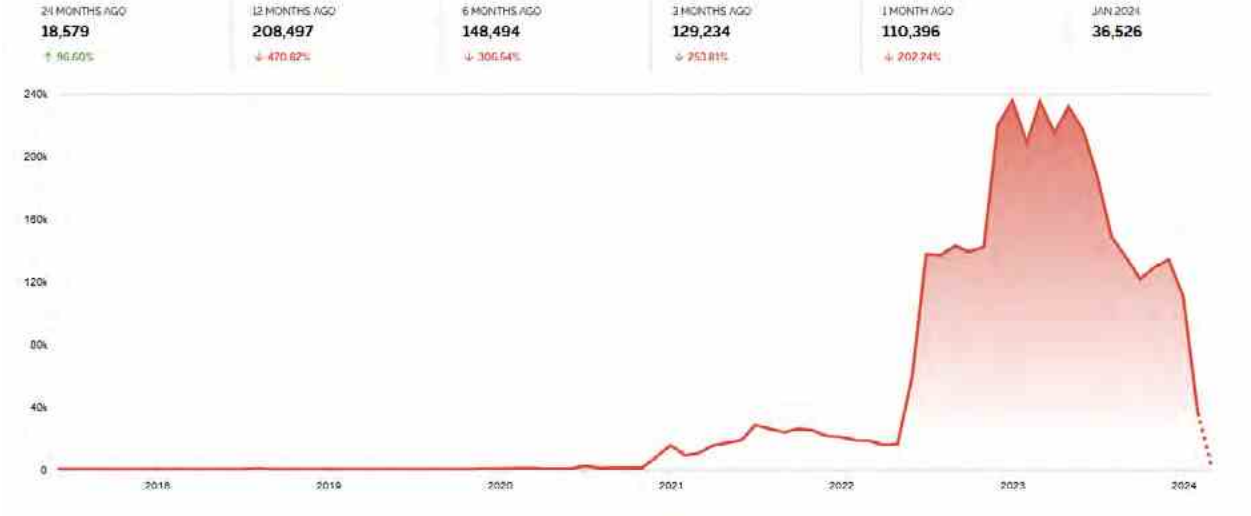


Figure 17. Shodan.io Trends Detection **Results for 'Quagga'**

Note

Shodan Trends shows historical data since 2017 while Shodan Search shows current device detections.

- Shodan Trends shows 2,288 detections in February 2024 while Shodan Search shows 38,810 detections.

There is a difference when searching Quagga vs Quagga Routing Software under Trends. The Quagga Routing Software query only shows China-based locations. We chose to display graphics from the Quagga query on Trends. A query using "Hello, this is Quagga" works as well.

Quagga results in a small number of detections beginning in 2017 (the beginning of Trends timeline) and increasing to 16,000+ pre-April 2022. Pre-April 2022, the US had about 8,000, followed by Japan and several other countries. The next month those countries had similar numbers but was then dwarfed by China with 40,000 detections. The Chinese numbers peaked in December 2023 with nearly 200,000 detections of a total of 235,000 that month.

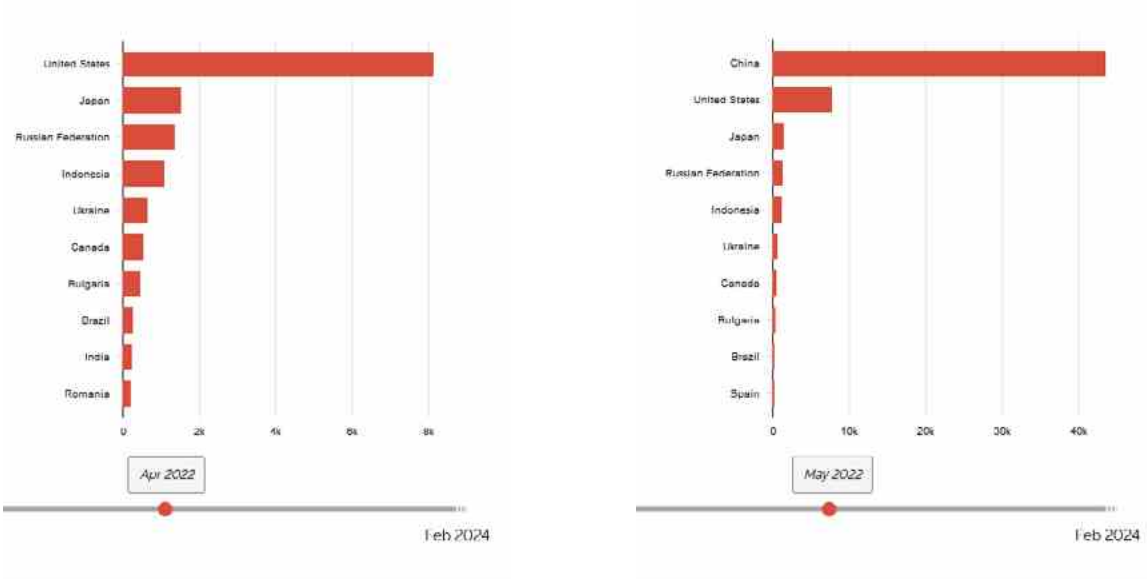


Figure 18. "Quagga" search results on Shodan.io for April 2022 (left) and May 2022 (right). The peak was 228,831 devices in April 2023.

The latest numbers for February 2024 only show 2,288 detections. China has 1,878 of those, followed by 238 for the US. Now, this is all using the Shodan Trends tool. If you look in their main search engine, it will show **38,000+ results** as recently as March.

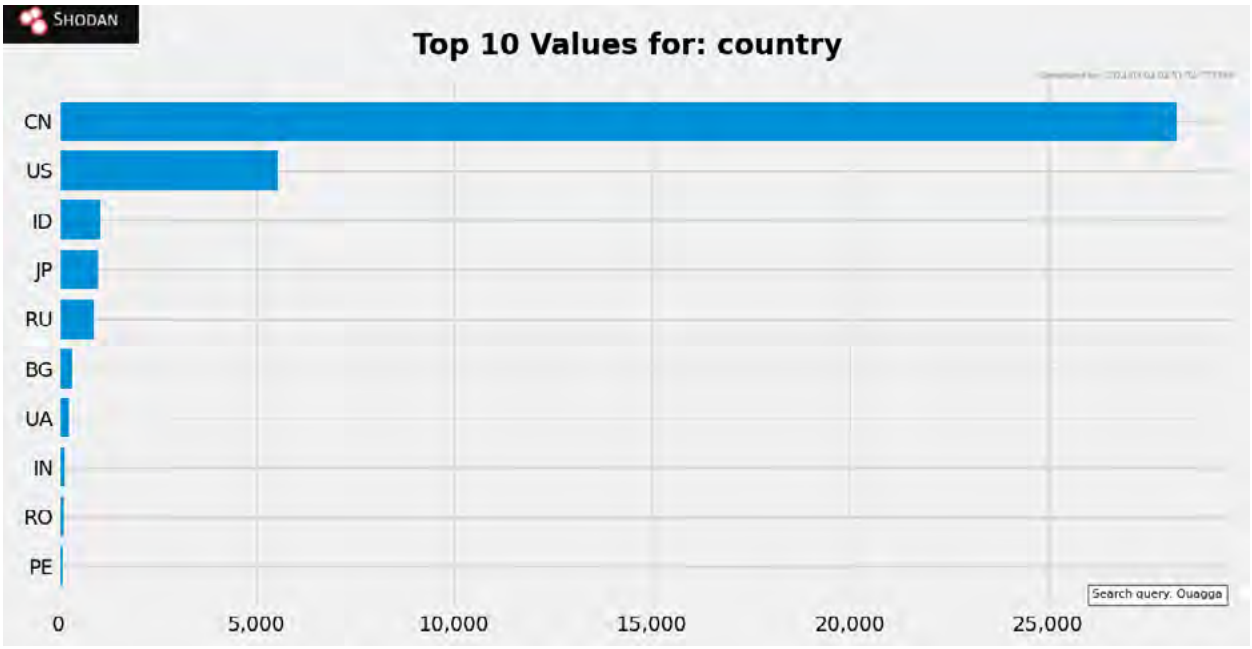


Figure 19. Top Countries from Shodan Search Query for 'Quagga'

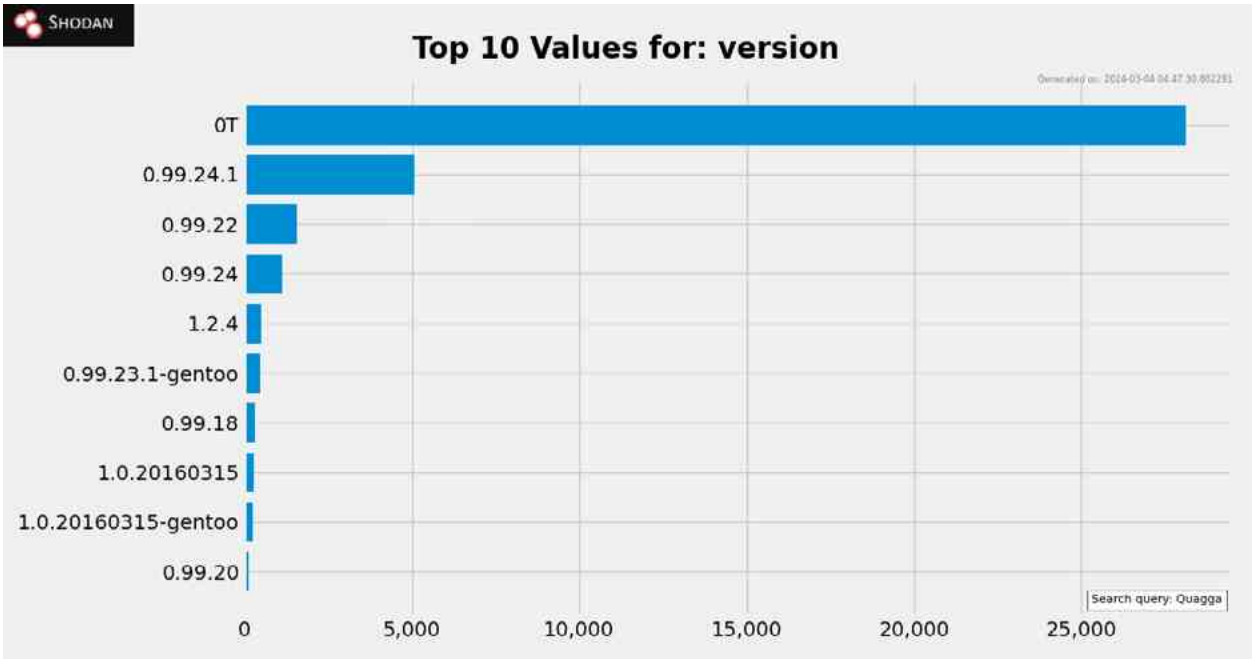


Figure 20. Top Quagga Versions Scanned by Shodan as of March 4, 2024

Rough estimates show only 1.7% of detections are from versions safe from the NOP Sled exploit. That is assuming the 0T version is a 0.x.x version and not representative of something else. Additionally, all those 0T versions are from China.

After digging through all these charts, we realized there was probably an explanation beyond randomness for the explosion of China-based detections. And there was. In 2022, several Border Gateway Protocol (BGP) message parsing vulnerabilities were **discovered** in FRRouting. That is Free Range Routing, a fork of Quagga and the default open-source network software organizations migrate too, as it is still maintained. FRRouting could be impacted by a DoS attack due to these discovered vulnerabilities.

A recent search on Shodan with the keyword "FRRouting" will show nearly 40,000 or so devices detected. China had over 98% of those detections. A separate search with a **'Hello, this is FRRouting (version 4.0)'** query comes up 100% in China, including one in Hong Kong. FRRouting v4.0 was released in 2018, so it was in no way protected from these vulnerabilities. Interestingly, FRRouting detections **began to rise** in December 2023, and peaked in January 2024. That is months after Quagga, when detections began increasing in May 2023.

FRRouting pushed out a quick patch to address these vulnerabilities. The same can't be said for Quagga. Therefore, all Quagga versions should be considered vulnerable. WatchGuard switched to FRRouting from Quagga last year at the release of Firewire v12.9. Earlier Fireware versions have Quagga v1.2.4 installed. Therefore, customers with Fireware versions v12.8.x or lower are protected from the NOP Sled exploit, and additional security tools such IPS prevent the later discovered DoS attacks.

Signature 1131523

This is the only signature that is new to the top 10 this quarter. It has been around in the top 50 for a while. Just last quarter it was #21, so it was a significant jump to reach ninth place this quarter. Although the first time in the top 10, it was in our most-widespread top 5 signature list last quarter. Now for a second time it is the #1 most-widespread signature. The signature is tied to one CVE, for a Microsoft Internet Explorer memory corruption vulnerability published in 2015. This was only applicable to Internet Explorer 11 (IE 11). Should a victim arrive on a malicious website, the attacker could perform a remote code execution to funnel malicious code or perform a denial-of-service attack.

When Microsoft published the vulnerability, they did it along with 18 other CVEs. It was only **CVE-2015-2425**, associated with this signature, that was known to have been exploited in the wild. There is minimal information available on this exploit, even with it being noted to have been exploited. CVE-2015-2425 has a 07/14/15 publication date, and the **Microsoft security bulletin** was published just a week later, likely leading to a subdued impact of the discovered vulnerability. Even with IE 11 being phased out, there is still a window of support until 2029 by Microsoft. The widespread use of Windows means there remains a large swath of systems with IE installed. It makes sense to see this in the most-widespread list as attackers will seek vulnerable systems. This is especially true for organizations who have yet to push out the latest patches and upgrades, even ones from years ago.

Signature 1059877

This directory traversal attack signature affects several products:

- SpecView 2.5 build 853
- ZPanel 10.1.0 and prior
- nginx 0.8.41 through 1.4.3 and 1.5.x (before 1.5.7)
- SysAid Help Desk prior to 15.2.

These products were in some form affected by how they handled accepting data. The lack of sanitation allowed an attacker to deliver malicious code to traverse a systems directory and then further their exploits by allowing for remote code execution. This signature has been in the top 10 since at least Q4 2020. It peaked at second place in Q2 2023 and has fallen to 10th place. There isn't any signature that has been consistently present in the top 10 each quarter, which can be seen in Figure 20. Additionally, it has maintained a presence in the most-widespread top 5 signatures since Q2 2022. It has stayed in third or fourth place. The four products we listed are wide-ranging in their uses. From SpecView used for SCADA monitoring, to SysAid Help desk for IT management software, and nginx, a webserver with a range of features. These are connected to the signature due to their CVEs, but there must be a greater swath of products affected by this attack due to how broad a vulnerability it is. It makes sense that we continue to see this in the top 10 and most-widespread signatures.

