ncc group | FOX IT part of ncc group

Cyber Threat Intelligence Report

Review of Q1 2026

Contents

Section 1
Executive Summary

The number of ransomware victims claimed in Q1 2026 declined modestly by 3%, suggesting that ransomware activity remains resilient despite multiple law enforcement operations. While Qilin and Akira continue to be the most prolific groups, this quarter also saw the emergence of Gentlemen and NightSpire as the third and fourth most active actors, respectively. However, the lack of verified victim listings raises questions about the legitimacy of their claims, as inflated and exaggerated claims remain a common practice within the ransomware ecosystem.

Beyond the numbers, the Ransomware Spotlight for this quarter highlights Interlock ransomware's exploitation of a Cisco zero-day vulnerability 36 days prior to its public disclosure, underscoring the group's increasing maturity and adaptability to evolving organisational defence postures. Interlock has rapidly evolved from conducting social engineering-based attacks to executing complex, multi-vector intrusions. Such progression signals a broader convergence between some financially motivated cybercrime and nation-state level tradecraft, reinforcing the need for organisations to adopt a robust, defence-in-depth security strategy.

Our Emerging Cyber Security Trend discusses how the growing weaponisation and insecure deployment of AI technologies continue to be a major cyber security concern in 2026. AI is highly likely to be the most significant single element affecting change in the landscape for the coming year. As AI rapidly reshapes the threat landscape, organisations must adapt their cyber security strategies by incorporating AI governance and policies, human oversight, training and threat intelligence, while balancing security with efficiency gains through responsible AI adoption.

Geopolitical developments focus on the outbreak, and development, of the U.S.-Israel-led war against Iran. Inconsistent and non-committal messaging combined with repeatedly delayed deadlines for U.S.-issued ultimatums, continue to make it difficult to infer with confidence the conditions which would allow the conflict to be assessed as successful, and end.

Two key developments occurred at the end of the month; Yemen's Iranian-linked Houthi militia joined the war on 28 March, and 30 March Iranian state media reported that the regime's military representatives (the IRGC) had declared a list of 18 prominent U.S. companies (mostly technology giants) as legitimate regional targets from 1st April; including Cisco, Oracle, Microsoft, Apple, and Google.

A new Dark Web Intelligence Review section is introduced this quarter, covering a large-scale coordinated wave of international law enforcement disruption across cybercrime forums, phishing services, and proxy infrastructure. These operations signal a strategic shift towards targeting shared enablers of the cybercrime ecosystem, though the impact remains short-lived as threat actors often rapidly adapt and migrate, resulting in a more fragmented and harder to monitor threat landscape.

Finally, the vulnerability threat landscape in Q1 2026 is marked by rising disclosure volumes, faster time-to-exploit, and increased targeting of internet-facing edge devices, with AI further accelerating exploitation. Mitigating this risk requires organisations to adopt an intelligence-led, risk-based vulnerability management, prioritising exposure and impact over severity scores.

Section 2

Timeline of Critical Incidents Q1 2026

January

03/01/2026

‘Scattered Lapsus$ Hunters’ (SLH) claimed to have breached U.S.-based cyber security firm Resecurity, alleging access to internal data including employee details and client information. However, Resecurity clarified that the incident involved a controlled honeypot environment designed to monitor adversaries. The accessed data consisted of synthetic and fabricated records, including dummy accounts, with no connection to real systems or customers. This aligns with a broader pattern of exaggerated or unverified claims by the group. As such, statements from SLH should be treated with caution, and future claims will likely remain difficult to validate without independent evidence.

28/01/2026

Match Group, the owner of popular dating platforms including Tinder, Hinge, and OkCupid, disclosed a cyber security incident following claims by the cybercriminal group ShinyHunters. The group alleged the theft of approximately 1.7 GB of compressed data containing over 10 million user records and internal documents. According to attacker claims and threat intelligence reporting, the intrusion may have involved social engineering techniques such as voice phishing (vishing) targeting single sign-on (SSO) accounts, potentially linked to Okta environments, and access to a third-party marketing analytics platform (AppsFlyer). Match Group stated that the incident involved limited data exposure, with no evidence that passwords, financial data, or private communications were compromised. This case highlights the persistent effectiveness of social engineering in bypassing technical controls by exploiting human factors, and reinforces the need for robust identity security and user awareness.

February

15/02/2026

Advantest Corporation, a major Japanese technology company specialising in semiconductor testing equipment, detected unusual activity within its IT environment and subsequently confirmed a ransomware-related cyber security incident affecting parts of its corporate network. Preliminary findings indicate that an unauthorised third party gained access to portions of the network and deployed ransomware. At this stage, Advantest has not confirmed whether any customer or employee data was compromised, and no ransomware group has claimed responsibility.

This incident reflects a broader trend of cyberattacks targeting organisations within the semiconductor sector, which are attractive targets due to their high-value intellectual property and critical role in global supply chains. Companies supporting chip production sit at the core of modern technology ecosystems, meaning disruptions can result in significant financial, operational, and reputational damage.

March

10/03/2026

Starbucks confirmed a data breach affecting 889 employees after attackers gained access to internal HR accounts through a credential phishing campaign involving impersonated Starbucks Partner Central login pages. According to a breach notification filed with the Maine Attorney General, unauthorised access occurred between 19 January and 11 February 2026, with the company detecting suspicious activity on 6 February. The breach exposed sensitive personal and financial information, including Social Security numbers, dates of birth, and bank account details.

The timeline suggests a delay between detection and full containment of the incident. This incident highlights the continued effectiveness of credential-based attacks against enterprise identity systems, particularly where human factors and phishing susceptibility remain key vulnerabilities.

11/03/2026

Stryker, a U.S.-based medical technology company, was hit by a cyberattack that disrupted their operations. Their ordering systems went offline forcing them to switch to manual processes. Handala, a nation-state actor linked to the Iranian Ministry of Intelligence and Security (MOIS) claimed responsibility for the attack. They allegedly wiped over 200,000 systems, servers, and mobile devices and stole 50 terabytes of data.

Reportedly, the adversary compromised an administrator account and created a new Global Admin. The attack is widely assessed as geopolitically motivated, potentially linked to escalating tensions in the Middle East, and reflects a shift toward destructive cyber operations targeting critical sectors such as healthcare. It also highlights the risks associated with centralised endpoint management platforms, where compromise of privileged accounts can enable large-scale disruption across enterprise environments.

