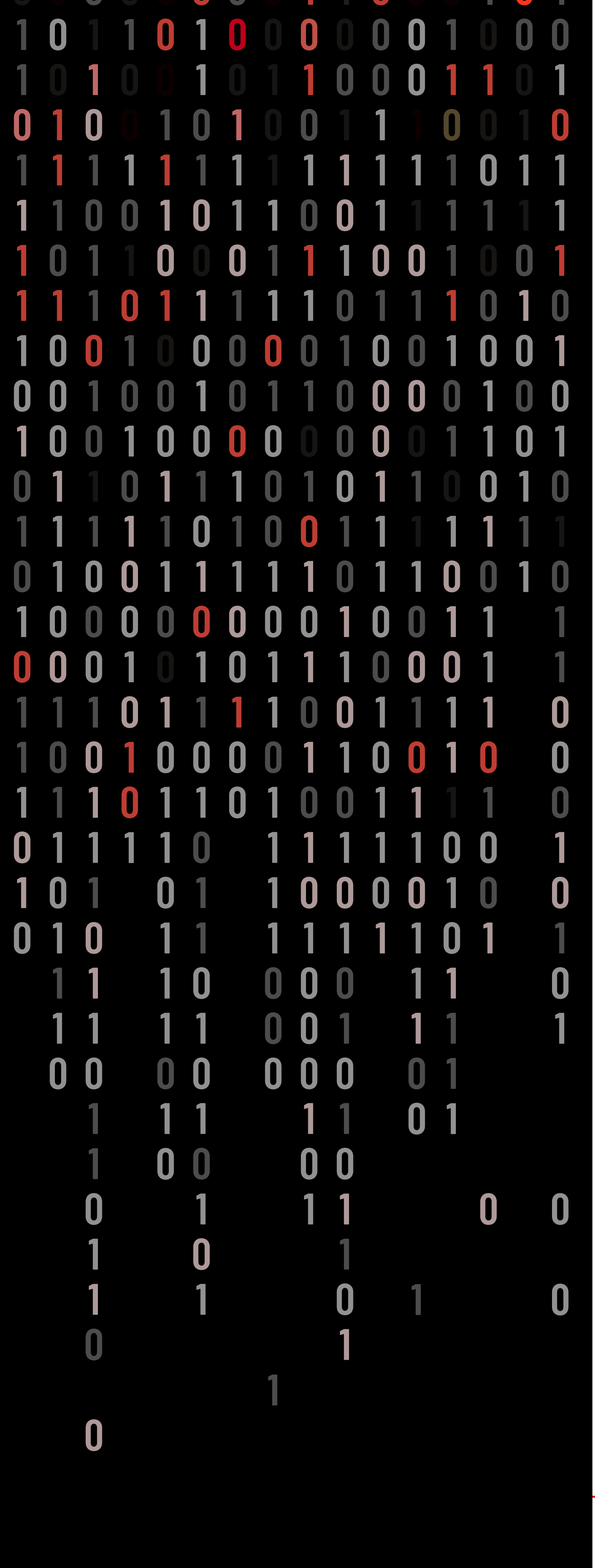
INTERNET SECURITY REPORT

WatchGuard



CONTENTS

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

INTRODUCTION

Like sailors who once checked the horizon each morning for the faintest signs of shifting weather, we have long published this report every quarter to help chart the changing climate of global cyber threats. Those regular scans served us well for many years and offered sharp snapshots of attacker behavior in motion. Yet as our vantage point has widened and our tools and methods have grown more precise, those quarter-to-quarter views have begun to resemble still frames in a slow-moving storm. They remain useful, but they are sometimes too narrow to reveal the deeper currents that truly define the threat landscape.

For that reason, beginning with this edition, we are moving from a quarterly cadence to a biannual one. This shift gives us a broader field of view and helps us reduce the noise created by short bursts of volatility. When we combine a longer stretch of data into a single analytical cycle, we hope the patterns that matter most become easier to see. Trends that once appeared subtle should now stand out clearly. This expanded cadence also gives us room to strengthen the depth of each report while reserving timely stand-alone updates for rare events that demand immediate attention.

Our mission has not changed. We continue to study and interpret the evolving behavior of attackers so we can recommend stronger, more effective defenses for the organizations and individuals who rely on our insights.

Within each report, we combine the threat intelligence gathered from our network security products, endpoint telemetry, and DNS filtering systems. This includes network-based malware trends, top malware families detected by volume and by prevalence, encrypted and evasive malware activity, regional threat distribution, DNS abuse patterns, individual malware sample analysis, network attack trends, endpoint threat behaviors, and insights into how ransomware groups adapt their techniques across time. These categories appear consistently throughout past reports in your archive and form the foundation for the long-term patterns we highlight for defenders today.

Welcome to the first H2 2025 Internet Security Report. With this new rhythm, we aim to provide a clearer and more revealing view of the threat environment and give defenders the knowledge they need to stay ahead of the tide.

Our ISR is broken down into the following sections:

EXECUTIVE SUMMARY

The second half (H2) of 2025 tells a malware story of contrasts and dichotomies. Like the first half of the year, network-based malware detection is up in volume. However, from the endpoint perspective, total malware is down overall in H2, dropping the most in Q4. Meanwhile, from the network perspective, evasive and sophisticated zero-day malware fell by more than half, despite the rise in overall malware volume. Yet again, the endpoint tells a different story with new and unique malware detections up in volume, exploding by over 1,500% in Q4 specifically. One thing remains the same though; despite the contrasting malware stories told by our endpoint and network products, you need to keep your eye on both types of malware detection to avoid this threat.

Meanwhile, network-based attacks and software exploits declined, as did the unique types of exploits we detected. The bulk of the top network detections continue to be older vulnerabilities, likely mass-scanned by automated botnets and exploit frameworks. We did dive further down into the top 50 to find some interesting exploits to cover later in the report though.

In the endpoint section of this report, we continue to see that the way threat actors deliver malware has been changing. Malicious scripts have been the number one malware vector for as long as I can remember, though they have been slowly dropping over the past year. However, this half, during Q4, Windows binaries became the most common way for malware to start to infect a system, likely as threat actors use living-off-the-land (LotL) tools to launch attacks, leveraging legit Windows binaries **(LOLBAS)**.

Here are some of the highlights you can expect from our H2 2025 report:

- **Network-based malware is up 26% half-over-half (HoH).** Malware increased in detection volume during the whole year. That said, **we also saw a significant decrease in zero-day malware (caught with our proactive services), down to only 23% of the overall detections.** While the more evasive malware declined, malware seen over encrypted connections is still high.
- **Total endpoint malware volume was down slightly** (~4.6%) for the second half of 2025. However, the volume technically grew during Q3 and dropped substantially in Q4. Meanwhile, **new, unique endpoint malware detections grew throughout H2, and exploded by more than 1,500% in Q4**, suggesting threat actors were focusing on new and evasive malware during the end of the year.
- **Threat actors continue using encryption to evade defenses.** Malware arriving over encrypted (TLS) connections stayed high for the second half of the year.
- **Malware detected with signatures over TLS stayed high but static**
- **Evasive malware detected over TLS increased by almost 2,000%**
- Our "per Firebox" malware results for various network malware detection services:
  - **Average total malware detections per Firebox: 1,260** (26% increase HoH)
  - **Average malware detections by GAV per Firebox: 978** (89% increase HoH)
  - **Average malware detections by IAV per Firebox: 188** (49% decrease HoH)
  - **Average malware detections by APT Blocker per Firebox: 94** (16% decrease HoH)
- We extrapolate that if the estimated active Fireboxes enabled all malware detection security services and were reporting to us, **Fireboxes would have seen at least ~567,000,000 malware detections during H2 2025.**
- **Just under a quarter (23%) of malware evaded signature-based methods.** We call this zero-day malware because it requires more proactive techniques (IAV/APT) to catch never-before-seen malware. The zero-day number increased greatly the first half of 2025, reaching two-thirds of all malware. However, it seems to have declined during the second half of 2025.
- **Adding to this, zero-day malware only accounted for 16% of malware detected over encrypted connections**, showing an unusual decline in evasive malware there, too.
- **Dropper malware accounted for six of the top 10 malware by volume (60%) and four of the top five encrypted threats (80%).** This continues a pattern we saw through the beginning of 2025. It makes sense as threat actors rarely start by directly delivering the intended malware payload to a victim. Rather, they use droppers, stagers, or loaders, to pave the way for attacks, potentially evading any legacy defenses and attempting to disable security along the way.
- **Meanwhile, network attacks decrease by 28% during H2 2025.** We also saw the amount of unique network exploits fall too. Web application attacks remain the predominant theme in our network attack section.
- **USB malware associated with cryptocurrency attacks remains.** During the second half of 2025, we continued to see some examples of threats that can spread over USBs and target cryptocurrency theft.

- Ransomware declines but cryptominers rise. **Ransomware, though up a tad in Q3, ended up declining 68.42% over the year. Meanwhile, we saw detections for cryptominers increase to almost the same high as in Q1.** Ransomware is not going away, but we suspect threat actors are focusing on big game hunting with very high ransom demands. This does not mean ransomware extortions are down; it just means ransomware attackers are targeting victims instead of sending ransomware to every potential victim. Meanwhile, cryptominers will likely remain a popular and easy way to monetize infected victims.

- **Living-of-the-land (LotL) Windows binaries become top endpoint malware vector.** For the last two years, malicious scripts (primarily PowerShell) have been the most common attack vector for malware on the endpoint by far. However, over the last year, the common attack vector has shifted more to targeting Windows binaries, browser issues, and remote access programs. During the second half of 2025, specifically in Q4, maliciously leveraged Windows binaries became the top malware attack vector. This is likely due to attackers continuing their LotL techniques but shifting away from scripts alone.

That's a high-level summary of the top cyberattack trends we saw during the second half of 2025, but our report includes much more detail and defense tips to help you protect yourself from these trends. Read on to learn more.

FIREBOX FEED STATS

WHAT IS THE FIREBOX FEED?

In this section of the report, we examine threat detection data from tens of thousands of WatchGuard Fireboxes deployed around the world that have opted in to sharing threat intelligence with us. This data allows us to view the specific malware and exploit activity that threat actors are using against small and midsize organizations worldwide.

The Firebox Feed is a collection of threat detections from five security services running on Firebox appliances:

Gateway AntiVirus (GAV): Signature-based malware prevention

IntelligentAV (IAV): Advanced AI-based malware prevention

APT Blocker: Sandboxed, behavioral-based malware prevention

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

DNSWatch: Domain-based threat prevention

We'll start with a review of both the high-level trends and a deep-dive analysis of specific malware threats blocked by the three layers of Firebox anti-malware services. After that, we turn our sights on the top network attacks blocked by the Intrusion Prevention Service before ending with a view into a handful of threats prevented by the DNSWatch domain-based firewalling service. Finally, we end with tips for defenders to help combat the threats we discuss throughout the section.

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

MALWARE TRENDS

In this Firebox Feed section, we collect anonymized proxy logs from participating Fireboxes to identify detected malware families and the specific WatchGuard service that blocked them (such as Gateway AntiVirus, IntelligentAV, or APT Blocker), identifying high-level malware trends along the way. Beyond these core details, we also focus on malware traveling over encrypted TLS connections and the geographic region of affected devices. With this focused data set from global deployments of reporting Fireboxes, we analyze patterns to reveal how malware targets real-world networks, highlight emerging tactics, and provide actionable guidance to help readers strengthen their defenses.

A key advancement in this report is our expanded ability to inspect actual file samples from some of the most prevalent threats caught exclusively by APT Blocker and IntelligentAV signature-less detections. Previously, we were limited to detection metadata for these services, but now we can perform detailed behavioral analysis as we choose, and in this report we do so on three notable samples, offering clearer insights into attacker techniques and more precise recommendations for mitigation. These enriched, real-world observations continue to empower security teams to anticipate threats and adapt protections effectively.

Network-based malware activity in the second half of 2025 showed a moderate overall increase, with the average Firebox blocking 1,260 total malware instances. This accounts for a 26% rise compared to the first half of the year.

As shown in the Firebox Feed Half-Year Overview, most detections continued to be handled by signature-based Gateway AntiVirus (average 978 hits per Firebox, up 89%), while cloud sandboxing via APT Blocker averaged 94 hits (down 16%), and IntelligentAV scans averaged 188 (down 49%). The sharp rise in traditional signature detections suggests attackers relied more on known but repacked variants during this period.

Encrypted malware remained the dominant delivery method, with 96% of blocked threats arriving over TLS connections – unchanged from the previous half. This near-total reliance on encryption continues to create significant blind spots for organizations that do not perform HTTPS inspection.

Among Fireboxes configured for TLS decryption, Gateway AntiVirus detections averaged 2,235 hits per device (up 9%), revealing the substantial volume of threats hidden in encrypted traffic. Even more strikingly, evasive malware delivered over TLS spiked dramatically, averaging 2,749 hits per Firebox – an approximately 2,000% increase. This surge reflects new or intensified campaigns leveraging advanced obfuscation and packing techniques specifically designed to exploit encrypted channels.

These trends reinforce critical defense priorities. Enabling TLS inspection to regain visibility into the traffic and layering advanced sandboxing to counter the growing wave of evasive and zero-day threats hiding within it.

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.

Average combined total malware hits per Firebox

1,260

Average detections per Firebox increased **16%**

Basic Gateway AntiVirus (GAV) service

978

Basic malware increased **89%**

APT Blocker (APT)

94

APT Blocker dropped by **16%**

IntelligentAV (IAV)

188

dropped by **49%**

GAV with TLS

2,235

TLS detections by GAV increased **22%**

Average evasive malware over TLS

2,749

TLS detections of evasive malware jumped a whopping **1,998%**

TLS malware

96%

Malware over an encrypted connection did not change.

Top 10 Malware Detections

The Firebox Feed's Gateway AntiVirus service tracks the malware variants blocked across all participating appliances, and we slice these results into many views, including the variants seen most often. For 2025 H2, the top 10 list continues to show a strong presence of droppers, which made up six of the top 10 detections by volume. These generic or heuristically detected droppers typically serve as initial payload deliverers for more sophisticated threats, including ransomware, banking trojans, and infostealers.

As shown in the Top 10 Malware Detections table, Heur.BZC.PZQ.Boxter claimed the top spot with over 705,000 detections. This heuristic signature represents a family of heavily obfuscated droppers that frequently change their appearance to evade signature-based defenses. Its dominant position reflects the continued reliance by attackers on polymorphic and packed malware techniques.

Following closely were several generic trojan and application signatures, including Trojan.Generic.38935134, Application.Agent.IIQ, and Application.Generic.4048548, all categorized as droppers. These high-volume detections highlight the ongoing flood of commodity malware that threat actors distribute through spam, malicious ads, and compromised websites.

Notably, the list also includes tools more commonly associated with post-exploitation and lateral movement phases. Generic.Application.Impacket.A.EF9749CB appeared in sixth place. This detection covers malicious or unauthorized use of the popular Impacket Python library, often leveraged by both red teams and real attackers for credential dumping, remote execution, and SMB/NTLM relay attacks. Its presence in the top 10 indicates active exploitation attempts against Windows environments.

Two Linux-oriented hacktools rounded out the lower half of the list: Trojan.Linux.Generic.411671 and Variant.Application.Linux.PNScan. These tools are frequently associated with IoT botnet recruitment and network scanning activity, suggesting continued attempts to compromise Linux-based servers, routers, and embedded devices exposed to the Internet.

Overall, the 2025 H2 top 10 demonstrates attackers' continued preference for evasive droppers as entry vectors while also incorporating specialized scripting and scanning tools for deeper network penetration. Defenders should ensure their network anti-malware solutions combine signature, heuristic, and behavioral analysis to catch both the high-volume generic threats and the more targeted hacktools appearing in these rankings.

Threat Name	Malware Category	Count
Heur.BZC.PZQ.Boxter	Dropper	705,396
Trojan.Generic.38935134	Dropper	238,280
Application.Agent.IIQ	Dropper	109,371
Application.Generic.4048548	Dropper	61,288
Application.Proxy.OTN	Proxy	49,226
Generic.Application.Impacket.A.EF9749CB	Script	46,123
Trojan.Linux.Generic.411671	Linux hacktool	45,954
Variant.Application.Linux.PNScan	Linux hacktool	45,941
Trojan.GenericKDZ.109967	Dropper	45,897
Generic.Botget.4DF58464	Dropper	45,897

Figure 1. Top 10 Malware Detections

*seen in past under Encrypted malware threats

Top 5 Encrypted Malware Detections

Encrypted malware remains a key challenge for network defenses, concealing payloads in TLS traffic that many organizations skip inspecting due to privacy or performance issues. Firebox Feed data for 2025 H2 confirms a substantial share of blocked malware used HTTPS, highlighting the critical need for TLS inspection.

As shown in the Top 5 Encrypted Malware Detections table, droppers dominated, taking four of the top five spots. Application.Agent.IIQ led the list, reflecting heavy use of HTTPS for payload delivery via malware and drive-by downloads.

Second place went to Application.Proxy.OTN, often flagging evasive loaders that connect to C2 servers over encrypted channels.

Variant.Lazy.452427, a dropper using lazy loading to delay execution and evade sandboxes, showing attackers combining encryption with timing tricks.

Fourth was Java.Trojan.GenericGB.29173, a generic signature for malicious Java archives spread through compromised sites or ads, targeting environments with outdated Java runtimes.

Threat Name	Malware Category	Count
Application.Agent.IIQ	Dropper	109,371
Application.Proxy.OTN	Dropper	49,226
Variant.Lazy.452427	Dropper	32,100
Java.Trojan.GenericGB.29173	Dropper	18,891
Trojan.JS.Phishing.FM	Password Stealer	15,797

Figure 2. Top 5 TLS Malware

Top 5 Widespread Malware Detections

The most-widespread malware detections affect the largest percentage of Fireboxes, often revealing persistent threats tied to unpatched vulnerabilities, malvertising, or broad distribution campaigns rather than highly targeted attacks.

As shown in the Top 5 Most-Widespread Malware Detections table, exploits dominated the 2025 H2 rankings, occupying the top three positions. Exploit.MathType-Obfs.Gen, an obfuscated exploit targeting the MathType equation editor, led with the broadest reach. If this sounds overly technical, essentially this is just an Equation Editor available in Microsoft Office documents. So this just means a malicious Office document could execute code if you haven't patched this older, 2017 Office vulnerability. It showed heavy concentration in Hong Kong (24.39%), Greece (23.66%), and Germany (21.12%), with EMEA devices most exposed at 12.75%.

Gen:Heur.Mint.Zard.24, a heuristic detection associated with the Zard/SmokeLoader family, took second place. Zard and/or SmokeLoader are just modular remote access trojans (RATs) or backdoors that allow threat actors to maintain persistence on a victim and potentially load other malware or run malicious commands. The United Kingdom (25.08%), France (24.12%), and Brazil (16.74%) saw the highest rates, driving elevated exposure in AMER (13.02%) and EMEA (9.34%).

Third was Exploit.CVE-2017-0199.05.Gen, leveraging the long-patched CVE-2017-0199 in Microsoft Office RTF files; another malicious Office document threat similar to the "MathType" flaw above. Poland (33.06%), Turkey (22.61%), and Greece (21.37%) topped the list, with EMEA again leading regionally at 12.08%.

Trojan.Zmutzy.Pong.2 (we've described Zmutzy in many previous reports) placed fourth, primarily impacting Hong Kong (18.29%), Malaysia (10.58%), and Germany (9.27%), with EMEA at 6.78%.

JavaScript adware Adware.Cryxos.14449 rounded out the top five, spread heavily via malvertising. Malaysia (24.04%), Brazil (13.12%), and Canada (11.18%) were most affected, showing notable impact in AMER (8.45%).

The prevalence of older exploits in these rankings underscores the enduring danger of unpatched software, particularly in productivity tools. Organizations should accelerate patch management for Office components and third-party editors, while deploying strong web filtering to block malvertising and exploit kit delivery.

Malware Name	Top 3 Countries by %			EMEA %	APAC %	AMER %
Exploit.MathType-Obfs.Gen	Hong Kong - 24.39%	Greece - 23.66%	Germany - 21.12%	12.75%	4.65%	5.07%
Heur.Mint.Zard.24	United Kingdom - 25.08%	France - 24.12%	Brazil - 16.74%	9.34%	1.40%	13.02%
Exploit.CVE-2017-0199.05.Gen	Poland - 33.06%	Turkey - 22.61%	Greece - 21.37%	12.08%	3.79%	2.88%
Trojan.Zmutzy.Pong.2	Hong Kong - 18.29%	Malaysia - 10.58%	Germany - 9.27%	6.78%	4.38%	2.30%
Adware.Cryxos.14449	Malaysia - 24.04%	Brazil - 13.12%	Canada - 11.18%	4.23%	3.52%	8.45%

Figure 3. Most-Widespread Malware

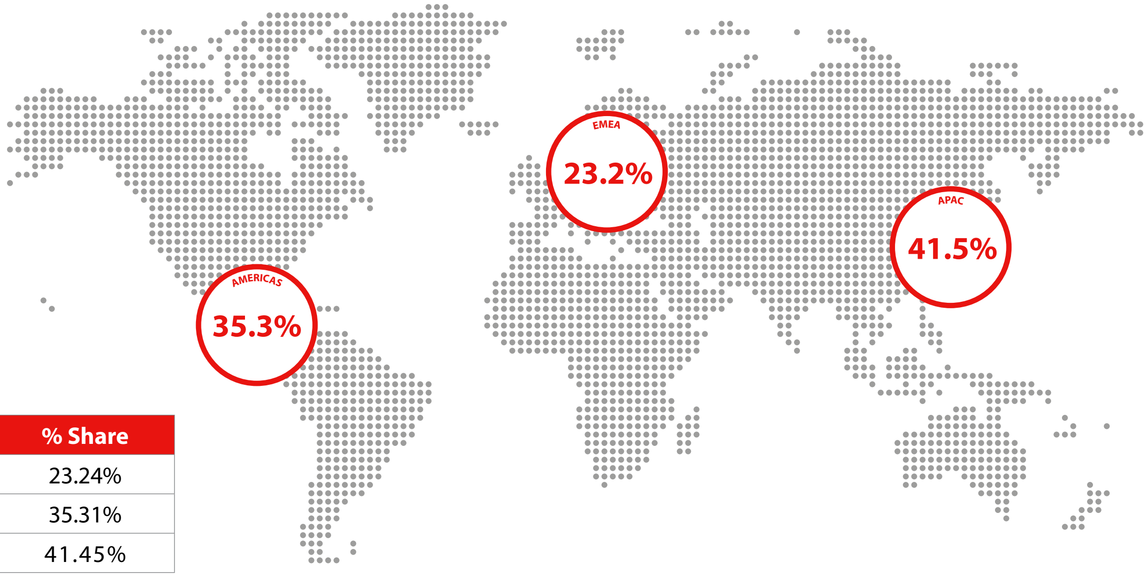
Geographic Threats by Region

Malware exposure varies significantly by region, influenced by factors such as Internet usage patterns, device types, patching habits, and regional threat actor preferences. The Firebox Feed normalizes detections by calculating the average number of malware blocks per participating Firebox in each region, providing a clearer picture of relative threat levels.

