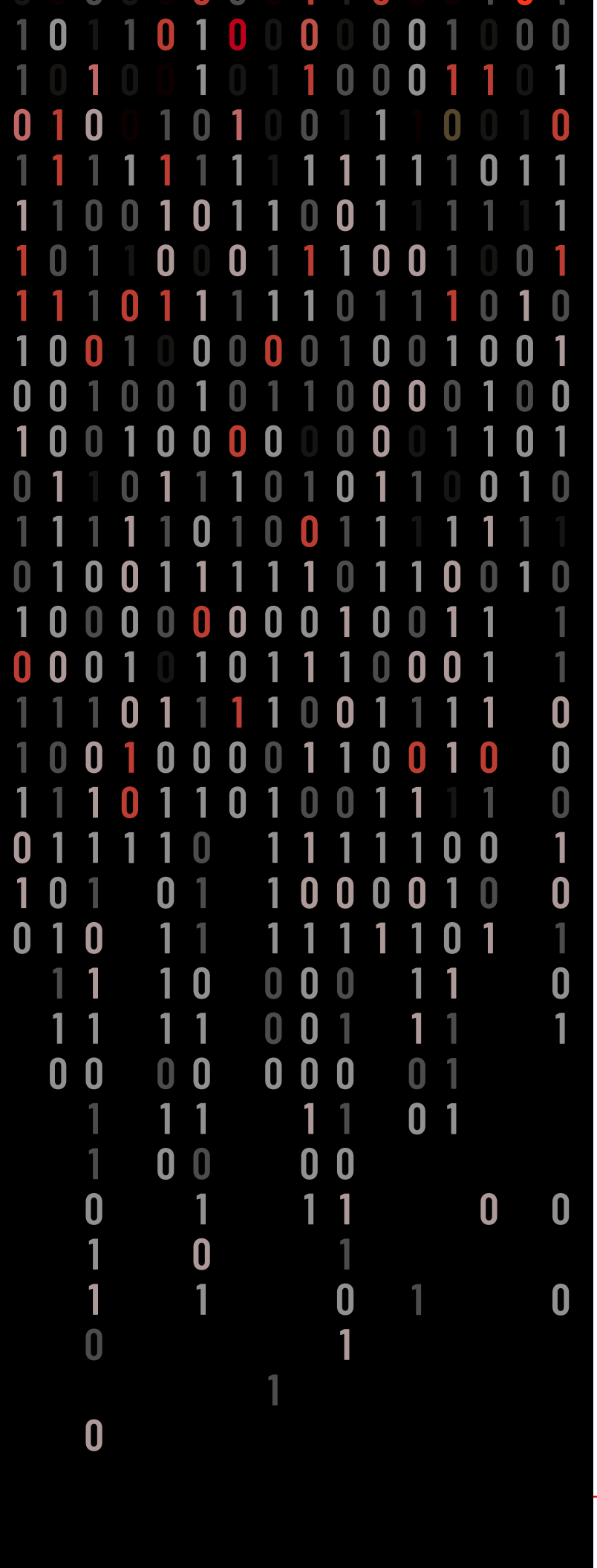
INTERNET SECURITY REPORT

Q4 2024

WatchGuard



CONTENTS

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

INTRODUCTION

With the ever-evolving landscape of cybersecurity, the threats we face morph as rapidly as the technologies we adopt. Much like a skilled sailor must continuously adjust their sails to navigate the capricious winds at sea, organizations must remain vigilant and responsive to the shifting tides of cyber threats. The threat landscape is not static; it is a dynamic arena where threat actors innovate their tactics, techniques, and procedures (TTPs), requiring us to adapt our defenses or risk being swept away by unforeseen challenges.

According to author William S. Burroughs, "When you stop growing, you start dying." This sentiment rings especially true in the field of cybersecurity. By diligently observing and analyzing the latest malware variants, network attacks, and malicious domains – from both a network and endpoint perspective – we can develop the insights necessary to learn how to fortify our defenses. Our quarterly Internet Security Report (ISR) encapsulates these critical findings, shedding light on the characteristics of emerging threats and providing actionable intelligence that helps organizations better prepare and grow defenses for potential attacks, rather than dying when their businesses succumb to a new threat.

In this report, we delve into the key malware trends observed from both network and endpoint malware detection solutions, offering a window into the shifting patterns of malware variants and their creators. Additionally, we highlight the top network security attacks or exploits detected by our network Intrusion Prevention Service (IPS) – each revelation acting as a beacon that guides us away from danger. By sharing these insights, we empower security teams to not only respond to current threats but to anticipate future ones, allowing for a proactive rather than reactive stance.

Our commitment to producing this report stems from the urgent need for organizations to understand the dangers they face in a digital realm, where adversaries are more tenacious and resourceful than ever. As we venture into 2025, it is our hope that this report serves as a guiding star, enabling all of us to reinforce our cyber defenses and ensure our organizational resilience amidst the tempest of continual change.

Let this report be not just a retrospective glance at past challenges, but a forward-looking analysis that inspires adaptive strategies in the face of persistent evolution. Together, we can navigate this complex cybersecurity terrain, always ready to adjust our sails in response to the winds of change.

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

In this report, we cover:

EXECUTIVE SUMMARY

At the highest level, network malware almost doubled, but endpoint malware reached an all-time low. We also saw sophistication in network-detected malware increase with the increase in our zero-day malware percentage, but at the endpoint, unique and new malware is way down, suggesting that what the endpoints saw was more generic and run-of-the-mill malware variants. Though these differences might seem unusual, one thing is sure – you need both network- and endpoint-based malware detection for the defense in depth necessary to prevent all these attacks.

As far as network-based attacks and exploit, those decreased by more than ¼ during Q4. While attackers did at least launch a slightly higher number of unique exploits, most of the top network attacks by volume and devices affected were almost identical to last quarter and mostly consisted of older or generic web application flaws. We still see threat actors trying to find servers vulnerable to ProxyLogin and HAProxy vulnerabilities.

That said, we have seen new trends across many of our security services. For instance, coinminers are back. Network and endpoint malware detection solutions saw an increase in them, and we saw many top malicious domains focused on malicious cryptocurrency mining or Etherhiding.

Here are some of the executive highlights from our Q4 2024 report:

- **Total network-based malware detections almost doubled, increasing 94%.** We saw this increase across all of our malware detection services, but the largest increases came from our more proactive services like IntelligentAV (increased 315%) and APT Blocker (increased 74%).
- **Strangely, endpoint unique malware detection shows a completely different picture, decreasing about 91% QoQ, and showing the lowest volume of unique detections we have seen this year.** While we saw a huge spike in unique endpoint detected malware during Q2, even if we consider that as an outlier, this quarter's malware still would have decreased ~65% compared to the rest of the year.
- Not only were endpoint unique malware detections down, **but new malware threats also hit an all-time low of only 8 new threats per 100,000 malware detections**. In general, we saw less targeted malware that only affected one or a few machines, and rather generic, sometimes-old malware that affected many machines
- **60% of malware spread over encrypted connections (TLS) during Q4,** which is an 8pt increase from last quarter, and a continued increase for the year.
- Our "per Firebox" malware results for various network malware detection services:
  - **Average total malware detections per Firebox:** 1,553 (~94% increase)
  - **Average malware detections by GAV per Firebox:** 543 (6% increase)
  - **Average malware detections by IAV per Firebox:** 883 (315% increase)
  - **Average malware detections by APT Blocker per Firebox:** 127 (74% increase)
- **We extrapolate** that if all the estimated currently active (licensed) Fireboxes enabled all malware detection security services and were reporting to us, **we would have had 600,127,343 malware detections during Q4 2024.**
- **More than half (53%) of malware detected evaded signature-based methods.** We call this **zero-day malware**, as it requires more proactive techniques (IAV/APT) to catch this never-before-seen malware. In general, zero-day malware has been on a declining trend over the past year or so, compared to old highs that almost always accounted for more than half and sometimes even three-fourths of detected malware in the past. This quarter is one of the first where we have seen it return to a significant level.
- **Furthermore, zero-day malware accounts for 78% of malware detected over encrypted connections.** This suggests that threat actors combine evasion techniques, both using encryption to avoid some security scans and then leveraging malware evasive techniques more often for these more advanced threats. If you aren't already decrypting and scanning TLS web traffic, you really should.
- Unlike network malware, **network attacks decreased 27% during Q4 2024**, with only 92 software exploits per Firebox caught by IPS signatures. That said, we did see a slight increase in the number of unique exploits attackers tried, with unique IPS signature hits up 13%.
- Coinminer malware and malicious cryptocurrency mining are on the rise again. Though we have seen many quarters of coinmining malware decreasing, during Q4 we saw it has returned. **A malicious coinminer made the second spot on our network malware top ten, it increased 141% QoQ** in endpoint detections, and some of the top malicious domains we blocked involved malicious cryptocurrency mining.

- Along with coinminers, we also saw more evidence of blockchain and cryptocurrency-related attacks like Etherhiding. Etherhiding is a malicious tactic of hiding malware on an immutable blockchain, which both leaves it there forever and can act as a back channel to hide malware delivery. In Q4, Etherhiding domains made their way onto our top compromised domain list.
- As far as endpoint malware delivery vectors, malicious scripts (primarily PowerShell) remain the most common way malware arrives on an endpoint. Windows binaries used to be the second most common, but not only did they drop precipitously, but for the first time in years browsers (specifically browser vulnerabilities or exploits) became the second most common malware delivery vector.

This is just a preview of the insights we found from our product threat intelligence during Q4 2024. If you need more help sailing the rough threat landscape, you can find more details about our findings, as well as what you can do about them, in the meat of this report.

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 threats 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 provides 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 highlight charts to provide 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

1,553

Average detections per Firebox jumped by **94%**

Basic Gateway AntiVirus (GAV) service

543

Basic malware increased **6%**

APT Blocker (APT)

127

APT blocker increased **74%**

IntelligentAV (IAV)

883

jumped a whole **315%**

GAV with TLS

663

TLS detections by GAV increased **21%**

APT Blocker with TLS

153

TLS detections of evasive malware increased by **363%**

TLS malware

60%

Malware over an encrypted connection increased **8 points**

MALWARE TRENDS

In Q4 2024, the malware landscape continues to challenge network security, as captured in detailed data from Firebox detections. This information, spanning regional trends, encrypted threats, and detection rates, offers a critical view into the evolving tactics of cybercriminals. To ensure its value, we rigorously analyze data, then transform raw numbers into actionable insights. Our process involves validating detection counts, cross-referencing regional distributions, and confirming malware classifications to eliminate noise and inconsistencies. Finally, we normalize figures to account for deployment variations. This meticulous approach increases reliability, enabling security teams to trust the data as a foundation for decision-making. From spotting encrypted malware surges to identifying regional hotspots, this refined data set empowers organizations to adapt defenses, prioritize resources, and stay ahead of threats like botnets, droppers, and exploits that dominated Q4.

Starting off with an overview, the table below shows average hits across various security services and their changes since the previous quarter. Total malware detections average 1,553 per Firebox, up 94%, reflecting a steady rise in threats. Gateway AntiVirus (GAV) logs 543 detections, with a modest 6% increase, while APT Blocker sees 127 detections, up 74%. IntelligentAV (IAV) stands out with 883 detections, surging 315%, indicating its growing role in catching sophisticated malware.

When inspecting TLS traffic, GAV hits rose to 663 – up 21%, and evasive malware over TLS, averaging 153 hits per Firebox, increased by 363%. This aligns with TLS malware's share jumping to 60%, an 8-point rise, highlighting encrypted channels as a favored attack vector. These evasive threats, often never seen before or polymorphic (where the malware changes itself), evade signature-based detection, driving the higher APT and IAV numbers.

The table paints a dual picture: basic malware persists, but advanced, encrypted threats are accelerating. The significant upticks in IAV and TLS evasive hits suggest attackers are leaning harder into obfuscation and encryption, challenging traditional defenses. Fireboxes equipped to decrypt and analyze TLS traffic are increasingly vital, as the 8-point TLS malware surge underscores a critical need for enhanced visibility and adaptive protection strategies.

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 latest Q4 2024 malware detection data gathered from Fireboxes offers a snapshot of the most prevalent threats targeting systems worldwide. This table lists the top 10 malware variants by detection count, providing actionable insights for security teams.

Topping the list is JS.Heur.Morpheus.1.E810619B.Gen, a Windows code injection malware with 194,709 detections. It often arrives via an email with a zipped attachment, which, when opened, connects to 0x0[.]st through a VBA script. Embedded within is a PowerShell script that installs a keylogger and spyware, quietly compromising systems. Another heavy hitter is Application.Linux.Generic.24096, a coinminer detected 181,752 times, showcasing the persistent profitability of this type of malware.

Droppers also loom large, with Trojan.GenericKD.71026669 (36,437 detections) and the newly emerged Trojan.Sesfix.1 (31,739 detections) delivering malicious payloads. Meanwhile, PasswordStealer.GenericKDS (46,201 detections) continues its credential-theft spree. A striking resurgence comes from Trojan.Linux.Mirai.1, a botnet malware with 45,903 detections. Known for crippling IoT devices with DDoS attacks, Mirai's return is notable. While we saw a loader in Q3, Q4 marks the full malware's comeback, targeting Linux-based systems with renewed vigor.

The table itself is a curated rundown of malware categories, counts, and last-seen timestamps, ranging from coinminers and hacktools to phishing and botnets. Beyond the top 10, an intriguing trend emerges: spots 11 through 13 are occupied by Linux-targeting threats. These include Masscan, a port-scanning tool for reconnaissance; Mirai.gen, another Mirai clone botnet; and a Monero Coinminer, quietly siphoning processing power. This trio underscores a growing focus on Linux environments, often perceived as secure but increasingly exploited.

By analyzing this Firebox data, we ensure it's not just numbers – it's a roadmap for action. From JS.Heur.Morpheus's stealthy spyware to Mirai's botnet revival and Linux-specific threats, the landscape demands proactive defenses tailored to these persistent and emerging risks.

Threat Name	Malware Category	Count	Last Seen
JS.Heur.Morpheus.1.E810619B.Gen	Win Code Injection	194,709	New
Application.Linux.Generic.24096	Coinminer	181,752	Q3 2024
Application.Agent.LGP (impacket)	Hacktool	110,594	Q1 2023
Application.Agent.IIQ	Dropper	88,777	Q1 2023
JS.Phishing.3.39554A09	Phishing	53,302	Q1 2023
PasswordStealer.GenericKDS	Password Stealer	46,201	Q3 2024
Trojan.Linux.Mirai.1	Botnet	45,903	Q3 2024
Trojan.GenericKD.71026669	Dropper	36,437	Q3 2024
Generic.Application.3Proxy.A.9560BBDD	Linux Hacktool	32,368	Q3 2024
Trojan.Sesfix.1	Dropper	31,739	New

Figure 1. Top 10 Malware Detections

Top 5 Encrypted Malware Detections

The Top 5 TLS Malware table, derived from Firebox detections, highlights malware traversing encrypted connections, posing unique challenges. With many threats cloaked by TLS, unmonitored connections create a blind spot attackers exploit.

Leading the list is Heur.BZC.PZQ.Pantera.157, a Windows code injection malware with 240,669 detections. This batch script harbors suspicious commands, executing stealthy injections over encrypted channels. Next, Application.Agent.IIQ, a dropper with 88,777 detections, delivers payloads discreetly. Office exploits follow, with VBA.Heur2.ObfDldr.9.63A9E772.Gen (18,135 detections) and Exploit.CVE-2017-0199.Gen (9,148 detections) leveraging encrypted traffic to target vulnerabilities.

Variant.MSILHeracles.156368, a code injection threat with 11,188 detections contains an "activator" or keygen to bypass software licensing. We find it often bundled with malware like Remcos or Formbook, amplifying its risk. See our 2023 Q3 report for more on Remcos.

Detecting these threats requires decrypting TLS traffic, a critical step given their reliance on encryption to evade traditional scans. Only 20% of Fireboxes configured to inspect this traffic, the majority miss these concealed dangers. Enabling TLS inspection is vital to unmasking scripts like Heur.BZC.PZQ and tainted tools like MSILHeracles, ensuring robust defense against encrypted threats.

Threat Name	Malware Category	Count
Heur.BZC.PZQ.Pantera.157 (variants)	Win Code Injection	240,669
Application.Agent.IIQ	Dropper	88,777
VBA.Heur2.ObfDldr.9.63A9E772.Gen	Office Exploit	18,135
Variant.MSILHeracles.156368	Win Code Injection	11,188
Exploit.CVE-2017-0199.Gen	Office Exploit	9,148

Figure 2. Top 5 TLS Malware

Top 5 Widespread Malware Detections

The Q4 2024 table of the most-widespread malware, detected across the highest number of Fireboxes, reveals key geographic trends in malware distribution. This data breaks down prevalence by country and region, highlighting where these threats are most pervasive. Notably, Europe, Middle East, and Africa (EMEA) consistently sees higher percentages of widespread malware compared to Asia-Pacific (APAC), while Americas (AMER) registers the lowest regional impact across the board.

Topping the list are familiar names from the previous quarter: Exploit.CVE-2017-0199.04.Gen, a Microsoft Office exploit, hits Greece (20.94%), Turkey (20.42%), and Cyprus (20%), with EMEA at 11.25%. Trojan.Zmutzy.834 and Trojan.Zmutzy.1305 also reappear, targeting Greece (22.38%) and Cyprus (15.38%) heavily, alongside Hong Kong. Exploit.RTF-ObfsObjDat.Gen, another holdover, dominates Greece (23.83%) and Turkey (16.25%), with EMEA at 10.03%. Rounding out the table is Trojan.HTML.Phishing.CHJ, led by Hong Kong (15.62%).

The recurrence of Zmutzy variants, CVE-2017-0199, and RTF exploits signals persistent attack vectors. EMEA's elevated exposure underscores regional targeting, while AMER's lower figures suggest less widespread impact, urging tailored defenses by region.

