ncc group

FOX IT
part of ncc group

Annual Cyber Threat Intelligence Report

2025

Content

Section 1
Forward

Matt Hull
VP of Cyber Intelligence
and Response, NCC Group

2025 did not introduce entirely new cyber threats. Instead, it offered repeated and often uncomfortable reminders about the cost of overlooking fundamentals in an environment where cyber risk is inseparable from how modern organisations operate.

Across the incidents we observed, attackers demonstrated patience rather than speed and understanding rather than brute force. Ransomware groups and intrusion teams increasingly relied on identity as their primary point of leverage. Many compromises began with familiar weaknesses, including infostealer harvested credentials, reused passwords, absent multi factor authentication, and well crafted social engineering. Once access was gained, attackers took time to learn how organisations actually functioned before acting.

High-profile incidents affecting organisations such as Marks and Spencer and Jaguar Land Rover reinforced this pattern, showing that scale, brand recognition, and prior investment do not remove exposure when identity controls and internal trust assumptions are exploited. This shift matters because it confirms that identity, not the network perimeter, now defines the front line of defence, and that resilience depends as much on operational discipline as on technology.

Artificial intelligence further altered the balance. It did not eliminate differences between advanced and less capable adversaries, but it significantly raised the baseline. Tactics that once signalled low sophistication, such as poorly written phishing emails or implausible impersonation, largely disappeared in larger breaches. Less experienced actors are now able to produce convincing communications, spoofed personas, and even deepfake audio at scale. The result is not simply more attacks, but greater ambiguity, placing increased pressure on human judgement and verification processes.

At the same time, critical infrastructure sectors experienced sustained attention from nation-state actors seeking to position themselves for future activity. Telecommunications, energy, and utilities were subject to probing, prepositioning activity that remained below the threshold of disruption yet signalled clear strategic intent. Public warnings linked activity to Russian and Chinese interests, alongside growing Iranian cyber capabilities and activity. The significance lies not only in potential disruption, but in the uncertainty these conditions create for organisations responsible for systems that underpin economic stability and public confidence.

Throughout the year, one pattern remained consistent: intelligence proved valuable only when it shaped decisions. CISOs and executives engaged most when intelligence clarified what genuinely demanded attention, rather than adding to already long lists of controls and threats. Regulatory expectations reinforced this shift, placing greater emphasis on demonstrable understanding of risk rather than procedural compliance. As a result, cyber threat intelligence is now firmly embedded in governance and resilience discussions, and intelligence teams are increasingly expected to translate insight into defensible and actionable recommendations for leadership.

Supply chain exposure remained one of the most persistent routes into organisations. Trusted relationships, shared services, and third party platforms provided pathways that were often better understood by adversaries than by those relying on them. These incidents highlighted a recurring condition rather than isolated failures. Risk is frequently distributed across ecosystems in ways that outpace visibility and oversight, even as accountability remains firmly retained.

So, looking over this year's Annual Threat Intelligence Report, we reach a consistent conclusion. Cyber resilience is no longer defined by the presence of controls or the scale of investment. It is shaped by how clearly organisations understand their own operations, dependencies, and assumptions, and how willing leadership is to test those assumptions before adversaries do.

Section 2

Timeline of Critical Incidents

January

13/01/2025

Halcyon reports that a threat actor dubbed as 'Codefinger' uses compromised AWS credentials to encrypt Amazon S3 buckets via Server-Side Encryption with customer-provided keys (SSE-C). This attack exploits AWS's secure encryption infrastructure in a way that prevents data recovery without the attacker-provided AES-256 key.

Following this, AWS Customer Incident Response Team observed a pattern involving a high volume of S3 CopyObject operations using SSE-C began to overwrite objects, which has the effect of re-encrypting customer data with a new encryption. AWS had deployed defensive tools to implement automatic mitigations; however, they have also advised customers to add additional security measures to reduce risk, including implementing short-term credentials, implementing data recovery procedures, monitoring AWS resources for unusual access patterns and blocking the use of SSE-C unless required by an application.

February

11/02/2025

A major leak of Black Basta's Matrix chat logs has been exposed by a user using the handle 'ExploitWhispers'. The leaked JSON chat data includes fields such as timestamps, sender/recipient, thread IDs and message content. Researchers attribute the leak to internal conflict within the group; the leaker claimed it was retaliation for Black Basta targeting Russian banks. The logs also surface insights of the gang's inner workings, detailing Black Basta's structure, tools, methods and discussion of exploits, stolen credentials, phishing methods and tools used like Cobalt Strike.

21/02/2025

Bybit, a cryptocurrency exchange, was hacked – resulting in the theft of a record $1.5 billion worth of Ethereum from their cold wallet. Attackers compromised a third-party multisig signer's environment (Safe{Wallet}).

When the Bybit signers were approving what they thought was a routine transaction, they were unaware they were signing over control of their wallets to the attackers. Post incident investigation shows that stolen ETH was funnelled through cross-chain bridges and mixers to obfuscate the trail. The movement pattern mirrored past DPRK-linked operations, indicating that the attack was planned rather than opportunistic. Further analysis confirmed that the tactics align with earlier operations attributed to North Korea, specifically the Lazarus Group.

March

12/03/2025

The FBI released an advisory to warn organisations about the Medusa ransomware group looking to attack Gmail and Outlook users. The warning urged users to implement two-factor authentication for all webmail and VPN accounts.

24/03/2025

INTERPOL arrested 306 suspects and confiscated 1,842 devices as part of an international operation codenamed Red Card that happened from November 2024 to February 2025. The operation focused on disrupting and dismantling cross-border criminal networks which cause significant harm to individuals and businesses. The seven participating countries in the operation were Benin, Côte d'Ivoire, Nigeria, Rwanda, South Africa, Togo, and Zambia.

April

19/04/2025

Marks & Spencer (M&S), a major British multinational retailer of clothing, beauty products and more, dealt with a major cyber incident over the Easter weekend (19–20 April 2025) that affected its online operations and store services, forcing M&S to suspend all ecommerce for weeks. The company confirmed that attackers had accessed personal customer information such as names, phone numbers, email addresses, addresses and order histories.

M&S also warned investors that the incident could reduce annual profits by approximately £300 million. According to reports, the ransomware group Dragonforce sent an abusive email using an employee email account to M&S CEO Stuart Machin. The message claimed responsibility for the hack, asserted that company servers had been encrypted and demanded payment. Meanwhile, law enforcement and cybercrime agencies have linked the attack to the Scattered linked threat group. The group is believed to have established initial access, and then deployed the DragonForce ransomware group to encrypt systems.

May

21/05/2025

Microsoft's Digital Crimes Unit (DCU), Europol, and international partners carried out a coordinated operation to disrupt the Lumma (LummaC2) infostealer's infrastructure, severing communications between the malicious tool and victims. Authorities seized or blocked ~2,300 malicious domains, and more than 1,300 domains seized or transferred to Microsoft, including 300 domains actioned by law enforcement with the support of Europol, will be redirected to Microsoft sinkholes.

28/05/2025

ConnectWise, the US-based IT management and remote access software company, has confirmed that it was a victim of a cyberattack attributed to a nation-state actor. The incident was centered on a flaw in ScreenConnect, their widely used remote access and control platform, that allows remote threat actors to execute malicious code on systems.

ConnectWise stated that only a small number of ScreenConnect customers were affected, and that they have already been contacted. ConnectWise also confirmed that it has coordinated with law enforcement regarding the incident.

June

25/06/2025

French authorities have arrested five individuals allegedly linked to infamous BreachForums, a hacking forum involved in trading leaked data, stolen databases, malware and other illicit hacking tools. The forum has been associated with multiple data breaches affecting major companies, including AT&T and Tokopedia. The Brigade de Lutte contre la Cybercriminalité (BL2C) of the Paris Police Headquarters have apprehended four hackers operating under the aliases 'ShinyHunters', 'Hollow', 'Noct' and 'Depressed'. A fifth individual known as 'IntelBroker' was arrested in February 2025 and remains in French custody.

Timeline of Critical Incidents

July

07/07/2025

Attackers have been actively exploiting the SharePoint ToolShell vulnerabilities since early July by abusing partially remediated spoofing and remote code execution flaws in on-premises Microsoft SharePoint servers. The issues were initially tracked as CVE-2025-49706 and CVE-2025-49704 and were later patched as CVE-2025-53770 and CVE-2025-53771.

Multiple proof-of-concept exploits have been published on GitHub. Several threat actors leveraged ToolShell in their campaigns, including Storm-2603, Threat Group-3390, and ZIRCONIUM. These activities impacted organisations in the finance, education, energy, and healthcare sectors across Asia, Europe, and the United States.

August

04/08/2025

Bouygues Telecom confirmed a data breach that exposed the personal information of 6.4 million customers. The company is one of France's largest telco communications providers with 14.5 million mobile subscribers. While the threat actor was not publicly identified, the incident mirrors recent attacks against US-based telecom operators linked to the Salt Typhoon group in late 2024. Stolen customer information included contact details, contract information, civil status data, company details, and international bank account numbers (IBANs).

07/08/2025

Salesloft disclosed a widespread supply chain breach involving its Drift application, where the threat actors abused compromised OAuth tokens to gain unauthorised access to Salesforce customer environments. The campaign enabled systematic data exfiltration, exposing CRM records such as contacts, accounts, opportunities, and support cases.

The attackers also scanned the stolen records for sensitive credentials, including AWS and Snowflake keys. The compromise was not limited to Salesforce integrations and affected other platforms connected to Drift, highlighting the risk posed by compromised third-party authentication tokens.

14/08/2025

Financial software provider Marquis Software Solutions has disclosed a data breach that impacted over 74 US banks and credit unions, exposing sensitive data of more than 400,000 customers. The Akira ransomware gang has been linked for the attack through a compromised SonicWall VPN, allowing them to access personal information such as names, addresses, Social Security numbers, Taxpayer Identification Numbers, financial account information, and dates of birth.

September

02/09/2025

Jaguar Land Rover (JLR) suffered a major cyberattack that disrupted global IT systems, halting manufacturing and retail operations.

The attack coincided with the UK's "New Plate Day," amplifying operational and financial impact. Production was suspended for over a month, resulting in losses exceeding $890 million and disrupting the broader supply chain, affecting thousands of downstream businesses and dealerships. The incident underscores the operational and economic risks that cyberattacks pose to major industrial manufacturers and their extended networks.

23/09/2025

A UK Ministry of Defence contractor, Dodd Group, has been targeted by the Russian ransomware group Lynx. The group claims to have stolen approximately 4 TB of data, including sensitive files from eight Royal Air Force and Royal Navy bases.

The breach exposed around 1,000 documents containing staff names, emails, phone numbers, vehicle details, and MoD contacts, with some files marked "Controlled" or "Official Sensitive." The stolen data could be exploited by state-backed actors for espionage or to carry out further cyberattacks.

October

10/10/2025

Vietnam Airlines Passengers Data Leak - Scattered LAPSUS$ Hunters, publicly released Vietnam Airlines customer data following a broader Salesforce related extortion campaign. The leak included over 7.3 million customer records with names, dates of birth, email addresses, phone numbers, and residential addresses from November 2020 to June 2025. The data was released after the group's October 10 deadline for payments due.

27/10/2025

INTERPOL Operation Sentinel, a coordinated effort across 19 African countries, led to the arrest of 574 suspects and the recovery of $3 million. The operation dismantled cybercrime networks by taking down over 6,000 malicious links, 30 fraudulent servers, and 43 malicious domains while decrypting six undisclosed ransomware variants. It disrupted business email compromise, digital extortion, and ransomware campaigns across the African continent.

November

06/11/2025

Coupang Data Breach Exposes information of 33.7 million Customers - South Korean retail giant Coupang confirmed a massive data breach, exposing personal information of 33.7 million users. The incident was linked to a former employee who misused unrecalled cryptographic signing keys to generate fake access tokens and access customer data from overseas. Names, contact details, shipping addresses, and order histories were compromised. South Korean authorities have launched an investigation, and Coupang may face penalties of up to 1 trillion won under the Personal Information Protection Act.

18/11/2025

The US Congressional Budget Office (CBO) confirmed a cyberattack that exposed sensitive communications between congressional offices and CBO analysts, including draft reports, economic forecasts, internal emails, and other confidential data. The breach discovered in early November has been attributed to the Chinese state-sponsored APT group Silk Typhoon. Officials warned that compromised communications could be used to craft highly targeted phishing attacks. This incident represents one of the most significant cyber security breaches targeting American legislative infrastructure.

December

03/12/2025

Everest Ransomware Group leaked 1TB of ASUS database – The Taiwan tech giant confirmed a third-party supplier breach resulted in the exposure of approximately 1 TB of data, including ASUS phone camera source code, firmware, binary modules, AI models, calibration files, test APKs, and internal tools. The incident was claimed by Everest ransomware group and published the sample data to its data leak site, claiming that they also hacked ArcSoft, and Qualcomm. Threat actors now have a complete blueprint for how a critical piece of hardware works, potentially enabling future exploits.

Section 3

Ransomware Key Statistics

50%

Global ransomware attacks increased by 50% in 2025

28%

Industrials accounted for 28% of ransomware attacks in 2025

13%

Qilin was responsible for 13% of attacks in 2025

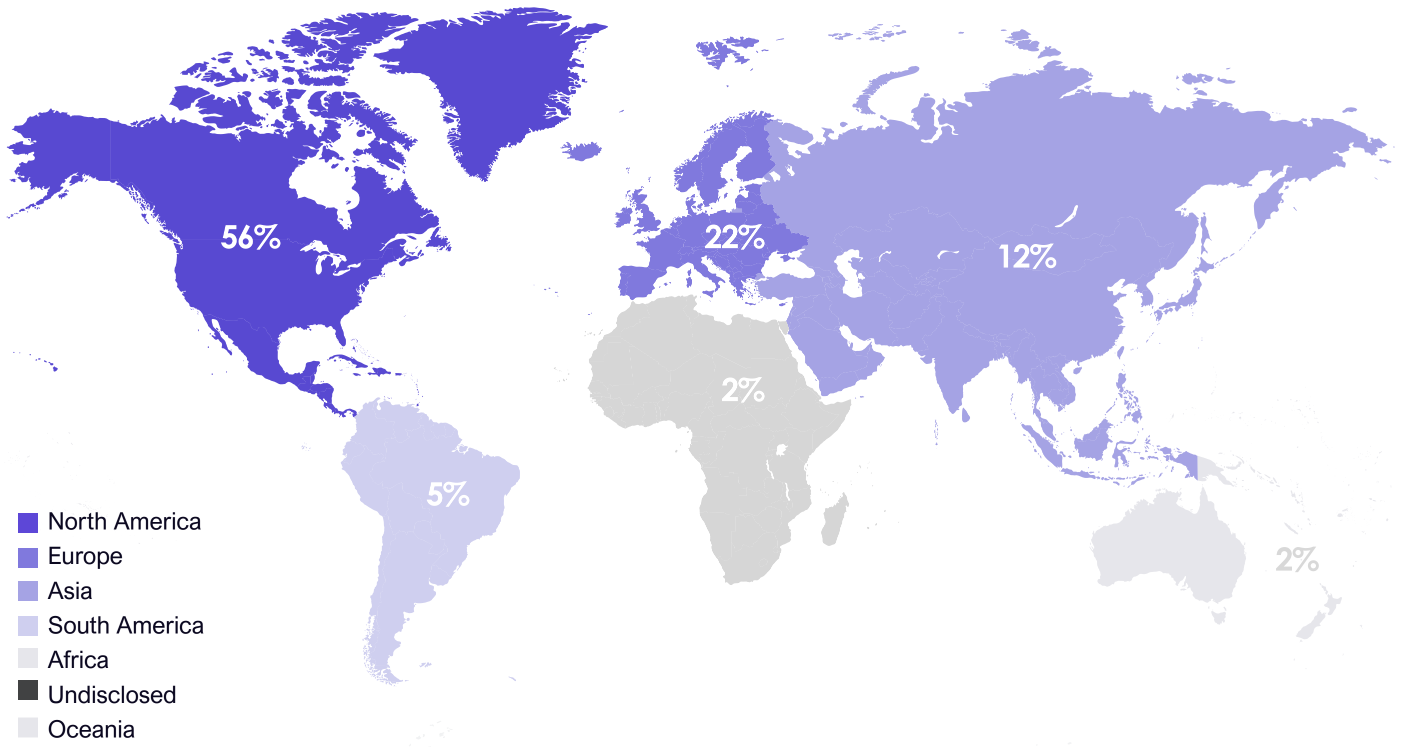


Figure 1 Number of Ransomware Attacks by Region 2025

NCC Group can support you in mitigating ransomware threats.
Please see our contact details at the end of this report, should you require assistance.