31/03/2026

A software supply chain attack was identified targeting the widely used npm package Axios, a JavaScript library commonly used to facilitate HTTP requests between frontend and backend services. The incident occurred after the npm account of an Axios maintainer was reportedly compromised, allowing attackers to publish malicious versions. Rather than modifying the core source code, the attackers introduced a hidden dependency via the package manifest.

The malicious versions were available for a limited time before being removed; however, due to Axios’s widespread use, the potential impact was significant. Reporting has linked the activity, with moderate confidence, to a suspected DPRK-affiliated threat cluster (UNC1069). This incident highlights the growing prevalence of supply chain attacks, in which attackers exploit trust in third-party dependencies and maintainers, often bypassing traditional security controls and impacting downstream environments at scale.

Section 3

Ransomware Statistics Q1 2026

3%

Global ransomware attacks decreased by 3% in Q1 of 2026

30%

Industrials accounted for 30% of ransomware attacks in Q1 of 2026

16%

Qilin was responsible for 16% of attacks in Q1 of 2026

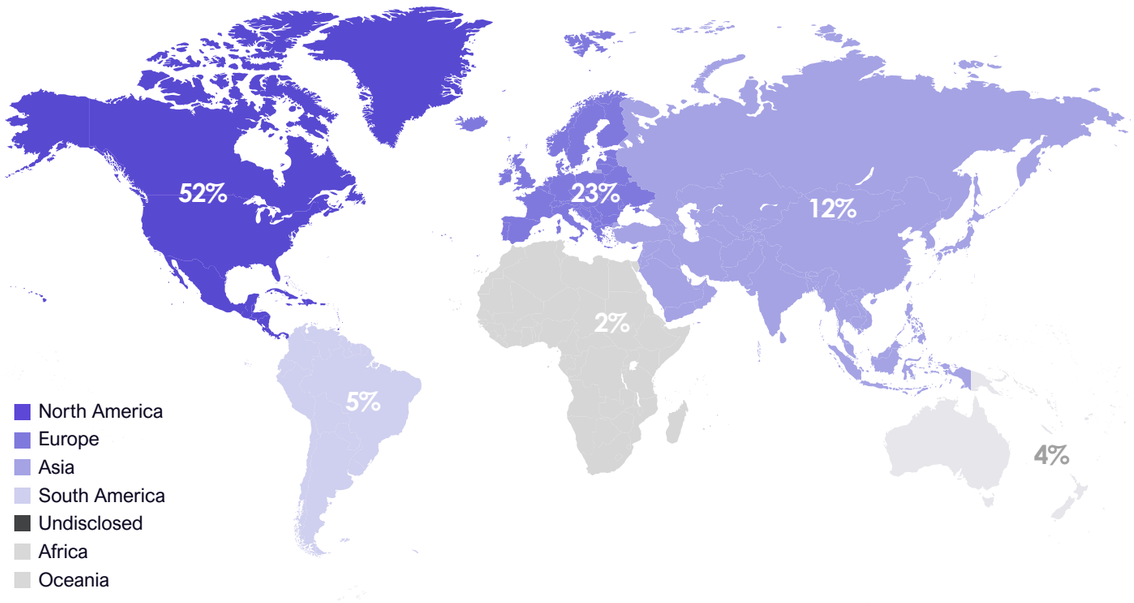


Figure 1 Ransomware Attacks by Region Q1 of 2026

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

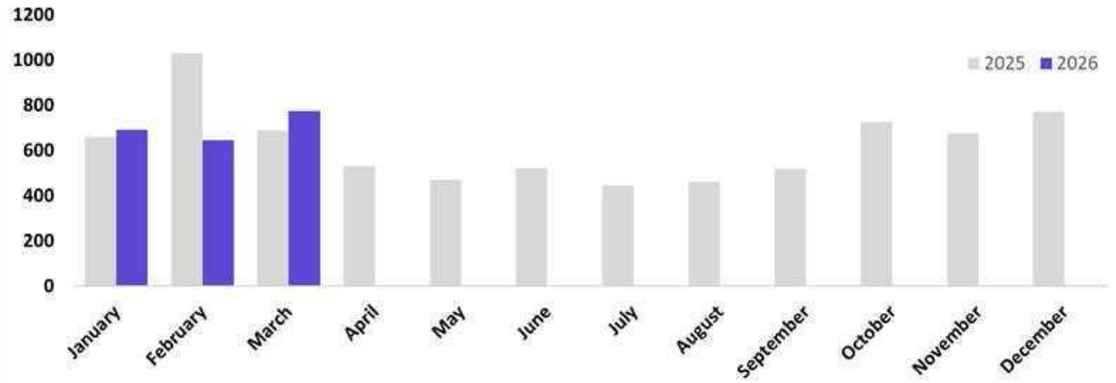


Figure 2 Ransomware Attacks by Month 2025 - 2026

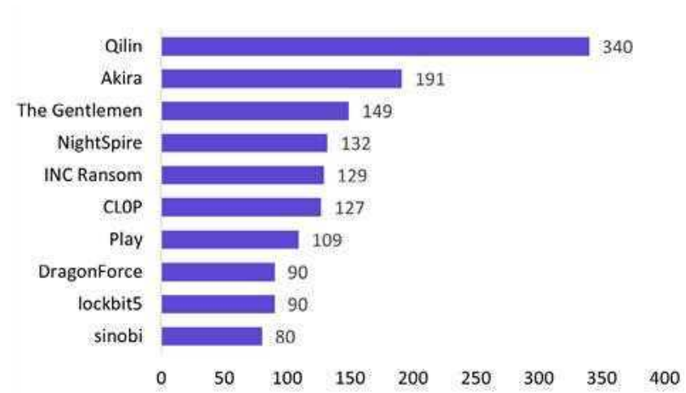


Figure 3 Top 10 Threat Actors Q1 of 2026

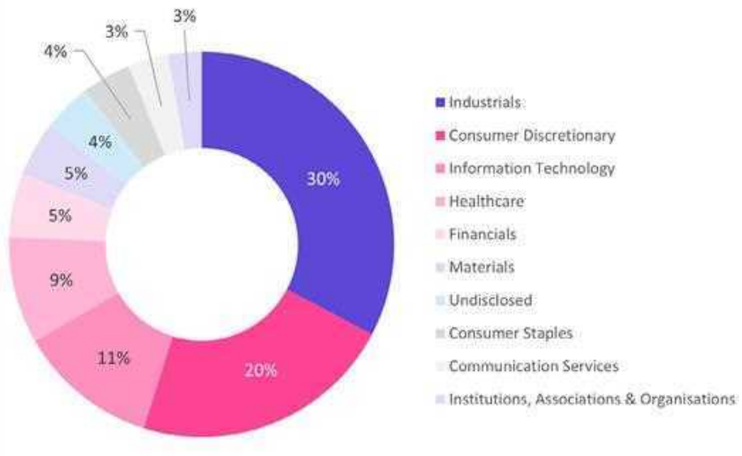


Figure 4 Top 10 Targeted Sectors Q1 of 2026

Key Events

02/01/2026
Garner Foods

Garner Foods (Texas Pete) was publicly claimed as a victim by the Play ransomware group in early January 2026. The attackers alleged they had exfiltrated internal corporate data, including employee payroll records, budgeting and financial documents, and other confidential operational files

05/02/2026
Conpet S.A.