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%

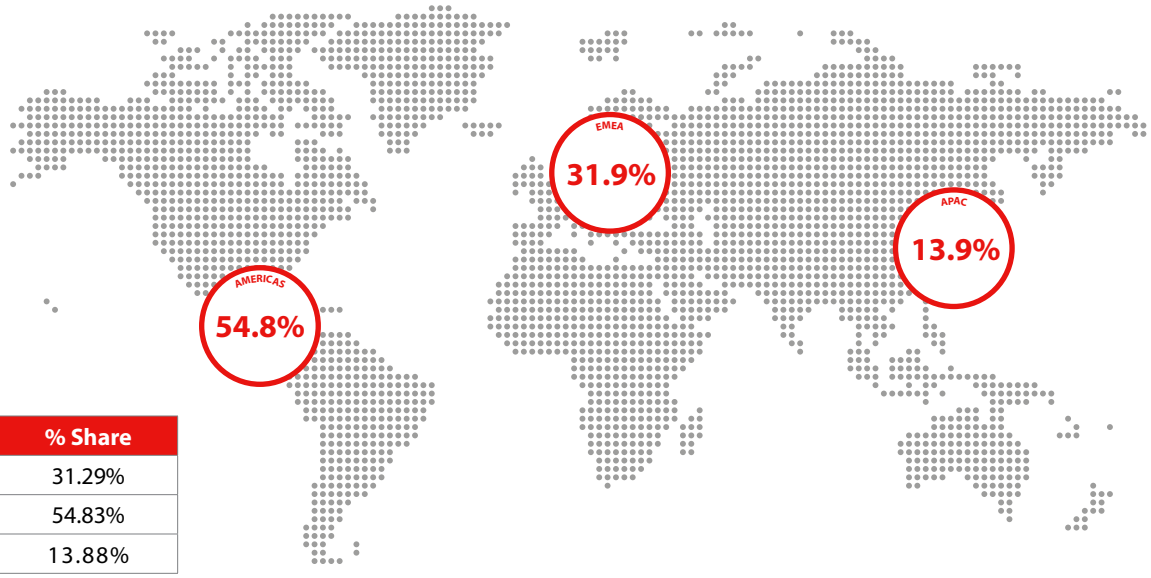
Figure 3. Most-Widespread Malware

Geographic Threats by Region

The Region table presents malware distribution across regions normalized by the number of Fireboxes deployed in each. This metric, expressed as a percentage per region, reveals the relative intensity of malware encounters, accounting for device density. Unlike raw counts, this normalization highlights exposure per unit, offering a clearer view of regional targeting.

AMER leads with 54.83% per Firebox, indicating a higher malware load per device compared to EMEA at 31.29% and APAC at 13.88%. This suggests that while AMER may see less widespread malware overall, its Fireboxes face a denser concentration of threats. EMEA follows, balancing moderate exposure, while APAC's lower percentage reflects fewer incidents per device.

Specific threats underscore this distribution. Trojan.Linux.Mirai.1, a botnet, heavily targeted Italy within EMEA, exploiting IoT vulnerabilities to build attack networks. Meanwhile, Application.Agent.LGP, a hacktool, zeroed in on the United States in AMER, likely aiding reconnaissance or lateral movement. These examples illustrate how regional targeting aligns with the normalized data, emphasizing AMER's elevated per-device risk and the need for region-specific defenses.



Region	% Share
EMEA	31.29%
AMER	54.83%
APAC	13.88%

Figure 4. Geographic Threats by Region

Catching Evasive Malware

The Zero-Day Malware table reveals the split between advanced evasive malware and basic, signature-detectable threats. Among devices with APT Blocker or IntelligentAV (IAV), 53% of detected malware contains zero-day, evasive threats, while 47% is catchable via signatures. For devices also inspecting encrypted traffic, the zero-day share jumps to 78%, with only 22% being basic malware.

These evasive threats lack family names, as they're either unique, never-before-seen attacks or leverage polymorphism to morph their code, dodging traditional detection. This shift highlights the growing sophistication of attacks, especially over encrypted channels, underscoring the critical need for advanced tools and TLS inspection to combat these elusive, shape-shifting dangers effectively.

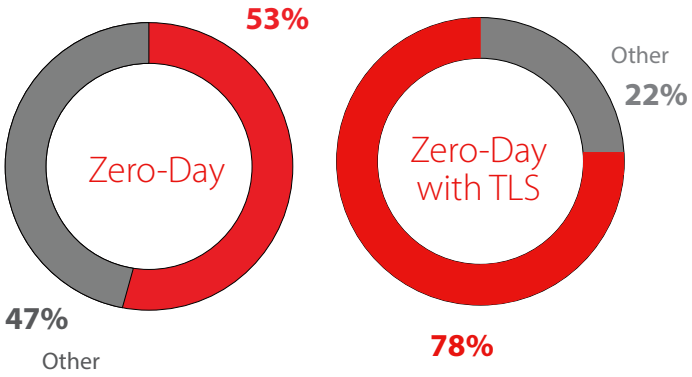


Figure 5. Zero-Day Malware

Individual Malware Sample Analysis

Trojan.Sesfix.1
A new malware detection identifies a VBA script. A Microsoft Office file will usually run this type of script; however, in this case another VBA script runs the file detected. We never found a malicious Microsoft Office file in this chain, but we still believe this is the original infection vector. The malware installs xmrig, a coinminer.

We've covered Xmrig in the past so we will just look at the infection path.

- Unknow Office file loads Logo.ICO
- Logo.ICO contains AppSetup.ICO
- AppSetup.ICO contains the main install script and uses contents from Logo.ICO
- AppSetup.ICO installs TProcHandler.exe, which is Xmrig

AppSetup.ico loads these files into memory. By loading all files in the infection path into memory, even if the antivirus catches one of these files the malware can recover itself. In this way, it gains persistence.

```
ON ERROR RESUME NEXT
DIM ACTIV_NAME
ACTIV_NAME = “APPSETUP.ICO”
DIM PASSIV_NAME
PASSIV_NAME = “LOGO.ICO”
DIM T_NAME, T_CONF_NAME
T_NAME = “TPROCHANDLER.EXE”
T_CONF_NAME = “TPROCCONF.DB”
DIM M_NAME, M_CONF_NAME
M_NAME = “MPROCHANDLER.EXE”
M_CONF_NAME = “MPROCCONF.DB”
```

We didn't find anything new in this malware sample, but the techniques used to infect and persist makes the malware dangerous. The sooner we can catch the malware the less damage we incur from it. If we prevent the malware from ever reaching the workstation then we don't even need to worry about the damage done.

Application.Agent.LGP (Impacket)
We found the Application.Agent.LGP malware family contains the hacktook Impacket, a powerful set of Python scripts listed on GitHub (**check it out here**). This isn't your typical library. It's built to manipulate low-level network protocols with precision. It can target Windows systems SMB shares or execute commands remotely on a machine.

What caught our eye is its versatility. It handles protocols like SMB, NTLM, and Kerberos, making it a go-to for testing network security. It's designed to authenticate and move through systems, often exploiting weaknesses like stolen credentials. Seeing Python3-Impacket on a corporate network isn't normal. It's a hacker's tool, not an admin's tool. One should never see this on a corporate network.

JS.Phishing.3
Microsoft credentials. At its core, it deploys a web page that's a near-perfect replica of the official Microsoft login portal. It has the same layout, fonts, and branding. Unsuspecting users enter their credentials, believing they're accessing their accounts, but instead of authenticating with Microsoft, the data is silently funneled to a malicious domain, panteraaaprojectionsi[.]sbs. This phishing tactic exploits trust in familiar interfaces, making it dangerously effective. Once credentials are harvested, attackers can infiltrate email, Cloud storage, or corporate systems, often undetected until it's too late. To stay safe, always verify the URL before logging in. Microsoft's legitimate domains will never redirect to obscure sites like this. Vigilance and two-factor authentication are your best defenses against this deceptive threat lurking in plain sight.

Below we see a CAPTCHA one receives when first visiting this page. In the next screenshot, we see the fake Microsoft login portal and the payload sent when we enter the password WGpassword. You can see "WGpassword" in the payload under the form data. Finally, in the next screenshot we see the login credentials passed to panteraaaprojectionsi[.]sbs

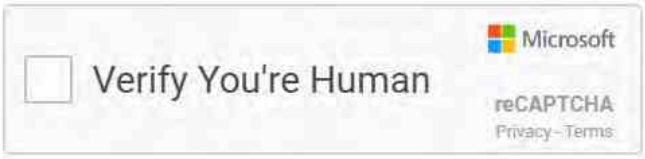


Figure 6. Phishing.3.human

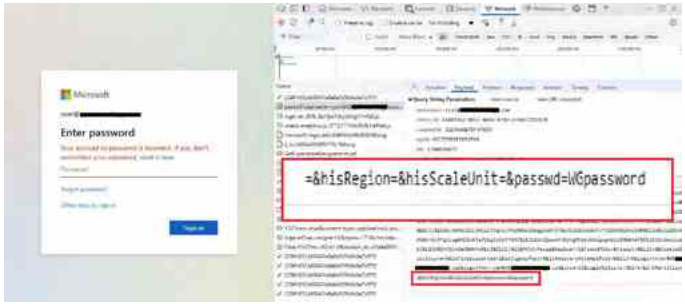


Figure 7. Phishing.3.human

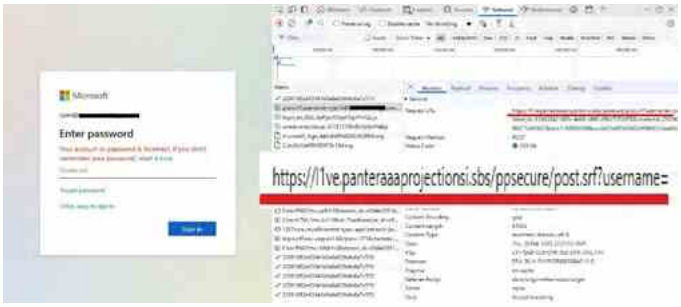


Figure 8. Phishing.3.header

Conclusion

Malware distribution varies by region, as seen by trends where certain families targeted areas like EMEA and AMER. Subscribing to threat feeds provides insights into local risks, enabling organizations to adjust firewall policies and security measures accordingly. This tailored approach ensures defenses align with the most relevant threats, boosting efficiency and resilience.

By combining advanced detection tools with regional threat intelligence, organizations can address both sophisticated and geographically specific malware challenges. This dual strategy enhances visibility, improves response capabilities, and significantly reduces vulnerability to cyberattacks. Adopting these practices equips businesses to stay ahead in the dynamic world of cyber threats.

NETWORK ATTACK TRENDS

Network exploits continued to bombard organizations in Q4 2024, with attack volumes remaining high and a mix of both old and new threats. In fact, many tried-and-true exploits persisted as top attacks this quarter – some more than five to ten years old – underscoring that attackers stick with what works. One notable trend was the enduring presence of critical vulnerabilities in widely used enterprise software. For instance, the Microsoft Exchange "ProxyLogon" flaw (a 2021 pre-authentication exploit) remained among the most-targeted attacks and a 2023 HAProxy web proxy request smuggling flaw stayed under active exploit. Overall, Q4's network attack landscape shows that while novel exploits emerge, attackers continue heavily leveraging unpatched legacy vulnerabilities at scale. The takeaway for this quarter is clear, organizations face a dual challenge of patching old holes and keeping up with new threats.

After an increase through the middle of the year, in Q4 we saw a sizable drop in network-based attacks targeting organizations around the world. This quarter, each Firebox saw, on average, 92 network attacks, a 27% drop compared to 126 for Q3. There was a notable 13% increase in the number of unique detection rules triggered over the quarter though, with 492 unique signatures compared to 435 in Q3. Even with overall attacks down for the quarter, the wider variety of attack techniques means defenders shouldn't let their guard down.

Throughout the rest of this section, we'll take a closer look at the network attack trends and specific attacker techniques targeting organizations worldwide in Q4 2024.

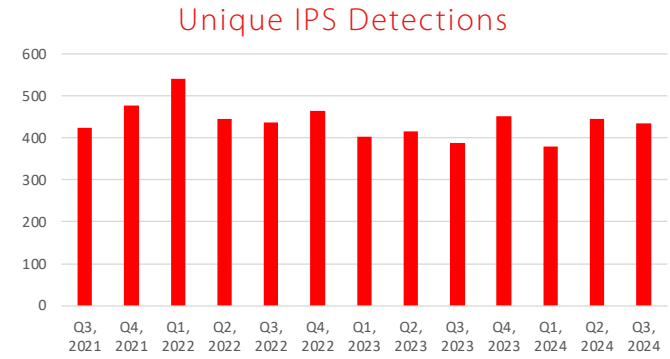


Figure 9. Unique IPS Detections

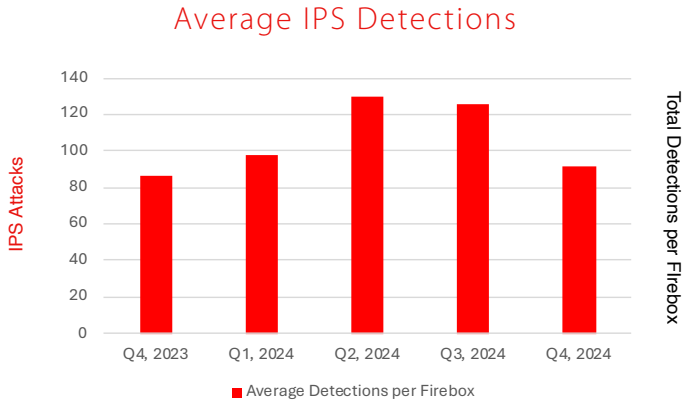


Figure 10. Average IPS Detections per Firebox

Top 10 Network Attacks Review

The top 10 network attacks by volume show us the overall trends of network attacks worldwide, in aggregate. In Q4 2024, the data reveals a heavy concentration of web application exploits. The list is dominated by web-based attacks – from file inclusion and path traversal to XSS and SQL injection – illustrating that web servers and applications remained prime targets. Many of these signatures represent broad classes of attacks rather than single vulnerabilities, covering a range of CVEs. Notably, even very old exploits (e.g. decades-old CVEs in file inclusion and XSS categories) still generate significant traffic, implying that attacks against unpatched legacy systems are widespread on the Internet.

Top 10 History

Signature	Type	Name	Affected OS	Percentage
1059877	Exploits	WEB Directory Traversal -8	Windows, Linux, Freebsd, Solaris, Other Unix	13.12%
1136822	Web Threats	WEB dotCMS CMSFilter assets Access Control Weakness (CVE-2020-6754)	Network Device, Others	7.26%
1138800	Web threats	WEB Microsoft Exchange Server Remote Code Execution Vulnerability -6 (CVE-2021-26855)	Windows	7.16%
1054837	Web Threats	WEB Remote File Inclusion /etc/passwd	Windows, Linux, Freebsd, Solaris, Other Unix	4.75%
1131523	Buffer Overflow	WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability -2 (CVE-2015-2425)	Windows	4.71%
1059958	Web Threats	WEB Directory Traversal -27.u	Windows, Linux, Others	4.56%
1055396	Web Threats	WEB Cross-site Scripting -9	Windows, Linux, Freebsd, Solaris, Other Unix, Network Device	4.35%
1231780	Web Threats	WEB HAProxy h1_headers_to_hdr_list Empty Header Name Access Control Bypass (CVE-2023-25725)	Network Device	4.13%
1133539	Web Attacks	WEB SQL injection attempt -2.u	Windows, Linux, FreeBSD, Solaris, Other Unix, macOS	3.82%
1058468	Web Attacks	WEB SQL injection attempt -25.a	Windows, Linux, FreeBSD, Solaris, Other Unix	3.46%

Figure 11. Top 10 Network Attacks by Volume

There were no new additions to the top 10 list by volume this quarter, but there were two returning signatures that had been absent for several years. Signatures 1133539 and 1058468 rounding out the end of the top 10 list were both absent from the top 10 since Q3 2021 and Q4 2022 respectively. Both signatures are designed to catch SQL injection attempts against exposed web services. Even in 2024, SQL injection vulnerabilities remain relevant targets for adversaries.

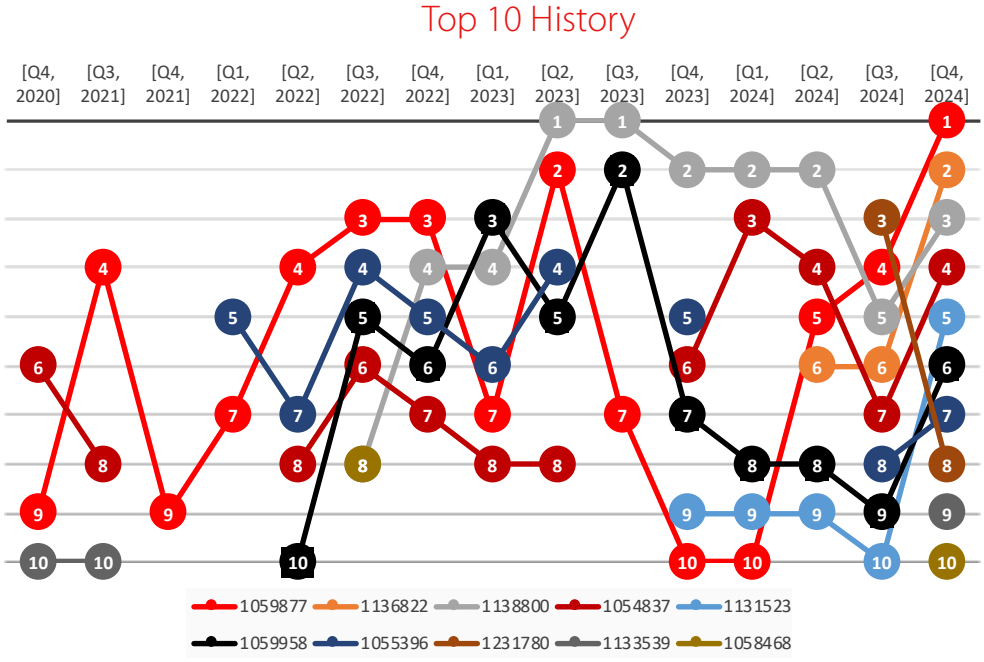


Figure 12. History of prominent signatures in the Top 10 since Q3 2022

New Detections in the Top 50

Signature	Type	Name	Affected OS	Rank
1138459	Web Threats	WEB SolarWinds Orion API Authentication Bypass -2 (CVE-2020-10148)	Other	39
1134968	Web Threats	WEB Moxa MXview Private Key Disclosure Vulnerability -2 (CVE-2017-7455)	Network Device	42
1134359	Web Threats	WEB Oracle WebLogic Server WorkContextX-mlInputAdapter Insecure Deserialization -1 (CVE-2017-10271)	Linux, Freebsd, Other Unix	45
1059436	DoS Attacks	WEB Apache Struts ParametersInterceptor ClassLoader Security Bypass -2 (CVE-2014-0094)	Windows, Linux, Freebsd, Solaris, Other Unix	46

Figure 13. New signatures this quarter among the top 50 signatures by volume.

Signature 1139459
This signature blocks exploit attempts against CVE-2020-10148, an authentication bypass vulnerability in the SolarWinds Orion platform. CISA pointed to this vulnerability in their analysis of the SUPERNOVA malware used in the attack against SolarWinds Orion customers at the end of 2020. The vulnerability stems from how the Orion web API handles certain HTTP request paths, allowing an attacker to skip authentication entirely by including particular substrings in the URL like WebResource.axd or ScriptResource.axd. The server mistakenly treats requests with these substrings in the request path as authenticated, which lets the attacker invoke API commands that should be restricted.

