CyberProof®
A UST Company

2026
Global Threat Intelligence Report

Mapping Threats and Trends

ust.com

Executive summary

Cyber activity in 2025 reflected a decisive shift in how modern intrusions are conducted and scaled. Rather than relying on novel malware or perimeter exploitation alone, threat actors increasingly combined speed, coordination, and identity abuse to turn initial access points into high-impact incidents. Vulnerability exploitation remained a dominant entry vector, with a 17% increase from 2024 comparatively, but the year was defined by how quickly disclosed flaws were weaponized and how often the same vulnerabilities were exploited in parallel by state-aligned and criminal actors.

Enterprise platforms—ERP systems, collaboration servers, identity services, and SaaS ecosystems—became preferred targets because compromise translated immediately into privileged access, operational disruption, and leverage over regulated data.

Cyber Incidents by the numbers[1]:

31,020

United States:
Recorded 31,020 cyber incidents in 2025, making it the most targeted country by a large margin (largest global share).

7,144

Germany:
Reported 7,144 incidents, representing a significant portion of Europe's total cyberattack volume.

2,622

United Kingdom:
Logged 2,622 cyber incidents, reflecting persistent targeting in financial, telecom, and retail sectors.

2,581

Canada:
Saw 2,581 reported attacks, closely aligned with broader North American threat activity.

41,974

Singapore:
cybercrime cases reported in 2025 (88.9% were online scams).

csa.gov.sg

5,735

Malaysia:
cyber incidents reported to CyberSecurity Malaysia's Cyber999 hotline from January–September 2025.

thestar.com.my

15,877

Hong Kong:
Logged 2,622 cyber incidents, reflecting persistent targeting in financial, telecom, and retail sectors.

hkpc.org

5.5 billion

Indonesia:
cyber-attack "anomalies" detected by BSSN (National Cyber and Crypto Agency) throughout 2025 – reflecting all malicious traffic/attack attempts, a seven-fold surge over recent years.

lestari.kompas.com

Across the year's most significant cyber events, consistent patterns emerged.

SaaS supply-chain abuse allowed attackers to pivot across hundreds of organizations without exploiting core platforms directly. Ransomware campaigns increasingly targeted operational continuity rather than encryption alone, disrupting production lines, logistics, and customer-facing services, with AIenabled automation accelerating phishing, payload generation, and attack execution at scale.

In sectors such as retail, automotive, aviation, and manufacturing, cyber incidents produced tangible economic effects, drawing regulatory scrutiny and, in several cases, direct government intervention. Cyber risk in 2025 was no longer confined to IT environments—it routinely spilled into business continuity, market confidence, and national resilience.

Ransomware activity against **the global retail sector** increased by **58%** in Q2 2025 compared to Q1, with UK-based retailers experiencing the highest concentration of attacks.[2]
80% of retailers faced a cyberattack in 2025.[3]

The manufacturing sector saw the steepest increase in activity, with attacks surging **61%** compared with the previous year. Manufacturing accounted for 26% of all attacks in 2025.[4]

Ransomware activity targeting **the education sector** increased by **23%** in the first half of 2025.[5]

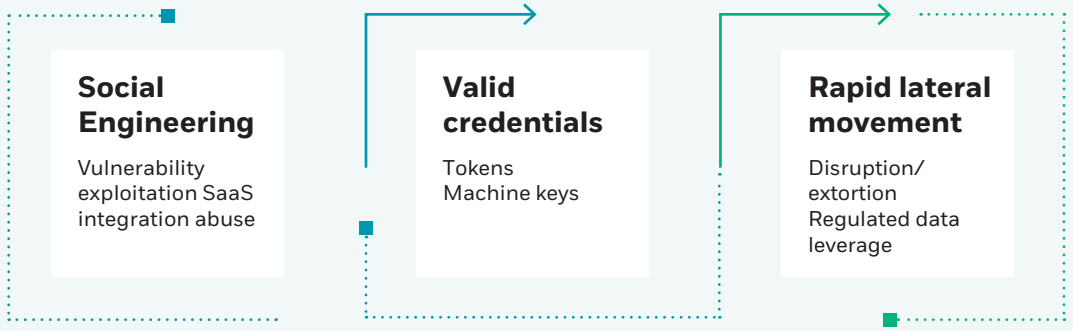
The threat landscape also tightened into fewer, repeatable playbooks. Criminal extortion groups adopted techniques traditionally associated with espionage, while state-aligned actors reused the same vulnerabilities, tooling, and access paths seen in financially motivated campaigns. Collaboration—formal and informal—became a force multiplier, with threat groups sharing infrastructure, affiliates, and tradecraft.

This ecosystem favored adaptation over novelty, enabling attackers to operate at a tempo that consistently outpaced defensive response. Cyber activity increasingly mirrored geopolitical escalation, unfolding alongside military and political events. This alignment extended the impact of conflicts beyond their immediate regions and into civilian and commercial environments.
These trends show that identity, cloud, and SaaS are now the primary targets for attacks, accounting for about 22% of incidents.[6]

Most major breaches involved attackers posing as legitimate users rather than exploiting technical vulnerabilities, through methods like IT staff impersonation or supply-chain compromise. This shift led to faster incident escalation, frequent operational and it also highlighted the limitations of traditional security. By 2025, identity assurance became the key security concern across industries.

The sections that follow break down how this played out across exploited vulnerabilities, major incidents, evolving attacker tradecraft, shifting threat environments, and cyber spillover from geopolitical conflicts.

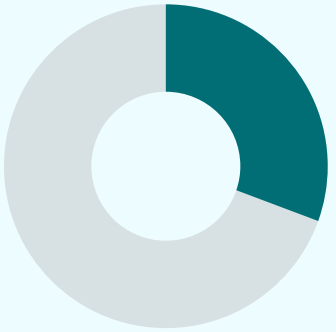
The 2025 intrusion model



How vulnerability exploitation shifted into business-critical systems

Vulnerability exploitation remained one of the most dominant intrusion vectors in 2025, but what distinguished this year was the unprecedented speed of weaponization and the clear shift toward business-critical platforms rather than traditional edge devices. Threat actors increasingly targeted ERP platforms, collaboration environments, SaaS identity layers, and browser credential stores—systems tightly connected to regulated data and privileged workflows. As a result, successful exploitation often triggered immediate operational impact, from data theft and impersonation of internal users to lateral movement into financial systems.

Another defining trend was the narrowing gap between statealigned and financially motivated operators, with both exploiting the same high-value common vulnerabilities and exposures (CVEs) within days of disclosure.



25–35%

Across observed intrusions, vulnerability exploitation accounted for an estimated **25–35%** of successful ransomware incidents.

With multiple CVEs abused within hours of becoming public—leaving defenders minimal reaction time.[7] A consistent pattern across incidents was the use of application-layer weaknesses, such as server-side request manipulation and insecure deserialization, to escalate privileges and assume valid identities inside the environment. This marked a clear shift in adversary strategy: exploitation became less about breaching a network perimeter and more about compromising the identity layer, where gaining trusted access through application vulnerabilities provided direct reach into sensitive systems and high-privilege operational processes.

Unauthenticated ERP RCE Enables Deep SAP NetWeaver Compromise

(SAP NetWeaver – CVE-2025-31324, CVSS 10.0)

The cases that follow illustrate how exploitation of a few enterprise platforms repeatedly allowed for identity leverage, persistence opportunities, and business disruption.

CVE-2025-31324 became one of the year's defining ERP vulnerabilities because it allowed unauthenticated remote code execution on SAP NetWeaver systems embedded in financial, human resources, supply chain, and operational processes. Multiple Chinese threat actors—including Chaya004 and Cotton Sandstorm—weaponized the flaw rapidly, deploying malware and web shells, harvesting credentials, and enumerating connected systems before pivoting deeper into core ERP environments.

The campaign affected dozens of organizations globally and demonstrated how quickly exploit code circulated through both espionage-driven actors and financially motivated groups once public proof-of-concept tooling appeared. The incident reinforced a broader trend: ERP vulnerabilities now deliver not only initial access but also strategic business insight and long-term persistence opportunities.[8]

SharePoint RCE Turns Collaboration Servers into Identity Gateways

(Microsoft SharePoint – CVE-2025-53770, CVSS 9.8)

The SharePoint vulnerability drove one of the widest exploitation campaigns of 2025. Attackers abused the ToolPane.aspx endpoint for remote code execution, deployed web shells, and extracted machine keys that allowed them to create valid authentication tokens. This effectively transformed compromised SharePoint servers into identity gateways and lateral-movement hubs.

More than 400 organizations were impacted globally, with activity attributed to China-linked espionage actors as well as ransomware groups such as Gold Salem, who leveraged the same weakness to deliver encryption payloads. The campaign showed how vulnerabilities in collaboration systems—often treated as routine IT infrastructure—can rapidly escalate into domain-wide compromise when identity components are tightly integrated.[9]

Cl0p Zero-Day Exploitation of Oracle ERP Core Systems

(Oracle E-Business Suite – CVE-2025-61882, CVSS 9.8)

CVE-2025-61882 defined one of the most damaging application-layer exploitation campaigns of the year after Cl0p adopted the flaw as a zero-day against Oracle E-Business Suite. The vulnerability enabled remote code execution deep inside ERP modules responsible for HR, finance, procurement, and supply-chain operations. Cl0p's campaign compromised more than a hundred organizations, including major enterprises and media outlets, and was active well before patches were released. Unlike earlier Cl0p operations that targeted edge appliances, this campaign focused directly on core business operations, giving attackers access to high-value regulated data and dramatically increasing extortion leverage. It also exemplified ransomware groups' migration toward exploiting application-layer vulnerabilities traditionally associated with espionage targeting.[10]

Successful exploitation in 2025 mattered less as a technical milestone and more as a business trigger: flaws in ERP, collaboration, and identity-linked platforms routinely translated into privileged access, regulated data exposure, and quick operational pressure. The speed at which the same high-value CVEs were weaponized—often by both statealigned and criminal actors in parallel—turned enterprise-platform vulnerabilities into immediate commodities rather than patch-cycle risks.

