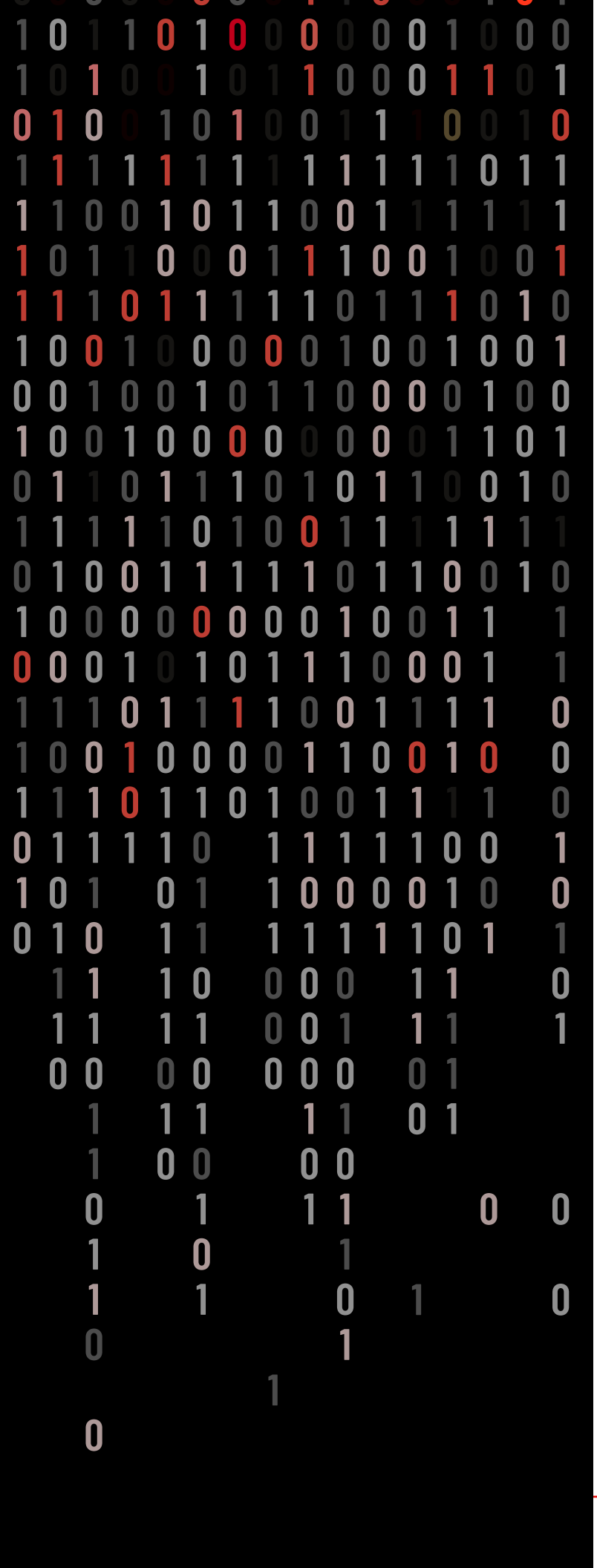
INTERNET SECURITY REPORT

Q1 2025



CONTENTS

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

INTRODUCTION

Upon our planet, an intricate and vibrant ecosystem thrives, where diverse life forms engage in a symbiotic dance that sustains and enriches all. Birds, animals, plants, insects, and humans coexist in a delicate balance, each doing its part to support the health and growth of everyone. Think of the diligent bee pollinating blossoms and promising fruit. Grazing animals control vegetation, preserving landscapes for the future. Trees exchange carbon for oxygen in a silent pact that provides the air we breathe. This is a world of deep interconnection, where mutual reliance underpins existence itself.

Yet, within this symphony of life, threats lurk. Invasive species upset the balance by snatching resources and spreading unchecked. Pollutants seep into pristine environments, threatening the stability on which life depends. Viruses act like phantom infiltrators, leaving destruction in their wake. These dangers remind us how fragile and vulnerable the natural world can be.

Much like this dynamic natural ecosystem, the cyber landscape is a rich and varied ecosystem. Businesses, governments, and individuals over time have connected a vast array of digital systems and technologies, which all interact in a web that fuels communication, trade, and innovation. This interconnected digital ecosystem fosters growth and opportunity, crossing borders to benefit all.

However, just as invasive species and pollution threaten nature, the digital world faces its own threats. Malicious actors like hacktivists, cybercriminals, and state-sponsored spies mimic nature's invaders. They launch a range of cyberattacks, from simple to sophisticated, that continue to evolve and disrupt information flow, exploit vulnerabilities, and threaten the digital terrain for their own gain.

Enter our Quarterly Internet Security (ISR) report as your guide. We, as cyber defenders, act like digital ecologists, analyzing every byte, signal, and network to understand the digital threat landscape. Using our insights, we build strong defenses that mimic nature's resilience. By understanding the attacker's perspective, we can help preserve the integrity and vitality of our shared digital ecosystem.

As you explore this report, think of it as a map of the digital jungle, highlighting recent threat evolutions and offering ways to keep this cyber ecosystem safe. More specifically, this report shares key threat trends seen by many of our products, including malware developments observed from both network and endpoint solutions, network attack findings from our intrusion prevention service (IPS), ransomware development throughout the quarter, and much more.

In our connected world, general cybersecurity awareness and proactive defense actions or refinements are our most powerful tools, which this report hopes to provide. Like ecologists protecting the Earth, we all have a part to play in safeguarding what sustains us to ensure a secure future.

In this report, we cover:

EXECUTIVE SUMMARY

Like last quarter, network malware close to doubled this quarter, rising 171 percent, while total endpoint malware detection dropped. However, we also saw a huge (712 percent) rise in new unique malware variants on the endpoints. Combine that with a substantial increase in zero-day malware detection on the network and this signals a sharp rise in evasive and sophisticated malware, which delivered trojans, information stealers, coinminers, and phishing threats. While our data doesn't always provide us with the explanations behind the changes we see, we theorize that the growth in AI tools on the underground has accelerated threat actors' ability to develop sophisticated threats quickly at scale.

Meanwhile, network-based attacks and exploits remained stable, only growing by one point. Malicious attackers also targeted a lower number of specific software flaws, with unique network exploits down 16 percent. Beyond that, we saw little change in our network attack trends, with no new exploits rising to our top 10 list, and old exploits like ProxyLogon and HAProxy still hanging around, despite their age.

Finally, our endpoint section was rife with interesting changes. While total malware is down, new unique malware variants exploded, as we shared above. We all saw pretty big changes in some of the regular trends concerning malware delivery vectors. However, ransomware and cryptominers declined.

To round things out, here are some executive highlights from our Q1 2025 report:

- **Total network-based malware detections increased again, rising 171% quarter-over-quarter (QoQ).** We saw this despite a small decrease in signature-based and behavioral detection engines, .as the lion's share of the growth (323% increase) came from our proactive AI and machine-learning service IntelligentAV.
- Endpoint total malware volume was down, but **we saw a surge in unique malware detection, increasing about 712%** QoQ, which paired with our network malware trends, shows threat actors are focusing on new evasive and complex malware.
- Threat actors continue to use encryption to spread malware, with **71% of malware arriving over encrypted (TLS) connections during Q1,** which is an 11-point 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:** 4,204 (171% increase)
  - **Average malware detections by GAV per Firebox:** 374 (31% decrease)
  - **Average malware detections by IAV per Firebox:** 3,735 (323% increase)
  - **Average malware detections by APT Blocker per Firebox:** 95 (25% decrease)
- **We extrapolate** that if all the estimated currently active (licensed) Fireboxes enabled all malware detection security services and were reporting to us, **Fireboxes would have seen 1,624,555,924 malware detections during Q1 2025.**
- **Over three-quarters (78%) of malware 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. The rise was completely due to a rise in malware detected via our machine-learning and AI methods.
- Adding to this, **zero-day malware accounts for 87% of malware detected over encrypted connections,** proving a continued rise in evasive malware delivery.
- Meanwhile, **network attacks increased by a single point during Q1 2025, with only 93 software exploits per Firebox caught by IPS signatures – one more than seen last quarter.** We also saw a decline in the number of unique exploits attackers tried, with unique IPS signature hits down 16%.
- **Ransomware declined 85% from the previous quarter.** This supports the industry trend of a decrease in crypto ransomware. Attackers are now shifting toward data theft instead of encryption, as improvements in data backups and recovery have been made.
- **Endpoints malware delivery vectors shifted appreciably in Q1.** For years, malicious scripts, primarily PowerShell, have remained the most common way malware arrives on an endpoint by a fairly large margin, while Windows binaries have continued to gain ground as the second-most common vector. However, this quarter we saw browsers and other vectors rising significantly on the list, suggesting that threat actors are returning to "drive-by download" tactics and delivering malware more often in piracy-related tools and remote software.

That's just a glimpse of the trends in invasive cyber species infiltrating our shared digital ecosystem. For much more detail and tips that will make you a better cybersecurity ecologist, read on.

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 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

4,204

Average detections per Firebox jumped by **171%**

Basic Gateway AntiVirus (GAV) service

374

Basic malware dropped **33%**

APT Blocker (APT)

95

APT Blocker dropped by **25%**

IntelligentAV (IAV)

3,735

jumped by **323%**

GAV with TLS

865

TLS detections by GAV increased **30%**

Average evasive malware over TLS

153

TLS detections of evasive malware increased by **323%**

TLS malware

71%

Malware over an encrypted connection increased **11 points**

MALWARE TRENDS

In Q1 2025, the malware landscape presents escalating challenges in evasive malware, as evidenced by our Firebox Feed detection data. This data set, covering regional patterns, encrypted threats, and detection metrics, provides a vital perspective on cybercriminals' evolving strategies. To ensure reliability, we meticulously validate detection counts, reference regional distributions, confirm malware classifications, eliminate noise, and remove inconsistencies. We normalize data to account for deployment variations, transforming raw figures into actionable insights. This rigorous process enhances trust, empowering security teams to make informed decisions. From tracking encrypted malware surges to pinpointing regional vulnerabilities, this data equips organizations to adapt defenses for threats like droppers, botnets, and coinminers.

The Quarterly Overview table highlights average detection hits across security services and their changes since Q4 2024. Total malware detections average 4,204 per Firebox, a 171% surge, signaling a sharp rise in threats. Gateway AntiVirus (GAV) records 374 hits, down 31%, while APT Blocker logs 95 hits, a 25% decline. IntelligentAV (IAV) jumped with 3,735 hits, soaring 323%, reflecting its critical role in detecting advanced malware. For TLS-inspected traffic, GAV hits reach 865, up 30%, while evasive malware over TLS averages 16 hits, down 11%. Notably, TLS malware accounts for 71% of detections, an 11-point increase, underscoring encrypted channels as a primary attack vector.

These evasive threats, often unique or polymorphic, alter their code to evade signatures and so require advanced detection through IAV and APT Blocker to detect. The table reveals that while basic malware persists, advanced, encrypted threats are intensifying. The dramatic IAV surge and elevated TLS malware highlight attackers' reliance on obfuscation and encryption, testing conventional defenses. Fireboxes with TLS decryption capabilities are essential, as the 11-point TLS malware rise emphasizes the need for enhanced visibility and adaptive security to combat these sophisticated, concealed threats effectively.

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

Top 10 Malware Detections

In Q1 2025, our analysis of malware detections from Fireboxes reveals critical trends in cyber threats, with the Top 10 Malware Detections table providing actionable insights for security professionals. This list, compiled from Firebox telemetry, highlights the most prevalent malware strains, their categories, and their impact. We review this data to ensure its accuracy and reliability, enabling organizations to prioritize defenses against the most pressing threats.

Leading the list is Trojan.Agent.FZPI, a dropper malware with 565,213 detections, a new threat in Q1 2025. Notably, it's the most common encrypted malware detection, leveraging encryption to evade traditional defenses. This trojan primarily targets systems in the United States, delivering malicious payloads that compromise networks. Its dominance underscores the growing sophistication of droppers in facilitating secondary infections.

Another significant entry, Application.Cashback.B.0835E4A4, with 277,359 detections, and its variant, Application.Cashback.B.66D22628 (69,105 detections), are both new droppers that create backdoors. We also see these detections in the most widespread malware.

The table also reflects a continued surge in Linux-targeting malware, a trend observed in previous quarters. Strains like Variant.Application.Linux.Miner.3 (423,156 detections) and Application.Linux.Generic.24096 (154,017 detections), both coinminers, exploit Linux systems for cryptocurrency mining. Similarly, Trojan.Linux.Mirai.1 (84,033 detections), a botnet, underscores the growing focus on Linux environments, often perceived as secure but increasingly targeted due to their widespread use in servers and IoT devices. Another significant threat, Variant.Trojan.Linux.Gafgyt.8, in the unseen 11th spot, comes as a dropper with 41,435 detections. Gafgyt often delivers botnets like Mirai, which are notorious for orchestrating large-scale distributed denial-of-service (DDoS) attacks. Its persistence highlights the enduring challenge of botnet-driven campaigns targeting vulnerable devices.

This data, meticulously validated, emphasizes the need for robust, platform-agnostic security measures. The prevalence of droppers, botnets, and Linux-specific threats in Q1 2025 signals that attackers will identify new vulnerable paths into previously secured networks. By leveraging insights from this table, organizations can strengthen their defenses, particularly against encrypted threats like Trojan.Agent.FZPI to stay ahead of evolving cyber risks.

Threat Name	Malware Category	Count	Last Seen
Trojan.Agent.FZPI	Dropper	565,213	new
Variant.Application.Linux.Miner.3	Coinminer	423,156	Q4 2024*
Application.Linux.Generic.24096	Coinminer	154,017	Q4 2024
Application.Cashback.B.0835E4A4	Dropper	277,359	new
Application.Agent.IIQ	Dropper	120,320	Q4 2024
Trojan.Linux.Mirai.1	Botnet	84,033	Q4 2024
Application.Cashback.B.66D22628	Dropper	69,105	new
Application.Linux.Generic.11804	Dropper	54,878	Q4 2024
SpamMalware-ZIP.Gen	Dropper	54,402	new
PasswordStealer.GenericKDS	Password Stealer	47,071	Q4 2024

Figure 1. Top 10 Malware Detections

*We have seen Linux coinminers in the past but now we have a specific family name for them.

Top 5 Encrypted Malware Detections

The Top 5 TLS Malware table from Firebox telemetry highlights malware detected over encrypted connections, emphasizing the critical need to inspect this traffic. These threats, identified through TLS scanning, reveal how attackers exploit encryption to evade detection. Only 20% of Fireboxes are configured currently to scan encrypted connections, underscoring the urgency of enabling this capability to uncover hidden threats.

Leading the list again is Trojan.Agent.FZPI, the same one we saw in the previous table, followed by Application.Agent.IIQ (120,320) and Trojan.SpamMalware-ZIP.Gen (54,348), both droppers. Trojan.VBA.Agent.BIZ (39,781), another dropper, and Trojan.PWS.Agent.SWV (16,381), a code injection threat, round out the table. These entries overlap with the Top 10 Malware Detections, indicating that encrypted channels are a common vector for prevalent threats.

These droppers serve as gateways to install additional malware, amplifying their impact. As you will see later, droppers like Trojan.Agent.FZPI deliver payloads that compromise systems, making early detection vital. The high volume of such threats in encrypted traffic highlights the risk of uninspected connections.

Threat Name	Malware Category	Count
Trojan.Agent.FZPI	Dropper	565,213
Application.Agent.IIQ	Dropper	120,320
Trojan.SpamMalware-ZIP.Gen	Dropper	54,348
Trojan.VBA.Agent.BIZ	Dropper	39,781
Trojan.PWS.Agent.SWV	Win code injection	16,381

Figure 2. Top 5 TLS Malware

Top 5 Widespread Malware Detections

The Top 5 Widespread Malware Detections table from Q1 2025 identifies the most prevalent malware encountered across numerous Fireboxes worldwide. We see malware with the broadest reach, detailing their distribution by top countries and regions. The table provides critical insights into pervasive threats across the world.

Topping the list is Application.Cashback.B.0835E4A4, a brand-new threat and one of the most widespread malware families ever observed, with significant impact in Chile (75.54%), Ireland (65.43%), and France (59.05%). Its counterpart, Application.Cashback.B.66D22628, also ranks high, affecting countries like Japan, Australia, and Switzerland. The table includes Exploit.CVE-2017-0199.05, a persistent Microsoft Office exploit family, and two variants of Trojan.Zmutzy that carries over from the previous quarters, demonstrates their enduring global presence.

