Acronis 總代理湛揚科技

Report
H2 2025

Acronis Cyberthreats Report, H2 2025: From exploits to malicious AI

Acronis Threat Research Unit

Table of contents

Authors:

Senior Research Team — Acronis Threat Research Unit (TRU)

Introduction and summary

The Acronis Cyberthreats Report covers the global threat landscape as encountered by the Acronis Threat Research Unit (TRU) and Acronis sensors in the second half of 2025. General threat data (including malware, ransomware, web and email threats, vulnerabilities, etc.) presented in the report is gathered from January–December of 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:

- In 2025, the number of email-based attacks per organization increased by 16% and the number of attacks per user increased by 20%.
- We identified almost 150 victims of ransomware gangs in MSP and telco groups in 2025.
- Phishing is the number one initial attack vector targeting MSPs — 52% of all cases.
- There was a sharp increase in advanced attacks in collaboration channels, from 12% in 2024 to 31% in 2025.
- South Korea was the most attacked country in terms of malware, with an average of 12% of users affected during the year.

Cybersecurity trends in H2 2025:

- PowerShell is the single most abused legitimate application across every observed month in Acronis telemetry. Its dominance is consistent in Germany, the United States and Brazil.
- In H2 2025, phishing accounted for 83% of all email threats, while advanced attacks represented only 1%.
- Although absolute numbers are small, 100% of MSP-platform vulnerabilities disclosed in 2025 were “high” or “critical,” reinforcing their disproportionate operational risk.
- During 2025, artificial intelligence was increasingly embedded into criminal operational workflows, rather than used experimentally or opportunistically.
- India, the U.S. and Netherlands experience the most mass infection / lateral-movement cases according to our telemetry.
- Makop was the most prevalent ransomware family in internal detections, significantly outpacing all others. Its sustained presence indicates continued use as a commodity ransomware by multiple affiliates rather than short-lived campaigns.
- Manufacturing and technology were the most attacked sectors by ransomware gangs, reflecting (a) high operational pressure to restore availability; (b) broad IT / OT and supplier connectivity; and (c) heterogeneous patching maturity across distributed sites.

What you will find in this report:

- Top ransomware gangs and their activity in 2025.
- What techniques are used to attack MSPs.
- Latest trends and statistics on phishing and other email-borne attacks.
- Vulnerabilities found on Acronis customers’ machines, and specific vulnerabilities against MSPs.
- Cases of AI-abuse by cybercriminals.
- Extensive Acronis data on malware, ransomware, vulnerabilities and web-based threats in 2025.
- Recommendations for how to stay safe.
- Forecast for 2026.

1

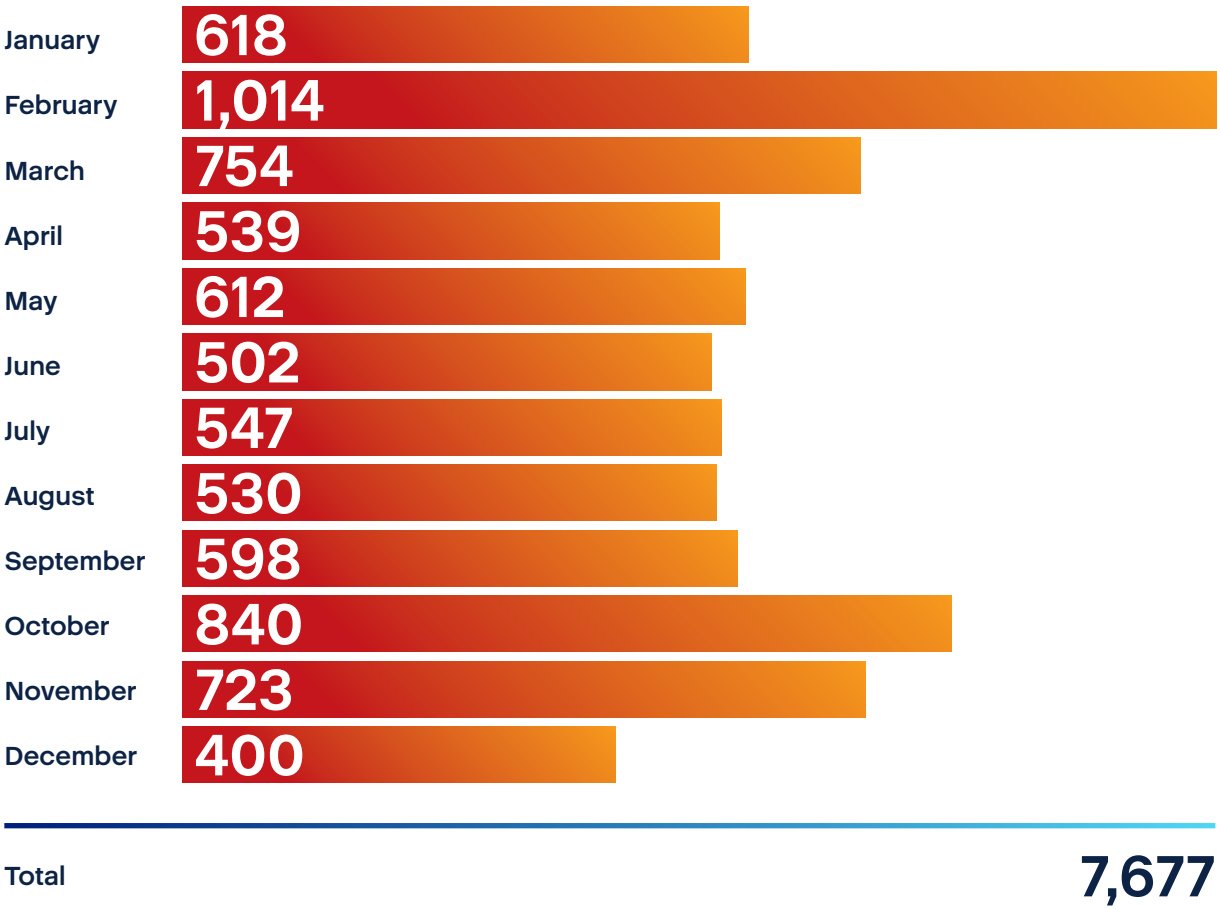
Key cyberthreats and trends in H2 2025

1. Ransomware outlook including the gangs targeting Acronis customers

Ransomware activity in 2025 remained persistently high and structurally resilient. Public disclosure data confirms that ransomware operators sustained pressure across all months, with multiple sharp spikes reflecting large-scale campaigns rather than isolated intrusions. The year was characterized by a fragmented but highly productive ecosystem, where a small number of dominant ransomware programs accounted for a disproportionate share of victims, while dozens of smaller or newly formed groups continued to emerge.

From January 1 to December 14, 2025, a total of 7,681 organizations were publicly named[1] as ransomware victims.

Monthly ransomware victims – 2025



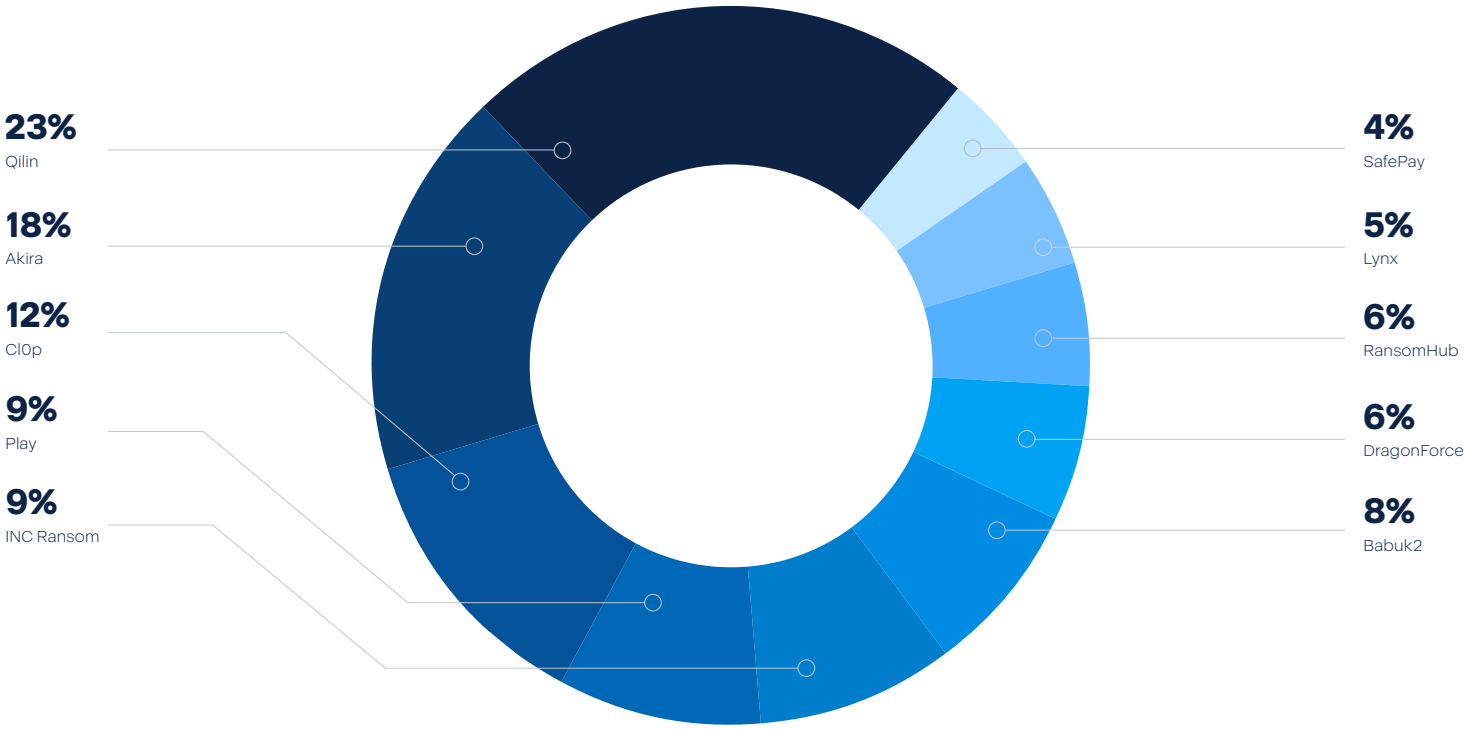
[1] Acronis Threat Research Unit (TRU). "SafePay ransomware: The fast-rising threat targeting MSPs." https://www.acronis.com/en-us/tru/posts/safepay-ransomware-the-fast-rising-threat-targeting-msps/, July 8, 2025.

Two clear peaks define the 2025 ransomware timeline. February, the most active month of the year, exceeded 1,000 publicly disclosed victims, suggesting the presence of highly scalable intrusion paths, typically associated with mass exploitation of exposed services, credential-based access at scale or third-party compromise cascades. The Cl0p gang heavily contributed back then[2] with their usage of infamous Cleo MFT vulnerability. October represented a second major escalation, consistent with post-summer remobilization of ransomware affiliates and increased disclosure pressure as groups seek to close the year with high-impact extortion outcomes. Again Cl0p played a role here by exploiting a critical vulnerability (CVE-2025-61882[3]) in Oracle E-Business Suite versions 12.2.3–12.2.14 to achieve remote code execution via server-side request forgery (SSRF).

Most active ransomware groups – 2025

Ransomware activity in 2025 was concentrated among a small number of high-volume operators, despite the presence of nearly one hundred active ransomware brands.

Top ransomware groups by publicly disclosed victims

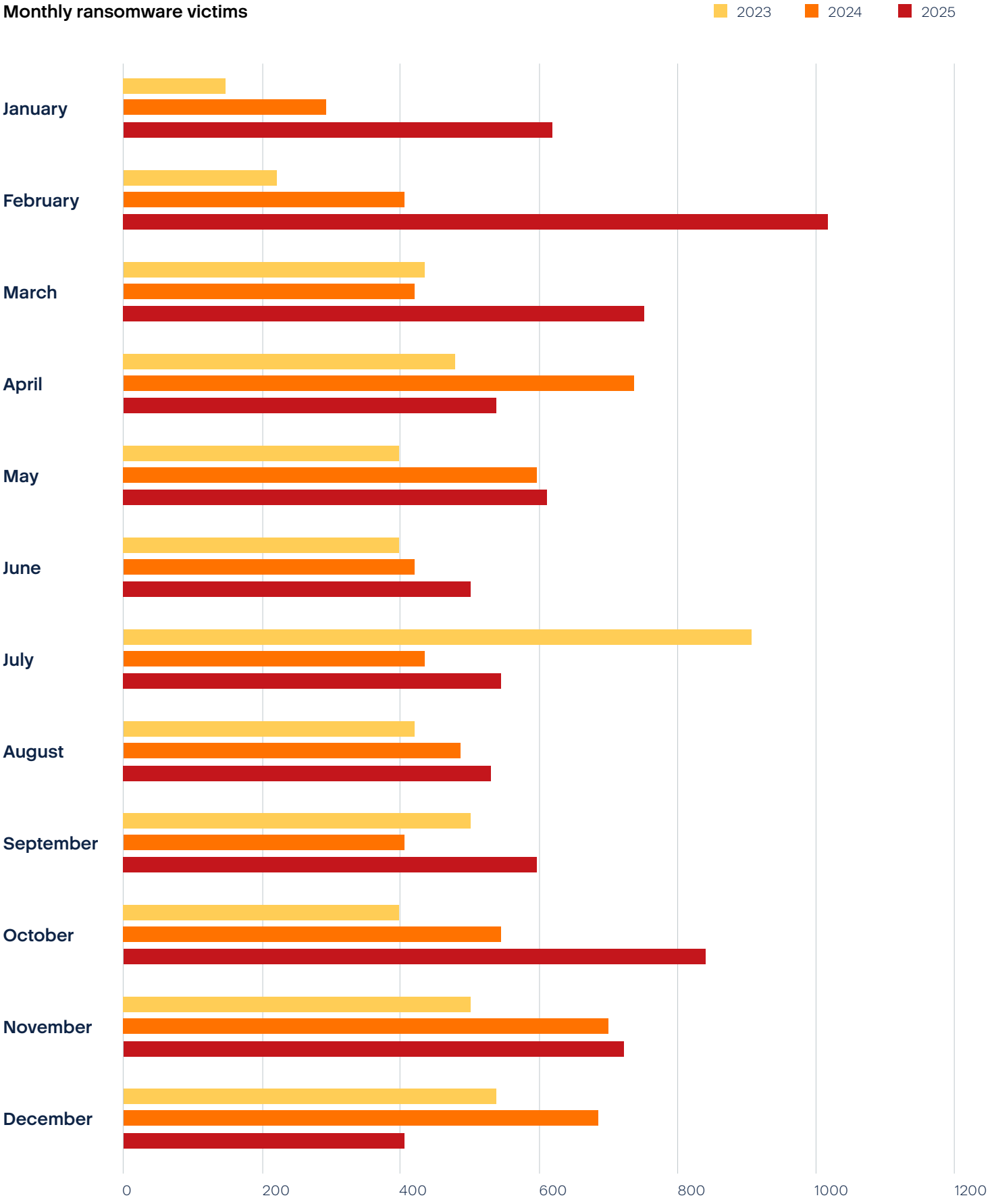


The top three groups alone accounted for a substantial share of total disclosed victims, underscoring the gravitational pull of mature RaaS ecosystems that provide affiliates with proven tooling, infrastructure and monetization workflows.

[2] Kovacs, Eduard. "CVE Assigned to Cleo Vulnerability as Cl0p Ransomware Group Takes Credit for Exploitation." SecurityWeek, December 16, 2024. https://www.securityweek.com/cve-assigned-to-cleo-vulnerability-as-cl0p-ransomware-group-takes-credit-for-exploitation/

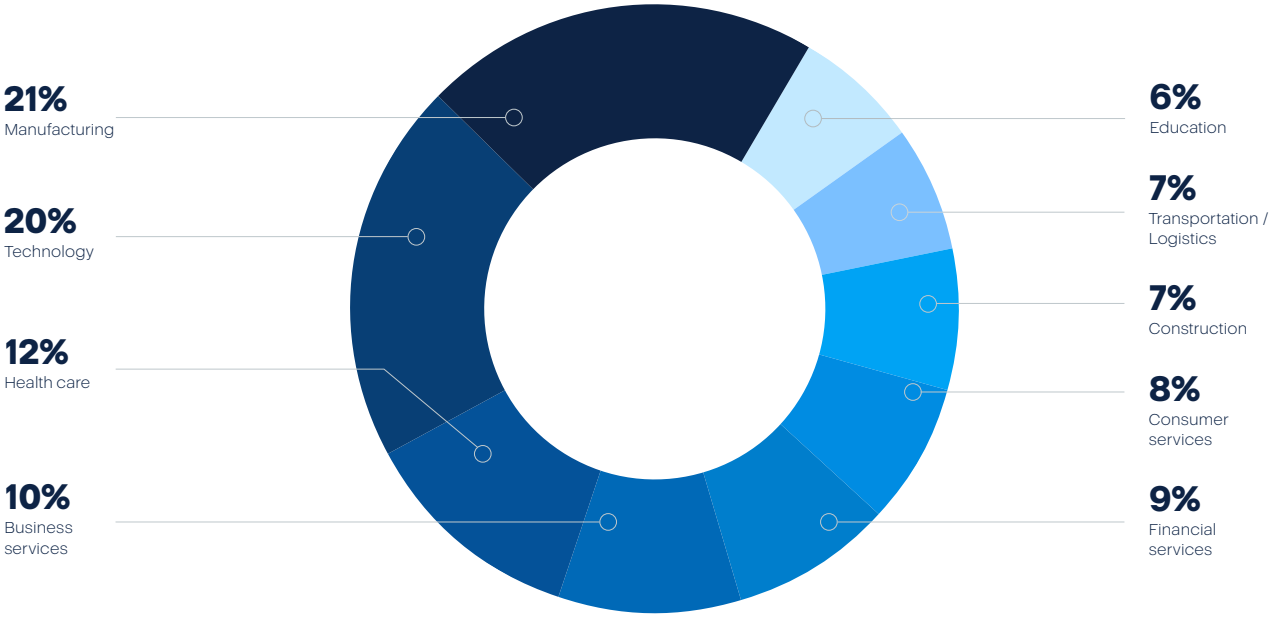
[3] Dutta, Tushar Subhra. "Hackers Registered 18,000 Holiday-Themed Domains Targeting 'Christmas,' 'Black Friday,' and 'Flash Sale.'" Cyber Security News, November 28, 2025. https://cybersecuritynews.com/hackers-registered-18000-holiday-themed-domains/

Monthly ransomware victims



Sector targeting (public-disclosure attribution)

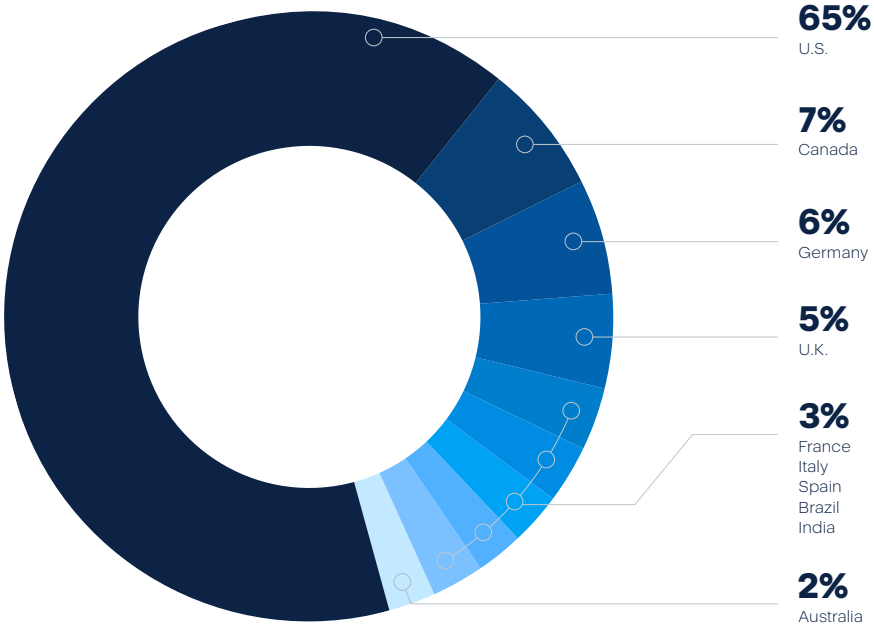
Most targeted sectors by disclosed victims:



Manufacturing and technology maintain consistently high exposure in disclosure data, typically reflecting (a) high operational pressure to restore availability; (b) broad IT / OT and supplier connectivity; and (c) heterogeneous patching maturity across distributed sites.

Regional concentration (country of victim)

Top countries by disclosed victims:



The U.S. remains the dominant locus in disclosure data, which is typically driven by a combination of (a) attacker ROI assumptions (ability to pay); (b) scale of addressable enterprise footprint; and (c) higher visibility / traceability of disclosed incidents. Cross-border spillover remains evident in the long tail of Europe and APAC.

ClOP remains one of the most technically consequential ransomware groups due to its repeated exoploitation of high-impact vulnerabilities in enterprise software.

Top ransomware groups: Tactics and exploited weaknesses

Qilin

Qilin emerged as the most prolific ransomware[4] operator of 2025. The group operates a RaaS model and deploys ransomware written in modern compiled languages, enabling cross-platform targeting of Windows and Linux environments. Qilin consistently employs a double-extortion technique, exfiltrating large volumes of sensitive data before encryption and using public leak sites as a primary coercion mechanism.

Public investigations link Qilin intrusions to exploitation of exposed remote services, phishing-based credential harvesting and abuse of weakly protected administrative interfaces. Once inside a network, Qilin affiliates demonstrate disciplined lateral movement, privilege escalation and staged data exfiltration prior to payload execution. This operational maturity allows Qilin to remain effective even against organizations with functioning backup and recovery strategies.

Akira

Akira ranked second in total disclosed victims in 2025 and is representative of ransomware operators emphasizing human-centric initial access. Public reporting associates Akira campaigns with phishing and social-engineering techniques designed to harvest credentials or deliver initial loaders, followed by exploitation of exposed VPN or RDP services.

Akira operations frequently include data theft prior to encryption, aligning with broader industry movement toward extortion-first ransomware. While Akira was not publicly tied to a single dominant zero-day vulnerability in 2025, its success reflects the continued effectiveness of credential compromise and identity-centric attack paths in environments with inconsistent MFA enforcement.

ClOp

ClOp remains one of the most technically consequential ransomware groups due to its repeated exploitation of high-impact vulnerabilities in enterprise software. In 2025, ClOp was publicly linked to exploitation of critical vulnerabilities in widely deployed platforms, including Oracle E-Business Suite, enabling unauthenticated remote code execution and large-scale data exfiltration.

Unlike many ransomware groups, ClOp often prioritizes data theft without immediate encryption, leveraging stolen information as the primary extortion mechanism. This approach has resulted in mass-victim disclosure events affecting hundreds of organizations simultaneously, particularly in supply chain-heavy environments where a single vulnerable application exposes many downstream entities.

[4] Ransomware.live. Ransomware Statistics for 2026. N.d., ca. 2026. https://www.ransomware.live/stats

New ransomware groups observed in H2 2025

Based on first appearance in the dataset, 34 groups are “newly observed” from H2 2025 (first seen on or after July 1). The most significant new entrants by disclosed victim count include:

151 Sinobi First seen July 5, 2025	**70** TheGentlemen First seen September 9, 2025	**61** CoinbaseCartel First seen September 15, 2025	**49** Pear First seen August 5, 2025
46 Beast First seen July 29, 2025	**46** ShinyHunters First seen October 3, 2025	**43** PayoutsKing First seen July 7, 2025	**39** LockBit5 First seen Dec. 7, 2025

The appearance of multiple new brands in H2 is consistent with RaaS fragmentation and rebranding dynamics; new “labels” can emerge rapidly when affiliates migrate, when operators retool infrastructure or when trust collapses in a prior program.

While many of these groups remain small, several demonstrated rapid victim accumulation.

- **Sinobi (151 victims):** Sinobi appeared in mid-2025 and quickly accumulated victims through opportunistic campaigns. Public disclosures suggest reliance on exposed remote access services and credential reuse rather than sophisticated exploit chains, indicating low operational overhead but high scalability.
- **TheGentlemen (70 victims):** This group targeted primarily small and midsize organizations, often exploiting outdated web applications and misconfigured servers. Its activity reflects a “fast-cycle” ransomware model focused on speed and volume over stealth.
- **CoinbaseCartel (61 victims):** Despite branding implications, this group has no known link to the cryptocurrency exchange. Disclosures indicate phishing-led intrusions followed by rapid lateral movement in lightly defended enterprise networks.
- **Pear (49 victims):** Pear’s victim set suggests exploitation of third-party service integrations and insecure APIs, pointing to a growing attack surface created by SaaS dependencies and outsourced IT workflows.
- **Beast (46 victims):** Beast appears to target organizations with weak identity controls, leveraging exposed VPN access and inconsistent MFA enforcement rather than zero-day exploitation.

These emerging groups illustrate how quickly ransomware operators can rebrand or launch new identities, limiting the long-term impact of takedowns against individual programs.

Overall, the ransomware landscape in 2025 reflects a mature criminal economy with three defining characteristics:

Scalability
High-impact months correlate with repeatable intrusion paths rather than bespoke attacks.

Fragmentation
Nearly 100 active ransomware brands reduce the effectiveness of single-group disruption.

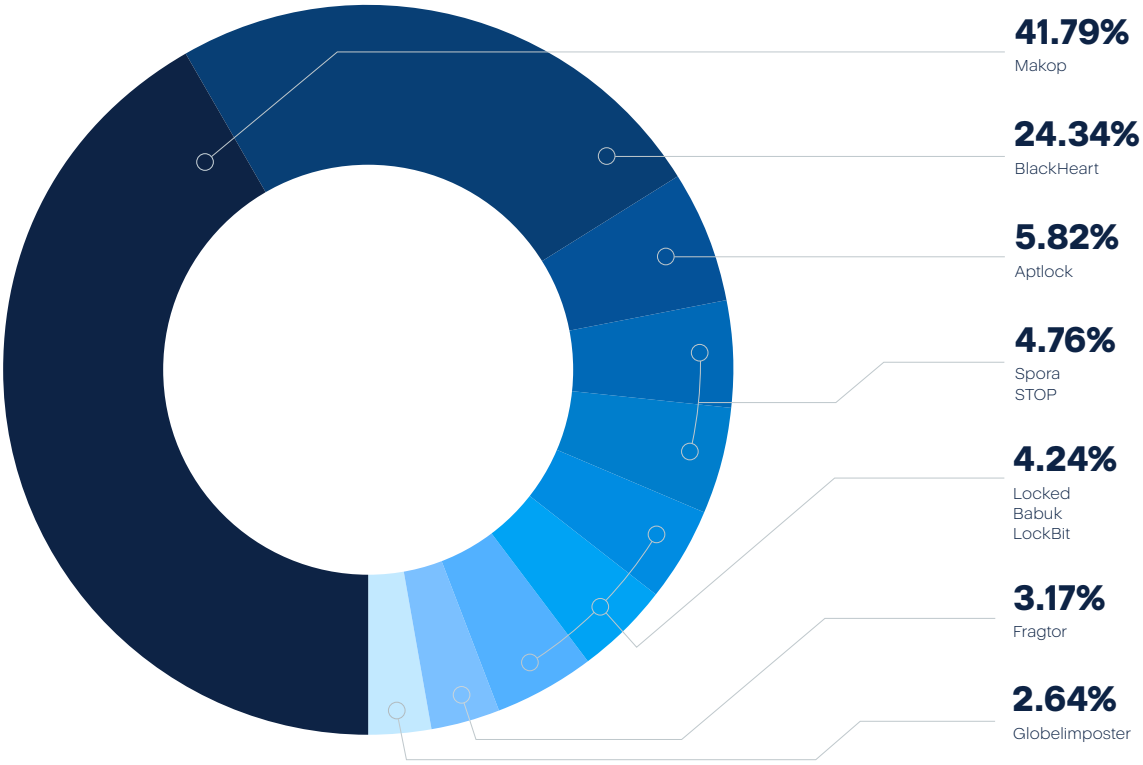
Extortion primacy
Data theft and disclosure pressure increasingly outweigh encryption as the primary coercive tool.

Together, these dynamics explain why ransomware volumes remain elevated despite increased defensive investment and law-enforcement activity.

Acronis ransomware telemetry analysis

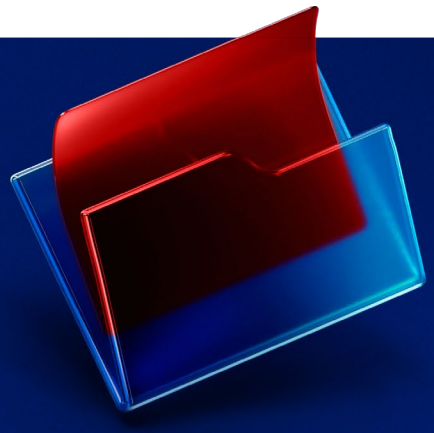
Based on first appearance in the dataset, 34 groups are “newly observed” from H2 2025 (first seen on or after July 1).

Ransomware family distribution detected and blocked by Acronis Active Protection, January–December 2025.



In this report, we also did a detailed analysis of Acronis Active Protection (in-house anti-ransomware technology used in Acronis products) telemetry. Internal ransomware detections observed throughout 2025 show a highly concentrated threat landscape, dominated by a small number of families and disproportionately affecting a limited set of countries. While many ransomware families appear sporadically, a handful demonstrate both scale and operational maturity, including advanced post-exploitation techniques such as code injection into trusted binaries.

Makop ransomware is the most prevalent ransomware family in internal detections.



