nccgroup

People powered tech-enabled cyber security

Cyber Threat Intelligence

Review of February 2025

FOX IT
part of nccgroup

Contents

Executive Summary

This month we continue to report high numbers of ransomware attacks, with 886 in February. This is marked by the bulk release of ransomware victims by Cl0p, following the group's exploitation of CVE-2024-50623 and CVE-2024-55956 in Cleo software. As such, these numbers should be considered carefully where representing the overall threat landscape and are further discussed in this report.

Away from the statistics, we explore LockBit 4.0, one year on from Operation Cronos, and 8Base, the most recent group to be targeted in a global law enforcement operation. Law enforcement operations continue to disrupt the ransomware landscape, yet ransomware numbers are on the rise.

Our Geopolitical Developments insights flag ongoing activity relating to the Trump Presidency which continues to attract concern. Both financially and geopolitically motivated threat actors have an opportunity to exploit the current state of confusion, disruption, and deviation from normal cyber security standards and processes.

For our Quarterly Thematic Output, we explore edge devices, often regarded as a first line of defense against threat actors. If edge devices are insecure, this can act as an open door to even the most unskilled threat actors, making it easier for them to find and exploit vulnerabilities. This follows Five Eyes cyber security agencies recently highlighting the need for organizations to protect their edge devices and appliances.

Finally, our Emerging Cyber Security Trend explores cloud security. As cloud infrastructure continues to drive digital transformation and becomes integral to modern business operations, the frequency and sophistication of cyberattacks targeting these environments has surged. We can anticipate that there will be an escalation of attacks to public cloud platforms, with a projected 21.5% growth in public cloud services in 2025. From identity-based attacks and ransomware to infrastructure laundering and critical infrastructure vulnerabilities, cloud threats are more complex than ever.

