NTT DATA

CTI Trends

Cyber Threat Intelligence

Second half of 2025

Index

Index

1. Executive summary

The **second half of 2025 (H2 2025)** confirmed a structural shift in the cyber threat landscape, driven by the convergence of geopolitical tensions, the industrialization of cybercrime, and the growing technical maturity of threat actors, rather than by the emergence of radically new techniques. The period was defined by a marked change in adversary operating logic, geared toward persistence, stealth, and the maximization of economic, strategic, and reputational impact.

Cyberspace has been confirmed as a central domain of hybrid confrontation, firmly integrated into global geopolitical dynamics. Protracted conflicts and strategic rivalries have extended into digital infrastructure, supply chains, and technology ecosystems, generating cross-cutting effects that impact governments, critical sectors, and private organizations alike.

Geoeconomic fragmentation, digital sovereignty initiatives, and the reconfiguration of technology alliances have reinforced a more volatile, less cooperative environment, with greater attribution challenges and reduced capacity for coordinated response. From an operational standpoint, the second half of 2025 was marked by a deliberate reduction in technical noise. **Threat actors increasingly prioritized low-profile intrusions based on the abuse of legitimate identities, cloud services, and widely used enterprise tools**, reducing reliance on traditional malware. This approach extends dwell time in compromised environments and makes early detection harder, shifting defensive focus from obvious technical indicators to weaker, distributed signals.

Ransomware and data-driven extortion reached an advanced level of industrialization. Innovation now lies less in encryption itself and more in end-to-end campaign orchestration through automation, the targeting of high-value information, staged pressure, and reputational leverage.

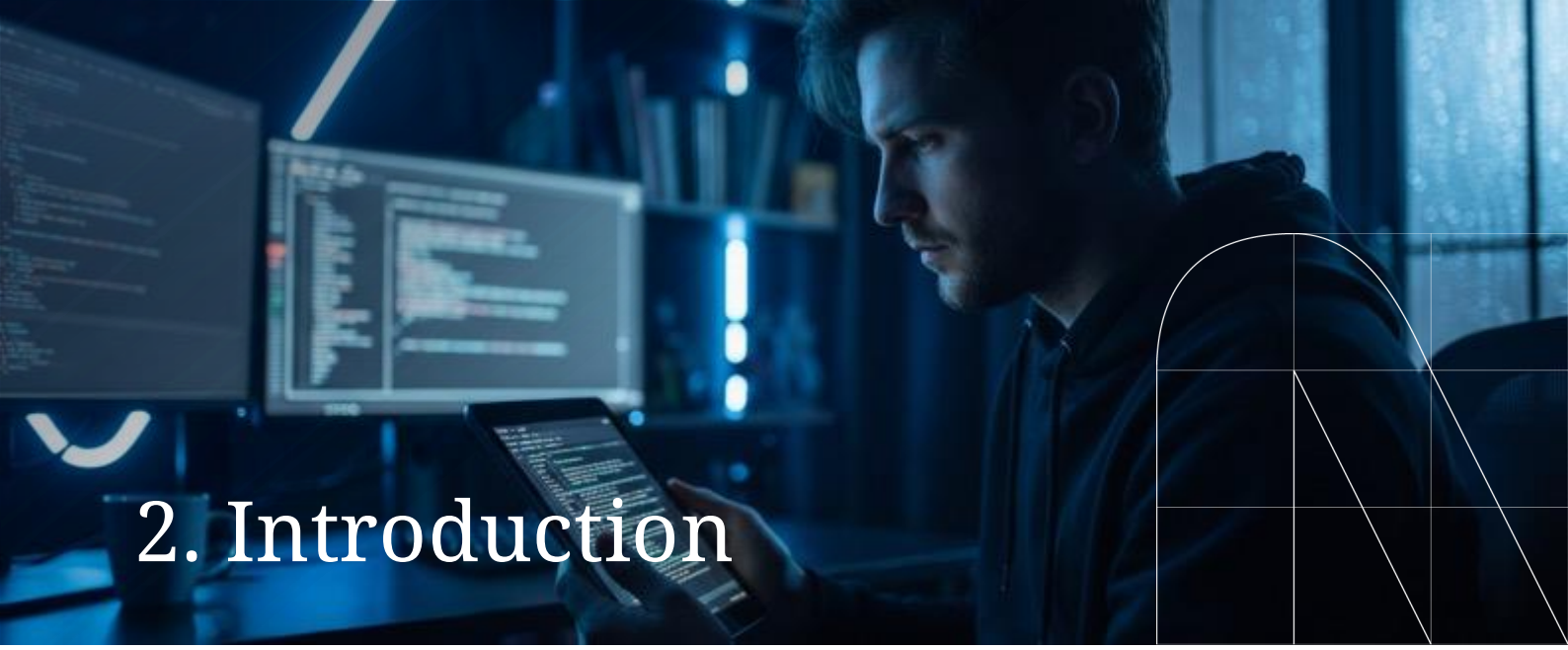
This model reduces dependence on direct operational disruption and enables monetization even when victim services are not fully taken offline.

Artificial intelligence (AI) has become a practical operational multiplier. Its use is now normalized to accelerate specific tasks such as social engineering, reconnaissance, and tool adaptation, lowering cost and barriers to entry without replacing human operators. At the same time, **exploitation of critical vulnerabilities** accelerated following public disclosure, widening the asymmetry between offensive and defensive capabilities.

In parallel, the **criminal ecosystem fragmented significantly,** with the collapse of major underground forums and centralized marketplaces redistributing activity toward specialized marketplaces, initial access brokers, and more opaque private channels, complicating monitoring and early intelligence collection.

The second half of 2025 also brought **stronger legal and regulatory frameworks, high-impact international law-enforcement operations**, and **incremental improvements in organizational defensive capabilities**. However, threat-actor adaptability continues to outpace these advances, exposing a persistent gap between regulatory compliance and real operational resilience.

Overall, the second half of 2025 shows that cybersecurity is no longer exclusively a technological problem, but a systemic challenge in which identity, trust, organizational processes, and geopolitical context are as decisive as technical controls. Effective risk management requires a comprehensive approach centered on contextual detection, resilience, and strategic anticipation in the face of persistent and highly adaptive threats.



2. Introduction

2.1. Purpose of the report

This report provides a detailed analysis of relevant trends, incidents, and developments in cyber threat intelligence during the **second half of 2025**. It covers emerging threats shaping the cybersecurity landscape, threat actors with notable activity, the most significant cyber campaigns, and critical vulnerabilities identified during the period. It also highlights recurring patterns and outlines plausible future scenarios that may influence risk management and mitigation strategies.

2.2. Geographic and temporal scope of the report

The analysis takes a global perspective to explain how threats evolve across interconnected geographic contexts. This approach supports the identification of shared dynamics as well as regional distinctions that deepen understanding of today's cyber environment.

The second half of 2025 was marked by clear shifts in threat behavior and by events with tangible impact across the digital ecosystem. This interval, **from July through December 2025**, is critical for anticipating near-term developments and strengthening response capabilities in an increasingly complex environment.

3. Global overview of threats

During the second half of 2025, the global threat landscape became **more volatile and fragmented**, driven by the convergence of geopolitical tensions, technological disruption, and adverse economic conditions. Together, these forces increased exposure for governments, businesses, and citizens, especially across critical sectors and highly interconnected digital ecosystems.

Digital risks no longer develop in isolation, as they interact and **reinforce one another**, producing systemic impacts across multiple strategic sectors at once (World Economic Forum, 2025). In this context, cyberspace has consolidated as a cross-cutting vector that amplifies pre-existing conflicts and accelerates broader dynamics of confrontation.

The increasing dependence on critical digital infrastructure, together with geoeconomic and regulatory fragmentation, has made international cybersecurity cooperation more difficult. The coexistence of divergent regulatory frameworks, technology models, and governance approaches increases operational complexity and weakens coordinated responses to cross-border incidents. These dynamics have reduced predictability and raised the cost of incident response for both public and private organizations. Accordingly, cybersecurity must be treated as a strategic variable tied to stability, competitiveness, and institutional trust.

This section outlines the **structural drivers that, by their systemic nature, shape the evolution** of cyber risk and the stability of digital ecosystems.

3.1 Geopolitics and cybersecurity

During the second half of 2025, the geopolitical–cybersecurity linkage intensified, with cyberspace operating as a central arena of strategic competition among states. Technological rivalries, economic tensions, and competition for control of critical resources are no longer confined to diplomacy or trade, as they increasingly project onto digital infrastructure, supply chains, and global technology ecosystems.

The period unfolded amid unbalanced multipolarity, marked by the absence of a stable international order and the coexistence of multiple power centers able to erode the system without establishing shared rules (Aznar Fernández-Montesinos, 2025). In this environment, the United States, China, and Russia continued to set the tempo of strategic confrontation, with direct implications for cyberspace stability.

Competition is increasingly expressed through geoeconomic instruments, including sanctions, technology controls, friendshoring, and regulatory pressure. These measures act as indirect catalysts for cyber operations against strategic sectors, redirecting pressure toward energy, transportation, advanced manufacturing, and financial services.

A key development is the consolidation of sovereign internet models that increase state control over traffic, services, and digital governance. Initiatives such as **RuNet** in Russia reflect a state-centric approach built on autonomous infrastructure and proprietary regulatory frameworks (Hernández, 2025). These models, potentially replicable elsewhere, have direct implications for attribution, incident visibility, and coordinated response, reinforcing fragmentation in cyberspace.

At the same time, **artificial intelligence** has consolidated its role as a strategic multiplier by reducing barriers to entry, accelerating attack cycles, and expanding the reach of hybrid campaigns for both state and advanced criminal actors.

Friendshoring is a strategy for reorganizing supply chains in which states or companies shift critical production, sourcing, or services to countries viewed as allies, strategic partners, or politically aligned, in order to reduce geopolitical, economic, and security risks.

Friendshoring is a strategy for reorganizing supply chains whereby states or companies shift critical production, sourcing, or services to countries considered allies, strategic partners, or politically aligned, with the aim of reducing geopolitical, economic, and security risks.

3.2 Geopolitics and key actors

During the second half of 2025, the main international conflicts did not shift abruptly, but their hybrid dimensions deepened, with cyberspace increasingly integrated into economic pressure, diplomatic maneuvering, and information narratives.

- **Russia–Ukraine: deepening of the hybrid dimension of the conflict**

Russia's war against Ukraine continued without major territorial changes, while its digital dimension intensified. Russia expanded cyber operations as a complement to political, economic, and diplomatic pressure, extending activity beyond Ukrainian targets to include European institutions and organizations supporting Kyiv.

The period was marked by increased denial-of-service activity, intensified attempts to disrupt essential services, and influence operations designed to shape public perception across the European Union. Targets included public-sector entities and digital infrastructure in European Union and NATO countries aligned with Ukraine. Convergence also increased between state actors and pro-Russian hacktivist groups, tightening the coupling between disinformation, vulnerability exploitation, and attacks against critical sectors.

The strategic objective centered on operational disruption and media impact rather than system destruction. A notable development was the shift toward more explicit public attributions by Western governments, signaling a deterrence-oriented approach aimed at raising political cost while accepting the risk of controlled escalation in the digital domain.

- **Middle East: cyberspace as a stage for indirect confrontation**

The second half of 2025 was marked by heightened tensions between Iran and Israel, with cyberspace serving as a channel for direct but contained confrontation. Observed operations combined intrusions, targeted leaks, selective sabotage, and information manipulation to degrade capabilities without triggering open military escalation. These campaigns often relied on access to third-party infrastructure, blurred lines between espionage and disruption, and rapid exploitation of exposed services.

A particularly material risk is regional spillover across interconnected energy, financial, and logistics systems. High infrastructure interdependence increases the likelihood of collateral impacts on third countries and private-sector actors. Unlike conventional conflict, where ceasefires can create clear turning points, cyber confrontation can persist autonomously even when physical violence declines.

- **China – West: systemic competition and technological pressure**

The rivalry between China and Western powers has not led to open conflict, but it has intensified significantly in the digital domain. During the second half of 2025, actors associated with Beijing increased cyber-espionage campaigns against strategic sectors such as semiconductors, telecommunications, renewable energy, advanced manufacturing, and financial services, in line with long-term industrial and technological objectives.

A distinctive feature of this period was the shrinking time between the disclosure of critical vulnerabilities and their operational exploitation, reflecting a highly efficient technical intelligence structure. This dynamic increases pressure on Western companies and reinforces the use of cyberspace as a tool to influence strategic decisions, especially in the Indo-Pacific and in tensions surrounding Taiwan.

Regional spillover: indirect spread of the impact of a conflict to third parties or interconnected regions.

- **North Korea and Africa: persistence and environments of opportunity**

North Korea maintained sustained activity aimed at obtaining financial resources and conducting strategic espionage, with growing indications of operational cooperation with Russian actors. This convergence expands the potential scope of operations and further complicates attribution.

At the same time, regions such as the Sahel continue to provide conditions conducive to the proliferation of hybrid actors. Institutional weakness, political fragmentation, and the presence of critical infrastructure enable opportunistic sabotage, espionage, and disinformation. These dynamics increase exposure for European companies operating in the region and for partners embedded in local supply chains.

More broadly, the second half of 2025 confirms that geopolitics, technology, and cybersecurity form an **interdependent system**. Strategic tensions propagate into cyberspace quickly, producing cross-cutting effects that extend beyond primary targets. Even when they do not escalate into open conflict, these dynamics are reshaping the global digital balance. As a result, states, strategic sectors, and private organizations face higher uncertainty and shorter decision cycles. Cyber risk management therefore requires closer integration with geopolitical and geoeconomic analysis.

3.3 Impact of cyberattacks on specific sectors

NTT DATA's Cyber Threat Intelligence Department reviews how cyberattacks evolved by sector and among the most affected countries to conclude the threat landscape assessment for the second half of 2025.

Data recorded from July through December shows that, while patterns from previous periods persist, there were meaningful shifts associated with intensified geopolitical tension and a broader set of disruptive actors. Compared to the first half of 2025, the sectoral distribution indicates changes in target prioritization and a sustained concentration of activity against foundational sectors for public administration and global economic functions.

The distribution again highlights a clear preference by state and non-state threat actors for strategic sectors that concentrate sensitive information, critical operational dependencies, and high potential impact in the event of disruption. Unlike the previous half-year, when attacks were concentrated in fewer sectors, this period recorded a broader rise in attack volume, particularly across the public sector, education, and financial services.

- **Public administration and government:**

The **public administration sector** continues to rank first by incident volume, with a total of 3,343 attacks in the last six months. This figure represents a significant increase compared to the first half of the year and reinforces the trend observed since late 2024, characterized by campaigns targeting public bodies at all levels. The constant exposure of administrative systems, combined with the critical nature of their operations, makes them a priority target for groups seeking to obtain strategic information, disrupt essential services, or exert political pressure through defacement and data leaks.

The rise in intrusions associated with politically motivated actors, including campaigns attributed to groups linked to Mexico during this period, underscores that government agencies remain one of the main impact vectors amid growing international cyber tension.

In the **government and public sector**, **590 confirmed attacks were recorded in the last six months**. While significantly lower than the volume observed across public administration overall, this figure confirms that the area remains a **recurring target** within the threat ecosystem. These incidents are concentrated mainly in agencies with high institutional visibility and in entities responsible for citizen services, where reputational and operational impact continues to be a key driver for threat actors.

The term "public sector" encompasses all entities controlled by the state, while "public administration" refers specifically to the administrative bodies and structures that implement public policies.

- **Education:**

With **1,460 cyberattacks, education remained among the most affected sectors**. Although the figure is slightly lower than in the first half of 2025, educational institutions continue to face high exposure. This exposure is driven by heterogeneous systems, decentralized asset management, and the presence of high-value personal, academic, and research data.

The second half of 2025 also showed a shift in predominant attack patterns. Alongside credential theft and internal network compromise, extortion campaigns based on data leaks increased. Threat actors exploited the limited response capacity of many regional and private institutions. Universities remained a primary target due to broad digital footprints and high-value data.

- **Financial services:**

The financial services sector **recorded 957 attacks, remaining among the three most affected sectors globally**. Incidents continued to concentrate on ransomware, unauthorized access, and theft of sensitive information.

The increasing sophistication of criminal techniques, combined with state interest in economic espionage, helps explain the sector's continued attractiveness. Interest also increased in fintech and digital payment platforms, whose rapid growth has expanded exposure and attracted opportunistic exploitation of critical vulnerabilities.

- **Information Technology and Telecommunications:**

IT Services, with **802 attacks**, and Telecommunications, with **614 attacks**, again faced heavy pressure. Many incidents were linked to exploitation of third-party vulnerabilities, attacks on managed service providers, and supply chain compromises. Because these industries are deeply interconnected, a single intrusion can scale laterally to customers and technology-dependent partners, creating multiplier effects. This pattern was especially visible in September and November, coinciding with global peaks in malicious activity.

- **Transportation, Logistics, and E-commerce:**

Transportation and Logistics, with **592 attacks, and E-commerce, with 532 attacks, continued to experience elevated pressure**. Common vectors between July and December included supply chain disruption, digital fraud campaigns, and manipulation of customer data. In e-commerce, the increase aligns with fourth-quarter shopping seasonality, including Black Friday, Cyber Monday, and the holidays. During these periods, threat actors attempt to maximize impact through carding, skimming, and platform compromise.