Signature	Type	Name	Affected OS	Percentage
1132793	Web threats	WEB SQL injection select from attempt -5.h	Windows, Linux, Freebsd, Solaris, Other Unix, Mac OS	9.89%
1138800	Web threats	WEB Microsoft Exchange Server Remote Code Execution Vulnerability -6 (CVE-2021-26855)	Windows	8.37%
1058470	Web threats	WEB SQL injection attempt -17.h	Windows, Linux, Freebsd, Solaris, Other Unix, Mac OS	8.30%
1056773	Buffer Overflow	WEB Web Server Connection Header Buffer Overflow	Windows	6.90%
1055396	Web threats	WEB Cross-site Scripting -9	Windows, Linux, Freebsd, Solaris, Other Unix, Network Device	5.38%
1054837	Web threats	WEB Remote File Inclusion /etc/passwd	Windows, Linux, Freebsd, Solaris, Other Unix	5.15%
1059958	Web threats	WEB Directory Traversal -27.u	Windows, Linux, Others	4.76%
1056247	Exploits	SHELLCODE NOP Sled	All	3.88%
1131523	Buffer Overflow	WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability -2 (CVE-2015-2425)	Windows	3.58%
1059877	Exploits	WEB Directory Traversal -8	Windows, Linux, Freebsd, Solaris, Other Unix	3.38%

Figure 21. Top 10 Network Attacks by Volume

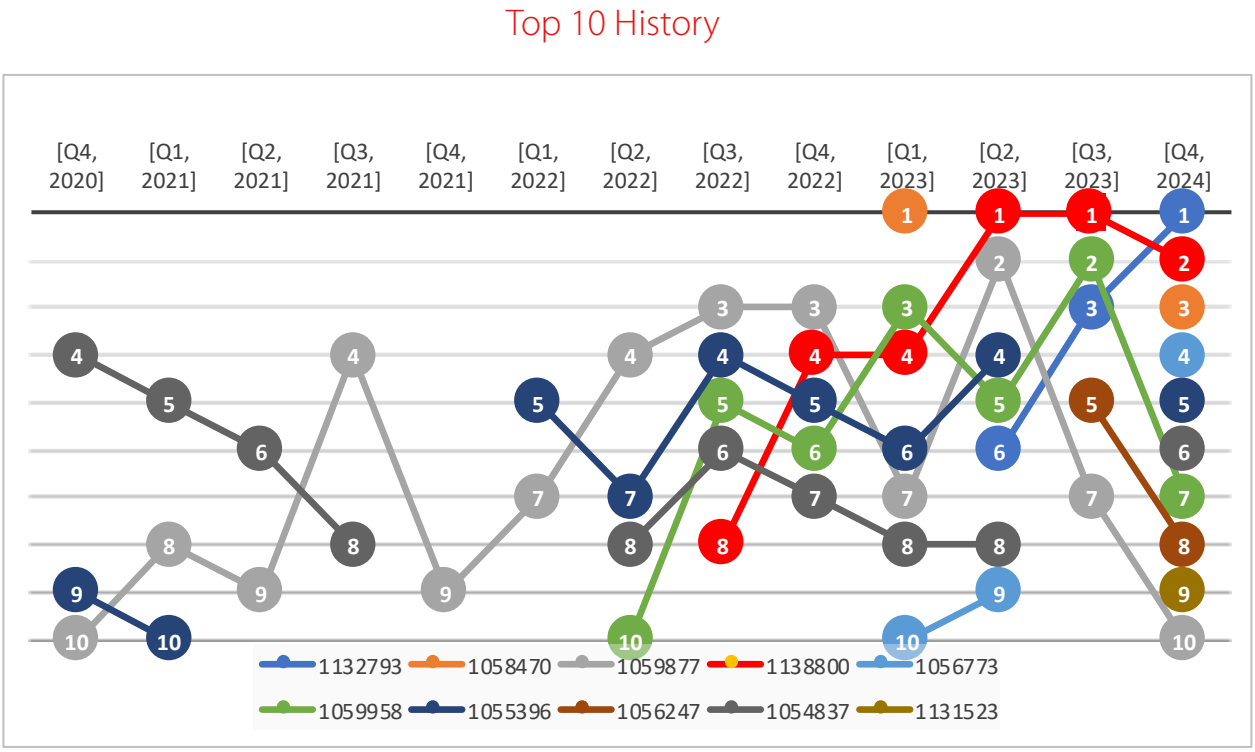


Figure 22. History of Prominent Signatures in the Top 10 Since Q2 2020

The top 10 history graphics display the longevity among our signatures that tend to quarter over quarter garner the most detections. Below are several noted signatures:

- Signature 1138800 (Red) is the ProxyLogon vulnerability. It fell to second place after holding first the previous two quarters. Even so, this signature holds a greater percentage of total volume this quarter since its inception.
- Signature 1132793 (Ocean Blue) for an SQL injection attack, it rose to first place this quarter. Our assumption is that the ATutor software (connected to this signature) is not the reason for the all these attacks, but instead targeting other systems vulnerable to SQL injections attacks.
- Signature 1059877 (Light Grey) is the directory traversal attack affecting a wide-range of IT software's.

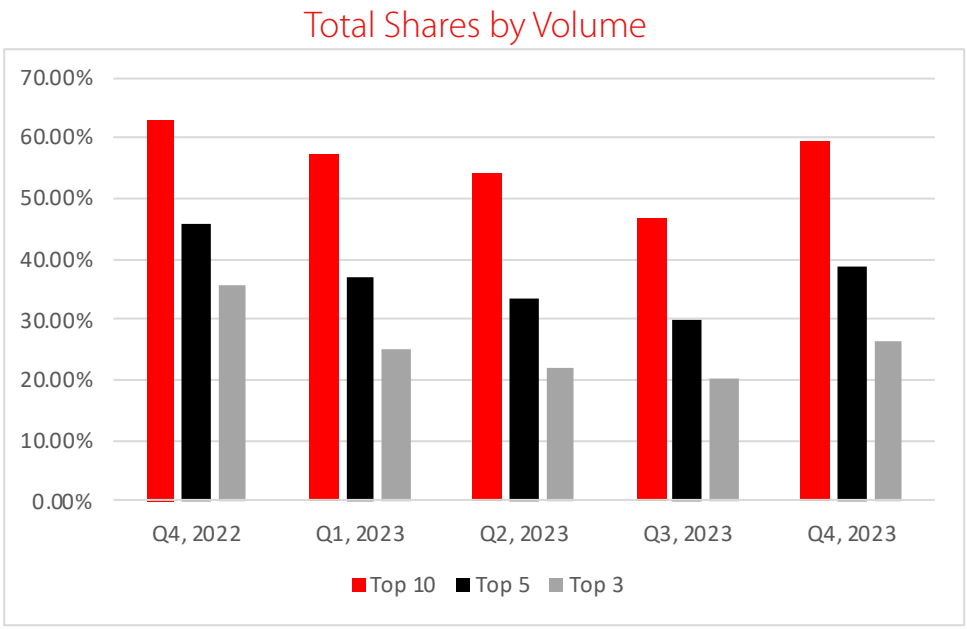


Figure 23. Total Share of Top Signatures by Volume Combined

Trends were reversed this quarter as the top signatures by volume accumulated a larger percentage of total detections. It remains to be seen if this is a blip, or whether top-heavy signatures will always remain a high concentration of total detections. The top 10 went from nearly 47% last quarter to nearly 60% this quarter. It is still way below the 80-86% range between 2021-2022. We show this chart so readers can grasp how IPS detections tend to accumulate to a small subset signature. That is, detected by all telemetry-enrolled Fireboxes. When there are juicy targets such as Microsoft Server and Exchange, it makes sense for those related signatures to garner the most detections.

Signature	Type	Name	Affected OS	Rank
1055435	Web threats	WEB Apache Struts 2 OGNL Script Injection -4	Windows	40
1133696	Buffer Overflow	WEB Microsoft IIS WebDAV ScStoragePath-FromUrl Buffer Overflow -2 (CVE-2017-7269)	Windows, Linux, FreeBSD, Solaris, macOS	44
1130593	Web threats	WEB Microsoft IIS HTTP.sys Remote Code Execution Vulnerability (CVE-2015-1635)	Windows	47

Figure 24. New Signatures in the Top 50 (Excluding Top 10) this Quarter

New Signatures in the Top 50

Among the 451 unique detections this quarter, the top 50 signatures by volume represented 92.02% of total signature detections. While an individual top 10 signature usually represents 3-10% of total volume, many of the top 50 represent at least 1%, which isn't significant. Due to the number of signatures, we are focusing on the new ones. As we mentioned at the beginning of the IPS section, these are "new" in that they have never been among the top 50 signatures by volume. They could very well be a 10-year-old vulnerability, or perhaps a more recent one. This quarter had three new signatures.

Signature 1055435

This is connected to two CVEs published in 2012 for Apache Struts 2, an open-source framework for Java EE web applications. Researcher Bruce Phillips published a blog post in February 2011 concerning these and several other vulnerabilities. We can see in addition to the two CVEs, CVE-2012-0391 and CVE-2012-0392, that CVE-2012-0393 and CVE-2012-0394 were published in connection to the underlying issue as well.

While the software had security protections in place, they could still be bypassed and vulnerable to remote code execution and arbitrary file overwriting. They both had sanitized inputs prevention in place, and preventive presets against calling arbitrary methods. The problem involved Object-Graph Navigation Language (OGNL), which is integrated into Java for changing property values. The OGNL value is not filtered, so when the ExceptionDelegator component receives an OGNL value, an attacker could easily include malicious Java code for remote code execution. The other vulnerability associated with this signature is the CookieInterceptor since it didn't use the acceptedParamNames filter to handle cookie name values. The other two vulnerabilities are from the Parameter-Interceptor component and DebuggingInterceptor component.

The recommendation from Apache Struts 2 is to update to Struts 2.3.18 and apply stronger acceptedParamNames filters to several of the components already mentioned.

CVE-2012-0391 – January 8, 2012 ← Directly connected to signature

CVE -2012-0392 – January 8, 2012 ← Directly connected to signature

CVE-2012-0393 – January 8, 2012

CVE-2012-0394 – January 8, 2012

Apache Struts 2 Security Bulletin

Signature 1133696

This is a 2017 critical buffer overflow vulnerability for Internet Information Services (IIS) 6.0 in Microsoft Windows Server 2003 R2. The ScStoragePathFromUrl function in the WebDAV service of IIS can be exploited by executing malicious code in a PROPFIND (URI-based) request header that begins with "If: <http://". This affects both 32-bit and 64-bit Microsoft Windows Server 2003 R2. This all depends on whether the attacker can elevate their privileges to compromise the system. An in-depth post on this can be found on the 0patch Blog. They mentioned in 2017 that there were over 600,000 accessible IIS 6.0 servers at the time, with an estimate 10% of those with WebDAV enabled. The small number is due to WebDAV not being enabled by default.

Of the total public IIS 6.0 servers currently online, Shodan shows that over 85,000 are still publicly web-facing. If 10% of the devices have WebDAV enabled, then there are still 8,500 vulnerable servers. This doesn't consider servers hidden away in private networks. As can be seen in figure 24, the US leads with over 31,000 public servers, followed by nearly 15,000 for China, and fourteen countries with 1000-2000 exposed servers. As with any unmaintained software, using an array of security tools is necessary for protecting a product that is ripe for exploitation. There are companies such as 0patch and others that offer outside-of-vendor patches for this vulnerability, but there are many more patches (for different vulnerabilities) needed for a very outdated product. That is why it is best to shut down any publicly exposed servers and find ways to ensure that your server is as isolated as possible within your organization's environment.

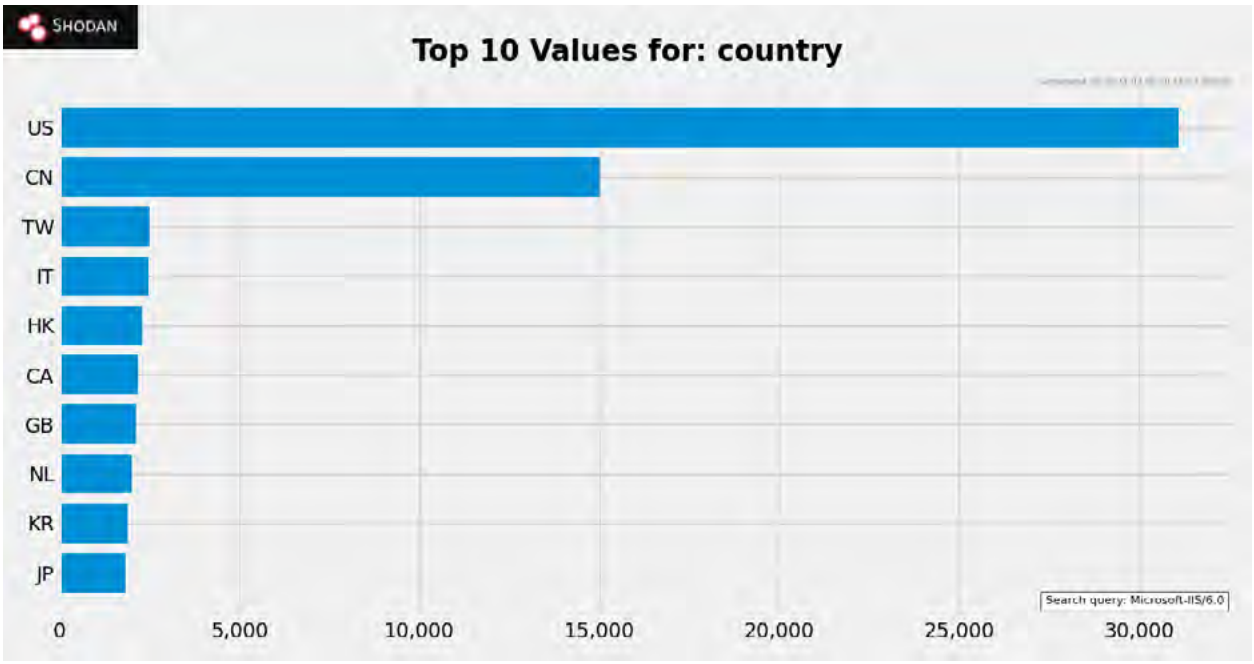


Figure 25. Countries with IIS 6.0 Installed in March 2024

Signature 1130593

Another IIS-related signature, this time for a remote code execution vulnerability in the HTTP protocol stack, due to how HTTP.sys handles data. Hypertext Transfer Protocol Stack (HTTP.sys) is the HTTP/S go-between for IIS. The listener receives an HTTP/S request and sends it to IIS for processing, and awaits a response from IIS. It then relays that back to the browser. Microsoft published the CVE-2015-1635 for this HTTP.sys vulnerability and recommended updating for Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2.

