Acronis

Report
H1 2025

Acronis Cyberthreats Report, H1 2025:

Phishing links lurk in email backups, attacks on collaboration apps soar

Acronis Threat Research Unit

Table of contents

Authors:

Alexander Ivanyuk — Senior Director, Technology

Irina Artioli — Cyber Protection Evangelist, Acronis Threat Research Unit

Introduction and summary

The biannual Acronis Cyberthreats Report covers the global threat landscape as encountered by the Acronis Threat Research Unit (TRU) and Acronis sensors on Windows endpoints in the first half of 2025. General threat data, including malware, ransomware, web and email threats, and vulnerabilities presented in the report has been gathered from January–June 2025 and reflects threats targeting endpoints we observed in this time frame.

Based on over 1,000,000 unique endpoints distributed around the world, the report includes statistics focused on threats targeting Windows operating systems, as they are much more prevalent than those targeting macOS and Linux.

All data collected was normalized, a method in which the number of detections per country per month was divided by the number of active clients in that country and which had at least one detection during the selected time period. Before processing, all data was anonymized. Only the percentage of affected clients in the selected countries is presented.

Key findings:

- Among the focus countries, India led the rankings for malware detections in May with 12.4% of affected clients, followed by Brazil (11%) and Spain (10.2%).
- Social engineering / BEC attacks increased from 20% to 25.6% in January–May 2025 compared to the same period in 2024, possibly due to the growth in AI use for crafting convincing impersonations.
- 20,000 malicious attachments were found in Microsoft 365 email backups among our customers. This includes old emails migrated to Microsoft 365.
- Among Acronis customers with one or more RMMs, TeamViewer was the MSP tool with the most vulnerabilities that required patching, affecting 4.56% of global customers.
- Manufacturing was the most targeted industry by ransomware gangs, representing 15% of all recorded cases in Q1 2025.

Among the cybersecurity trends we saw in the first half of 2025 (January–June):

- Ransomware continues to be the major threat to large and medium-sized businesses, with numerous ransomware gangs abusing AI for automation.
- AI is everywhere and widely used for malicious purposes; however, it has not yet been incorporated into the full cyberattack kill chain. Because many malicious AI services have been shut down, cybercriminals abuse legitimate ones or use solutions trained in house.
- In Q1 2025, the most frequently observed MITRE ATT&CK technique was T1055.001 Process Injection, with which attackers inject malicious code into legitimate processes — commonly via DLL injection — to evade detection and execute stealthy payloads. PowerShell followed closely behind. It is often used to run obfuscated scripts and quietly download malware. These trends underline the need for robust EDR, strict script policies and behavior-based detection to counter evasive threats.
- Phishing attacks in collaboration apps rose sharply from 9% to 30.5%, while advanced email attacks increased from 9% to 24.5%.

What you will find in this report:

- Top ransomware gangs and their activity in H1 2025.
- Common techniques used to attack MSPs, including compromising RMMs.
- Latest trends and statistics on phishing and other email-borne attacks.
- Vulnerabilities found on Acronis customers' machines and vulnerabilities exploited to attack MSPs.
- Cases of AI-abuse by cybercriminals.
- Malware, ransomware and web-based threats in H1 2025.
- Recommendations for how to stay safe.

1

Key cyberthreats and trends in H1 2025

1. Ransomware gangs continue to wreak havoc

Methodology

The data in this section is based on information collected from publicly available, open-source intelligence (OSINT) repositories, including threat actor leak sites and data-leak portals, including ransomfeed.it and ransomware.live. Publicly available open source data is then correlated with data from previous Acronis Cyberthreats Reports from H1 2023 to H1 2024.

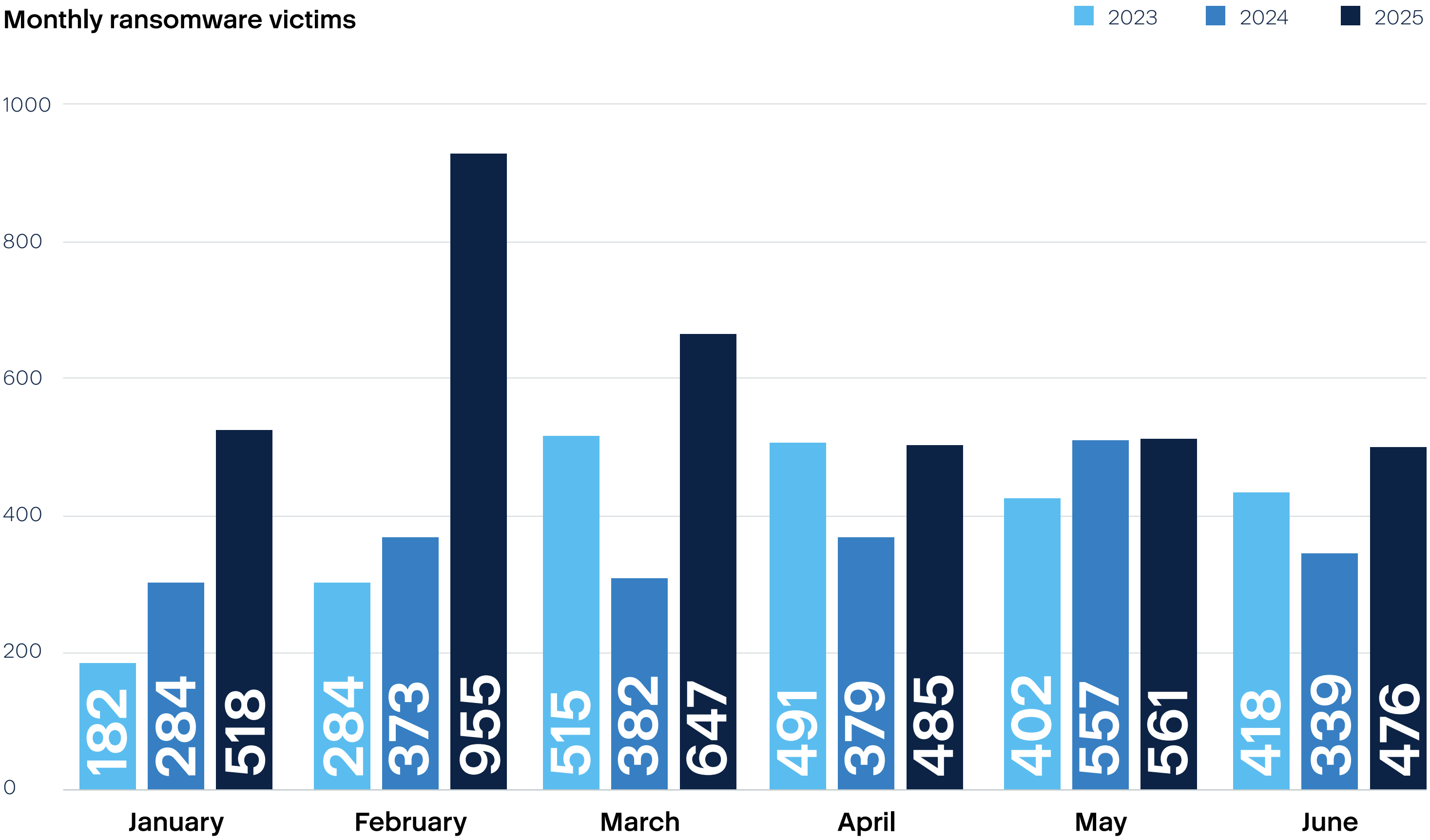
To ensure accuracy and eliminate duplications, Acronis systematically reviews and refines all collected data; however, publicly reported incidents may not fully reflect the true volume of attacks, as some actors suppress or retract victim disclosures upon ransom payment, furnish partial victim information, or exaggerate their operational scope. Despite these inherent variances, the resulting dataset delivers a reliable, consolidated view of today's ransomware and extortion threat landscape.

Based on data from publicly available sources, the following ransomware gangs were the most active (in terms of total numbers of victims) from January–June 2025:

↘ Cl0p (402)   ↘ Akira (346)   ↘ Qilin (324)   ↘ Play (212)   ↘ SafePay[1] (187)

The total number of claimed ransomware victims from January–June is 3,642.

Monthly ransomware victims



[1] Acronis Threat Research Unit (TRU). "SafePay ransomware: The fast-rising threat targeting MSPs." https://www.acronis.com/en-us/tru/posts/safepay-ransomware-the-fast-rising-threat-targeting-msps/, July 8, 2025.

❶ The number of publicly known ransomware victims from January 2025 to June 2025 increased nearly 70% compared to the same period in both 2023 and 2024.

❷ February 2025 saw the highest number of ransomware victims (955) in the observed period. Cl0p[2] alone was responsible for 335 of those cases — a 300% month-over-month surge that leveraged the mass exploitation of high-severity vulnerabilities in CLEO MFT platforms (Harmony, VLTrader, Lexicom)), CVE-2024-50623 (remote code execution) and CVE-2024-55956 (command injection). Between December 2024 and Q1 2025, Cl0p compromised approximately 390 organizations in one of the most aggressive campaigns of the period. Manufacturing and supply chain sectors, including logistics, accounted for more than 20% cases, followed by retail and other industries. Cl0p concentrated its campaign in North America, with most victims in the U.S. The remaining victims were distributed across Europe, Asia-Pacific and other regions.

❸ This sustained high cadence reflects the scalability of RaaS operations, including Cl0p, Play and RansomHub, which capitalize on fragmented patch management and delayed mitigations to maintain relentless pressure on victims.

❹ By mid-2025, the slight plateau in victim counts (ranging from 476–647 from March to June) points to a tactical shift toward quieter data-theft extortion and zero-day exploitation, foreshadowing more surgical, stealth-first intrusions rather than volume-based attacks.

❺ The drop in ransomware victims in Q2 2025 (1,522) compared to Q1 (2,120) is likely due to law enforcement crackdowns,[3] rebranding pauses by major groups, and improved corporate defenses. Additionally, seasonal slowdowns and shifts toward data extortion without encryption may have reduced reported incidents.

In February, global law enforcement dealt a major blow to the threat landscape: The 8Base gang was dismantled, and Phobos operators, who compromised over 1,000 victims using sophisticated encryption and evasion methods, were arrested in Thailand.[4]

In April, RansomHub abruptly shut down,[5] shaking the ransomware-as-a-service (RaaS) model and forcing affiliates to migrate. Some regrouped under established names, including Qilin and DragonForce, while others formed spin-offs, including VanHelsing and RansomBay.[6] Amid this reshuffling, DragonForce stands out as a new cartel, offering branding freedom to affiliates, while stealthier variants like Anubis and ELENOR-corp gained traction, favoring anti-forensic strategies and pure extortion models.

[2] Cl0p is widely known for orchestrating large-scale campaigns by exploiting zero-day vulnerabilities in managed file transfer platforms — a pattern also covered in Acronis Cyberthreats H2 2023 report, which detailed the devastating MOVEit Transfer attacks that affected over 2,600 organizations and 85 million individuals, including high-profile victims like Maximus (a $4.25 billion U.S. government services contractor with global operations), resulting in an estimated financial impact of nearly $10 billion.

[3] Ionut Ilascu. “BlackCat ransomware shuts down in exit scam, blames the ‘feds.’” Bleeping Computer. https://www.bleepingcomputer.com/news/security/blackcat-ransomware-shuts-down-in-exit-scam-blames-the-feds/, March 5, 2024.

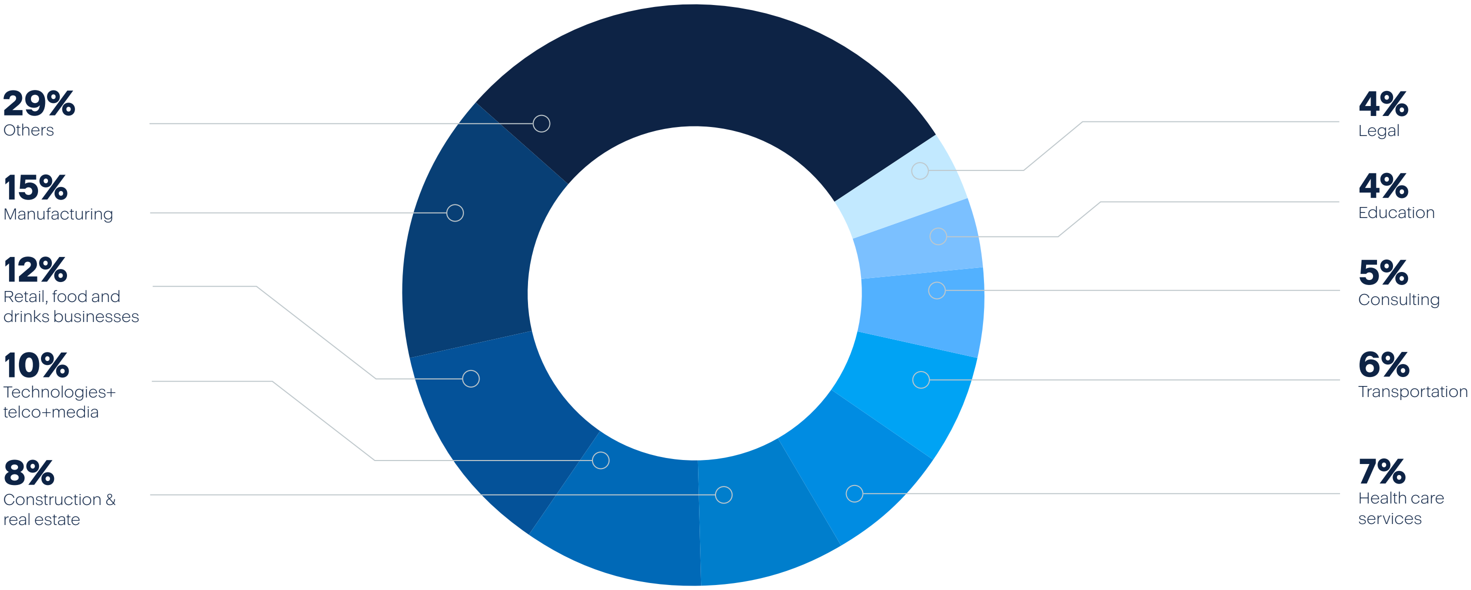
[4] U.S. Department of Justice. “Phobos Ransomware Affiliates Arrested in Coordinated International Disruption.” https://www.justice.gov/opa/pr/phobos-ransomware-affiliates-arrested-coordinated-international-disruption, February 20, 2025.

[5] Ravie Lakshmanan. “RansomHub Went Dark April 1; Affiliates Fled to Qilin, DragonForce Claimed Control.” The Hacker News. https://thehackernews.com/2025/04/ransomhub-went-dark-april-1-affiliates.html, April 20, 2025.

[6] James Coker. “Ransomware Attacks Fall in April Amid RansomHub Outage.” Infosecurity Magazine. https://www.infosecurity-magazine.com/news/ransomware-fall-april-ransomhub, May 5, 2025.

Manufacturing, retail and technologies[7] were the most targeted industries for ransomware attacks in Q1 2025. Lets take a deeper look into one of those industries.

Most targeted industries, Q1 2025

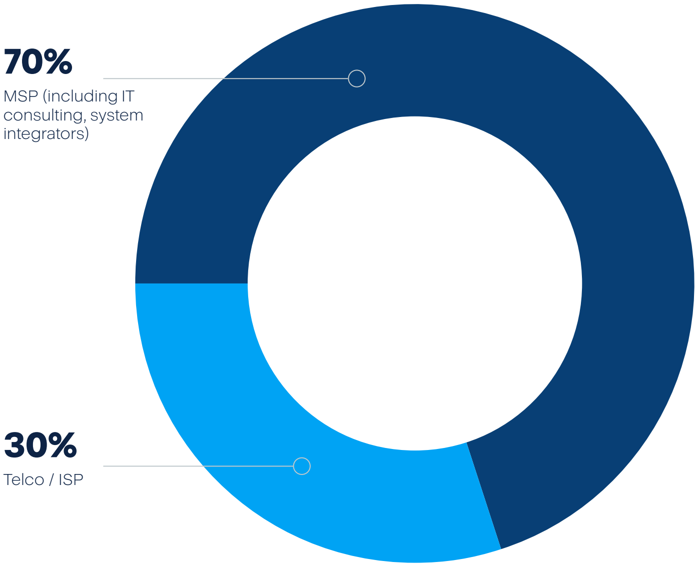


2. MSPs under attack

Based on data collected from across the globe,[7] this section examines cyberattacks targeting internet service providers (ISPs) / telecommunications and managed service providers (MSPs), including IT consulting firms and system integrators, from January 2025–May 2025.

The data reveals 67 cyberattacks, with the following division by categories:

Distribution by service types



The below chart shows the number of attacks on telcos / ISPs and MSPs in 2025 compared to the first half of 2024:

Category	2024	2025
Telco / ISP	14	20
MSP (including IT consulting, system integrators)	76	47
Total	**90**	**67**

[7] Data is compiled and sorted based on information collected from publicly available open-source intelligence (OSINT) repositories: ransomfeed.it; ransomware.live.

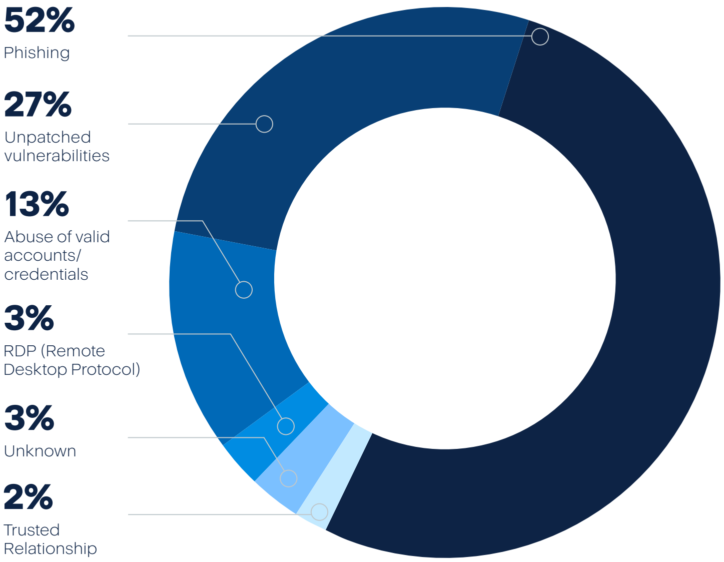
The rise in incidents targeting telco / ISP providers reflects growing attacker interest in infrastructure-level access, which can offer broad leverage over downstream services. Acronis observed this rise at the end of 2024, when we reported that APT-related groups were targeting telco companies.[8] Meanwhile, the drop in attacks against MSPs (from 76 to 47) might indicate improved security maturity or shifting attacker priorities — though MSPs' central role in client environments still makes them desirable targets. Let's dive into the details.

To maintain continuity with earlier reports, we are including IT consulting companies and system integrators under the broader category of MSPs. While their service offerings may vary, IT consulting companies, system integrators and MSPs share a core business model: providing outsourced IT expertise, infrastructure management and technical support to multiple clients. From a threat actor's perspective, they represent high-value targets with privileged access to numerous environments — making them operationally similar in terms of attack surface and risk exposure.

Therefore, we have combined both categories (telcos and MSPs) when analyzing initial access vectors, as they are frequently targeted through the same techniques and exploitation paths.

Let's take a look at the initial attack vector distribution through the recorded cases:

Initial access vectors



Phishing

MSPs can be breached when employees receive deceptive emails posing as clients or partners. These messages often lead to stolen credentials or malware infections through fake MFA (multifactor authentication) prompts or malicious attachments. In one case, attackers used a phishing email to steal an admin's RMM credentials, gaining access to multiple client environments.

Unpatched vulnerabilities

Attackers exploit known but unpatched flaws in MSP software such as RMM platforms or VPN tools. In several incidents, vulnerabilities in Atlassian Jira — including remote code execution and authentication bypass — were successfully leveraged to gain initial access. Once inside, attackers deployed infostealers to harvest credentials and tokens, enabling further lateral movement across MSP and client environments.

Valid account abuse / credential theft

MSPs are often targeted for their admin credentials, session tokens or reused passwords across platforms. Once attackers log in using stolen data, they bypass MFA and access cloud dashboards or RMM systems undetected. For instance, a hijacked Microsoft 365 session token allowed silent control over multiple client tenants.

Remote Desktop Protocol (RDP)

Attackers target exposed or misconfigured RDP services to gain remote access to MSP or client systems. They often brute-force credentials or exploit systems that trust MSP IPs. One breach occurred when an attacker accessed a vulnerable MSP backup server via RDP and then pivoted into internal and client environments.

Trusted relationship exploitation

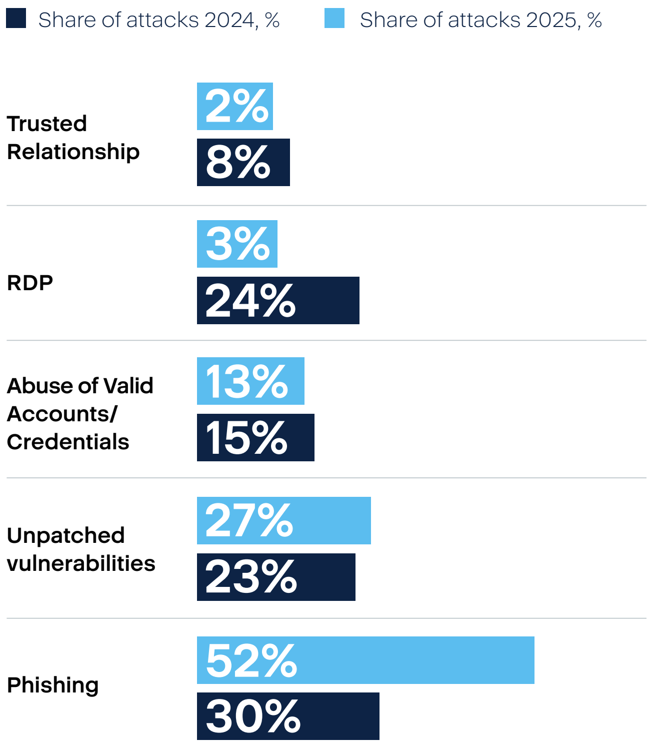
Once attackers compromise an MSP, they exploit built-in trust to access client systems via VPNs (virtual private networks) or remote tools. They may impersonate the MSP to deploy malicious updates or issue fraudulent support instructions. In one attack, ransomware was pushed to clients as a routine update through the MSP's RMM console.