- **Health and Healthcare services:**

The healthcare sector recorded **526 incidents**. Although lower than in previous periods, this figure still places healthcare among the most critical targets. Ransomware remains the primary threat, given its potential to disrupt clinical services, compromise medical data, and directly impact patient care.

During the second half of the year, incidents concentrated notably in mid-sized entities and private providers. This pattern suggests that threat actors are prioritizing targets with less capacity to invest in security but comparable operational relevance.

Compared to the first half of the year, the composition of the most affected sectors shifted significantly. While most sectors held similar positions, manufacturing, which had ranked among the ten most attacked in the previous period, dropped out of the top ten.

Construction recorded 445 attacks during the second half of the year and gained enough weight to enter the top ten by incident volume. This shift signals a recalibration of malicious-actor priorities, with greater emphasis on sectors associated with higher economic value and monetization potential.

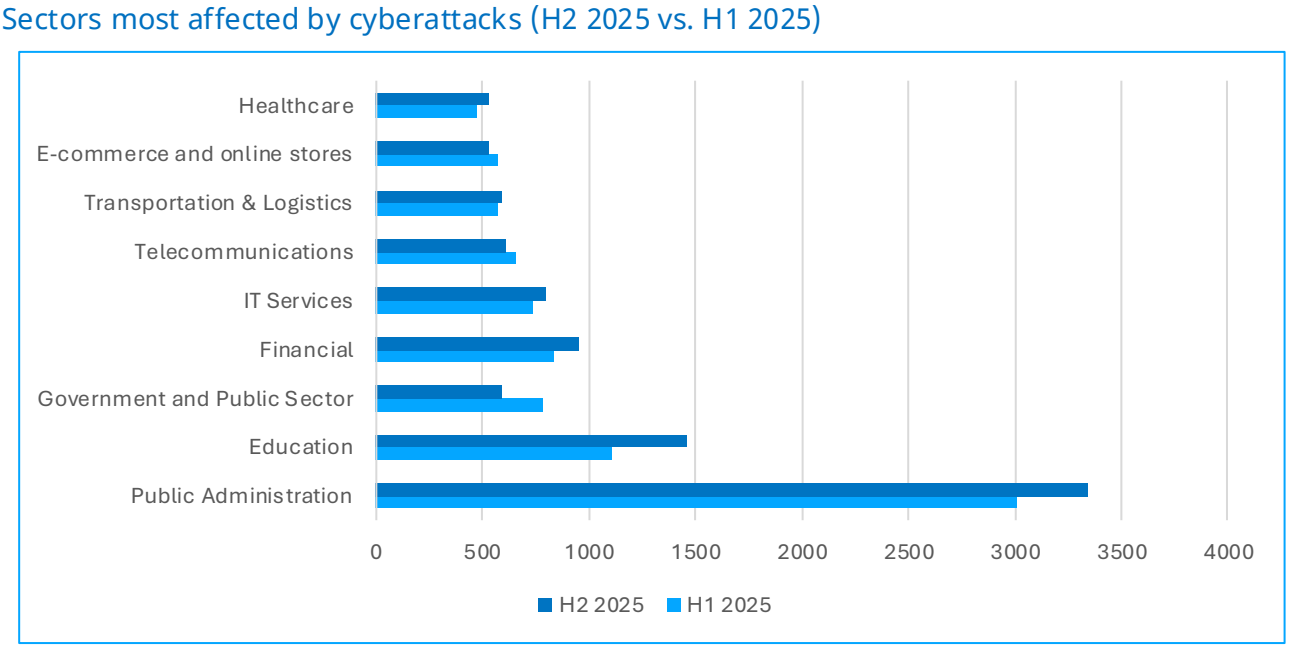


Figure 1 | Sectors most affected by cyberattacks in the second half of 2025.

Data from the second half of 2025 confirms a consistent geographic impact pattern, with cyberattacks concentrated in highly digitized countries with geopolitical weight, close alignment to major alliances, or large technology ecosystems.

- **The United States** remains the most affected country, with a total of **3,963 attacks**. **Although the total declined slightly compared to the previous period, the United States continues to register the highest attack volume globally.** This volume reflects both the country's economic leadership and its central role in technological and geostrategic competition, particularly its rivalry with China and its involvement in the war in Ukraine.

- **Thailand**, with **1,341 attacks**, **reached the top five most affected countries for the first time in the period under review.** The increase in cyberattacks is linked to the expansion of digital payment infrastructure, the growth of e-commerce, and greater exposure to large-scale phishing and ransomware campaigns in Southeast Asia

- In **India**, which recorded **1,244 attacks**, malicious activity continued in connection with both regional tensions and the country's rapid digitalization. India remains a priority target for criminal and state-linked actors due to its population size, the growth of its technology sector, and its strategic role in the Indo-Pacific.

- **Israel** ranks fourth with **1,233 attacks**, a volume consistent with ongoing regional tensions despite a decline compared to the previous six months. Cyber activity affecting Israel combines offensive operations attributed to adversarial state-linked groups with hacktivism campaigns driven by developments in the Middle East.

- Finally, **Germany** recorded **856 attacks** and remains one of the primary targets in Europe. Malicious activity concentrated on industrial sectors, government services, and financial institutions, in a context shaped by the economic impact of the war in Ukraine and Germany's role as a leading technology and industrial power within the European Union.

Distribution of cyberattacks by country (H2 2025)

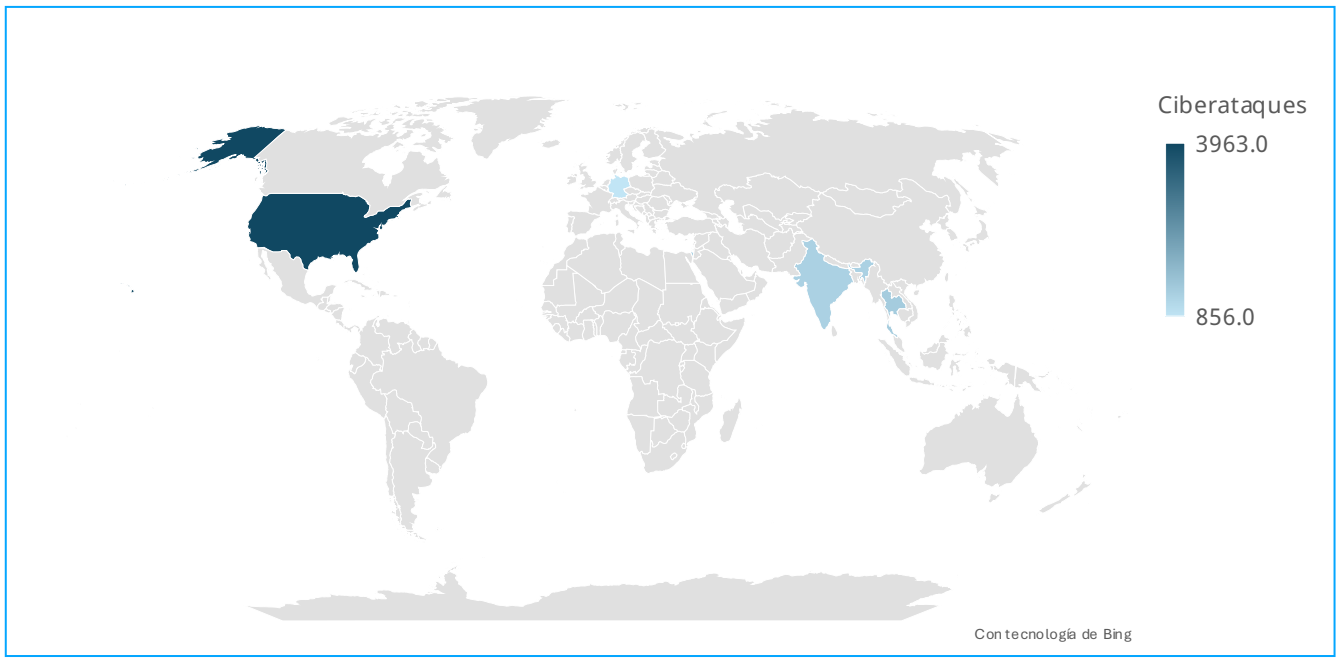


Figure 2 | Geographic distribution of the impact of cyberattacks in the second half of 2025.

4. Major global threats

During the second half of 2025, the global threat landscape was marked by high operational intensity, with more coordinated campaigns, greater actor professionalization, and growing impact on critical infrastructure, large organizations, and supply chains.

Convergence between ransomware, espionage, and digital sabotage became more entrenched, with actors reusing techniques and capabilities across criminal and state-linked ecosystems. The period reinforced a shift toward more persistent, selective, and harder-to-attribute attacks, underscoring the structural nature of cyber risk at the global level.

4.1. Notable cyber incidents and major campaigns

The most significant cyber incidents during the period reflected an escalation in scope and sophistication, with high-impact campaigns targeting strategic sectors, essential services, and large corporations. Prolonged operations dominated, enabled by compromised credentials, trusted infrastructure, and Living-off-the-Land (LotL) techniques that make early detection difficult. The major campaigns observed show clear emphasis on large-scale data exfiltration, multiple extortion, and operational disruption, consolidating more aggressive and more effective attack models.

NTT DATA's Cyber Threat Intelligence Department has documented a selection of the most significant cyber incidents from the second half of 2025, chosen for their representative value of the main threats observed during the period.

Victims	Sector	Attacker	Country/region affected	Origin of attacker	Date of incident	URL
SonicWall	Cybersecurity	Akira Ransomware Group	Global	Unknown	07/22/2025	Source
Salesforce/Salesloft	Cloud	UNC6395	Global	Unknown	08/09/2025	Source
Jaguar Land Rover (JLR)	Automotive/Manufacturing	Scattered Lapsus$ Hunters	Global	Unknown	09/01/2025	Source
Stellantis	Automotive	ShinyHunters	North America	Unknown	09/21/2025	Source
Claro Colombia	Telecommunications	Crimson Collective	Colombia	Unknown	09/25/2025	Source
Asahi Group Holdings	Beverages and food products	Qilin	Japan	Unknown	09/29/2025	Source
Red Hat	*Software*	Crimson Collective	Global	Unknown	10/01/2025	Source
Muji/Askul	*Retail*	Unknown	Japan	Unknown	10/19/2025	Source
Knownsec	Cybersecurity	Unknown	Global	Unknown	11/02/2025	Source
Anthropic	Artificial intelligence	Unknown	Global	China	11/13/2025	Source
Logitech	Electronics	Cl0p	Global	Unknown	11/14/2025	Source
Pornhub	Entertainment	ShinyHunters	Global	Unknown	12/16/2025	Source
French Ministry of the Interior	Government/Public Safety	Unknown	France	Unknown	12/17/2025	Source
European Space Agency (ESA)	Space	888	Europe	Unknown	12/31/2025	Source

Table 1 | Major cybersecurity incidents in the second half of 2025.

As anticipated in the previous report, the second half of 2025 featured a more automated, stealthier, and more sector-specific threat ecosystem, driven by the convergence of generative AI, supply chain compromise, and operations with a pronounced geopolitical component.

Cyberattack campaigns grouped by target (H2 2025)

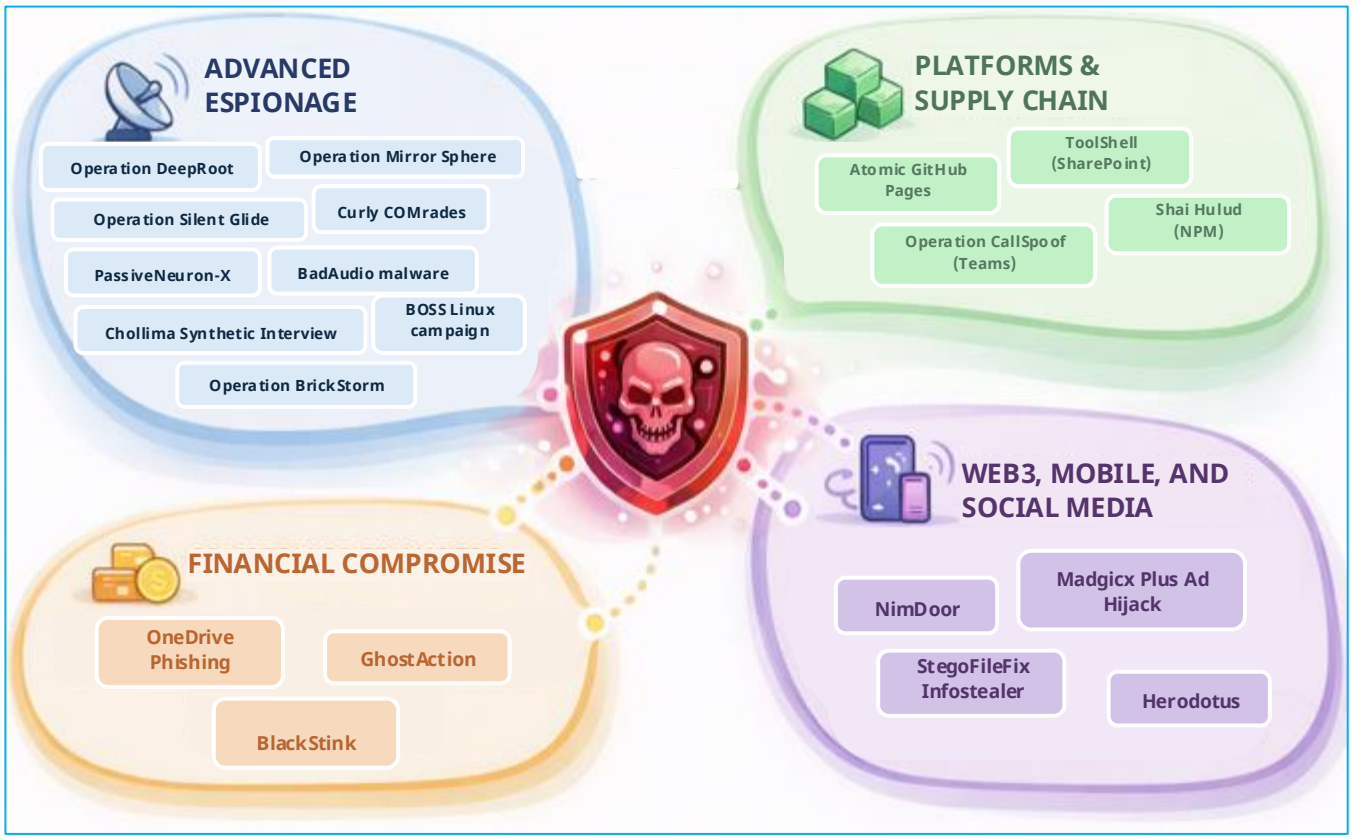


Figure 3 | Major campaigns detected in the second half of 2025.

4.2 Emerging attack trends

In the second half of 2025, trends indicating a structural shift in attack models gained traction, with greater automation, tool modularity, and low-profile initial access, reinforcing a dynamic environment in which persistence, evasion, and economic impact prevail.

In this context, the following technical and operational trends stand out as defining features of activity in cyberspace during the second half of the year.

4.2.1 Low-noise and malware-free attacks supported by legitimate infrastructures

The use of Living-off-the-Land techniques and the increasing abuse of legitimate services, especially cloud and SaaS, has become established as a way to persist and move laterally with minimal artifacts and a reduced forensic footprint, including the use of OneDrive, Google Drive, Slack, GitHub, Discord, and OAuth services as covert command-and-control channels, the abuse of valid authentications and legitimate tokens instead of persistent malware, and the replacement of malicious binaries with native scripts, scheduled tasks, and abuse of system utilities (LOLBins).

4.2.2 Artificial intelligence as an operational multiplier

Once again, AI emerged as a sustained trend during the period. Its use was primarily observed in accelerating specific phases of the operational cycle, including automated reconnaissance, more convincing phishing, polymorphic payload development, and campaign automation (ransomware, fraud, synthetic identity), dynamically tailored to the victim profile.

4.2.3. Rise in software supply chain and development platform compromise

Attacks observed during the period showed growing interest in compromising development tools and processes, including malicious code injection into NPM packages, PyPI, and GitHub repositories (for example, **Shai-Hulud 2.0** or **Glassworm** in VS Code extensions), CI/CD pipeline manipulation with cascading effects across multiple applications, and the publication of cloned or backdoored dependencies that propagate without active intervention once integrated.

4.2.4 Consolidation of the cloud and SaaS as the primary attack surface

The sustained rise in intrusions into cloud and SaaS environments reflects a shift from classic endpoints to interconnected cloud ecosystems, with threat actors prioritizing exploitation of insecure configurations in multi-tenant environments, abuse of OAuth applications to maintain persistent access without credentials, and lateral movement enabled by SaaS synchronization, leveraging excessive permissions and over-trusted application integrations.

4.2.5 Advanced espionage with a strong geopolitical component

Espionage observed during the period showed recurring technical characteristics, including more distributed persistence through redundant mechanisms rather than a single point of failure, fragmented and covert command and control embedded in legitimate traffic, and irregular beaconing that avoids detectable patterns by adjusting frequency based on user activity.