Most-Widespread Network Attacks

Most-widespread network attacks are attack signatures that the most unique Fireboxes detect during the quarter. This section shows the threats that the average Firebox is defending against on a global scale. In first place, signature 1131523 has kept the same spot for a second consecutive quarter. We already discussed this signature as it is in the top 10 for the first time this quarter. It is a Microsoft Internet Explorer memory corruption vulnerability, and to no surprise is a technology as widespread as can be, even with its deprecation and replacement to Microsoft Edge. Signature 1059877 has been the longest running signature in the top 5 most-widespread since Q2, 2022.

Signature 1138800 (ProxyLogon) has been present in the top 5 most-widespread signatures since Q4 2022, except during Q2 2023. It has risen to second place among the most-widespread. That is in conjunction with it increasing in total volume 8.37% of all detections, the highest since we began tracking it. It has been mentioned already in the IPS section, and repeatedly in prior Internet Security Reports, but if you don't update your Microsoft assets, in this case Windows Exchange, then you at least need to address how you'll protect the asset.

Attackers seek big prizes and Microsoft products are often at the center of their exploit path. That brings us to two new signatures this quarter. Signature 1139539 and 1231674, in fourth and fifth place respectively. Last quarter we wrote in detail on signature 1231674, as it was totally new among the top 50 signatures we track. One signature is related to ProxyShell and the other ProxyNotShell. As ProxyLogon, ProxyShell, and ProxyNotShell names are confusing to read through, we'll try to lay it out in a clean format:

Signature 1138800 – ProxyLogon

Affects On-Premises and Hybrid environments for Exchange Server 2010, 2013, 2016, and 2019.

CVE-2021-26855 – March 2, 2021 ← Directly connected to signature

CVE-2021-26857 – March 2, 2021

CVE-2021-26858 – March 2, 2021

CVE-2021-27065 – March 2, 2021

Microsoft Guidance

Signature 1139539 (and Signature 1139536) – ProxyShell

Affects On-Premises and Hybrid environments for Exchange Server 2013, 2016, and 2019.

CVE-2021-31207 – May 11, 2021

CVE-2021-34473 – July 13, 2021 ← Directly connected to both signatures

CVE-2021-34523 – July 13, 2021

Microsoft Exchange Blog Post

Signature 1231674 – ProxyNotShell
Affects On-Premises and Hybrid environments for Exchange Server 2013, 2016, and 2019.

CVE-2022-41040 – September 30, 2022 ← Directly connected to signature

CVE-2022-41082 – September 30, 2022

Microsoft Guidance and Microsoft Analyses

We included signature 1139536 as it represents the same vulnerabilities as signature 1139539 but happens to have a different signature name. It isn't uncommon to see this. Signature 1139536 is the 8th most-widespread (though not shown in the table). Combined, it may have come out higher in the most-widespread signature rankings.

ProxyLogon, ProxyShell, and ProxyNotShell are all from Exchange Server vulnerabilities. All the Microsoft publications related to these Proxy vulnerabilities recommend updating servers immediately.

Signature	Name	Top 3 Countries by %			AMER %	EMEA %	APAC %
1131523	WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability -2 (CVE-2015-2425)	UK 65.44%	USA 61.62%	France 59.08%	56.94%	53.14%	47.08%
1138800	WEB Microsoft Exchange Server Remote Code Execution Vulnerability -6 (CVE-2021-26855)	Germany 21.51%	Portugal 21.10%	Canada 15.71%	10.19%	13.85%	10.51%
1059877	WEB Directory Traversal -8	Germany 19.42%	Portugal 18.35%	Australia 14.02%	9.18%	13.80%	14.40%
1139539	WEB Microsoft Exchange ProxyShell -3 (CVE-2021-34473)	Germany 18.62%	Portugal 11.93%	Australia 8.41%	5.48%	11.79%	7.39%
1231674	WEB Microsoft Exchange EwsAutodiscover-ProxyRequestHandler SSRF(CVE-2022-41040)	Portugal 15.60%	Germany 14.44%	Canada 13.09%	7.56%	9.56%	5.84%

Figure 26. Top 5 Most-Widespread Network Attacks

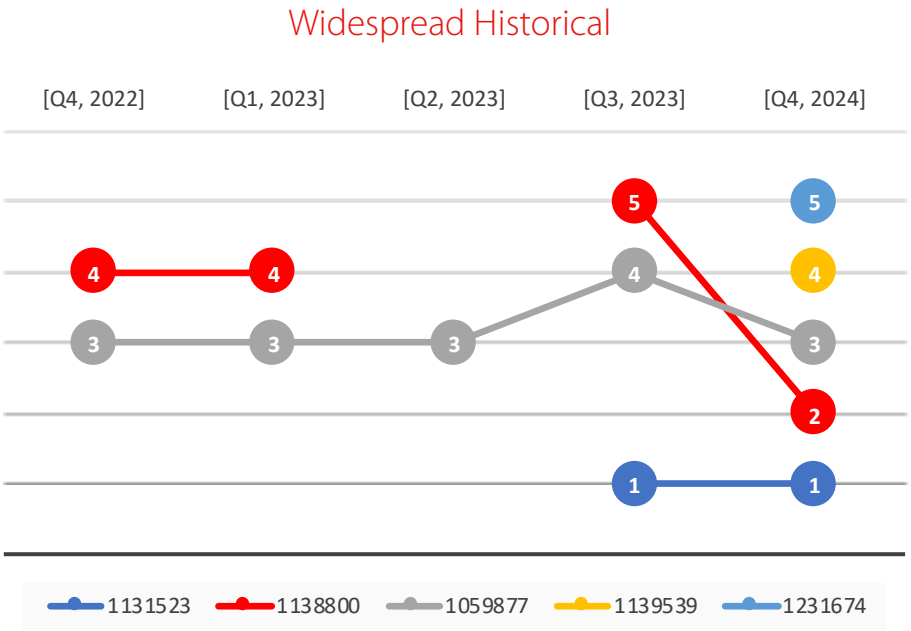


Figure 27. History of Prominent Widespread Signatures since Q4 2022

We have added a widespread historical graph for the first time. Figure 27 shows the signatures in the top 5 this quarter and their presence since Q4 2022. Figure 28 below shows over two years of the top signatures since Q4 2021, including signatures that have been absent for one or more quarters. In a similar rational for displaying the top 10 history, we include these charts to show how enduring certain signatures can be due to the vulnerabilities' widespread reach. That is on display as four of the five signatures are Microsoft-related. It wasn't until this quarter that two long-lasting signatures disappeared from the top 5 such as 1130592 (green, second place in Q3 2023) a buffer overflow vulnerability, and 1110932 (dark blue, third place in Q3 2023), a 2009 GDI+ buffer overflow vulnerability in a wide array of Microsoft products.

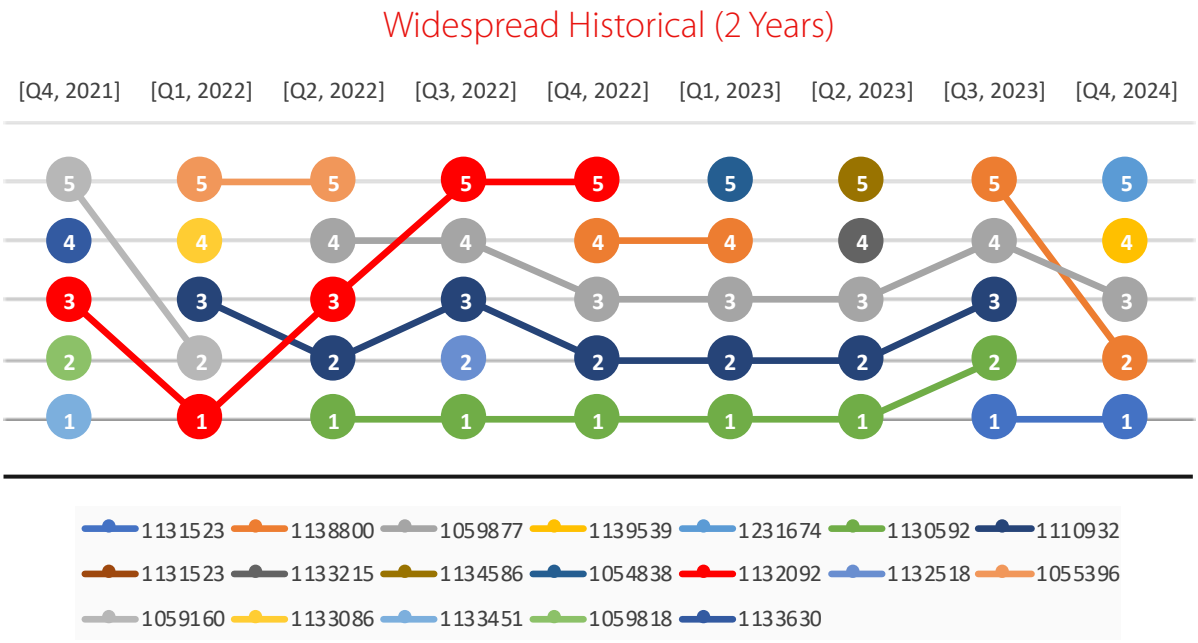


Figure 28. History of prominent widespread signatures since Q4 2021

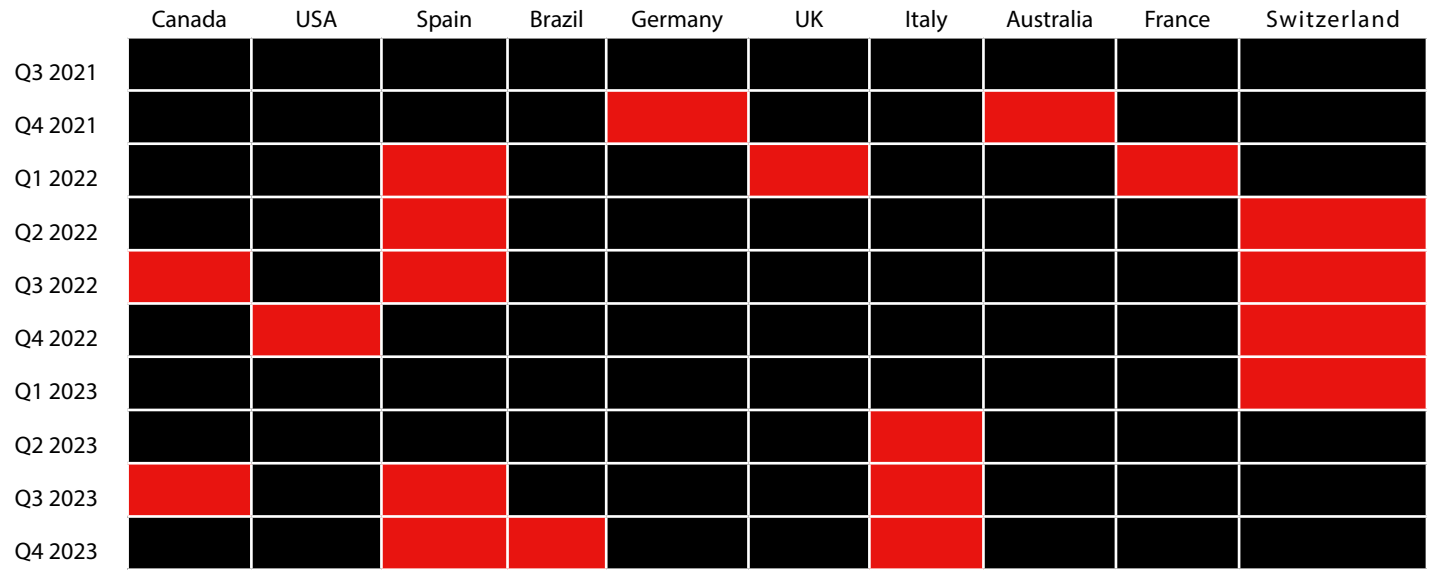
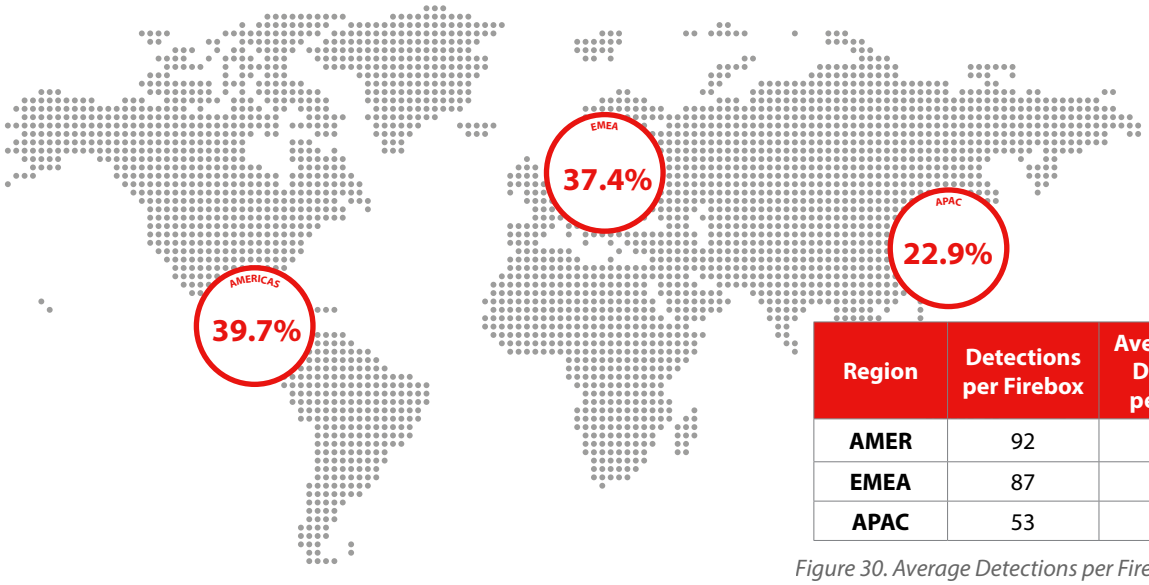


Figure 29. Countries listed among one or more widespread attack signatures who were most affected

The countries listed in Figure 29 were one of the most-affected per widespread signature. We list the top three countries per signatures and highlight it in green on this chart. Red is used when it isn't present for that quarter. Countries that are relatively wealthy and with a common world language continue to be the leading destination for the most-widespread network-based attacks. If you look at the most-widespread signature table on Figure 26, you will notice a concentration of a few countries. That is noticeably Germany and Portugal. Each was present in four out of five of the signatures. Previous quarters they were often in only two or three signatures. Pointing out this fact does not mean we have a causal explanation for it. At minimum, organizations operating in those countries should be on notice that attack patterns are heavily directed at them.