That "small foothold, oversized impact" pattern is the thread that carries into the major incidents that follow.

Identity, supply chain, and operational disruption in major incidents

The exploitation characteristics outlined in the previous section set the conditions for many of the year's most disruptive attacks. Even when incidents did not originate from a disclosed vulnerability, the underlying mechanics were remarkably consistent: limited access was amplified through identity compromise and trusted third-party integrations.

Salesforce ecosystem and OAuth supply-chain breaches

One of the defining campaigns of 2025 was the wave of intrusions affecting organizations using Salesforce and its connected SaaS ecosystem. The activity was driven primarily by ShinyHunters, with involvement from Scattered Spider and LAPSUS$, which used similar access techniques and pursued the same downstream targets. Rather than exploiting a vulnerability in Salesforce itself, the actors systematically abused OAuth integrations and connected apps such as Salesloft's Drift and, later, Gainsight, to obtain legitimate API access into customer CRM environments.

Attacker claims and third-party reporting indicate that the campaign affected hundreds of Salesforce tenants, with exposed data amounting to millions of records per organization and more than a billion across the wider ecosystem. Victims spanned multiple sectors, including aviation, luxury retail, and financial services, with several airlines reporting unauthorized access to booking and loyalty data, major consumer brands experiencing customer-data exposure, and at least one large insurer linked to leaks involving large-scale record exposure.

Across all incidents, access flowed through trusted integrations, not through vulnerabilities in Salesforce's core platform. Once OAuth tokens or connected-app credentials were compromised, attackers could query CRM objects—customer profiles, sales pipelines, support cases—without interacting with the platform directly. Social engineering accelerated entry, with lures mimicking Salesforce login flows and brand-support portals. The campaign extended when Gainsight integrations were also abused, prompting token revocations and the takedown of affected applications.

The JLR cyber incident reshaped automotive sector weaknesses

Jaguar Land Rover (JLR) experienced a major cyber incident that disrupted core digital systems supporting vehicle production and registration, forcing manufacturing shutdowns. The outage affected systems closely integrated with JLR's production workflows and prompted direct government involvement due to its impact on the broader automotive supply chain.[11] The scale of the disruption positioned the event as one of the UK's most economically significant cyber incidents of the year, with ripple effects observed across parts suppliers, regional manufacturing networks, and even the UK's GDP.[12]

Across the wider automotive sector, there was a sharp increase in attacks targeting manufacturers and their suppliers, with adversaries exploiting the industry's dependence on distributed digital networks rather than breaching OEMs directly. Intrusions affecting design environments, HR and employee-data processors, dealership and customer-data systems, and connected-vehicle service platforms at organizations including Nissan, Volvo Group, Stellantis, Toyota/Lexus, BMW, Renault, Hyundai, Mazda, and Volkswagen France highlighted how attackers increasingly leverage third-party access and shared digital infrastructure to generate pressure and extortion leverage.

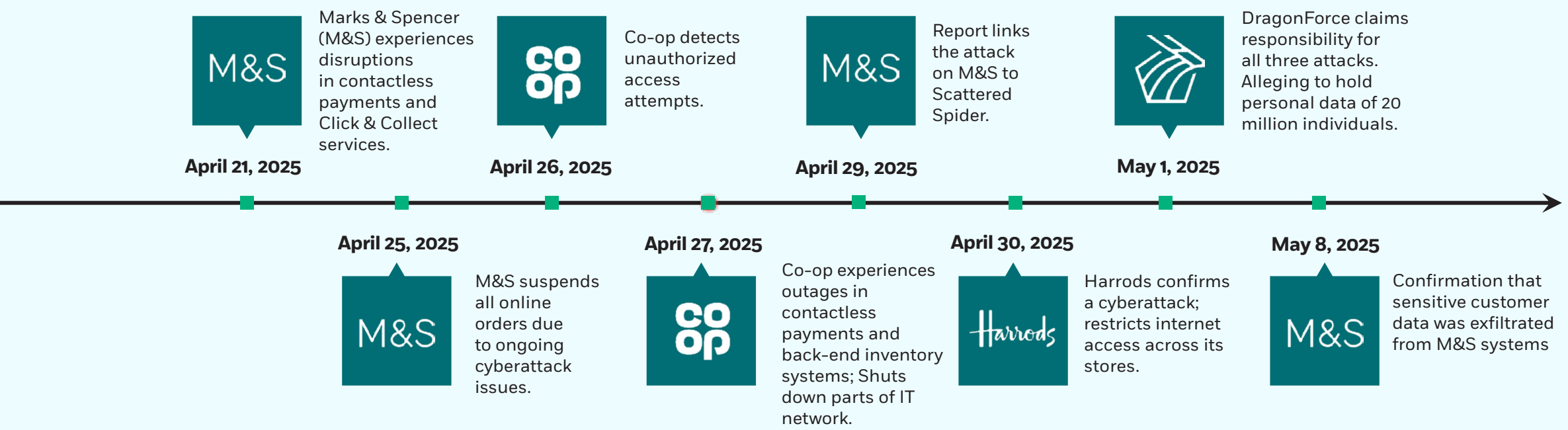
The JLR incident illustrates how disruption in the automotive sector no longer requires direct interference with vehicle or factory control systems. By targeting enterprise IT and vendor-connected platforms that support production scheduling, registration, and supplier coordination, attackers were able to halt manufacturing and trigger supply-chain fallout. The impact extended beyond JLR itself, drawing government attention and highlighting how dependency on shared digital infrastructure has become a primary operational risk for automotive manufacturers.

Retail sector attacks and the expansion of identity-driven extortion campaigns

During the second quarter of 2025, publicly disclosed ransomware incidents in the global retail sector increased by 58% quarter over quarter. This surge contributed to one of the sector's most destabilizing years on record , with coordinated attacks affecting major UK brands such as Marks & Spencer, Harrods, and Co-op, as well as grocers and luxury retailers globally.[13]

Threat actors linked to Scattered Spider, ShinyHunters, and LAPSUS$ clusters carried out sustained campaigns that disrupted operations, exposed customer data, and triggered significant financial losses.[14] The attack on Marks & Spencer was cited as one of the most expensive in UK retail history and contributed to senior leadership fallout.[15]

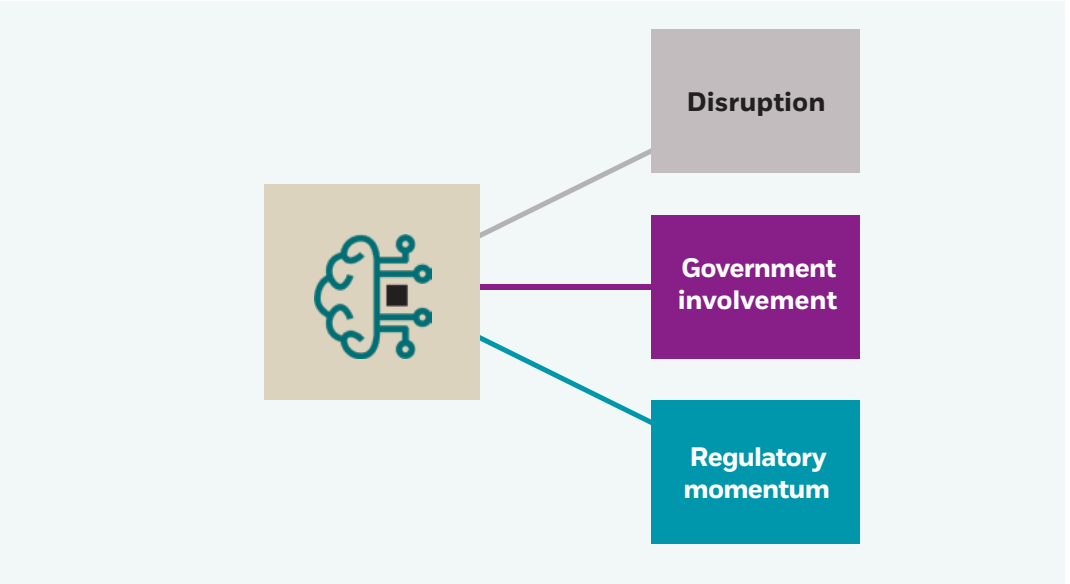
Timeline of events



A defining feature of these incidents was identity compromise, with attackers gaining access by manipulating IT personnel into resetting credentials or granting elevated access. This allowed adversaries to bypass multi-factor authentication (MFA) and operate using valid identities inside core retail systems. Once inside, attackers moved quickly to exfiltrate customer records, access connected SaaS platforms, and disrupt operational systems tied to inventory, logistics, and online sales.

