
ncc group
FOX IT
part of ncc group
Cyber Threat Intelligence Report
Review of April 2026

Contents

Section 1
Executive Summary

For April's edition of the Threat Pulse, there were 748 recorded ransomware listings, with the Industrials sector being the most targeted, consistent with previous reporting periods. Despite the relatively modest decline in numbers compared to March, 2026 continues to show a higher baseline than that observed in 2025. The sustained elevated level of activity is assessed to be partially driven by the proliferation of Ransomware-as-a-Service (RaaS) operations, which have reduced the entry barriers for threat actors.

While Qilin remained the most prolific ransomware operation, The Gentlemen rose to prominence as the second most active group, accounting for 10% of observed victim listings. Given its expanding market presence and growing operational profile within the threat landscape, this month's Ransomware Spotlight focuses on The Gentlemen's Ransomware-as-a-Service (RaaS) operation. The analysis highlights affiliate use of SystemBC, demonstrating the increasingly interconnected ransomware ecosystem, where threat actors leverage shared tooling, established access mechanisms, and repeatable intrusion methodologies. The group's rapid growth in early 2026, combined with sophisticated proxy infrastructure and obfuscation techniques, suggests organisations should expect faster intrusion cycles and reduced dwell times before encryption deployment.

April's Geopolitical Developments section discusses, among other key developments, China's expanded supply chain security regulations and the renewed strategic importance of the Artemis programme. These developments are likely to drive increased nation-state cyber activity focused on supply chain compromise and intelligence collection operations targeting a wide range of organisations.

Finally, this month's Emerging Cyber Security Trend section explores the potential implications of Anthropic's Claude Mythos on the cyber threat landscape. While Mythos appears to mark a shift in AI-assisted vulnerability discovery and exploitation, its real-world impact remains unclear due to restricted access and limitations surrounding its operational effectiveness. Even so, the model is likely to accelerate the identification and weaponisation of existing weaknesses. Organisations should therefore adopt continuous, proactive vulnerability and attack surface management practices to keep pace with evolving AI-enabled cyber threats.

