nccgroup

People powered tech-enabled cyber security

Cyber Threat Intelligence

March Pulse: Review of Q1 2025

FOX IT
part of nccgroup

Contents

Executive Summary

Hack and leak numbers were at an all-time high in Q1 2025, although this was heavily skewed by the bulk release of Cl0p's victims, inflating the numbers. Additionally, the emergence of Babuk 2.0 has raised many questions as to the legitimacy of their claims.

The security community and ransomware actors alike believe that Babuk 2.0 is a fraudulent group, recycling data from previous breaches and claiming them as their own. What is clear is that threat actors remain creative in their attempts to maximise profits.

Away from the numbers, the spotlight explores the recent chat leaks from the BlackBasta ransomware group. Notably, previous research has explored the group's Tactics, Techniques, and Procedures (TTPs) from a post-attack perspective.

Now, the chat leaks enrich previously discovered TTPs from an internal perspective, along with a look into the group's internal dynamics, which may be limited from a post-attack standpoint.

The logs provided insights into the range of vulnerabilities, malware, and misconfigurations that the group allegedly utilised on their targets and can support the security community in better understanding ransomware actors, as well as defending themselves.

Our Emerging Cyber Security Trend explores malvertising, a pervasive threat, exploiting online advertisements to disseminate malware. This comes as the number of malvertising attacks heavily increased throughout 2024 and is likely to remain a pervasive threat in 2025.

Of note, Microsoft Threat Intelligence uncovered nearly one million devices globally implicated in a large-scale malvertising campaign in March, which uses GitHub repositories, Discord and Dropbox as its command and control (C2).

Geopolitical developments see the continued impact of changes made by the new US government, notably in Ukraine and Canada. The US government itself suffered a breach when a media editor was accidentally added to a Signal group chat named 'Houthi PC small group', relating to attack planning against the rebels.

This has raised major concerns regarding intelligence sharing practices and the disclosure of sensitive information, alongside cyber security practices in government .

Finally, our Quarterly Thematic Output wraps up coverage on the theme of vulnerabilities, with a discussion on zero-days. Several key zero-days from the Quarter are explored, and numbers gathered from a Vulnerability Monitoring Database suggest that zero-days have increased rapidly compared to the same time last year.

All in all, threat actors remain active, adjusting and adapting their methods to their advantage.