Signature 1134968
This is a vulnerability in Moxa MXview, a network management application. Version 2.8 of the application stored the private key for its web server in a publicly accessible location. Anyone with network access to the application could retrieve the private key from the server and use it to decrypt all other communications to and from the server.

Signature 1134359
This is an insecure deserialization vulnerability in Oracle WebLogic Server (part of Oracle Fusion Middleware) that was patched and disclosed in 2017. An unauthenticated attacker could exploit this vulnerability by sending a SOAP request with a specially crafted XML body. Deserialization vulnerabilities like this happen when an application converts user-supplied input into a programming object (like a function or a data variable) without sanitizing it. With the right payload, an attacker can trick the server into executing arbitrary code. In web servers, attackers commonly exploit deserialization flaws to deploy web shells, giving them extended remote shell access to the server that can even survive patching the original vulnerability.

Signature 1059436
The final new entry to the top 50 signature detections for the quarter was a decade-old flaw in the popular Apache Struts framework. This vulnerability allows an attacker to access and even modify sensitive internal Java class objects on a vulnerable web server. The vulnerability is caused by the Apache Struts' ParamtersInterceptor function, which is responsible for copying request parameters into the corresponding Java object's properties on the server. The function lets the attackers use a parameter named "class" to access and invoke the getClass() method of the action object that handles their request. Through this invocation, they can access the original class object and ultimately access other classes through the built-in getclassLoader() method. Ultimately, attackers can use this vulnerability to chain together an exploit capable of executing arbitrary code on the server.

Most-Widespread Network Attacks

While some network attacks generate high volumes of detections due to repeated exploitation attempts against a few vulnerable systems, others stand out because they impact a large number of unique networks. These widespread attacks often indicate opportunistic threat campaigns, where attackers scan broadly for exposed systems rather than targeting specific organizations. The prevalence of these attacks underscores the importance of proactive defense measures, as even well-maintained networks can be probed for weaknesses.

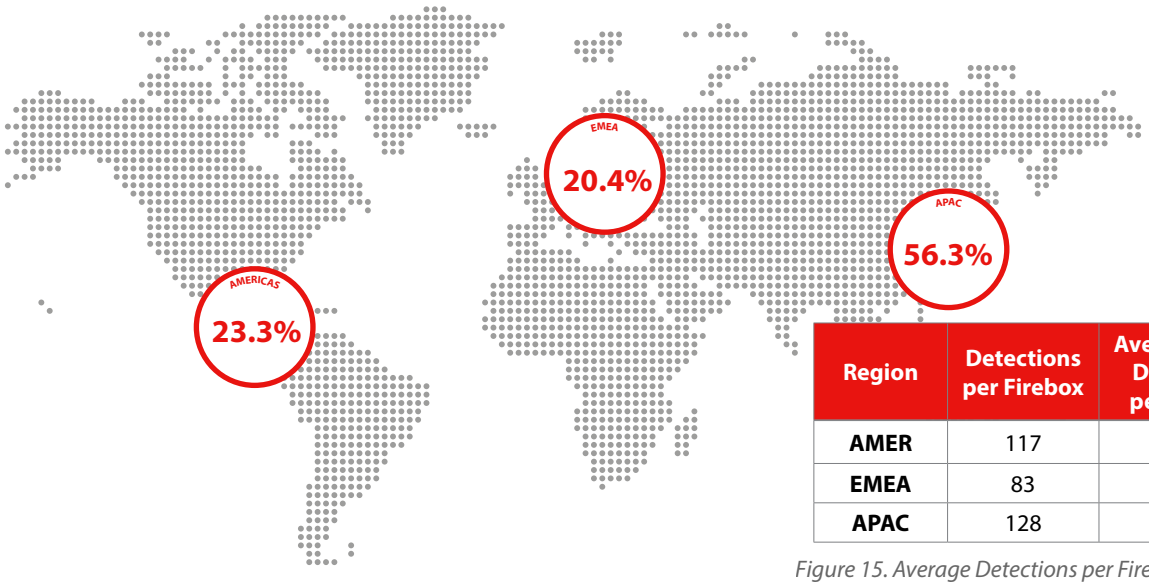
Signature	Name	Top 3 Countries by %			AMER %	EMEA %	APAC %
1131523	WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability -2 (CVE-2015-2425)	Spain 74.01	France 70.99	Poland 67.05	57.82	60.68	46.75
1136822	WEB dotCMS CMSFilter assets Access Control Weakness (CVE-2020-6754)	Germany 38.29	Brazil 31.55	Canada 15.05	12.99	21.20	10.39
1059877	WEB Directory Traversal -8	Switzerland 28.92	Australia 22.73	Germany 21.8	11.03	16.03	22.51
1138800	WEB Microsoft Exchange Server Remote Code Execution Vulnerability -6 (CVE-2021-26855)	Germany 20.51	Portugal 14.71	Switzerland 14.46	9.00	12.76	10.39
1132643	WEB Cross-Site Scripting -32	Brazil 27.38	USA 23.89	Canada 19.35	22.30	8.58	9.96

Figure 14. Top 5 Most-Widespread Network Attacks

The Most-Widespread Network Attacks table remains entirely unchanged from Q3 2024, with no new additions and in fact, the exact same rankings for each of the 5 exploits. With that said, there were some major changes in the countries that these exploit attempts most affected. For example, Spain showed up as the top target for the #1 most-widespread threat, with 74% of all networks having at least one detection. Meanwhile, central Europe remained a popular target for the generic Web Directory Traversal detection (1059877), with Switzerland showing up as the top victimized country.

Network Attacks by Region

For much of 2024, the APAC region (consisting of Asia and the Pacific) had an outsized share of network attacks. In Q4, we saw a minor rebalancing with APAC's share of network attacks dropping to just 39% of detections (weighted by the number of reporting networks). The bulk of the volume that left the APAC region made its way to the Americas, which increased from 22% of the share in Q3 to just shy of 36% in Q4. Europe, the Middle East, and Africa (EMEA) rose slightly from 19% in Q3 to 25% in Q4.



Region	Detections per Firebox	Average % IPS Detections per Firebox
AMER	117	35.67%
EMEA	83	25.30%
APAC	128	39.02%

Figure 15. Average Detections per Firebox by Region

Detections Percentage by Region

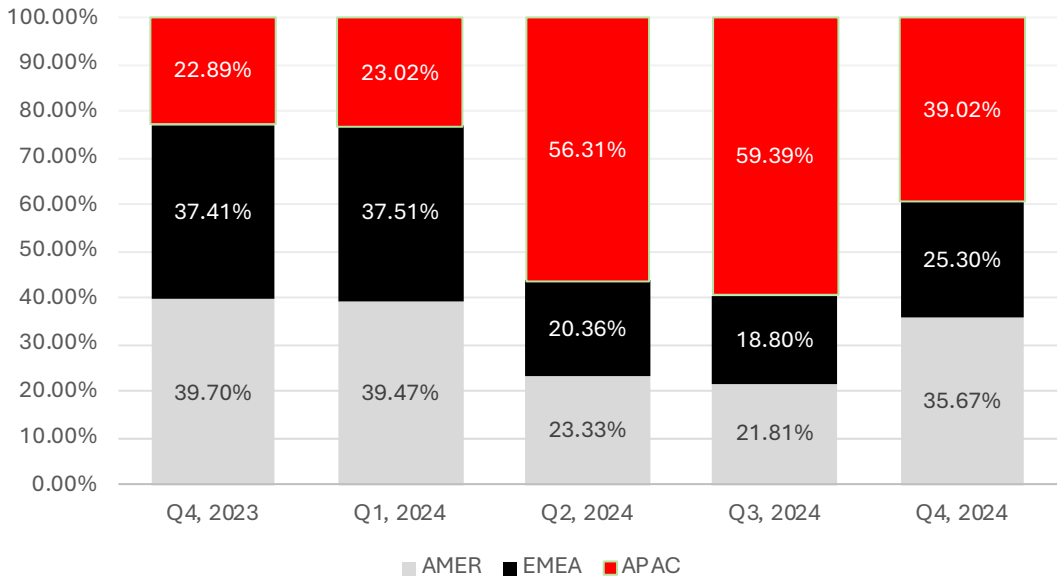


Figure 16. Average Detection per Firebox Percentage since Q4 2023

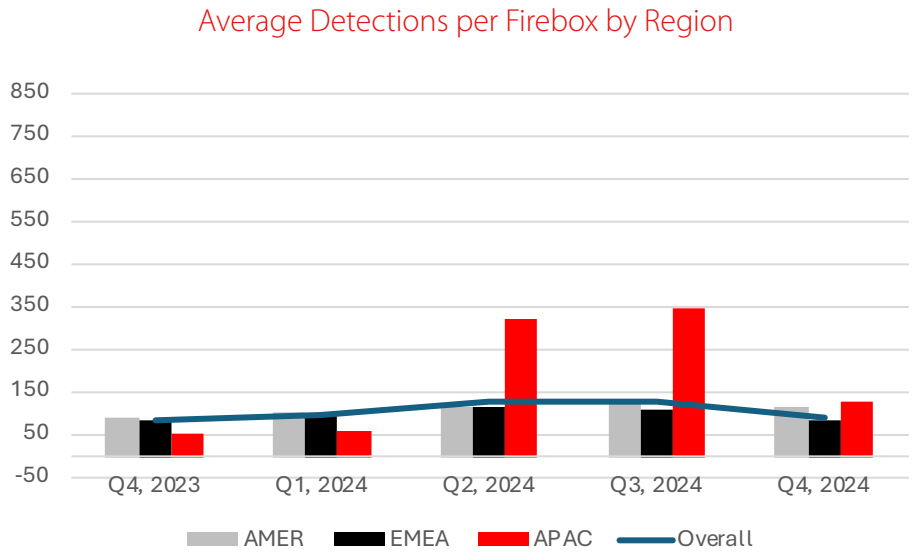


Figure 17. Average Detections per Firebox by Region since Q4 2023

Conclusion

Q4 2024's network attack trends reveal a cybersecurity landscape where old habits die hard for attackers. Many of the quarter's leading attack vectors were familiar from past reports, a clear indication that adversaries continue to find success exploiting years-old weaknesses. As we've observed before, once attackers identify an effective exploit, they will reuse it persistently rather than abandon it. This quarter was no exception; well-known vulnerabilities in web servers (from Microsoft IIS to open-source platforms) and infrastructure software remained lucrative targets. High-value systems like Microsoft Exchange and popular web apps continued to be in the crosshairs too, which is unsurprising given the potential payoff of compromising email or web servers.

From a defense perspective, the quarter's findings reinforce a two-pronged strategy: patch diligently and layer your defenses. Organizations must ensure that critical patches are applied, especially for the vulnerabilities named in this report, to close off the well-known holes attackers are probing. Many of these top attacks succeed due to unpatched systems or misconfiguration – issues that good security hygiene can address. At the same time, a robust intrusion prevention service (IPS) remains vital as a safety net, blocking exploit attempts (old and new alike) in case something slips through. In short, Q4's network attack trends highlight the importance of staying vigilant with the basics: keep systems updated, monitor for abnormal activity, and use layered defenses to catch the inevitable exploit attempts. By doing so, organizations can greatly mitigate the threats exemplified this quarter and be prepared for whatever new twists future quarters may bring.

DNS ANALYSIS

Domain names play a crucial role in cyberattacks, serving as gateways for phishing campaigns, malware distribution, and command and control infrastructure. Cybercriminals continue to employ tactics such as domain impersonation, typosquatting, and leveraging legitimate Cloud-based services to disguise malicious activity. This makes DNS filtering an essential component of a layered security strategy, helping organizations detect and block threats before they reach their targets. WatchGuard's DNSWatch service actively monitors domain resolution requests, preventing users from accessing known malicious sites and analyzing emerging trends in DNS-based threats.

Malware
polyfill[.]io
newage[.]newminer-sage[.]com
newage[.]radnew-age[.]com
p2[.]feefreepool[.]net *
t[.]ouler[.]cc
t[.]hwqloan[.]com
profetestruec[.]net
pcdnbus[.]ou2sv[.]com
backstage[.]cn[.]com
facturacionmx[.]autos

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.

* New in Q4 2025

Figure 18. Top Malware Domains

Top Malware Domains

Cybercriminals continue to rely on malicious domains for malware distribution, command and control (C2) operations, and illicit cryptomining. WatchGuard's DNSWatch service actively monitors and blocks these domains to protect organizations from DNS-based threats.

In Q4 2024, the top malware domains list remained largely unchanged from previous quarters, with one notable new entry: p2[.]feefreepool[.]net. This domain hosts a crypto mining pool, allowing Monero cryptocurrency miners to work together and pool their mining power. We added this specific mining pool domain to our block list in October after researchers found the Prometei botnet heavily using it in cryptomining attacks. Prometei is a stealthy, modular malware that spreads across networks using exploits, stolen credentials, and brute force attacks.

By hijacking system resources, Prometei forces infected machines to mine cryptocurrency without the victim's knowledge. The presence of p2.feefreepool.net in this quarter's DNS data confirms that cryptojacking remains an active and evolving threat.

Top Phishing Domains

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

Figure 19. Top Phishing Domains

Phishing remains one of the most effective cyberattack tactics, with threat actors continuously leveraging deceptive domains to trick users into revealing sensitive information. Attackers frequently impersonate well-known brands, financial institutions, and Cloud-based services to increase the credibility of their fraudulent campaigns. WatchGuard's DNSWatch service actively blocks access to these deceptive domains, protecting users from credential theft, malware infections, and financial fraud.

In Q4 2024, the top phishing domains list remained unchanged from the previous quarter, highlighting the continued use of persistent and high-impact phishing infrastructure. The SharePoint-themed phishing domains – such as unitednations-my[.]sharepoint[.]com, edusoantwerpen-my[.]sharepoint[.]com, and nucor-my[.]sharepoint[.]com – suggest that attackers are still exploiting business email compromise (BEC) tactics to target organizations relying on Microsoft 365 services. These phishing pages often mimic legitimate login portals to harvest credentials.

Additionally, domains like bestsports-stream[.]com and www[.]898[.]tv demonstrate how attackers use entertainment and streaming-themed lures to attract unsuspecting users. Fraudulent promotional emails or pop-ups often redirect victims to these phishing pages, where they are prompted to enter personal information or download malicious files.

Despite no new domains appearing on the list, the persistence of these phishing sites underscores the importance of ongoing security awareness training, email filtering, and DNS-layer protection. Organizations should continue monitoring phishing trends and reinforcing best practices, such as verifying URLs before entering credentials and enabling multi-factor authentication (MFA) to mitigate credential theft risks.

Top Compromised Domains

Compromised
ssp[.]adriver[.]ru
www[.]sharebutton[.]co
www[.]omegabrasil[.]net *
wieczniezywechoinki[.]pl
fernandestechnical[.]com *
www[.]uniodonto[.]coop[.]br
epicunitscan[.]info
eficacia[.]com[.]co *
stopify[.]co
a[.]pomf[.]cat

* New in Q4 2024

Figure 20. Top Compromised Domains

Cybercriminals continue to exploit legitimate but compromised websites to distribute malware, launch phishing attacks, and conduct financial fraud. Unlike domains specifically registered for malicious purposes, these websites often belong to reputable businesses, making them more likely to bypass traditional security measures. Attackers inject malicious scripts, host payloads, or leverage vulnerabilities in content management systems (CMS) to turn these sites into unwitting vectors of cyber threats. WatchGuard's DNSWatch service monitors and blocks these compromised domains, helping prevent users from unknowingly accessing malicious content.

In Q4 2024, the top compromised domains list saw three new additions, all of which were linked to distinct cyberattack campaigns.

www[.]omegabrasil[.]net and eficacia[.]com[.]co joined our threat feed in June 2024. Both domains were associated with an "Ether-Hiding" attack, where threat actors embedded malicious code within the Binance blockchain. Attackers injected fake web browser update notifications into these otherwise-benign websites, tricking visitors into downloading and executing malware. This technique demonstrates how cybercriminals are abusing decentralized infrastructure to evade detection and maintain persistence.

We added fernandestechnical[.]com to our feed in March 2024 after finding it used by Magnet Goblin, a financially motivated threat actor that we previously covered in our reports. Magnet Goblin has targeted businesses with custom malware payloads and stealthy persistence techniques, often exploiting known software vulnerabilities to compromise legitimate websites.

Beyond these new entries, previously listed compromised domains continued to pose risks, serving as launch points for malvertising, credential theft, and malware distribution. The growing trend of leveraging blockchain technology and deceptive browser-update lures highlights the need for proactive website security, timely patching, and DNS filtering to mitigate these evolving threats.

FIREBOX FEED: DEFENSE LEARNINGS

The cyber threat landscape underscored the need for robust, proactive defenses. As attackers evolve their tactics, securing your data doesn't stop where the data resides but extends to all devices and users interacting with your network. From endpoints to IoT, every touchpoint is a potential vulnerability. Below are three critical takeaways to strengthen protections, ensuring comprehensive coverage across the ever-expanding attack surface in this dynamic digital environment.

01 Monitor and Restrict Unusual Tools:

Users should report suspicious downloads, like keygens linked to Variant.MSILHeracles, which often bundle malware such as Remcos or Formbook, amplifying risks. Admins must vigilantly monitor networks for unauthorized tools like Impacket (Application.Agent.LGP), a Python-based hacktool suite used for protocol manipulation and credential theft. By setting up alerts for unusual activity and restricting execution of unknown scripts, admins can halt reconnaissance or lateral movement. This proactive stance prevents attackers from leveraging legitimate-looking tools to infiltrate systems unnoticed, safeguarding critical infrastructure.

02 Layer Protection for Endpoints and IoT Devices

With droppers like Trojan.Sesfix.1 delivering coinminers and botnets like Trojan.Linux.Mirai.1 targeting Linux and IoT, layered security is critical. The data supports hardening these systems through zero trust, strong credentials, and firmware updates to curb malware persistence and spread. Memory-loading techniques and IoT exploitation, as seen in Xmrig infections, highlight vulnerabilities requiring proactive measures. We recommend implementing these steps to limit resource-hijacking and DDoS risks, addressing Q4's diverse threat vectors effectively.

03 Prioritize Relentless Patching

The report underscores that patching remains vital, with attackers exploiting old vulnerabilities like CVE-2017-0199 in Office and ProxyLogon in Exchange, alongside newer flaws like HAProxy. Security professionals should advocate for rigorous update schedules across servers and endpoints, coupled with audits of web servers and CMS platforms to eliminate misconfigurations. This shrinks the attack surface against persistent exploits like SQL injection and directory traversal still thriving a decade on, ensuring organizations don't fall prey to adversaries banking on outdated systems.