Region	Detections per Firebox	Average % IPS Detections per Firebox
AMER	92	39.70%
EMEA	87	37.41%
APAC	53	22.89%

Figure 30. Average Detections per Firebox by Region

Network Attacks By Region

WatchGuard has a greater install base in AMER and EMEA regions, and many countries within these regions remain prime targets against ransomware groups and other malicious actors. This causes data to skew heavily to AMER and EMEA regions. EMEA traffic is three times that of AMER this quarter and has been like that in previous quarters. But only going back a year, we did have relatively balanced numbers between AMER and EMEA. Further back in 2022, APAC numbers were sometimes a quarter to half the size of the other regions, while presently they are dwarfed by AMER and EMEA. Therefore, we normalize the data to reflect actual average detections per regional Fireboxes instead of just using a sole number among all regions.

Detections among all regions were 87 per Firebox this quarter. Coincidentally, EMEA arrived at the same figure. Additionally, the gap in detections is closing between AMER and EMEA, though it may only be temporary. Last quarter the numbers were more balanced among all three regions with APAC having a higher average detections per Firebox than EMEA. These can be seen in Figure 31, as well display of percentage balance between regions on Figure 32.

This quarter had an 8.14% increase in Firebox IPS telemetry enrollment with much of the increase coming from EMEA Fireboxes. Even so, the increase in EMEA Fireboxes did not result in an increase in average detection due to the normalization of data. In total, the average increase in Firebox IPS telemetry enrollment is 0.84% since Q4 2021. When we have around an 8% upswing this quarter, a 12% downswing in Q1 2022, or a near 0% change in Q2 2023, it shows that the relatively stable number of enrolled Fireboxes isn't static. Many organizations choose to unenroll or enroll for one reason or another. Therefore, when we look at this data during this quarter compared to Q4 in 2022, the subset of customers could be quite different. For this reason, we are cautious about making inferences on data that is continually changing – although we still do make them.

One common inference that can be made is that the Christian holiday schedule aligns to where many of our customers are based, hence the increased traffic during Q4, the same as Q4 last year. Even though EMEA covers the Arabic region, our customer base is weightier in Europe. The numbers show a clear picture of this in Figure 30.

Average per Firebox Detections by Region

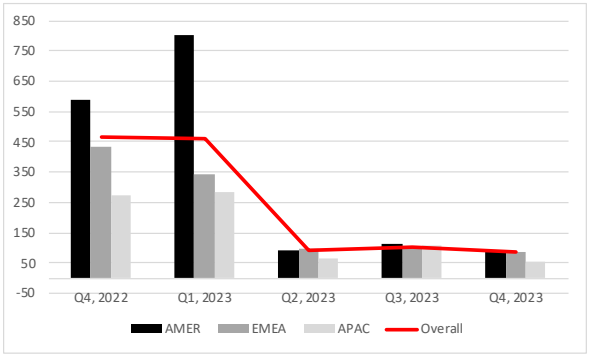


Figure 31. Average Detections per Firebox by Region since Q4 2022

Detections Percentage by Region

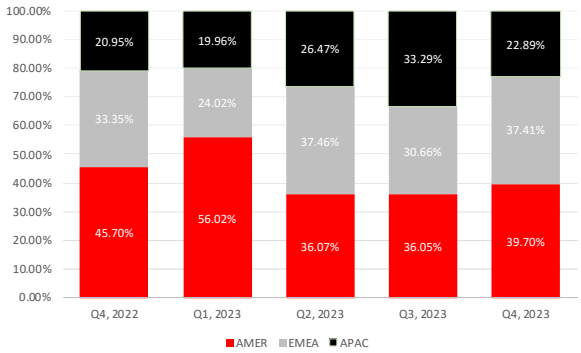


Figure 32. Average Detections per Firebox by Region

Conclusion

The Intrusion Prevention Service, while a simple defensive solution, is one that works. With an actively updated database of known attacks, it stopped over 470,000 attempted intrusions (of telemetry-enrolled devices) this quarter. Microsoft products continue to be a major target. That won't change in our lifetime, probably? Several of our top signatures are associated with old and no-longer-maintained software. Chances are those signatures are targeting an expansive number of products with the same underlying vulnerability. Still, we know there is outdated ATutor and Quagga software continuing to be used. Shodan vouched for that. So, try to do the best you can with what software your organization continues to host. If it's an ancient version of IIS, then at least our network security product can be of use.

DNS ANALYSIS

Attackers like to register malicious domains that deviate from their legitimate siblings by just a single character or a slight misspelling. Sometimes they can even leverage legitimate domains like sharepoint.com and register their own subdomains to host malicious content. These techniques can make it exceptionally difficult for victims to spot malicious links, meaning organizations must rely on technical controls to block connections when a user clicks. DNSWatch works by analyzing DNS requests from protected endpoints and redirecting malicious connections to a safe blackhole instead of the attacker's servers. In this section, we will review the top malicious domains WatchGuard DNSWatch customers encountered in Q4 2023.

Top Malware Domains

Malware domains are malicious domains that either hosted malware or were involved in the malware command and control infrastructure. Detections in this category can come from users clicking on links to malicious files or even infected devices secretly beaconing back home to attacker-owned servers.

Malware
b410n0l2k4j3a[.]cc *
carsfootyelo[.]com
t[.]hwqloan[.]co
t[.]zz3r0[.]com
mapdatamsna[.]info*
mapdatamsnb[.]info*
mapdatamsnc[.]info*
mapdatamsnd[.]info*
pixel-install[.]me*
get[.]promsmotion[.]com*

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 33. Top Malware Domains

There were seven new malicious domains in the top malware domains list in Q4 2023, though four of them share a close relationship to each other. Starting with those, mapdatamnsna[.]info through mapdatamsnd[.]info initially made it onto our block list in August of last year after another security vendor identified them as associated with a malicious DNS tunneling campaign. You may remember four different domains from the same campaign that made the list in Q3 2023.

Another new addition was b410n012k4j3a[.]cc, which we originally added in 2018 after finding it associated with malware and spyware delivery campaigns. The domain remains under control of an adversary and in active use, even nearly six years after we initially discovered it.

The sixth new domain, pixel-install[.]me, is associated with a malvertising campaign that leverages malicious advertisements to redirect users to graphic content and even a Flubot malware campaign at one point. We've seen the malvertising campaign hosted on both traditional websites and even with ads hosted within mobile games.

The final new malware domain from the quarter was get[.]promsmotion[.]com. We added this domain in October 2023 after finding it hosting a Balada malware campaign. The Balada Injector has been active since 2017 but became more prominent in 2023 after its operators compromised over 1 million vulnerable WordPress websites by leveraging worm-like auto propagation across the Internet.

Top Compromised Domains

Compromised domains are legitimate websites that threat actors have compromised to host illegitimate content. Attackers typically exploit a vulnerability in the underlying content platform like WordPress or Drupal that lets them upload their own files and create their own pages. They'll typically leave the existing website undisturbed and hide their malicious content on un-linked child pages. In Q4 2023, we had one new addition to the top 10 list.

Compromised
ssp[.]adriver[.]ru
www[.]sharebutton[.]co
www[.]granerx[.]com
archive[.]org
wieczniezywechoinki[.]pl*
1[.]top4top[.]net
stopify[.]co
dinatds[.]com
granerx[.]com
dodgersdigest[.]com

Figure 34. Top Compromised Domains

The only previously unseen (at least in the top 10 list) in Q3 2024 was wieczniezywechoinki[.]pl. We added this domain in February 2019 after finding a malicious page hosting a phish that leveraged a fake phishing invoice as the lure.

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
unitednations-my[.]sharepoint[.]com
ulmoyc[.]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*
googlestates[.]com

Figure 35. Top phishing domains

The only new addition this quarter, agzagope-my[.]sharepoint[.]com, continues a noticeable trend where adversaries leverage the legitimate SharePoint file and site-hosting services to deliver malicious content. We added this particular domain to our threat feed back in 2020 after finding it hosting a DHL shipping notification phish. Adversaries use legitimate services like SharePoint to benefit by the otherwise good reputation of the parent domain while delivering malicious content.

Conclusion

Cyber threat actors have multiple techniques available to them to mask their attacks from unsuspecting victims. While social engineering training is still an important pillar of a resilient cyber defense, technical controls like DNS firewalling services are still necessary to fill in where user training fails.

Generative AI continues to fuel growth in spear phishing at scale, which means organizations must deploy a layered defense to defend against social engineering and malware attacks.

FIREBOX FEED: DEFENSE LEARNINGS

The solar eclipse that will go through the US, Mexico, and Canda will only last a few minutes in the right areas. If one doesn't know about this event than they wouldn't be ready and might miss it. The only damage from missing the solar eclipse is missing a fantastic show, but if we miss one network attack, open one fake phishing attachment, or enter our credentials into tone wrong form, then we will pay the price. By understanding the threat landscape and knowing whats coming, you can increase your cyber resilience and be better defended against adversaries. Here's some specific tips to adopt so you can be prepared.

01 AI-based Antivirus Picks Up on What Signatures Miss

Web-based malware like malvertisments, credential stealers, and coinminers all use obfuscated code. When users visit these websites, it can be difficult for basic anti-malware tools to determine if a website contains malicious code, especially well-crafted code. Humans can sometimes identify these nefarious websites if we see a misspelling, or if the format looks off but this can be difficult to identify especially if we visit a new webpage. With advanced AI-based anti-malware engines like IntelligentAV, we don't need to know specifically what the code does, we only need to know that the page is trying to hide something. AI-based anti-malware engines can even identify obfuscated code and block it if necessary. Leveraging these advanced tools can help keep users safe as they go about their work day.

02 Avoid End-Of-Life Software

We constantly see Microsoft products targeted by threat actors, especially Windows Server and Microsoft Exchange. In this report we even saw malicious hackers targeting old End-of-Life (EOL) Microsoft software too. Why do we see so many attacks on old software? Attackers know some businesses still use old EOL software and exploits for old software become more widely available as time goes on. This results in nefarious but low-skilled hackers who don't know how to exploit the latest threats using prewritten scripts for exploitation. Script kiddies, as we sometimes call them, make up much of the networks attacks and malware because it takes very low effort to create the attack. This is why we don't recommend using software that's EOL even for a short time. If you must use it than you should have additional security measures to protect it until you can upgrade to a secure software package.

03 All Servers Need the Same Quality Protection

Over the last year we have seen an increase in Linux-based malware attacks on servers to turn them into coinminers for the cryptocurrency Monero. Monero coin doesn't use the graphics card to mine like most other cryptocurrencies so Linux servers that use a high-powered processor become valuable targets for the coinminer to exploit and mine Monero. The malware will also worm through the network if administrators don't adopt sufficient safeguards. Keep your Linux servers safe using the same standards we use on Windows servers. This includes adopting zero trust practices like segmenting the network, protecting credentials to access these servers, and using a layered defense to ensure no malware makes it through to infect the server.

ENDPOINT THREAT TRENDS

It's the final endpoint iteration for 2023, and it's back with only a few minor edits and additions from Q3. We have made a few tweaks by adding a new table in the Attack Vectors section and altering the MITRE Tactics and Techniques table and the Alerts by Top 30 Countries map. We also made a minor tweak in representing malware frequency, but we will get to that soon since that is the first subsection. Those are the only significant differences from Q3 to Q4. Here's what you can expect this quarter:

- Total unique malware threats
- Brand new threats blocked per 100k active machines
- Number of alerts by the number of machines affected
- Ratio of the number of alerts over the number of machines for each country (alert coefficient), showing the top 30 affected countries each quarter
- Top 10 most prevalent malware
- Top 10 most prevalent potentially unwanted programs (PUPs)
- Number of alerts by which WatchGuard technology invoked the alert
- Attack vectors
- Browser-based detections
- Alerts by exploit type
- (Threat hunting) MITRE ATT&CK tactics and techniques
- Firebox ransomware detections
- Ransomware group double extortions
- Notable ransomware breaches

The data for this section comes from WatchGuard EPDR (also known as Panda AD 360) detectors worldwide. We hope this report helps you understand current attacks and trends and how EPDR defends against the latest malware campaigns. Without further ado, the Endpoint section begins with the malware frequency on endpoints.

MALWARE FREQUENCY

We measure malware frequency in two ways. The first measures the total malware threats WatchGuard EPDR customers faced, commonly called the "raw" total, including both old and new malware. This summation counts the number of unique hashes that EPDR classified as malware for the quarter. For this specific data piece, we've moved away from representing this number as "per 100k active machines." Representing it this way was confusing, and we've rectified that issue.

The second measurement is the uniqueness of attacks on endpoints, which is the number of never-before-seen threats, or hashes, we observe. This number is still represented using "per 100k active machines" In lay terms, the first measurement is the total number of unique threats (unique MD5s) in Q4; the other is brand-new threats (unique MD5s we've never seen before). This two-pronged view allows us to view frequency by the two U's – ubiquity and uniqueness.

Unique Attacks Blocked per 100k Active Machines	95,586

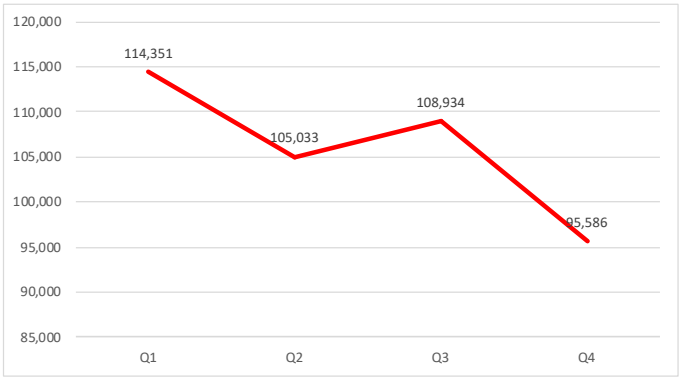


Figure 36: 2023 QoQ Total Malware Threats

In the final quarter of 2023, we observed a further reduction in new malware threats, with 95,586. That is a 12.25% decrease from Q3. On the surface, these numbers are great! However, don't digest these numbers in a vacuum. Historically, for WatchGuard, Q4 tends to be the quarter with the least malicious activity for endpoints, with Q2 being a close second. Furthermore, improvements in other products, such as email security and training, prevent malware from getting onto endpoint systems. Malware has decreased throughout the year, but it's vital to extrapolate other contexts in this report's overall threat landscape. Don't get complacent!