4.2.6 Reusable modular toolkits

The adoption of modular architectures has enabled threat actors to change objectives without redesigning entire operations. This practice continues to drive group professionalization as a natural evolution of the underground market, consistent with patterns observed earlier in the year.

Frameworks combining financial theft, corporate espionage, and selective exfiltration have become more common, alongside reuse of lightweight implants with selective activation and the rise of persistent access ecosystems as a service, where infrastructure is provided to APT groups.

4.3 Global statistics on security incidents, types of attacks, and threat actors involved

During the second half of 2025, the global cybersecurity landscape was marked by consolidation of mature threats, especially ransomware, and by acceleration of enabling vectors such as advanced social engineering and the use of artificial intelligence. Rather than declining after the early-year peak, the data indicates stabilization at high levels, accompanied by greater technical and organizational sophistication among threat actors.

4.3.1 Security incidents

Ransomware remained the primary generator of high-impact incidents, with **1,592 victims** reported on data leak sites during the third quarter of 2025, averaging approximately 535 victims per month. Although this is below the peak observed in the first quarter of 2025 (**2,289 victims**), it confirms that the second half of the year sustained historically high activity levels and rules out a scenario of meaningful containment of the threat (Check Point Research, 2025). of the threat (Check Point Research, 2025).

At an aggregate level, **ransomware** was involved in approximately **44% of security breaches** recorded in 2025, up from around 32% in 2024, reinforcing its position as the primary driver of operational and economic impact.

4.3.2 Types of attacks and predominant vectors

After ransomware, **supply chain** attacks accounted for **30%** of incidents in 2025, consolidating their role as a major risk amplifier, while non-ransomware **malware** (trojans, spyware, infostealers, and similar) represented around **17%**, primarily used to prepare environments and establish persistence, and DDoS accounted for a more limited **5%**, maintaining a tactical and complementary role.

Regarding entry vectors, phishing remained the most common, representing **approximately 16% of breaches**, given its low cost and adaptability, while **third-party compromise** as an access point (**15%**) reached nearly the same level, confirming a shift beyond an organization's own perimeter, and **credential compromise (10%)** further highlighted abuse of legitimate identities, consistent with patterns observed throughout the report.

From a technology evolution perspective, **approximately 16%** of incidents incorporated some use of **artificial intelligence** by threat actors, primarily for phishing content generation, identity theft, and campaign automation (Khalil, 2025). While AI does not replace traditional techniques, it increases their scale, credibility, and effectiveness, acting as a risk multiplier.

4.3.3 Threat actors and ecosystem dynamics

The criminal ecosystem in the second half of 2025 showed unprecedented fragmentation, particularly in ransomware. In the third quarter, at least 85 active ransomware groups were identified, the highest number recorded to date (Check Point Research, 2025).

The criminal ecosystem in the second half of 2025 showed unprecedented fragmentation, particularly in the ransomware domain. In the third quarter, at least **85 active ransomware groups** were identified, the highest number recorded to date (Check Point Research, 2025). This increase does not necessarily indicate greater overall capacity, but rather greater atomization of the Ransomware-as-a-Service (RaaS) model, with a proliferation of brands, affiliates, and smaller-scale campaigns. This dynamic complicates attribution, reduces the impact of targeted disruption efforts, and increases overall ecosystem volatility.

A constant rotation of criminal tools and services was also observed.

The **86%** drop in **Lumma Stealer** activity in the second half of the year compared to the first (ESET Research, 2025) does not indicate reduced credential theft, but rather rapid tool replacement following takedown actions against MaaS infrastructure. This pattern confirms that law-enforcement operations have impact, but also accelerate migration to new malware families.

Overall, statistics from the second half of 2025 reflect a more mature, resilient, and adaptable criminal ecosystem capable of absorbing disruption and reorganizing quickly.

Global statistics by type of attack (2025)

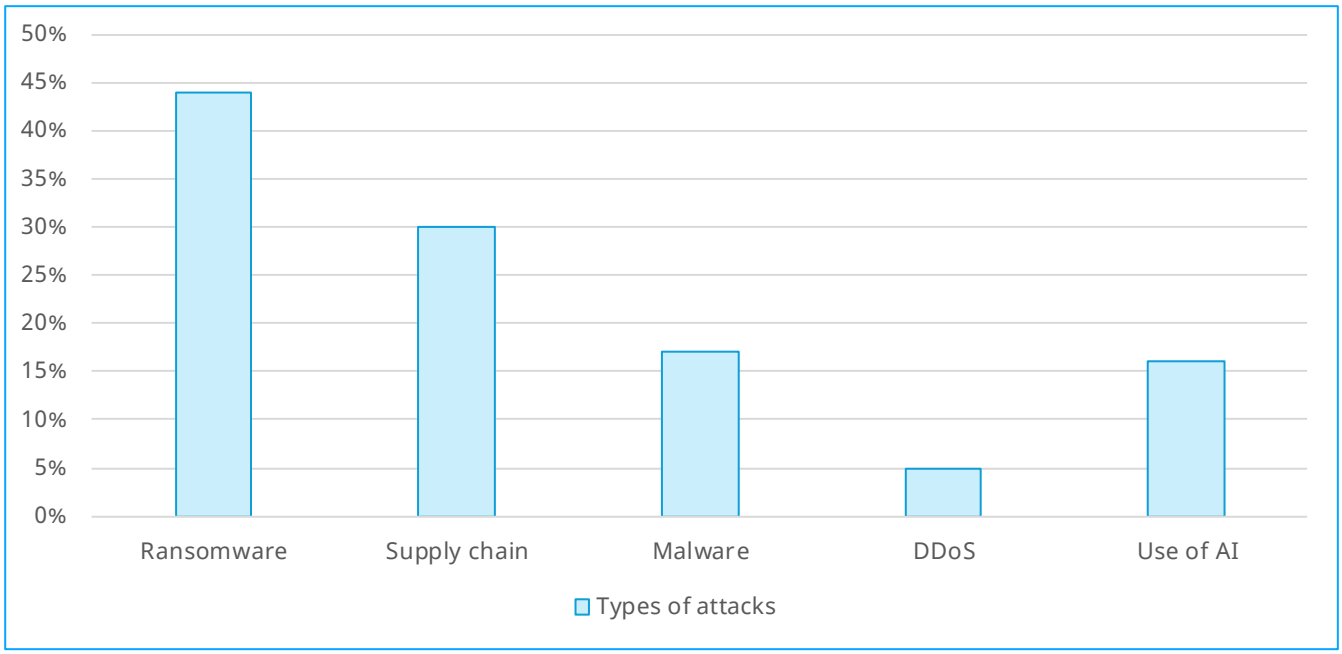


Figure 4 | Frequency of attacks by type during 2025.

4.4 Costs of cyberattacks for organizations

In 2025, the estimated economic impact of cybercrime reached approximately **$10.5 trillion** per year, reinforcing its nature as a systemic risk for organizations.

Operationally, **ransomware** remained the most frequent incident type, and while average ransom demands were around **$115,000**, **64%** of organizations chose not to pay, shifting the economic burden to indirect costs such as **operational disruption**, technical recovery, and legal and reputational consequences, with an average total cost per incident of **$5.08 million** including downtime and recovery.

Globally, the **average cost of a data breach reached $4.44 million**, **9%** lower than the 2024 average. In the **United States**, the figure rose to **$10 million** in regulated sectors such as healthcare, finance, and critical infrastructure. The **Middle East** averaged approximately **$7.3 million** per breach, an **18%** reduction compared to 2024 attributed to higher cybersecurity investment and use of AI-based defenses, while Europe averaged around **$4 million**, influenced by more mature data protection frameworks and more standardized response processes.

Structurally, key factors identified in 2025 act as multipliers of economic impact. **Incidents affecting third parties** drive the largest increase, with an average additional cost of **$227,000**.

These are followed by overly **complex security architectures (+$207,000)** and **shadow IT (+$200,000)**, both of which hinder detection and response. In addition, **malicious use of AI** or the **absence of proper governance** adds around **$193,000** to the average breach cost, and **Shadow AI** is particularly notable, as unsupervised use can increase economic impact by approximately an additional **$670,000** per incident.

By contrast, organizations that integrate security measures from the design stage have significantly reduced economic impact. Adopting **DevSecOps** reduces average cost by **$227,000**, **AI/ML-based** security analytics by **$223,000**, robust **threat intelligence** programs by **$211,000**, and extensive **data encryption** by **$208,000**, and the combined use of AI and automation in defense enables an average cost reduction of **34%**, widening the gap between high-maturity organizations and those with reactive approaches (Khalil, 2025).

Market estimates published during 2025 placed global spending on information security and risk management at around **$213 billion**, representing year-on-year growth of close to **14%** (Stamford, 2025).

This data reflects a key reality of the second half of the year, namely sustained growth in security investment in response to rising threat complexity, without a proportional reduction in incident-driven economic impact.

Although this report focuses on trends observed during the second half of 2025, the statistics used correspond to aggregate data for the entire year. These figures are included to contextualize dynamics that consolidated throughout 2025 and to support interpretation at fiscal year end.

5. Legal framework and arrests in cybersecurity

NTT DATA's Cyber Threat Intelligence Department considers it essential to analyze the security measures implemented, cybersecurity laws enacted, and arrests carried out globally by law enforcement agencies during the second half of 2025.

This analysis assesses countries' commitment to regulating and controlling current and emerging technologies, as well as their responsible application. It also reflects joint efforts by legislative, judicial, and defense bodies to address corporate security breaches and combat illegal activity in cyberspace.

5.1 Main laws in cybersecurity

In the second half of 2025, the global legal and regulatory framework for cybersecurity evolved significantly, driven by the need to strengthen digital resilience, improve technology governance, and harmonize obligations across sectors and jurisdictions. During the period, national and international bodies published or enacted new laws, strategies, and technical standards that reinforce a shift from a purely preventive posture to one centered on verifiable compliance and active oversight.

Among the most significant developments are full implementation of the **DORA Regulation** in the European Union, legislative reforms in Italy, Singapore, and Brazil, and updates to international reference frameworks such as **ISO/IEC 27001** and **NIST** guidance, which together lay foundations for broader regulatory convergence in cybersecurity.

Continent	Regulations	Institution	References
North America	**NIST SP 800-53 – Release 5.2.0** (Aug. 27, 2025)	NIST/CSRC	Notice and summary of changes in release 5.2.0.
	NIST SP 800-88 Rev.2 – Media Sanitization (IPD Jul 21, 2025; final publication Sep 2025) **Obsolete**	NIST/CSRC	NIST Computer Security Resource Center
	NIST SP 800-18 Rev.2 – System/Privacy/SCRM Plans (IPD, June-July 2025)	NIST/CSRC	NIST Computer Security Resource Center
South America (Brazil)	**Decree No. 12,573/2025 – E-Ciber (National Cybersecurity Strategy)** (Aug. 4, 2025)	Presidency of Brazil (Planalto)	Official Gazette in Planalto
Asia	**Cybersecurity (Amendment) Act 2024 – Commencement Notification 2025** (comes into force on October 31, 2025, various sections)	Gov. of Singapore (AGC/Statutes Online)	Notification S 677/2025 with details of sections and date sso.agc.gov.sg
	Cybercrime and Mutual Assistance Package (third reading approved; heading for Budapest Convention)	NZ Government	Official note (Beehive) July 24, 2025; context in Ministry of Justice
Europe	**DORA – RTS ICT Outsourcing** (Delegated Regulation **(EU) 2025/532**, July 2, 2025)	European Commission/EUR-Lex	Text in OJEU
	DORA – Guide to the supervision of Critical ICT Providers (CTPPs) (July 15, 2025)	ESAs (EBA/EIOPA/ESMA)	Joint guidance published by the ESAs
	DORA – Roadmap for Designation of CTPPs (July 2025)	ESAs (EBA/EIOPA/ESMA)	Official note/roadmap
	RED/EN 18031 (series) – harmonized cybersecurity standards (applicable from Aug. 1, 2025)	European Commission/EUR-Lex	Implementing Decision **(EU) 2025/138** citing EN 18031-1/-2/-3 with restrictions
	Law 132/2025 – AI (deepfakes, aggravating factors in cybercrime, governance) (effective Oct. 10, 2025)	Italian Republic (Gazzetta Ufficiale)	Official publication (GU No. 223, Sept. 25, 2025)
International	**ISO/IEC 27001:2022 – end of transition** (**October 31, 2025**)	IAF/BSI (accreditation & certification)	Timeline (BSI) and transition criteria (IAF MD26)
	ISO/IEC 19790:2025 (cryptographic modules) & **ISO/IEC 24759:2025** (testing)	ISO/IEC	Official ISO 19790:2025 fact sheet Official ISO 24759:2025 fact sheet

Table 2 | Laws passed or in force in the second half of 2025.

These legal and technical standards, both national and international, reflect meaningful progress toward consolidation of a global cybersecurity regulatory framework focused on operational resilience, critical infrastructure protection, and technology risk management.

5.2 Major arrests in the field of cybersecurity

During the second half of 2025, international law-enforcement and judicial cooperation against cybercrime remained highly active. Multiple operations were conducted during the period to neutralize threat actors and dismantle criminal infrastructure associated with ransomware, crime-as-a-service, hacktivism, and financial fraud.

These actions, coordinated across **Europol, INTERPOL, Eurojust, the U.S. Department of Justice, and multiple national security agencies**, reflect a sustained shift toward collaborative disruption models in which technical intelligence and cross-border cooperation directly affect criminal operational capacity.

The table below summarizes the major operations conducted in the second half of 2025, highlighting outcomes and the roles of the participating agencies.

Operation	Threat sector group	Security forces and agencies	Results	References
Eastwood	Pro-Russian hacktivism (**NoName057(16)**)	Europol, Eurojust, authorities in Germany, France, Spain, Sweden, Switzerland, and the US.	Dismantling of **>100** infrastructure systems; part of the core taken offline; **6** arrest warrants (DE).	Europol – Eastwood
Arrest of XSS.is admin	Underground ecosystem/sale of access and malware	French National Police, Paris Public Prosecutor's Office, SBU (Ukraine), Europol	Arrest of alleged admin; platform with **>50k** users; profits **>€7M**.	Europol – Press Release
Checkmate (BlackSuit/Royal)	Raas/extortion	U.S. Department of Justice (DOJ), FBI, international partners	**4 servers** and **9 domains** seized; **≈$1M** seized.	DOJ Press Release
Zeppelin Case	Ransomware/crypto money laundering	DOJ (US), FBI	Seizure of **>USD 2.8 million** in crypto, **USD 70k** in cash, and a vehicle; indictment of Ianis A. Antropenko.	DOJ – Zeppelin Indictment
Contender 3.0	Online fraud/BEC/mass phishing	INTERPOL + 25 African countries	**260 arrests**, **81** criminal organizations dismantled; **1,463** victims; losses **≈$2.8 million**.	INTERPOL Press Release

Table 3 | Major operations to dismantle cybercriminal gangs carried out in H2 2025.

Operation	Threat sector group	Law enforcement agencies	Results	References
Serengeti 2.0	Transnational cybercrime (ransomware, fraud, BEC)	INTERPOL + 18 African countries and the United Kingdom	**1,209 arrests**, **11,432** malicious infrastructures dismantled; **USD 97.4 million** recovered.	INTERPOL Press Release
SIMCARTEL Takedown	Crime-as-a-Service (SIM-box/OTP bypass/telecom fraud)	Europol, Eurojust, Latvian police, Austria, Estonia, Finland	**7 arrests**, **1,200** SIM boxes, **40,000** SIM cards, **5** servers; losses **≈€4.5 million (AT)** and **€420k (LV)**; 2 websites seized.	Europol SIMCARTEL
Collins Aerospace arrest/ EU airports	Intrusion/Disruption of critical infrastructure	NCA (United Kingdom), collaboration with European forces	1 arrest in the UK; investigation ongoing; incident reported on **Sept. 19**.	NCA Press Release
Eurojust–Europol Crypto Fraud	Investment Fraud/Money Laundering	Eurojust, Europol, authorities in France, Belgium, Cyprus, Germany, and Spain	**9 arrested**; network defrauded **>€600M** via fake "investment platforms."	Eurojust Case Release
Endgame – phase Nov-2025	Malware/Crime-as-a-Service (Rhadamanthys infostealer ecosystem, VenomRAT RAT, Elysium botnet)	Europol, Eurojust, and LEAs from 10 countries (including the US, UK, DE, FR, CA, AU, NL, GR)	**1,025 servers** dismantled/disrupted; **20 domains seized;** main **VenomRAT** suspect **arrested in Greece (Nov. 3, 2025)**	Europol (official) BleepingComputer The Hacker News
Arrest in Phuket (Thailand)	APT/State-sponsored (espionage) – alleged links to Void Blizzard/ColdRiver (press)	Cyber Crime Investigation Bureau (Thailand) in coordination with FBI (US)	**1 arrested (Nov. 6, 2025);** devices seized; **extradition proceedings to the US** initiated	AP (NPR/AP syndication)
US DOJ – Account Takeover Fraud	Financial fraud	US Department of Justice (DOJ), FBI	Seizure of domain and infrastructure; database with stolen credentials; estimated losses **≈USD 14.6 million**; **more than 5,100 victims**.	DOJ Press Release
Sentinel	Online fraud/BEC/ransomware	INTERPOL + 19 African countries	**574 arrests**; **approximately USD 3 million recovered**; dismantling of transnational criminal networks and closure of malicious infrastructure.	INTERPOL Press Release

Table 3 | Major operations to dismantle cybercriminal gangs in the second half of 2025.