Conpet S.A., Romania's national oil pipeline operator, suffered a Qilin-linked ransomware attack. It disrupted corporate IT systems and took its website offline but did not affect pipeline operations or SCADA systems.

02/03/2026
Getulio Vargas Foundation

Fundação Getulio Vargas (FGV), a leading Brazilian education and policy research institution, was claimed as a ransomware victim by the DragonForce group, which alleged the theft of approximately 1.52 TB of sensitive data. FGV confirmed a cyber incident and temporary system disruptions and acknowledged that related data appeared on the dark web.

Section 4

Ransomware Insights

The first quarter of 2026 saw a decrease of 3% in the total ransomware attacks (from 2175 attacks in Q4 2025 down to 2112 attacks in Q1 2026). This decline coincided with sustained pressure from government and private sector initiatives. The FBI, DOJ, and U.S. Attorney's office seized RAMP (Russian Anonymous Marketplace), one of the last major Russian-language cybercrime forums still permitting RaaS advertising, disrupting affiliate recruitment and access-broker activity.[1] In addition, the FBI also launched Operation Winter SHIELD, which focuses on strategic containment and resilience-focused controls designed to reduce real-world exploitation rather than relying on post-incident response.[2] Additionally, Europol in collaboration with international law enforcement groups disrupted 'SocksEscort', a malicious proxy which allegedly compromised over 369,000 routers and IoT devices in 163 countries, degrading the anonymity and infrastructure used by ransomware operators.[3]

These disruptions likely increased operational friction across the ransomware ecosystem, potentially constraining affiliate scalability and contributing to a short-term reduction in attack volume. Disruptions to forums, proxy services, and supporting infrastructure are likely to have raised costs, slowed affiliate onboarding, and reduced scalability for threat groups, particularly infrastructure-heavy RaaS operations.

While groups such as The Gentlemen and NightSpire rose into the top 10 rankings, Qilin and Akira remained the leading threat groups in Q1 2026. Their continued dominance likely reflects operational resilience and diversified affiliate ecosystems, suggesting that enforcement actions did not displace these groups from the top tier of the ransomware landscape. It is also worth noting that the surge in Q1 2025 was largely driven by the Cl0p ransomware group's February bulk listings of victims, which inflated ransomware figures; excluding this anomaly, baseline activity in 2026 remains higher than in the previous year, reflecting an increasingly fragmented threat landscape and a growing number of emergent ransomware groups.

The Gentlemen

The Gentlemen emerged as one of the most active ransomware groups, accounting for 149 attacks out of 2112 total attacks representing 7% of global ransomware activity in Q1 2026.

This reflects an estimated 496% increase from Q4 2025. The group mainly targeted industrials, consumer discretionary, and information technology sectors, suggesting focus on environments where operational continuity and access to sensitive data are critical to business function.[4]

However, it is worth noting that while The Gentlemen ransomware group has been confirmed by security researchers as conducting real intrusions against organisations in multiple sectors and countries, the number of its claimed victims cannot be independently verified. Some researchers have questioned the reliability of these claims, making it difficult to accurately assess the overall scale and impact of The Gentlemen's threat.[5] As such, it is plausible that, while the threat itself is credible, the scale of reported victimisation may be inflated, consistent with patterns observed across many other ransomware operations that exhibit inconsistent claim accuracy.

NightSpire

With 136 claimed attacks, NightSpire emerged as the fourth most active ransomware group in Q1 2026. Unlike The Gentlemen, whose claims remain less substantiated, NightSpire's activity has been more widely observed and, in some cases, supported by partial evidence such as data samples.[6] However, the majority of its publicly claimed victims remain unverified.

NightSpire ransomware was first identified in February 2025 and remained active throughout the year.[7] Researchers assess with high confidence that the group is likely a rebrand of the Rbfs ransomware operation, a previously low-profile threat actor, based on observed overlaps in known victims and indications of shared operators.[8] Rebranding and splintering are common within the ransomware ecosystem and continue to complicate efforts to accurately assess the prevalence and scale of ransomware activity.

Section 5

Ransomware Spotlight: Interlock's Evolving Tradecraft

On 18 March, Amazon's threat intelligence team revealed the details of an active Interlock ransomware campaign exploiting CVE-2026-20131, a critical-severity vulnerability in Cisco Secure Firewall Management Centre (FMC) with a maximum CVSS score of 10.0.[9] The vulnerability, disclosed by Cisco on 04 March 2026, allows an unauthenticated remote attacker to execute arbitrary Java code with root-level privileges. Amazon's investigation found that Interlock began exploiting this flaw on 26 January 2026, giving the group an estimated 36-day window of exposure.[10]

These findings reinforce the assessment that, despite its relatively recent emergence, Interlock has demonstrated steadily increasing operational maturity.

Interlock Ransomware: Overview and Capability Development

According to a July 2025 joint advisory by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center, Interlock was first observed in late September 2024, targeting organisations in North America and Europe.[11]

Unlike many contemporary ransomware groups, Interlock does not appear to operate a Ransomware-as-a-Service (RaaS) model, with no visible affiliate recruitment and a relatively low-volume leak-site presence compared to leading groups.[12] Interlock employs a double-extortion tactic, in which victim data is exfiltrated prior to file encryption, allowing the group to apply additional pressure by threatening data disclosure should ransom demands not be met.

The group has been observed gaining initial access through a drive-by download hosted on compromised legitimate websites or via the ClickFix social engineering technique, where victims are tricked into executing a malicious payload by clicking a fake CAPTCHA prompt. In observed ClickFix campaigns, victims are socially engineered into pasting and executing malicious PowerShell commands, which subsequently drop remote access trojans (RATs) such as Interlock RAT and NodeSnake RAT.[13] These RATs are then used to conduct reconnaissance, stage additional payloads, and deploy ransomware.