The impact extended beyond individual brands into food and consumer-goods supply chains. Grocery retailers such as Natural Grocers (US), Ahold Delhaize (Europe/US), and Auchan (Europe) experienced IT outages that translated directly into delayed deliveries, fulfillment disruptions, and reduced stock availability at the store level—illustrating how cyber incidents can quickly disrupt consumer access to essential goods. Parallel attacks on luxury retailers—including LVMH, Cartier, Dior and Victoria's Secret—demonstrated a different monetization path, where loyalty data, high-networth customer profiles, purchase histories, and identity documentation were targeted as high-value extortion assets, leading to distribution delays, suspended online ordering, and customer-facing service disruptions.[16]

The UK became one of the hardest-hit regions this past year, with cyberattacks increasing by 129% year over year. Disruptions across automotive, retail, and transport sectors exposed deep reliance on third-party vendors and identitydriven systems, while 43% of UK businesses reported experiencing at least one cybersecurity breach or attack.[17] The scale of the JLR and retail incidents forced direct government involvement, including emergency financial support for affected sectors and renewed scrutiny of national cyberreadiness.

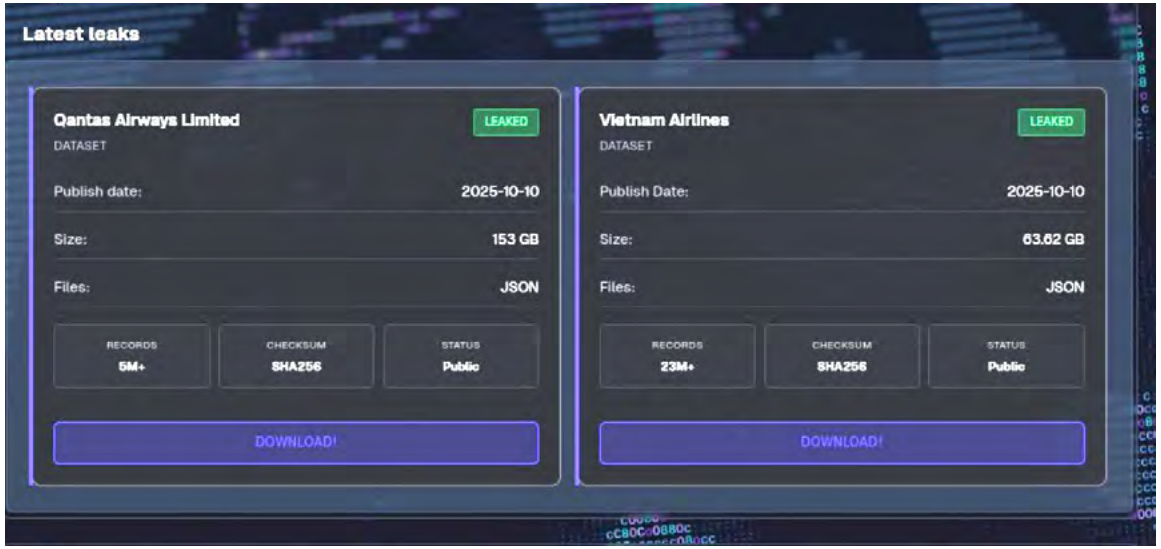


This trend extended beyond the private sector, with the UK government confirming a significant breach affecting internal systems in October 2025, highlighting how cyber risk in the UK had escalated into a national-level concern. Together, these incidents accelerated regulatory momentum, including efforts to discourage ransom payments and strengthen mandatory reporting, as cyber disruption increasingly intersected with economic stability and public governance. These dynamics were not unique to the UK, but the scale of disruption in this region highlights how cyber incidents increasingly trigger state-level response when economic and national interests are affected.

Aviation's digital footprint created new exposure

Airlines and airport operators faced sustained disruption driven largely by attacks on shared aviation technology providers rather than airline systems alone. A ransomware incident at Collins Aerospace—whose platforms support check-in and boarding at major European hubs—forced manual fallback procedures and caused delays across airports in London, Brussels, and Berlin.[18] Kuala Lumpur International Airport experienced similar operational downtime after a cyberattack disabled flight information displays, check-in counters, and baggage handling systems. These incidents showed how compromise of a single vendor can cascade across multiple businesses and locations simultaneously.

Airlines also disclosed parallel data-access incidents. Qantas, Vietnam Airlines, Envoy Air, Aeroflot, and others reported intrusions affecting customer-service systems and large volumes of passenger data, in some cases exposing millions of records.[19] Korean Air and KLM–Air France experienced similar impacts tied to compromised third-party environments.[20] While flight-control systems were not affected, the concentration of passenger identity data, loyalty profiles, and travel itineraries make airlines particularly attractive targets for extortion and fraudoriented groups.



Qantas and Vietnam air mentioned on “Scattered Spider, ShinyHunters, and LAPSUS$ “ leak site[21]

The sector also experienced cyber-physical spillover. Indian airports reported coordinated GPS-spoofing activity that disrupted satellite-based navigation procedures and forced flight diversions.[22] This combination of IT, OT, and operational aviation systems surfaced a key insight for 2025: the aviation sector now behaves as a single, interconnected attack surface, where threats to vendor software, customer-service platforms, airport OT, and navigation infrastructure produce the same outcome—rapid, highvisibility disruption.

For threat actors, aviation offers maximum leverage with minimal intrusion scope, making it one of the highestpressure extortion and disruption targets.

Across these incidents, a consistent pattern emerged: attackers targeted the junctions where identity, operational systems, and third-party services intersect. Whether the outcome was data theft, manufacturing downtime, retail outages, or transport disruption, the mechanics were the same—limited access rapidly expanded through compromised credentials, vendor relationships, and shared digital infrastructure.

The most damaging incidents were not the most technically complex, but those that exploited structural dependencies and generated immediate operational pressure. This defines the enterprise risk landscape entering 2026 .

Tactics and intrusion patterns that shaped attacker success

Following the large-scale incidents outlined in the previous section, a consistent set of intrusion techniques emerged across sectors. Instead of relying on direct exploitation of network defenses, threat actors focused on abusing trust relationships—targeting identity infrastructure, help-desk workflows, SaaS authentication flows, and user-initiated actions.

The most disruptive campaigns combined social engineering, application-layer abuse, browser-based delivery mechanisms, and coordinated extortion tactics, allowing limited initial access to escalate rapidly into operationally significant compromises.

It staff impersonation emerged as a core initial-access vector

Impersonating IT staff became one of the most successful social-engineering techniques of 2025,with Scattered Spider emerging as the most visible practitioner of this method. Threat actors posing as internal IT administrators, support technicians, or even senior executives convinced help-desk teams to reset MFA tokens or grant remote access through tools such as Quick Assist, enabling attackers to obtain valid identities without needing to exploit vulnerabilities or overcome security controls directly

Cyber attack chain model

The technique extended beyond voice-based social engineering into collaboration platforms: adversaries exploited Microsoft Teams impersonation flaws to mimic internal IT staff and prompt victims to install remote-support utilities or enter credentials into phishing pages.[23] Similar impersonation tactics were adopted by multiple actors. Matanbuchus campaigns combined IT impersonation with malicious MSI delivery via Quick Assist, while Black Basta leveraged Teamsbased spoofing to persuade users into executing loader payloads.

Across these campaigns, organizational trust in IT and support workflows became a primary point of failure. Help-desk processes—designed for availability rather than adversarial resistance—were repeatedly leveraged to bypass authentication controls and establish trusted access.

Ransomware's shift toward AI-enabled automation

AI-powered ransomware accelerated sharply in 2025, transforming both the scale and tempo of financially motivated intrusion activity. Reporting indicated that around 80% of ransomware campaigns incorporated AI at some stage of the attack lifecycle—from enhanced social-engineering pretexts to automated malware development and payload generation.[24]

Around **80%** of ransomware campaigns incorporated AI at some stage of the attack lifecycle.

The emergence of PromptLock—the first publicly confirmed AI-directed ransomware proof-of-concept—demonstrated how large language models could autonomously create dynamically changing ransomware payloads, reducing signature-based detection and enabling rapid end-to-end execution of an attack.

Threat groups also adopted AI-enabled adaptive encryption, allowing ransomware to analyze system resources and document content to prioritize valuable data and adjust encryption behavior on the fly. Affiliates such as KillSec and Funklocker used AI-generated tooling in many incidents, lowering the technical barrier to entry and allowing less-skilled actors to deploy highly customized ransomware at scale.[25] [26]

AI did not replace existing ransomware tradecraft this past year—but it amplified it, allowing threat actors to operate faster and increase operational impact.

Narrative control as a new layer of extortion strategy

Threat actors increasingly treated public narrative management as part of the attack's lifecycle rather than a post-breach byproduct. Throughout the year, ransomware groups deliberately used media exposure, public statements, and open communication channels to influence attribution, shape victim behavior, and increase leverage during negotiations. By controlling how incidents were framed externally, actors applied pressure beyond the compromised environment itself.


BBC

Co-op cyber attack affects customer data, firm admits, after hackers contact BBC

Joe Tidy

Cyber criminals have told BBC News their hack against Co-op is far more serious than the company previously admitted.

Snippet from DragonForce's interview with the BBC following the attack on Co-op in April-May 2025

IntelBroker illustrated this shift by giving direct interviews to an online cyber magazine and a German podcast, using those platforms to challenge law-enforcement attribution and position himself as an independent operator rather than a geopolitically aligned actor.[27]

Similarly, the attackers behind the Co-op cyberattack reached out to the BBC to assert the seriousness of their hack, using mainstream coverage as an indirect lever to signal capability and intent. Monitoring of Telegram activity further indicated deliberate testing and refinement of messaging, reflecting growing awareness of how threat actors are perceived outside underground forums.

By integrating narrative manipulation into their operational model, threat actors expanded the scope of extortion from technical compromise to reputational, legal, and regulatory pressure. In 2025, managing public perception became a repeatable tactic— used alongside data theft and disruption—to influence outcomes long after initial access was achieved.