Featured case: Operation Eastwood — Dismantling of the pro-Russian hacktivist network NoName057(16)

In July 2025, **Europol**, with **Eurojust** and law enforcement authorities in Germany, France, Spain, Sweden, Switzerland, and the United States, conducted **Operation Eastwood** targeting **NoName057(16)**, one of the most active pro-Russian hacktivist networks since the start of the war in Ukraine (EUROPOL, 2025).

The group was responsible for thousands of coordinated DDoS attacks against critical infrastructure, government entities, and European media outlets, primarily in countries supporting Ukraine.

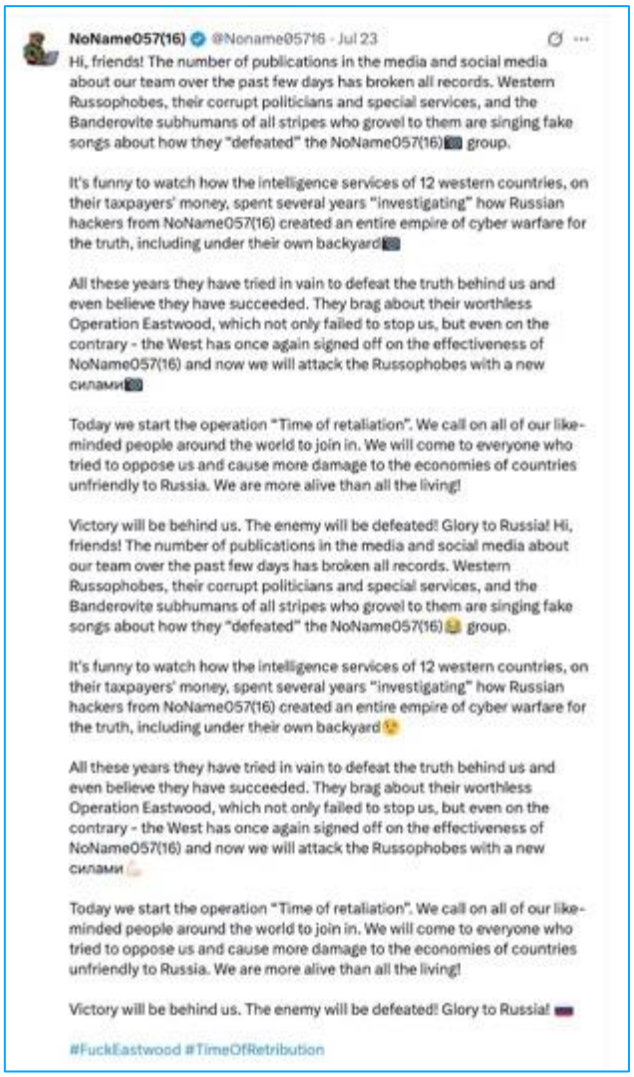
The operation dismantled a distributed infrastructure of more than one hundred servers used to coordinate attacks and manage the DDoSIA platform, which enabled automation of denial-of-service campaigns through a gamified "volunteering" model.

In addition, seven international arrest warrants, six of them issued in Germany, were issued for individuals identified as key members of the group, and two arrests were made in Europe, in France and Spain.

Investigations also identified more than a thousand active users across Telegram recruitment channels, many of whom received cryptocurrency incentives for participating in attacks.

The significance of **Operation Eastwood** extends beyond the technical domain. It represents a milestone in international cooperation against coordinated hacktivism, as it is the first multinational operation of its kind to neutralize a network by combining judicial, law enforcement, and cyber intelligence capabilities.

The approach adopted by participating agencies reflects operational maturity, prioritizing infrastructure neutralization, prosecution of responsible individuals, and dismantling of the digital financing and recruitment model that sustained the campaign.



NoName057(16) @Noname05716 · Jul 23

Hi, friends! The number of publications in the media and social media about our team over the past few days has broken all records. Western Russophobes, their corrupt politicians and special services, and the Banderovite subhumans of all stripes who grovel to them are singing fake songs about how they "defeated" the NoName057(16) group.

It's funny to watch how the intelligence services of 12 western countries, on their taxpayers' money, spent several years "investigating" how Russian hackers from NoName057(16) created an entire empire of cyber warfare for the truth, including under their own backyard.

All these years they have tried in vain to defeat the truth behind us and even believe they have succeeded. They brag about their worthless Operation Eastwood, which not only failed to stop us, but even on the contrary - the West has once again signed off on the effectiveness of NoName057(16) and now we will attack the Russophobes with a new силами

Today we start the operation "Time of retaliation". We call on all of our like-minded people around the world to join in. We will come to everyone who tried to oppose us and cause more damage to the economies of countries unfriendly to Russia. We are more alive than all the living!

Victory will be behind us. The enemy will be defeated! Glory to Russia! Hi, friends! The number of publications in the media and social media about our team over the past few days has broken all records. Western Russophobes, their corrupt politicians and special services, and the Banderovite subhumans of all stripes who grovel to them are singing fake songs about how they "defeated" the NoName057(16) group.

It's funny to watch how the intelligence services of 12 western countries, on their taxpayers' money, spent several years "investigating" how Russian hackers from NoName057(16) created an entire empire of cyber warfare for the truth, including under their own backyard

All these years they have tried in vain to defeat the truth behind us and even believe they have succeeded. They brag about their worthless Operation Eastwood, which not only failed to stop us, but even on the contrary - the West has once again signed off on the effectiveness of NoName057(16) and now we will attack the Russophobes with a new силами

Today we start the operation "Time of retaliation". We call on all of our like-minded people around the world to join in. We will come to everyone who tried to oppose us and cause more damage to the economies of countries unfriendly to Russia. We are more alive than all the living!

Victory will be behind us. The enemy will be defeated! Glory to Russia!

#FuckEastwood #TimeOfRetribution

Illustration 1 | NoName057(16)'s public statement of intent and call to action against Operation Eastwood.

In strategic terms, **Operation Eastwood** illustrates the evolution of the European approach to geopolitically motivated hacktivism, highlighting that hybrid tactics and the mobilization of "digital volunteers" are now treated as a structured transnational threat.

This case reinforces the trend toward closer collaboration among law enforcement agencies, judicial bodies, and private-sector partners to respond in an integrated way to complex threats that combine political, technical, and financial motivations.

6. Dark web insights

During the second half of 2025, the underground forum ecosystem underwent a significant reconfiguration, driven by sustained pressure from law enforcement agencies, the dismantling of critical infrastructure used by high-profile actors, and the fragmentation of long-established communities.

Although large traditional hubs continue to lose traction, new platforms are emerging that absorb part of the flow of criminal activity, while others disappear or transform due to arrests, seizures, or internal conflicts.

This period is characterized by three key dynamics:

- **Continuous disruption of established forums**, causing mass migration and loss of trust among actors.
- **The emergence of alternative spaces or the resurgence of pre-existing communities**, which are positioning themselves as new centers of activity.
- **Increased use of parallel channels (Telegram, Tox, private panels)** in response to the growing perception of risk in public and semi-private forums.

This context requires adapting CTI monitoring to a more distributed and opaque environment, in which prestige and digital reputation have become critical factors in accessing useful intelligence for decision-making.

6.1 The fall of DarkForums: the last giant to collapse

DarkForums, the natural heir to BreachForums and one of the nerve centers of cybercrime in 2025, collapsed during the second half of the year in a process that was as rapid as it was revealing.

What had started as a refuge for actors expelled from other forums ended up collapsing under its own weight, driven by growing law enforcement pressure, internal conflicts, and technical deterioration that was impossible to hide.

First came rumors of infiltration. Then came failures in access systems, constant outages, and accusations among moderators. By September, the most veteran members were already publicly recommending abandoning the platform. By November, migration to Telegram, Tox, and other private channels was massive. In a matter of weeks, **DarkForums** went from being "the new **BreachForums**" to becoming a ghost town, with no activity or credibility.

The fall of DarkForums not only marks the end of the last major centralized forum, but also symbolizes a structural change in the criminal ecosystem. Threat actors, traditionally active in deep and dark web forums, are showing a loss of confidence even in these relatively stable infrastructures and are opting for more fragmented, ephemeral, and compartmentalized environments, such as private channels, temporary markets, or encrypted platforms, which are much more opaque and difficult to monitor.

6.2 Active underground forums

During the second half of 2025, the underground forum ecosystem remains active despite the fall of **DarkForums** and constant law enforcement pressure on Russian- and English-speaking communities. Activity is redistributed to more fragmented platforms, technical niches, and private enclaves that serve as meeting points for criminal actors of varying levels of sophistication.

The most relevant and active forums during this period are highlighted below.

- **Exploit.in** has more than 15 years of activity and remains the epicenter of Russian-speaking technical cybercrime. It is one of the few forums with real continuity after multiple crashes of other spaces, and maintains a highly experienced community where 0-days, RCE exploits, intrusion kits, and high-value initial access circulate.
- **Dread** has regained its activity after months of instability due to DDoS attacks and has once again become the major social hub of the darknet. It acts as an "underground Reddit" where market crashes, vendor reputations, law enforcement operation analyses, and scam alerts are discussed.
- **Cracked.io** resurged strongly following Operation Talent and remains one of the most active forums in the English-speaking ecosystem. Its content is dominated by exposed credentials, stealer configurations, automated tools, leaks, and low/medium-level intrusion tutorials.
- **Nulled.to** has historically been considered one of the largest cracking and leak forums and maintains a solid user base. It is dedicated to sharing leaked databases, technical manuals, malicious scripting, and easy-to-adopt attack tools.
- **Sinister.ly** combines hacker culture aesthetics with technical content focused on phishing, carding, offensive automation, and Python development. This mix makes it popular among young profiles who are beginning to enter the ecosystem, serving as an "**informal academy**" where accessible but effective techniques are shared.
- **RAMP (Ransomware Affiliate Market Place)** is not a traditional forum, but it remains a critical hub for the **ransomware** and **RaaS operations**. Throughout 2025, it hosts affiliate recruitment ads, panel tests, and sales of access used for intrusions associated with ransomware groups.
- **The Post-XSS ecosystem of fragmented subforums and Russian** clans emerged after the fall of **XSS.is**, with several successor communities attempting to fill the space left by what was once one of the largest Russian-speaking criminal forums.
- **RuTor/Ru.Tor** is not a criminal forum in the strict sense, but its semi-clandestine community functions as an environment where lightweight malware, carding tools, anti-fraud services, cashout methods, and scripts for criminal automation circulate.
- **KernelForum/Kern3l** is an advanced technical forum focused on malware development, reversing, loaders, crypters, and offensive OPSEC. Although small in size, the technical quality of its users makes it a space where new techniques often appear before they are used in real campaigns.
- **Communities specializing in botnets and stealers (R0 Crew, etc.)** include small forums dedicated specifically to cracking stealer panels, exchanging configurations for popular botnets (RedLine, Lumma, Raccoon, etc.), and selling logs. Although modest in volume, they are very useful for identifying new variants, distribution patterns, and developments in the commoditized malware ecosystem.
- **KickAss Forum** is an emerging forum that has gained relevance among malware developers for its focus on loaders, crypters, custom panels, and private malware. It is increasingly used by actors seeking more "premium" tools without exposing themselves in mass forums.

During the second half of 2025, a change in dark web activity was observed, marked by an increase in the sale of logs and compromised access, driven by infostealer malware infections and growing demand for stolen credentials.

Main publications on the dark web (H2 2025)

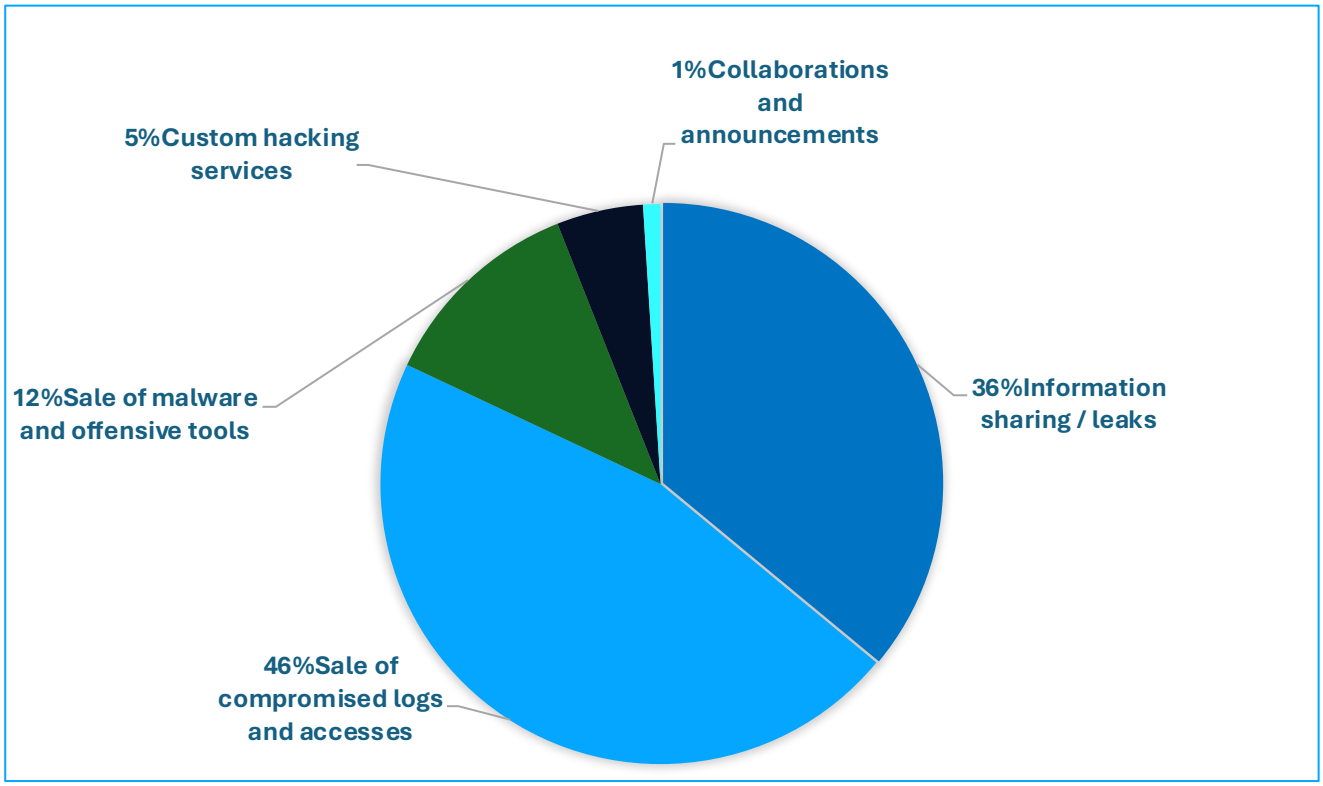


Figure 5 | Main categories of publications on the dark web in the second half of 2025.

The estimated data shows a criminal ecosystem increasingly oriented toward **monetizing access** and exploiting credentials, while public leaks are losing ground due to the fragmentation of traditional forums. At the same time, activity in **malware and offensive tools** continues to rise, consolidating these categories as key elements of the second half of 2025.

6.3 Active underground markets

During the second half of 2025, the underground market ecosystem has continued to show sustained activity, albeit with significant structural changes compared to previous periods. Disruptions to generalist marketplaces have not led to a reduction in criminal volume, but rather to a **reconfiguration of the ecosystem**, characterized by greater fragmentation, functional specialization, and a growing dependence on markets oriented toward data, access, and services associated with intrusion.

Infostealer logs continue to be one of the most sought-after assets on the underground. Families such as **Lumma**, **RisePro**, and **RedLine** continue to be recurrent in this ecosystem, with large volumes of credentials in circulation and a clear prioritization of frequent inventory updates. This model reinforces the role of markets as direct providers of initial access, closely connected to ransomware and fraud campaigns.

Consolidated markets

- **Russian Market** remains one of the main hubs for stolen credentials and stealer logs. Its model of constant updating and high inventory turnover makes it a key player in the criminal supply chain, especially for Initial Access Brokers (IAB) and ransomware operators.
- **Brian's Club** continues to be a **historical benchmark for carding**, with a significant volume of compromised cards. Although carding is losing relative importance compared to the sale of access and credentials, it remains a structural market within the financial fraud ecosystem.
- **Exodus Market** is gaining relevance as a market focused on the **sale of privileged access, exploits, and intrusion-related services**, with a particular focus on corporate environments. It stands out for its implementation of stricter reputation and verification mechanisms, indicative of increasing professionalization.

Markets in decline or collapse

- **Abacus Market**, after its prominence during the first half of 2025, suffered **critical disruptions in July**, ending with its collapse. The signs observed point to a probable exit scam, reinforcing the trend of instability of generalist DNMs and the loss of confidence in centralized platforms.
- During the period analyzed, **multiple short-lived general-purpose marketplaces** with limited volume and brief life cycles were observed, none of which succeeded in establishing themselves as relevant actors within the ecosystem.