New Threats Blocked per 100k Active Machines	108

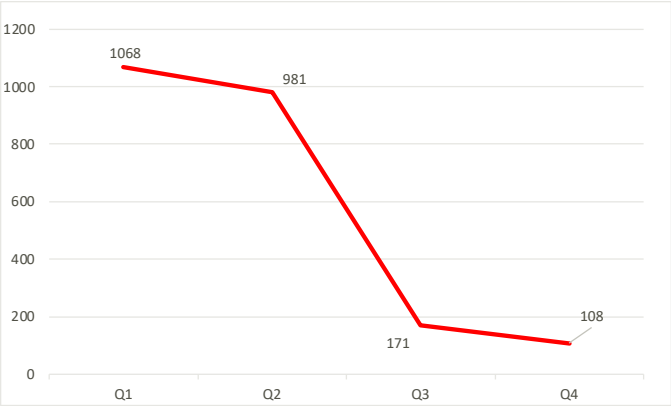


Figure 37. 2023 QoQ New Threats Blocked per 100k Active Machines

The most important thing to remember for the frequency data shown for the New Threats Blocked Per 100k Active Machines is that these represent the never-before-seen MD5 hashes. Furthermore, we represent new threats "per 100k active machines," allowing us to replicate a large organization and understand how many new threats they would have observed.

In Q4, we observed 108 brand-new threats per 100k active machines. This is a further reduction of 36.84% from the quarter prior, which was 171 per 100k active machines. From Q2 to Q3, we saw a steep decrease in unique malware hash observations (-82.57%), and the numbers remain down at those levels, as you can see in the following figure. Interestingly, our threat-hunting rules triggered significantly more in Q4 than in Q3, but we observed decreased detections. This could suggest our threat-hunting rules are catching more PUPs or false positives. We will continue to monitor these developments.

Alerts by Number of Machines Affected

The Malware Frequency section unveils the overall malware we see, and the rest of the subsections are ways of looking at this data through different lenses. For example, the Alerts by Number of Machines Affected section filters the overall malware frequency by how many machines each threat appeared on. This means that if a malicious sample appeared on only one machine throughout the quarter, the 1 counter would increase. If a threat appeared on 15 machines, the >=2 & <50 counter would increase. Typically, threats that appear on many machines are large malware email phishing campaigns with malicious attachments or obscure links that download malware. Unfortunately, these campaigns have several potential victims per campaign. We block these and categorize them appropriately.

Alerts by Number of Machines Affected

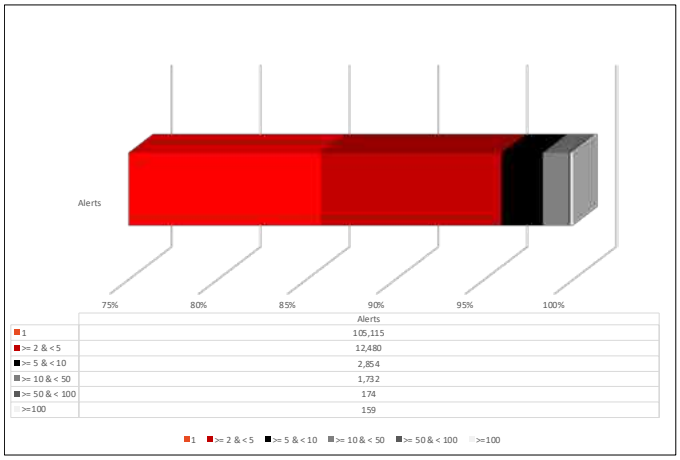


Figure 38. Alerts by Number of Machines Affected

The bullet points below define and describe the parameters for which we log this data:

- **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 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 Q3 except for threats affecting two and five machines. You can observe the differences in the table.

Number of Machines	Q3 Alerts	Q4 Alerts	Difference from Q3	Percentage Difference from Q3
1	121,468	105,115	-16,353	-13.46%
>= 2 & < 5	12,034	12,480	446	3.71%
>= 5 & < 10	2,894	2,854	-40	-1.38%
>= 10 & < 50	2,013	1,732	-281	-13.96%
>= 50 & < 100	235	174	-61	-25.96%
>=100	180	159	-21	-11.67%

Figure 39. Alerts by Number of Machines Affected

Alerts by Top 30 Countries Affected

This section observes malware frequency by country. We can't just display the raw frequency by country and interpret it that way because WatchGuard has Fireboxes and endpoint solutions globally, with some countries having significantly more of these solutions than others. Therefore, to ensure we interpret each country equally, we have derived what we call the Alert Coefficient (AC), which is the total malware and PUPs per active machine. For example, Grenada had an AC of 1.00. That means that, on average, there was at least one malware or PUP per active machine in that country. Saudi Arabia had an AC of 0.50, meaning, on average, there was about one malware or PUP per two active machines. So on and so forth. The higher the ratio of malware and PUPs to active machines, the higher the AC.

Regarding the top 30 AC rankings, there were quite a few changes from Q3 to Q4. The top-ranked country this quarter, Sao Tome and Principe, moved up 11 rankings from the quarter prior with a record-breaking 7.14 AC. The country that moved up most in the rankings was Trinidad and Tobago, moving up 16 spots from the quarter prior. The country that moved down the most was Jordan, moving down 24 spots. Five countries appeared this quarter that didn't appear in the top 30 from Q3: Grenada, Saudi Arabia, Thailand, Cyprus, and Bulgaria. You can see those and the other countries in the top 30 ranking table and corresponding map, which we've revised with a black background to make it easier to discern the countries.

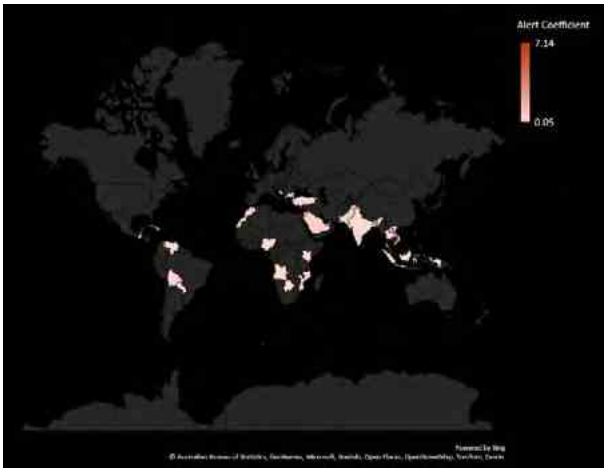


Figure 40. Alerts by Top 30 Countries Affected

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 41. Alerts by Top 30 Countries Affected (with QoQ Differences)

TOP MALWARE AND PUPS

The Top Malware and PUPs section is a favorite among readers and researchers. We show the top 10 most prevalent malware and PUPs from Q4. What we mean by the most prevalent is the MD5 hash on the most machines. That means that if the same hash appeared on a system twice, we wouldn't count it. For example, if we had 400 alerts for an MD5 hash associated with Agent Tesla, but 15 of those alerts appeared on a machine it had already been on, we wouldn't count it, and the alert count would be 385. Let's see what appeared the most this quarter.

Top 10 Most Prevalent Malware

Surprisingly, the most prevalent malware in Q4 was the same as last quarter. Even more surprising is that this same malware sample was the second most prevalent in Q2. It's evident that Glupteba, and this specific sample precisely, has been a nuisance throughout the year. However, EPDR has been blocking this sample for as long as we've known about it. Glupteba didn't appear again in the top 10 list for this quarter.

Another reoccurring malware from the previous quarters is MyloBot. We believe this specific MyloBot sample delivers Khalesi, but EPDR prevents MyloBot from running, and thus, Khalesi wouldn't run either. The Glupteba and MyloBot samples are the only two repeats in the top 10 for Q4.

Sometimes, we observe malware families in the top 10 multiple times. Q4 is no exception, having two malware families in the top 10 numerous times. GuLoader, which always makes the top 10, appeared five times, and Agent Tesla appeared three times. Two of the Guloader samples delivered Agent Tesla, showing a synergistic effect for those two in the top 10. GuLoader is a downloader, and Agent Tesla is an information stealer. So, seeing these two in the same toolkit for threat actors is common. A new malware appearing in Q4 is Conficker, which you can read the description about in the definitions below.

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.

Conficker

Conficker is a worm that 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).

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.

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. This malware is a sample we cannot directly attribute to a particular family. 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.

GuLoader

This malware is sent in waves by attackers who send out 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.

MD5	Signature	Affected Machines per 100k	Classification Attestation
6CC8D5F1CB1819791E4897F902FAF365*	W97M/Downloader.DDE	1,281	Glupteba
FBD8778D87C08492EF10A95AC7C30612	Trj/WLT.F	937	Conficker
3E86685246C1FDCC9EEF8B95986BA4E4*	Trj/RnkBend.A	644	MyloBot delivering Khalesi
EFF4D5E54A097A08B7140E7BCA042102	Trj/Agent.JTM	341	Agent Tesla
7F45D3AE1250A354A3C0955E0414F9EC	Trj/GdSda.A	325	GuLoader delivering FormBook
A116A2037582A261B91F92F33407A934	Trj/CI.A	315	GuLoader delivering Agent Tesla
33F64AE22AA24D0DFFEBB22AA8EBBBBC	Trj/Agent.MK	307	GuLoader delivering Agent Tesla
C94A42B8695A8D1BE0CD2F74181A5540	Trj/Chgt.AD	296	GuLoader
E5386EC1666AFD49B7A21D15B32C923E	Trj/Chgt.AD	244	GuLoader delivering FormBook
2253836bb8b0b5479a1f77974b82b1f0	Trj/RnkBend.A	221	Unknown Malware (Injector)

Figure 42. Top 10 Most Prevalent Malware

*Seen last quarter

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.

Top 10 Most Prevalent PUPs

The most prevalent PUPs is arguably the most uneventful section for this quarter. Eight of the top 10 are repeats from the quarter prior, with the only two new additions being the third- and fourth-ranked files. The third-ranked file is an open-source AutoKMS tool that activates Windows licenses called KMS_VL_ALL_AIO. The fourth-ranked file is another open-source file, but this is a Mesh Service Agent application. This software allows users to remotely administer another machine, commonly used by threat actors to perform remote commands. See the description of each PUP signature below.

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.

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.

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.

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/RemoteAdmin

PUPs with the RemoteAdmin signature are those files that allow users to perform remote commands on another machine. Threat actors typically use these to perform remote malicious commands on victim machines to deploy more malware or steal data. Some of the most common RemoteAdmin tools are AnyDesk, TeamViewer, Total Commander, RAdmin, and there are many others.

MD5	Signature	Affected Machines per 100k	Classification Attestation
8D0C31D282CC9194791EA850041C6C45*	HackingTool/ AutoKMS	2,759	KMSPico
01C283988C93D390D4C81C38BF00ABEE*	PUP/BundleOffer	2,707	PDFCreator 5.1.2 Setup Wizard
2914300A6E0CDF7ED242505958AC0BB5	HackingTool/ AutoKMS	1,258	KMS_VL_ALL_AIO
E5ECC38FE9B2D29ADC9C871D8AB7D7D9	PUP/RemoteAdmin	1,256	Mesh Agent Service
1E2A99AE43D6365148D412B5DFEE0E1C*	PUP/BundleOffer	811	PDF Power 4.0.1.0 Setup Wizard
6A58B52B184715583CDA792B56A0A1ED*	Hacktool/ PortScanner	786	Advanced Port Scanner
30C7E8E918403B9247315249A8842CE5*	HackingTool/ AutoKMS	773	Unknown Software Installer
CFE1C391464C446099A5EB33276F6D57*	HackingTool/ AutoKMS	758	AutoPico
C9E4916575FC95BEDBD12415AB55CC84*	PUP/Hacktool	728	CVE-2014-0160 (Heartbleed) JavaScript Exploit Script
CD8AF8E8A07D6C58A500A23B501560B6*	PUP/Hacktool	717	Unknown Hacking Tool

Figure 43. Top 10 Most Prevalent PUPs

*Seen last quarter

Defense in Depth

For this section, we zoom out and look at alerts based on which technology invoked the alert. WatchGuard EDPR uses a defense-in-depth methodology (hence the section's name), which means redundancy and fail-safes for each line of defense, catching more malware using various techniques. The first line of defense is endpoint detection, followed by behavioral learning and Cloud, digital signatures, and defined rules. If it exceeds those, our analysts perform manual attestation to classify the file accordingly. We explain each of these technologies below:

- **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.

Looking at the bar graph in Figure 44 shows how each technology contributes to the overall EPDR solution. Endpoint Detection accounts for roughly half of all alerts. Following this, behavioral learning accounts for about one-fourth of all alerts. Then, the other four technologies comprise the rest of the alerts.

Specifically, Endpoint Detections comprised 52.14% of all alerts, and behavioral learning accounted for 20.01%. The other 27.85% of alerts were from the other four technologies. Not only does Endpoint Detection account for the most alerts, but it rose in the number of alerts from Q3 by 36.77%. Behavioral Learning, on the other hand, saw a reduction of 19.31% from the quarter prior. Cloud, Digital Signatures, and Defined Rules all saw increases from Q3, improving by 1.96%, 17.65%, and 8.09%, respectively. The Q4 Manual Attestation alerts count was similar to Q3 but slightly decreased at 0.35%.

ATTACK VECTORS

The Attack Vectors section is the longest-living section from the Endpoint portion of the report. We still use the same attack vectors (with a few additions) and the same pie graph to display the results. However, we've added a few enhancements here and there. As usual, we begin with the attack vector descriptions, including Acrobat, which has returned from being omitted in the last two quarters.

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.