Section 1

28%

Global hack and leak attacks increased by 28% in Q1 of 2025

25%

Consumer Discretionary accounted for 25% of ransomware attacks in Q1 of 2025

19%

Cl0p was responsible for 19% of attacks in Q1 of 2025

Ransomware Key Statistics

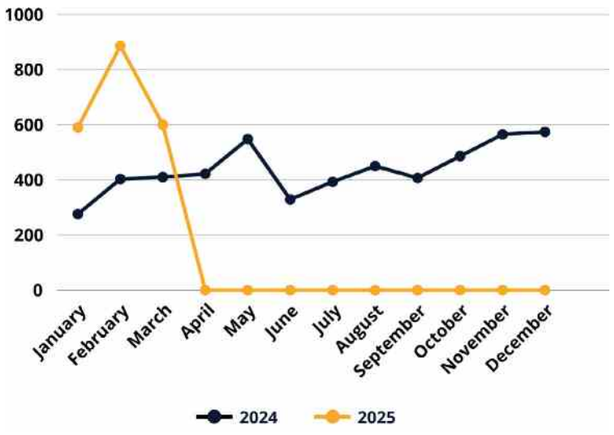


Figure 1 Ransomware Attacks by Month 2024 - 2025

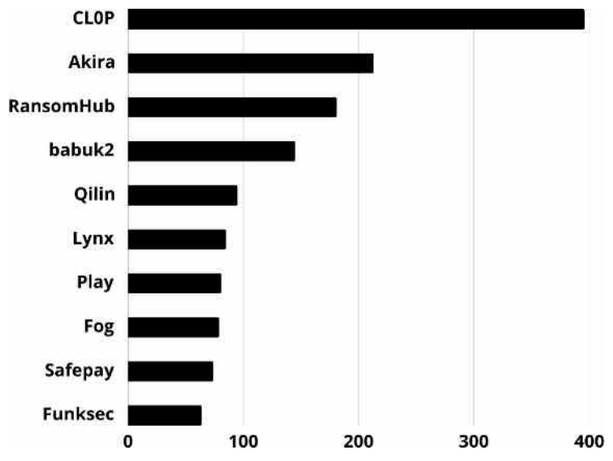


Figure 3 Top 10 Threat Actors Q1 of 2025

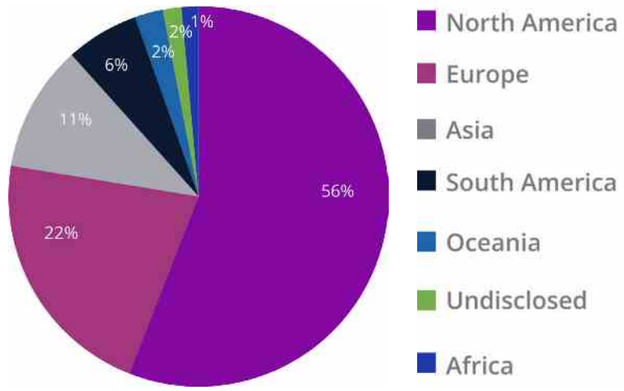


Figure 2 Ransomware Attacks by Region Q1 of 2025

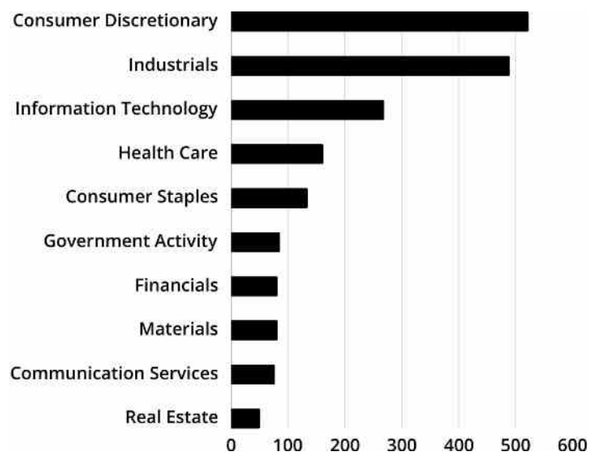


Figure 4 Top 10 Targeted Sectors Q1 of 2025

Cl0p Ransomware Group exploited Cleo File Transfer Tool (CVE-2024-50623)

Cl0p ransomware group exploited CVE-2024-50623 in Cleo's file transfer tools to gain unauthorised access, upload malicious backdoors, execute remote commands and steal sensitive data. This allowed them to infiltrate networks and extort companies by threatening to disclose stolen information. This attack was part of a broader campaign where Cl0p exploited zero-day vulnerabilities in Cleo's software.

Key Events

January 02, 2025

Atos

Space Bears claimed to have stolen data from Atos on December 28 and threatened to publish it on January 8. Atos found no evidence of a compromise or ransomware affecting their systems, and no ransom demand had been received.

February 12, 2025

Unimicron

The Sarcoma ransomware group attacked Unimicron, a Taiwanese PCB maker, claiming to hold 377 GB of stolen SQL files and documents. They published samples and threatened to leak everything if a ransom was not paid.

March 12, 2025

Department of Health Services for the state of Yap

A state in Micronesia is dealing with ransomware hackers who forced its government health agency's computers offline, leading to zero internet connectivity as the entire network was shut down to prevent further damage.

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.

Ransomware Insights

In the first quarter of 2025, 45% (935/2074) of ransomware attacks were attributed to four groups, Cl0p, Akira, RansomHub, and Babuk 2.0.

Babuk 2.0

Babuk 2.0 emerged in January 2025, despite the original group having shut down in 2021. This new version claimed 145 attacks in Q1 2025 but has been met with scrutiny surrounding the legitimacy of their claims.

Secondary research from security firms revealed that 90% of their January claims were false, as the group failed to provide legitimate evidence of an actual breach.[1]

This has frustrated other groups in the ransomware community, claiming Babuk 2.0 to be a fraud, with the original Babuk version claiming no connection to the new operation.