How ClickFix turned verification prompts into infection paths

ClickFix emerged as a highly adaptive browser-based social-engineering technique, using highly convincing fake CAPTCHAs and verification prompts to push users into executing malicious scripts. Threat actors embedded fraudulent Cloudflare-style prompts, countdown timers, fake “users verified” counters, and instructional videos into compromised or spoofed websites, creating urgency and legitimacy while tailoring payloads automatically to Windows, macOS, or Linux systems.

In 2025, ClickFix activity increased by over 500% , representing close to 8% of blocked attack attempts and establishing it as the second most common intrusion vector after conventional phishing. [28]

ClickFix activity in 2025

500%+	8%	2nd
increased by over 500%	representing close to 8% of blocked attack attempts	second most common intrusion vector after conventional phishing.

Distribution was driven primarily through poisoned search results and malvertising, with nearly half of observed ClickFix activity delivered via fake Cloudflare CAPTCHA pages surfaced through Google search pathways. To limit detection and analysis, campaigns relied on rapid domain rotation, botprotection services, and heavily obfuscated JavaScript code designed to execute only after user interaction.

By turning verification prompts into a self-infection mechanism, ClickFix blurred the boundary between phishing and malware delivery, establishing itself as a reliable initial-access vector throughout 2025.

2025 Became the year of identity-driven attacks

Across these techniques, a single pattern was clear: trusted access replaced technical intrusion as the primary driver of impact. Whether through OAuth abuse, IT staff impersonation, compromised machine credentials, or SaaS integrations, attackers operated as legitimate users from the earliest stages of intrusion. This access model explains the speed and scale of escalation seen throughout the year, where limited footholds quickly translated into widespread disruption.

By the end of 2025, identity assurance—not perimeter defense—had become the most consequential control point shaping intrusion outcomes across sectors.

How collaboration, scale and identity abuse shaped the adversary landscape

In 2025, access, infrastructure, and operational roles increasingly moved between threat actors rather than remaining within individual groups. Initial footholds were reused, tooling circulated across systems, and campaigns spread through informal collaboration rather than centralized command. This section examines how cooperation—both deliberate and opportunistic—enabled threat actors to repeat successful intrusion models across sectors at speed, turning isolated compromises into sustained, multi-industry pressure.

Collaboration became a competitive advantage

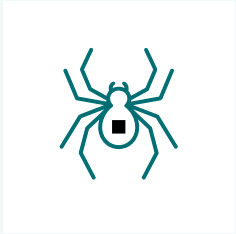
The threat landscape this year was shaped less by the emergence of new groups and more by the rapid evolution and coordination of established ones. Several groups— most notably Scattered Spider, ShinyHunters, Qilin, and a cluster of North Korean and Chinese APTs—set the tempo of global activity, driving large-scale incidents across retail, automotive, aviation, SaaS providers, and critical manufacturing.

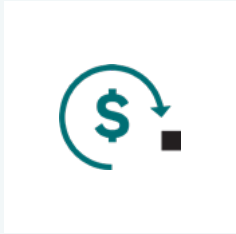
What emerged was an ecosystem where access, tooling, and tradecraft moved between actors—making campaigns faster to repeat and harder to contain. This shift was most visible in criminal ecosystems, where loose alliances mattered more than brand names.

The rise of the scattered LAPSUS hunters collective

The most visible illustration of adversary collaboration was the growing overlap between Scattered Spider, ShinyHunters, and LAPSUS$.[29] This loose but highly active collective drew from a pool of young Englishspeaking SIM-swappers, social engineers, and credential-harvesting specialists who had previously operated under brands such as Octo Tempest (Scattered Spider), Strawberry Tempest (LAPSUS$), and ShinyHunters.

What distinguished this grouping was not formal structure, but the speed at which tradecraft and infrastructure were reused, with identity compromise serving as the common entry point.





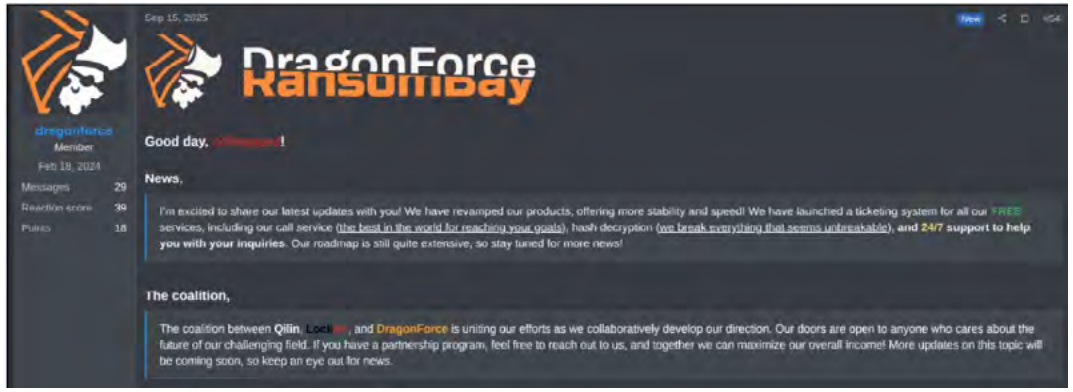
Across campaigns targeting the Salesforce supply chain, Jaguar Land Rover, airline and retail organizations, the collective demonstrated a repeatable playbook: reconnaissance of highprivilege employees, creation of credible corporate personas, and aggressive social-engineering operations to reset MFA, hijack help-desk workflows, or execute SIM-swapping attacks.

Scattered Spider remained the sharp end of this strategy, often initiating compromise, while ShinyHunters amplified impact through large-scale data theft and leak-site pressure. The collaboration blurred the line between initial access and extortion, allowing the same access paths to be repurposed across sectors and operations to outpace typical defensive response cycles.

The LockBit, DragonForce, and Qilin ecosystem

The past year also highlighted a growing unification between LockBit, DragonForce, and Qilin, characterized by shared tooling, overlapping affiliate networks, and the continued influence of leaked Conti v3 source code.[30] Reporting throughout the year showed these groups adopting similar payload frameworks, encryption routines, and access methods, allowing operators to move between brands without changing their tradecraft.

DragonForce re-emerged as a Conti-linked ransomware cartel, enabling affiliates to white-label payloads and rapidly expand victim reach, while Qilin became one of the most prolific ransomware groups of the year, frequently appearing in incidents involving compromised MSPs and RMM tooling.



LockBit, DragonForce, and Qilin announcement on joining forces[31]

LockBit, despite law-enforcement disruption, remained a central influence in the ransomware environment, sharing infrastructure and operational routines with DragonForce and Qilin.

The result was a ransomware landscape that functioned less as discrete groups and more as a shared operating environment. This amplified operational tempo and widened the attack surface for defenders, allowing LockBit-DragonForce-Qilin to generate disproportionate impact across enterprise, government, and critical-services sectors.

North Korea's APT environment becomes operationally integrated

North Korea's cyber activity in 2025 was marked by an unusual degree of coordination between Kimsuky and Lazarus, with reporting indicating shared infrastructure and parallel tasking across espionage and financially motivated operations. Multiple analyses described campaigns in which both clusters targeted critical sectors—including defense, energy, finance, and aerospace—while leveraging the same zero-day exploits, backdoors, and spear-phishing frameworks to establish access and exfiltrate data.[32]

Operational lines between the two groups continued to blur. Kimsuky's traditional focus on credential harvesting and longterm intelligence collection increasingly fed into Lazarus operations, which weaponized compromised identities for follow-on attacks, financial theft, and supply-chain intrusion. Several reports noted coordinated campaigns that combined Kimsuky's reconnaissance and lure development with Lazaruslinked malware, enabling seamless transitions from initial espionage access to rapid operational impact.

This division of labor created an end-to-end intrusion chain that enabled North Korean threat actors to scale activity across multiple regions and sectors with unprecedented efficiency.

Growing operational alignment between Russian and North Korean APTs

Separate from the Kimsuky–Lazarus relationship, 2025 also saw a deepening operational alignment between Russian and North Korean threat actors.[33] Both players increasingly pursued overlapping targets—including Western critical infrastructure, financial institutions, and government networks—with several campaigns exhibiting multiple similarities and activity unfolding in parallel during geopolitical flashpoints.

This alignment went beyond isolated coincidences. Russian and North Korean clusters were observed reusing elements of each other's malware ecosystems, adopting similar spear-phishing frameworks, and staging campaigns that reinforced shared operational objectives.

The result was a combined threat footprint that proved more resilient, more diverse in capability, and more difficult for defenders to attribute or disrupt.

By the end of the year, this cross-state alignment had become one of the more consequential developments in the cyber domain, expanding both countries' reach and increasing sustained pressure on sectors already subject to prolonged advanced persistent threat (APT) activity.

The following threat actors best illustrate how collaboration, identity abuse, and operational scale translated into real-world impact during the year.

Threat actor spotlight: **Scattered Spider**

The most influential threat actor of 2025

Scattered Spider emerged as the most influential threat actor of 2025, driving high-impact intrusions across retail, aviation, insurance, and SaaS environments through a refined identitycentric playbook. Their operations shifted toward tightly coordinated sector-wide attack waves, where multiple organizations within the same industry—such as UK retailers M&S, Co-op, and Harrods—were breached within days, often via DragonForce-linked ransomware deployments. This campaign structure, paired with rapid reconnaissance of high-privilege users and targeted social engineering, allowed the group to move from initial access to operational disruption within short timeframes.

What set Scattered Spider apart was the consistency and structure of its social-engineering operations. The group routinely impersonated internal IT staff, exploited helpdesk workflows to trigger MFA resets, and leveraged thirdparty IT providers to extend access across cloud, SaaS, and identity. These techniques—combined with vishing (voice fishing), SIM-swapping, and platform impersonation—formed a repeatable access model that was later adopted by other criminal groups.