ENDPOINT THREAT TRENDS

WatchGuard Endpoint Protection, Detection and Response (EPDR) combines both Endpoint Protection (EPP) and Endpoint Detection and Response (EDR) into one comprehensive solution. Users can expect moment-in-time protection from malware and non-intrusive response to suspicious threats across all protected endpoints. Advanced EPDR users receive additional threat hunting service granularity and more telemetry, all in one central location. Of these users, some opt to send WatchGuard anonymous data, which we aggregate into this report; specifically, the Endpoint section herein. The more data we get, the more we can share in this report!

WatchGuard EPDR data is not the only inclusion in this section. We also use the Ransomware Tracker data, which includes double extortion victim summations and active and inactive group coverage. We then sprinkle in notable breaches from these groups and other ransomware-related events to help decision-makers to know which industries and organization types are targeted by these groups. Couple that data with specific endpoint telemetry from WatchGuard EPDR and we believe this report better enables MSPs and businesses to prioritize where to focus their time.

Here is this quarter's coverage:

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

If you have read the Internet Security Report before, you are familiar with our due diligence in trying to expand the endpoint data set and improving readability. Whether that is in the form of changing the way a graph looks, altering data types, or drilling down into a subsection to augment understanding. This quarter is no exception to this tradition. In fact, we have made more changes this quarter than ever before. Not only that, but it is the last quarter of the year and we include data that only appears in Q4. We will summarize the changes and then notify you again when we get to the appropriate subsections.

The first major change for this quarter is the alteration of raw numbers into composition percentages. When we present a table or graph with various large numbers, the human mind instinctively attempts to determine the ratio of a data point with respect to the entire data set. For example, if there is a table with five data points, one has 100,000 and the other four have 50,000. We instinctively try to determine how much 100,000 is with respect to the sum of all data points (e.g., 100,000/(100,000+50,000*4) -> 100,000/300,000 = 33.33%). This change is present in the Number of Machines Affected, Alerts by Technology, Alerts by Exploit Type, and Attack Vectors subsections.

Other sections had other subtle changes such as adding a table column to discern the quarter-over-quarter differences. For example, in the Alerts by Exploit Type subsection, we altered the raw data to alert composition, as described above, and then added a column that calculates the alert composition difference from the quarter prior. Other subsections with these minor changes include the Top 30 Countries, Top 10 Threat Hunting Rule Invocations, and the Threat Hunting MITRE ATT&CK matrix alert subsections.

The most notable change this quarter is the Attack Vectors subsection, which has evolved more than any other subsection. Years ago, we tracked five or six data points for Attack Vectors and included a summation pie graph to visualize a threat actor's manner of infection. Then, we drilled down into each data point to provide more granular attack vectors. Now, as of this quarter, we have added more data points and are now providing this granular data for every data point. The increase in data we ingest allows us to relay that information to readers. We will expand on these data points when we get to the Attack Vectors subsection.

The final changes made to the Endpoint section primarily pertain to it being the last quarter of the year, but we also enhanced the notable ransomware breaches subsection. That subsection now includes notable ransomware events including law enforcement actions and modifications to the inner workings of ransomware groups. We differentiate breaches and events using the Notable Ransomware Events and Notable Breaches labels. The Alerts by Number of Machines Affected, Alerts by Technology, and Ransomware Landscape subsections include annual changes only appearing for those in the fourth quarter.

That is enough staging for now. Let us begin with Malware Frequency as is customary for the Endpoint section.

MALWARE FREQUENCY

We discussed at length the changes throughout this report, but the Malware Frequency subsection had absolutely no alterations except for the data itself. We define Malware Frequency in two ways. The first is the total number of malware threats, which is the number of unique malware hashes observed in the quarter. Thus, we do not count multiple instances of the same malware hash. Right out of the gate, total unique malware threats are significantly down for the quarter, showing historically low rates. Considering Q3 had uncharacteristic high malware threats, combined with Q4's atypically low levels, the quarter-over-quarter reduction is also a historic 91.14% decrease. If we assume the third quarter was an outlier, the change from Q2 to Q4 is still abnormal with a 64.51% decrease. Therefore, we have observed never-before-seen low rates of unique malware threats this quarter, however you put it.

Total Malware Threats	37,250

Figure 21. Q4 2024 QoQ Total Malware Threats

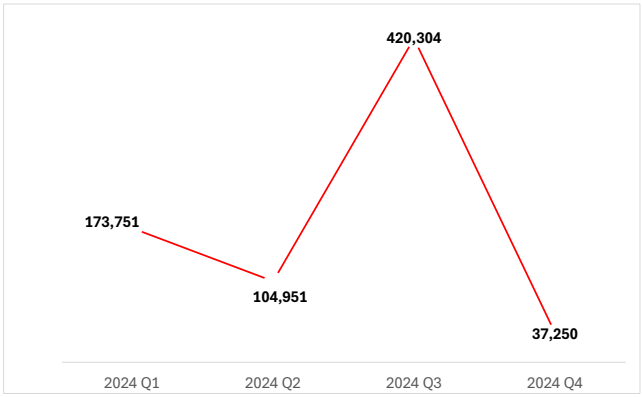


Figure 22. Q4 2024 QoQ Total Malware Threats

The second way we determine malware frequency is all the newly observed malware threats previously unseen and unclassified by WatchGuard. We then set this to a ratio of "per 100k active machines" to simulate a moderate-sized organization, meaning we skew the number of alerts for every 100k active EPDR-protected systems. If the total malware threats were historically low, it is almost a certainty that we will not see a bunch of new malware, and that is the case here. We tallied only eight new threats per 100k active machines this quarter, which again is historically low. Last quarter we observed 36 per 100k active machines even with an outlying high number of total malware threats. This equals a 77.78% reduction from last quarter. We use other subsections below to try and better understand what constituted this reduction, and if we are lucky, what caused it.

New Threats Blocked per 100k Active Machines	8

Figure 23: Q4 2024 New Malware Threats (Previously Unknown)

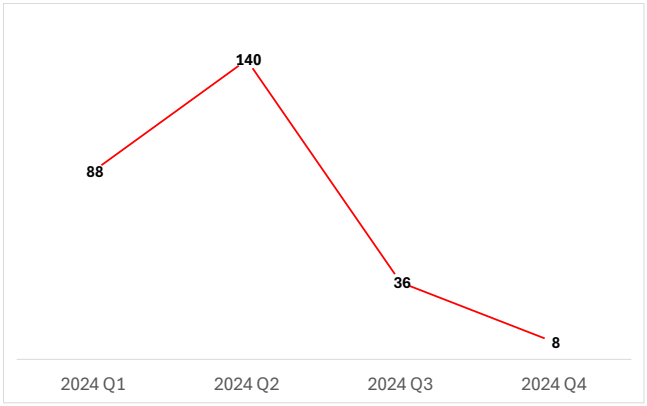


Figure 24. Q4 2024 QoQ New Malware Threats Per 100k Active Machines

Alerts by Number of Machines Affected

The next few subsections, including this one, take the malware threats from the previous Malware Frequency subsection and expands on it. It attempts to better understand why the Malware Frequency numbers the way they are. Alerts by Number of Machines Affected helps explain threats that are isolated or are more widespread. Malware appearing on only one machine is more targeted or isolated. Whereas malware appearing on more than one hundred machines, for example, are usually spam attacks or widespread botnet campaigns targeting whichever users click on a phish or accidentally navigate to infected websites. We define the schema for how we tally data points from this subsection below.

- **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.

By no surprise, the composition of alerts skews towards malware on one machine with 87.80% of all alerts. However, considering most alerts are for those appearing on only one machine, a 9.64% decrease from the quarter prior is a significant drop. This is in line with the massive decrease in total malware threats earlier in the section. The reduction in Malware Frequency is due to a decrease in targeted or one-off attacks described by this data. In its place, malware appearing on between two and five machines saw the increase this quarter – 6.99%. The others saw minor increases that are almost negligible to the overall count.

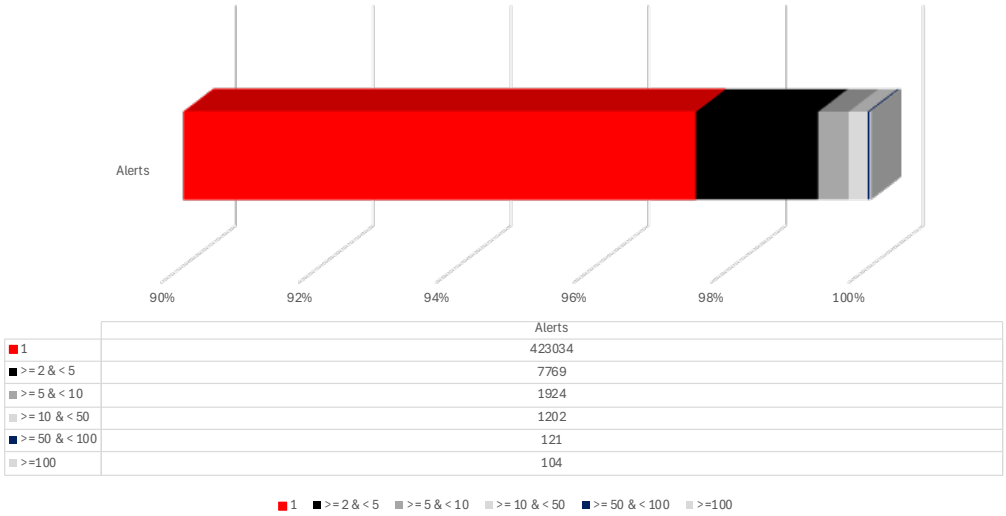


Figure 25. Q4 2024 Alerts by Number of Machines Affected

For this quarter only, we have included another graph that shows the alert composition totals for each schema. The x-axis defines the four quarters, left to right. The y-axis is the alert composition total, beginning at 80%. The colors are the different schemas. The graph shows a similar sharp increase like malware frequency's Total Malware Threats that correlates to malware on only one machine. This supports the theory that isolated malware was the cause of the atypical increase in total malware threats for last quarter.

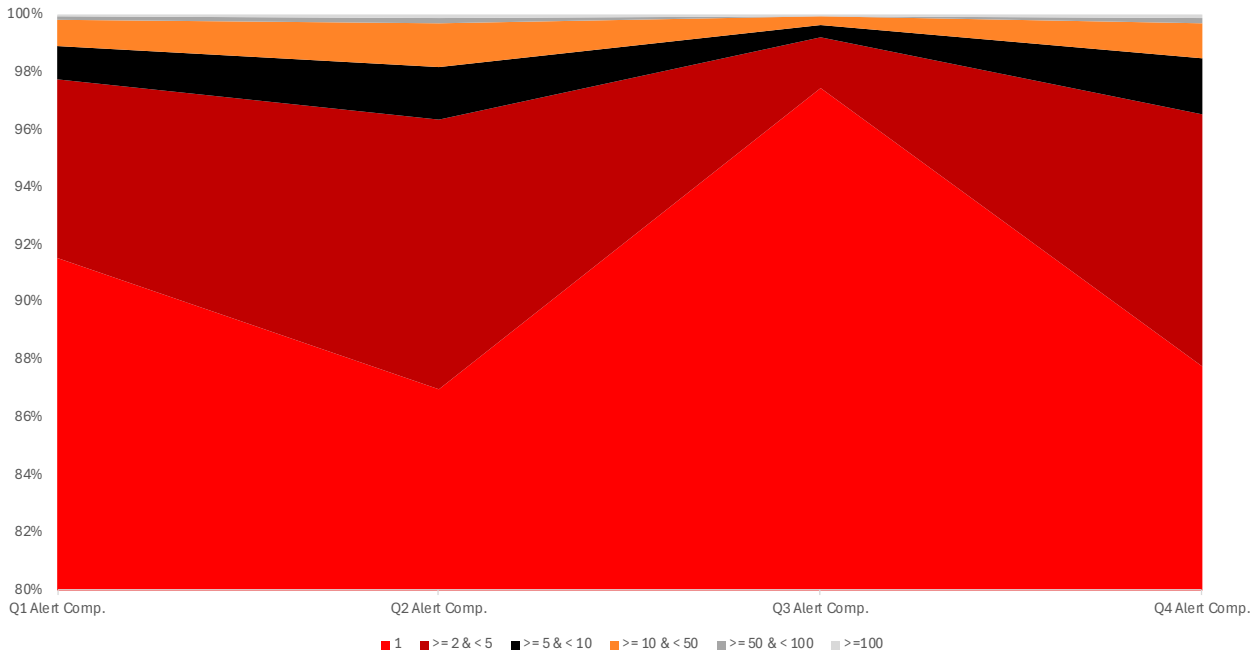


Figure 26. Q4 2024 Alerts by Number of Machines Affected

Defense in Depth

Defense in depth gets its name from the idea that multiple technologies layered on top of one another provide a stepping-stone defensive posture that attacks must try and navigate through. Thus, bypassing only one technology will not necessarily result in a block attack. Threat actors must successfully bypass all technologies. This is why defense in depth is the recommended approach for both networks and endpoints. In fact, network solutions combined with endpoint solutions in and of itself is defense in depth, but if these measures exist across the network and all endpoints, the defense in depth compounds. For WatchGuard EPDR-protected endpoints, we employ the following six technologies to thwart attacks.

Endpoint Technologies

- **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.

Total malware threats, never-before-seen malware, and malware appearing on one machine all saw drastic reductions from last quarter. So, which technology compliments this reduction? The only technology with a decreasing quarter-over-quarter alert composition was AD360 Endpoint Detection, which is traditionally the first line of defense for EPDR. AD360 Endpoint Detection functions as an antivirus that detects malware by signatures. Interestingly, a sharp decrease in all these numbers was akin to quarter two of this year, which showed the same behaviors. Therefore, it's easy to surmise that easy-to-detect malware threats appearing on only one machine comprise most of the malware landscape, and these are subsequently blocked immediately upon arriving on a protected endpoint.

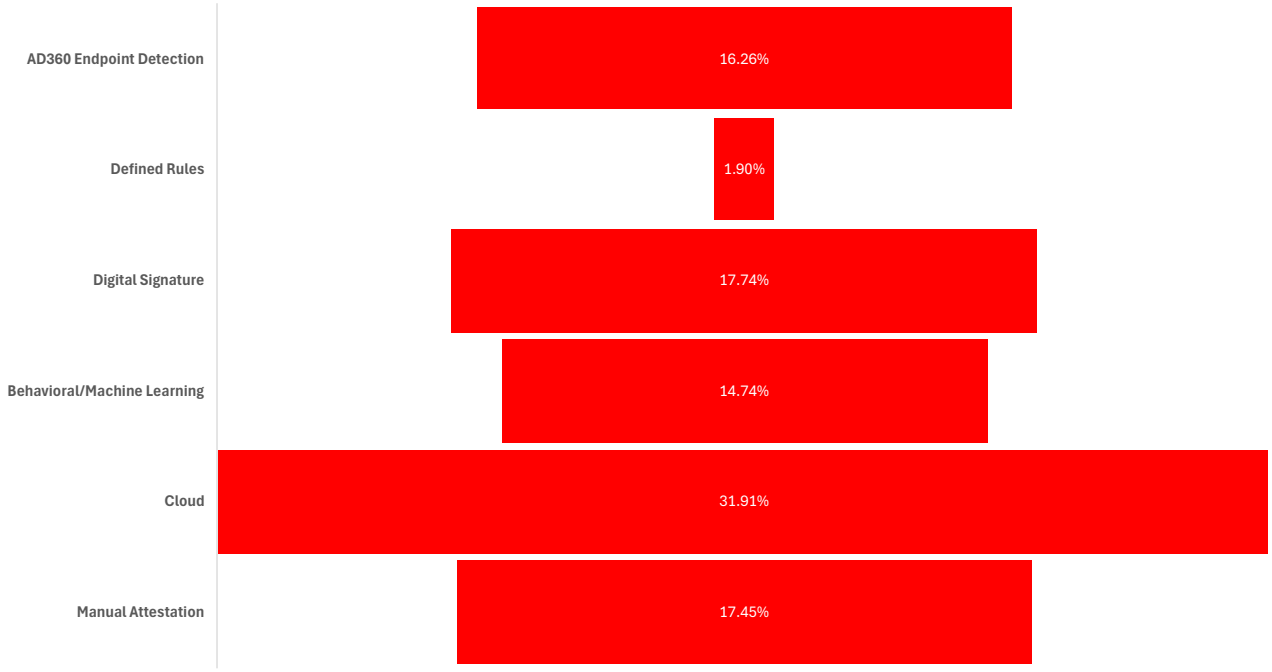


Figure 27. Q4 2024 Alerts by Number of Machines Affected

As promised, we have included annual data for this section since it is the last quarter of 2024. This year we observed a zigzag malware landscape where quarters one was similar to Q3, and Q2 was similar to Q4. There was no consistency throughout the year, which is a nightmare for decision-makers. We can also conclude that neither of these quarters are true outliers because any given quarter had a different complimentary quarter in terms of the data. Q1 and Q3 were driven by AD360 Endpoint Detections. Whereas Q2 and Q4 were more balanced, but spearheaded by Cloud detections. This quarter was the most balanced of them all, with all technologies receiving a similar number of alerts, except for Defined Rules.

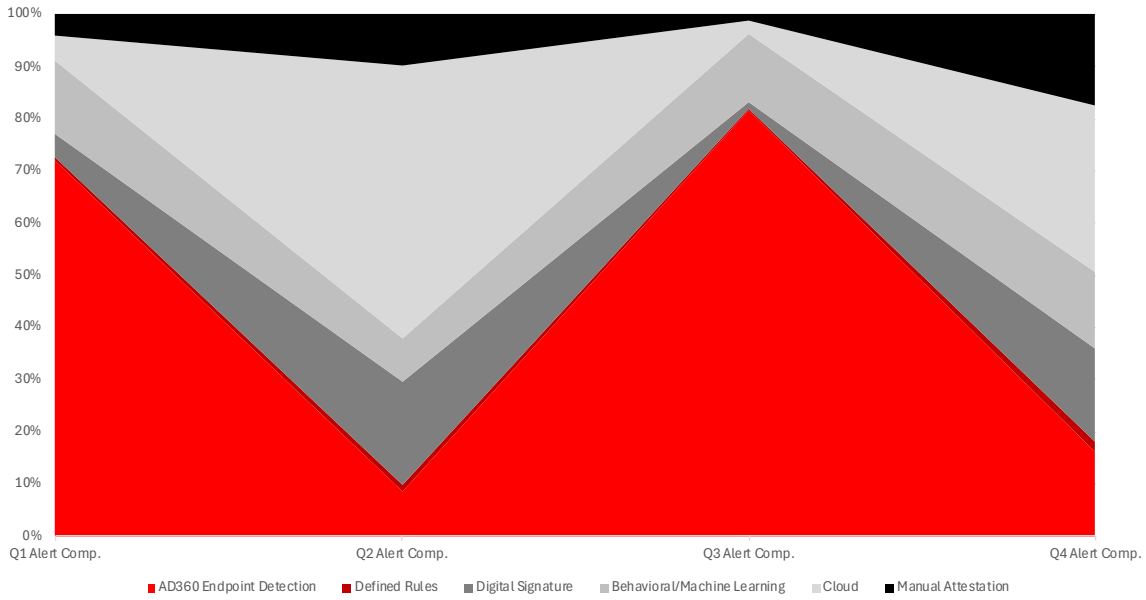


Figure 28. Q4 2024 Alerts by Number of Machines Affected

Alerts by Exploit Type

As opposed to Alerts by Number of Machines Affected and Defense in Depth, the data in this subsection begins to describe which behaviors resulted in a blocked detection. Alerts by Exploit Type are exactly what it sounds like; these are alerts invoked via common exploit behaviors. For example, if malware attempts to hollow out a process and inject itself into it, we define that in our RunPE exploit label, and each block from that technique tallies there. You can review more about the definitions of each exploit on WatchGuard's Knowledge Base article located **here**.