This newer version is said to be exploiting the brand name Babuk to gain credibility, and it is suggested that threat groups Skywave and Bjorke are responsible for the operation. This appears to be a rebranding stunt rather than the true revival of the group, a common tactic among ransomware operators to confuse defenders, attract affiliates, and inflate their reputation.

The threat actors are seen to be using data from previous leaks to extort victims, commoditising the data for profit.

We are reviewing the claims associated with Babuk 2.0 to assess their credibility and will provide a dedicated write-up in the April Pulse.

Cl0p

Cl0p claimed 396 attacks this quarter, largely attributed to the successful exploitation of two zero-day vulnerabilities in Cleo software in late 2024, CVE-2024-50623 and CVE-2024-55956.

The subsequent bulk release of hack and leak victims caused a surge in the overall numbers, as discussed in our February Pulse.

This behaviour is typical of the group, with similar behaviours observed when exploiting the 2023 MoveIT and GoAnywhere vulnerabilities, which saw a high volume of victims claimed over a short period of time.

Akira

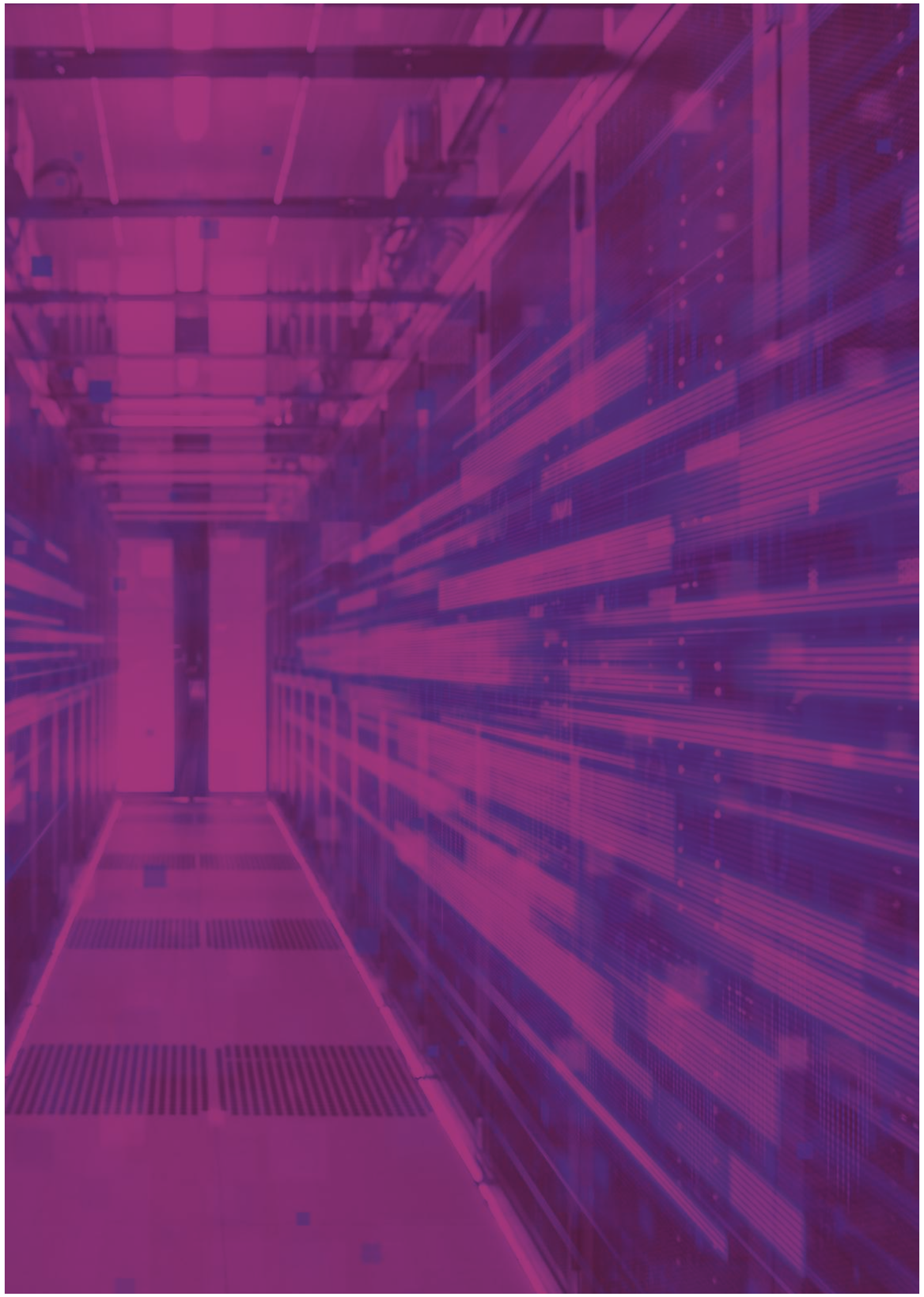
Akira operates a standard Ransomware-as-a-Service (RaaS) operation which relies on exploiting known critical vulnerabilities on VPN software. The group operates an 80/20 commission structure in favour of affiliates. 213 attacks were attributed to the group, up from 140 attacks in Q4 of 2024.