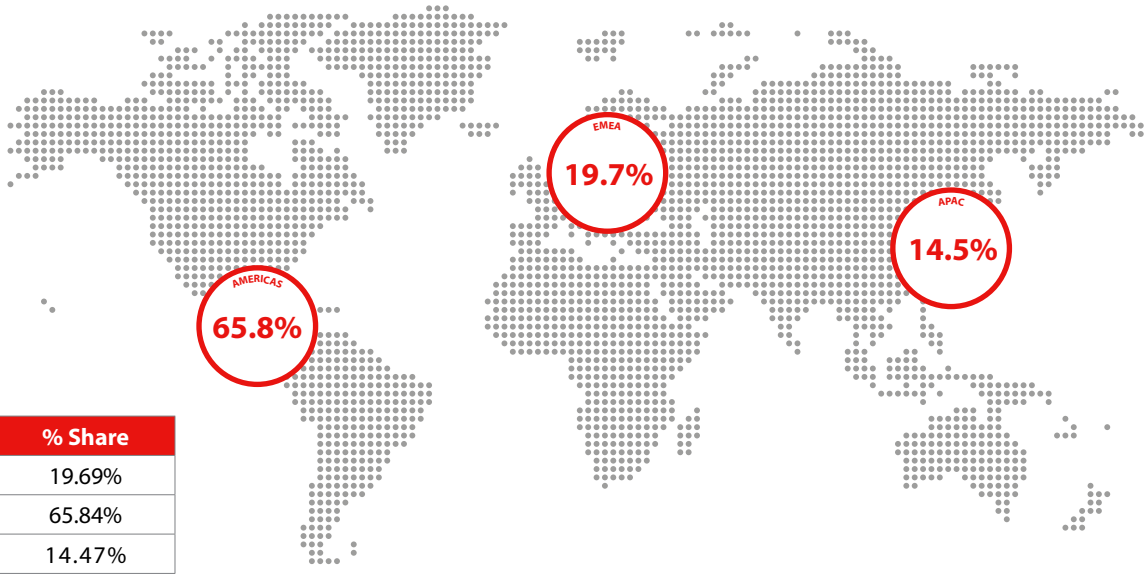
The prominence of Application.Cashback variants signals a new wave of widespread threats, while the continued detection of Exploit.CVE-2017-0199.05.Gen and Trojan.Zmutzy underscores the resilience of established malware.

Malware Name	Top 3 Countries by %			EMEA %	APAC %	AMER %
Application.Cash-back.B.0835E4A4	Chile - 75.54%	Ireland - 65.43%	France - 59.05%	40.45%	26.42%	35.22%
Application.Cash-back.B.66D22628	Japan - 27.15%	Australia - 27.15%	Switzerland - 24.3%	10.89%	21.65%	18.05%
Exploit.CVE-2017-0199.05.Gen	Greece - 14.94%	Czech Republic - 11.27%	Portugal - 11.24%	6.68%	2.60%	1.86%
Trojan.Zmutzy.1301	Hong Kong - 22.22%	Greece - 16.09%	Czech Republic - 14.08%	5.67%	3.59%	1.27%
Trojan.Zmutzy.834	Hong Kong - 18.52%	Czech Republic - 15.49%	Greece - 11.78%	4.79%	3.45%	1.26%

Figure 3. Most-Widespread Malware

Geographic Threats by Region

The Region table shows the percentage of malware detections per region, normalized by the number of Fireboxes in each area. This ensures a fair comparison of malware prevalence. The Americas (AMER) lead with 65.84% of detections, followed by Europe, Middle East, and Africa (EMEA) at 19.69%, and Asia-Pacific (APAC) at 14.47%. The data highlights regional disparities in malware activity. For example, we see Trojan.Agent. FZPI heavily targeted the United States, leveraging encryption to evade detection. This table emphasizes the need for region-specific defenses, particularly in AMER, to counter sophisticated threats.



Region	% Share
EMEA	19.69%
AMER	65.84%
APAC	14.47%

Figure 4. Geographic Threats by Region

Catching Evasive Malware

The Zero-Day Malware table shows the prevalence of advanced evasive malware versus basic, signature-detectable malware. Among devices with APT Blocker and IntelligentAV, 78% of detections are zero-day threats, with only 22% caught by signatures. For devices also inspecting HTTPS traffic, zero-day detections rise to 87% versus 13% signature-based. These evasive threats, lacking family names, are unique or use polymorphism to alter their code, rendering them invisible to traditional defenses. The growing challenge of never-before-seen malware, particularly over encrypted connections, increases the need for advanced detection tools like IAV and APT Blocker to combat these sophisticated, ever-changing threats effectively.

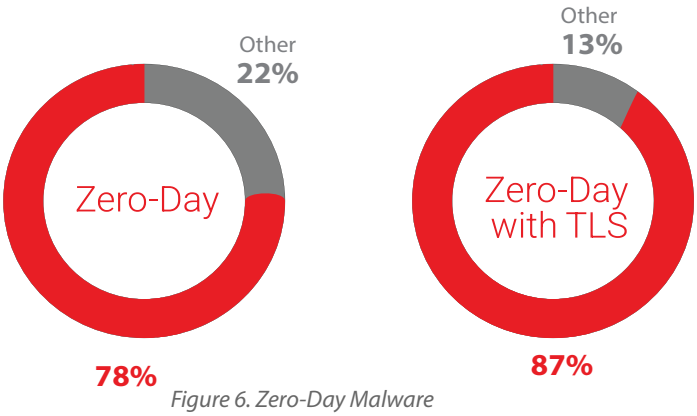


Figure 6. Zero-Day Malware

Individual Malware Sample Analysis

Application.Cashback

Google recently deprecated an older version of the manifest file. The manifest file in browser extensions, typically named "manifest.json", is a configuration file that defines the extension's properties, behavior, and permissions. It serves as the blueprint for how the browser should handle the extension. This made it more difficult to use browser extensions to block ads. Many users looked for alternatives, and bad actors took advantage of this.

We investigated a sample of this malware, and at first we dismissed it as a false positive. We didn't find any indicators that this file does anything suspicious, but we did find it contains stolen code from the ABP adblocker. We could tell this code was stolen because it connected to a site not related to ABP called fnet-vpn[.]ru. More on this site later.

This file comes as an extension for Chrome and as previously mentioned, it blocks adware. An unscrupulous way to finance adware projects is to have websites pay the adblocker not to include their ads in any blacklists or simply replace ads with ads they serve. Because this no longer functioned, we were unable to verify this.

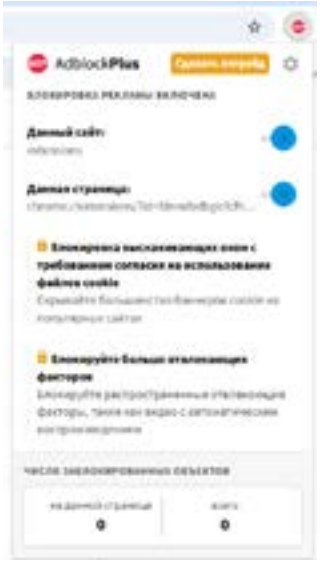


Figure 5. adblocker.ABP

The website we found, fnet-vpn[.]ru, to which the malware connects, has a sister site, snet-vpn[.]ru, that provides known malicious Chrome extensions, this time as a VPN extension. They both provide browser extensions, use the same infrastructure, and stopped providing these extensions around the end of April. This connection indicated a malicious intent for the file detected, even though we saw no such indication from the fake ABP extension by itself.

Be careful of unknown extensions. It might be easy to just try an unknown extension to get rid of annoying adware, but this could lead to leaked confidential details or worse.

Figure 7. Trojan.Agent.FZPI

Trojan.Agent.FZPI, a malicious HTML-based dropper, emerged as a dominant threat in Q1 2025. This malware begins its attack by downloading TXRTN_2636021.zip, which requires the password embedded in the HTML to access. The zip contains TXRTN_2636021.iso, which houses 102755.dll, WindowsCodecs.dll, TXRTN_2636021.lnk, and a non-malicious calc.exe. Analysis indicates it sideloads Qbot, a notorious banking trojan, by infecting the legitimate Windows calc.exe on the victim's system. However, if the system's calc.exe is unavailable, it leverages calc.exe in the package to ensure infection, though parts of the installation chain remain missing.

Figure 8. Trojan.Agent.FZPI.iso

As the most-detected encrypted malware, Trojan.Agent.FZPI, uses TLS to evade detection, primarily targeting the United States. Its multi-stage delivery, blending legitimate-looking files with encrypted communication, highlights its evasiveness. Organizations must adopt robust TLS inspection, behavioral analysis, and endpoint protection to detect and neutralize this threat. By disrupting the initial infection mechanism, security teams can prevent Qbot infections and safeguard critical systems from this high-impact, stealthy malware campaign.

Figure 9. SpamMalware-ZIP.Gen-email

Figure 10. SpamMalware-ZIP.Gen-icon

SpamMalware-ZIP.Gen is a malicious email campaign delivering Trojan.Zmutzy. The email appears polished, but a critical clue to its intent lies in the mismatched "from" address and the email address in the signature. This discrepancy serves as an effective way to identify suspicious emails. The email's attachment, a ZIP file, harbors Trojan.Zmutzy, a trojan "loader" that downloads additional malware like Agent Tesla, which stealthily steals sensitive data, including clipboards, browser cookies, and keystrokes. See our Q4 2023 report for more on Zmutzy. To combat this deceptive threat, organizations must implement robust email filtering and educate users to scrutinize email inconsistencies, ensuring protection against this insidious malware.

NETWORK ATTACK TRENDS

Network exploit attempts remained relatively stable in Q1 2025 compared to previous quarters. This quarter, the average Firebox defended against 93 network attacks, up slightly from 92 in Q4 2025. This came alongside a decrease in the unique number of signatures triggered at 412 for Q1, down from 492 in Q4. In other words, attackers concentrated on a narrower set of exploits this quarter at scale. The implication is clear – adversaries doubled down on a few efficient attack techniques and blasted them broadly across the Internet. Defenders are now contending with an onslaught of repeated exploit attempts, even as the overall mix of attack types briefly narrows. That said, the quarter's onslaught included a mix of both old and new threats, echoing a familiar pattern where tried-and-true exploits persist alongside emerging techniques. One notable continued trend was the enduring presence of critical vulnerabilities in widely used enterprise software: the infamous Microsoft Exchange "ProxyLogon" flaw from 2021 remained a fixture on our top lists, and a 2023 HAProxy request smuggling bug still saw active exploitation. Ultimately, Q1's network attack landscape underscores that while novel exploits do appear, attackers continue to heavily leverage unpatched legacy vulnerabilities at scale – forcing organizations to address both fronts simultaneously.

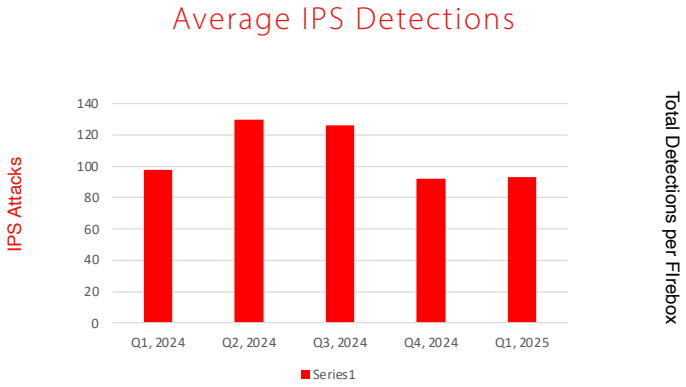


Figure 11. Average IPS Detections per Firebox

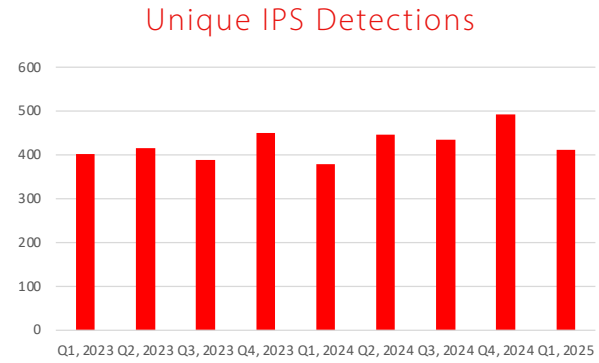


Figure 12. Unique IPS Detections

Top 10 Network Attacks Review

The top 10 network attack signatures by volume this quarter reveal a heavy concentration of web application exploits, with everything from file inclusion and directory traversal to SQL injection in the mix. Many of these signatures represent broad classes of attacks covering multiple vulnerabilities, and even decades-old exploits are still generating significant traffic. In fact, all of Q1's "Top 10" were familiar returnees from previous reports. Most of the top 10 returned directly from Q4 2024, but two threats, SHELLCODE NOP Sled (ID 1056247) and WEB Local File Inclusion – win.ini (ID 1054838), made a return after over a year outside the top 10.

Top 10 History

Signature	Type	Name	Affected OS	Percentage
1059877	Exploits	WEB Directory Traversal -8	Windows, Linux, Freebsd, Solaris, Other Unix	8.96%
1136822	Web threats	WEB dotCMS CMSFilter assets Access Control Weakness (CVE-2020-6754)	Network Device, Others	8.21%
1131523	UNKNOWN	UNKNOWN	UNKNOWN	5.37%
1138800	Web threats	WEB Microsoft Exchange Server Remote Code Execution Vulnerability -6 (CVE-2021-26855)	Windows	5.12%
1056247	Exploits	SHELLCODE NOP Sled	All	4.71%
1059958	Web threats	WEB Directory Traversal -27.u	Windows, Linux, Others	4.32%
1054837	Web threats	WEB Remote File Inclusion /etc/passwd	Windows, Linux, Freebsd, Solaris, Other Unix	4.28%
1231780	Web threats	WEB HAProxy h1_headers_to_hdr_list Empty Header Name Access Control Bypass (CVE-2023-25725)	Network Device	4.26%
1133539	Web threats	WEB SQL injection attempt -2.u	Windows, Linux, Freebsd, Solaris, Other Unix, macOS	4.00%
1054838	Web threats	WEB Local File Inclusion win.ini -1.u	Windows	3.48%

Figure 13. Top 10 Network Attacks by Volume

This list was dominated by web server and web app exploits, a trend consistent with previous reports. Broadly speaking, attackers continued hammering on common web vulnerabilities. For instance, a generic directory traversal attack (signature 1059877) was again the single most-frequent attack by volume this quarter (as it was last quarter), accounting for a significant share of all IPS hits. Similarly, an access control weakness in dotCMS (CVE-2020-6754) remained near the top of the list, demonstrating that attackers are still aggressively scanning for vulnerable content management systems. We also saw Microsoft Exchange Server exploits holding strong in the rankings, notably the ProxyLogon remote code execution attack (CVE-2021-26855) persisted as a top-five volume threat in Q1, just as it did throughout 2024. The continued prevalence of ProxyLogon over two years since disclosure highlights that many Exchange servers out there are still unpatched, and adversaries know it. Rounding out the top 10 were several other web-based attacks, including SQL injection attempts and cross-site scripting injections, which have appeared in our top lists many times before.

Notably, there were no brand-new 2025 CVEs cracking the top 10 by volume – the list was essentially a reshuffling of known exploits. This reiterates the point that attackers often find more value in exploiting long-standing, unpatched flaws than in deploying bleeding-edge 0-days. Organizations should take this as motivation to double-check patch management on those older, "boring" vulnerabilities that continue to drive massive attack traffic.

New Detections in the Top 50

This quarter, three new IPS signature detections broke into the top 50 by volume for the first time, highlighting both newly emergent exploits and the resurfacing of older vulnerabilities. These include a long-known Windows Shell exploit, a flaw in an embedded web server, a generic file upload attack pattern, and a critical VPN authentication bypass. Each is summarized below with technical context and implications.

Signature	Type	Name	Affected OS	Rank
1134327	Web threats	WEB EmbedThis GoAhead Web Server CGI Remote Code Execution (CVE-2017-17562)	Network Device	38
1133321	Web threats	WEB Generic Remote Javascript Upload and Execution -2.b	Windows, Linux	44
1232238	Web threats	WEB Ivanti Connect Secure and Policy Secure Gateways Authentication Bypass -1.1 (CVE-2023-46805)	Windows, Linux	48

Figure 14. New signatures this quarter among the top 50 signatures by volume.

Signature 1134327
This signature represents a remote code execution vulnerability in the EmbedThis GoAhead web server, commonly used in embedded and IoT devices. The flaw (CVE-2017-17562) affects GoAhead versions prior to 3.6.5 and stems from how the server handles CGI requests. If CGI functionality is enabled with dynamically linked executables, an attacker can abuse environment variables to execute arbitrary code. In practice, the exploit involves sending a crafted HTTP request that includes a malicious LD_PRELOAD parameter and a payload library; the GoAhead CGI handler unwittingly loads the attacker's shared object into memory, leading to code execution with system privileges. This vulnerability is known to be actively exploited (it's on CISA's KEV list) and can fully compromise affected devices. Network administrators should ensure any IoT or network appliance running GoAhead is updated to 3.6.5 or later, or disable unnecessary CGI modules, to mitigate this risk.

Signature 1133321
This detection covers a class of web application vulnerabilities that allow attackers to upload and execute malicious scripts on a server. It's a "generic" signature triggered by multiple products' exploits, one example being a past Oracle Beehive flaw. In Oracle's Beehive collaboration software (Services for Beehive component), a bug allowed file uploads with dangerous extensions by inserting a null byte in a filename, thereby letting an attacker create a .jsp file on the server and execute arbitrary Java code. Another instance (ZDI-15-550) in 2015 was an Oracle Beehive voice server vulnerability that permitted writing arbitrary content to the web root, leading to remote code execution as SYSTEM. In general, Signature 1133321 alerts on attempts to exploit these file-upload RCE paths.