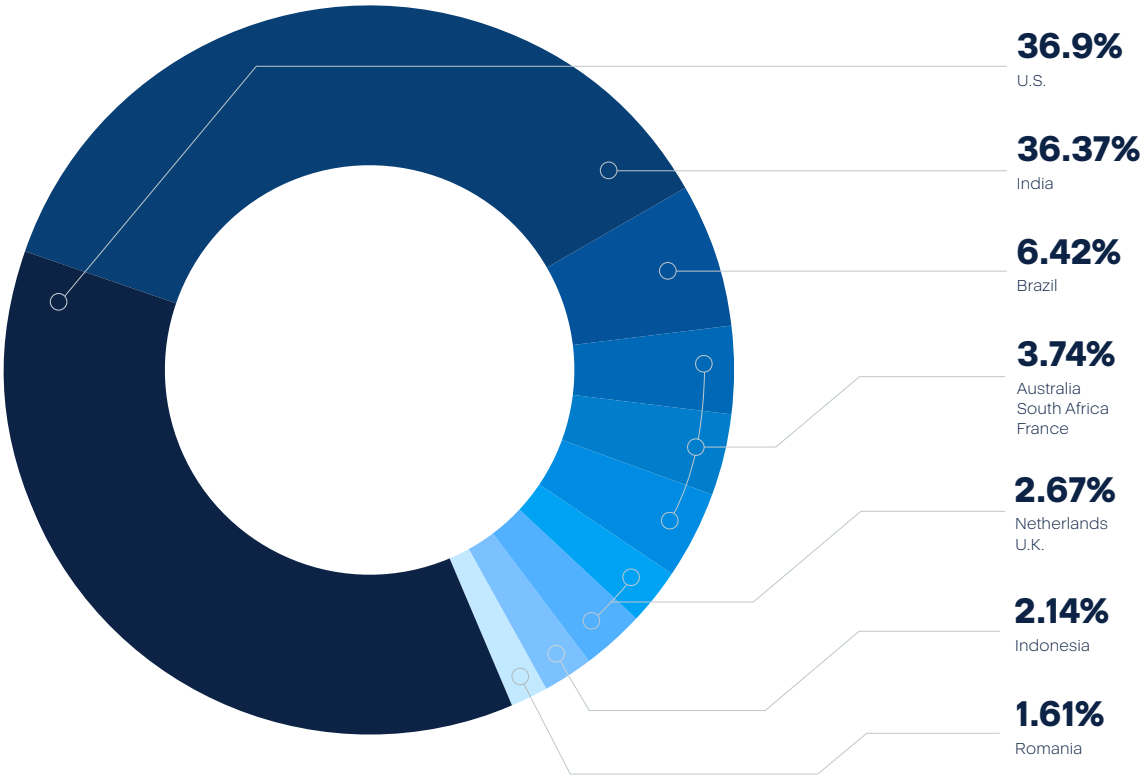
Ransomware family landscape

The family distribution is strongly skewed: Makop[5] is the most prevalent ransomware family in internal detections, significantly outpacing all others. Makop reemerged in late 2025 and was mostly focused on Asia. BlackHeart emerged as the second most detected family, suggesting growing adoption and potentially more aggressive targeting strategies.

A second tier of families, including Aptlock, Spora, STOP, LockBit, Babuk and Locker had moderate but persistent activity, consistent with affiliate-driven or regionally focused operations. A long tail of ransomware families (e.g., Akira, GlobeImposter, BabyLockerKZ, Cryak, Mallox and Black) had with low detection counts, indicating either highly targeted attacks, short campaign lifetimes or limited telemetry visibility.

Geographic distribution of ransomware detections

Geographical distribution of attacked machines globally, January–December 2025

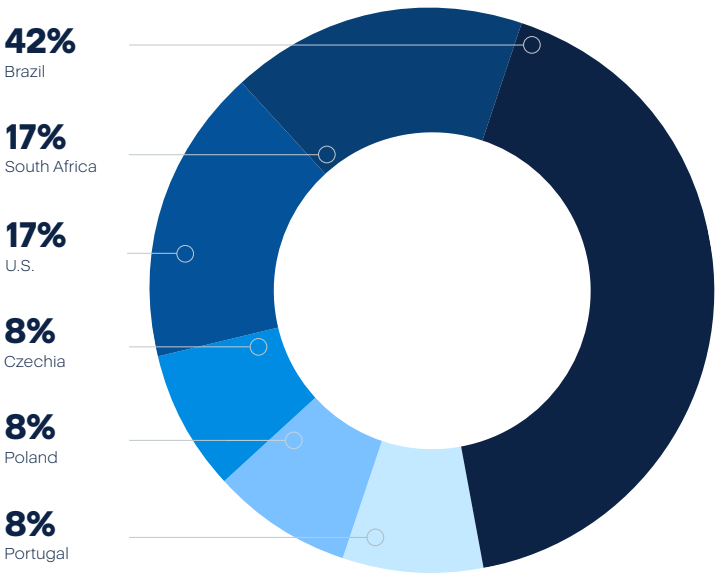


[5] Acronis Threat Research Unit. "Makop ransomware: GuLoader and privilege escalation in attacks against Indian businesses." Acronis. December 8, 2025. https://www.acronis.com/en/tru/posts/makop-ransomware-guloader-and-privilege-escalation-in-attacks-against-indian-businesses/

Country-level analysis shows clear concentration: The U.S. and India lead in total ransomware detections, reflecting a combination of large endpoint populations, broad industry exposure and high attacker ROI. Brazil ranks third, standing out as the most affected country in Latin America and a recurring hotspot across multiple ransomware families. Australia, South Africa, France and the Netherlands form a secondary cluster, indicating consistent but lower-volume targeting. Detections across Europe and Asia are widely distributed, but most countries show only isolated cases, suggesting opportunistic or single-incident compromises rather than sustained campaigns.

Attackers continue to prioritize large, digitally mature economies with high ransomware monetization potential. However, the broad geographic spread confirms that ransomware remains a globally scalable threat, not confined to any single region.

Injection into trusted binaries: Deeper technical insight



This highlights a high-risk behavioral pattern: ransomware activity involving process injection into trusted or legitimate binaries. While these injection cases represent a relatively small fraction of total ransomware detections, they are strategically significant, as they reflect deliberate investment in defense-evasion techniques rather than opportunistic, large-scale execution.

Within the observed dataset, injection activity is concentrated in a narrow set of ransomware families, primarily Locked, STOP and GlobeImposter, including XXX, which analysis confirms to be GlobeImposter variants. Among these, the Locked family clearly dominates injection-based activity, with multiple distinct samples consistently exhibiting process-injection behavior. This pattern suggests a repeatable and intentional execution strategy, rather than isolated experimentation. STOP and GlobeImposter (including its variants) appear less frequently but still demonstrate selective use of injection, likely to reduce visibility during payload deployment or early execution stages.

From a geographic perspective, Brazil accounts for the majority of observed injection cases, followed by detections in the U.S., South Africa and several European countries, including Czechia, Poland and Portugal. This distribution may indicate either more mature attacker tradecraft targeting these regions or a higher prevalence of environments where trusted-binary abuse remains effective against endpoint security controls.

Process injection is commonly leveraged to evade signature-based detection, blend malicious activity into legitimate process trees, and delay or bypass endpoint defenses during the execution phase. Although not widely adopted across all ransomware operations, its presence marks a higher-sophistication subset of ransomware attacks in 2025, where operators prioritize stealth and reliability over raw volume.

When correlating families, geography and techniques, a clear separation becomes evident. High-volume families such as Makop and BlackHeart predominantly rely on scale and repetition, with little indication of advanced injection-based evasion. In contrast, Locked, STOP and GlobeImposter demonstrate that injection techniques are applied selectively and strategically, likely during high-value intrusions or post-compromise escalation, rather than as a default delivery mechanism. Regions exhibiting recurring injection cases — particularly Brazil and the U.S. — also correspond to countries with elevated ransomware exposure overall, reinforcing their attractiveness as targets for more sophisticated ransomware operators.

Strategic implications

This data collectively confirms that ransomware in 2025 was not only widespread but increasingly bifurcated between scale-driven and sophistication-driven operations, requiring layered detection and response strategies. Defensive strategies should prioritize behavior-based detection and process-level monitoring, particularly for abuse of trusted binaries. Organizations in high-impact regions should assume ransomware operators are capable of evasion-focused techniques, not just mass encryption events. Continuous telemetry-driven analysis is essential to distinguish high-volume noise from low-frequency, high-risk ransomware behavior.

2. Public MSP attack cases

This section quantifies MSP / supply chain exposure using public ransomware victim disclosures. Provider-layer targeting remained economically rational: MSP and telecom providers represent "access aggregation," enabling attackers to monetize one intrusion repeatedly across tenants. The exploitation-to-propagation chain tightened: 2025 cases show a compressed path from initial access (often RMM / admin plane) to downstream deployment. This reduces defender reaction time and increases likelihood of multitenant impact. Extortion-first dynamics increased supply chain blast radius: Even when encryption is contained, data theft from a provider can create secondary harm for customers (regulatory reporting, contractual penalties, fraud risk), increasing attacker leverage.

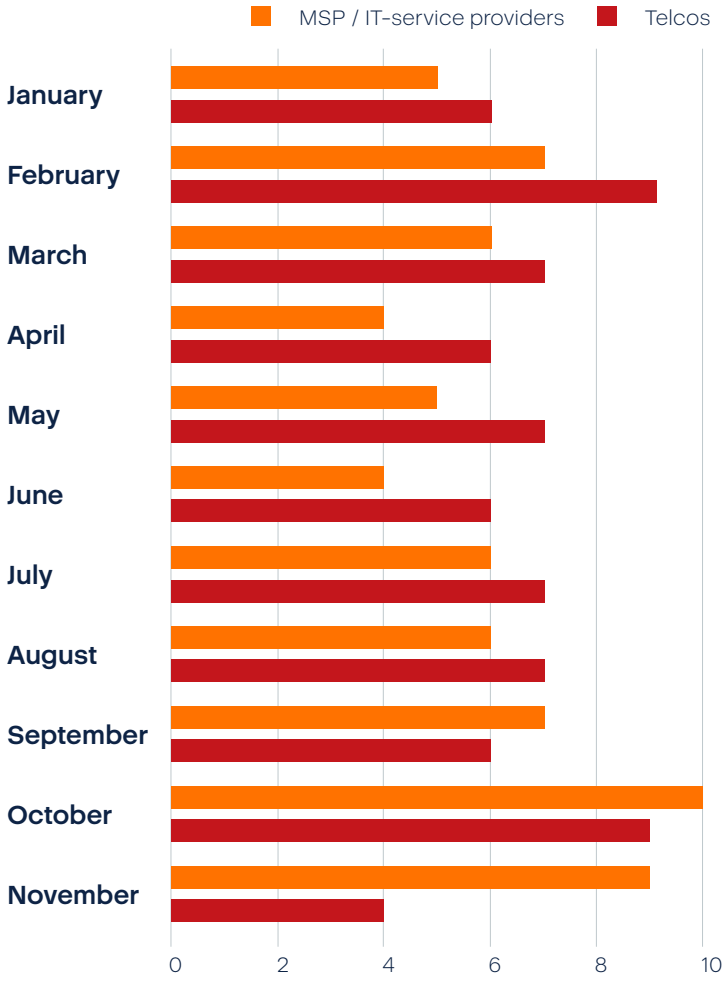
MSP vs. telco victims – 2025

Based on available public information we identified 143 provider-type victims in 2025:

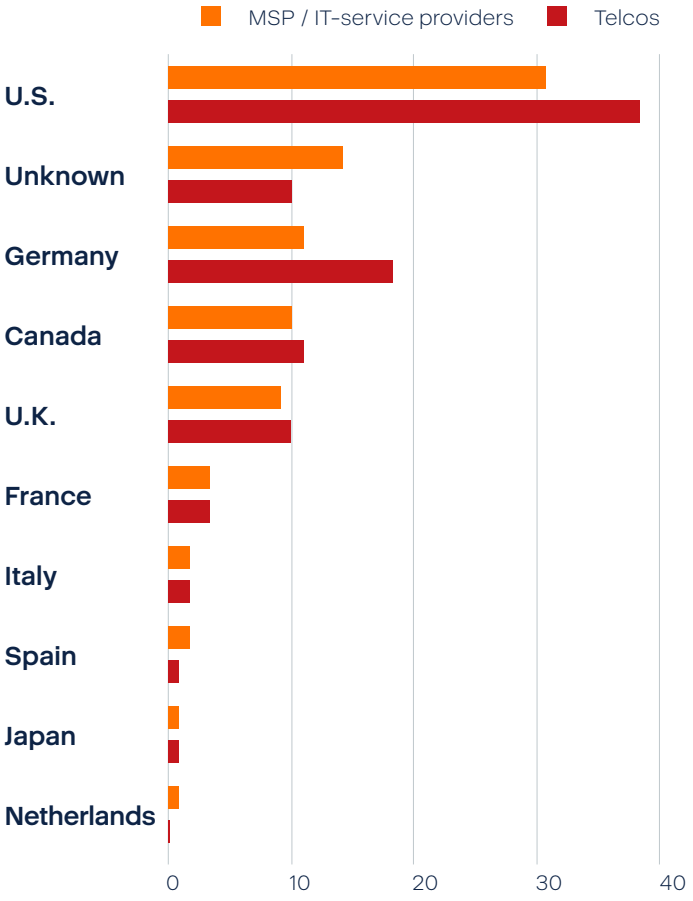
69 MSP / IT-service providers (≈0.9% of all publicly known 2025 victims)

74 Telecommunications providers (≈1.0% of all publicly known 2025 victims)

Attribution is based solely on explicit wording in ransomware disclosure titles and descriptions. No enrichment, inference or downstream assumptions were applied.



Both MSP and telco ransomware disclosures follow the same seasonal curve as the broader ransomware ecosystem, with a clear Q4 concentration. Telco incidents remained relatively stable throughout the year, while MSP disclosures showed a sharper rise in October–November, consistent with access-aggregation and delayed disclosure dynamics.



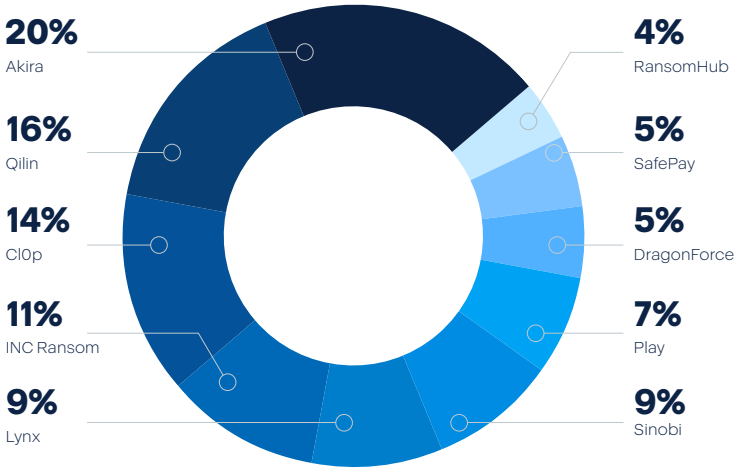
MSP / IT-service providers – country share (%)

Telcos – country share (%)

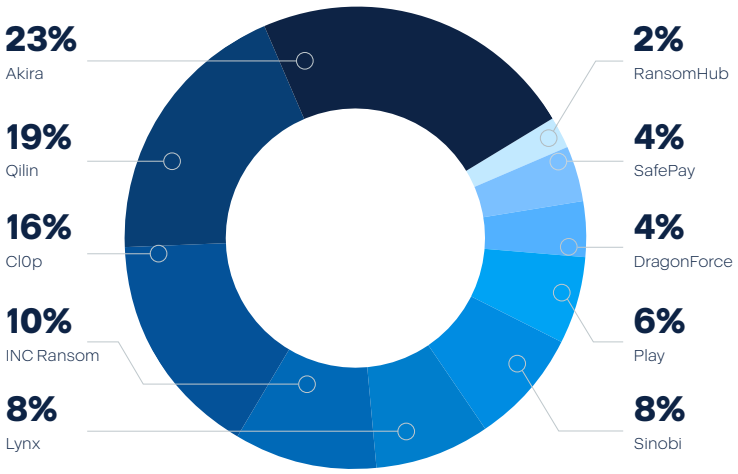
The U.S. dominance is evident across both categories, reflecting provider concentration and stronger disclosure visibility. Telco incidents are slightly more geographically distributed, consistent with the global footprint of telecommunications operators.

Ransomware group attribution – 2025

MSP / IT-service providers



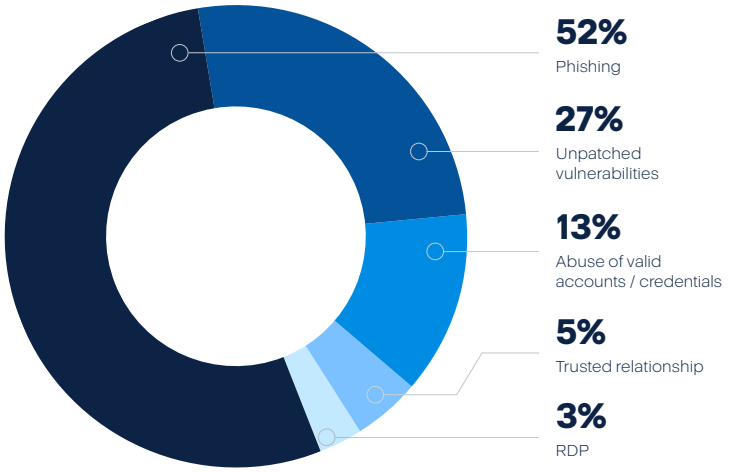
Telcos



The same dominant ransomware groups are responsible for attacks across both MSPs and telcos. There is no evidence of actor specialization by provider type; instead, groups opportunistically target whichever provider-layer access yields the greatest leverage at a given time.

In 2025 ransomware disclosures, telecommunications providers were slightly more frequently identified than MSPs or IT service providers. However, both categories exhibit similar seasonality, geographic concentration, and threat actor overlap, reinforcing that provider-layer compromise is driven by access aggregation and scale, not sector-specific targeting.

Initial access vectors – 2025



Phishing remains the most common human-centric access vector, frequently enabling credential capture or malware delivery that later facilitates broader compromise. While phishing is more dominant in general ransomware campaigns, its lower share here highlights attackers' preference for indirect access paths when targeting service providers.

Exploitation of unpatched software was the dominant initial access vector in MSP and supply chain ransomware incidents in 2025. This reflects attackers' continued success in targeting internet-facing applications, remote access infrastructure and enterprise management platforms where patch latency creates scalable entry points.

Credential abuse appears less frequently as a standalone primary vector in public disclosures, though it is widely understood to be underreported. In many cases, credential compromise likely acts as an intermediate step following phishing or third-party access.

Trusted relationship access captures cases where attackers entered environments through compromised partners, suppliers or delegated access. This vector reflects initial access via inherited trust, not lateral propagation after compromise, and is a defining characteristic of supply chain-driven ransomware activity.

Direct exploitation of exposed RDP services is rare in MSP and supply chain disclosures. This reflects a broader shift away from noisy, easily detected entry points toward more reliable and less conspicuous access mechanisms.

RMM tool abuse examples

Cybercriminals continued to abuse remote monitoring and management (RMM) tools throughout the second half of 2025, with ransomware actors in particular relying on them as a reliable mechanism for persistence, lateral movement and payload deployment. Multiple H2 2025 investigations showed attackers deliberately targeting RMM platforms because they provide trusted, administrative-level access that blends into normal MSP operations. In several ransomware incidents reported in late 2025, threat actors used stolen credentials to access legitimate RMM consoles and then deployed ransomware simultaneously across multiple endpoints, dramatically increasing blast radius and speed of impact.

Other cases documented attackers installing their own RMM agents post compromise, effectively turning a victim environment into a remotely managed asset under attacker control. These tools were also used to disable security software, execute scripts and exfiltrate data before encryption. The continued misuse of RMMs underscores why ransomware groups view MSP tooling as a force multiplier: Once an RMM is compromised or abused, attackers can scale operations rapidly across customer environments while evading detection by appearing as legitimate administrative activity. Here just a few notable examples of attacks involving RMM systems.

Month (2025)	RMM / Remote access tool	Ransomware group(s) explicitly linked	How it was used
August	**N-able N-central**	(No ransomware attribution stated by CISA)	Actively exploited vulnerabilities in MSP-used RMM. This is “RMM abuse” via platform exploitation (initial access / code execution risk).
September	**Splashtop Remote Access**	Qilin	Used as part of a chain to execute a Linux ransomware binary on Windows hosts, leveraging legitimate remote tooling to reduce detection noise.
October	**AnyDesk / ScreenConnect / Splashtop (tooling set)**	Qilin	Qilin affiliates use legitimate remote management / remote access tools including AnyDesk, ScreenConnect and Splashtop as part of their operations in H2 2025.
November	**AnyDesk / LogMeIn**	Akira	USG advisory update stated Akira actors used legitimate remote access tooling to pivot / lateral movement under “normal admin tool” cover.
December	**ScreenConnect / AnyDesk / TeamViewer / Splashtop**	DragonForce (via Scattered Spider enablement)	Scattered Spider enabled DragonForce deployments and explicitly cited RMM tools used for persistence / remote control (named tools listed).

What changed in the second half of 2025

Provider-layer targeting remained economically rational, but under disclosed:

While only 1.9% of disclosures explicitly identify MSP or provider-layer victims, this figure reflects labeling behavior, not true exposure. Ransomware actors and leak sites typically name the directly extorted legal entity — often an end customer, subsidiary or operating company — rather than the upstream service provider whose infrastructure, tooling or access pathways were abused during the intrusion.

In practice, MSPs frequently appear as indirect or intermediary victims: Compromised remote-management platforms, shared administrative credentials, backup systems or monitoring agents are leveraged to gain initial access, propagate laterally or maximize impact across multiple downstream organizations. These scenarios are rarely labeled as “MSP incidents” in public disclosures, even when the service provider represents a critical failure point in the attack chain.

As a result, the apparent underrepresentation of MSPs in public reporting reflects attribution and disclosure bias, not reduced risk. The true exposure of MSPs is better inferred from technical indicators such as the abuse of RMM tools, identity systems, backup infrastructure and multitenant platforms rather than from victim labels alone. Consequently, MSPs remain a high-value and structurally attractive target for ransomware operators, despite their limited visibility in public leak-site statistics.

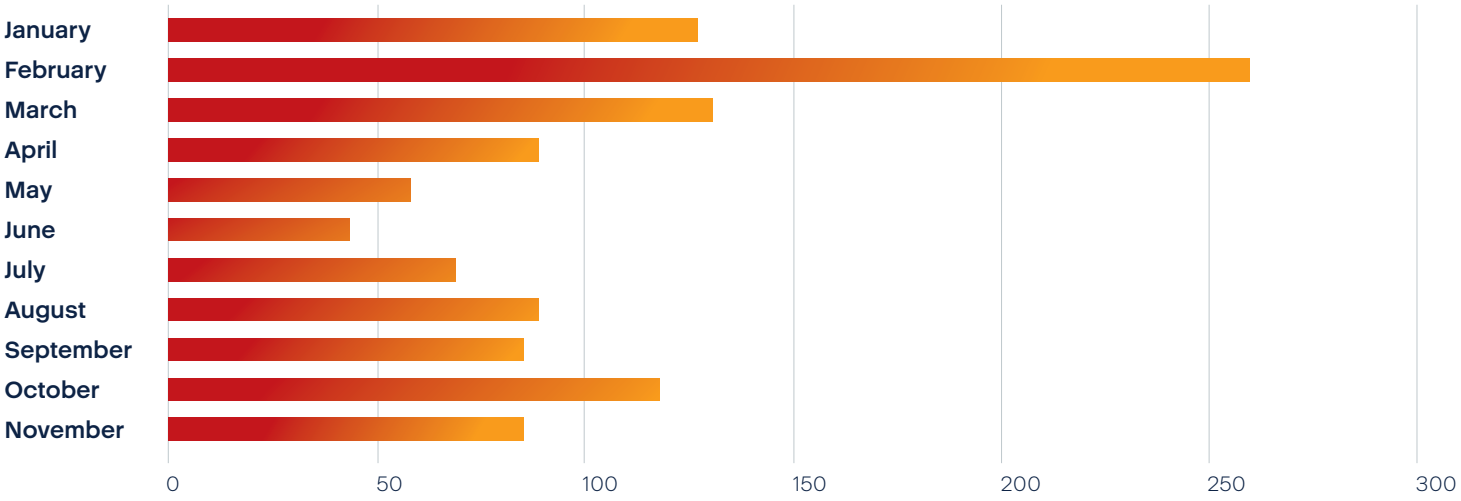
MSPs and SaaS providers remain high-value targets because they concentrate administrative access and customer-adjacent data, enabling attackers to maximize leverage from a single intrusion. Confirmed 2025 MSP cases frequently show a compressed path from initial access to downstream impact, often involving administrative tooling or shared infrastructure. This reduces defender reaction time and increases the probability of multitenant exposure before containment. Even where encryption is limited to provider infrastructure, data theft alone can trigger secondary consequences for customers, including regulatory notifications, contractual penalties and fraud risk. This dynamic increases attacker leverage without requiring full-scale downstream deployment.

MSPs and SaaS providers remain high-value targets because they concentrate administrative access and customer-adjacent data, enabling attackers to maximize leverage from a single intrusion.

3. Living off the land, lateral movement and other sophisticated techniques used to attack Acronis customers

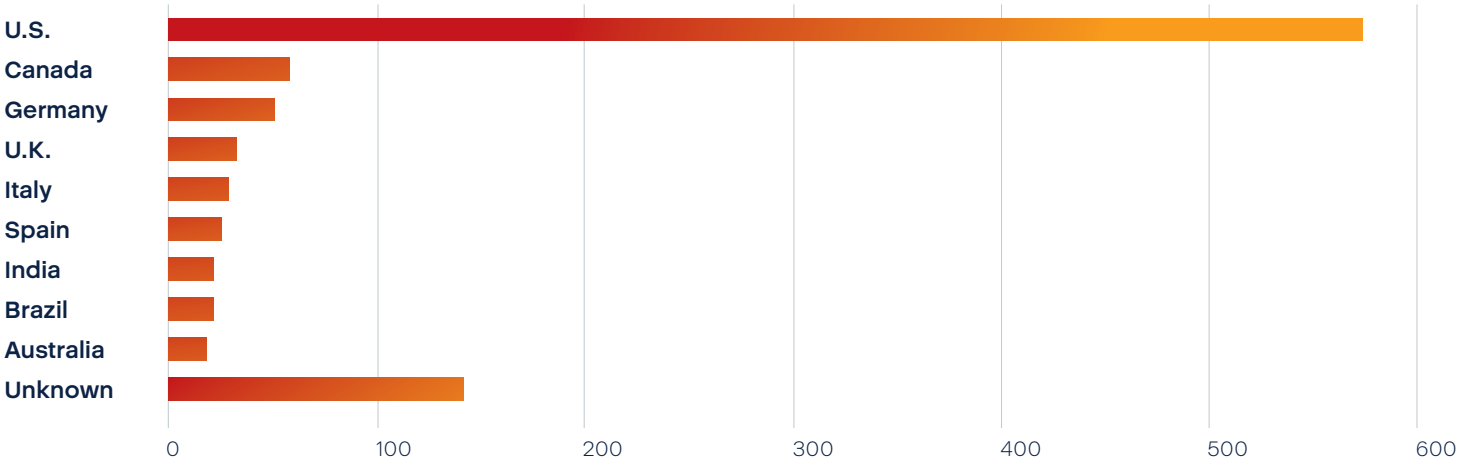
The supply chain and third-party compromise remained a persistent and structurally important attack pattern throughout 2025, affecting at least 1,200 publicly identified victims between January and November. Rather than being evenly distributed, these incidents clustered in specific periods, reflecting the way third-party risk scales when a widely used vendor, platform or service provider is exploited. February stands out as the peak month, with 260 victims — more than double the monthly average. This spike is consistent with real-world supply chain dynamics, where exploitation of a single shared dependency can rapidly propagate across many downstream organizations before detection and mitigation measures are fully deployed. Subsequent months show lower but steady volumes, indicating continued exploitation of residual access, delayed patching and secondary abuse of compromised third-party relationships.

Total victims with explicit supply chain / third-party indicators – January–November 2025



The country distribution further reinforces the systemic nature of supply chain exposure. The U.S. accounts for nearly half of all identified victims, reflecting both the high concentration of enterprises reliant on shared service providers and the strong reporting visibility in that region. A significant “Unknown” category highlights the opacity that often surrounds supply chain incidents, where the ultimate victim may be difficult to attribute or publicly disclose. Canada, Germany, the U.K. and several EU countries follow, underscoring that third-party compromise is not region-specific but instead tracks global technology and service adoption patterns rather than local threat activity alone.