Section 1

50%

Global ransomware attacks increased by 50% in February 2025

31%

Consumer Discretionary accounted for 31% of ransomware attacks in February 2025

37%

Cl0p was responsible for 37% of attacks in February 2025

Ransomware Key Statistics

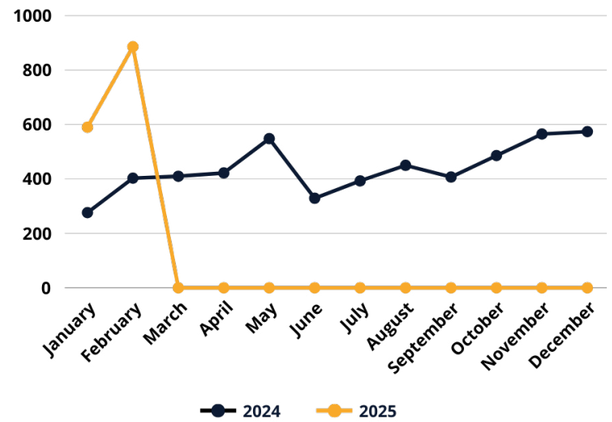


Figure 1 Ransomware Attacks by Month 2024 - 2025

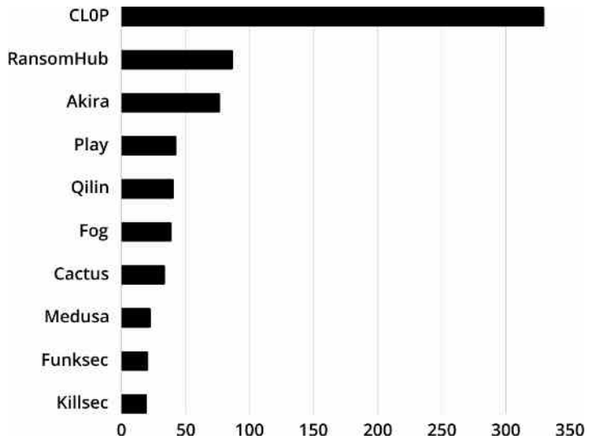


Figure 3 Top 10 Threat Actors February 2025

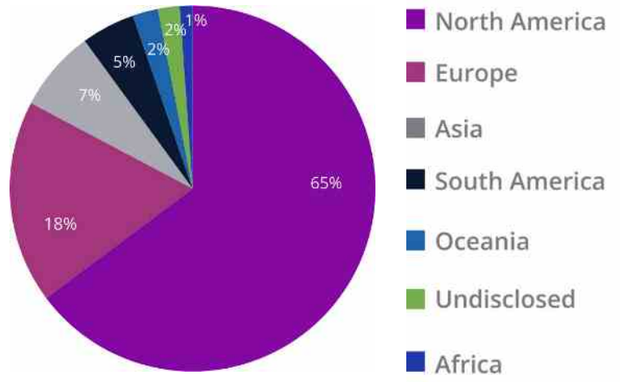


Figure 2 Ransomware Attacks by Region February 2025

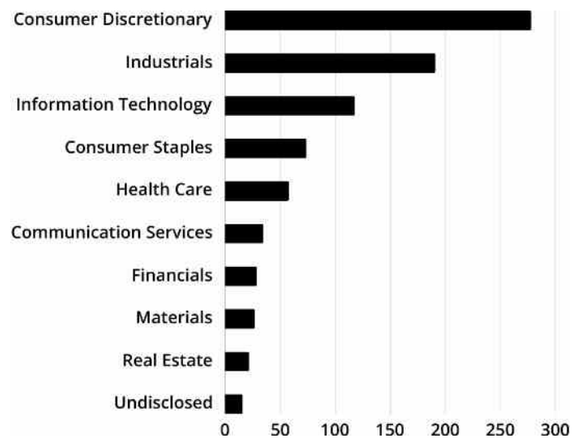


Figure 4 Top Targeted Sectors February 2025

LockBit Black Ransomware exploits Atlassian Confluence Vulnerability

A notable ransomware attack involved the exploitation of a critical Atlassian Confluence vulnerability (CVE-2023-22527). Hackers used this vulnerability to deploy LockBit Black ransomware across enterprise networks within two hours of initial compromise.

Key Events

February 09, 2025

DISA Global Solutions

The breach impacted over 3.3 million individuals, compromising their data, including names, social security numbers, driver's license numbers, financial account information, and drug testing details.

February 12, 2025

Mars Hydro

A massive IoT data breach exposed 2.7 billion records, including Wi-Fi passwords, IP addresses, and device identifiers.

February 20, 2025

HCRG Care Group

Medusa ransomware gang demanded $2M from HCRG Care Group, threatening to leak 2.275 TB of stolen data if the ransom wasn't paid by February 27, 2025.

NCC Group Services

NCC Group can support you to mitigate against the ransomware threat. Please see our contact details at the end of this report should you require assistance.

Cl0p Ransomware Contributes to 37% of February's Figures

In February 2025, 886 attacks were identified, of which 330 victims (37%) were attributed to Cl0p. This is not only a 460% increase from their attacks in January but contributed to an overall surge in ransomware numbers.

This is the likely result of their successful exploitation of two zero-day vulnerabilities in Cleo software in late 2024, CVE-2024-50623 and CVE-2024-55956. The subsequent release of hack and leak victims in bulk has, therefore, caused a surge in the overall numbers. Notably, this is not new for Cl0p, who previously adopted a similar approach when exploiting the 2023 Go Anywhere and MoveIT vulnerabilities. The recent increase in Cl0P victims, therefore, mirrors their past campaigns, targeting vulnerable file transfer software and releasing victims in bulk, and can be considered a key part of their Modus Operandi (MO).

The spike in overall attack numbers is, therefore, likely inflated due to the bulk release of victims breached in previous months. Moreover, ransomware claims made by Cl0p may be exaggerated to attract more attention. Such activities have also been observed in other threat actors within the ransomware landscape. Hence, whilst the data was sourced from the group's Data Leak Site (DLS), the overall numbers of ransomware attacks in February should be considered carefully.

If we consider the overall ransomware threat landscape including Cl0p's attacks, the following trends are observed (see Figure 5). Note that Cl0p re-emerged in December 2024, in line with the exploitation of the Cleo vulnerability. In December 2024, they were responsible for 68 attacks, 59 in January 2025, and 330 in February 2025. Including Cl0p, this sees 574 attacks in December 2024, 590 in January 2025, and 886 in February 2025.