Emerging markets and alternative spaces

- **Exploit.in** has established itself as one of the main venues for **selling initial access**, including RDP, VPN, corporate credentials, and persistent access. During the second half of 2025, there was an increase in offers related to business environments, reinforcing its role as a reference space for IAB.
- **2easy Market** is a marketplace specializing in **infostealer logs and stolen credentials**, with a strong presence of reusable corporate access. Its operating model, focused on the availability and search for recent credentials, increases its value for actors operating in the early stages of intrusion.
- **Styx Market** is a marketplace focused on **tools and services for phishing campaigns**, kits, and operational support for malware distribution. During this period, it remains a significant platform for supporting intrusion operations.
- **B1ack's Stash** is identified as an **emerging carding marketplace**, focused on the sale of stolen cards and recent dumps. Its emergence reflects the fragmentation of financial fraud, with short-lived platforms, high commercial aggressiveness, and rapid monetization.
- **TorZon Market** is a generalist DNM that has absorbed part of the residual traffic following the collapse of other marketplaces, although without achieving a dominant position. Its activity reflects the **partial shift of traffic** toward less established alternatives.
- **Other fragmented markets and spaces** includes low-profile IAB forums, private log search services, resales of derivative datasets (including models inherited from dismantled markets), and closed channels accessible by invitation. This category reflects the high degree of fragmentation and decentralization observed in the second half of the year.

Evolution of the underground marketplace ecosystem

During this half-year, there has been a **significant redistribution of activity** compared to the first half of 2025, marked mainly by the decline of generalist marketplaces and the increase in the relative weight of platforms focused on access, credentials, and intrusion services.

The previous disappearance of players such as **Abacus Market** and **Breach Forums** has not led to a reduction in criminal volume, but rather a shift in activity toward specialized markets, IAB-centric forums, and private channels, as well as toward less visible and more difficult to monitor environments. In this context, platforms such as **Russian Market**, **Exploit.in**, and specialized markets such as **Exodus Market** have increased their operational relevance.

Likewise, **greater fragmentation of the ecosystem** can be observed, with the emergence of multiple niche markets, especially in **carding** and the sale of initial access, characterized by shorter life cycles, lower public visibility, and rapid inventory turnover.

During the second half of 2025, several of these actors have been frequently associated with intrusion and ransomware campaigns, acting as suppliers of initial access, stolen credentials, and reusable data. This model reinforces the role of **underground marketplaces as critical infrastructure within the cybercrime value chain**, beyond their traditional function as simple trading platforms.

In terms of **operational communication**, although **Telegram** continues to be a leading platform, a sustained increase in the use of private channels and end-to-end encrypted applications (such as Signal, TOX, and decentralized solutions) has been identified. This trend responds to a greater perception of risk on the part of criminal actors and the search for less exposure to infiltration, infrastructure seizures, and OSINT monitoring.

Below is the estimated distribution of the main underground sales platforms active during the second half of 2025, based on their observed activity volume and relevance within the cybercriminal ecosystem.

Underground sales platforms (H2 2025)

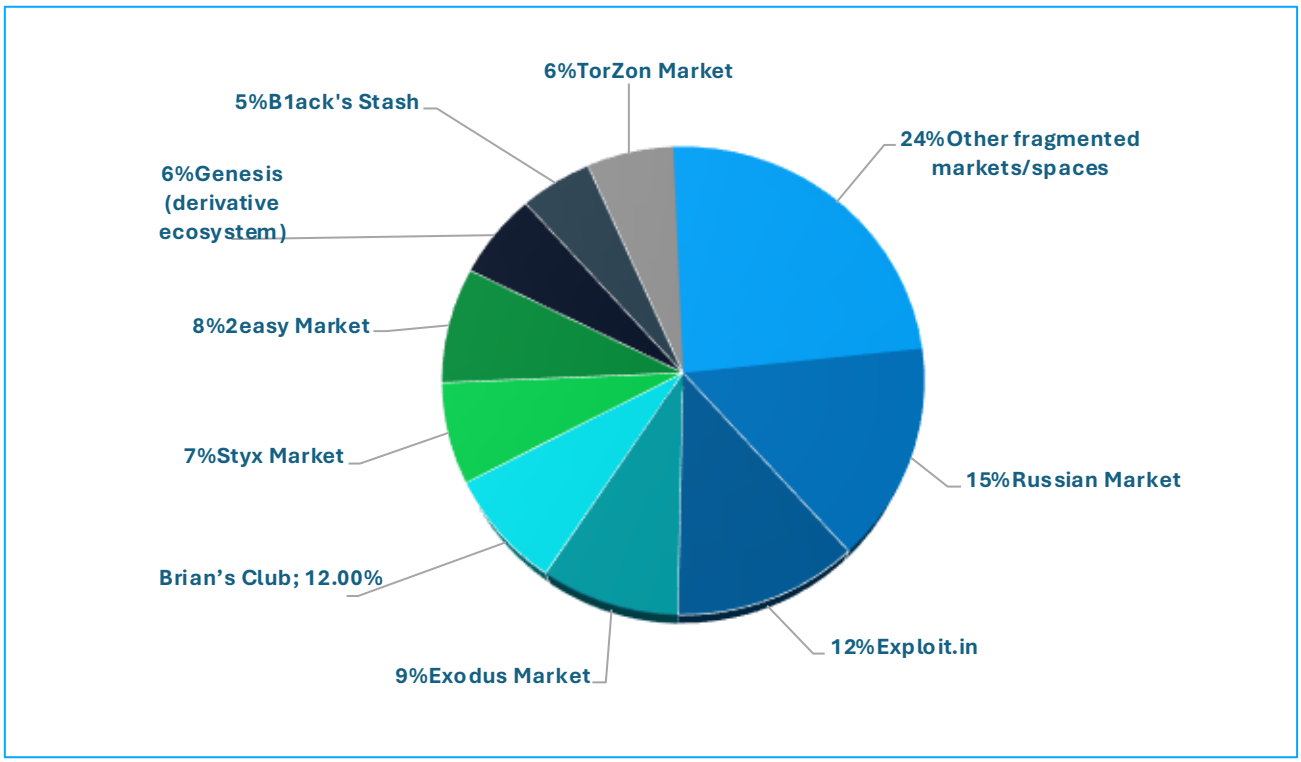


Figure 6 | Main underground sales platforms identified in the second half of 2025.

7. Threat actors

The period confirmed a more hybrid and harder-to-attribute ecosystem, where cybercrime, espionage, and hacktivism converge in techniques, infrastructure, and objectives.

Selective exfiltration, advanced social engineering, and abuse of legitimate services predominated, while small, agile groups and temporary alliances proliferated, sharing TTPs and amplifying the impact of their operations.

7.1 Newly identified threat actors

The previous report anticipated increased collaboration between criminal groups, as well as progressive convergence between cybercrime and cyber espionage. The newly identified threat actors during this period clearly illustrate this evolution, with small, highly dynamic groups and flexible structures combining extortion techniques, covert intrusions, and the exploitation of legitimate access. Their activity reflects a more fragmented landscape, in which the separation between financial and operational motivations has blurred and selective data exfiltration has become the dominant vector.

FulcrumSec

Detected in September 2025, **FulcrumSec** stands out for focusing exclusively on extortion through data exfiltration, without **deploying ransomware**, and then publishing the data on its leak site (clearnet and dark web) or Telegram channel, with the intention of selling the database to a single buyer and maximizing profit. Its main targets are high-profile companies. Although only two notable victims in the technology sector—both involved in the global distribution of components and solutions—have been publicly confirmed to date, the group's "wall of fame" suggests access to highly sensitive data, including personally identifiable information (PII) and corporate secrets, from at least a dozen multinational corporations through exposed backend systems. However, its Telegram channel and dark web site have been inactive since early November, with no confirmation of a complete disappearance or a temporary hiatus to prepare for new attacks (Shenouda, 2025).

NetMedved

This actor was identified in mid-October 2025 as responsible for a campaign targeting mainly companies in Russia. Its tactic includes **phishing** emails containing ZIP files with deceptive access (an LNK file disguised as an invoice or business request), to deploy **NetSupportRAT** malware for espionage or subsequent movement within the network. This combination of social engineering, abuse of legitimate tools such as PowerShell scripts, multiple delivery domains, and persistence suggests a more refined tactical evolution, possibly inherited from previous campaigns (Shenouda, 2025) (AlienVault, 2025).

Zestix

Zestix is an emerging actor in December 2025, focused on **data exfiltration and direct sale**, without the use of ransomware. Its most notable operation involved accessing legal and customer information from Mercedes-Benz USA through the supply chain by compromising third parties that managed sensitive documentation. The group demonstrates prior reconnaissance, selection of high-value files (legal strategies, claims, corporate data), and rapid monetization through underground forums. It has also been credited with two database sales containing project information from a Turkish robotics company and a Peruvian mechanical and gas engineering company. Its activity reflects a growing trend of new and loosely structured actors combining classic intrusion techniques with an almost corporate intelligence orientation, prioritizing indirect access and strategic data over massive volumes (Shenouda, 2025).

7.2 Ransomware

Ransomware has evolved toward data-based extortion models, greater affiliate autonomy, and sustained global expansion. Alliances between groups have strengthened coordination, resource sharing, and public pressure campaigns, consolidating a more professionalized ecosystem geared toward maximizing visibility and monetization.

7.2.1 New groups

The temporal distribution shows an expanding but highly volatile ecosystem (DarkFeed, 2025). July and August recorded the highest volume of new groups, reflecting an entry phase by opportunistic actors and the consolidation of data-based extortion models, with SLH marking a milestone that accelerated cooperation among groups.

September brought an additional layer of specialization, with niche-oriented groups (crypto, selective leaks, aggressive branding), signaling maturity and segmentation in the criminal market.

From October onward, operational noise increased with rebranding and short-lived groups, whereas in November activity volume declined even as the technical profiles of newly identified threat actors became more defined.

Overall, the pattern confirms a half-year marked by early-to-mid proliferation, diversification at the midpoint, and specialization toward the end of the period.

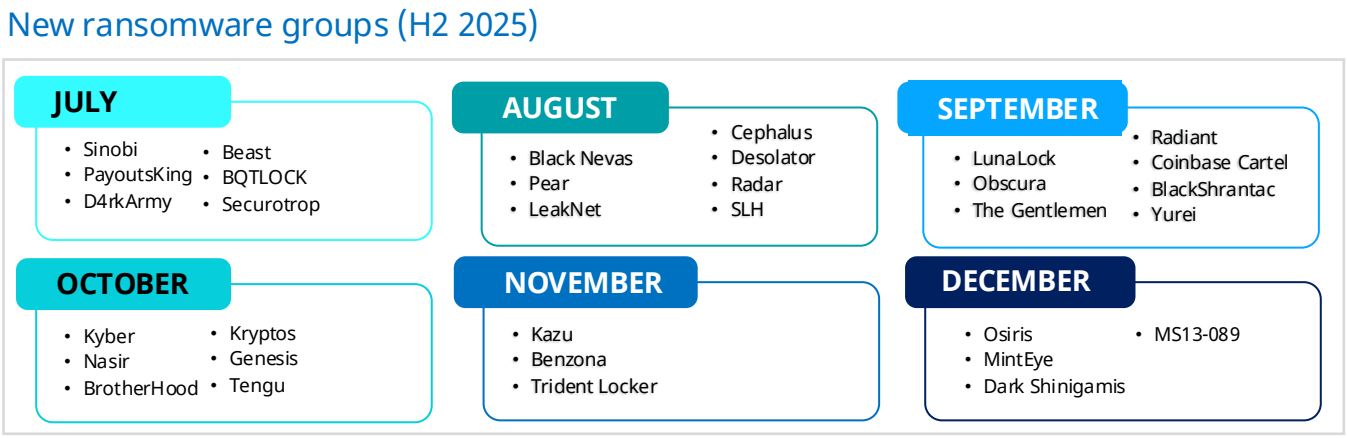


Figure 7 | Ransomware groups detected in the second half of 2025.

This period, the **Scattered LAPSUS$ Hunters (SLH)** collective has stood out, representing an operational merger between three of the most notorious criminal groups: **Scattered Spider**, **LAPSUS$**, and **ShinyHunters**. It emerged in August 2025 as a federated model of extortion and data exfiltration. Under this umbrella, the groups shared Telegram channels to coordinate operations, recruit affiliates, and amplify public pressure campaigns, reflecting a hybrid structure that combines cybercrime operations with underground branding strategy. SLH operates primarily through **extortion as a service (EaaS)**, calling on associates to demand payments in exchange for use of its established reputation, and has used classic social engineering techniques, spear-phishing, SIM swapping, and compromise of platforms such as Salesforce to gain initial access and exfiltrate sensitive data. This alliance illustrates a concerning trend of closer collaboration between previously independent groups, with exchanges of tactics and resources that make attribution more difficult and increase the impact of global extortion campaigns (Lakshmanan, 2025).

7.2.2 Most active groups

Ransomware activity in the second half of the year remained high and stable, but with a more pronounced feature than in previous periods, namely operational fragmentation and affiliate mobility, reflecting a more mature, decentralized, and competitive RaaS market.

- **Qilin** has established itself as the main magnet for affiliates in the period. Its growth has been driven less by disruptive technical innovation and more by its ability to capitalize on destabilization across other RaaS groups, offering operational continuity, stable infrastructure, and reliable monetization. It represents an industrialized and scalable ransomware model, closer to a platform than a traditional group.
- **Akira** has maintained a steady top-tier presence without sharp peaks, suggesting a stable core of affiliates and well-integrated campaigns in the RaaS market. Its persistence reinforces the trend toward sustained, lower-risk operations that prioritize continuity and profitability over visibility or aggressive expansion.
- **INC Ransomware** stands out as an example of accelerated growth during the period, with a clear focus on high-impact targets. Its evolution points to rapid positioning through more selective campaigns, making it relevant to explaining the shift toward critical sectors and environments with higher time pressure for negotiation.

- **Play** has reinforced its role as a consistent player, aligned with less sophisticated but sustained campaigns over time. Its behavior fits an ecosystem in which profitability comes from repetition and standardization rather than technical innovation or sector specialization.
- **Safepay** shows an irregular evolution, with a progressive reduction in activity until November, followed by an abrupt rebound in December. This pattern suggests a selective reactivation strategy consistent with controlled growth and lower operational exposure, focusing on mid-sized organizations and exploiting attack surfaces less saturated by large RaaS operators.

Top ransomware groups (H2 2025)

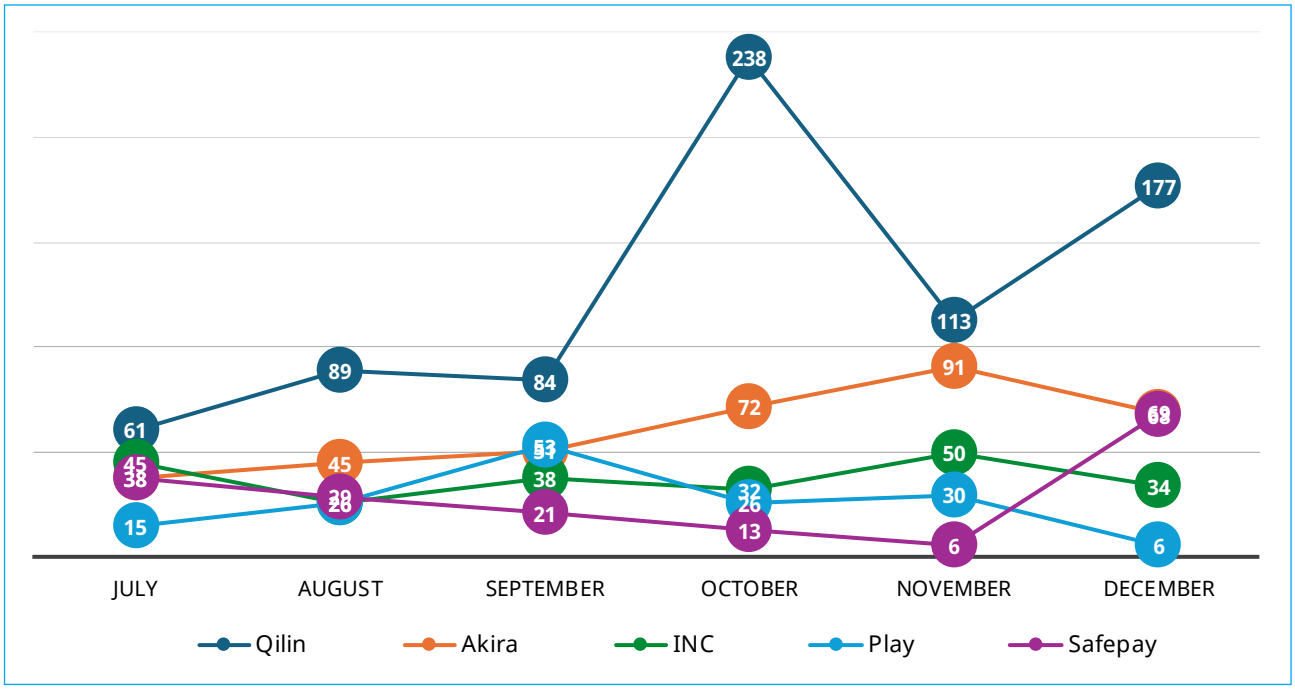


Figure 8 | Activity of the most active ransomware groups in the second half of 2025.