A successful attack in this category typically results in the adversary gaining a foothold on the server, for example, by planting a web shell or malicious script.

The appearance of this signature in the top 50 suggests that attackers are actively probing older web apps for unpatched file upload flaws. Ensuring web servers and CMS platforms have up-to-date patches (for vulnerabilities like CVE-2010-4417, etc.) and restricting file uploads (by type and location) are crucial defenses.

Signature 1232238
Rounding out the new top 50 entries is an authentication bypass in Ivanti Connect Secure (formerly Pulse Secure) and Ivanti Policy Secure VPN appliances. CVE-2023-46805 is a critical flaw disclosed in January 2024 that allows an unauthenticated attacker to gain privileged access to the VPN's web portal by manipulating the URL path. The vulnerability is caused by insufficient validation of HTTP request paths – effectively, an attacker can include directory traversal sequences (..) in API endpoints to evade access control checks and impersonate an authenticated session. In real-world attacks, threat actors chained this bug with a follow-on command injection (CVE-2024-21887) to achieve full remote code execution on unpatched VPN servers. Even alone, the authentication bypass can expose sensitive configuration and give attackers a foothold into the internal network via the VPN. This signature's debut in the top 50 reflects active, wide-scale scanning for vulnerable Ivanti VPNs. Security teams should immediately apply Ivanti's patches and advisories for these gateways and monitor them closely, as these devices continue to be high-value targets for attackers.

Each of these new detections underscores the importance of timely patch management and network defenses. From decades-old Windows and web server bugs to recent VPN zero-days, attackers are leveraging any weakness, old or new, to infiltrate systems. IT and security professionals should verify that the associated vulnerabilities (and similar ones) are addressed in their environments, deploy virtual patching/IPS where available, and remain vigilant for signs of exploitation. By taking these steps, organizations can blunt these emerging attack trends and reduce their exposure to both legacy and cutting-edge threats.

Most-Widespread Network Attacks

While the above top 10 reflects sheer volume of detections, another critical perspective is prevalence – which network attacks are striking the widest range of victim networks. Often, an exploit with modest total hits can still be extremely widespread if it's being opportunistically sprayed across the Internet. In Q1 2025, the list of most-widespread network attacks (those seen on the highest percentage of Fireboxes) remained largely consistent with the prior quarter's findings, with just one new addition to the list.

Signature	Name	Top 3 Countries by %			AMER %	EMEA %	APAC %
1131523	WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability -2 (CVE-2015-2425)	United Kingdom 76.58	France 72.86	Canada 67.18	57.03	63.19	45.69
1136822	WEB dotCMS CMSFilter assets Access Control Weakness (CVE-2020-6754)	Germany 38.43	Brazil 31.58	Canada 16.79	12.18	21.20	12.52
1059877	WEB Directory Traversal -8	Germany 20.89	Italy 19.71	Australia 19.48	10.40	14.49	24.87
1138800	WEB Microsoft Exchange Server Remote Code Execution Vulnerability -6 (CVE-2021-26855)	Germany 20.52	Australia 12.99	Italy 10.75	7.51	12.11	13.20
1132643	WEB HAProxy h1_headers_to_hdr_list Empty Header Name Access Control Bypass (CVE-2023-25725)	Australia 20.78	USA 17.7	United Kingdom 17.67	16.18	9.21	16.24

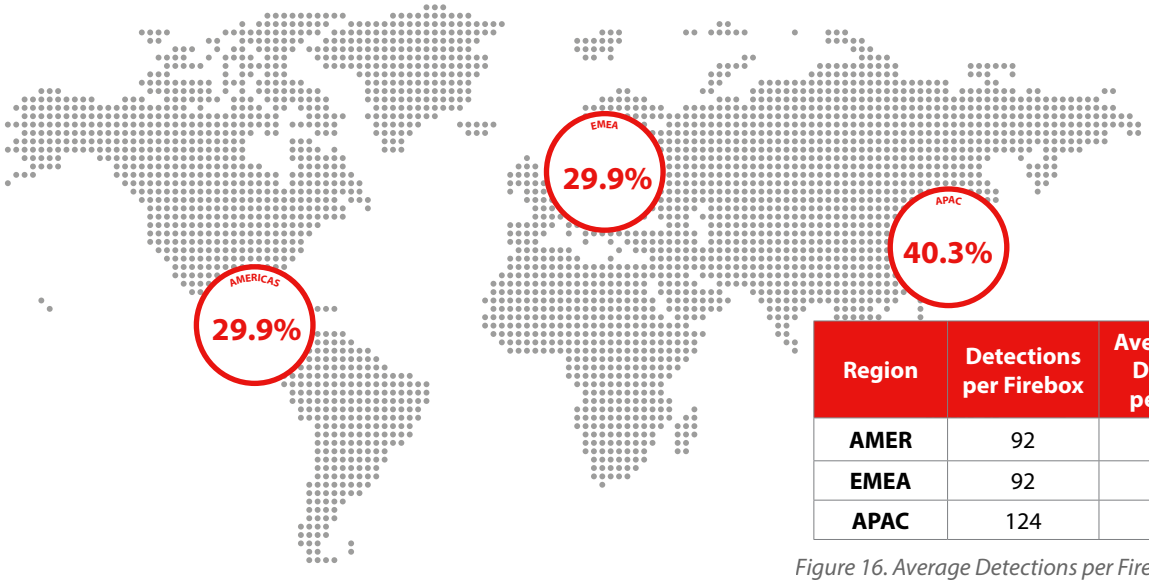
Figure 15. Top 5 Most-Widespread Network Attacks

Signature 1231780 detects attempted exploits of CVE-2023-25725, an HTTP request smuggling vulnerability in HAProxy that has been a mainstay in our top network attacks by volume list since Q1 2024. We originally discussed this vulnerability in Q2 2023 when it showed up in our top 50 by volume data set shortly after HAProxy disclosed the issue. It makes sense that this issue would eventually break into the most widespread list of vulnerabilities since HTTP request smuggling opens up a suite of attack paths, like access control bypass, for adversaries.

Overall, the most-widespread attacks this quarter reinforce that attackers often stick with what works, spraying older exploits far and wide to cast a wide net. The top five threats saw virtually no turnover from last quarter aside from the HAProxy flaw. This is a clear indication that adversaries are still finding unpatched systems for the same well-known vulnerabilities. Even as new exploits arise, these tried-and-true techniques (some dating back 5-10+ years) continue to offer plenty of yield for attackers. This should serve as a warning: just because a CVE is old does not mean it isn't being actively used against targets every single day. From a defender's standpoint, broad-based attacks like these emphasize the importance of an Internet-wide view of threat trends, if a particular exploit attempt is hitting over half of all organizations, every company should ensure they aren't exposed to it.

Network Attacks by Region

The geographic spread of network attacks can tell us where adversaries are focusing their efforts, either because of high-value targets or networks with limited defenses. For the 4th quarter in a row, the region encompassing Asia and the Pacific (APAC) had the largest share of network attacks at 40%, up only slightly from Q4 (39%). Interestingly, the Americas (AMER) and Europe the Middle East and Africa (EMEA) both had a nearly identical share of network attack volume at 30% each. This returned to a multi-year trend of AMER and EMEA being relatively similar, with APAC accounting for either notably more or significantly less of a share.



Region	Detections per Firebox	Average % IPS Detections per Firebox
AMER	92	29.87%
EMEA	92	29.87%
APAC	124	40.26%

Figure 16. Average Detections per Firebox by Region

Detections Percentage by Region

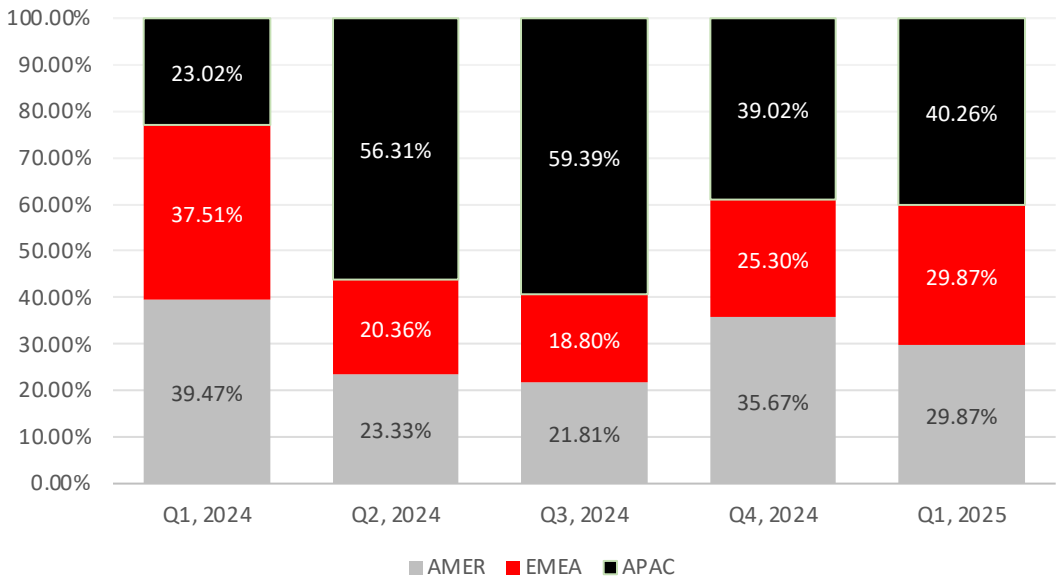


Figure 17. Average Detection per Firebox Percentage since Q4 2023

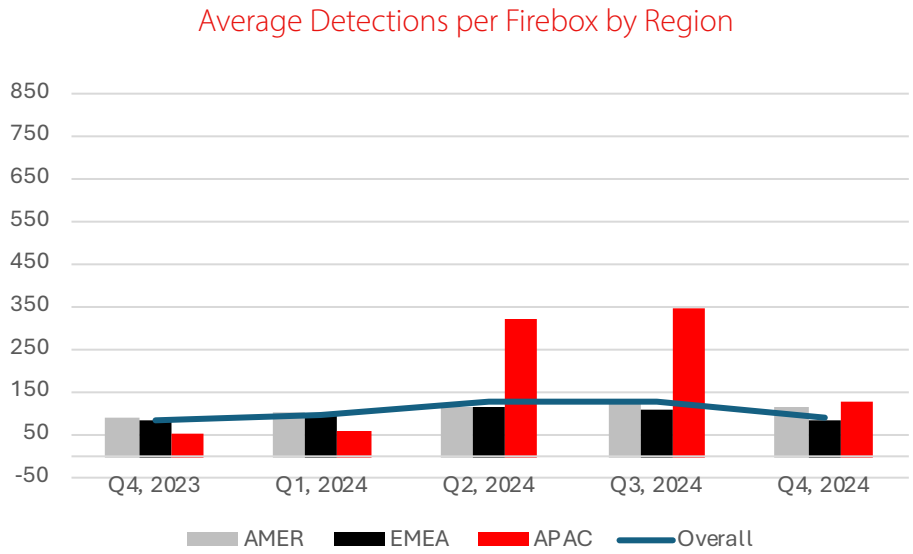


Figure 18. Average Detections per Firebox by Region since Q4 2023

Conclusion

In summary, Q1 2025's network attack trends show a threat landscape where old habits die hard for attackers, even amid surges in activity. Many of the quarter's leading attack vectors were familiar from past reports, which is a clear sign that adversaries continue to find success exploiting years-old weaknesses. At the same time, the sudden spike in overall attack volume reminds us that attackers can rapidly scale up their efforts when needed, whether due to new campaigns or automated tools. The takeaway for defenders is two-fold: we face a dual challenge of patching old holes while keeping up with new threats. Organizations must remain vigilant with the cybersecurity basics, keep systems updated, harden those long-standing vulnerabilities, monitor for abnormal activity, and maintain layered defenses to catch the inevitable exploit attempts that slip through initial layers. By doing so, businesses can greatly mitigate the risk from both the steady drumbeat of legacy exploits and the spikes of novel attack techniques alike. The data this quarter makes it clear that neither can be ignored.

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
p2[.]feefreepool[.]net
newage[.]newminer-sage[.]com
newage[.]radnew-age[.]com
thaus[.]top
t[.]hwqloan[.]com
pcdnbus[.]ou2sv[.]com
rqmetrixd[.]info *
rqmetrixb[.]info *
rqmetrixc[.]info *

* New in Q1 2025

Figure 19. Top Malware Domains

WARNING

It should go without saying that you should not visit any of the malicious links we share in this report; at least not without knowing exactly what you are doing. Anytime you see us share a domain or URL where we have purposely added brackets around a dot (e.g. www[.]site[.]com), we are both making the hyperlink unclickable and warning you not to visit the malicious site in question. Please avoid these sites unless you are a fellow researcher who knows how to protect yourself.

Top Malware Domains

Attackers rely on malicious domains to host both malware distribution, command and control communications, and cryptomining against unsuspecting victims. WatchGuard DNSWatch is well-positioned to identify and block connections that might facilitate malware distribution or oversight, preventing and mitigating malware-based attacks against endpoints. This section highlights the top 10 malware domains involved in malware distribution and management in Q1 2025.

Polyfll[.]io remained the top blocked domain this quarter, with nearly 10x as many blocked connections as #2 on the list. Even half a year after the world became aware of the hostile takeover of this once-popular JavaScript library, many web applications continue to include it.

There were three new additions to the top 10 list in Q1 2025, all involved in the same CoinLoader cryptomining campaign that we originally discussed in the Q3 2024 Internet Security Report. The CoinLoader malware used these domains for DNS tunneling, a cover communication channel that uses domain name resolution to send and receive information. DNS tunneling can be an effective method of command control in networks that blanket allow outbound DNS without any additional protection.

Phishing
unitednations-my[.]sharepoint[.]com
data[.]over-blog-kiwi[.]com
nucor-my[.]sharepoint[.]com
t[.]go[.]rac[.]co[.]uk
ulmoyc[.]com
e[.]targito[.]com
www[.]namunvida[.]es *
ptekuwiny[.]pro *
bestsports-stream[.]com
edusoantwerpen-my[.]sharepoint[.]com

Figure 20. Top Phishing Domains

Top Phishing Domains

After a couple of quarters of no meaningful change, this quarter we saw two domains break into the top 10 phishing domains by volume. As a reminder, phishing domains are directly associated with social engineering campaigns against WatchGuard DNSWatch customers. Their most common objectives include tricking victims into willingly entering credentials into legitimate-looking authentication portals, or convincing them to run malware on their machines.

We added the first new domain, www[.]namunvida[.]es, to DNSWatch's phishing domain feed nearly six years ago after finding a Microsoft 365 phishing campaign hosted on it. Attackers used this domain to host what looked like a real Microsoft 365 login form that was designed to send credentials to a server under the attacker's control.

Figure 21. Phishing redirect to malicious file

The second new domain, ptekuwiny[.]pro, joined our list four years ago after we found it involved in a phishing campaign that involved redirecting victims through a series of domains before ultimately serving them up a malicious file download. The file claimed to be a Flash SD card reader app.

Top Compromised Domains

The top compromised domains list is a collection of legitimate websites that attackers have compromised to host malicious content. Compromised websites aren't always overt. Often, cyber-criminals will leave the legitimate pages untouched to avoid raising alarm and instead add their own additional content on unlinked paths. This quarter, there were two new domains in the top 10 list.

We added the first new domain, www[.]oaloo[.]com[.]br, about a year ago after finding it involved in the EtherHiding that we discussed in the Q2 2024 Internet Security Report. As a reminder, this campaign used the Binance blockchain to host a malicious PowerShell script. When a victim visited the compromised website, JavaScript on the site retrieved the PowerShell script from the blockchain and prompted the user to download and run it on their machine.

We added the second new domain, serfir[.]com, about a year ago as well, after finding it involved in a malvertising campaign that redirected victims to a sketchy ecommerce website. The attackers appear to have targeted a webpage indexed by Google Search so that when victims clicked a search result link, they were ultimately redirected to the ecommerce site.

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 Q1 2025

Figure 22. Top Compromised Domains

FIREBOX FEED: DEFENSE LEARNINGS

This quarter, we saw a significant volume of threats involving phishing emails and other social engineering, paired with a massive increase in evasive malware threats. These are indicators that cyber threat actors have found more automation opportunities, likely thanks to an increased adoption of artificial intelligence. We're in a new age of automation, both in attack and defense, and the organizations that don't adapt will face the consequences. We've provided a few more specific tips below to help defend against these modern threats.

01 Machine Learning Adoption Is Critical

This quarter saw a significant rise in evasive threats that evaded basic signature-based detections. Malware authors are already relying on AI and machine-learning capabilities to create these threats at scale, which means defenders need to adopt technologies capable of detecting and preventing these threats at scale. Anti-malware services that use machine learning are an important tool in your tool belt to efficiently and effectively identify evasive threats before they can impact your network.