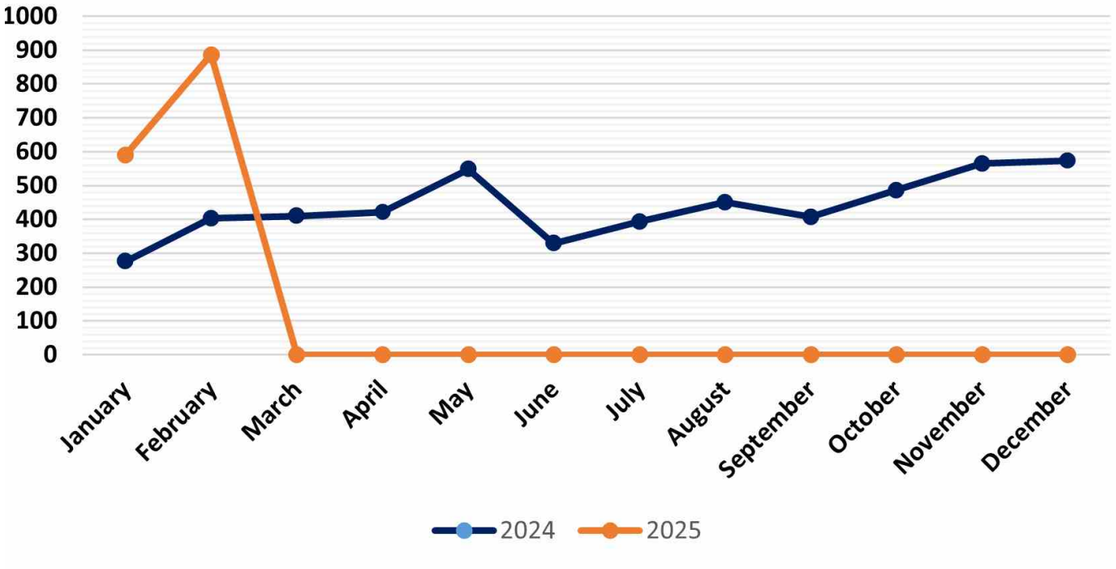


Figure 5 Number of ransomware attacks by month including Cl0p, 2024-2025

If we remove Cl0p's activity from 2024 and 2025 (Figure 6), this totals at 506 attacks in December 2024, 531 attacks in January 2025, and 556 in February 2025.

Although still high, they illustrate a more stable growth between the months. Importantly, whilst Cl0p's bulk data release inflates the data at present (Figure 5), we still observe an increased threat from ransomware attacks overall when removing this anomaly.

As such, the data continues to suggest that ransomware attacks are on the rise.

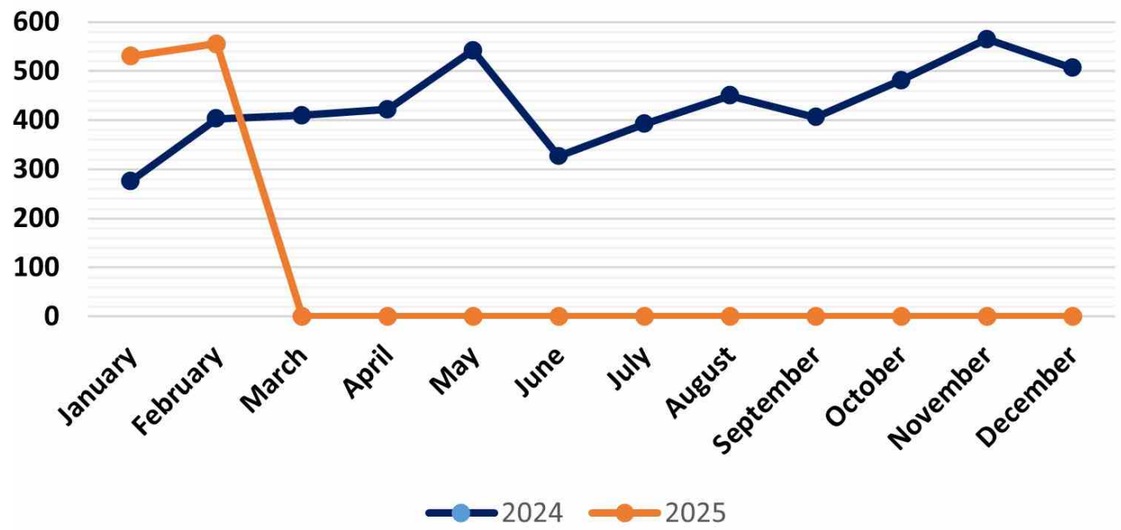


Figure 6 Number of ransomware attacks by month excluding Cl0p, 2024-2025

Taking a closer look at Cl0p's activity alone reveals how their MO of exploiting CVE's and bulk-releasing data is reflected in the numbers. Looking at Figure 7, in 2023, March illustrates a spike in attack numbers following the exploitation of the Go Anywhere MFT Flaw.

This is observed again in June and July, following the exploitation of the MOVEit CVE. Activity quietens in 2024 until the recent exploitation of the Cleo software vulnerability reflected in the December 2024 to February 2025 increase.

Hence, we observe a patten in which Cl0p's activity spikes following CVE exploitation, otherwise, the group remains quiet.

This provides further understanding of the groups' MO, as well as the importance of patching where CVE's continue to be exploited by ransomware actors.