7.2.3 Global impact

The geographic distribution of victims confirms that ransomware groups continued to concentrate activity in developed economies, with a clear epicenter in the **United States** and gradual expansion into Europe, Asia-Pacific, and, to a lesser extent, the Middle East. In the July–December data, the United States remained consistently the primary target (from 280 to 461 incidents per month) (DarkFeed, 2025), consolidating its position as the "world capital of ransomware" in terms of asset value, digital maturity, and payment capacity, rather than population or market size.

In second place is a set of highly exposed Western countries. The **United Kingdom, Germany, France, Canada, Spain, and Italy** show sustained figures and, in some cases, notable growth during the quarter (for example, Canada and France tripled their figures in October).

This pattern is consistent with victimization concentrated in North America and Europe, where complex supply chains, high dependence on digital services, and regulatory frameworks requiring incident reporting increase statistical visibility.

Starting in September, diversification toward Asia-Pacific and other regions was also observed.

South Korea, India, Thailand, Japan, and Australia gained prominence, and in October significant activity was also recorded in the United Arab Emirates, indicating extension of campaigns toward the Middle East.

In these regions, the RaaS model and ecosystem fragmentation facilitate simultaneous campaigns across multiple geographies.

Overall, the trend in the second half of the year points to a dual axis. Total volume remains concentrated in the United States and Western countries, as discussed in the previous report, while operations show an increasingly globalized focus, with affiliates rotating infrastructure and victim lists across regions to maximize pressure, avoid saturating local defenses, and exploit regulatory or cybersecurity maturity windows that vary by country.

Countries most affected by ransomware (H2 2025)

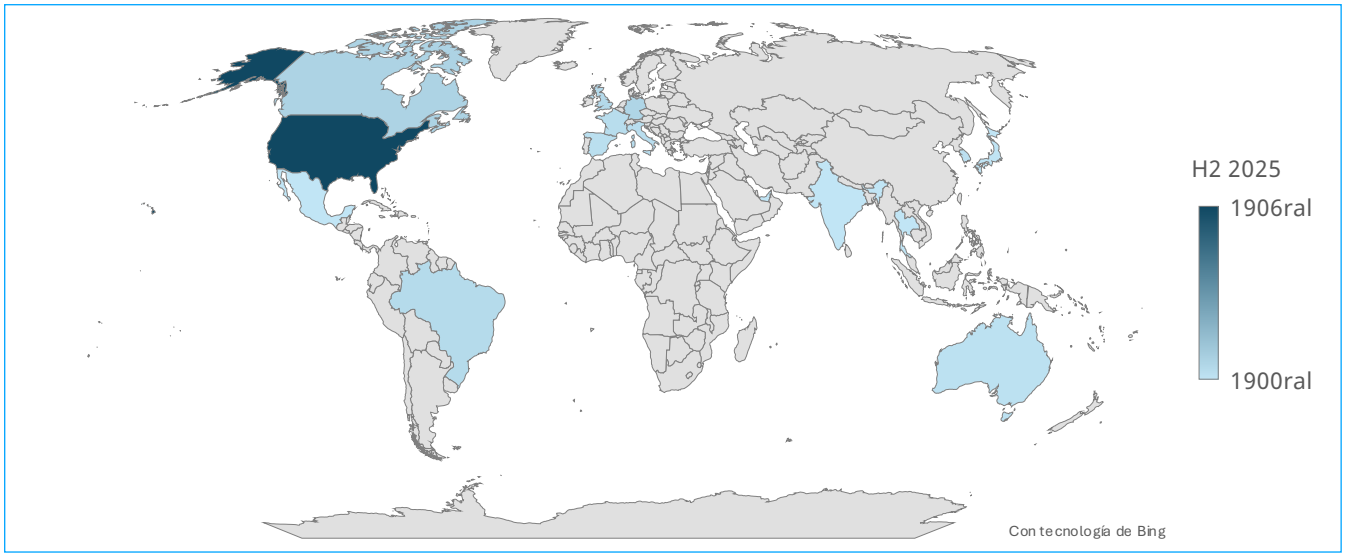


Figure 9 | Countries most affected by ransomware in the second half of 2025.

On the other hand, sectoral analysis for the second half of 2025 confirms sustained concentration of ransomware impact in sectors with high operational dependency and low tolerance for disruption, rather than those that are simply more digitized.

Consulting (professional services+legal) is the main aggregate sector for the period, with clear growth since October.

Manufacturing has maintained constant and cross-cutting pressure, driven by exposure of hybrid IT/OT environments, the criticality of industrial systems, and the high costs associated with production stoppages. This core is complemented by **retail** and **discretionary consumption**, which is sensitive to second-half seasonality, and IT and professional services, whose attractiveness lies in the potential to generate chain-reaction impacts across multiple organizations.

From a structural perspective, the half-year demonstrates the strategic maturity of the ransomware ecosystem, as actors prioritize sectors where time, regulatory, or reputational pressure accelerates victim decision-making.

Healthcare, **public administration**, and **education** have remained consistently affected, not because of volume but because of their coercive value, while the sustained weight of these sectors reinforces the shift toward attacks designed for operational impact rather than broad mass exploitation. The difference compared to previous periods is not a change in target sectors, but tighter target optimization, with campaigns more closely aligned to business cycles and sustained pressure, indicating that this risk pattern is likely to persist through 2026.

Ransomware attacks by sector (H2 2025)

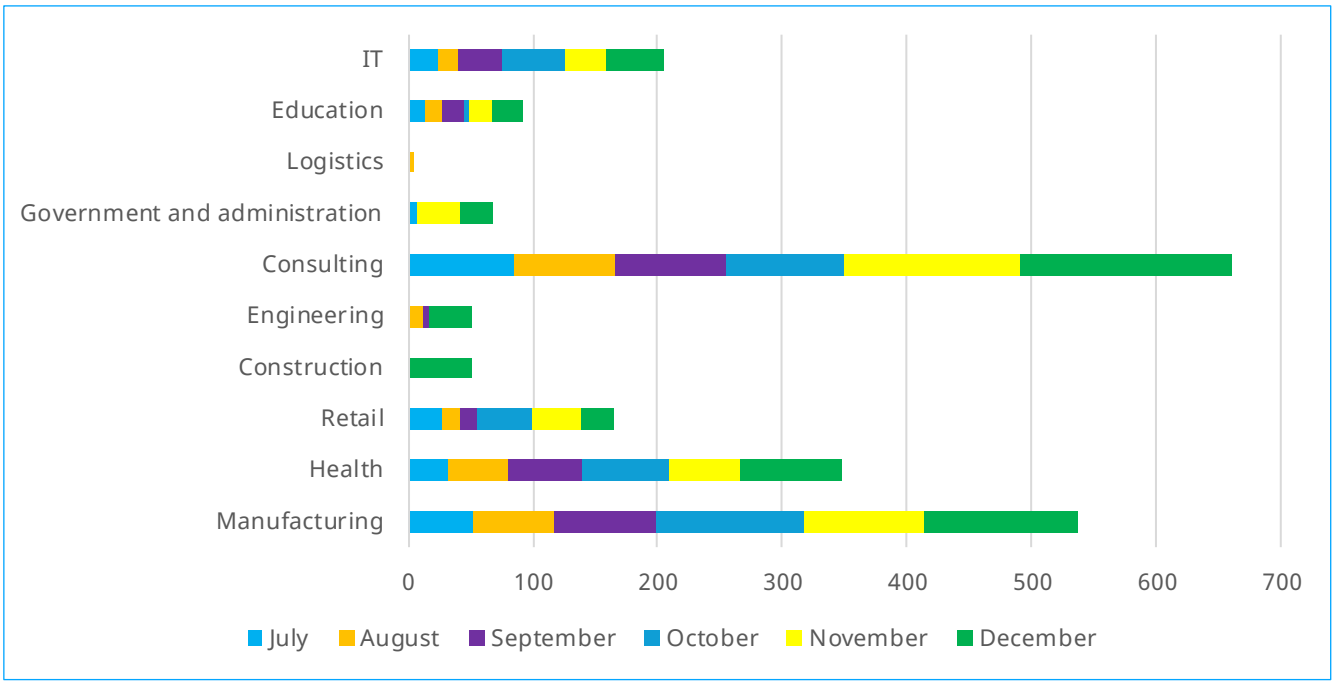


Figure 10 | Sectors most affected by ransomware in the second half of 2025.

7.3 Hacktivism

During the second half of the year, there has been a clear intensification of hacktivism, characterized less by the emergence of new actors and more by **consolidation of coordination models between groups** and closer alignment with defined geopolitical agendas (FalconFeeds.io, 2025).

The ecosystem has structured itself around regional blocs and ideological affinities, with the pro-Russian environment standing out on one side, organized around groups such as **NoName057(16)** and **Anonymous Russia**, which have operated as coordination nodes and capability aggregators.

These groups have acted as the backbone of distributed campaigns, mainly targeting infrastructure, institutions, and entities associated with NATO countries and Ukraine.

At the same time, a second bloc has consolidated in the Asia-Pacific environment, particularly active in Southeast Asia and organized around **BD Anonymous, Nullsec Philippines,** and **Cyber Team Indonesia**, where multiple groups have operated under a federated logic, sharing resources, narratives, and objectives, enabling regional campaigns with greater reach and persistence, and compensating for limited technical capabilities through volume, continuity, and coordination in specific time windows.

A third axis has been formed by actors aligned with the Palestinian cause and other related anti-Western and political-religious ideological currents, such as **Al-Mujahideen Force 313, Red Eye of Palestine, and Cyber Islamic Resistance**, which have progressively increased transregional cooperation.

These groups have shown greater interconnection with other geographic clusters, amplifying visibility and impact, especially during periods of high geopolitical tension.

The analysis also identifies several **connector groups** that function as high-level nodes, facilitating spread of TTPs and infrastructure between ecosystems. **BD Anonymous** is the most frequent player in alliances during this period, **NoName057(16)** and **Dark Storm Team** play a hub role in the pro-Russian environment, Keymous+ and Clobelsec provide stable links among groups from Bangladesh, the Middle East, Europe, and Russia, and **Hezi Rash, Hider_Nex,** and **LunarisSec** reinforce the technical network toward the end of the period.

Observed activity confirms a profile geared toward disruption and symbolic pressure rather than deep espionage, with DDoS attacks, defacements, selective leaks, and propaganda amplification, alongside heavy reuse of infrastructure, known tools, and cross-group claims to maximize visibility.

Overall, the second half of the year confirms hacktivism's evolution toward a more organized, coordinated, and persistent model, based on flexible alliances among groups that are **highly reactive to the geopolitical context** and able to sustain prolonged campaigns and direct attacks against targets of high symbolic and operational value. This pattern reinforces the risk of synchronized actions with greater impact against critical infrastructure and strategic entities across multiple regions.

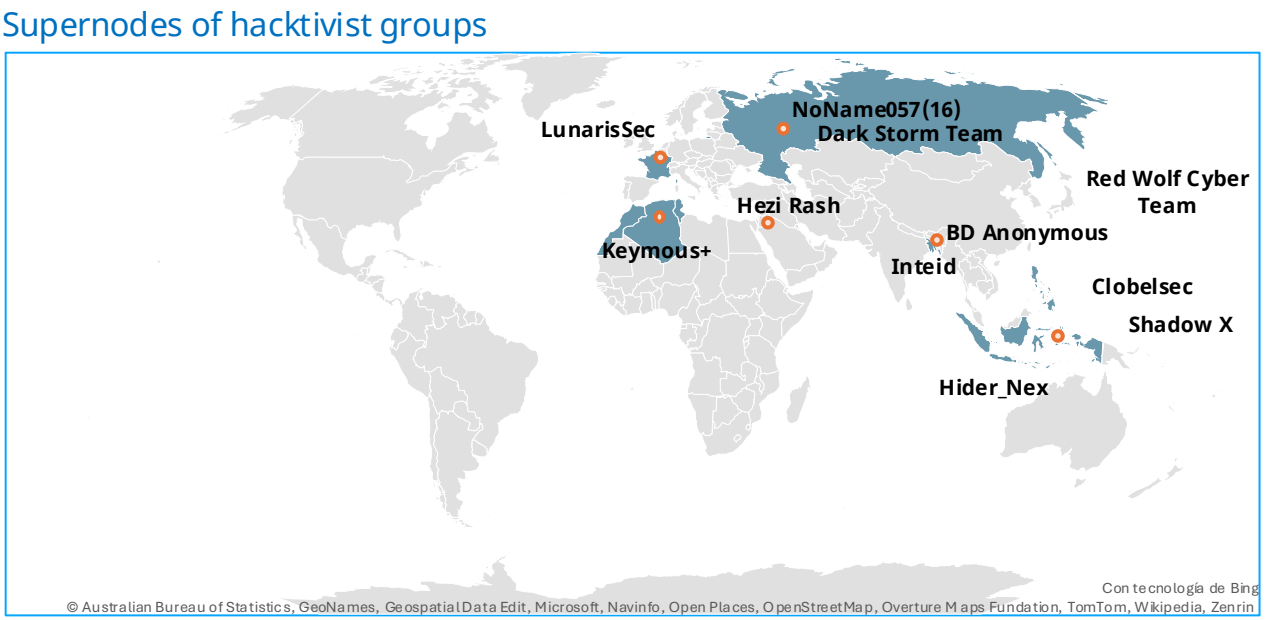


Figure 11 | Hacktivist connector groups by geographic location.

7.4 APT

Between July and December 2025, a clear pattern emerged: higher technical sophistication, geographic expansion of campaigns, and growing emphasis on long-term commitments that deliver strategic advantages, both geopolitical and economic (ESET Research, 2025).

- **Russian APTs**

In the second half of the year, activity shifted from overt aggression in the first half to a strategy of prolonged infiltration, with active campaigns focused mainly on Ukraine and European states. Among prominent actors, **RomCom** exploited a zero-day vulnerability in **WinRAR (CVE-2025-8088)** to distribute malware and establish persistent access, while **Gamaredon** remained one of the most active groups, characterized by large-scale spear-phishing campaigns, intensive use of customized malware, and high infrastructure turnover, aimed at tactical espionage and intelligence collection in Ukrainian and European government entities. **Sandworm** maintained its profile of destructive and disruptive operations by deploying wipers such as **ZEROLOT** and **Sting** against government, energy, and logistics entities. Activity from the **InedibleOchotense** cluster was also identified, focusing on spear-phishing with payloads that combine legitimate tools and proprietary backdoors. Finally, the hacktivist ecosystem showed less operational convergence than in the first half of the year, as DDoS campaigns and information leaks remained frequent, but technically coordinated operations decreased and execution became more fragmented.

- **Chinese APTs**

Campaigns identified during the second half of the year showed diversification of targets, mainly transportation, government, manufacturing, and education. Persistence increased more than new capability breadth, as political and strategic intelligence operations with long operational cycles were prioritized. Intense activity was observed from groups such as **Mustang Panda**, **Flax Typhoon**, **Speccom**, and **FamousSparrow**, the latter particularly active in Latin America with intrusions into multiple governments.

A notable increase was observed in the use of adversary-in-the-middle (AitM) techniques for initial access and lateral movement, as well as exploitation of routers, updates, and other vectors. Compared to the first half of the year, no equivalent to large malware pieces (such as **NanoSlate**) was detected, but rather incremental optimization of existing arsenals and greater confidence to deploy backdoors, as observed in groups such as **SinisterEye** and **PlushDaemon**.

- **Iranian APTs**

The Iranian focus shifted toward infiltration and social engineering through more credible and harder-to-detect techniques, reinforcing the global trend toward covert persistence. **MuddyWater** stood out for intensifying global spear-phishing campaigns by using compromised internal mailboxes to send malicious emails, a technique already identified in the first half of the year. Other actors such as **BladedFeline** (part of **OilRig**) and **GalaxyGato** evolved their arsenals, incorporating DLL-search-order hijacking and new versions of backdoors such as C5, designed for credential theft, persistence, and evasion. Primary targets remained government agencies and strategic sectors in the Middle East, with expansion into Europe and Central Asia, consolidating a broader and more technical espionage presence.

- **North Korean APTs**

Groups linked to North Korea maintained a high level of activity, combining espionage with operations aimed at generating income for the state, consolidating a hybrid APT–crime model. Actors such as **Lazarus**, **Kimsuky**, **DeceptiveDevelopment**, and **Konni** maintained diversified campaigns targeting governments, diplomacy, technology, and especially the cryptocurrency sector.

During this period, **Kimsuky** and **Lazarus** engaged in unprecedented cooperation, aligning espionage capabilities with technical exploitation in coordinated global campaigns. **Kimsuky** initiates intrusions with targeted emails (for example, academic invitations with FPSpy malware and keyloggers) to map networks and collect credentials.