As shown in the Geographic Threats by Region figure, APAC experienced the highest average malware detections per Firebox in 2025 H2 at 41.45%, followed by AMER at 35.31%. EMEA recorded the lowest rate at 23.24%.

The elevated exposure in APAC continues a long-standing trend, often driven by widespread use of Internet-exposed Linux devices, IoT systems, and aggressive malvertising campaigns targeting the region's diverse markets. AMER's higher rate compared to EMEA may reflect differences in software ecosystems or greater reliance on cloud services that attract opportunistic attacks.

Organizations operating across multiple regions should maintain consistent security policies and ensure perimeter defenses are uniformly configured. Regional variations underscore the value of localized threat intelligence, but strong gateway anti-malware and regular vulnerability scanning remain essential everywhere.



Region	% Share
EMEA	23.24%
AMER	35.31%
APAC	41.45%

Figure 4. Geographic Threats by Region

Catching Evasive Malware

Attackers continue to employ sophisticated evasion techniques to bypass traditional signature-based malware detection. These include heavy obfuscation, packing, and encryption, but through advanced behavioral analysis and cloud sandboxing we can identify these zero-day and evasive threats before they execute.

As shown in the Catching Evasive Malware figure, on Fireboxes equipped to catch zero-day malware, 23% of blocked malware in 2025 H2 was zero-day, detected by IAV and APT Blocker's sandbox analysis. The remaining 77% was caught by signature-based methods.

This means that without APT Blocker enabled, nearly one in four threats would have reached endpoints undetected at the network perimeter. Among devices configured for TLS encryption inspection, 16% of encrypted malware required IAV or APT Blocker for detection, while 84% was blocked via signatures.

The lower zero-day rate in encrypted traffic may reflect attackers' confidence in evasive malware, but it still underscores the compounded risk: without TLS decryption, all encrypted malware goes unseen. Enabling deep packet inspection for HTTPS, paired with APT Blocker, is critical to closing this gap to ensure comprehensive protection against evasive threats.

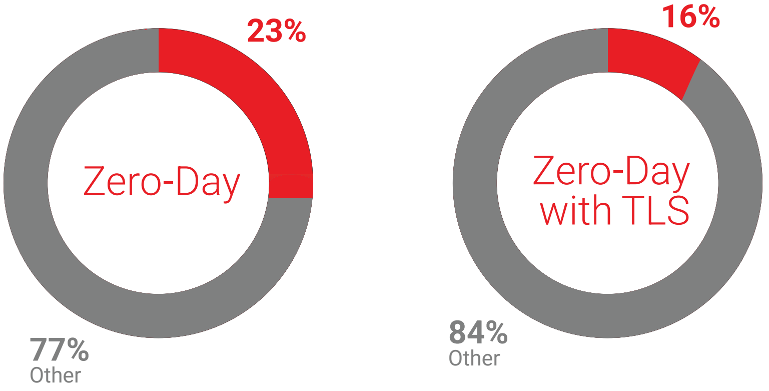
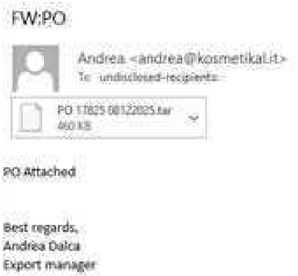


Figure 6. Zero-Day Malware

Individual Malware Sample Analysis

Guloader Downloading Snake Keylogger
With our ability to reference files detected by IntelligentAV (IAV) and APT Blocker more easily now, we found a file that IAV detected that acts like a Win Code Injection loader. In the ever-evolving world of cyber threats, GuLoader stands out as a particularly cunning malware downloader. Often arriving disguised as innocent files, it installs suspicious processes to deploy payloads such as the SnakeKeylogger. This malware steals sensitive data, from browser credentials to keystrokes, and sends it off to attackers. What makes it dangerous is how it hijacks legitimate Windows processes to stay hidden. Let's break down how these risky processes collaborate and what red flags you should watch for.



FW:PO

Andrea <andrea@kosmetika.lt>
To: undisclosed-recipients

PO 17825 08122025.tar
460 KB

PO Attached

Best regards,
Andrea Dalca
Export manager

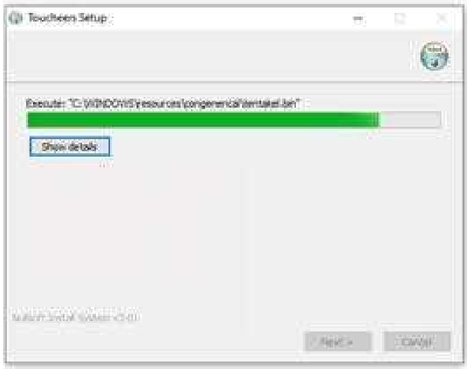
Figure 5. PO 17825 email.png

GuLoader's processes don't just drop a single malicious file and call it a day. It orchestrates a multi-stage assault using everyday system tools to evade detection:

1. **PowerShell Evasion**
   The infection starts when you run the executable. It immediately spawns multiple instances of PowerShell (both the classic powershell.exe and the modern pwsh.exe) along with conhost.exe to handle console operations quietly. These run heavily obfuscated scripts pulled from hidden folders deep in your AppData directory. This stage handles everything from anti-analysis checks (scanning for debuggers or virtual machines) to downloading additional payloads from cloud services.
2. **Scouting the Terrain with WMI**
   Next, it uses wmiadap.exe and wmiprvse.exe. These legitimate Windows Management Instrumentation tools are abused to quietly query your system for running processes, hardware details, or even open windows. The malware uses this intel to decide whether it's safe to proceed or if it should self-terminate to avoid sandboxes and security tools.
3. **The Final Payload**
   The real damage happens during injection. PowerShell creates a suspended instance of msiexec.exe (the Windows Installer service) and injects shellcode directly into it using techniques like Early Bird APC (Asynchronous Procedure Calls). Once resumed, the compromised msiexec.exe file runs the Snake Keylogger under the cover of a trusted system process.

If anything goes wrong (like a deliberate crash for evasion), WerFault.exe steps in as the error reporter, further masking the activity.

This chain hides in normal Windows behavior. We did catch it installing tentakel.bin, which could be related to the process controller Tentakel.



Execute: "C:\WINDOWS\resources\congenerical\tentakel.bin"

Figure 7. Tentakel.png

While not available from a network anti-malware device, know that Endpoint Detection and Response (EDR) solutions, like WatchGuard's EPDR, detect a lot of this sort of activity as different indicator of attacks (IoAs). EDR solutions are specifically designed to monitor processes and other OS artifacts as they are first run and continue to run. EPDR would have detected a lot of the activities described above for you.

GuLoader thrives on social engineering like an urgent-looking invoice. Never open unexpected executables, keep your antivirus updated with the latest definitions, and consider enabling advanced monitoring tools like EPDR. By understanding how these processes team up, you can better recognize when something is seriously wrong.

Detecting GuLoader early can prevent serious data loss. Here are the key indicators to monitor on your system:

- **Unusual Process Behavior**
  Look for PowerShell launching from odd parents (like Explorer or random user executables) with long, garbled command lines involving file reads from hidden AppData paths or substring manipulations. Sudden suspended process creations are a big warning sign of injection attempts.
- **Suspicious Files and Registry Changes**
  Randomly named folders or files appearing in %AppData% (e.g., strange paths with words like "spgefuldhed" or "Sable. Pun"). Also, watch for new entries in registry locations like HKCU\Software or Environment variables used for persistence.
- **Network Activity**
  Unexpected outbound traffic to cloud storage sites, geo-IP check services, Telegram APIs, or obscure IPs. Look especially for encrypted POST requests or connections on ports commonly used for email (like 587 for SMTP exfiltration).
- **System Oddities**
  Spikes in CPU usage from delay loops, unusual WMI queries, or signs of keyboard hooking (e.g., attempts to access browser data folders). If security tools suddenly stop working or the system behaves erratically after opening a "PDF" attachment, investigate immediately.

FormBook + Lumma Stealer

Job seekers and recruiters beware: one of the oldest tricks in the malware playbook is still highly effective. Cybercriminals frequently send phishing emails with attachments posing as resumes or CVs – often with convincing names like "CurriculumVitae-MariaTeresaReyes.exe." This FormBook sample arrives exactly that way.

We found an email associated with this sample and we translated it from Spanish to English.

Buen día,

Mi nombre es Maria Teresa Reyes, les escribo con el fin de ser considerado para cualquier vacante disponible que esté a mi alcance.

Adjunto mi CV y quedo a su entera disposición para concertar una entrevista.

Muchas gracias por tu tiempo.

English translation of the email above:

Good morning

My name is Maria Teresa Reyes, I am writing to you in order to be considered for any available vacancy that is within my reach. I attach my CV and remain at your entire disposal to arrange an interview.

Thank you very much for your time.

Clicking the attachment unleashes an infostealer that harvests browser passwords, cookies, email profiles, and more while you think you're just opening a document.

FormBook specializes in credential theft through form grabbing, direct file access, and browser hooking. This variant combines social engineering with system abuse for maximum impact:

1. **The Initial Deception**
   The victim runs the attachment, which immediately triggers consent.exe to display a User Account Control (UAC) prompt – often disguised as part of "opening" or "processing" the document. It then launches slui.exe (activation dialog), sppextcomobj.exe, and sppsvc.exe to show fake Windows activation or progress screens, distracting the user while the real work happens in the background. Cmd.exe and PowerShell execute hidden commands, with taskhostw.exe helping orchestrate timing or persistence.
2. **Clearing Rivals and Preparing the Ground**
   The malware terminates competing processes, including wmiprvse.exe, certain svchost.exe instances, and suspicious executables in random folders (e.g., mpea.exe, pztc.exe). This eliminates interference from other infections and reduces the chance of detection.

3. **Injection and Data Harvesting**
   Temporary files flood %Temp% with random names ("horrify," "isochronally," etc.) for staging components. The payload then injects into a legitimate syswow64\svchost.exe process for stealth. From there, it directly reads browser databases, queries registry keys for Outlook and Thunderbird profiles, and even launches Firefox or Internet Explorer to hook active sessions and capture forms. Anti-analysis routines (IsDebuggerPresent, GetTickCount) help it avoid sandboxes, while mutexes prevent multiple instances.

Stolen data is exfiltrated via HTTP to attacker-controlled domains (e.g., spierai.info), with numerous fallbacks for reliability. Spotting this type of phishing early can protect your accounts and network. Key indicators include:

- **Unexpected Email Attachments**
  Unsolicited "CV" or resume files arriving as executables (.exe) – especially with double extensions or names like "CurriculumVitae.pdf.exe." Legitimate resumes are usually PDFs or Word docs, never raw executables.
- **Suspicious Prompts and Dialogs**
  Opening the attachment triggers UAC elevation followed by unexpected Windows activation screens (slui.exe) or progress dialogs that don't match a simple document view.
- **Process and File Anomalies**
  Sudden terminations of background processes, bursts of oddly named temp files, or injections into svchost.exe. Watch for PowerShell or cmd launching silently from a desktop file.
- **Browser and Network Activity**
  Browsers opening automatically without input, direct access to credential files, or outbound connections to obscure domains shortly after opening the attachment.

FormBook thrives on phishing. Never open attachments from unknown senders, even if the subject line seems professional. Hover over links and filenames to check extensions and enable "show file extensions" in Windows. Use email filtering, keep antivirus with real-time behavioral detection enabled, and consider sandboxing suspicious attachments. For recruiters or anyone handling frequent applications, verify senders through other channels before downloading. FormBook has been around for years, but its simplicity and reliable delivery keep it dangerous. A moment of caution with that "CV" attachment can save you from a major credential compromise. Stay vigilant!

The Hidden Risks of Clover.exe, the Tabbed Explorer Alternative caught by APT Blocker

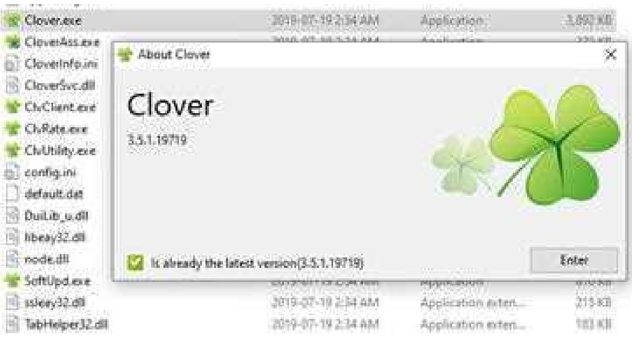
In the quest for a more efficient Windows File Explorer, many users turn to third-party tools like Clover.exe. Developed by Chinese company EJIE Technology, Clover adds handy Chrome-style tabs to Explorer windows, making file management feel modern and streamlined. It's lightweight, free, and has a loyal following. However, beneath the convenience lies a history of security red flags. Like a previously discussed tool, Ammyy Admin, it makes a risky choice for everyday use.

Clover integrates directly into Windows Explorer, overlaying tabs without replacing the core system. Unlike built-in Windows features, Clover relies on automatic updates pulled directly from the developer's servers. This auto-update mechanism, while convenient, introduces significant risks. Over the years, users report malware installed with the Clover installation. Past incidents **reported by users** and its own **release notes** show that it has spread adware and pop-ups without users knowing the adware installed with Clover. We call this type of malware activity "Softcnapp," indicating its hidden adware installation. As with any program that hides adware in its installation, we can never trust these ads because they often spread malware. Even if Clover is clean today, a future update could bundle unwanted software if the distribution channel is ever hijacked.

While not always outright malicious, these flags often stem from bundled adware in older installers or opaque update practices. The developer's track record raises questions about rigorous security vetting, echoing Ammyy Admin's troubles, where legitimate downloads turned into malware vectors.

Many versions of Clover are signed with digital certificates, but the origins matter. The software signed with the Shanghai Oriental Webcasting Co., Ltd. certificate indicates this software comes from China.

Always download from official, reputable sources. For critical systems, stick to signed software from reputable companies to minimize third-party risks. Clover may work fine for some, but its past issues, auto-update reliance, and certificate concerns make it a tool best approached with extreme caution. In cybersecurity, convenience should never trump safety. Choose wisely!



☑ Is already the latest version(3.5.1.19719)

Figure 8. Clover malware

NETWORK ATTACKS

The Intrusion Prevention Service (IPS) on Firebox appliances is responsible for detecting and preventing exploit attempts against vulnerabilities in network-connected applications. This includes both client applications, like a web browser and server applications, like websites and self-hosted tools. In the second half of 2025, Firebox appliances with IPS enabled reported a moderate decrease in network attack volume globally. During this period, each Firebox saw an average of 845 detections, down slightly from the 1,181 detections per Firebox we saw in the first half of the year. Meanwhile, attackers continued to show the web is the battleground, with common web app flaws accounting for the overwhelming majority of the top detected threats.

Top 10 History

Signature	Type	Name	Affected OS	Percentage
1136822	Web threats	WEB dotCMS CMSFilter assets Access Control Weakness (CVE-2020-6754)	Network Device, Others	22.24%
1231780	Web threats	WEB HAProxy h1_headers_to_hdr_list Empty Header Name Access Control Bypass (CVE-2023-25725)	Network Device	10.10%
1056247	Exploits	SHELLCODE NOP Sled	All	8.92%
1059877	Exploits	WEB Directory Traversal -8	Windows, Linux, Freebsd, Solaris, Other Unix	6.08%
1230275	Web threats	WEB Apache log4j Remote Code Execution -2.h (CVE-2021-44228)	Windows, Linux, Freebsd, Other Unix	6.04%
1058468	Web threats	WEB SQL injection attempt -25.u	Windows, Linux, Freebsd, Solaris, Other Unix	5.75%
1055396	Web threats	WEB Cross-site Scripting -9	Windows, Linux, Freebsd, Solaris, Other Unix, Network Device	4.86%
1059958	Web threats	WEB Directory Traversal -27.u	Windows, Linux, Others	3.91%
1054837	Web threats	WEB Remote File Inclusion /etc/passwd	Windows, Linux, Freebsd, Solaris, Other Unix	2.99%
1138800	Web threats	WEB Microsoft Exchange Server Remote Code Execution Vulnerability -6 (CVE-2021-26855)	Windows	2.62%

Figure 9. Top 10 History

New Detections in the Top 50

While the top threats typically remain relatively unchanged throughout the year, when we look further down the list, things get more interesting. In the second half of 2025, three new IPS signature detections appeared in the top 50 by volume for the first time. The first new entry, 1132896, is a generic signature designed to catch common shellcode strings sent over a network connection. The second new detection, 1055529, prevents exploit attempts against a vulnerability in the popular Apache web server from 2012. The final new signature, 1136037, prevents exploit attempts against a serious vulnerability in the Telerik front-end web framework from 2017. We dive deeper into each of these signatures below.

New Detections in the Top 50

Signature	Type	Name	Affected OS	Rank
1132896	Exploits	WEB Remote Shell Command Execution -1	Linux, Freebsd, Solaris, Other Unix	19
1055529	Web threats	WEB Apache HTTPD mod_log_config Cookie Handling Denial of Service	Windows, Linux, Freebsd, Solaris, Other Unix, Mac OS, Others	20
1136037	Web threats	WEB Telerik UI For ASP.NET AJAX Arbitrary File Upload	Windows	21

Figure 10. New signatures this quarter among the top 50 signatures by volume.

Signature 1132896

This is a generic signature designed to catch common web shell code strings sent over a network connection. Generic signatures like this one help us to catch unknown threats by looking for common exploitation steps. Interestingly, nearly 40% of all detections were in the United States, with another 30% in Germany.

Signature 1055529

Back in 2012, Apache disclosed and patched CVE-2012-0021, a denial-of-service (DoS) vulnerability in the popular web server. This vulnerability was trivial to exploit, requiring only an empty HTTP cookie with no name and no value to crash the vulnerable web server. While most web servers can automatically recover from a crash, repeatedly sending a malicious request would effectively keep the server offline for the duration of the attack.

Nearly all detections (98%!) came from the United States, making this one of the more heavily skewed detections in terms of victim location. It's likely attackers were targeting a handful of potentially vulnerable systems and flooding them with malicious requests.

Signature 1136037

The final new signature prevents exploit attempts against two vulnerabilities, CVE-2017-11357 and CVE-2017-11317. This pair of CVEs was for an arbitrary file upload vulnerability in the Telerik UI library for ASP.NET. Telerik is a paid library for .NET web developers. ASP.NET applications are server-side programs, meaning the web server renders the page content and delivers it as HTML, JavaScript, and CSS to the visitor's browser. This is in comparison to modern web application frameworks like React, which operate as a single-page application (SPA), where the server delivers the entire website's logic to the visitor's browser at once and then loads data through API calls.

These file-upload vulnerabilities gave attackers a foothold on the web server by uploading arbitrary files to locations on the server. Attackers could exploit this vulnerability to gain code execution on the server by uploading their own ASP.NET file to a web-accessible location and then remotely executing it.

Most-Widespread Network Attacks

Signature	Name	Top 3 Countries by %			AMER %	EMEA %	APAC %
1136822	WEB dotCMS CMSFilter assets Access Control Weakness (CVE-2020-6754)	Germany 60.58	Brazil 36	Spain 14.63	12.91	35.02	9.62
1132896	WEB Remote Shell Command Execution -1	USA 49.25	Italy 43.7	France 32.84	38.83	23.54	10.26
1059877	WEB Directory Traversal -8	Germany 25.96	Portugal 22.06	Italy 20.08	11.78	19.57	22.44
1231780	WEB HAProxy h1_headers_to_hdr_list Empty Header Name Access Control Bypass (CVE-2023-25725)	United Kingdom 31.99	USA 20.48	Canada 18.33	19.16	14.09	20.51
1132381	WEB-CLIENT Javascript Obfuscation in Exploit Kits - 44 (Possible Exploit Kit)	USA 41.42	United Kingdom 12.59	Brazil 10.4	31.86	9.22	13.46

Figure 11. Top 5 Most-Widespread Network Attacks

While the top network attacks by volume show us which vulnerabilities attackers are targeting with the most force, the most widespread network attacks show us the vulnerabilities under attack on the most individual networks worldwide. Four of the most widespread network attacks were returnees from earlier in the year, with signature 1132896 (Web Remote Shell Command Execution -1) as the only new addition. We already discussed this signature in the previous section, which highlighted new detections showing up in our Top 50 by Volume list for the first time ever. Despite being a new addition to our feed, a significant number of networks in the Americas and Europe had detections for this signature. Particularly, 49% of Fireboxes in the US had at least one detection in the second half of the year, as did 43% of Fireboxes in Italy and 33% in France. It's clear that web shells were a popular technique for threat actors at the end of 2025.

The #4 most widespread attack in Q2 was the big surprise: a brand-new signature (ID 1132381) for WEB-CLIENT JavaScript Obfuscation in Exploit Kits. This detection, added in the latest signature set, had never appeared in our top 50 before, yet it suddenly showed up on Fireboxes all over the world, making it the fourth most ubiquitous attack this quarter. We suspect this signature is catching malicious obfuscated JavaScript commonly used by exploit kits or malvertising campaigns. The fact that it registered on so many Fireboxes (e.g. over 32% of Fireboxes in the Americas and 43% in the United States specifically saw it at least once) despite not generating a high volume per device illustrates a broad but low-frequency campaign – perhaps drive-by browser attacks or mass advertising payloads that touched many networks without heavily targeting any single one.