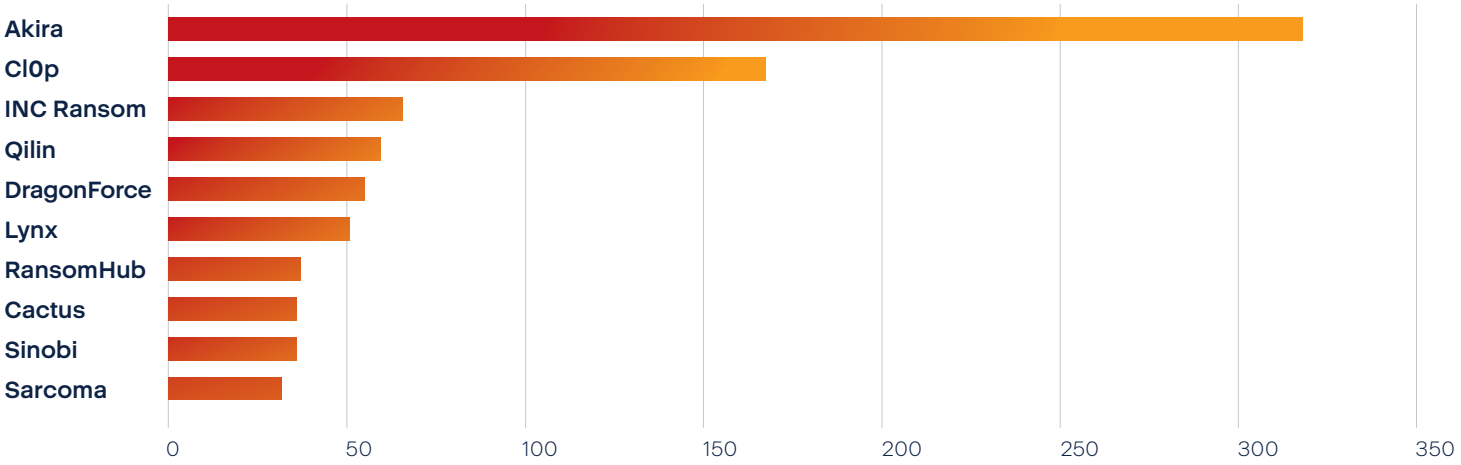
Top 10 countries with explicit supply chain / third-party indicators – January–November 2025



The threat actor breakdown shows a clear concentration among a small number of ransomware groups that have consistently demonstrated the capability and intent to exploit third-party access at scale. Akira and Cl0p dominate the dataset, together accounting for a substantial share of all supply chain-signalling victims. Both groups have a documented history of targeting MSPs, file-transfer platforms, and shared infrastructure to maximize impact. The presence of multiple other ransomware groups with moderate but sustained victim counts indicates that supply chain exploitation has become a broadly adopted tactic rather than a

niche capability. Overall, the data illustrates that third-party compromise is no longer an outlier scenario but a repeatable, scalable attack model that ransomware operators continue to refine, posing ongoing risk to interconnected organizations and service ecosystems.

Top 10 active groups in the supply chain-signalling subset – January–November 2025



Within the supply chain-signalling subset, victim volume alone does not adequately reflect actor capability. Instead, meaningful differentiation emerges when examining tradecraft, targeting strategy and operational intent.

Cl0p represents the most structurally sophisticated actor in this cohort. Its activity is characterized by highly selective operations that deliberately exploit shared services, trusted platforms and centralized third-party infrastructure to achieve disproportionate downstream impact. Rather than pursuing broad victim coverage, Cl0p consistently prioritizes precision, leverage and amplification, indicating mature reconnaissance, tooling alignment with specific technologies, and a strategic understanding of supply chain dependencies.

By comparison, Qilin demonstrates a more aggressive and high-tempo operational model, with frequent campaigns and rapid execution cycles. Its activity reflects strong operational discipline and a willingness to deploy advanced techniques when advantageous, but overall it favors reliable, repeatable intrusion paths over bespoke supply chain exploitation. Qilin's presence in the supply chain-signalling subset is therefore better understood as opportunistic intersection with shared environments rather than a primary strategic focus.

Akira, the most active group by victim count in this subset, combines scale with technical adaptability. Its operations show consistent expansion across platforms and environments, allowing it to operate effectively in provider-adjacent and third-party contexts without relying on a single access vector. Akira's supply chain relevance appears driven by operational breadth and targeting flexibility, rather than deliberate ecosystem-level exploitation.

Other groups in the top ten — INC Ransom, DragonForce, Lynx, RansomHub, Cactus, Sinobi and Sarcoma — exhibit varying degrees of operational maturity but generally lack persistent indicators of purpose-built supply chain attack strategies. Their appearance in this subset is more consistent with access reuse, shared infrastructure exposure or affiliate-driven overlap, rather than sustained investment in third-party compromise as a core operating model.

Overall, this distribution reinforces a key distinction: Supply chain relevance does not imply uniform sophistication. A small number of actors treat third-party compromise as a strategic multiplier, while most encounter supply chain exposure incidentally as part of broader ransomware activity. Understanding this distinction is critical for accurately assessing risk and prioritizing defensive controls at the provider and ecosystem level.

Compromised software and service providers quickly lead to downstream customer exposure.

High-impact MSP and supply chain cases

Let's look at some specific cases from 2025 illustrating how MSP and supply chain compromise propagates.

MSP supply chain ransomware via SimpleHelp RMM

A DragonForce ransomware gang breached an MSP and then used the MSP's SimpleHelp RMM to move from the provider into downstream customer environments, deploying encryptors and stealing data. This is a canonical example of "one-to-many" propagation: Compromise of the management plane becomes compromise of managed endpoints. Reporting links the intrusion to exploitation of known SimpleHelp vulnerabilities (commonly cited as a chain of CVEs in SimpleHelp), demonstrating how RMM exposure can become a direct ransomware distribution channel at tenant scale. Even when customers have strong perimeter controls, a trusted MSP tool can bypass them if the MSP plane is compromised.

Enterprise software exploitation leading to broad third-party exposure

A high-volume Cl0p extortion campaign in 2025 was tied to exploitation of Oracle E-Business Suite, including discussion of CVE-2025-61882 (unauthenticated remote code execution) and resulting customer extortion attempts. This illustrates a classic supply chain dynamic: Exploitation of a widely deployed enterprise platform yields broad victim exposure, often through shared operational dependencies and delayed patching. Patch latency and internet-exposed enterprise applications can convert a single vendor defect into multisector, multiregion victimization at scale.

Dealership software provider incident with downstream impact

A ransomware incident affecting a dealership software provider within the Motility / Reynolds and Reynolds ecosystem[6] resulted in regulatory disclosures indicating the theft of sensitive personal data belonging to hundreds of thousands of individuals. The incident was publicly claimed by the PEAR ransomware group, which asserted responsibility and alleged large-scale data exfiltration. While such claims originate from the threat actor, the scope of the notification confirms a material impact consistent with a significant data-compromise event. This case demonstrates how compromises of software vendors and service providers can quickly become downstream customer exposure events, even if the direct victim is a third-party provider. Third-party providers often aggregate high-value data (PII, financial records, identity data) across many customers, increasing both attacker leverage and regulatory exposure.

"Integrated partner" compromise impacting a verification provider

A major 2025 breach at an identity verification / credit-check provider was attributed to compromise of an integrated partner and abuse of an API validation process, resulting in large-scale exposure. While not a traditional ransomware leak-site case, it is a direct supply chain failure mode: partner compromise + integration weakness → customer data exposure. Supply chain security is not only patching; it includes partner assurance, API abuse resistance and monitoring for high-velocity or anomalous access.

[6] Bischoff, Paul. "Auto dealership software company notifies 767,000 people of data breach claimed by ransomware gang." Comparitech. October 1, 2025. https://www.comparitech.com/news/auto-dealership-software-company-notifies-767000-people-of-data-breach-claimed-by-ransomware-gang/

Legitimate tool abuse

We also looked into telemetry collected from Acronis Cyber Protect Cloud to identify the top 15 countries by month experiencing the highest volume of attacks abusing legitimate applications. The analysis focuses on techniques commonly referred to as living off the land (LotL), where attackers leverage trusted system tools and widely deployed applications to evade detection and blend malicious activity into normal system behavior.

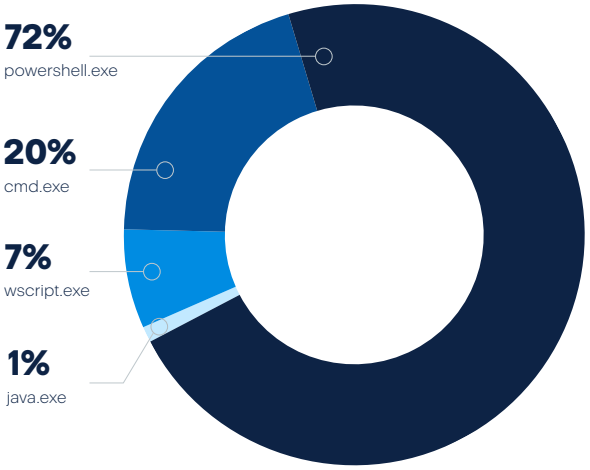
Germany and the U.S. emerged as the two most affected countries across the entire observation period. Germany recorded the highest cumulative volume of detections, maintaining a leading position in most months, while the U.S. closely followed with similarly sustained activity. The persistence of these two countries at the top of the monthly rankings indicates long-term, continuous abuse rather than short-lived campaigns, reflecting their large enterprise footprint and extensive use of standard administrative tooling.

Brazil and Mexico formed the next tier of high-activity countries. Brazil showed strong and repeated representation in the monthly top 15, frequently associated with abuse of cmd.exe and powershell.exe, suggesting widespread post-compromise activity rather than isolated intrusion attempts. Mexico displayed a similar pattern, with consistent month-over-month presence, reinforcing the assessment that legitimate tool abuse is entrenched in attacker workflows targeting Latin American environments.

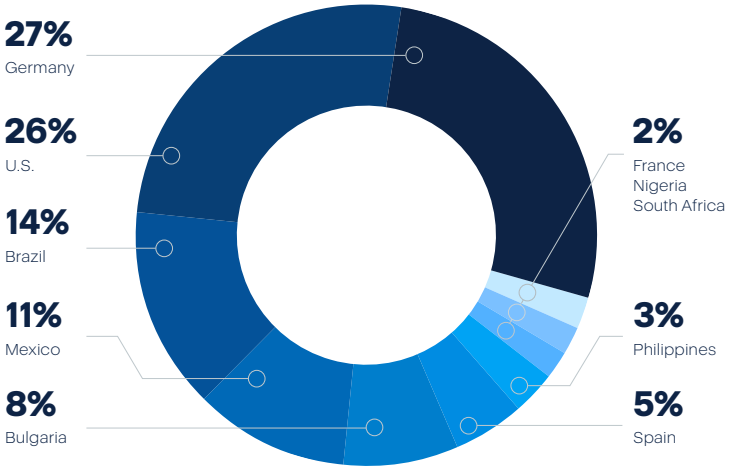
In Europe, beyond Germany, Bulgaria, Spain and France stand out. Bulgaria was notable for its disproportionately high detection volume relative to market size, appearing persistently across multiple months. Spain showed elevated activity during several consecutive months, often ranking within the upper half of the top 15, while France maintained steady but slightly lower volumes, indicating sustained but less aggressive campaign intensity.

In the Asia-Pacific and African regions, the Philippines, South Africa and Nigeria repeatedly appeared in the monthly distributions. The Philippines showed pronounced spikes in several months, particularly linked to PowerShell abuse, pointing to campaign-driven surges rather than background noise. South Africa maintained a stable presence throughout the year, while Nigeria appeared more episodic, with higher concentrations in specific months rather than continuous dominance.

MSP / IT-service providers



Top 10 countries by abused legitimate tools – 2025



Germany and the U.S. emerged as the most affected. Germany recorded the highest cumulative detections, maintaining its leading position for most months.

Most abused legitimate applications

Across all months and countries, the telemetry clearly indicated that attackers overwhelmingly relied on a small, consistent set of built-in Windows utilities:

- **PowerShell (powershell.exe)** was the single most abused legitimate application across every observed month. Its dominance was consistent in Germany, the U.S. Brazil, the Philippines and Spain, reflecting its flexibility for payload delivery, in-memory execution and post-exploitation control.
- **Windows Command Prompt (cmd.exe)** ranked second, frequently used in conjunction with PowerShell for execution chaining, environment reconnaissance and lateral movement.
- **Windows Script Host (wscript.exe / cscript.exe)** appeared regularly, particularly in detections from Germany, France and the Philippines, indicating continued reliance on script-based loaders.
- **rundll32.exe and regsvr32.exe** were less dominant but consistently present, primarily associated with stealthy execution and defense evasion techniques.

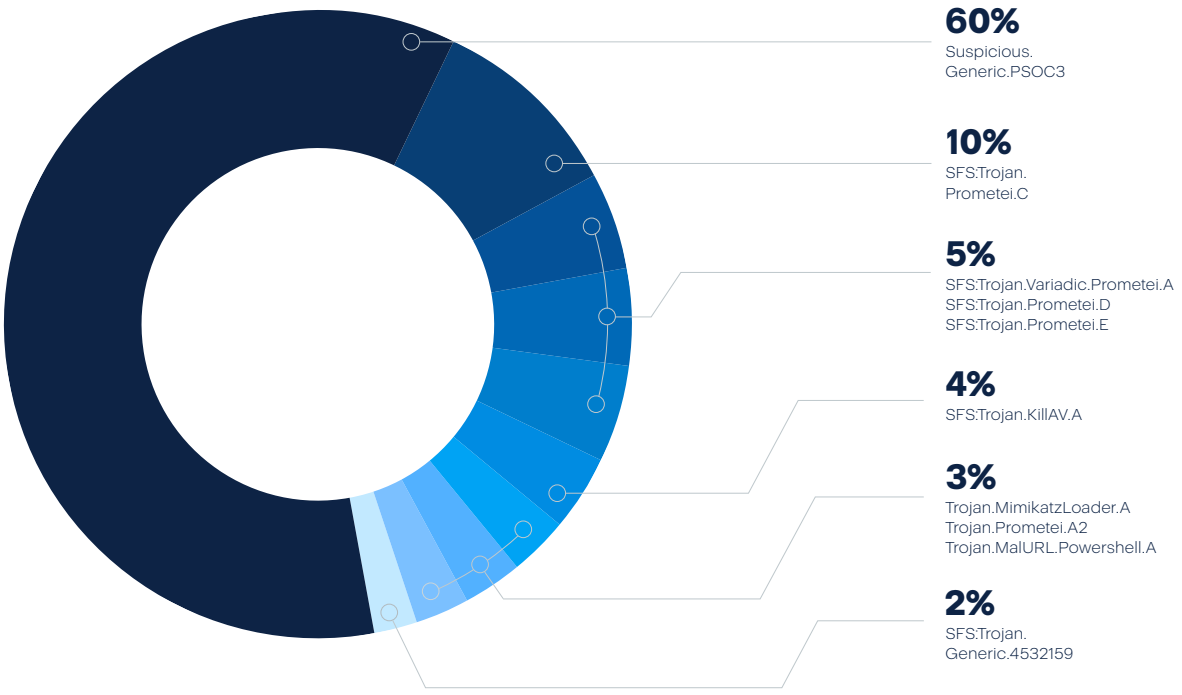
Notably, the relative share of these tools remained stable throughout the year, with no meaningful shift toward new or exotic binaries. This confirmed that attackers prioritized reliability and ubiquity over innovation when abusing legitimate applications.

The 2025 telemetry confirmed that abuse of legitimate applications is a persistent, industrialized attack technique rather than a campaign-specific anomaly. Germany, the U.S. Brazil, Mexico, Spain, France, Bulgaria, the Philippines, South Africa and Nigeria consistently dominated monthly detections, with minimal geographic drift. At the same time, PowerShell and Command Prompt remained the primary execution mechanisms, reinforcing the need for behavioral monitoring and contextual process analysis rather than trust-based controls.

Mass infection and lateral movement patterns by country

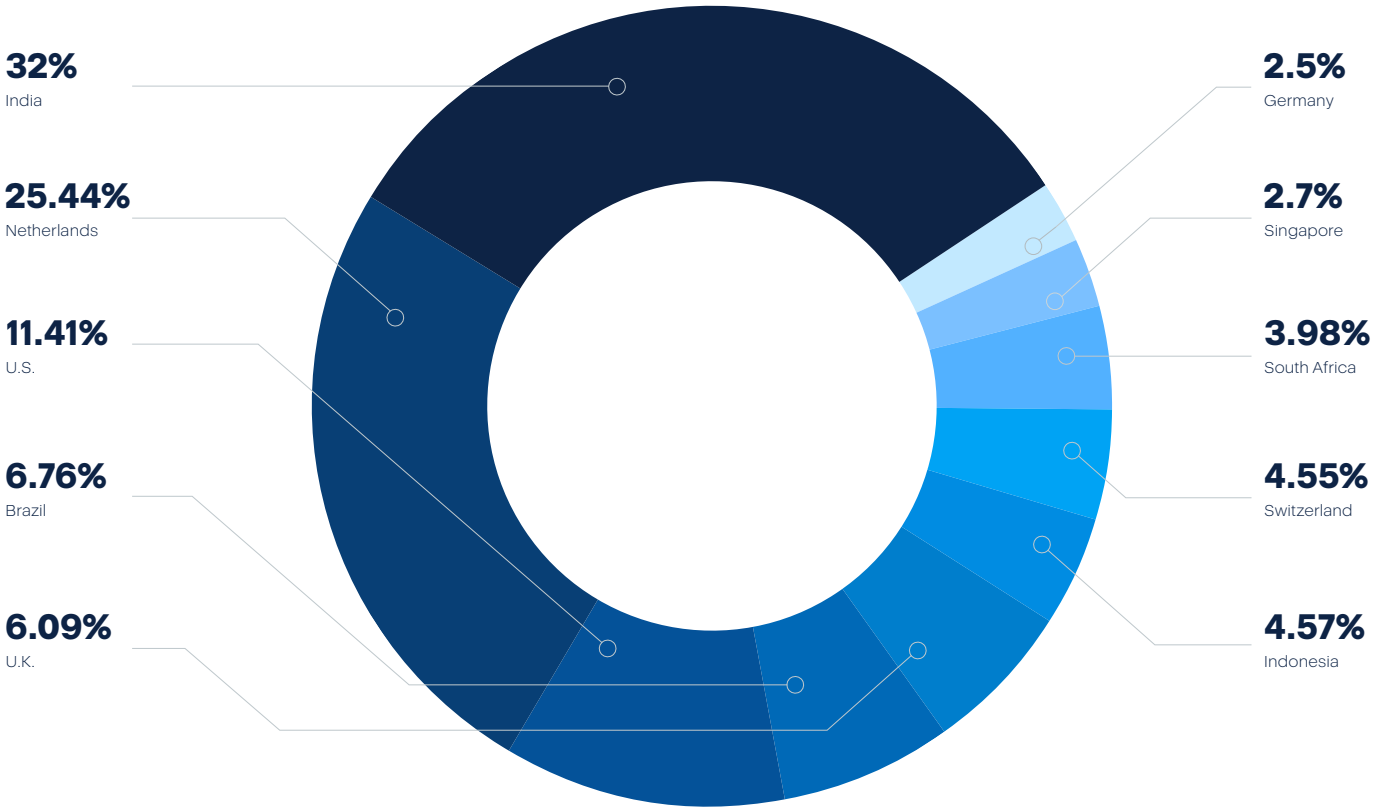
This section analyzes telemetry from Acronis Cyber Protect Cloud to identify countries where individual organizations experienced large-scale, multiendpoint compromise events, a strong indicator of internal propagation or lateral-movement-enabled attacks. The metric reflects the number of distinct machines affected within the same tenant by the same threat in a given month.

Top 10 lateral movement detections – global, 2025



Countries most affected by mass infection

India stands out as the most impacted country in 2025 by a significant margin. Across multiple months, Indian organizations experienced repeated large-scale infection events. The majority of these incidents were associated with the Prometei malware family (SFS:Trojan.Prometei.*), which is well known for worm-like propagation, credential harvesting and SMB-based lateral movement. High-impact months showed individual Prometei incidents affecting 70–80 endpoints within a single organization, strongly indicating uncontrolled internal spread.



The Netherlands ranked second overall. Activity here was dominated by generic suspicious and post-exploitation detections (for example, Suspicious.Generic.PSOC3), often appearing in pairs of large incidents within the same month. January and February showed particularly strong concentration, with single cases exceeding 130 affected endpoints, suggesting lateral movement following successful initial compromise rather than broad malware delivery.

Unlike India, U.S. cases showed greater threat diversity, including both Prometei variants and generic post-exploitation detections. Individual events are typically smaller than those seen in India or the Netherlands, but the repeated appearance of multiendpoint cases indicates persistent exposure to internal spread scenarios rather than isolated infections.

In Brazil and the U.K. incidents recurred across several months. These cases frequently involved Trojan and loader-style malware, suggesting that lateral movement occured after an initial foothold was established through commodity malware or credential reuse. The size of individual events was moderate but consistent, pointing to systemic gaps in segmentation or privilege management.

Malware families driving lateral spread

Across all countries and months, the dataset was heavily dominated by Prometei malware variants,[7] which accounted for the largest and most consistent mass infection events. Prometei's ability to move laterally using weak credentials and exposed services explains the unusually high number of endpoints affected per organization, particularly in India.

Alongside Prometei, generic suspicious detections and post-exploitation tooling played a major role, especially in European countries. These detections typically reflect hands-on-keyboard activity, where attackers leverage built-in tools and scripts to pivot internally rather than deploying additional malware samples.

Conclusions

Mass infection events were not evenly distributed throughout the year. Early-year months — particularly January through March — showed the highest concentration of large-scale incidents, especially in India and the Netherlands. Midyear activity became more geographically dispersed, while late-year months showed fewer extreme spikes but continued presence of multiendpoint cases, indicating that lateral movement remains a persistent risk rather than a seasonal phenomenon.

The 2025 data confirms that lateral movement and internal propagation remain a critical risk, with a small number of countries accounting for the majority of large-scale infection events. India and the Netherlands were the most affected, driven primarily by Prometei-based propagation and post-exploitation activity, while the U.S., Brazil and the U.K. exhibited sustained but more diverse lateral movement patterns.

Most importantly, these incidents were organizationally concentrated: A single successful intrusion frequently results in dozens of endpoints compromised within the same tenant. This reinforces the conclusion that preventing lateral movement — through credential hygiene, network segmentation and behavioral detection — is just as important as blocking initial infection vectors.

[7] Malpedia. Prometei. N.d., ca. 2026. https://malpedia.caad.fkie.fraunhofer.de/details/win.prometei

4. Email threats

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

Email and collaboration platform threats: Comparative analysis and trends

Throughout 2025, messaging-based attack vectors continued to dominate the initial access landscape for enterprises and MSP-managed environments. However, the year was characterized by a divergence in attacker behavior between email and collaboration platforms, rather than a simple migration from one channel to another. While email remained the primary and most scalable delivery mechanism, collaboration platforms experienced disproportionate growth in sophistication, particularly in advanced and impersonation-based attacks.

This section compares H1 and H2 2025 trends, contrasts email versus collaboration channels and assesses the implications for MSPs.

H1 2025 vs. H2 2025: Intensification rather than expansion

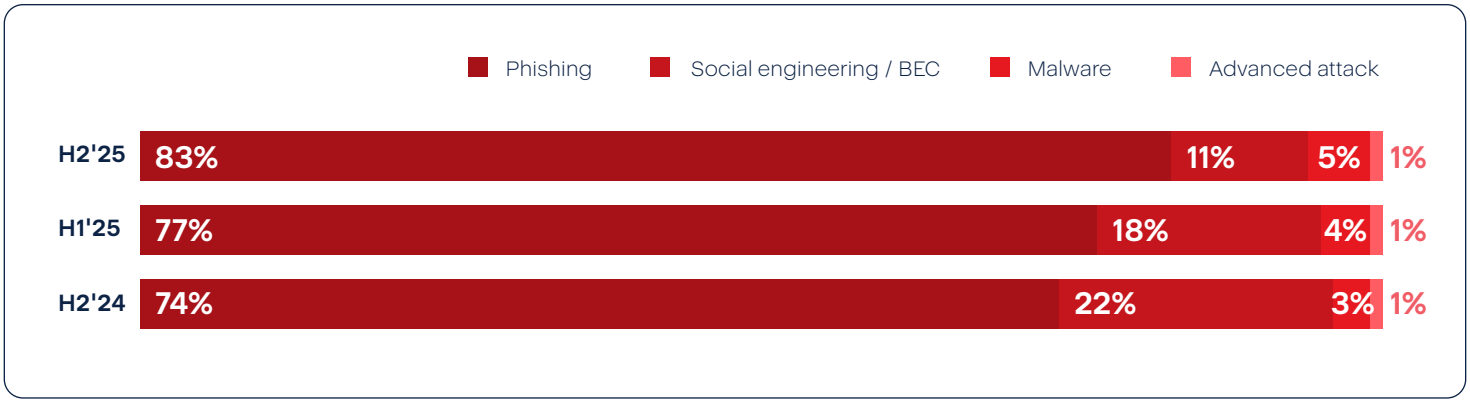
Between the first and second halves of 2025, messaging threats intensified at a rate exceeding environmental growth. While the number of protected organizations and users grew significantly during the year, attacks per organization increased by 16% and attacks per user increased by 20% in H2 compared to H1, indicating denser targeting rather than broader distribution.

Before we dive into figures, phishing represents deceptive messaging designed to manipulate recipients into revealing credentials, approving actions or interacting with fraudulent links or documents, typically relying on impersonation and contextual trust rather than technical exploits. Social engineering and business email compromise (BEC) encompass targeted impersonation attacks that abuse business context, such as executive, supplier or internal role spoofing, to induce fraudulent payments, data disclosure or unauthorized approvals, often without delivering malware.

Malware-based attacks refer to messages that attempt to deliver malicious payloads via attachments or links, enabling endpoint compromise, persistence or follow-on intrusion, and are characterized by executable or script-based content. Advanced attacks denote lower-volume, higher-sophistication campaigns that combine tailored targeting, evasion techniques or multistage workflows, often blending social manipulation with technical abuse to bypass standard detection mechanisms.

Email attacks in H2 2025 increased by 36% compared to H1, confirming that email remains the most effective large-scale delivery channel despite continued improvements in filtering and detection. Importantly, this growth occurred alongside a decline in technically malicious content, reinforcing the conclusion that attackers are optimizing for deception rather than exploit delivery.

Threat composition shifted notably between H1 and H2. Phishing increased from 77% in H1 to 83% in H2, while malware-based email attacks increased from 4% to 5%. Social engineering and business email compromise stabilized at 11%, reflecting a sustained emphasis on impersonation and contextual fraud rather than payload-based compromise.



This evolution indicates that attacker success is increasingly determined by process exploitation and identity abuse rather than technical evasion.

Email Attacks: H2 2025 vs H1 2025

+36%
attacks total

+16%
attacks per organization per month

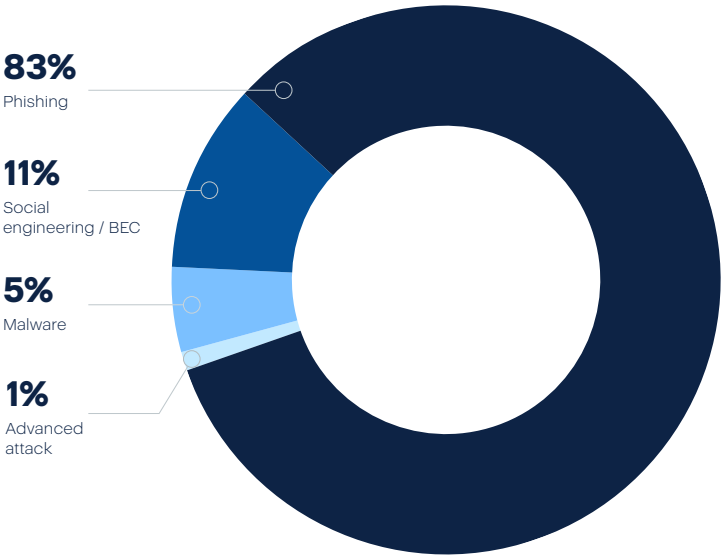
+20%
attacks per user per month

Email versus collaboration platforms: Volume versus sophistication

Despite increased attention on collaboration platforms (Microsoft Teams, Microsoft SharePoint / OneDrive, Slack, Google Workspace and Zoom), email remains the dominant threat vector by volume and reach. Email provides universal external access, predictable business workflows, and minimal friction for first contact, making it the preferred channel for phishing and credential harvesting campaigns.

In H2 2025, phishing accounted for 83% of all email threats, while advanced attacks represented only 1%. This distribution highlights email's continued role as a mass delivery mechanism, optimized for scale rather than complexity.

Types of threats



Collaboration platforms, by contrast, exhibited a fundamentally different threat profile. In H2 2025, advanced attacks accounted for 31% of collaboration platform threats, more than thirty times the proportion observed in email. Malware accounted for 54%, while phishing represented only 15%.

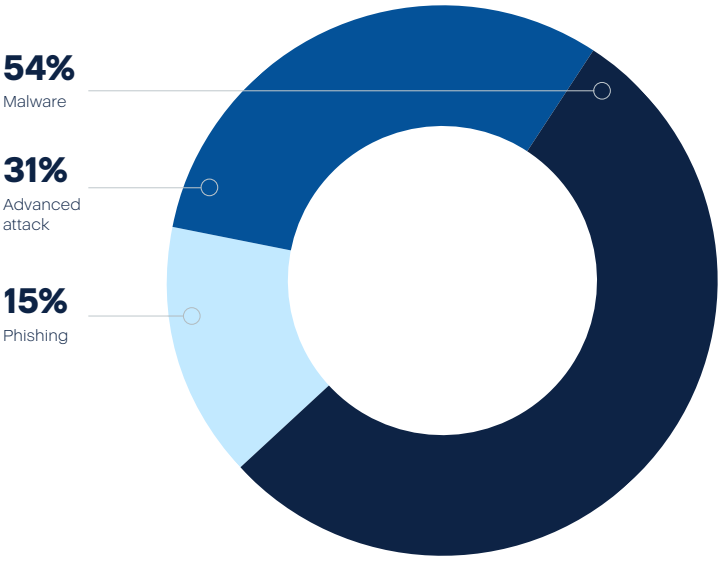
In collaboration platforms, advanced threats typically manifest through abuse of trusted in-platform features rather than overt malicious content. Malware delivery often occurs via shared files or links posted in chat channels or direct messages, frequently disguised as internal documents or meeting artifacts and executed once users open or sync them locally.