[8] Acronis. "Acronis Cyberthreats Report, H2 2024: The rise of AI-driven threats." https://www.acronis.com/en-us/resource-center/resource/acronis-cyberthreats-report-h2-2024/, February 2025.

Compared to the same period in 2024, in the first half of 2025, the number of reported initial access incidents involving MSPs and similar providers declined from 90 to 67, signaling a positive trend likely driven by improved security practices. Phishing, however, has surged to dominate 52% of all cases. This marks a major shift in attacker tactics toward using social engineering schemes and exploiting human behavior over technical flaws — a trend amplified by AI-generated lures and hybrid work environments.[9]

In the same period, RDP-based exploits dropped sharply from 24% to just 3%, suggesting that widespread MFA adoption and improved endpoint hardening are paying off. Trusted relationship attacks also declined, falling from 8% to 2%, possibly due to better segmentation and zero trust principles adoption, such as least priviledge access, stronger identity verification and network segmentation, which has made it harder for attackers to move laterally via third parties. Some organizations have tightened third-party access, limiting what vendors can see or do inside the network.

Meanwhile, credential abuse remains persistent, with only a slight decrease (15% to 13%), as attackers continue to harvest valid tokens and passwords via infostealers.


Initial attack vectors: January-May comparison, 2024 vs. 2025

3 vulnerabilities in third-party software products that have been exploited in MSP-related attacks:

1. CVE-2024-50623 & CVE-2024-55956 – Vulnerabilities in Cleo file transfer tool

Although these CVEs date back to 2024, they continue to be exploited into 2025. Affecting the Cleo file transfer tool, the vulnerabilities allow attackers to bypass authentication or manipulate the system into providing unauthorized access. Notably, the Cl0p ransomware group exploited these vulnerabilities to breach a number of organizations, including financial institutions. Given that some MSPs rely on such tools to manage file transfers for their clients, these vulnerabilities represent a significant supply chain risk.

2. Cisco vulnerabilities (e.g., CVE-2023-20198 & CVE-2023-20273)

Although these Cisco vulnerabilities were disclosed in 2023, they continue to pose a threat in 2025 due to unpatched Cisco IOS XE devices in telecom networks. Exploited by Salt Typhoon (a China-linked APT group) and other threat groups, the vulnerabilities affect core networking devices in telco infrastructures. Once attackers gain access, they can intercept call and text metadata and potentially leverage these devices as a foothold into larger systems.

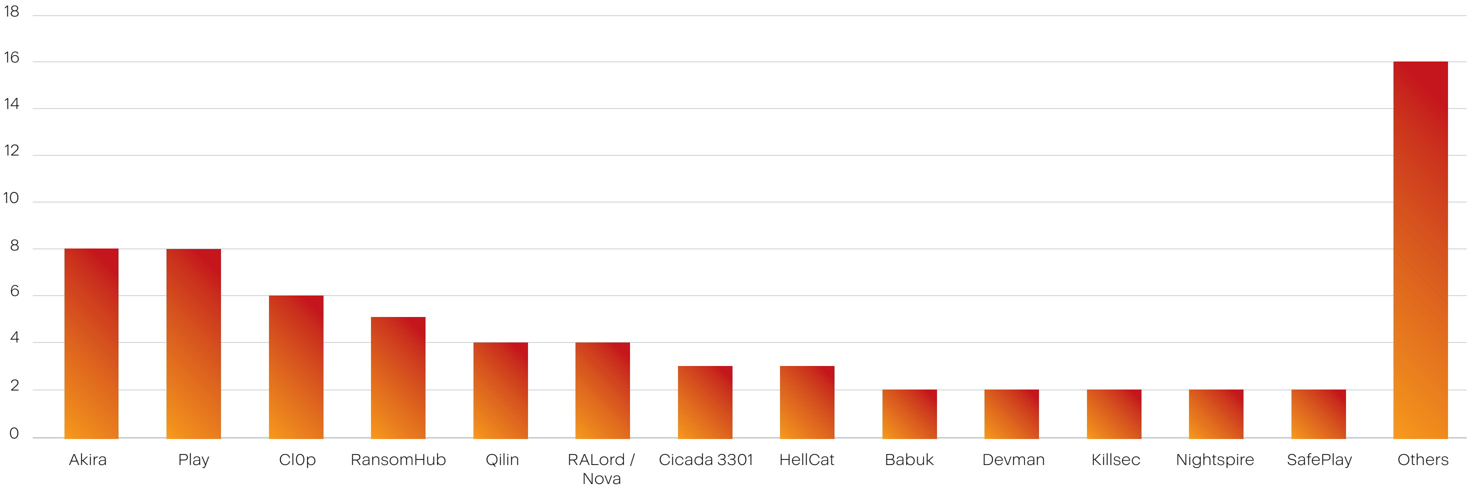
3. SimpleHelp RMM (CVE-2024-57726, CVE-2024-57727, and CVE-2024-57728)

On June 4, 2025, CISA, the FBI and other federal agencies issued a joint #StopRansomware advisory detailing how multiple ransomware groups, including initial access brokers linked to the Play ransomware gang, exploited CVE-2024-57727 in SimpleHelp RMM software. Threat actors exploited the flaw (T1190: Exploit Public-Facing Application) to gain remote access and execute malicious commands (T1059.001: Command and Scripting Interpreter) on SimpleHelp installations. Compromised SimpleHelp servers were used to deploy ransomware payloads and steal sensitive data by using backdoors such as Sliver across multiple U.S.-based entities.

[9] Lauren Goode. "Deepfakes, Scams, and the Age of Paranoia." Wired. https://www.wired.com/story/paranoia-social-engineering-real-fake, May 12, 2025; Zipdo. Social Engineering Statistics. https://zipdo.co/social-engineering-statistics, May 30, 2025.

The collected data reveals the number of victims per ransomware group from January 2025 to May 2025. The category "others" includes ransomware groups such as Abyss, ArcusMedia, BianLian, Ciphbit, Fog, Frag, FunkSec, Hunters International, INC Ransom, JGroup, Kraken (Hello Kitty), LockBit, Medusa and SilentRansomGroup (SRG).

Ransomware groups targeting MSPs



In H1 2025, Akira, Play, Cl0p, RansomHub, Qilin and RALord / Nova (covered in detail in the ransomware chapter of this report) emerged as the most active ransomware groups targeting MSPs and telecom providers. These groups display varied preferences for initial access: While Cl0p[10] continues exploiting known vulnerabilities in third-party software, others such as Akira[11] and RansomHub[12] rely heavily on phishing and credential theft, often supported by infostealers. These preferences reflect a broader trend toward flexible, multivector intrusions that provide the most efficient path based on the target's defenses and exposure.

Attacks on MSPs in H1 2025

Attacks on MSPs now occur on regular basis and affect providers of all sizes and in regions around the world. Below are just three cases, each revealing the damage that can result from breaches on service providers who have unfettered access to client infrastructure.

1 In January 2025, Telefonica,[13] a Spanish telecommunications company, suffered a breach that exposed the personal data of over 20,000 employees and leaked sensitive information from its internal Jira system. Allegedly linked to the Hellcat ransomware group, attackers used infostealer malware (Redline) to compromise the credentials of at least 15 employees to gain initial access to corporate systems. They then used social engineering tactics, posing as internal staff to extract critical information, escalate privileges and exfiltrate 2.3GB of data, including customer records, internal documents and over 500,000 Jira issues. In one case, a fake Jira ticket submitted via a compromised Telefonica account tricked admins into confirming the correct server for SSH access. This enabled the attackers to focus their brute-force efforts and bypass internal segmentation. The breach revealed critical vulnerabilities in Telefonica's infrastructure and highlighted the widespread presence of infostealers — more than 500 employee devices were infected in 2024. There were 4,200 instances in which employees infected by infostealers (Lumma infostealer) had used their corporate credentials to access third-party systems, such as Office365, Salesforce, Fortinet and others.

[10] Arun KL. "Cl0p Ransomware." TheSecMaster. https://thesecmaster.com/blog/clop-ransomware, March 14, 2025.

[11] Cybersecurity and Infrastructure Security Agency (CISA). "#StopRansomware: Akira Ransomware." https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a, April 18, 2024.

[12] Cybersecurity and Infrastructure Security Agency (CISA). "#StopRansomware: RansomHub Ransomware." https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a, August 29, 2024.

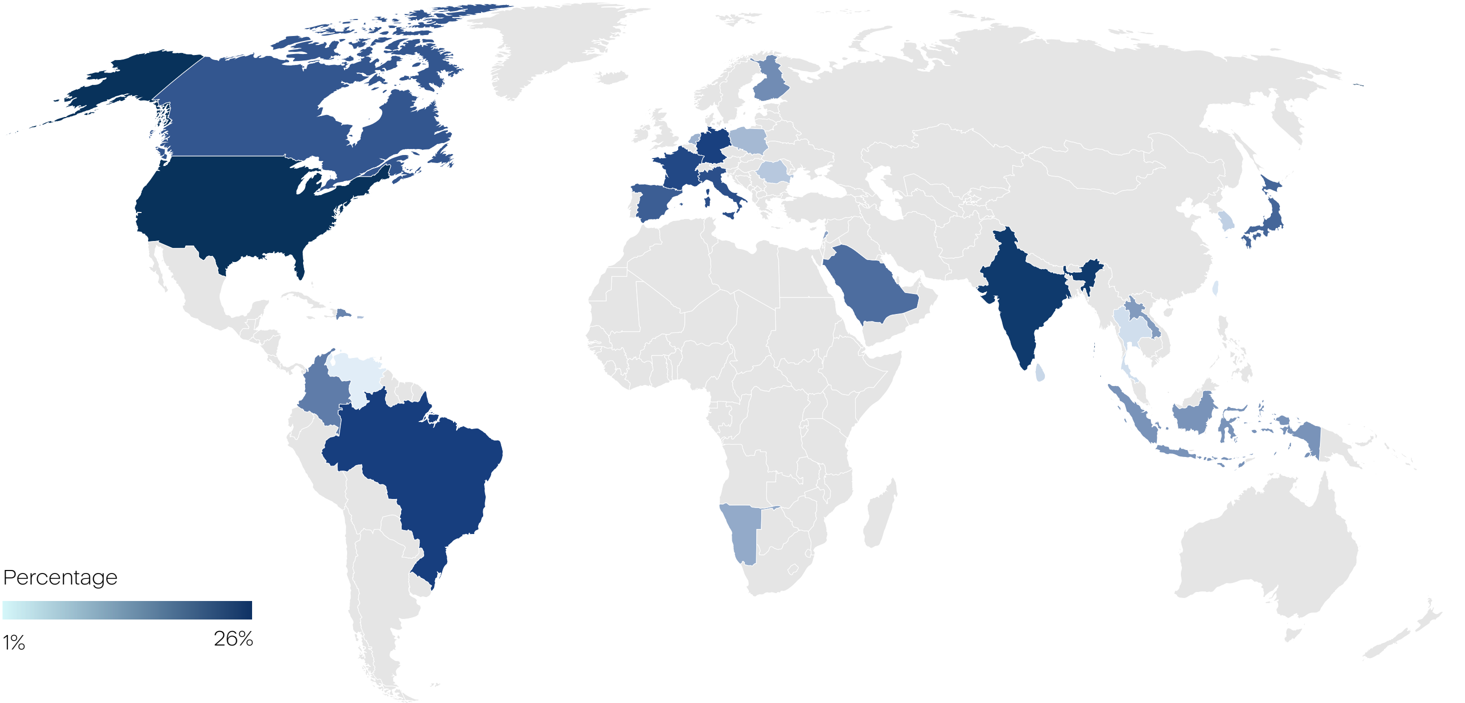
[13] Gal, Alon. "Telefonica Breach: Infostealer Malware Opens Door for Social Engineering Tactics." Infostealers. https://www.infostealers.com/article/telefonica-breach-infostealer-malware-opens-door-for-social-engineering-tactics/, January 11, 2025.

❷ In February 2025,[14] the Qilin ransomware group claimed responsibility for the breach of Virtual IT, a technology provider serving businesses across several U.S. cities. While the exact method of compromise remains unconfirmed, Qilin is known for leveraging phishing emails, credential theft or exploiting unpatched vulnerabilities to infiltrate networks and encrypt sensitive data. Their tactics align with a broader ransomware trend targeting service providers, using access to one IT partner to potentially reach multiple downstream clients.

❸ In April 2025,[15] the HellCat ransomware group struck IT solutions provider Asseco Poland by exploiting Jira credentials previously stolen via infostealer malware. Asseco Poland belongs to the multinational Asseco Group, Europe's sixth-largest software vendor, operating in 62 countries with 34,000 employees and the largest software producer on the Warsaw Stock Exchange. The breach trail led to StealC infostealer, which silently harvested credentials from infected machines months before the attack, enabling HellCat to infiltrate Jira, move laterally across systems, exfiltrate sensitive data and ultimately deploy ransomware.

While all MSPs are potential targets for cyberattacks, MSPs in certain countries were targeted more than others from January to May 2025, with the largest share being in North America.

Most targeted countries for MSP attacks from January 2025–May 2025



The expectation of enforcement of the EU NIS 2 Directive enforced in October 2024 might have influenced improved cybersecurity postures among MSPs and infrastructure providers, potentially reducing attack volumes observed across several European countries in 2025. Germany, Spain, the Netherlands and Belgium reported fewer ransomware incidents, possibly due to preparations for stricter supply chain security, mandatory risk assessments and rigorous incident reporting requirements under NIS 2. Meanwhile, the U.S. leads among the targeted countries, but compared to the same period in 2024, attackers shifted focus to regions outside the Directive's scope, including Brazil, and emerging markets such as India, the Dominican Republic and Namibia — where cybersecurity regulations and maturity remain comparatively lower.

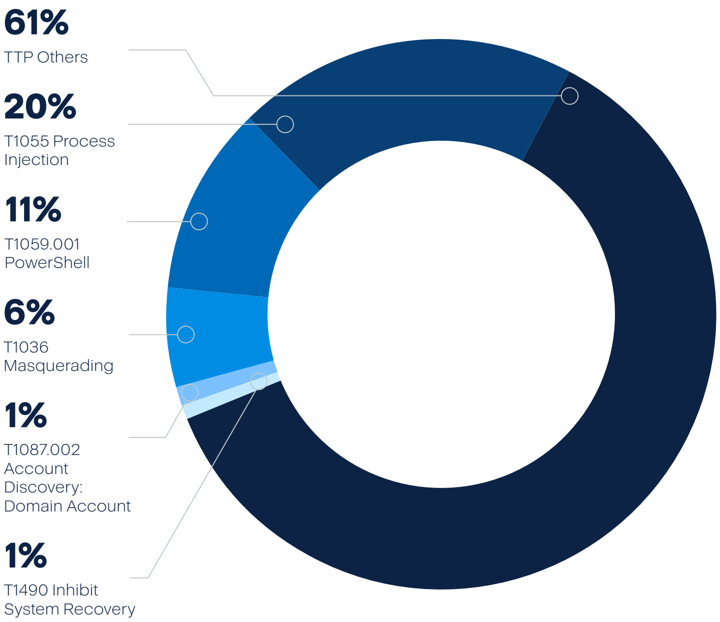
[14] Undercode News. "Ransomware Attack Alert: Qilin Targets Virtual IT and Altair Travel." https://undercodenews.com/ransomware-attack-alert-qilin-targets-virtual-it-and-altair-travel/, February 3, 2025.

[15] Alon Gal. "HELLCAT Ransomware Group Strikes Again: Four New Victims Breached via Jira Credentials from Infostealer Logs." Infostealers. https://www.infostealers.com/article/hellcat-ransomware-group-strikes-again-four-new-victims-breached-via-jira-credentials-from-infostealer-logs/, April 5, 2025.

Most used MITRE techniques

The MITRE ATT&CK framework categorizes adversary behavior into tactics and techniques. This helps malware analysts efficiently identify, assess and respond to threats. The collected information is based on Acronis telemetry from Acronis EDR from January 1, 2025–March 31, 2025.

Top 5 most frequently seen MITRE ATT&CK techniques, Q1 2025



Process Injection (T1055.001)

Summary: Attackers inject malicious code into legitimate processes, such as via DLL injection, to evade detection.

Detection: Look for anomalous API calls (e.g., CreateRemoteThread) and monitor processes for unexpected memory modifications or behavior. EDR solutions can provide real-time detection of injection attempts.

Mitigation: Implement EDR with behavior-based detection, enable memory integrity features and enforce strict application control policies to reduce exploitation opportunities.

PowerShell (T1059.001)

Summary: PowerShell is often abused to execute scripts with hidden windows (e.g., powershell.exe -WindowStyle Hidden), allowing threat actors to run obfuscated commands without drawing user attention.

Detection: Detect anomalous PowerShell activity through detailed logging. Monitor for suspicious command-line arguments, unusual Base64-encoded payloads, hidden windows or unexpected network connections initiated by scripts.

Mitigation: Enforce signed-script policies, utilize logging and and script-block logging for enhanced visibility.

Masquerading (T1036)

Summary: Adversaries disguise files, processes or services to appear legitimate (e.g., using renamed files / executables to match legitimate files).

Detection: Identify inconsistencies in metadata and file paths, and apply application white listing to block unauthorized executables.

Mitigation: Apply application white listing and enforce file execution policies to block unapproved executables and scripts.

Account Discovery: Domain Account (T1087.002)

Summary: Attackers query Active Directory to gather information on domain accounts for lateral movement.

Detection: Identify unusual LDAP queries or enumeration attempts, and limit account permissions and access to directory services.

Mitigation: Limit the visibility of account information through least privilege principles, disable unnecessary accounts and use tools like honeypot accounts to detect enumeration attempts.

Inhibit System Recovery (T1490)

Summary: Common in ransomware, this technique disables Windows system recovery features like shadow copies to prevent rollback.

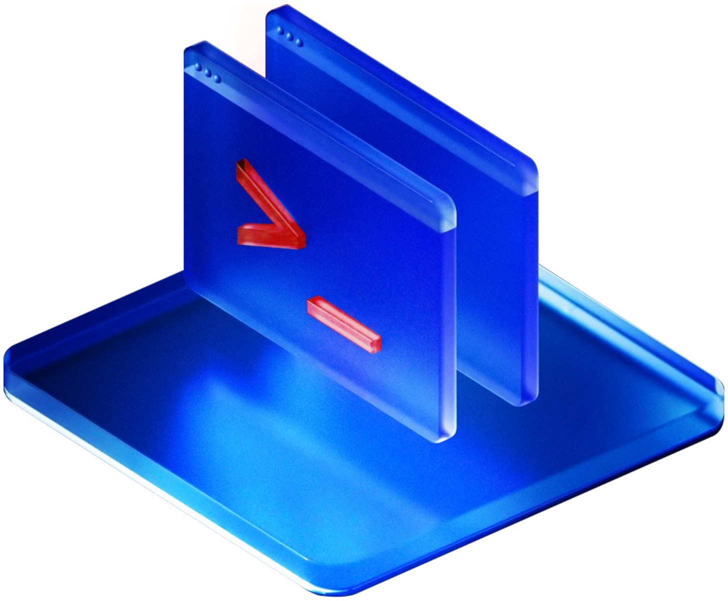
Detection: Identify unauthorized deletion of backups and enforce backup protection policies with restricted access and versioning controls.

Mitigation: Enforce backup protection policies, restrict access to system recovery tools and ensure versioning and off-site backups are in place.

3. RMMs: A growing attack vector

Remote monitoring and management (RMM) tools, once a cornerstone of efficient IT operations, have increasingly become a double-edged sword in the cybersecurity domain. Originally designed to help MSPs, MSSPs and IT departments remotely manage endpoints, push updates and troubleshoot issues, these tools offer powerful capabilities, including remote access, automation and centralized control.

Unfortunately, those same features are now being weaponized by cybercriminals seeking stealth, persistence and scale in their operations. Ransomware actors are abusing RMM platforms to blend into legitimate administrative activity, evade endpoint defenses, and silently deploy malicious payloads. This tactic, aligned with “living off the land” (LotL) techniques, allows attackers to operate under the radar by exploiting trusted, preinstalled applications rather than dropping unfamiliar binaries that could trigger detection. Initial access is often obtained through phishing, social engineering, stolen credentials or unpatched vulnerabilities — after which, adversaries deploy RMM agents or hijack existing ones to move laterally, exfiltrate data and execute ransomware at scale.