By mid-year, their influence expanded further with the formation of the Scattered LAPSUS$ Hunters Collective—a merger with LAPSUS$ and ShinyHunters that created an “extortion-as-a-service” model that allowed affiliates to rent infrastructure and branding for a percentage of ransom proceeds. Through this clustering, Scattered Spider’s identity-driven intrusion model propagated across a wider pool of affiliates, amplifying both scale and consistency. Their techniques became not only a signature of the year’s major breaches but also the core methodology copied by ransomware groups, and even some state-aligned clusters.

Threat actor spotlight: **ShinyHunters**

The most economically destructive data-extortion group of 2025

ShinyHunters became one of the most consequential cybercrime groups, leading large-scale data-extortion campaigns that heavily impacted Salesforce customers across aviation, luxury retail, and financial services. Their operations exposed more than a billion records from organizations including LVMH, Chanel, Adidas, Qantas, and Air France–KLM, and showed a clear pivot toward high-value financial targets as domain registrations mimicking banks and insurers rose sharply through mid-2025. This pivot reflected a deliberate focus on sectors with both sensitive data and high ability-topay, creating some of the year's most costly cyber incidents.

A defining feature of ShinyHunters' tradecraft was its use of social engineering to obtain cloud-native access rather than exploiting platform vulnerabilities directly. The group relied heavily on vishing attacks to obtain Salesforce credentials, often impersonating internal IT staff and directing employees to approve actor-controlled applications—frequently modified versions of the Salesforce Data Loader—to gain long-term access to enterprise cloud environments.

ShinyHunters' impact escalated further after joining Scattered Spider and LAPSUS$ within the Scattered LAPSUS$ Hunters Collective. The group leaked data samples via platforms like LimeWire, issued public countdowns, and threatened mass disclosure—pressure tactics that pushed some ransom demands into the seven-digit range.34 These campaigns demonstrated how data theft, public signaling, and affiliate-driven scale combined to make ShinyHunters one of the most economically disruptive actors of the year.

Threat actor spotlight: **Qilin**

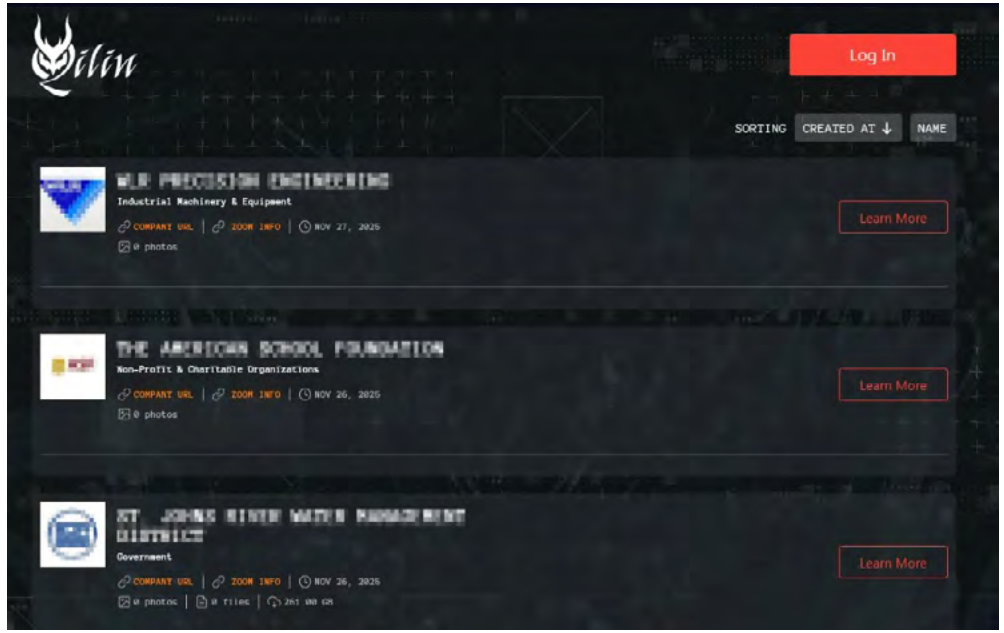
The highest-volume ransomware actor of 2025

Qilin emerged as the most prolific ransomware threat, sustaining a consistently high operational tempo and leading global incident volume.35 Through Q2 and Q3 2025, the group published more than 40–100 victims per month on its leak site, surpassing Akira and overtaking RansomHub as the dominant ransomware actor across enterprise and public-sector environments.

Much of Qilin's impact stemmed from its focus on manufacturing, professional services, and wholesale trade — sectors that rely heavily on interconnected operational systems and have limited tolerance for downtime.

Analysis across multiple cases showed the group adopting a highly efficient double-extortion model while employing unusual reconnaissance techniques, such as repurposing legitimate Windows applications to sift through sensitive files, reducing behavioral detection by blending activity into normal user workflows.

This combination of speed, stealth, and operational pragmatism enabled Qilin to scale attacks with remarkable consistency.



Screenshot of Qilin's leak site in November 2025[36]

Qilin's rise was further strengthened by its alignment with DragonForce and LockBit clusters, forming an ecosystem that shared infrastructure, payload frameworks, and affiliate networks. This organizational maturity allowed Qilin to be positioned as one of the most important ransomware groups heading into 2026.

APT blending and strategic targeting increased

A similar shift was visible among state-aligned threat actors, where operations were no longer confined to a single purpose such as espionage or disruption. Instead of separating operations by purpose, several APT groups reused the same tooling, exploits, and infrastructure across intelligence collection, financial theft, and disruptive activity, targeting sectors such as aerospace, energy, and financial services with the same playbooks.

Chinese and North Korean APTs illustrated this shift most clearly. Chinese clusters rapidly weaponized enterprise vulnerabilities in platforms such as SAP, SharePoint, and Oracle, using the resulting access to collect intelligence while maintaining persistent footholds in manufacturing and technology supply chains. At the same time, North Korean operators reused the same phishing lures, malware families, and command-and-control infrastructure across espionage, financial theft, and cryptocurrency-related campaigns, often without changing tooling between mission types, making attribution and incident response more difficult.

In 2025, state-aligned operations increasingly combined intelligence gathering, monetization, and pressure tactics within a single intrusion, marking a practical breakdown of the traditional separation between espionage and financially motivated activity.

Across both criminal and state-aligned environments, the most successful threat actors were those able to blend identity compromise, cloud-native intrusion techniques, and collaborative operational models. Groups such as Scattered Spider, ShinyHunters, Qilin, and North Korea's APT clusters demonstrated that scale no longer comes from malware sophistication alone, but from the ability to rapidly reuse shared infrastructure, and exploit the same identity-layer weaknesses across multiple sectors.

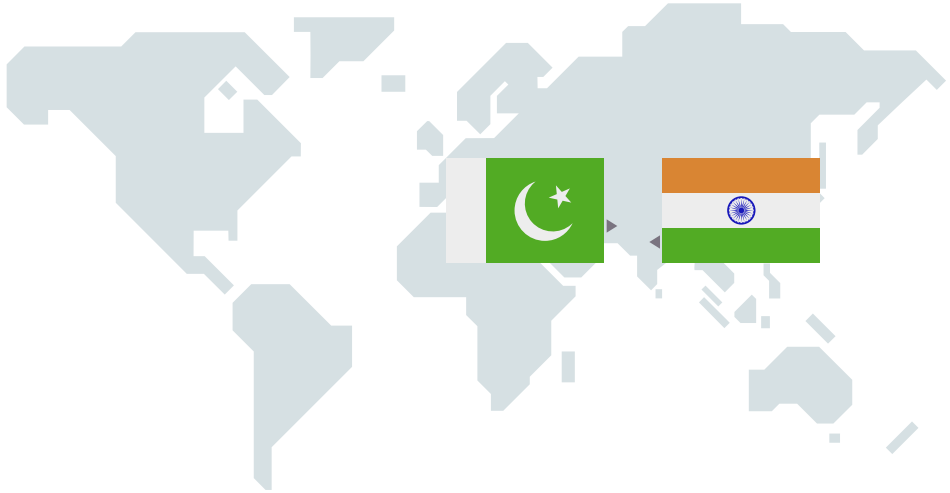
This merging—between social engineering, cloud access, and shared tooling—reshaped the adversary landscape into one where intrusions spread faster, crossed organizational boundaries more easily, and consistently outpaced traditional defensive assumptions.

Geopolitical tension and cyber spillover in 2025

Cyber operations in 2025 increasingly mirrored global political tensions, with regional conflicts triggering coordinated waves of hacktivism, state-linked espionage, and disruptive cyber activity. Rather than isolated incidents, nation-state disputes in the Middle East, South Asia, and Eastern Europe spilled directly into the digital domain, affecting government services, financial institutions, and critical infrastructure. These cyber responses often unfolded within hours of geopolitical events, showing how tightly coupled cyber response is to military and political escalation today.