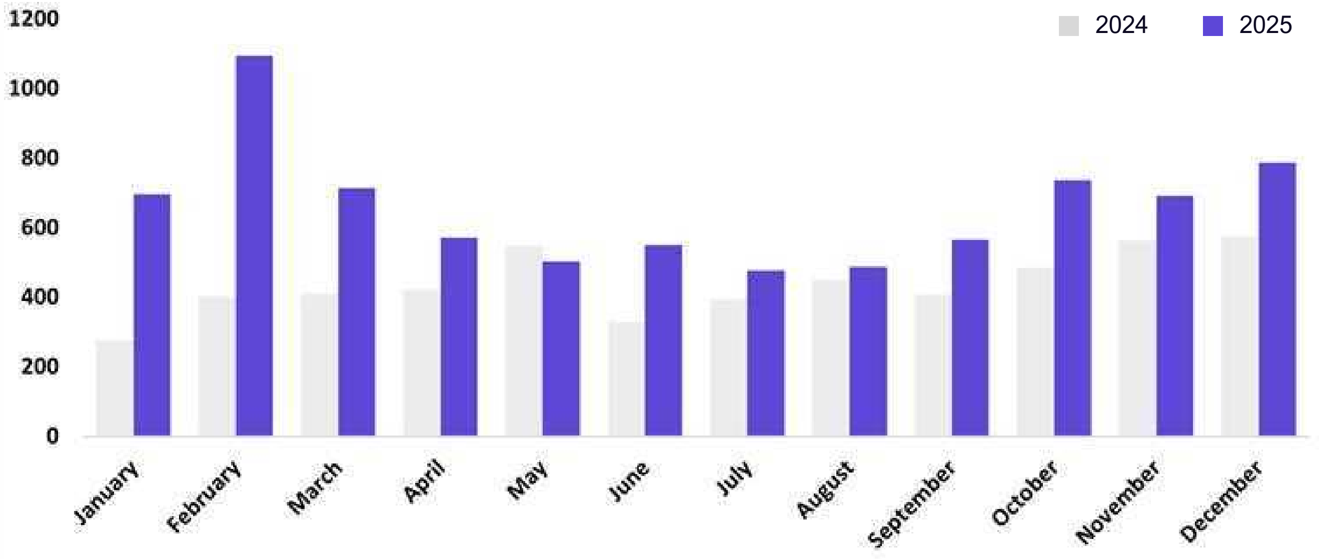


Figure 2 Number of Ransomware Attacks 2024 vs 2025

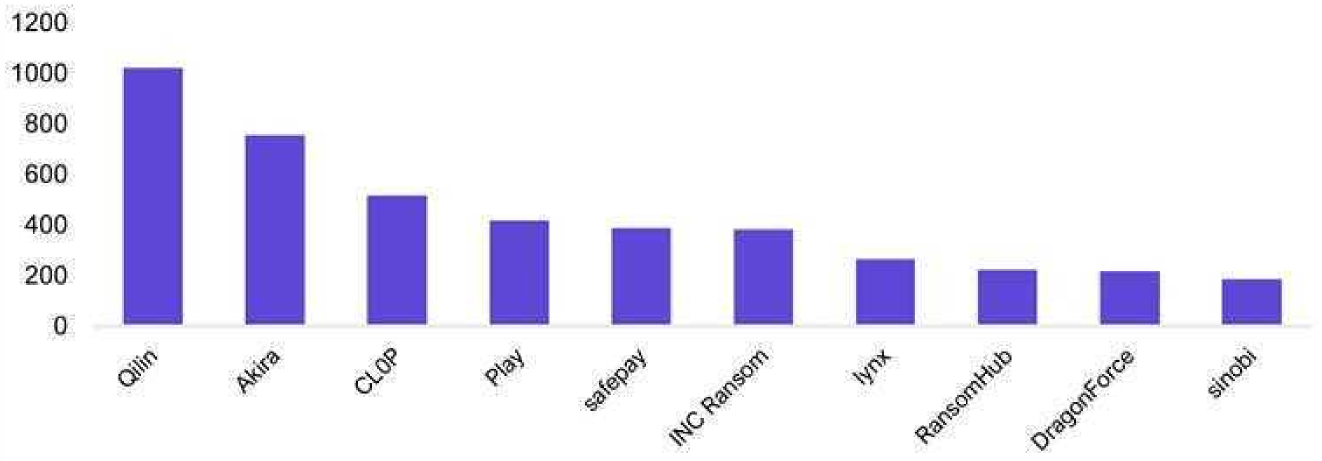


Figure 3 Top 10 Threat Actors 2025

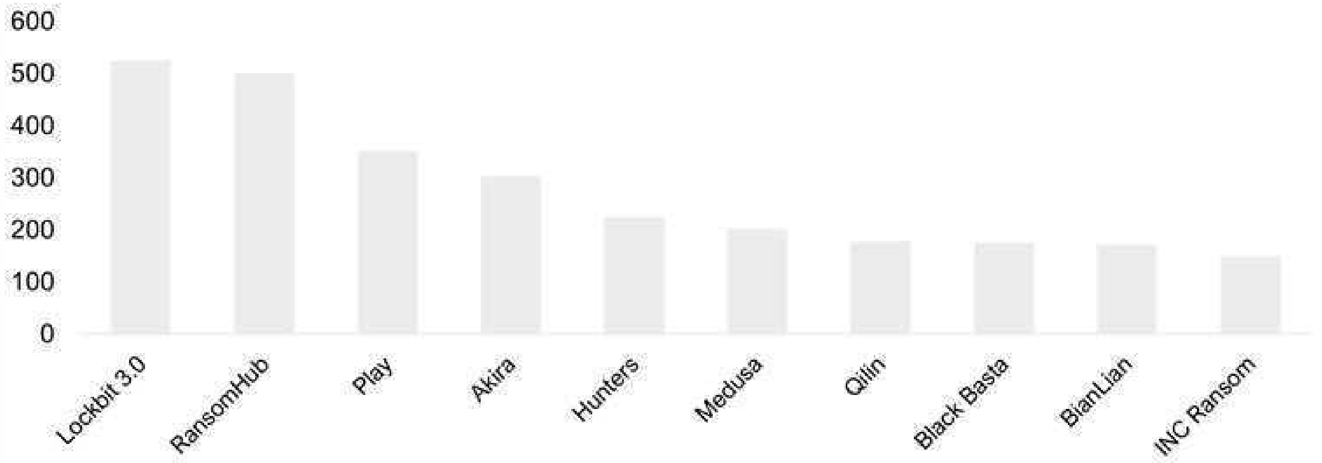


Figure 4 Top 10 Threat Actors 2024

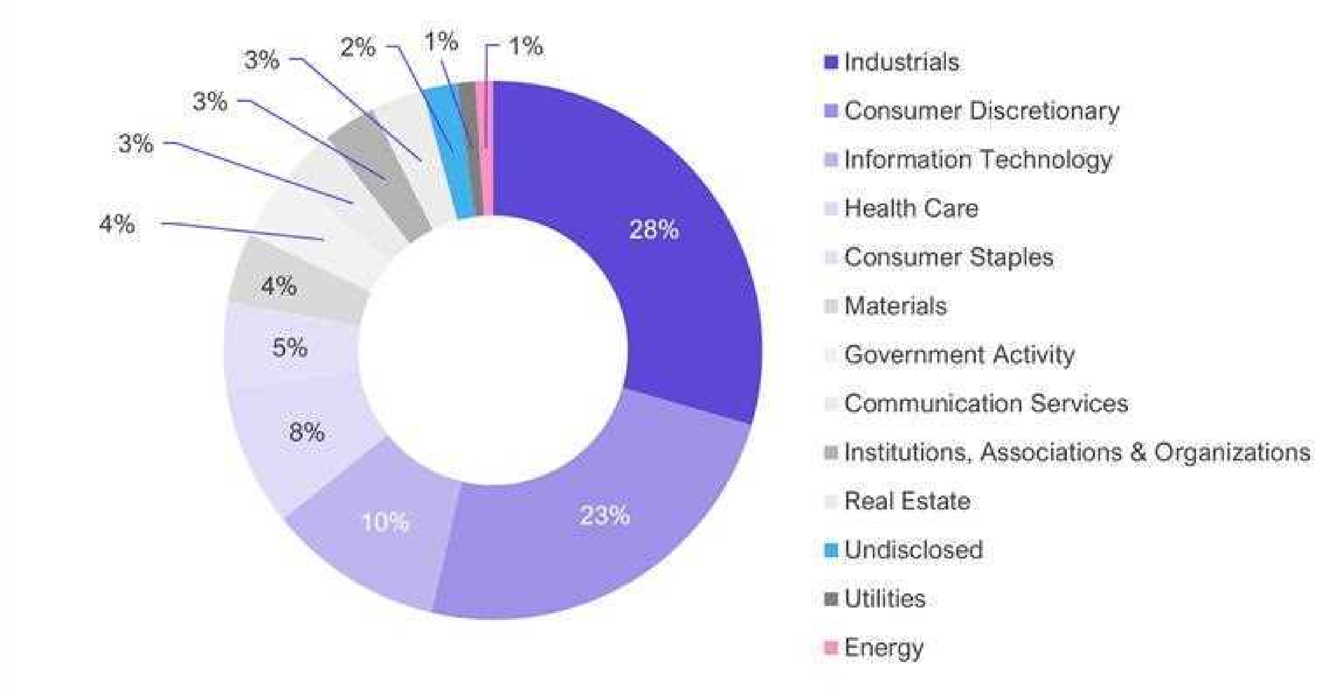


Figure 5 Top Targeted Sectors 2025

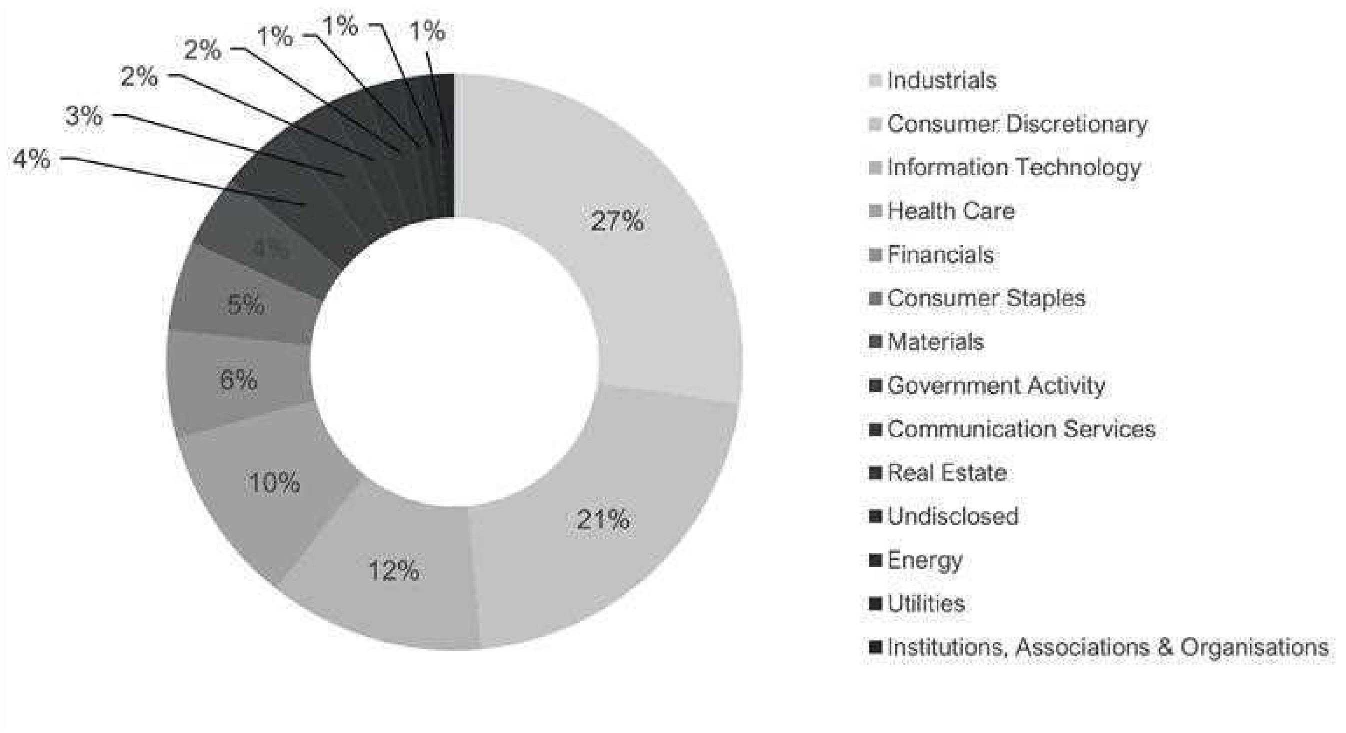
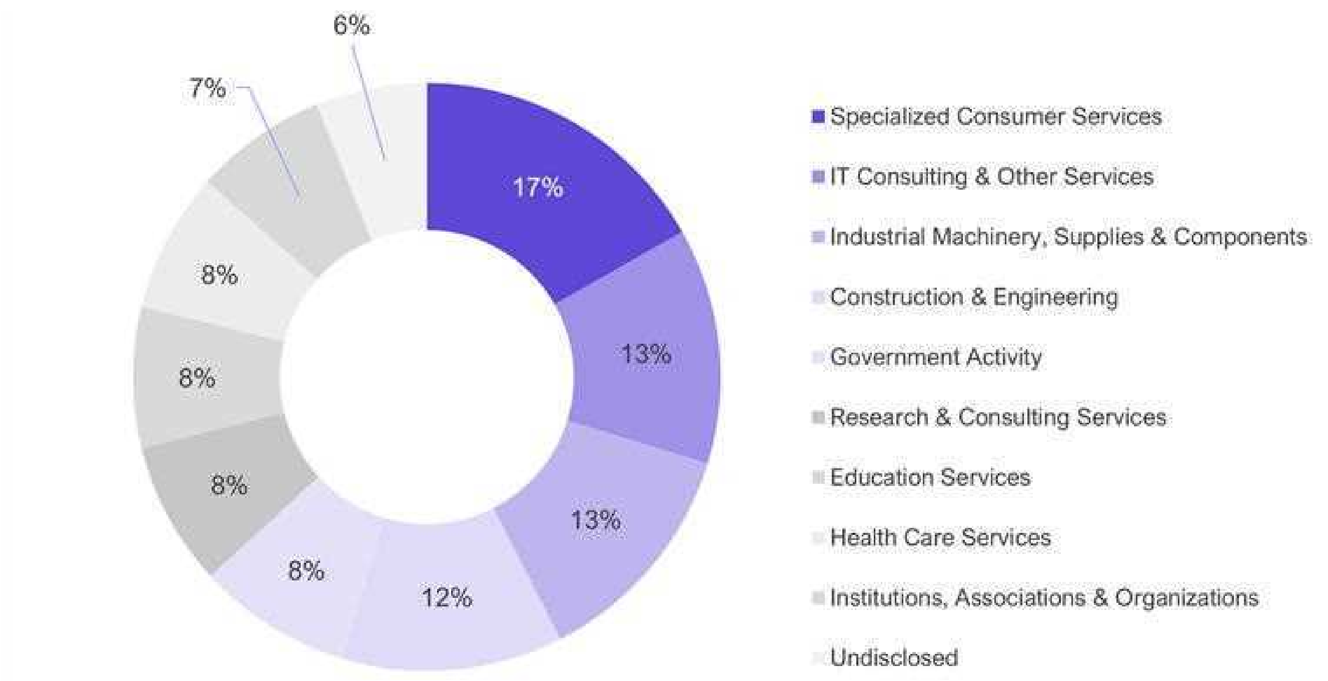
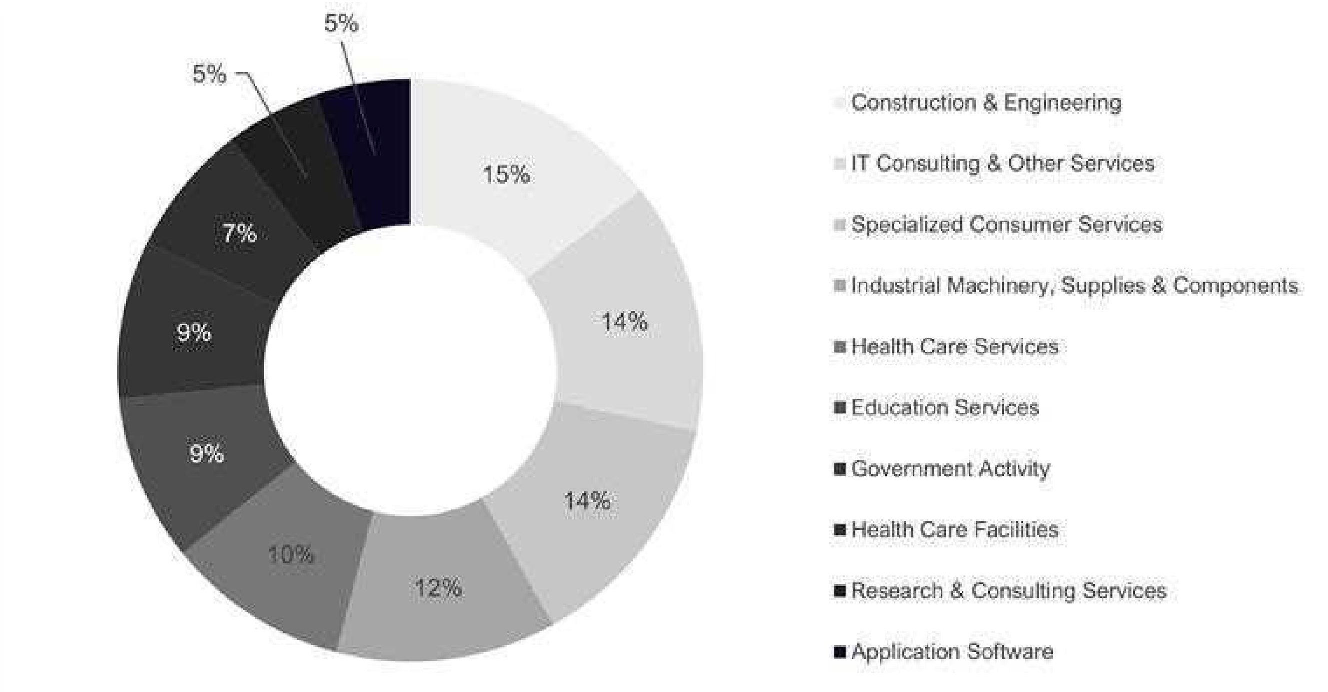


Figure 6 Top Targeted Sectors 2024



*Statistics shown represent percentages calculated from the top ten entries

Figure 7 Top 10 Ransomware Attacks by Sub-Industry 2025



*Statistics shown represent percentages calculated from the top ten entries

Figure 8 Top 10 Ransomware Attacks by Sub-Industry 2024

NCC Group can support you in mitigating ransomware threats.
Please see our contact details at the end of this report, should you require assistance.