In 2025, the trend accelerated, with over 51 RMM solutions identified as potential attack vectors. Some tools are more frequently targeted than others. Splashtop, ConnectWise ScreenConnect and Atera have been repeatedly abused in real-world intrusions.[16]

[16] 1. [Akira ransomware]. Cybersecurity and Infrastructure Security Agency (CISA). “#StopRansomware: Akira Ransomware,” https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a, April 18, 2024; Arun KL. “Akira Ransomware.“ TheSecMaster. https://thesecmaster.com/blog/akira-ransomware, February 24, 2025

2. [ALPHV Blackcat ransomware]. Cybersecurity and Infrastructure Security Agency (CISA). “#StopRansomware: ALPHV Blackcat.” https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a, February 27, 2024; Bill Cozens. “Why ransomware gangs love using RMM tools—and how to stop them.” Threat-Down – Malwarebytes. https://www.threatdown.com/blog/why-ransomware-gangs-love-using-rmm-tools-and-how-to-stop-them/, February 22, 2024.

3. [BianLian ransomware]. Arun KL. “BianLian, The Shape-Shifting Ransomware Group.” TheSecMaster. https://thesecmaster.com/blog/bianlian-the-shape-shifting-ransomware-group, March 15, 2025.

4. [Black Basta ransomware]. Cybersecurity and Infrastructure Security Agency (CISA). “#StopRansomware: Black Basta.” https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a, November 8, 2024.

5. [Cactus ransomware]. Halcyon. “Halcyon Ransomware Malicious Quartile Q1-2025.” https://www.halcyon.ai/resources/reports/halcyon-ransomware-malicious-quartile-q1-2025, April 14, 2025.

6. [LockBit ransomware]. Deeba Ahmed. “TeamViewer Exploited to Obtain Remote Access, Deploy Ransomware.” Hack Read. https://hackread.com/teamviewer-exploited-remote-access-ransomware/, January 23, 2024.

7. [Medusa ransomware]. Cybersecurity and Infrastructure Security Agency (CISA). “#StopRansomware: Medusa Ransomware.” https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a, March 12, 2025.

8. [Play ransomware]. Cybersecurity and Infastructure Security Agency (CISA). #StopRansomware: Play Ransomware.” https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a, June 4, 2025.

9. [RansomHub ransomware]. Cybersecurity and Infastructure Security Agency (CISA). “#StopRansomware: RansomHub Ransomware.” https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a, August 29, 2024.

10. [Royal ransomware]. Bill Cozens. “Why ransomware gangs love using RMM tools—and how to stop them.” ThreatDown – Malwarebytes. https://www.threatdown.com/blog/why-ransomware-gangs-love-using-rmm-tools-and-how-to-stop-them/, February 22, 2024;

11. [DragonForce ransomware]. Lawrence Abrams. “DragonForce ransomware abuses SimpleHelp in MSP supply chain attack.” Bleeping Computer. https://www.bleepingcomputer.com/news/security/dragonforce-ransomware-abuses-simplehelp-in-msp-supply-chain-attack/, May 27, 2025; Cybersecurity and Infrastructure Security Agency (CISA). “Ransomware Actors Exploit Unpatched SimpleHelp Remote Monitoring and Management to Compromise Utility Billing Software Provider.” https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-163a, June 12, 2025.

RMMs / RaaS	Cactus	BianLian	ALPHV	LockBit	Medusa	Royal	RansomHub	Black Basta	Akira	Play	DragonForce
Action1				✓							
Atera		✓	✓	✓	✓	✓		✓			
ConnectWise ScreenConnect			✓	✓	✓	✓	✓	✓		✓	
GoTo								✓			
LogMeIn						✓					
N-Able					✓		✓				
QuickAssist								✓		✓	
RustDesk									✓	✓	
Splashtop	✓	✓	✓	✓	✓		✓	✓		✓	
SuperOps	✓										
SimpleHelp										✓	✓
TeamViewer		✓	✓	✓					✓	✓	

Once RMM access is achieved, adversaries can disable backups, push ransomware to multiple endpoints and wreak havoc — often without triggering traditional security alerts. To counter this growing threat, organizations must treat RMM infrastructure as a high-value asset. Critical defenses include enforcing multifactor authentication, rigorously applying patches, auditing RMM configurations and continuously monitoring for unusual remote access behavior. Leaving RMM tools underprotected is not just a risk — it's an open invitation.

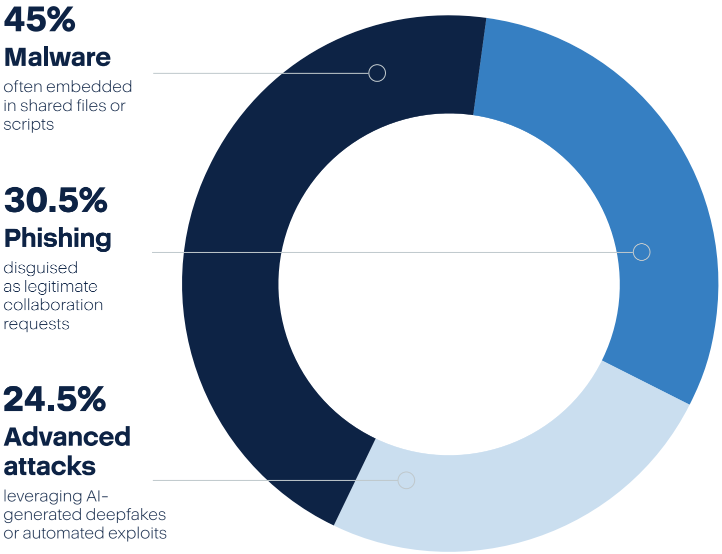
4. Cybercriminals switching attacks from email to collaboration apps

The following email, phishing and collaboration apps statistics were collected from Acronis Email Security, which is powered by Perception Point. Acronis and Perception Point work together to protect organizations and ensure they remain safe from email-borne threats. The data was gathered for the first half of 2025 and combined with Acronis telemetry data for malware and URL blocks on endpoints. Later in this report, you'll find a dedicated section highlighting a collection of malicious websites that have been blocked.

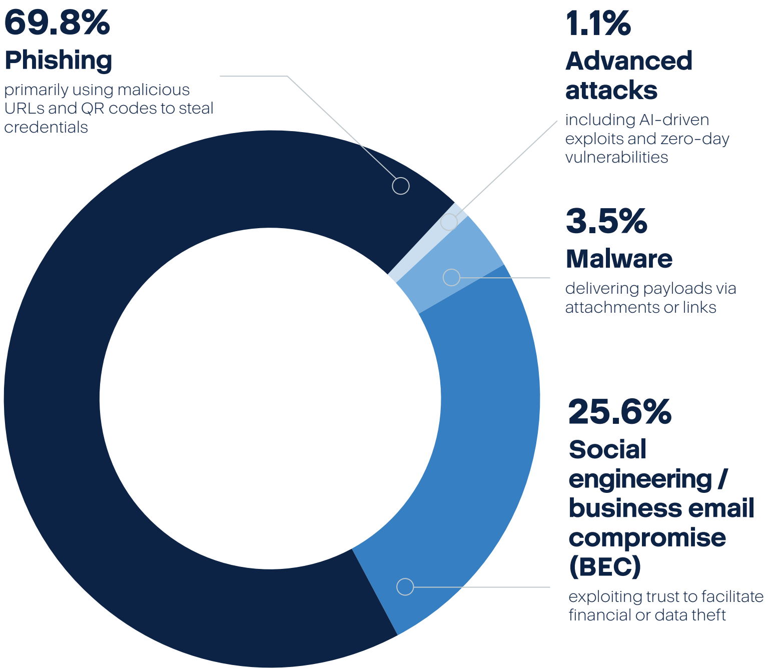
Email and collaboration apps, such as Microsoft 365 and Microsoft Teams, continue to be prime targets for cybercriminals due to their critical role in organizational communication. The first half of 2025 has revealed a dynamic threat landscape, with attackers leveraging advanced techniques like AI-driven phishing and malware to exploit these platforms.

From January 1, 2025 to May 15, 2025, Acronis Email Security scanned 714,637,634 emails and 1,278,047,714 files and URLs. A total of 7,201,107 attacks were detected, equating to 205 attacks per organization per month. Of the scanned emails, 30.2% were classified as spam, and 1.1% were malicious, containing phishing links, malware or advanced attack payloads.

We also observed a new trend: Cybercriminals started to focus more on collaboration apps. The below graphic shows the distribution of attacks in collaboration apps, with advanced attacks rising dramatically to almost 25%:



Email attack types were distributed as follows:



Additionally, in an examination of Microsoft 365 email backups in Acronis Cyber Protect Cloud, 1.47% of the scanned resources were affected by malware. Forty percent of URLs in the email backups were phishing links and 30% were malicious links.

Year-over-year changes

Malware in collaboration apps fell sharply from 82% to 45%, while alarmingly, phishing rose from 9% to 30.5% and advanced attacks increased from 9% to 24.5%. This shift indicates attackers are diversifying tactics, focusing on phishing and possibly AI-driven attacks in collaboration platforms.

Total email attacks decreased by 6.5% (7.2 million vs. 7.7 million), and attacks per organization per month dropped by 29.6% (205 vs. 291). This reduction seems to indicate that improved email filtering technologies are blocking more threats before they reach users.

The spam ratio rose slightly from 27.6% to 30.2%, indicating persistent high-volume, low-effort attacks. The malicious email ratio fell from 1.5% to 1.1%, suggesting attackers are shifting toward more targeted, high-impact attacks.

Phishing dropped from 79% to 69.8% but social engineering / BEC increased from 20% to 25.6%, reflecting the use of AI to craft convincing impersonations. Malware declined slightly from 4% to 3.5%, with cybercriminals focusing on delivering malware at later stages of attacks. Advanced attacks remained stable at 1%–1.1%.

However, if we look back to 2023, the overall picture has remained relatively stable in terms of spam and malware ratios. The small fluctuations observed are similar to the seasonal variations typically seen in overall threat volumes.

Report	Spam ratio (%)	Malicious / phishing ratio (%)
H1 2023	30.3%	1.3%
H2 2023	~33.4%	1.3%
H1 2024	27.6%	1.5%
H2 2024	31.4%	1.4%
H1 2025	30.2%	1.1%

Notable phishing campaigns

CoGUI phishing campaign (January–April 2025)

The CoGUI phishing kit, active since October 2024, sent over 580 million emails between January and April 2025, targeting payroll and payment platforms to steal credentials and execute wire fraud. The campaign impersonated brands like Amazon, PayPal and tax agencies, with a peak of 172 million emails in January alone.[17]

The sheer volume suggests millions of potential victims, particularly in Japan, though the U.S., Canada, Australia and New Zealand were also targeted. The focus on financial systems heightened the risk of significant economic losses.

CoGUI's unprecedented email volume and multicountry targeting, facilitated by multiple threat actors (likely from China), make it one of the largest phishing campaigns tracked in 2025.

DarkWatchman and Sheriff malware campaign (January–May 2025)

This campaign delivered DarkWatchman and Sheriff malware via phishing emails with password-protected malicious archives, targeting organizations in Eastern Europe.[18] The Sheriff backdoor, hosted on Ukraine's ukr.net, exfiltrated data and captured screenshots, while DarkWatchman focused on stealth and persistence.

The campaigns affected numerous organizations, potentially disrupting critical infrastructure and supply chains due to its geopolitical focus. The campaign's nation-state-like tactics and regional targeting, combined with advanced malware, mark it as a sophisticated threat with espionage or disruption motives.

PointyPhish and TollShark smishing campaign (February–May 2025)

Powered by the Darcula phishing-as-a-service platform[19], this smishing (SMS phishing) campaign sent texts posing as toll agencies or reward programs, using over 5,000 domains to steal payment information. It targeted users globally via iMessage and RCS.

In a campaign that affected millions worldwide, 884,000 credit cards were stolen from 13 million clicks on malicious links. The campaign's use of iMessage / RCS to bypass SMS firewalls and its massive domain infrastructure mark it as a highly scalable threat.

Fake recruitment targeting CFOs (May–June 2025)

A recent spear-phishing campaign was identified targeting chief financial officers (CFOs) and financial executives across various global regions, including Europe, Africa, Canada, the Middle East and South Asia.[20] Attackers impersonated recruiters from Rothschild & Co., offering enticing "strategic opportunities" to lure victims. It featured emails containing links that redirected to a Firebase-hosted page, where the actual malicious URL was encrypted and only revealed after the victim completed a CAPTCHA challenge.

This tactic is designed to evade automated security systems. Upon solving the CAPTCHA, victims download a ZIP archive containing a Visual Basic Script (VBScript), which initiates a multistage infection process. This process ultimately installs legitimate remote access tools — NetBird and OpenSSH — on the victim's system. The malware then creates a hidden local account, enables remote desktop access, and ensures persistence by configuring NetBird to launch on system reboot, all while removing desktop shortcuts to avoid detection. This sophisticated attack underscores the increasing use of legitimate tools by cybercriminals to establish and maintain unauthorized access to targeted systems.

[17] Genina Po, Kyle Cucci, et. al. "CoGUI Phish Kit Targets Japan with Millions of Messages." Proofpoint. https://www.proofpoint.com/us/blog/threat-insight/cogui-phish-kit-targets-japan-millions-messages, May 6, 2025.

[18] Alessandro Mascellino. "Large-Scale Phishing Campaigns Target Russia and Ukraine." Infosecurity Magazine. https://www.infosecurity-magazine.com/news/phishing-campaigns-targets-russia/, 1 May 2025.
Daryna Antoniuk. "DarkWatchman cybercrime malware returns on Russian networks." The Record. https://therecord.media/darkwatchman-malware-russia-cybercrime-hive0117, April 30, 2025.

[19] Bill Toulas. "Darcula PhaaS steals 884,000 credit cards via phishing texts." Bleeping Computer. https://www.bleepingcomputer.com/news/security/darcula-phaas-steals-884-000-credit-cards-via-phishing-texts/, May 5, 2025.

[20] Srini Seethapathy. "A Flyby on the CFOs Inbox: Spear Phishing Campaign Targeting Financial Executives with NetBird Deployment." Trellix. https://www.trellix.com/blogs/research/cfo-spear-phishing-netbird-attack/, May 28, 2025.

Cybercriminals are adapting and diversifying

The H1 2025 data reveals a sophisticated and adaptive threat landscape. While phishing, malware distribution and account takeover are not new, they are now increasingly targeting collaboration apps. Attackers are exploiting the trust users place in real-time communication tools, using tactics like deepfake-based BEC to impersonate CEOs to bypass traditional defenses. The persistence of advanced attacks, though low in volume, indicates that zero-day exploits and AI-driven threats remain a critical concern.

While phishing remains the dominant email attack vector, its decline from 79% to 69.8% indicates that traditional phishing tactics are being countered by improved detection systems. Yet, as noted in section 2 of this report, phishing was the initial attack vector in half the attacks on MSPs.

The rise in social engineering / BEC, driven by AI-generated content, underscores the need for behavioral analysis to detect subtle impersonation tactics. The reduction in overall attack volume suggests that organizations are improving their defenses, but the diversification of attack types in collaboration apps indicates that cybercriminals are adapting to exploit new vulnerabilities.

5. Vulnerabilities: A big headache for MSPs

According to the National Vulnerability Database (NVD), the total number of Common Vulnerabilities and Exposures (CVEs) published January–April 2025 is as follows:

Month	CVEs
January 2025	~1,200
February 2025	~1,100
March 2025	~1,300
April 2025	~1,400

This totals to around 5,000 CVEs reported industrywide in the first four months of 2025. This represents a significant increase compared to the same period in 2024, where approximately 4,000 CVEs were reported. Acronis attributes the increase to heightened security research activities and improved vulnerability disclosure practices.

Total vulnerabilities patched across all vendors
According to our conservative estimate based on vendor patch cycles and bulletins, vendors patched approximately 2,400 CVEs, compared to the estimated 5,000 reported between January 2025 and April 2025. This estimate is based on aggregation of publicly disclosed security advisories, vendor-specific patch bulletins (e.g., Microsoft, Adobe, Cisco, Google, Oracle and others), and automated feeds from major repositories such as CISA's Known Exploited Vulnerabilities Catalog and vendor APIs. Only CVEs explicitly listed as resolved or addressed in official bulletins were counted.

The above estimate excludes duplicates, reclassifications or advisories lacking formal CVE attribution. To ensure a conservative approach, CVEs tied to legacy or unsupported product lines were excluded unless explicitly labeled as patched. Data was normalized across vendors with varying disclosure formats to reduce double counting. That fewer than half of reported vulnerabilities were patched is not surprising, and it reveals that many vulnerabilities remain unpatched for long periods of time and possess serious security risks.

Notable zero-day vulnerabilities

There were several notable cases of critical zero-day vulnerabilities that were identified from the beginning of 2025 and were patched during this period:

- **CVE-2025-21333, CVE-2025-21334, CVE-2025-21335:** Elevation of privilege vulnerabilities in Windows Hyper-V, allowing attackers to gain SYSTEM privileges.
- **CVE-2025-21391:** Elevation of privilege vulnerability in Windows Storage, enabling attackers to delete targeted files, potentially leading to service unavailability.
- **CVE-2025-21418:** Elevation of privilege vulnerability in the Windows Ancillary Function Driver for WinSock, allowing attackers to gain SYSTEM privileges.
- **CVE-2025-24985:** Remote code execution vulnerability in the Windows Fast FAT File System Driver, exploitable via specially crafted virtual hard disks.
- **CVE-2025-24993:** Remote code execution vulnerability in Windows NTFS, exploitable through crafted virtual hard disks.
- **CVE-2025-26633:** Security feature bypass vulnerability in Microsoft Management Console, allowing attackers to circumvent security measures.

These vulnerabilities were actively exploited in the wild,[21] underscoring the importance of timely patching and system updates.

What we see among our customers

Acronis Cyber Protect Cloud includes a vulnerability assessment feature that automatically inspects endpoints for known vulnerabilities, and Acronis RMM automatically patches those vulnerabilities. Due to the native integration of security and RMM in Acronis Cyber Protect Cloud, we have global insights into the vulnerability landscape based on data from our customers' machines.

[21] Cybersecurity and Infrastructure Security Agency (CISA). "Known Exploited Vulnerabilities Catalog." https://www.cisa.gov/known-exploited-vulnerabilities-catalog, updated June 25, 2024.

Top 10 vulnerable software products globally among Acronis customers (January–May 2025)

Product	Unique CVEs	Percentage of affected clients
Windows 11	1,288	41.35
Windows Server 2019	2,707	31.87
Windows 10	2,875	30.97
7-zip	10	22.52
Microsoft .NET 8.0	14	18.53
Mozilla Firefox	1,833	16.93
Microsoft Visual Studio 2010	6	16.51
Microsoft Visual Studio 2008	14	12.16
Microsoft OL EDB Driver 18 For SQLServer	1	10.32
Microsoft Server Operating System-21H2	473	10.24

Unsurprisingly, among Acronis customers, those using Windows OSs experienced the largest amount of vulnerabilities — Windows 11 is the most popular desktop operating system in use. However, when examining Window Server OS usage, we see an alarming trend: Even when the number of vulnerabilities in Windows Server exceeds those of Windows 11, admins are quicker to patch Windows 11. The same trend applies to Windows 10, despite it having far more vulnerabilities than Windows 11. If you still use Windows 10 in your environment, we highly recommend paying attention to it.

Internet browsers and Adobe software products made the list of the top 10 software products with the largest number of vulnerabilities and users affected. Among the software used by Acronis MSP partners, TeamViewer, WireShark and AnyDesk had the most unique CVEs.

If we investigate specific software used in MSP environments, we see a huge prevalence of TeamViewer vulnerabilities. Almost 5% of our customers have unpatched vulnerabilities in TeamViewer. AnyDesk is used less and fewer vulnerabilities were detected. It is, however, a remote management tool and highly vulnerable from a security perspective as remote access tools are very often used in attacks, making patching a top priority. The total number of customers with nonpatched vulnerabilities is low, revealing that people are adopting patch management and applying patches in a timely way.

As noted in the MSP threats section of the report, software vulnerabilities are frequently exploited in attacks on MSPs. The MSP software tools noted below are three potential access points for attackers.

Top 3 most vulnerable MSP software tools for Windows (January 2025–May 2025)

Product	Unique CVEs	Percentage of affected clients
TeamViewer	9	4.56%
WireShark	79	0.06%
AnyDesk	3	0.05%

6. AI-powered cyberthreats: Hyper-realistic phishing, autonomous malware and deepfake social engineering

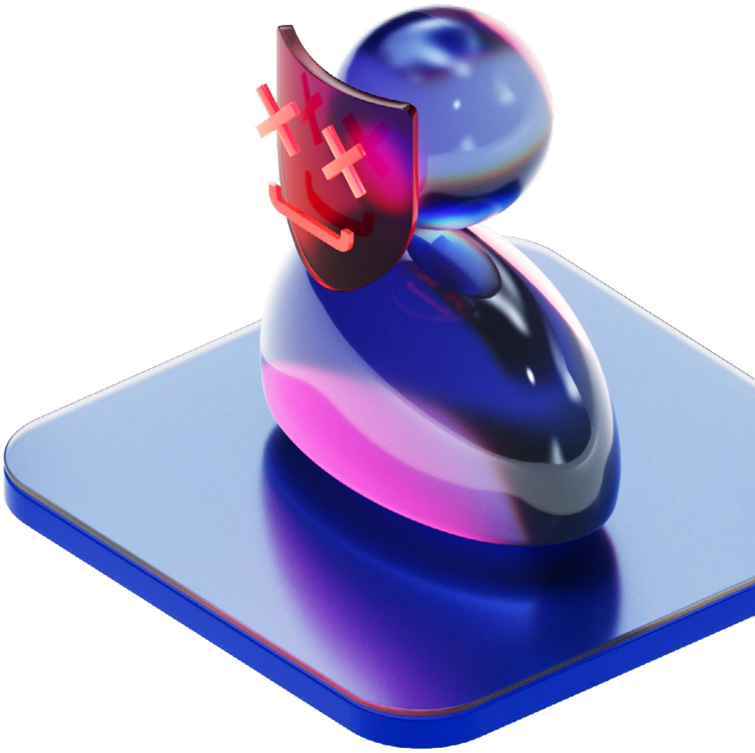
In 2025, the integration of AI into cybercriminal activities contined to shape the cybersecurity landscape. The rise of AI-powered cyberthreats has led to the proliferation of cybercrime-as-a-service (CaaS) models. On the dark web, AI-driven tools and services are being offered to less technically skilled criminals, democratizing access to sophisticated attack capabilities. This trend lowers the barrier to entry for cybercrime, enabling a broader range of actors to conduct complex attacks.