02 Defend Against Malicious Attachments

Several of the top new malware threats this quarter were malware droppers that arrived as email attachments. Attackers are using ZIP archives and HTML files to evade file-type-based protections and trick victims into interacting with the phish. Make sure you have security controls that evaluate ALL email attachments for malicious content, regardless of file type, and include unpacking ZIP archives to review their contents.

03 Secure Your Remote Access Tools

One of the new threats to break into the top 50 network attacks this quarter was a 2023 vulnerability in the Ivanti Connect Secure remote access tool. By nature, traditional VPN and remote access tools must be exposed to the Internet to facilitate legitimate remote access connections, but this exposes them to cyber threat actors as well. At a minimum, make sure you have MFA protecting all remote authentication and a process in place to quickly identify and remediate vulnerabilities as fast as possible.

ENDPOINT THREAT TRENDS

It's a new quarter of a new year, with new data. Typically, we try to ingest an increasing amount of data every quarter and expand on this section, and we use this expansion to refine how we portray visuals and make modifications. Basically, we attempt to make changes in the Endpoint section every quarter, but this quarter is different. The turn of the new year is a perfect opportunity to pause on the ever-changing modifications and work with what we have. If you're a returning reader, you've probably noticed how extensive this section has gotten over the past few quarters.

Last quarter, we made massive expansions to the Attack Vectors section and added additional visual aids to show annual summations from Q1 to Q4. This quarter, however, we've dialed it back. We've removed the annual summation visuals, and we made no changes to any section or subsection. Therefore, you won't have to worry about what's different this quarter and what to look out for.

Before we dive into Q1, as a precursor, we plan on making slight additions to Threat Hunting in Q2. After this report we will have enough contiguous data from WatchGuard's Endpoint Protection, Detection and Response (EPDR) to add more there. Improvements to EPDR allow us to non-intrusively ingest and analyze more data as we protect, detect, and respond to threats. However, that's only if WatchGuard-protected users opt-in to anonymously send aggregate data, which we use in these reports!

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

MALWARE FREQUENCY

The Malware Frequency subsection contains the first two data points that best describe the overall landscape for any given quarter. It's direct. It allows us to quickly observe the total malware blocked on endpoints and any never-before-seen malware threats, which we deterministically define as a ratio of "per 100k active machines." In recent quarters, we've seen a seesawing of observable threats on EPDR-protected endpoints. For example, in Q2 2024 there were around 100,000 total threats. Then, in the following quarter, that number surged to over 400,000, a four-fold increase. In Q4 2024, the total threats plummeted to 37,250, significantly less than the over 400,000 from the prior quarter, and a far cry from the 100,000 in Q2. Now, in Q1 2025, the number has stabilized (for now), decreasing a modest 21.81% to 29,127, which is a good sign for readers protected by EPDR-protected systems.

Total Malware Threats	29,127

Figure 23. Q1 2025 QoQ Total Malware Threats

Figure 24. Q1 2025 QoQ Total Malware Threats

We've observed a significant drop in total malware threats this quarter and last, but it's a different story for new malware threats. For three quarters straight, we've observed a decrease in new threats. However, for Q1 2025 we observed a 712.50% increase in new malware threats on endpoints. Therefore, we can assume that in Q4, new threats have "bottomed out." Anecdotally, many of these new threats were RATs and AutoIT scripts that download additional malware. For example, we blocked LummaStealer samples downloaded from AutoIT scripts, similar with DarkCloud malware. Also, we blocked newer RATs such as NetSupport and VenomRat, and we continue to see AsyncRAT samples across endpoints. In short summary, we've seen a modest decrease in total malware threats and a significant increase in new malware.

New Threats Blocked per 100k Active Machines	65

Figure 25. Q1 2025 New Malware Threats (Previously Unknown)

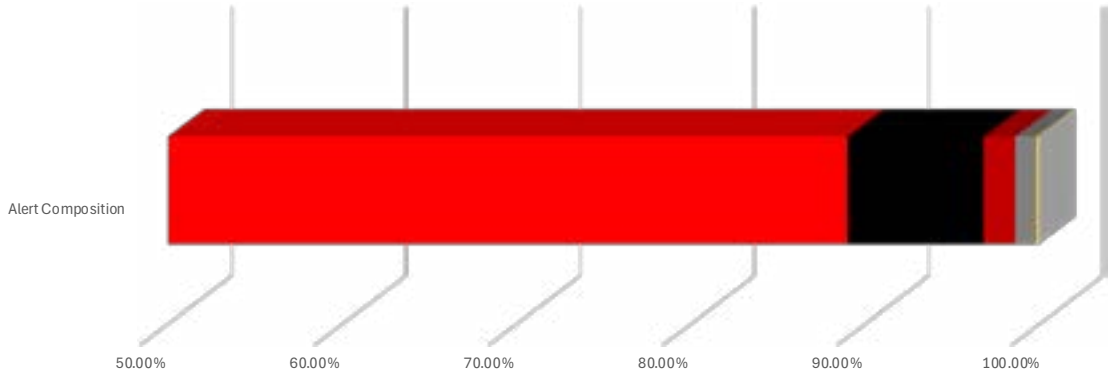
Figure 26. Q1 2025 QoQ New Malware Threats Per 100k Active Machines

Alerts by Number of Machines Affected

We now pivot and spotlight the aforementioned malware threats in a different manner. It's simple to portray overall malware frequency, but providing increased telemetry showcases more about these threats as opposed to if we saw more or less malware. The Alerts by Number of Machines Affected subsection gives insight into which of these malware threats appeared on one, two, or a handful of machines, and which ones appeared on tens of hundreds of machines. In other words, how many malware threats were lone attacks or widespread campaigns. To easily show the differences from quarter to quarter we've defined the following schema for this subsection:

- **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.

To be frank, there's not much difference from the quarter prior. The raw numbers and alert composition, which is a ratio of alerts to the sum of all alerts, are relatively the same. The only schema that increased were the threats detected and blocked on only one machine, which is also the schema that comprises almost all the alerts each quarter. This is because many malware campaigns use payloads that are ever-so-slightly different, which causes the hash to be different. On the other hand, all other threats existing on two or more machines slightly decreased from quarter to quarter. All in all, there's not much doing for this quarter.



	Alert Composition
1	88.99%
>= 2 & < 5	7.82%
>= 5 & < 10	1.81%
>= 10 & < 50	1.15%
>= 50 & < 100	0.13%
>=100	0.10%

Figure 27. Q1 2025 Alerts by Number of Machines Affected

Defense in Depth

The Defense in Depth subsection results differ drastically from the Alerts by Number of Machines Affected. First off, it highlights completely different perspectives. This subsection displays malware threats in terms of which EPDR technology blocked them, employing a de-facto defense-in-depth on endpoints combined with network-related protections provide several layers of protection. EPDR combines six major technologies to defend against malware:

Endpoint Technologies

- **Endpoint Detection** – As the typical 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.

Based on the differences from Q4, almost every technology has flipped in Q1. We previously observed most threats blocked via Cloud technology, followed by all the others except for Defined Rules. Now, in Q1, Behavioral/Machine Learning blocked the most malware, which makes sense considering we saw a surge in new malware threats this quarter. Old threats are quickly blocked by the first line of defense, AD360 Endpoint Detection, and Defined Rules, which are more static manners of blocking manner. These include previously seen malware hashes and easy-to-detect threats based on EPDR-embedded rules. These two technologies, AD360 Endpoint Detection and Defined Rules, only comprised around 20% of all blocks. Whereas Behavioral/Machine Learning thwarted 36.45% of all attacks.

Additionally, Manual Attestation continues to increase quarter-over-quarter and has risen to account for over 21% of malware blocks. Manual Attestation is the last line of defense on endpoints and is where suspicious files go to our attestation analysts to manually analyze files and make determinations about maliciousness. Logically, this means that more and more sophisticated files are observed on endpoints and need more granular inspection. Nevertheless, malware threats continue to be blocked by EPDR.

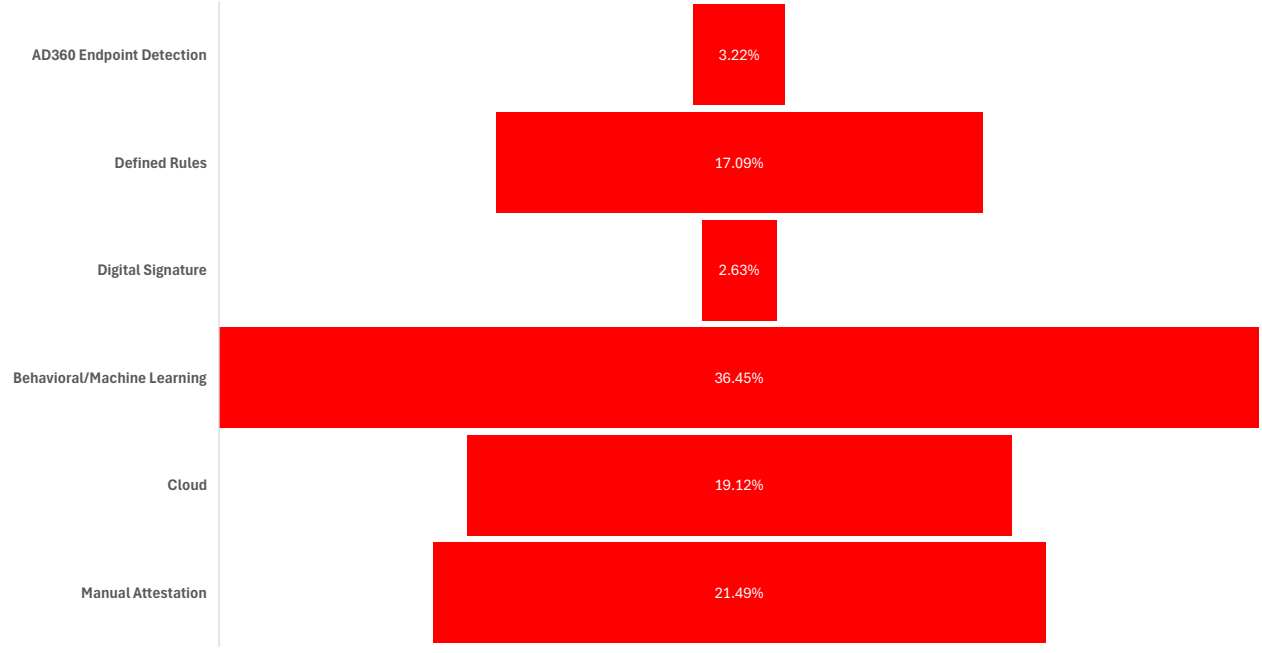


Figure 28. Q1 2025 Alerts by Number of Machines Affected

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.

You can review more about the definitions of each exploit on WatchGuard's Knowledge Base article located **here**.

Exploit	Description of Exploit	Q1 Alert Composition	Difference from Q4
RemoteAPCInjection	Remote code injection via APCs	39.48%	29.32%
RunPE	Process Hollowing Techniques	21.87%	16.62%
PsReflectiveLoader1	Files that leverage PowerShell to allocate and inject payloads directly within the memory of it's own process (E.g. Mimikats) (Local)	18.57%	-42.64%
WinlogonInjection	Remote Code Injection into winlogon. exe process	7.10%	4.36%
APC_Exec	Local code execution via APC	4.83%	3.01%
NetReflectiveLoader	Code execution on MEM_PRIVATE pages that do not correspond to a PE	4.04%	-5.49%
DumpLsass	LSASS Process Memory Dump	1.66%	0.83%
AmsiBypass	Techniques that bypass Windows' Antimalware Scan Interface (AMSI)	1.30%	0.76%
PsReflectiveLoader2	Files that leverage PowerShell to allocate and inject payloads directly within the memory of it's own process (E.g. Mimikats) (Remote)	0.35%	0.26%
ShellcodeBehavior	.NET files that allocate and inject payloads directly within the memory of it's own process (Assembly.Load)	0.30%	-7.05%
ROP1	Return Oriented Programming	0.23%	0.12%
ThreadHijacking	A process injection technique that allows the execution of arbitrary code in a separate process	0.12%	-0.13%
IE_GodMode	GodMode technique in Internet Explorer	0.09%	0.01%
HookBypass	Detection of memory allocation in base addresses; typical of heap spraying	0.02%	0.01%
ReflectiveLoader	Reflective executable loading (Metasploit, Cobalt Strike, etc.)	0.02%	0.00%
DynamicExec	Execution of code in pages without execution permissions (32 bits only)	0.01%	0.00%

Figure 29. Q1 2025 Alerts by Exploit Type

Alerts by Top 30 Countries Affected

We've shown the overall malware frequency observed and blocked on endpoints, followed by the number of machines affected by each malware sample, and the technologies and exploits responsible for each of these blocks. This subsection pivots geography and is most closely related to the Alerts by Number of Machines Affected subsection. That's because we define affected countries as a ratio of machines to infections. For example, if there is one EPDR-protected machine in a country and it has 50 different infections, they would have an Alert Coefficient (AC) of 50 (50/1). You can see the simple Alert Coefficient equation below.

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

In a surprise for this quarter, São Tomé and Príncipe, which didn't appear in the top 30 list at all last quarter, leapfrogged into the top affected country in terms of AC. Additionally, the top country last quarter, Laos, remained at the top, in second, even though there was a significant reduction in AC quarter-over-quarter. The other countries with significant reductions in AC were Morocco (still in third), China, and Armenia. Conversely, no other country had much of an increase in AC, which coincides with the overall malware frequency landscape, which saw a reduction from last quarter.

Even though this subsection highlights the countries that are most affected, the top 30 countries are better reflected by regions (i.e., which regions were affected the most). Aside from a few countries in the Caribbean, North America was largely unaffected (in terms of AC), and Europe appeared only a handful of times. Turkey, which appears on the list, is arguably both Asia and Europe and is seen as s gateway between both continents. The regions appearing most on the list were the oceanic region and eastern Asia, with Africa also having numerous countries appearing. This doesn't mean we observed more malware there, it just means that per machine, there was a high number of blocked attacks.

Country	Alert Coefficient	Order Difference from Q4
São Tomé and Príncipe	0.50	*NEW*
Laos	0.41	*-1*
Morocco	0.32	*-1*
Cuba	0.25	-
Zimbabwe	0.14	*+5*
China	0.11	*-1*
Angola	0.08	*+19*
Pakistan	0.07	*+1*
Bangladesh	0.06	*+2*
India	0.06	*-4*
Tajikistan	0.05	*+2*
Paraguay	0.05	*+16*
Nigeria	0.04	*+1*
Bolivia	0.04	*-6*
Turkey	0.04	
Armenia	0.04	*-13*
Panama	0.03	*NEW*
Dominican Republic	0.03	*+6*
Indonesia	0.03	*NEW*
Singapore	0.03	*-1*
Trinidad and Tobago	0.03	*-1*
Thailand	0.02	*+5*
Malaysia	0.02	*-2*
Botswana	0.02	*NEW*
Bulgaria	0.02	*NEW*
Venezuela	0.02	*NEW*
Kenya	0.02	*NEW*
Ghana	0.02	*+1*
Andorra	0.02	*-6*
Colombia	0.01	*NEW*

Figure 30. Q1 2025 Alerts by Country

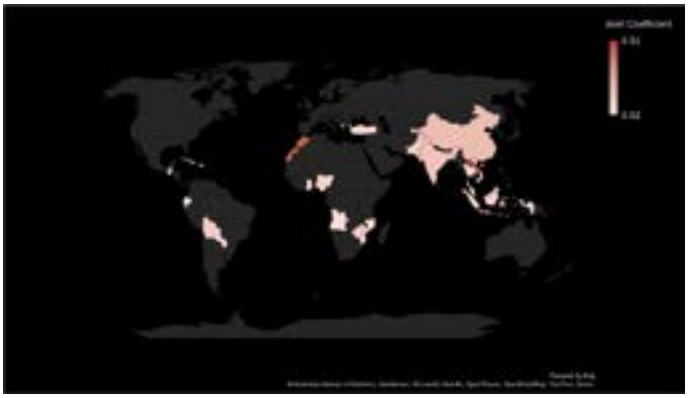


Figure 31. Q1 2025 Alerts by Top 30 Countries Affected

TOP MALWARE AND PUPS

The top malware and PUPs for each quarter reveal the top 10 most prevalent for each. However, for the most prevalent malware, we exempt test files such as EICAR because these aren't technically malware. Files such as EICAR are ways to test if an endpoint security solution is functioning properly. If the EICAR file is detected successfully, it means the solution is functioning properly, for the most part.

Top 10 Most Prevalent Malware

If you're a returning reader and remember last quarter, you'd remember that, for the first time since we've recorded this data, a ransomware sample and a coinminer sample both made the top 10 list. However, last quarter, there were three files in the top 10 related to the Black Basta ransomware group, which, as a spoiler for the ransomware subsection, had their chat logs leaked by an unknown entity. More on that later. In yet another surprise for this quarter, there was yet another ransomware sample in the most prevalent malware this quarter. This time, it was a Termite ransomware payload. Termite is a group that appeared last quarter and hasn't made too much noise in terms of victims and news-worthy anecdotes, but a sample of its encryptor is the second-most prevalent malware for this quarter.