The high number of attacks are linked to the group's effective use of Python-based malware and exploitation of critical infrastructure vulnerabilities.[2] Competitive commissions along with the recent exodus of affiliates from other groups like BlackBasta may also contribute to the boost in Akira's numbers.[3]

RansomHub

Similarly, RansomHub operates a 90/10 commission structure which likely increases the appeal of working with the group.[4] The group also exhibits long-term experience in ransomware operations with the use of phishing, known vulnerabilities and previously compromised credentials.

Both their expertise in conducting ransomware attacks, and attractive affiliate structure, will likely contribute to the high number of claims associated with the group this quarter (181).



Section 2

Ransomware Spotlight: BlackBasta Chat Leaks

On February 11, 2025, BlackBasta's internal chat messages were leaked via Telegram through a user named "ExploitWhispers".[5]

There is limited information behind the alleged leaker, however internal conflicts are suspected to be a primary motivation behind the events. This resulted in a race by security companies to quickly analyse the messages to gain valuable threat intelligence about one of the most prolific ransomware gangs.

The leaks, which span September 2023 to September 2024, provided insight into how the group's internal issues resulted in an ongoing exodus of various affiliates. Moreover, the chats also showed the range of vulnerabilities, malware, and misconfigurations that the group allegedly utilised on their targets.

Previous research has explored the group's Tactics, Techniques, and Procedures (TTPs) from a post-attack perspective. Now, the chat leaks can enrich previously discovered TTPs from an internal perspective, along with a look into the group's internal dynamics, which may be limited from a post-attack standpoint.

The BlackBasta leaks also provide additional evidence into the wider trends that have been observed in the ransomware landscape. Specifically, the constant movement of affiliates to other groups and the creation of new variants.

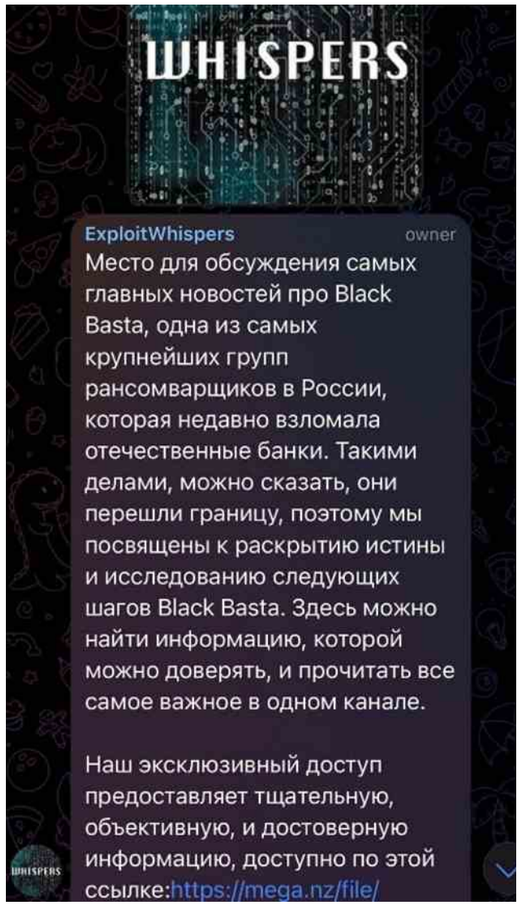
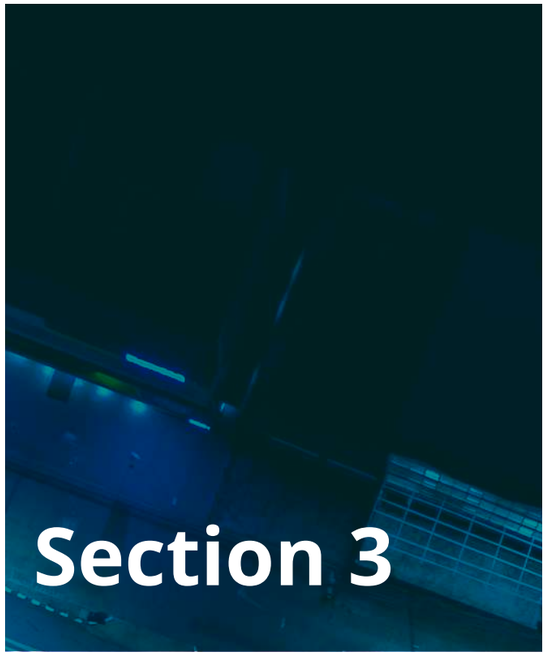