Let's look into some key cases we observed in the first half of 2025.

1. North Korean operatives use AI and deepfakes to infiltrate technology companies

In one of the most alarming examples of AI misuse in 2025, North Korean cyber operatives were discovered using synthetic identities and deepfake technologies to gain employment at Western technology companies. These operatives posed as remote developers by fabricating job histories and credentials, and then passed real-time video interviews using deepfake avatars that masked their true identity. U.S. officials reported that in many cases, the group relied on legitimate LinkedIn profiles, resumes and remote job boards like Upwork and Freelancer to blend in. These operatives were fully employed at companies, receiving salaries and access to critical systems for months before being detected.

The U.S. Department of Justice (DOJ) charged two U.S.-based facilitators[22] who helped more than 150 North Korean workers gain employment across various firms. In these roles, the operatives not only collected income that was funneled back to the Democratic People's Republic of Korea's (DPRK) weapons programs but also had potential access to sensitive source code, internal documents and, in some cases, proprietary AI development environments. According to FBI and DOJ statements, many of these positions were granted without in-depth onboarding verification or identity checks, a vulnerability that these actors exploited at scale. The use of AI-driven deepfake software enabled the attackers to participate in interviews by lip-syncing prerecorded or generated video, masking language barriers and location discrepancies.



[22] U.S. Department of Justice. "Two North Korean Nationals and Three Facilitators Indicted for Multi-Year Fraudulent Remote Information Technology Worker Scheme that Generated Revenue for the Democratic People's Republic of Korea." https://www.justice.gov/opa/pr/two-north-korean-nationals-and-three-facilitators-indicted-multi-year-fraudulent-remote, January 23, 2025.

That many of these operatives were placed at IT service companies and SaaS providers raises questions about downstream access risks. The incident shows how AI tools, when combined with low operational risk and high monetary incentives, can empower nation-state actors to bypass even well-guarded hiring processes. This also emphasizes the need for continuous employee monitoring and endpoint behavior analytics to detect anomalous activity, even after an employee is onboarded.

2. DeepSeek AI model exposes sensitive data

In January 2025, cybersecurity researchers uncovered significant vulnerabilities within the DeepSeek AI model,[23] a tool developed by a Chinese AI startup. These weaknesses, known as prompt injection attacks, allowed hackers to manipulate the AI's responses by embedding hidden instructions in input data. When exploited, these prompts led the AI to leak sensitive data or perform unintended actions that could compromise organizational security. While these types of vulnerabilities are not exclusive to DeepSeek, the scope is broad, affecting everything from chatbots to autonomous AI agents and multistep tool-using systems. Further investigation revealed that DeepSeek's mobile app sent unencrypted user data to servers controlled by ByteDance, raising concerns over privacy violations.

This case exemplifies the potential risks of deploying large language models without adequate security measures, especially when sensitive information is involved. We have some recommendations about where to start in our final section of this report.

3. Deepfake investment scams on social media

AI-generated deepfake technology is being exploited by scammers to impersonate well-known public figures to trick users into engaging in fraudulent investment schemes on social media platforms such as Instagram, Facebook and WhatsApp. One of the most alarming cases in 2025 saw the likeness of Financial Times journalist Martin Wolf being used to promote fake investment opportunities[24] in cryptocurrency and stocks, which reached nearly a million unsuspecting users across the EU. The deepfake video featured a convincingly fake interview with Wolf, in which he allegedly praised certain high-risk investments.

These scams prey on the trust users have in familiar figures, making it difficult for the average person to detect the fraud. Users should remain highly skeptical of investment advice or financial endorsements appearing in videos or messages on social media, even when featuring trusted public figures. Always verify such content through official channels, such as the public figure's verified website or mainstream media, and never act on investment opportunities promoted via private messages or unfamiliar pages.

[23] Gal Nagli. "Wiz Research Uncovers Exposed DeepSeek Database Leaking Sensitive Information, Including Chat History." Wiz. https://www.wiz.io/blog/wiz-research-uncovers-exposed-deepseek-database-leak, January 29, 2025.

[24] [Press release] "FT statement on deepfake videos of Martin Wolf." Financial Times. https://aboutus.ft.com/press_release/statement-on-deepfake-videos-of-martin-wolf, April 25, 2025.

2

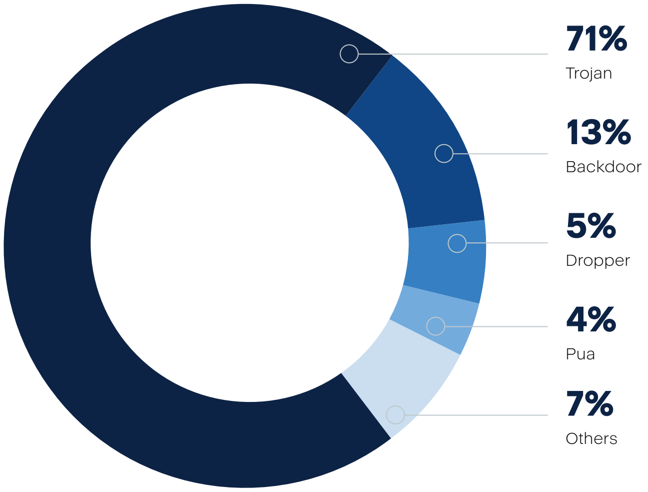
General malware threats

While the sheer volume of malware remains significant, the nature of threats has evolved. Proliferation of malware-as-a-service platforms has democratized access to malicious tools, allowing even less technically skilled individuals to launch attacks. This trend underscores the importance of robust cybersecurity measures and continuous vigilance, as the threat landscape becomes more complex and accessible to a broader range of actors.

As per table below, in January 2025, approximately 5.7% of global Acronis customers experienced at least one malware attack that was successfully blocked on their endpoints. This percentage peaked at 7.2% in March before falling to just over 5% in May. The number of affected users varies by country — users in developed countries tend to be better protected due to more enforced security measures and higher overall awareness. Still, between three and 10 out of every 100 users encounter threats that are ultimately blocked by Acronis Cyber Protect Cloud.

Month	Percentage of clients with blocked malware
January	5.7%
February	5%
March	7.2%
April	5.2%
May	6.7%
June	6.5%

It is important to note that these statistics are based solely on endpoint detections, meaning that any threats already blocked by proxy or email security earlier in the chain are not reflected here. In the first quarter of 2025, malvertising (malicious advertising) was the leading initial infection vector for several prevalent malware strains, including SocGholish, ZPHP and LandUpdate808. These campaigns often employed deceptive ads, such as fake browser updates, to trick users into downloading malicious software.



AV-TEST Malware types detected in the last two weeks of May 2025 (source: av-test.org)

The most common malware type are Trojans, making up more than half of the blocked threats. Below are some of the most commonly seen malware families in H1 2025, suggesting a focus on bots and information stealers:

- SocGholish
- Mirai
- Lumma Stealer
- Agent Tesla
- VenomRAT
- DarkGate
- Prometei
- Formbook
- AsyncRAT
- Snake

The average lifetime of a malware sample in May 2025 was a mere 1.4 days, after which it disappeared and was never seen again by Acronis. Malware is shorter-lived than ever as attackers use automation to create new and personalized malware at blazing speeds in an effort to bypass traditional detection mechanisms. Of all the samples observed, 69.3% were seen only once across our customer base.

Among the focus countries, the most clients experiencing malware detections in May were India (12.4%), Brazil (11%) and Spain (10.2%). In June, India topped the list with 13.2%, followed by Brazil with 9.5% and Spain with 8.8%. The countries highlighted in the below table were selected based on a combination of malware detection volumes and strategic relevance. These are regions where Acronis maintains strong visibility through our customer base and threat telemetry. This focus ensures that our analysis is both data driven and grounded in real-world observations from environments we actively protect.

Monthly normalized percentage of global malware detections by country

Country	JAN	FEB	MAR	APR	MAY	JUN
India	9.5%	8.1%	11.5%	8.3%	12.4%	13.2%[25]
Brazil	8.6%	7.4%	10.7%	9%	11%	9.5%
Spain	7.9%	7.4%	6.4%	4%	10.2%	8.8%
United Arab Emirates	7.1%	6.4%	10.1%	5.8%	9%	8.4%
Italy	6.2%	5.5%	9%	5.8%	7.4%	7.1%
Germany	6.3%	4.7%	7.4%	5.1%	7.1%	6.9%
Switzerland	4.5%	3.1%	8.1%	4.4%	5.4%	5.9%
United States	4.2%	3.2%	5.3%	3.7%	4.8%	5.1%
France	3.5%	5%	6.4%	3.9%	4.5%	4.8%
Japan	3.1%	2.9%	3%	2.3%	4%	3.9%
Australia	3.4%	2.6%	4.5%	3%	4.1%	3.7%
Sweden	2.8%	2.1%	4.3%	3.8%	4.2%	3.4%
United Kingdom	2.9%	2.6%	5.1%	3.4%	3.1%	3.4%
Singapore	3.4%	2.5%	6.5%	4.5%	3.7%	3.3%
Denmark	3.4%	2.9%	3.5%	2.4%	2.9%	3.2%
Canada	2%	1.6%	3.1%	2.2%	3.2%	3.1%

We collected threat data from Acronis-protected endpoints with anti-malware enabled, ensuring user privacy by analyzing only anonymized detection metadata without accessing any personal or content-level information. To maintain statistical reliability, we normalized the data by calculating detection rates as the ratio of affected endpoints to total antivirus-enabled clients. The resulting dataset was interpreted monthly to highlight relative threat exposure across geographies.

[25] A value of 13.2% means that from all machines protected by Acronis in India with anti-malware enabled, 13.2% had at least one malware detection in June 2025.

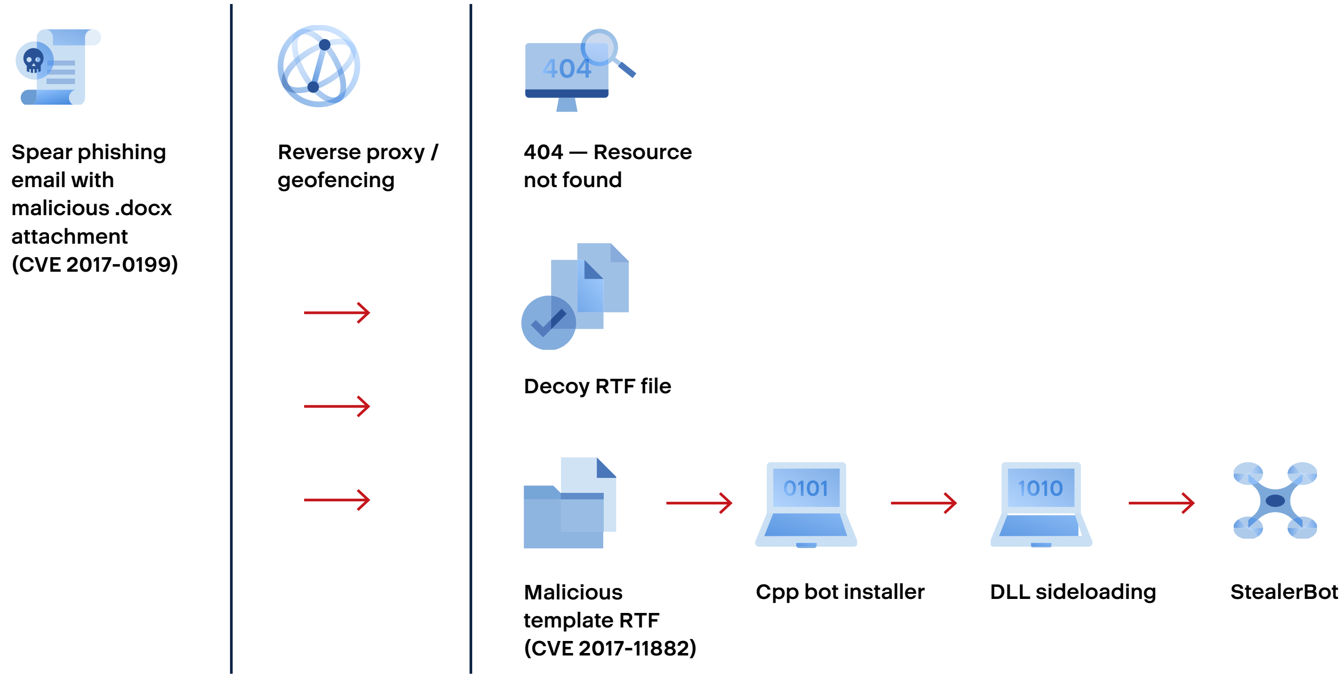
Prevalent malware in the spotlight: SideWinder APT

In the first half of 2025, the Acronis Threat Research Unit (TRU) conducted in-depth analyses of several sophisticated malware campaigns. The SideWinder APT group intensified their activities, which targeted South Asian public sector entities using spear-phishing campaigns that exploited known vulnerabilities to deploy geofenced malware payloads.

Depending on the victim's location (IP address) and user-agent, the server will present the next stage of the infection chain, a 404 error or a decoy RTF file.

Key findings:

- The attackers used spear phishing emails paired with geofenced payloads to ensure that only victims in specific countries received the malicious content.
- Malicious Word and RTF files exploiting CVE-2017-0199 and CVE-2017-11882 were used as initial infection vectors — two long-known but still effective vulnerabilities.
- The intrusion chain features multistage loaders, shellcode-based payload delivery and server-side polymorphism to evade detection.
- The final stage delivers StealerBot, a credential stealer used for data exfiltration and persistent access, blending classic espionage with cybercrime-style credential harvesting.


Spear phishing email with malicious .docx attachment (CVE 2017-0199)
Reverse proxy / geofencing
404
404 — Resource not found
Decoy RTF file
Malicious template RTF (CVE 2017-11882)
0101
Cpp bot installer
1010
DLL sideloading
StealerBot

Additional Acronis malware research

Additionally, the Acronis Threat Research Unit reported on the emergence of a sophisticated malware delivery chain dubbed "Nietzsche" that utilizes multiple scripting languages to deploy high-profile malware like DCRat and Rhadamanthys infostealer. This complex attack chain, observed by Acronis researchers, involves phishing emails with malicious attachments that execute a PowerShell script, incorporating Friedrich Nietzsche quotes as nonfunctional comments.

TRU also identified new variants of Chaos RAT,[26] an open-source remote administration tool, actively targeting Linux and Windows systems. Evolving since 2024, Chaos RAT's latest samples exploit a critical vulnerability in its web panel, enabling remote code execution on servers. Attackers lure victims with a deceptive network troubleshooting utility for Linux, leveraging the malware's Golang-based cross-platform compatibility. Despite its limited use, Chaos RAT's low detection profile facilitates espionage, data exfiltration and ransomware footholds. Acronis TRU's analysis of a Linux variant provides actionable detection strategies, including YARA rules, indicators of compromise and EDR-based threat-hunting tips to bolster defenses against this persistent threat.

These studies underscore the evolving complexity of cyberthreats and the necessity for enhanced security measures across all sectors.

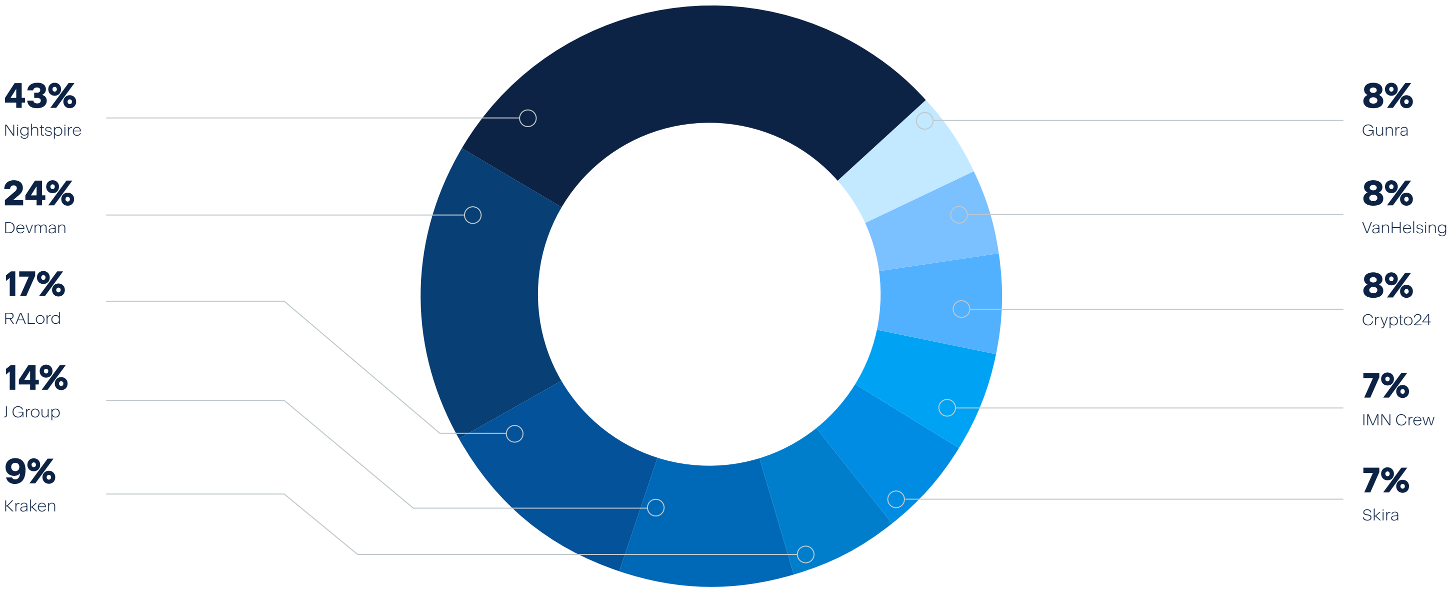
New ransomware actors

From January to May 2025, Acronis noted the appearance of many new ransomware groups, of which we chose the top 10 in terms of known victims. In total, these groups account for 145 victims globally for the stated period of time.

Devman operates as ransomware-as-a-service (RaaS), enabling its malware and infrastructure to be used by other attackers in exchange for a cut of the ransom. Devman is known to share its encryption tools with other groups, including Qilin and RansomHub. This may suggest direct collaboration or that the same developers are behind multiple brands. Devman uses classic double-extortion techniques, meaning it not only encrypts a victim's files but also threatens to leak them publicly if the ransom isn't paid.

Nightspire is another relatively new ransomware group that surfaced in early March 2025. There is evidence suggesting it might be a rebranded or an evolved version of a previous group called Rbfs, with some of the same members. While it's unclear whether NightSpire operates as a full-fledged RaaS or as a closed group, it has shown similar behavior to known affiliate models. Like many others, it uses double extortion tactics. NightSpire's victim list mainly includes small to mid-sized companies in industries such as manufacturing, logistics and finance.

New ransomware gangs



[26] Acronis Threat Research Unit (TRU). "From open source to open threat: Tracking Chaos RAT's evolution." https://www.acronis.com/en-us/tru/posts/from-open-source-to-open-threat-tracking-chaos-rats-evolution/, June 4, 2025.

RALord, also known by its new name, "Nova," emerged in March 2025 and rebranded just a month later. Like Devman, it operates as RaaS. RALord / Nova provides its affiliates with tools and infrastructure to carry out attacks, and the group itself is responsible for publishing stolen data if a ransom isn't paid. They use a combination of disruption, public embarrassment and online exposure to pressure victims into paying. RALord is also known for publishing detailed explanations of how they breached their victims, aiming to humiliate them and boost the group's reputation. RALord allows affiliates to buy or rent their encryption tools and promote their services across darknet forums and Tor-based leak sites.[27]

Most active ransomware gangs

Of the top 10 most active ransomware families we observed and tracked in Q1 2025, three highly active groups stand out as the primary contributors, collectively responsible for about 40% of the attacks. Among these groups, Cl0p takes the lead, accounting for 19% of attacks, followed by RansomHub and Akira with 11% and 10% respectively.