Section 2

Ransomware Key Statistics: April 2026

7%

Global ransomware attacks decreased by 7% in April 2026

28%

Industrials accounted for 28% of ransomware attacks in April 2026

14%

Qilin was responsible for 14% of attacks in April 2026

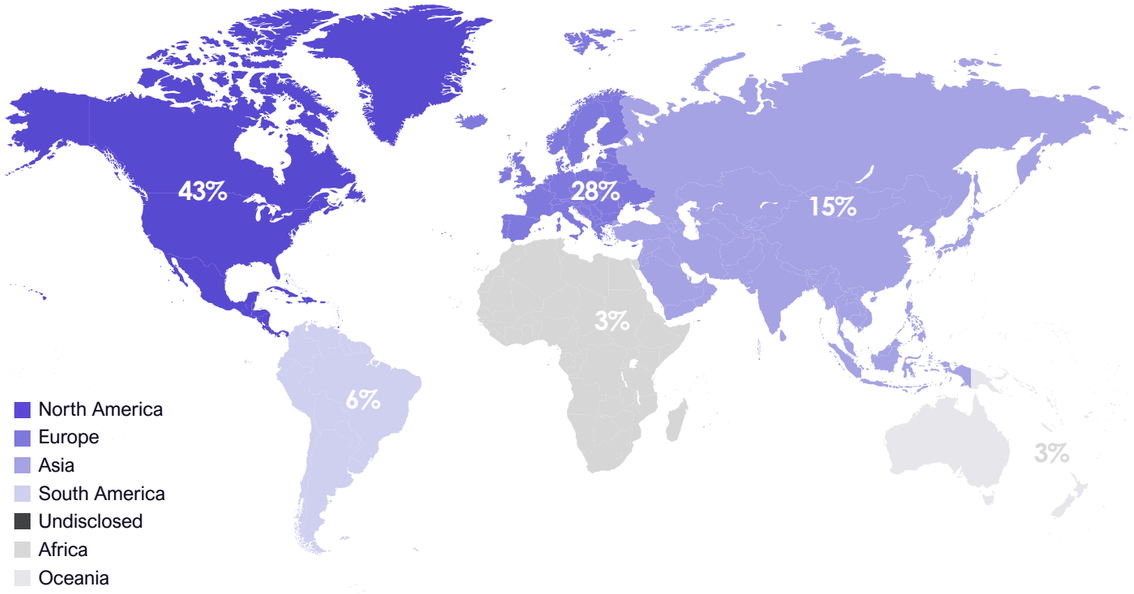


Figure 1 Ransomware Attacks by Region – April 2026

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

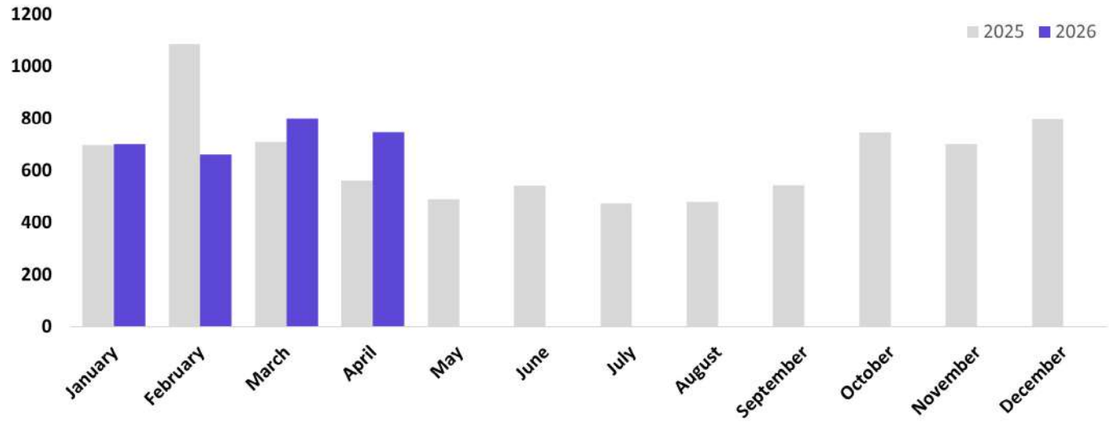


Figure 2 Ransomware Attacks by Month 2025 - 2026

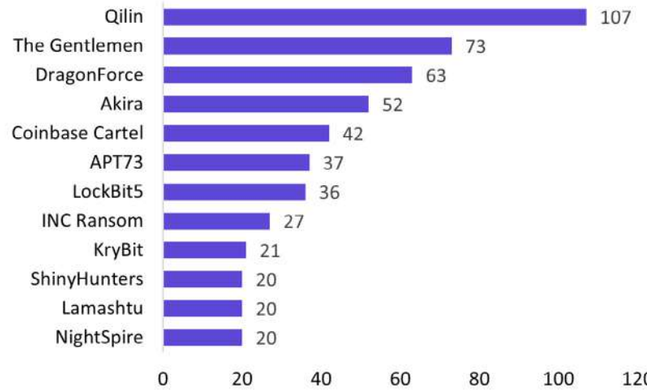


Figure 3 Top Threat Actors – April 2026

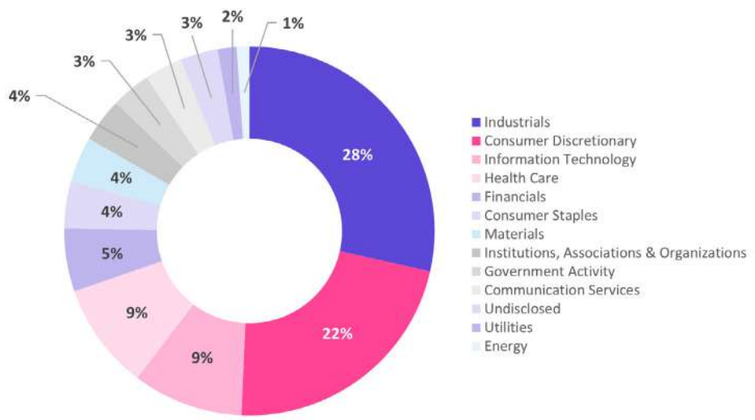


Figure 4 Top Targeted Sectors – April 2026

Key events

01/04/2026
Die Linke

Qilin added the German political party Die Linke to its data leak site, claiming to have stolen around 1.5 TB of internal data, including sensitive communications and administrative files. While the party acknowledged the cyber incident, it did not confirm the scope of the breach.

06/04/2026
Winona County

Winona County, Minnesota suffered a ransomware-related cyberattack that disrupted county operations and forced multiple systems offline. Later reporting linked the incident to the Interlock ransomware group, which claimed to have stolen county data and later allegedly leaked some information online.