Once environments are compromised, Lazarus exploits zero-day vulnerabilities and distributes malicious packages that gain SYSTEM privileges and deploy the InvisibleFerret backdoor, designed for EDR evasion and exfiltration of high-value assets (including crypto).

Both groups use a shared infrastructure for coordination, execution, and cleanup, and have targeted critical sectors such as defense, finance, energy, and blockchain.

This alliance has reinforced the trend toward more integrated APT operations, where the combination of espionage and financial cybercrime techniques increases the effectiveness of campaigns (De Jong, 2025).

NSFOCUS, 2025 identifies the following factors as defining the period::

Key trends in APT groups (H2 2025)

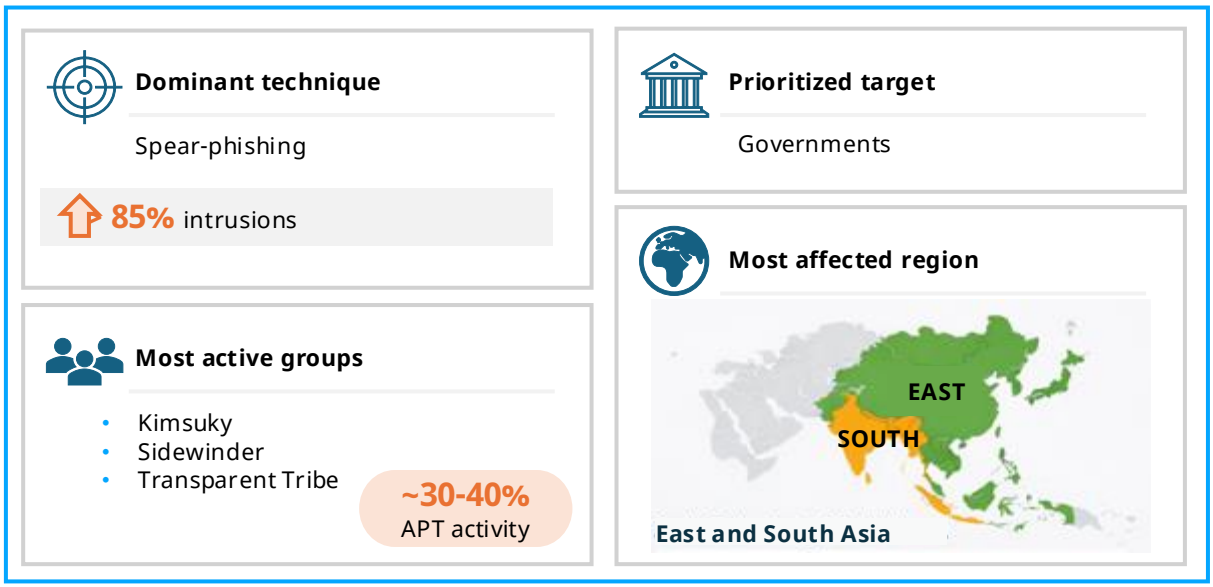


Figure 12 | Key trends for APT groups during the second half of 2025.

Analysis of the second half of 2025 confirms a predominance of persistent espionage campaigns by APTs aligned with China, North Korea, and South Asian groups, compared to a more disruptive and destructive component in actors linked to Russia and, to a lesser extent, Iran. This operational differentiation, shaped by the geopolitical context, reveals clear regional patterns and enables anticipation of a shift toward longer-lasting, stealthier intrusions designed to secure medium- and long-term strategic advantages.

8. Tactics, Techniques and Procedures (TTPs)

During the second half of 2025, **NTT DATA's Cyber Threat Intelligence** team analyzed the evolution of tactics, techniques, and procedures (TTPs) used by cybercriminal groups and geopolitically motivated actors. The analysis confirms a clear trend that attackers do not rely primarily on radically new techniques, but on a combination of familiar TTPs executed with greater speed, scale, and automation, increasingly supported by artificial intelligence-based tools.

Data collected in industry benchmark reports shows that financially motivated cybercrime continues to dominate the global landscape, accounting for more than 70% of interactive intrusions observed in the last year (CrowdStrike, 2025). In this context, ransomware, multiple extortion, identity abuse, and exploitation of exposed infrastructure remain the operational pillars of most campaigns.

8.1 Most common TTPs used by cybercriminals

Compared to the first half of 2025, the TTPs observed in the second half did not introduce new techniques within the MITRE ATT&CK framework, but they did reflect a shift in how **existing techniques are used and combined**. There was increased emphasis on techniques related to **persistence, credential access, and defense evasion**, in contrast to the more direct and noisy approaches seen in the previous semester. The **exploitation of valid identities and remote services**—particularly in cloud environments—also gained prominence, while data exfiltration became more firmly established as a precursor to ransomware, reinforcing double extortion schemes.

Overall, the second half of 2025 **reflects greater operational maturity among threat actors**, who are more focused on maintaining access and maximizing impact than on deploying novel techniques.

Tactic	MITRE ATT&CK ID	Description
Persistence (TA0003)	T1098 – Account Manipulation	threat actors modify existing accounts (local users, cloud accounts, or service accounts) to maintain persistent access and hinder detection.
	T1136.001 – Create Account: Local Account	Creation of additional local accounts to ensure persistence after initial access.
	T1547.001 – Startup Execution: Registry Keys/Startup Folder	Establishing persistence through auto-start keys on Windows systems.
	T1133 – External remote services	Use of exposed services (RDP, VPN, web applications) to access or persist in the compromised environment.
	T1098.004 – Account manipulation: Additional cloud keys	Adding keys, tokens, or credentials in cloud environments to maintain persistent access.
Privilege escalation (TA0004)	T1134 – Access token manipulation	Misuse of tokens to execute actions under a context of higher privilege.
	T1548 – Abuse of privilege escalation mechanisms	Exploiting weak configurations or inadequate controls to elevate privileges.

Table 4 | Most common TTPs during the second half of 2025.

Tactic	MITRE ATT&CK ID	Description
Defense Evasion (TA0005)	T1562.001 – Disable or modify security tools	Disabling antivirus, EDR, or protection mechanisms to avoid detection.
	T1562.004 – Modify or disable system firewall	Alteration of firewall rules to facilitate attacker communication.
	T1070.001 – Indicator removal: Deleting logs	Deleting system logs to hide traces of the intrusion.
	T1564.008 – Hiding artifacts: email concealment rules	Use of email rules to hide malicious communications or data exfiltration.
Access to credentials (TA0006)	T1003 – OS credential dump	Extraction of credentials stored in memory or system files.
	T1552 – Unprotected credentials	Obtaining credentials stored in plain text, scripts, or configurations.
	T1528 – Application access token theft	Theft of valid tokens for accessing remote applications and services.
Discovery (TA0007)	T1046 – Network service discovery	Enumeration of services and ports to identify additional targets.
	T1082 – Discovery of system information	Obtaining details about operating system and hardware.
	T1016 – Network configuration discovery	Identifying network topology and connections using native commands.
	T1057 – Process Discovery	Enumeration of active processes to identify security software or critical targets.
	T1087.001 – Account Discovery: Local Account	Enumeration of local user accounts to facilitate subsequent movements.
Lateral movement (TA0008)	T1021 – Remote Services	Use of RDP, SMB, or other services to move laterally within the network.
Exfiltration (TA0010)	T1041 – Exfiltration over command and control channel	Exfiltration of data through channels already established with the attacker.
Impact (TA0040)	T1486 – Data encryption for impact	Encryption of systems and files as part of ransomware campaigns.
	T1490 – System recovery inhibition	Deletion or deactivation of backups to prevent recovery.

Table 4 | Most common TTPs during the second half of 2025.

8.2 Most common entry vectors

During the second half of 2025, entry vectors used by cybercriminals remained broadly consistent with those observed in the first half of the year. However, **NTT DATA's Cyber Threat Intelligence** analysis confirms that their relevance lies not in technical novelty, but in their **consolidation as silent, persistent, and low-visibility initial access mechanisms**.

In contrast with earlier periods, initial access increasingly depends on **identities, legitimate credentials, organizational trust relationships, and the abuse of correctly configured services**, rather than on the direct exploitation of visible vulnerabilities.

Identity as an access vector	Identity-oriented social engineering	Cloud environments and APIs
The abuse of valid identities is becoming one of the main mechanisms for initial access. Threat actors use stolen credentials, session cookies, and access tokens to operate without deploying malware, significantly reducing visibility and increasing detection time. This vector favors prolonged intrusions and facilitates lateral movement from early stages.	Use of social engineering techniques aimed at obtaining credentials or user consent, including vishing, technical support spoofing, BEC campaigns, and abuse of common authentication flows. This vector exploits trust in everyday processes and allows initial access without the need for direct technical exploitation.	Increased initial access through configuration errors in cloud environments, excessive permissions, exposed API keys, and abuse of trust relationships between services. This vector is particularly relevant in hybrid and multicloud architectures, where visibility and control are more limited.
Advanced infostealers	**Unauthorized software/shadow IT**	**Abuse of legitimate remote services**
Evolution of the use of infostealers as a structural preliminary phase to ransomware attacks, fraud, and unauthorized access. The automated theft of credentials, cookies, and browser data positions this vector as one of the most effective of the semester, both for its scalability and its low operating cost.	Use of professional tools and software downloaded outside official channels as an initial gateway. This vector takes advantage of operational pressure and trust in seemingly legitimate applications, introducing persistent access and reducing security detection and update capabilities.	Use of RDP, VPN, and remote administration tools with valid credentials as an initial access mechanism. This vector allows threat actors to operate through legitimate services, minimizing the technical footprint of access and complicating early detection by defensive teams.

Table 5 | Most common entry vectors used in the second half of 2025.

Overall, during the second half of 2025, initial access no longer relies primarily on obvious technical failures and increasingly centers on **identities, trust, and the legitimate use of services**. This approach raises the difficulty of early detection and increases potential impact by enabling adversaries to establish access without generating immediate alerts or clearly anomalous behavior.

This evolution reinforces the need to secure initial **access through a combined approach that includes technical controls, identity management, visibility into cloud environments, and oversight of human processes**, laying the foundation for understanding the operational evolution described in attack innovation.

8.3 Innovation in attacks: new techniques and tactics

During the second half of 2025, innovation in cyberattack campaigns has not manifested in the emergence of radically new techniques within the MITRE ATT&CK framework, but in **a structural shift in adversary operating logic**. Unlike the more direct and opportunistic approaches observed in the first half of the year, the second half consolidated a model based on **persistence, automation, and systematic exploitation of trust**, where the objective is not only to compromise systems, but also to embed within normal organizational processes over an extended period. This shift does not appear in the initial access phase, described in the section on entry vectors, but rather in how **threat actors operate once inside the compromised environment** — how they manage time, minimize detection signals, and maximize final impact.

From noisy attacks to prolonged, low-profile operations

One of the main differences from the first half of the year is the **deliberate reduction of technical noise**.

Threat actors increasingly prioritize hands-on-keyboard techniques, the use of legitimate system tools, and human-assisted execution rather than mass deployment of persistent malware. Threat hunting reports confirm that a growing proportion of interactive intrusions occur without deploying traditional malware, making early detection difficult and significantly extending dwell time in compromised environments (CrowdStrike, 2025).

In this context, **time becomes a strategic asset for the adversary**. Prolonged presence allows actors to understand the environment, identify critical assets, observe operational patterns, and prepare the final impact with greater precision. This approach reflects a clear transition from opportunistic campaigns to **selective operations**, where value lies less in initial speed and more in remaining undetected while fragmenting defensive signals across multiple domains (identity, endpoint, and cloud).

Industrialization of ransomware and consolidation of multiple extortion

During the second half of the year, ransomware ceased to be a one-off impact technique and became a **highly structured business process**. Available data indicates that global revenues associated with ransomware payments exceed $2 billion, reflecting the economic and organizational maturity of the model (Financial Crimes Enforcement Network [FinCEN], 2025).

Innovation lies less in encryption itself and more in **comprehensive campaign orchestration**. Threat actors automate classification of stolen information, prioritize the most sensitive data, and use partial and staged leaks as a bargaining mechanism. This model reinforces double and triple extortion schemes and reduces reliance on encryption as the sole means of pressure, allowing monetization even without fully disrupting victim operations.

Artificial intelligence as a tactical accelerator, not a substitute

While artificial intelligence appeared primarily as an emerging trend in the first half of the year, the second half of 2025 reflects its practical and systematic integration across multiple phases of attack activity. AI is used to accelerate specific tasks including generating social engineering content, linguistic and cultural adaptation, analysis of victim background information, and support for developing and modifying malicious tools (IBM Security, 2025).

In malware development, documented cases include tools built or adjusted with AI support to reduce coding errors, improve obfuscation, or adapt payloads to different operating environments (ESET, 2025; Garaschenko, 2025). However, these developments still require human oversight, confirming that AI **does not replace the operator but rather reduces the cognitive and operational burden of the attack**, enabling campaigns to scale with less effort and at greater speed.

Exploiting trust and organizational processes as an operational vector

A clear differentiator in the second half of the year is the **instrumentalization of legitimate organizational processes as a central element of attack strategy**. Beyond initial access, threat actors leverage processes such as hiring, technical collaboration, remote work, and everyday use of professional tools to **normalize their presence within the organization**.

Campaigns have been identified in which malicious actors use synthetic identities and AI-based assistance to pass technical interviews, integrate into teams, and maintain prolonged access to internal systems. These tactics shift the focus from technology infrastructure to **operational and cultural trust**, expanding the attack surface and blurring the boundary between external and internal threats (CrowdStrike, 2025).

Speed of exploitation and time pressure on defense

The second half of the year brought a **sharp reduction in defensive response times**. Critical vulnerabilities are exploited increasingly quickly after public disclosure and are integrated almost immediately into automated campaigns. This behavior increases pressure on defensive teams and disproportionately impacts organizations with slow patch cycles, limited visibility, or dependence on manual processes (Arctic Wolf, 2025; Wright, 2025).

The combination of automation, artificial intelligence, and criminal specialization turns the public disclosure of a vulnerability into an **asymmetric race** in which threat actors can respond more quickly than many organizations on the defensive.

Overall, the second half of 2025 marks a qualitative evolution from the first half of the year with **less emphasis on initial access and greater emphasis on how to operate inside organizations undetected**. Innovation is expressed not in isolated new techniques, but in the combination of persistence, automation, artificial intelligence, and abuse of trust to execute more targeted, durable, and profitable attacks.

This dynamic reinforces the need to approach cybersecurity not only as a technological discipline, but as a comprehensive capability that includes **processes, organizational culture, and contextual detection** that can interpret weak signals and activity distributed across multiple domains.

9. Vulnerabilities

The second half of 2025 consolidated critical vulnerabilities as one of the main vectors of initial compromise, with a clear pattern of rapid exploitation, targeted campaigns, and recurring use of zero-days. The activity observed reflects a sustained reduction in the time between disclosure, and in some cases even before disclosure, and active exploitation, demonstrating a high level of operational maturity among threat actors.

During this period, exploitation was not limited to opportunistic attacks, but was integrated into **structured campaigns** combining initial access, lateral movement, and persistence.

Below is a monthly analysis of the most notable vulnerabilities of the period, serving as a basis for understanding the major campaigns detected.

- **July:**

The vulnerability known as **SharePoint ToolShell Exploitation** refers to an exploitation campaign targeting on-premises **Microsoft SharePoint** servers that were not properly patched. The campaign relied on critical security flaws that enabled remote code execution and impersonation techniques, resulting in full compromise of affected systems.

Initial reporting associated the exploit with **CVE-2025-49706** and **CVE-2025-49704**, which were later expanded and correlated with **CVE-2025-53770** and **CVE-2025-53771**. These vulnerabilities exposed on-premises SharePoint installations to elevated risk in organizations that delayed applying security updates

The campaign was attributed to several advanced threat actors. These include **Storm-2603**, a ransomware actor linked to China, as well as **Threat Group-3390** and **ZIRCONIUM**, the latter mainly associated with cyber-espionage activity. The diversity of actors involved underscores the strategic value of these vulnerabilities and their use for both economic and intelligence objectives.

Information and attribution for this campaign is documented by **MITRE ATT&CK**, where it is listed as a specific exploitation campaign under the corresponding identifier and serves as a reference for analysis and mitigation of this type of threat (MITRE, 2025).

- **August:**

The **Directory Traversal** vulnerability in **WinRAR** corresponds to a critical security flaw identified in the Windows version of the compression software. This weakness allows an attacker to manipulate internal paths within compressed files to write or execute files outside the intended directory, enabling arbitrary code execution on the victim's system.

Registered as **CVE-2025-8088**, the vulnerability was exploited through specially crafted compressed files. When opened by a user, these files enabled silent installation of malicious code without requiring elevated privileges or additional interaction, directly compromising the integrity of the affected system.

The flaw was actively exploited globally, notably by the **RomCom** threat group, an actor aligned with Russian interests. **RomCom** used the vulnerability as an initial access vector to deploy backdoor malware, enabling remote control, persistence on compromised systems, and subsequent malicious activity.

Technical information and monitoring of this vulnerability were documented by multiple threat intelligence sources, which warned of active exploitation and the need to update WinRAR to mitigate risk associated with this attack vector (Strobes, 2025).