Additionally, there are two cryptominer-related files in the top 10 for this quarter, both coming from the same campaign. Researchers from Red Canary published research about a campaign and threat actor they dubbed Tangerine Turkey, which used USB flash drives to deliver a VBScript worm, ultimately delivering a cryptominer for the Zephyr cryptocurrency (ZEPH). We've included more information on that and the others in the top 10 below.

MD5	Signature	Alerts	Classification Attestation
5E3E47FBBC5218B4EB44F6272CCEB0D0	Trj/CI.A	300	Dumpert (LSASS dumper)
B140A1175BF560690AD36940B09EBD03	Trj/GdSda.A	99	Termite Ransomware
7D9542EF7C46ED5E80C23153DD5319F2*	W32/Conficker.C.worm	93	Conficker Worm
EBDA2CC87E6B5D137B4D0454EDDE70CC	Trj/Chgt.AD	93	Zephyr Miner/Tangerine Turkey
21D807EB0A57414799474D99BAAEBD47	Trj/Genetic.gen	88	Unknown Malware
E2A2521CB16DA1BED01565C503772125	W32/Conficker.C.worm	73	Conficker Worm
2B313CEEA938698985ABF3CB5DAA8D7E	Trj/CI.A	64	Unknown Dropper
32478E26A0E8A1B592C11F0BF9A3F396	Trj/RnkBend.A	62	Zephyr Miner/Tangerine Turkey
157FBD8E2EC496FF6FA66C17974C9E30	Trj/RnkBend.A	59	GuLoader (Dropping Snake Keylogger)
A0B8569F8ED559D7BE637C1125D5AB6F	Trj/Agent.AY	59	Unknown Malware (Enigma Protector)

Figure 32. Q1 2025 Top 10 Most Prevalent Malware

**Appeared in previous quarter*

Malware Descriptions

Dumpert
BODY Dumpert is an LSASS memory dumper tool using direct system calls and API unhooking. LSASS is Windows' security policy enforcement mechanism for things such as logging onto systems, handling passwords, and creating access tokens. Considering LSASS handles sensitive information on a machine, attackers leverage this to get access to system components by bypassing user mode and performing direct kernel mode instructions. Dumpert is a hacking tool that simplifies this process, more easily facilitating LSASS memory dumping.

Termite
Termite is a ransomware group that we first observed in November 2024. By all public accounts, it is the modern run-of-the-mill ransomware group that exfiltrates data, encrypt systems, and attempts to extort victims by publishing data on its dark web data leak site (DLS). As of Q1 2025, the group has posted 18 victims to its DLS. The group's targets primarily reside in Europe and the United States but also have one victim in Australia and Oman. Research shows that the group uses a modified encryptor from Babuk.

Read more about Termite on the **Ransomware Tracker:**

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).

Zephyr Miner/Tangerine Turkey
A Zephyr Miner is a legitimate tool used to mine Zephyr Protocol (ZEPH) cryptocurrency. However, there is a threat actor dubbed Tangerine Turkey that is leveraging the Zephyr Miner to mine ZEPH on victim machines. This campaign delivers a VBScript worm from a USB thumb drive that eventually drops a cryptomining payload that mines ZEPH.

Unknown Malware
An "unknown malware" is one we can't attribute to a specific malware family, but we can at least generically identify it as a malware tool.

Unknown Dropper
An "unknown malware" is one we can't attribute to a specific malware family, but we can at least generically identify it as a malware. Droppers are malware that "drop" additional malware as part of a daisy chain of infections.

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

Top 10 Most-Prevalent PUPs

Potentially unwanted programs (PUPs), which are sometimes referred to as potentially unwanted applications (PUAs), are explicitly not malware, but implicitly not goodware. They lie somewhere in between, and the programs designated as PUPs differ from each endpoint antivirus vendor. Again, PUPs are specifically not malware, else they would be labelled as such. However, these programs often perform unwanted actions relative to the user, hence the name. The most common PUPs are adware, or software that serves unwanted advertisements; bundle installers, which are installers bundled with additional and most likely unwanted software; and keygens, which are software that produce keys that often are used to bypass legitimate paid licensing. The table below shows the top 10 most prevalent PUPs for this quarter along with some additional information about their signatures.

MD5	Signature	Alerts	Classification Attestation
0DC8874DA66480B329F42292768CEA53	PUP/EpiBrowser	5,221	EpiBrowser Installer
38DE5B216C33833AF710E88F7F64FC98	HackingTool/ AutoKMS	1,967	KMSPico
DA64D2346B80015FF9621F725843B6A6	PUP/EpiBrowser	756	EpiBrowser
F7191FE14D2F5E7C4939C2FCA5F828C2*	PUP/Generic	713	RVEraser
2914300A6E0CDF7ED242505958AC0BB5*	HackingTool/ AutoKMS	694	KMS_VL_ALL_AIO
6D7FDBF9CEAC51A76750FD38CF801F30	HackingTool/ AutoKMS	605	KMSPico
BDD5FF92AB3B6F6271FEA6B0BA94F862	PUP/OneStart	587	OneStart AI Browser
FC3B93E042DE5FA569A8379D46BCE506*	PUP/Hacktool	531	Mail PassView
3D9D2A24671C63F167E1E42B1A86E6E3	PUP/Softonic	519	Softonic
BCA43E19E7013331D99FF788EA6B42A0	HackingTool/ AutoKMS	463	MS Office 2010 KeyGen

Figure 33. Q1 2025 Top 10 Most Prevalent PUPs
**Appeared in previous quarter*

PUP Signature Descriptions

PUP/EpiBrowser
EpiBrowser is most referred to as EpiStart, and it's an open-source Chromium-based web browser. It's considered a PUP because it contains redirects to a fraudulent search engine, which most people call browser hijackers. However, EpiBrowser is a web browser itself.

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/Generic
This is 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/OneStart
OneStart is an open-source Chromium-based web browser that claims to be an artificial intelligence (AI) assisted browser. The installer also contains software that installs a browser toolbar, which also makes this a bundle installer, also a PUP (PUP/Bundle-Installer). OneStart also contains unwanted redirects to third-party search engines.

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/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.

ATTACK VECTORS

"Attack Vectors" is a fancy way of defining the methods attackers use to infiltrate endpoints. It's more abstract than Attacks by Exploit Type and the MITRE ATT&CK matrix tactics and techniques. Attack vectors are more categorical than specific. For example, one of the attack vectors is Scripts. PowerShell, Bash, AutoIT, and even Python are scripting languages. Attackers often use PowerShell to infiltrate a system, gather information, and exfiltrate data. If applicable, the powershell.exe process is blocked and throws an alert. This doesn't define what the PowerShell script did (i.e., what exploits or mechanisms they tried to use.) It only defines the attack vector they used. That is what the Attack Vectors explains, and our defined attack vectors are below.

Attack Vector Descriptions

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

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

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 processes 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

There are nine defined attack vectors that we track. Of the nine, Scripts are the most observed attack vector. It's always the most observed, in some quarters reaching above 90% of all attack vector detections. This quarter is a bit different. Only 36.11% of all attack vectors were from scripts as opposed to almost 83% last quarter, a significant decrease. Microsoft 365 applications were the only other attack vector to decrease. On the other hand, the Other and Windows categories saw the highest increase from quarter to quarter. All the other attack vectors saw slight increases.

Attack Vector	Q4 Alert Comp.	Q1 Alert Comp.	Difference From Q4
Acrobat	0.76%	3.13%	2.37%
Browsers	4.36%	11.51%	7.15%
Coding Software	0.08%	0.40%	0.32%
Database Software	0.11%	0.14%	0.02%
Microsoft 365	2.92%	1.61%	-1.31%
Other	4.14%	23.45%	19.30%
Remote Access Software	1.10%	1.48%	0.39%
Scripts	82.94%	36.11%	-46.82%
Windows	4.03%	22.16%	18.13%

Figure 34. Q1 2025 Attack Vectors

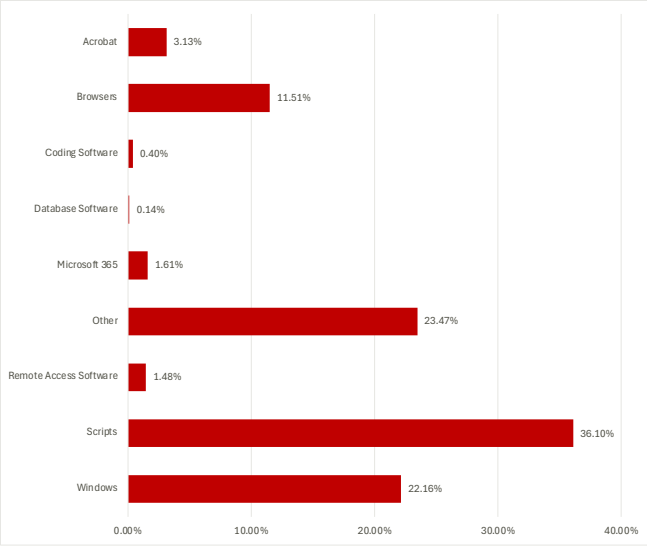


Figure 35. Q1 2025 Attack Vectors

Browser Attack Vectors

Almost every quarter, we see the big-name web browsers that almost everyone uses: Google Chrome, Mozilla Firefox, and Window's built-in browsers, Internet Explorer and Edge. As cryptocurrency adoption increases, we see more and more Brave browser detections, which is a Chromium-based browser that has embedded privacy and cryptocurrency integrations. For the first time ever, we've seen detections from Waterfox and Wave. Waterfox is a privacy-focused browser based on Mozilla Firefox, and Wave is a web browser that claims to make life simpler and more productive.

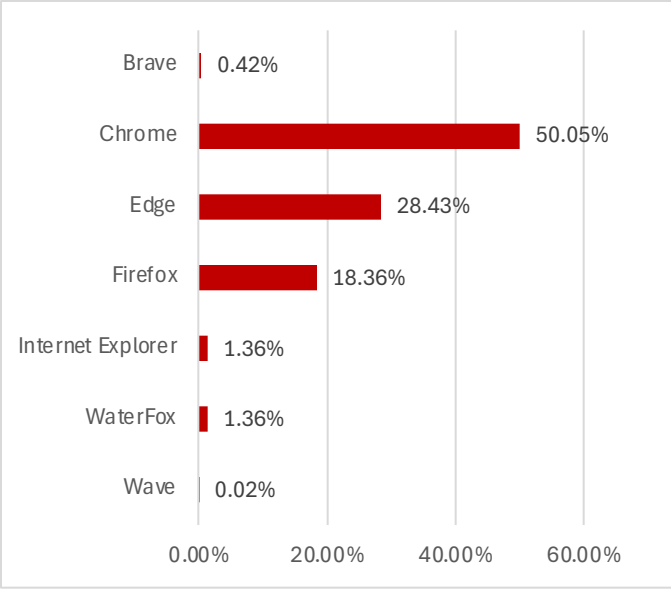


Figure 36. Q1 2025 Browser Detections

Coding Software Attack Vectors

We began tracking coding software attack vectors a quarter ago. So, we have little historical context to work from, but both times there have been only three major coding software (excluding Python, which we put under Scripts). Two JavaScript libraries, NodeJS and ElectronJS, and then Java. Based on the numbers, this could easily be called the Java(Script) attack vector, but we never know what the future brings. We anticipate other languages to appear in the future such as Rust.

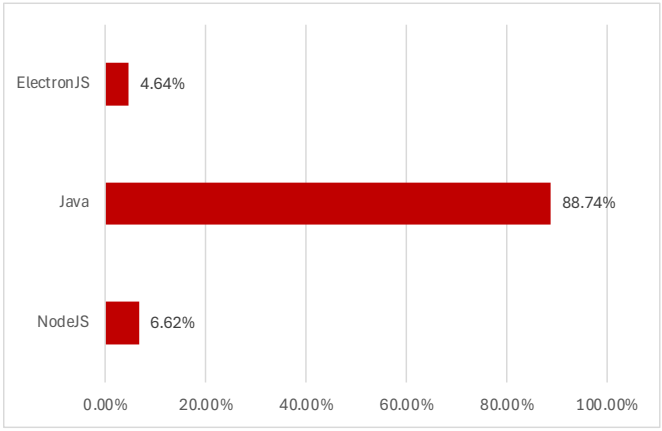


Figure 37. Q1 2025 Coding Software Detections

Database Software Attack Vectors

Database software is synonymous with Structured Query Language (SQL). Most databases on Earth use SQL, or some form of it. There has been an emergence of an increase in NoSQL languages, predominately MongoDB. Yet, there were no MongoDB attack vector detections this quarter, or last for that matter. Access, PostgreSQL, and SQL Server are all different database software to manage SQL-based servers. Similarly, these three attack vectors all have similar numbers of detections for this quarter, as shown in the graph.

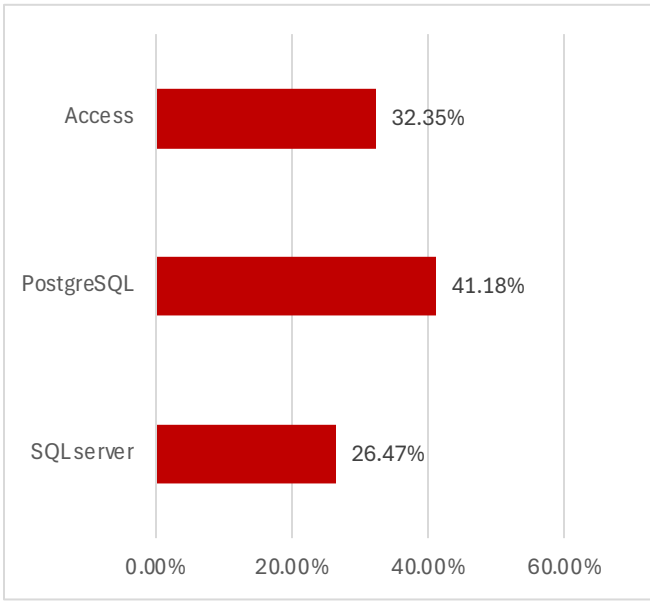


Figure 38. Q1 2025 Database Detections

Microsoft 365 Attack Vectors

Last quarter, when we added a few attack vectors and made some other changes to this subsection, we made a change to what was previously called the Microsoft Office attack vector and is now called Microsoft 365. The difference is due to changes with Microsoft as they have expanded their Office suite of products and now call it Microsoft 365. We included a hyperlink in Attack Vectors Descriptions a few paragraphs prior.

Since Microsoft 365 includes a smorgasbord of applications, there's a lot of helper files and sub-applications that don't particularly fit into one single application. For example, there are several DLLs that facilitate Office and others. That is why Office Misc. is the most observed attack vector here. Surprisingly, OneNote is the second most observed, followed by Microsoft Word. We also include Microsoft Access here because it's both Microsoft 365 and database software. However, for summation purposes, we include Access in the database software attack vector.

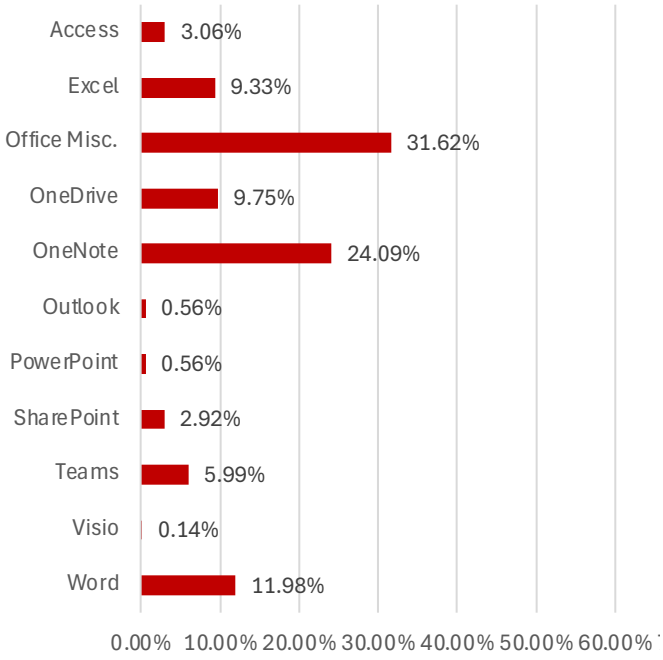


Figure 39. Q1 2025 Microsoft 365 Detections

Remote Access Attack Vectors

Remote Access tools are commonly used by attackers by leveraging Remote Access Tools (RATs) or ransomware. RATs using remote access tools is a given, but these are proprietary tools created by the RATs themselves. Hence the name. Ransomware operators and other actors performing social engineering attacks, for example, utilize well-established remote access software such as LogMeIn, Radmin, TeamViewer, and others. This allows them to control or deliver payloads without having to use malicious RATs that are sometimes blocked by endpoints. Legitimate, non-cracked remote access tools are usually not blocked by endpoint solutions and allow unfettered access to endpoints and sensitive systems. This quarter's remote access attack vector detections are shown in the bar graph.