The only exploit behavior with a drastic increase in occurrences was PsReflectiveLoader1, which describes malware that locally leverages PowerShell to inject payloads in its own memory. An example of this is Mimikatz. On the other hand, the exploit with the sharpest decrease from last quarter was the second most alerted exploit – RemoteAPCInjection. The description of this exploit is quite literal. RemoteAPCInjection is when malware uses Asynchronous Procedure Calls (APCs) to inject code remotely. As for the rest of the exploits, the results were a mixed bag, and we will let the data on the table (and the Knowledge Base article) do the talking.

Technology	Q3 Alerts	Q4 Alerts	Raw Difference from Q3	Percentage Difference from Q3
PsReflectiveLoader1	7,087	94,583	+87496	61.21%
RemoteAPCInjection	7,407	15,698	+8291	10.16%
NetReflectiveLoader	2,155	14,731	+12576	9.53%
ShellcodeBehavior	757	11,352	+10595	7.35%
RunPE	2,836	8,111	+5275	5.25%
WinlogonInjection	1,031	4,236	+3205	2.74%
APC_Exec	35	2,811	+2776	1.82%
DumpLsass	1,295	1,286	-9	0.83%
AmsiBypass	1,813	835	-978	0.54%
ThreadHijacking	430	385	-45	0.25%
ROP1	2,004	173	-1831	0.11%
PsReflectiveLoader2	2	131	+129	0.08%
IE_GodMode	132	120	-12	0.08%
ReflectiveLoader	29	37	+8	0.02%
DynamicExec	20	19	-1	0.01%
HookBypass	24	15	-9	0.01%

Figure 29. Q4 2024 Alerts by Number of Machines Affected

Alerts by Top 30 Countries Affected

This subsection shows where the alerts came from no matter what technology blocked it, how many machines it was on, or what behavior invoked it. Naturally, the countries with more EPDR licenses will have the most alerts. To combat this, we have created a simple ratio formula to even the playing field. We take the alerts for a given country and divide it by the active machines (machines with active EPDR licenses). It is important to remind you that this only pertains to the EPDR-protected systems that have also opted in to share anonymous data.

The simple Alert Coefficient (AC) equation is below.

In the introduction to this section, we touched on how this was one of the enhanced subsections where we added an additional column to provide more insight. The column we added is "AC Diff from Q3," which takes the difference of the Alert Coefficient from the quarter prior. We placed it between the Alert Coefficient (AC) column and the Order Diff from Q3 column. Of course, if the country was not on the list in the quarter prior, we would simply label both columns as NEW.

Laos saw the largest increase from Q3, which made it into the top country affected this quarter based on AC. Other countries with AC increases were Armenia, Tajikistan, and Nigeria. There were a myriad of new countries that did not appear in Q3: China, India, Zimbabwe, Luxembourg, Macedonia, Singapore, Mozambique, Dominican Republic, Angola, Ghana, and Ecuador. Surprisingly, three countries had the exact same AC as the quarter prior: Norfolk Island, Vietnam, and Trinidad and Tobago. The rest of the countries in the list saw slight-to-moderate AC decreases, expect for Cuba, which was the top country for last quarter and had a significant decrease of -0.92.

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

Country	Alert Coefficient	Order Difference from Q2
Laos	0.51	*+5*
Morocco	0.38	*+1*
Armenia	0.28	*+1*
Cuba	0.14	*-3*
China	0.11	*NEW*
India	0.09	*NEW*
Norfolk Island	0.06	*+10*
Bolivia	0.06	*+1*
Pakistan	0.06	*-7*
Zimbabwe	0.06	*NEW*
Bangladesh	0.06	*+2*
Vietnam	0.06	*+4*
Tajikistan	0.05	*+8*
Nigeria	0.05	*+11*
Turkey	0.04	-
Luxembourg	0.04	*NEW*
Indonesia	0.04	*-3*
Macedonia	0.03	*NEW*
Singapore	0.03	*NEW*
Trinidad and Tobago	0.03	*+8*
Malaysia	0.03	*-2*
Mozambique	0.03	*NEW*
Andorra	0.03	*-3*
Dominican Republic	0.03	*NEW*
Guatemala	0.02	*-14*
Angola	0.02	*NEW*
Thailand	0.02	*-3*
Paraguay	0.02	*-6*
Ghana	0.02	*NEW*
Ecuador	0.02	*NEW*

Figure 30. Q4 2024 Alerts by Top 30 Countries Affected

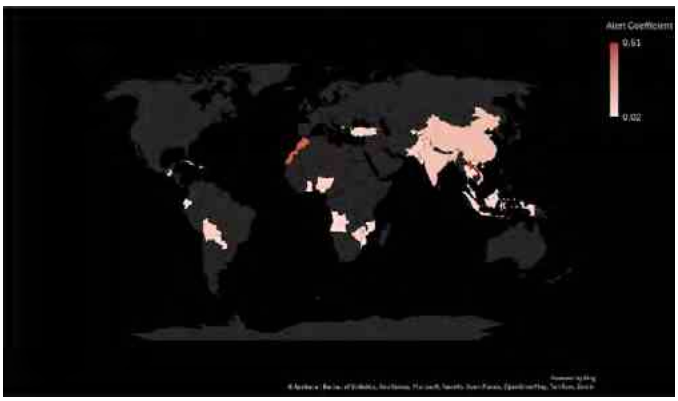


Figure 31. Q4 2024 Alerts by Top 30 Countries Affected

TOP MALWARE AND PUPS

The top 10 malware and PUPs for each quarter are a favorite for many readers because it does not describe arbitrary aggregated data. It defines and describes specific malware families and software that is attempting to intrude on systems. The theme for this quarter appears to be record-shattering, because the top 10 malware for this quarter was also historic. The top five from the list are all related to ransomware, which foreshadows the ransomware landscape section later in this section (hint: the ransomware numbers are up across the board!). On the other hand, the top 10 PUPs are more of the same from last quarter.

Top 10 Most Prevalent Malware

As we just touched on, five of the top 10 malware were ransomware related. However, only three of these were ransomware encryptor payloads. There were two Black Basta payloads and one Play encryptor. The other two ransomware-related files were a Black Basta loader and an OpenSSL DLL used by the group. The other five files were mostly information stealers or had information-stealing capabilities. A malicious coinminer steals computer resources to mine cryptocurrency on behalf of a threat actor. Lumma, Conficker, and Moonlight all have information-stealing capabilities, with the latter two having worm capabilities. The other malware in the top ten was a LNK (shortcut) file that executed a PowerShell script. This is common for malware to use to download additional payloads. We provide additional details about each of these malware families below.

MD5	Signature	Alerts	Classification Attestation
0CC6739009F44EEC91FAED0A63F9CC81	Trj/Agent.OOX	464	Malicious OpenSSL DLL (Black Basta)
EAE2C3ED7CE3E11A0668304B21077320	Trj/Agent.OOX	456	Black Basta Ransomware
C6D541E4D782D8EE8967EC8DFF0E886B	Trj/Agent.OOX	452	Black Basta Loader
8018A731E57DA5E697C96E21632D4476	Trj/Agent.OOX	450	Black Basta Ransomware
C2945F7ACA2C017D6E4D35C5EA41255D	Trj/GdSda.A	250	Play Ransomware
1F5FFF9F9E92965F29BFA92B60BFC0FF	Trj/Agent.AEZG	239	Malicious Coin Miner
9B20069911C33DBB8DC65640CF193731	Trj/LnkRun.B	108	LNK that executes PS1
6AE17B0BDDDA685EAA622CEF4BA2E805	Trj/CI.A	103	Lumma Stealer
7D9542EF7C46ED5E80C23153DD5319F2	W32/Conficker.C.worm	100	Conficker Worm
D60361B58C0CAABA002CD9427A8DE32D	W32/Moonlight.A.worm	100	Moonlight Worm

Figure 32. Q4 2024 Top 10 Most Prevalent Malware

Black Basta

Black Basta is both the name of the ransomware group and the name of the group's encryption software. They first appeared around February 2022 and is widely believed to be composed of former Conti and Revil members, another two ransomware groups. Black Basta is also a ransomware-as-a-service (RaaS) that allows affiliates and other users to use their encryption software and infrastructure for a small cut of the financial gains. Most splits are 90/10 and 80/20. Later in 2022, the group upgraded their encryptor to Black Basta v2. The first version used a combination of Cha-Cha20 and RSA-4096 and their second version leveraged a hybrid encryption scheme of XChaCha20 and the NIST P-521 elliptical curve algorithm. Using these encryptors, the group has coerced hundreds of victims, only a fraction of which are ever published.

Read more about **Black Basta** and **Black Basta v2** on the Ransomware Tracker.

Play

Play is a ransomware group with several connections to the old Conti ransomware group and Quantum, which was an offshoot operation with former Conti members. The Play group operators primarily use phishing email attachments and software exploits to infiltrate systems. They have been known to exploit a known FortiGate exploit to begin their infection chain. From there they use common hacker tools and living-off-the-land binaries to perform continued attacks on systems rresulting in encryption via their encryptor. The encryptor utilizes AES to encrypt files and RSA to encrypt the AES symmetric key.

Read more about **Play** on the Ransomware Tracker.

Malicious Coinminer

Coinminer is short for cryptocurrency miner and is inherently non-malicious. Cryptocurrency mining is a natural process for acquiring cryptocurrency on some blockchains, the most obvious being bitcoin. What makes a coinminer malicious is the context and telemetry of the file in question. An example of a malicious coinmining is executing software that installs a coinminer without the user's knowledge or consent or is dropped from an information stealer.

Malicious LNK-PS1
A LNK file (.lnk) is a Windows shortcut file that points to another file location on the system. These commonly exist on the desktop where users can double-click them and run an executable in another location on the computer. Threat actors leverage LNK files to execute scripts without the user's knowledge. The path location is actually a small script that loads additional malware.

Lumma Stealer
Lumma Stealer is a malware-as-a-service information stealer that has existed since late 2022. It targets the usual information on victim machines such as browser extensions, passwords, and cryptocurrency wallets. It also has capabilities as a loader to install additional payloads and exfiltrates stolen data using HTTP POST requests.

Conficker
Conficker is a worm that has been around since 2008. It is usually spread via USB thumb drives and attempts to self-propagate to other systems and networks because it is a worm. What is unique about Conficker is that it uses a domain-generation algorithm (DGA) to connect to URLs that host additional malware or function 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).

Moonlight
Moonlight is a worm that spreads in multiple ways. Once on a system, it harvests information like an information stealer and then duplicates itself to several locations for persistence. It then uses stolen emails and sends phishing attacks to these users to spread further. It also attempts to spread to network share drives disguised as legitimate files. What makes Moonlight even more unique is its polymorphic nature that, in addition to propagation, makes it difficult to detect with basic antivirus products. A more robust solution is necessary to fully disinfect.

Top 10 Most-Prevalent PUPs

The top 10 PUPs (potentially unwanted programs) were mostly uneventful. Seven of the 10 appeared in the top 10 list last quarter. We denote repeats with a red asterisk in the table. The three new ones include the Browser Security application, which is a legitimate application that tracks user behavior, earning it a PUP designation. The second was Jdownloader 2, again, another genuine application, but the installer comes bundled with adware in the form of toolbars. The last new addition is a Softonic installer. Softonic is also genuine software, but it to has an installer bundled with adware. Noticing a theme here? If your software uses an installer bundled with other external software, it is a PUP.

MD5	Signature	Alerts	Classification Attestation
2914300A6E0CDF7ED242505958AC0BB5*	HackingTool/ AutoKMS	752	KMS_VL_ALL_AIO
FC3B93E042DE5FA569A8379D46BCE506*	PUP/Hacktool	431	Mail PassView
136C60612962C8FA36B6A46009BF8CE8	PUP/ BrowserSecurity	399	Browser Security
F7191FE14D2F5E7C4939C2FCA5F828C2*	PUP/Generic	371	RVEraser
8D0C31D282CC9194791EA850041C6C45*	HackingTool/ AutoKMS	367	KMSPico
CFE1C391464C446099A5EB33276F6D57*	HackingTool/ AutoKMS	335	AutoPico
219218AE29B2F9DFC8F6B745C004B1E3*	PUP/Patcher	249	AMTLib
A9DAAD0505339EC723069CAFD14C781B	PUP/Multitoolbar	198	Jdownloader 2
AC8CA19033E167CAE06E3AB4A5E242C5	PUP/Softonic	180	Softonic Installer
B4440EEA7367C3FB04A89225DF4022A6*	PUP/TechUtilities	180	PDFixers

Figure 33. Q4 2024 Top 10 Most Prevalent PUPs

PUP Signature Descriptions

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

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 cannot 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 is the proprietary ones that we usually label as malware.

PUP/BrowserSecurity
Browser Security is a legitimate application and is not explicitly malicious. However, most endpoint solutions consider this a PUP because it usually installs on users computers without their consent. These are usually always classified as PUPs, but because Brower Security collects information about browsing activity, which could include sensitive data, there is no doubt it is, at minimum, a PUP.

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

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

PUP/Multitoolbar
This signature defines software that installs multiple toolbars or extensions on a system, usually without the user's explicit consent. These are commonly bundled in installers where a good portion of users click the button that will progress them through the installation the fastest, not knowing these toolbars are bundled in; they are checked by default and must be disabled during installation. Many of them come with additional adware too.

PUP/Softonic
Softonic is a legitimate file download service used by numerous applications. It is almost always classified as a PUP because the software included in their installations includes adware, toolbars, or other PUPs. Endpoint solutions and analysts sometimes classify these installers as PUP/BundleInstaller. Both are correct and both are PUPs by WatchGuard's standards.

PUP/TechUtilities
"TechUtilities" refers to software meant for computer administrators but performs possible suspicious or unwarranted actions. An example of a TechUtility PUP are PC optimization tools that mess with system settings that have not been requested by the user.

ATTACK VECTORS

In the introduction, we talked about how Attack Vectors contained the most drastic changes for this quarter, and this will be apparent when seeing the subheaders and corresponding graphs. For one, there are more graphs, a lot of them! The section got a complete overhaul on how we collect the data, and we collect more of it internally, which allows us to relay that to readers. Previously, we collected data on these Attack Vectors: Acrobat, Browsers, Office, Other, Scripts, and Windows. Now, we also have Coding Software, Database Software, and Remote Access Software. Also, we have renamed the Office Attack Vector to Microsoft 365, which encompasses all Microsoft 365 software, not just Office-related software. Additionally, we have revamped the Windows Attack Vector to highlight living-off-the-land binaries. We renamed it to Windows (LOLBAS) to reflect this change. Each attack vector now has a subsection within them (except the Other Attack Vector) to highlight exactly what processes we are seeing throw alerts. All Attack Vectors have more granular descriptions 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.

Coding Software – Attack Vectors here are from software used for coding (i.e., software engineering). If an Attack Vector is both coding software and a scripting tool, we determine the purpose of the processed invoked and increment there. Therefore, if there is a Python executable and a Python-related DLL, the Python executable is a Script – it is used to run a Python script – and we count the DLL as Coding Software.

Database Software – Database Software is an Attack Vector describing software used to manage and operate databases. Common database software is PostgreSQL, Microsoft Access, and MongoDB.

Microsoft 365 – This Attack Vector encompasses all applications under the Microsoft 365 umbrella. The complete list is located **here.**

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.

Remote Access – Attackers commonly use remote access software to remotely control victim systems. Hence the name. These tools are important for system admins and other IT professionals, but hackers notoriously abuse them to distribute malware. Some remote access tools include Radmin, LogMeIn, TeamViewer, and Impero.

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 attacked operating system, it is no wonder PowerShell continues to skew the results for Windows detections.

Windows (LOLBAS) – 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. These are commonly called living-off-the-land binaries (LOLBAS).

Attack Vectors Summation

Aside from the aforementioned changes, we also made the alteration to track data in alert composition percentages as opposed to raw numbers. We always calculated this data when collecting and analyzing this data, and we instinctively use alert compositions to describe the data, and we figured it made sense to report it as such. Do not worry, we calculated the alert composition for the quarter prior to determine the differences shown in the table below.

Since we have three new Attack Vectors, there is no difference in calculation, and we made sure the table reflects this so as not to be confusing. Besides that, the table is straightforward. All the attack vectors decreased from Q3 aside from Scripts, which saw a sharp increase (39.48%). For this quarter, it comprises 82.94% of all attack vectors. Now that we include graphs for each attack vector, we can show you just how PowerShell dominates the landscape.