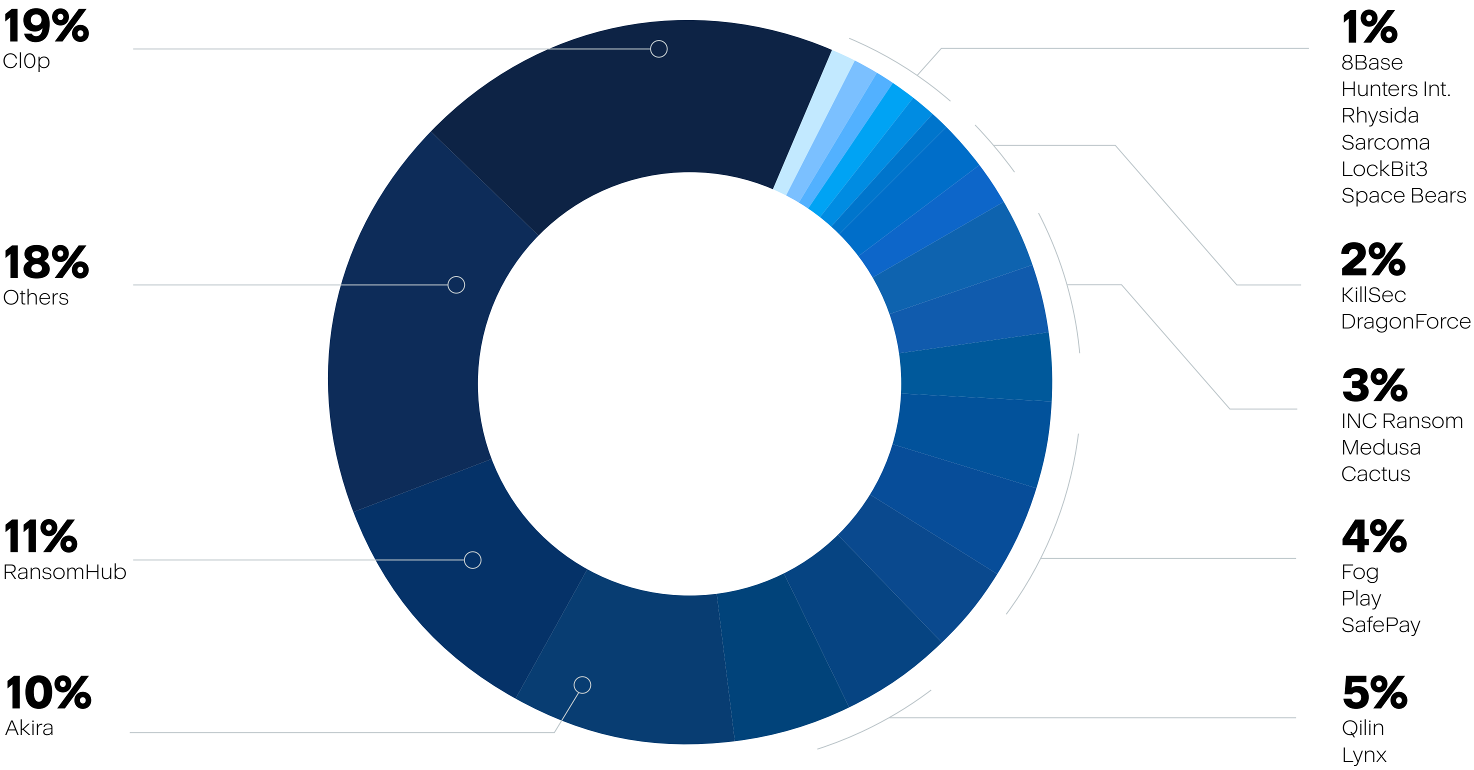
Acronis tracked 2,120 publicly mentioned ransomware cases in Q1 2025 — 200% more than in Q1 2024. The below graph illustrates the percentage distribution of activity among ransomware groups from January 2025 to March 2025. By the end of 2024,[28] leading ransomware groups included RansomHub, LockBit and Play. By Q1 2025, the landscape shifted with Cl0p, RansomHub and Akira emerging as the most active. RansomHub's rise to prominence can be attributed to its aggressive recruitment and lucrative RaaS offerings, overtaking LockBit as the most prolific group. Akira, known for targeting vulnerabilities in VPN and backup solutions, has become a significant threat, especially to SMBs.

1	Cl0p
2	RansomHub
3	Akira
4	Qilin
5	Lynx
6	Fog
7	Play
8	SafePay
9	INC Ransom
10	Medusa

[27] http://novazzitmugtbjwuttc5hhsemkmvwh3iyt27oeeunu5mkw62qpfeykid.onion/registration.php

[28] Kevin Poireault. "The Top 10 Most Active Ransomware Groups of 2024." Infosecurity Magazine. https://www.infosecurity-magazine.com/news-features/top-10-most-active-ransomware, 27 December 2024.

Ransomware group activity, Q1 2025



It is important to recognize that these statistics only capture part of the story. Some victims choose to negotiate with — and ultimately pay — their attackers to avoid public exposure. However, paying a ransom offers no assurance that the stolen data will be deleted. Past incidents have shown that even after victims comply with ransom demands,[29] they are often targeted for further extortion, have their data sold to other malicious actors or see it leaked online.

Acronis Cyber Cloud combines AI-powered Active Protection,[30] automated patching and integrated backup and disaster recovery, enabling organizations to defend against modern ransomware threats while ensuring rapid data restoration without paying a ransom.

We have normalized the ransomware detection numbers by calculating the ratio of detections to the total number of workloads with Acronis Active Protection enabled. The analysis is based on anonymized metadata from Acronis-protected endpoints, ensuring user privacy while providing a statistically reliable view of ransomware exposure.

Ransomware detections normalized

Country	Ransomware cases per 10,000 workloads in focus countries (January–June 2025)
Germany	179
Japan	119
Canada	106
Switzerland	46
United States	42
Australia	38
Sweden	31
United Kingdom	26
France	23
Spain	21
Italy	19
Denmark	10
Singapore	6
India	5
United Arab Emirates	3
Brazil	3

[29] Federal Bureau of Investigation. "Ransomware." https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware, n.d.

[30] Active Protection: Acronis. "Active Protection by Acronis." https://www.acronis.com/en-us/technology/active-protection/#:~:text=Ransomware%20is%20a%20particularly%20painful,your%20Acronis%20Cyber%20Backup%20files, n.d.

Between January and June 2025, ransomware detection rates per 10,000 protected workloads varied widely across regions. Germany led with 179 detections per 10,000 workloads, followed by Japan (119) and Canada (106), suggesting more frequent targeting or broader campaign reach. At the lower end, markets such as the UAE, Brazil and India recorded five or fewer detections per 10,000 workloads. While these numbers may appear low, ransomware remains a high-impact threat where a single successful attack can cause severe operational and financial damage. Additionally, low detection numbers may reflect proactive defenses, such as behavioral-based prevention and backup strategies already in place on Acronis-protected workloads.

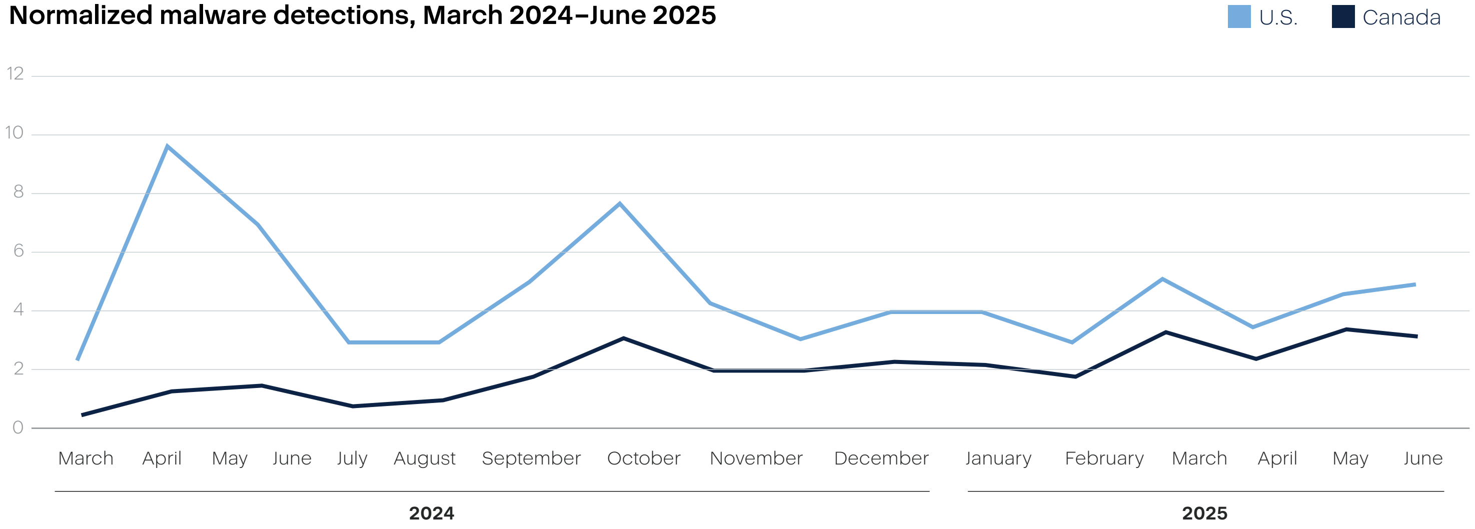
Finally, it's important to consider that visibility is limited to what is detected, and these figures may not account for ransomware attempts blocked before delivery, or those executed through supply chain and credential abuse vectors. Moreover, ransomware detections typically represent a last line of defense — triggered only when all prior security layers have been bypassed. Acronis Active Protection steps in not as a first responder but the final safeguard against encryption, which naturally leads to lower detection counts in environments where other controls are doing their job effectively.

Telemetry data in focus countries

In 2025, cybercriminals continue to target organizations of all sizes and industries, driven by the pursuit of sensitive data. This trend is clearly reflected in the sharp rise in both malware detections and malicious URL activity. Attackers no longer rely on just one method — they use layered techniques like infostealers, phishing and web-based traps to increase their chances of success. The motivation remains financial, and every compromised endpoint or credential feeds the larger cybercrime ecosystem. Every company, regardless of its size, industry or niche is a potential target.

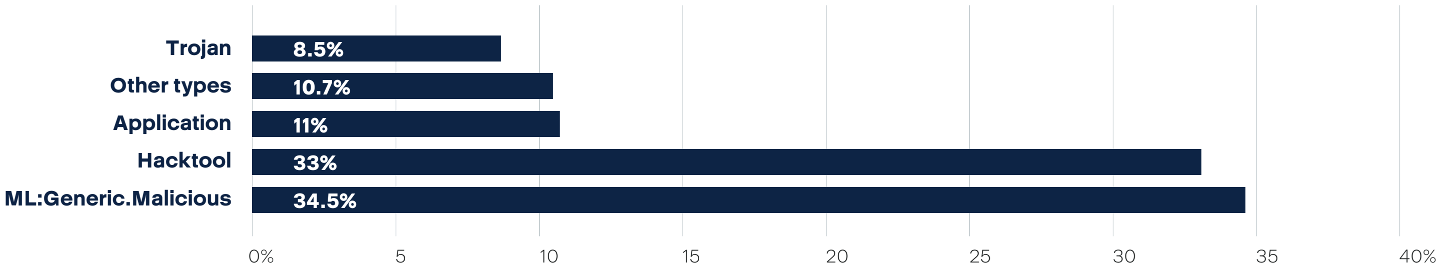
U.S. and Canada

Normalized malware detections, March 2024–June 2025



The graph shows normalized malware detections in Canada and the U.S. from March 2024 to June 2025. Notably, the U.S. experienced a spike in April 2024, likely linked to tax season scams, including malware-laced phishing targeting attacks. A second peak in September 2024 might have been related to back-to-school campaigns, which are often exploited via educational-themed lures.The third peak came in March 2025. Canada experienced a steadier increase, with minor peaks around September 2024 and March 2025 — potentially tied to fiscal year-end activities and seasonal phishing. The U.S. maintained higher detection rates overall, possibly due to larger attack surfaces or higher reporting / monitoring density.

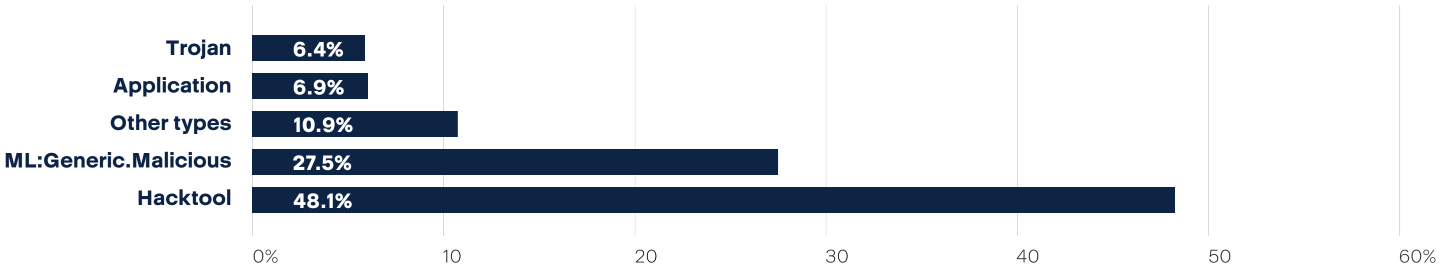
Canada Distribution of detected malware types, March 2024–June 2025



According to Acronis telemetry data in Canada, no single malware family accounted for more than 50% of detections. The most common malware family was ML:Generic.Malicious with 34.5%, reflecting a steady presence of malicious executables used for initial compromise and efficiently detected by our machine learning model. The near-equal volume of Hacktool detections (33%) suggests active misuse of legitimate administrative tools — potential signs of post-compromise activity and lateral movement attempts.

The Application category represents unwanted or risky software running in the environment, potentially indicating weak application control or shadow IT behavior. The presence of Trojans highlights attempts to establish persistent covert access, often tied to phishing or credential abuse campaigns. Although adware appear in smaller numbers in the Other types category, it represents initial access vectors and hygiene issues that can escalate into more severe breaches if overlooked. These threats were primarily caught by behavioral-based detection, real-time Active Protection, and application of strict execution policies, demonstrating the value of multilayered, AI-enhanced endpoint security.

U.S. Distribution of detected malware types, March 2024–June 2025

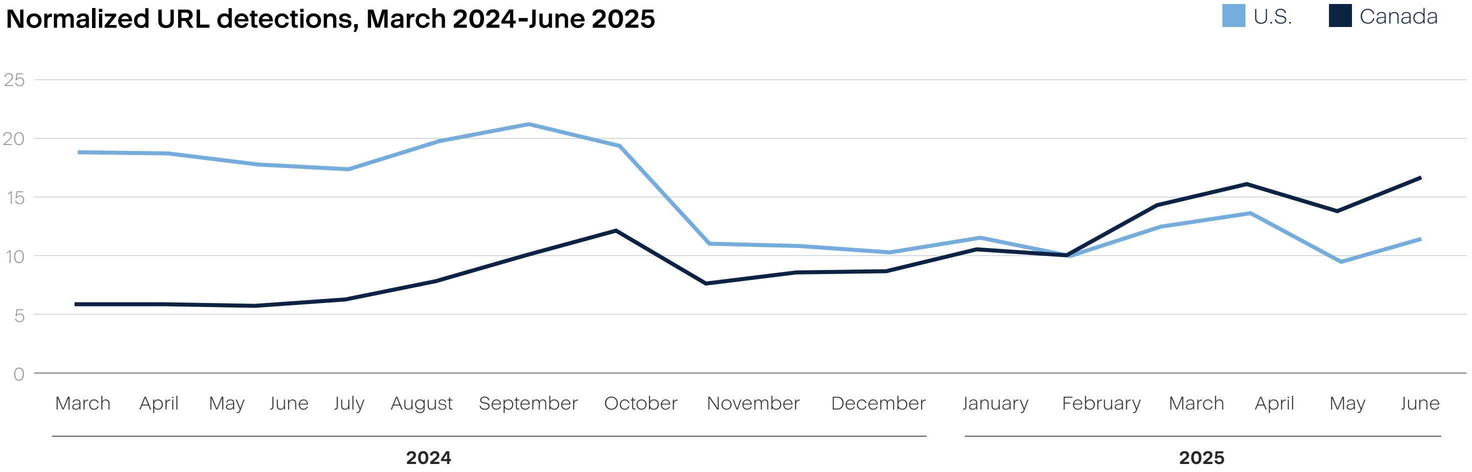


The U.S. threat landscape is dominated by Hacktools (48%), pointing to a strong presence of post-exploitation activity and widespread use of dual-use tools — likely in both cybersecurity simulations and real-world intrusions. The high count of ML:Generic.Malicious (27.5%) suggests a significant volume of obfuscated or novel payloads bypassing static defenses and being flagged through behavioral analysis. Other types (10.9%) and Application-related detections (6.9%) further highlight the challenge of managing authorized versus suspicious software in large, diverse environments.

Trojans (6.4%), while lower in rank, still represent substantial attempts at initial access and persistence, often tied to phishing or credential compromise. These threats are primarily intercepted by advanced behavioral detection, execution control and memory protection technologies that activate when conventional filters are evaded. This highlights the critical role MSPs play in delivering and managing these multilayered defenses at scale across diverse client environments in the U.S. market.

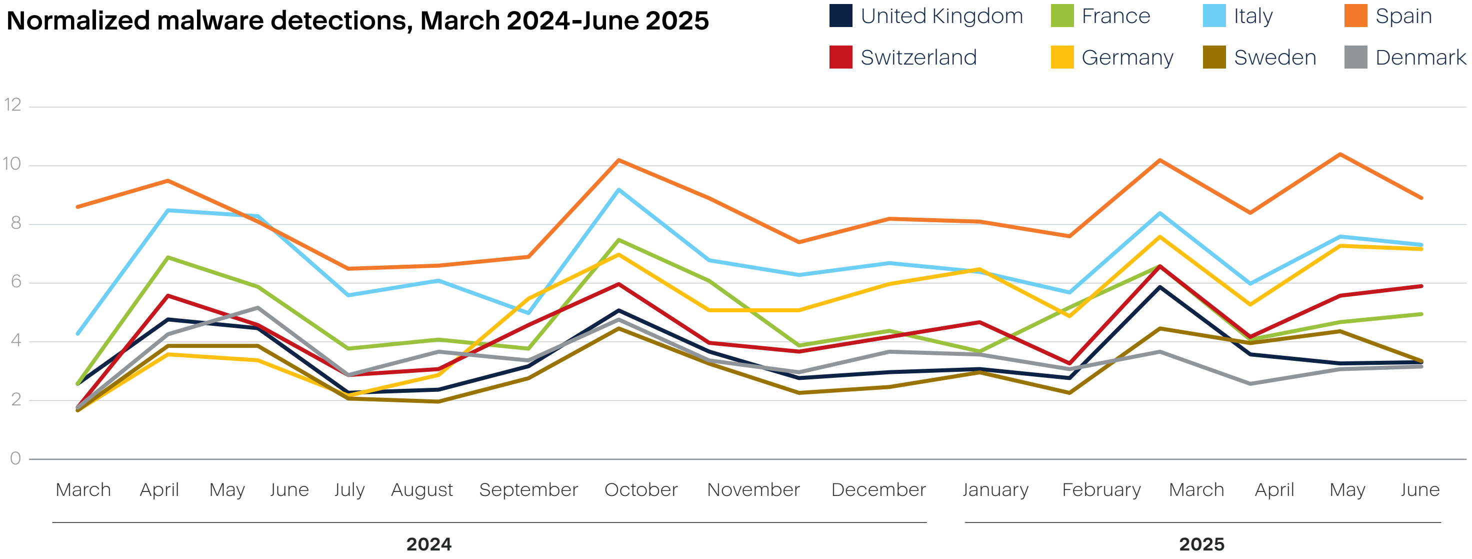
The below graph shows normalized URL detections in Canada and the U.S. from March 2024–June 2025. The U.S. led in URL detections until September 2024, when a sharp decline occurred. This aligns with the URL filtering technical refinement, which reduced false positives and stale detections, enhancing data accuracy. This technical refinement explains the sudden drop rather than an actual decline in threat volume. Meanwhile, Canada has shown a gradual but consistent rise in URL detections similar to the malware detections trend above, increased in April 2025, potentially due to increased phishing activity tied to tax season[31] or targeted regional campaigns. In June 2025, news outlets reported a wave of scams that featured Instagram ads impersonating Canadian banks, including Bank of Montreal (BMO) and EQ Bank (Equitable Bank).[32] The scams leveraged AI-generated deepfake videos combined with official branding to deceive victims. The Instagram ads led users to carefully crafted malicious domains — URLs designed to closely mimic legitimate bank websites — where victims were tricked into submitting sensitive personal and financial information. The surge in phishing as a service (PhaaS) and the fusion of AI-powered impersonation with deceptive URLs have enabled cybercriminals to evade traditional security measures and scale their attacks effectively.

Normalized URL detections, March 2024-June 2025



Denmark, France, Germany, Italy, Spain, Sweden, Switzerland, U.K.

Normalized malware detections, March 2024-June 2025



[31] Ellen Jennings-Trace. "Look out for tax-themed scams this month, Microsoft warns." Techradar. https://www.techradar.com/pro/security/look-out-for-tax-themed-scams-this-month-microsoft-warns, April 5, 2025.

[32] Ax Sharma. "Instagram ads mimicking BMO, EQ Bank are finance scams." Bleeping Computer. https://www.bleepingcomputer.com/news/security/instagram-ads-mimicking-bmo-eq-bank-are-finance-scams/, June 17, 2025.

Across the observed European markets, Spain has shown the highest normalized malware detection rates, with marked peaks in April 2024, September 2024, March 2025 and May 2025 — suggesting widespread exposure, likely driven by phishing and infostealer campaigns during vacation and tax filing periods. In contrast, the U.K. has shown generally low and stable detection rates, with occasional spikes in April 2024 and September 2024 — possibly linked to seasonal phishing waves. The March 2025 peak (5.7%) might have been connected to increased threat activity exploiting end-of-fiscal-year vulnerabilities and software misconfigurations.