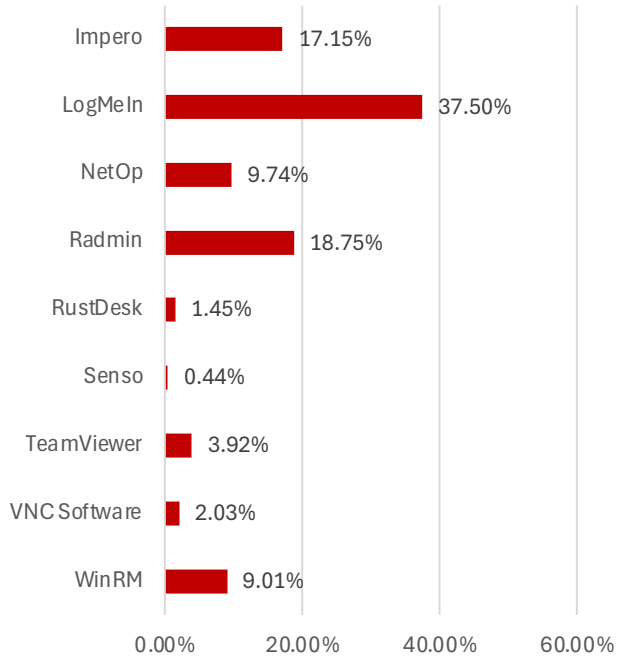


Figure 40. Q1 2025 Remote Access Detections

Script Attack Vectors

As we previously hinted on, the Script attack vectors are the most observed every quarter. Often, it significantly leads the way. However, this quarter saw scripts comprised a little over a third of all detections. Zooming into these detections, we see that it's spearheaded by PowerShell (of course), and then Visual Basic scripts. If you remember, Tangerine Turkey used VBScripts to drop a cryptominer. This is just one example though. The other notable scripting languages with detections were Python and AutoIT, which we also touched on in the Top 10 Most Prevalent Malware subsection.

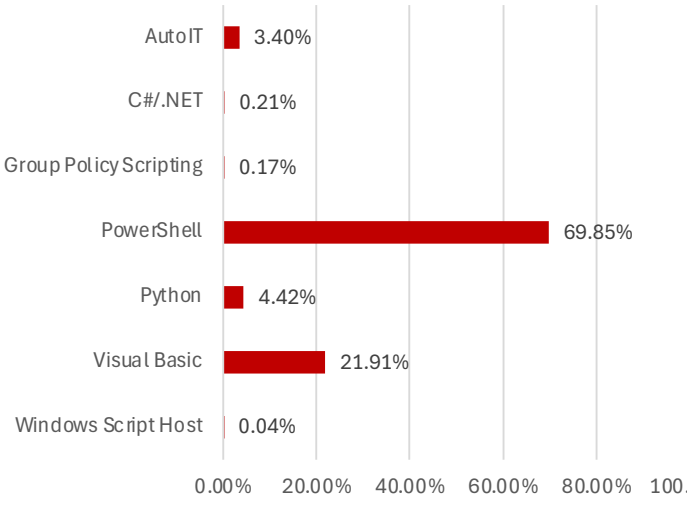


Figure 41. Q1 2025 Script Detections

Windows (LOLBAS) Attack Vectors

The final attack vector we take a magnifying glass to is the Windows section. However, we don't cover all processes within the Windows attack vector. We highlight living-off-the-land binaries (LOLBAS), which is a sub-attack vector of Windows. All LOLBAS processes are Windows attack vectors, but not all Windows attack vectors are LOLBAS. LOLBAS are those that are commonly leveraged by attackers to facilitate further attacks. They are "living off the land" in a sense.

There are a handful of LOLBAS that comprise the most detections: Cmd.exe, the Command Prompt; EXPLORER.EXE, Windows Explorer; msedge.exe, which is Microsoft Edge, also a browser; schtasks.exe, the Task Scheduler; and vbc.exe, which is the Visual Basic Compiler, a script attack vector. All the others are relatively miniscule in terms of alert composition.

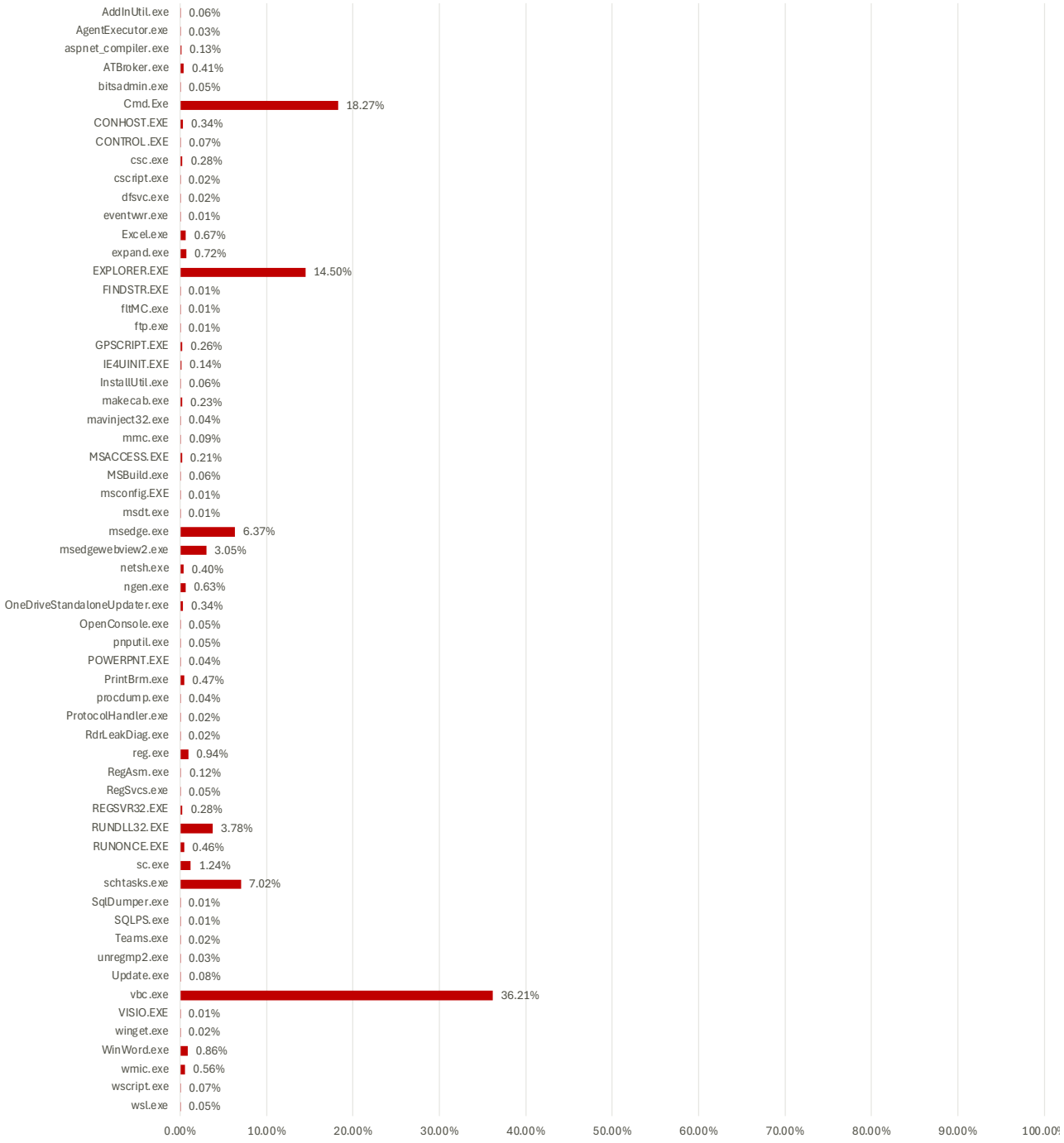


Figure 42. Q1 2025 Windows (LOLBAS) Detections

Cryptominer Detections

There were a few quarters where we omitted cryptominer detections because the detections were significantly low. This is likely due to crypto-miners being labeled as information stealers or password stealers. Often, malware that steals information also steals cryptocurrency wallets and drops a cryptominer, and vice versa. Cryptominers are legitimate programs used to mine cryptocurrency, but they can also be used maliciously to mine crytocurrency using an unknowing victim's computer on behalf of the attacker. In other words, someone is mining crypto on a victim machine and sending it to a wallet under their control.

Recently, we've returned to including these detections as the number of alerts has gone up and cryptocurrency becomes more adopted, which in turn usually means more detections. They're correlated. Last quarter we observed a relatively large number of cryptominer alerts because there existed cryptominers in the most prevalent malware. Additionally, this quarter we observed Tangerine Turkey, which landed on the top 10 malware twice. However, the number of detections from Q4 2024 to Q1 2025 decreased 28.30%.

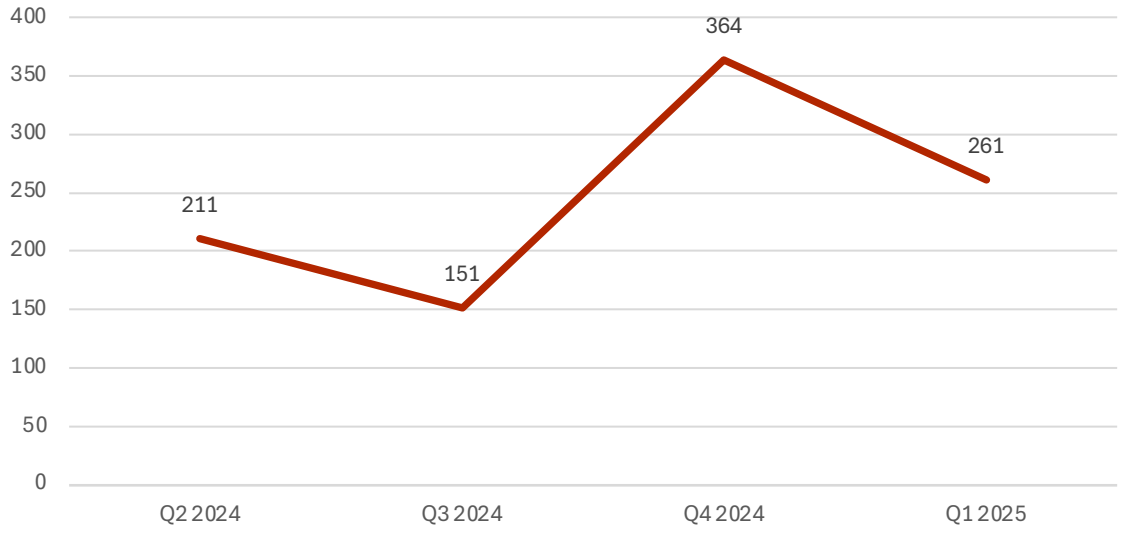


Figure 43. QoQ Cryptominer Detections

Threat Hunting

All the subsections within the Endpoint section of the report are reactive countermeasures that block threats and log telemetry. However, threat hunting is a more proactive countermeasure (sometimes reactive) that seeks suspicious actions on endpoints and roots them out before they cause damage. However, threat hunting can also be reactive and attempt to analyze attacks in their early stages.

We leverage this MITRE ATT&CK Enterprise Matrix for defining and detecting tactics and techniques from attackers. This matrix uses real-world attacks to define adversary methodologies in an easy-to-digest knowledge base. Organizations can then use this normalized database to create threat models and implement countermeasures directed towards certain behaviors.

You can read more about the MITRE ATT&CK Enterprise Matrix **here**.

As a refresher, the tactics and technique data points for the Threat Hunting subsection are:

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.

Utilizing the MITRE ATT&CK Matrix, we filtered our threat hunting data to showcase the top 10 most-used techniques for each quarter. In the following table, we combine the top techniques into their respective tactics, which is the left-most column. For brevity, we also include the definition of each tactic, techniques, and sub-technique to prevent you from having to reference the matrix. The right two columns show the technique count and then their respective rank within the top 10.

The most detected technique for this quarter was TA0007-0, which is the generic technique for discovery-related behaviors. Discovery behaviors are those that include scans and enumeration tools for finding out network, server, and endpoint information. The next technique is the execution of PowerShell scripts, which we discuss at length in the Attack Vectors section almost every quarter. The most observed tactic for this quarter was TA0005, which are various forms of Defense Evasion techniques. This includes mass file deletion, abusing Regsvcs and Regasm proxy code execution, and installing root certificates.

MITRE Tactic	MITRE Technique	Tactic :: Technique :: Sub-Technique	Technique Count	Rank
TA0002	TA0002	Execution	1,727,371	8
	T1059.001	Execution :: Command and Scripting Interpreter :: PowerShell	5,811,891	2
TA0003	TA0003	Persistence	3,149,604	4
TA0005	TA0005	Persistence :: Create or Modify System Process :: Container Service	2,248,572	9
	TA0004	Privilege Escalation	1,290,167	7
	TA0005	Defense Evasion	2,360,748	3
	T1218.009	Defense Evasion :: System Binary Proxy Execution :: Rundll32	1,253,587	10
TA0007	TA0007	Discovery	7,764,462	1
TA0011	TA0011	Command and Control	2,704,339	6
TA0040	T1561.001	Impact :: Disk Wipe :: Disk Content Wipe	3,476,147	5

Figure 44. Q1 2025 Exploits by MITRE ATT&CK® Tactic

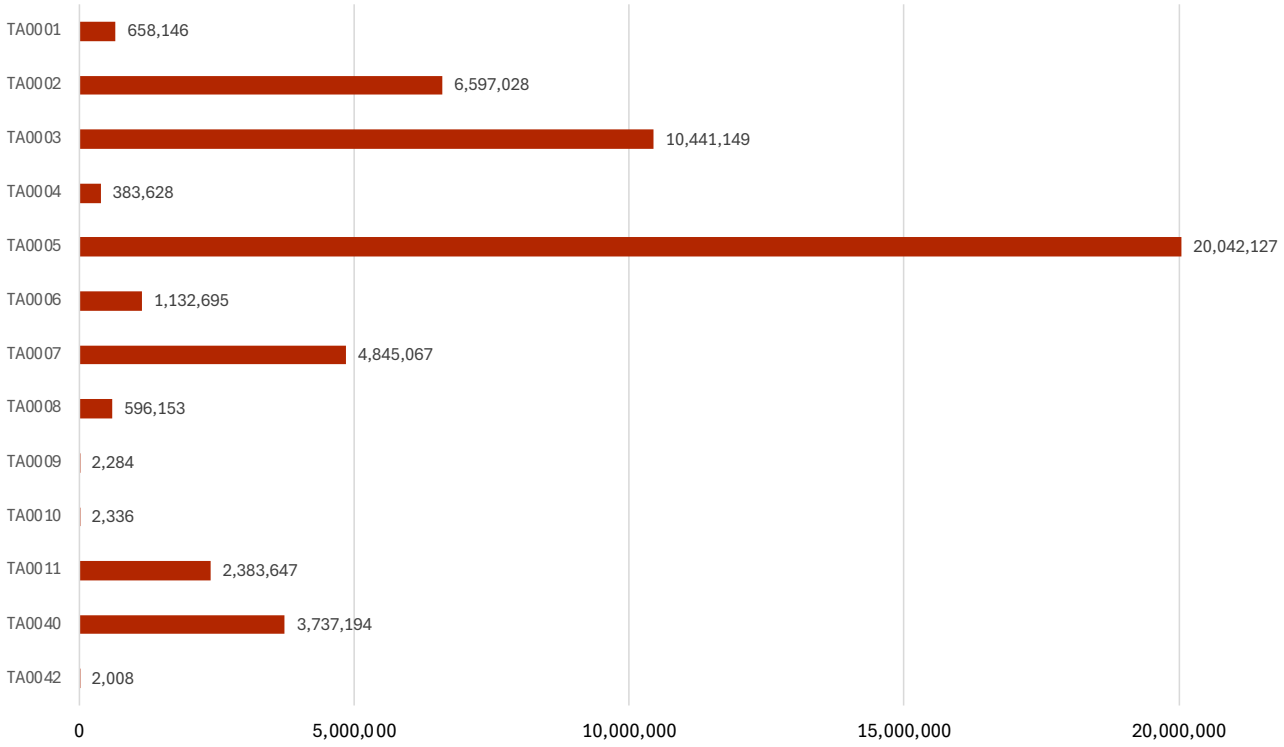


Figure 45. Q1 2025 Exploits by MITRE ATT&CK® Tactic

In terms of raw numbers, the differences from quarter to quarter were quite eventful. In Q1, there were two tactics that saw more than two times the alerts from the quarter prior – TA0005 (Defense Evasion) and TA0009 (Collection). Additionally, TA0003 (Persistence) and TA0010 (Exfiltration) also saw modest increases. On the other hand, TA0002 (Execution), TA0004 (Privilege Escalation), TA0006 (Credential Access), and TA0007 (Discovery) significantly receded from Q4 2024. As for the others, they were a mixed bag, and you can see them in the Exploits by MITRE ATT&CK® Tactic table.