Attack Vector	Q1 Count	Q2 Count	Raw Difference From Q1	Percentage Difference From Q1
Acrobat	284	588	304	107.04%
Browsers	1716	6123	4,407	256.82%
Coding Software	-	127	-	-
Database Software	-	241	-	-
Microsoft 365	2058	0	-2,058	-100.00%
Other	1859	8666	6,807	366.16%
Remote Access Software	-	1068	-	-
Scripts	11260	125151	113,891	1011.47%
Windows	7898	4452	-3,446	-43.63%

Figure 34. Q4 2024 Attack Vectors

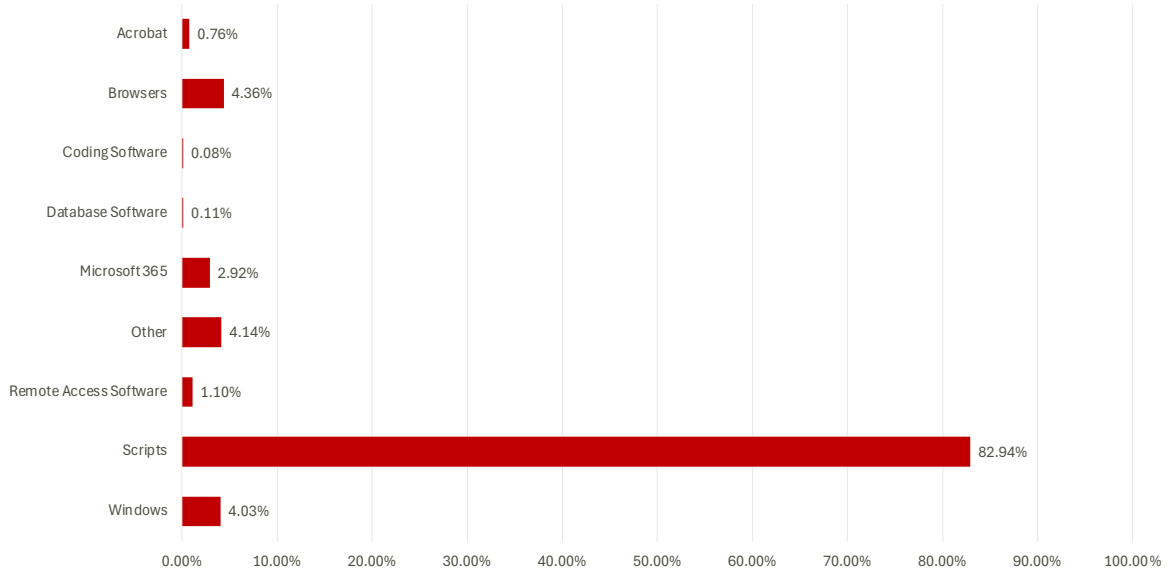


Figure 35. Q4 2024 Attack Vectors

Browser Attack Vectors

We have included the Browser Attack Vector subsection for a few quarters now. It was the first one we created in addition to the summation chart. Then we added Office (Microsoft 365) earlier this year. Now, with the additional data, we expanded them to all attack vectors, except for Other. With that ingestion of additional data, we caught a few more browser detections that usually do not make the list, although they have before. Those browsers are Brave and Opera. The usual suspects appear too: Chrome, Edge, Firefox, and Internet Explorer. This quarter, Chrome led the way with 71.54% of all detections, followed far behind by Edge, Firefox, and Internet Explorer, respectively. There were a few detections from Brave and Opera, who shared the spoils of last place.

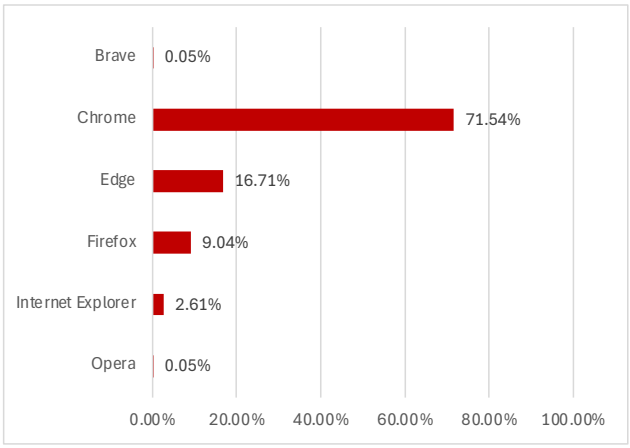


Figure 36. Q4 2024 Browser Detections

Coding Software Attack Vectors

Coding Software is the smallest Attack Vector subsection by raw numbers, and it is a two-horse race between NodeJS and Java. Then a few invocations from ElectronJS. Java and NodeJS were pretty even, but we observed slightly more NodeJS than Java. Keep in mind that all three of these combined equated to 0.08% of all alerts.

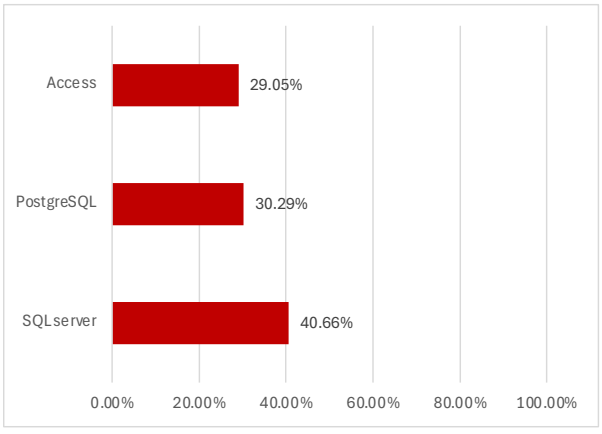


Figure 37. Q4 2024 Coding Software Detections

Database Software Attack Vectors

Database Software is akin to Coding Software in that it was responsible for a miniscule number of alerts with respect to the other attack vectors. Coding Software accounted for 0.08% of alerts whereas Database Software Attack Vectors accounted for 0.11%. With that in mind, the database-related alerts were relatively even across the board. SQL server led the way with 40.66% of all alerts, followed by Access and PostgreSQL. We had no other alerts from any other database software this quarter.

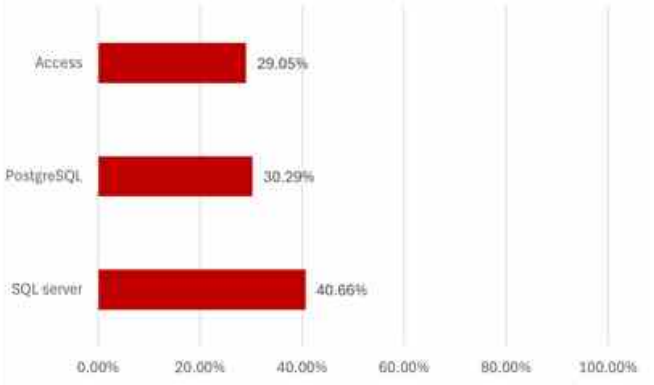


Figure 38. Q4 2024 Database Software Detections

Microsoft 365 Attack Vectors

This attack vector encompasses all Microsoft 365 applications. So, if an application is not in the graph, it did not invoke any alerts on our endpoints. Office Misc. is a label for Office-related helper files, such as the Office application itself. Those files alerted the most, followed closely behind by OneDrive, Outlook, and Word. The next tranche of alerts came from Access (which also appears in the Database Software Attack Vector), Excel, and Teams. Finally, there were a select few applications that invoked a handful alerts here and there: Clipchamp, OneNote, PowerPoint, and Visio. The exact ratio for each is in the bar graph.

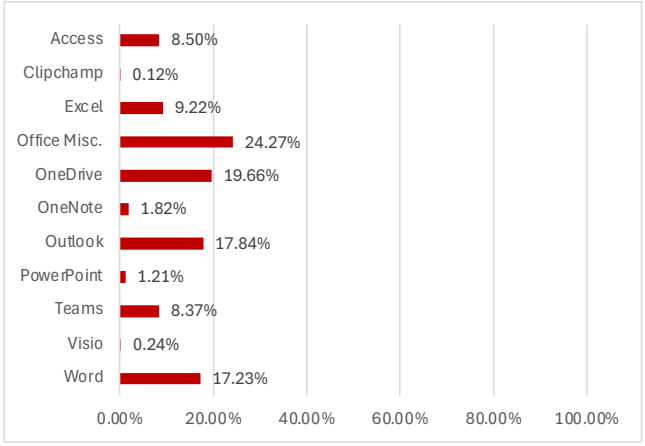


Figure 39. Q4 2024 Microsoft 365 Detections

Remote Access Attack Vectors

Threat Actors love remote access tools because they are trusted software that allows for remote control of a victim machine. If an attacker has remote access to your system, the possibilities are endless as to what destruction they can cause. The Remote Access Attack Vectors data points highlight what we observe on end-points, and it gives you an idea of which ones attackers leverage for their ill-gotten gains. For example, we observed Imperio the most, followed closely by LogMeIn. Threat actors also commonly used NetOp, Radmin, and WinRM. Then, there were several that made the cut, but just barely: Devolutions RDM, NinjaOne RMM, Quick Assist, RustDesk, Senso, ReamViewer, and Total Commander combined for around 5% of all remote access tool invocations.

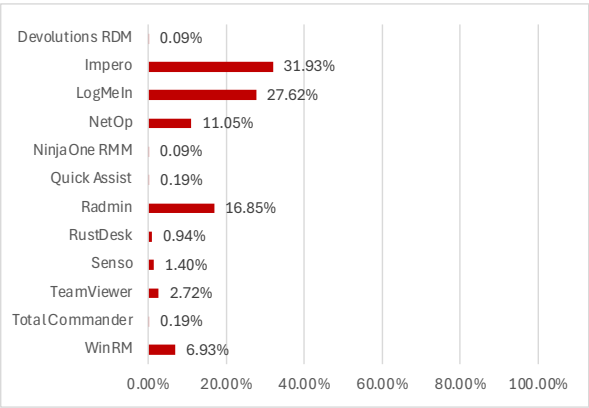


Figure 40. Q4 2024 Remote Access Detections

Script Attack Vectors

The chart for this one requires little explanation. Scripts accounted for nearly 83% of all attack vectors, and of that ~83%, 97.29% of them were from PowerShell. In short, PowerShell is responsible for the vast majority of threat actors' avenue of attack. The reason is simple. It is on every system (unless disabled) and can perform almost any action. Let us not discredit Python, AutoIT, and Visual Basic. These are commonly used scripting tools for malware authors. Threat actors use AutoIT to drop or download additional payloads, and Python is a ubiquitous language for information security programmers.

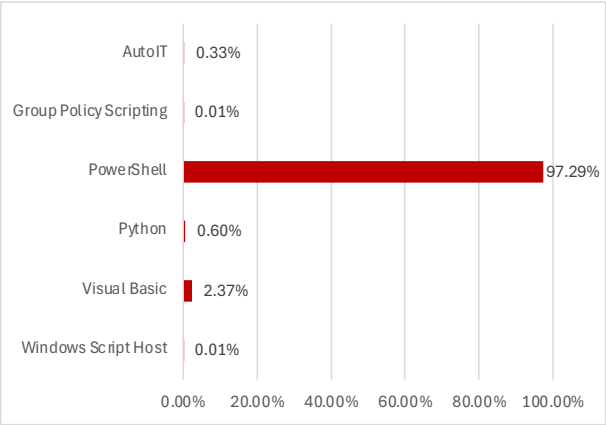


Figure 41. Q4 2024 Script Detections

Windows (LOLBAS) Attack Vectors

The Windows data points look like quarters prior. However, we expanded the data set and now focus on living-off-the-land binaries (LOLBAS). These are trusted Windows binaries, usually signed, that live on systems that threat actors leverage for malicious purposes. For example, cmd.exe is the Command Prompt process commonly leveraged by threat actors to perform tasks. Those accounted for 24.01% of LOLBAS alerts. Vbc.exe, the Visual Basic compiler, had the most alerts with 46.75% composition. There was a myriad of other LOLBAS alerts that we have conveniently placed in a bar graph below.

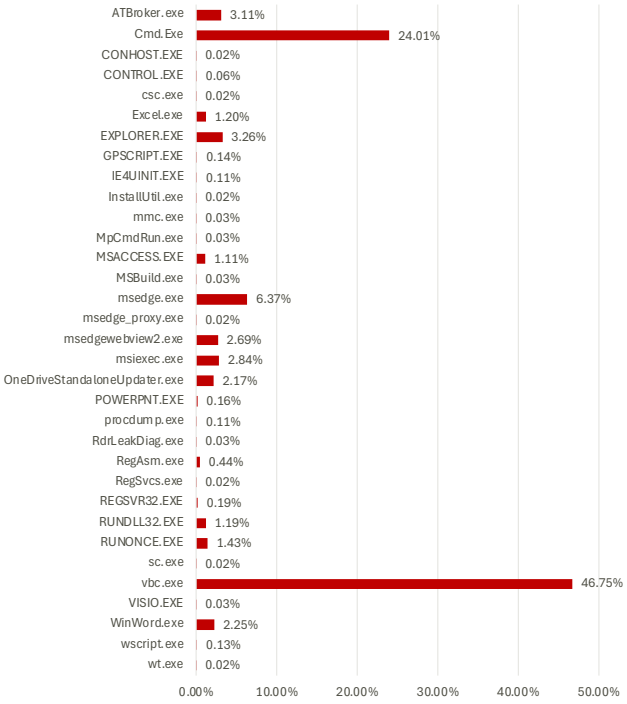


Figure 42. Q4 2024 Windows (LOLBAS) Detections

Cryptominer Detections

Cryptominers have not appeared in every Internet Security Report. We removed it for a handful of quarters because the numbers became melded with information stealers. We just simply were not seeing enough cryptominer alerts to warrant a subsection for it. However, these numbers rose significantly in Q4. From Q3 to Q4, cryptominer detections skyrocketed 141.06%. What is interesting is that the cryptominer detections seem to rise as the price of bitcoin goes up. At least, that is our theory.

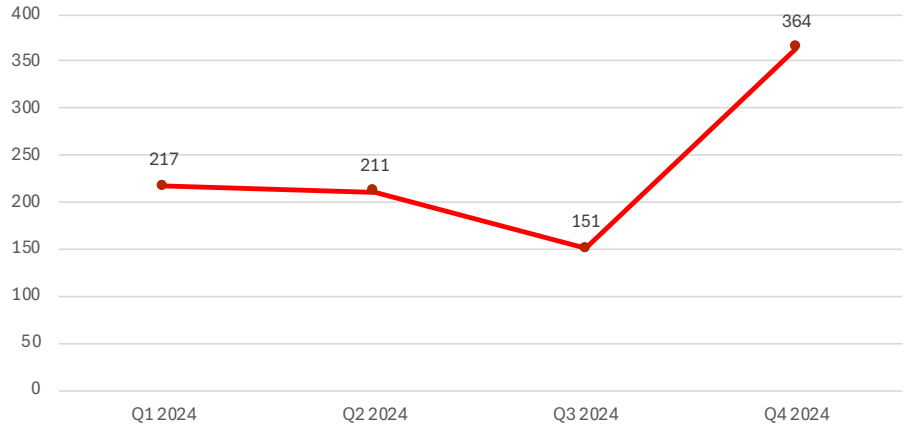


Figure 43. 2024 QoQ Cryptominer Detections

THREAT HUNTING

The Threat Hunting subsection pertains to all EPDR users, but Advanced EPDR users receive additional non-deterministic indicators of compromise. All users receive these indicators mapped to the MITRE ATT&CK matrix, which is a normalized knowledge base describing tactics and techniques of threat actors. A single attack can contain several tactics and techniques, and thus, the alerts invoked in this subsection are significantly higher than malware threats in prior subsections. As a refresher, the tactics and technique data points for the Threat Hunting subsection are listed 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.

To begin, we provide a table for the top 10 tactics and techniques determined by which sub-technique invoked the most alerts. For example, TA0007 is the Discovery Tactic (ranked first this quarter) that describes behaviors to enumerate networks and systems on any given endpoint. This does not mean the action is malicious. In fact, many discovery-related alerts are performed by users or network administrators. This supports the importance of threat hunting analysts who know which alerts to prioritize and are anomalous to endpoint baseline behavior. WatchGuard has such threat hunting-as-a-service for EPDR-protected systems.

Another example of an exploit in the table is TA0002::T1059.001. TA0002 describes an execution action, T2059 confirms the execution is from a Command and Scripting Interpreter, and 001 are PowerShell scripts. Thus, TA0002::T1059.001 are for those alerts from PowerShell execution invocations, which relates to the Script Attack Vector discussed in the prior section. That particular sub-technique ranked second this quarter. The other eight exploit detections are in the table below.

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 44. Q4 2024 Exploits by MITRE ATT&CK Tactic and Technique

From the top 10 Threat Hunting exploits, we zoom out to the MITRE ATT&CK Tactic summations. For these data points, we group all techniques and sub-techniques for each tactic and record the total. In addition to the bar graph, we also have added a table to provide more insight into the numbers and the difference from the quarter prior, like other subsections within Endpoint.

There are four major tactics alerted on EPDR-protected endpoints, in descending order: TA0005 (Defense Evasion), TA0002 (Execution), TA0007 (Discovery), and TA0003 (Persistence). Defense Evasion are actions to, you guessed it, evade defense mechanisms on endpoints, and these alerted the most this quarter and increased almost 23% from last quarter. Execution actions are intentionally broad and define any malicious code invocation. Actions defined by this tactic also saw a rise from the last quarter of 18.52%. Discovery tactics are when adversaries try "to figure out your environment." These can be as simple as a 'whoami' command or actions such as enumerating Active Directory (AD). Discovery-related alerts rose 26.21% from Q3 to Q4. The final and fourth major tactic adversaries use are Persistence-related activities, which are actions to remain on a system even after disinfection routines or computer reboots. Many of these actions relate to registry settings. Persistence alerts remained stagnant from last quarter, decreasing by a miniscule 0.07%.

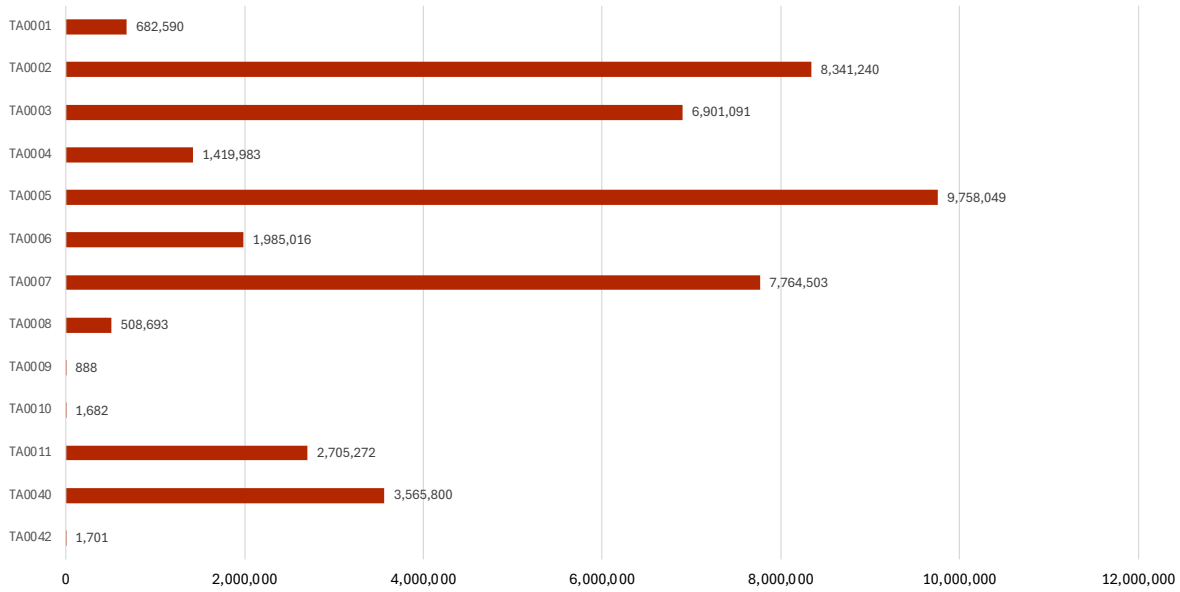


Figure 45. Q4 2024 Exploits by MITRE ATT&CK Tactic and Technique

MITRE Tactic	Q3 Tactic Sum	Q4 Tactic Sum	Difference	% Difference
TA0001	732,452	682,590	-49,862	-6.81%
	TA0002	7,037,978	+1,303,262	18.52%
TA0003	6,905,976	6,901,091	-4,885	-0.07%
	TA0004	2,297,717	-877,734	-38.20%
TA0005	7,935,408	9,758,049	+1,822,641	22.97%
TA0006	1,588,155	1,985,016	+396,861	24.99%
	TA0007	6,152,159	+1,612,344	26.21%
TA0008	450,625	508,693	+58,068	12.89%
TA0009	901	888	-13	-1.44%
TA0010	1,789	1,682	-107	-5.98%
TA0011	2,172,031	2,705,272	+533,241	24.55%
TA0040	3,009,864	3,565,800	+555,936	18.47%
TA0042	1,205	1,701	+496	41.16%

Figure 46. Q4 2024 Exploits by MITRE ATT&CK® Tactic

The MITRE ATT&CK techniques define more in-depth actions from each tactic. For example, TA0004 is Privilege Escalation and T1543, Create or Modify System Process, describes the technique within that tactic. Thus, the process creation or modification was to escalate privileges. However, some techniques are generic detections denoted with a '0'. This is evident in the bar graph and table below. These describe behaviors that do not fit within a specific technique, but we still count them. TA0007, Discovery, led the charge with the most technique (tactic) alerts, followed by TA0002:T1059.001, PowerShell executions. The rest were all relatively similar in terms of the numbers.