Figure 5 Leak by telegram user "ExploitWhispers"



Section 3

Emerging Cyber Security Trend: Malvertising

Malvertising has become a pervasive threat, often exploiting online advertisements to disseminate malware. Malvertising, or “Malware advertising”, refers to the use of specially crafted online advertisements to spread malware across devices.

Malvertising campaigns often begin with malicious ads embedded in illegal streaming websites, employing complex redirection chains to obscure their origins. The estimated total damages for malvertising and other malware-related frauds stands at $10.5 trillion by the end of 2025.[6]

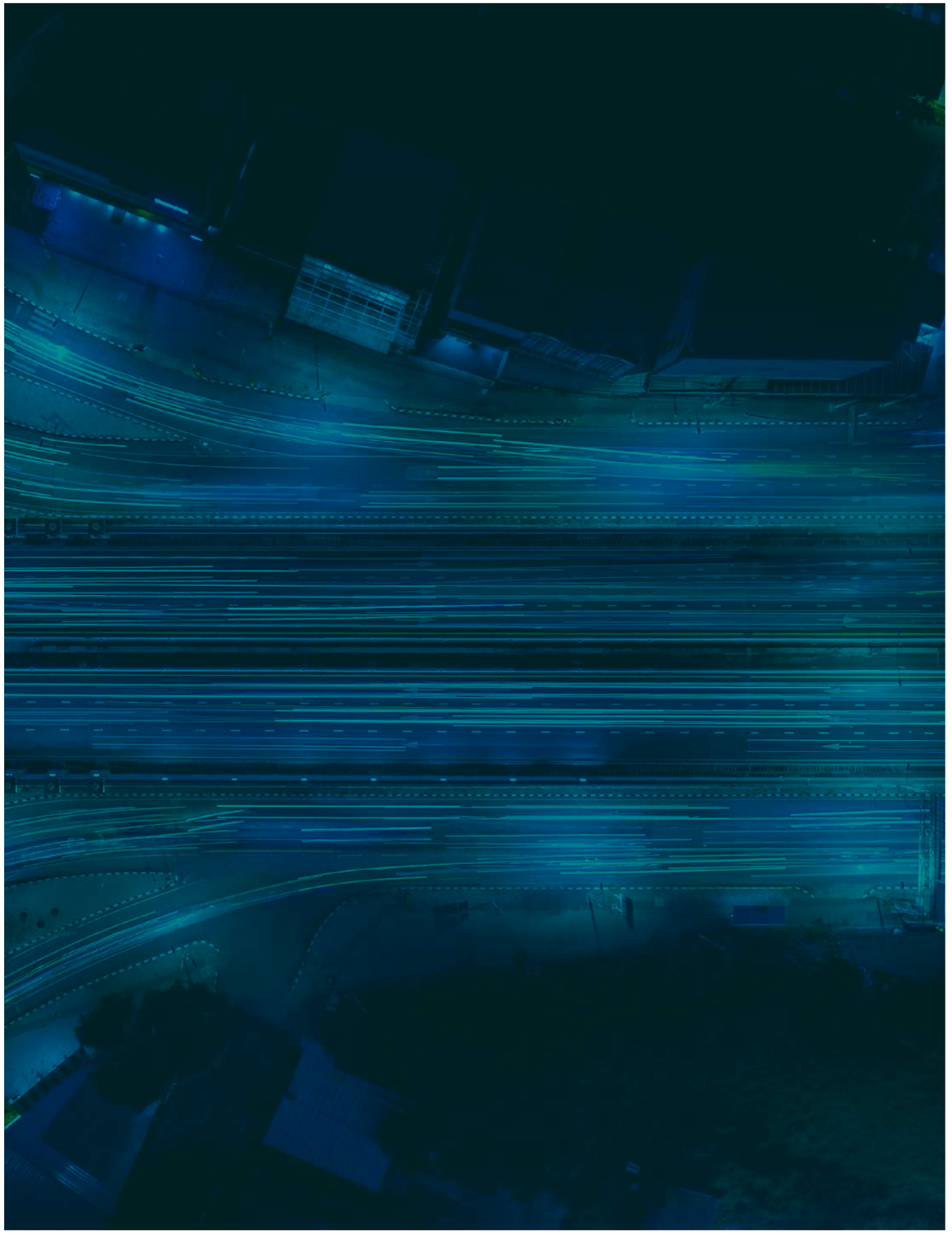
Microsoft discovered nearly one million devices infected by a malvertising campaign in December 2024.[7]