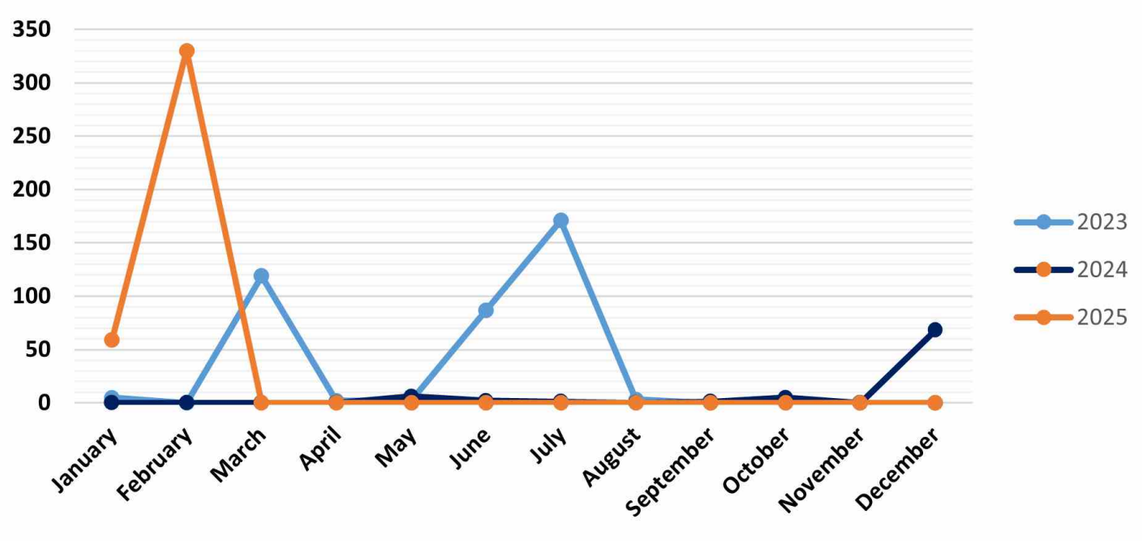


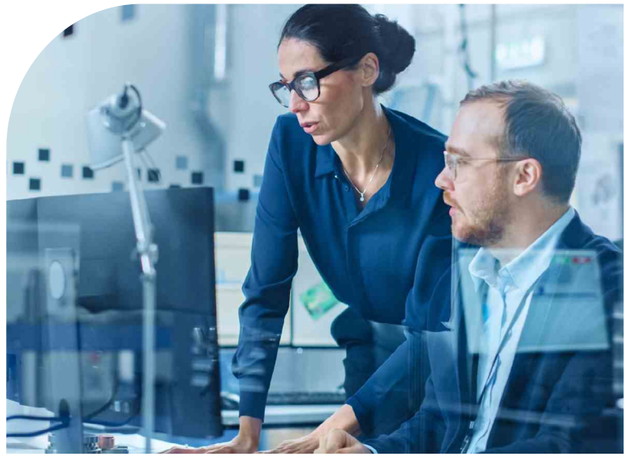
Figure 7 Number of Cl0p ransomware attacks by month 2023-2025

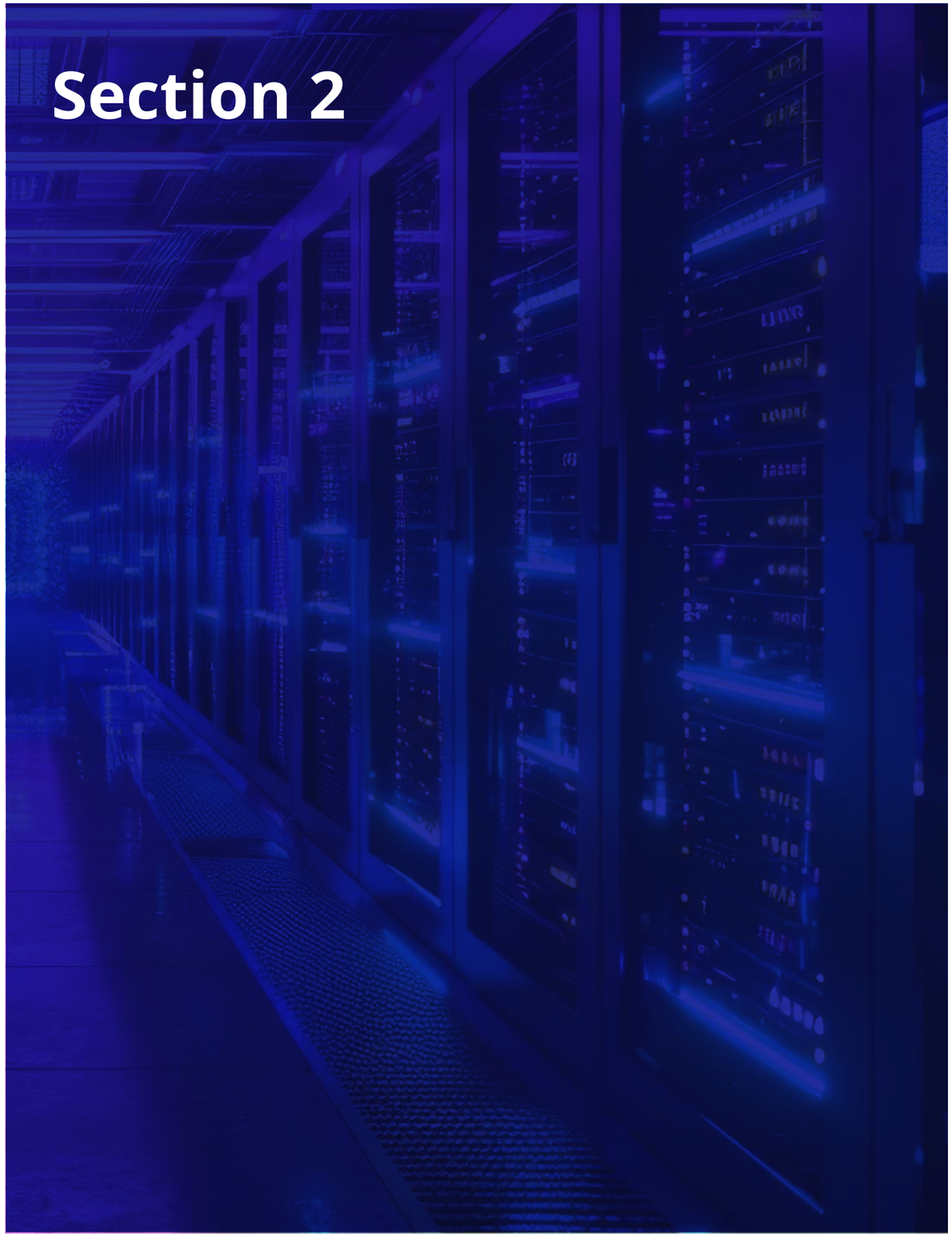
Vulnerabilities Exploited:

- CVE-2024-50623 allows attackers to upload malicious files to the server. These files can then be executed to gain remote code execution (RCE) on the affected system. The issue was regarding improper handling of file uploads in the Autorun directory, which attackers can exploit by sending a specially crafted request to retrieve files from a server or upload malicious files. This also gives the attackers persistent access and control over the compromised system.

- CVE-2024-55956 allows RCE through the Autorun directory. This vulnerability allows unauthenticated users to import and execute arbitrary Bash or PowerShell commands on the host system by leveraging the Autorun directory's default settings. This also enables the attackers to deploy modular Java backdoors to steal sensitive data, and move laterally within networks, leading to potential full system compromise. Cleo software is widely utilised in many organisations, increasing the overall impact of their recent attacks.

The US Cybersecurity and Infrastructure Security Agency (CISA) urged immediate patching of the Cleo Software to version 5.8.0.24, as this patch resolves both CVE-2024-50623 and CVE-2024-55956, but many organisations remain vulnerable due to delayed updates or insufficient mitigations. Disabling the Autorun directory temporarily can prevent attackers from executing unauthorised commands.[3] If not already done, please ensure to patch against this vulnerability.





Ransomware Spotlight: LockBit 4.0 Reemergence(?) and 8Base Seized by Law Enforcement

February marked two notable events in the ransomware threat landscape. The first, the anniversary of LockBit's seizure in February 2024, and the anticipated arrival of a LockBit 4.0 version. Since LockBit was seized during Operation Cronos in February 2024, the group has maintained a low profile. This is evidenced by a decrease in victims on their leak site following the seizure of their infrastructure by authorities. In December 2024, however, LockBit drew attention to themselves when an alleged group admin announced the anticipated release of version 4.0 in 2025. This could have been an attempt to revive or salvage the brand's reputation, as law enforcement operations continue.

Additionally, law enforcement disrupted the 8Base ransomware group; the events resulted in the arrest of alleged members and the seizure of their infrastructure.[4] The theme of ransomware takedowns therefore remains topical, as well as their overall effectiveness, given potential group resurgence and the increasing number of attacks in our ransomware database.

One year on from Operation Cronos, there has been limited LockBit activity, notably when compared to their heyday in 2023. NCC Group data shows that LockBit activity has halved from 1034 claims in 2023 to 526 claims in 2024. The arrests of developers and affiliates likely caused many members to go into hiding or to find another Ransomware-as-a-Service (RaaS) operator with less law enforcement attention.[5,6] In December 2024, alleged LockBit admins teased the release of their 4.0 ransomware locker that promised improved capabilities in several areas such as encryption and evasion.[7]

However, there has been limited discussion on major forums. Threatening the release of 4.0 may have been a psychological tactic by LockBit to leverage the group's historical reputation to maintain an external image that their operations are ongoing. A similar strategy was observed in September 2024, when the group had recycled over 40% of their attacks from previous breaches.[8]

Further operations by law enforcement have continued to positively impact the threat landscape by disrupting additional cybercriminal networks. On February 10, 2025, law enforcement agencies from Europe, North America, and Asia, engaged in Operation Phobos Aetor, seized the 8Base Data Leak Site (DLS) and arrested four individuals in Thailand. The individuals were allegedly involved in compromising the networks of 17 Swiss companies in 2023 and 2024 and face possible extradition to Switzerland.[9] Similar to Operation Cronos, authorities disrupted cybercriminal activities by seizing critical infrastructure, such as their DLS, crypto wallets, and personal computers.

Overall, law enforcement operations have varied effects on the ransomware landscape. These effects are mostly positive, with ransomware groups disrupted, less trust amongst groups due to identities being revealed, as well as increased personal risk due to international arrests and extradition. Organisations, however, must remain vigilant as they continue to face risks due to the adaptability of these groups against external pressures.