Top Threat Hunting Rule Invocations

The final Threat Hunting subsection before the Ransomware Landscape section covers the top 10 rules invoked on protected endpoints. These are different than the MITRE ATT&CK matrix invocations because they are internally created rules as opposed to mapping alerts to the matrix. In essence, these rules are mapped to the MITRE ATT&CK matrix but are more granular in their definitions. For example, the top ranking rule this quarter is PowershellCommandDiscoveryRule. If we were to map this to the MITRE ATT&CK matrix, this would be TA0002::T1059.001, which is Execution::Command and Scripting Interpreter.PowerShell. This would also map to TA0007, which is Discovery. However, within one rule we can determine that an alert triggered from this rule is a PowerShell script meant for system and network discovery. It's a two-for-one.

Aside from the PowerShell rule invocation discussed in the previous paragraph, all other rules saw reductions in alerts for this quarter. The only exception is the new rule appearing in the top 10, LolBasRule, which describes threat hunting alerts from living-off-the-land binaries. These are subject to several false positives because these binaries are already inherently trusted on the endpoint. So, it's important to hunt for alerts from this rule that are abnormal. For example, if explorer.exe connects to the Internet on an arbitrary port, this is highly suspicious and cause for further investigation.

Rule Name	Alerts	Rank
PowershellCommandDiscoveryRule	5,475,657	1
DisableSecurityProtectionsRule	4,597,263	2
DeleteFilesOrPartitionsRule	3,476,121	3
PowershellCommandsDecodedDesofusRule	3,384,206	4
HijackExecutionFlow	3,178,869	5
PersistenceServicesBinPath	2,248,371	6
RemoteFileCopyRule	2,191,057	7
PowershellDangerousCommandLinesRule	2,014,471	8
NetAdminAddRule	1,361,029	9
LolBasRule	1,313,884	10

Figure 47. Q4 2024 Threat Hunting Invocations Top 10

RANSOMWARE LANDSCAPE

Only one data point in the Ransomware Landscape section is from EPDR-protected endpoints, and that is the number of ransomware detections. The other subsequent data within is from our Ransomware Tracker data collection efforts, specifically of double extortion groups. This duo of data provides both an internal and external point of view of the breadth of ransomware attacks. This quarter, both of those numbers are moderately to sharply up.

Because of Black Basta and Play appearing on the Top 10 Most Prevalent Malware lists, the WatchGuard ransomware blocks for this quarter are way up. Keeping with the theme of this quarter, the quarterly increase from Q3 to Q4 is also historic, rising 627.75%. Around 90% of these detections were from Black Basta and Play alone. If we negate those detections, the overall numbers decreased substantially from last quarter.

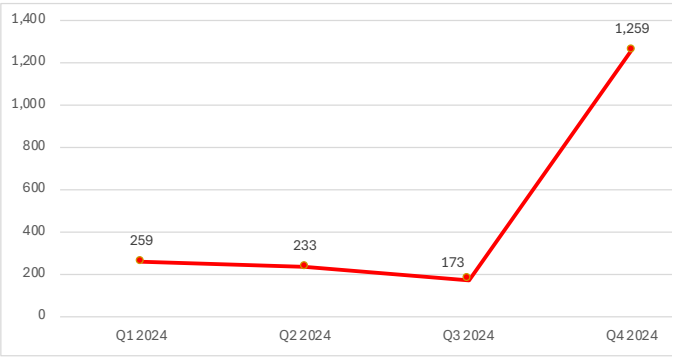


Figure 48. 2024 QoQ Ransomware Detections by Quarter

Extortion Groups

All the data from here on out does not apply to EPDR-protected endpoints. It is auxiliary data aimed at supplementing the ransomware detections from the WatchGuard ransomware detections, and the numbers support the quarter-over-quarter increase seen on these endpoints. While these endpoints saw a catastrophic increase of 627.75% from Q3, the number of extortion victims did not increase nearly as much. However, they did increase much more than normal, rising 40.92%, which again, is historically high according to our numbers. Keep in mind that double extortions have only existed for around six years with the first true double extortion being attributed to the Maze group in late 2019. So, our data is limited because the data itself is limited. Yet, based on this limited data, we rarely, if ever, see around 40% increases from quarter to quarter.

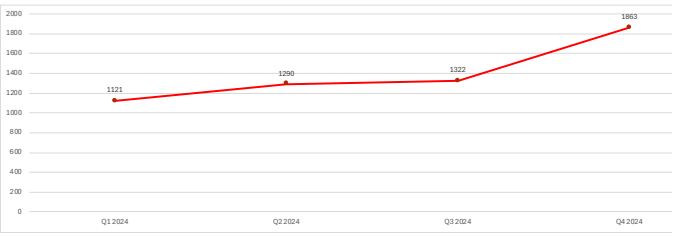


Figure 49. 2024 QoQ Public Extortions by Group

We almost seem like a broken record at this point, as there were an abnormally high number of newly active and inactive groups this quarter. We began tracking 21 new ransomware groups and removed 18 ransomware groups that recently became inactive or dormant. Two of the new ransomware groups were rebrands or evolutionary changes – Kill Security announced a rebrand to Kill Security 3.0 and LockBit announced a new dark web domain with the next evolution of their locker, LockBit 4.0, also called LockBit Green. WikiLeaks v2 appears to be the second iteration of WikiLeaks operated by Julian Assange. However, researchers have uncovered a link between this data leak site and the Qilin ransomware group. It's possible the group runs the site or has direct connections to their operators.

New Groups	Inactive Groups
Anubis	BlackByte
Apos Security	Chort
Argonauts Group	dAn0n
Bluebox 1.0	DarkVault
Chort	Dispossessor
CyberVolk	Donut Leaks
FunkSec	HelloGookie
HELLCAT	IRLeaks
INTERLOCK	Kill Security
Kairos	MADDLL32
Kill Security 3.0	Mallox
LEAKEDDATA	PlayBoy
LockBit 4.0	RA Group
Morpheus	Ransomcortex
Nitrogen	SenSayQ
PlayBoy	Valencia
SafePay	Vanir Leaks
SKIRA TEAM	Werewolves
Termite	
Weyhro	
WikiLeaksV2	

Figure 50. Q4 Newly Active and Inactive Ransomware Groups

The next few graphs and tables show our overall numbers we tracked for this quarter and throughout 2024, including the quarter-over-quarter bar graph that we only produce for Q4. The first of which is what we call "The Big Red Graph" that simply shows the numbers for the quarter in an easy-to-read format. We then include two tables, one that displays the numbers from the previous quarter and from this quarter, with the corresponding differences, and then the other is a descending chart, which is basically a filter on which groups had more extortions from the quarter prior. Finally, we include another large bar graph that is The Big Red Graph delimited over each quarter.

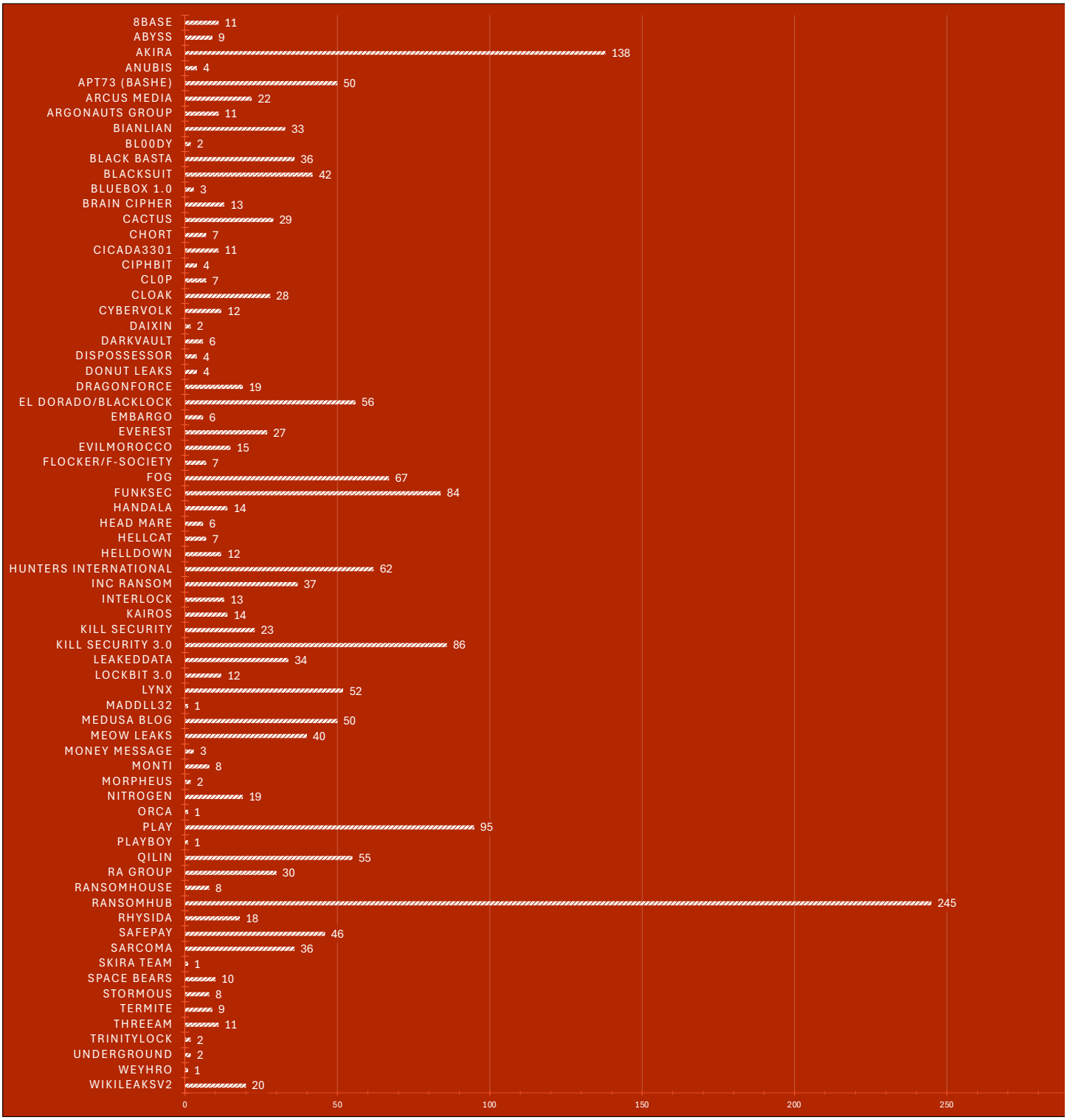


Figure 51. Q4 2024 Public Extortions by Group

Name	Q3	Q4	Difference
8base	13	11	-2
Abyss	13	9	-4
Akira	48	138	+90
AlphaLocker	2	0	-2
Anubis	-	4	NEW
APT73 (Bashe)	3	50	+47
Arcus Media	10	22	+12
Argonauts Group	2	11	+9
BianLian	43	33	-10
Bl00dy	0	2	+2
Black Basta	7	36	+29
BlackByte	2	0	-2
BlackSuit	37	42	+5
Bluebox 1.0	-	3	NEW
Brain Cipher	12	13	+1
Cactus	27	29	+2
Chort	-	7	NEW
Cicada3301	27	11	-16
CiphBit	4	4	0
CL0P	2	7	+5
Cloak	17	28	+11
CyberVolk	5	12	+7
DAIXIN	1	2	+1
dAn0n	4	0	-4
DarkVault	15	6	-9
Dispossessor	16	4	-12
Donut Leaks	7	4	-3
DragonForce	32	19	-13
DungHill Leak	1	0	-1
El Dorado/Black-Lock	14	56	+42
EMBARGO	5	6	+1
Everest	10	27	+17
EvilMorocco	6	15	+9
Flocker/ F-SOCIETY	6	7	+1
FOG	18	67	+49
FunkSec	-	84	NEW
Handala	16	14	-2
Head Mare	1	6	+5
HELLCAT	-	7	NEW
Helldown	21	12	-9
Hunters International	57	62	+5
INC Ransom	30	37	+7
INTERLOCK	-	13	NEW
IRLeaks	12	0	**-12**
Kairos	-	14	NEW
Kill Security	32	23	-9
Kill Security 3.0	-	86	NEW
LEAKEDDATA	-	34	NEW
LockBit 3.0	85	12	-73
Lynx	30	52	+22
MADDLL32	13	1	-12
Mallox	2	0	-2
Medusa Blog	43	50	+7
Meow Leaks	76	40	-36
Metaencryptor	4	0	-4
Money Message	0	3	+3
Monti	14	8	-6
Morpheus	-	2	NEW
Nitrogen	-	19	NEW
Orca	2	1	-1
Play	90	95	+5
PlayBoy	-	1	NEW
Pryx	3	0	-3
Qilin	48	55	+7
RA Group	6	30	+24
Ransomcortex	4	0	-4
RansomHouse	14	8	-6
RansomExx2	7	0	-7
RansomHub	195	245	+50
Rhysida	38	18	-20
SafePay	-	46	NEW
Sarcoma	23	36	+13
SKIRA TEAM	-	1	NEW
Space Bears	14	10	-4
Stormous	9	8	-1
Termite	-	9	NEW
ThreeAM	7	11	+4
TrinityLock	5	2	-3
Underground	2	2	0
Valencia	5	0	-5
Vanir Group	3	0	-3
Weyhro	-	1	NEW
WikiLeaksV2	2	20	+18
Total	1322	1863	+541

Figure 52. Q3-Q4 2024 Ransomware Extortion Differences

Name		Name	
Akira	+90	DungHill Leak	-1
RansomHub	+50	Orca	-1
FOG	+49	Stormous	-1
APT73 (Bashe)	+47	8base	-2
El Dorado/Black-Lock	+42	AlphaLocker	-2
Black Basta	+29	BlackByte	-2
RA Group	+24	Handala	-2
Lynx	+22	Mallox	-2
WikiLeaksV2	+18	Donut Leaks	-3
Everest	+17	Pryx	-3
Sarcoma	+13	TrinityLock	-3
Arcus Media	+12	Vanir Group	-3
Cloak	+11	Abyss	-4
Argonauts Group	+9	dAn0n	-4
EvilMorocco	+9	Metaencryptor	-4
CyberVolk	+7	Ransomcortex	-4
INC Ransom	+7	Space Bears	-4
Medusa Blog	+7	Valencia	-5
Qilin	+7	Monti	-6
BlackSuit	+5	RansomHouse	-6
CL0P	+5	RansomExx2	-7
Head Mare	+5	DarkVault	-9
Hunters Interna-tional	+5	Helldown	-9
Play	+5	Kill Security	-9
ThreeAM	+4	BianLian	-10
CiphBit	0	Dispossessor	-12
Underground	0	IRLeaks	-12
		MADDLL32	-12
		DragonForce	-13
		Cicada3301	-16
		Rhysida	-20
		Meow Leaks	-36
		LockBit 3.0	-73

Figure 53. Q3-Q4 2024 Ransomware Extortion Differences Descending

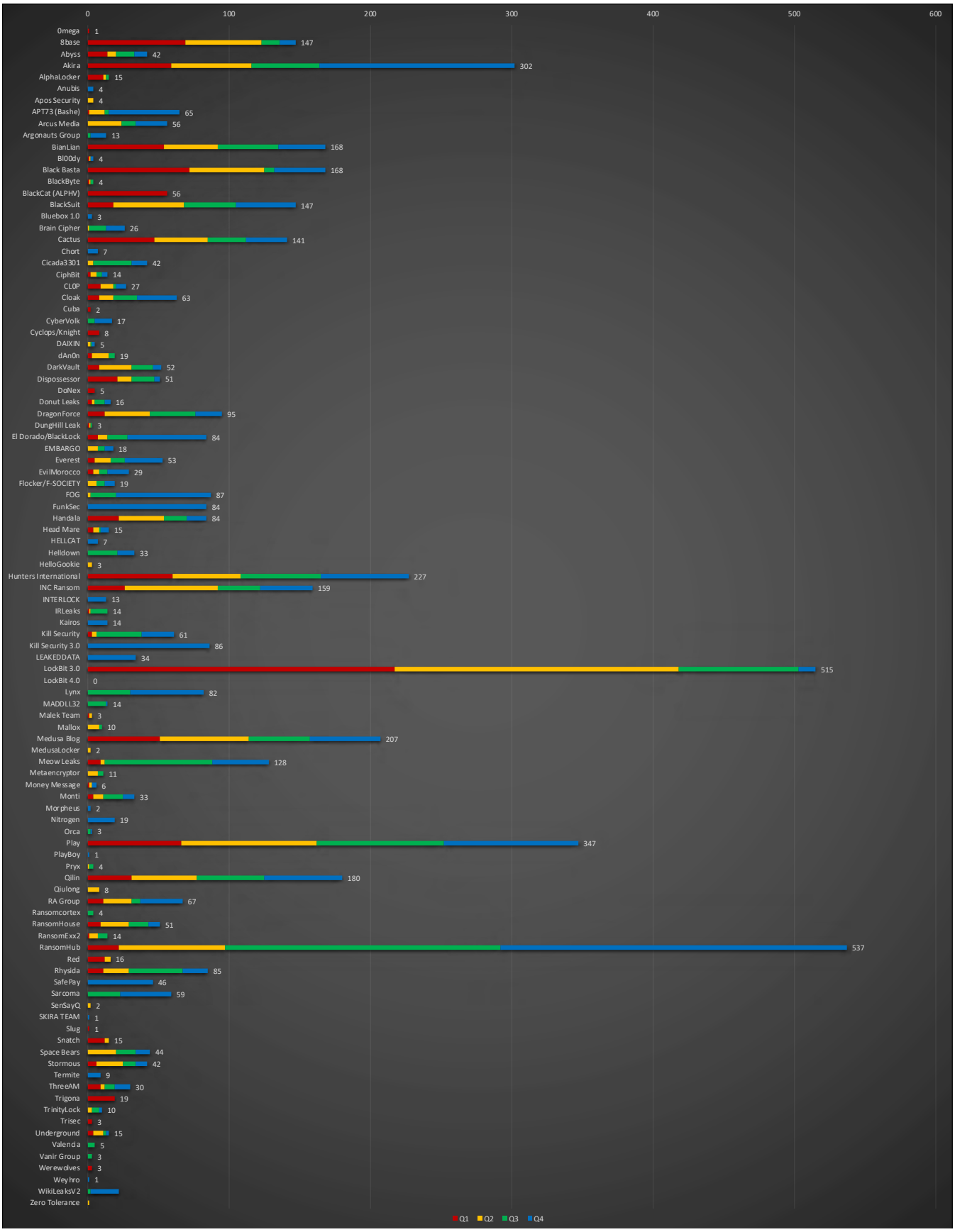


Figure 54. 2024 QoQ Public Extortions by Group

Notable Ransomware Events

Law Enforcement Actions

BitPaymer & LockBit – On October 1, the very first day of Q4, the United States Justice Department announced tri-lateral action with the United Kingdom and Australia against Aleksandr Viktorovich Ryzhenkov (Александр Викторович Рыженков), a member of Evil Corp and a BitPaymer ransomware affiliate commonly referred to as Beverley, and other ransomware-enabling individuals. Aleksandr is an Evil Corp developer and support administrator with several others, including his brother Sergei. According to the Justice Department, Ryzhenkov began deploying BitPaymer in 2017 with his conspirators. Law enforcement published all the details on the seized LockBit data leak site under Operation Cronos and included further details about arrests including an admin of Bulletproof, a hosting provider, and two other affiliates.