ESET's H2 2024 cyber threat report revealed a staggering 400% surge in Lumma Stealer malware, heavily used in malvertising campaigns.[8] Additionally, there have been an average of 2.8 million malware, adware or unwanted software attacks that target mobile devices each month, totalling over 33 million attacks for the year 2024.[9]

Malvertising is likely to remain a pervasive threat in 2025, with the potential to increase. The consequences of these attacks are significant, affecting both consumer and enterprise devices, leading to data theft and system compromise.

The rise in large-scale campaigns and exploitation of search results for malware distribution shows that security measures should keep up the pace. Accessibility to tools like Malware-as-a-Service (MaaS) and DeepSeek AI lowers the gap for attackers to implement sophisticated attacks without high technical skills.

Addressing this threat requires collaboration between industries and government to strengthen their threat intelligence. Proactive measures and global cooperation will be key to staying ahead of threat actors. The future of cyber security and cyber space hinges on our ability to anticipate and counter these evolving threats.



Section 4

Geopolitical Developments

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

11/03/25

Following bilateral talks between Ukrainian and American officials in Saudi Arabia, a joint-statement confirmed that Ukraine accepted the 'US proposal to enact an immediate, interim 30-day ceasefire' subject to 'acceptance and concurrent implementation by the Russian Federation'.

On 18/03/25, Russia agreed to implement a partial cease-fire; limited to energy infrastructure targets.

Efforts to expand the agreement to the Black Sea have so far not been realised and are currently dependent on Russian conditions which include those which the EU state they will not support.[10]

On 30/03/25 President Trump expressed his anger at Russian President Putin and referenced hypothetical tariffs if he feels Russia is at fault if a ceasefire cannot be agreed.[11]

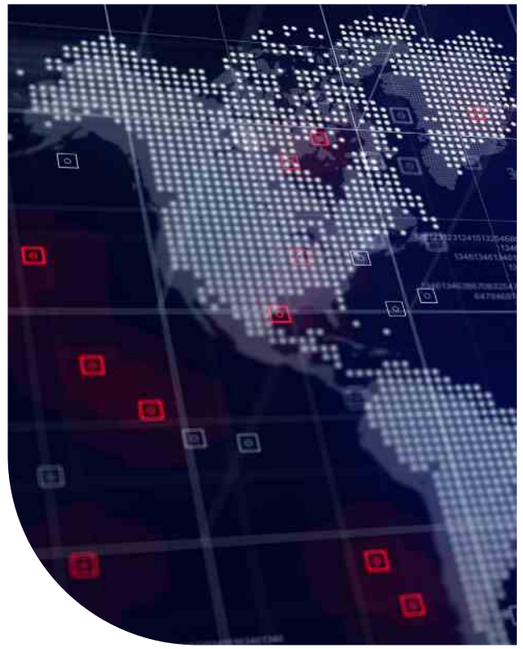
14/03/25

President Trump's leadership of the USA has triggered significant changes in the Canadian political landscape. Initial pressures contributed to the resignation of Prime Minister Trudeau in January 2025, who has led his party and Canada for almost a decade.[12]