Section 3

Quarterly Thematic Output: Vulnerabilities in Edge Devices

Edge devices are at the perimeter of an organisation's network and act as barriers between internal enterprise networks and the internet. As such, they can be regarded as a first line of defence against threat actors; consequently, organisations should focus on securing this perimeter to proactively mitigate against any threats. If edge devices are insecure, this can act as an open door to even the most unskilled threat actors, making it easier for them to find and exploit vulnerabilities.[10]

Routers are a common device exploited by Organised Criminal Groups (OCGs) and recruited into large botnets, often used to conduct Distributed Denial of Service (DDoS) attacks. Multiple botnets are known to exploit vulnerabilities in routers, industrial, Small Office Home Office (SOHO), and personal, to turn internet-capable devices into "zombie" devices.

Routers frequently come under attack from nation-state groups alike with the same devices being targeted by both nation-states and OCGs. It is not uncommon to witness routers being compromised multiple times by different groups working towards their own goals.

Procuring devices which are secure-by-design is one of the best steps an organisation can take. However, security teams may be unfamiliar with the infrastructure on the network and will first need to identify where an organisation's network's edge is and what devices are on it.

Once identified, these devices should then be monitored specifically for any anomalous behaviour or emerging threats such as zero-day vulnerabilities.[11] Any devices which are identified to be at end-of-life should be removed as soon as practically possible and replaced with devices which are secure-by-design.[12]

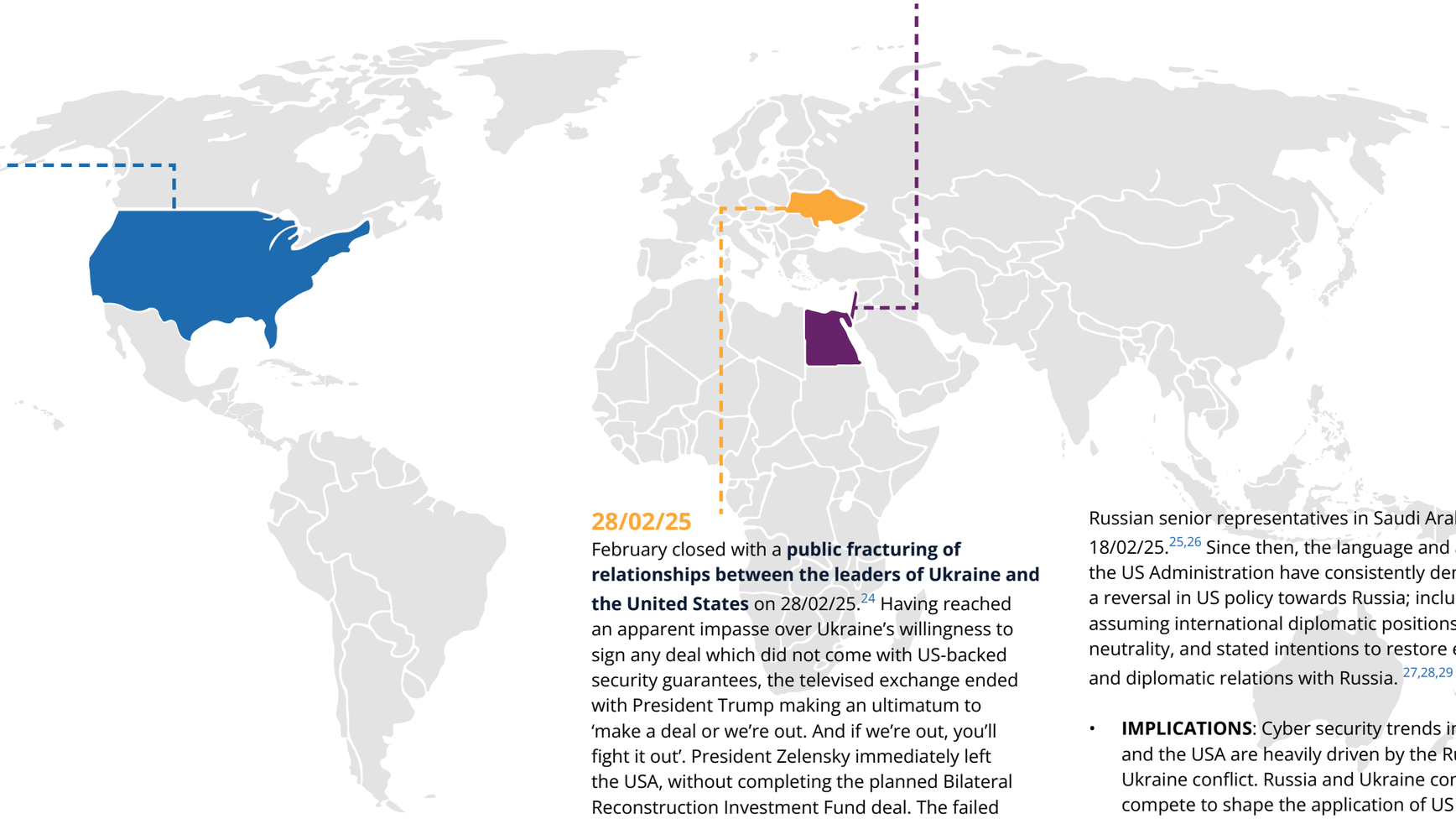
Devices should not be used as-is. Instead, they should be assessed as to how they meet an organisation's specific needs and have unnecessary features and ports disabled or closed to reduce the potential attack surface.