Alerts by Technology

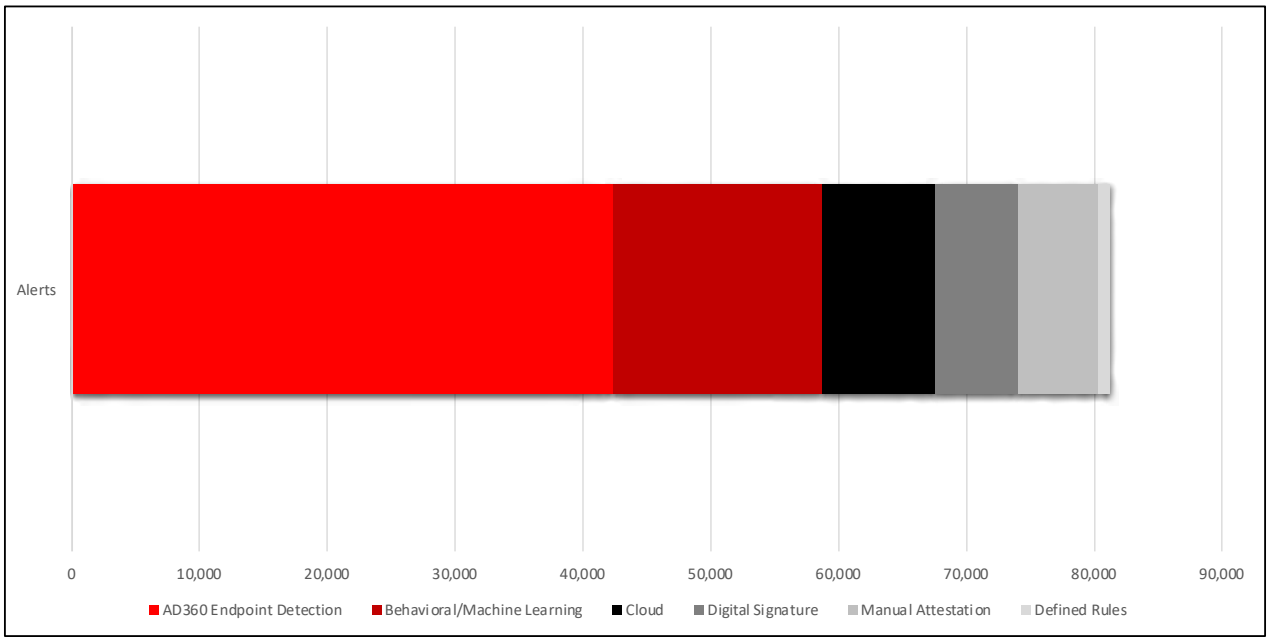


Figure 44. Alerts by Technology

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.

This quarter, the number of Acrobat alerts increased dramatically, and we forcefully had to reintroduce the attack vector again. In Q3, there were no Acrobat-based alerts; in Q4, that number increased to 692, as you can see in the table. Other than that, the number of alerts from each attack vector varied significantly for each. Scripts rose the most, up 77.26% from Q3. Browsers also rose significantly, up 56.56% from the quarter prior. Finally, the number of Office alerts rose 22.52%. By contrast, Windows and Other decreased -32.73% and -34.15%, respectively.

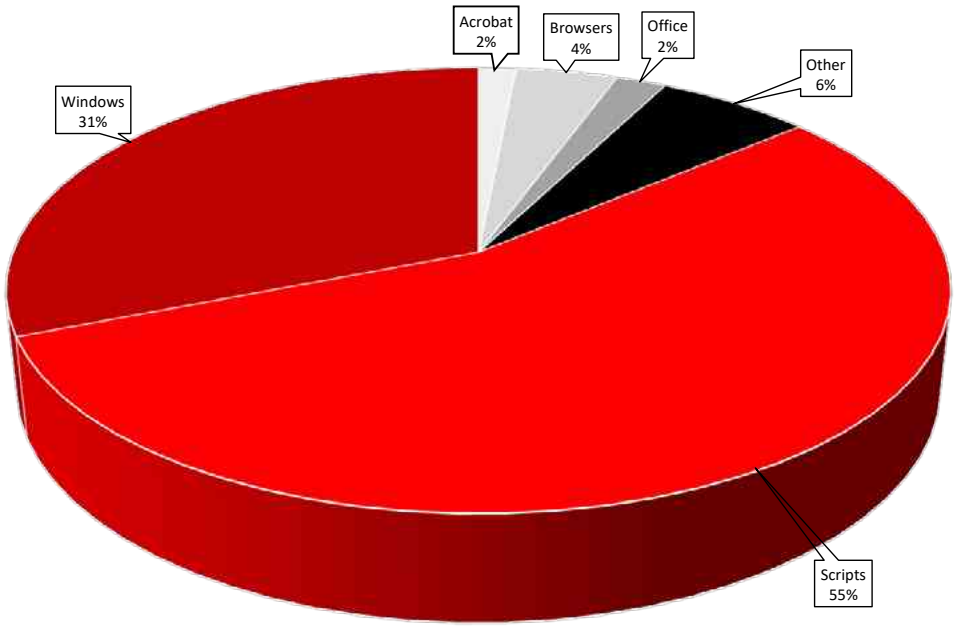


Figure 45. Top exploited software

Attack Vector	Q3 Count	Q4 Count	Raw Difference From Q3	Percentage Difference From Q3
Acrobat	0	692	692	n/a
Browsers	1,876	4,319	2,443	56.56%
Office	922	1,190	268	22.52%
Other	2,844	2,120	-724	-34.15%
Scripts	25,203	110,855	85,652	77.26%
Windows	14,152	10,662	-3,490	-32.73%

Figure 46. Attack Vectors

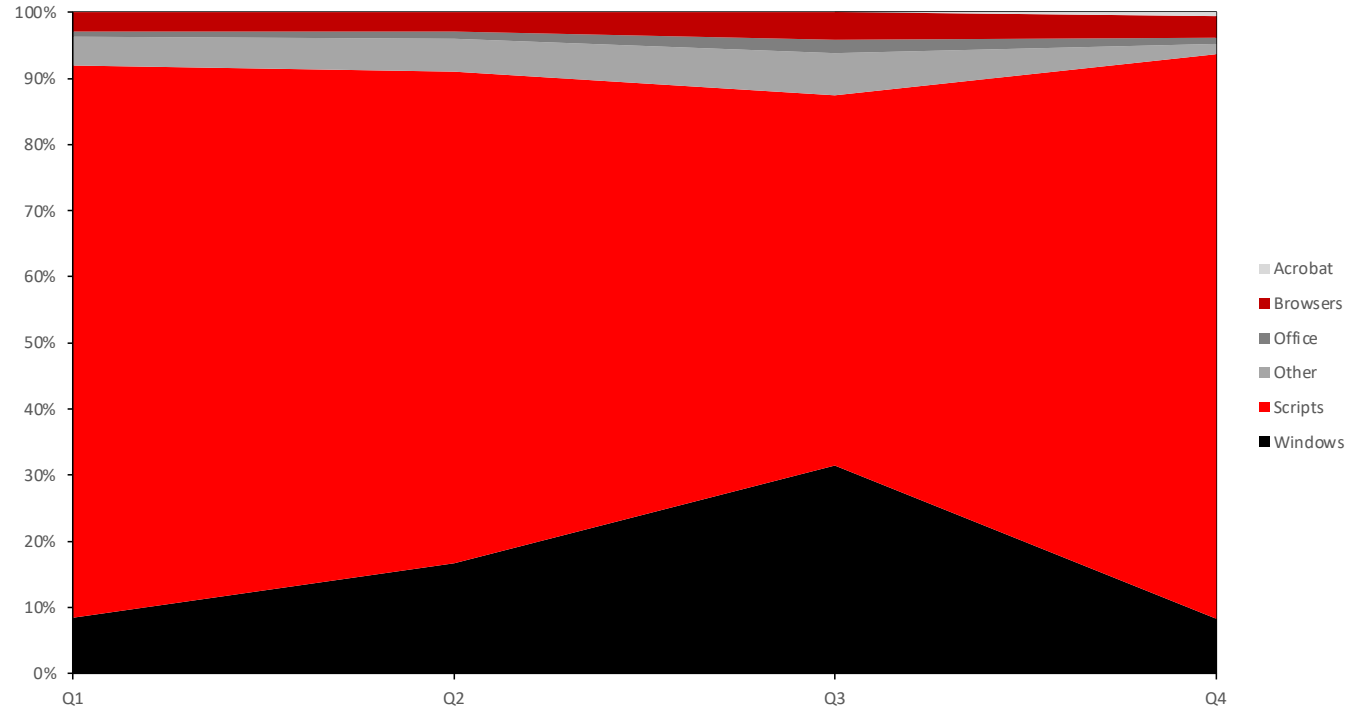


Figure 47. 2023 QoQ Attack Vectors Percentage Totals

Browser Attack Vectors

This subsection looks at the Browser Attack Vector to see which web browsers caused the most quarterly alerts. Last quarter, Chrome had the most alerts, followed by Internet Explorer and Firefox. This quarter, the numbers are entirely different. Firefox had 62% of the alerts. On the other hand, Chrome had 25% and Internet Explorer 13%. Practically everyone who uses the Internet uses a web browser. So, it's interesting to know which browsers attackers leverage.

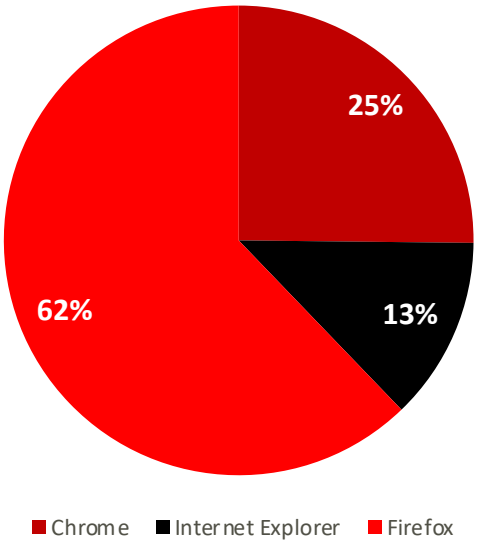


Figure 48. Comparative Browser Detections

Alerts by Exploit Type

Moving on, we turn our attention from generalized malware frequencies to the specific type of exploit used for each attack. The alert counts in this section are similar to those in Q3 but with a few minor exceptions. First, NetReflectiveLoader (when malware uses MEM_PRIVATE pages that do not correspond to an executable) has taken the top spot regarding the number of alerts this quarter. It has flipped rankings with ShellcodeBehavior, which are .NET files that inject payloads into the memory of its process. This is commonly called process injection. Aside from those, every other ranking didn't move or shuffled a few spots. The exploit that moved the most was AmsiBypass, which moved up nine rankings from the prior quarter. Finally, one new exploit made the list this quarter, ranking last, PsReflectiveLoader2. This exploit describes malware that leverages PowerShell to inject payloads into memory from a remote tool such as Mimikatz.

Exploit	Alert Count	Description of Exploit
NetReflectiveLoader	100,630	Code execution on MEM_PRIVATE pages that do not correspond to a PE
ShellcodeBehavior	13,334	.NET files that allocate and inject payloads directly within the memory of its own process (Assembly.Load)
RemoteAPCInjection	5,179	Remote code injection via APCs
RunPE	5,028	Process Hollowing Techniques
PsReflectiveLoader1	3,117	Files that leverage PowerShell to allocate and inject payloads directly within the memory of its own process (E.g. Mimikats) (Local)
AmsiBypass	865	Techniques that bypass Windows' Antimalware Scan Interface (AMSI)
WinlogonInjection	741	Remote Code Injection into winlogon.exe process
ROP1	525	Return Oriented Programming
ThreadHijacking	515	A process injection technique that allows the execution of arbitrary code in a separate process
IE_GodMode	341	GodMode technique in Internet Explorer
DumpLsass	269	LSASS Process Memory Dump
DynamicExec	209	Execution of code in pages without execution permissions (32 bits only)
APC_Exec	197	Local code execution via APC
HookBypass	163	Detection of memory allocation in base addresses; typical of heap spraying
ReflectiveLoader	18	Reflective executable loading (Metasploit, Cobalt Strike, etc.)
ReverseShell	9	Detection of reverse shell
JS2DOT	8	.NET Reflective Loading Technique
PsReflectiveLoader2	2	Files that leverage PowerShell to allocate and inject payloads directly within the memory of its own process (E.g. Mimikats) (Remote)

Figure 49. Alerts by Exploit Type

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.

We've changed how we display the Exploits by MITRE ATT&CK Tactic and Technique table. Previously, we listed the top 25 tactics and techniques. However, this became cluttered, and the lower-ranked techniques had negligible alerts. As such, we've dwindled the top 25 to the top 10, similar to other lists in this report. In the revised top 10 list, you will find a format identical to the one before, but with the addition of a new column that provides the rank of each (1 through 10). Rank one is the technique with the most alerts, and rank 10 has the fewest alerts. We have sorted the table in descending order, filtered first by MITRE tactic and then by technique.

This quarter, TA0002-T1059.001 (Execution :: Command Scripting Interpreter :: PowerShell) ranked first in alerts. This ranking matches our Attack Vectors section, which shows that Scripts, specifically PowerShell, are the number one attack vector hackers use when they are on endpoints. Ranking last was TA0003-T1543.003 (Persistence :: Create or Modify System Process :: Windows Service), which explains IoCs that create or modify existing Windows processes to execute payloads and gain persistence. That table and corresponding graph, with the corresponding rankings, are below.

MITRE Tactic	MITRE Technique	Tactic :: Technique :: Sub-Technique	Technique Count	Rank
TA0002	TA0002	Execution	2,962,272	7
	T1059.001	Execution :: Command and Scripting Interpreter :: PowerShell	8,247,671	1
TA0003	TA0003	Persistence	3,753,937	6
	T1543.003	Persistence :: Event Triggered Execution :: Accessibility Features	1,396,350	10
TA0004	TA0004	Privilege Escalation	2,170,537	9
TA0005	TA0005	Defense Evasion	5,596,290	5
	T1218.009	Defense Evasion :: System Binary Proxy Execution :: Rundll32	6,367,064	3
TA0007	TA0007	Discovery	6,706,355	2
TA0011	TA0011	Command and Control	2,583,768	8
TA0040	T1561.001	Impact :: Disk Wipe :: Disk Content Wipe	5,579,634	4