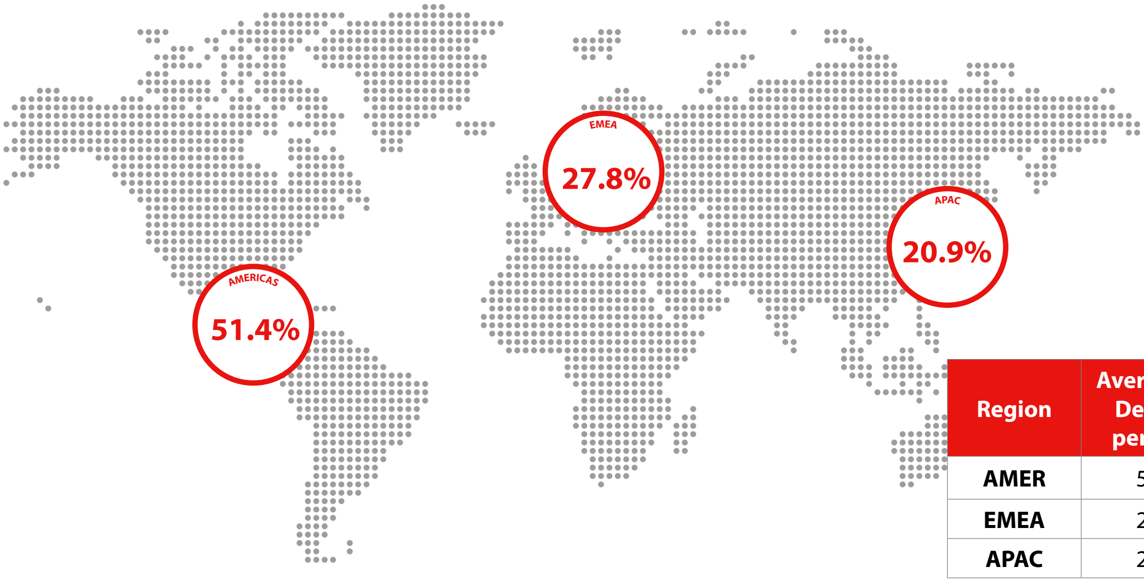
This is a classic example of an attack that is widespread but not volumetric. It's an anomaly worth highlighting: defenders might not notice it by volume, but its wide reach means many organizations were probed. For SMBs, this is a reminder that even if an exploit attempt against your systems is blocked only once, the same attempt may be occurring across thousands of other networks globally. A new threat technique can achieve extensive coverage very quickly via automated kits.

Finally, the #5 most-widespread attack was CVE-2023-25725 (HAProxy HTTP/2 Header Bypass), the same as last quarter's fifth place. It remained widely seen, especially in APAC and Americas (with around 16–21% of Fireboxes logging it). This persistence shows attackers are still actively seeking out unpatched HAProxy instances in SMB environments to exploit the access control bypass. Notably, one formerly widespread threat, the Exchange ProxyLogon exploit, dropped out of the top five this quarter (it was in Q1's widespread list but fell in Q2). Its place was taken by the aforementioned new exploit kit signature. This suggests a possible shift in attacker focus away from Exchange (perhaps as more systems got patched or attackers moved on) and toward front-door attacks on end users via web content.

Overall, the widespread attacks data reinforces that older vulnerabilities in ubiquitous software (browsers, web frameworks, open-source tools) continue to be leveraged broadly. Even as new exploits arise, adversaries often stick with "tried-and-true" methods that yield a broad reach. For SMB defenders, focusing on these widely targeted weaknesses – ensuring browsers are updated, and web servers and VPN devices are patched, and using defenses like URL filtering and script blocking – can provide outsized protection given how common these attack attempts are.

Network Attacks by Region

The spread of network attacks, when compared to H1, remained relatively unchanged. The Americas (AMER) accounted for slightly more than half of the total attack volume, in line with the number of reporting devices in the region. Europe, the Middle East, and Africa (EMEA) came in a distant second with 28% of the attack volume, with Asia and the Pacific (APAC) making up the remaining 21%.



Region	Average % IPS Detections per Firebox
AMER	51.35%
EMEA	27.79%
APAC	20.85%

Figure 12. Average Detections per Firebox by Region

Conclusion

Attackers showed interest in both old and new during the second half of 2025, targeting vulnerabilities from more than a decade ago alongside more recent issues like Log4Shell and Exchange ProxyLogon. While adversaries went after plenty of application-specific issues, the bulk of the top detections came from generic signatures designed to catch classes of vulnerabilities. Despite decades of awareness, training, and testing capabilities, common flaws remain a mainstay in modern web applications. As more of our workloads move to web applications (both self-hosted and Software-as-a-Service), the need for strong security controls, like IPS, increases.

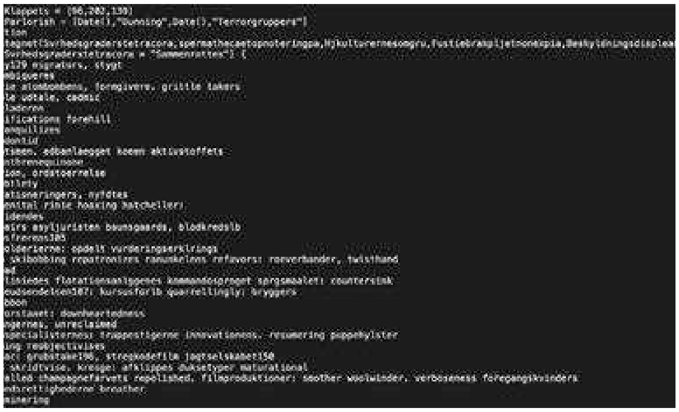
DNS ANALYSIS

Most modern attacks are reliant on DNS in at least one of their stages. Phishing links, botnet command and control, malware download servers – all of these rely on DNS to translate a malicious domain into an IP address to connect to. This makes DNS firewalling tools like DNSWatch a perfect control to stop attacks early. In previous reports, we looked at the top 10 malicious domains in specific categories. This time around, we're taking a different approach by diving deeper and pulling out trends that span multiple malicious domains for the period. We highlight those trends below.

Remcos

From the end of September through the beginning of October, we saw the domain malverneng[.]top hosting a malicious PowerShell script that acted as a stager for downloading the Remcos Malware-as-a-Service remote access trojan (RAT). These attacks typically started with a phishing email containing a malicious attachment.

For example, in one attack, the phishing email contained an attachment purporting to be an invoice from a popular air compressor manufacturer. The filename ended with _DOCX.js, making it look like a Word document despite being a JavaScript file. The JavaScript was highly obfuscated, including long blocks of random words likely designed to throw off automated analysis tools, as well as a block of base64 text to trick signature-based tools into allowlisting it as benign.



```
Klappets = [96,202,139]
Parlorish = [Date(),"Dunning",Date(),"Terrorgruppers"]
tion
tegnet(Svrhedsgraderstetracora,spermathecaetopnoteringpa,Hjkulturernesomgru,fustiebrampljetnonexpia,Beskyldningsdisplea
Svrhedsgraderstetracora = "Sammenrotter"] {
y129 migrators, stygt
mbiqueres
ie alomdombens, formgivere, grittle takers
le udtale, cadmic
ladrren
ifications forehill
enquilizes
dontid
timen, edbanlaegget koenn aktivstoffets
nthrenequinone
ion, ordstoerrelse
bility
atisneringers, nyfdtes
enital rinie hoaxing hatchellers
idendes
airs asyljuristen baunsgaards, blodkredslb
nfreregn305
olderierne: opdelt vurderingserklrings
 skibobbing repatroniers ranunkelens refavors: ronverhander, twisthand
ed
linieders flotationsanlggenes kommandosproget sprgsmaalet: countersink
oudsendelsen107; kursusforlb quarrellingly: bryggers
boon
orslaaet: downheartedness
ngernes, unreclaimed
specialisternes: trappestigerne innovationens, resumering puppehylster
ing reobjectivises
aci grubstake196, stregkodefilm jagtselskabet150
 skridtvise, kreoge: afklippes duksetyper maturational
alled champagnefarvets repolished, filmproduktioner: smother woolwinder, verboseness foregangskvinders
ndsrettighederne breather
minering
```

Figure 13. Remcos

When executed, the JavaScript downloads an encrypted second stage from malverneng[.]top, saves it locally, then decrypts it and launches it with PowerShell. This PowerShell script is solely responsible for downloading and executing the Remcos malware payload.

RedLine Stealer

In the second half of 2025, we saw Redline Stealer as a popular threat with short-lived campaigns. For example, sms-szfang[.]com showed up on October 9th and quickly generated 2,445 detections across WatchGuard DNSWatch customers, primarily in Japan. This domain hosted the second-stage payload for RedLine Stealer attacks. These attacks usually started with a fake software update hosted at another location, which in turn downloaded the actual RedLine malware from sms-szfang[.]com.

RedLine Stealer is a Malware-as-a-Service threat that, as the name suggests, steals sensitive information from the compromised Windows system where it runs. When it runs on a victim's machine, it grabs any credentials saved in their web browsers, cookies for visited websites, cryptocurrency wallets, and generic system information to determine the victim's identity. It includes capabilities to load other malware payloads, making it a popular choice for initial access brokers.

The filenames in these campaigns were almost entirely in Japanese, suggesting either direct targeted attacks or regional watering-hole attacks.

Takeaways

Commoditized malware has become the standard for many modern attacks. Threat actors no longer need software development and systems administration skills to create and distribute malware. Instead, they can hop on the dark web and license access to highly evasive malware with no more difficulty than signing up for a ChatGPT subscription. As the barriers for entry are lowered, the volume of potential threat actors increases. Paired with the emergence of automated, agentic AI-powered attacks, organizations need to be prepared to defend against increasingly frequent attacks.

FIREBOX FEED: DEFENSE LEARNINGS

In the second half of 2025, we continued to see attackers rely on scale, encryption, and user interaction to bypass traditional perimeter defenses. Encrypted malware delivery, exploits against exposed web applications, and script-based payloads delivered as email attachments all featured prominently across observed detections. These techniques are not novel, but their reliability makes them persistent. The following defensive practices remain among the most effective ways to reduce risk against these common attack paths.

01 Inspect Encrypted Traffic to Stop Malware Earlier

A majority of malware observed at the network perimeter in the second half of the year was delivered over HTTPS. Encryption protects our data as we browse the web, but it also shields malicious payloads from inspection when security teams allow encrypted traffic to pass unchecked. Without HTTPS inspection, perimeter defenses are limited to inspecting destination metadata rather than actual content, leaving organizations blind to the malware itself.

Enabling HTTPS inspection on perimeter network firewalls allows anti-malware and intrusion prevention engines to evaluate encrypted traffic before it reaches users. While certificate management has historically been a barrier to adoption, modern security platforms like the Firebox increasingly simplify deployment and management, making encrypted traffic inspection a practical and high-impact control.

02 Keep Internet-Facing Web Applications Fully Updated

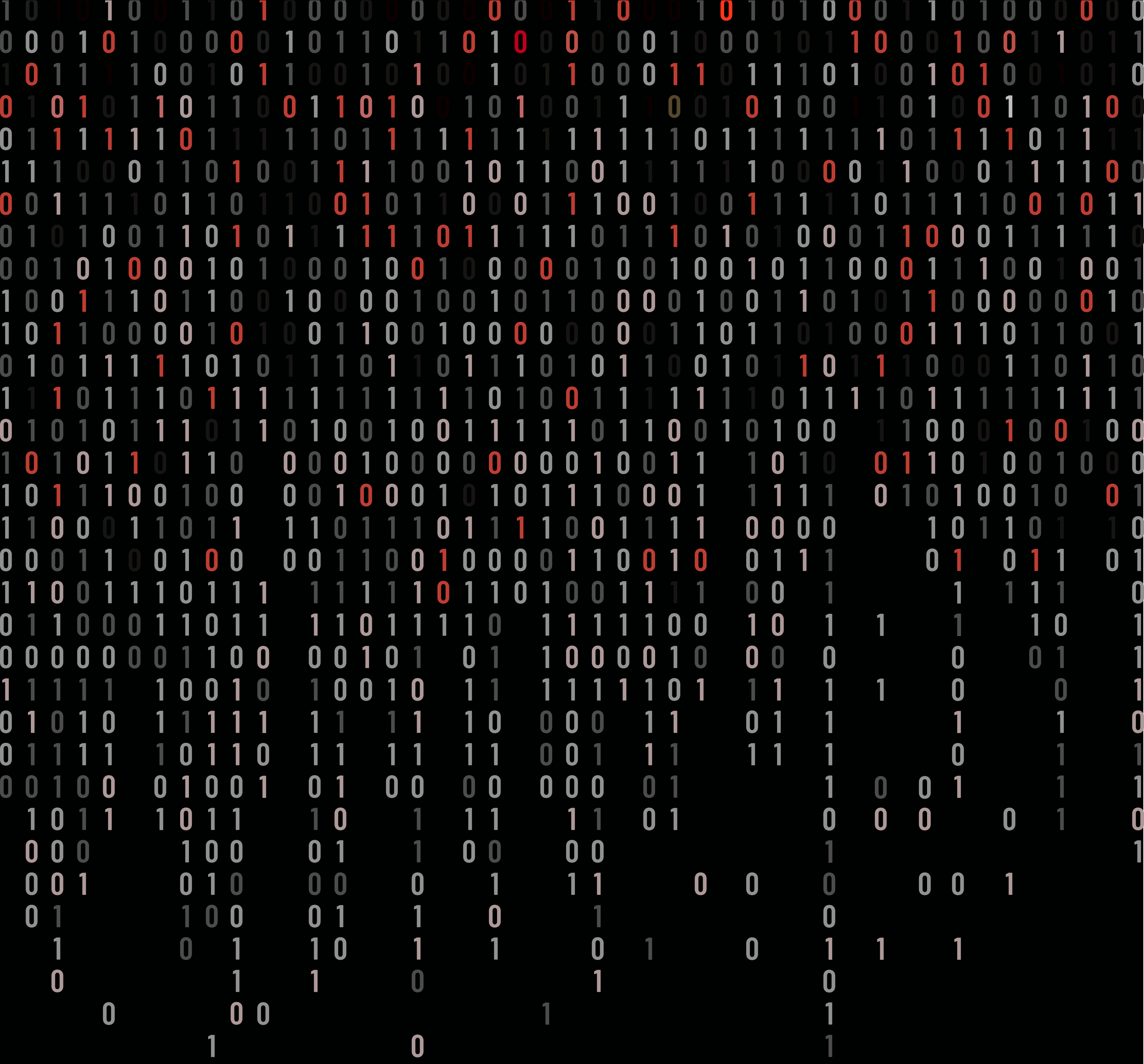
Attackers continue to favor both known vulnerabilities and common flaw exploits targeting exposed web applications. In the second half of the year, threat actors heavily targeted vulnerabilities that have had mitigations available for years. These attacks succeed not because the vulnerabilities are unknown, but because patching is delayed or visibility just isn't there.

Organizations should treat web application updates as a security priority, not just a maintenance task. This includes maintaining visibility into third-party components and dependencies and ensuring that vulnerability disclosures translate quickly into remediation actions. Reducing patch latency on Internet-facing services significantly lowers the likelihood of opportunistic compromise.

03 Block JavaScript in Email Attachments, Including Inside ZIP Files

Script-based malware delivered through email remains one of the most reliable initial access techniques for attackers. During the second half of the year, threat actors used JavaScript attachments with benign-looking filenames to kick off living-off-the-land attacks.

There is generally no reason to accept JavaScript attachments over email. Security controls should explicitly block or quarantine JavaScript email attachments, regardless of whether they are delivered as stand-alone files or packaged within compressed archives. Email security solutions must also unpack and inspect archive contents rather than relying solely on the outer file type. Preventing script execution at the email gateway eliminates an entire class of high-success social engineering attacks before users ever interact with them.



ENDPOINT THREAT TRENDS

Endpoints are physical and virtual devices where humans interface with computer networks. These include traditional desktops, laptops, smartphones, and servers, as well as virtual machines, IoT devices, and even APIs. If you can interface with it, it's an endpoint. WatchGuard protects compatible endpoints with Endpoint Protection, Detection, and Response (EPDR), and does exactly what the name implies – protects by detecting and responding to threats in real time. This section uses data derived from EPDR, provided that the system owner enables anonymous aggregate data sharing with us. Therefore, this data is a reliable sample of all EPDR-protected systems.

The structure and flow of the endpoint section are typically based on data from any given quarter. Since this iteration of the Internet Security Report includes both Q3 and Q4, we've altered some sections into full annual portrayals instead of distinct quarter-to-quarter contrasts as usual. This approach keeps this lengthy section as concise as possible without omitting important data points.

Speaking of omitting data points, we were unable to obtain both Q3 and Q4 threat hunting data due to backend changes. We expect to have this data again in the quarters ahead. However, due to the missing data, we've excluded the threat hunting section in its entirety. We've also removed the inactive ransomware groups data point because groups come and go so often that this data could become outdated by the time it is published. So, we are only including the newly discovered groups going forward. Meanwhile, we've improved some tables and charts for better readability.

Here is the coverage for this quarter:

- Total malware threats
- New malware threats per 100k active machines
- The number of alerts by the number of machines affected
- The number of alerts by which WatchGuard technology invoked the alert
- The top 30 affected countries each quarter
- The top 10 most-prevalent malware
- The top 10 most-prevalent potentially unwanted programs (PUPs)
- Attack vectors
- Alerts by exploit type
- Cryptominer detections
- Ransomware detections (WatchGuard)
- Ransomware double extortion landscape
- Notable ransomware events

MALWARE FREQUENCY

Malware Frequency is split into two parts: Total Malware Threats and New Threats. Total Malware Threats is the raw number of blocks for a unique threat. More specifically, it's the total number of unique hashes blocked. This means that if the same payload is sent to hundreds or thousands of users, and all of them are blocked, that counts as one block because it's only one unique payload. Contrarily, if for example, a polymorphic worm that alters its code subtlety with each unique system it touches is blocked, each unique iteration of that worm counts as a block.

The other side of Malware Frequency is brand new malware hashes we've not seen before, denoted as New Threats. We skew this number to be represented in terms of a typical large organization – 100,000 active machines – because it's more easily digestible. A malware hash can be counted for both Total Malware Threats and New Threats. In fact, New Threats is a subset of Total Malware Threats; the filter being if we've previously recorded the hash in our database prior to seeing it over a given timeframe.

As discussed, we've combined much of the Q3 and Q4 data into annual composites as we typically do with Q4. Every quarter in 2025 saw an increase in new threats from the quarter prior. Relatively speaking, Q1 to Q2 and Q2 to Q3 saw slight-to-modest increases of 26.15% and 20.73% respectively. However, Q3 to Q4 puts things in more perspective. The total number of new threats increased 1548.48%, over 15 times from Q3 to Q4!

New Malware Threats Per 100k Active Machines

Q1	Q2	Q3	Q4
65	82	99	1,632

Figure 14. QoQ New Malware Threats Per 100k Active Machines

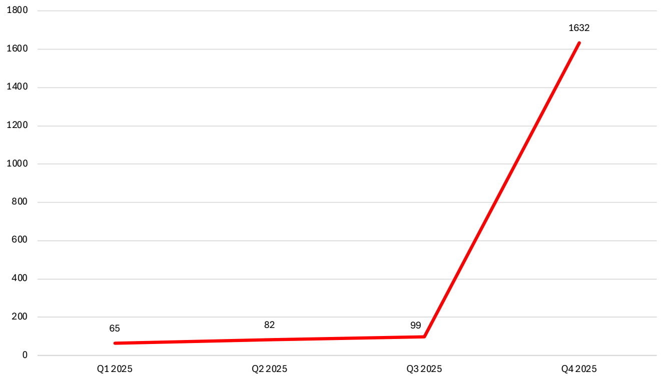


Figure 15. QoQ New Malware Threats Per 100k Active Machines (Graph)

Usually, there is a correlation later in the data that better explains a sudden surge like this, but there's nothing that immediately sticks out. From Q3 to Q4, the Total Malware Threats decrease; there exists no spike or drop in alert composition for subsequent sections like Number of Machines Affected and Alerts by Different Technologies; there are no geographical anomalies; no malware in the top 10 with many blocks, nothing. This leaves the most logical possibility: we observed many diverse malware hashes we haven't seen before, and we blocked them.

QoQ Total Malware Threats Table

Q1	Q2	Q3	Q4
29,127	28,178	29,348	25,326

Figure 16. QoQ Total Malware Threats

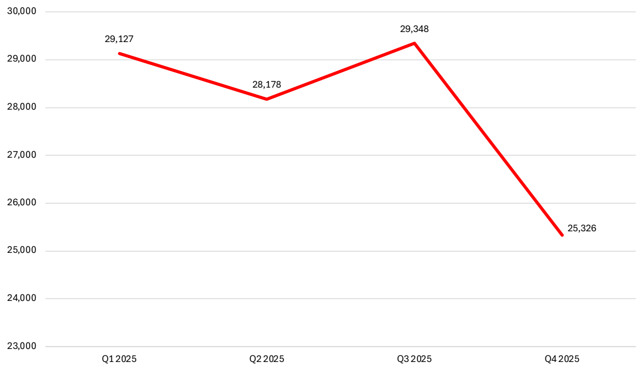


Figure 17. QoQ Total Malware Threats

Seeing a sharp increase in new malware threats would leave one to assume the total malware threats would increase in tandem. This isn't the case here. Not only did the total number of threats move inversely to the new threats, but it also decreased a relatively large amount, down a little under 14% (-13.70%). Whereas the rest of 2025 remained stagnant. In lay terms, we blocked slightly fewer threats towards the end of 2025, but of those threats, many were unique hashes we haven't seen before. This leads us to conclude that more malware is being blocked at the network level before it reaches endpoints, and the never-before-seen malware that slips through is increasingly blocked.

Alerts by Number of Machines Affected

The data covered in Alerts by Number of Machines Affected subsection is self-explanatory. We gather all alerts (blocks) and filter them by the number of machines on which each malware hash appeared. For example, if a JavaScript script that downloads additional malware is blocked on one machine and that hash is subsequently blocked on three other machines throughout the quarter, that would be four alerts (1+3).

We then normalize these alerts into five different schemas, as defined below:

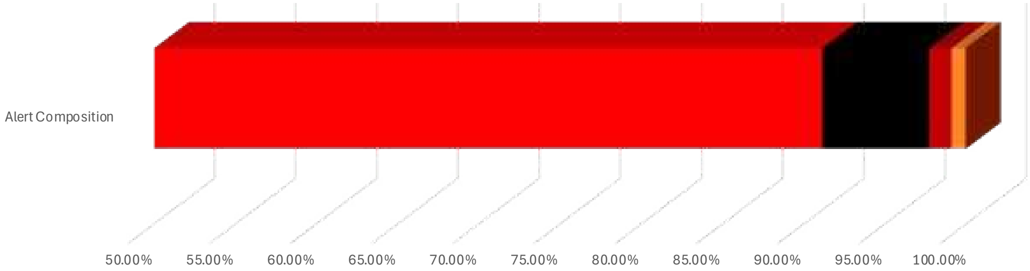
- **1** – Exactly one machine alerted on this file/process.
- **>=2 & < 5** – Between two and five machines alerted on this file/process.
- **>=5 & < 10** – Between five and ten machines alerted on this file/process.
- **>=10 & < 50** – Between ten and fifty machines alerted on this file/process.
- **>=50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

Typically, there's not much swing in the differing alert compositions from quarter to quarter. Alerts appearing on only one machine are the norm. That's because most malware is for one-time use or is specially crafted for each potential victim, and this trend is increasing as AI LLMs are able to produce code snippets spontaneously. This data point is more associated with the threat actor's goal. Malware threats appearing on, for example, more than 100 machines are almost always campaigns that spam email attachments or drive-by downloads on compromised websites, and so on. Malware threats appearing on one machine are more targeted towards a specific system.