Key dynamics of Cyber-kinetic escalation

Cross-border hacktivism and targeted disruptions in the India–Pakistan conflict

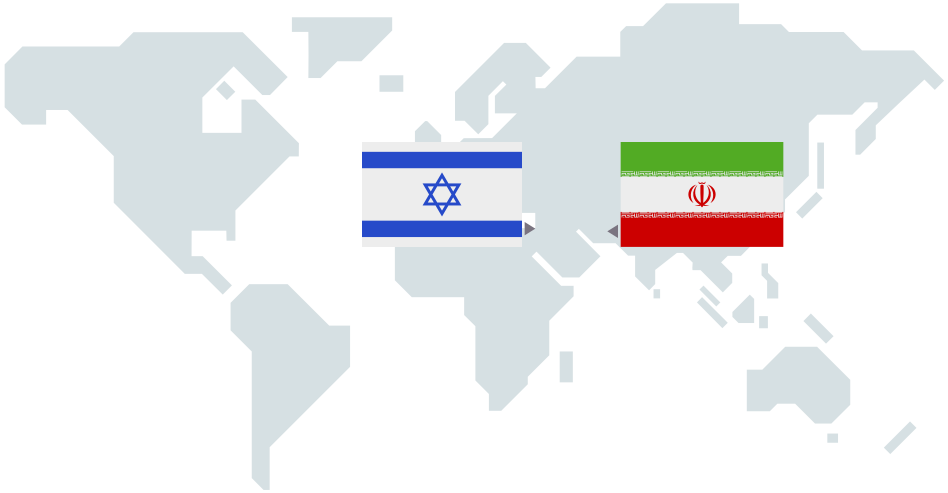


Geopolitical tensions between India and Pakistan rapidly trickled into cyberspace, with the aftermath of the April 2025 Pahalgam attack and India's subsequent "Operation Sindoor" triggering a surge in hostile digital activity. Both sides saw intensified waves of DDoS attacks, website defacements, and symbolic intrusions, as hacktivist collectives mobilized in response to realworld events.[37]

Campaigns branded under hashtags like #OpIndia drove most of the activity, with pro-Pakistan groups targeting Indian government, defense, and telecom sites, while Indian volunteer collectives retaliated by defacing Pakistani government platforms and leaking limited databases. At the same time, APT36 weaponized Pahalgam-themed phishing documents to target Indian government and defense personnel, demonstrating how espionage actors capitalized on the broader hacktivist noise.

While the operational impact of these attacks remained mostly limited, the speed and scale of mobilization highlighted a deeper regional shift: cyber operations have become an immediate extension of geopolitical crises. The India–Pakistan confrontation showed how nationalist hacktivism, combined with targeted APT activity, can generate persistent digital instability even without causing major infrastructure damage.

Coordinated cyber retaliation and psychological operations in the Israel–Iran escalation



The June 13, 2025 launch of Operation Rising Lion marked the year's most direct alignment of kinetic action and cyber escalation between Israel and Iran. Within days, cyberattacks against Israeli networks surged, driven largely by pro-Iranian hacktivist groups conducting DDoS campaigns, website defacements, data theft, and coordinated disinformation operations.

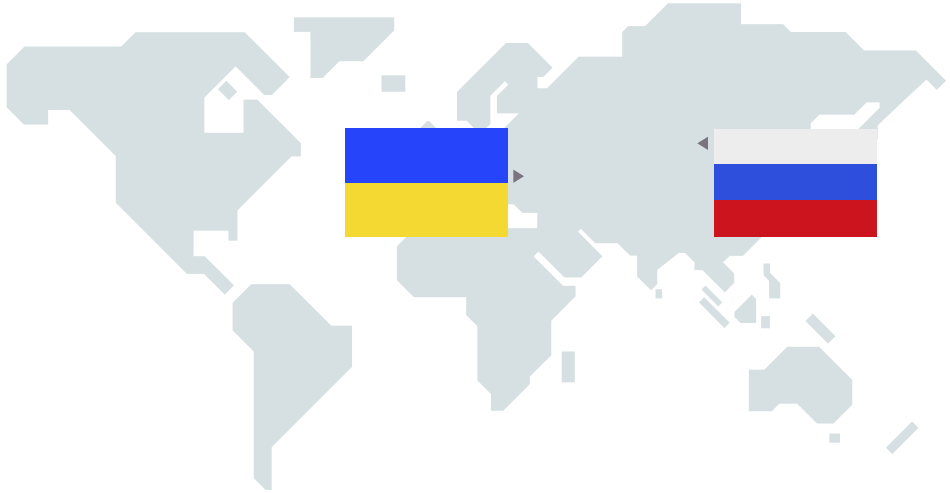
A notable development was the manipulation of emergency alert systems and GPS-spoofing activity affecting maritime and aviation navigation across Israel and neighboring regions.

While Iran-aligned collectives—including Handala and Educated Manticore—targeted Israeli government, telecom, finance and emergency-services sectors, the conflict also saw activity from Predatory Sparrow, a group widely believed to be aligned with Israel. Their attacks on Bank Sepah and the Nobitex cryptocurrency exchange[38] caused service outages and destroyed tens of millions of dollars in crypto assets, demonstrating the use of cyber operations for signaling rather than financial gain.

Predatory Sparrow's post on X following the Bank Sepah attack

The conflict's cyber dimension extended far beyond the region. U.S. agencies issued warnings that Iranian operators may exploit exposed systems belonging to defense industrial base organizations, particularly those with ties to Israeli research and defense sectors. With both hacktivist and state-aligned actors using cyber campaigns to amplify battlefield effects and shape public perception, the Israel–Iran confrontation highlighted how regional conflicts now generate global cyber effects across operations, information integrity, and public perception.[39]

AI-driven intrusions and coordinated targeting in the Russia–Ukraine conflict



Cyber activity between Russia and Ukraine escalated significantly in 2025 with Ukraine's CERT handling more than 3,000 incidents in the first half of the year—an increase from 2500 in late 2024 and a clear indication of Russia's heightened operational tempo.[40] Russian groups increasingly integrated AI into their attack chains, using AIgenerated phishing, AI-modified code, and automated "steal-and-go" scripts to speed up intrusions and evade detection.

The surge in activity coincided with a shift in targeting: attacks on local authorities and military entities intensified, while those on central government and energy infrastructure decreased.

A defining feature of the past year was the continued synchronization of cyber operations and kinetic activity. Several Russian campaigns—including activity attributed to Sandworm—were synchronized with missile and drone strikes, with cyberattacks often preceding or amplifying physical operations. Incidents included the March 2025 disruption of Ukrainian Railways' ticketing systems[41] and widespread phishing campaigns leveraging legitimate cloud hosting (like Bitbucket, Dropbox, Google Drive, OneDrive) to disguise payload delivery.

During this time, Russian operators relied heavily on Living-offthe-Land techniques, PowerShell automation, and cloud-based infrastructure to maintain long-term access while minimizing detection. By mid-year, the conflict had evolved into a persistent hybrid campaign in which cyber operations played a central role in strategic disruption, intelligence collection, and shaping the operational environment around kinetic attacks.

The geopolitical cyber incidents of 2025 did not emerge from new rivalries but from long-standing conflicts that evolved into more coordinated, more aggressive, and more technologically complex operations. India–Pakistan, Israel–Iran, and Russia–Ukraine each demonstrated how cyber activity now scales alongside physical escalation—shifting from symbolic website defacement to targeted disruption, coordinated espionage, data-driven psychological operations, and AI-supported intrusion campaigns.

Together, these conflicts showed that cyber operations are no longer peripheral to geopolitical crises, but a central instrument of state power, shaping both regional stability and global threat patterns with every escalation.

2025 Top attack indicators

Top attack indicators are specific pieces of data or observations that strongly point to potential or confirmed malicious activity within a system or network. These can include unusual network traffic patterns, suspicious file executions, unauthorized access attempts, or connection to known malicious IP addresses or domains.

Here are some of the top threat signals that the CyberProof Threat Research Team observed in breaches and attacks:

Top attack vectors
- Phishing
- NPM supply chain attacks
- SEO poisoning
- Identity based attacks
- Vulnerability exploitations

Top active ransomware groups
- Qilin
- Akira
- Cl0p
- Play
- INCransom

Top malwares
- Asyncrat
- Remcos
- Vidar
- Xworm
- OysterLoader

Top LOLBins
- PowerShell
- Mshta
- Certutil
- Schtasks.exe
- Wmic.exe

Top abused RMMs
- AnyDesk
- UltraVNC
- MeshAgent
- ScreenConnect
- LogMeIn

Top 5 tools used in attacks
- Psexec
- ADFind
- Netscan
- Angryipscanner
- DCSync

Top abused third-party platforms
- WhatsApp
- Transfer.sh
- Temp.sh
- Github
- SalesForce

Top state sponsored threat groups
- Lazarus – Famous Chollima
- APT36
- APT35
- Volt Typhoon
- Storm Groups

In 2025, the cyber threat landscape demonstrated a clear trajectory toward more sophisticated and evasive attack methodologies, setting the stage for what we anticipate in 2026. Threat hunting activities revealed that phishing remains the most prevalent initial access vector, now augmented by AI-driven content generation to increase success rates. Supply chain compromises, particularly through malicious NPMs targeting development environments and CI/CD pipelines, continued to rise, while SEO poisoning emerged as a favored tactic for malware distribution. Identity-based attacks exploiting federated authentication systems and the persistent exploitation of zero-day vulnerabilities underscore the need for proactive defense strategies.

As mentioned previously, ransomware groups such as Qilin, Akira, Cl0p, Play, and INCransom maintained dominance, refining extortion techniques with double and triple extortion models. Concurrently, adversaries leveraged commodity malware families—including Asyncrat, Remcos, Vidar, Xworm, and OysterLoader—alongside living-off-the-land binaries (LOLBins) like PowerShell, Mshta, Certutil, Schtasks.exe, and Wmic.exe to evade detection. A notable trend was the weaponization of legitimate remote monitoring tools such as AnyDesk, UltraVNC, MeshAgent, ScreenConnect, and LogMein, enabling attackers to blend seamlessly into normal operational traffic.