Section 4
Ransomware Statistical Trends 2025

2025 had a major shift in the number of attacks per month within the ransomware threat landscape. 7,874 attacks were recorded, an increase of 50% from 2024.

This surge was noticeable in the 1st and 4th quarters of the year, with February and December experiencing the highest monthly number of attacks with 1093 and 788 respectively. This is the same trend that we saw last year, where there was an increase in attacks in December. The increase in ransomware activity in December is a deliberate tactic by threat actors, who seek to exploit reduced staffing levels and heightened business pressure during the holiday period. Organisations should therefore strengthen their defensive posture in advance by enforcing multi-factor authentication (MFA), ensuring systems are fully patched before the holiday break, and reinforcing employee awareness of seasonal phishing.

Ransomware activity increased across most regions in 2025. North America remained the most targeted region with 4,372 attacks, an increase of 52% from 2024. Asia was hit by 906 attacks, a 59% increase from 2024, and South America saw 414 attacks, a 50% increase from 2024. Europe, Africa and Oceania experienced a modest increase in ransomware attacks.

Qilin became the most prominent threat actor of the year after ascending the top list in June 2025. The group maintained its dominance through the second half of the year by sustaining a high operational tempo, aggressive double-extortion tactics, and a focus on industrial and manufacturing sectors with high business continuity impact.

The rise in attacks in 2025 was driven by attackers prioritising operational disruption over data theft, alongside the maturity of Ransomware-as-a-Service (RaaS) ecosystems, widespread availability of initial access brokers and persistent security gaps in the industrial and Operational Technology (OT) environments. Additionally, the widespread adoption of generative AI introduced new attack vectors that were quickly abused by threat actors.

FunkSec is an example of a ransomware operation that relies on generative AI for code development, including encryption and evasion features.[1]

The group's ransomware strain, FunkLocker, is using AI to expedite its development while relying on abusing legitimate Windows utilities to disable security defences and disrupt systems.[2] The development of FunkLocker shows signs of AI snippet coding patterns, which resulted in inconsistent code generation.[3]

Prompt injection and indirect prompt injection attacks enabled the manipulation of AI systems without deploying malware.[4] AI assisted social engineering, reconnaissance and malware deployment significantly reduced the attacker's effort and increase campaign effectiveness.

Despite law-enforcement pressure and takedowns, the threat landscape fragmented, resulting in sustained high activity throughout the year with industrial, manufacturing and other critical sectors bearing its impact.

Industrial Remains the Top Ransomed Sector

The Industrial sector remained the most targeted in 2025, having 2,190 attacks, an increase of 54% from 2024. This sustained targeting reflects threat actors' focus on environments where operational disruptions yield maximum extortion leverage, and downtime can lead to significant financial and supply-chain losses.

Qilin, Akira, and Play were top ransomware groups targeting the Industrial sector, having 298, 283 and 178 attacks respectively throughout the year. Qilin combined encryption with data exfiltration to increase its extortion leverage, which pressured organisations into payment. Similarly, Akira maintained a strong focus on industrial targets, exploiting exposed services and weak credentials to compromise networks before encrypting critical systems and backups. In addition, Play continued to target organisations with mixed IT-OT environments, leveraging fast-moving intrusion techniques to disrupt business operations.

The industrial sector's reliance on highly interconnected supply chains significantly amplifies the impact of ransomware attacks. A single successful compromise can cascade across suppliers, logistics providers, and downstream partners, magnifying disruption well beyond the initial target organisation. This interconnectedness continues to make the industrial sector an attractive target for ransomware groups seeking to maximise scale and impact.

Attacks on the Industrial sectors, such as disruptions at Jaguar Land Rover, resulted in prolonged production shutdowns and downstream impacts on suppliers. Multiple attacks against logistics and industrial services firms that halted operations for days or weeks.[5] Similarly, the Marks & Spencer ransomware incident illustrated how attackers apply similar tactics to retail environments with industrial-like operational dependencies.[6]

This incident led to the suspension of online sales for more than six weeks, disrupted payment and inventory systems, and was estimated to cost approximately £300 million. This highlights how ransomware campaigns increasingly target organisations where digital and physical operations are tightly coupled.

The sustained targeting of industrial and adjacent sectors in 2025 highlights the need for organisations to move beyond reactive security measures. As ransomware threat actors continue to exploit operational dependencies, legacy systems and supply-chain connections, improving cyber resilience through stronger IT-OT visibility, segmentation and incident readiness is critical to reducing operational and financial risk.

Most Active Ransomware Threat Actors: Qilin, Akira, and Cl0p

In 2025, Qilin, Akira and Cl0p emerged as the three most active ransomware threat actors, collectively accounting for a significant number (2,294 out of 7,874) of total global ransomware activity. While each group employed distinct operational models and targeting strategies, all three demonstrated a clear focus on high-impact organisations, particularly within industrial, manufacturing, and logistics sectors.

Qilin rose sharply in activity from mid-2025 and sustained its position as the most prominent ransomware threat actor (1,022 attacks) through consistent victim disclosures and high operational tempo. This RaaS operation prioritises operational efficiency, leveraging access to exposed VPNs, RDP or stolen credentials, followed by living-off-the-land execution, short-lived C2 beaconing, and fast, enterprise-wide encryption using Go or Rust-based payloads.[7] The group also released a legal services offering on its platform, introducing the 'Call a Lawyer' feature to help guide affiliates with their targets.[8]

Qilin stands out through a centralised, franchise-style RaaS model in which affiliates (typically low-to-mid-skill) are responsible only for gaining initial access, while core operators control payload configuration, negotiations, payments, and data-leak operations.

This structure lowers risk, allowing high-volume targeting across all industries and is further differentiated by Qilin's use of external 'legal counsel' in negotiations to apply regulatory and reputational pressure.

Akira maintained a steady and widespread presence throughout 2025, continuing to target a broad range of sectors, with notable concentration in Industrials (283 out of 755 attacks) and Consumer Discretionary (169 out of 755 attacks). The group demonstrated its continuous evolution alongside its partners. CISA released an update to Akira's TTPs, highlighting its reliance on exploiting unpatched VPN and backup systems, credential abuse, and the use of legitimate remote management tools to blend in with normal administrative activity. This is typically followed by lateral movement, data exfiltration, and faster-encrypting Akira_v2 variants that increasingly target virtualised environments.[9] Akira's consistent activity and rapid execution made it a persistent threat, especially for organisations with limited visibility across IT and OT environments.

Cl0p remained highly impactful (517 attacks) due to its focus on large-scale, opportunistic campaigns, often involving vulnerabilities in third-party software and supply-chain components, such as MOVEit, Cleo, and Oracle E-Business Suite.[10,11]

Rather than widespread encryption, the group frequently relied on data theft and extortion, affecting numerous organisations simultaneously through a single exploitation vector. This approach reinforced the growing risk posed by supply-chain dependencies in interconnected industrial ecosystems.

Collectively, the activity of Qilin, Akira, and Cl0p in 2025 highlights a ransomware landscape characterised by high operational impact, varied extortion models, and increasing reliance on speed and scale. Their sustained activity underscores why it is crucial for sectors to reinforce their organisational resilience not only against encryption-based disruptions but also against data theft, supply-chain compromise, and rapid, automated victimisation.

Additionally, organisations need to enhance their preventive measures, complemented by robust third-party risk management, identity and access hardening, continuous monitoring for data exfiltration, and rehearsed response playbooks that assume compromise will occur.

Regional Ransomware Trends

North America (4,372 attacks) and Europe (1,718 attacks) continued to record the highest number of attacks, consistent with trends observed since 2021. Asia saw a notable increase of 59%, and South America 50% rise in attacks. Africa experienced a modest increase of 32%, and ransomware activity in Oceania also increased by 21%.

North America continued to experience a high frequency of ransomware attacks in 2025, particularly across Industrials (1,301 attacks), Consumer Discretionary (1,088 attacks) Information Technology (383 attacks), and Health Care sectors (404 attacks).

A widely reported incident impacting North America was the Ingram Micro ransomware attack in July 2025, when SafePay disrupted global ordering and internal systems, affecting operations in the US, Canada, and beyond before systems were gradually restored.[12]

Europe also experienced numerous high-impact ransomware campaigns targeting Industrials (544 attacks), Consumer Discretionary (398 attacks), and Information Technology (211 attacks). Incidents such as the Jaguar Land Rover production disruption and the Kido international ransomware attack against a London-based education provider demonstrated how attackers focused on both operationally critical systems and sensitive data targets.[13,14] Ransomware activity in the region continued to leverage double-extortion tactics, combining both encryption and data theft to increase pressure on victims.

In the APAC region, Industrials (196 attacks), Information Technology (157 attacks), and Consumer Discretionary (145 attacks) saw increasing ransomware pressure in 2025. Incidents were reported across Japan, South Korea, India, and Southeast Asia, with threat actors often leveraging exposed OT infrastructure and third-party access. These campaigns disrupted production and logistics operations, even when incidents were not widely publicised.

The observed downward trend in ransomware payments continued into 2025, with the share of organisations paying ransoms declining to a record low of 23%.[15] According to a survey of IT professionals across regions, the APAC region reported the highest proportion of ransomware payments (85%), followed by the UK (68%), North America (66%), and Europe (50%).[16] Regulations and law enforcement responses influences the payment behaviour across regions. For example, the UK decided to ban public sector bodies from paying ransom outright and introduced requirements for private organisations mandating them to notify authorities before making any ransom payments.[17]

This measure intends to reduce financial incentives driving ransomware activity. Globally, regulators and law enforcement agencies across the globe have continued to discourage ransom payments, linking them to increased targeting. Instead, they emphasise the importance of reporting, coordinated response, and pursuit of threat actors over negotiation.

Such regulatory developments have become part of a wider international debate, with governments including Australia, several EU member states, the US, Canada, and Singapore exploring similar restrictions and signing up to the International Counter Ransomware Initiative pledge, which discourages organisations from paying ransoms. However, the pledge is not legally binding, and no countries outside the UK and Australia have so far pursued outright bans.

The potential consequences of moving toward banning or tightly regulating ransomware payments remain uncertain, but such measures could significantly reshape organisations' incident response timelines, cost of recovery assessments and insurance relationships.[18]

Conclusion

In 2026, ransomware activity is expected to continue increasing, in line with the observed trend since 2021. Next-generation ransomware variants such as LockBit 5.0, may allow the group to reclaim significant market share within the ransomware threat landscape and potentially drive shifts in attacker tactics and affiliate behaviour.

The upgrade in architecture and advanced evasion techniques, such as control-flow obfuscation, API hashing, and aggressive EDR bypass, enhances stealth and success rates, making such variants a major threat to watch out for.[19] Should established ransomware brands successfully regain trust among affiliates, the landscape may temporarily recentralise around a smaller number of highly efficient RaaS operations.

At the same time, the use of AI-based tools is expected to rise and develop further, intensifying the trend of low- to mid-skilled threat actors executing high-impact attacks. Generative AI and LLMs are increasingly leveraged to automate phishing campaigns, enhance social engineering pretexts, generate malware variants, and assist with reconnaissance and negotiation processes. This lowers the barrier to entry for ransomware operations while increasing attack speed at scale.

Organisations should prioritise resilience over prevention alone, focusing on having strong identity controls, rapid detection and response, fast backup and recovery processes, and effective management of third-party risks to reduce both the likelihood and impact of ransomware incidents.

Section 5

Law Enforcement Targeting Ransomware

In 2025, law enforcement carried out a series of major international operations targeting cybercriminal infrastructure.

Efforts like Operation Endgame took down hundreds of servers and domains used for ransomware and malware. Authorities also issued international arrest warrants and seized millions in illegal cryptocurrency. Key actions included dismantling the Lumma Stealer network, responding to the Collins Aerospace ransomware attack, and ongoing efforts against groups such as Scattered Spider.

Sanctions on Russian hosting providers, shutting down forums like Cracked and Nulled, and targeting North Korean IT worker schemes showed the global scope of these operations. Although criminals adapted quickly, these actions made cybercrime riskier, more fragmented, and temporarily reduced the scale and confidence of criminal groups.

Operation Endgame

Operation Endgame supported by authorities in Europe and North America as well as private partners, aimed to disrupt the ransomware supply chain. In May 2025, the operation shut down approximately 300 servers and 650 domains, issued 20 international arrest warrants, and seized €3.5 million in cryptocurrency, bringing total seizures to over €21 million.[20,21]

The team also targeted loader malware, antivirus services, and key tools such as Rhadamanthys, VenomRAT, and the Elysium botnet. Whilst these actions haven't eliminated ransomware, they impact the cost of running an attack and weaken criminal networks.

Criminals could respond by changing tactics, becoming more secretive, or pausing activities. These disruptions may also reduce trust among threat groups, particularly if they suspect law enforcement infiltration. While some groups may attempt to fill gaps left by others, these efforts could have a lasting impact and temporarily deter new groups. However, cybercriminal networks have historically adapted quickly, and new services or marketplaces may emerge.

Lumma Stealer

In May 2025, Microsoft's Digital Crimes Unit led an international operation against the Lumma Stealer malware-as-a-service (MaaS) ecosystem.[22] Lumma's modular, subscription-based stealer enabled attackers of all skill levels to target Windows systems, resulting in the theft of credentials, cookies, wallet data, and other sensitive information.

Law enforcement obtained a US court order to seize and redirect over 2,300 Lumma-controlled domains to Microsoft's infrastructure.[23] This enabled traffic monitoring and coordinated international actions that dismantled command-and-control servers and disrupted Lumma's marketplace.

In the short term, this likely caused instability in ransomware and malware ecosystems, particularly for initial-access brokers and affiliates who lost infrastructure and distribution channels. Increased law enforcement pressure is expected to prompt stricter security and more careful vetting within threat groups, as concerns grow about compromised developers and shared infrastructure. This environment may further reduce trust, push activity into smaller, closed networks, and slow criminal collaboration.

Replacement capabilities, such as alternative loaders, rebuilt infrastructure, or successor marketplaces, are likely to emerge, reflecting the resilience of the MaaS model. However, the combined impact of domain and server seizures, takedowns of crypting and obfuscation services, marketplace disruption, arrests, and financial enforcement significantly raises operating costs and complexity. These pressures slow reconstitution and reduce overall scale, resulting in meaningful deterrence rather than permanent suppression, unless sustained and repeated law enforcement action continues.

NCA Response to the Collins Aerospace MUSE Ransomware Attack

In September 2025, the UK's National Crime Agency (NCA) and international partners responded to a ransomware attack on Collins Aerospace that disrupted its MUSE check-in and boarding platform at major European airports.[24] Airports, including Heathrow, Brussels, Berlin Brandenburg, Dublin, and Cork switched to manual processing, resulting in widespread delays and cancellations.[25] Law enforcement identified and pursued the supply-chain attack, arresting a man in his forties in West Sussex under the Computer Misuse Act.[26]

Reports and regulatory filings confirmed a "cyber-related disruption" to MUSE consistent with ransomware, and researchers linked the attack to HardBit. The Everest cartel later claimed responsibility, but attribution remains unclear, as is common in early stages of complex supply-chain incidents.[27] This caused short-term instability for aviation IT vendors, airlines, and affiliates, prompting calls for improved security, more careful vetting of partners, and a shift to smaller, private channels. The fear of infiltration will reduce trust between developers and affiliates, and substitute services are likely to emerge, given the sector's history of rapid recovery. Permanent disruption is unlikely, but international pressure, NCA arrests, and cross-border cooperation increase risks and costs for offenders, leading to losses and fragmentation in the ransomware supply chain.

Scattered Spider Law Enforcement action

Throughout 2025, law enforcement maintained steady pressure on the social engineering group Scattered Spider, also known as Octo Tempest, UNC3944, or 0ktapus. As the group shifted from targeting retail and insurance to airlines and transportation, sector-specific warnings increased, indicating a clear trend. These incidents were planned, human-driven attacks rather than random malware.

In July 2025, the UK's NCA arrested four individuals connected to the April attacks on M&S, highlighting both the authorities' persistent efforts and the group's complex, affiliate-style structure, which complicates large-scale attribution and prosecution.[28] In June 2025, the FBI also issued a public warning, alerting airlines and transportation companies to Scattered Spider's ongoing intrusions.[29,30] In August 2025, a Florida man previously charged in connection with Scattered Spider was sentenced to 10 years in prison and ordered to pay nearly $13 million for SIM swapping and related fraud.[31]

From a threat intelligence perspective, law enforcement actions in 2025 led to a temporary decline in Scattered Spider's activities, demonstrating that authorities can disrupt individuals but not the main group. While some members became inactive after arrests, new attacks soon targeted other industries, highlighting the group's resilience and the ongoing challenge of dismantling loosely connected criminal networks.