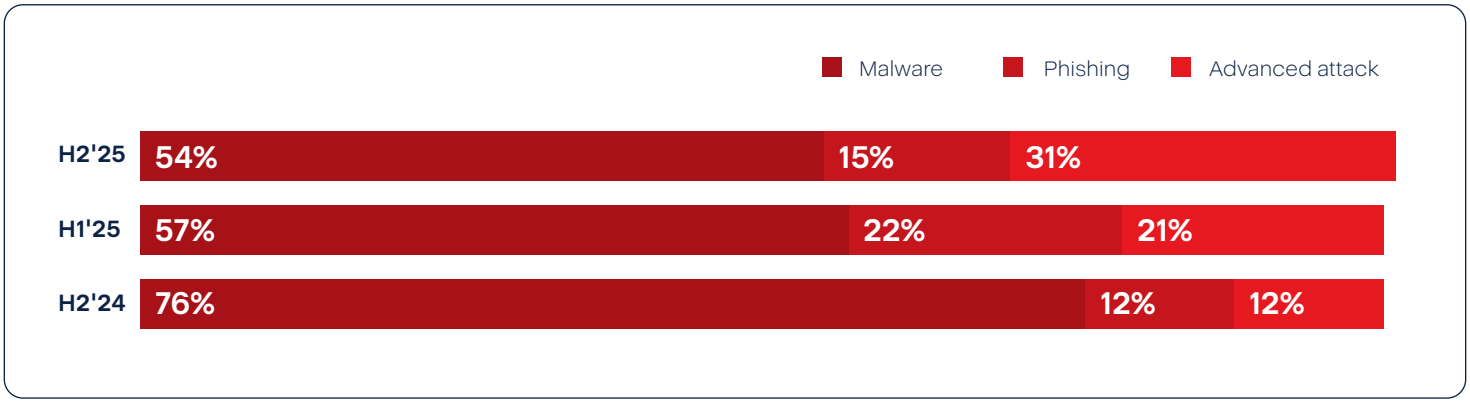
Advanced attacks include token theft, session hijacking and abuse of OAuth or third-party app integrations, allowing attackers to persist without repeated credential use and to move laterally across users and channels. Phishing, while less dominant than in email, still appears in the form of impersonated internal users or spoofed system notifications, leveraging the implicit trust users place in collaboration tools to prompt credential submission or malicious interaction.

This disparity reflects the structural constraints of collaboration platforms. Unlike email, collaboration tools typically require tenant access, accepted invitations or compromised internal identities. As a result, attackers deploy fewer but more targeted and higher-impact techniques, often following initial access achieved through email or credential compromise.

Rather than replacing email, collaboration platforms function as a secondary exploitation layer, used for impersonation, lateral movement and escalation within trusted environments.

Types of threats





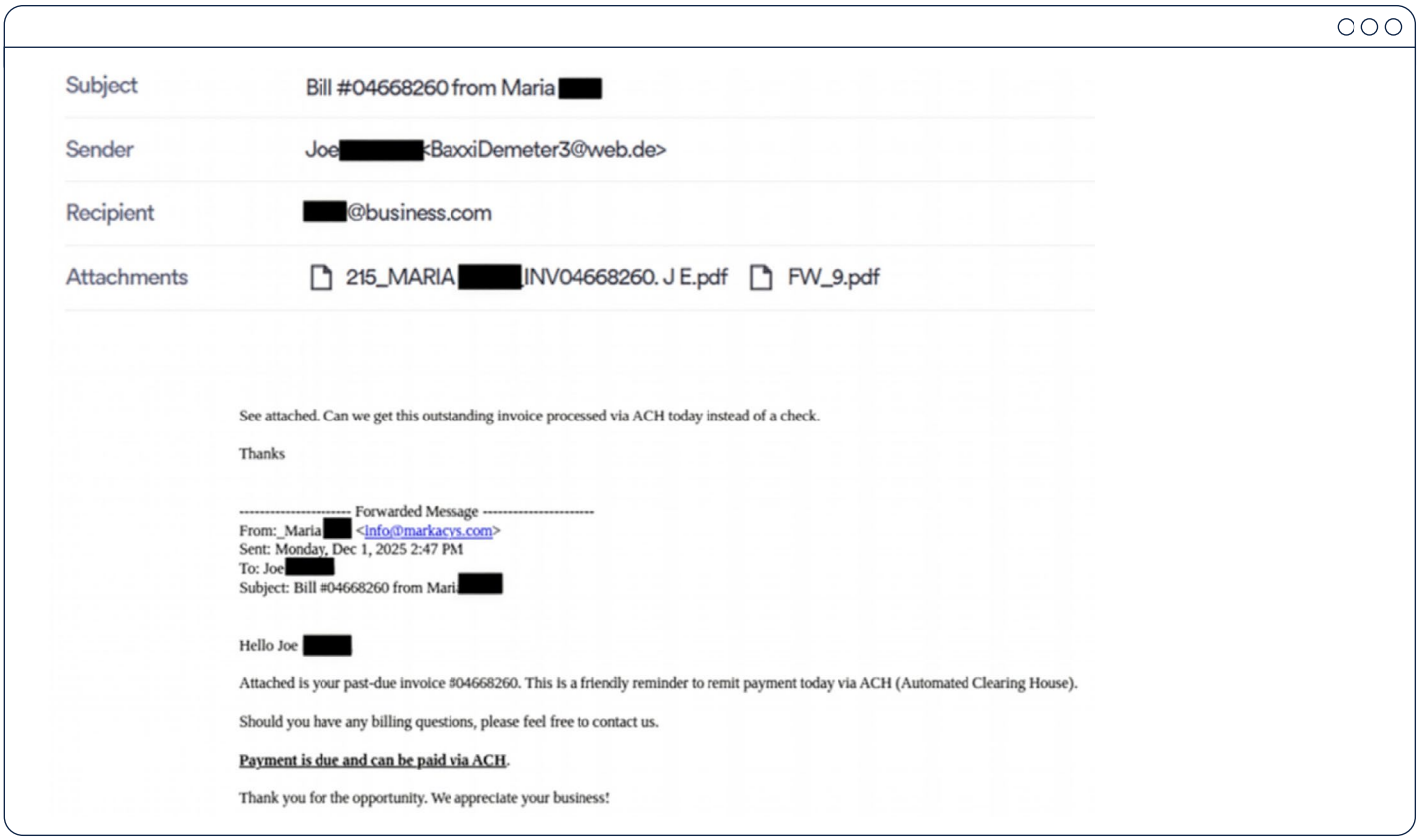
Cross-channel attacker strategy

Taken together, the data indicates a two-stage attacker model in 2025:

- First, attackers use email for initial access, credential harvesting and broad reconnaissance, leveraging its scale and low entry barriers.
- Second, once trust or access is established, collaboration platforms are used for precision attacks, including internal impersonation, fake approval requests and advanced social engineering.

This layered approach explains why email remains dominant in volume, while collaboration platforms show a disproportionate rise in advanced attack techniques.

Let's look into a specific example caught by our mail security:



The attacker created a fake email thread between a customer and a company executive, then sent it as if it came from the executive. The email included two files, both were clean and nonmalicious. Our detection engine, powered by regex patterns, identified the fake thread. And our executive-impersonation engine detected the misuse of C-level identities.

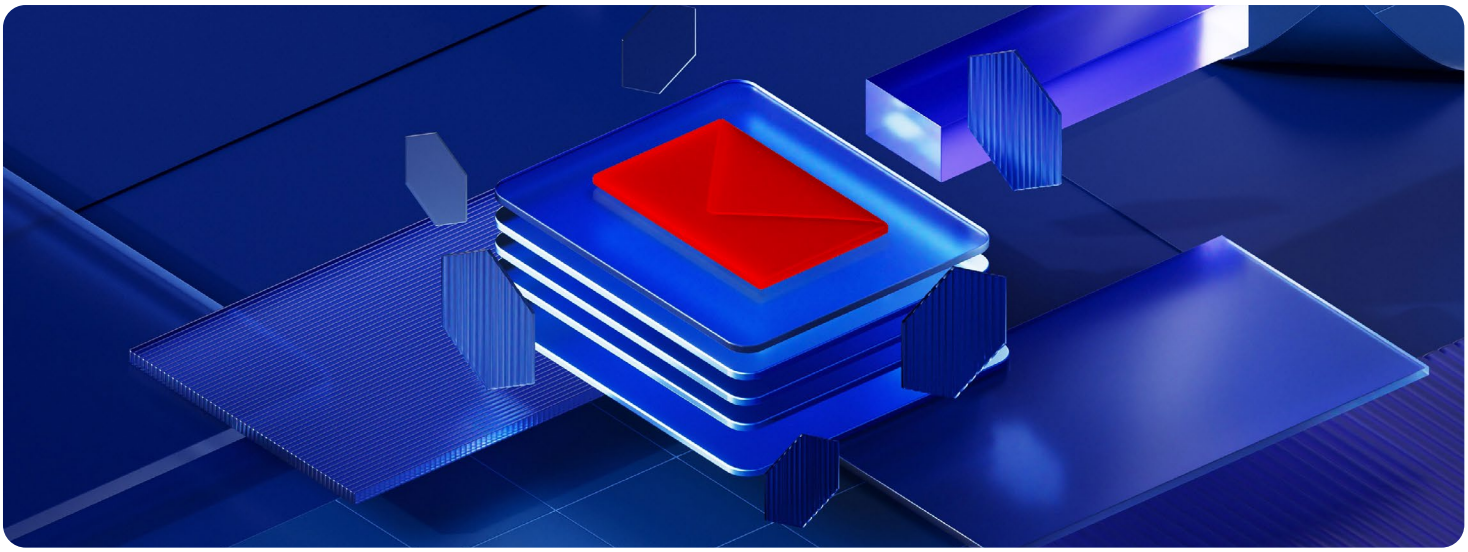
Notable phishing, email and collaboration platform malicious campaigns

Microsoft 365 "Direct Send" spoofing for internal-looking phishing

During 2025, security researchers documented[8] sustained abuse of Microsoft 365's "Direct Send" capability to deliver phishing emails that appeared to originate from within the victim organization. By leveraging this mechanism, attackers were able to spoof internal senders without compromising a legitimate mailbox, creating messages that closely resembled routine internal workflows or system notifications.

The primary objective of these campaigns was credential harvesting, with phishing pages designed to capture Microsoft 365 usernames, passwords and, in some cases, authentication tokens. Because the emails appeared to be sent from trusted internal sources, users were more likely to interact with them, significantly increasing click-through rates. Successful credential compromise enabled attackers to escalate activity through mailbox rule abuse, lateral phishing within the tenant and downstream business email compromise-style fraud. This technique effectively bypassed assumptions that internal-looking emails imply account takeover, making detection more challenging.

[8] Barnea, Tom. "Ongoing Campaign Abuses Microsoft 365's Direct Send to Deliver Phishing Emails." Varonis. October 8, 2025. https://www.varonis.com/blog/direct-send-exploit



Abuse of trusted link wrapping to bypass email security controls

Another prominent campaign pattern observed[9] in multiple waves throughout 2025 involved the abuse of trusted link-wrapping services commonly used by email security providers. In these campaigns, attackers embedded malicious URLs behind legitimate, security-branded rewriting domains, reducing user suspicion and weakening the effectiveness of static URL reputation checks.

Email lures typically referenced familiar business scenarios, such as document signatures, shared files from collaboration platforms, or voicemail notifications. Once clicked, the wrapped links redirected victims to fake Microsoft 365 login portals designed to steal credentials, and in some cases to multistage redirect chains leading to malware staging infrastructure. The operational benefit for attackers was twofold: Improved email deliverability and higher user engagement due to the perceived legitimacy of "sanitized" links. For victim organizations, this increased the likelihood of tenant-wide identity compromise and enabled secondary internal campaigns launched from trusted accounts.

Microsoft Teams social engineering for interactive account compromise

Throughout 2025, threat actors demonstrated a growing and explicit focus on Microsoft Teams[10] as an initial access vector. Instead of relying solely on email, attackers initiated contact through Teams chat messages — often using external chat functionality — and impersonated IT support or helpdesk staff. Interactions frequently escalated to voice calls or screen-sharing sessions to increase credibility and apply real-time social pressure.

These campaigns relied on operator-in-the-loop execution rather than a single static payload. Victims were persuaded to disclose credentials, approve authentication requests, enable remote access tools or execute follow-on scripts. This approach significantly compressed the time from initial contact to validated access and lateral movement. The abuse of Teams is particularly impactful for MSPs and enterprise environments, as it exploits a trusted internal communication channel and can bypass controls that are primarily designed to detect email-based phishing activity.

[9] Cloudforce One. "Attackers abusing Proofpoint & Intermedia link wrapping to deliver phishing payloads." Cloudflare. July 30, 2025. https://www.cloudflare.com/threat-intelligence/research/report/attackers-abusing-proofpoint-intermedia-link-wrapping-to-deliver-phishing-payloads/

[10] Deliu, Isuf. "Sliding into your DMs: Abusing Microsoft Teams for Malware Delivery." Permiso. August 28, 2025. https://permiso.io/blog/sliding-into-your-dms-abusing-microsoft-teams-for-malware-delivery

[11] Acronis Threat Research Unit. "Fake adult websites pop realistic Windows Update screen to deliver stealers via ClickFix." Acronis. November 25, 2025. https://www.acronis.com/en/tru/posts/fake-adult-websites-pop-realistic-windows-update-screen-to-deliver-stealers-via-clickfix/

"ClickFix" social engineering technique and user-led execution chains

In 2025, analysts identified a recurring social engineering pattern commonly referred to as the "ClickFix" technique.[11] This approach typically began with a phishing email, malicious advertisement or compromised website and transitioned into guided instructions that convinced the victim to perform a series of "fix" steps to resolve a supposed benign issue.

The defining characteristic of this technique was that the user was induced to execute commands or scripts themselves, often under the guise of troubleshooting or system maintenance. While the secondary malware or tooling varied by threat actor, the core risk stemmed from user-initiated execution rather than exploitation of a software vulnerability. This materially undermined security controls focused on blocking known malicious binaries and shifted the challenge toward preventing human-driven execution in enterprise environments.

The broader problem is that ClickFix attacks operate at the intersection of usability and security: They evade traditional detection by avoiding exploits or attachments, rely on legitimate system tools and user actions, and therefore require layered defenses that combine strong user-interface protections, behavioral detection and security awareness rather than signature-based blocking alone.

Discord invite link abuse for multistage malware delivery

Mid-2025 reporting highlighted[12] the growing use of Discord invite links as a collaboration-adjacent infection vector. Attackers abused malicious, hijacked or recycled invite links to funnel victims through controlled redirection chains that ultimately delivered malware.

Observed campaigns used this technique to deploy multistage payloads, including remote access trojans and credential stealers. While Discord is not a primary enterprise collaboration platform, its widespread adoption and relatively limited monitoring in many organizations made it an effective delivery channel. The resulting impact included credential theft, session or token compromise and the enablement of secondary access paths into victim environments.

Conclusions

Several conclusions emerge from the combined H1 and H2 2025 data: Email is not being displaced. It remains the primary and most scalable attack vector, with increased attack density and a growing reliance on phishing and impersonation. Collaboration platforms are not replacing email but are becoming high-impact secondary channels, characterized by a much higher proportion of advanced attacks. Attackers are shifting from technical exploitation toward human and process exploitation, targeting trust relationships rather than systems. For MSPs, the most material risk is not a single message or platform, but the chaining of email-based access with collaboration-based escalation.

To address these trends, MSPs and enterprises should prioritize the following measures:

- Strengthen identity and workflow controls around email-driven processes, particularly password resets, invoice changes and access requests, recognizing that phishing content may be technically clean but operationally malicious.
- Extend monitoring and protection to collaboration platforms with the same rigor applied to email, focusing on impersonation detection, anomalous behavior and privilege abuse rather than malware alone.
- Redesign service desk and administrative workflows to assume credible impersonation, requiring step-up verification for high-risk actions regardless of the communication channel.
- Finally, treat email and collaboration security as a single, integrated threat surface, rather than isolated technologies, reflecting the attacker's end-to-end operational model.

[12] Check Point Research. "Hijacked Trust: How Malicious Actors Exploited Discord's Invite System to Launch Global Multi-Stage Attacks." June 12, 2025. https://blog.checkpoint.com/research/hijacked-trust-how-malicious-actors-exploited-discords-invite-system-to-launch-global-multi-stage-attacks/

5. Vulnerabilities landscape

Between 2023 and 2025, the global volume of disclosed vulnerabilities continued to grow, with 2024 representing the peak year in the dataset. While managed service provider (MSP)-specific platforms account for a very small share of total CVEs, vulnerabilities affecting MSP tooling and MSP-managed control planes consistently demonstrate higher severity, privileged access and multitenant blast radius. The data confirms that risk to MSPs is driven by exposure and control-plane access rather than raw vulnerability volume.

Overall vulnerability volume and severity trends

Year	Total CVEs	Year-over-year change
2023	30,616	–
2024	38,858	+8,242 (+26.9%)
2025	41,260	+2,402 (+6.2% vs 2024)

The updated CVE data for the last three years shows a sharp expansion in publicly disclosed vulnerabilities in 2024, followed in 2025 by continued growth at a moderated pace, rather than a reversal of the trend.

In 2024, the total number of CVEs rose to 38,858, representing a year-over-year increase of 8,242 vulnerabilities, or approximately 26.9%. This surge reflects sustained growth in vulnerability discovery and disclosure across software ecosystems, driven by an expanding attack surface, increased security research activity, and more mature disclosure and reporting processes, rather than a sudden deterioration in overall software quality alone.

In 2025, the total number of disclosed CVEs reached 41,260, exceeding the 2024 figure by 2,402 vulnerabilities, or approximately 6.2% year over year. While this confirms a new all-time high in absolute volume, the significantly lower growth rate compared to 2024 indicates a normalization of disclosure velocity, suggesting that vulnerability reporting has entered a phase of high but more stable output rather than rapid acceleration.

Severity distribution (CVSS based)

The 2025 year-to-date severity distribution shows a clear concentration of risk in the upper CVSS bands, based on the severity thresholds defined for this analysis. While these bands are intentionally broad and reflect practitioner-driven categorization rather than formal standards, they provide a useful lens for understanding operational exposure.

More than half of all scored CVEs in 2025 fall into the High severity range (CVSS 6.0–9.0), accounting for just over 56% of disclosures. This highlights that the dominant challenge for defenders is not a small number of extreme outliers, but a large volume of vulnerabilities that are serious enough to require timely remediation yet numerous enough to strain patching and prioritization workflows.

Severity	CVEs	Scored CVEs
Critical (>9.0)	2,921	8.55%
High (6.0–9.0)	19,137	56.02%
Medium / Low (<6.0)	12,106	35.43%

The Critical band (CVSS > 9.0) represents approximately 8.6% of scored vulnerabilities. While smaller in absolute share, this category still translates into nearly three thousand vulnerabilities within a partial year, reinforcing that truly severe, potentially high-impact flaws continue to emerge at a steady pace. From an operational standpoint, this volume

makes it unrealistic to treat all critical CVEs as exceptional events; instead, they form a continuous stream that must be handled through mature triage and response processes.

At the same time, Medium and Low severity CVEs collectively account for more than one-third of disclosures. Although these issues are individually less urgent, their aggregate volume contributes to long-term exposure, particularly when combined with misconfigurations, chaining opportunities or delayed patching.

Overall, the distribution suggests that vulnerability risk in 2025 is heavily skewed toward actionable, higher-severity issues, rather than being dominated by low-impact noise. For MSPs and enterprise security teams, this reinforces the need to move beyond severity-only prioritization and incorporate exploitability, asset criticality and exposure context into remediation decisions, especially given the sustained volume of High and Critical CVEs.

Core MSP platforms

This category includes platforms that directly manage endpoints, credentials, automation and customer environments across multiple tenants, including RMMs and PSAs.

Product	Vendor	2023	2024	2025 YTD	Total (23–25)
N-able RMM / N-central	N-able	1	5	8	14
ConnectWise Automate	ConnectWise	1	2	2	5
ConnectWise Control (ScreenConnect)	ConnectWise	0	1	2	3
ConnectWise Manage	ConnectWise	0	1	1	2
Passportal	N-able	0	1	1	2
Total		**2**	**10**	**14**	**26**

Severity profile – Core MSP platforms – 2025

Severity	CVEs	% of scored CVEs
Critical (>9.0)	6	42.9%
High (6.0–9.0)	8	57.1%
Medium / Low (<6.0)	0	0%

Although absolute numbers are small, 100% of MSP platform vulnerabilities disclosed in 2025 are High or Critical, reinforcing their disproportionate operational risk.

Remote access software is widely used by MSPs for day-to-day administration and incident response and is frequently abused post compromise.

Remote access CVEs – 2025

Severity	CVEs	Critical	High (6–9)	<6
TeamViewer (all variants)	19	2	16	1
AnyDesk	2	0	2	0
ConnectWise Control (overlap)	2	0	2	0
Total	**29**	**2**	**20**	**1**

Remote access tools consistently show a severity skew toward High and Critical, aligning with their frequent use in lateral movement and hands-on-keyboard attacks.

Identity and access management (MSP control plane)

Identity platforms are not MSP products themselves but are universally deployed and managed by MSPs, making them a critical shared control plane.

Identity platform CVEs – 2025

Product	CVEs	Critical	High (6–9)
Microsoft Entra ID (Azure AD)	97	11	63
Okta	12	2	9
Duo Security	4	0	4
OneLogin	3	0	3
Total	**116**	**13**	**79**

Identity systems alone contribute four times more CVEs than all core MSP platforms combined, with a consistently elevated criticality profile.

Patch and vulnerability management tools

Product	CVEs (2023–25)	Observations
Ivanti Patch Management	18	Often overlaps with broader Ivanti platform vulnerabilities.
ManageEngine Patch Manager Plus	7	Frequently bundled with endpoint management CVEs.
GFI LanGuard	2	Low volume, typically higher severity.

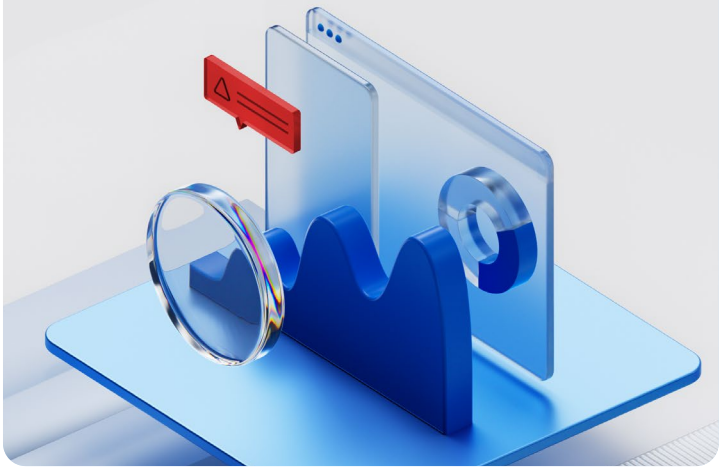
MSP-focused risk interpretation

From a pure CVE-count perspective, MSP platforms still represent a small fraction of global vulnerability disclosures. However, this metric significantly understates real-world risk. In the complete 2025 dataset, MSP-relevant exposure is concentrated in privileged control-plane software, including RMM platforms, remote access tools, identity providers and patch management systems.

Core MSP platforms show low volume but high severity concentration, while remote access and identity systems dominate attacker utility during post-compromise operations. Patch and endpoint management ecosystems — particularly Ivanti — contribute the largest absolute CVE volume among MSP-adjacent tools. Taken together, these patterns confirm that MSP risk is driven by blast radius, privilege and automation, not by raw vulnerability counts.

Effective MSP defense strategies must therefore prioritize control-plane hardening, rapid patch SLAs, identity protection and detection of administrative tool abuse, rather than relying on CVE volume as a proxy for operational risk.

MSP-relevant exposure is concentrated in privileged control plane software, including RMM platforms, remote access tools, identity providers and patch management systems.



Top zero-day vulnerabilities affecting Windows software (2025)

This section includes only vulnerabilities affecting software that runs on Microsoft Windows (endpoint OS, Windows components or Windows-native applications).

A vulnerability is classified here as a zero day if it meets at least one of the following criteria:

- Actively exploited in the wild at the time of disclosure.
- Publicly disclosed as a zero day by the vendor or authoritative security bodies.

Top Windows zero-day vulnerabilities of 2025

#	CVE	Affected Windows software	Vulnerability type	Exploitation status	MSP relevance
1	CVE-2025-62221	Microsoft Windows Cloud Files Mini Filter Driver	Local Privilege Escalation	Confirmed in the wild	High
2	CVE-2025-21802	Windows Win32 Kernel Subsystem	Local Privilege Escalation	Confirmed in the wild	High
3	CVE-2025-21424	Microsoft Windows SmartScreen	Security Feature Bypass	Confirmed in the wild	High
4	CVE-2025-20694	Microsoft Windows NTFS	Privilege Escalation	Confirmed in the wild	Medium
5	CVE-2025-21335	Microsoft Windows Hyper-V	Privilege Escalation	Confirmed exploitation	Medium
6	CVE-2025-13223	Google Chrome (Windows)	Browser Sandbox Escape	Confirmed zero day	High
7	CVE-2025-6558	Google Chrome (Windows)	Use-after-free RCE	Confirmed zero day	High
8	CVE-2025-21377	Windows Kernel Streaming	Elevation of Privilege	Active exploitation observed	Medium
9	CVE-2025-24813	Windows Print Spooler	Remote Code Execution	Exploited prior to patch	High
10	CVE-2025-24983	Windows Common Log File System (CLFS)	Privilege Escalation	Confirmed in the wild	High

70% of Windows zero days in 2025 targeted local privilege escalation, confirming that attackers heavily rely on post-compromise elevation rather than standalone RCE.

Why this matters for MSPs

From an MSP perspective, Windows zero-day vulnerabilities represent a disproportionate risk because of their fleet-wide impact. When exploited, these flaws typically affect large numbers of endpoints simultaneously, often spanning thousands of managed systems across multiple customer environments. In many observed cases, such vulnerabilities have the ability to bypass or weaken core security controls, including endpoint detection and response tools, SmartScreen protections and kernel-level safeguards. As a result, a single delayed or missed patch can quickly cascade into a multitenant incident, exposing several customers at once rather than remaining isolated to a single organization.

These vulnerabilities are rarely used in isolation. In real-world attacks, they are most often incorporated into exploit chains rather than serving as the initial point of entry. Commonly observed patterns include pairing Windows flaws with phishing campaigns, weaponized documents or browser-based compromises. This chaining approach mirrors the incident response cases typically handled by MSPs, in which attackers move from initial user interaction to deeper system compromise by combining multiple techniques rather than relying on a single exploit.

Detection further complicates the risk. Kernel-level privilege escalation exploits tend to produce minimal security telemetry and frequently operate below the visibility of user-mode security tools. In many cases, malicious activity is only detected after a secondary payload has already executed, at which point the attacker may have achieved elevated privileges, persistence or lateral movement. This creates a narrow window for prevention and places greater emphasis on rapid patching and proactive exposure management.

When viewed through an MSP-specific risk lens, these factors collectively elevate the threat level. Patch urgency is effectively immediate, with day-zero or day-one remediation required to reduce exposure. Detection difficulty remains high due to limited visibility and evasion of conventional tooling, while the potential for automation enables attackers to scale exploitation rapidly across managed fleets. Most critically, the impact is rarely confined to a single tenant: Weak isolation and shared management processes can amplify the blast radius, turning a single vulnerability into a cross-customer security event.

ATT&CK mapping (MSP-operational view)

This mapping is designed for MSP SOC and response playbooks (what stage the vulnerability typically supports in real intrusions):

CVE group	ATT&CK phase	Likely ATT&CK techniques (examples)	Practical MSP detection focus	Countermeasures
Chrome 0-days (CVE-2025-13223, CVE-2025-6558)	Initial Access / Execution	Drive-by compromise patterns; user execution	Browser process exploitation signals, suspicious child process chains, rapid post-exploit payload drops.	Aggressive browser auto-patch enforcement; browser isolation or hardened profiles for high-risk users; exploit-chain detection; DNS and URL reputation controls for post-exploit callbacks.
Access 0-days (CVE-2025-21366, CVE-2025-21395)	Initial Access / Execution	Malicious file delivery; user execution	Email-to-process correlation, suspicious Access spawning script interpreters or LOLBins.	Attachment detonation and content disarm for Office files; default-deny for Office spawning. PowerShell, cmd, wscript, mshta; ASR rules targeting Office child processes; email origin + execution correlation alerts.
PowerShell (CVE-2025-54100)	Execution / Defense Evasion	Command and scripting abuse	Tight logging, constrained language mode where applicable, strong script block + AMSI monitoring.	Full PowerShell Script Block Logging + AMSI integration; deny or alert on encoded commands and remote script execution; role-based PowerShell usage (admins vs. users); automatic isolation on suspicious PowerShell execution chains.
Windows EoP (CVE-2025-62221, CVE-2025-62215)	Privilege Escalation	Local escalation to SYSTEM	Watch for privilege transitions, suspicious driver/file-system interactions, rapid credential dumping post escalation.	Driver allowlisting and block-by-default for vulnerable drivers; detection of user-to-SYSTEM transitions; LSASS protection and credential dumping prevention.
Hyper-V EoP (CVE-2025-	Privilege Escalation / Lateral Movement enablement	Host-level takeover enabling broader movement	Hyper-V host hardening, segmentation, strict admin tiering, monitoring of virtualization management operations.	Strict admin tiering between guests and hosts; limit Hyper-V management access to dedicated jump hosts; continuous monitoring of VM management APIs and service actions; patch prioritization for virtualization stacks.

Key takeaways

Windows remains the primary zero-day target in 2025 due to its ubiquity in MSP-managed environments. Privilege escalation dominates, reinforcing that attackers assume some level of initial access. Patch latency is the single most important risk factor for MSPs regarding zero-day exposure. CVE volume alone understates the true operational risk posed by Windows zero-days.

What we see among our customers

Acronis Cyber Protect includes built-in of vulnerability assessment functionality, which automatically checks the endpoints for known vulnerabilities. If Acronis RMM product in place, you can seamlessly in the same automatic manner patch these vulnerabilities. Below is the overall global vulnerability landscape on our users' machines.

Top 10 vulnerable software products globally among Acronis customers –January–November 2025

Product	Unique CVEs	Affected clients
Microsoft Windows 10	5,129	45.5%
Microsoft Windows 11	1,894	43.3%
Microsoft Windows Server 2019	3,365	32.2%
7-zip	18	21.5%
Microsoft Visual Studio 2010	7	21.5%
Microsoft .net 8.0	18	18%
Mozilla Firefox	1,964	16.4%
Rarlab Winrar	14	15%
Oracle Java Runtime Environment	823	14.7%
Microsoft Visual Studio 2008	14	14.6%

Unsurprisingly Microsoft operating systems continue to dominate the list of the most vulnerable software products observed among Acronis customers. Windows 10 this time is a leader, affecting nearly half of all monitored environments, which reflects both its broad deployment footprint and the large volume of disclosed, patchable vulnerabilities accumulated over its lifecycle. Windows 11 follows closely, indicating that even newer desktop platforms rapidly become significant attack surfaces once adoption reaches scale.