06/04/2026
Adaptavist Group

The Gentlemen ransomware group claimed an attack on Adaptavist Group LTD, alleging data theft. Adaptavist later confirmed unauthorised access but disputed claims that sensitive customer or production data was compromised.

Section 3

Ransomware Spotlight: The Gentlemen's RaaS and the role of SystemBC in scaling enterprise intrusions

This report examines the rapid growth of The Gentlemen's ransomware-as-a-service (RaaS) ecosystem in early 2026 and highlights how SystemBC signals increasing affiliate sophistication in human-operated attacks. Since mid-2025, the group has expanded, adopting multi-platform encryption and double extortion, while ranking among the most active groups in Q1 2026.

A key development is that at least one affiliate used SystemBC, a proxy and backdoor tool linked to human-operated ransomware. Check Point's DFIR team linked this to a SystemBC command-and-control server connected to a botnet of over 1,570 victims, largely in corporate environments. This analysis explores what these changes reveal about affiliate maturity, how SystemBC improves attack effectiveness, and what defenders should prioritise to reduce the risk of widespread encryption and disruption.

The Gentlemen has quickly shifted from an emerging threat to a highly active RaaS operation. Despite first appearing in July 2025, the group demonstrates technical maturity typically associated with more established ransomware groups, suggesting experienced operators and potential overlap with other ransomware ecosystems.[1] By April 2026, The Gentlemen has recorded 73 victims, totalling 231 so far in 2026, underscoring its growing impact. The group operates a double-extortion model and supports a wide range of platforms including Windows, Linux, NAS, BSD, and VMware ESXi, making it well suited to enterprise environments. Its use of XChaCha20 and Curve25519 encryption indicates a technically advanced toolkit capable of fast, scalable encryption, and secure key management.[2]

The Gentlemen operates globally and increasingly appears in successful attacks across multiple industries. It primarily targets Industrials, Consumer Discretionary, and IT sectors, with notable victims including Synergy France, UK Electronics, and Equity Life. Targeting is opportunistic and driven by affiliate access rather than ideology, reinforcing its role as a financially motivated RaaS operation.[3]

While Europe (especially the UK and Germany) and the US are most affected, attacks focus on organisations with vulnerable internet-facing infrastructure regardless of location.

SystemBC and the industrialisation of affiliate-led intrusions

Recent reporting highlights the use of SystemBC by The Gentlemen's affiliate, with infrastructure revealing a botnet exceeding 1,500 compromised hosts.[4] SystemBC allows infected systems to act as SOCKS5 proxies, enabling attackers to route traffic through legitimate networks, masking C2 activity and complicating detection.[5] This proxy capability enhances lateral movement and internal pivoting, allowing operators to navigate segmented networks without depending on exposed external infrastructure. In combination with RaaS scalability, this reflects a shift from isolated attacks to repeatable, industrialised intrusion models accessible to a wider affiliate base.

SystemBC's modular design also supports payload staging, enabling the delivery of additional tools after initial compromise. This increases stealth and resilience while allowing deeper network penetration before ransomware deployment. The scale of infections linked to SystemBC suggests much of this activity occurs earlier in the intrusion lifecycle, such as initial access or credential harvesting, stages that are less visible in public reporting. The discovery of SystemBC during an incident response investigation suggests it is being used, or potentially trialled, as part of an affiliate's post exploitation workflow. It also may reflect the tooling preference of a specific affiliate rather than a standard component of The Gentlemen's core operations. Reporting showed that an affiliate operated with high privileges, conducted remote execution, attempted to establish SystemBC for covert tunnelling and movement, and aimed to enable rapid, large scale ransomware deployment.

Enterprise attack chain, detection challenges, and defensive implications

The Gentlemen follows an enterprise-focused chain beginning with initial access, via vulnerable internet-facing services or stolen credentials. Analysis suggests The Gentlemen can adapt and change tactics during an attack, such as manipulating GPOs, compromising privileged accounts, and using custom methods to bypass endpoint protections.[6]

Deploying ransomware via GPOs or central management tools enables near-simultaneous execution across domain-joined systems, drastically reducing defenders' response time and increasing the risk of large-scale disruption. The use of proxies like SystemBC further complicates defence by masking attacker traffic, allowing covert lateral movement and tool deployment while obscuring the true source of activity. This increases the possibility of widespread compromise, credential theft, and potential re-entry, ultimately prolonging recovery and complicating remediation due to missed internal pivot points.