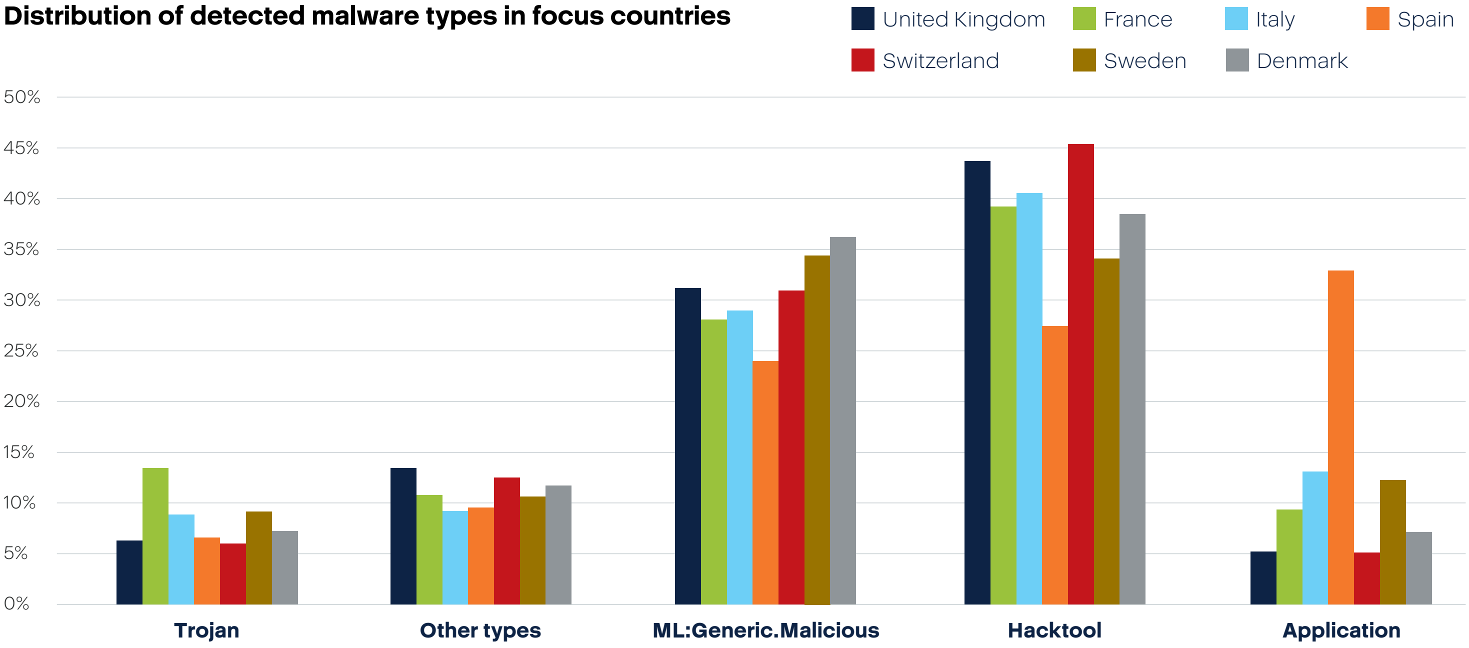
France experienced a sharp peak in September 2024, which could reflect targeted ransomware and phishing activity around the back-to-school period. Notably, the sustained rise in early 2025 suggests evolving tactics in social engineering and increased exposure in hybrid environments. Italy maintains consistently high detection levels, peaking in late summer and early spring — periods often exploited by ransomware operators leveraging social engineering and limited off-season monitoring.

According to ACN,[33] in September 2024, the most widespread malware types in Italy were backdoors, information stealers and banking trojans, while the most widespread malware types in Europe overall were banking trojans, information loaders and information stealers. The sectors most affected in Italy included central public administration, telecommunications and financial services — in which a targeted phishing campaign drove the spike — alongside a notable spear-phishing attack on a strategic company in the energy sector. Germany experienced a sharp rise from August 2024–March 2025, which may reflect increasing cybercriminal focus on industrial targets, particularly in supply chains and manufacturing. Elevated activity in Q1 2025 could also correlate with phishing tied to annual financial disclosures and vendor renewals.

Switzerland experienced intermittent spikes in April 2024, September 2024 and March 2025, which could be linked to hybrid phishing-malware campaigns exploiting financial services and international conferences. The relatively lower baselines in winter suggest effective containment or seasonal attacker shifts away from high-trust regions. Sweden has shown low overall detection rates with modest increases in April 2024 and September 2024, likely tied to social engineering campaigns exploiting government or academic sector vulnerabilities. The small but clear rise in March 2025 might have been related to seasonal invoice-fraud surges. Denmark's trends show slightly elevated activity in May 2024 and September 2024, potentially correlating with localized phishing campaigns during post-vacation business reactivation. The lower variability may reflect more consistent endpoint hygiene and enforcement policies.

Now, let's take a look at the distribution of detected malware types in the focus countries from March 2024–

Distribution of detected malware types in focus countries



[33] National Cybersecurity Agency (ACN). Operational Summary — September 2024. https://www.acn.gov.it/portale/en/w/operational-summary-settembre-2024, October 18, 2024.

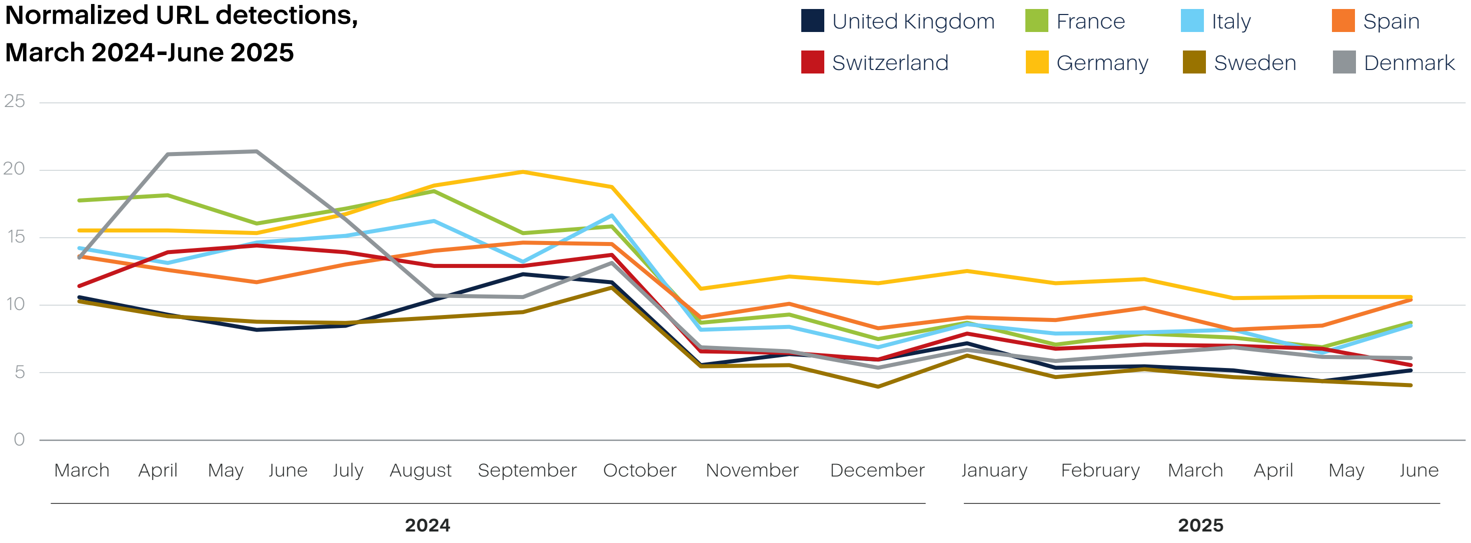
Hacktools and ML-detected threats are the most prevalent across all presented countries, underscoring attackers' reliance on stealthy, modular tooling.[34] The relatively high number of ML-detected generic malware suggests attackers are increasingly adapting techniques that require behavioral analysis, such as custom droppers, polymorphic malware and staged payloads. Hacktools are the most prevalent malware type across all focus countries, accounting for over 45% of detections in Switzerland, over 43% in the U.K., 40% of detections in Italy and nearly 39% in France, indicating a consistent focus on post-exploitation and lateral-movement tools. ML:Generic.Malicious detections show similar proportional levels in all regions, highlighting the widespread use of obfuscated or evasive malware caught by ML-driven defenses.

In contrast, Application-type threats dominated in Spain at 32.8%, suggesting a higher exposure to adware or potentially unwanted programs compared to Italy (13%) and Sweden (12.2%). France stands out for having the highest proportion of Trojans (13.2%), pointing to a stronger presence of classic credential-stealing or remote-access malware.

Denmark, despite showing a relatively moderate volume of threats overall, experienced a disproportionately high presence of ML-detected malicious files (36.2%) and Hacktools (38%), suggesting a shift from commodity malware to stealthier, evasive and post-compromise techniques. This pattern aligns with Denmark's advanced digital economy, characterized by extensive e-government services, a high degree of cloud adoption, and heavy reliance on connected operational technology in sectors such as energy, pharma and maritime logistics — all prime targets for well-resourced threat actors. In response, the Danish Agency for Social Security (SAMSIK)[35] prioritized backup, recovery and crisis management in its supervision of major telecom providers,[36] anticipating the July rollout of NIS 2-aligned legislation. These inspections aim to ensure resilience against threats that may remain undetected for extended periods and disrupt critical services.

In Switzerland and the U.K., both highly connected financial hubs with strong infrastructure protection, Hacktools represented 45% of all malware detections, reflecting persistent interest from threat actors in exploiting legitimate tools to evade detection — likely due to the higher potential payoff from successful breaches. To counter these trends, organizations should combine AI-powered threat detection with strict application control and endpoint hardening to reduce exposure to evasive malware and unwanted software. Regular threat hunting, user awareness training and proactive monitoring of post-exploitation tools like Hacktools are essential to disrupt attacker activity early in the intrusion cycle.

Normalized URL detections, March 2024-June 2025



[34] Our systems have detected the presence of Hacktools identified as Advanced Port Scanner A and Advanced Port Scanner B, which are typically used for network reconnaissance and may indicate early-stage malicious activity or unauthorized internal scanning. The detection of Advanced Port Scanner is intentional, as attackers frequently use it to map networks, identify devices, and gather intelligence for exploitation. This tool also enables file transfers and remote access (SSH, RDP), making it valuable for both attackers and legitimate users. Due to its dual-use nature, Acronis classifies it as PUA (potentially unwanted application).

[35] Centre for Cyber Security (Denmark). "Fokusområder for tilsyn i 2025." (Focus areas for supervision in 2025). https://www.cfcs.dk/da/nyheder/2025/fokusomrader-for-tilsyn-i-2025/, February 20, 2025.

[36] Centre for Cyber Security (Denmark). "Ny trusselsvurdering: Cybertruslen mod telesektoren." (New threat assessment: The cyber threat to the telecommunications sector). https://www.cfcs.dk/da/nyheder/2025/ny-trusselsvurdering---telesektoren/, March 13, 2025.

Since performing technical refinements in Acronis URL filtering in September 2024, all monitored countries experienced a significant and consistent drop in URL filtering detections. This reduction reflects improved accuracy through the elimination of false positives and cleanup of stale or unsupported convictions, leading to fewer escalations and higher trust in the alerts shown — indicating enhanced precision rather than diminished detection capability.

In Germany, elevated detection levels persisted through late 2024 and early 2025, likely driven by increased phishing campaigns targeting the industrial and manufacturing sectors during vendor renewal and financial reporting periods. Switzerland's detection curve remained relatively stable through mid-2024, with a spike in January 2025. Interestingly, according to National Cyber Security Centre (NCSC), Switzerland experienced a surge in phishing and impersonation campaigns. Fraudsters impersonated trusted entities such as the Federal Tax Administration (FTA) and the NCSC[37] itself, sending emails and messages that lured users with tax refund promises or fake legal threats.

Sweden also experienced a spike in January 2025, which reflects systemic cybersecurity shortcomings across public administration. As highlighted by MSB's 2024 Cybersecurity Survey,[38] nearly 60% of organizations lacked basic controls and management commitment. This widespread vulnerability, combined with limited participation from critical private-sector actors, has created ideal conditions for phishing and link-based attacks to bypass defenses and proliferate rapidly.

Denmark experienced a notable surge in phishing and malicious URL activity, peaking in May 2024, followed by a decline and smaller, isolated spikes in January 2025 and April 2025 — indicating a shift from broad-based campaigns to more targeted, periodic activity. URL detections play a critical role in identifying early-stage intrusion attempts in state-sponsored campaigns like those highlighted in Denmark's 2025 warning[39] about phishing and malicious redirection tactics used to target telecom infrastructure.

The U.K. saw a marked dip after September 2024 but experienced minor rebounds early in 2025, possibly linked to renewed phishing waves exploiting end-of-fiscal-year pressures. France mirrored this pattern with small spikes in early 2025, reflecting evolving social engineering tactics in hybrid work environments. In one recent example, a French woman lost €830,000 after scammers used AI-generated deepfake images and videos to pose as Brad Pitt, convincing her to send money for a fake kidney treatment.

As AI-powered impersonation grows, cybersecurity leaders emphasize employee simulation training to combat these increasingly sophisticated scams. In a similar case from Italy, scammers used AI-driven voice cloning to impersonate Defence Minister Guido Crosetto,[40] targeting high-profile business leaders with spoofed government phone numbers to enhance legitimacy. While the primary vector involved sophisticated voice and phone spoofing, these campaigns frequently leverage malicious URLs or phishing sites to facilitate fraudulent transactions and harvest credentials.

In another example from April–May 2025, Italy experienced a phishing campaign identified by CSIRT Italia,[41] involving over 300 emails sent from a compromised account targeting the energy sector, directing recipients to a malicious website designed to steal credentials. This convergence of advanced impersonation techniques with deceptive web domains underscores the urgent need for comprehensive employee simulation training and enhanced URL threat detection to mitigate evolving social engineering risks.

[37] National Cyber Security Center NCSC (Switzerland). "Current Incidents." https://www.ncsc.admin.ch/ncsc/en/home/aktuell/aktuelle-vorfaelle.html, July 18 2025.

[38] Swedish Civil Contingencies Agency. "Sex av tio organisationer har allvarliga brister i sitt säkerhetsarbete" (Six out of ten organizations have serious deficiencies in their security work). https://www.msb.se/sv/aktuellt/nyheter/2025/januari/sex-av-tio-organisationer-har-allvarliga-brister-i-sitt-sakerhetsarbete/, January 31 2025.

[39] Centre for Cyber Security (Denmark). "Ny trusselsvurdering: Cybertruslen mod telesektoren." (New threat assessment: The cyber threat to the telecommunications sector). https://www.cfcs.dk/da/nyheder/2025/ny-trusselsvurdering---telesektoren/, March 13 2025.

[40] Amy Kazmin and Silvia Sciorilli Borrelli. "Italian tycoons targeted by fake defence minister in suspected AI scam." Financial Times. https://www.ft.com/content/8e911f1e-6eb7-4e8e-b4e0-3aba62575f23, February 9, 2025.

[41] National Cybersecurity Agency (ACN) "Operational Summary - maggio 2025." https://www.acn.gov.it/portale/en/w/operational-summary-maggio-2025, n.d., March 2025.

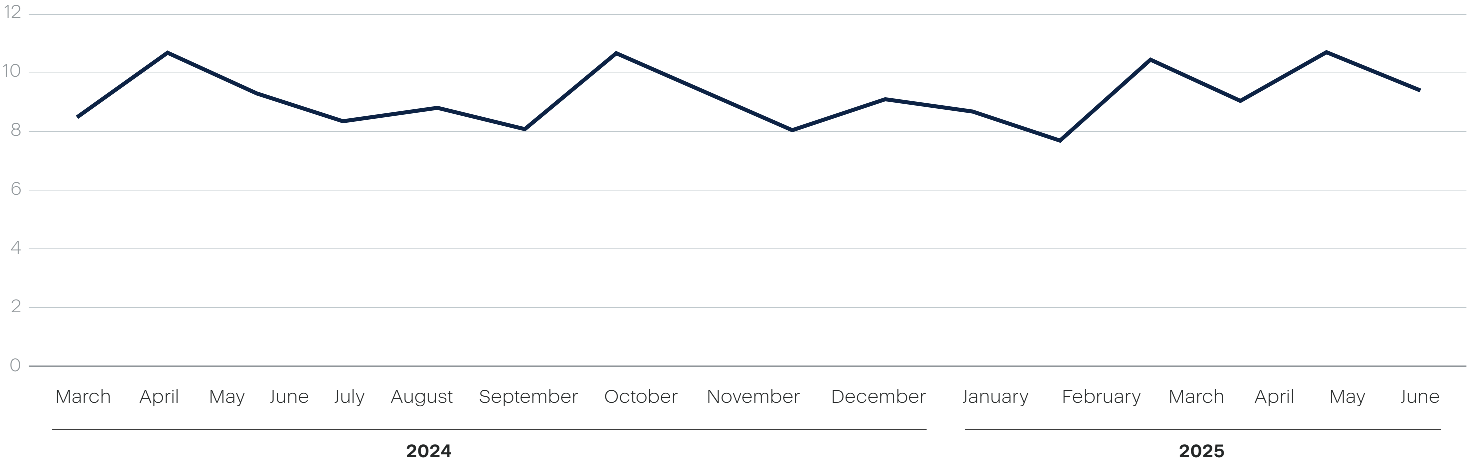
The spike in May 2025 in France correlated with a coordinated phishing campaign impersonating Amazon and leveraging leaked ISP "Free" data that resulted in over 160,000 French users clicking malicious URLs in 17 waves of the attack.

In Spain, following a nationwide blackout in late April 2025, scammers launched phishing attacks exploiting the chaos, including fake airline ticket schemes and credential-stealing sites. Spain also experienced a massive surge in abuse of ".es" domains for phishing,[42] with over 1,300 subdomains hosting malicious pages by May 2025. A series of high-profile cyber incidents — including a Senate email breach[43] and a Telefonica data leak affecting 22 million customers contributed to the sharp rise in malicious URL detections.

According to the EU Cybersecurity Index 2024 published on June 17, 2025,[44] the overall cybersecurity posture of the European Union presents a moderate but cohesive level of maturity, with an average index score of 62.65 / 100. The vast majority of Member States cluster within ±10 points of this average, reflecting a shared baseline in capabilities across the region. The Index evaluates four core areas: Capacity, Operations, Market / Industry and Policy. Policy development and implementation ranks highest (66.09), though it shows the widest variability — revealing uneven progress on vulnerability disclosure and supervisory frameworks under NIS 2. By contrast, Operations — measuring resilience capabilities — scored lowest (57.63), revealing the need for further investment. From a threat readiness standpoint, indicators tied to basic hygiene (e.g., absence of data breaches in SMEs and large enterprises, secure internet behavior and CSIRT presence) report high scores — above 90 across the board. However, underreporting and low incident awareness, especially among SMEs, might distort this picture. Strategic gaps also persist: Adoption of AI in cybersecurity, CSIRT certification and risk assessment practices remain underdeveloped across most Member States. These weaknesses, alongside low cybersecurity investment by critical entities, signal pressing areas for improvement as the threat landscape evolves.

Brazil

Normalized malware detections, March 2024-June 2025



Brazil showed consistent high detection rates throughout the 15-month period, peaking in March and September of 2024 and again in March and May of 2025, which aligns with repeated spear-phishing campaigns delivering Astaroth.[45] As per Acronis TRU research, the malware showed a strong industry-specific focus, with 27% of compromises affecting manufacturing organizations and 18% targeting the IT sector. Lets take a look at the distribution of detected malware types in Brazil during the reported period.

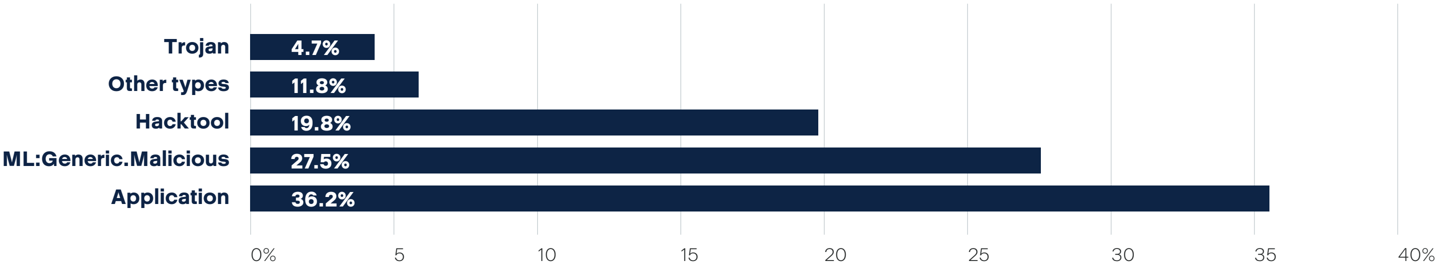
[42] "Connor Jones. "Massive spike in use of .es domains for phishing abuse." The Register. https://www.theregister.com/2025/07/05/spain_domains_phishing, July 5, 2025.

[43] Juan Cabrera. "Principales ciberataques en Espana en 2025." LBC. https://www.channelpartner.es/seguridad/principales-ciberataques-en-espana-en-2025, June 4, 2025.

[44] European Union Angency for Cybersecurity (ENISA). "The EU Cybersecurity Index 2024." https://www.enisa.europa.eu/publications/the-eu-cybersecurity-index-2024, June 17, 2025.