Of particular concern is the strong presence of Windows Server 2019, which shows a high number of unique CVEs and a substantial share of affected clients. Server platforms usually host business-critical workloads and are patched more conservatively due to uptime and compatibility considerations. This creates a higher risk exposure window compared to desktop systems, where update cycles are usually faster and more automated.

Beyond operating systems, widely used third-party and development tools such as 7-Zip, WinRAR, Mozilla Firefox, Java Runtime Environment and multiple generations of Microsoft Visual Studio and .NET illustrate how common auxiliary software significantly contributes to the overall vulnerability landscape. Although the absolute number of CVEs for these products is lower, their high penetration across environments results in a meaningful percentage of affected clients.

Overall, the data highlights a dual challenge for organizations: managing vulnerability sprawl in legacy and widely deployed operating systems, while also maintaining consistent patching discipline for commonly installed productivity and development software. Environments that continue to rely heavily on older platforms or long-lived server systems should treat vulnerability management and update prioritization as a critical operational risk rather than a routine maintenance task.

6. AI-powered cyberthreats

During H2 2025, artificial intelligence (AI) was increasingly embedded into criminal operational workflows, rather than used experimentally or opportunistically. The dominant trend was not the creation of new attack techniques, but the acceleration and scaling of existing ones: ransomware negotiations, data extortion, reconnaissance, fraud and attack orchestration. In several cases, AI systems were observed performing semi-autonomous task execution under human direction, reducing attacker workload and compressing timelines.

The following five cases represent documented H2 2025 activity, with attribution based on primary sources and corroborated reporting.

1 GLOBAL GROUP ransomware: AI-driven negotiation automation

In July 2025, GLOBAL GROUP ransomware operation introduced an AI-driven chatbot[13] into its victim negotiation portal. Operationally, the chatbot replaces or supplements human negotiators during the early stages of extortion. After a victim accesses the negotiation portal, the AI system handles routine communication: Responding instantly, maintaining pressure through deadlines and guiding victims toward payment steps or "proof" requests. Human operators reportedly intervene only for high-value victims or stalled negotiations.

The use of AI here does not alter the ransomware infection chain itself. Instead, it scales the monetization phase, allowing the group to manage more concurrent victims with fewer operators, while applying consistent psychological pressure.

2 GTG-2002: AI-assisted data extortion at scale

In August 2025, GTG-2002 used Claude Code to support a multivictim data theft and extortion campaign.[14] The activity was independently summarized by Reuters, confirming that accounts linked to the operation were terminated. GTG-2002 used AI not only for text generation, but for practical intrusion support. The actor relied on AI tools to generate and debug scripts, assist with credential harvesting and network traversal and rapidly analyze stolen datasets to identify sensitive or high-leverage information. These summaries were then used to tailor extortion demands to each victim.

No public attribution to a named ransomware brand is provided in the source material, and the correct attribution remains GTG-2002 (Anthropic tracking identifier). The key operational impact is that AI reduced the effort required to run end-to-end extortion campaigns, enabling a single operator or small team to handle more victims in parallel.

3 Chinese state-aligned intrusion: Agentic AI task execution

In November 2025, an AI-assisted intrusion campaign[15] was attributed with high confidence to a Chinese state-sponsored threat actor. Unlike earlier cases focused on drafting or scripting assistance, this operation demonstrated agentic AI behavior: The system was used to execute sequences of tasks with limited human intervention. Human operators defined goals and targets, but the AI system handled chained actions such as reconnaissance, credential use and environment interaction, looping through tasks until objectives were met or blocked. While the campaign was primarily espionage-oriented rather than financially motivated, it represents an escalation in how AI can be operationalized within real attacks.

[13] Büyükkaya, Arda. "GLOBAL GROUP: Emerging Ransomware-as-a-Service, supporting AI driven negotiation and mobile control panel for their affiliates." EclecticIQ. July 15, 2025. https://blog.eclecticiq.com/global-group-emerging-ransomware-as-a-service

[14] Lakshmanan, Ravie. "Anthropic Disrupts AI-Powered Cyberattacks Automating Theft and Extortion Across Critical Sectors." The Hacker News. August 27, 2025. https://thehackernews.com/2025/08/anthropic-disrupts-ai-powered.html

[15] ANTHROP\C. "Disrupting the first reported AI-orchestrated cyber espionage campaign." November 13, 2025. https://www.anthropic.com/news/disrupting-AI-espionage

4 Virtual kidnapping scams using AI-altered “proof of life”

In December 2025, the FBI Internet Crime Complaint Center (IC3) issued a public advisory warning[16] that criminals were using AI-altered photos and videos as fake “proof of life” in virtual kidnapping and extortion scams. The advisory described cases in which attackers harvested publicly available images and used manipulation tools to fabricate evidence supporting urgent ransom demands.

The FBI does not attribute these scams to a specific organized group; the correct attribution is unattributed criminal actors, per IC3. The technical novelty is limited, but the psychological effectiveness is significantly enhanced. AI lowers the cost and skill barrier required to create convincing coercion material, allowing scammers to operate at higher volume and with greater success.

5 RaaS ecosystems advertising AI and automation

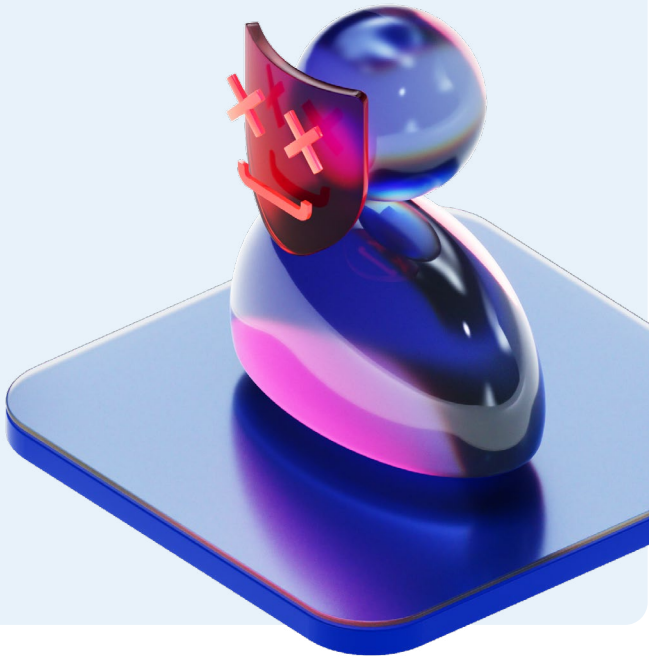
On underground forums, particularly RAMP, automation and “AI” features are now widely advertised within RaaS platforms. Approximately 80% of tracked RaaS offerings promote[17] capabilities such as automated detection of EDR / AV products and automated termination of defensive processes. Qilin gang is the best example of a RaaS operation advertising advanced automation features — emerging groups such as The Gentlemen and DragonForce are likely to adopt similar capabilities.

Operationally, these features compress attacker timelines by removing manual steps between initial access and ransomware execution. Whether branded as “AI” or advanced automation, the outcome is the same: faster breakout times, increased likelihood of successful encryption and greater risk of cross-customer impact in MSP-managed environments.

Conclusion

H2 2025 cases showed that AI is no longer peripheral to cybercrime operations. It was being applied where it provided immediate economic and operational advantage: negotiation, extortion targeting, reconnaissance and automation. Importantly, AI is not replacing attackers, but it is changing the balance between effort and impact, allowing smaller teams to operate at greater scale and speed.

For MSPs and enterprises, the practical implication is a continued erosion of response time and trust-based controls. Defenders must assume that attackers can now iterate faster, communicate more convincingly and sustain pressure more efficiently than in previous reporting periods.



[16] Federal Bureau of Investigation. “Criminals Using Altered Proof-of-Life Media to Extort Victims in Virtual Kidnapping for Ransom Scams.” December 5, 2025. https://www.ic3.gov/PSA/2025/PSA251205

[17] Reliaquest Threat Research. “Threat Spotlight: How Automation, Customization, and Tooling Signal Next Ransomware Front Runners.” Reliaquest. October 21, 2025. https://reliaquest.com/blog/threat-spotlight-how-automation-customization-and-tooling-signal-ransomware

2

General malware threats

While the overall volume of malware activity remains substantial, the 2025 data clearly shows that malware exposure was not evenly distributed, either over time or geographically.

Across the year, malware exposure followed a well-defined lifecycle:

- Elevated activity in Q1, culminating in a broad peak in March.
- Sustained pressure through Q2, with several regions peaking again in May–June.
- A structural decline from July onward, stabilizing at lower levels through September–November.

This pattern was visible across both high-risk and low-risk countries, indicating that the trend was campaign-driven rather than region specific. Attackers appeared to front-load activity early in the year and lose effectiveness as detection, takedowns and defensive tuning accumulated.

Month	Normalized percentage of Acronis clients with blocked malware
January	5.2%
February	4.7%
March	6.7%
April	4.8%
May	6.2%
June	6.1%
July	5.1%
August	4.6%
September	3.3%
October	3.5%
November	3.5%
December	3.6%

Countries including Vietnam, South Korea, Peru, Venezuela, India, Thailand and Brazil consistently recorded significantly above-average exposure during the year: Multiple months exceeded 10% of protected clients experiencing blocked malware. Peaks occurred predominantly in March, May and June. Despite elevated early-year risk, most of these countries showed clear improvement by September–November, converging toward mid-single-digit levels. This pattern indicates burst-style malware campaigns rather than sustained compromise pressure, with endpoint protection playing a decisive containment role.

A second group — including Romania, Spain, Mexico, Israel, Indonesia, Colombia and several Central and Eastern European countries — showed early-year exposure, typically in the 5%–10% range. Noticeable volatility was tied to specific campaign windows. There was progressive decline after midyear, reaching lower and more stable levels by Q4. These regions illustrated how incremental improvements in hygiene, patching and security configuration materially reduce malware success rates over time.

Countries including Japan, Singapore, Canada, the U.S., the U.K. Australia, Switzerland, Sweden, Denmark and Belgium consistently remained on the lower end of the spectrum: Malware exposure usually remained below 4%, even during peak months. Variability was limited, and no extreme spikes were observed. By September–November, exposure levels clustered around 2%–3%. This strongly correlates with mature security postures, broader use of layered defenses and higher baseline user awareness.

Across virtually all countries (January–November) March represented the highest systemic risk month; May–June acted as secondary amplification periods; and August onward showed sustained normalization. This reinforces the conclusion that attackers optimized campaigns for early-year scale before infrastructure reuse, signature coverage and behavioral detection reduced effectiveness.

Top 15 countries: Normalized percentage of global malware detections – 2025

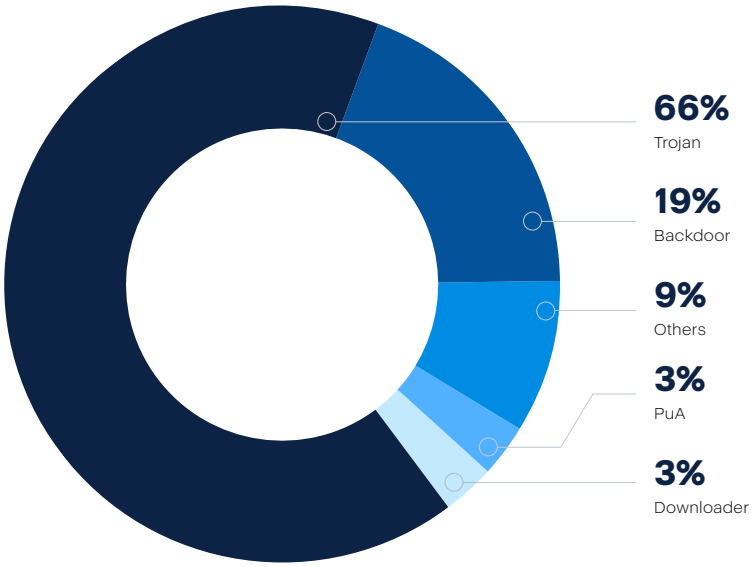
Country	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEPT	OCT	NOV	DEC
South Korea	13.37	11.52	11.58	9.67	17.88	15.6	13.56	12.5	10.36	9.6	10.59	9.55
Vietnam	16.55	11.99	12.4	8.6	14.51	15.29	11.09	8.76	13.91	10.85	9.86	7.97
Taiwan	6.52	6.85	6.65	5.58	10.35	10.23	10.3	10.79	9.74	9.83	9.44	7.64
Peru	10.94	12.36	13.9	9.52	13.67	16.41	11.88	10.21	8.09	7.31	7.77	5.83
India	9.69	8.33	11.76	8.47	12.52	13.31	9.97	9.33	7.53	7.28	7.69	6.57
Venezuela	10.8	8.44	10.5	6.71	13.97	21.94	13.83	9.76	7.3	7.5	7.49	4.42
Brazil	8.81	7.59	11	9.27	11.22	9.68	8.25	6.98	4.87	5.7	6.24	4.59
Israel	5.23	4.94	12.17	6.75	11.46	9.65	6.93	6.77	4.07	4.87	5.99	4.13
Indonesia	7.95	6.12	8.2	5.34	8.32	10.29	7.56	5.82	4.97	5.39	5.73	4
Romania	4.76	4.03	9.57	9.85	11.44	8.84	7.36	6.11	4.68	4.42	5.58	4.58
Dominican Republic	8.96	7.4	10.21	7.48	7.85	8.03	7.49	6.37	3.31	3.07	4.77	5.47
Spain	7.4	6.97	10.63	7.74	9.63	8.37	6.85	6.16	3.61	4.22	4.75	3.77
Thailand	10.51	11.02	11	8.69	9.35	9.82	9.45	9.15	6.28	4.92	4.66	4.32
United Arab Emirates	6.9	6.28	9.9	5.74	8.88	8.22	7.24	6.25	3.46	5.16	4.24	3.87
Mexico	7.39	7.35	9.08	7.32	7.99	8.44	7.12	6.69	6.76	4.59	4.01	3.24

Key conclusions

To summarize: Malware exposure was highly uneven across countries, with certain regions experiencing sustained double-digit risk early in the year. The first half of 2025 represented the primary threat window, with March as the universal peak month. Exposure consistently declined after midyear, indicating shorter campaign lifetimes and improving defensive response. Developed markets demonstrated structurally lower exposure, validating the effectiveness of layered security and enforcement. Endpoint security remained a critical safety net, capturing threats that evaded earlier controls.

For January–November 2025, the data confirmed that modern malware operations favored scale and speed over persistence. While attackers could easily acquire tools through malware-as-a-service (MaaS) ecosystems, organizational maturity ultimately determined impact.

Most common malware types



AV-TEST

Malware types detected in mid-December 2025
(source: av-test.org)

The most common malware type is Trojans (a type of malicious software that disguises itself as a legitimate or useful program to trick users into executing it, after which it silently delivers unauthorized actions such as data theft, remote access or additional malware installation), making up more than half of the blocked threats.

Several clear patterns emerged from the family-level submission data:

- Credential stealers dominated by volume, reflecting attackers' focus on account takeover, resale and downstream compromise.
- RATs and loaders remained structurally important, serving as control layers and staging mechanisms rather than final payloads.
- High submission volume was driven less by novelty and more by ease of repacking, MaaS availability and distribution scale.
- The malware ecosystem in 2025 favored quantity and reuse over innovation, with many families persisting year over year.

1 Lumma Stealer

Lumma is the most consistently dominant family in sample submissions throughout 2025. Its modular design, active MaaS ecosystem and frequent repacking drive a very high submission rate, especially from phishing and cracked-software delivery chains. Lumma's prominence reflects the continued prioritization of credential theft and session hijacking.

2 RedLine Stealer

RedLine remains one of the most widely submitted families, sustained by its low cost, easy operation and strong integration into affiliate-based crimeware operations. Despite its age, RedLine's adaptability keeps it among the top credential-stealing families by volume.

3 AgentTesla

AgentTesla continues to generate a large number of submissions due to its email-centric distribution, frequent minor variants and long-standing popularity among lower-skill actors. Its persistence in 2025 highlights how legacy stealers still dominate sample volume, even as newer families emerge.

4 AsyncRAT

AsyncRAT remains a major contributor to MalwareBazaar submissions, driven by widespread use in remote access, botnet control and secondary payload staging. Its open availability and ease of customization result in constant recompiled variants, inflating submission counts.

5 Remcos

Remcos continues to rank highly as a commercial RAT abused by criminal actors. In 2025, it remains especially visible in malspam and loader-based infection chains, often paired with stealers or used for persistence and lateral movement.

6 XWorm

XWorm's presence increased further in 2025, particularly in low-cost RAT and loader ecosystems. Its frequent repacking and use by novice actors contribute to high submission volume despite relatively simple functionality.

7 Rhadamanthys

Rhadamanthys solidified its position as a high-volume modern stealer, frequently observed in cracked software, fake updates and social-engineering campaigns. Its steady stream of submissions reflects both active development and broad affiliate adoption.

8 DCRat

DCRat remains a common submission due to its long lifecycle, modular design and continued use in commodity campaigns. Like AsyncRAT, frequent customization leads to a large number of unique hashes.

9 SmokeLoader

SmokeLoader continues to appear prominently as both a standalone loader and a delivery mechanism for secondary malware. Its position in the ranking reflects its role as an enabler, often preceding ransomware or stealer deployment.

10 FormBook / XLoader

FormBook and its macOS-oriented successor XLoader collectively maintain high submission volume, driven by phishing campaigns and credential harvesting. Their continued presence underscores the durability of simple, effective data-stealing malware.

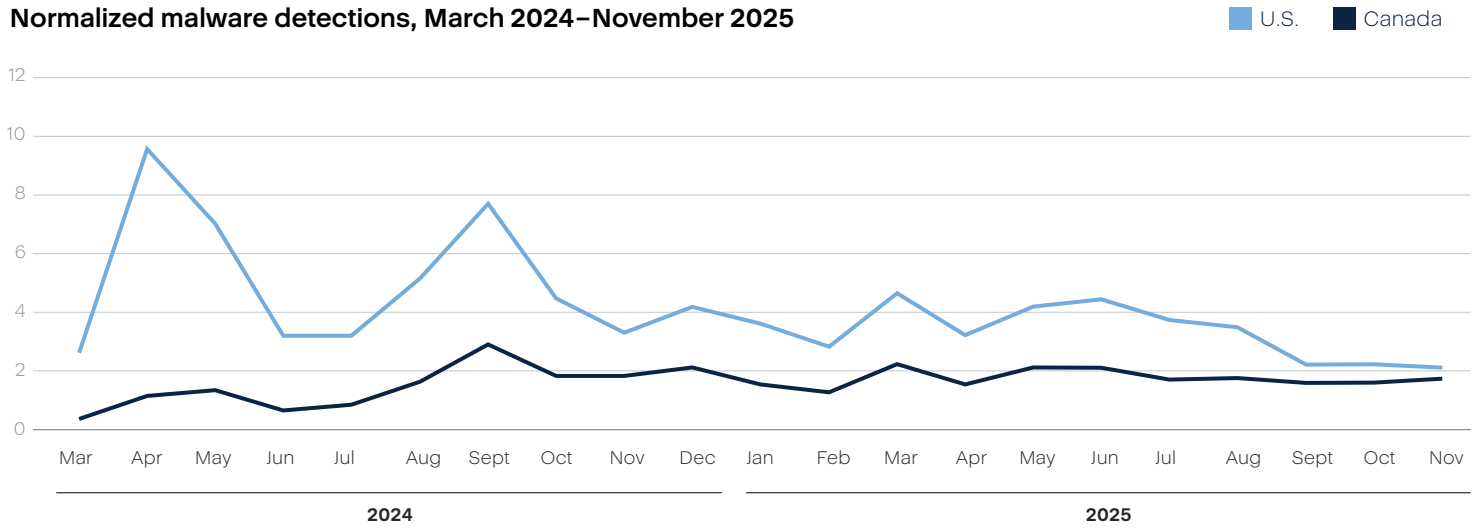
Telemetry data in focus countries

U.S. and Canada

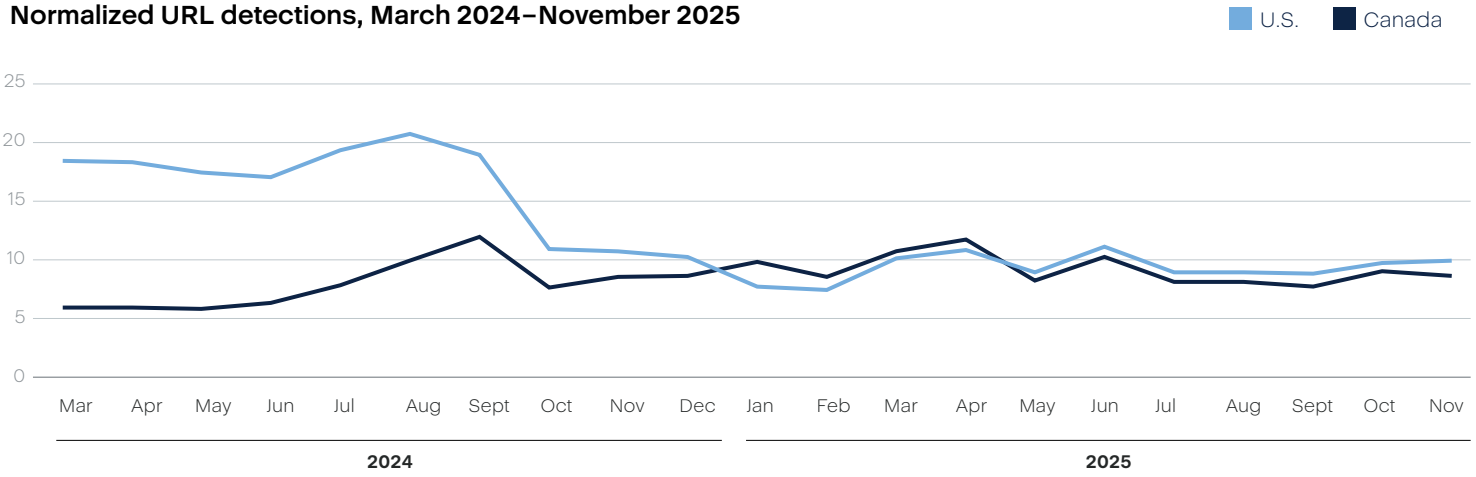
Across the observed period, the U.S. has consistently shown higher normalized malware detection rates than Canada, indicating a higher relative exposure to endpoint-level malware activity. The most notable anomaly was a pronounced spike in the U.S. during spring 2024, followed by several secondary peaks in mid-2024, suggesting short-lived but intensive malware campaigns. Canada, by contrast, remains consistently lower and more stable, with only modest increases and no extreme outliers. In 2025, both countries converged toward lower, steadier levels, with Canada continuing to demonstrate a flatter profile and fewer sharp fluctuations than the U.S.

For web-based threats, the U.S. again recorded higher normalized levels than Canada throughout most of the timeline, particularly in 2024, in which the U.S. experienced very high exposure early in the year, peaking well above Canada. One notable anomaly was the sharp drop in U.S. exposure toward late 2024, after which both countries operated within a narrower and more comparable range. In 2025, Canada and the U.S. tracked closely, with alternating minor peaks, indicating similar exposure patterns and suggesting that web-borne threats affected both environments in a broadly comparable way once normalized.

Normalized malware detections, March 2024–November 2025

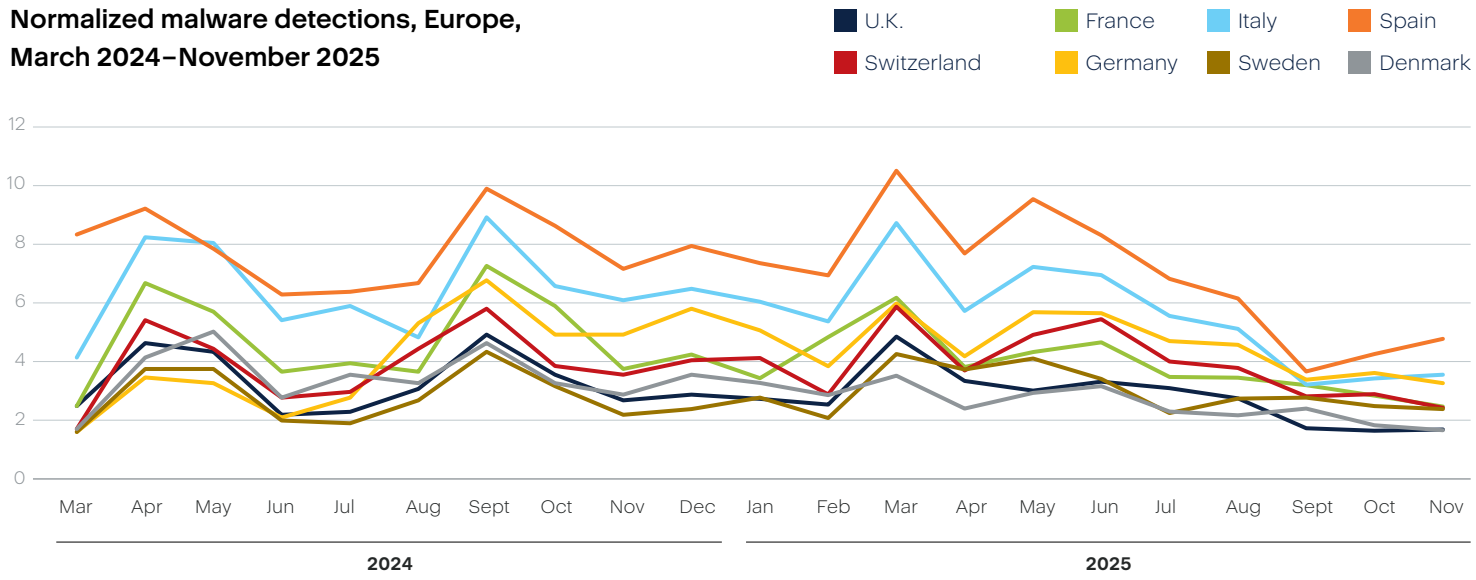


Normalized URL detections, March 2024–November 2025

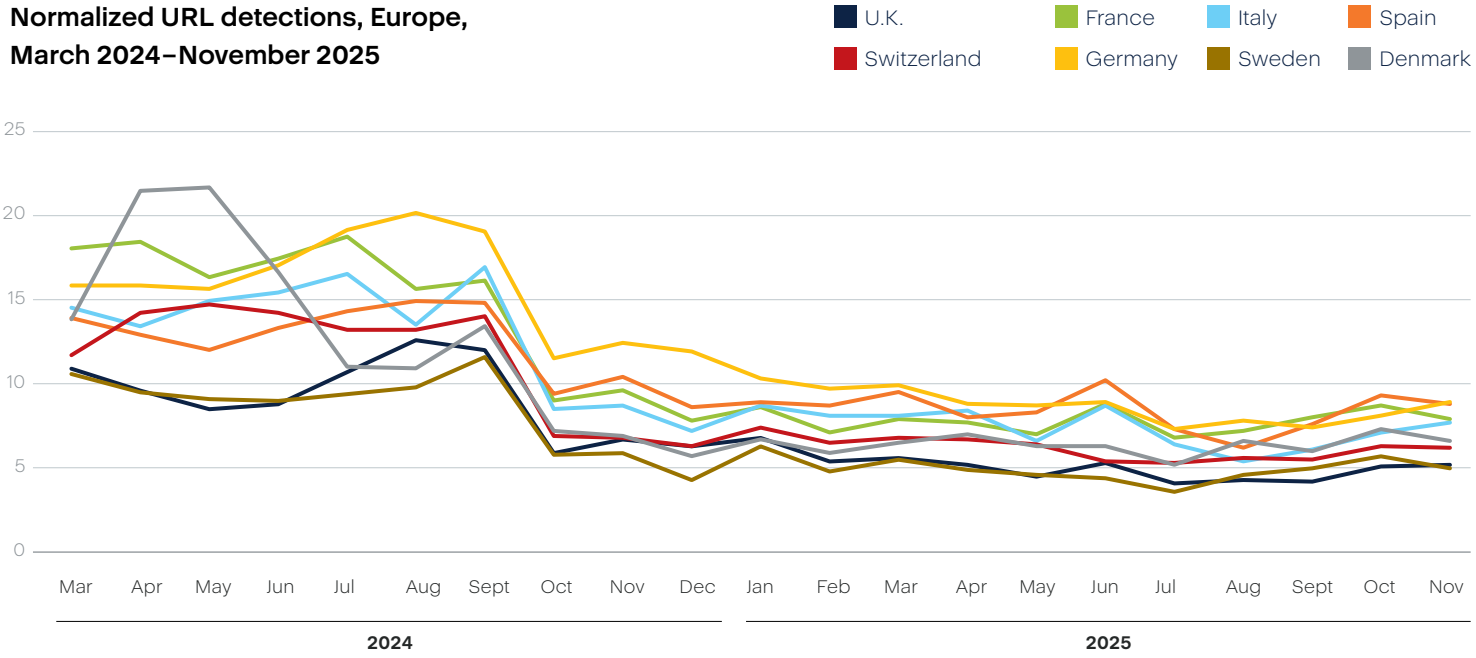


⚠ Differences between 2024 and 2025 are not interpreted as year-over-year trends, as changes are primarily driven by calculation methodology updates rather than underlying threat dynamics.

Normalized malware detections, Europe, March 2024–November 2025



Normalized URL detections, Europe, March 2024–November 2025



Across both charts, the patterns point to campaign-driven activity rather than steady background noise, and the differences between countries were more pronounced than the differences between years, which should not be over-interpreted due to the methodology change.