We've kept both tables and graphs for Q3 and Q4 and included the quarter-to-quarter differences, as usual. The data is somewhat inverted from Q2 to Q3 and Q3 to Q4. Alerts on only one machine increased from Q2 to Q3, and that flipped in the last two quarters of the year, resulting in a wash overall. The end results are about the same: about 90% of all threats appear on only one machine, and the rest appear on a handful of machines (between two and five).

Number of Machines	Q2 Alert Comp.	Q3 Alert Comp.	% Diff from Q2
1	88.19%	91.13%	2.94%
>= 2 & < 5	9.18%	6.58%	-2.59%
>= 5 & < 10	1.59%	1.38%	-0.21%
>= 10 & < 50	0.89%	0.78%	-0.11%
>= 50 & < 100	0.09%	0.06%	-0.02%
>=100	0.08%	0.07%	-0.01%

Figure 18. Q2 to Q3 Alerts by Number of Machines Affected

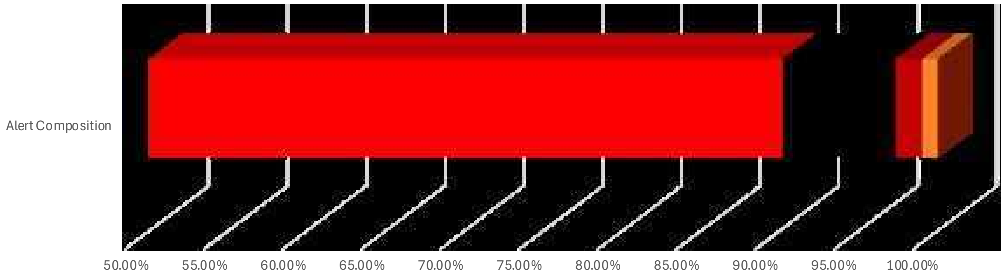


	Alert Composition
🟥 1	91.13%
⬛ >= 2 & < 5	6.58%
🟥 >= 5 & < 10	1.38%
🟧 >= 10 & < 50	0.78%
🟨 >= 50 & < 100	0.06%
🟫 >=100	0.07%

Figure 19. Q2 to Q3 Alerts by Number of Machines Affected (Graph)

Number of Machines	Q3 Alert Comp.	Q4 Alert Comp.	% Diff from Q3
1	91.13%	90.10%	-1.02%
>= 2 & < 5	6.58%	7.18%	0.60%
>= 5 & < 10	1.38%	1.67%	0.30%
>= 10 & < 50	0.78%	0.89%	0.11%
>= 50 & < 100	0.06%	0.08%	0.02%
>=100	0.07%	0.07%	0.00%

Figure 20. Q3 to Q4 Alerts by Number of Machines Affected



	Alert Composition
🟥 1	90.10%
⬛ >= 2 & < 5	7.18%
🟥 >= 5 & < 10	1.67%
🟧 >= 10 & < 50	0.89%
🟨 >= 50 & < 100	0.08%
🟫 >=100	0.07%

Figure 21. Q3 to Q4 Alerts by Number of Machines Affected (Graph)

When considering the entire year of 2025, from Q1 to Q4, there's a difficult-to-discern shift from alerts appearing on the bottom half of the table to the top half of the table. In other words, there's a slight increase in threats appearing on fewer machines; attacks are becoming more targeted. If attackers can create code more easily (as we touched on with AI LLMs section), then they can more easily craft them towards specific targets.

Number of Machines	Q1 Alert Comp	Q2 Alert Comp	Q3 Alert Comp	Q4 Alert Comp
1	88.99%	88.19%	91.13%	90.10%
>= 2 & < 5	7.82%	9.18%	6.58%	7.18%
>= 5 & < 10	1.81%	1.59%	1.38%	1.67%
>= 10 & < 50	1.15%	0.89%	0.78%	0.89%
>= 50 & < 100	0.13%	0.09%	0.06%	0.08%
>=100	0.10%	0.08%	0.07%	0.07%

Figure 22. QoQ Alerts by Number of Machines Affected

Defense in Depth

A quick checkpoint: From Q1 to Q3 in 2025, most of the data shows slight increases or decreases here and there, but Q4 altered that trend. The total number of threats decreased while the number of new threats exploded. Of those threats, 90% consistently appear on only one machine, and there appears to be a trend towards more targeted attacks, based on the data alone. This subsection then describes the technologies within EPDR that work in synergy to block these threats if they were to bypass network firewalls and other countermeasures. There are six primary technologies, and they are:

Endpoint Technologies

1. **Endpoint Detection** – The typical legacy endpoint antivirus solution, endpoint detection displays the number of hashes invoking an alert located in our known-malicious hash database. This is commonly called a signature-based detection antivirus solution.
2. **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.
3. **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.
4. **Digital Signature** – Digital signatures are methods of determining the authenticity and legitimacy of the sending user and ensuring it has not 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.
5. **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 appears suspicious, one of WatchGuard's attestation analysts performs the analysis and assigns a classification. Once a file reaches this stage, a classification, whether goodware, PUP, or malware, is always determined.
6. **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.

For the Defense in Depth section, we've included both Q3 and Q4 data as we did with the Alerts by Number of Machines Affected subsection. The notable changes from Q2 to Q3 were the shift in cloud detections and away from defined rules and manual attestation, but only slightly. Conversely, Q3 to Q4 saw a modest move away from cloud-based detections and back to manual attestation. Although there were some increases in machine-learning detections. Interestingly, the Defined Rules category slipped down even further, only accounting for 7.72% of all detections in Q4.

That leaves us with a quarter-over-quarter overview of different technologies and how they detect and block threats on endpoints. There is one technology that tells the story here: defined rules. From the beginning of the year to the end, the number of detections for defined rules has slipped significantly. Those threats are increasingly being detected by machine learning, cloud, and manual attestation. Basically, all the static-analysis-focused tools are catching less, and endpoint detection is more reliant on dynamic analysis, including manual analysis from analysts within WatchGuard's attestation service. This indicates that threats are becoming more complex. So, all in all, we're seeing less overall malware, but the malware we are seeing is increasingly complex and unique.

Technology	Q2 Alert Comp	Q3 Alert Comp	Difference From Q2
AD360 Endpoint Detection	4.66%	3.97%	-0.68%
Defined Rules	13.43%	9.80%	-3.63%
Digital Signature	1.92%	1.69%	-0.23%
Behavioral/Machine Learning	39.05%	39.64%	0.59%
Cloud	19.20%	25.35%	6.15%
Manual Attestation	21.74%	19.54%	-2.20%

Figure 23. Q2 to Q3 Alerts by Technology

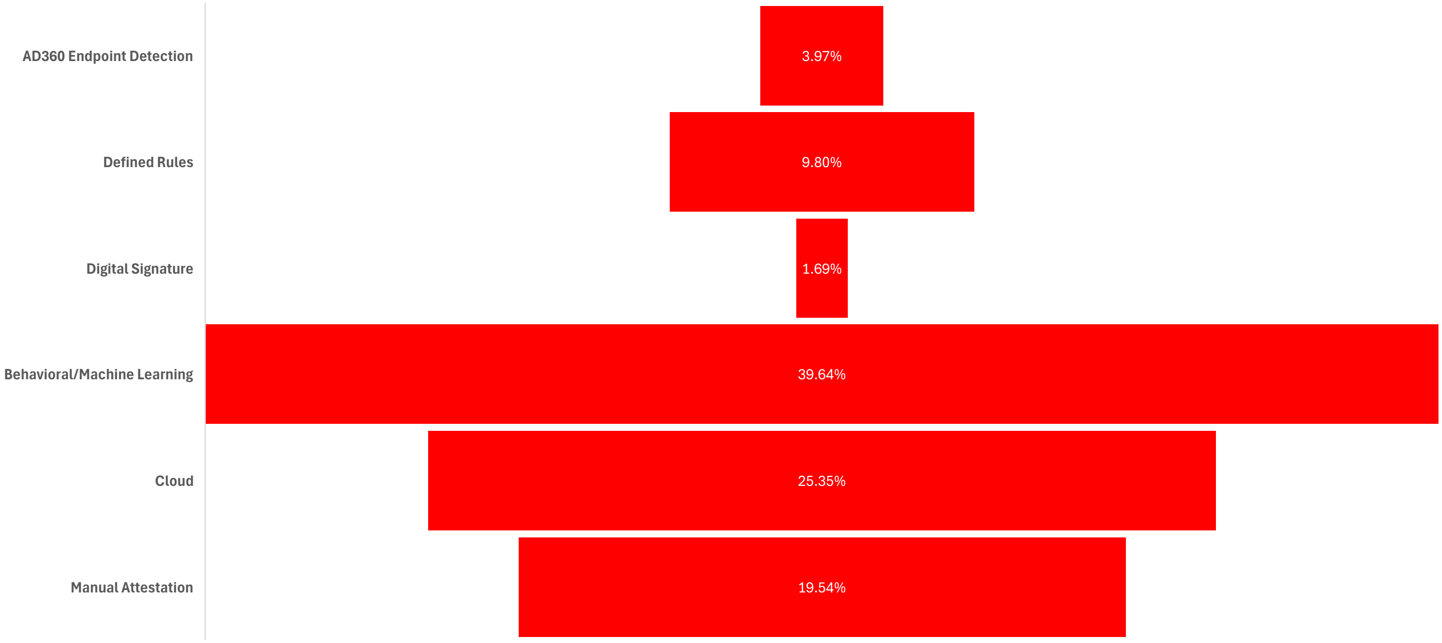


Figure 24. Q2 to Q3 Alerts by Technology (Graph)

Technology	Q3 Alert Comp	Q4 Alert Comp	Difference From Q3
AD360 Endpoint Detection	3.97%	3.77%	-0.20%
Defined Rules	9.80%	7.72%	-2.08%
Digital Signature	1.69%	2.24%	0.54%
Behavioral/Machine Learning	39.64%	42.63%	2.98%
Cloud	25.35%	20.81%	-4.54%
Manual Attestation	19.54%	22.84%	3.30%

Figure 25. Q2 to Q3 Alerts by Technology

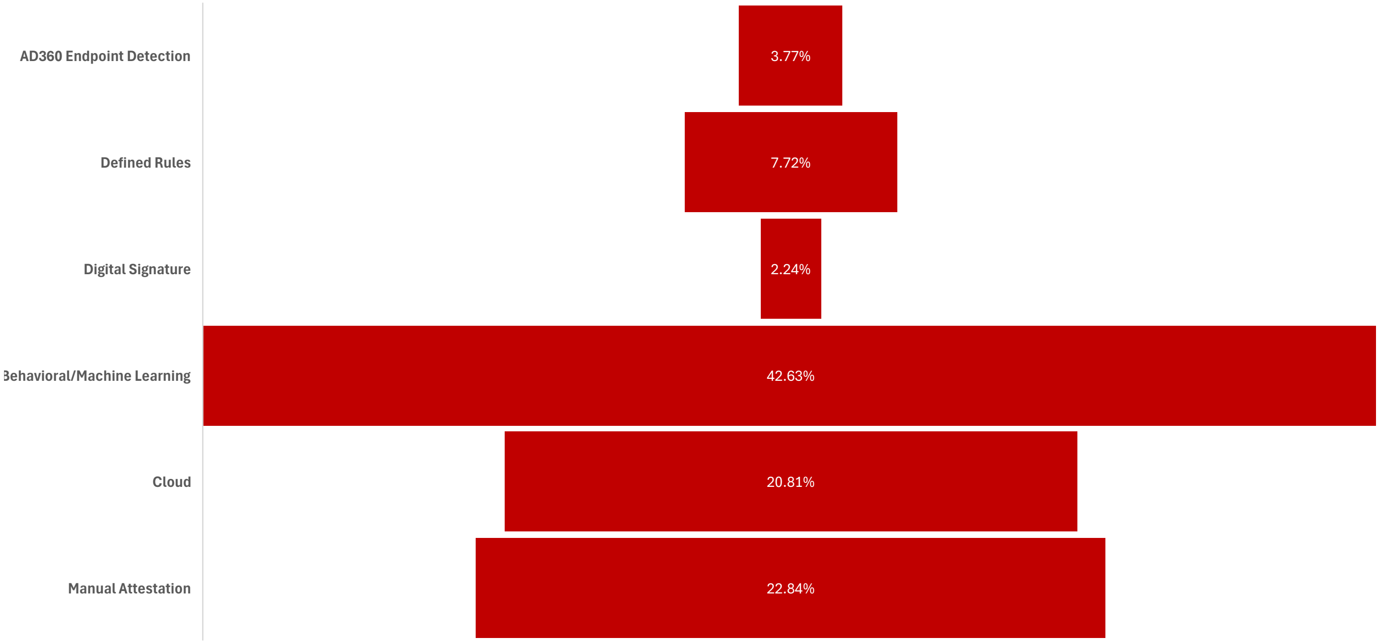


Figure 26. Q3 to Q4 Alerts by Technology (Graph)

Technology	Q1 Alert Comp	Q2 Alert Comp	Q3 Alert Comp	Q4 Alert Comp
AD360 Endpoint Detection	3.22%	4.66%	3.97%	3.77%
Defined Rules	17.09%	13.43%	9.80%	7.72%
Digital Signature	2.63%	1.92%	1.69%	2.24%
Behavioral/Machine Learning	36.45%	39.05%	39.64%	42.63%
Cloud	19.12%	19.20%	25.35%	20.81%
Manual Attestation	21.49%	21.74%	19.54%	22.84%

Figure 27. QoQ Alerts by Technology

Alerts by Top 30 Countries Affected

Most threat actors are opportunists in that they tend to target the path of least resistance, meaning that they target systems that are insecure. A small percentage of threat actors target specific industry sectors or even individuals, and occasionally, will target certain countries or regions. For example, geopolitical events such as wars or conflicts tend to increase cyberattacks against everyone involved. This subsection shows the data we have for systems in each country. However, there are a few caveats for this data.

First and foremost, this is a subset of all EPDR-protected systems, as this data comes from those users who explicitly opt in. For example, if a country has relatively fewer users and the users that do opt in happen to be those with riskier user behaviors, that could incorrectly alter the actual Alert Coefficient (AC). The AC is a simple formula to help subdue this skew by using a ratio of malware alerts to active machines. This solves the issue of whether a country has significantly more machines than another one; the numbers are normalized.

Here is the Alert Coefficient (AC) ratio formula:

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

The focus on these data points tend to center around the top countries in the list and geographical regions. For example, the highest ACs for Q3 and Q4, and throughout all 2025 for that matter, hovered around 0.5, excluding Q2, which topped 0.25. In Q3, Malaysia, Brazil, and South Africa all had ACs of 0.5 and above, meaning there were, on average, one alert for every two active machines. Regionally, these countries are nowhere near each other. So, there's no geographical correlation we can draw from Q3. However, the top country in Q4 was the Philippines with an AC of 0.5. The top countries in Q3 and Q4 were in Southeast Asia. We've posted all four maps from each quarter to show the visual geographical differences, which typically reside in South America, Africa, and Asia.

Q1		Q2		Q3		Q4	
Country	AC	Country	AC	Country	AC	Country	AC
São Tomé and Príncipe	0.5	Egypt	0.25	Malaysia	0.56	Philippines	0.5
Laos	0.41	São Tomé and Príncipe	0.25	Brazil	0.55	Madagascar	0.25
Morocco	0.32	Grenada	0.2	South Africa	0.5	Laos	0.12
Cuba	0.25	Laos	0.17	Thailand	0.33	Morocco	0.07
Zimbabwe	0.14	China	0.11	Indonesia	0.18	Pakistan	0.05
China	0.11	Trinidad and Tobago	0.08	Venezuela	0.11	Vietnam	0.05
Angola	0.08	Armenia	0.07	Turkey	0.06	Bolivia	0.05
Pakistan	0.07	Zimbabwe	0.06	Paraguay	0.06	Mozambique	0.04
Bangladesh	0.06	Tajikistan	0.05	Zimbabwe	0.05	Andorra	0.04
India	0.06	Bangladesh	0.05	Bolivia	0.05	Angola	0.03
Tajikistan	0.05	Singapore	0.04	Bangladesh	0.04	Bangladesh	0.03
Paraguay	0.05	Paraguay	0.04	Botswana	0.04	Singapore	0.03
Nigeria	0.04	Pakistan	0.04	Panama	0.03	Nigeria	0.03
Bolivia	0.04	Nigeria	0.04	Singapore	0.03	Kenya	0.02
Turkey	0.04	Bosnia and Herzegovina	0.03	Nigeria	0.03	Turkey	0.02
Armenia	0.04	Bolivia	0.03	Laos	0.03	Thailand	0.02
Panama	0.03	Panama	0.03	Trinidad and Tobago	0.03	Paraguay	0.02
Dominican Republic	0.03	Turkey	0.03	Kenya	0.03	Macedonia	0.02
Indonesia	0.03	Kenya	0.02	Pakistan	0.03	Malaysia	0.02
Singapore	0.03	Indonesia	0.02	Ghana	0.03	Tajikistan	0.02
Trinidad and Tobago	0.03	Guatemala	0.02	United Arab Emirates	0.02	Panama	0.02
Thailand	0.02	Angola	0.02	Guatemala	0.02	Indonesia	0.02
Malaysia	0.02	Malaysia	0.02	Vietnam	0.02	Botswana	0.02
Botswana	0.02	South Africa	0.02	Egypt	0.02	South Africa	0.02
Bulgaria	0.02	Dominican Republic	0.02	Phillippines	0.02	Brazil	0.01
Venezuela	0.02	Botswana	0.02	China	0.02	Luxembourg	0.01
Kenya	0.02	Uruguay	0.02	Tajikistan	0.02	Serbia	0.01
Ghana	0.02	Thailand	0.02	Swaziland	0.01	Venezuela	0.01
Andorra	0.02	Venezuela	0.01	São Tomé and Príncipe	0.01	Zimbabwe	0.01
Colombia	0.01	Macedonia	0.01	Madagascar	0.01	Uruguay	0.01

Figure 28. 2025 QoQ Alerts by Top 30 Countries Affected

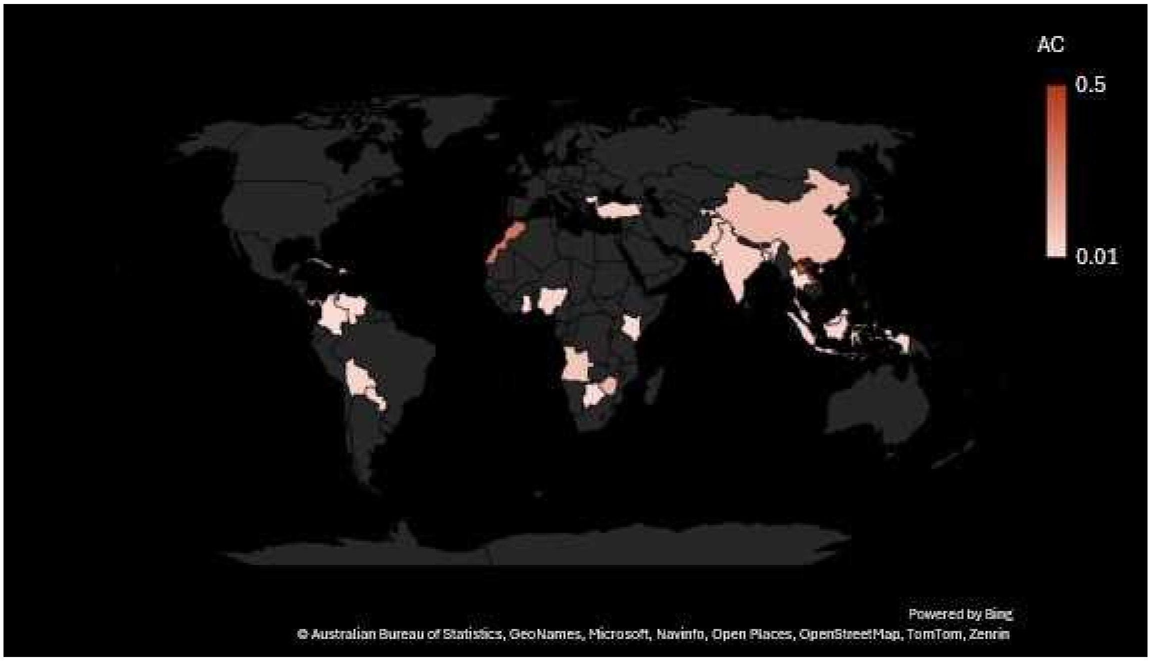

AC
0.5
0.01
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Figure 29. Q1 Alerts by Top 30 Countries Affected).

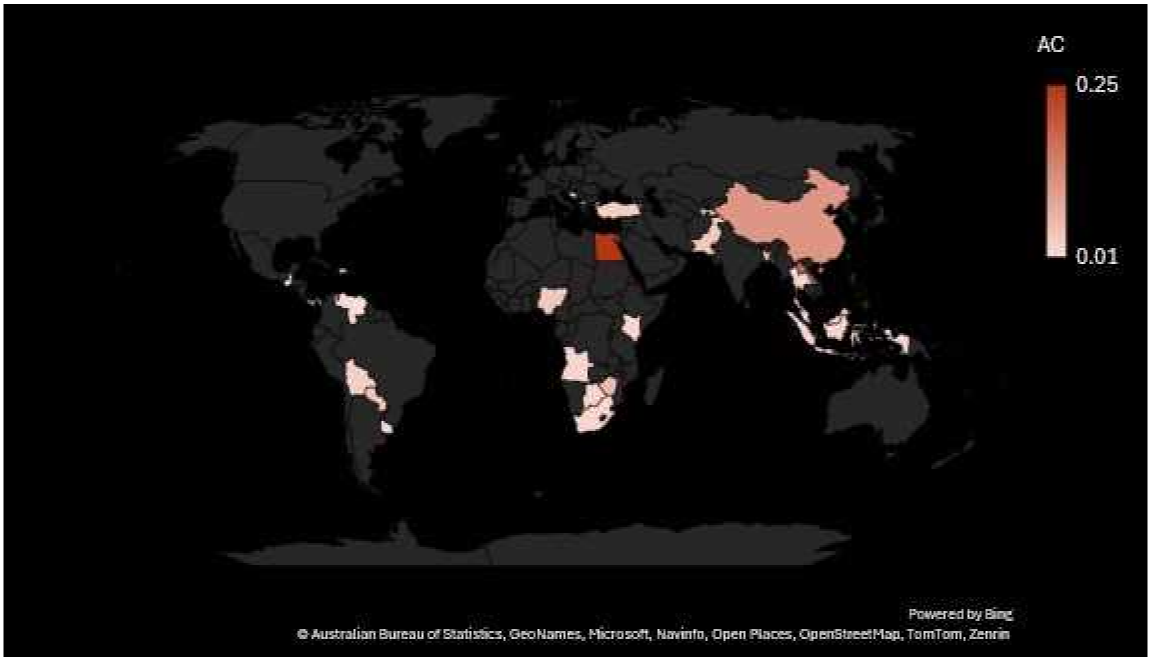

AC
0.25
0.01
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Figure 30. Q2 Alerts by Top 30 Countries Affected).