The governing Liberal Party elected new leader Mark Carney – an experienced leader of international banking institutions with no political experience.[13]

Carney was sworn in as Prime Minister on 14/03/25, and immediately prioritised international trips to France and the United Kingdom to begin efforts to strengthen relationships outside of north America.[14,15,16]

On 23/03/25 Carney announced a snap general election on 28/04/25.[17]



24/03/25

Expansive media attention and scrutiny has been directed at the US government since a media organisation reported on a US government data breach involving their editor being added to a Signal group chat named 'Houthi PC small group'.[18]

The group was subsequently confirmed as involving 18 of the US government's senior members and security advisors. The purpose of the group related to consideration of attack planning against Houthi rebels in Yemen and then progress updates on the attacks.

Content shared includes advanced operational information which experienced intelligence, military and security professionals have widely agreed would ordinarily have been graded as classified at the time shared.

After the US government continued to downplay the content shared in the chat, and dispute the credibility of the journalism, a follow-up report was published on 26/03/25 sharing the actual content from 15/03/25 – the day the US government undertook a military attack in Yemen.[19]

What NCC Group are watching at present?

Based on its reporting and investigation, global media organisation Reuters described the UK as 'Russia's public enemy number one'. Drawing on historic narratives around British involvement in European conflict, Russia seeks to portray the UK as a 'warmonger'.

The UK government's assumed role as liaison between the US and Europe during current times of strained relations, continued vocal support for Ukraine and leadership activities towards creating a 'coalition of the willing' for future Ukrainian security are perceived as provocative by Russia.[20]

Whilst the UK is not the only country to receive overt Russian focus currently, warming relations between the US and Russia potentially could cause significant shifts in the threat landscape for the UK and its allies.[21,22]

- On 14/03/2024 Reuters reported information from 3 Russian official sources that internally Britain is now considered Russia's main adversary. The role the UK government has played in bringing together allies and pushing collective opposition against Russia was highlighted. UK Prime Minister Kier Starmer's attempts to act as a bridge between the EU and the US has been received by Moscow as provocative.

Section 5

Quarterly Thematic Output: Zero-Days 2025

To round off the theme of vulnerabilities, we consider potentially the most sensational type of vulnerability: the zero-day. Zero-days are unknown to developers until they are publicly disclosed or become attacked, leaving them zero days to release a patch before it is exploited in the wild.

Zero-days have been increasing over the last couple of years, with significant growth in their discovery in 2024. It is especially timely given the significant impact the exploitation of a zero-day vulnerability recently had in the ransomware landscape.

There were 886 observed ransomware attacks in February, 330 of which were attributed to Cl0p. This is largely the result of exploiting zero-days CVE-2024-50623 and CVE-2024-55956 in Cleo software in late 2024. The bulk release of targeted organisations subsequently inflated the ransomware attacks numbers as a result.

Five Eyes intelligence agencies released advisories in late 2024 highlighting that, for the first time, the most-exploited vulnerabilities of 2023 were zero-days. This is a shift from 2022 and previous years when zero-days represented less than 50% of the most-exploited vulnerabilities of the year.

In late 2024, Ollie Whitehouse, the Chief Technology Officer at the UK's National Cyber Security Centre (NCSC) stated, "more routine initial exploitation of zero-day vulnerabilities represents the new normal which should concern end-user organisations and vendors alike as malicious actors seek to infiltrate networks."[23]

Insights from the Zero-Day Vulnerability Database suggests that zero-days have increased rapidly compared to the same time last year.

2025 so far has seen 35 zero-days, an increase of 12 over the 23 observed in Q1 2024, a rise of 52%.[24] The vendor most affected by the increase in zero-days is Microsoft, who have been victim to more than 34% of all exploited zero-days so far in 2025.[25]

They also represent the most affected vendor amongst NCC Group's TI Alerts, with 19 CVEs of the 97 total we have alerted on this quarter.