In the malware detections chart, Spain stood out as the country with the consistently highest normalized exposure, with several sharp spikes that were mirrored at lower levels in Italy, Germany and France. These synchronized peaks, particularly around spring and early Autumn, are typical of coordinated malware or ransomware distribution waves rather than local, isolated incidents.

Similar timing was observed in widely reported ransomware and loader campaigns during those periods, in which initial access was gained at scale and then monetized quickly before infrastructure was burned. Countries like Sweden, Denmark and Switzerland showed a flatter profile with smaller amplitudes, suggesting either more effective upstream filtering or a lower success rate of the same campaigns rather than a fundamentally different threat mix.

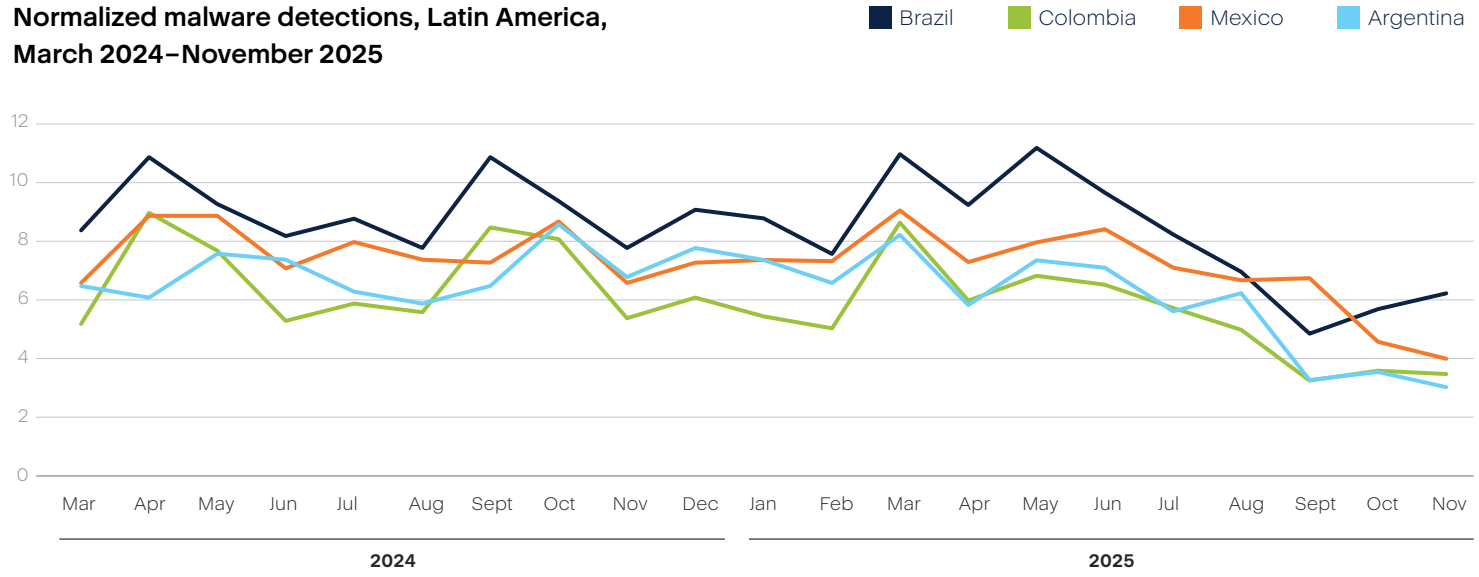
The URL detections chart shows a different but related story. Here, all countries experienced much higher normalized exposure earlier in the timeline, followed by a clear step down and stabilization. This pattern aligns well with the broader industry observation that malicious URLs and phishing links have overtaken attachments as the primary delivery mechanism.

Large phishing and malvertising campaigns tend to create wide but short-lived spikes in URL detections, often affecting multiple countries at once. The convergence of country lines in the later period suggests that, once normalized, web-based threats impact European countries in a relatively similar way, even if absolute volumes differ.

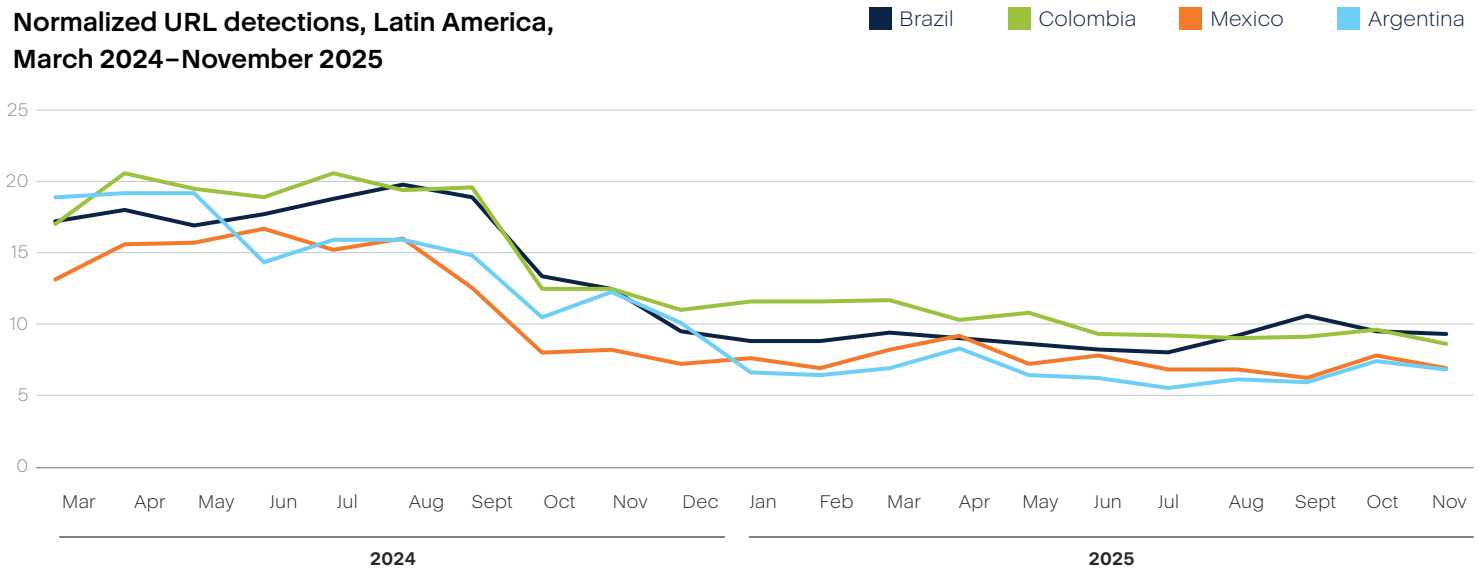
Looking at both charts together, a plausible interpretation is that URL-based activity often precedes or accompanies malware waves. Elevated URL detections reflect phishing, fake login portals and malicious redirects used for credential theft or initial access. When these campaigns are successful, they are followed by bursts of endpoint malware detections as second-stage payloads are executed. The fact that malware spikes are sharper and more uneven across countries, while URL detections are broader and more uniform, supports this attack-chain view.

Overall, the data suggests that European threat exposure during this period was shaped by episodic, large-scale campaigns, likely tied to ransomware ecosystems and initial-access brokers, rather than by a slow increase in baseline risk. Differences between countries appear to reflect relative susceptibility and defensive posture, not fundamentally different threat actors or techniques.

Normalized malware detections, Latin America, March 2024–November 2025



Normalized URL detections, Latin America, March 2024–November 2025



Focusing on 2025, the most visible feature is the coordinated uplift in Q1–Q2 2025 across Mexico, Argentina and Colombia, which looks much more like regional campaign activity than isolated, country-specific incidents. In the malware chart, Mexico and Argentina climbed into a clear peak around March–May 2025 and then trended downward into the second half of the year. That shape matches what we ordinarily see when a phishing-led distribution wave runs hard for a few months and then loses momentum as infrastructure is blocked and lures burn out.

For that early-2025 spike, two widely reported campaigns fit both the timing and the geography. First, Grandoreiro distribution campaigns were observed in March 2025[18] targeting Mexico and Argentina using phishing emails impersonating tax agencies and delivering malicious ZIP / VBS chains that drop the banking trojan. That kind of infection chain would raise both web exposure (users interacting with malicious content delivered via email / links / attachments) and downstream endpoint malware detections when the payload executes.

Grandoreiro distribution campaigns were observed in March 2025 targeting Mexico and Argentina using phishing emails impersonating tax agencies and delivering malicious ZIP / VBS chains that drop the banking trojan.

The synchronized spikes in Europe and LATAM were driven by shared campaigns and reused infrastructure, not independent regional outbreaks. LATAM-based groups like those behind Grandoreiro have typically tested and scaled phishing and loader chains in markets such as Mexico and Argentina, then rapidly repurposed the same delivery mechanisms for Europe, adjusting only language and lures.

Spain acted as a bridge market, which explains its higher and sharper peaks. The same waves then propagated into Italy, Germany and France at lower intensity. The spring and early-Autumn timing reflects coordinated distribution bursts that were monetized quickly before infrastructure was burned, while flatter profiles in countries like Sweden or Switzerland indicated lower success rates of the same campaigns, not a different threat mix.

Second, in April 2025 a phishing operation used malicious HTML[19] "invoice / financial document" lures to spread Horabot, specifically targeting Spanish-speaking users in Latin America; multiple summaries of that research list Argentina, Colombia and Mexico among the affected countries. This maps well to the multicountry bump you see in Q2 2025.

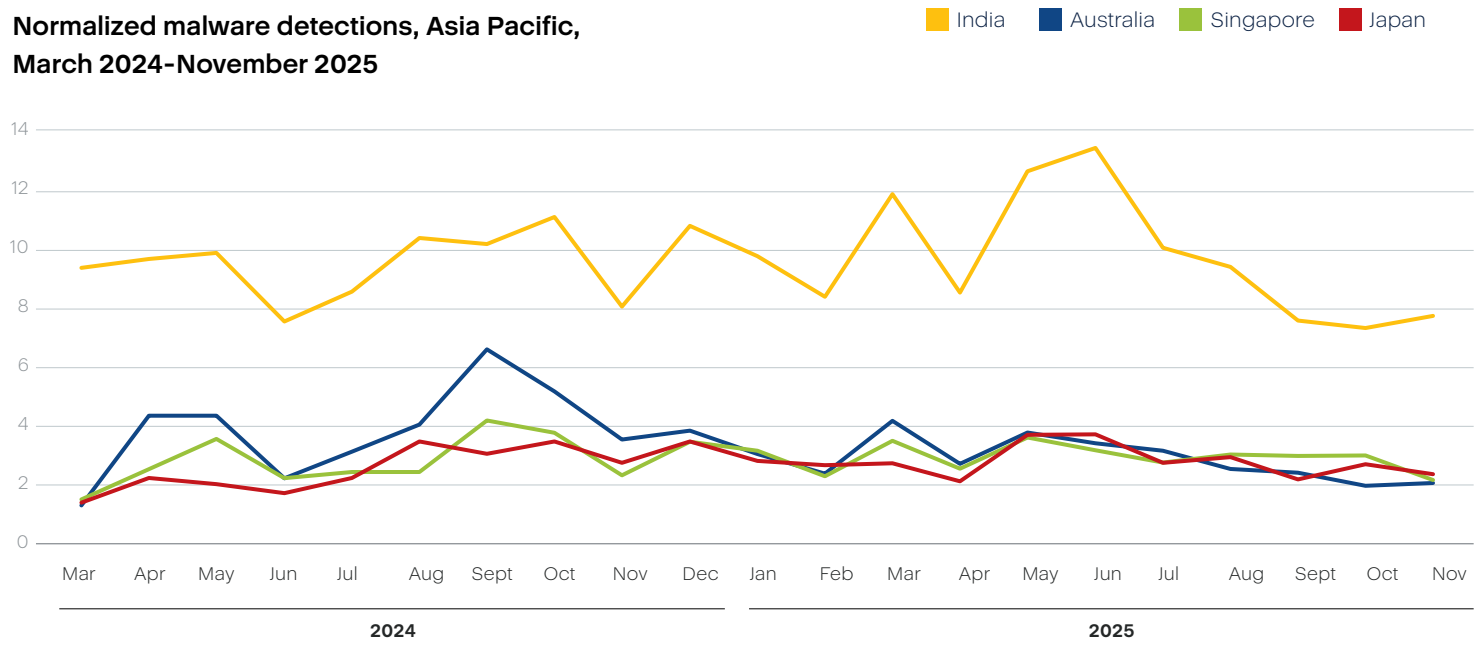
Colombia's 2025 profile is also consistent with targeted lure themes. TRU documented an ongoing Colombia-focused campaign in June 2025 ("Shadow Vector") using court-themed decoys and SVG smuggling to deliver malicious payloads. That type of technique usually shows up first as URL / web threat detections (delivery and user interaction) and then as malware detections when the final stage runs.

Brazil remains the highest baseline country in these charts, but for 2025 specifically the public sources above support stronger, cleaner attribution for the Mexico / Argentina / Colombia wave than for Brazil's month-to-month movement. The most defensible conclusion from the evidence is that the main 2025 anomalies in your curves are driven by phishing-led, Spanish-language LATAM campaigns (notably Grandoreiro distribution in March 2025 and Horabot in April 2025), with Colombia also showing activity consistent with local-theme social engineering (court notifications) in mid-2025.

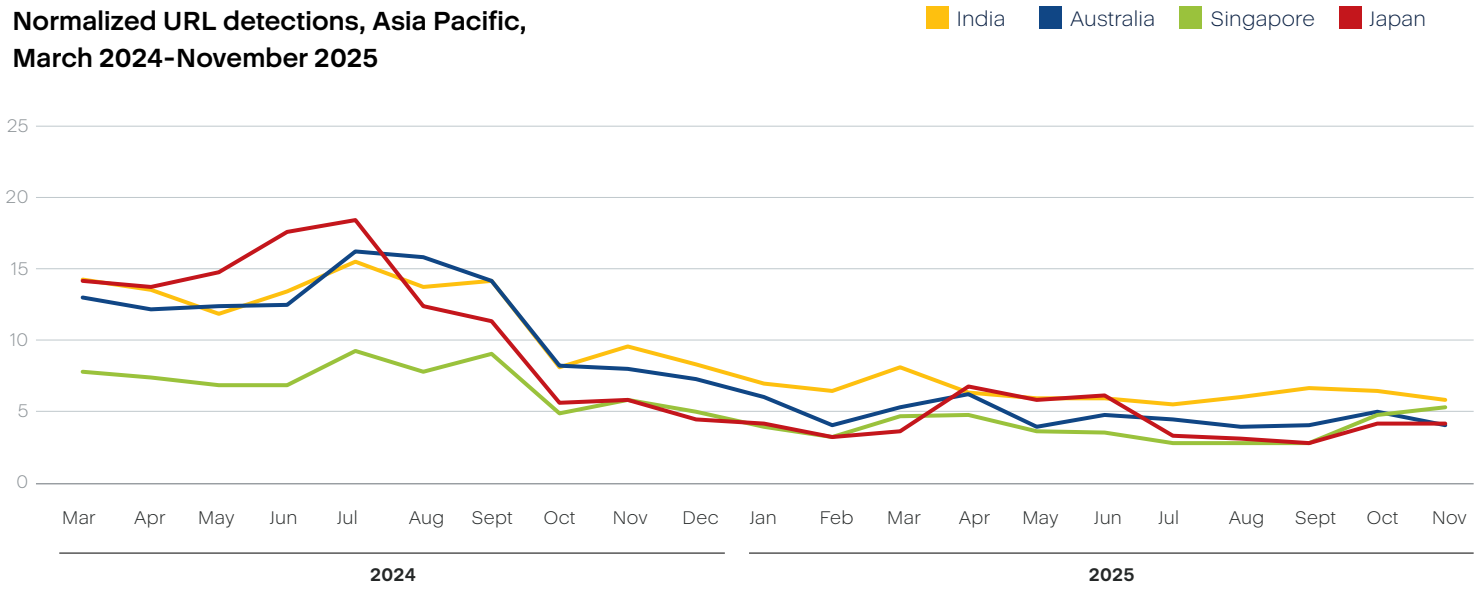
[17] Lab52. "Grandoreiro Stealer Targeting Spain and Latin America: Malware Analysis and Decryption Insights." April 4, 2025. https://lab52.io/blog/2805-2/

[18] Lin, Cara. "Horabot Unleashed: A Stealthy Phishing Threat." Fortinet. May 12, 2025. https://www.fortinet.com/blog/threat-research/horabot-unleashed-a-stealthy-phishing-threat

Normalized malware detections, Asia Pacific, March 2024-November 2025



Normalized URL detections, Asia Pacific, March 2024-November 2025



In the malware detections chart for 2025, India clearly stands out with a much higher and more volatile normalized exposure, peaking around late spring and early summer before declining toward the end of the year. That pattern is typical of large-scale, commodity malware campaigns rather than targeted intrusions.

India was frequently highlighted in threat reporting as a high-volume target for phishing-led malware delivery, including loaders, RATs and banking or credential-stealing malware, often distributed through fake invoices, tax notices or job-related lures. The sharp rise around March–June 2025 was consistent with such campaigns being pushed aggressively for a limited window and then losing effectiveness as infrastructure and lures are blocked.

Australia showed a short-lived spike in early 2025, but at a much lower level than India and without sustained elevation. This shape suggests campaign spillover rather than primary targeting — for example, global phishing or malware waves that also reached Australian users but did not maintain traction for long. Singapore and Japan remain low and comparatively flat throughout 2025, indicating that while the same campaigns likely reached these countries, they resulted in fewer successful endpoint executions. This is consistent with stronger upstream

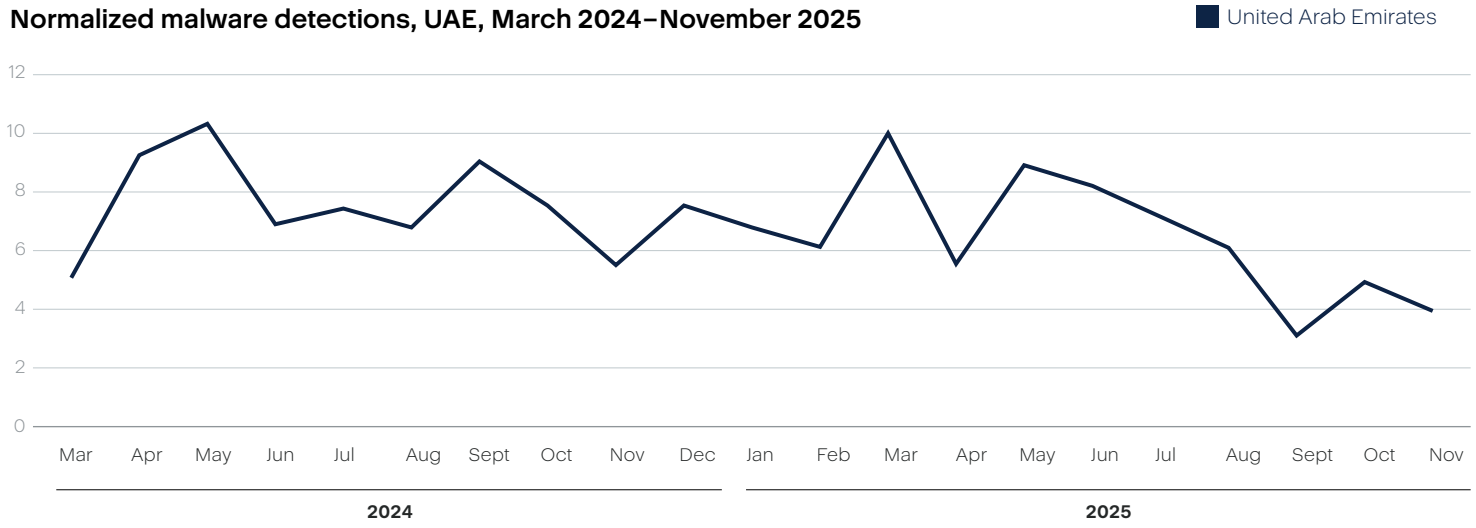
controls and user behavior reducing the likelihood that phishing-delivered malware progresses to execution.

In the URL detections chart for 2025, the picture changes slightly. All four countries clustered much closer together, especially from spring onward, which suggested that web-based threats were broadly distributed across the region, even if they do not always result in malware execution. India again sat somewhat higher, but the gap was far smaller than in malware detections. This supports a common attack-chain interpretation: Many users across these countries are exposed to phishing links, malicious redirects or scam infrastructure, but only in some environments — most visibly India — did that exposure translate into a higher rate of endpoint malware detections.

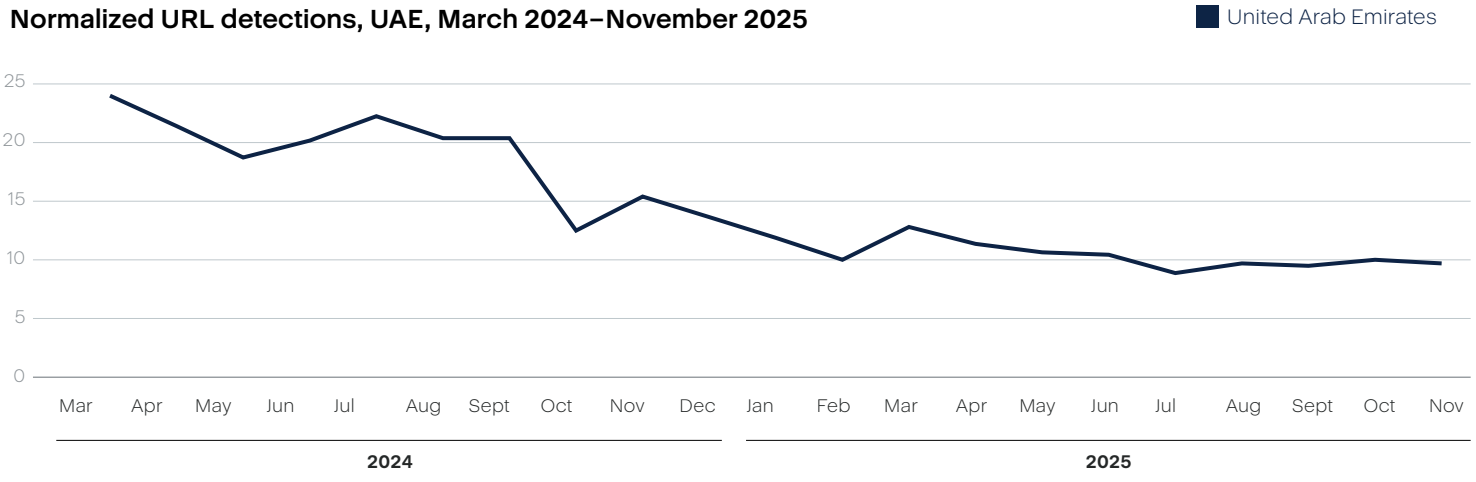
The gradual stabilization and mild convergence across all four countries in the second half of 2025 point to campaign fatigue rather than a fundamental reduction in threat actor activity. Once phishing domains, URLs and delivery mechanisms were identified and blocked at scale, URL detections leveled off and malware execution dropped even more sharply. Singapore and Japan illustrated this especially well: URL exposure continued at modest levels, but malware detections remained consistently low, implying that most attacks were being stopped earlier in the chain.

Taken together, the 2025 data suggests that the same phishing- and URL-driven campaigns were reaching all four countries, but the downstream impact differed significantly. India appeared to be the primary environment where those campaigns translate into widespread malware execution, while Australia saw intermittent effects and Singapore and Japan largely contained the threat before it escalated beyond web exposure.

Normalized malware detections, UAE, March 2024–November 2025



Normalized URL detections, UAE, March 2024–November 2025



The UAE stands out as a case where the relationship between web exposure and actual malware execution becomes very clear over time.

In the malware detections chart, activity was noticeably higher and more uneven in the first months of the year, with a clear rise around March, followed by a gradual but steady drop through the summer. This kind of pattern usually points to short-lived campaign bursts rather than constant background infections. The early spike fit well with the types of business-themed phishing and malware delivery campaigns that regularly target organizations in the Gulf region, using invoices, payment requests or logistics-related lures. Once those campaigns were disrupted or lost their effectiveness, the impact fell off relatively quickly, which is exactly what happened from mid-2025 onward.

The URL detections chart tells a slightly different story. In 2025, exposure to malicious links in the UAE stayed consistently high, even as malware detections declined. Rather than sharp drops, the URL curve eased down slowly and then leveled out. This suggests that users continued to encounter phishing links and malicious websites, but fewer of those encounters led to malware actually running on endpoints. The threats were still "out there," but they were being stopped earlier, before they could do real damage.

Seen together, the two charts suggest a decoupling of exposure and impact as the year progressed. Early in 2025, web-based threats more often resulted in malware execution. Later in the year, similar types of threats were still reaching users, but defenses appeared to be more effective at breaking the attack chain. Compared with other regions in the report, the UAE's 2025 profile looked less like a constant pressure from commodity malware and more like a series of brief, targeted, phishing-driven waves that flare up and then fade as controls catch up.

Top 10 Acronis EDR / XDR detections by volume in focus countries

A separate analysis of specific threats that were detected by Acronis EDR and XDR. The following tables present the top 10 Acronis EDR / XDR detections by volume for each focus country in 2025. Each table reflects actual security detections observed on protected endpoints, aggregated by threat or behavioral detection name and ranked by the total number of detection events during the year.

It is important to note that these tables do not represent unique incidents or victims, but rather the frequency with which specific malicious behaviors or threat types were detected and blocked. As such, higher numbers may reflect repeated execution attempts, automated activity or prolonged attacker presence on affected systems, rather than a single, isolated infection.

The detection names shown in the tables include a mix of:

- **Behavior-based EDR detection**s, mapped to attacker techniques (for example, discovery, process injection, masquerading or remote execution).
- **Malware and trojan classifications,** including generic and family-level signatures.
- **Script and PowerShell-related detections**, commonly associated with living-off-the-land and fileless attack techniques.

Because Acronis EDR / XDR emphasizes behavioral and post-compromise visibility, many of the leading detections reflect attacker actions after initial access, such as internal reconnaissance, credential-related activity, lateral movement, evasion and persistence. As a result, the tables should be interpreted as an indicator of how attackers operate within environments, not only how they initially gain access.

Each country's table is followed by a qualitative interpretation that focuses on dominant attack trends and techniques, helping contextualize the raw detection volumes and highlight regional differences in attacker behavior and operational focus.

Germany

Germany's detections were overwhelmingly shaped by MSHTA–PowerShell execution chains, with Suspicious.Generic.HTAPS1 / HTAPS2 and multiple MSHTA-spawned PowerShell rules indicating that HTA-based loaders remain a primary entry and staging technique. MSHTA detections refer to security alerts triggered when mshta.exe — a legitimate Windows binary used to execute HTML Application (HTA) files — is abused by attackers as a Living-off-the-Land Binary (LOLBin) to execute malicious code.

HTAPS1 / HTAPS2 detections are classifications used by security engines to identify malicious or suspicious use of HTML Application (HTA)–based scripts, typically executed via mshta.exe, with the numeric suffix indicating severity, confidence or stage of the attack chain. HTAPS1 generally represents early-stage or lower-confidence HTA abuse.

All this points to repeatable playbooks that use native Windows components to bootstrap second stages. The strong presence of Infostealer.LALALA.A signals that many cases move quickly into credential theft and persistence, consistent with monetization and / or preparation for lateral movement.

Post-compromise evasion is visible through Trojan.RenPWS.A and related EDR detections, where PowerShell (or PowerShell-like execution) is renamed / masked to look legitimate. This is reinforced by Suspicious.Masquerade_PWS_Generic.A, indicating deliberate process masquerading around PowerShell rather than noisy standalone malware. Finally, Trojan.GenericBatRunner.Vbs.A shows the continued use of VBS as a wrapper to run BAT payloads, adding reliability / fallback execution paths.

Overall, Germany reflects mature, script-led intrusion chains that consistently progress into credential theft and evasion.

Threat name	MD5
Suspicious.Generic.HTAPS1	CB5971A176EF0CFD5FC77792E2000558
Trojan.MSHTASpawnedPWS.B	A97E6573B97B44C96122BFA543A82EA1
Suspicious.Generic.HTAPS2	909A2EEC5534F01DFF87B7D47E57BFF7
Infostealer.LALALA.A	B8ED3F707000C22AEE6BBF961879EA99
Malicious.MshtaSpawnedPowershell.A	CB5971A176EF0CFD5FC77792E2000558
Trojan.MSHTA_SpawnedPWS.B	9D8E30DAF21108092D5980C931876B7E
Trojan.RenPWS.A	097CE5761C89434367598B34FE32893B
EDR:Suspicious.Masquerade_PWS_Generic.A	097CE5761C89434367598B34FE32893B
EDR:Trojan.RenPWS.A	097CE5761C89434367598B34FE32893B
Trojan.GenericBatRunner.Vbs.A	CE5AB0E53E0877BD574CD2583AD5A01B

Japan

Japan is dominated by script-host scheduling and scripting abuse, led by Trojan.GenericSCH.Wscript.A, which indicates scripted persistence / execution via wscript and scheduled-task style patterns. A distinctive element is AMSI.Suspicious.PowerShellKeyloggingActivity.T1056, implying PowerShell activity associated with keylogging behaviors detected through AMSI telemetry. Initial access is also visible: ML:Generic.MaliciousDoc suggests malicious documents remain a meaningful delivery channel. Japan also shows selective enterprise tradecraft: Suspicious.ImpackectCmdSMBexec.A points to SMB command execution consistent with Impacket-style lateral movement.

Two detections stood out for outcome and data movement: SFS:PUA.NiceHashMiner.A reflected cryptomining PUA activity (monetization), and CurlPostArchiveToInternet indicates archived data being posted outward using curl (exfil-style behavior). The presence of Suspicious.Generic.T1055.012 showed injection / memory manipulation is present but not the dominant theme.

Japan's pattern was operationally "script-first" (wscript + PowerShell), with keylogging signal, occasional SMB execution and a mix of exfil / monetization.