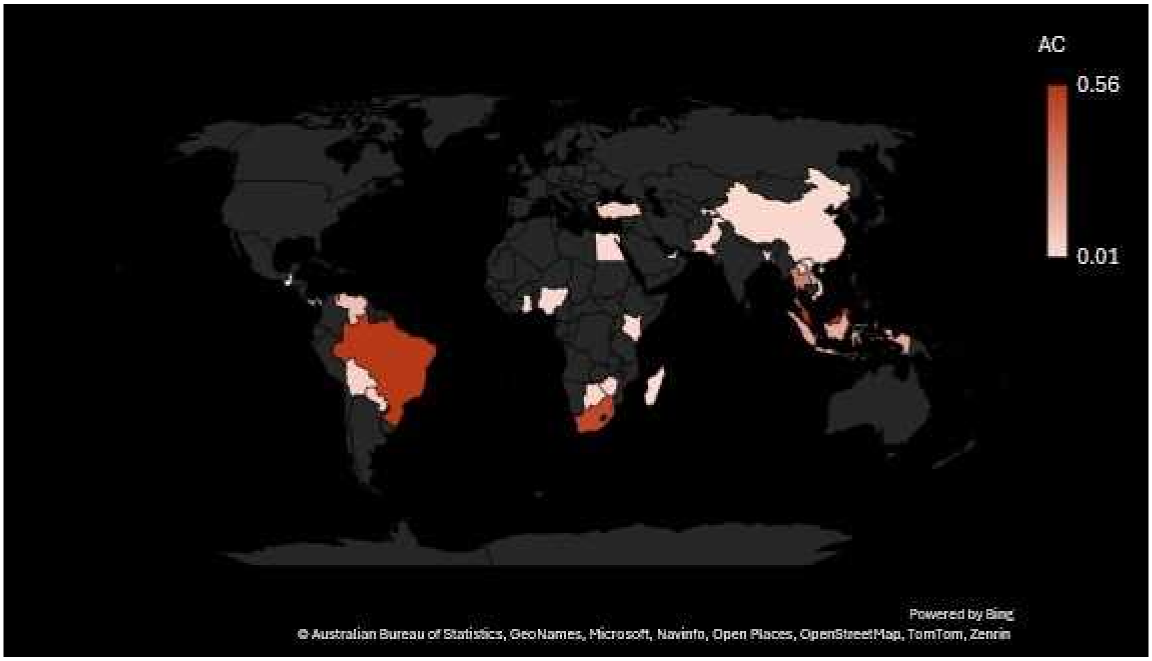

AC
0.56
0.01
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Figure 31. Q3 Alerts by Top 30 Countries Affected).

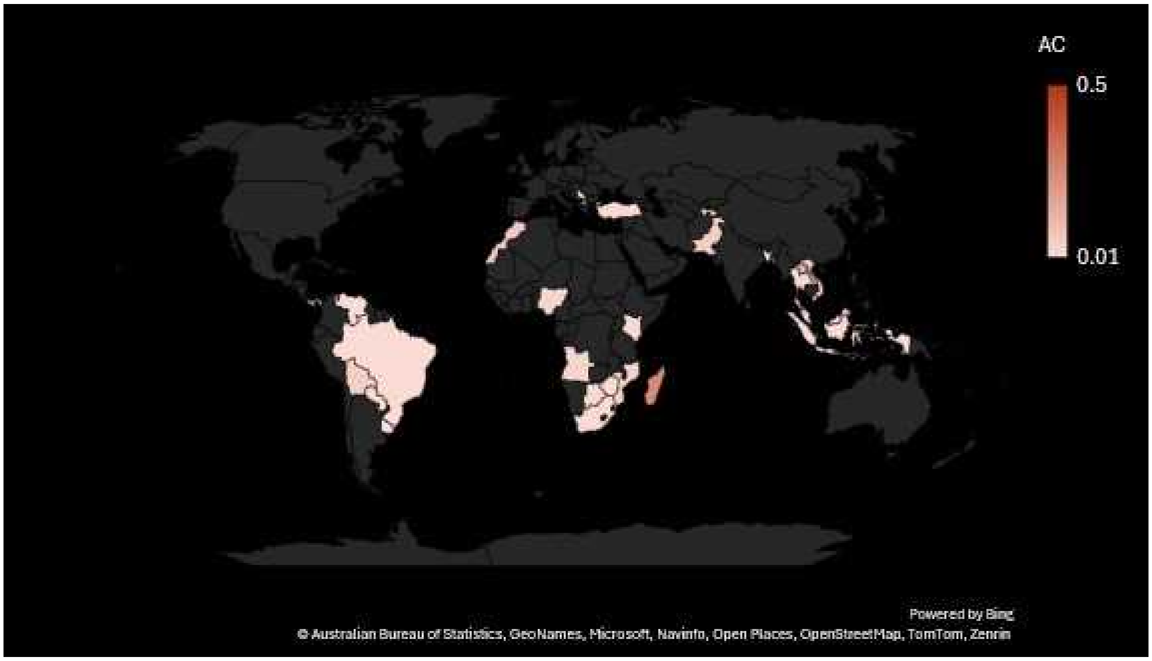

AC
0.5
0.01
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Figure 32. Q4 Alerts by Top 30 Countries Affected).

TOP MALWARE AND PUPS

Whenever we first observe the total and new malware threats for each iteration of the report, the first instinct is to wonder which malware families were responsible for these numbers, and the top malware and PUPs (potentially unwanted programs) are the best way to find out. For example, in some quarters, we see a spike in coinminers due to a new USB coinminer campaign, as happened in Q4. In Q1, we saw a surge in ransomware numbers driven by a Termite ransomware attack that was blocked and appeared in the top 10.

Top 10 Most Prevalent Malware

It doesn't take much explaining to tell you which malware campaign gained the most traction in Q3. The top nine malware for Q3 were all from the same campaign, called ManualFinder. The campaign got its name from the first samples being of a trojanized manual searching application called ManualFinder. The application performed persistence on the victim machines for further attacks. All proceeding applications resembled realistic-looking PDF modification applications. All these applications had signed certificates to make it look more legitimate, and the PDF applications worked.

Contrastingly, Q4 was much more diverse in terms of malware families. There were two coinminer droppers distributed via USB drives, similar to what happened in Q1. Then there were a malicious version of the Dumpert LSASS dumper tool and the Mimikatz password-stealing tool. There were two worms: Conficker and Neshta.

MD5	Signature	Alerts	Classification Attestation
213ECA72F00563FA2ED788A1212C67E0	Trj/Agent.CTG	2,409	ManualFinder
F28A0CF84E09873B77F9E2E5A800FD67	Trj/PhxBzA.A	1,059	ManualFinder
F2AEB79EFC4D15F1A1B786D6DE45F13A	Trj/PhxBzA.A	947	ManualFinder
4E8BD351AA8BC45D94C5F60086B5DAD4	Trj/Agent.CTG	379	ManualFinder
4ED4EB595F001CA50A69F0527F255AAD	Trj/Agent.CTG	375	ManualFinder
DE792AF1F053F582BB6FE971BCB16A20	Trj/Agent.CTG	249	ManualFinder
D79985F517044FD3D091C7A215474175	Trj/PDF	248	ManualFinder
87C52C2497449D40FBE523776FEEF3E4	Trj/Agent.CTG	146	ManualFinder
6FD6C053F8FCF345EFAA04F16AC0BFFE	Trj/Agent.CTG	114	ManualFinder
924689AA0AF023420C3F739ABBD1BC3E	HackingTool/ Mimikatz	110	Mimikatz

Figure 33. Q3 2025 Top 10 Most Prevalent Malware

MD5	Signature	Alerts	Classification Attestation
4BF6FE55240267398BEF02703F1A6182	Trj/Agent.ABC	119	Coin Miner Dropper
5E3E47FBBC5218B4EB44F6272CCEB0D0	Trj/Cl.A	102	Dumpert (LSASS dumper)
A4F2C851F5D4336FAA3F0955F9008326	Trj/Agent.ABC	96	Coin Miner Dropper
7D9542EF7C46ED5E80C23153DD5319F2	W32/ Conficker.C.worm	74	Conficker Worm
C38F92B1484E0FFEB3C30402D7A6BEAC	Trj/Agent.OOW	60	PlugX
5750ED7241A42D58FD6CD54C14A98A18	Trj/Agent.OOW	59	GuLoader delivering AgentTesla
924689AA0AF023420C3F739ABBD1BC3E	HackingTool/ Mimikatz	57	Mimikatz
C261AAE160D140353F1AF0C6A5F059FF	W97M/Downloader. DDE	54	Cyber Essentials Live Test File
E01A57998BC116134EE96B6D5DD88A13	Trj/Cl.A	52	Panda Cloud Test File
2B313CEEA938698985ABF3CB5DAA8D7E	Trj/Cl.A	50	Neshta

Figure 34. Q4 2025 Top 10 Most Prevalent Malware

Malware Descriptions

ManualFinder

ManualFinder is a malware campaign that disguised itself as legitimate applications with signed certificates. The trojanized applications resembled PDF editors and manual searchers. The name comes from the first mention of the campaign, which used a manual searching application called ManualFinder. However, this attestation is a family of applications to install persistence on a machine.

Mimikatz

Mimikatz is an open-source post-exploitation hacking tool used to perform password dumping and various other password-related modification actions. The tool is either classified as malware or as a PUP depending on the context. Official Mimikatz hashes are classified as PUPs, whereas tweaked Mimikatz are typically classified as malware.

Coinminer Dropper

Coinminer is short for cryptocurrency miner and is inherently non-malicious. Cryptocurrency mining is a natural process for acquiring cryptocurrency on some blockchains – the most obvious being Bitcoin. What makes a coinminer malicious is the context and telemetry of the file in question. An example of a malicious coinminer is one that executes software that downloads and installs a coinminer without the user's knowledge or consent.

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's 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 serve as command-and-control (C2) servers. A DGA algorithm dynamically creates a domain for the malware to connect to using a specific pattern. For example, a malicious file could use a DGA that dynamically generates domains with 16 alphanumeric characters and end in '.net' (e.g., 01234567890abdef.net).

PlugX

PlugX is a multi-faceted remote access trojan (RAT) most often associated with the China-based threat actor Mustang Panda. As such, its capabilities are designed for evasion, persistence, and data exfiltration without being traced. Considering its purpose, PlugX payloads are crafted for specific targets using spear phishing.

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, Raccoon Stealer, Vidar, and FormBook. It is persistently on the top 10 list, or close to it, and is the most prevalent malware that we've observed since we've started tracking this data.

AgentTesla

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

Cyber Essentials Live Test File

The Cyber Essentials Live Test File is an intentionally flagged file designed to test the efficacy of an endpoint solution from a Cyber Essentials audit.

Panda Cloud Test File

The Cyber Essentials Live Test File is an intentionally flagged file designed to test the efficacy of the Panda Cloud endpoint solution.

Neshta

Neshta is a malware that has existed since around 2003. The first samples indicated it was Neshta 1.0 and was written by an author in Belarus. The malware is a polymorphic file infector that changes its persistence upon every computer reboot. Its main goal is to spread and steal information.

Top 10 Most-Prevalent PUPs

Potentially unwanted programs, or PUPs, are programs that are not malware, but they do abnormal actions or are corrupted. They're the gray area between malware and goodware, but they're explicitly not either. The vast majority of PUPs are AutoKMS tools, hacking tools, and adware. AutoKMS tools are applications that bypass Windows activation licensing. These tools either exploit software or produce keys that bypass activation, but key producers are classified as PUP/Keygen if that's all they do. Hacking tools and adware are self-defined. Additionally, there exists a classification called PUP/Generic, which is the most generic classification possible. It's akin to being "unknown but not malicious."

MD5	Signature	Alerts	Classification Attestation
38DE5B216C33833AF710E88F7F64FC98*	HackingTool/AutoKMS	1,111	KMSPico
2914300A6E0CDF7ED242505958AC0BB5	HackingTool/AutoKMS	598	KMS_VL_ALL_AIO
FC3B93E042DE5FA569A8379D46BCE506	PUP/Hacktool	434	Mail PassView
F96E7F402273FCB0A9AAA4A42B9C4E35	PUP/Generic	397	Generic
F7191FE14D2F5E7C4939C2FCA5F828C2	PUP/Generic	371	RVEraser
33F914D2A2C1D8A6F4CEA578A4A76DC5	PUP/Generic	321	DriverHub Installer
8D0C31D282CC9194791EA850041C6C45	HackingTool/AutoKMS	295	KMSPico
CFE1C391464C446099A5EB33276F6D57	HackingTool/AutoKMS	293	AutoPico
6D7FDBF9CEAC51A76750FD38CF801F30	HackingTool/AutoKMS	288	KMSPico
219218AE29B2F9DFC8F6B745C004B1E3	PUP/Patcher	267	AMTLib

Figure 35. Q3 2025 Top 10 Most Prevalent PUPs

MD5	Signature	Alerts	Classification Attestation
38DE5B216C33833AF710E88F7F64FC98	HackingTool/AutoKMS	1,094	KMSPico
2914300A6E0CDF7ED242505958AC0BB5	HackingTool/AutoKMS	595	KMS_VL_ALL_AIO
789B70BDFFD2167383E04A92BF131A3F	PUP/Corrupt.A	516	Corrupt File
FC3B93E042DE5FA569A8379D46BCE506	PUP/Hacktool	463	Mail PassView
D4D6E3E6446228ACC479DA10BADB58C3	PUP/Adware	334	Adware
0498EB9BBA70AB7E1BE41BF0934BFB92	PUP/NetUtils	333	WLAN Scan
8D0C31D282CC9194791EA850041C6C45	HackingTool/AutoKMS	296	KMSPico
CFE1C391464C446099A5EB33276F6D57	HackingTool/AutoKMS	285	AutoPico
BBB1AB345527B79D388AAF8C413FFE01	PUP/Generic	273	DriverIdentifier Installer
F7191FE14D2F5E7C4939C2FCA5F828C2	PUP/Generic	273	RVEraser

Figure 36. Q4 2025 Top 10 Most Prevalent PUPs

PUP Signature Descriptions

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

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

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 whether a malicious threat actor uses a hacktool. Most open-source tools are PUPs or goodware. It is the proprietary ones that we usually label as malware.

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 a file may earn this classification is if the sample performed suspicious actions that were not exactly malicious, but were not commonly associated with legitimate behavior. Many of these behaviors take the sample's context and telemetry into account.

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

PUP/Corrupt.A
This classification applies to files that are corrupt and unanalyzable.

PUP/Adware
Adware is a portmanteau of the words advertising and software (ad-ware). Files classified as adware knowingly or unknowingly attempt to download software that performs popups without user interaction.

PUP/NetUtils
NetUtils is a catchall term for various network administrative tools external to what is supplied by a machine's operating system. This doesn't mean that all third-party tools are PUPs, but suspicious network-related tools are often labeled as PUPs, and if they are associated with malware, they are usually labeled as such.

ATTACK VECTORS

Attack vectors is fancy terminology to describe the techniques and processes attackers use for their attacks. These can either be malware-authored files or hijacked files that were injected with other malware or tweaked to perform their prescribed goals. Attack vectors are recorded by process names and then placed into one of nine data buckets. If the process resembles an attack vector or uses a known attack vector process name, it is placed in the corresponding data bucket. The nine 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 process invoked and increment there. Therefore, if there is a Python executable and a Python-related DLL, the Python executable is a script – that is, it is used to run a Python script – 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 includes 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 trigger the most detections each quarter, are files derived from or using a scripting programming language. Malware uses 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 in this group are included 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

Q3 – It used to be the norm that the Scripts attack vector was close to 90% of all attack vector detections. It wasn't even uncommon for this number to surpass 95%. There would be the occasional 70% or so, which is still most of all detections. The Script attack vector itself was led by PowerShell detections, meaning most attack vectors leveraged PowerShell. However, that dominance is beginning to slip, and it's showing in the data. In Q2, Script detections barely composed a majority, and this continued in Q3. In fact, script detections expanded from Q2 to Q3, one of only three to do so.

Attack Vector	Q2 Alert Comp.	Q3 Alert Comp.	Difference From Q2
Acrobat	2.14%	2.00%	-0.14%
Browsers	17.05%	14.31%	-2.75%
Coding Software	0.81%	0.74%	-0.07%
Database Software	0.45%	0.60%	0.15%
Microsoft 365	2.25%	3.71%	1.46%
Other	20.00%	18.06%	-1.94%
Remote Access Software	0.66%	0.50%	-0.16%
Scripts	29.88%	35.59%	5.71%
Windows	26.76%	24.49%	-2.27%

Figure 37. Q2 to Q3 2025 Attack Vectors

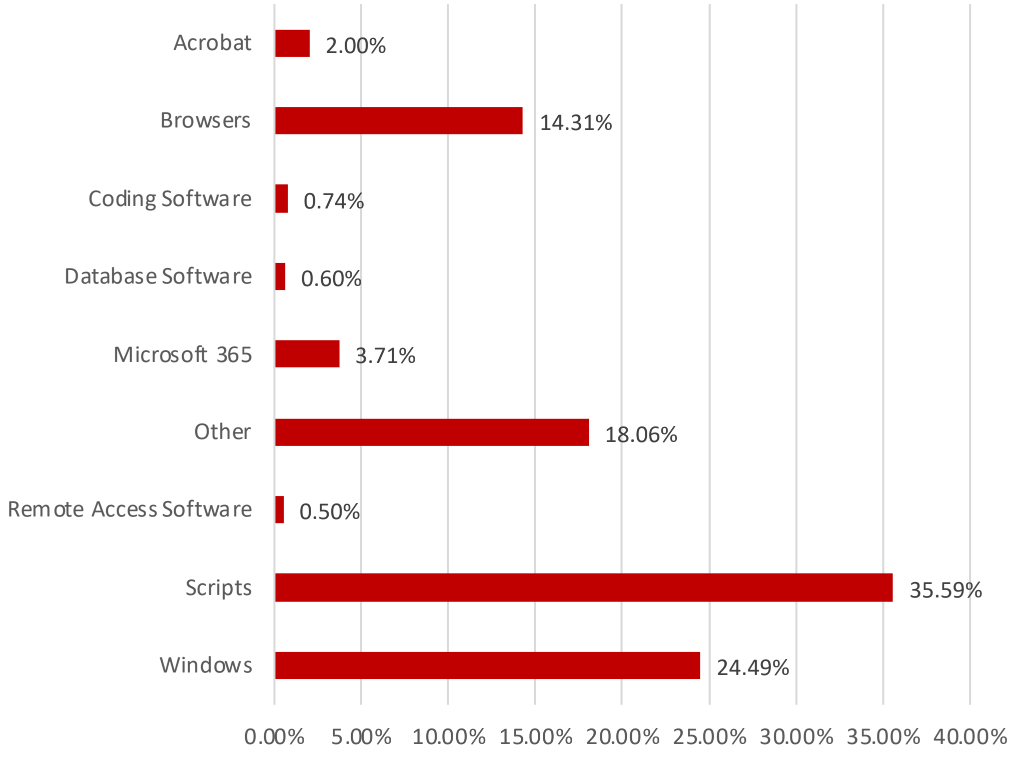


Figure 38. Q2 to Q3 2025 Attack Vectors (Chart)

Attack Vector	Q3 Alert Comp.	Q4 Alert Comp.	Difference From Q3
Acrobat	2.00%	1.64%	-0.36%
Browsers	14.31%	13.34%	-0.97%
Coding Software	0.74%	0.60%	-0.14%
Database Software	0.60%	0.24%	-0.36%
Microsoft 365	3.71%	2.46%	-1.25%
Other	18.06%	24.69%	6.63%
Remote Access Software	0.50%	0.35%	-0.15%
Scripts	35.59%	17.43%	-18.16%
Windows	24.49%	39.25%	14.76%

Figure 37. Q3 to Q4 2025 Attack Vectors

Q4 - As is the theme for the second half of 2025, Q4's numbers flipped from Q3 like almost every other subsection prior. Windows-based attack vectors decreased in Q3 and flipped to a massive increase in Q4. Reciprocally, Scripts rose in Q3 and in Q4 those numbers decreased significantly, which tells most of the story for attack vectors in the second half of 2025. The lion's share of attack vectors pivoted to Windows away from Scripts. Every other attack vector remained relatively subdued, expect for Other.