Coordinated Sanctions Against Zservers and Aeza

In February 2025, the United States, Australia, and the United Kingdom jointly sanctioned Zservers, a Russian bulletproof hosting provider supporting LockBit, to disrupt ransomware operations.[32] US Office of Foreign Assets Control (OFAC), Australia's Department of Foreign Affairs and Trade (DFAT), and the UK's Foreign, Commonwealth & Development Office (FCDO) also named two Zservers administrators, Alexander Igorevich Mishin and Aleksandr Sergeyevich Bolshakov, for enabling ransomware and other crimes.[33]

The Treasury reported that Zservers promoted 'bulletproof' services on cybercriminal forums and leased numerous IP addresses used by LockBit affiliates to organise and launch attacks. Canadian law enforcement found evidence linking a ZServers-subleased IP to a LockBit management interface. The US. State Department stated this action, under E.O. 13694 as amended, is part of a broader effort with Five Eyes partners to weaken networks enabling Russian actors to target US and allied critical infrastructure.[34]

LockBit was also linked to the November 2023 breach of ICBC's US broker-dealer, illustrating how hosting services support major ransomware campaigns. Authorities followed up with another major action, sanctioning Aeza Group, a global bulletproof hosting service that facilitates ransomware, infostealers, and technology theft targeting US and international victims. OFAC's action, coordinated with the NCA, extended to Aeza's network, including its UK company Aeza International Ltd. Russian subsidiaries Aeza Logistic LLC and Cloud Solutions LLC, and four leaders: Arsenii Penzev, Yurii Bozoyan, Vladimir Gast, and Igor Knyazev. The Treasury cited Aeza's infrastructure supporting BianLian ransomware and the Meduza, Lumma, and RedLine infostealers.[35] These activities have targeted the US defence industrial base and technology firms, as well as hosting for BlackSprut, a Russian marketplace for drugs.

Cracked and Nulled Takedown

In January 2025, a coordinated law enforcement action known as Operation Talent dismantled the infrastructure behind two of the world's largest cybercrime forums, Cracked and Nulled.[36] German authorities led the operation, supported by Europol and several other countries, targeting a range of criminal activities. Europol's investigation found that both platforms facilitated entry into cybercrime by openly selling Cybercrime-as-a-Service (CaaS) including stolen data, malware, and hacking tools.

Authorities targeted both the main forum infrastructure and supporting services. DOJ details show the FBI and partners identified several Cracked servers and eight domain names. They also found infrastructure for its payment processor, Sellix, and a related bulletproof hosting service, all of which were seized through legal processes. Europol reported that 12 domains linked to Cracked and Nulled were seized during the operation, and that services such as Sellix and StarkRDP, a hosting service promoted by the suspects, were also taken down. The European operation resulted in two arrests, seven property searches, the seizure of 17 servers and over 50 devices, and the recovery of approximately €300,000.[37]

Simultaneously, US authorities unsealed charges against Lucas Sohn, a 29-year-old Argentinian living in Spain, identified as a Nulled administrator handling escrow for transactions involving stolen credentials and data.[38]

Cracked and Nulled were key components of supply chains supporting credential stuffing, initial access brokerage, and malware distribution, all of which drive ransomware campaigns. Europol noted that the growth of CaaS makes cybercrime more accessible to less-skilled actors and highlighted the use of AI-based tools on these platforms, such as scripts that scan for vulnerabilities, enhance attacks, and create more convincing phishing messages.

The DOJ also reported that products from Cracked were allegedly used in sextortion and cyberstalking, demonstrating how these marketplace tools can lead to large-scale victimisation.[39]

US Law Enforcement Action Against North Korea's Remote "IT Worker" Schemes

In June 2025, US law enforcement acted against North Korea's remote IT worker schemes. The DOJ announced two indictments, a plea agreement, an arrest, searches of 29 suspected laptop farms in 16 states, and the seizure of 29 financial accounts linked to money laundering and fraudulent websites operated by Russian national Mykhalio Petrovich Chudnovets.[40,41]

This network enabled more than 100 US companies to be infiltrated by workers using stolen or fake identities, often with assistance from US-based facilitators who arranged devices, payroll, and credentials. In July 2025, the US OFAC sanctioned Song Kum Hyok, a Russia-based facilitator (Gayk Asatryan), and four entities involved in contracting and hosting DPRK IT workers in Russia.[42]

North Korea sends skilled IT workers abroad to secretly obtain jobs with companies in the UK, US, and other countries, raising funds for the regime. These workers typically operate from Russia and China, posing as non-DPRK nationals to secure freelance work, often using fake identities and external assistance to conceal their origins. The money they earn is used to purchase banned goods and military equipment, supporting North Korea's illegal weapons and missile programs. Many DPRK IT workers earn significant incomes by holding multiple jobs simultaneously, often while freelancing.

As part of the broader June actions, prosecutors in Atlanta unsealed charges against Kim Kwang Jin, Kang Tae Bok, Jong Pong Ju, and Chang Nam Il.[43] They are accused of using fake identities to obtain remote developer jobs and subsequently stealing and laundering over $900,000 in virtual currency in 2022.

The State Department stated that the scheme is intended to raise funds for weapons of mass destruction and missile programs, often by impersonating Americans and transferring money through digital assets.

Sanctions are designed to make it more difficult for these networks to pay, place, and protect North Korean operatives, and to warn companies, especially in tech and crypto, that hiring individuals with false identities poses a significant compliance risk. Law enforcement actions increase costs and risks for recruiters, disrupt daily operations, and encourage organisations to strengthen their hiring checks.

Authorities Seize BreachForums New Clearnet Cybercrime Marketplace Domain

In October 2025, law enforcement agencies seized breachforums[.]hn, the latest public domain used by BreachForums.[44] They replaced the site with a multilingual banner displaying the seals of the US Department of Justice, the FBI, and France's BL2C and JUNALCO.

Just before the seizure, Scattered LAPSUS$ Hunters, an alliance named after ShinyHunters, Scattered Spider, and LAPSUS$, threatened to leak one billion data records allegedly from Salesforce customers unless their demands were met. Within hours of the domain seizure, the alliance posted on Telegram that law enforcement had "seized and destroyed" backend servers and old database backups, but claimed their broader campaign remained active.

Anyone visiting the domain, and its onion site, saw a notice stating, "This domain has been seized," indicating law enforcement control.[45] BreachForums has returned several times after previous shutdowns. It was originally established to replace RaidForums, which was taken down in 2022.

The original administrator, Conor Brian Fitzpatrick (known as "Pompompurin"), was arrested in March 2023, leading to a shutdown and subsequent restart under new leadership.[46]

The seizure of BreachForums demonstrates that agencies are now focusing on shutting down marketplaces and systems that support cyber-extortion, rather than solely targeting individuals. However, past cases show that these communities often split into duplications, private forums, or Telegram channels. Leak sites can also continue operating outside the seized domains, so risks to organisations still persist.

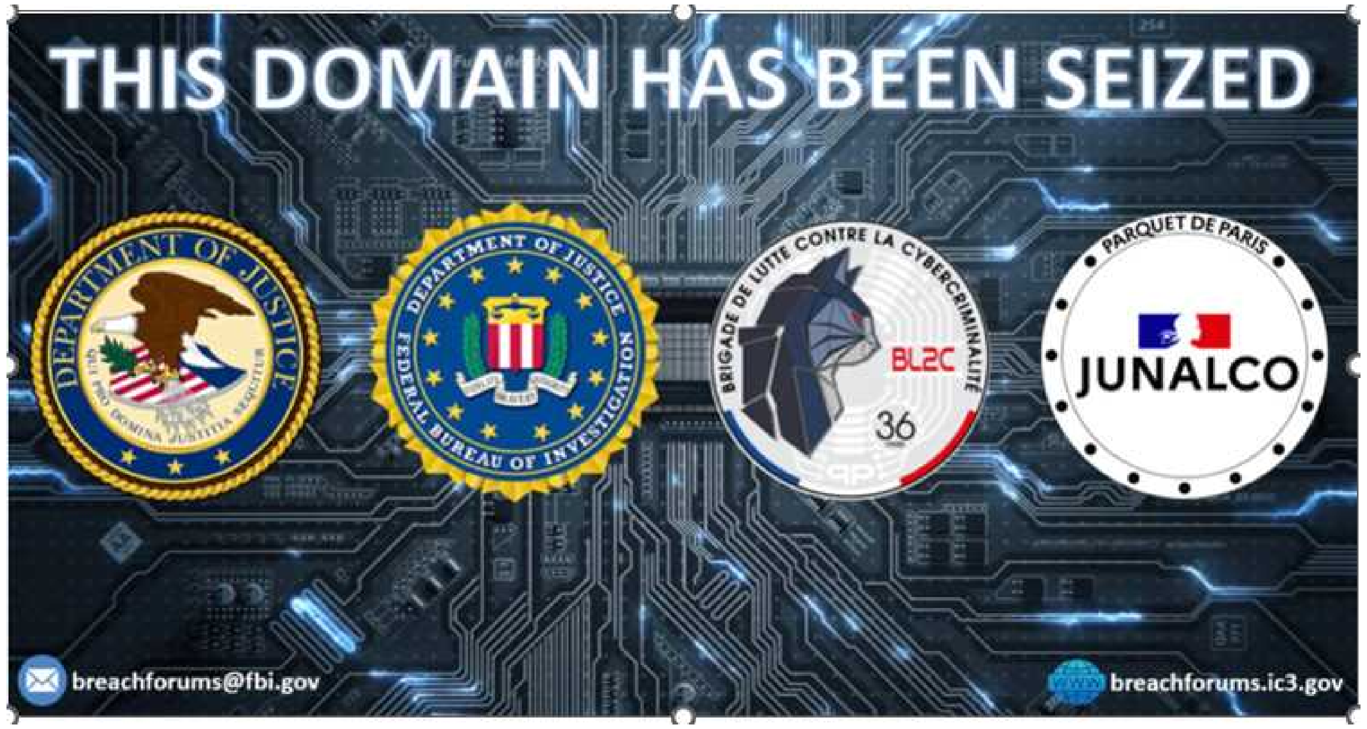

THIS DOMAIN HAS BEEN SEIZED
DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
BRIGADE DE LUTTE CONTRE LA CYBERCRIMINALITÉ
BL2C
36
PARQUET DE PARIS
JUNALCO
breachforums@fbi.gov
breachforums.ic3.gov

Figure 9 Seizure announcement[47]

Section 6

APT Activity in 2025 - Geopolitical Uncertainty Driving Information Advantage Through Cyber-Capabilities

As the cyber-capability most strongly associated with exercise of strategic nation-state power, analysts often look to geopolitical activities and stated national priorities to contextualise and understand publicly reported APT activity, and to draw inferences that support an intelligence-led shift in defensive posture.

This is arguably of particular interest in 2025 – a year which was geopolitically 'hot' by any standards. In addition to more conventional forms of cyber-espionage and intelligence gathering, cyber-attacks are framed as one tactic within a broader strategy of hybrid-warfare.[48] Officials describe the current period as a volatile and fragile state between war and peace, setting the conditions for pre-positioning and destructive attacks. [49,50,51] Influence operations, purported hacktivist campaigns, and even highly disruptive cyber-attacks which present as cybercrime, coincide with geopolitical events and adversary nations' strategic goals.

It is beyond the scope of this report to provide an overview of the high volume of reported APT activity globally in 2025. Instead, framed by the realities of current and anticipated geopolitics, analysis aims to highlight publicly reported APT activity which demonstrates how they align with real world goals and influence the threat landscape of Western nations and their allies.

Espionage

Nation-states with externally facing strategic goals, international dependencies influenced by geopolitical factors, or fears of international interference in domestic affairs have a strong demand for information; specifically, information capable of contributing to intelligence assessments on how nations or organisations of interest may act in the future or respond to potential scenarios.

Private sector organisations delivering or influencing government policy, or holding large data sets, can provide softer targets for high value information than traditional government or military targets.

Russian espionage interests take a stronger political and military focus, the two mechanisms by which Russia may be effectively opposed. The inferred goals of activities reported in 2025 have a common, very conventional, goal of espionage activity; to secure access to sensitive communications using cyber resources to creatively circumvent security and encryption mechanisms. Organisations and nations directly supporting Ukraine's defence against Russia's war, as well as Western centres of power such as the EU and NATO, are consistently targeted. Notable developments in these activities include:

- Two new APT groups active outside of Ukraine were disclosed: Void Blizzard (also tracked as Laundry Bear) and Curly COMrades.[52,53] In May, together, the Dutch government and Microsoft reported targeting of the Dutch police and members of the European defence sector by Void Blizzard as part of a global credential abuse campaign.[54]

  In August, CurlyCOMrades was reported to have targeted post-Soviet countries Georgia and Moldova. Both countries are seeking EU and NATO membership, and experienced notable Russia-linked influence operations coinciding with national elections in 2025. CurlyCOMrades shared infrastructure with Russian military intelligence (GRU)-linked Sandworm, also known as APT44, suggests the group may have broader objectives.[55]

- Turla, also tracked as Snake, Secret Blizzard, and Venomous Bear, continues to participate in broad espionage campaigns, including Attacker-in-the-Middle (AiTM) attacks to bypass multi-factor authentication and compromise the devices of international diplomats stationed in Moscow.[56]

  Through delivered spyware, encryption was disabled on the devices, allowing communications on Russian telecommunications infrastructure to be intercepted in an unencrypted format.

- Microsoft authentication processes were targeted using a range of attack methods. For example, using Device Code Authentication phishing, 1-1 social engineering through video call joining instructions, and watering hole campaigns.[57,58,59]

- Reporting detailed widespread compromise of encrypted chat applications including Signal, WhatsApp, and Telegram. Attacks were concentrated on intelligence gathering within Ukraine, often against individuals actively engaged in the conflict, and utilised malicious QR codes and phishing-based methods to abuse 'linked device' functionality.[60,61]

For China, economic and trade activities, foreign policy in the Asia-Pacific (specifically around Taiwan, and Hong Kong to a lesser extent), and initiatives intended to reduce supply chain dependencies on China in technology and critical minerals are assessed as priority areas to gather intelligence.

Reflecting the breadth and depth of the resources, and commitment to an intelligence-led strategy, Chinese APTs continue to set the standard for advanced capabilities to achieve persistence in desirable networks. Data leaks continue to provide an insight into the complex, coordinated and well-resourced private-sector blended environment within which Chinese APTs operate.[62]

As with Russian espionage activity, compromise of telecommunications networks remains a common theme, although Chinese APTs demonstrate a preference for technical initial access methods rather than social engineering. The use of quieter methods, known as 'living off the land' techniques, and layers of redundancy demonstrate a clear prioritisation of long-term access (and even pre-positioning for future needs), rather than one-off intrusions to satisfy short-term intelligence requirements.[63] The use of compromised telecommunication networks as means to pivot into networks with valuable data sets, including US lawful intercept authorisation systems and one state's Army National Guard network, is a notable distinction from Russian activities.[64,65]

- Reporting on the high profile compromise of the US telecommunications sector which began in September 2024 continued into 2025, culminating in an international advisory highlighting the global extent of the Salt Typhoon-like threat globally in August.[66] Further disclosures identified new telecommunications and Internet Service Providers (TSPs and ISPs) compromises in the USA, as well as the UK, South Africa and Canada, and across mainland Europe.[67,68,69] A Chinese data leak in July 2025 indicated the group was tasked by Chinese Intelligence agencies with targets across Asia and Europe.[70] This extreme exposure, combined with sanctions against their supporting real-world infrastructure, provides one explanation for the lack of identified reporting of new activity since July.[71]

- Reported persistent compromise of telecommunication networks was not limited to Salt Typhoon. Other APT groups were attributed to the compromise of email-exchanges used by Belgian intelligence services between 2021 and 2023, a 4-year compromise of a major Asian telecommunications company discovered during an unrelated investigation, and a 10-month campaign targeting interconnected mobile roaming networks across multiple countries in south-west Asia. [72,73,74]

- Highlighting Chinese breadth and depth in exploiting vulnerabilities in telecommunications networks, Violet Typhoon – a threat actor also known as APT31 which is well known for political espionage targeting policy and influence groups – was observed using vulnerability scanning to secure access in target organisations.[75]

For Iran and North Korea, espionage outside of their regional rivalries and adverse relations with the USA is less commonly reported and inferred to be more closely tied to entities involved in developing control measures against their nuclear and military programmes, including sanctions. An Iranian data leak related to Charming Kitten, also known as APT35, indicates that cyber capabilities utilised for domestic repression extend out to global espionage.[76]

- For example, social engineering attempts resulting in the compromise of the MEP chairing the European Parliament's delegation for Iran was reported following social engineering attempts.[77] The attack was publicly attributed to APT42, the same group alleged to have hacked and leaked President Trump's election campaign communications in 2024.
- North Korean cyberespionage threat actor Kimsuky, also tracked as APT43, was reported to have conducted spear-phishing attacks on individuals working in international affairs in Europe, the USA, and Asia.[78]

Defenders assessing their organisation as a potentially high value target for espionage are advised to avoid overly tailoring their defences to published TTPs of established cyberespionage actors, particularly in the areas of initial access.

The prevalence of info stealers, accessibility of compromised credentials, and widespread data theft for extortion provides nation-states with the opportunity to buy access/data indirectly from opportunistic threat actors or data/initial access brokers. For espionage, the use of TTPs associated with opportunistic and/or financially motivated cyberattacks provides additional cover, or even plausible deniability for espionage activities.