In some cases, users are misled into running malicious commands under the pretext of software updates, using familiar Windows shortcuts (for example, Win+R followed by Ctrl+V), effectively bypassing traditional perimeter-based security controls through user-assisted execution.[14] Later reporting suggested that Interlock may also have leveraged credentials obtained via initial access brokers (IABs) in certain intrusions, providing immediate privileged access and bypassing the need for privilege escalation within the target environment.

Zero-Day Exploits and Evolving Tradecraft

Zero-day exploitation remains less prevalent in ransomware operations, where threat actors continue to prioritise identity-based access, credential theft, social engineering, and the exploitation of previously known vulnerabilities.[15] However, in several cases, ransomware operators have been observed incorporating zero-day exploitation into their operations. Google's 2025 Zero-Day Exploitation Review reported the exploitation of nine zero-day vulnerabilities by likely or confirmed financially motivated threat groups, including two cases where zero-day use directly led to ransomware deployment. This figure represents a significant increase from the five observed in 2024.[16] This trend suggests an increase in the technical capability of ransomware operators and broader access to advanced exploit techniques. Given their resilience and opportunistic nature, ransomware actors are likely to continue adapting their tactics to improve their operational success.

Mitigations and Recommendations

The exploitation of zero-day vulnerabilities highlights a limitation in traditional vulnerability management. When attackers exploit flaws before public disclosure, as Interlock did in this case, even well maintained patching programs cannot fully prevent compromise. The estimated 36-day pre-disclosure window increases the likelihood that the threat actor was able to operate undetected. During this period, they may have established persistence or made environmental changes including but not limited to modifying firewall policies, creating accounts, or altering access controls to support long-term access.

Defenders should operate under the assumption that compromised systems may have been modified in ways that are not immediately visible. Security teams should closely review firewall rules, management settings, and access controls, with particular attention to any changes made since January 2026, to identify configurations that could support persistent or hidden access. Indicators of compromise should be used not only to block known activity, but also to proactively hunt for suspicious behaviour across logs, authentication records, and network traffic.

A defence in depth approach remains essential, including limiting exposure of management interfaces, enforcing network segmentation, watching for abnormal activity on critical infrastructure systems and deploying effective endpoint security solutions. Such a multi-layered approach, while often complex and resource-intensive to implement, helps protect systems during periods when some preventative controls are likely to be insufficient.

Section 6
Emerging Cyber Security Trend: Increasing Prevalence, Weaponisation, and Insecurity, of AI

Widespread Adoption and Awareness of AI

Throughout 2025, AI became increasingly prevalent in the cyber security landscape. This is a trend which has only continued, and accelerated, as we close off the first quarter of 2026. Nearly 95% of respondents to a survey about major cyber security concerns in 2026 identified AI to be the most significant single element affecting change in the landscape for the coming year. Those security professionals actively assessing the security of their AI tools has nearly doubled, from 37% in 2025 to 64% in 2026, highlighting the increasing awareness of the risks posed by this still-developing technology.[17]

As AI becomes more widely adopted, more users are becoming aware of the risks that can be simultaneously posed alongside its potential benefits. 78% of CISOs highlighted data leaks as their top concern, according to recent survey results released by Splunk. To combat this risk, many CISOs and organisations are deploying AI tools in private environments with strict training guardrails combined with firewall monitoring and tool instrumentation.

This additionally combats the use of shadow AI throughout an organisation, which itself increases the risk of data leaks. However, as AI is more commonly used to counter common threats, users are becoming more cautious of the risks posed: 90% of gen-AI users ranked shadow AI as one of their top three concerns, versus 79% of non-users, whilst 75% of gen-AI users highlighted data leakage as their number one risk, versus 71% of non-users. These trends highlight how organisations further along their journey of AI maturity may identify that some of its potential risks outweigh the potential benefits.[18] Evidence of this increasing awareness of the potential risks of AI is shown by AI security specialists being one of the most widely hiring roles in the cyber security industry for 2026.[19]

Weaponisation of AI:

Just like CISOs and cyber security professionals across industries, malicious actors are becoming increasingly aware of the potential advantages posed by adopting AI into their workflows. Threat actors of all types, from nation state-backed APTs to hacktivists to purely financially motivated Organised Crime Groups (OCGs), are rapidly adapting to the new landscape and incorporating AI into their attacks.

Generative AI is being used to create ever more convincing "deep fake" content. This is a technique used by actors of all calibres; from OCGs to APTs and all the script kiddies in between. Scammers are taking advantage of heightened geopolitical tensions to push AI generated content online. In early January 2026, a channel on YouTube published a video documenting the alleged destruction of a Ukrainian port in Mykolaiv by a Russian attack. This video appeared convincing, though the events it purported to document never actually occurred. Instead, it turned out that the channel which published it is part of a network which, collectively, has amassed nearly two million subscribers and billions of video views.[20]

In February, Google reported that nation-state actors from Iran, China, India, and Russia were all found to be utilising Google's Gemini AI tool in multiple stages of their attacks. For example, threat actors use AI to craft more convincing phishing emails, still one of the main intrusion vectors for threat actors of all backgrounds.

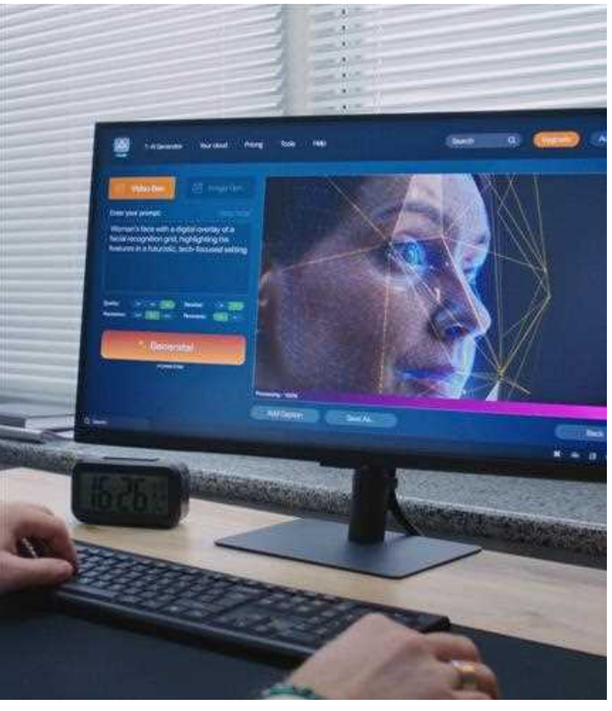
AI helps these actors both linguistically; translating whatever their message or instruction is into appropriate terminology in their target's language, and stylistically; making their lures appear like legitimate communications. Another way is through enabling reconnaissance efforts. The North Korean actor UNC2970 was observed using Gemini in way which blurs the line between typical professional research and malicious reconnaissance.