As much as possible, threat detection and monitoring should be centralised to reduce segmentation of security teams and difficulties in communicating when threats are detected.[13] Hardening your edge devices not only secures your organisation but also protects others from cyberattacks.

Section 4

Geopolitical Developments

NCC Group's Threat Intelligence Team highlights geopolitical developments from the month which have the capacity to influence the cyber threat landscape.



04/02/25

President Trump ordered his administration to resume a 'maximum pressure' approach to Iran to 'end its nuclear threat, curtail its ballistic missile program, and stop its support for terrorist groups'.[14] President Trump expressed personal regret over the measures and a desire to make a deal. New related sanctions were subsequently announced.[15,16,17]

On 25/02/25 Iran's Foreign Minister excluded the possibility of direct negotiations with the US 'as long as maximum pressure is being applied'. Iran's Supreme Leader called for further investment in Iran's military capabilities, whilst the UN warned that political solutions are 'running out of time' to prevent Iran from successfully developing nuclear weapons.[18,19]

- **IMPLICATIONS:** An effective sanctions regime reduces Iran's capabilities to create income from oil exports, and places additional strain on the global oil economy – particularly for Iran's primary customer, China. Under greater financial pressure, expansion and evolution of Iran's state-sponsored cyber-capabilities towards revenue-generating attacks, including increasing existing relations with the cyber-crime economy, is a realistic option.

04/02/25

As part of the state visit of Israeli Prime Minister Benjamin Netanyahu to the United States, **President Trump made a broad statement on US-Israeli interests which included outlining a future for Gaza.**[20] This vision included relocation of Palestinians from Gaza, to allow the US to own and redevelop the area into an international hub. The plan appears to have been widely interpreted as inconsistent with both international law and a two-state solution for peace.[21] An independent report assesses more than $50 billion will be required for recovery and reconstruction over 10 years.[22] Saudi Arabia and Egypt are leading on efforts to create an alternative recovery plan, prioritising Palestinian interests.[23]

- **IMPLICATIONS**: Key nation-states with advanced cyber-capabilities have expressed their support for Palestinians. Hacktivist groups already engaged with the Israel-Palestine conflict and opposed to US-influence are likely to view the plan negatively and as provocation to respond for as long as the story continues to develop

28/02/25

February closed with a **public fracturing of relationships between the leaders of Ukraine and the United States** on 28/02/25.[24] Having reached an apparent impasse over Ukraine's willingness to sign any deal which did not come with US-backed security guarantees, the televised exchange ended with President Trump making an ultimatum to 'make a deal or we're out. And if we're out, you'll fight it out'. President Zelensky immediately left the USA, without completing the planned Bilateral Reconstruction Investment Fund deal. The failed meeting followed President Trump's announcement on 12/02/25 that US officials would begin talks to establish a negotiated peace for the Ukraine-Russia war, and a related meeting between American and Russian senior representatives in Saudi Arabia on 18/02/25.[25,26] Since then, the language and actions of the US Administration have consistently demonstrated a reversal in US policy towards Russia; including assuming international diplomatic positions of neutrality, and stated intentions to restore economic and diplomatic relations with Russia. [27,28,29]

- **IMPLICATIONS**: Cyber security trends in Europe and the USA are heavily driven by the Russia-Ukraine conflict. Russia and Ukraine continue to compete to shape the application of US influence towards shifting the course of the war, this development has the potential to shift the focus of pro-Russian threat actors away from US entities and interests.

Section 5

Emerging Cyber Security Trend: Cloud Security Challenges & Rise of Zero Trust

As Cloud infrastructure continues to drive digital transformation and becomes integral to modern business operations, the frequency and sophistication of cyberattacks targeting these environments has surged. We can anticipate that there will be an escalation of attacks to public cloud platforms since there is a projected 21.5% growth in public cloud services in 2025.[30]

From identity-based attacks and ransomware to infrastructure laundering and critical infrastructure vulnerabilities, the landscape of cloud threats is more complex than ever. Traditional security models relying on network perimeters are no longer sufficient.