Destructive Attacks

2025 provided multiple examples of the potential impact on national interests capable of being achieved through destructive cyber-attacks:

- The Jaguar Land Rover (JLR) attack, which was assessed by the UK's Cyber Monitoring Centre as 'the most economically damaging cyber event to hit the UK', caused a 29% fall in British motor vehicle production in September.[79]
- Outages with Google, AWS, and Microsoft Azure caused significant disruption over the year.[80]
- In September, a cyber-attack on the software supporting check-in and boarding processes disrupted airport activity in London, Berlin, and Brussels.

Whilst none of these high-profile incidents have been attributed to a state-sponsored threat actor or APT group, European leaders have increasingly raised awareness of hybrid-campaigns and other destructive attacks with links to foreign powers, often Russian.[81]

- In Poland, the current level of sabotage attempts on critical infrastructure – between 20-50 attempts per day– was cited as justification for a 60% increase in cyber security budget to €1 billion.[82]
- Officials described the compromise of an Italian passenger ship with malware supporting remote system control whilst docked in France, as the action of "an organized group" "serving the interests of a foreign power".[83,84]
- The EU's cyber reserve was deployed for the first time in support of Moldova after alleged Russia-linked threat actors targeted the Central Election Commission a few days before national elections.[85]
- Particularly in the period around the 12-day war between Israel, the USA, and Iran, the risk of disruptive cyber-attacks by Iran was publicised. The UK's NCSC assessed the risk as 'highly likely [to extend] to the UK'.[86]

Whilst more typical 'hacktivist' activity falls outside the scope of this report, a cyber-attack which took control of a Norwegian dam, including opening a flood gate, was attributed by Norwegian authorities to pro-Russian hackers and described as a hybrid attack.[87] The trend of pro-Russian hacktivists moving away from denial of service attacks towards targeting of control systems in critical infrastructure was so reliable that Forescout successfully deployed a fake water treatment network as a honeypot trap.[88]

Although high impact destructive cyber-attacks by Russia in the Ukraine war failed to be sustained, military conflicts during 2025 provide examples of how cyber-capabilities are used in active conflict: described broadly as 'projecting power' rather than delivering military gains.[89] These observations are suggestive of the challenges of delivering these sorts of cyber-operations during an active war, and by inference the importance of pre-positioning.

- GRU-linked threat actors (including Sandworm and its subclusters) have consistently targeted Ukrainian critical infrastructure by sending malicious PDFs from fake potential customers of ICT suppliers (domestic and international).[90] Wiper malware was repeatedly deployed by Sandworm; targeting a university, government sectors, and critical infrastructure such as energy, logistics providers, and agricultural exports.[91]
- Ukrainian hackers and their supporters continue to claim destructive attacks against Russian targets, including repeat and large-scale deletions of content from national court systems, grounding Russia's national airline, designing custom malware to disable sensors used by Moscow's utilities, and damaging the IT infrastructure of a large Russian drone supplier.[92,93,94,95]
- During the India-Pakistan conflict between 22/04/25 and 10/05/25, destructive attacks were predominantly low-impact denial of service and defacement campaigns, with reported APT activity limited to espionage.[96]
- During the 12-day war between Israel and the USA, and Iran in June, expansive attacks were made on the Iranian financial sector and cryptocurrency exchange (including theft of $81.7 million in digital assets).[97] Iranian offensive attacks were more superficial in nature; suggesting limited capacity to re-deploy internal resources to react at pace with impact. Hacktivist activity surged; involving almost 100 groups claiming involvement, the majority pursuing anti-Israeli activities, including DDoS, defacement and hack-and-leak activities.[98] Media reporting found Israel had hacked the phones of the body guards of key individuals to guide the targeting of missile strikes during the war.[99]

Data Theft

Whilst data theft and espionage have the common goal of data exfiltration, the strategic goals of some nation-state actors may not always have the same requirements for long-term, undetected persistence. Proprietary information can be directly used to make progress in advanced or military technology or expand commercial opportunities in particular sectors. Alternatively, information commonly found on enterprise networks may be stolen in support of future attacks, i.e. digital or physical reconnaissance, or social engineering attack lures.

China's rapid technological advances are partly credited to long-term intellectual property theft using their cyber capabilities.[100] Acknowledging the continued threat, Dutch officials explicitly warned of Chinese attempts to acquire their semiconductor technology IP, and Japan report consistent targeting of their advanced technology.[101,102]

- Multiple reports in 2025 reported activities of Chinese APTs targeting supply chain software, professional services providers such as Business Process Outsourcers (BPO), in advanced technology fields.[103]

- Analysts studying the targeting patterns and behaviours of threat actors inferred these activities supported access to vendors in sectors which China seeks to dominate, potentially supporting the development and exploitation of zero-day vulnerabilities.

- Opportunistic attacks such as the Microsoft SharePoint zero-day were exploited by Linen Typhoon to selectively compromise research institutions and the advanced technology manufacturing sector commercially prioritised by China.[104]

Consistent with their goal to develop an effective (nuclear) military deterrent, Iranian threat actors reportedly delivered their own version of the 'Dream Job' campaign (see below) in Israel, the Middle East, and in European countries, including Denmark, Sweden, and Portugal.[105,106] Organisations in satellite and aerospace manufacturing were targeted. With common goals, North Korea's Lazarus group were attributed to preparations to conduct spear-phishing attacks on the aerospace and defence sector.[107]

Financial Gain

North Korea remains the primary nation-state consistently using advanced APT capabilities for financial gain. Chain Analysis estimates North Korea have stolen at least $6.75 billion in cryptocurrency, including $2.02 billion in 2025 alone.[108] This included $1.5 billion from the February attack on Bybit cryptocurrency exchange.[109]

North Korea supports their campaigns through extensive reconnaissance work, supported by two main forms of data theft campaigns. In fake IT worker campaigns, North Korean assets pose as legitimate remote workers to infiltrate target organisations.[110] In 'Operation DreamJob', North Korean assets pose as recruitment professionals and use malicious content to deliver malware to professionals working in the target sectors. Both operations have received extensive coverage in the media and threat intelligence community, with some notable developments being observed.

- Coinciding with reporting that North Korea may seek to develop the capability to manufacture drones to mitigate against Russian supply gaps, North Korea's Lazarus group was attributed to an "Operation DreamJob" campaign targeting individuals working within the European unmanned aerial vehicle (UAV) sector.[111,112]

- In August 2025, Operation DreamJob tactics were observed targeting an Asian subsidiary of a major European manufacturer. In this attack, a project engineer was socially engineered to download and open a malicious file in WhatsApp Web.[113]

Like North Korea, Russia and Iran have significant economic pressures and strategic goals requiring high levels of resources. Cybercrime provides an opportunity to monetise internal APT capabilities. For example, Iranian threat actors facilitate cybercrime as initial access brokers.[114] In Russia, the state is considered less likely to dedicate internal capabilities to cybercrime, instead potentially leveraging 'conditional safe haven' influence on cybercrime and potentially taking a cut/fee for protection.[115]

Now What

The trend for greater public attribution by national leaders is inferred to be both building public awareness of adverse nation-state activity and also prioritising disruption by exposure over covert monitoring of detected activities. A consequence of this policy shift towards exposure is that it sets the conditions for attackers to invest in their capabilities to rapidly adapt and change the techniques, infrastructure, and behaviours which defenders used to detect and disrupt attack attempts and persistence. Greater development of specialist skill sets, more routine collaboration (including with organisations operating as private sector companies), rapid weaponisation of vulnerabilities, and experimentation with AI are already evident and anticipated to expand. For example:

- Chinese threat actor group UNC5174, is understood as a specialist in credential compromise, serving as an IAB for Chinese APT activity.[116] Sophisticated network structures such as Flax Typhoon's botnet and the continued compromise of (vulnerable) routers and other devices to create ORB networks, enable operations to be launched from outside Chinese infrastructure and may assist with broader detection avoidance across campaigns.[117,118] In multiple instances, the supporting threat actor has been attributed to a physical Chinese technology company.[119] In October 2025, Trend Micro proposed a sophisticated model of coordinated access sharing across threat actor groups once persistence has been achieved.[120]

- 2025 saw suspected North Korean, Iranian, Russian[121] and Pakistani[122] espionage campaigns observed utilising, and adapting, the 'ClickFix' social engineering technique initially used by financially motivated IABs.

- Rapid adaptation to TTP exposure was also seen in Russian APT Coldriver, a group known to target high-profile military and intelligence professionals in NATO countries, as well as influential figures in thinktanks, journalism or NGOs – in this case, the operationalisation of new malware families within 5 days.[123,124]

- Whilst received with scepticism and challenge from some parts of the cyber-security sector, in November 2025, Anthropic reported the first known observation of threat actors using agentic AI capabilities to execute global attacks on approximately 30 organisations; specifically, a Chinese espionage campaign.[125,126]

- Silk Typhoon's targeting of IT networks and cloud-based software demonstrated the opportunities available from rapid exploitation of zero-days.[127,128,129] Multiple Chinese APTs made use of the same SharePoint zero-day vulnerability.[130]

Equally, as public attribution becomes more common, the value of non-public threat intelligence has increased. This may explain attempts reported in June 2025 to compromise the cyber security vendor SentinelLABS.[131] Separately, North Korea applied their Contagious Interview campaign to compromise cyber intelligence platforms and monitor understanding of their infrastructure.[132] Finally, the breach of US cyber security company F5 in August 2025 involving theft of undisclosed vulnerabilities and source code suggests a similar motivation.[133]

Collaboration between nations with existing advanced capabilities and the proliferation of commercial cyber intrusion capabilities (CCICs) also risks complicating the threat landscape. Adversary nations such as North Korea, Russia, and Iran continue to announce commitments for greater collaboration, including in cyberspace; the potential for knowledge transfer is concerning from both a capability and attribution perspective.[134,135]

Away from the traditional high capability adversary nations of Russia, China, Iran, and North Korea, an increasing lack of confidence in international norms and previously well-established alliances, combined with the availability of CCICs risks less traditionally monitored adversaries attempting to conduct cyberespionage in new areas. For example, in July, an Indian-APT was attributed to a spearphishing campaign targeting foreign policy officials in southern Europe.[136,137,138]

2025 underscored how cyber operations have become an integral instrument of statecraft, with nation-states exploiting geopolitical flashpoints to justify, conceal, or amplify APT activity. Given ongoing global instability, this pattern is likely to continue in 2026, as states look to align their cyber operations with diplomatic, military, and economic objectives.

Section 7
Disinformation in 2025

The spreading of inaccurate or inauthentic information, widely referred to now as disinformation when intentional and misinformation when done unwittingly, is not a new phenomenon.

It has a storied history going back hundreds of years, and indeed we have written about it previously. We are examining the topic again because of how modern and evolving technology is changing and fuelling advancements in the practice. Social media and the rise of generative AI deepfakes have changed how disinformation is created and spread, as well as how it can be identified and countered.

Deepfake AI tools have been growing increasingly common and effective. The number of deepfake tools available on the dark web doubled between Q1 2023 and Q1 2024. They come in a range of prices, from a few dollars to multiple tens of thousands, and are consequently capable of a range of features.[139]

One of the reasons that deepfake AI content is so effective at spreading disinformation is that it blurs the line between reality and fabricated information; what actually is, and what we each want things to be. People's inherent biases are easier to manipulate when there is seemingly endless evidence proving all their suspicions and theories were right all along, and the rise of algorithmic social media helps spread disinformation at speeds propagandists and trolls of the past could only dream of.[140]

Whilst there is evidence that disinformation can influence people's beliefs, it is currently inconclusive just how effective it can be. This ambiguity has not stopped entities from engaging in the spread of disinformation, to the extent that in January 2024 the World Economic Forum (WEF) labelled disinformation as the biggest short-term risk around the world. This is particularly due to its potential to impact democratic elections and promote societal unrest.[141]

Big Business

Disinformation is spread not only by those looking to interfere in the political process of their own, and other nations, but also by those seeking a profit.

The spreading of disinformation has become a lucrative business, especially when it concerns such emotive topics as politics and elections. Going back to 2022, the 40 US-based websites which were found to be most responsible for spreading election disinformation generated over $40 million in advertising revenue.[142]

A Russian-funded disinformation network was found to be interfering with Moldova's recent Parliamentary elections in September 2025. The group offered to pay individuals to post pro-Kremlin propaganda on social media and used ChatGPT for advice on how to improve engagement through the use of, for example, satire. A Russian-linked platform was identified as interfering in the same election. This platform, known as Restmedia, published Kremlin talking points and was discovered to have paid engagement farms in Africa to amplify pro-Russian narratives via verified social media pages in an "amplification-for-hire" scheme.[143,144]

Disinformation, particularly through the use of AI deepfakes, exploded in 2025. Deepfake-as-a-Service (DaaS) emerged onto the scene and became one of the fastest growing tools for the entrepreneurial cybercriminal. These tools offer ready to use AI tools to clone voices and videos as well as generate images and simulate personas. They are not only used in disinformation, but also in more traditional cybercriminal attacks. AI-powered deepfakes were found to be involved in over 30% of corporate impersonation attacks in 2025, whilst deepfake-driven fraud resulted in more than $200 million in financial losses in just the first quarter of 2025.[145,146]

Deepfake Disinformation in Global Elections

Ireland

Only a handful of days before the October 2025 Irish Presidential election, a generative AI deepfake video swept Irish social media in an apparent attempt to impact the outcome of the election.

The deepfake video was comprised of two segments. The first impersonated the voice and appearance of RTÉ, the national Irish broadcaster, News presenter Sharon Ní Bheoláin announcing that presidential candidate, Catherine Connolly, had announced her withdrawal from the presidential race, whilst at a campaign event.

This section was followed by one which impersonated RTÉ Political Correspondent Paul Cunningham introducing the video which impersonated presidential candidate, and eventual election winner, Catherine Connolly, appearing to say, "It is with great regret that I announce the withdrawal of my candidacy and the ending of my campaign". This second segment additionally stated that the election had been outright cancelled, as only one candidate was left in the race and so there was no need for voters to go to the polls on election day.[147]

These videos were hosted on Meta's Facebook, Google's YouTube, and Elon Musk's X platforms for at least a day before being taken down after official complaints by Catherine Connolly's campaign team, to both the social media platforms themselves, as well as the Electoral Commission.[148]

Other deepfake disinformation videos attempting to influence the cause and course of democracy, likewise, impersonated known RTÉ personalities and were shared thousands of times across social media in the run-up to the election.

Speaking on the slew of disinformation in the run up to the election, emeritus professor of computing at Dublin City University (DCU) and member of the government's AI Advisory Council Alan Smeaton, stated "social media platforms have a lot to answer for."[149]

The Philippines

The Philippines hosted a range of elections in 2025 from the senatorial to municipal level. These elections were an opportunity for approximately 70 million voters to have their voices heard and be represented in nearly 20,000 representative seats. It was also an opportunity for bad actors to spread disinformation in an attempt to influence these elections. Topics which were particularly susceptible to deepfakes include territorial disputes in the South China Sea, as well as specific political candidates.[150]

A network of inauthentic accounts on X, formerly Twitter, with apparent Chinese origins were discovered to be behind the spreading of disinformation and fuelling discord amongst Filipinos. This network was particularly active in response to criticism of the Duterte family. Additionally, posts focused on the dispute surrounding the West Philippine Sea, criticising officials within the Philippine Coast Guard, and spread debunked accusations against sitting President Ferdinand Marcos Jr.[151]

It is not only foreign-linked networks which spread disinformation. It is also a domestic issue, with politicians spreading AI-powered disinformation to promote themselves. Senator Ronald Dela Rosa, allied to the Duterte family, shared an AI-generated video to his official Facebook page in June. The video showed a young man criticising the "selective justice" levied at Sara Duterte and was viewed nearly ten million times before it was taken down. Sara Duterte, the sitting Vice President at the time of the video's release, stated in response that there was "no problem sharing an AI video supporting me as long as it's not for profit."[152]

Rest of the World

German voters were subjected to disinformation campaigns in an effort to affect the federal elections in February 2025. As part of what has now been linked to a known Russian disinformation campaign known as Storm-1516, deepfake videos of alleged witnesses to corruption, and whistleblowers, were created to spread disinformation about various prominent politicians. This included claims that an already-elected parliamentarian was actually a Russian spy. This was an obvious attempt to sully the representative's credibility and authenticity as a candidate.[153]

In another example of Russian-linked disinformation campaigns, Australia's May 2025 federal elections also received attempts at interference. What made this campaign notable, however, was that the disinformation wasn't directed at human users for the most part. Rather, it was designed to seed thousands of misleading articles which promoted pro-Kremlin talking points and propaganda to attract search engine crawlers used to build AI chatbots.

This was in an attempt to distort the data which the tools draw on to give responses and influence them to provide pro-Kremlin narratives. A test of 300 prompts of popular chatbots showed that nearly 17% of chatbots' answers amplified the false narratives. Despite seeming like only a small percentage, it shows significant levels of success for only moderate investment into a cheap technique.[154]

What to expect in 2026

Moving forward into 2026, we can expect to see AI deepfakes used more and more, both in traditional cybercriminal activities such as social engineering and vishing in pursuit of illicit profit, and in attempts to interfere with democracy. Elections are being held in dozens of countries this year, with a combined electorate of over 1.5 billion voters. This is ripe ground for malicious parties to attempt to influence general, local, presidential, and parliamentary elections around the globe.