They used Gemini to conduct OSINT gathering on high-value targets, often in major cyber security and defence companies, finding information such as salary information and technical specifications for job roles. This enabled the actor to craft high-fidelity personas to use in phishing and spearphishing attacks, as well as identify targets for initial compromise.[21]

Insecurity of AI Platforms and Practices:

As AI becomes more widely adopted in legitimate industry, the more is discovered about how vulnerable it and its use cases can be. As an example, vibe coding was found to generate unsecure code in up to 45% of all use cases according to a 2025 study.[22] This over-reliance on AI, without comprehensive auditing, can lead to significant security concerns. Should the implementation of AI exceed the ability to conduct security audits and hygiene checks, we can expect to see this statistic increase in 2026 and beyond.

Recent research from AI specialists Irregular found that the three major models, ChatGPT, Claude, and Gemini, all produced highly predictable and insecure passwords. AI agents are not designed to generate truly random passwords like dedicated password managers such as 1Password and LastPass, but they are still widely used to do so. AI models that generate passwords based on patterns in their training data can produce strong-looking passwords, but these are actually predictable and therefore a significant vulnerability in organisations' defences. Combined with increased use of AI in coding projects, this presents a major problem. AI-generated passwords are already being found in live code used in apps, programmes, and websites, and hundreds of instances of these AI-generated passwords can be found on GitHub already.[23]



Final Thoughts

AI has already begun, and will continue to, shake up the threat landscape. Defenders are being forced to adapt to new threats and to shift from tried-and-true methods for defence to new ones. For instance, instead of signature-based detections, anomalous behavioural analysis is becoming more and more essential. Constant monitoring and some automated detection and response will become indispensable.[24]

What response is appropriate to meet the security challenges posed by the increased adoption of AI, and how to balance that with the potential for increased efficiency which AI can deliver, will be dependent on your organisation's profile. Is AI already a part of your operational reality, how widespread in your environment is it deployed, and what it is used for will all need to be taken into account. Additionally, relevant threat intelligence to know the threat landscape for your organisation can inform what type of AI-driven/assisted threats you may face from actors who have also begun adopting AI into their arsenals. Some measures will appear unrelated to AI and yet will still affect how it can impact your organisation. Phishing training, for instance, has always been important and will continue to be a key factor in an organisation's defences as actors use AI to hone their phishing attacks and they become more convincing. A comprehensive online exposure monitoring solution, such as OXM offered by NCC, can help stay on top of what information is publicly exposed, in turn reducing the available data for threat actors' AI to scrape as part of hostile reconnaissance.

To stay ahead of the curve, businesses will need to identify areas where AI can help their organisations as well as present a threat. For help with this journey, contact your account manager to see how NCC Group can help your organisation make the most of its AI solutions.

Section 7
Geopolitical Developments

Iran War Feature

Following the start of a U.S.-Israeli air campaign against Iran on 28 February 2026, a regional war has been sustained throughout March; entering its sixth week at the time of writing. Inconsistent and non-committal messaging combined with repeatedly delayed deadlines for U.S.-issued ultimatums, continue to make it difficult to infer with confidence the conditions which would allow the conflict to be assessed as successful, and end.[25,26,27] As additional U.S. troops arrived in the Middle East at the end of the month, President Trump suggested 'productive' diplomatic efforts to resolve the war continued, and Pakistan indicated the country was preparing to host formal talks.[28,29]

Two key developments occurred at the end of the month; Yemen's Iranian-linked Houthi militia joined the war on 28 March, and on 30 March Iranian state media reported that the regime's military representatives (the IRGC) had declared a list of 18 prominent U.S. companies (mostly technology giants) as legitimate regional targets from 01 April; including Cisco, Oracle, Microsoft, Apple, and Google.[30,31,32]

Drawing upon analysis shared with clients throughout the last month, in the following extended report, NCC analysts consider the key thematic areas of the ongoing conflict, including the use of cyber-capabilities and impact on the broader threat landscape.

Cyber War

Whilst NCC do not assess the conflict as having significantly changed the nature of cyber threats driven by geopolitical events in the Middle East, the scale and risk associated with these threats have increased; both due to participants in the war directly utilising their cyber capabilities tactically as part of the conflict, or indirectly by influencing the drivers of wider cyber activity.

A conflict supported by cyber capabilities

In the days following 28 February, multiple cyber-enabled disruptive and information operations were reported to have targeted Iranian websites, including media sources. Several popular applications were temporarily hijacked to display anti-Iranian government messages.[33]

One of the notable incidents was the targeting of the widely popular prayer application, BadeSaba, to deliver notifications urging military personnel to defect and resist.[34]

Recent reporting also reveals that Israeli intelligence had spent years hacking nearly all of Tehran's traffic cameras, using the intercepted footage for travel patterns analysis of Supreme Leader Ali Khamenei which supported the Israeli air strikes which killed him and several senior IRGC officials.[35,36]

IMPLICATIONS:

The limitations of an air campaign to effect changes in Iran perceived as desirable to the U.S. and Israel, coinciding with Iran's willingness to escalate the conflict regionally and create global harm to preserve their survival, has created a challenging geopolitical situation from which it will be difficult to create lasting stability. Lack of popular support domestically, upcoming elections in both the USA and Israel, and the risks of inadvertently empowering the new Iranian regime and hardening Iranian resolve against future interference, creates a need for the USA to engineer an opportunity for an end to the active military conflict as soon as possible.[37,38] The complexity and unique features of the current situation make it difficult to predict outcomes and implications with confidence. Some key themes are highlighted below.