Threat name	MD5
Trojan.GenericSCH.Wscript.A	3F859AA82A01F6F62D4608DCCB6B3078
EDR:AMSI.Suspicious.PowerShellKeyloggingActivity.T1056	39288D0C371353CD7FC10F68F39407D4
EDR:Suspicious.ImpackectCmdSMBexec.A	BF93A2F9901E9B3DFCA8A7982F4A9868
EDR:Trojan.GenericSCH.Wscript.A	FA94A8411B9F4A3806B7E66135A870D1
ML:Generic.MaliciousDoc	8010F08D5466F8B94724EF2B2633DA14
SFS:PUA.NiceHashMiner.A	E6D51CC17C842426A5EDFAC1BADE5387
EDR:Suspicious.Generic.T1055.012	C317B7CA43C5B70C94BAEF9E529F82D4
EDR:AP.Suspicious.Trojan.Generic.T1486.DELETE_FULL_READ	DAD69304585AA6445EE6181485A2FED1
SFS:Trojan.Generic.4532159	E3ADC55FBF4DD5B006E17E623341ECC1
EDR:CurlPostArchiveToInternet	2538C12B71F10C2FCCB45CB7200DB15B

Canada

Canada showed a classic “commodity malware into post-exploitation” trajectory. Trojan.Emotet.G indicated widespread Emotet activity (established loader/ecosystem), while RAT.RemCosRat.D adds clear remote-access capability in many incidents. Post-compromise discovery/credential access is evidenced by Suspicious.Netsh_Wlan_Password_Dump.1555, which specifically covers netsh-based Wi-Fi password dumping.

Lateral movement was explicit: Suspicious.ImpackectCmdSMBexec.A indicated SMB command execution consistent with Impacket tooling. Execution stealth was also present: Injector.Generic.M / MP represent injection patterns using remote thread / context techniques (the file described injection flows with SetThreadContext/ETW patterns across variants). Canada additionally showed credential / value targeting: Infostealer.GenericCryptowallet.A pointed to cryptowallet enumeration and sensitive path access.

The presence of EDR:Suspicious.Rundll32DllregisterServer.T1218 indicated living-off-the-land execution via rundll32 dllregisterserver behavior.

Overall, infections in Canada commonly have begun with known malware families and then mature into credential access, lateral execution and injection-based payload staging.

Threat name	MD5
Trojan.Emotet.G	82A925CB317C39042521C693EB0D09A2
RAT.RemCosRat.D	62D09F076E6E0240548C2F837536A46A
EDR:Suspicious.Netsh_Wlan_Password_Dump.1555	9D8E30DAF21108092D5980C931876B7E
EDR:Suspicious.ImpackectCmdSMBexec.A	FE48494F2B5A9C452F12E9BBE93A6BE6
Injector.Generic.M	62D09F076E6E0240548C2F837536A46A
Injector.Generic.MP	596CBA7B6CBE273E58E9A39DE9778B9F
Trojan.PWSInjectorNetFrameWorks.C1	A97E6573B97B44C96122BFA543A82EA1
ML:Generic.MaliciousDoc	A2DA0AEDC6D8FFA0207E750E6772CCCF
Infostealer.GenericCryptowallet.A	F8E68D6ABE411CE0C71D6B8C1C1B9048
EDR:Suspicious.Rundll32DllregisterServer.T1218	2FAFAA93AA691553B5303616A6044A42

South Korea

South Korea was strongly characterized by PowerShell-based download and obfuscation, led by Trojan.DownloadStringPowershellEncoded Command.A, which detected encoded-command downloadstring activity typical of fileless delivery. Trojan.Generic.HTA added a clear HTA execution component, reinforcing script-led initial stages.

Post-access execution breadth was visible through Trojan.WMIExecution.A, indicating WMI command execution with HTTP downloads via cmd / PowerShell.

Injection was present via Suspicious.Generic. T1055.002, aligning with process injection behavior rather than purely script-only chains.

There was also a clear opportunistic monetization layer: SFS:PUA.XMRigMiner.A indicates XMRig miner PUA activity.

Taken together, the country profile is “near-fileless by design”: encoded PowerShell delivery + HTA/WMI execution, with selective injection and opportunistic mining in the mix.

Threat name	MD5
Trojan.DownloadStringPowershellEncodedCommand.A	852D67A27E454BD389FA7F02A8CBE23F
Trojan.Generic.HTA	5746BD7E255DD6A8AFA06F7C42C1BA41
EDR:Suspicious.Generic.T1055.002	158D28E569B408E3ABC9E368BCD2DEC0
Trojan.WMIExecution.A	F5AE03DE0AD60F5B17B82F2CD68402FE
SFS:Trojan.Generic.31952689	03E0579C582E9AB6EDF03EA483A5435F
SFS:Win32.Floxif.A	B8C909CF240FFD6BED71062236FC4133
Malware.BundloreX.H2	0A8AE8636DA060FAE846958D66FD3841
EDR:Malware.BundloreX.H2	2A6D92A9C97249C91F78192FD801EAC2
SFS:PUA.XMRigMiner.A	2A0D26B8B02BB2D17994D2A9A38D61DB
Trojan.Generic.557a040b	4AF4C15092110057CB0A97DF626C4EF4

Australia

Australia showed a consistent progression from initial access to internal reconnaissance and exfil, rather than only malware delivery. Suspicious.Generic.T1087_002 is a direct indicator of account discovery/enumeration activity. Lateral execution was visible via Suspicious.ImpackectCmdSMBexec.A, consistent with SMB remote command execution using Impacket-like methods. Entry vectors remained present: ML:Generic.MaliciousDoc indicated document-based delivery was still common.

Payload staging and runtime tradecraft appear via Trojan.MalURL.Powershell.A (malicious URLs in PowerShell) and Trojan.PWSInjectorNetFrameWorks.A plus Injector.Generic.R, reflecting PowerShell / injection-assisted execution stages. Two detections were particularly telling for hands-on outcomes: Dropper.ScreenConnect.A suggests ScreenConnect-style remote admin dropper activity, and Suspicious.RcloneExfiltration.RenamedRcloneExecution indicated renamed rclone used for exfiltration.

Australia's pattern was fewer events, but many reached discovery, remote execution and exfiltration staging.

Threat name	MD5
EDR:Suspicious.Generic.T1087_002	097CE5761C89434367598B34FE32893B
EDR:Suspicious.ImpackectCmdSMBexec.A	5A6BE4D2519515241D0C133A26CF62C0
ML:Generic.MaliciousDoc	ECF81DA628C8448133A97E67450A58BE
Trojan.MalURL.Powershell.A	9D8E30DAF21108092D5980C931876B7E
Injector.Generic.R	9D8E30DAF21108092D5980C931876B7E
Trojan.PWSInjectorNetFrameWorks.A	9D8E30DAF21108092D5980C931876B7E
SFS:Win32.Grenam.A	4BC0EB7313A25A611CF5751A22A76EBE
SFS:PUA.NiceHashMiner.A	E6D51CC17C842426A5EDFAC1BADE5387
Dropper.ScreenConnect.A	852EE5587D6CB0B8B17E981FE84A31D4
EDR:Suspicious.RcloneExfiltration. RenamedRcloneExecution	2B40C98ED0F7A1D3B091A3E8353132DC

France

France was dominated by cryptomining and intrusion tooling appearing side-by-side. Trojan.Cryptominer.C plus Linux.XMRigEmbed.A and PUP-CryptoMiner_21 point to large-scale cryptomining outcomes across Windows and Linux. At the same time, France showed strong enterprise post-exploitation signals: Suspicious.ImpackectCmdSMBexec.A indicated SMB execution / lateral movement, and Suspicious.OS.Credential.Dumping.Ntds.SAM.T1003.003 indicated credential dumping involving NTDS / SAM copying.

Execution and staging were reinforced by Trojan.MalURL.Powershell.A and Trojan.PWSInjectorNetFrameWorks.B plus Injector.Generic.R, indicating PowerShell delivery combined with injection-assisted runtime behavior.

Finally, AP.Suspicious.Trojan.Generic.T1486.WRITE_OFFSET indicated ransomware-like write behaviors (file writes at offsets) appearing in the environment, suggesting some compromises were moving toward destructive / monetization endpoints beyond mining.

Overall, France reflected both opportunistic cryptomining at scale and a meaningful layer of intrusion-grade tradecraft.

Threat name	MD5
Trojan.Cryptominer.C	BD542C1197F3B5217B5C5B5C4A25BD0C
EDR:Suspicious.ImpackectCmdSMBexec.A	2B40C98ED0F7A1D3B091A3E8353132DC
Trojan.MalURL.Powershell.A	909A2EEC5534F01DFF87B7D47E57BFF7
SFS:Linux.XMRigEmbed.A	BF8E5B056184A37D8E5BBD247473F8CA
Trojan.RenPWS.A	7353F60B1739074EB17C5F4DDDEFE239
Injector.Generic.R	A97E6573B97B44C96122BFA543A82EA1
Trojan.PWSInjectorNetFrameWorks.B	2E5A8590CF6848968FC23DE3FA1E25F1
EDR:Suspicious.OS.Credential.Dumping.Ntds.SAM.T1003.003	8A478ED65D29A427D54C5854F2331F9B
EDR:PUP-CryptoMiner_21	055EAEC478C4A8490041B8FA3DB1119D
EDR:AP.Suspicious.Trojan.Generic.T1486.WRITE_OFFSET	5E1A7ACD2828DD3A9CA0792784EF5AE8

U.S.

The U.S. showed the broadest end-to-end intrusion footprint. Trojan.MimikatzLoader.A was a direct indicator of credential theft tooling (Mimikatz loader). Massive volumes of Suspicious.Generic.PSOC2 / PSOC3 indicated heavy use of PowerShell obfuscation using character and byte-escape techniques. This behavior is consistent with fileless delivery and defense evasion.

Injection was central via Injector.Generic.R, and scripted persistence / execution appeared via Trojan.GenericSCH.Wscript.A. Lateral movement was explicit through Suspicious.ImpackectCmdSMBexec.A, while remote control capability was reflected by Trojan.AsyncRat.D (AsyncRAT).

Finally, the appearance of MitreEval.Linux.ChmodAddSuid.1 suggested Linux privilege escalation mechanics (adding SUID bit) were also represented, reinforcing that U.S. environments are seeing cross-platform attacker behaviors.

Overall, the U.S. profile reflected full-spectrum intrusion activity: credential theft, obfuscation, injection, persistence, lateral execution and cross-platform post exploitation.

Threat name	MD5
Trojan.MimikatzLoader.A	6BB54B2D7A3D63578559239A79700EA3
Suspicious.Generic.PSOC3	2E5A8590CF6848968FC23DE3FA1E25F1
Suspicious.Generic.PSOC2	2E5A8590CF6848968FC23DE3FA1E25F1
Injector.Generic.R	BD542C1197F3B5217B5C5B5C4A25BD0C
Trojan.GenericSCH.Wscript.A	C23ABA633C8C7B1715E591E2DC3D1AEF
Trojan.PWSInjectorNetFrameWorks.B	2E5A8590CF6848968FC23DE3FA1E25F1
EDR:Suspicious.ImpackectCmdSMBexec.A	F0DEE540C8FCC20E2F885D4F9ADC42C2
Trojan.AsyncRat.D	BD542C1197F3B5217B5C5B5C4A25BD0C
EDR:MitreEval.Linux.ChmodAddSuid.1	D7BC3CE3B6B7AC53BA2918A97D806418
Trojan.PWSInjectorNetFrameWorks.A	2E5A8590CF6848968FC23DE3FA1E25F1

New Zealand

New Zealand was led by visible initial access and a lighter — but present — post-exploitation layer. ML:Generic.MaliciousDoc indicated document-borne delivery was a primary driver.

Win32.Neshta suggested classic file infection activity appeared in the dataset, while Suspicious.Generic.SMSH indicates suspicious shell modification behaviors post compromise. There were also ransomware-adjacent signals: AP.Suspicious.Trojan.Generic. T1486.DELETE_FULL_READ points to file deletion / full read behaviors associated with ransomware operations.

Remote tooling appeared but at modest scale: PUA.ConnectWise.A indicates ConnectWise PUA presence, and a generic infostealer variant was also present (Infostealer.Generic.9e6270f1).

Persistence and deeper tradecraft exist but were less dominant: T1547_002 (run keys) and T1055.002/.003 (injection / thread hijacking) showed up at low volumes, and AMSI suspicious T1070.001 suggests some PowerShell evasion / anti-forensics patterns.

In summary, phishing- and document-led compromise was most visible, with selective escalation into persistence, injection and ransomware-like behaviors.

Threat name	MD5
ML:Generic.MaliciousDoc	E49604DBFF32FA055F55F35F22751E70
SFS:Win32.Neshta.A	38B6564889AC3BD1654140F3790A21AF
EDR:Suspicious.Generic.SMSH	4994004209606F427D66D97035247064
EDR:AP.Suspicious.Trojan.Generic.T1486.DELETE_FULL_READ	805DA6B86137E6439B0928453D72930E
SFS:PUA.ConnectWise.A	ABEB46D054C60313162ED8AA4B7CA6EC
Infostealer.Generic.9e6270f1	B585A0B86DEA3821EAEE0EA7ECED2747
EDR:Suspicious.Generic.T1055.003	EB1071A4D69294F036D40D1FBF61C375
EDR:Suspicious.Generic.T1547_002	FAA90DD7AF5633802F27756D367D3D44
EDR:Suspicious.Generic.T1055.002	2A2562ABC95E695EAB3EEFFBE16EAD5F
EDR:AMSI.Suspicious.Generic.T1070.001_Powershell_2	44413FAFC3FC7BDFDDFEFCC305609454

U.K.

The U.K. detection set reflected true cross-platform intrusion activity, combining macOS malware execution with advanced Windows post exploitation. The prominence of Malware.OSX.Generic.A9 confirmed active macOS endpoint targeting rather than incidental noise, indicating attackers were deliberately operating across heterogeneous environments.

On Windows systems, AMSI.Suspicious.PowerShellKeyloggingActivity.T1056 highlighted PowerShell-based keylogging detected through AMSI telemetry, signalling credential interception via script tooling rather than standalone keyloggers. PowerShell obfuscation was reinforced by Suspicious.Generic.PSOC3, which detected byte-escape obfuscation techniques used to evade static and AMSI inspection.

Post-access execution stealth is further visible through Suspicious.Generic.T1055.012, indicating process injection or memory manipulation.

Initial access remained present via ML:Generic.MaliciousDoc and Trojan.LNK.Padded.A, confirming document- and shortcut-based delivery. The appearance of LNK.RenamedAutoITCompiler.A shows execution masquerading via renamed AutoIT tooling.

Overall, the U.K. profile reflected multi-OS, script-enabled intrusions, where attackers combined macOS footholds with Windows credential theft and injection.

Threat name	MD5
Malware.OSX.Generic.A9	ABF8B7B3E2F1BAF1AD318D9E9E8A33F4
EDR:AMSI.Suspicious.PowerShellKeyloggingActivity.T1056	6BB54B2D7A3D63578559239A79700EA3
PUA.TNTCrack.A1	BE699E18C03B55C3E833F1ECD7FD158A
SFS:Win32.Neshta.A	C661B3C0F754F0FBB03F440864282387
ML:Generic.MaliciousDoc	1F5E9665863131A4C5BC606E55F6AE36
EDR:Suspicious.Generic.T1055.012	0CF09BB7D4935FB66B3CA5A0FD6EBC27
Suspicious.Generic.PSOC3	2E5A8590CF6848968FC23DE3FA1E25F1
SFS:Trojan.LNK.Padded.A	AD34BEDDEB943ADC1F99A90B618CBA21
SFS:LNK.RenamedAutoITCompiler.A	B2839A677A24E7C6F6D70EA4EC1A31EB
EDR:AMSI.Suspicious.Generic.T1070.001_Powershell_2	9D8E30DAF21108092D5980C931876B7E

Italy

Italy's detections were strongly driven by lateral movement and execution masquerading. The dominance of Suspicious.ImpackectCmdSMBexec.A confirmed frequent SMB-based remote command execution using Impacket tooling that indicated attackers commonly operated post compromise with valid credentials. A major secondary theme was AutoIT abuse, visible through Trojan.RenamedAutoITSignedProcess.A and Suspicious.RenamedAutoITSignedProcess.A, which detected renamed signed AutoIT binaries used to evade allowlisting.

This was paired with Trojan.DllSideLoading.C, indicating DLL sideloading via trusted executables. Persistence and evasion were reinforced by Suspicious.Generic.T1564_003, which could detect hidden files or directories.

Initial access remained script driven, with Suspicious.Generic.HTAPS1 / HTAPS2 confirming MSHTA-spawned PowerShell execution. Trojan.PSDownloadString.A further confirmed PowerShell download-string delivery.

Italy reflected credential-enabled intrusions, where trusted tooling abuse and lateral spread dominated.

Threat name	MD5
EDR:Suspicious.ImpackectCmdSMBexec.A	BF93A2F9901E9B3DFCA8A7982F4A9868
Trojan.RenamedAutoITSignedProcess.A	C56B5F0201A3B3DE53E561FE76912BFD
Trojan.DllSideLoading.C	C56B5F0201A3B3DE53E561FE76912BFD
Suspicious.RenamedAutoITSignedProcess.A	C56B5F0201A3B3DE53E561FE76912BFD
Injector.Generic.R	9D8E30DAF21108092D5980C931876B7E
EDR:Suspicious.Generic.T1564_003	29602B687189BE90101617B8CA737419
Suspicious.Generic.HTAPS1	86F05E66502036DB5B678B917E5D5B17
Suspicious.Generic.HTAPS2	2E5A8590CF6848968FC23DE3FA1E25F1
Trojan.PSDownloadString.A	9D8E30DAF21108092D5980C931876B7E
Trojan.GenericSCH.Wscript.A	3F859AA82A01F6F62D4608DCCB6B3078

Singapore

Singapore's activity was defined by stealth-first, injection-heavy execution, consistent with attackers adapting to mature defensive environments. Multiple Injector.Generic variants (F1, G, R, K) indicated repeated in-memory injection across different execution flows rather than reliance on disk-resident payloads. Execution masquerading was reinforced by SvchostProcessTyposquatting, which detected typosquatted svchost processes used to blend malicious activity into legitimate system services.

Data handling and staging were unusually prominent: Suspicious.Compression.Activity detected bulk file compression in user directories, while LinuxSensitiveFilesArchived.P.3.NotSys indicated archiving of sensitive Linux files outside system paths.

Commodity malware still appeared — Malware.FormBook.E and Malware.NanoCore.B confirmed credential theft and RAT functionality — but clearly within broader intrusion chains. The presence of Trojan.Snake.A added a strong persistence-focused signal.

Singapore reflected low-noise, post-compromise operations, optimized for stealth and data access.

Threat name	MD5
Injector.Generic.F1	9E66D005C6BE3AD054309F7FC4F27458
EDR:Suspicious.Compression.Activity	210C0CB186955620494F9DF28F403A07
Injector.Generic.G	ABD8BFA34BC73E1DE106F2C6B172B0CD
Injector.Generic.R	ABD8BFA34BC73E1DE106F2C6B172B0CD
EDR:LinuxSensitiveFilesArchived.P.3.NotSys	B750DD56C702D2CBFC78040E818AE598
Injector.Generic.K	ABD8BFA34BC73E1DE106F2C6B172B0CD
EDR:SvchostProcessTyposquatting	D37D0E14DA679564BBEA624CDB61E2C5
Trojan.Snake.A	555ABB74B0B3FD5F7B855BFF558338B4
Malware.NanoCore.B	0859B8C36A12546022FD3436DB822D83
Malware.FormBook.E	E14E8AF8B219F2DE750410E5604F7005

Mexico

Mexico's detections consistently pointed to credential-driven post-compromise exploitation. Suspicious.ImpackectCmdSMBexec.A dominated, confirming extensive SMB-based remote execution using Impacket. PowerShell obfuscation is a major theme, with Suspicious. Generic.PSOC1 / PSOC2 detecting string concatenation and char-escape obfuscation used to hide script logic.

Execution masquerading was visible via Trojan.RenamedAutoITSignedProcess.A and LNK.RenamedAutoITCompiler.A, showing abuse of trusted AutoIT tooling. Trojan. FakeWindowsProcess_SPOOLSV.A confirmed impersonation of critical Windows services for stealth. Trojan.MalURL. Powershell.A reinforced PowerShell-based payload retrieval.

Mexico's profile reflected hands-on-keyboard intrusions, where valid access was leveraged aggressively for internal movement.

Threat name	MD5
EDR:Suspicious.ImpackectCmdSMBexec.A	FE48494F2B5A9C452F12E9BBE93A6BE6
Suspicious.Generic.PSOC1	2E5A8590CF6848968FC23DE3FA1E25F1
SFS:LNK.RenamedAutoITCompiler.A	8D7506701FF1EE2110AD56C0C54CD542
Suspicious.Generic.PSOC2	2E5A8590CF6848968FC23DE3FA1E25F1
SFS:Trojan.Agent.ERJ	7574CF2C64F35161AB1292E2F532AABF
EDR:Suspicious.Generic.PSOC2	0E9CCD796E251916133392539572A374
Trojan.RenamedAutoITSignedProcess.A	0ADB9B817F1DF7807576C2D7068DD931
EDR:Generic.Suspicious.P.SCAR	882CB5EC995B5B7EDBE631D7C0B93210
Trojan.MalURL.Powershell.A	6BB54B2D7A3D63578559239A79700EA3
Trojan.FakeWindowsProcess_SPOOLSV.A	E82A518FD23E3FBFDF11203344C1947D

India

India exhibited extreme-scale evasion and post-compromise activity. The overwhelming dominance of Trojan.MimicCriticalProcess.M / G indicated systematic impersonation of critical Windows processes to hide execution.

Defense suppression is explicit through SFS:Trojan.KillAV.A, confirming malware designed to disable endpoint protection. Script-based execution and persistence remain core, with Trojan.GenericSCH.Wscript.A appearing in both EDR and non-EDR variants. Credential and value theft are visible via Infostealer.

Kryptik.91524c8c and Trojan.Kryptik.e9c7751f, alongside Trojan.Miner.T cryptomining activity. Win32.Neshta indicated file-infecting malware spreading execution further.

India reflected high-volume, persistence- and evasion-centric attacks, optimized for long-term exploitation.

Threat name	MD5
Trojan.MimicCriticalProcess.M	C2DF05D287C648D598A8FE26DB59E20B
Trojan.MimicCriticalProcess.G	1C5161E2267CCBF613D6A40A653788B7
Trojan.Miner.T	F908F69FED49C82DA2B2E6554D304E78
Infostealer.Kryptik.91524c8c	08A9A3A35B606A9714E7B835D9F0FB7F
SFS:Trojan.KillAV.A	B306B59F97399C33432423137A5910DE
EDR:Trojan.GenericSCH.Wscript.A	1BC87886C5D8A35A7D6F00C5A4CF2576
Trojan.GenericSCH.Wscript.A	1BC87886C5D8A35A7D6F00C5A4CF2576
SFS:Win32.Neshta.A	142A5FD4814C612C8A32021CDD2C36E9
EDR:AP.Suspicious.Trojan.Generic.T1486.DELETE_FULL_READ	D91D31DF87E8C4AE6822C962CB8B8F69
Trojan.Kryptik.e9c7751f	D7EE8E95229529AC5BA90CB15A7564B9

Colombia

Colombia's detections showed a repeatable intrusion workflow centered on scripting and remote execution. Suspicious.ImpackectCmdSMBexec.A again dominated, confirming routine SMB-based lateral execution.

Scripted persistence is reinforced by Trojan.PWS_GenericSCH.A and its EDR counterpart, indicating scheduled PowerShell execution. Initial access remained visible through Trojan.GenericSCH.Wscript.A and Trojan.MalURL.Script.A, confirming script-host delivery.

Injection and fileless execution appeared via Trojan.PSReflectionGeneric.B and AMSI.Trojan.ReflectiveCodeLoading.A, indicating reflective code loading in PowerShell. RAT.Remcos.A added explicit remote-control capability.

Colombia reflected structured, repeatable intrusion playbooks rather than random malware spread.

Threat name	MD5
EDR:Suspicious.ImpackectCmdSMBexec.A	FE48494F2B5A9C452F12E9BBE93A6BE6
Trojan.PWS_GenericSCH.A	2E5A8590CF6848968FC23DE3FA1E25F1
EDR:Trojan.PWS_GenericSCH.A	2E5A8590CF6848968FC23DE3FA1E25F1
Trojan.GenericSCH.Wscript.A	A47CBE969EA935BDD3AB568BB126BC80
EDR:Trojan.GenericSCH.Wscript.A	FA94A8411B9F4A3806B7E66135A870D1
SFS:RAT.Remcos.A	2AC1F767464660CD6A902BCED0FAEBE5
Trojan.MalURL.Script.A	1BC87886C5D8A35A7D6F00C5A4CF2576
Trojan.PSReflectionGeneric.B	BD542C1197F3B5217B5C5B5C4A25BD0C
AMSI.Trojan.ReflectiveCodeLoading.A	BD542C1197F3B5217B5C5B5C4A25BD0C
Trojan.DllSideLoading.B	0F00C8B026148991862BE9F30CFC609E

Brazil

Brazil was defined by evasion through trust abuse at scale. Masquerade_VulnerableDllSideloadingExe.T1036 and Trojan.DllSideLoading.C confirmed widespread DLL sideloading via trusted executables. Massive volumes of RenamedAutoITSignedProcess detections highlighted systematic AutoIT masquerading.

Trojan.FakeWindowsProcess_SPOOLSV.A and Masquerade_Autoit_Process.A confirmed impersonation of critical system processes. Suspicious.ImpackectCmdSMBexec.A showed these evasion techniques were paired with lateral movement. Scripted persistence remained present via Trojan.GenericSCH.Wscript.A.

Brazil reflected large-scale masquerading-driven intrusions, optimized to bypass trust-based controls.

Threat name	MD5
EDR:Suspicious.Masquerade_VulnerableDllSideloadingExe.T1036	0ADB9B817F1DF7807576C2D7068DD931
Trojan.RenamedAutoITSignedProcess.A	C56B5F0201A3B3DE53E561FE76912BFD
Trojan.DllSideLoading.C	C56B5F0201A3B3DE53E561FE76912BFD
Trojan.FakeWindowsProcess_SPOOLSV.A	E388E2E057A19BF898EB2C208154B8A6
EDR:Suspicious.Masquerade_Autoit_Process.A	C56B5F0201A3B3DE53E561FE76912BFD
EDR:Trojan.RenamedAutoITSignedProcess.A	279274F8A137BF31425A9C2C14444B66
EDR:Suspicious.ImpackectCmdSMBexec.A	2B40C98ED0F7A1D3B091A3E8353132DC
Trojan.GenericSCH.Wscript.A	596CBA7B6CBE273E58E9A39DE9778B9F
Trojan.MimicCriticalProcess.O	E79ED9E70FBC22A54BC9F4B573EEDC18
Trojan.FakeAutoIt.C	C56B5F0201A3B3DE53E561FE76912BFD

Netherlands

The Netherlands showed a PowerShell-centric intrusion profile. Trojan.RenPWS.A indicated a renamed PowerShell execution used for evasion. This was reinforced by Suspicious.Generic.PSOC1 / PSOC3, that confirmed heavy use of PowerShell obfuscation techniques.

Trojan.DownloadStringPowershellEncoded Command.A confirmed encoded PowerShell downloadstring delivery. Initial access remained visible via ML:Generic.MaliciousDoc and Trojan.LNK.Padded.A. Injection via T1055.003 and remote admin tooling (Application.RemoteAdmin.Ammy.A) appeared at lower volumes, indicating selective escalation.

The Netherlands reflected script-driven intrusions, with PowerShell as the central execution and evasion mechanism.

Threat name	MD5
Trojan.RenPWS.A	097CE5761C89434367598B34FE32893B
Suspicious.Generic.PSOC1	BD542C1197F3B5217B5C5B5C4A25BD0C
Suspicious.Generic.PSOC3	909A2EEC5534F01DFF87B7D47E57BFF7
SFS:Trojan.Generic.37940051	69F21DAE932751BC4160B40302197BE3
Trojan.DownloadStringPowershellEncodedCommand.A	F4F684066175B77E0C3A000549D2922C
ML:Generic.MaliciousDoc	FD382AD9FABB96076C2E33FAD274CD4F
EDR:Suspicious.Generic.T1055.003	FC01B4963B10D5D1A4812184B0998E8F
SFS:Application.RemoteAdmin.Ammy.A	90AADF2247149996AE443E2C82AF3730
SFS:Trojan.LNK.Padded.A	647053CF585CDCD8509A8426126141DD
SFS:Win32.Neshta.A	0E0868A4024A353B4F58633FBB391E49

Overall strategic takeaway

Across all focus countries, the 2025 EDR / XDR data consistently showed that post-compromise behavior dominated detections, not just initial malware delivery. Living-off-the-land techniques (PowerShell, WMI, SMB exec, injection) were pervasive. Attackers increasingly prioritized stealth, masquerading and persistence.

Evolving initial access and trust abuse across the malware delivery ecosystem

Throughout 2025, TRU documented how threat actors were refining initial access techniques by blending social engineering, trusted tooling abuse and delivery chain hardening. Together, these campaigns reflected a shift from vulnerability exploitation to user-assisted execution, where attackers relied on deception and trusted mechanisms rather than technical exploits. Malware is delivered through coerced command execution, legitimate RMM software or signed installers, pushing detection efforts toward execution context, tool misuse and post execution behavior instead of exploit based indicators.

ClickFix[20] and FileFix[21] marked a notable escalation in user-assisted execution techniques. For the first time, TRU observed FileFix deployed at scale beyond proof of concept activity, including the use of steganography to hide PowerShell loaders and encrypted executables inside image files. This represents a new level of delivery chain hardening for *Fix-style attacks. ClickFix activity also evolved, introducing highly realistic, full screen Windows Update lures designed to create urgency and guide victims through command execution. A new operational pattern emerged where a single ClickFix interaction resulted in the deployment of multiple stealer families, demonstrating a shift toward maximizing payload delivery per infection rather than single malware installs.