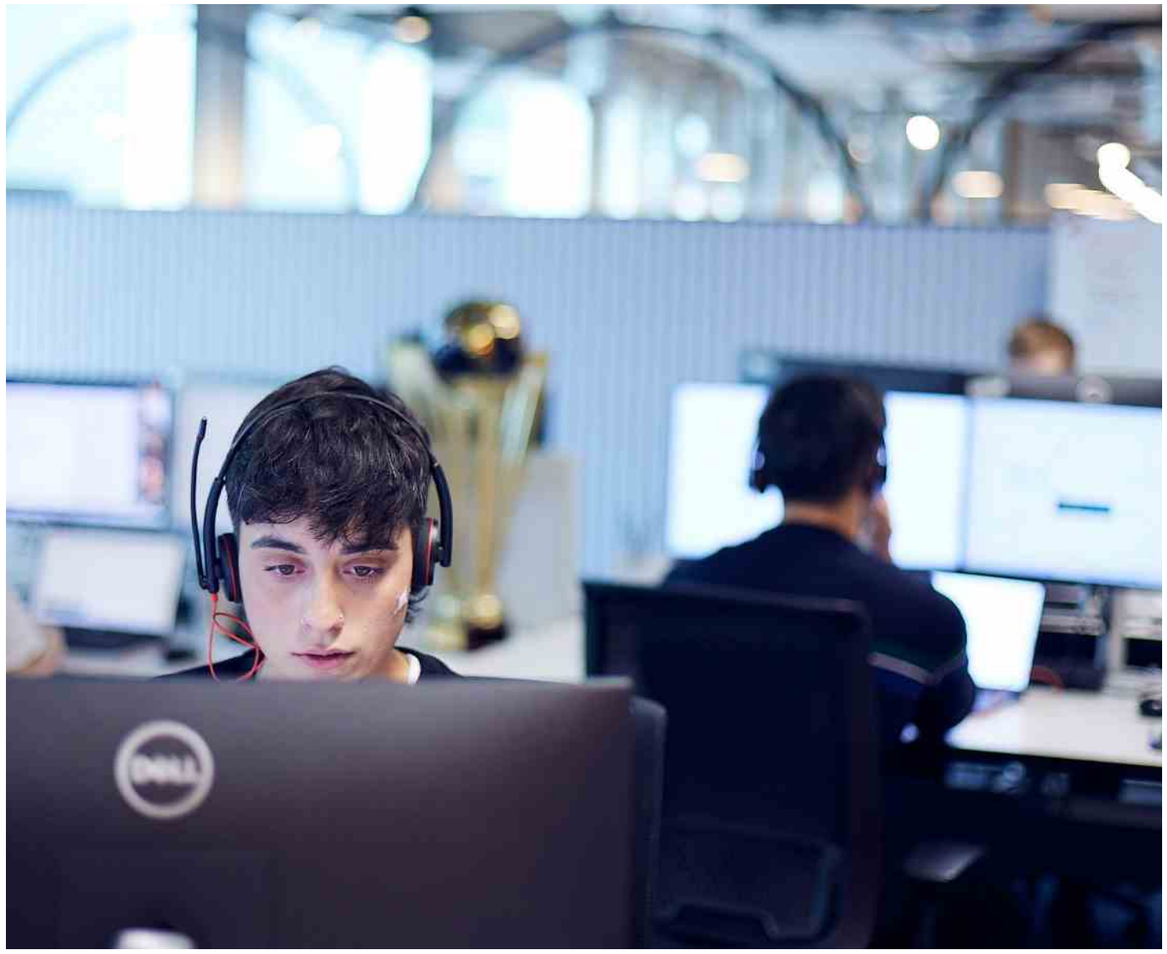
The full versions of our spotlight, quarterly thematic output, and emerging cyber security trend research can be viewed in our Premium Threat Pulse.

This is available to Managed Service clients and those that purchase our Intelligence Subscription Service. If you are interested in key insights and explorations on the current threat and geopolitical landscape, look no further than our research insights.

These will provide you with an in-depth view of pertinent topics from AI, emerging threat actors, nation-state activity, and more.

Sign up here

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