- It is anticipated that the cyber threat landscape will remain relatively consistent whilst active warfare continues. As the conflict extends, nation-state linked APT activities may shift to shorter-term intelligence collection goals; as seen with Russia in relation to the war in Ukraine. In parallel, hacktivist (genuine and proxy) are expected to continue with mostly high-visibility, low-impact operations aimed at shaping perceptions rather than causing meaningful disruption. While Distributed Denial-of-Service (DDoS) attacks will likely still account for most claimed activity, the trend for proportion of data leak incidents may not yet have reached its peak.
- Reflecting observe efforts to dominate narratives around the conflict within traditional and social media, cyber-enabled influence operations are also likely to continue.[39] The scale and speed of AI-enabled content generation are saturating the information environment, increasingly outpacing fact-checking efforts. As such, the risk of perceiving manipulated content as credible continues to grow, reinforcing the need for scrutiny of conflict-related media. Exaggerated (or fabricated) hacktivist claims overlap with these information campaigns.[40]
- Beyond cybercrime activities aligned with Iranian interests, conflict creates opportunities for broader cyberactivity, including cyber-crime at scale and opportunistic network compromise. Since the 28th February, Akamai reported that 40% of malicious traffic identified was attributed to financial services, with other highly targeted sectors including e-commerce (25%), gaming (10%) and technology (10%).[41] Much of this traffic is from botnet-driven discovery, including a 70% rise in botnet reconnaissance, 65% in automated scanning, 45% in credential harvesting and a 38% increase in pre-DDoS reconnaissance. Conflict related lures are also being observed at scale; including registration of thousands of conflict-related domains supporting financially motivated threat actors.[42]

Beyond the direct impacts of the regional war, the conflict appears to be influencing broader geopolitical factors with the capability to influence the cyber threat landscape.

- President Trump repeatedly expressed frustration with the international community over widespread refusal to expand involvement in the war cumulated with new statements that he was considering leaving NATO.[43,44] Tensions from the conflict have the potential to create further divisions within NATO.[45]
- President Trump's planned visit to China on 31st March was rescheduled to 14th May, risking undermining ongoing efforts to reduce the impact of strategic rivalry between the two superpowers, including volatile trade wars.[46] China appears to be leveraging it's existing relations with Pakistan to attempt to influence a resolution to the conflict indirectly, whilst potentially also taking advantage of the current distraction from its ambitions towards Taiwan.[47,48,49]
- Whilst the war risks further reducing Russian influence in the Middle East, prolonging the war (including through cyber and intelligence support to Iran) offers potential advantages to Russian interests; including boosting the Russian economy through potential further reductions in sanctions against Russian oil and gas, increasing demand for Russian fertilisers, reduced capacity for the U.S. to exert pressure on Russia to deliver a ceasefire in Ukraine, and reduced availability of U.S. resources (including military stockpiles) to support Ukraine.[50,51]

Section 8
Dark Web Intelligence Review

In the first quarter of 2026, multiple major cybercrime platforms were disrupted due to enhanced international public-private cooperation. This shift from isolated takedowns to targeting shared cybercrime infrastructure marks a significant trend in enforcement activity. While these operations have temporarily disrupted the cybercrime landscape, the resilient and adaptive nature of cybercriminal operations allows them to rapidly reorganise, rebuild infrastructure, or migrate to alternative platforms.

On 28 January 2026, the FBI and DOJ seized RAMP (Russian Anonymous MarketPlace), one of the most popular cybercrime forums that emerged since 2021. RAMP had distinguished itself as a leading forum for ransomware recruitment, affiliate advertising, and operational coordination. The takedown was confirmed by a former administrator, 'Stallman', who stated on the XSS forum that there would be no attempt to rebuild.

In early March 2026, an international joint operation, 'Operation Leak', seized LeakBase Forum, a major cybercrime forum used to trade stolen credentials, hacking tools, and compromised data since 2021.

Despite thirteen arrests and one hundred enforcement actions across multiple countries, the forum was relaunched within days, with over 140,000 members and 33,000 threads recorded by 12 March, indicating that the impact of the operation was limited.[52] However, a subsequent shutdown announced on 13 March was later confirmed by Russian authorities, who arrested a suspected administrator later that month.[53]

Following these disruptions, users migrated to successor forums: T1erOne, a closed and vetted forum launched in February 2026, and Rehub, an open forum that had already attracted major ransomware groups. In addition to migrating forums, some actors have shifted to Telegram entirely. The trend toward closed, harder-to-infiltrate platforms is making CTI monitoring considerably more difficult.

Section 9

Vulnerability Threat Landscape

The exploitation of vulnerabilities remains a primary attack vector for both financially motivated and nation-state threat actors. Year-on-year, the increasing number of disclosed vulnerabilities and the declining time-to-exploit highlight the urgent need for a proactive, risk-based approach to vulnerability management.

Edge devices, including VPNs, firewalls, and other boundary systems, are highly likely to remain attractive targets for threat actors. These appliances are often exposed and lack comprehensive logging, serving as high-value gateways to internal networks. In several instances, exploitation attempts against edge devices were observed shortly after disclosure, with automated scanning tools enabling a rapid attacker response.

This section of the quarterly report examines key developments in the vulnerability threat landscape, focusing on trends in disclosure and exploitation during the first quarter of 2026.

Statistical Overview of Q1 2026

Figures show a continued upward trend in vulnerability disclosures year on year. 15,178 CVEs were added to the NVD this quarter, representing a 27% increase compared to Q1 2025. The NCC Group's annual threat report assesses that disclosure volumes will continue to rise, driven by several factors.

These include the expansion of the attack surface, as well as an increasing capacity for vulnerability discovery and disclosure. In addition, the use of automation and early adoption of AI are accelerating vulnerability discovery, further contributing to higher CVE volumes. Based on these factors, CVE disclosures are highly likely to continue increasing beyond 2026.