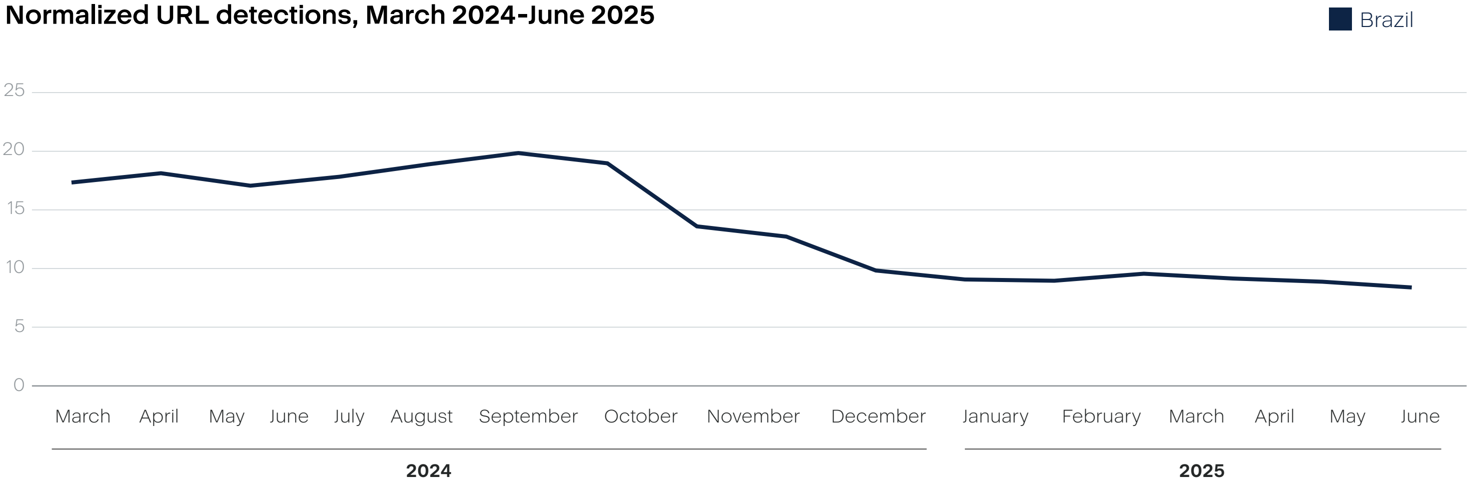
[45] Norbert Biro, Jozsef Gegeny, et. al. "Astaroth unleashed." Acronis Threat Research Unit. https://www.acronis.com/en-us/cyber-protection-center/posts/astaroth-unleashed, April 15, 2025.

Distribution of detected malware types, March 2024–June 2025



Application-based threats consistently rank highest (36.2%), signaling widespread exposure to potentially unwanted programs and misuse of legitimate software — often a blind spot in traditional endpoint controls and common in environments lacking robust application allowlisting. The strong presence of ML:Generic. Malicious detections (27.5 %) indicates that attackers leveraged obfuscated, evasive malware strains that require behavioral-based detection. Notably, Brazil also shows elevated levels of Hacktools 19.8%, which are often used by threat actors and insiders alike to conduct lateral movement, evade defenses or exploit vulnerabilities. The low percentage of Trojans (4.7%) might mean attackers are pivoting away from legacy malware toward fileless and modular strains. These patterns emphasize the need for regionalized defenses that combine application control, insider threat monitoring and advanced malware analytics.

Normalized URL detections, March 2024-June 2025



Throughout 2024, Brazil experienced a surge in malicious URL detections, peaking at 19.9% in August, fueled by phishing campaigns exploiting national themes and services. While the trend showed a gradual decline through early 2025 after Acronis' URL filtering technical refining, cybersecurity alerts persisted — particularly regarding tax fraud attempts, which rely on shortened or cloud-hosted URLs, impersonating Receita Federal.[46] A major campaign,[47] documented in May 2025, involved the abuse of RMM tools through malicious URLs targeting Portuguese-speaking users. In this campaign, attackers used fake NF-e (Nota Fiscal eletrônica) invoice alerts to lure users into clicking links hosted on platforms like Dropbox. The links led to installers for RMM software tools, including N-able Remote Access and PDQ Connect, which, once deployed, gave attackers access to the victims' systems, allowing them to read and write files remotely. Additionally, it enabled them to install secondary tools like ScreenConnect, increasing persistence.

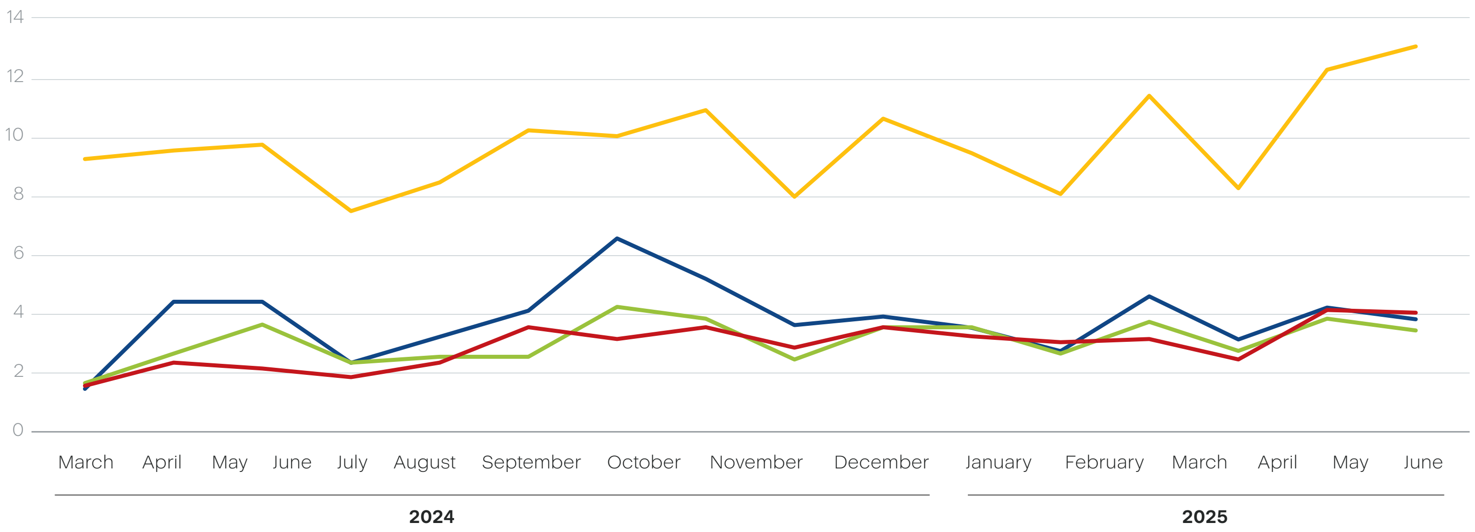
[46] gov.br [Brazil]. "Receita Federal alerta para retorno de golpe por correspondência com uso indevido do seu nome." (Federal Revenue warns of return of mail scam with misuse of your name). https://www.gov.br/receitafederal/pt-br/assuntos/noticias/2025/marco/receita-federal-alerta-para-retorno-de-golpe-por-correspondencia-com-uso-indevido-do-seu-nome, March 11, 2025.

[47] Ravie Lakshmanan. "Initial Access Brokers Target Brazil Execs via NF-e Spam and Legit RMM Trials." The Hacker News. https://thehackernews.com/2025/05/initial-access-brokers-target-brazil.html, May 9, 2025.

The primary targets of this campaign were C-level executives and financial departments across multiple sectors, including education and government. This operation was linked to an initial access broker (IAB) exploiting free RMM trials to establish unauthorized footholds in corporate environments. The campaign exemplifies how phishing trends in Brazil continue to evolve, using credible local lures and remote tooling to bypass detection and compromise organizations.

Australia, India, Japan, Singapore

Normalized malware detections, March 2024-June 2025



Across the APAC region, malware detection trends from March 2024–June 2025 clearly correlate with seasonally driven campaigns and high-impact APT activity, rather than random noise. Peaks in India during March and May of 2025 likely reflect fiscal-year-end phishing and APT 36,[48] which launched a sophisticated campaign spoofing India Post domains. The campaign tricked both Windows and Android users with malicious PDFs and APKs that deployed remote access trojans (RATs) via fake government site postindia[.]site.

Singapore experienced moderate upticks in September 2024, March 2025 and May 2025, consistent with the malware campaigns tied to national budget cycles. In Australia, elevated detections in April 2024, September 2024 and March 2025 follow ATO-themed QR code and tax refund phishing scams — attested by official alerts.

Detections in Japan remained low, with minor seasonal increases during Golden Week.

The malware-detection spikes in August and October of 2024 align with high-profile ransomware intrusions[49] and hacktivist activity in Japan. The government's disclosures around the MirrorFace / APT10[50] campaign in January revealed at least 200 cyberattacks targeting ministries, JAXA, think tanks and airlines. This heightened threat awareness likely drove detection activity as organizations responded to suspected state-backed intrusions.

These patterns underscore that observed fluctuations stem from legitimate threat activity tied to fiscal timelines, public events and targeted APT operations, highlighting the need for prioritized, context-aware defenses.

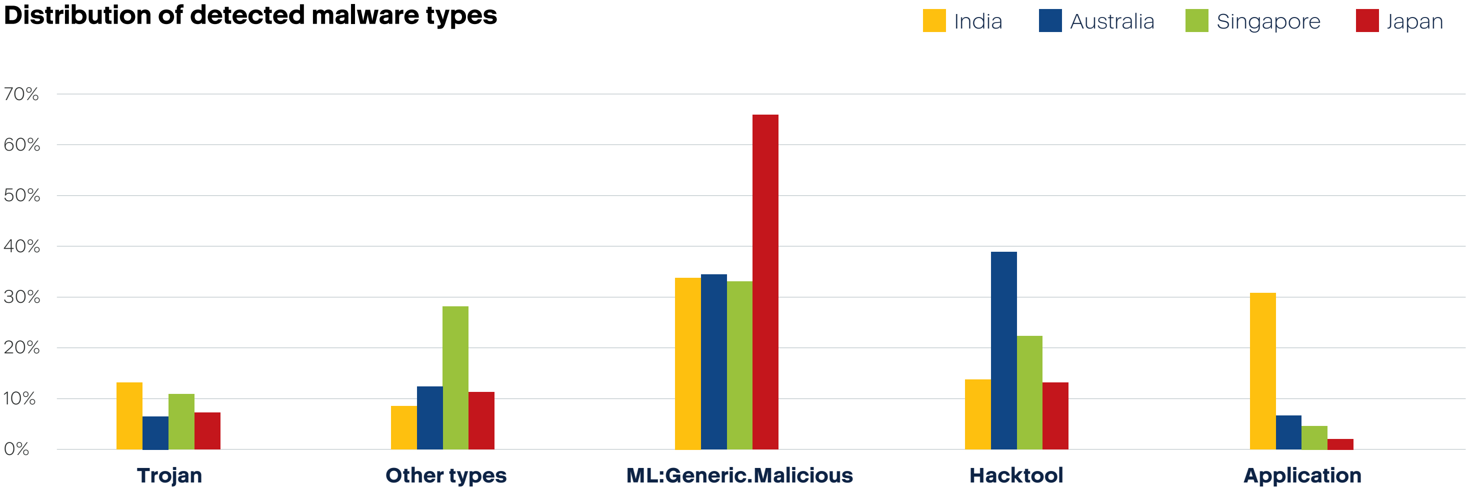
[48] Ravie Lakshmanan. "APT36 Spoofs India Post Website to Infect Windows and Android Users with Malware." https://thehackernews.com/2025/03/apt36-spoofs-india-post-website-to.html, March 27, 2025.

[49] https://en.wikipedia.org/wiki/2024_cyberattack_on_Kadokawa_and_Niconico

[50] Alessandro Mascellino. "Japan Faces Prolonged Cyber-Attacks Linked to China's MirrorFace." Infosecurity Magazine. https://www.infosecurity-magazine.com/news/japan-faces-cyberattacks-china, January 9, 2025.

Let’s take a look at the distribution of detected malware types in APAC during the reported period from March 2024 to June 2025.

Distribution of detected malware types

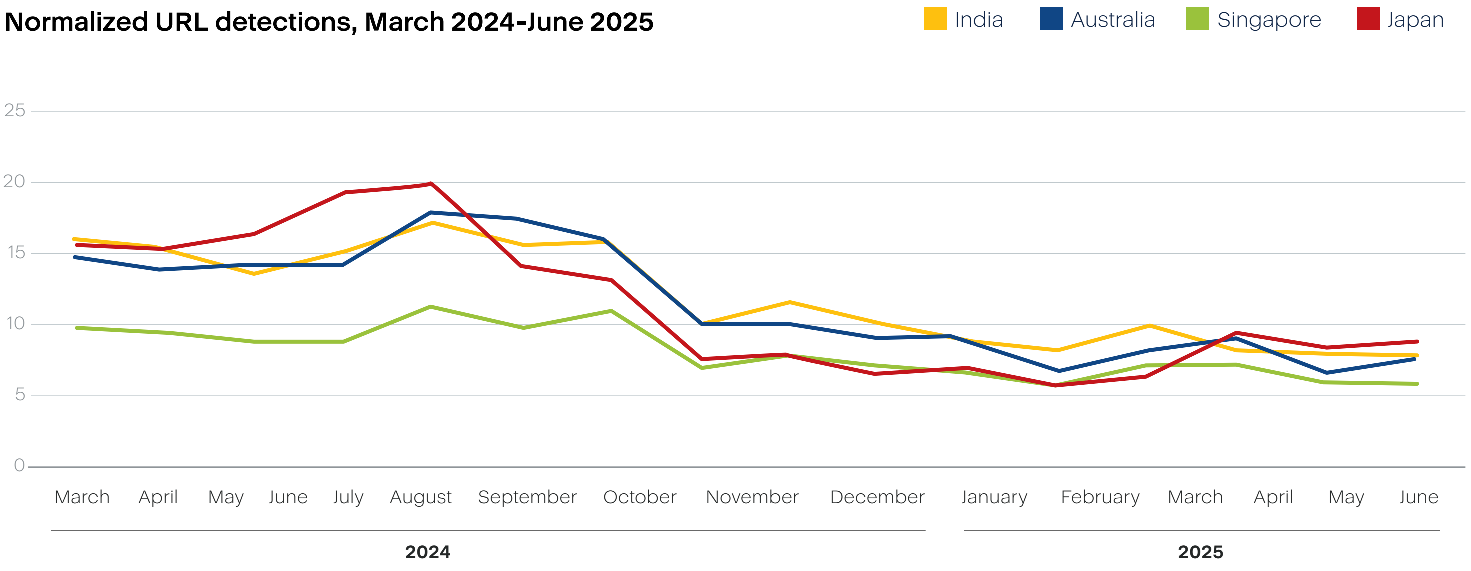


Japan’s exceptionally high ML-detected malicious activity (65.8%) suggests both advanced attacker sophistication and high digital dependency, making it critical to safeguard national infrastructure and maintain business continuity. In India, 34% of detected malware types were ML detections, followed by elevated application-based threat levels (31%), which point to widespread misuse of legitimate tools and calls for stronger application control policies in its booming IT sector.

Australia faced the highest proportion of Hacktools (38.9%), indicating risks tied to admin tool abuse and possible lateral movement within critical systems. Singapore, with notable levels of Hacktools (22.9%) and ML detections (33.2%), remains a high-value target due to its financial and tech prominence. Trojans are also a consistent vector in India and Singapore, highlighting the ongoing success of phishing and credential theft.

For MSPs, this distribution underscores the urgent need to deploy ML-powered detection engines, implement EDR, regulate application use and monitor admin tool activity across diverse client environments. Proactive threat hunting and regional threat intelligence sharing can help MSPs stay ahead of evolving attack vectors.

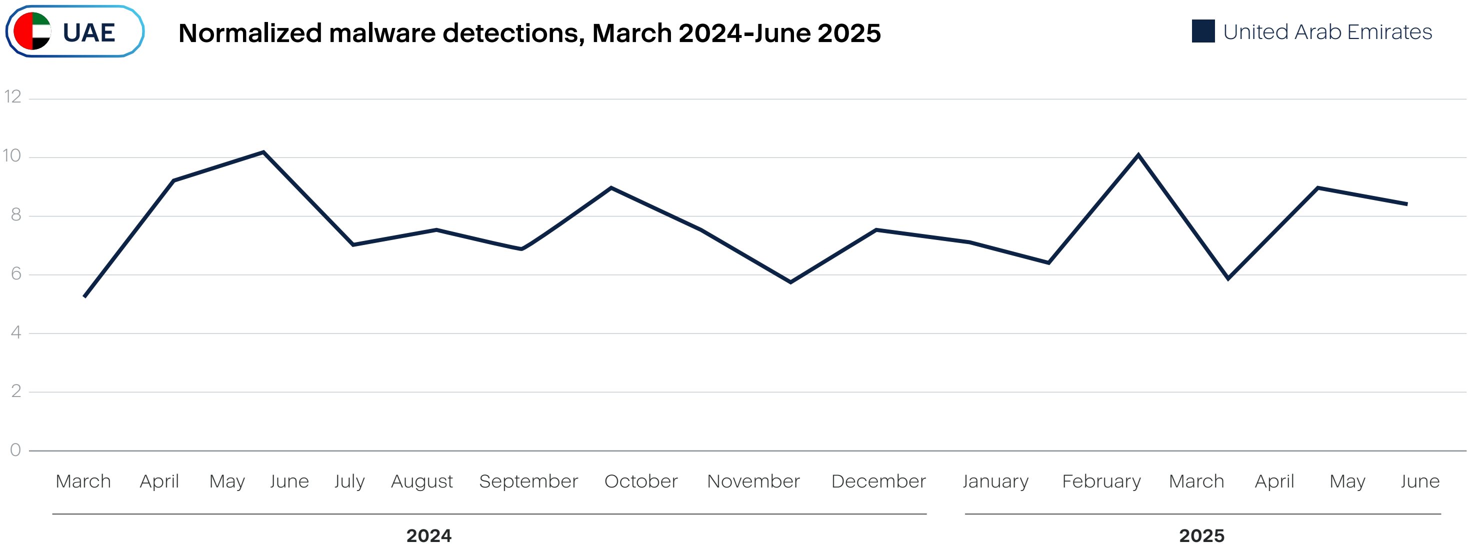
Normalized URL detections, March 2024-June 2025



India showed moderate activity throughout the year, with a notable decline after September, suggesting that improved filtration helped reduce noise from widespread, low-quality phishing kits often hosted on compromised blogs and forums. Singapore recorded elevated detection rates midyear, which may align with financial phishing tied to CPF (Central Provident Fund) scams and Singpass spoofing — attacks frequently observed before national budget announcements and year-end benefits processing.

Australia's relatively stable baseline, with brief rises in mid-2024, corresponds to campaigns impersonating telecom and postal services (e.g., Optus and Australia Post), known to ramp up during winter sales and end-of-financial-year offers. And also the recorded surges align with ATO-themed phishing, including QR-laced tax refund scams[51] impersonating the ATO and MyGov.

These campaigns illustrate that despite filtering advancements, seasonal schemes remain potent. Japan showed the lowest detection levels overall, consistent with high maturity in endpoint hygiene and early URL resolution filtering, though subtle rises in July 2024 and April 2025 suggest waves of invoice fraud and payment redirection campaigns tied to seasonal business cycles. It also correlates with the CoGUI phishing campaign mentioned earlier in the report. Active since at least October 2024, it unleashed over 580 million phishing emails between January and April of 2025. The campaign peaked at 172 million in January and impersonated brands like Amazon, PayPal and tax agencies in Japan, Australia, the U.S., Canada and New Zealand, mirroring the earlier PointyPhish / TollShark smishing surge in Japan and Australia with its focus on financial credential theft and wire fraud. Overall, while detections dropped, the precision of these signals has improved — surfacing more meaningful insights tied to phishing trends with national or seasonal context across the APAC region.


UAE Normalized malware detections, March 2024-June 2025

The UAE experienced a steady volume of malware detections with notable peaks in April 2024, September 2024, March 2025 and May 2025, possibly due to fake e-commerce invoice phishing targeting expatriate communities. The peak correlates with one of the most disruptive events in recent UAE history: record-breaking floods on April 16, 2024 affected multiple emirates, including Dubai and Sharjah. Such natural disasters often disrupt essential services and shift organizational focus toward emergency response, which can increase system vulnerabilities and reduce immediate cybersecurity monitoring.

In March 2025, a sharp spike in malware detections coincided with the UAE signing several Comprehensive Economic Partnership Agreements (CEPAs)[52], expanding cross-border digital activity and introducing new third-party and supply chain risks. This surge likely reflects increased adversary interest in sectors such as finance and logistics, as well as targeted social engineering campaigns exploiting the diplomatic momentum.

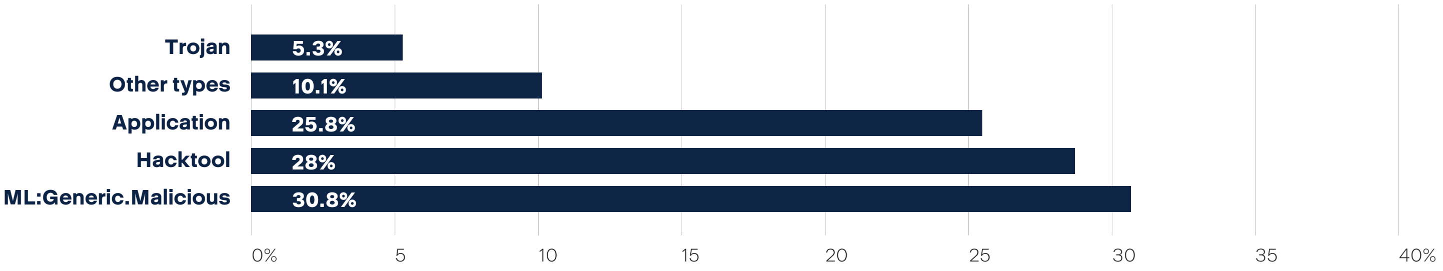
[51] Daisy Dumas. "Scammers are targeting myGov accounts during tax time. How can users protect their ATO refunds?" The Guardian. https://www.theguardian.com/australia-news/article/2024/aug/01/ato-mygov-tax-return-refund-scam, July 31, 2024.