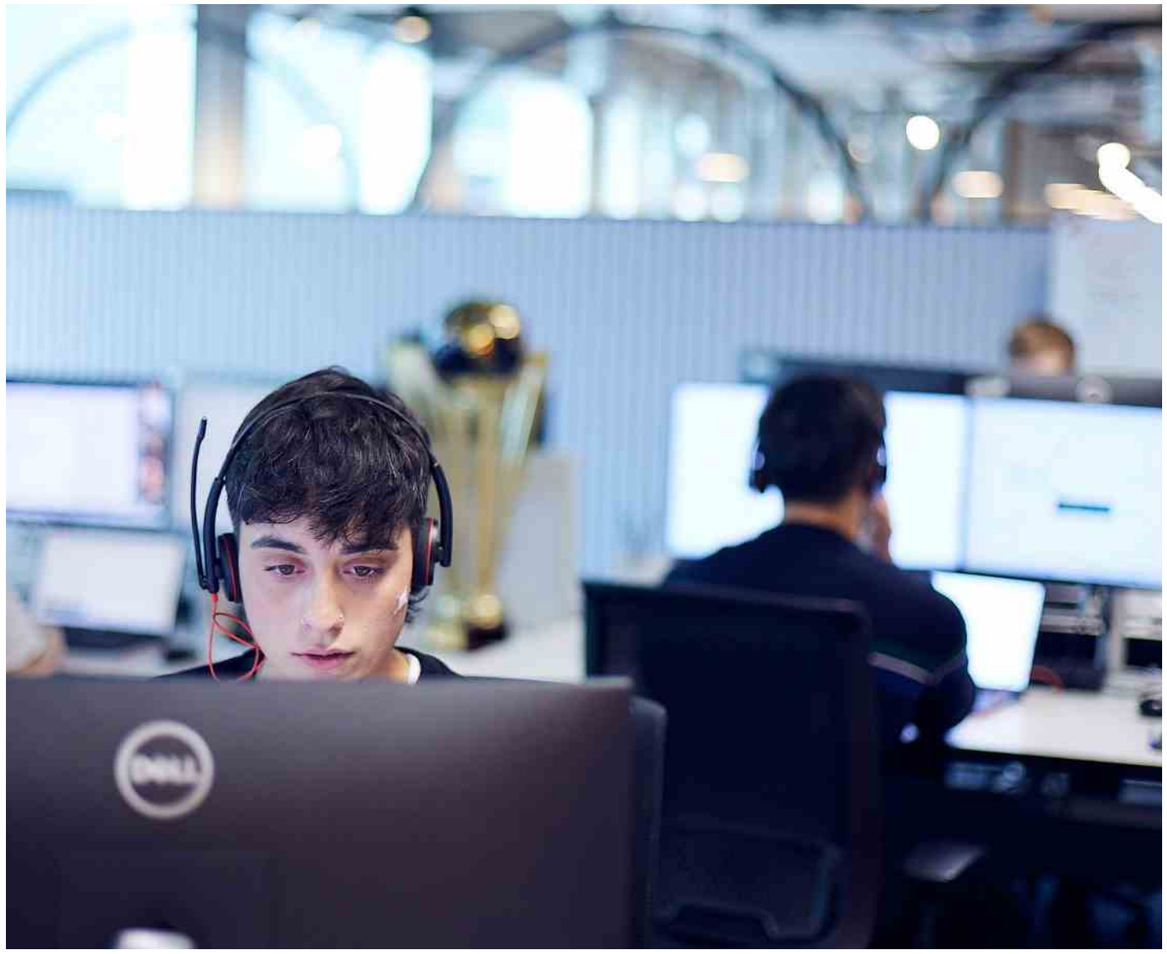
To address cloud security challenges, one effective solution is adopting a Zero Trust model. This ensures continuous verification of every user and device, regardless of their location, to protect sensitive data and resources. Zero Trust is a security model which eliminates implicit trust and continuously verifies every access request. It assumes that threats can originate from anywhere – both inside and outside the organisation.[31]

This model enforces the principle of "Never Trust, Always Verify", with a critical component of being Identity and Access Management (IAM), which ensures that only authorised users and devices can access sensitive cloud resources. This can provide users with a seamless single sign-on (SSO) experience for cloud-hosted networks.[32]

Zero Trust is required for maintaining the integrity and security of cloud infrastructure and providing ongoing training and awareness programs to employees as well as conducting regular security assessments such as Vulnerability and Penetration Testing, are important for identifying and mitigating risks in the cloud environment.

Organisations should also comply with the latest cloud infrastructure and industry standards such as General Data Protection Regulation (GDPR) and ISO 27001. By proactively addressing these challenges and implementing Zero Trust with strong IAM methods, businesses can build secure, resilient cloud infrastructure.

About NCC Group



NCC Group is a global cyber and software resilience business, operating across multiple sectors, geographies and technologies.

As society's dependence on the connected environment and associated technologies increases, we use our global expertise to enable organisations to assess, develop and manage their cyber resilience posture to confidently take advantage of the opportunities that sustain their business growth.

With circa 2,400 colleagues, we have a significant market presence in the UK, Europe and North America, and a growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contact us

+44 (0) 161 209 5200
UK & Europe

+1 (800) 813 3523
North America

reponse@nccgroup.com
www.nccgroup.com

nccgroup

People powered tech-enabled cyber security

FOX IT

part of nccgroup