Figure 50. Exploits by MITRE ATT&CK Tactic and Technique, Q1 2023

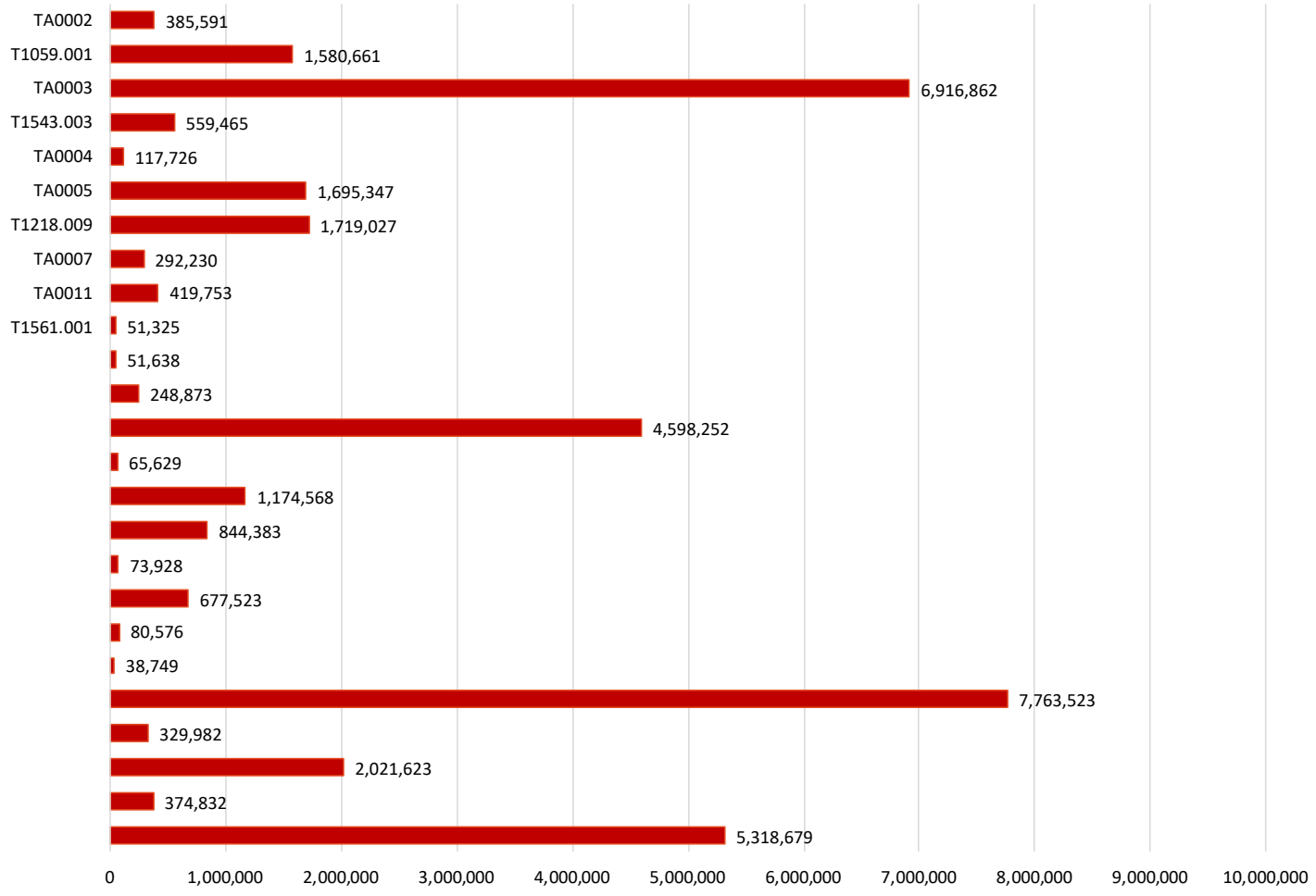


Figure 51. Exploits by MITRE ATT&CK Tactic and Technique, Q3 2023

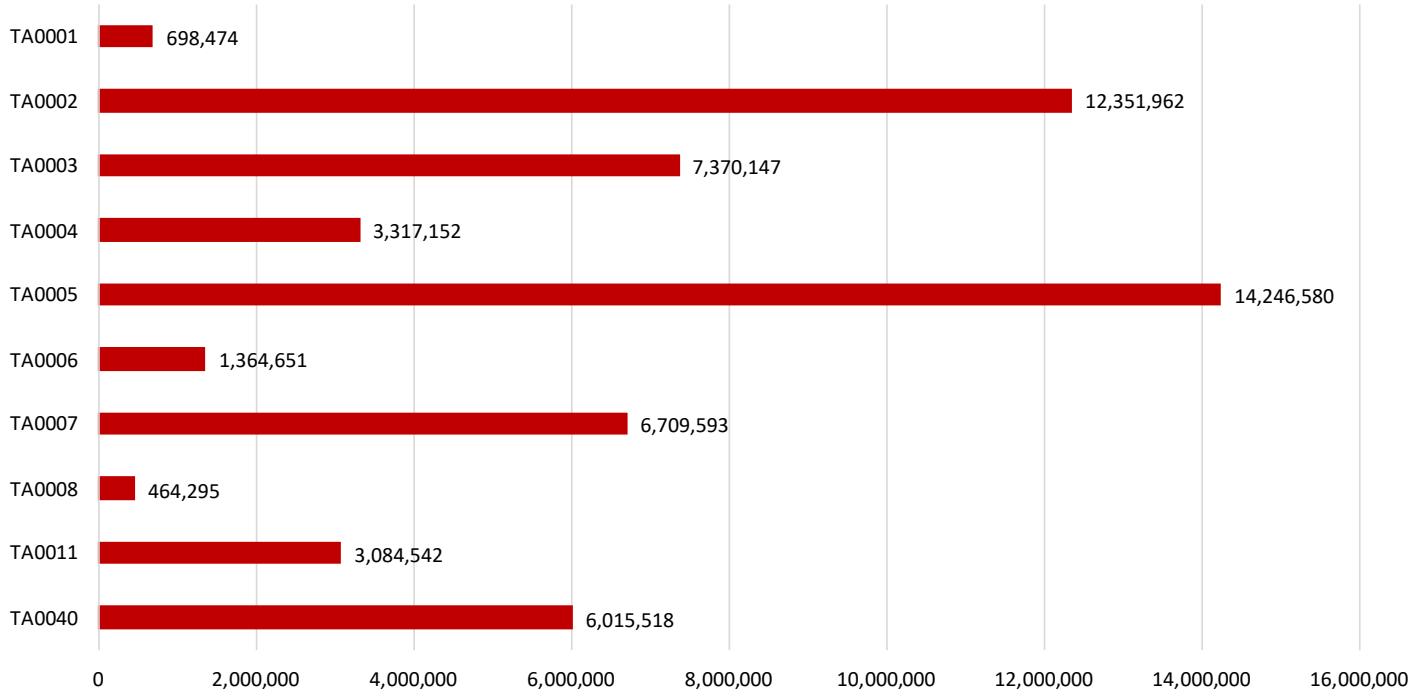


Figure 52. Exploits by MITRE ATT&CK® Tactics Summation

RANSOMWARE LANDSCAPE

Rounding out the endpoint for this quarter's ISR ends with the overall ransomware landscape. This data combines EPDR detections and ransomware double extortions observed in the wild. We first talk about ransomware-related alerts on endpoints caught by WatchGuard's EPDR solution and how that has progressed, or regressed, quarter over quarter. After that, we dig into each ransomware group that performs double extortion attacks and posts victims to their corresponding data leak sites, most of which are on the dark web. We use the victims posted to paint a picture of which groups are performing most of these attacks and to dissect any patterns in the data. More data than is shown in this report is on our Ransomware Tracker page.

This quarter, we continue to see a decline in the number of ransomware-related alerts from EPDR. In Q3, there were 421 alerts, and in Q4, that number decreased to 338, a 19.72% reduction. There is one probable explanation for this. Ransomware operators perform various exploits and tasks before ultimately deciding to deploy ransomware. Ransomware isn't one of the first tools used by these operators. Usually, there is the initial effort of getting into a network, then gaining persistence, pivoting, and usually, data exfiltration. Finally, they deploy ransomware once they finish all the other tasks. This leaves a lot of opportunities to catch these operators before the deployment of ransomware. In other words, EPDR is likely catching these threat actors before they even have a chance to deploy ransomware, and thus, the overall ransomware numbers have been decreasing. The double extortion landscape, however, tells a different story.

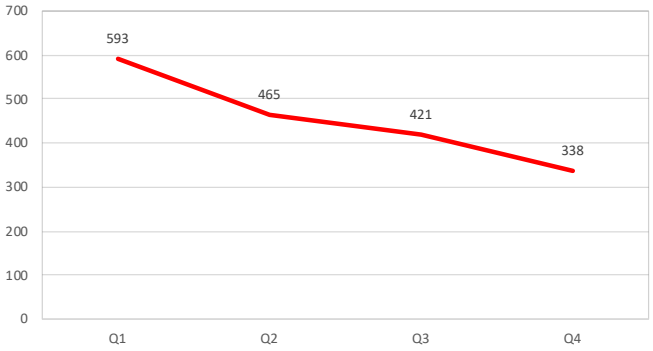


Figure 53. Ransomware detections by quarter

Extortion Groups

The extortion groups are the leading players in the ransomware space. These groups operate the most-used ransomware infrastructures on the planet. Most of these operators run a ransomware-as- a-service (RaaS) model, where they create encryptors and infrastructure for affiliates to buy and use. The operators take a small cut of the proceeds for each victim, and the affiliates keep most of it. Typically, these models are 80/20 or 90/10, where the operators take 20% or 10% of each ransom, and the affiliates keep the rest. This quarter, there were quite a few developments with these groups, and we describe some of the most notable ransomware breaches to wrap up the endpoint section.

Arguably, the biggest story of Q4 regarding ransomware groups is the dissolution of the Ragnar Locker group. In October, in coordination with the FBI and other law enforcement agencies, Europol announced the arrest and takedown of Ragnar Locker and its operators. Typically, you'll see the takedown of ransomware operator infrastructure without any arrests, and the corresponding groups rebrand and regroup and come back as something else. However, since there were associated arrests of the operators, it looks like the Ragnar Locker operation is no more. Ragnar Locker is one of the few groups that halted operations or had no victims in Q4. The others include CryptBB, DataLeakes, Karakurt, LostTrust, Nokoyawa, Rancoz, and Royal.

On the flip side, several new groups appeared in Q4:

New Groups:

- **DragonForce**
- **Hunters International**
- **Malek Team**
- **Meow Leaks**
- **Raznatovic**
- **Toufan**
- **Werewolves**

Researchers believe two of these groups are rebrands or derivatives of prior groups; one is more certain than the other. Hunters International claims they bought the sold source code of the Hive group, which law enforcement seized at the beginning of 2023. However, researchers believe this is a rebrand of Hive and not another group. The jury is still out on that one. Raznatovic, on the other hand, is undoubtedly a rebrand of RansomedVC. We know this because they said so themselves and the timeline of their operations coincides with their claims.

The following two lists are those groups that increased and decreased from the quarter prior, respectively.

Groups with increases from Q3 to Q4	Groups with decreases from Q3 to Q4
0mega (+2)	8base (-15)
Black Basta (+35)	Abyss (-3)
BlackSuit (+9)	Akira (-7)
Cuba (+3)	Arvin Club (-7)
Knight (+7)	BianLian (-24)
DAIXIN (+3)	BlackByte (-8)
INC Ransom (+18)	ALPHV (-28)
LockBit 3.0 (+1)	Cactus (-19)
Lorenz (+4)	CiphBit (-5)
Medusa Blog (+8)	Cloak (-24)
MedusaLocker (+1)	CL0P (-170)
Metaencryptor (+1)	CryptBB (-6)
NoEscape (+2)	DataLeakes (-2)
Play (+52)	Donut Leaks (-10)
Qilin (+6)	DungHill Leak (-5)
Ransom House (+2)	Everest (-25)
RansomExx2 (+3)	Karakurt (-8)
Snatch (+5)	LostTrust (-2)
	Mallox (-3)
	Money Message (-2)
	RA Group (-19)
	Ragnar Locker (-13)
	Rancoz (-3)
	Rhysida (-6)
	Royal (-1)
	Stormous (-7)
	ThreeAM (-1)
	Trigona (-4)

Figure 54. Increases and Decreases from Quarter Prior

Overall, the number of double extortions and known victims from ransomware groups was down from Q3 to Q4. In Q3, there were 1,432 of these victims, and in Q4, that number dropped to 1,305. That's an 8.87% decrease from Q3, a further reduction from Q2 to Q3 numbers, which was 6.47%. We predict the numbers will further decrease in Q1 2024 because of law enforcement action against LockBit that severely hindered their operations. Find more about that next quarter. Until then, we end with the quarter-over-quarter victim chart, followed by the numbers for each group for Q4 and throughout the year. See you next quarter!