[52] Gulf Today. "CEPA programme strengthens UAE's global economic position." https://www.bilaterals.org/?cepa-programme-strengthens-uae-s, March 31, 2025.

In April 2025, detections briefly dropped — possibly due to enhanced cybersecurity measures following these agreements[53] — before rising again in May, suggesting attackers quickly adapted to new defenses. The overall trendline illustrates the classic cycle of expansion-driven exposure, followed by brief stabilization and renewed threat activity as adversaries evolve.

Let's take a look at the distribution of detected malware types in the UAE from March 2024 to June 2025:

Distribution of detected malware types, March 2024–June 2025

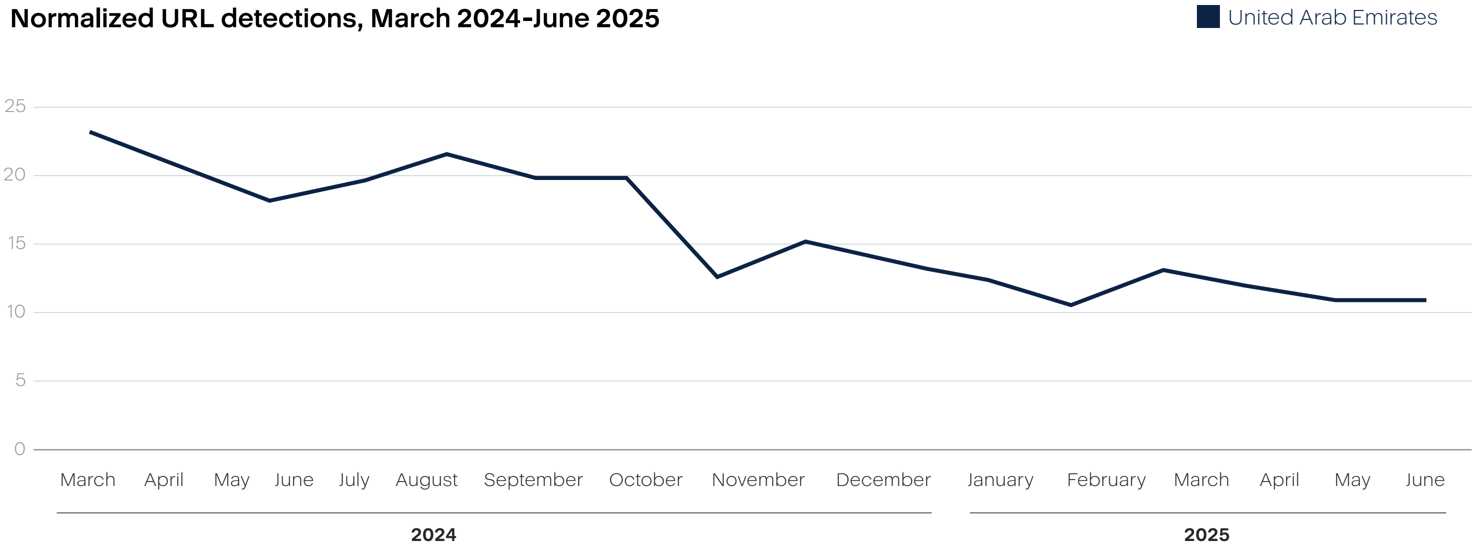


The UAE's high volume of ML:Generic.Malicious detections (31%) suggests growing use of evasive, obfuscated malware, often tied to financially motivated campaigns or targeted espionage and requiring advanced behavioral analysis to detect. Hacktools (28%) rank nearly as high, signaling active use of penetration testing tools repurposed by threat actors for lateral movement, privilege escalation and persistence within corporate environments — particularly risky in critical infrastructure and finance sectors.

The significant presence of Application-based threats (26%) indicates exposure to potentially unwanted programs or misused business software, often introduced through shadow IT or unmanaged third-party tools in hybrid cloud environments. Though lower in volume, Trojans (5.3%) remain a critical concern due to their role in credential theft, backdoors and ransomware deployment.

This distribution reflects a threat landscape where cyberattacks are becoming stealthier and more automated. To stay ahead, MSPs in the UAE should focus on AI-augmented threat detection, deploy robust EDR solutions, enforce strict control over administrative tools, and implement proactive vulnerability management to safeguard client environments and ensure business continuity.

Normalized URL detections, March 2024-June 2025



[53] Reuters. "UAE non-oil business grows steadily in April as hiring speeds up, PMI shows." https://www.reuters.com/world/middle-east/uae-non-oil-business-grows-steadily-april-hiring-speeds-up-pmi-shows-2025-05-05/, May 5, 2025.

As with other regions that experienced declines in URL detections, the decline in URL detections in the UAE from September 2024 onward aligns with the refinement of the the Acronis filter, reducing false positives and stale convictions. This cleanup increased detection quality, not just reduced volume — giving security teams greater confidence in what is flagged and why. UAE saw high rates in Q2–Q3 2024 that aligned with major campaigns spoofing government portals, Etisalat billing scams and e-commerce payment fraud. Among the known cases, Dubai resident U.B.[54] was tricked into entering her payment details and OTP on a fake Etisalat website, resulting in an unauthorized withdrawal of Dh1954.75 from her account.

The other spike happened in March 2025, which correlates to a surge in fake advertisements and deceptive links promising unrealistic offers — from bogus rentals to fake bank messages. As a result, Ajman Police[55] launched the "Your Security is in Your Awareness" campaign to educate the public on these evolving electronic fraud tactics and encourage vigilance against suspicious online activity.

Malicious websites

TRU blocked 27,576,489 phishing and malicious URLs[56] in Q1 2025, which is 2% less than in Q1 2024. Q2 2025 detections increased by 10.8% compared to Q1 2025, but when comparing to Q2 2024, it increased 28.5%.

Month	Blocked URLs	Total for the quarter
January	7,635,824	27,576,489
February	9,058,847	
March	10,881,818	
April	8,931,663	30,556,837
May	10,888,295	
June	10,736,879	

An average of 9.6% of endpoints tried to access malicious URLs in Q1 2025. The average slightly dropped in Q2 2025 to 9.2%

Month	Percentage of users that clicked on malicious URLs
January	10%
February	9.1%
March	9.7%
April	9.8%
May	8.5%
June	9.2%

Among the focus countries analyzed, Canada had the largest percentage of blocked malicious URLs at the endpoint in May 2025 (13.5%), followed by the UAE with 10.9% and Germany with 10.8%.

Countries	Normalized URL detections, %
Canada	13.5
United Arab Emirates	10.9
Germany	10.8
United States	9.4
Spain	8.7
Japan	8.6
Brazil	8.5
India	8
France	7.1
Switzerland	7
Italy	6.7
Australia	6.7
Denmark	6.4
Singapore	6
Sweden	4.6
United Kingdom	4.6

[54] Lara Palmer. "Dubai Resident Falls Prey to Etisalat Scam, Loses Over Dh1900." World Arabia. https://world-arabia.com/articles/dubai-resident-falls-prey-to-etisalat-scam-loses-over-dh1900/, June 13, 2024.

[55] Ruqayya Al Qaydi. "UAE: Fake rental, job ads among top online scams, say Ajman Police." Khaleej Times. https://www.khaleejtimes.com/uae/ajman-police-warn-against-fake-ads-scam-links, June 25, 2024.

[56] Methodology: The data is based on Acronis TRU telemetry collected from Acronis-protected endpoints with URL filtering enabled. The total count reflects all attempts to access suspicious (phishing,malicious, etc.) URLs that were proactively blocked by Acronis. The collected data relies on threat feeds and open-source threat intelligence (VT, APWG, URLHaus, etc.).

3

Acronis recommendations to stay safe in the current and future threat environment

The relentless surge of cyberattacks, data breaches and ransomware incidents reveals a stark truth: Conventional cybersecurity strategies are falling short. Weak technologies, overly complex systems and human errors exploited through sophisticated social engineering tactics consistently undermine defenses. MSPs and MSSPs, entrusted with securing client networks, face heightened risks due to their roles as gatekeepers of sensitive data. To overcome these challenges, a holistic cyber protection strategy is essential, integrating advanced detection, response and recovery capabilities into a cohesive platform. Acronis Cyber Protect Cloud unifies extended detection and response, endpoint protection, anti-malware, data loss prevention, email security, patch management, remote monitoring and backup functionalities, ensuring streamlined operations, enhanced compatibility and rapid recovery from threats.

Below, we expand on each recommendation with specific cases from this report to illustrate their importance.

Fortify backup and recovery systems

Backup systems are a critical line of defense but are often targeted by ransomware gangs to prevent recovery. In H1 2025, the Cl0p ransomware group compromised approximately 300 organizations by exploiting high-severity vulnerabilities in Cleo MFT platforms (CVE-2024-50623 and CVE-2024-55956), often disabling backups to maximize disruption. Similarly, the T1490 MITRE technique (Inhibit System Recovery) was used to disable system recovery features like shadow copies, as seen in multiple ransomware attacks. These cases highlight the vulnerability of standalone backup systems to compromise or configuration failures, leading to prolonged downtime and data loss.

An integrated cyber protection platform, Acronis Cyber Protect Cloud, addresses these threats by embedding backup within a comprehensive security framework. When threats disrupt data or systems, the platform instantly identifies the issue and restores affected assets from secure, tamper-proof backups, minimizing disruption. Unlike fragmented solutions, where separate anti-malware and backup agents operate independently and delay recovery, a unified system ensures real-time coordination, automatically triggering restoration without manual oversight. This approach empowers MSPs to maintain client trust and operational continuity, even in the face of sophisticated attacks.

Enhance threat detection and prevention

This report data shows a rise in sophisticated threats, including the use of T1055.001 (Process Injection) and T1059.001 (PowerShell) MITRE techniques to evade detection. The Telefonica breach in January 2025 involved infostealer malware (Redline) compromising credentials, enabling attackers to move laterally and exfiltrate data. SideWinder APT used spear-phishing emails paired with geofenced payloads to deliver StealerBot, a credential-stealing malware, to exploit long-known vulnerabilities like CVE-2017-11882 and CVE-2017-0199 in malicious Word and RTF files. The attack chain featured multistage loaders, shellcode-based payload delivery and server-side polymorphism to evade detection, blending classic espionage with cybercrime-style credential harvesting. These tactics highlight the need for advanced, multilayered detection to counter evasive threats that target specific regions and sectors.

Proactive defense is the foundation of modern cybersecurity and requiries tools that anticipate and neutralize threats before they cause harm. Integrated platforms leverage multilayered technologies, including AI-based, to detect anomalies and block malicious activities across endpoints, networks and cloud app environments. Extended detection and response (XDR) capabilities provide comprehensive visibility, simplifying threat analysis and enabling swift remediation for MSPs managing diverse client systems. Endpoint protection monitors device activities to identify suspicious behaviors indicative of ransomware or malware. Email and collaboration app security, and web filtering further shield against phishing attempts, a common entry point for attacks. By consolidating these defenses into a single agent like Acronis Cyber Protect Cloud, MSPs reduce operational complexity and strengthen their ability to protect client assets, ensuring robust security without the burden of juggling multiple tools.

Implement strong access controls with zero trust principles

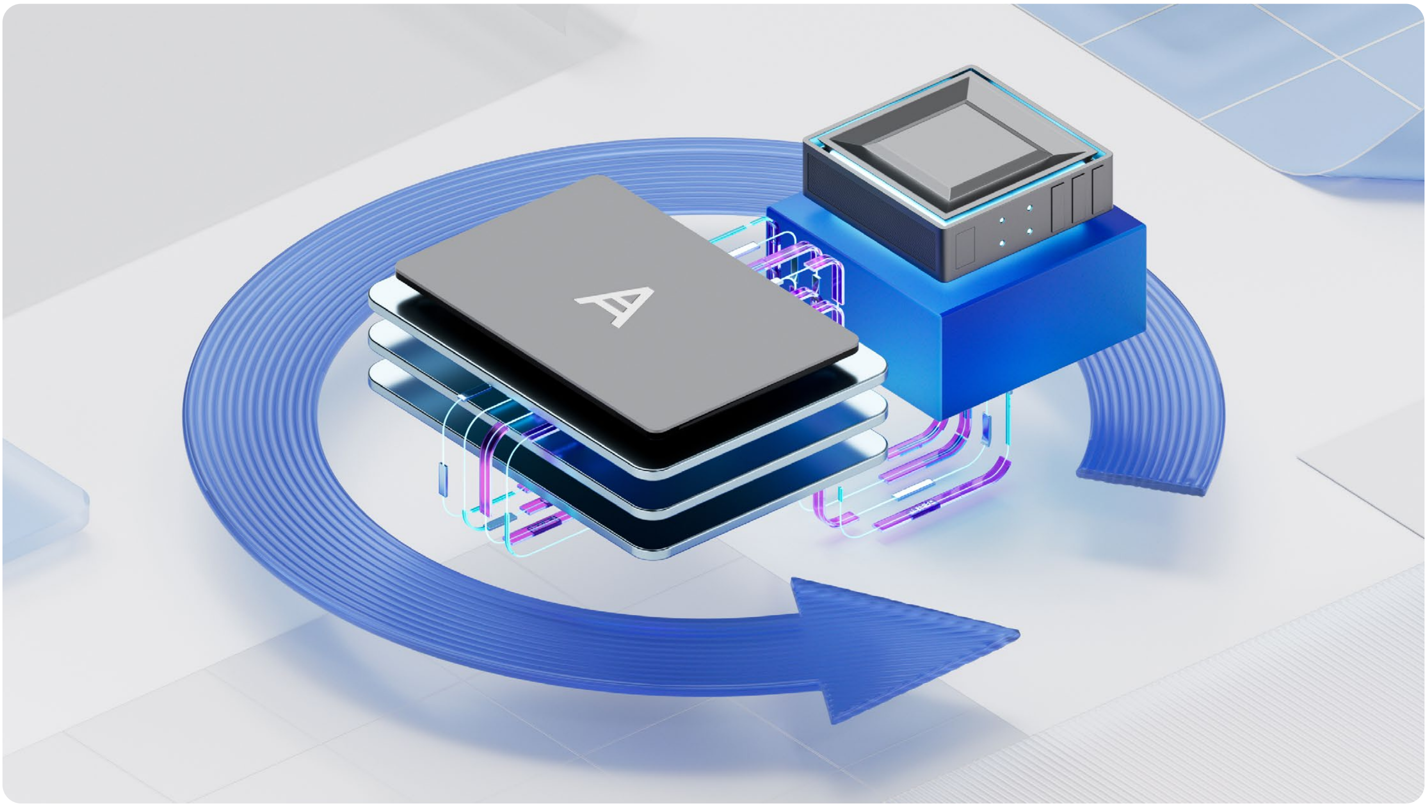
Credential theft and abuse of valid accounts were prevalent in H1 2025, with 13% of MSP-related attacks involving stolen credentials. The Asseco Poland breach in April 2025, perpetrated by the HellCat ransomware group, exploited Jira credentials harvested by the StealC infostealer to gain access and deploy ransomware. Similarly, the fake recruitment campaign targeting CFOs used malicious links to install legitimate remote access tools (NetBird and OpenSSH) and create hidden accounts for persistent access.

Securing access to systems and data is paramount for MSPs and MSSPs, starting with robust password management. Passwords should be long, unique, complex, and managed through a trusted password manager to maintain consistency across client services. Short, simplistic passwords are easily compromised and undermine even the strongest defenses.

Multifactor authentication must be mandated wherever possible to add a critical barrier against unauthorized access. Physical security is equally vital. Workstations, whether in offices or remote settings, must be locked when unattended to prevent data theft or tampering. MSPs should enforce policies requiring employees to secure devices and restrict workspace access, mitigating risks from insider threats or opportunistic breaches. Finally, regular audits of access controls ensure compliance and identify potential weaknesses before they can be exploited.

Prioritize software and system updates

Unpatched vulnerabilities remain a significant entry point for attackers, with 27% of MSP-related attacks in H1 2025 exploiting known flaws. The SimpleHelp RMM vulnerabilities (CVE-2024-57726, CVE-2024-57727 and CVE-2024-57728) were exploited by Play ransomware to gain remote access. Additionally, TeamViewer was the most vulnerable MSP tool among Acronis customers, with 4.56% affected by unpatched vulnerabilities, emphasizing the risks of delayed patching in remote access tools.



Keeping software and operating systems up to date is a fundamental defense against cyberthreats. Attackers frequently target outdated applications and systems, exploiting weaknesses that updates address. MSPs must ensure that Windows and critical software, such as productivity tools, communication platforms and remote access clients, receive automatic updates. User reluctance to install updates, especially those requiring restarts, often leaves systems exposed, so clear policies and automated processes are essential. Acronis Cyber Protect Cloud simplifies this task with built-in patch management to identify outdated software, prioritize critical updates, and apply them across client endpoints with minimal disruption. Detailed reporting verifies update success, enabling MSPs to maintain a secure posture and demonstrate compliance to clients and reducing the risk of preventable breaches.

Counter phishing, social engineering and attacks on collaboration apps

Phishing attacks targeting collaboration apps surged dramatically in H1 2025, with attacks on MSPs rising from 9% to 30.5%. A notable example is the DarkWatchman and Sheriff malware campaign, which leveraged phishing emails with password-protected archives to deliver malicious payloads through Microsoft Teams. These attacks tricked users into downloading remote access tools disguised as legitimate collaboration app updates, exploiting trust in platforms like Microsoft Teams to facilitate credential theft and system compromise. This underscores the growing threat of social engineering within collaboration platforms, where attackers exploit user familiarity to bypass traditional defenses. Acronis Cyber Protect Cloud enhances resilience with advanced email security and URL filtering, scanning communications and blocking access to harmful content in real time for collaboration cloud apps as well.

MSPs should complement these technologies with comprehensive employee training to teach staff to recognize suspicious messages and avoid clicking on unsolicited links or attachments. Simulated phishing campaigns reinforce awareness, helping employees develop instincts to question unexpected requests. By fostering a culture of vigilance, MSPs can significantly reduce the likelihood of successful social engineering attacks, protecting both their operations and client data.

Safeguard use of AI tools and services

AI-powered threats surged in H1 2025, with groups like FunkSec using AI to automate ransomware creation and claim over 150 victims. North Korean operatives employed AI-driven deepfakes to infiltrate tech companies and gain access to sensitive systems, while the DeepSeek AI model's vulnerabilities allowed prompt injection attacks to leak sensitive data. These cases demonstrate how AI tools amplify cybercriminal capabilities and introduce new risks when inadequately secured.

MSPs must establish clear AI usage policies, restricting the upload of sensitive client data to external platforms and limiting access to vetted tools. Specialized security measures, such as endpoint protection and access monitoring, prevent unauthorized AI misuse. This is especially important in highly regulated industries. For example, compliance with data privacy regulations such as GDPR, PCI DSS or HIPAA, requires encryption and strict access controls for AI interactions. Training cybersecurity teams on AI-specific risks, including attacks that manipulate machine learning models, is crucial. Continuous monitoring of AI activities, supported by logging and auditing, helps detect anomalies like unauthorized outputs, ensuring responsible and secure AI integration.

Build robust incident response plans

In March 2025, the Qilin ransomware group mentioned earlier in this report targeted Cobb County, Georgia, compromising 150GB of sensitive data, including autopsy photos, Social Security numbers and driver's licenses, forcing the county's IT department to shut down servers for a week to contain the breach. This prolonged downtime disrupted critical services for over 750,000 residents, highlighting the severe operational impact of ransomware when rapid response mechanisms are inadequate. The attack, claimed on Qilin's dark web leak site, underscores the need for robust incident response plans to mitigate extended disruptions and prevent data exposure in large-scale breaches.

Because no cybersecurity strategy is infallible, a well-defined incident response plan is essential for MSPs. Clear protocols for identifying, containing and eradicating threats, with assigned roles for technical and leadership teams, ensure rapid action during a breach. Regular tabletop exercises simulate scenarios like ransomware or data leaks, and prepare staff to respond effectively under pressure. Acronis Cyber Protect Cloud enhances response by combining threat detection with automated recovery, restoring systems from secure backups without delay. Off-site, immutable backups provide a failsafe against tampering and ensuring data integrity. Finally, MSPs should test restoration processes quarterly to verify that client systems can be recovered swiftly to maintain trust and minimize downtime.

About Acronis

Acronis is a global cyber protection company that provides natively integrated cybersecurity, data protection, and endpoint management for managed service providers (MSPs), small and medium businesses (SMBs), and enterprise IT departments. Acronis solutions are highly efficient and designed to identify, prevent, detect, respond, remediate, and recover from modern cyberthreats with minimal downtime, ensuring data integrity and business continuity. Acronis offers the most comprehensive security solution on the market for MSPs with its unique ability to meet the needs of diverse and distributed IT environments.

A Swiss company founded in Singapore in 2003, Acronis has 45 locations across the globe. Acronis Cyber Protect is available in 26 languages in 150 countries and is used by over 20,000 service providers to protect over 750,000 businesses.

Acronis

Acronis Threat Research Unit

Learn more at
[acronis.com](https://www.acronis.com)