The Justice Department released an image of Evil Corp members and affiliates where Aleksandr Ryzhenkov is at the bottom right:

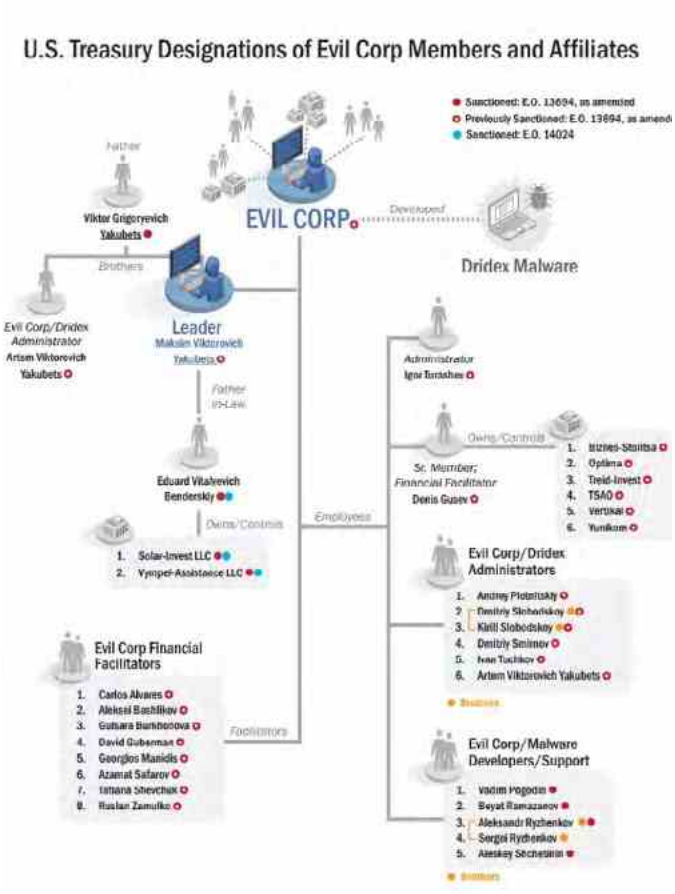


Figure 55. **US Treasury Evil Corp Organizational Chart**

Black Basta

BT Group – BT Group, formally known as British Telecommunications or British Telecom, is one of Europe's leading telecommunications services. So, it is no wonder that we have included this as a notable breach. The Black Basta group claims to have exfiltrated around half a terabyte of data, including NDAs, and user, financial, and other organizational data. We do not know what exact data was exfiltrated, but it could include phone and text logs, geolocation, personal financial data, and so on. What we do know is that 500 gigabytes of data is a lot. There is a good chance that if the data is legit, it is notable and concerning for their users.

Brain Cipher

Deloitte – There is a chance that Deloitte is familiar to you. So, we will not explain their background, but they are one of the "Big 4" audit firms in the world along with Ernst & Young (EY), Klynveld Peat Marwick Goerdeler (KPMG) and PricewaterhouseCoopers (PwC). These four companies perform a large share of the world's accounting audits. Therefore, the data they possess and manage is vast and sensitive, and any breach of this data is costly. Brain Cipher claims to have exfiltrated about one terabyte of their data from Deloitte UK. The company claims otherwise.

Cactus

Housing Authority of the City of Los Angeles (HACLA) – Ransomware groups have posted the HACLA on at least three occasions, of which we are aware. In late 2022, LockBit posted the HACLA on their data leak site claiming to have 15 terabytes of data, and then again three months later with an updated data log. Then, the Dispossessor group, which is known to publish leaks of other groups and claim it as their own, published the same exact post of the second LockBit post – all but confirming this was a re-leak. Now, Cactus is the latest to post a successful breach and claims to have 861 gigabytes of data. This is notable because the HACLA is one of the largest housing authorities in the United States.

Cl0p

Cleo Managed File Transfer (MFT) – In October 2024, Cleo divulged a vulnerability tracked as CVE-2024-50623 that permitted unrestricted file uploads and downloads. A second vulnerability was discovered in December 2024 (tracked as CVE-2024-55956). Cl0p exploited these two vulnerabilities to perform data supply chain exfiltration attacks against many of the users of Cleo's software, which they are still posting as of this writing. They have published hundreds of alleged victims on their data leak site and point to these recent zero-day vulnerabilities as the avenue of attack. On December 15, 2024, the ransomware group finally claimed responsibility for the recent spate of data theft attacks that targeted organizations using Cleo-managed file transfer (MFT) software solutions. Expect Cl0p's numbers to be much higher for Q1 of 2025 than they were all of 2024.

Embargo

American Associated Pharmacies (AAP) – This breach appears on the notable breach list because of the way the Embargo operators have allegedly extorted American Associated Pharmacies. Before that, a disruption to pharmacies could have literal deadly consequences, and a successful breach could hinder their ability to administer life-saving medication. The group claims in their dark web data leak site to have around 1.5 terabytes of data, to which the AAP paid a $1.3 million ransom for decryption. However, Embargo claims they owe another $1.3 million (known as double extortion) for the deletion of the data. Considering this is likely a lie, and that data is considered forever exposed, it is doubtful that AAP would pay an additional amount, if they paid any in the first place.

HellCat

Schneider Electric – This breach is notable for two reasons. The first is that Schneider Electric is large organization out of France focused on automation and electric energy. Hence the name. They have acquired numerous companies in the same sector to expand their offerings. They have a significant presence in industrial manufacturing and automation, and in energy management, which is their big money maker. Thus, a breach or any disruption in operations could have a downspout effect. Luckily, that was not the case here. The second notable aspect of this breach is that the group, HellCat, demanded $125,000 in baguettes – a derogatory stereotype of the organization being headquartered in France. Based on the ransom demand, it is logical to assume that the extortion demand is a dead end.

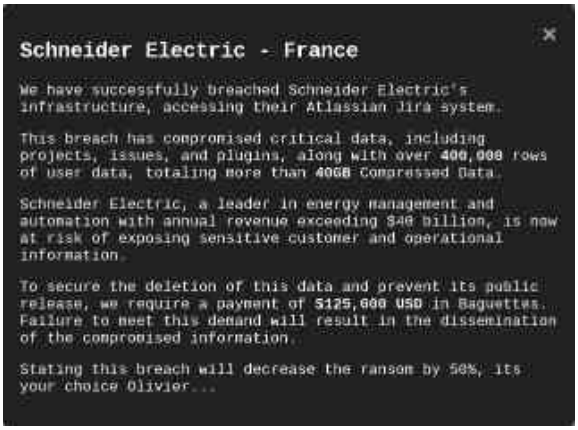


Figure 56. HellCat – Schneider Electric Double Extortion

INC Ransom

Liverpool's Alder Hey Children's Hospital, Liverpool Heart and Chest Hospital, and Royal Liverpool University Hospital – On November 28, the INC Ransom group published what appeared to be valid stolen data from "NHS Alder Hey," certainly alluding to Liverpool's Alder Hey Children's Hospital in England. The group claimed to have stolen a large swathe of data, including patient records, donor reports, and procurement data, all from 2018 to 2024. The same day, the hospital released an official statement saying they are aware of the published data on INC Ransom's dark web data leak site and are investigating its authenticity. A week later, on December 4, they released an updated statement confirming that there was a cyberattack, and it affected not only their hospital, but also Liverpool Heart and Chest Hospital and a small amount of data from Royal Liverpool University Hospital. Services at all three hospitals were unaffected, but the data released is notable, considering that one of the hospitals is meant for children. So, yet again, we have another ransomware group attacking children's hospitals and similar critical services.

RansomHub

Bologna Football Club – Bologna FC published an official statement on November 29 discussing their awareness of a ransomware attack and that data from the club would appear online. They also left a concise statement warning individuals that possession of this data is a crime. Less than two weeks prior, RansomHub published this club on their dark web data leak site with claims of having a large amount of data. They claim to have:

- All sponsorship contracts and documents.
- All Financial data spanning the club's entire history.
- All personal and confidential data of players, academy players, fans, and employees.
- All transfer strategy documentation.
- All medical records of players and staff.
- All confidential data related to different structures and stadiums.
- All commercial strategies and business plans.
- Documents that could potentially violate FIFA and UEFA regulations, including financial fair play.

The disclosure of these types of documents could have ripple effects on players, staff, fans, and football teams globally.

Conclusion

In conclusion, this quarter was historic and record-breaking in multiple ways. We observed significantly fewer new malware threats and a record-breaking reduction in total malware threats, decreasing 91.14% from last quarter. We also blocked an abnormally high number of ransomware attacks on WatchGuard endpoints, particularly from the Black Basta and Play ransomware groups. Both groups appeared in the Top 10 Most Prevalent Malware list for this quarter, as did some of their helper malware files. This was coupled with a sharp increase in ransomware extortions throughout the ransomware landscape. We also made a myriad of changes to the Attack Vectors subsection, where the Scripts attack vector increased over ten-fold, spearheaded by PowerShell invocations.

All in all, total threats across the board decreased significantly, but of those detections, many of them were ultra-destructive ransomware attacks. This is a wake-up call to understand that just because there were fewer threats, does not mean that the threats that do attempt to slip through defenses will be simple attacks. Most threat actors are opportunists, and some are more patient than others. Therefore, it's paramount to not overlook not overlooked small alerts . One small alert could lead to widespread attacks if not tended to quickly and diligently. Let this quarter be a lesson in that.

CONCLUSION & DEFENSE HIGHLIGHTS

CONCLUSION AND DEFENSE HIGHLIGHTS

As we navigate through the volatile seas of cybersecurity, the findings of our Q4 2024 report illuminate the adjustments organizations must make to stay ahead. Much like skilled sailors tuning their sails to face shifting winds, cybersecurity teams must continuously adapt their defenses to counter the evolving threat landscape. Our analysis reveals an intriguing dichotomy between the rise of network-based malware detections and the decline in endpoint unique malware detections, underscoring the importance of a multi-layered defense strategy.

Network-based malware detections surged, highlighting a significant increase in zero-day threats, especially those leveraging encrypted connections to evade detection. This resurgence of sophisticated threats requires organizations to proactively enhance their protective measures, ensuring their security systems are capable of decrypting and analyzing encrypted traffic. The return of coinminers and the emergence of blockchain-related attacks like Etherhiding signal a warning that cybercriminals are innovating and leveraging new technologies to exploit vulnerabilities.

Conversely, the decrease in unique endpoint malware detections presents an opportunity to evaluate and refine endpoint protection strategies. While the volume of endpoint malware dropped, its generic nature indicates that well-established defenses can effectively block many of these threats. However, the rise in browser-based malware delivery vectors calls for an enhanced focus on securing web browsers and ensuring they are regularly updated against known vulnerabilities.

The slight decline in network attacks, albeit with a variety of new exploits surfacing, suggests that while overall attack volume decreases, diversification and innovation by threat actors continue to develop. This necessitates organizations to not only maintain vigilance but to deepen their understanding of evolving attack vectors and adapt their intrusion prevention systems accordingly, perhaps even adding newer network detection and response (NDR) security controls to the mix.

If you can't patch perfectly, patch programmatically.

In every quarterly security report we've ever released, we consistently find that threat actors primarily exploit old vulnerabilities – often fixed months, if not years, prior. The prevalence of zero-day exploits pales in comparison to these well-known, outdated vulnerabilities. This reality underscores our repeated advice: regularly and swiftly patch your software to yield significant returns on your security work investment. You already know this.

However, real-world business constraints can hinder organizations from keeping up with patches. For example, some may need to rely on outdated applications that function only on end-of-life operating systems. While this isn't ideal, finding a replacement may take time. Similarly, small teams may struggle to manage extensive infrastructures. Regardless of the challenge, it's crucial to prioritize quickly patching the most critical vulnerabilities.

What should you do if perfect patching isn't feasible?

Implement a structured patching policy with clearly defined SLAs that prioritize critical vulnerabilities. If you can't address every patch, ensure that you focus on the important ones first. While this concept is foundational, lacking a formal patch policy with SLAs and severity definitions, tailored to your organization's risk assessments, necessitates immediate action.

At a high level, prioritize swift patch SLAs for software flaws with the highest criticalities. For instance, address high and critical patches within 30 days, while allowing 90 to 180 days for medium and low severity. Consider exposure as a key factor; if a software service is exposed externally, your patch SLA should be much faster, whereas internal low-risk vulnerabilities might warrant a longer wait.

In conclusion, strive to patch everything possible as quickly as you can. If that's unachievable, take the time to develop a risk-based policy. Employ automated patching and monitoring tools to ensure you meet your SLAs effectively.

Protect Linux computers and IoT as equally as Windows machines.

Yeah. We all know that attackers, by far more often, target the Windows operating system (OS) with malware and attack it over any other. However, just because Windows is the biggest target doesn't mean attackers aren't targeting Linux devices, and IoT, which tends to use Linux too. This quarter, we saw a rise in Top 20 malware that affected Linux machines, including coinminers, which tend to prefer Linux servers. In short, your Linux server better have good endpoint detection and response software too, and luckily, WatchGuard products like EPDR work great on Windows, Mac, or Linux machines.

However, some IoT devices do not easily allow you to install endpoint security applications and may still remain vulnerable to malware. For IoT, we recommend you both segment them away from more trusted devices and computers, only allowing the bare minimal access between those segments, and you can also deploy network detection and response products, like WatchGuard's ThreatSync + NDR to monitor all the traffic going to and from an IoT device for malicious behaviors.

Embrace a Defense-in-Depth Approach to Combat Evolving Malware

Today's malware landscape is characterized by its sophistication and constant evolution, making a defense-in-depth security strategy essential for organizations aiming to protect their networks and endpoints. We have observed fluctuations in the prevalence of network and endpoint malware; while this quarter's findings indicate a rise in network-based threats, endpoint malware detections have notably decreased. This dynamic nature of threats requires a multi-layered approach to ensure comprehensive protection against the diverse tactics employed by cybercriminals.

The risk of sophisticated malware capable of bypassing standard security measures underscores the necessity of integrating various prevention techniques. For instance, while classic signature-based antivirus solutions have been foundational in identifying known threats, they often fall short against newer, more evasive malware variants. To bolster defenses, organizations should incorporate endpoint detection and response (EDR) systems, such as WatchGuard's EPDR, which provide advanced capabilities to detect, respond to, and mitigate threats that traditional methods may overlook.

Moreover, from a network security perspective, leveraging multiple malware detection engines enhances the ability to identify and neutralize threats before they can cause harm. Employing solutions that utilize artificial intelligence and behavioral analysis, such as IntelligentAV and APT Blocker, allows organizations to stay ahead of attackers by recognizing patterns and anomalies indicative of potential breaches. This multi-faceted approach not only improves the detection of both sophisticated and common malware but also fortifies an organization's overall security posture.

Ultimately, the unpredictable nature of malware threats necessitates that organizations prioritize a defense-in-depth strategy. By employing a comprehensive array of security controls – from network-based protections to endpoint solutions – organizations can ensure they effectively mitigate risks associated with diverse malware vectors. As the landscape continues to shift, embracing this proactive stance will empower teams to better anticipate and respond to the challenges that lie ahead, safeguarding their assets and operations against ever-evolving cyber threats.

As we conclude this quarter's report, let it serve not only as a reflection of the year past but as a beacon of guidance and prudence. By leveraging these insights, we hope to empower organizations to grow resiliently, transforming each challenge into an opportunity to fortify defenses. Together, we can ensure a secure voyage through the unpredictable waters of cybersecurity in the year ahead and beyond. Be sure to return next quarter to keep up with the latest changes in the threat landscape. As always, leave your comments or feedback about our report at SecurityReport@watchguard.com, and keep frosty online!

COREY NACHREINER

Chief Security Officer

Recognized as a thought leader in IT security, Corey spearheads WatchGuard's security vision. Corey has operated at the frontline of cybersecurity for 22 years, evaluating and making accurate predictions about information security trends. Corey has the expertise to dissect complex security topics, making him a sought-after speaker at forums such as Gartner, Infosec and RSA. He is also a regular contributor to leading publications including CNET, Dark Reading, Forbes, Help Net Security, and more. Find him on www.secplicity.org.

MARC LALIBERTE

Director of Security Operations

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

TREVOR COLLINS

Information Security Analyst

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

RYAN ESTES

Intrusion Analyst

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

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.