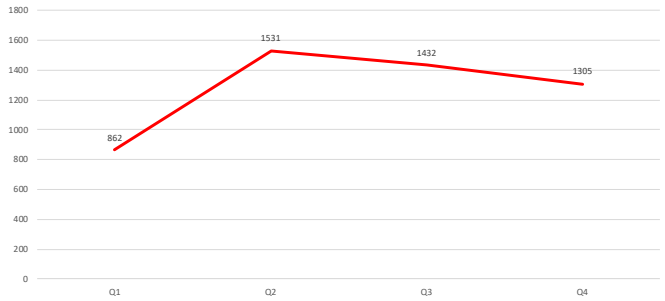


Figure 55. 2023 QoQ Public Extortions by Group

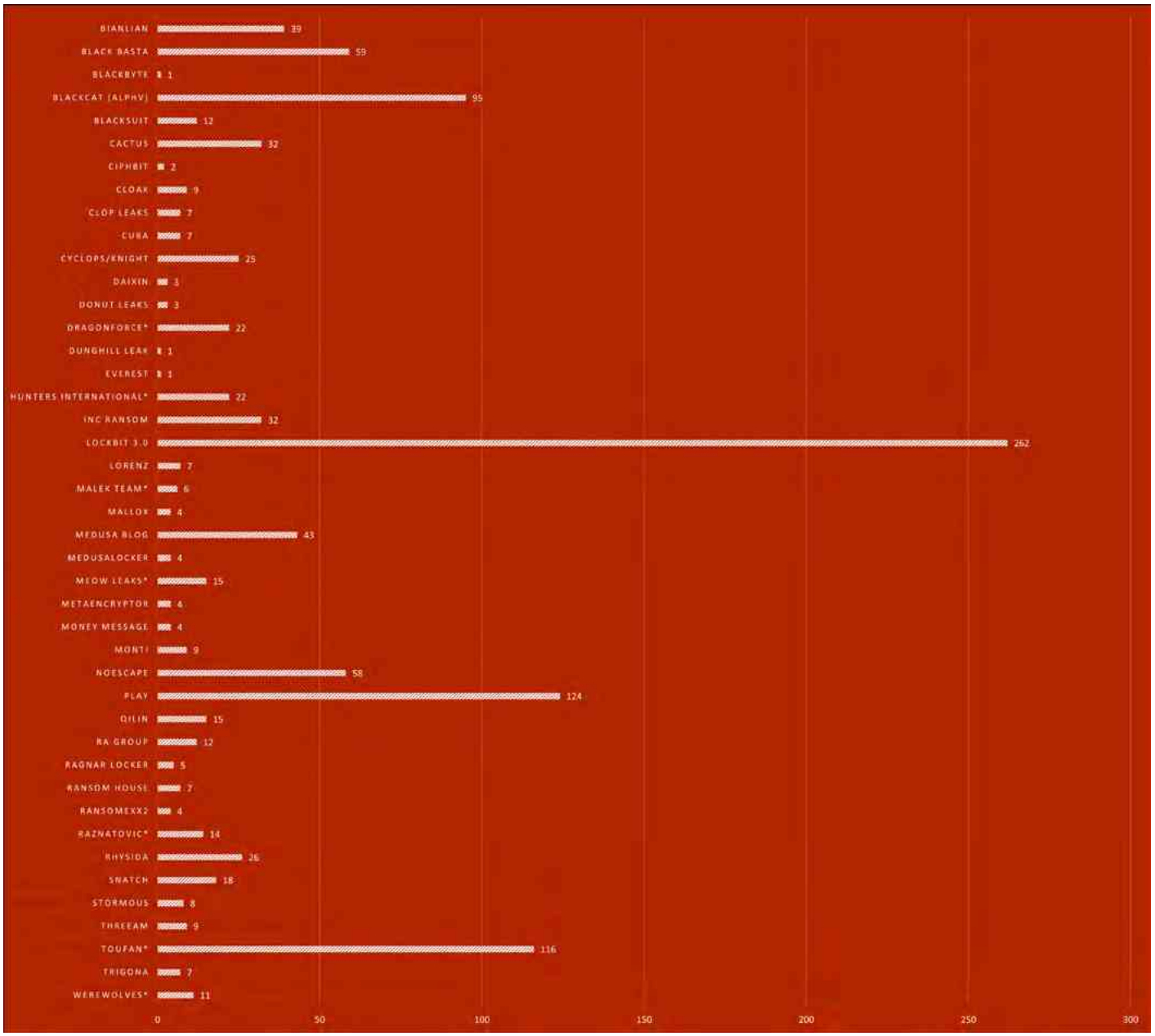


Figure 56. Q4 2023 Public Extortions by Group

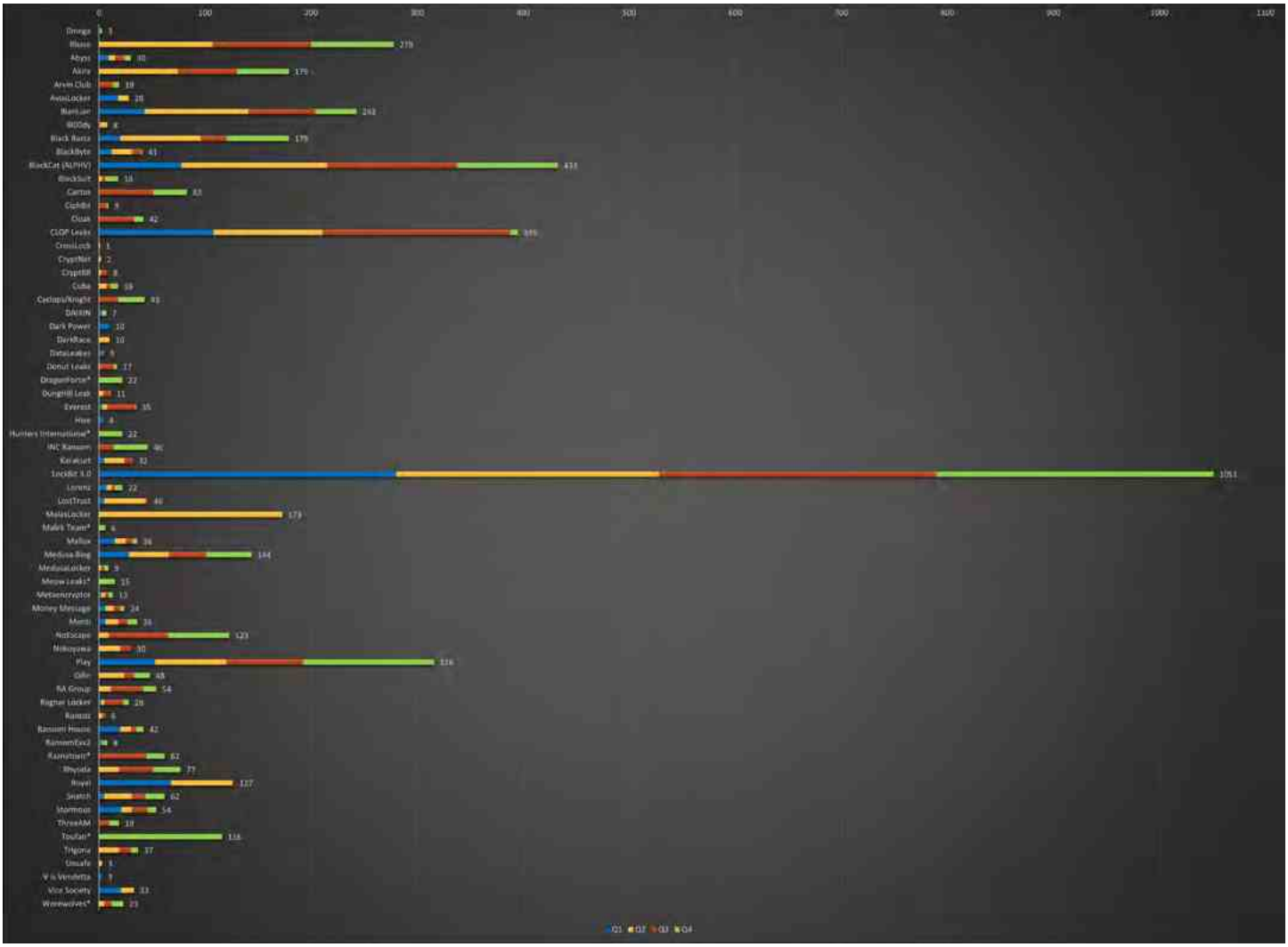


Figure 57. 2023 QoQ Public Extortions by Group Summation

Notable Ransomware Breaches

Akira

Nissan – Nissan was one of two major automotive groups breached in Q4. The other was Toyota Financial Services (TFS). In mid-to-late December, the Akira ransomware group claimed to have breached Nissan Australia's internal systems and exfiltrate 100 GB of data. The group claimed to have data on employees, NDAs, projects, and information about clients and partners. To our knowledge, it doesn't look like Nissan paid any ransom.

ALPHV

Fidelity – Fidelity National Financial filed an 8-K form to the SEC confirming a data breach on its systems in November 2023. The attack was from ALPHV, which took one of Fidelity's subsidiary's systems offline for about one week and included ransomware and data exfiltration. Users of this subsidiary reported confusion and anger about what was going on. Interestingly, ALPHV listed Fidelity and, shortly after that, removed it, which usually means negotiations are ongoing or the victim paid the ransom. However, we have no evidence of that. All in all, Fidelity stated that 1.3 million customers were affected by this breach.

MeridianLink –MeridianLink provides digital lending solutions and data to financial institutions, including banks, credit unions, and fintechs. In mid-November, ALPHV, more commonly known as BlackCat in the media, posted the group to its data leak site. What's unique about this entry is that the ALPHV operators allegedly filed an SEC complaint against MeridianLink due to failing to file a notice to the SEC for a cybersecurity incident, as required by law. Because of this, we added "Regulatory Complaint" to our list of extortion types on our Ransomware Tracker.

DragonForce

Ohio Lottery – DragonForce appeared at the end of 2023 and into 2024, coincidentally, the year of the dragon. Arguably, their most prolific breach was the Ohio state lottery. Unfortunately, the attack occurred on Christmas Eve, and shortly after that, an entry appeared on the group's data leak site. The attack took several systems offline, which hindered the operation of the lottery service. Also, the group exfiltrated an alleged hundreds of gigabytes of information. The data possibly included sensitive personal information of lottery users.

Hunters International

Fred Hutchinson Cancer Center – The Fred Hutchinson Cancer Center sent a notice to their patients on December 22, 2023, declaring a cybersecurity incident on November 19, 2023. They also sent a preliminary statement on December 1 claiming an incident. However, before the cancer center could publish the announcement to patients, Hunters International posted them on their dark web data leak site, claiming to have stolen 533 GB of data. What's interesting about this breach is that local news reported that patients received emails from the operators. The ransomware operators were extorting patients one by one by claiming that they had the patient's data and would remove it for $50.

LockBit 3.0

Boeing –Reportedly, LockBit affiliates hit aviation giant Boeing with a ransomware attack in Q4. The ransomware group listed Boeing on its data leak site in late October, and Boeing claimed that they were responding to a cyberattack on November 2. We can only assume that this response was about the LockBit breach. If a victim doesn't pay the ransom, the group posts them on its data leak site with a few data samples for proof. Aside from this small sample, Boeing hasn't mentioned much else about the incident, and we don't know whether they paid the ransom or not.

CDW – In October, public reporting uncovered that CDW, a technology company on the Fortune 500, was allegedly breached by affiliates of LockBit 3.0, who demanded a whopping $80 million ransom. The company claimed that the breach occurred on one of its small US subsidiary support systems and was non-customer-facing. The group claims the CDW representatives were willing to pay $1.1 million, a vastly smaller number compared to the extortion amount. We're uncertain if CDW paid any ransom at the time of this writing.

Industrial & Commercial Bank of China (ICBC) –If we had to choose one breach that was the most notable for Q4, it was this one. In early November, news quickly spread that one of China's largest lenders, the Industrial and Commercial Bank of China (ICBC), was dealing with a cyber incident. The incident disrupted financial trading, which included trading US treasury bonds. According to Reuters (and others), LockBit representatives claimed the ICBC paid the ransom. In the middle of Q1, 2024, the US Department of Treasury produced its report on what happened, and if they commented on it, you know the breach had an impact. Shortly after this announcement, law enforcement disrupted LockBit's operations in Operation Cronos. However, you can read more about that next quarter.

Medusa Blog

Toyota Financial Services (TFS) – In mid-November, TFS's Europe and Africa division confirmed that it experienced a cyber incident. Around the same time, the Medusa Blog (Medusa group) published TFS to its dark web data leak site, demanding an $8 million ransom. A few weeks after the notification, TFS sent letters to the affected customers confirming the attack and notifying customers about the affected data. The attack specifically targeted and affected the German division of TFS - Toyota Deutschland GmbH.

Rhysida

Insomniac Games – You may not recognize this organization without playing video games. However, if you are a gamer, you probably know of Sony's game development studio – Insomniac Games. Unfortunately, the Rhysida group posted Insomniac Games to its data leak site, claiming to have stolen 1.67 TB of data from 1,318,733 files. Insomniac Games posted a statement to their Twitter/X account explaining the situation. They claim the Rhysida group stole employee information and development details on their new game, Marvel's Wolverine, for PlayStation 5. Although the studio said the situation was distressing, development on Wolverine and other games continues.

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.

CONCLUSION & DEFENSE HIGHLIGHTS

CONCLUSION AND DEFENSE HIGHLIGHTS

So there's our cyber threat "map" for Q4 2024. We hope our quarterly threat landscape exploration highlighted the dangers you might find traveling online.

This quarter we saw increase in network malware detection, which required advanced malware services to keep up with, and may have positively contributed to the decline in malware detection we also saw at the endpoint.

Network attacks have declined, which is great news. Unfortunately, old but critical flaws like ProxyLogon continue to flood victims. So, it's important to keep your defenses up and your software up to date.

At the endpoint, we still see smart and sneaky threat actors live off the land with malicious scripts used to evade certain types of defenses. Make sure you enable endpoint detection and response (EDR) to catch these evasive attacks.

And finally, hackers will continue to socially engineer you with tricks, whether it be using seemingly legitimate SharePoint subdomains or burying hidden malicious links on legitimate compromised WordPress sites.

With that cyber threat map in your hand, you have a guide that can start you on a plan for the right defense. In that regard, here are three final defense strategies that you can apply to your Q4 2024 threat landscape map:

Combine network and endpoint protections for fortified defense.

As we continue to produce this cyber threat map every quarter over the years, we continue to see fluctuations in how malware and threats arrive, whether over the network or direct to endpoints. This quarter, network-based malware detection was up a lot. Meanwhile endpoint-based malware and ransomware was down. Perhaps endpoint-based malware is down specifically because the perimeter defenses are catching more malware? On the flip side, we have seen this same trend reverse. When network malware detections are down, you better make sure to have great endpoint protection to pick up the slack and detect more malware the perimeter may have missed. Whatever the case, both network and endpoint defenses are good, but neither are infallible. The best way to increase your chance of avoiding a breach is the layered defense of combining both. Make sure you have implemented both strong network and endpoint defense in your organization. Add some strong identity protections, like multi-factor authentication (MFA), to the mix, and you have some pretty hardened defenses to protect your company or home.

Don't skimp on the advanced malware protections of AI-based solutions.

Over 60 percent of malware gets past our and others' signature-based anti-malware solutions. This isn't because our products don't work, it's a problem that all signature-based solutions have. If you have to wait for a human or system to recognize a new malware variant, and design specific patterns to catch it before it can offer any protection, you will always be at least a few days, if not a few weeks, behind the latest malware.

This quarter, we saw one of our more proactive services, IntelligentAV (IAV) catch a huge amount of malware that signature-based solutions missed. Its detection increased 196% and it caught more than the other two anti-malware services combined. If our Gateway AntiVirus (GAV) service misses malware, IAV is the first service to take over. It leverages its machine-learning model, trained by tens of millions of good and bad files seen over the years, to immediately and proactively decide if a file is malware, without the need for a signature or human analyst. If you didn't have it enabled during Q4, you likely missed a ton of malware at your perimeter Firebox. Don't let this happen to you. Use our Total Security package for the Firebox and be sure to enable IAV (and APT Blocker while you are at it).

For goodness sakes, don't be the last to patch or update old software.

By now, you should be sick of hearing security companies warn you about ProxyLogon, and other old flaws. This vulnerability surfaced in the wild during 2020 and hasn't gone away since. It's an extremely critical vulnerability that is easy to exploit, and all of security media has warned you about it for years. Nonetheless, we know there are still people who haven't fixed this vulnerability as we still see attackers aggressively targeting it.

ProxyLogon isn't the only one like this either. ProxyShell and ProxyNotShell, and many other big-name vulnerabilities turn up all the time. Patches come out, but threat actors are still able to sometimes exploit them long after the fact. Meanwhile, software ages out too. Tools like like ATutor or Quagga fall out of support or go end of life, yet we continue to see some organizations use them well after their expiration date.

Cyberattackers bank on this apathy. They know people forget to patch for months or years at a time – especially so with hardware or IoT systems that run the same software but sit in some network rack. They also know some of you continue to leverage outdated software. Whether it's simply forgetting an old server exists, or even knowingly using old software because an internal process or app critical to your business still relies on it, SHODAN scans prove that threat actors can find a lot of legacy network services online.

Don't be the lazy or ignorant software administrators that cyberattackers assume you are. Patch critical vulnerabilities immediately, and don't leave issues like ProxyLogon unhandled. And decommission or upgrade end-of-life software. If a business case relies on it, well then do the hard work of updating that business process with a new app. We continue to see attackers target old vulnerabilities, often in old systems. Simple patching and upgrading can ensure you don't become a target.

We hope you found our Q4 2023 Internet threat landscape map enlightening and continue to use it to route your defenses. Return next quarter to see how the landscape continues to alter and we promise to return as your humble cybersecurity cartographer. 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.