MITRE Tactic	Q4 Tactic Sum	Q1 Tactic Sum	Difference	% Difference
TA0001	682,590	658,146	-24,444	-3.58%
TA0002	8,341,240	6,597,028	-1,744,212	-20.91%
TA0003	6,901,091	10,441,149	+3,540,058	51.30%
TA0004	1,419,983	383,628	-1,036,355	-72.98%
TA0005	9,758,049	20,042,127	+10,284,078	105.39%
TA0006	1,985,016	1,132,695	-852,321	-42.94%
TA0007	7,764,503	4,845,067	-2,919,436	-37.60%
TA0008	508,693	596,153	+87,460	17.19%
TA0009	888	2,284	+1,396	157.21%
TA0010	1,682	2,336	+654	38.88%
TA0011	2,705,272	2,383,647	-321,625	-11.89%
TA0040	3,565,800	3,737,194	+171,394	4.81%
TA0042	1,701	2,008	+307	18.05%

Figure 46. Q1 2025 Exploits by MITRE ATT&CK® Tactic

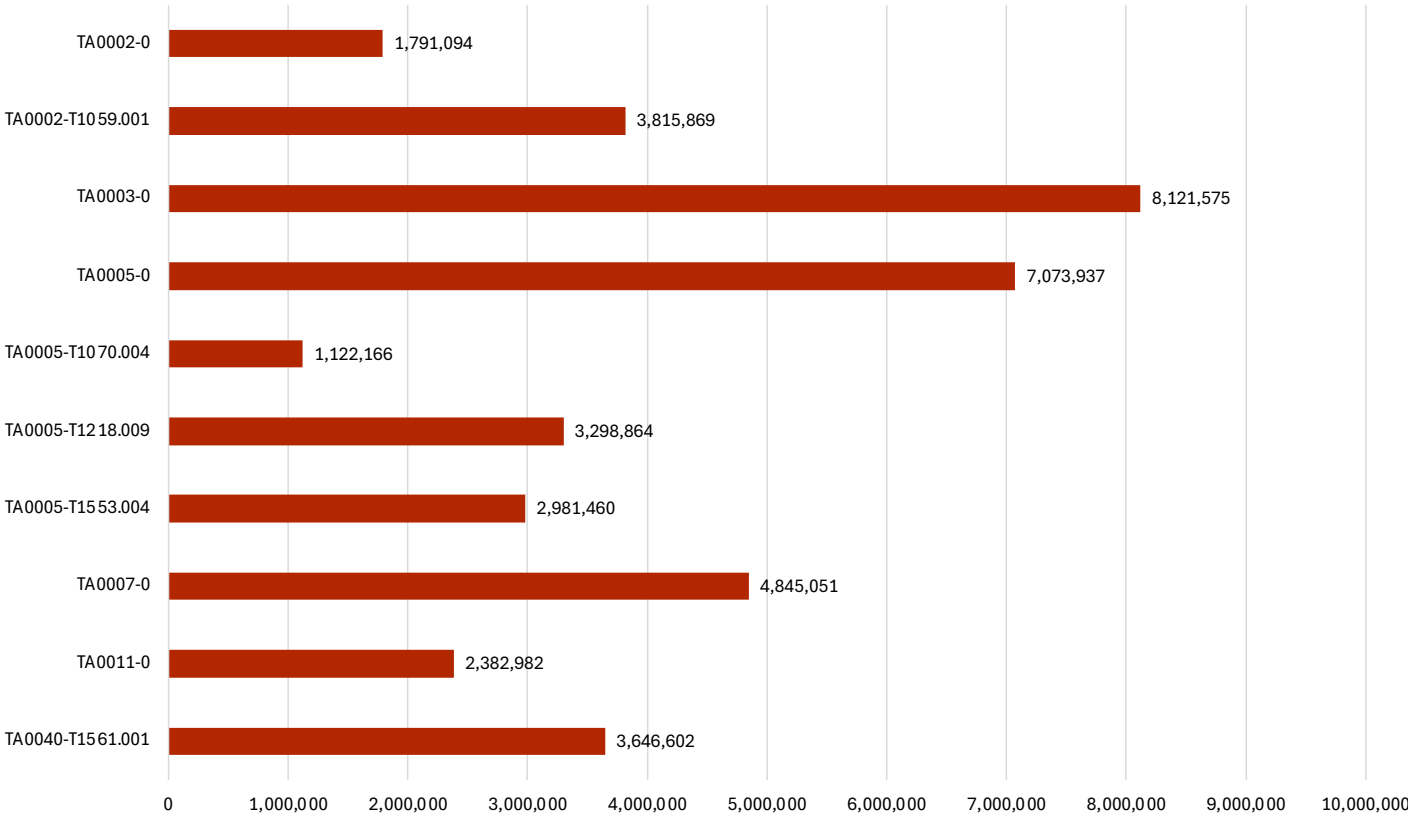


Figure 47. Q1 2025 Exploits by MITRE ATT&CK® Tactic

As for the techniques within the tactics, there was a significant increase in TA0005-0 (Defense Evasion) tactics and TA0003-0 (Persistence) tactics. Contrarily, TA0002-T1059.001 (Command and Scripting Interpreter: PowerShell) and TA0007-0 (Discovery) reduced from quarter to quarter. This coincides with our Attack Vector data that showed a decrease in PowerShell-related detections. Finally, there were three techniques not observed last quarter that were in the top 10. As such, they receive a N/A designation; we have no historical data to work with.

Top Threat Hunting Rule Invocations

The last threat hunting subsection leveraged the MITRE ATT&CK Enterprise Matrix to define, alert, and log behaviors. However, this subsection is more proprietary to EPDR, and these overlap with the previous tactics and techniques, although, they are more internally defined. These aren't based on a normalized matrix, but the threat hunting rule names are intuitive. For example, the top threat hunting rule invocation for this quarter was TrustControlEvasionRule, which is a rule that alerts behaviors that attempt to evade trust controls. The other new one to the list was DeleteSystemLogsRule, which, as you can guess, is a rule that defines behaviors for deleting system logs. The other threat hunting rules are all returning rules from last quarter and their differences from Q4 are in the table.

MITRE Tactic	MITRE Technique	Q4 Technique Sum	Q1 Technique Sum	Difference	% Difference
TA0002	TA0002-0	1,727,371	1,791,094	+63,723	3.69%
	T1059.001	5,811,891	3,815,869	-1,996,022	-34.34%
TA0003	TA0003-0	3,149,604	8,121,575	+4,971,971	157.86%
TA0005	TA0005-0	2,248,572	7,073,937	+4,825,365	214.60%
	T1070.004	-	1,122,166	N/A	N/A
	T1218.009	-	3,298,864	N/A	N/A
	T1553.004	-	2,981,460	N/A	N/A
TA0007	TA0007-0	7,764,462	4,845,051	-2,919,411	-37.60%
TA0011	TA0011-0	2,704,339	2,382,982	-321,357	-11.88%
TA0040	TA0040-T1561.001	3,476,147	3,646,602	+170,455	4.90%

Figure 48. Q1 2025 Exploits by MITRE ATT&CK® Technique

RANSOMWARE LANDSCAPE

Cryptominers are a type of malware that we both dedicated a section to and landed on the top 10 malware list. Ransomware is also a malware that fits both criteria. Last quarter, we observed three Black Basta-related files on the top 10 malware list. This quarter, there was only one, and it was an encryptor payload from the Termite ransomware group, which was first observed last quarter, in November. Therefore, last quarter, it was no surprise that the EPDR ransomware detections skyrocketed. Coinciding with the overall malware frequency decreasing this quarter, as did the ransomware detections, and by a lot. Even though there was a ransomware detection on the top 10 list, the number of ransomware detections are akin to the numbers from quarters prior, as can be seen in the line graph, showing a decrease of 84.91%.

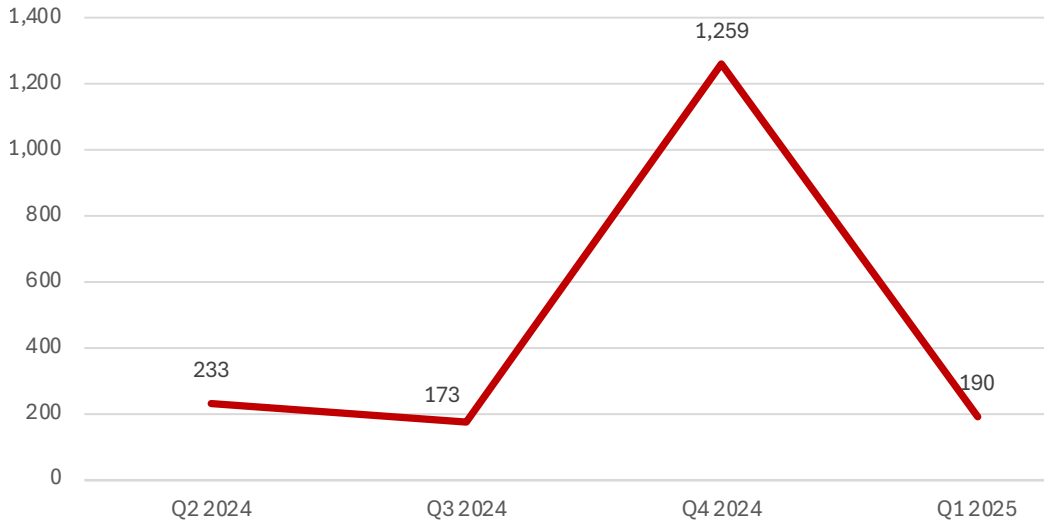


Figure 49. QoQ Ransomware Detections by Quarter

Extortion Groups

Extortions Groups differ from the WatchGuard ransomware detections. The prior ransomware detections only cover ransomware samples detected and blocked by EPDR. Extortion Groups are counters for publicly announced victims by ransomware groups, primarily on their data leak sites and on social media. This means that these numbers are alleged victims, even though some of them were confirmed in media reports or by companies themselves. Nevertheless, the number of extortions has increased for several consecutive quarters now. For the first time, the number of public extortions has surpassed 2000, increasing to 2,107. This is an increase of 13.10%.

This increase coincides with a whopping 17 new ransomware groups discovered in the quarter and is mainly attributed to Cl0p's throng of victims resulting from the Cleo MFT zero-day exploit discussed last quarter.

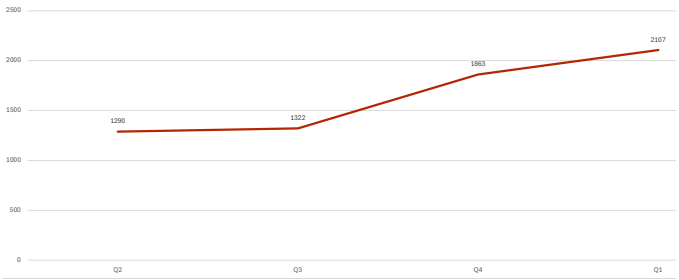


Figure 50. QoQ Public Extortions by Group

New Groups	Inactive Groups
Arkana Security	0mega
Belsen Group	8base
Bjorkanism	Argonauts Group
CHAOS	Belsen Group
Crazyhunter	Bl00dy
Frag	Black Basta
GD LockerSec	Bluebox 1.0
J Group	Cactus
Kraken	Chort
Linkc	Crazyhunter
NightSpire	FOG
OX Thief	FunkSec
RALord	GD LockerSec
Run Some Wares	GD LockerSec
SECP0	Helldown
VanHelsing	Linkc
OX Thief	Malek Team
	Meow Leaks
	OX Thief
	Pryx

Figure 51. Q1 2025 Newly Active and Inactive Ransomware Groups

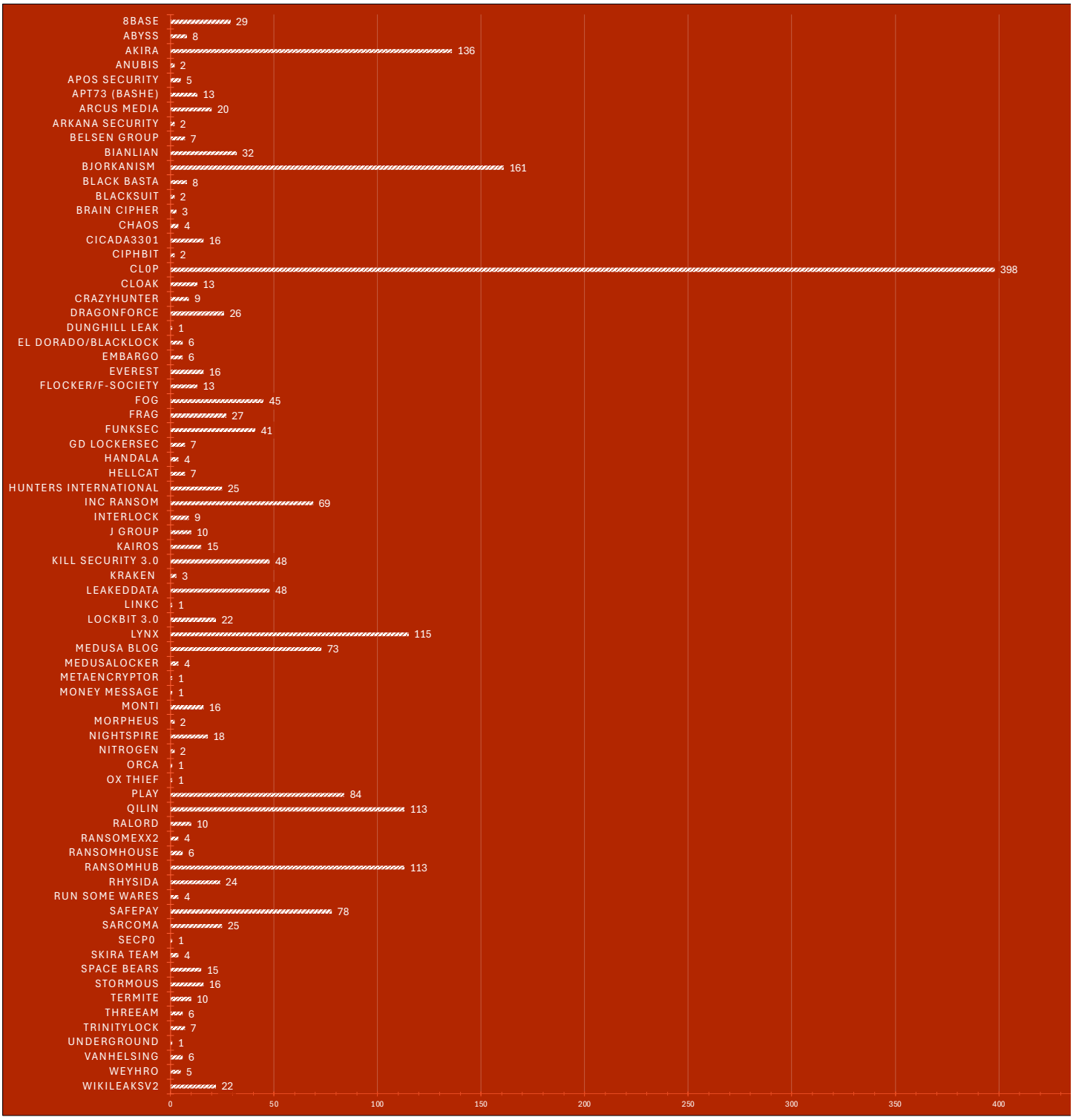


Figure 52. Q1 2025 Public Extortions by Group

Name	Q3	Q4	Difference
8base	11	29	+18
Abyss	9	8	-1
Akira	138	136	-2
Anubis	4	2	-2
Apos Security	0	5	+5
APT73 (Bashe)	50	13	-37
Arcus Media	22	20	-2
Argonauts Group	11	0	-11
Arkana Security	-	2	NEW
Belsen Group	-	7	NEW
BianLian	33	32	-1
Bjorkanism	-	161	NEW
Bl00dy	2	0	-2
Black Basta	36	8	-28
BlackSuit	42	2	-40
Bluebox 1.0	3	0	-3
Brain Cipher	13	3	-10
Cactus	29	0	-29
CHAOS	-	4	NEW
Chort	7	0	-7
Cicada3301	11	16	+5
CiphBit	4	2	-2
CL0P	7	398	+391
Cloak	28	13	-15
Crazyhunter	-	9	NEW
CyberVolk	12	0	-12
DAIXIN	2	0	-2
DarkVault	6	0	-6
Dispossessor	4	0	-4
Donut Leaks	4	0	-4
DragonForce	19	26	+7
DungHill Leak	0	1	+1
El Dorado/Black-Lock	56	6	-50
EMBARGO	6	6	0
Everest	27	16	-11
EvilMorocco	15	0	-15
Flocker/F-SOCI-ETY	7	13	+6
FOG	67	45	-22
Frag	-	27	NEW
FunkSec	84	41	-43
GD LockerSec	-	7	NEW
Handala	14	4	-10
Head Mare	6	0	-6
HELLCAT	7	7	0
Helldown	12	0	-12
Hunters Interna-tional	62	25	-37
INC Ransom	37	69	+32
INTERLOCK	13	9	-4
J Group	-	10	NEW
Kairos	14	15	+1
Kill Security	23	0	-23
Kill Security 3.0	86	48	-38
Kraken	-	3	NEW
LEAKEDDATA	34	48	+14
Linkc	-	1	NEW
LockBit 3.0	12	22	+10
Lynx	52	115	+63
MADDLL32	1	0	-1
Medusa Blog	50	73	+23
MedusaLocker	0	4	+4
Meow Leaks	40	0	-40
Metaencryptor	0	1	+1
Money Message	3	1	-2
Monti	8	16	+8
Morpheus	2	2	0
NightSpire	-	18	NEW
Nitrogen	19	2	-17
Orca	1	1	0
OX Thief	-	1	NEW
Play	95	84	-11
PlayBoy	1	0	-1
Qilin	55	113	+58
RA Group	30	0	-30
RALord	-	10	NEW
RansomExx2	0	4	+4
RansomHouse	8	6	-2
RansomHub	245	113	-132
Rhysida	18	24	+6
Run Some Wares	-	4	NEW
SafePay	46	78	+32
Sarcoma	36	25	-11
SECP0	-	1	NEW
SKIRA TEAM	1	4	+3
Space Bears	10	15	+5
Stormous	8	16	+8
Termite	9	10	+1
ThreeAM	11	6	-5