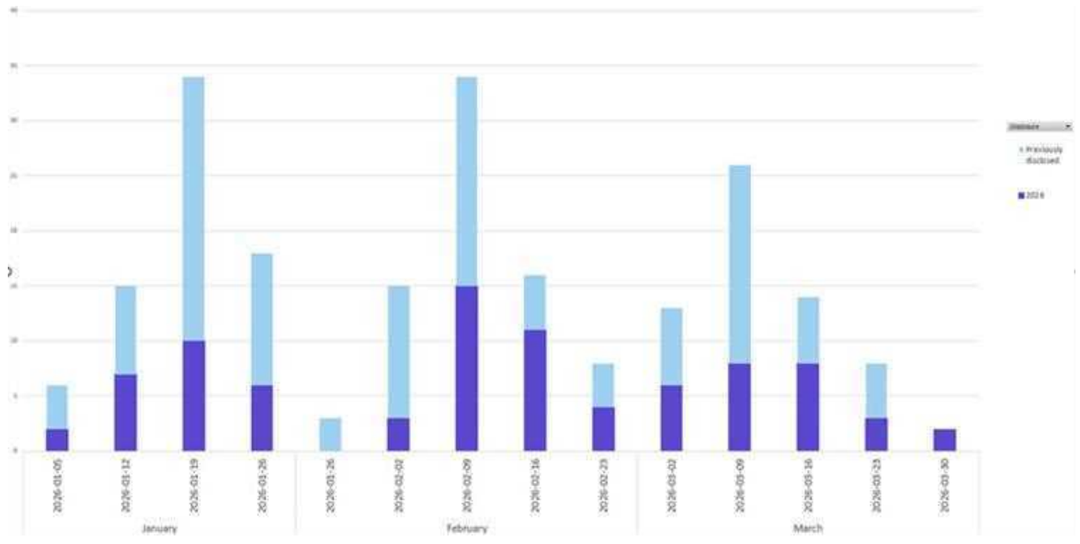


Figure 6: Timeline Distribution of Reportedly Exploited Vulnerabilities as per VulnCheck

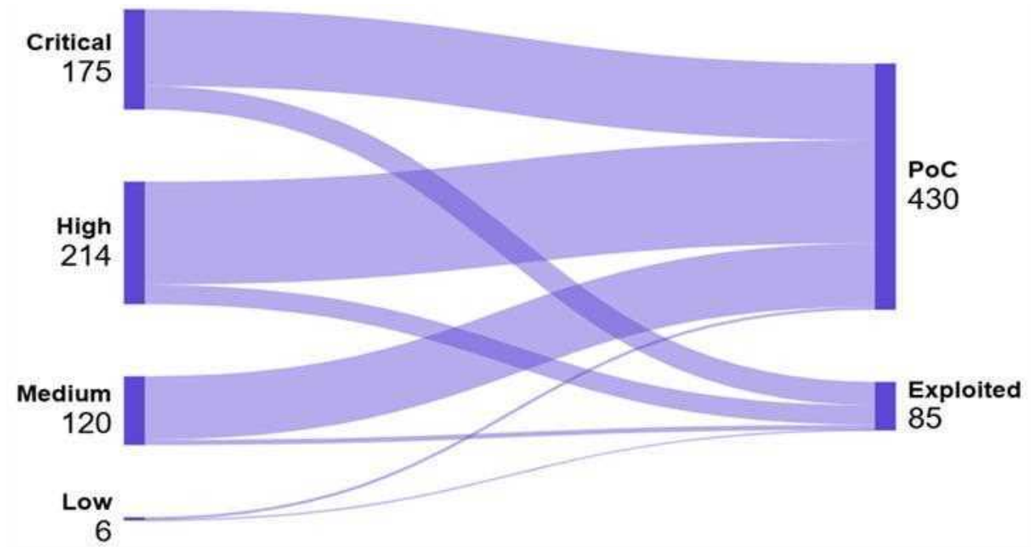


Figure 7: Available PoCs and Reported Exploitation Across CVE Severity Levels CVEs Disclosed in Q1 2026

When looking at exploited vulnerabilities, the Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities (CISA KEV) catalogue reports that 71 vulnerabilities were exploited during this reporting period.[54] However, due to strict inclusion criteria and a focus on U.S. federal agencies, this figure is unlikely to reflect the true scale of exploitation, as broader assessments indicate higher numbers.

For example, VulnCheck reported 212 exploited vulnerabilities, 85 of which were disclosed in Q1 2026.[55] Research further indicates that proofs-of-concept (PoC) are publicly available for at least 430 of these vulnerabilities. While not all PoCs provide readily usable exploit code, many contain sufficient technical detail to enable the development of exploits.

Approximately 60% of reportedly exploited vulnerabilities were disclosed prior to 2026 (Figure 6), with some dating back more than 15 years. The continued operational relevance of legacy vulnerabilities demonstrates that exploitation activity is not constrained by vulnerability age but is instead driven by exposure and persistent remediation gaps across enterprise environments.

Recommendations

The growing volume of disclosed vulnerabilities is likely to result in security gaps and patching backlogs, particularly for systems that require maintenance windows or have complex dependencies. Disclosure rates are approaching levels that exceed organisations' capacity to respond to every disclosed CVE immediately, necessitating a more targeted approach.

The increasing volume of vulnerabilities and rapid exploitation require organisations to adopt an intelligence-led prioritisation model, focusing remediation on vulnerabilities most likely to be exploited and those with the highest impact. To measure risk effectively, organisations should refrain from relying solely on CVSS levels, instead considering broader risk factors when prioritising remediation, as this metric reflects intrinsic vulnerability severity based on technical characteristics. Integrating threat intelligence into vulnerability management improves remediation efficiency and enhances risk reduction efforts. Threat intelligence enriches vulnerability assessment with organisational context and visibility of exploitation trends, enabling a more complete and actionable understanding of risk.