September:

The arbitrary code execution vulnerability in **Windows** refers to a critical security flaw that allowed execution of malicious code on affected systems through user interaction. This directly compromised the confidentiality, integrity, and availability of vulnerable Windows systems.

This vulnerability could be used as an initial access vector leading to code execution and compromise of the affected endpoint, without necessarily requiring elevated privileges.

Identified as **CVE-2025-9491**, the vulnerability was actively exploited prior to release of an official patch. Its abuse affected the confidentiality, integrity, and availability of compromised systems.

Exploitation was attributed to the threat actor **UNC6384**, a group affiliated with China. The actor targeted high-value systems belonging to European diplomats in Belgium, Hungary, and other European Union member states, indicating a clear cyber-espionage motivation.

Information about this vulnerability and its exploitation has been recorded and serves as a reference for monitoring the threat and implementing security measures to prevent such attacks in Windows environments (Girnus, 2025).

- **October:**

The **CVE-2025-41244** vulnerability affected specific VMware components, including **VMware** Tools and VMware Aria Operations, and was associated primarily with local privilege escalation scenarios on vulnerable systems. Several security advisories indicated signs of exploitation in real environments, reinforcing the need to urgently apply updates and mitigations published by the vendor.

While the vulnerability does not in itself enable remote code execution or lateral movement, its exploitation can strengthen an attacker's position after initial access, increasing the impact of an intrusion already underway within corporate infrastructures.

In campaigns observed during the period, once initial access was obtained through other vectors, threat actors used remote access tools such as **ScreenConnect** for interactive operation and persistence, as well as for lateral movement within the corporate network. These techniques should be understood as post-compromise TTPs rather than mechanisms inherent to direct exploitation of **CVE-2025-41244**.

The malicious activity associated with these attack chains was attributed to the **UNC5174** threat group, an actor with advanced capabilities and experience in complex enterprise environments, highlighting the risk posed by flaws in widely deployed virtualization platforms and the importance of disciplined vulnerability management and post-exploitation detection in **VMware** environments (SOCRadar, 2025; SOCRadar Extended Threat Intelligence, 2025).

- **November:**

In November 2025, a critical deserialization flaw in **Microsoft Windows Server Update Services (WSUS)** was identified and actively exploited. The vulnerability affected exposed **WSUS** servers and enabled remote code execution with system privileges, resulting in full compromise of the affected server.

Registered as **CVE-2025-59287**, the vulnerability was a zero-day during the initial exploitation period until **Microsoft** released the corresponding security patch. Threat actors used the flaw as an initial access vector, taking control of **WSUS** and using it as an entry point into internal infrastructure.

Following exploitation, threat actors deployed the **ShadowPad** modular backdoor, an advanced tool that provides persistent remote control, espionage capability, and command execution. The use of **ShadowPad** is particularly relevant because it is commonly associated with Chinese state-sponsored cyber-espionage groups, suggesting a strategic motivation behind the attacks.

Information about this vulnerability and its exploitation was documented in threat intelligence reporting that emphasized impact severity and the urgent need to apply the relevant security updates to mitigate risk associated with **CVE-2025-59287** (Lakshmanan, 2025).

- **December:**

In December 2025, a critical flaw **in React Server Components**, known as **React2Shell**, was identified and actively exploited. It affected exposed web applications using certain server-side **React** versions. The vulnerability enabled remote code execution on the target server, compromising the application and underlying environment without requiring prior authentication.

Registered as **CVE-2025-55182**, the vulnerability received a CVSS score of 10.0 due to its critical impact. The flaw stemmed from insecure handling of the deserialization process for data sent from browser to server via the **React Flight** protocol. By sending a single specially crafted HTTP request, an attacker could interfere with the application's internal logic and achieve execution of arbitrary **JavaScript** code with the same privileges as the affected application. This weakness directly impacted frameworks based on **React Server Components**, such as **Next.js**, significantly expanding the attack surface.

Following initial exploitation, multiple post-exploitation activities were observed on compromised systems, including download and execution of malicious loaders, covert installation of **Node.js**, creation of persistence mechanisms using **systemd**, **cron**, and **rc.local**, communications with command-and-control infrastructure hosted on public cloud services, network reconnaissance tasks, basic information exfiltration, and use of webhooks and **Canarytokens** to confirm successful intrusion.

Multiple investigations attributed exploitation to advanced threat actors mainly linked to China, including infrastructure associated with groups such as **Earth Lumia** and **Jackpot Panda**. However, publication of proof-of-concept code rapidly increased risk of opportunistic exploitation, expanding impact beyond state espionage, and reporting emphasized the urgent need to apply published security patches and review exposure of internet-accessible React applications to mitigate risk associated with **CVE-2025-55182** (Westman y Sophos, 2025).

Trends in the exploitation of these vulnerabilities

The second half of 2025 confirms and reinforces trends already observed during the first half of the year, which **anticipated increasingly early and systematic exploitation of critical vulnerabilities** as the main initial access vector. Far from stabilizing, abuse of high-impact flaws intensified during the second half of the year, consolidating a scenario marked by increasingly narrow exposure windows between disclosure and active exploitation.

As predicted in the first half of 2025, threat actors prioritized vulnerabilities in widely adopted **enterprise technologies**, including Microsoft platforms, virtualization infrastructures, mass-market software, and modern web components.

Exploitation observed during the second half of the year was not solely opportunistic, but was repeatedly integrated into **structured campaigns** across both cyber-espionage operations and financially motivated activity.

The monthly analysis for the period also confirms another forecast from the first half of the year, **namely that exposure of critical services, hybrid environments, and internet-accessible applications** continues to amplify the impact of these vulnerabilities.

Persistent weaknesses in patch management and a lack of prioritization based on real-world exploitation remain determining factors. This reinforces the need for proactive and continuous vulnerability management approaches to reduce operational risk in real environments.

10. Future outlook

What to expect in 2026

Looking ahead to 2026, the cyber threat landscape points to a consolidation and deepening of the dynamics observed during 2025, rather than a radical disruption of the attack model. Cybercrime will continue to evolve toward highly specialized and persistent structures designed to maximize operational and reputational impact, supported by an increasingly fragmented but resilient underground economy.

The continued professionalization of ransomware, together with the reuse of infrastructure, affiliates, and tools from dismantled or weakened groups, will foster a more distributed ecosystem that is less dependent on specific brands, while state actors and ideologically aligned groups will further blur the line between espionage, sabotage, and economic crime by using cyberspace as a strategic domain for sustained pressure rather than as a vector for one-off attacks.

During 2026, a sustained increase in campaigns based on **silent persistence**, identity abuse, and exploitation of relationships of trust, both human and technical, is expected. The offensive use of artificial intelligence will continue to expand, less through disruptive techniques than as an accelerator of existing processes, including automated reconnaissance, advanced personalization of social engineering, generation of synthetic content, and optimization of target selection, further lowering barriers to entry into cybercrime and expanding the base of actors able to execute complex attacks.

At the same time, growing geopolitical fragmentation and digital deglobalization will reinforce the regionalization of threats, with campaigns aligned with active conflicts, national strategic interests, and economic tensions. Critical sectors, public administrations, technology infrastructures, and supply chains will continue to concentrate much of the risk, acting as amplifiers of the systemic impact of incidents.

In this context, 2026 is expected to be a year marked by **fewer visible attacks but more prolonged intrusions**, where value will lie not only in immediate exploitation but in threat actors' ability to remain inside compromised environments, influence decisions, shape operations, and monetize access flexibly over time.

11. References

- AlienVault (2025, November 26). *The 'Bear' attacks: what we learned about the phishing campaign targeting Russian organizations*. AlientVault. https://otx.alienvault.com/pulse/6926cae8043aabe58197d11e
- Arctic Wolf (2025). *2025 Arctic Wolf Threat Report*. Arctic Wolf. https://arcticwolf.com/resource/aw/arctic-wolf-threat-report-2025?lb-mode=overlay
- Aznar Fernández-Montesinos, F. (2025). *The great geopolitical challenge of the 21st century: Unbalanced multipolarity (IEEE Analysis Document 06/2025)*. Spanish Institute for Strategic Studies – Spanish Ministry of Defense. https://www.ieee.es/Galerias/fichero/docs_analisis/2025/DIEEEA06_2025_FAFM_Multipolaridad.pdf
- Check Point Research (2025). *Threat Intelligence Reports*. Check Point. https://research.checkpoint.com/intelligence-reports/
- Check Point Research (2025, JANUARY 14). *5 KEY CYBER SECURITY TRENDS FOR 2025*. Check Point. https://blog.checkpoint.com/research/5-key-cyber-security-trends-for-2025
- CrowdStrike (2025). *CrowdStrike 2025 Threat Hunting Report*. CrowdStrike. https://www.crowdstrike.com/en-us/resources/reports/threat-hunting-report/
- DarkFeed (2025). *RANSOMWARE GROUPS: 2025 ACTIVITY*. [X Publications]. X. https://x.com/ido_cohen2/
- De Jong, L. (2025, NOVEMBER 22). *Kimsuky and Lazarus join forces in coordinated attacks*. CYBERWARZONE. https://cyberwarzone.com/2025/11/22/kimsuky-and-lazarus-join-forces-in-coordinated-attacks/
- ESET (2025, September 2). *ESET discovers the first AI-based ransomware*. ESET. https://www.eset.com/pa/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/eset-descubre-el-primer-ransomware-basado-en-ia/
- ESET Research (2025, NOVEMBER 6). *ESET APT ACTIVITY REPORT Q2 2025–Q3 2025*. ESET. https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q2-2025-q3-2025.pdf
- ESET Research (2025, December 16). *ESET Threat Report H2 2025*. ESET. https://web-assets.eset.com/fileadmin/ESET/IT_2/Agenzia_Davide/H2-2025_Threat-Report.pdf
- EUROPOL (2025, July 16). *Global operation targets NoName057(16) pro-Russian cybercrime network*. EUROPOL. https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network
- FALCONFEEDS.IO (2025). *ALERT: NEW HACKTIVIST ALLIANCE*. [X Publications]. X. https://x.com/FalconFeedsio
- Financial Crimes Enforcement Network [FinCEN] (2025, December 4). FinCEN Issues Financial Trend Analysis on Ransomware. FinCEN. https://www.fincen.gov/news/news-releases/fincen-issues-financial-trend-analysis-ransomware
- Garaschenko, V. (2025, November 14). *AI Malware and LLM Abuse: The Next Wave of Cyber Threats*. SOC Prime. https://socprime.com/blog/latest-threats/ai-malware-and-llm-abuse/

- Girnus, P. (2025, March 18). *(0Day) Microsoft Windows LNK File UI Misrepresentation Remote Code Execution Vulnerability*. Trend Micro Zero Day Initiative. https://www.zerodayinitiative.com/advisories/ZDI-CAN-25373/
- Hernández, A. (2025, November 20). *The Internet on Russia's national security agenda: RuNet and digital sovereignty*. UCM. https://doi.org/10.5209/geop.95098
- IBM Security (2025). *IBM X-Force 2025 Threat Intelligence Index*. IBM. https://www.ibm.com/reports/threat-intelligence
- Khalil, M. (2025, November 29). *Cybersecurity Statistics 2025: Breach Costs, Ransomware & AI Threats*. DeepStrike. https://deepstrike.io/blog/cybersecurity-statistics-2025-threats-trends-challenges
- Lakshmanan, R. (2025, November 4). *A CYBERCRIME MERGER LIKE NO OTHER — SCATTERED SPIDER, LAPSUS$, AND SHINYHUNTERS JOIN FORCES*. The Hacker News. https://thehackernews.com/2025/11/a-cybercrime-merger-like-no-other.html
- Lakshmanan, R. (2025, NOVEMBER 24). *ShadowPad Malware Actively Exploits WSUS Vulnerability for Full System Access*. The Hacker News. https://thehackernews.com/2025/11/shadowpad-malware-actively-exploits.html
- Macías, E. (2025, October 15). *Mango suffers cyberattack through its supply chain*. COMPUTERWORLD. https://www.computerworld.es/article/4072830/mango-sufre-un-ciberataque-a-traves-de-su-cadena-de-suministro.html
- MITRE (2025, October 15). *SharePoint ToolShell Exploitation*. MITRE. https://attack.mitre.org/campaigns/C0058/
- NSFOCUS (2025, August 25). *NSFOCUS MONTHLY APT INSIGHTS – JULY 2025*. NSFOCUS. https://nsfocusglobal.com/nsfocus-monthly-apt-insights-july-2025/
- NSFOCUS (2025, SEPTEMBER 18). *NSFOCUS MONTHLY APT INSIGHTS – AUGUST 2025*. NSFOCUS. https://nsfocusglobal.com/nsfocus-monthly-apt-insights-august-2025/
- NSFOCUS (2025, NOVEMBER 12). *NSFOCUS MONTHLY APT INSIGHTS – SEPTEMBER 2025*. NSFOCUS. https://nsfocusglobal.com/nsfocus-monthly-apt-insights-september-2025/
- NSFOCUS (2025, NOVEMBER 28). *NSFOCUS MONTHLY APT INSIGHTS – OCTOBER 2025*. NSFOCUS. https://nsfocusglobal.com/nsfocus-monthly-apt-insights-october-2025/
- Pico, R. (2025, August 28). Elche is the latest city council to be blocked by a cyberattack. COMPUTERWORLD. https://www.computerworld.es/article/4047504/elche-es-el-ultimo-ayuntamiento-bloqueado-por-un-ataque-informatico.html
- SHENOUDA, J. (2025, OCTOBER 29). *NEW THREAT ACTOR: FULCRUMSEC*. SHENOUDA.NL. https://www.shenouda.nl/new-threat-actor-fulcrumsec/
- SHENOUDA, J. (2025, NOVEMBER 29). *NEW THREAT ACTOR: NETMEDVED*. SHENOUDA.NL. https://www.shenouda.nl/new-threat-actor-netmedved/

- SHENOUDA, J. (2025, DECEMBER 2). *NEW THREAT ACTOR: ZESTIX*. SHENOUDA.NL. HTTPS://WWW.SHENOUDA.NL/NEW-THREAT-ACTOR-ZESTIX/
- SOCRADAR (2025, OCTOBER 1). *VMWARE CVE-2025-41244 EXPLOITED: WHAT YOU NEED TO KNOW ABOUT THE LATEST FLAWS*. SOCRADAR. HTTPS://SOCRADAR.IO/BLOG/VMWARE-CVE-2025-41244-EXPLOITED/
- SOCRADAR EXTENDED THREAT INTELLIGENCE (OCTOBER 2025). *VMWARE CVE-2025-41244 EXPLOITED BY UNC5174 APT GROUP*. LINKEDIN. HTTPS://WWW.LINKEDIN.COM/POSTS/SOCRADAR_VMWARE-CVE-2025-41244-EXPLOITED-WHAT-YOU-ACTIVITY-7379088943851536385-ZS75/
- STAMFORD, C. (2025, JULY 29). *GARTNER FORECASTS WORLDWIDE END-USER SPENDING ON INFORMATION SECURITY TO TOTAL $213 BILLION IN 2025*. GARTNER. HTTPS://WWW.GARTNER.COM/EN/NEWSROOM/PRESS-RELEASES/2025-07-29-GARTNER-FORECASTS-WORLDWIDE-END-USER-SPENDING-ON-INFORMATION-SECURITY-TO-TOTAL-213-BILLION-US-DOLLARS-IN-2025
- STROBES (AUGUST 2025). *CVE-2025-8088*. HTTPS://VI.STROBES.CO/CVE/CVE-2025-8088
- VALDEOLMILLOS, C. (OCTOBER 20, 2025). *SPAIN IS THE FIFTH COUNTRY TO HAVE SUFFERED THE MOST CYBERATTACKS IN THE FIRST HALF OF 2025, ACCORDING TO MICROSOFT*. MCPRO. HTTPS://WWW.MUYCOMPUTERPRO.COM/2025/10/20/ESPANA-QUINTO-PAIS-CIBERATAQUES-PRIMERA-MITAD-2025-MICROSOFT
- WORLD ECONOMIC FORUM. (2025, JANUARY 13). *GLOBAL CYBERSECURITY OUTLOOK 2025*. WORLD ECONOMIC FORUM. HTTPS://WWW.WEFORUM.ORG/REPORTS/GLOBAL-CYBERSECURITY-OUTLOOK-2025
- WESTMAN, R., & SOPHOS COUNTER THREAT UNIT RESEARCH TEAM (2025, DECEMBER 11). *REACT2SHELL FLAW (CVE-2025-55182) EXPLOITED FOR REMOTE CODE EXECUTION*. SOPHOS. HTTPS://WWW.SOPHOS.COM/EN-US/BLOG/REACT2SHELL-FLAW-CVE-2025-55182-EXPLOITED-FOR-REMOTE-CODE-EXECUTION
- WRIGHT, R. (MARCH 31, 2025). CISA WARNS NEW MALWARE TARGETING IVANTI ZERO-DAY VULNERABILITY. CYBERSECURITY DIVE. HTTPS://WWW.CYBERSECURITYDIVE.COM/NEWS/CISA-WARNS-MALWARE-TARGETING-IVANTI-ZERO-DAY/743967/


NTT DATA