The exploitation of trusted platforms for command-andcontrol and data exfiltration—such as WhatsApp, Transfer.sh, Temp.sh, GitHub, and Salesforce—further complicated detection efforts. Nation-state actors, including Lazarus (Famous Chollima), APT36, APT35, Volt Typhoon, and various Storm groups, sustained high levels of activity, focusing on espionage and disruption campaigns. Case studies highlighted Brazilian banking trojan campaigns distributed via WhatsApp phishing, as well as early detection of suspicious remote monitoring activity that preempted exploitation of vulnerabilities like SimpleHelp. Additionally, the abuse of collaboration platforms such as Microsoft Teams for phishing and malware delivery emphasized the growing need for robust SaaS security controls.

These developments point to a critical imperative for organizations: strengthening identity security through multi-factor authentication and continuous monitoring, securing supply chains with rigorous code validation, deploying behavioral analytics to detect anomalous remote access, and applying zero-trust principles across SaaS environments. As we move into 2026, these measures will be essential to counter increasingly adaptive and stealthy adversaries.

2026 Predictions

1 Cyber criminals will have a tactical advantage with AI

Cybercriminals will gain a decisive tactical advantage in 2026 if security and AI organizations fail to prioritize risk as a core principle. Attackers leveraging AI do not need the same level of precision as defenders, enabling them to innovate and iterate at a much faster pace. This asymmetry means that adversaries can deploy increasingly sophisticated social engineering campaigns and adaptive attack strategies without the constraints of compliance or operational rigor. As a result, defenders who remain focused on traditional security models will struggle to keep up with the speed and complexity of AI-driven threats.

The rapid adoption of agentic AI compounds this challenge. These autonomous agents mimic human behavior and interact with systems in ways that blur the line between legitimate and malicious activity. While market demand accelerates the deployment of agentic AI, security controls and governance frameworks lag behind, creating exploitable gaps. Organizations that fail to rethink identity access management and privilege models for an AI-driven environment will expose themselves to systemic vulnerabilities. Attackers will capitalize on these weaknesses, using AI agents to bypass authentication, escalate privileges, and orchestrate multi-vector attacks at scale.

The rush to implement agentic AI without a solid cybersecurity foundation will amplify risk. Many enterprises lack robust estate management and data integrity practices, leaving them ill-prepared to secure AI ecosystems. Without trusted data and resilient infrastructure, organizations cannot effectively monitor or control AI agents, creating blind spots that adversaries will exploit. In short, unless security leaders shift their mindset from reactive defense to proactive risk prioritization, cybercriminals will dominate the battlefield in 2026, leveraging AI to outpace and outmaneuver traditional security paradigms.

2 The Rise of Vishing, Deepfakes, and Identity Deception

The convergence of voice-based social engineering and artificial intelligence is set to define a new era of attacks in 2026, with a significant rise predicted in vishing attacks embedding deepfake technology. The second half of 2025 saw a noticeable increase in vishing attacks leveraging platforms like Microsoft Teams . The introduction of features like “Chat with anyone” on Teams, which allows contact between individuals across different tenants, creates a critical new attack vector. An attacker can easily impersonate a trusted entity, such as an IT staff member, to initiate a social engineering attack.

The attack sequence, which is becoming dangerously efficient with deepfake components and the condensed time to execute, usually looks similar to this:

Initial contact: The attacker contacts an employee via the collaboration platform and sends a malicious URL.

Credential theft: The link prompts for credentials and subsequently attempts to install an RMM tool—again, weaponizing legitimate software.

Lateral Movement and Deception: If successful, the attacker gains remote access. To further manipulate the victim and their colleagues, the attacker introduces deepfake technology. This highly convincing impersonation can be used to instill a false sense of security so the victim will authorize fraudulent transactions, or provide further access,

This combination of vishing and deepfake technology is predicted to dramatically reduce the overall attack time and accelerate data exfiltration and financial theft by rapidly enabling lateral movement and manipulating human verifcation safeguards.

3 Cloud misconfigurations settings will persist

In 2026, cloud misconfigurations will continue to be a leading cybersecurity threat, despite increasing awareness and investment in cloud security. As organizations expand their use of complex, multi-cloud environments, the overall attack surface grows—introducing more potential entry points and vulnerabilities than ever before.

The risk of human error—such as misconfigured settings and insecure APIs—will persist as a primary entry point for attackers. The ongoing challenge of managing these dynamic and sprawling cloud ecosystems means that misconfiguration is expected to remain the top cause of cloud-related breaches next year.

4 Increasing use of regulatory exposure as deliberate leverage

In 2026, we expect extortion groups to increasingly use regulatory exposure as deliberate leverage. After the major consumer-facing breaches and stricter reporting rules that followed, attackers have realized that the threat of investigations, fines, and public scrutiny can be more damaging to organizations than the breach itself.

Ransom notes are already referencing GDPR, UK reporting timelines, and sector-specific disclosure rules, with some groups threatening to notify regulators directly or leaking small data samples to force mandatory reporting. This turns compliance obligations into an attack surface: the pressure doesn't only come from encrypted systems or stolen data, but from the legal and reputational consequences adversaries now know how to exploit.

5 The blurring lines: Abuse of legitimate soft

The year 2026 is projected to see a continued surge in the abuse of legitimate software, particularly Remote Management and Monitoring (RMM) tools. Attackers are successfully turning these necessary administrative utilities into powerful conduits for their campaigns, allowing them to gain “hands-on-keyboard” access to target environments.

This technique is highly effective because RMM tools are often trusted, whitelisted, and essential for business operations. Once control is established, attackers perform reconnaissance and collect critical user and machine information, setting the stage for devastating, later-stage attacks, most notably extortion (ransomware) campaigns.

Some illustrative case studies we’ve seen this year includes:

RMM Vulnerability Exploitation: In February 2025, a vulnerability in SimpleHelp RMM was reported. While the initial discovery protected some clients, a subsequent campaign around May 2025 saw the DragonForce ransom cartel successfully abuse this vulnerability to attack a Managed Service Provider (MSP) in the UK, highlighting the speed at which exploits move from discovery to weaponization. [42]

Supply Chain Subversion: Further demonstrating the challenge of software trust, CyberProof researchers identified ConnectWise ScreenConnect binaries with valid digital signatures making outbound connections to suspicious command-and-control (C2) servers.43 This attack involved Authenticode Stuffing—injecting malicious code while preserving the integrity of the original signature. Although the certificate was later revoked, these backdoored droppers were subsequently used by other threat actors to distribute infostealers, underscoring the risk of compromised software integrity.

6 Shadow AI will emerge as the next unmanaged risk surface

As enterprises continue to rush to harness generative AI, many are discovering that their greatest risk may lie not in external attacks but in potential exposures due to ungoverned internal use. Employees are increasingly adopting personal or unvetted AI tools to accelerate daily tasks, introducing the idea of shadow AI. Without clear policies on data access, model usage, and output validation, sensitive information can easily be exposed or misused.

The KPMG AI Security Benchmark Survey found that a significant portion of organizations lack defined AI vulnerability processes, incident-response playbooks or resilience plans.44 In 2026, this unmanaged layer will grow as generative models become embedded in productivity platforms and code environments. In addition, while existing policies have been well developed over the past decade to ensure that wider technologies and tools are well-integrated and subject to approval processes, the sheer volume of the logs creates a serious visibility challenge, taking many companies back to square one in regards to shadow IT. Forward-looking organizations will respond by embedding AI-governance controls into existing cyber and data-protection programs, treating model access, prompt integrity, and data lineage as core exposure-management priorities.

Recommendations for improving cyber readiness

1 Treat identity as the primary security control plane

The majority of high-impact incidents in 2025 began with attackers operating as legitimate users rather than exploiting technical defenses. Organizations should prioritize identity assurance as a core security discipline, with continuous validation of user behavior, privilege use, and authentication context across cloud, SaaS, and on-prem environments. Controls designed solely to protect network perimeters or endpoints are no longer sufficient when attackers can bypass them through credential abuse, OAuth misuse, or helpdesk manipulation.

2 Harden help-desk and IT support workflows against social engineering

Repeated breaches across retail, aviation, and enterprise SaaS environments demonstrated that IT support functions have become a preferred intrusion vector.

MFA reset procedures, account recovery processes, and remote-support approvals should be treated as high-risk transactions and protected with strict verification requirements, escalation controls, and monitoring. Organizations should assume that attackers will impersonate internal IT staff and design workflows accordingly, rather than relying on informal trust or speed-of-service incentives.

3 Enforce governance and visibility over SaaS integrations and OAuth access

OAuth abuse and connected-app compromise enabled attackers to access hundreds of organizations without exploiting core platforms in 2025. Enterprises should maintain continuous visibility into SaaS integrations, enforce leastprivilege API access, and regularly audit token scope, duration, and usage patterns.

Token revocation, application allow listing, and behavioral monitoring of API activity should be treated as standard controls, not incidentresponse measures.

4 Reduce single-point dependency risk in third-party and supply-chain systems

Incidents across automotive manufacturing, aviation, and food retail highlighted how disruption of a single vendor or shared service can cascade across entire ecosystems. Organizations should identify third-party platforms that support operational continuity—such as production scheduling, logistics, identity services, or customer-facing systems—and incorporate them into resilience planning, incident response exercises, and contractual security requirements.

Cyber risk management should explicitly account for operational blast radius, not just data exposure.

5 Prepare for ransomware that prioritizes disruption over encryption

Ransomware campaigns in 2025 increasingly focused on operational pressure rather than file encryption alone. Defensive planning should account for scenarios where attackers steal data, disrupt services, or manipulate systems without deploying traditional ransomware payloads.