About NCC Group

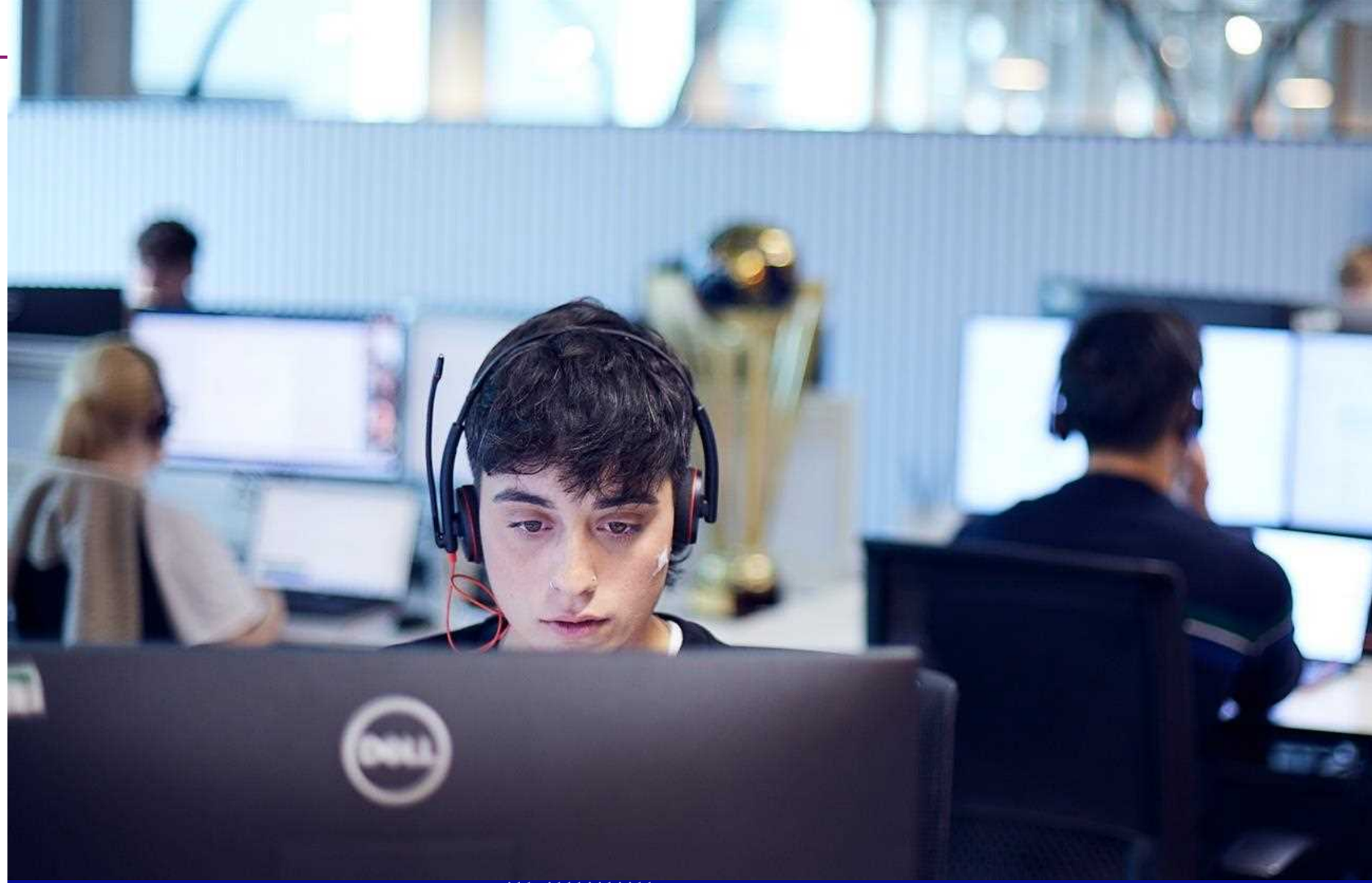
People powered, tech-enabled cyber security

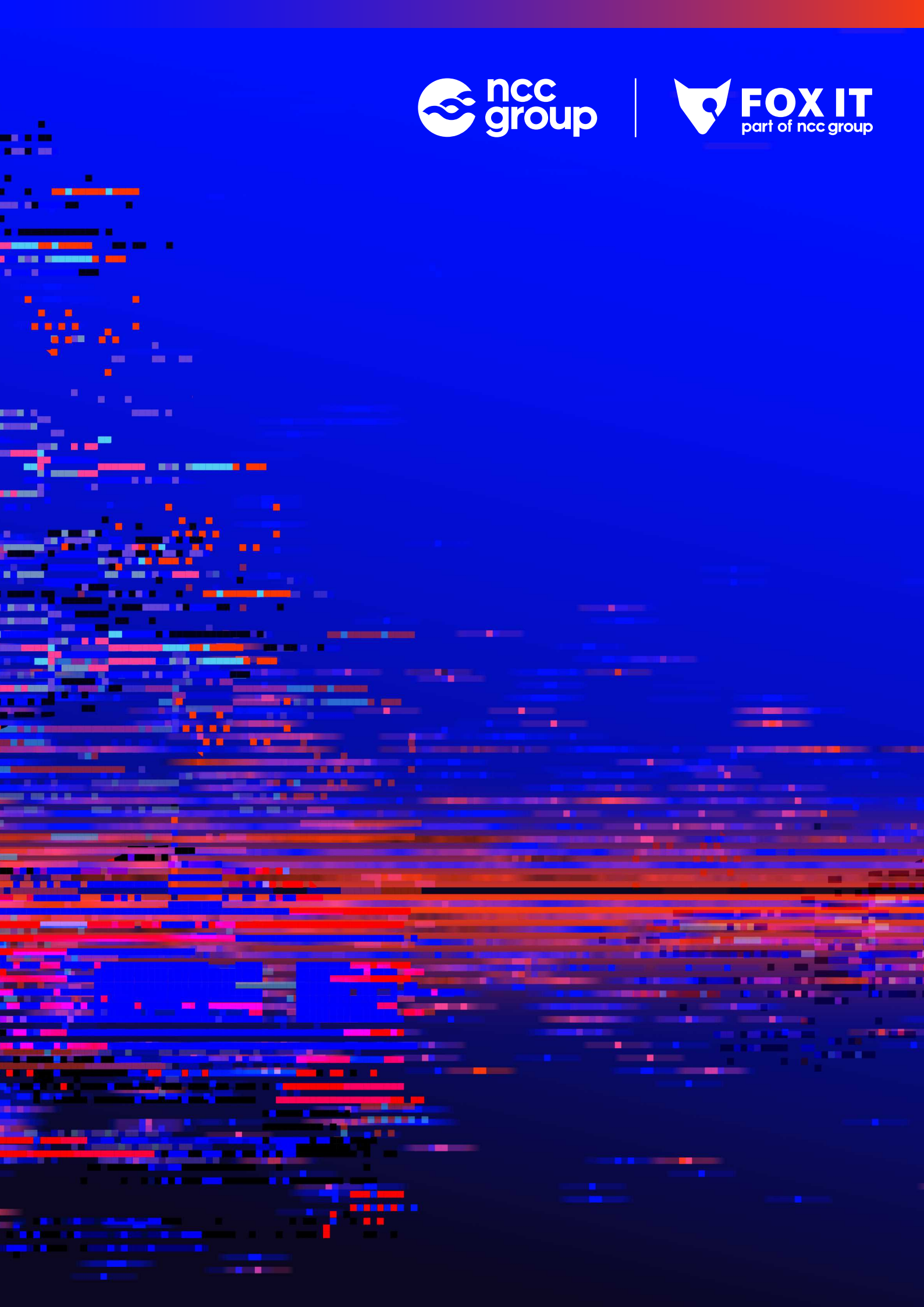
We're a people powered, tech-enabled global cyber security and resilience company with over 2,200 colleagues around the world.

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.

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




ncc group
FOX IT
part of ncc group