Elections of note which may garner extra threat actor attention and experience more deepfake disinformation include Bangladesh's general elections in February, the nation's first national vote since student-led protests ousted Sheikh Hasina and ended her 15-year rule. Hungary will hold parliamentary elections in April, and observers should be alert to the presence of disinformation in the run-up to the election. Hungary has become a potential flashpoint in Europe, with incumbent Prime Minister Orban being a vocal supporter of Russia and Putin, and a frequent challenge to pro-Ukrainian factions within European politics.[155,156]

Amongst the most sensitive and potentially impactful elections, Israel's parliamentary elections currently scheduled for October, and the US midterm elections in November. Both of these have the potential to significantly impact events on a global scale and so are likely to be the subject of substantial disinformation campaigns.

Conscientious observers should also be on the lookout for AI-powered disinformation used domestically in political matters outside of the scope of elections. This could originate from political actors themselves who have no qualms about either using, or benefiting from, AI-powered disinformation which furthers their cause.

Additionally, it could originate from third parties and be seized upon by enough of the populace to cause confusion and muddy the waters over what exactly happened. This can be seen in the recent instance of the ICE shooting of Renee Good in Minneapolis.

An AI-altered image, generated by xAI's chatbot Grok, spread widely on social media. Though it did not appear to substantively alter the events witnessed and recorded by many, it does muddy the waters on the details of what actually happened.[157]

As AI tools and deepfakes become more advanced, and cheaper and easier to use, it will become harder to successfully identify what content has been altered. Some tips to help in identifying altered content include:[158]

- Does the content provoke an emotional response? If so, how sensationalist or biased in the presentation?

- Has the content spread virally on unregulated or loosely moderated platforms such as Reddit, X, or Facebook?

- Adopt a "don't trust, verify" approach when dealing with content. Even the most well-meaning of our networks may themselves be duped by inauthentic content and so should be treated with caution.

- Use fact-checking websites to verify the claims made in suspect content.

Section 8
Proactive Cyber Defence Through HITS-Based Threat Hunting

In today's volatile cyber landscape, shaped by geopolitical tensions, economic uncertainty, and increasingly sophisticated adversaries, organisations cannot rely solely on reactive measures.

A proactive approach is essential to reduce dwell time, uncover hidden threats, and strengthen resilience and posturing. This is where Threat Hunting becomes a cornerstone of modern cyber security.

What is Threat Hunting?

Threat hunting is the proactive pursuit of adversary behaviours and undetected threats within an environment before they escalate into full-scale incidents. Unlike traditional detection, which waits for alerts and detections to be generated, threat hunting actively seeks to identify detection-gaps, attacker behaviours, and tactics, techniques, and procedures (TTPs) that are being missed.

It combines research, hypothesis-driven analysis, and collaboration to uncover these stealthy threats that evade automated and legacy controls.

Our Approach: The HITS Framework

NCC Group's threat hunting capability is powered by our proprietary HITS Framework.

Developed by our Senior Global Threat Hunting Manager, Joshua Mountney, this structured methodology delivers consistency, scalability, and measurable outcomes through an iterative process across four operational phases:

- **Targeting, Preparation & Intelligence Gathering** – Align hunts with emerging threats, client context, and intelligence insights to formulate hypotheses based on attacker behaviours and environmental factors.
- **Execution & Analysis** – Deploy advanced query logic across telemetry sources to identify anomalies and validate hypotheses.
- **Consolidation** – Aggregate and analyse results globally for depth and accuracy.
- **Collaboration** – Share actionable findings with the wider ecosystem, feeding insights into TI, Detection Engineering, Incident Response, and Vulnerability Management Teams.

This phased approach ensures depth, rigour, and repeatability – maximising the value of every hunt.

Collaboration at the Core

Threat hunting does not operate in isolation. Our hunters work hand-in-hand with Threat Intelligence, SOC, DFIR, and Offensive Security teams alike.

Intelligence informs hypothesis creation, while hunt outcomes enrich the intelligence lifecycle, creating a virtuous cycle of continuous improvement and iteration.

This synergy ensures hunts are informed by the latest adversary tradecraft and that findings translate into stronger detection engineering and strategic defence.

Supporting the Threat Intelligence Lifecycle

Hunting activities contribute to multiple stages of the TI lifecycle:

- **Direction & Collection** – Intelligence feeds and campaign reports shape hunt priorities.
- **Processing & Analysis** – Hunt findings validate or challenge assumptions, providing real-world evidence.
- **Dissemination & Feedback** – Outputs such as detection logic and telemetry gap analysis strengthen future reporting and client advisories.

This bidirectional flow ensures intelligence evolves continuously through operational insights from live environments.

Annual Overview: Threat Hunting in 2025

In 2025, NCC Group's dedicated HITS-based Threat Hunting capability delivered:

- 18 distinct hunt campaigns focused on separate threat actors and groups.
- 70+ targeted, hypothesis-led hunts across global clients and verticals.
- Numerous validated findings, new analytics, and tuned detections.
- Evidenced validation of network defences, improving assurance and auditability.

These achievements were realised through close collaboration with Threat Intelligence, SOC, IR, and Detection Engineering teams, reinforcing our integrated defence model.

How HITS Delivered Measurable Value

- **Structured cadence and scale** – Monthly HITS phases ensured consistency and depth.
- **Tangible security posture enhancements** – Hunts surfaced control gaps and visibility deficits.
- **Evidence-led assurance** – Findings provided defensible proof of control effectiveness.
- **Integrated intelligence lifecycle** – Hypotheses informed by TI; outputs strengthened advisories and watchlists.

Case Studies:

Success in Proactive Identification and Action

ScatteredSpider –
Anticipating Retail Sector Attacks

Months before UK retail attacks occurred, our team executed a proactive hunt campaign targeting ScatteredSpider's tradecraft, including MFA fatigue and SIM-swapping techniques. Outcomes included:

- Early risk mitigation for retail clients.
- Enhanced detection engineering for identity abuse indicators.
- Strategic intelligence contribution to NCC Group's TI lifecycle.

Unexpected Discoveries – Identifying Missed Threats

A targeted hunt for Lazarus Group behaviours uncovered an unrelated phishing campaign that had evaded Microsoft's native detections. Impact:

- Immediate containment for affected customers.
- New indicators and behavioural artefacts fed into TI workflows.
- Proof that proactive hunting uncovers threats beyond its original scope.

Protecting Organisational Integrity – Insider Threat

Through iterative telemetry analysis, we identified insider-driven reputational risk. Collaborative response enabled swift interdiction and reinforced acceptable use policies, showcasing hunting's role in mitigating internal threats.

Driving Strategic Value

Threat hunting delivers more than detection – it strengthens resilience by:

- Enhancing visibility and telemetry coverage.
- Improving detection engineering and triage playbooks.
- Providing contextual risk insights and operational maturity.

In short, HITS-based hunting transforms intelligence into action, enabling organisations to anticipate, detect, and respond to threats with confidence.

Looking Ahead

As the adversaries evolve, so too will our resolve.

In 2026, NCC Group will continue to expand our HITS-based hunting capability, deepening integration with the TI ecosystem, and delivering proactive defensive solutions for our customers at scale.

Section 9
The Impact of Generative AI on the Cyber Threat Landscape

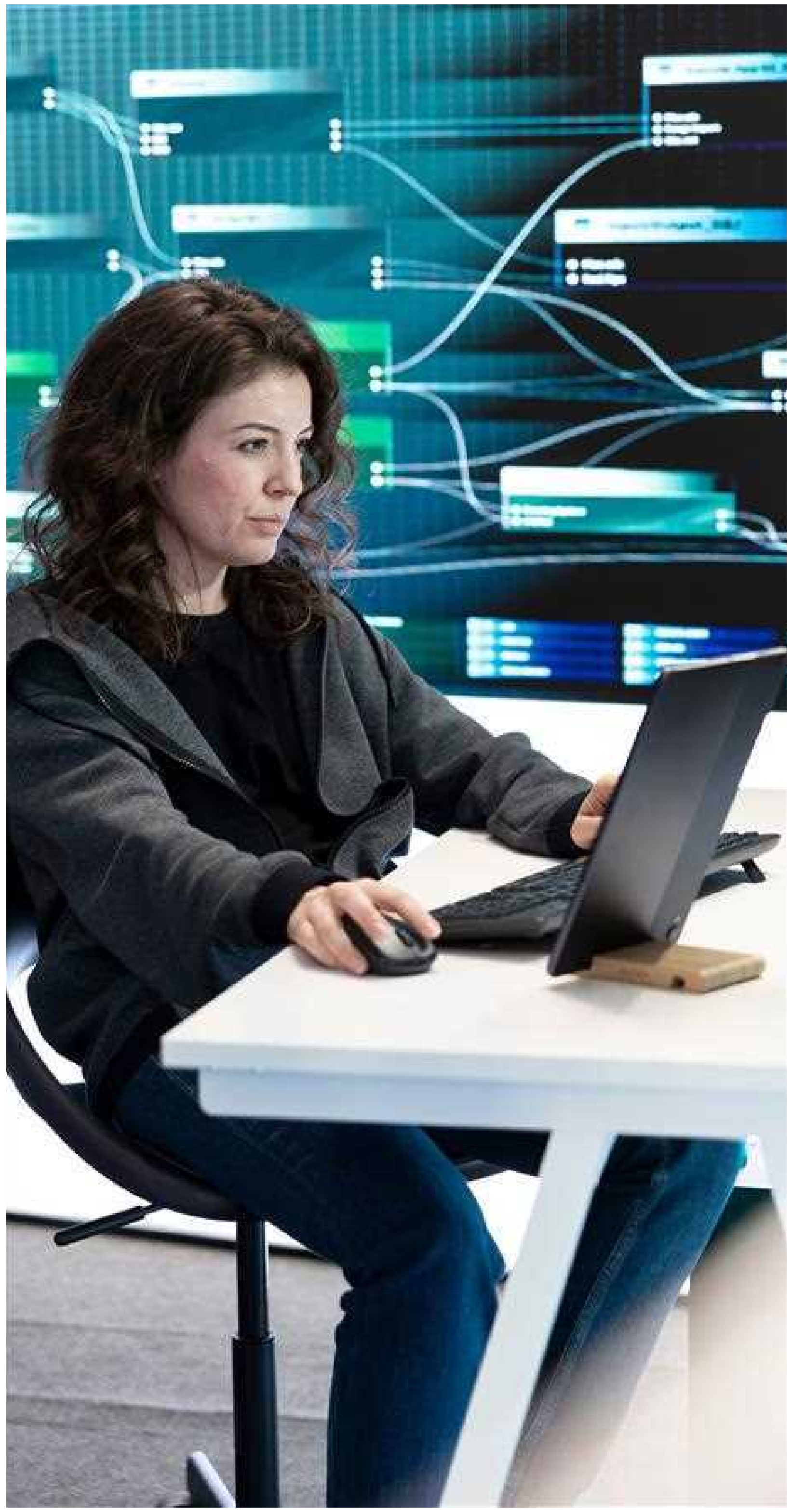
Since its emergence in late 2022, generative AI continues to evolve with the introduction of new workflows, expanding its applications across different business operations. This is particularly the case in 2025, often characterised as 'the year of AI agents', where AI technology has begun to move beyond text generation towards executing real-world tasks.[159] According to McKinsey's 2025 State of AI survey, 88% of organisations are reported to use AI for at least one business function.[160] Global spending on generative AI reflects this trend, increasing from $11.5B in 2024 to an estimated $37B, making it the fastest-growing software category in history.[161] However, the widespread adoption of generative AI has not translated into a clear understanding of its impact on the cyber security landscape, as rapid development continues to outpace understanding of its implications.

This section of the annual report provides a snapshot of how AI has influenced, and is likely to influence, the threat landscape. AI is currently assessed as an amplifying force, increasing the scale and speed of existing threats and capabilities, rather than as a paradigm-shifting development. The primary risk associated with AI lies in its widespread and poorly secured integrations, which expands the attack surface and introduces new vectors for exploitation.

A healthy AI adoption would require risk-aware practitioners and robust governance frameworks to ensure the delivery of productivity gains without jeopardising security. Notably, AI-associated risks extend beyond cyber security to include broader societal impacts such as algorithmic bias, economic disruption, over-reliance, privacy, and misinformation. These considerations are outside the scope of this section, which focuses on direct cyber security risks that dominated the AI security discussion in 2025.

Expanding Attack Surface

The wide and rapid adoption of AI has expanded the attack surface, introducing AI-specific exploitation vectors. Multiple components of the AI lifecycle present new opportunities for adversaries, from model development to integration into user-facing applications. Alongside traditional technical and social attack vectors, generative AI introduces a synthetic cognitive attack surface, providing a new angle for exploitation through prompt injection.



AI systems can be deceived in ways that do not affect humans. This technique allows attackers to embed malicious instructions within input data, causing the system to override its original guardrails.[162] OWASP continues to rank prompt injection as the top Large Language Model (LLM) risk (LLM01:2025), indicating that defensive measures are currently insufficient.[163]

By using specially crafted prompts, threat actors can bypass security, access sensitive data, and alter responses. Studies show 56% of tested models are susceptible, with advanced attack techniques targeting sectors like healthcare and finance.[164] In fact, the UK's National Cyber Security Centre (NCSC) has recently warned that prompt injection may never be totally mitigated.[165] Prompt injection has often been compared to SQL injection; however, unlike SQL injection, which can be mitigated through deterministic controls, LLM systems lack a formal separation between instructions and data and are therefore inherently confusable. To mitigate the risk, organisations should focus on impact reduction through strict privilege separation, architectural isolation, input and output validation, and continuous red teaming.

The risk of prompt injection is amplified by the emergence of AI browsers, such as ChatGPT Atlas and Perplexity's Comet, which integrate agentic AI capabilities into web browsers.[166] This integration promises productivity gains by facilitating information gathering, form completion, and task execution.

To do this, AI browsers operate with a degree of autonomy and may be granted access to authenticated sessions and user data. A third-party survey reported that 28% of surveyed enterprises had at least one employee who downloaded ChatGPT Atlas shortly after its launch, indicating the risk is not theoretical.[167] In addition to privacy concerns, AI agents with access to browsing sessions and the ability to ingest arbitrary content introduce multiple attack paths. Unlike traditional automation, agentic AI workflows execute actions and access resources, making them prime targets for a new class of identity-based attacks.

Traditional security controls remain insufficient in this context, as filtering cannot reliably differentiate between malicious and legitimate instructions embedded in natural language. As a result, mitigations such as intent-based security are being proposed.[168] These approaches focus on evaluating the intended actions of an AI agent and enforcing policy at the action level. Security researchers continue to address the risks arising from AI's non-deterministic nature through various solutions. One such example is the development of NOVA rules, an open-source framework for detecting and analysing malicious prompt activity. NOVA defines rules, similar to YARA, using keyword and LLM-based matching to identify prompt injection and jailbreaking attempts.[169]

Prompt injection is not the only AI use case that creates novel security risks. Vibe coding, defined as the use of natural language to generate code, is an increasingly prevalent practice. The Stack Overflow 2025 Developer Survey reported that 84% of developers use AI tools, compared to 76% in 2024.[170] Reporting describes this practice as a potential 'security crisis' driven by 'synthetic vulnerabilities'.[171] A large-scale study of AI-generated code samples shows that AI produces insecure patterns and hallucinates abstractions that are undetectable by static application testing tools.[172] These findings point to a systemic risk rather than isolated implementation issues.

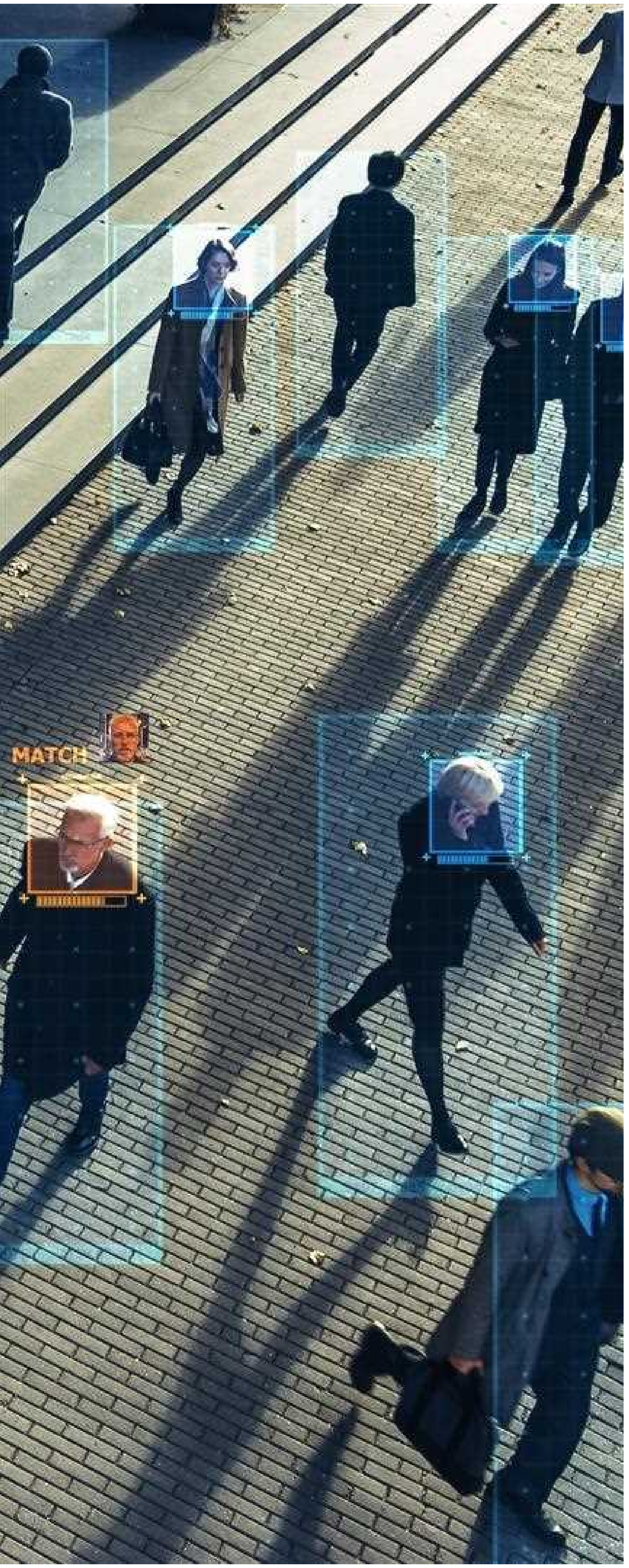
Beyond direct model interaction, AI supply-chain risk has emerged as another major security concern. AI systems depend on a complex ecosystem of dependencies, including training data and supporting libraries. Many of these components are implicitly trusted and distributed through open repositories, increasing exposure to data poisoning and backdooring. Supply-chain compromise affects system integrity at a more granular level, shifting trust upstream and limiting the effectiveness of security controls. Researchers have already identified malicious AI models, hosted on Hugging Face, evading detection by exploiting Pickle, a Python serialisation module.[173]

The emergence and growing adoption of the Model Context Protocol (MCP) has broadened the AI supply-chain risk by introducing runtime dependencies on external tools. MCP is the proposed new standard for connecting LLMs with external resources.[174] A recent study analysed more than 8,000 MCP servers, indicating an ecosystem marked by uneven maintenance and extensive use of security-sensitive APIs.[175]

While these findings do not confirm active exploitation or exposure, they point to a rapidly growing dependency layer whose compromise could have a systemic impact. By enabling extensibility at runtime, MCP shifts trust from static to dynamically consumed third-party components. Compromise at this layer would allow adversaries to influence model behaviour without altering the underlying model, increasing the likelihood of difficult-to-detect manipulation.