Backup strategies, recovery testing, and incident response playbooks must address partial outages, identity compromise, and SaaS disruption—not just encrypted endpoints.

6 Monitor and respond to narrative and reputation-based extortion

Threat actors increasingly integrated media outreach, leak-site signaling, and public messaging into their extortion strategies. Organizations should treat narrative control as part of incident response, with predefined processes for monitoring attacker communications, coordinating legal and communications teams, and managing public disclosure timelines.

Ignoring attacker-driven narrative escalation can amplify operational and regulatory impact even when technical containment is achieved.

7 Align cyber preparedness with geopolitical risk exposure

Cyber activity in 2025 repeatedly escalated alongside geopolitical conflict, with spillover affecting organizations far beyond conflict zones. Enterprises operating in sensitive sectors or regions should integrate geopolitical risk into threat modeling, monitoring, and response planning.

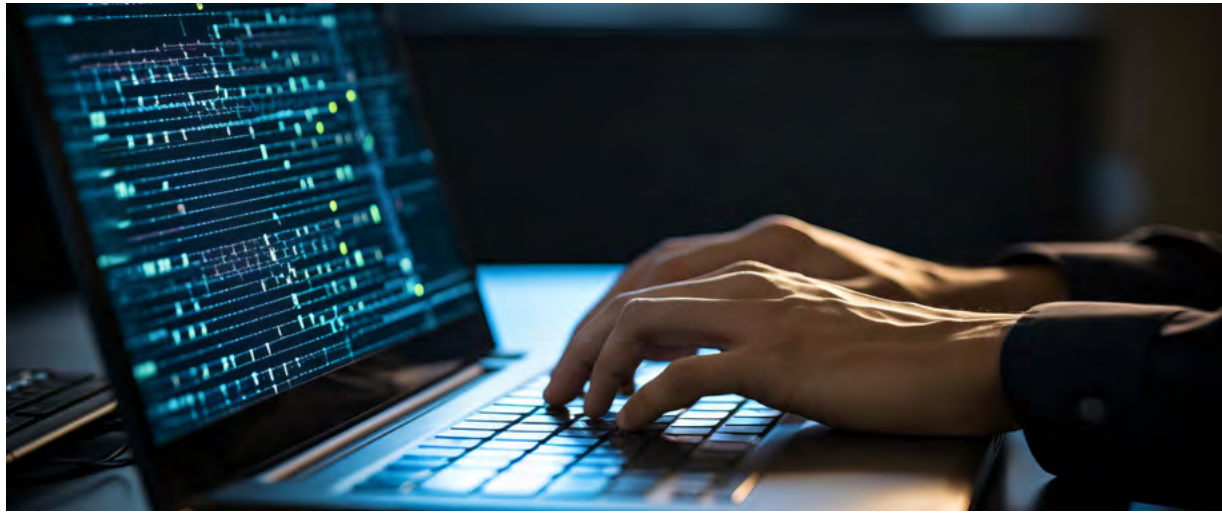
This includes anticipating hacktivist surges, statealigned opportunistic targeting, and increased exploitation of exposed systems during periods of political unrest or military escalation.

Conclusion

The events and trends of 2025 illustrate a threat landscape that has matured in both structure and intent. Attackers no longer rely on isolated exploits or single-point compromises; instead, they blend vulnerability exploitation, social engineering, identity abuse, and supply-chain leverage into cohesive intrusion models designed for scale and speed. The rapid combination of state-aligned and criminal tradecraft has reduced defenders' margin for error, turning newly disclosed vulnerabilities and trusted access paths into immediate strategic risks.

What distinguished 2025 was not the emergence of entirely new threats, but the efficiency with which existing ones were executed and replicated. Collaboration among threat actors, the industrialization of extortion, and the systematic targeting of enterprise platforms transformed cyber incidents into business-level crises with regulatory, financial, and geopolitical implications. At the same time, ongoing geopolitical conflicts demonstrated how cyber operations are now routinely integrated with physical and political pressure, reinforcing their role as a permanent feature of modern conflict.

As organizations move forward, the lessons of 2025 are clear. Security strategies built primarily around perimeter defense and reactive patching are no longer sufficient. Trust relationships, identity systems, and third-party dependencies now represent the most challenging terrain. Understanding how attackers chain these elements together—and how quickly they operationalize successful techniques—will be critical to navigating the threat landscape in the year ahead.



About CyberProof, a UST company

CyberProof delivers threat-led, co-managed security operations with the belief that better security is achieved through the right partnerships, technology and client experiences. Our threat-led, cloud-first, and AI-powered approach to security, delivers industry-leading security services which drives real and measurable business outcomes.

Learn about our cyber security solutions

We believe that working closely with our clients and partners through a better security, together model, jointly empowers us to defend against the greatest of threats.

Endnotes

1. https://www.cloudsek.com/knowledgebase/countriesmosttargetedbycyberattacks
2. https://www.infosecuritymagazine.com/news/retailransomwarejumpgloballyq2/
3. https://heimdalsecurity.com/blog/retailcybersecuritystatistics/
4. https://deepstrike.io/blog/topindustriestargetedbyhackers2025
5. https://cybersecuritynews.com/mostoftheransomwareattackstargetingorganizations/
6. https://deepstrike.io/blog/compromisedcredentialstatistics2025
7. https://cybersecuritynews.com/mostoftheransomwareattackstargetingorganizations/
8. https://www.bleepingcomputer.com/news/security/chinesehackersbehindattackstargetingsapnetweaverservers/
9. https://techcrunch.com/
10. https://gbhackers.com/clopransomware/
11. https://www.darkreading.com/cyberattacksdatabreaches/jaguarlandrovercyberincident
12. https://www.reuters.com/world/uk/ukeconomygrows01q320251113/
13. https://www.cysecurity.news/2025/09/retailcyberattackssurgeasservice.html
14. https://www.cyberproof.com/blog/coordinatedcyberattacksstrikeonukretailsector/
15. https://www.webpronews.com/marksspencercdorachelhighamdepartsafter300mcyberattack/
16. https://www.cyberproof.com/blog/whenhackersemptytheshelvesgroceryretailsupplycyberthreats/
17. https://itbrief.co.uk/story/ukcyberattackssurge129fuellingrisklosses
18. https://www.bbc.com/news/articles/cqjeej85452o
19. https://infotechlead.com/security/qantasairwaysconfirmscybersecurityincidenttargetingcontactcenters90151
20. https://www.bleepingcomputer.com/news/security/airfranceandklmdisclosedatabreachesimpactingcustomers/
21. https://ia.acs.org.au/article/2025/qantascustomerdataleakedtodarkweb.html
22. https://www.cybersecurityinsiders.com/indianairportstargetedbygpsspoofingcyberattack/?utm_source=chatgpt.com
23. https://www.cyberproof.com/blog/teamssocialengineeringattackthreatactorsimpersonateittostealcredentialsviaquickassist/
24. https://cybersecuritynews.com/aipoweredransomware/
25. https://www.cyberproof.com/cyberthreatintelligence/cyberproof2025midyearcyberthreatlandscapereport/
26. https://cyberinsider.com/firstaipoweredransomwarepromptlockdiscoveredinthewild/
27. https://thecyberexpress.com/intelbrokerinterviewexclusive/
28. https://www.cysecurity.news/2025/11/clickfixsilentcyberthreattricking.html
29. https://www.infosecuritymagazine.com/news/scatteredspidershinyhunters/
30. https://thehackernews.com/2025/10/lockbitqilinanddragonforcejoin.html
31. https://thehackernews.com/2025/10/lockbitqilinanddragonforcejoin.html 32. https://malware.news/t/kimsukyandlazarusjoinforcesincoordinatedattacks/101864
33. https://www.techworm.net/2025/11/russianorthkoreapotentiallysyncingcyberattacks.html
34. https://krebsonsecurity.com/2025/10/shinyhunterswagebroadcorporateextortionspree/
35. https://gbhackers.com/qilinransomware3/
36. https://socradar.io/blog/darkwebprofileqilinagendaransomware/
37. https://www.cyberproof.com/blog/cyberattacksriseastensionmountsacrossindiapakistanborderpostterroristattack/
38. https://www.bleepingcomputer.com/news/security/proisraelhackershitiransnobitexexchangeburn90mincrypto/
39. https://www.cyberproof.com/blog/beyondtheblastradiusiransdigitalretaliationexpandswestward/
40. https://securityaffairs.com/183222/apt/ukraineseessurgeinaipoweredcyberattacksbyrussialinkedthreatactors.html
41. https://www.reuters.com/world/europe/ukrainerailwaysaysitsonlinesystemstargetedlargescalecyberattack20250324/
42. https://www.cyberproof.com/casestudies/advancedthreathunting/ 43. https://www.cyberproof.com/blog/connectwisescreenconnectattackscontinuedsurgeinrmmtoolabuse/
44. https://kpmg.com/kpmgus/content/dam/kpmg/pdf/2024/2024kpmgaisecuritybenchmarksurveyresults.pdf

Since 1999, UST has worked side by side with the world's best companies to make a powerful impact through transformation. Powered by technology, inspired by people, and led by our purpose, we partner with our clients from design to operation. Our digital solutions, proprietary platforms, engineering, R&D, products, and innovation ecosystem turn core challenges into impactful, disruptive solutions. With deep industry knowledge and a future-ready mindset, we infuse expertise, innovation, and agility into our clients' organizations—delivering measurable value and positive lasting change for them, their customers, and communities around the world. Together, with 30,000+ employees in 30+ countries, we build for boundless impact—touching billions of lives in the process.

ust.com

Version 0104-20260429