Trojanized ScreenConnect installers[22] highlighted the continued abuse of legitimate RMM software as a primary foothold rather than a post compromise tool. TRU observed threat actors distributing malicious ScreenConnect installers, particularly via ClickOnce runners, to establish interactive access and automate secondary payload deployment. Once installed, ScreenConnect was used to push multiple RAT families and custom PowerShell tooling, with persistence established through scheduled tasks and script-based loaders. This abuse model allows attackers to blend into legitimate IT activity, delay follow on actions, and operate with reduced visibility, reinforcing RMM misuse as a durable and scalable initial access vector.

Modern malware delivery increasingly prioritizes coercion, perceived legitimacy and operational stealth.

TamperedChef campaigns[23] revealed further industrialization of trust abuse at the delivery layer. While signed malware is not new, TRU documented the systematic use of shell companies to repeatedly obtain and rotate legitimate code signing certificates, including Extended Validation certificates, at scale. This allowed attackers to distribute trojanized installers that appeared indistinguishable from legitimate software and to maintain trust even after certificate revocations. The campaign demonstrated a supply chain adjacent threat model in which attackers did not need to compromise vendors to abuse the same trust mechanisms used by legitimate software distribution.

Taken together, these cases have shown that modern malware delivery increasingly prioritizes coercion, perceived legitimacy and operational stealth. For researchers and defenders, the key takeaway is the growing importance of monitoring how software is introduced and executed, how trusted tools and signatures are abused, and what behaviors follow initial execution, rather than relying primarily on exploit detection or file reputation alone.

[20] Acronis Threat Research Unit. "Fake adult websites pop realistic Windows Update screen to deliver stealers via ClickFix." Acronis. November 25, 2025. https://www.acronis.com/en/tru/posts/fake-adult-websites-pop-realistic-windows-update-screen-to-deliver-stealers-via-clickfix/

[21] Acronis Threat Research Unit. "FileFix in the wild! New FileFix campaign goes beyond POC and leverages steganography." Acronis. September 16, 2025. https://www.acronis.com/en/tru/posts/filefix-in-the-wild-new-filefix-campaign-goes-beyond-poc-and-leverages-steganography/

[22] Acronis Threat Research Unit. "Trojanized ScreenConnect installers evolve, dropping multiple RATs on a single machine." Acronis. September 3, 2025. https://www.acronis.com/en/tru/posts/trojanized-screenconnect-installers-evolve-dropping-multiple-rats-on-a-single-machine/

[23] Acronis Threat Research Unit. "Cooking up trouble: How TamperedChef uses signed apps to deliver stealthy payloads." Acronis. November 19, 2025. https://www.acronis.com/en/tru/posts/cooking-up-trouble-how-tamperedchef-uses-signed-apps-to-deliver-stealthy-payloads/

Ransomware landscape in 2025

The Acronis telemetry data for 2025 has shown significant disparity in ransomware pressure across countries, even after normalizing by endpoint count. This highlighted that ransomware activity is driven less by sheer market size and more by attacker focus, regional exposure and defensive maturity.

Germany consistently recorded the highest ransomware rates among all focus countries, ranging roughly 13–27 detections per 10,000 endpoints, with a clear escalation in the middle of the year. This positioned Germany as the most persistently targeted market in this dataset. This disparity existed because ransomware groups target where returns are highest, not where markets are largest, and Germany offered a consistently attractive balance of economic value and exploitable exposure. Its dense base of midsize industrial, health care and public-sector organizations created high disruption pressure and stronger ransom leverage compared to smaller or more mature markets.

At the same time, many German organizations ran complex hybrid and legacy environments with uneven patching and security maturity, making lateral movement and privilege escalation more achievable. Even when normalized by endpoint count, the elevated detection rate reflected deliberate, sustained targeting, which positioned Germany as a strategic ransomware focus rather than a victim of scale alone.

South Korea stood out for its volatility, with sharp spikes reaching above 20 detections per 10,000 endpoints in some months. This pattern suggested episodic, campaign-driven ransomware activity rather than steady background noise. Japan showed a sustained upward trend, moving from low single-digit values early in the year to double-digit levels (≈12–14) later on, indicating increasing attacker interest.

Canada also operated in the upper-mid tier, with values commonly between 7 and 11, reflecting stable but nontrivial ransomware exposure. The United States sat in a moderate band, usually around 4–7 detections per 10,000 endpoints. While not leading in normalized impact, the consistency suggested ransomware remains a persistent operational risk.

Australia, the U.K. and France cluster closely together, mostly between 2–6, indicating regular ransomware activity but at materially lower intensity than top-tier targets. New Zealand had noticeable month-to-month swings, including isolated spikes, which may reflect small-sample sensitivity or targeted campaigns.

Italy remained in the lower-mid range, generally around 2–3, with no extreme spikes. Mexico, Singapore, India, Colombia and Brazil consistently recorded very low ransomware rates, often below one detection per 10,000 endpoints. These countries appeared significantly less affected in normalized terms, either due to lower attacker focus, different victim profiles or underrepresentation of high-value ransomware targets.

Overall perspective

Across all 15 countries, a rough cross-country average fell in the mid-single-digit range per 10,000 endpoints, but this average masks a clear two-tier reality:

- A small group of countries (Germany, South Korea, Japan, Canada) experienced disproportionately high ransomware pressure.
- Most other regions operated at an order of magnitude lower exposure.

Ransomware risk is highly concentrated geographically, even after normalization. European and advanced Asian economies dominated the high-exposure group, reinforcing the view that attackers prioritized environments with higher operational disruption and payout potential. Volatility in countries like South Korea and New Zealand indicated campaign-based targeting, not uniform background activity. Low figures in markets such as Singapore and Brazil should not be interpreted as absence of risk, but rather lower relative targeting within this observation window.

From a defensive and MSP perspective, these results reinforce the need for region-specific ransomware readiness, rather than assuming uniform global exposure.

Normalized percentage of global malware detections by focus countries – 2025

Country	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEPT	OCT	NOV	DEC
Germany	14.82	12.49	13.58	13.9	14.38	19.32	17.03	15.83	20.41	26.55	27.11	25.88
South Korea	1.45	10.15	1.45	7.25	10.15	21.75	14.5	8.7	17.4	13.05	23.2	9.92
Japan	4.59	4.66	6.02	6.1	11.83	11.04	12.76	13.27	12.62	14.2	14.56	13.58
Canada	5.73	4.46	7.72	9.55	6.37	8.84	7.33	7.64	7.96	8.92	11.63	12.46
Netherlands	0	1.05	3.79	4	4.42	6.52	7.15	7.99	7.36	8.84	8.63	8.05
U.S.	4.02	3.68	4.25	4.42	3.61	5.35	5.05	4.52	5.2	7.35	6.58	7.12
Australia	3.09	2.55	3.22	3.49	3.62	3.36	5.1	4.97	3.22	4.83	6.04	6.24
New Zealand	2.48	1.24	0	3.72	1.24	2.48	4.96	4.96	4.96	7.44	11.16	4.88
U.K.	2.53	1.6	2.69	2.82	2.57	3.33	2.95	3.62	3.83	4.55	4.38	4.09
France	2.93	2.4	1.76	2.18	1.81	2.29	2.13	2.71	3.03	3.67	3.19	3.45
Italy	1.88	1.65	2.31	1.69	2.31	2.08	2.55	1.88	2.43	3.57	3.37	2.86
Mexico	0.51	1.16	1.03	0.77	1.03	1.28	1.03	1.54	1.41	1.28	0.9	1.38
India	0.37	0.22	0.37	0.74	0.81	0.74	0.59	0.52	1.03	1.03	0.81	1.37
Singapore	0.45	0.57	0.11	0.45	0.34	0.57	0.23	0.23	0.45	0.34	0.34	0.45
Brazil	0.1	0.12	0.24	0.48	0.39	0.39	0.22	0.29	0.24	0.29	0.24	0.26
Colombia	0.16	0.16	0.16	0.33	0.16	0.16	0.08	0.08	0.25	0.16	0	0.4

Malicious URLs

The numbers differ a bit from the H1 2025 report as we continuously improve our telemetry processing methodology, refining it every month and recalculating figures to present the most realistic global picture.

The dataset below represents the percentage of all customers in each country that experienced at least one malicious URL detection during a given month. As such, the figures reflect prevalence and spread of web-based threats across customer populations, not intensity per endpoint. Similar to the malware detection statistics, we normalized the numbers depending on the number of active machines in each country and with at least 150 blocked URLs.

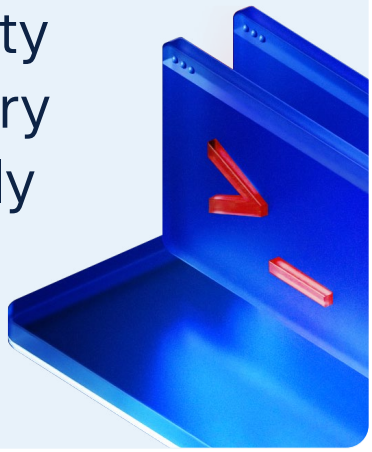
Overall, the data shows wide disparity in URL threat exposure between countries, indicating that attacker focus, browsing behavior and security posture vary significantly by region.

Countries with the highest customer impact

North Macedonia consistently recorded the highest share of affected customers, starting above 21% in January, peaking again above 21% in May–June and remaining in the mid-teens for the rest of the year. This indicates persistent, broad exposure rather than isolated spikes. Sri Lanka showed a clear escalation pattern, rising from around 15% early in the year to over 27% by November, the highest single-month value in the entire dataset. This suggests rapidly increasing exposure across the customer base. Egypt demonstrated sustained high prevalence, frequently ranging between 15% and 21%, with repeated peaks in spring and summer, pointing to ongoing widespread URL-based threats. Vietnam maintained double-digit impact throughout the year, with values often between 13% and 21%, indicating consistently elevated exposure across customers. Croatia, Zimbabwe and Bulgaria also remained in the upper tier, generally between 10% and 15%, with limited seasonal relief.

Month	Percentage of users that clicked on malicious URLs
January	9.24%
February	8.47%
March	9.05%
April	9.14%
May	7.9%
June	8.66%
July	7.36%
August	7.49%
September	7.66%
October	8.19%
November	8.38%
December	8.79%

The data shows wide disparity in URL threat exposure between countries, indicating that attacker focus, browsing behavior and security posture vary significantly by region.



Overall perspective

Across the full telemetry dataset, most countries fell within a 5%–10% monthly affected-customer range, but a distinct top tier regularly exceeds 15%, demonstrating that URL-based threats can reach a large fraction of customers simultaneously in certain regions. Sudden surges (e.g., Israel, Sri Lanka) indicated campaign-driven events capable of rapidly expanding impact.

This reinforces that malicious URL activity is not evenly distributed and often reflects localized campaigns, regional infrastructure differences and user interaction patterns rather than global background noise. Lower percentages do not imply absence of risk, but rather lower relative spread within the customer population. MSPs should prioritize region-specific web protection policies, user awareness and proactive URL filtering based on local threat prevalence, not global averages.

Number of ransomware cases per 10,000 endpoints in focus countries

Country	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEPT	OCT	NOV	DEC
Vietnam	18.1	21.5	17.9	16.2	15.8	19	14.9	13.1	11.8	12.8	18.2	16.6
Peru	12.6	11.4	15.5	14.3	12.5	13.7	11.6	10.8	10.8	12.7	12.7	11.9
Portugal	14.6	14.2	13.2	12.8	11.2	9.7	11.4	10.3	10.9	11.9	10.9	9.5
Hong Kong	10.9	12.9	13.1	10.4	10.6	11.4	11.2	10.6	9.6	10.8	11.1	11.7
United Arab Emirates	12	10.2	12.9	11.5	10.8	10.6	9.1	9.9	9.7	10.2	9.9	8.9
Colombia	11.6	11.6	11.7	10.3	10.8	9.3	9.2	9	9.1	9.6	8.6	8.8
Israel	5.5	4.8	6.3	8.8	6.7	6.8	7.1	6.9	5.9	18.1	21.2	20.6
Poland	7.8	7.9	8.1	12.7	8.2	8.8	9.1	8.3	8.9	11.3	13.5	11
Canada	7.7	7.4	10.1	10.8	8.9	11.1	8.9	8.9	8.8	9.7	9.9	10.7
United States	9.8	8.5	10.7	11.7	8.2	10.2	8.1	8.1	7.7	9	8.6	9.9
Brazil	8.8	8.8	9.4	9	8.6	8.2	8	9.2	10.6	9.5	9.3	8.9
Germany	10.2	9.6	9.8	8.7	8.6	8.8	7.2	7.7	7.3	8	8.8	9.7
India	9	8.5	10.1	8.4	8	8	7.6	8.1	8.7	8.5	7.9	8.6
Spain	8.8	8.6	9.4	7.9	8.2	10.1	7.2	6.1	7.5	9.2	8.7	8.8
New Zealand	9.2	7.5	11.9	9.8	8.2	7.5	6.3	8	7.5	7.3	7.1	7.2

3

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

Threat activity observed in the second half of 2025 confirms that the cybersecurity environment continues to deteriorate in both scale and sophistication. Attackers increasingly rely on trusted platforms, legitimate tools and human interaction rather than overt malware delivery. For MSPs and MSSPs, this evolution is particularly dangerous: A single compromise can rapidly propagate across managed environments, amplifying impact and operational disruption. Addressing this reality requires a unified cyber protection strategy that combines prevention, detection, response and recovery into a single operational platform, reducing complexity while improving resilience.

The following recommendations are grounded primarily in H2 2025 incidents and campaigns highlighted in this report.

Strengthening backup and recovery against modern ransomware operations

In H2 2025 the ransomware threat continued to expand, with ransomware attacks rising sharply compared with the previous year. Groups such as Qilin, Sinobi and Akira drove a reported 50% year-over-year increase in ransomware incidents through October as attackers broadened both their tooling and targets.

React2Shell exploits (CVE-2025-55182) were actively exploited to deliver advanced malware like EtherRAT, demonstrating that adversaries now pair exploitation of high-severity flaws with post-compromise activities that often include backup tampering or deletion.

This underscores that backups cannot simply be a separate data protection function. They must be embedded within a security platform that can detect malicious activity and trigger rapid, automated restoration from immutable, tamper-resistant snapshots. Only tightly integrated backup and recovery, coordinated with detection telemetry, can prevent attackers from undermining recovery while maintaining operational continuity for multiple customers.

Improving detection and prevention for evasive, multistage attacks

Threat actors demonstrated a continued shift toward low-noise, multistage attack chains designed to evade traditional defenses. Campaigns increasingly relied on process injection, script-based execution and legitimate administrative tooling to blend malicious activity into normal system behavior. Rather than deploying a single identifiable payload, attackers staged operations incrementally, delaying detection until access and persistence were firmly established.

Several investigations detailed how attackers combined phishing or collaboration-based lures with subsequent abuse of scripting environments and memory-resident techniques. This approach significantly reduced the effectiveness of signature-based detection and perimeter-only controls. In response, MSPs require layered detection that correlates behavior across endpoints, identities, email and cloud services. Integrated XDR capabilities provide this visibility, enabling faster identification of abnormal activity and reducing dwell time across managed environments.

Enforcing strong identity controls and zero-trust access models

Credential abuse continues to drive a large share of successful breaches. In H2 2025, phishing and social engineering evolved beyond email into messaging platforms with a surge of attacks targeting officials via WhatsApp and Signal, where adversaries impersonated support teams to harvest access codes and linked devices.

For MSPs, this means moving firmly to zero trust access architectures: implement strong password hygiene, enforce multifactor authentication (MFA) universally and continuously monitor access behavior for anomalies. These measures limit the effectiveness of stolen credentials and reduce the likelihood that attackers achieve unauthorized lateral movement within client environments.

Defending against phishing and collaboration platform abuse

One of the most significant developments in H2 2025 was the continued migration of social engineering attacks from email into collaboration platforms. Attackers increasingly abused Microsoft Teams and similar tools to impersonate internal staff, deliver malicious links, and conduct real-time social engineering. These campaigns often bypassed traditional email security controls and relied on user trust in internal communication channels to accelerate compromise.

H2 reporting documented multiple cases in which initial phishing emails served only as a bridge into collaboration-based interactions, after which attackers persuaded users to install remote access tools, disclose credentials or execute malicious commands. This shift highlights the need for security controls that extend beyond email to include collaboration applications, as well as continuous user education focused on interactive social engineering scenarios.

Accelerating patch management for high-risk software and tools

Attackers continue to prioritize exploitation of known vulnerabilities, particularly in remote access software, management tools and widely deployed enterprise applications. Delayed patching remains one of the most reliable pathways to compromise, especially in MSP-managed environments where a single vulnerable component may be deployed across many tenants.

Recent incidents demonstrated how quickly newly disclosed vulnerabilities were weaponized, often within days of public disclosure. With almost 3,000 critical vulnerabilities discovered in 2025, this is a huge threat. This reinforces the need for automated, risk-based patch management that prioritizes exposed and high-impact systems. Integrated cyber protection platforms simplify this process by continuously identifying vulnerable assets, deploying critical updates at scale and validating successful remediation. For MSPs, this capability is essential to maintaining consistent security posture across diverse customer environments.

Managing and securing the use of AI technologies

AI-related risks became more pronounced in H2 2025, both as a force multiplier for attackers and as a new source of enterprise exposure. Threat actors increasingly leveraged AI to accelerate malware development, automate reconnaissance and enhance social engineering campaigns. Also, the GLOBAL GROUP ransomware operation introduced an AI-driven chatbot into its victim negotiation portal. At the same time, organizations faced growing risk from uncontrolled use of external AI services, including data leakage through prompt injection and misuse of sensitive information.

MSPs must establish clear governance around AI usage, including restrictions on data sharing, access controls and monitoring of AI interactions. Security teams should be trained to recognize AI-specific threats, while logging and auditing mechanisms help detect anomalous or unauthorized activity. Responsible AI adoption requires treating AI platforms as part of the attack surface, rather than as neutral productivity tools.

Preparing for incidents with tested response and recovery plans

H2 2025 incidents demonstrated that even well-defended environments can suffer disruptive breaches when attackers move quickly or exploit trusted access paths. Extended outages, data exposure and operational paralysis were common outcomes when response processes were unclear or recovery options were limited.

MSPs must maintain well-defined incident response plans that clearly outline escalation paths, decision-making authority and technical response procedures. Regular tabletop exercises help ensure readiness under real-world conditions. Integrated cyber protection platforms enhance incident response by linking detection with automated recovery, enabling rapid restoration from immutable backups. Routine testing of recovery processes ensures that MSPs can respond decisively when incidents occur, minimizing downtime and protecting customer trust.

4

Acronis cyberthreat predictions for 2026

The consistent thesis for next year is that attackers will increasingly optimize for throughput and leverage: Compromises that deliver the maximum blast radius in the minimum time. For MSPs, this translates into a continued shift toward control-plane compromise (identity, RMM / PSA, virtualization layers, SaaS admin and cloud entitlements) and data-centric extortion that does not require full encryption to be disruptive. Adversaries will use AI as the norm, while simultaneously intensifying focus on cybercrime ecosystems and high-impact compromise paths, including virtualization and agent misuse.

AI systems become both a target and a liability surface

AI systems will introduce a new class of operational risk that sits between traditional security vulnerabilities and human process failure. Indirect prompt injection, agent workflow manipulation and data leakage via connectors will increasingly be exploited to influence AI behavior rather than to compromise the underlying platform. Prompt injection in particular is likely to remain intrinsically difficult to fully mitigate and should be treated as a "confused deputy" style risk: the system behaves as designed, but is misled about intent or trust boundaries. As a result, this class of risk must be engineered around system design and control separation, not simply filtered or patched away.

For MSPs, the most practical and immediate risk is agent-driven change without robust guardrails. AI-enabled ticket triage, scripted remediation, configuration recommendations and knowledge assistants are often granted implicit trust and broad contextual access. If these systems are exposed to untrusted input or loosely scoped connectors, they can be manipulated into unsafe actions, incorrect prioritization or inadvertent disclosure of sensitive customer or operational data. The challenge is less about AI making errors and more about the speed, scale and opacity with which those errors can propagate across environments when human approval, isolation and auditing controls are insufficient.

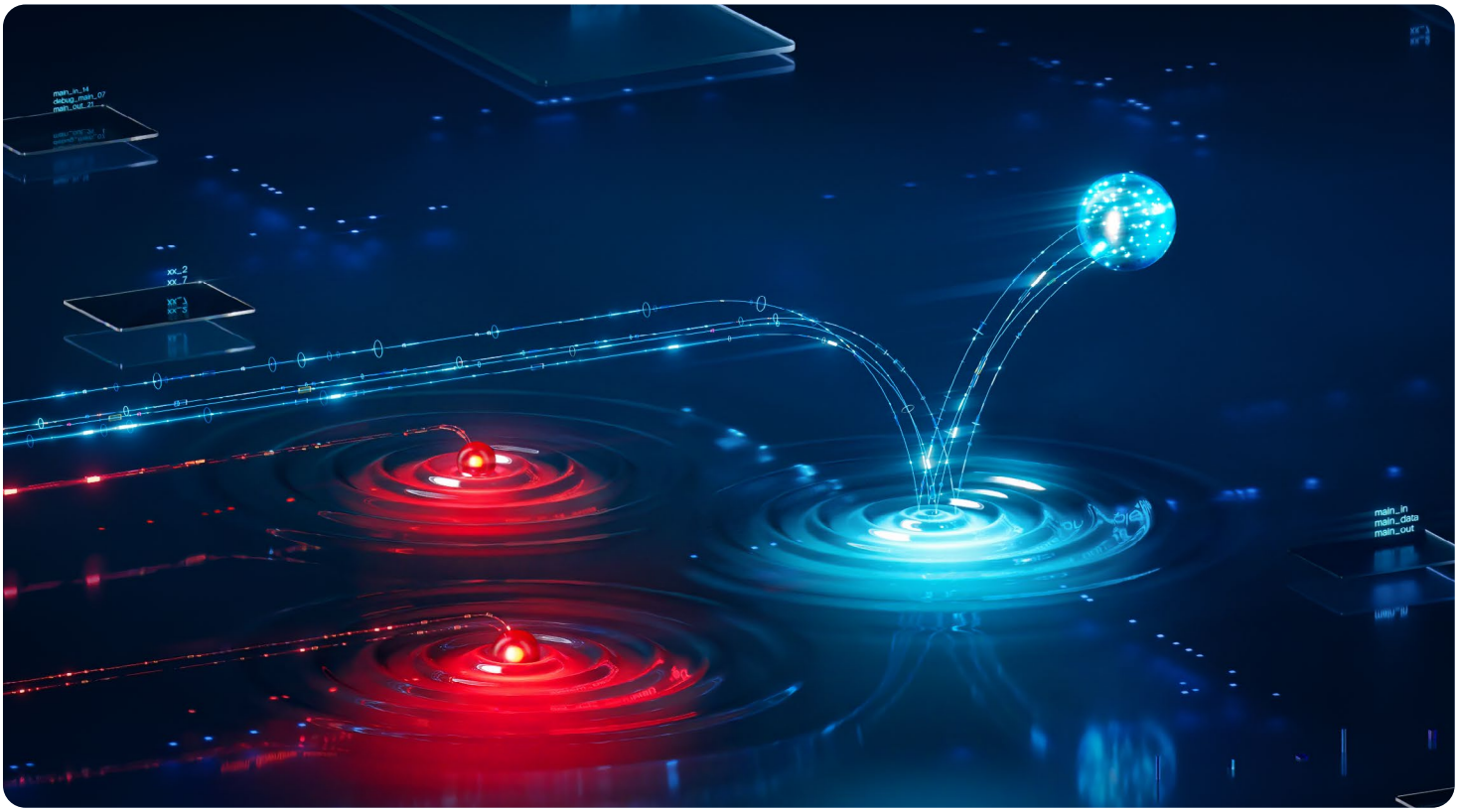
AI systems will introduce a new class of operational risk that sits between traditional security vulnerabilities and human process failure.

Ransomware continues, but “extortion-first” dominates operational impact

A central 2026 trend we expect is the continued evolution from traditional encryption-led ransomware to data theft, disruption and coercion as the primary monetization model. Attackers will maximize leverage with exfiltration, regulatory pressure and business disruption rather than on encryption. Encryption will be deprioritized in many campaigns, with extortion pressure moving “up the stack” toward customers, partners, regulators and insurers. For MSPs, the practical implication is that resilience cannot be measured only by backup recovery performance. The defining risk becomes multitenant data exposure and downstream notification / compliance shockwaves, especially when MSP tooling or shared repositories provide cross-customer visibility.

Control-plane attacks expand: Identity, SaaS admin and nonhuman identities

Compromised identity will be the most scalable intrusion path. Security shift from human authentication to governance of nonhuman identities (service accounts, workload identities, tokens and delegated entitlements) frames compromised identity as a dominant driver of cloud breaches. For MSPs, this is a structural risk: MSPs maintain privileged accounts across many customers, often with standing access. In 2026, successful attackers will increasingly aim to compromise the MSP’s identity fabric (SSO, privileged access, API keys, automation accounts) rather than individual endpoints, because that path offers repeatable, high-scale impact.



Supply chain and shared components remain the highest-leverage entry point

Third-party and supply chain compromise remains a repeated 2026 prediction, driven by dependency sprawl (SaaS apps, plugins, managed integrations, APIs, open-source modules). Third-party risk and the emergence of "shadow agents" (unauthorized AI agents and automations) will create invisible data pipelines and new trust paths. Attackers will target upstream systems because it scales across many downstream organizations.

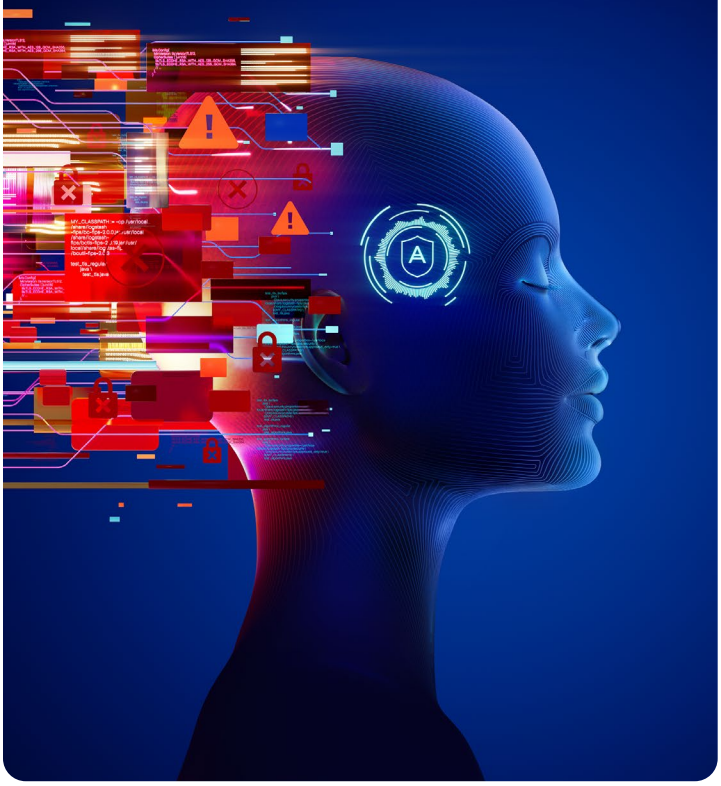
For MSPs, this points to two likely 2026 patterns: compromise of MSP-adjacent vendor ecosystems (RMM / PSA / documentation / remote access) and compromise of customer environments through trusted MSP integrations (e.g., OAuth grants, app connectors, automation runbooks and delegated administration).

Quantum risk moves from theory to migration planning, impacting MSP-delivered trust services

Quantum computing is unlikely to "break the internet" in 2026, but 2026 is widely viewed as a transition period where post-quantum cryptography (PQC) planning becomes operational, especially for long-lived data and foundational trust services. NIST finalized its first post-quantum encryption standards in 2024 and encouraged administrators to begin transitioning, and NIST's transition guidance outlines a long runway culminating in deprecation of quantum-vulnerable algorithms by 2035. For MSPs, the 2026 implication is procurement and architecture: PKI, VPN / ZTNA, certificate lifecycle, firmware signing and identity assurance services will increasingly be expected to offer PQC-aware roadmaps. This becomes an MSP differentiator and a potential compliance requirement in regulated sectors.

Scams, phishing and impersonation become multichannel and industrialized

Scams are becoming even more AI-driven, AI-scaled and "emotion-engineered," with attackers moving victims across SMS, chat apps, fake websites and payment rails more efficiently than before. For MSPs, this raises operational risk in helpdesk and change-control processes: attackers will target password resets, MFA reenrollment, device onboarding, invoice changes and "urgent admin actions," exploiting the fact that MSP service desks are designed to be responsive. In 2026, "verification" must assume realistic impersonation and multi-channel pretexting.



Cloud and API exploitation shifts toward misconfiguration, entitlements and IaC

Cloud compromise becoming more about exploitation of misconfiguration, over-privilege, exposed services and IaC drift. Cloud identity, IaC and SaaS governance will require new controls and skills. There will be a growing need to govern agents and automate defense, and cloud environments will be "too fast" for manual-only security operations. For MSPs, the expected 2026 failure mode is not simply "a cloud breach," but a repeatable entitlement failure replicated across customers via templates, baseline scripts or standardized deployments.

Conclusion

The most important 2026 message for MSPs is that cybersecurity risk will be shaped less by any single malware family and more by systemic properties of the MSP model: centralized privilege, shared tooling and repeatable deployments. Forecasts converge on an environment where attackers operate with higher throughput, better impersonation and faster exploitation of trust paths, while quantum risk drives early-stage migration pressure in identity and cryptographic infrastructure. Organizations that treat identity, control-plane governance and automated response as critical infrastructure will be best positioned to reduce blast radius in 2026.

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 總代理湛揚科技

Acronis Threat Research Unit

Learn more at
acronis.com