Despite the aforementioned risks, banning AI use is not a viable control measure, as it increases exposure to shadow AI, where employees rely on unapproved AI tools. In 2025, a Gartner survey reported that 69% of organisations had suspected or confirmed employee use of prohibited AI tools.[176]

This introduces unmanaged risks, including data leakage and regulatory non-compliance. Sensitive business information may be submitted to AI services outside approved environments, which reduces visibility and auditability.



Organisations should therefore prioritise governed adoption and the improvement of AI literacy among their employees. AI-related risks are not confined to a single component; they arise from how systems are built, integrated, used, and governed, requiring a holistic approach across the AI lifecycle.

At NCC Group we support clients in strengthening their cyber security posture across AI-enabled environments. This includes intelligence-led red teaming and penetration testing to evaluate the resilience of generative AI components against real-world threats, with a focus on data integrity, model reliability, and resistance to adversarial attacks. Our holistic approach provides assessments of generative AI pipelines, policies, and processes through application code reviews, DevOps security assessments, and tailored consulting.

AI-Enabled Threat Activity

Over the past year, multiple threat intelligence reports have discussed the adversarial misuse of AI. Of note is a November 2025 report from Google's Threat Analysis Group documenting the first known malware families to use AI during execution: PROMPTFLUX and PROMPTSTEAL.[177] These malware families have been reportedly observed calling an LLM to modify their code at runtime. While this step signals a progression towards more autonomous malware, the report characterised the use of LLMs as experimental rather than a mature capability. Some researchers challenged the report, arguing that most so-called AI-driven malware was low-quality and did not meaningfully alter the threat landscape.[178,179]

Other reporting has examined threat actors' use of AI to automate attacks. A widely cited Anthropic report published in November 2025 assessed with high confidence that a China-nexus group, tracked as GTG-1002, misused Claude Code to support espionage operations against 30 entities.[180]

Anthropic stated that the threat actor used Claude's agentic capabilities to automate multiple stages of the kill chain, including reconnaissance, discovery, exploitation, lateral movement, and data exfiltration. As with Google's report, Anthropic's findings were met with some scepticism, with critics citing exaggerated claims and limited technical evidence.[181]

To date, most observed AI-enabled threat activity aligns with Levels 1 to 3 of the AI Malware Maturity Model (AIM3).[182] AI primarily functions as a force multiplier for existing capabilities rather than a source of a novel capability beyond established tradecraft. That said, the absence of fully mature autonomous weapons does not suggest that AI-enabled threat activity is completely unfounded.

Current evidence indicates that AI lowers technical barriers and enhances attackers' effectiveness. Public discourse on AI threats has at times been polarised, limiting nuanced assessment. Hyped reporting, reinforced by vendor marketing and media amplification, often presents incremental developments as disruptive milestones. This framing often undermines our understanding by blurring the line between actual capability and theoretical possibility.

Early-stage adversarial experimentation with AI is expected to be uneven and low-quality. This, however, does not diminish the potential risk of AI weaponisation by threat actors.

AI and Cyber Defence

In response to the growing demands posed by AI threats, cyber defenders have also experimented with AI to increase their efficiency. A 2025 benchmark study by the Cloud Security Alliance found that AI-assisted SOC investigations were completed 45–61% faster and with 22–29% higher accuracy than manual analysis.[183] IBM's 2025 Cost of a Data Breach Report also shows that security teams integrating generative AI into their workflow reduced the overall breach lifecycle by approximately 80 days.[184]

Generative AI has been integrated into a range of cyber security services. Security Copilot, for example, supports SOC analysts with threat hunting and incident response activities. According to Microsoft, users of Security Copilot achieved a 30% reduction in mean time to resolution (MTTR).[185]

The use of AI in defensive operations shows potential but remains early in its maturity. Many SOC solutions claim transformative capabilities through AI assistance, yet these claims have to be validated in operational environments.[186] Gartner places AI SOC agents in the early stages of its development with low market adoption and unproven benefits, recommending cautious pilot testing before broader deployment.[187] AI-assisted red teaming has also demonstrated measurable effectiveness in 2025. A Stanford-led trial found that an AI agent identified valid vulnerabilities more efficiently than nine of ten human testers.[188]

The study notes that AI agents perform well in parallel tasks and cost efficiency, but lag in contextual judgement, GUI interaction, exploit chaining, and prioritisation. AI agents in offensive security are assessed as augmentative rather than substitutive for human expertise.

These results align with the broader understanding that generative AI systems rely on probabilistic sequence prediction of LLMs rather than genuine creativity or intent.

This architecture constrains generative AI systems' ability to apply contextual awareness and intuitive judgement in complex real-world tasks.

Due to this design, an asymmetry exists between offensive and defensive applications of generative AI in cyber security. AI currently favours attackers, who can iterate through trial and error at minimal cost. Defenders, by contrast, rely on high-confidence detection, where even limited false negatives can result in compromise.

Final Thoughts

As of late 2025, evidence suggests that AI is incrementally changing, rather than fundamentally transforming, the cyber threat landscape. Generative AI primarily functions as an accelerator and amplifier of existing threats and capabilities. Unless a new breakthrough occurs in AI technology itself, the scenario of a superintelligent AI that completely alters the security landscape remains unlikely.

Generative AI introduces new risks through its deployment and integration, which expand the attack surface. These risks primarily stem from AI workflows that can access systems and execute tasks while remaining vulnerable to weaknesses, some of which currently lack effective mitigation. Addressing this challenge requires robust governance frameworks and proactive defensive approaches.

Although AI has been criticised by some researchers for overpromising and underdelivering, dismissing its impact at this stage would be unwarranted. The technology is here to stay, and AI agents have already been observed exploiting legacy systems, with capability improvement expected over time. As these agents increasingly operate autonomously, non-human identities (NHI) are increasingly likely to become a primary attack surface going forward. IBM assesses that AI will dominate the threat landscape in 2026, potentially requiring organisations to redesign identity, accountability, and cryptography to match the machine speed of AI agents.[189]

For cyber professionals, AI is highly likely to become essential for managing the growing threat complexity and operational volume without eliminating the need for humans. Cyber security practitioners are therefore required to invest in AI fluency to understand the technology's capabilities and limitations, and to learn when human judgement is warranted.

Section 10
Vulnerability Threat Landscape

The exploitation of vulnerabilities remains a primary initial access vector for both financially motivated and nation-state threat actors.

The 2025 Verizon Data Breach Investigations Report found that 20% of breaches resulted from vulnerability exploitation, ranking second to identity abuse as an initial access vector.[190]

This section examines statistical trends and targeting patterns to assess the evolution of the vulnerability threat landscape in 2025. Notable observations include a year-on-year increase in volume, a growing share of weaponised Common Vulnerabilities and Exposures (CVEs), and a declining timeframe between disclosure and real-world exploitation.

Rapid patching and proactive, risk-based vulnerability management practices are therefore critical to reducing organisational risk.

Statistical and Exploitation Trends in 2025

The 2025 figures demonstrate a continued upward trend in vulnerability disclosures, with 48,448 CVEs disclosed, compared to 40,287 in 2024, representing a 20% increase.[191]

In previous annual reports, NCC Group predicted that vulnerability disclosures are likely to continue increasing year-on-year, driven by expanded attack surfaces, wider adoption of bug bounty programmes, advances in agentic AI, and maturing disclosure processes.[192]

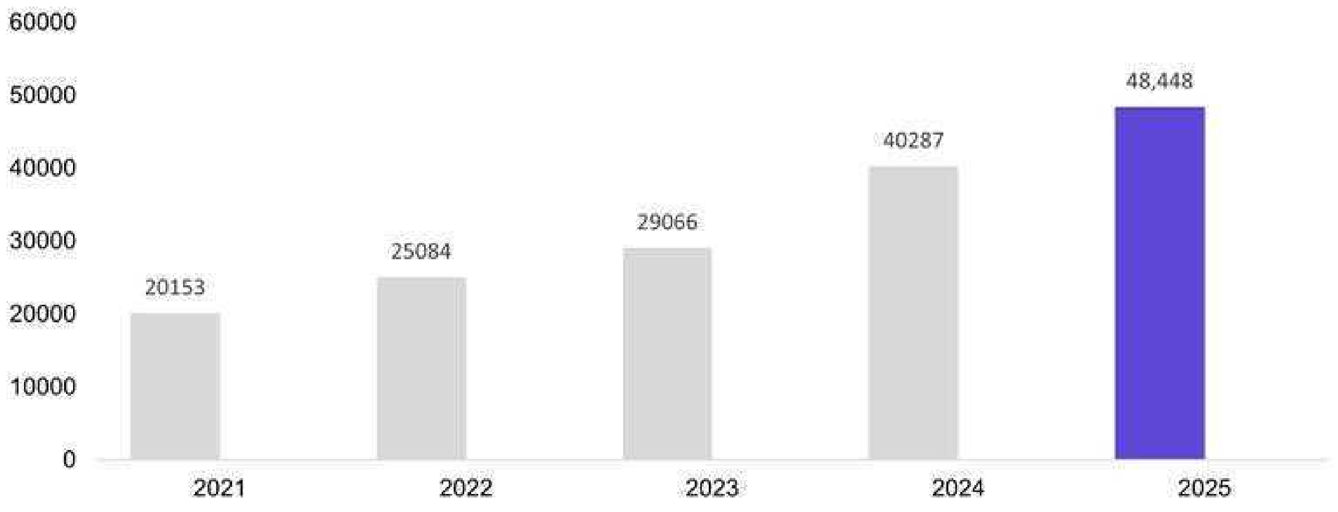


Figure 10: Vulnerability disclosure by year 2021-2025

The increase in the proportion of exploited vulnerabilities was even more pronounced over the past year. CISA added 245 vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue in 2025, compared to 186 in 2024, representing an increase of 32%.[193] CISA's figures are generally considered conservative, as inclusion in the catalogue requires strict criteria.

Other assessments indicate that the number of exploited vulnerabilities exceeds those recorded in the KEV catalogue. According to VulnCheck, 432 vulnerabilities were weaponised in the first half of 2025 alone.[194] Although this remains a small proportion of total disclosures, weaponised vulnerabilities pose a disproportionately high risk to organisations.

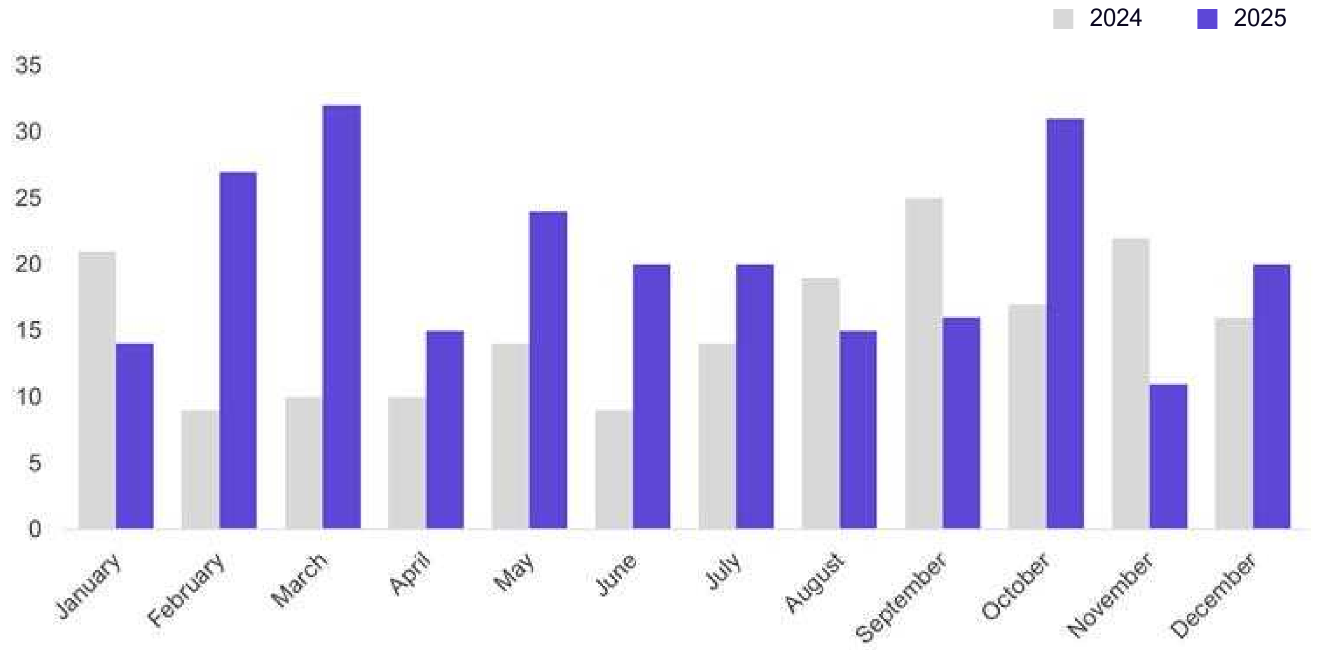


Figure 11: Distribution of Exploited Vulnerabilities by Month (2024-2025) from CISA's KEV Catalogue

The speed at which new vulnerabilities are weaponised has emerged as one of the defining trends in 2025. The average Time-to-Exploit (TTE), defined as the average time it takes threat actors to exploit a vulnerability before or after a patch is available, has fallen substantially. Reporting indicates that TTE declined from five days in 2024 to approximately one day, and to only a few hours in some cases.[195,196]

Threat actors are increasingly capable of rapidly weaponising disclosed vulnerabilities, a trend likely accelerated by AI-driven automation.[197] The use of AI to assist in identifying exploitable conditions and generate proof-of-concept code has shortened the window between disclosure and exploitation.

As a result, not only advanced threat actors but also less technically capable adversaries are able to exploit high-value vulnerabilities at pace. Ongoing advances in AI are likely to further compress this window and lower the technical barrier for threat actors.

Another trend observed in 2025 is increased targeting of perimeter systems, including firewalls and VPNs. Internet-facing applications remain attractive as they open portals into internal networks. Zero-day exploitation of edge devices increased by 19 percentage points compared to the previous year.[198] Data from the first half of 2025 shows that edge and gateway devices accounted for 17% of observed exploitation, matching the share of Microsoft products.[199] Meanwhile, remediation efforts are modest, with 54% of known edge device vulnerabilities remaining unpatched, leaving organisations exposed to ongoing risk.

Despite the increasing volume and speed of exploitation, MITRE's 2025 Top 25 Common Weakness Enumeration (CWE) list highlights the prevalence of long-standing issues such as cross-site scripting (XSS) and SQL injection.[200] The continued high rank of input validation and object handling flaws indicates enduring failure in engineering practices. Addressing these systemic issues requires a cultural shift towards embracing secure-by-design principles.

Widely Exploited CVEs in 2025

Defining and quantifying mass exploitation of vulnerabilities remains a challenging task due to uneven reporting and inconsistencies across vendors and data sources. To capture exploitation trends, this subsection outlines examples of low-effort, high-impact vulnerabilities reportedly exploited at scale in 2025, affecting organisations across multiple sectors and geographies. The list prioritises vulnerabilities that impacted widely deployed technologies and were weaponised by state-nexus threat actors and/or ransomware groups. Examples include:

Ivanti Connect Secure VPN
In January 2025, a critical zero-day, CVE-2025-0282, was disclosed, affecting Ivanti Connect Secure, Ivanti Policy Secure, and Ivanti Neurons for ZTA gateways.[201] This stack-based buffer overflow flaw affects code designed to handle IF-T connections. Successful exploitation allows an unauthenticated, remote attacker the ability to achieve remote code execution and malware deployment.[202]

Exploitation of this vulnerability has been linked to a confirmed intrusion affecting the UK internet domain registry, Nominet.[203] Mandiant also reported that several unnamed organisations were targeted, attributing the activity to UNC5221, and Microsoft to Silk Typhoon, both of which are assessed to be China-nexus threat actors.[204,205] Although there is insufficient evidence to conclusively determine whether these activities were conducted by the same group, overlapping targeting patterns suggest they are likely part of the same threat cluster. This vulnerability demonstrates how flaws in VPN appliances can enable full system compromise, increasing risk for organisations that rely on these systems.