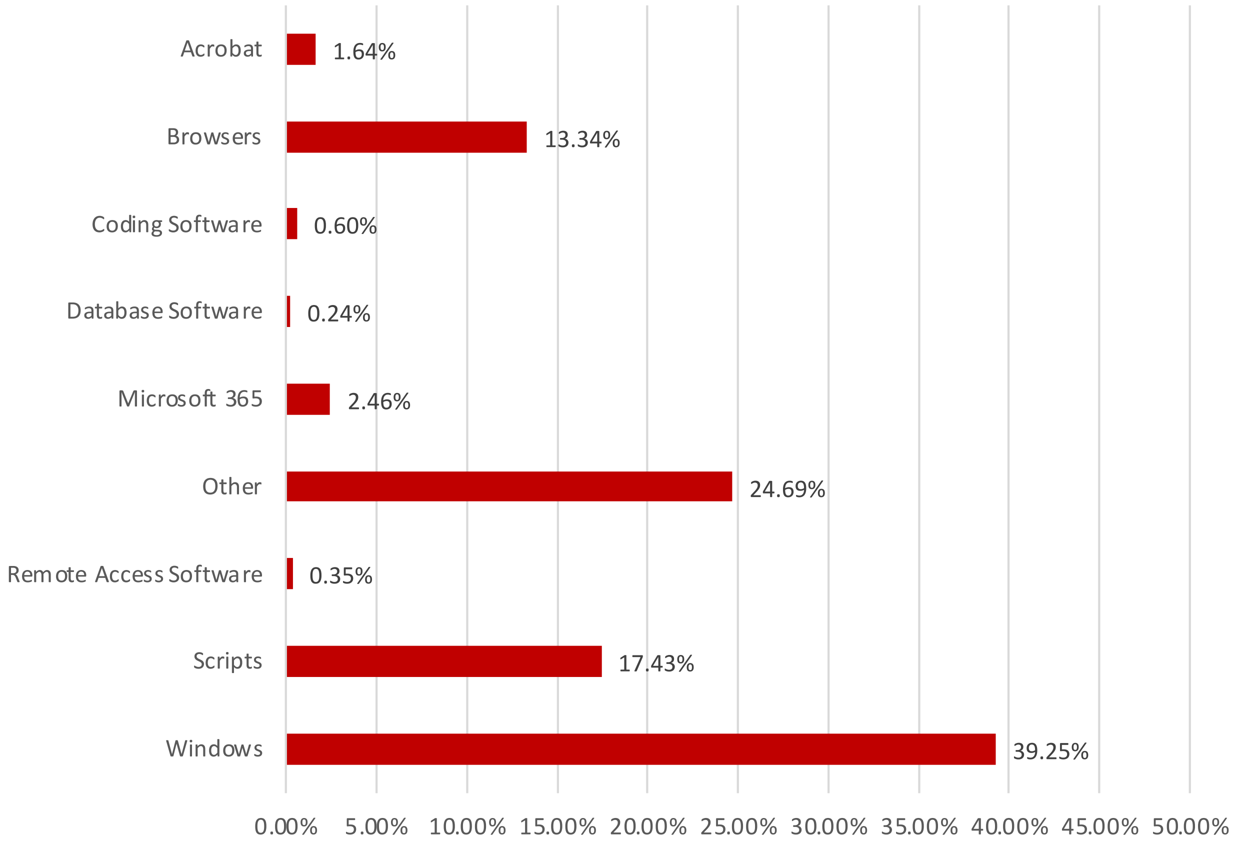


Figure 39. Q3 to Q4 2025 Attack Vectors

Browser Attack Vectors

Q3 - When we first began extracting specific browsers from the browsers attack vector, the list consistently included Windows-based browsers Internet Explorer and Edge, Google Chrome, and Firefox. We'd occasionally get an Opera detection here and there, but that was the gist of it. Now, we're increasingly seeing more third-party browsers, specifically, privacy-focused browsers. There's been a noticeable but not impactful increase in Brave Browser detections and WaterFox, too. Of course, Internet Explorer detections have decreased due to its replacement by Edge. At the end of the day, Chrome and Chrome-related attack vectors continue to be the most detected by a long shot, accounting for over half of all browser-based attack vector detections (57.75%).

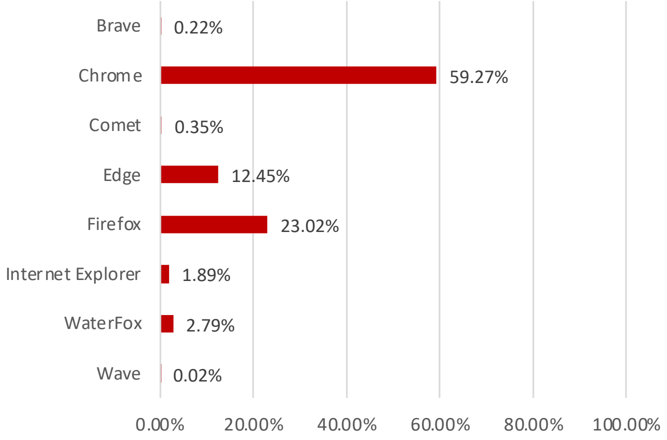


Figure 40. Q3 2025 Browser Detections

Q4 - The difference from Q3 to Q4 is visually obvious. There was a surge in Chrome-based detections that replaced most Firefox detections. The specific Firefox-related attack vector was from the official firefox.exe process, likely from trojanized Firefox-looking applications. It wasn't just that Firefox detections were reduced, but Chrome attack vectors inversely increased. One of the main drivers of this increase was the use of the Google Chrome update tool that uses the updater.exe process. Attackers were tweaking or modifying this process to carry out additional malicious actions.

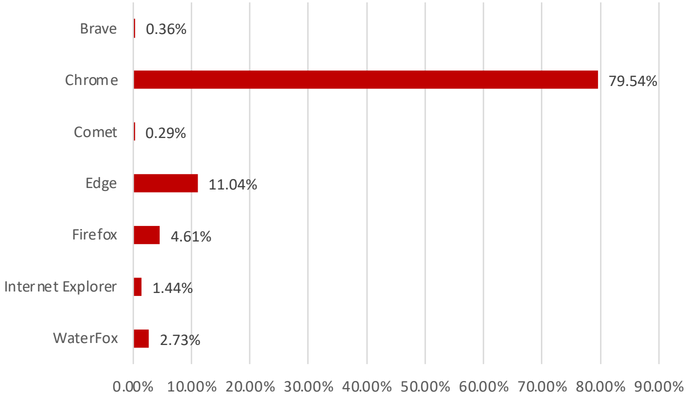


Figure 41. Q4 2025 Browser Detections

Coding Software Attack Vectors

Q3 – Coding software attack vectors include development environments and the languages that use them, excluding popular scripting languages such as PowerShell and Python. Some coding software detections are from payloads spoofing legitimate software names such as "java.exe" or "node.exe," but the majority are from .NET applications (29.05%). .NET applications are native to Windows, so it's logical that most of these detections are from these attack vectors.

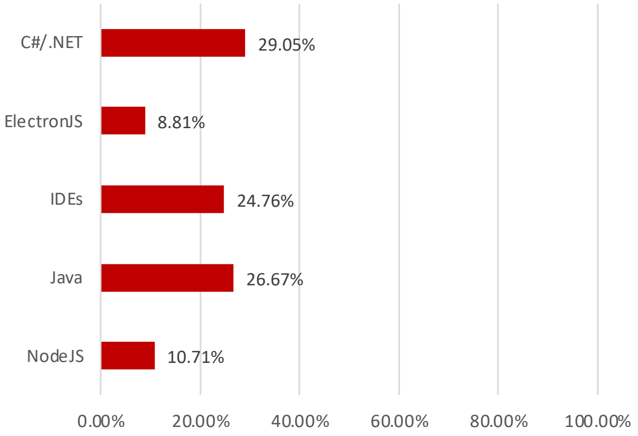


Figure 42. Q3 2025 Coding Software Detections

Q4 – Q4 tells a different story than Q3 for .Net and NodeJS detections. Remember, this is the alert composition, meaning the ratio of alerts to total alerts for a given quarter. Therefore, when you see a decrease in .NET alert composition, it's not because these values have decreased much. For Q4, the reason for the .NET decrease and subsequent NodeJS increase is a specific malware campaign called Shai-Hulud. This was a worm that propagated through NodeJS package repositories, so when users updated their packages and libraries, they were served with this worm, which further propagated it. Thus, leading to an increase in NodeJS detections for Q4.

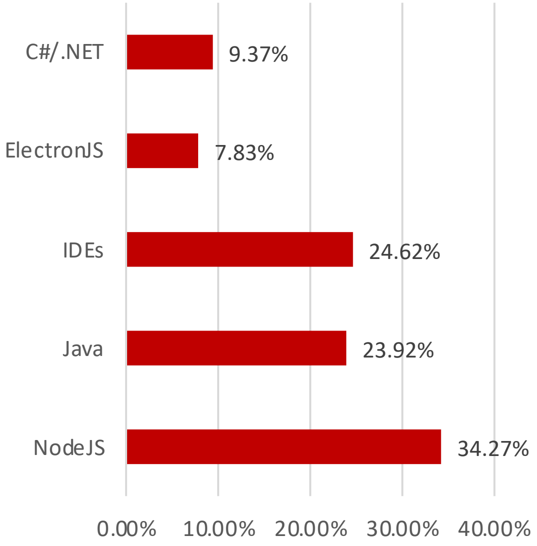


Figure 43. Q4 2025 Coding Software Detections

Database Software Attack Vectors

Q3 & Q4 - Databases are usually not the attack vector but the goal, the endgame. However, knowing that databases are required for practically all software applications, it's not unusual to leverage this knowledge to blend in with the crowd. For Attack Vectors, we've been segmenting this iteration of the report into the two separate quarters, but the differences between Q3 and Q4 are subtle and don't warrant additional headings.

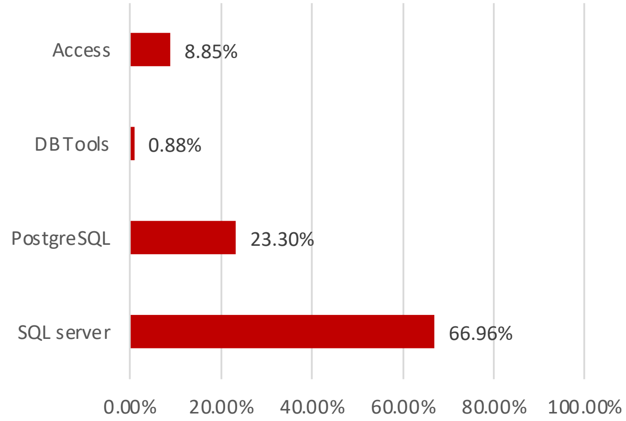


Figure 44. Q3 2025 Database Software Detections

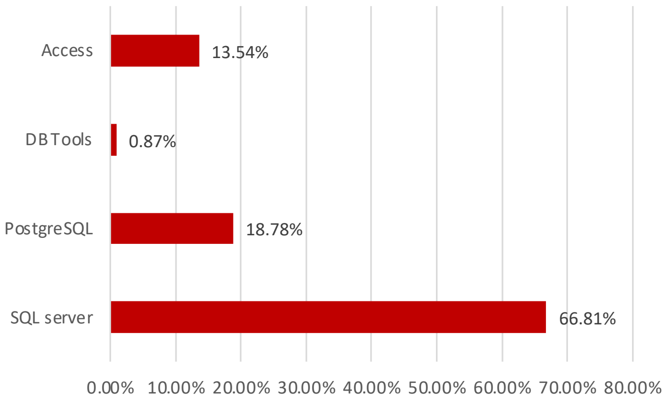


Figure 45. Q4 2025 Database Software Detections

Microsoft 365 Attack Vectors

Q3 –We previously labeled Microsoft 365 attack vectors as Office because it focused on applications such as Word, Excel, PowerPoint, and so on. Then, Microsoft rebranded its Office Suite to Microsoft 365 (MS365), encompassing even more applications. The Office Misc. attack vectors are those that are Office Suite and helper processes, not specific to any one tool. There are a lot of these executables and DLLs, so the bulk of the detections come from them. Excluding those attack vectors, though, the results are mixed. For Q3, most detections came from SharePoint, which, in many organizations, stores sensitive documents and data. Similarly, OneDrive was the next most prominent attack vector in Q3, and it's also where critically important documents may reside.

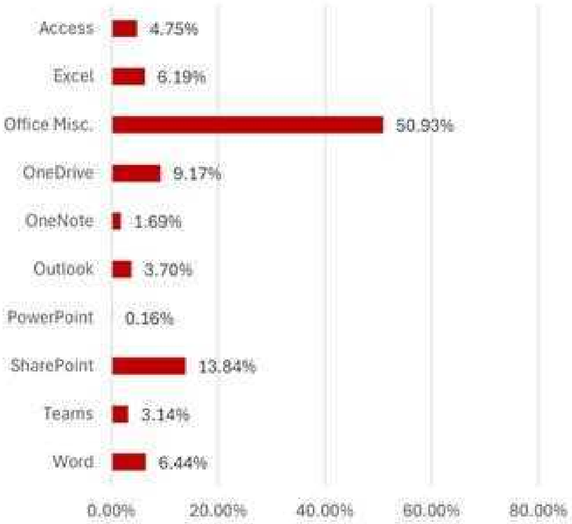


Figure 46. Q3 2025 Microsoft 365 Detections

Q4 - In the fourth quarter, Office Misc. continued to lead with the most detections, as expected, and the composition of detections towards Office Misc. increased by about 15%. The second-most-prominent attack vector was OneDrive, by a wide margin. This seems to stem from the lack of SharePoint detections, which bottomed out in a bizarre detection drought. From there on out, the detections lay with the primary Office apps: Excel, Outlook, and Word.

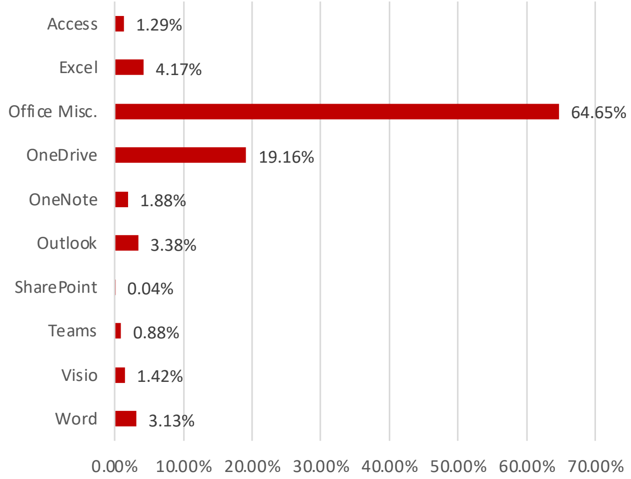


Figure 47. Q4 2025 Microsoft 365 Detections

Remote Access Attack Vectors

Q3 - Remote access tools fall into two primary categories: remote access trojans (RATs) and genuine remote access software. The former is multifaceted malware that allows attackers to perform remote actions on infected systems. If you recall PlugX in the Top 10 Malware subsection, that is one such RAT. The latter are genuine remote-access software created by companies. Examples include LogMeIn, TeamViewer, and Ninja RMM. These are legitimate remote access tools for support services or remote control of a machine. However, some attackers tweak these tools to use them for remote access to a machine for nefarious purposes. The top attack vectors for Q3 were LogMeIn, followed by Radmin, and then NetOp.

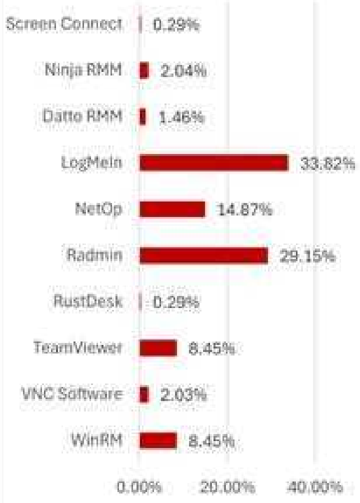


Figure 48. Q3 2025 Remote Access Detections

Q4 – In Q4, on the other hand, Radmin led the pack convincingly with 65.53% of all remote access detections. From there, WinRM and TeamViewer were in the top three, respectively. This keeps up with the theme that Q4 flipped from Q3. The only constant was Radmin detections, but beyond that, there was no consistent pattern. Attackers will likely leverage their preferred remote access tool or use what they think or know the prospective victim company is using. If they're using TeamViewer, the attacker will use TeamViewer, and so on.

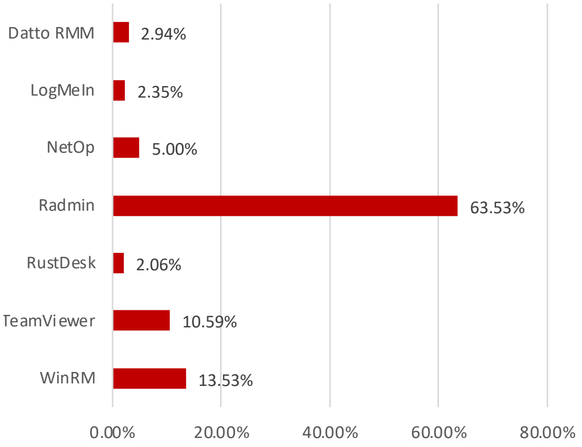


Figure 49. Q4 2025 Remote Access Detections

Script Attack Vectors

Q3 & Q4 - The Scripts attack vector is best described in terms of how many PowerShell detections we observed, because it's not only the top attack vector for Scripts, but for all attack vectors. PowerShell detections make up most of all detections, more than every other detection combined, and this is for good reason – PowerShell is native to the Windows operating system, and it's a powerful tool. Hence the name, PowerShell; it's a powerful shell.

In Q3, PowerShell detections were relatively low compared to all other quarters, only making up 64.84% of all detections. Still, almost two-thirds of all cript attack vectors. This was followed by Visual Basic scripts and Python scripts. Although AutoIT scripts were a small share of all detections, many information-stealing malware use AutoIT scripts to download additional malware; they just don't often make it to endpoints. Q4 followed the same data trends as Q3, but with PowerShell detections leading with more detections at 80.37% alert composition.

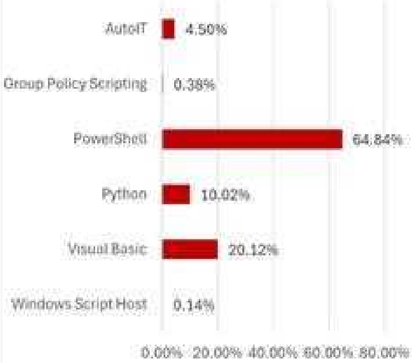


Figure 50. Q3 2025 Script Detections

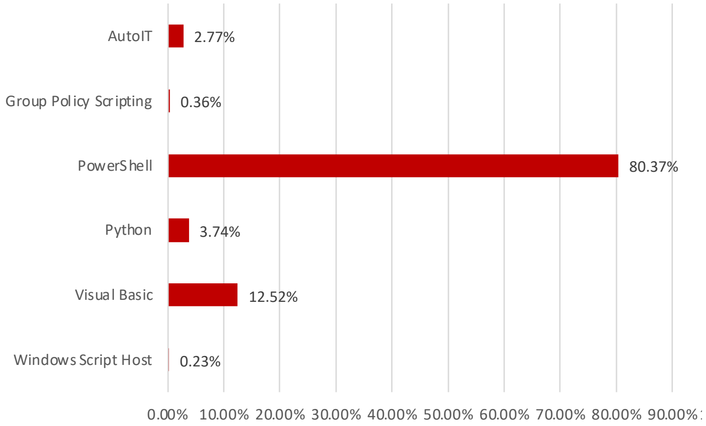


Figure 51. Q4 2025 Script Detections

Windows (LOLBAS) Attack Vectors

Q3 & Q4 – Aside from PowerShell detections, Windows-based attack vectors are responsible for most other detections. The reason for this is that, just like PowerShell, Windows attack vectors are native to Windows, obviously. More specifically, attackers leverage what are called living off the land binaries and scripts (LOLBAS). These are processes and services that Windows uses to perform certain tasks, and attackers hijack these to use for malicious purposes. They are effective because these are trusted process names and binaries that look non-malicious. The usual composition of LOLBAS detections involves cmd.exe (Command Prompt), explorer.exe (File Explorer), msedge.exe (Edge), and vbc.exe (Visual Basic Compiler). In Q3 and Q4, this held true as those were the top LOLBAS we observed.

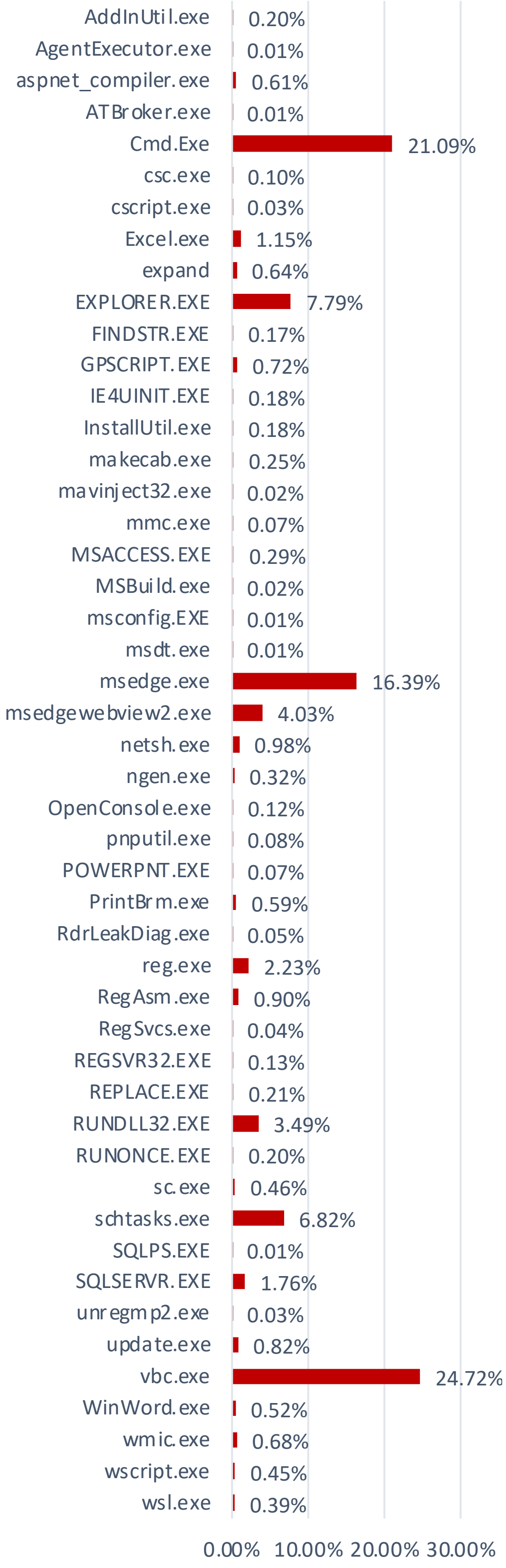


Figure 52. Q3 2025 Windows (LOLBAS) Detections

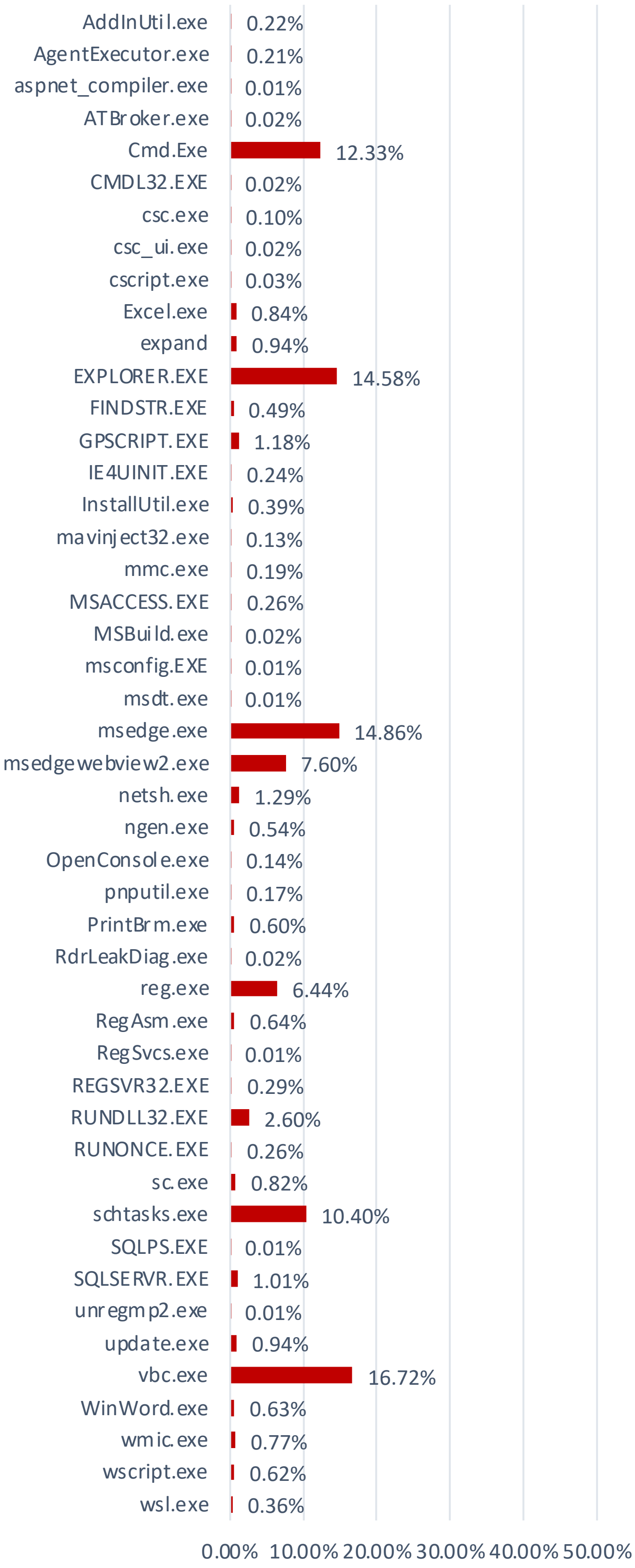


Figure 53. Q4 2025 Windows (LOLBAS) Detections

Attack Vectors Annual Summation

We discussed how scripts accounted for most alerts for most of the year, and it usually was the vast majority. However, in Q4 we observed scripts not being the most observed attack vector for the first time. Windows-based detections surged dramatically, taking the place of scripts in what looks like a swap. The other attack vector that increased was other, which doesn't tell you much directly because it's a sort of miscellaneous catch-all that doesn't fit into any other attack vector. We can say that there were many detections related to Computrace, a rootkit used by computer manufacturers for asset management. Contrastingly, every other attack vector decreased from Q3 to Q4. One interesting decrease over the year was in remote access software. From Q1 to Q4, these types of attack vectors decreased over 76% (76.35%).