TrinityLock	2	7	+5
Underground	2	1	-1
VanHelsing	-	6	NEW
Weyhro	1	5	+4
WikiLeaksV2	20	22	+2

Figure 53. Q4-Q1 2025 Ransomware Extortion Differences

Name		Name	
CL0P	391	Abyss	-1
Lynx	63	BianLian	-1
Qilin	58	MADDLL32	-1
INC Ransom	32	PlayBoy	-1
SafePay	32	Underground	-1
Medusa Blog	23	Akira	-2
8base	18	Anubis	-2
LEAKEDDATA	14	Arcus Media	-2
LockBit 3.0	10	Bl00dy	-2
Monti	8	CiphBit	-2
Stormous	8	DAIXIN	-2
DragonForce	7	Money Message	-2
Flocker/F-SOCIETY	6	RansomHouse	-2
Rhysida	6	Bluebox 1.0	-3
Apos Security	5	Dispossessor	-4
Cicada3301	5	Donut Leaks	-4
Space Bears	5	INTERLOCK	-4
TrinityLock	5	ThreeAM	-5
MedusaLocker	4	DarkVault	-6
RansomExx2	4	Head Mare	-6
Weyhro	4	Chort	-7
SKIRA TEAM	3	Brain Cipher	-10
WikiLeaksV2	2	Handala	-10
DungHill Leak	1	Argonauts Group	-11
Kairos	1	Everest	-11
Metaencryptor	1	Play	-11
Termite	1	Sarcoma	-11
EMBARGO	0	CyberVolk	-12
HELLCAT	0	Helldown	-12
Morpheus	0	Cloak	-15
Orca	0	EvilMorocco	-15
		Nitrogen	-17
		FOG	-22
		Kill Security	-23
		Black Basta	-28
		Cactus	-29
		RA Group	-30
		APT73 (Bashe)	-37
		Hunters International	-37
		Kill Security 3.0	-38
		BlackSuit	-40
		Meow Leaks	-40
		FunkSec	-43
		El Dorado/BlackLock	-50
		RansomHub	-132

Figure 54. 2025 QoQ Public Extortions by Group Summation

Ransomware Groups

Law Enforcement Actions

8 Base – In February, Europol and federal law enforcement agencies from 14 different countries across the globe conducted a takedown of the 8base/Phobos ransomware group that has been ongoing for years. The operation, dubbed Phobos Aetor, saw 27 servers linked to the group taken down and the arrest of four Russian nationals, two women and two men, in Phuket, Thailand. These actions follow previous law enforcement actions against the group in 2023, arresting a Phobos affiliate in Italy, and 2024, where a Phobos administrator was extradited to the United States from South Korea. However, Phobos Aetor seems to be the killing blow to the group's operation as all the known infrastructure has been seized and there have since been no subsequent actions from the group. It appears 8base is no more.

https://www.europol.europa.eu/media-press/newsroom/news/key-figures-behind-phobos-and-8base-ransomware-arrested-in-international-cybercrime-crackdown

LockBit – LockBit, which has, in recent months, had their operations curtailed by prior law enforcement actions, has had yet another setback in Q1 2025. The United States Department of the Treasury's Office of Foreign Assets Control (OFAC), Australia's Department of Foreign Affairs and Trade, and the United Kingdom's Foreign Commonwealth and Development Office jointly sanctioned Zserver for aiding in LockBit-related attacks. Zserver is a Russian-based bulletproof hosting (BPH) service provider, meaning it's an Internet hosting provider that is resilient to complaints of illicit activities; it's "bulletproof."

https://home.treasury.gov/news/press-releases/sb0018

Ransomware Group Rebrands

RA Group, RALord, and Nova

RA Group / RA -> RA World -> RALord -> Nova – The RA Group, or simply, RA, began around or near April 2023 and began extorting a few victims per month. At least, that is what is known; it's likely more. According to one of their extortions, they ransomed victims per customer record. For example, one ransom note states that they were charging $0.50 per customer for one victim. About a year later, they rebranded to RA World, which, given the name, was an obvious rebrand of the same group. They didn't exactly try to mask their name.

Fast-forward an additional year, they rebranded again and even changed their dark web data leak site domain. Their new name, RALord, is another rebrand that was obvious. However, that was short-lived because a few months later they rebranded again to Nova, which is completely different than the "RA" name they've used for over two years.

See more information about RA/Nova here:

https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/ra-group
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/ralord
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/nova

Leaks

Black Basta – A significant amount of chat logs were leaked in another blow to a major ransomware group, Black Basta. In February, a user named ExploitWhispers leaked a large JSON file, about 50 MB, in a Telegram server disclosing communications between members of the Black Basta group. This exposed not only the member aliases but also unveiled a lot of the tools and tactics affiliates and members used to deploy encryptors and steal data. Since then, the group's data leak site has died down and it looks like many of the members are laying low. Considering Black Basta is widely believed to come from old Ryuk and Conti members, there's a good chance the group could disband or rebrand.

Notable breaches

Arkana Security

WideOpenWest (WOW!) – WOW! Is the eighth largest Internet provider in the United States, with coverage in the Midwest and Southeast of the country. Any disruption of this service would cause headaches for thousands, at minimum, and severe financial losses in most scenarios. Thankfully, there wasn't any known widespread disruption to services for WOW! Users. Still, Arkana Security, a new ransomware group, listed WOW! on their data leak site, indicating that possible data exfiltration occurred and the group is ransoming the organization.

BianLian

Nippon Steel – Nippon Steel is well known for being the largest steel producer in Japan, in terms of raw output in tons. It's also well-known in the United States as it's attempting to acquire U.S. steel, making Nippon the second largest steel producer in the world, still significantly behind Baowu, the world's largest producer. Considering the significance of steel production in almost every economic sector, having BianLian post Nippon Steel as a ransomware victim is significant. There's been no significant disruptions, but the possible exfiltration of data from this organization could have some unknown side effects, especially for the company itself.

Cl0p

Rackspace, Sam's Club, and hundreds of others – Last quarter we spoke about yet another 0-day attack from the Cl0p ransomware group, which seems to be their modus operandi. There were around 300 organizations listed because of the exploit of the 0-day vulnerability in Cleo's Managed File Transfer (MFT) service. Two of the names that stood out were Rackspace and Sam's Club. Although, we can't discount the others. However, Rackspace, like AWS, is a cloud solution service, and Sam's Club, is one of the largest retail wholesale organizations in the United States, headed by Walmart.

Codefinger

Amazon Web Services (AWS) – AWS needs no introduction. It's the world's largest cloud-based web service providers for one of the world's largest companies. It's well known, which is also why it's obviously on this quarter's list of notable breaches. Hacker's using the name Codefinger apparently encrypted AWS cloud storage buckets using built-in tools from AWS. The attackers used AWS's server-side encryption with customer keys to encrypt the data hosted in each bucket. This isn't a widespread attack as the threat actors must navigate to each bucket to perform the attacks but considering that there's no method to recover the data, this breach is both notable and concerning for ransomware attacks in the future.

HellCat

Jaguar Land Rover (JLR) – In March, the Hellcat ransomware group claimed to have stolen hundreds of gigabytes of information from JLR. Apparently, threat actors from Hellcat claim to have accessed JLR networks via stolen Jira credentials. This is notable for a few reasons. The first is the amount of data; hundreds of gigabytes of data is a significant amount. The second is the company involved, JLR. The final reason is the method in which Hellcat was able to get into systems, which is through stolen credentials. Many believe that ransomware groups are sophisticated entities performing complex attacks but let this be one of many examples of how threat actors often use stolen credentials to perform widespread attacks.

Telefónica – Hellcat, just as they did with JLR, claims to have infiltrated another large organization, Telefónica, using stolen credentials of an employee. This time, more information is known, as the group claims to have received the credentials from information-stealing malware originating from a social engineering attack. It's likely the JLR attack happened the same way. Telefónica is a Spanish telecommunications company operating in multiple countries.

INC Ransom

Stark Aerospace – INC Ransom has taken responsibility for a ransomware attack on Stark Aerospace, a United States missile weapons manufacturer out of Mississippi. The group claims to have stolen around four gigabytes of data, which could be used by adversaries in nefarious ways. Although we aren't certain about the data stolen, we can assume it's sensitive in nature considering this company creates weapons systems for the U.S. Department of Defense.

Unknown

Astral Foods – Astral Foods is the largest poultry provider in South Africa, and any disruption to food supply is dangerous. The company claims they experienced a cybersecurity incident, which is usually a different way of saying a ransomware attack (but not always!). Astral reported costs of around $1.1 million to restore systems back to normal, which impacted deliveries. It's unknown who was responsible for the attack, and we likely never will.

Turks and Caicos Government – Any time a government of a country is alleged to have been attacked by ransomware, it's going to be notable. However, this one is especially so because the ransomware attack had a noticeable impact on computer systems throughout the country, including on tax collection systems and the department of motor vehicles. It's also worth noting that this attack technically occurred at the very end of 2024, but most of the information wasn't yet known until the turn of the year.

Conclusion

In summary, we observed a massive surge in new, never-before-seen malware threats this quarter, while at the same time observing a modest decrease in total overall threats. Of the total malware threats we blocked, a good chunk of them were new. Most of these threats were blocked using behavioral and machine learning, with an increasing number of threats ending up in the hands of our attestation analysts. Like last quarter, we observed a ransomware sample and cryptominers in the top 10 most prevalent malware. Last quarter we observed a handful of Black Basta-related files, whereas this quarter we observed a Termite encryptor payload. Also appearing on the list was a malicious Zephyr cryptominer dubbed Tangerine Turkey that used USB thumb drives as the initial attack vector.

As for the ransomware landscape, there was a plummeting of ransomware observed on EPDR endpoints, even with Termite appearing on the top 10 most prevalent malware list. However, we also track public extortions on data leak sites and forums, and those numbers continue to go up quarter over quarter. In fact, for the first time, the number of public extortions surpassed 2,000. This was spearheaded by Cl0ps extortions of victims from the Cleo MFT zero-day exploit and contributing were the 17 new groups discovered in Q1. More groups had a reduction from quarter to quarter than saw a rise, but that didn't matter. Let's hope for public extortion numbers to decrease in Q2.

CONCLUSION & DEFENSE HIGHLIGHTS

CONCLUSION AND DEFENSE HIGHLIGHTS

After completing this quarter's report, we hope you've gained new awareness and ideas to become a better digital ecologist and steward of our shared cyber ecosystem. As malware volumes grow and new, evasive threats emerge – many leveraging malicious AI tools to accelerate their illicit activities – the cybersecurity battleground is increasingly becoming an AI-driven war.

But this war is far from lost. The threats outlined in this report highlight attacks we have identified and prevented. They serve as vital intelligence for cybersecurity professionals and IT administrators in your role as digital ecologists working to monitor, understand, and protect the ecosystem we all depend on. While attack methods are growing more sophisticated and techniques like phishing and evasive tactics evolve, we are also seeing positive signs. Ransomware and cryptomining attacks are declining, demonstrating that our collective efforts to safeguard the cyber landscape are beginning to bear fruit.

With this in mind, here are three cybersecurity strategies that every digital ecologist should consider to help maintain the delicate balance of our interconnected, shared digital world:

AI defense is the only solution to AI attacks

This quarter, most of the malware we prevented was due to our machine learning- and AI-based solution, IntelligentAV, and AI security tools continue to play an increasingly important role in catching more evasive and complex threats and attacks. We believe this is because threat actors are benefiting from the power of AI for malicious use as well.

We have seen AI tools infiltrating the hacker underground. Most phishing kits have incorporated various levels of AI to assist in writing convincing emails and even automating the generation of more targeted spear phishing. Threat actors are actively leveraging AI to write new malware or adjust it to evade detection. Social engineers leverage a myriad of deepfake tools to make their scams and lures much more convincing and enticing, and all this is just the start. We believe attackers have barely scratched the surface of how they can leverage AI to improve their attacks.

However, you can fight fire with fire, as most wildfire fighters know. The only solution to keeping up with the power, speed, and scale of malicious AI tools is for you to leverage the same powerful AI technologies for defense. Here at WatchGuard, through acquisition and development, we have leveraged machine learning and AI for ten years and continue to build more AI technologies in all our network, endpoint, and identity products. As a defender, you should leverage tools that focus on continuing to increase their AI-assisted capabilities.

Increase or update your web protections.

Every quarter, web-based threats fill our Top 10 Network Attack list. By far, the most common threats we see over the network are web applications attacks and vulnerabilities targeting your web clients. Meanwhile, in our endpoint section, we have seen web browsers jump onto the scene as a top infection vector in the second or third spot, suggesting that attackers are bringing back drive-by download attacks.

You likely have some web-based defenses already, but it might be time to re-check them and add new ones. Below is a quick list of many options to protect your web servers and clients:

- **Web Server Protection**
  - Patch your web servers and external web frameworks and follow secure code practices for your custom web code.
  - Web application firewalls (WAF) can proactively block common web-app attack.
  - Follow hardening guides to protect whatever web servers you employ.
  - Don't forget IOT and other products often expose web services for management. They need the same protections as your stand-alone web servers.
  - Make sure to use IPS and, better yet, upgrade to a network detection and response (NDR) product, such as WatchGuard's ThreatSync+ NDR, to leverage AI and network anomaly detection to disrupt new attacks that get past IPS.

- **Web Browsers and Client**
  - Use domain, IP, and URL filtering products and services to prevent users from accessing malicious web sites that exploit your clients.
  - Leverage malware protection services that can catch the malicious payloads that drive-by downloads try to force.
  - As always, patch your browsers and clients, plug-ins, or extensions regularly, and avoid dangerous web extensions.
  - And like above, leverage IPS and NDR.

Harden all remote access and require MFA

The entire industry sees the continued growth in the trend of threat actors targeting remote access services, whether VPN services, remote desktop applications, or any other product or appliance that allows your dispersed employees to work from wherever they may be. This stems from these tools usually requiring exposure to the entire digital world for them to function. Meanwhile, users still leverage bad password practices while attackers continue to successfully phish, steal, and crack our credentials. In Q1, we saw attackers targeting remote access products from Ivanti while also seeing an increase in the "other" endpoint attack vector, which includes remote access tools. Finally, regulatory agencies, compliance and standards groups, and even cyber insurers also realize the risk of unhardened remote access and are enforcing stricter security standards for it.

What should you do about it? Step one, never expose remote access without multi-factor authentication (MFA). This step alone can protect you from a huge majority of remote access attacks. Obviously, you should also follow the normal best password and credential practices and use unique and strong passwords or other strong credentials.

Next, security is about limiting risk with things like the least privilege principle. This is not just identity-based; it can include limiting network access. Remote access tools are unique in that they are intended to give secure remote access, but if you want anyone to reach them wherever they are, it seems like you must expose all of them to the entire Internet. However, you have another option that can lessen the risk: require VPN or zero trust network access (ZTNA) authentication before allowing users to access remote access tools. Yes, most remote access tools advertise that they secure traffic on their own, without the need for an additional VPN. However, these tools can suffer "pre-authentication" issues that, when set up this way, expose that flaw to the world. VPN or ZTNA solutions may too, but if you require it first, that is the only service you must expose to the work, and it will provide additional protection on top of anything built into the remote access app.

Finally, as always, patch your remote access, VPN, and ZTNA tools aggressively, and investigate their configurationsettings of all remote access apps to see they have any app-specific hardening options.

You've reached the end of our Q1 2025 Internet Security report. Congratulations. Be sure to come back next quarter to keep up with the latest changes in the threat landscape. As always, leave your comments or feedback about our report at **SecurityReport@watchguard.com**, and keep frosty online!

COREY NACHREINER

Chief Security Officer

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

MARC LALIBERTE

Director of Security Operations

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

TREVOR COLLINS

Information Security Analyst

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

RYAN ESTES

Intrusion Analyst

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

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.