SAP NetWeaver
In April 2025, SAP disclosed a critical vulnerability affecting NetWeaver Visual Composer, tracked as CVE-2025-31324.[206] The flaw allows unauthenticated attackers to upload arbitrary files and achieve remote code execution, resulting in full system compromise. Exploitation is performed by simply sending crafted HTTP requests to the /developmentserver/metadatauploader endpoint. Following disclosure, the vulnerability was rapidly weaponised by multiple threat actors, including ransomware and state-linked threat actors.

A blog post published by ReliaQuest in April 2025 reported exploitation of CVE-2025-31324 in threat activity linked to the BianLian and RansomEXX operations.[207] In May 2025, EclecticIQ reported exploitation of CVE-2025-31324 by China-nexus threat actors targeting critical infrastructure organisations in the United Kingdom, the United States, and Saudi Arabia.[208]

The prolific exploitation of this CVE demonstrates how rapidly threat actors, regardless of motivational background, respond to newly disclosed vulnerabilities. This is particularly evident for easily exploitable CVEs affecting widely deployed, internet-facing components, stressing the need for timely and proactive vulnerability management.

Microsoft SharePoint
In July 2025, Microsoft published a blog detailing the observed exploitation of CVE-2025-53770, a critical zero-day vulnerability affecting on-prem SharePoint referred to as 'ToolShell'.[209] The disclosure assessed the vulnerabilities as a bypass for previously patched vulnerabilities which were addressed during the July Patch Tuesday update.[210]

The vulnerability enables unauthenticated remote code execution through the abuse of unsafe deserialisation of untrusted objects within SharePoint servers. According to Microsoft, exploitation activity was attributed to Chinese nation-state threat actors tracked as Linen Typhoon and Violet Typhoon.[211] Microsoft has also observed exploitation by a financially motivated group tracked as Storm-2603, which is assessed with medium confidence to be a China-based threat actor, deploying Warlock and LockBit Black ransomware variants. Public reporting indicated that organisations across the automotive manufacturing, education, and government sectors were impacted.[212]

The Microsoft SharePoint vulnerability demonstrates the risk of patch circumvention in widely deployed platforms. This once again shows that easily exploitable, high-value flaws quickly attract a diverse range of threat actors, who are increasingly adept at operationalising impactful flaws.

React2Shell
In November 2025, a security researcher identified a critical-severity vulnerability in React Server Components (RSC) versions that allows remote, unauthenticated attackers to achieve code execution.[213] The flaw, tracked as CVE-2025-55182, stems from insecure deserialisation within the RSC Flight protocol, where malicious object references embedded in HTTP requests can trigger code execution on Node.js servers running RSC.[214] The vulnerability poses a significant risk due to the widespread adoption of React within modern web infrastructure. Researchers at Wiz reported that 39% of surveyed cloud environments contained at least one vulnerable instance, indicating broad exposure.[215]

The combination of low attack complexity and high impact prompted comparisons to Log4Shell; however, researchers assessed the ubiquity of affected systems to be comparatively limited. In response, major service providers, including Cloudflare, deployed emergency mitigation measures that temporarily caused widespread service disruption.[216,217,218]

This disruption highlights the existing operational trade-offs of rapid defensive action following vulnerability disclosure.

Within hours of public disclosure, active exploitation attempts were observed worldwide. Amazon Threat Intelligence attributed this activity to Chinese state-linked threat actors, including Earth Lamia and Jackpot Panda.[219] The exploitation of CVE-2025-55182 reinforces a recurring pattern observed in 2025, where threat actors act as early adopters of high-impact vulnerabilities during the narrow window between disclosure and widespread defensive mitigation.

As we move into 2026, the window between vulnerability disclosure and weaponisation is likely to shrink further. Advances in agentic AI systems are expected to accelerate discovery and exploitation, reducing the effectiveness of reactive security management. Going forward, effective security strategies should therefore prioritise resilience by design and continuous exposure management, treating the attack surface as persistently targeted asset.

Exploitation of Older CVEs

Despite increased disclosure volumes of new vulnerabilities, older CVEs remain relevant, with a growing share among weaponised vulnerabilities. In 2025, 38% of vulnerabilities added to CISA's KEV catalogue were disclosed prior to that year, a trend likely to continue and accelerate into 2026. Many organisations continue to rely on legacy systems, resulting in persistent exposure points. At the same time, automated scanning capabilities are advancing, creating sustained opportunities for threat actors to exploit these security blind spots.

Edge technologies such as VPNs, routers, and firewalls accounted for more than 50% of the resurgent vulnerabilities, reflecting their increasing value as an entry point.[220] The exploitation of CVE-2018-13379, a path traversal vulnerability affecting Fortinet FortiOS SSL VPNs is an example. A joint advisory from CISA and the FBI in February 2025 reported its exploitation by the Ghost ransomware group, alongside other resurgent vulnerabilities in public-facing applications, to gain initial access.[221]

Other notable examples of historic CVEs include CVE-2017-9841, a critical remote code execution vulnerability in the PHPUnit framework. Kinsing malware operators leveraged the vulnerability to conduct cryptojacking activity.[222] In another striking example of sustained exploitation, CISA added Internet Explorer vulnerability CVE-2010-3962 to its list, following its observed exploitation by advanced threat groups. Historical vulnerabilities demonstrate that even bugs disclosed more than a decade ago can remain operationally relevant. As threat actors are mining and repurposing older tooling, a healthy defensive strategy should include continuous exposure assessments to identify potential security blind spots and areas of disproportionate risk. NCC Group offers multiple services that help organisations strengthen their defensive posture holistically. This includes External Attack Surface Management (EASM), which maps an organisation's internet-facing assets, including forgotten assets, to eliminate blind spots.

Threat Intelligence Alert Subscription

The growing volume of vulnerabilities, reduced time to exploitation, increased weaponisation, and resurgent CVEs stress the need for a decision-making process grounded in real-world risk. By correlating disclosed vulnerabilities with observed threat activity, exposure, and business-critical assets, intelligence can help organisations prioritise remediation. This approach enables vulnerability management to function as a measurable, risk-based process that improves the efficiency of organisational risk reduction.

NCC Group provide a regular Threat Intelligence Alerting Service, which provides customers with details of emerging threats including critical vulnerabilities being actively exploited. The aim of these alerts is to furnish our customer base with intelligence to allow for situational awareness and prompt patching prioritisation and mitigation activities.

This is available as part of our NCC Group MXDR Services or by subscribing to our Threat Intelligence Services.

Section 11

Online Exposure Monitoring (OXM)

NCC Group's Online Exposure Monitoring (OXM) service is a Threat Intelligence solution which offers organisations a robust service for continuously tracking and managing their digital footprint, ensuring their online presence is both secure and compliant.

This service is designed to identify external threats as early as possible to minimise impact and provides actionable insights that empower clients to proactively identify and mitigate risks associated with unauthorised data exposure, reputation damage and compliance breaches allowing clients to stay one step ahead of threat actors.

Lockheed Martin's Cyber Kill Chain has 7 stages, OXM primarily focuses on stage 1, the reconnaissance stage. This provides organisations with early insight into attack vectors, allowing for adjustment to security before it progresses to the next stage of the attack chain.

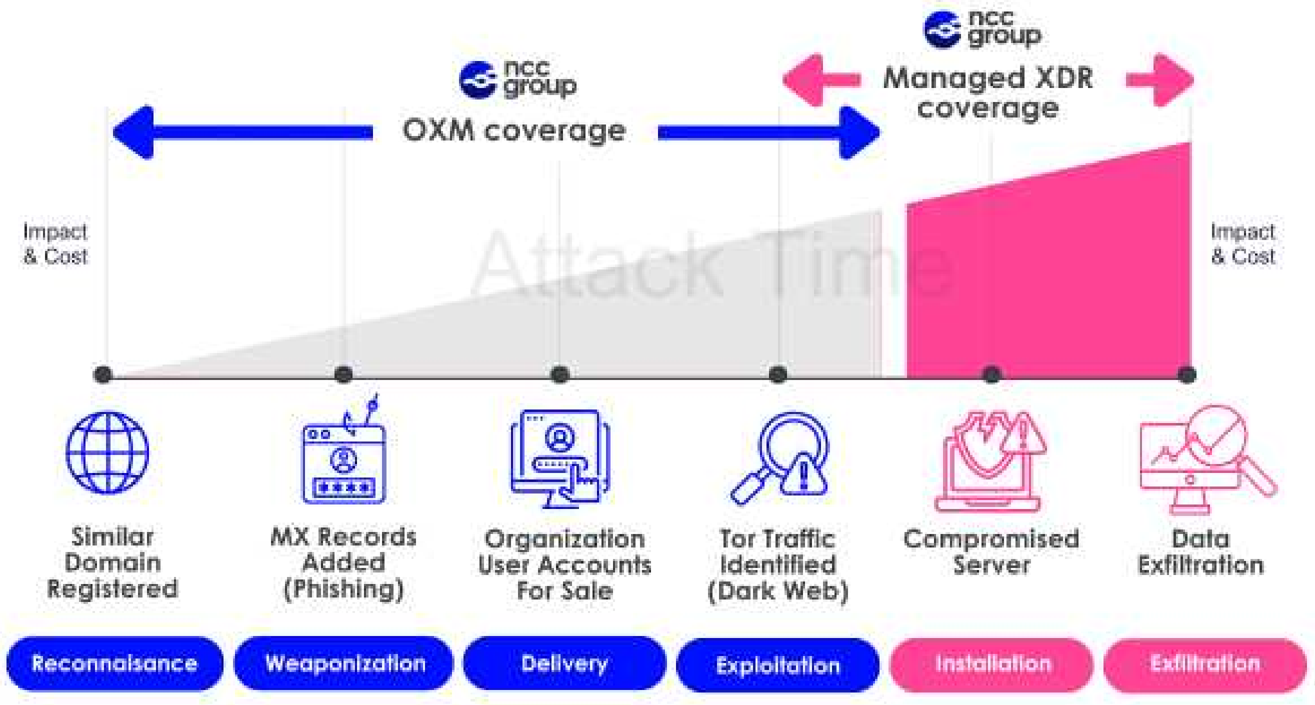


Figure 12: OXM coverage

OXM Capabilities

Ransomware Detection

- Alerting for data leak sites (DLS) for mentions of clients and data. Allowing the organisation to be proactive, responsive and act upon the threat actors' claim.

Dark Web Traffic Monitoring

- Real-time dark web traffic monitoring which stems from client networks. This provides clients with better visibility of dark web connections and prevent data exfiltration.

Credential Detection

- Alerts for client credential leaks including third parties. Exposed information includes plaintext passwords, hashed passwords or Personal Identifiable Information (PII), enabling clients to be proactive against threats before they can be weaponised.

Potential Phishing Detection

- Alerts against potential phishing domains likely to affect the client or are imitating their brand. This enables clients to take proactive measures against threats before they can be weaponised.

Exposed File Detection

- Alerting clients to the mentions of sensitive files which have been uploaded to misconfigured cloud buckets and VirusTotal. This enables clients to conduct necessary actions to prevent data loss, unauthorised access and minimise reputational damage.

GitHub Monitoring

- Alerting clients to potential credentials and classification terms mentioned in public GitHub repositories. This enables clients to conduct necessary actions to detect data loss, prevent unauthorised access and minimise reputational damage.

Network Detections

- Alerts for vulnerabilities (CVEs), expiring SSL certificates, open ports and DNS misconfigurations within the client's infrastructure. This enables the organisation to have an insight of their network security and help eliminate the early stages of an attack.

About NCC Group

“People powered, tech-enabled cyber security”

We’re a people powered, tech-enabled global cyber security and resilience company with over 2,200 colleagues around the world.

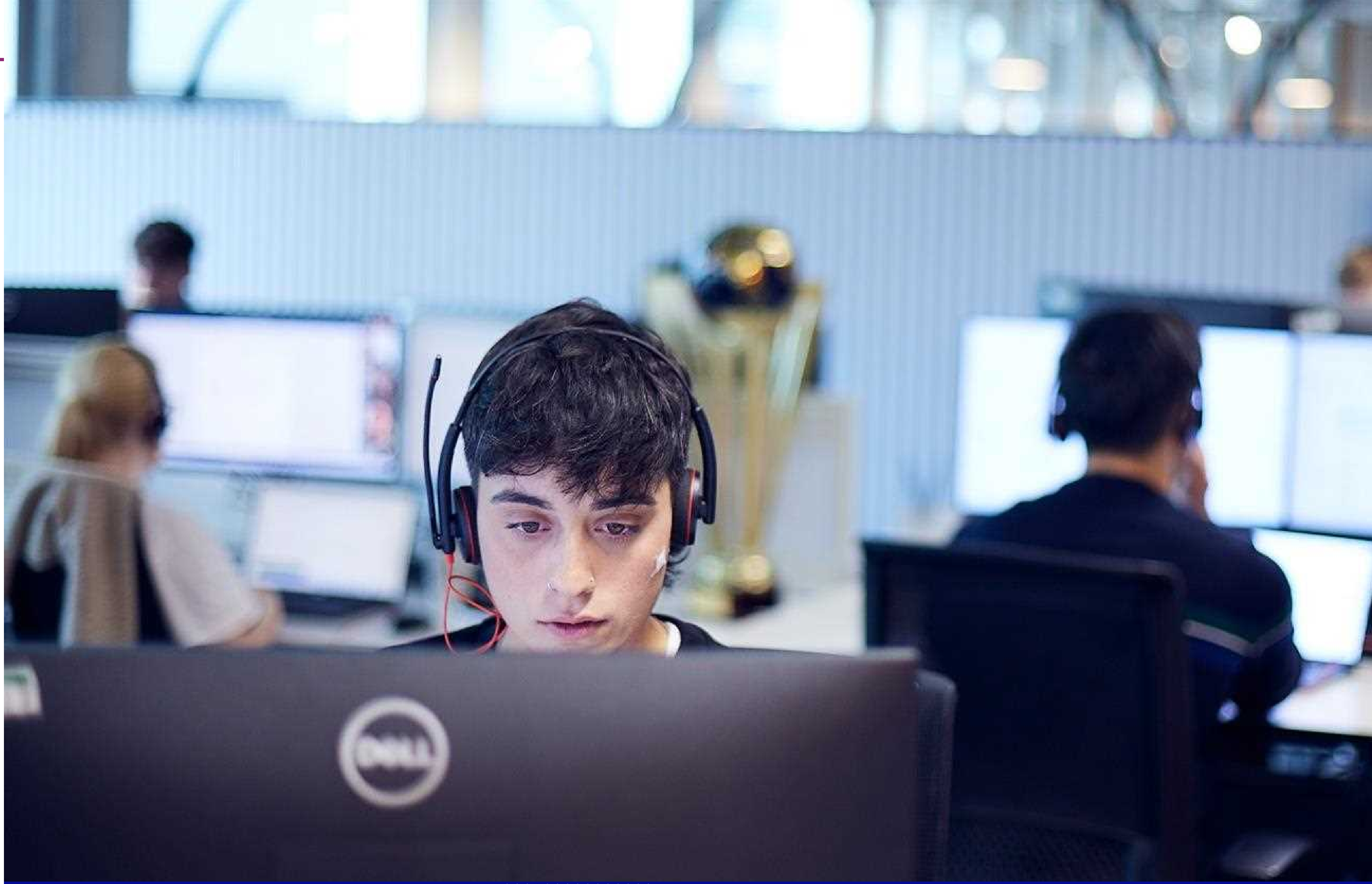
For over 25 years, we’ve been trusted by the world’s leading companies and governments to manage and deliver cyber resilience, working together to create a more secure digital future. We are proud to deliver important and groundbreaking projects for our clients.

We operate as one global business, with in-country delivery tailored to local needs and cultures, as well as a global delivery team to respond quickly to our clients’ challenges. Headquartered in the UK, we also have a significant market presence in Europe, North America and APAC.

“NCC Group’s research in areas like ML and threat intelligence shapes its resilience and offensive security, helping clients anticipate new threat tactics and techniques. Its offensive security services are staffed by deeply technological and operational teams, which offer services that combine expert human insight with tech.”

- The Forrester Wave™ Cyber Security Consulting Services in Europe, Q4 2025

+44 (0) 161 209 5200
response@nccgroup.com
www.nccgroup.com



We are here for you

Contact us today to learn more about global cyber security regulations.

UK & Europe
+44 (0) 161 209 5200

U.S. & Canada
+1 (800) 813 3523

Australia
+61 (0) 2 9552 4451

Singapore
+65 6800 0950

Fox-IT - Benelux
+31 (0)85 799 0680 (NL)
+32 2304 22 19 (BE)

Philippines
+63 2 8540 9450

Cyber attack?

Call our 24/7 Hack Hotline now.

UK & Europe
+44 331 630 0690

U.S. & Canada
(855) 684-1212

Australia
1800 975 310

Singapore
+61 2 8379 7870

Fox-IT - Benelux
0800 369 23 78 (NL)
+32 2304 22 16 (BE)
+31 (0) 88 369 23 78 (Int)

ncc group

FOX IT
part of ncc group