Attack Vector	Q1	Q2	Q3	Q4
Acrobat	3.13%	2.14%	2.00%	1.64%
Browsers	11.51%	17.05%	14.31%	13.34%
Coding Software	0.40%	0.81%	0.74%	0.60%
Database Software	0.14%	0.45%	0.60%	0.24%
Microsoft 365	1.61%	2.25%	3.71%	2.46%
Other	23.45%	20.00%	18.06%	24.69%
Remote Access Software	1.48%	0.66%	0.50%	0.35%
Scripts	36.11%	29.88%	35.59%	17.43%
Windows	22.16%	26.76%	24.49%	39.25%

Figure 54. 2025 Attack Vectors

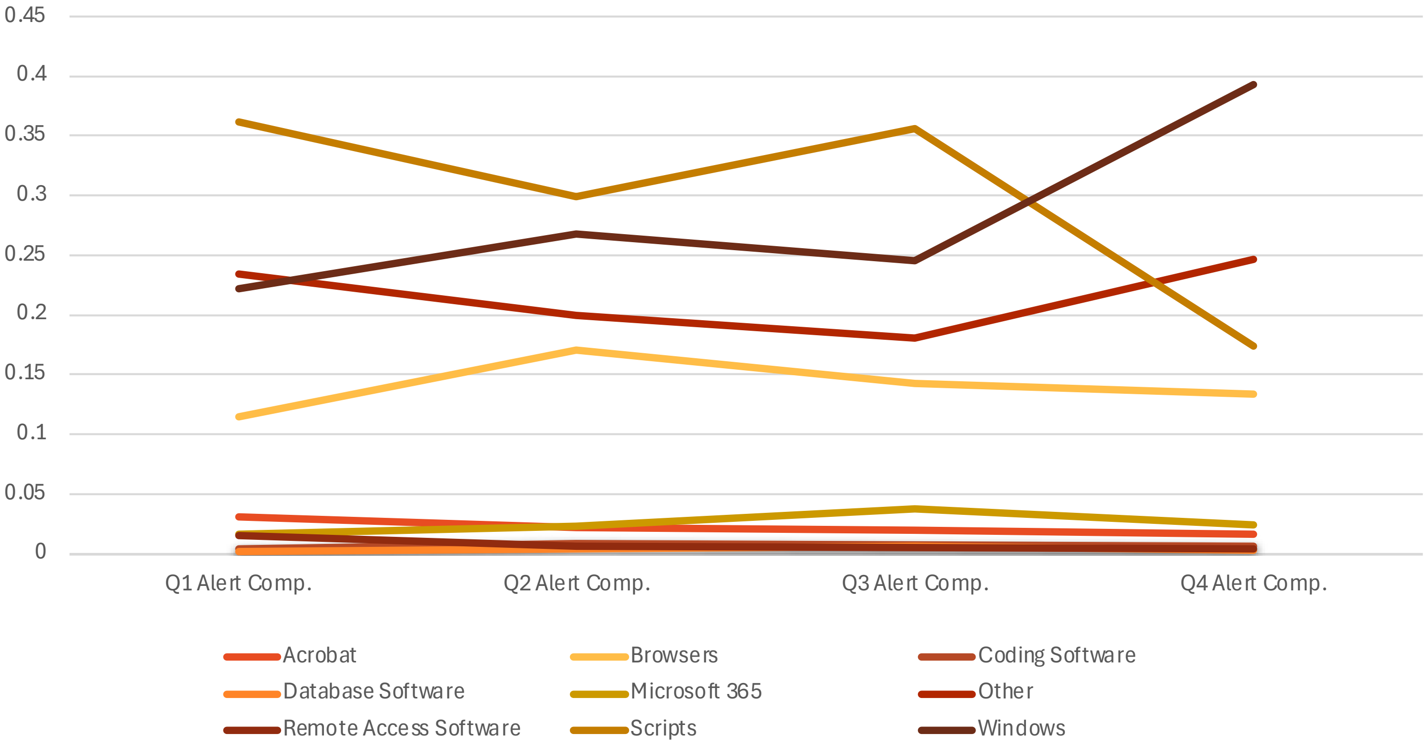


Figure 55. 2025 Attack Vectors

Alerts by Exploit Type

If Attack Vectors describes how threat actors infiltrate and propagate on systems, then the Alerts by Exploit Type describes the specific techniques and methodologies used in tandem with these vectors. If we were to extract a specific hash and determine: if it was unique or not before we saw it, how many machines it was on, what technology initially blocked that hash, what countries it appeared in, its attack vector, and the exploitation methods used, we can paint a vivid picture of the malware's intent without a designated classification, provided it's designated as malware or a PUP already. Nonetheless, the exploit types best describe the specific behaviors used for any given quarter, and they're often consistent in terms of their rankings.

To better understand the exploit types, WatchGuard has a Knowledge Base article that describes all of them:

https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Endpoint-Security/_kb-articles/exploit-techniques.html

As stated, many of the exploit types don't change much in terms of their rankings, but they do change a lot based on their alert composition. In fact, this is arguably one of the most dynamic sections. Although it may not seem that way, the data speaks for itself. We've combined all the alert compositions into one table, which includes corresponding quarter-to-quarter differences.

The dynamism comes from the difference columns. Only three exploit types showed less than 10% variation in alert composition differences from quarter to quarter. Meanwhile, four exploit types increased more than 100%! So, what does this all mean? It means that attackers utilize various exploit types, whether or not the attack vectors or the victims themselves change. Attackers are always looking for the next vulnerability before defenses have a chance to block them. This is why behavioral analysis is so important: the behaviors are scrutinized. Static analysis tools are often less effective against newer attacks because they've never seen them before. There's little to no historical context.

Exploit	Q1 Alert Comp	→	Q2 Alert Comp	→	Q3 Alert Comp	→	Q4 Alert Comp
RemoteAPCInjection	39.48%	22.79%	48.48%	-16.07%	40.69%	-7.86%	37.49%
RunPE	21.87%	-10.26%	19.63%	0.37%	19.70%	121.90%	43.72%
PsReflectiveLoader1	18.57%	-31.77%	12.67%	63.09%	20.66%	-50.94%	10.14%
WinlogonInjection	7.10%	14.96%	8.16%	4.34%	8.52%	-61.33%	3.29%
NetReflectiveLoader	4.04%	25.37%	5.07%	18.26%	6.00%	-43.34%	3.40%
DumpLsass	1.66%	79.66%	2.98%	-56.02%	1.31%	-82.54%	0.23%
APC_Exec	4.83%	-76.78%	1.12%	60.61%	1.80%	-53.48%	0.84%
ShellcodeBehavior	0.30%	94.92%	0.58%	-79.76%	0.12%	-38.47%	0.07%
AmsiBypass	1.30%	-55.68%	0.58%	-28.10%	0.41%	-75.59%	0.10%
ROP1	0.23%	44.47%	0.33%	-39.40%	0.20%	-51.46%	0.10%
JS2DOT	-	-	0.13%	-	-	-	0.001%
ThreadHijacking	0.12%	-17.35%	0.10%	78.15%	0.18%	88.03%	0.33%
ReflectiveLoader	0.022%	301.73%	0.087%	212.87%	0.271%	-65.35%	0.094%
IE_GodMode	0.090%	-50.10%	0.045%	-57.98%	0.019%	-89.13%	0.002%
HookBypass	0.024%	-44.42%	0.013%	554.79%	0.086%	14.77%	0.099%
DynamicExec	0.011%	22.27%	0.013%	30.96%	0.017%	-16.32%	0.014%
PsReflectiveLoader2	0.349%	-97.30%	0.009%	83.34%	0.017%	342.33%	0.076%

Figure 56. 2025 Alerts by Exploit Type

RemoteAPCInjection	Remote code injection via APCs
RunPE	Process Hollowing Techniques
PsReflectiveLoader1	Files that leverage PowerShell to allocate and inject payloads directly within the memory of its own process (E.g. Mimikats) (Local)
WinlogonInjection	Remote Code Injection into winlogon.exe process
NetReflectiveLoader	Code execution on MEM_PRIVATE pages that do not correspond to a PE
DumpLsass	LSASS Process Memory Dump
APC_Exec	Local code execution via APC
ShellcodeBehavior	.NET files that allocate and inject payloads directly within the memory of it's own process (Assembly.Load)
AmsiBypass	Techniques that bypass Windows' Antimalware Scan Interface (AMSI)
ROP1	Return Oriented Programming
JS2DOT	js2-mode is a JavaScript editing mode for GNU Emacs (a free, customizable text editor). If Endpoint Security detects a JS2DOT technique, it appears as an exploit technique.
ThreadHijacking	A process injection technique that allows the execution of arbitrary code in a separate process
ReflectiveLoader	Reflective executable loading (Metasploit, Cobalt Strike, etc.)
IE_GodMode	GodMode technique in Internet Explorer
HookBypass	Detection of memory allocation in base addresses; typical of heap spraying
DynamicExec	Execution of code in pages without execution permissions (32 bits only)
PsReflectiveLoader2	Files that leverage PowerShell to allocate and inject payloads directly within the memory of its own process (E.g. Mimikats) (Remote)

Figure 57. Exploit Descriptions

Cryptominer Detections

Based on our historical accounts of cryptominers within the ISR, there are often two results for cryptominer detections: extremely low or a sudden spike because a prevalent coinminer campaign was effective (although they were blocked on WatchGuard endpoints as they arrived). For example, in Q1 and in Q4, there were cryptominer campaigns that appeared in the Top 10 Most Prevalent Malware lists, all of which were USB drive coinminer dropper campaigns. Every time we see these, we obviously see a spike in cryptominer detections, but the point is, if there isn't a widespread campaign, most cryptominers don't even arrive at endpoints, or they are bundled with other information-stealing malware and are classified differently.

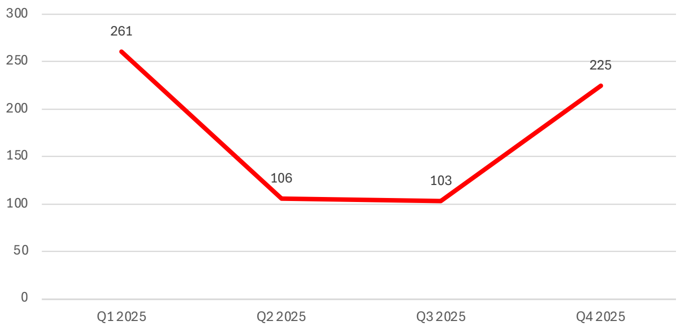


Figure 58. 2025 Cryptominer Detections Graph

Extortion Groups

Zooming out from WatchGuard-protected systems, we can get a better idea of the overall ransomware landscape, and it tells a different story. From Q1 to Q2, there was a moderate decrease in extortions, but since then, it's been all increases. Based on the graph, it seems that extortion groups took summer vacations and returned with intent. Then, in Q3, there was a large influx of new groups, 25 more in total. This was followed by an additional 15 groups in Q4, resulting in 40 new groups in the second half of 2025. All these new groups resulted in a record number of extortions in Q4 at 2588, a 47.63% increase from Q3.

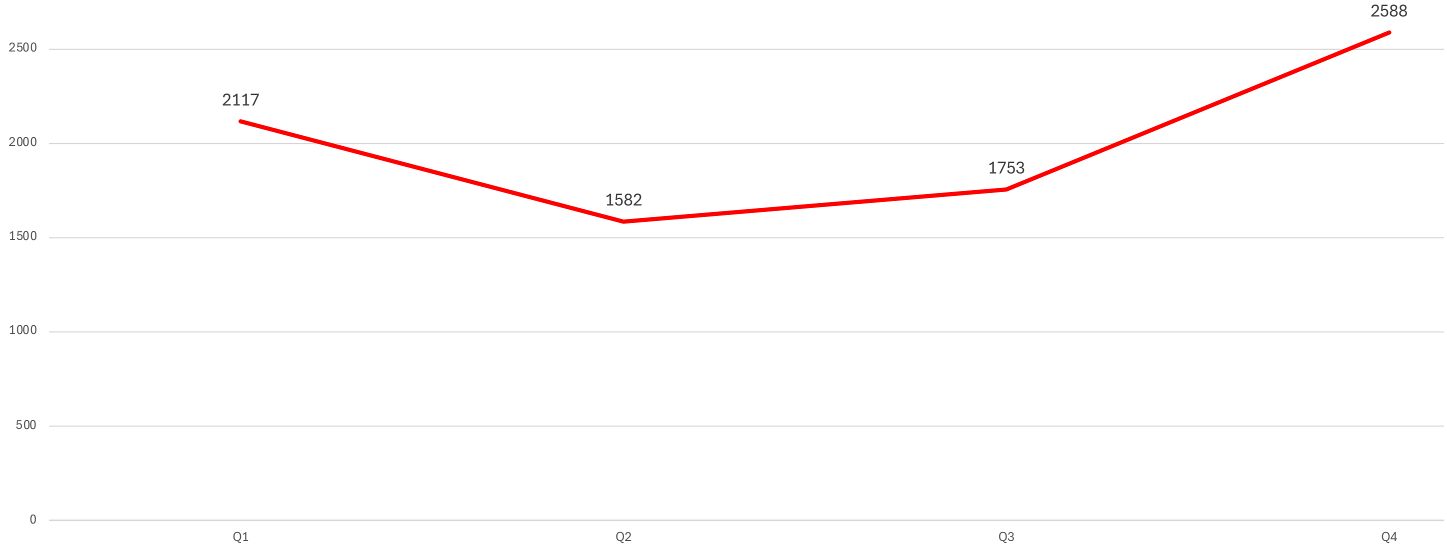


Figure 59. 2025 Public Extortions by Group

The record number of extortions in Q4 was due to an influx of new groups and a particular handful of groups. The top groups in Q4 were Qilin, Akira, Cl0p, INC Ransom, Sinobi, LockBit 5.0, and Devman. All these groups had over 100 extortions in Q4, and Akira and Qilin surpassed 200. Akira had 227, and Qilin had a record quarter, unfortunately, with 472 public extortions. Qilin's extortions more than doubled from Q3 to Q4.

In Q1 and Q2, Qilin was the top group by a large margin, having more than 1,000 public extortions. Akira and Cl0p were the other top three for the year, as you can see from the comprehensive totals table. Wilin and Akira had such high numbers because of their extensive Ransomware-as-a-Service (RaaS) model with various affiliates working on their behalf. Cl0p, on the other hand, utilizes zero-day exploits in software to steal data and extort victims. They tend to post victims in large batches, which usually means there's an ongoing exploit in some software affecting a myriad of systems.

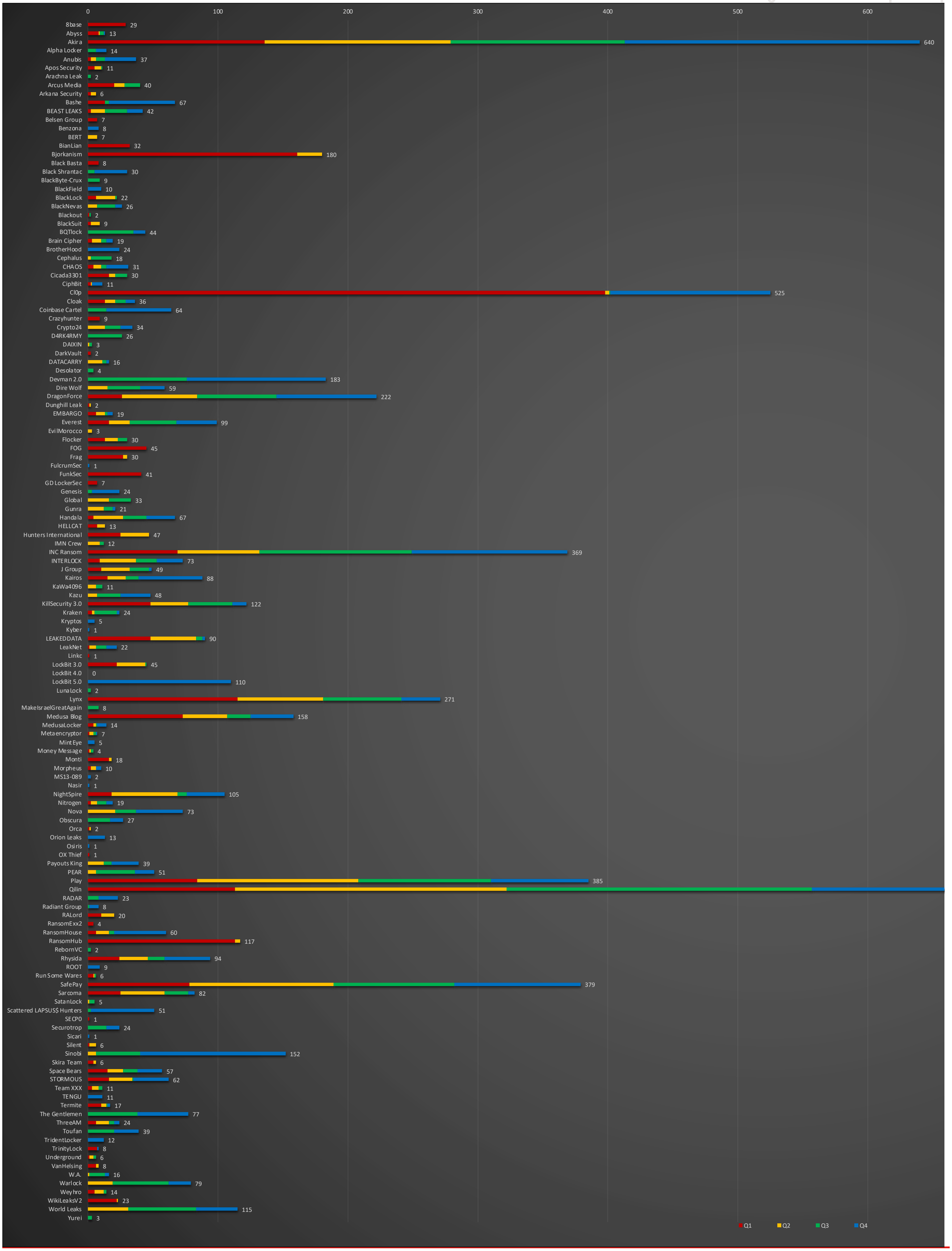
New Groups - Q3	New Groups - Q4
Arachna Leak	BEAST
Black Nevas	Benzona
Black Shrantac	Brotherhood
BlackByte-Crux	FulcrumSec
BlackField	Kryptos
BQTLock	Kyber
Coinbase Cartel	MintEye
D4RK4RMY	MS13-089
Desolator	Nasir
Devman 2.0	Orion Leaks
Genesis	Osiris
KAZU	ROOT
LeakNet	Sicari
LockBit 5.0	TENGU
LunaLock	TridentLocker
MakeIsraelGreatAgain	
Obscura	
RADAR	
Radiant Group	
RebornVC	
Scattered LAPSUS$ Hunters	
Securotrop	
Sinobi	
The Gentlemen	
Yurei	

Figure 60. Q3 and Q4 New Ransomware Groups

Name	Q1	Q2	Q3	Q4	2025 Total
8base	29	0	0	0	29
Abyss	8	1	3	1	13
Akira	136	143	134	227	640
Alpha Locker	0	0	6	8	14
Anubis	2	4	7	24	37
Apos Security	5	5	1	0	11
Arachna Leak	-	-	2	0	2
Arcus Media	20	8	12	0	40
Arkana Security	2	4	0	0	6
Bashe	13	0	3	51	67
BEAST LEAKS	2	11	17	12	42
Belsen Group	7	0	0	0	7
Benzona	-	-	-	8	8
BERT	-	7	0	0	7
BianLian	32	0	0	0	32
Bjorkanism	161	19	0	0	180
Black Basta	8	0	0	0	8
Black Shrantac	-	-	5	25	30
BlackByte-Crux	-	-	9	0	9
BlackField	-	-	0	10	10
BlackLock	6	15	1	0	22
BlackNevas	-	7	14	5	26
Blackout	1	0	1	0	2
BlackSuit	2	7	0	0	9
BQTlock	-	-	35	9	44
Brain Cipher	3	7	4	5	19
BrotherHood	-	-	-	24	24
Cephalus	-	2	16	0	18
CHAOS	4	6	4	17	31
Cicada3301	16	5	9	0	30
CiphBit	2	1	0	8	11
Cl0p	398	3	1	123	525
Cloak	13	8	8	7	36
Coinbase Cartel	-	-	14	50	64
Crazyhunter	9	0	0	0	9
Crypto24	-	13	12	9	34
D4RK4RMY	-	-	26	0	26
DAIXIN	0	1	2	0	3
DarkVault	2	0	0	0	2
DATACARRY	-	11	3	2	16
Desolator	-	-	4	0	4
Devman 2.0	-	-	76	107	183
Dire Wolf	-	15	25	19	59
DragonForce	26	58	61	77	222
Dunghill Leak	1	1	0	0	2
EMBARGO	6	7	2	4	19
Everest	16	16	36	31	99
EvilMorocco	0	3	0	0	3
Flocker	13	10	7	0	30
FOG	45	0	0	0	45
Frag	27	3	0	0	30
FulcrumSec	-	-	0	1	1
FunkSec	41	0	0	0	41
GD LockerSec	7	0	0	0	7
Genesis	-	-	3	21	24
Global	-	16	17	0	33
Gunra	-	12	7	2	21

Name	Q1	Q2	Q3	Q4	2025 Total
Handala	4	23	18	22	67
HELLCAT	7	6	0	0	13
Hunters International	25	22	0	0	47
IMN Crew	-	9	3	0	12
INC Ransom	69	63	117	120	369
INTERLOCK	9	28	16	20	73
J Group	10	22	15	2	49
Kairos	15	14	10	49	88
KaWa4096	-	6	5	0	11
Kazu	-	7	18	23	48
KillSecurity 3.0	48	29	34	11	122
Kraken	3	2	17	2	24
Kryptos	-	-	-	5	5
Kyber	-	-	-	1	1
LEAKEDDATA	48	35	5	2	90
LeakNet	1	5	8	8	22
Linkc	1	0	0	0	1
LockBit 3.0	22	22	1	0	45
LockBit 4.0	0	0	0	0	0
LockBit 5.0	-	-	-	110	110
LunaLock	-	-	2	0	2
Lynx	115	66	60	30	271
MakelsraelGreatAgain	-	-	8	0	8
Medusa Blog	73	34	18	33	158
MedusaLocker	4	2	1	7	14
Metaencryptor	1	3	2	1	7
MintEye	-	-	-	5	5
Money Message	1	1	2	0	4
Monti	16	2	0	0	18
Morpheus	2	4	0	4	10
MS13-089	-	-	-	2	2
Nasir	-	-	-	1	1
NightSpire	18	51	7	29	105
Nitrogen	2	5	7	5	19
Nova	-	21	16	36	73
Obscura	-	-	17	10	27
Orca	1	1	0	0	2
Orion Leaks	-	-	-	13	13
Osiris	-	-	-	1	1
OX Thief	1	0	0	0	1
Payouts King	-	12	6	21	39
PEAR	-	6	30	15	51
Play	84	124	102	75	385
Qilin	113	209	235	472	1029
RADAR	-	-	8	15	23
Radiant Group	-	-	1	7	8
RALord	10	10	0	0	20
RansomExx2	4	0	0	0	4
RansomHouse	6	10	4	40	60
RansomHub	113	4	0	0	117
RebornVC	-	-	2	0	2
Rhysida	24	22	13	35	94
ROOT	-	-	-	9	9
Run Some Wares	4	1	1	0	6
SafePay	78	111	93	97	379
Sarcoma	25	34	18	5	82
SatanLock	-	1	4	0	5
Scattered LAP-SUS$ Hunters	-	-	2	49	51
SECP0	1	0	0	0	1
Securotrop	-	-	14	10	24
Sicari	-	-	-	1	1
Silent	1	5	0	0	6
Sinobi	-	6	34	112	152
Skira Team	4	2	0	0	6
Space Bears	15	12	11	19	57
STORMOUS	16	18	1	27	62
Team XXX	3	5	3	0	11
TENGU	-	-	-	11	11
Termite	10	4	1	2	17
The Gentlemen	-	-	38	39	77
ThreeAM	6	10	4	4	24
Toufan	0	0	20	19	39
TridentLocker	-	-	-	12	12
TrinityLock	7	0	0	1	8
Underground	1	3	2	0	6
VanHelsing	6	2	0	0	8
W.A.	-	1	12	3	16
Warlock	-	19	43	17	79
Weyhro	5	7	2	0	14
WikiLeaksV2	22	1	0	0	23
World Leaks	-	31	52	32	115
Yurei	-	-	3	0	3

Figure 61. 2025 Ransomware Group Extortion Totals


0
100
200
300
400
500
600
8base 29
Abyss 13
Akira 640
Alpha Locker 14
Anubis 37
Apos Security 11
Arachna Leak 2
Arcus Media 40
Arkana Security 6
Bashe 67
BEAST LEAKS 42
Belsen Group 7
Benzona 8
BERT 7
BianLian 32
Bjorkanism 180
Black Basta 8
Black Shrantac 30
BlackByte-Crux 9
BlackField 10
BlackLock 22
BlackNevas 26
Blackout 2
BlackSuit 9
BQTlock 44
Brain Cipher 19
BrotherHood 24
Cephalus 18
CHAOS 31
Cicada3301 30
CiphBit 11
Cl0p 525
Cloak 36
Coinbase Cartel 64
Crazyhunter 9
Crypto24 34
D4RK4RMY 26
DAIXIN 3
DarkVault 2
DATACARRY 16
Desolator 4
Devman 2.0 183
Dire Wolf 59
DragonForce 222
Dunghill Leak 2
EMBARGO 19
Everest 99
EvilMorocco 3
Flocker 30
FOG 45
Frag 30
FulcrumSec 1
FunkSec 41
GD LockerSec 7
Genesis 24
Global 33
Gunra 21
Handala 67
HELLCAT 13
Hunters International 47
IMN Crew 12
INC Ransom 369
INTERLOCK 73
J Group 49
Kairos 88
KaWa4096 11
Kazu 48
KillSecurity 3.0 122
Kraken 24
Kryptos 5
Kyber 1
LEAKEDDATA 90
LeakNet 22
Linkc 1
LockBit 3.0 45
LockBit 4.0 0
LockBit 5.0 110
LunaLock 2
Lynx 271
MakeIsraelGreatAgain 8
Medusa Blog 158
MedusaLocker 14
Metaencryptor 7
Mint Eye 5
Money Message 4
Monti 18
Morpheus 10
MS13-089 2
Nasir 1
NightSpire 105
Nitrogen 19
Nova 73
Obscura 27
Orca 2
Orion Leaks 13
Osiris 1
OX Thief 1
Payouts King 39
PEAR 51
Play 385
Qilin
RADAR 23
Radiant Group 8
RALord 20
RansomExx2 4
RansomHouse 60
RansomHub 117
RebornVC 2
Rhysida 94
ROOT 9
Run Some Wares 6
SafePay 379
Sarcoma 82
SatanLock 5
Scattered LAPSUS$ Hunters 51
SECP0 1
Securotrop 24
Sicari 1
Silent 6
Sinobi 152
Skira Team 6
Space Bears 57
STORMOUS 62
Team XXX 11
TENGU 11
Termite 17
The Gentlemen 77
ThreeAM 24
Toufan 39
TridentLocker 12
TrinityLock 8
Underground 6
VanHelsing 8
W.A. 16
Warlock 79
Weyhro 14
WikiLeaksV2 23
World Leaks 115
Yurei 3
🟥 Q1
🟨 Q2
🟩 Q3
🟦 Q4

Notable Ransomware Events

Operation Checkmate – Operation Checkmate likely took its name from the ransomware group it was targeting. The now-defunct Royal ransomware group used a chess theme before rebranding to BlackSuit. In July, law enforcement successfully deconstructed the BlackSuit infrastructure, deactivating that group. However, it is now believed that after the BlackSuit takedown, they rebranded yet again to CHAOS, which is currently active as of this writing. This group has been around for several years and has rebranded multiple times. In fact, it is believed that some or most of the members of this group were from the notorious Conti ransomware group – meaning this is their fourth iteration, at minimum. Their lineage looks something like this:

Conti -> Royal -> BlackSuit -> CHAOS

https://www.justice.gov/opa/pr/justice-department-announces-coordinated-disruption-actions-against-blacksuit-royal
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/royal
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/chaos
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/blacksuit

Operation Sentinel – This operation focused on several African countries and hundreds of individuals. It was a widespread operation involving law enforcement from 19 countries resulting in 574 arrests and the recovery of millions of dollars. The operation focused on extortions and business email compromise (BEC) attacks. This is mentioned here because it also involved six ransomware variants that were analyzed and decrypted to recover encrypted data from a financial institution. Specifically in Ghana, researchers successfully reverse-engineered the encryption mechanism and recovered a large portion of the encrypted data.

https://www.interpol.int/en/News-and-Events/News/2025/574-arrests-and-USD-3-million-recovered-in-coordinated-cybercrime-operation-across-Africa

Scattered Spider Arrests – Scattered Spider, as the name implies, is a decentralized group of individuals who perform breaches and extort victims. They're primarily known for their social engineering tactics, where they call into support centers and either bribe support representatives or impersonate victims to get account access in furtherance of more attacks. There were several arrests of the Scattered Spider group in the second half of 2025. The first tranche was in July when four individuals in the United Kingdom were apprehended. The individuals' ages ranged from 17-20. In September, there were two additional arrests of two teenagers in the UK, again. They found over $50 million in stolen cryptocurrency. The final action against Scattered Spider was the arrest of an individual in Las Vegas, who is a juvenile, and not much more is known about them for that reason

https://www.justice.gov/opa/pr/justice-department-announces-coordinated-disruption-actions-against-blacksuit-royal
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/scattered-lapsus-hunters

LockBit Activity – LockBit is one of the most notorious ransomware groups and encryptors in the world. They've been around for several years and have numerous affiliates that have also created a few of their own ransomware operations using the LockBit builder(s). LockBit 3.0 existed for a long time and was responsible for hundreds of breaches. That is, until law enforcement acted against several affiliates and the LockBit infrastructure, including doxxing the LockBit leader. After that, they regrouped and formed LockBit 4.0, but it was short-lived and had the uphill battle of lost reputation from law enforcement actions. Then they created LockBit 5.0 and dumped over 100 victims onto their data-leak site. Here are some of the members and affiliates who were apprehended in the second half of 2025:

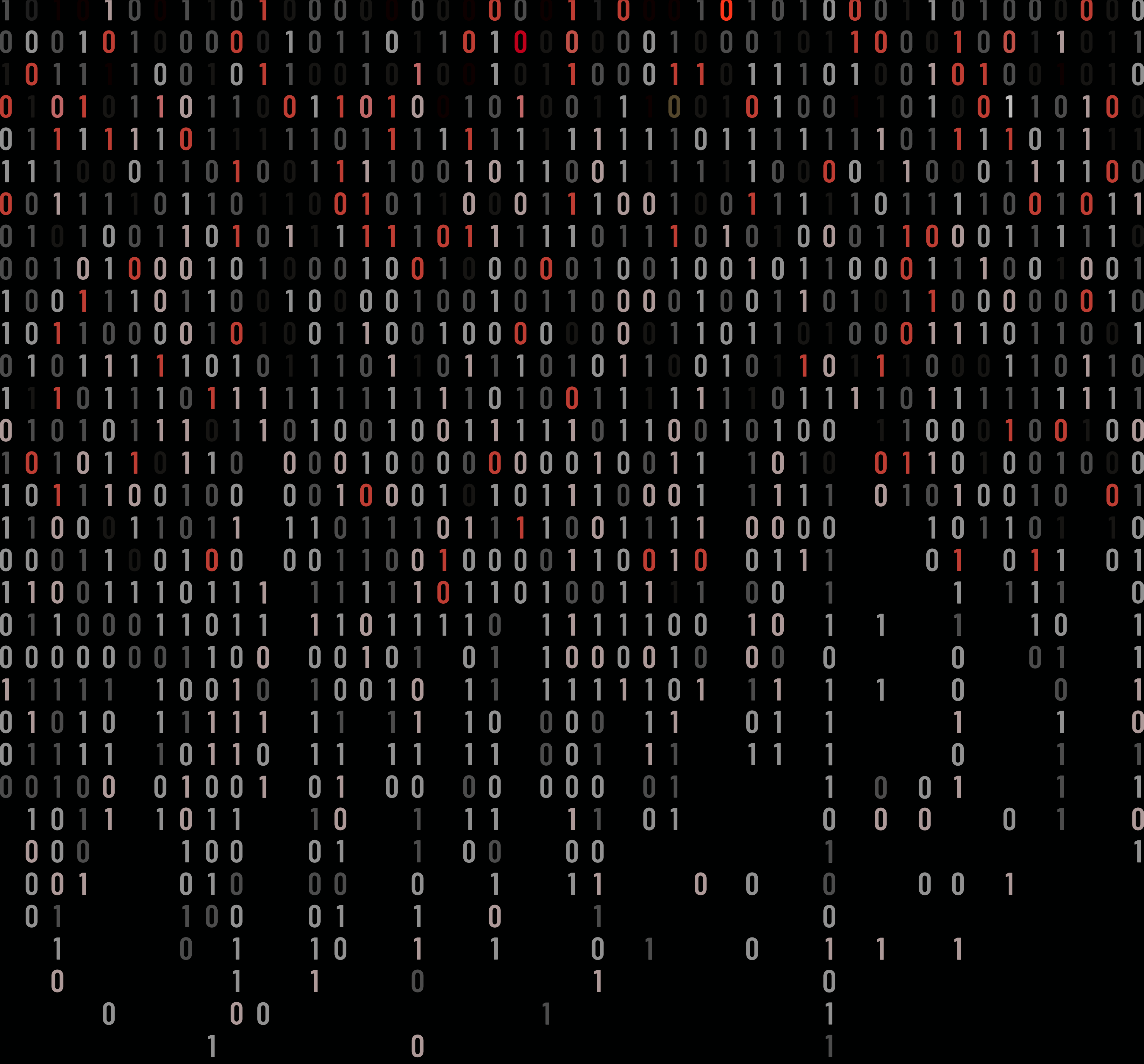
- **Rostislav Panev:** A Russian Israeli national who helped develop LockBit
- **Mikhail Vasiliev:** A Russian Canadian national affiliate
- **Rusian Astamirov:** An affiliate
- **Four unknown individuals:** Apprehended via Operation Cronos Phase 3. One French national who helped develop LockBit, two UK-based affiliates, and one hosting provider in Spain

https://www.justice.gov/usao-nj/pr/dual-russian-and-israeli-national-extradited-united-states-his-role-lockbit-ransomware
https://www.justice.gov/usao-nj/media/1361006/dl?inline
https://www.justice.gov/archives/opa/pr/russian-national-arrested-and-charged-conspiring-commit-lockbit-ransomware-attacks-against-us

Conclusion

In conclusion, the second half of 2025 was a tale of two quarters, literally and figuratively. Q3 was less active in terms of alerts, whereas Q4 flipped the script and we saw a surge of unique and new malware. From Q3 to Q4, there was an explosion of never-before-seen malware, over 15 times more! This coincided with a drop in total malware threats, meaning attackers are using fewer of the same payloads. Attacks are tweaked or altered according to their victims or are polymorphic, changing the code to also alter the hash. Most of these payloads were only observed on one machine, which hasn't changed much over the past few quarters, but what has changed is the migration of static analysis-related detections and more blocks from dynamic analysis tools such as sandboxes, machine learning, and manual attestation analyses.

Q3 can best be defined by the top malware observed in that quarter: ManualFinder. This campaign leveraged realistic PDF and document tools to gain persistence of victim machines upon installing the software. There were several of these applications, which is the reason nine of the top 10 malware were from this campaign. On the other hand, Q4 had more variety, containing coinminers, hacking tools, RATs, information stealers, loaders, and test files. However, the main takeaway from Q4 is the new malware threats and the public ransomware extortion numbers. Both were at record highs. There were almost 2,600 victims publicly extorted, led by the Qilin group. The almost 50% increase from Q3 was unexpected because Q4 is usually when threat actors slow down for the year and take time off, believe it or not. Yet, the numbers tell the whole story: ransomware groups and their affiliates are unfortunately thriving. The numbers are going the wrong way.



CONCLUSION & DEFENSE HIGHLIGHTS

CONCLUSION AND DEFENSE HIGHLIGHTS

As we close out the second half of 2025, the shifting atmosphere of the cyber landscape feels much like the horizon sailors once studied at dawn – wide, restless, and full of subtle signals that only reveal their meaning when viewed over time. By stepping back from the quarter to quarter snapshots and widening our perspective across an entire half year, the deeper currents have come into focus. What looked at first like scattered gusts – an explosion of new malware hashes, a pivot from scripts to Windows binaries, a surge in encrypted threats – now show themselves as part of a much larger weather pattern.

Attackers are no longer merely casting wide nets; instead, they are shaping storms for specific targets. The 1,500% rise in unique, never before seen endpoint malware, paired with the fact that 90% of threats touched only a single machine, reinforces a trend we've been watching for several years: the age of mass spray attacks is giving way to tailored, evasive campaigns. At the same time, adversaries continued to hide nearly all network-borne malware within encrypted tunnels – so much so that encrypted traffic has become the default backdrop of modern attack delivery. And on endpoints, the familiar script-heavy winds shifted sharply, replaced by a surge of Windows living off the land binaries and hijacked system utilities.

Gain Visibility into Encrypted Threats with HTTPS/TLS Inspection

The overwhelming volume of malware we observed this half arrived over encrypted connections. This underscores an uncomfortable truth: defenders who avoid TLS inspection are effectively navigating without a horizon. Encryption has become both the backbone of the modern web and the perfect cover for attackers. Without decryption at the perimeter or inspection on the endpoint, entire classes of droppers, RAT installers, and polymorphic payloads slip by unnoticed.

To counter this, organizations should treat HTTPS inspection as a foundational control rather than an optional add on. Deploy TLS inspection where policies, privacy requirements, and performance budgets allow, and ensure that endpoint agents can analyze encrypted flows locally when network level inspection is not possible. Coupling decryption with advanced behavioral sandboxing closes the visibility gap attackers are now relying on. TLS inspection is a free feature of the Firebox regardless of your license, so we recommend you use it.

Finally, defenders must plan for this shift operationally. Successful TLS inspection requires certificate management, policy tuning, and regular rule maintenance; it's not a "set and forget" feature. But the payoff is undeniable: without reclaiming visibility into encrypted traffic, organizations will continue sailing through fog, unaware of the looming hazards beneath the surface.

Harden Endpoints Against Living-off-the-Land Techniques

The sharp pivot in H2 from script-heavy attacks to Windows living-off-the-land (LotL) binaries reflects how adversaries have adapted to modern detection stacks. Instead of bringing their own tooling, attackers increasingly repurpose msiexec.exe, powershell.exe, wmiprvse.exe, browser updaters, and even system activation dialogs to establish persistence and deliver payloads. These tools blend effortlessly into legitimate workflows, allowing attackers to remain hidden long after initial compromise.

Defending against LotL abuse requires a layered approach. Start by restricting unnecessary PowerShell functionality, enforcing logging, and applying AMSI integrations to catch suspicious execution chains. Then tighten process control policies: block unsigned execution of core Windows binaries, monitor for unauthorized parent/child relationships, and enforce strict rules around credential-sensitive utilities like LSASS assessors or process injectors. An easy way you can do many of these things is by deploying an Endpoint Detection and Response (EDR) solution, like WatchGuard's EPDR. Our product scrutinizes Windows processes for malicious activity, monitors the scripts running, and includes many indicators of attack and exploit detection capabilities to find and block many types of LotL attacks.

Finally, organizations should normalize continuous monitoring of rarely touched system tools and treat unexpected appearances as early-stage indicators of compromise. LotL activity is often the storm warning horn before the winds pick up – the advance signal that either a larger intrusion or a second-stage payload is imminent.

Update security awareness training for latest email and MaaS lures

If encryption and LotL tactics form the hidden currents of today's threats, phishing remains the tide that carries them to shore. H2 continued the long-running trend of highly polished social engineering campaigns delivering commodity Malware-as-a-Service (MaaS) payloads such as Remcos, RedLine, FormBook, and GuLoader. These threats lowered the barrier to entry for attackers and enabled even low-skilled operators to deploy sophisticated credential theft, RAT installation, and multi-stage dropper chains with near professional consistency.

Defenders should assume that users will continue to face convincing, well-localized phishing lures, such as fake resumes, invoices, legal notices, and software updates, which often are embedded with obfuscated JavaScript, disguised executables, or archive bundles weaponized with droppers. Robust email filtering, pre-delivery sandboxing, impersonation detection (DMARC), and attachment type restrictions can drastically reduce the volume of these threats that ever reach endpoints. Combining these controls with domain-aware DNS filtering, with services like DNSWatch, further cuts off command and control or malware staging domains early in the attack sequence.

But technology alone isn't enough. Regular security training, phishing simulations, and user-friendly prompts reminding employees not to engage with unexpected attachments add an important human layer of resilience. The most successful social engineering defenses blend automated filtering with improved user instinct, helping teams recognize when the outwardly calm seas of their inbox hide a deeper undercurrent.

Congratulations. You've reached the end of our first bi-annual, H2 2025 Internet Security Report. Be sure to come back mid-2026 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

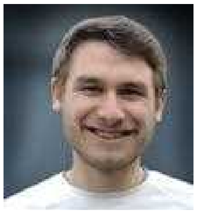
Director of Security Operations

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 an 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 is a global leader in unified cybersecurity, purpose-built for managed service providers. Unlike others, WatchGuard delivers Real Security for Real World environments through its Unified Security Platform®, bringing networks, endpoints, and identities together with AI and zero trust advances for strong protection that scales. Trusted by more than 17,000 security resellers and managed service providers protecting over 250,000 companies, WatchGuard helps partners grow fast, eliminate operational drag, and deliver strong outcomes – without added vendors, consoles, or complexity. WatchGuard is headquartered in Seattle, Washington, with offices worldwide. Learn more at 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.