SystemBC amplifies these challenges by enabling stealthy movement and hidden payload delivery, increasing the chance that compromised systems remain undetected.

Combined with The Gentlemen's ability to adapt tactics across different environments, this highlights the limitations of static defences. The Gentlemen's ability to adjust tactics for different security setups also shows that one-time fixes are not enough; defenders should expect attackers to adapt, use backup methods, and try again after being blocked.

Mitigations and recommendations

Defensive strategies should shift from responding to static ransomware signatures to identifying behaviours that enable ransomware attacks. Organisations should focus on early-stage behavioural indicators, such as privilege escalation, lateral movement and domain control as these occur before encryption and provide the best opportunity to prevent significant business impact.[7]

Organisations should focus on controls that break The Gentlemen's attack chain, especially steps that reduce the likelihood of domain-wide deployment via GPO and limit hidden tunnelling via SystemBC. This includes enforcing MFA for remote and admin access, limiting domain admin use, and setting strong change controls for any GPO changes.[8] Detection of proxy or backdoor activity should be improved such as SOCKS-style tunnelling, and outbound connections to proxy traffic.[9] Limiting lateral movement through network segmentation, restricting SMB/RPC, and monitoring administrative activity can further reduce risk.[10] Organisations should maintain secure, offline backups and regularly test the restoration processes as these attacks leave little time for a reactive response.

Final thoughts

The link between The Gentlemen and SystemBC shows that ransomware risk now comes from entire ecosystems with affiliates, shared tools, and repeatable attack methods, not just from individual ransomware programmes. While RaaS has existed for years, the speed, scale, and operational maturity observed in early 2026 mark a significant evolution.

What's most notable is not just the technical skills, but the attackers' objective to maintain persistence, work quickly, and use speed and scale to their advantage. This shifts the main defensive question from 'Can we stop ransomware?' to 'Can we reliably spot and disrupt the steps that lead to ransomware?'.

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.

07/04/2026

In China, new regulations regarding commercial trade activities were published on 7th and 13th April, effective immediately.[11] Justified on national and economic security grounds, the regulations consolidate and extend existing controls on import and export activities, and multinational companies operating within China. Key features of regulations, named 'Provisions on Industrial and Supply Chain Security' and the 'Provisions on Countering Foreign Unlawful Extraterritorial Jurisdiction' include:[12]:

- Extension of the potential triggers for the Chinese state to effect retaliatory countermeasures from the actions of foreign states (i.e. new tariffs, export controls or sanctions measures) to the actions of individual foreign companies which 'interrupts normal transactions' or introduces 'discriminatory measures' capable of causing 'substantial harm' to China's supply chain security.
- Introduction of a ban on foreign entities from conducting data collection or investigations on or within China in relation to supply chains (i.e. regulatory requirements, journalistic investigation, threat and risk analysis).
- New duty imposed on all Chinese entities and individuals located within China to comply with any related countermeasures imposed following an investigation under these regulations. Foreign individuals or companies operating within China are not exempt.

Whilst framed as policy changes to mitigate against risks associated with China's supply chains and industrial sector, analysts assess them as a response to specific global (geopolitically driven) trends. Specifically, imposing controls on exports of advanced technology to China, reducing dependencies on China for critical supply chains, exerting economic pressure indirectly on nations such as Iran and Russia through sanctioning China, and increasing regulatory demands (and broader pressure) on European companies to demonstrate that their manufacturing supply chains do not include human rights abuses such as forced labour.[13,14,15]

So what?

- Multinational companies operating within China will be concerned over the commercial and legal implications of falling within the scope of these broad regulatory measures, and subsequently attracting countermeasures imposed by the Chinese state. The cyber security implications are unclear but potentially significant. Multinational companies operating within China are generally understood to be exposed to additional cyber security risks around espionage and IP theft. The regulations are framed as necessary for the protection of national interests and security; it is reasonable to infer that any related 'investigation' would be supported by the most powerful investigative tools. Under new powers, network intrusions or data breaches by Chinese nation-state threat actors may be framed as lawful exercise of 'investigations', rather than covert (or at least unacknowledged) espionage/ intelligence collection activities.
- Within the legislation, investigations are described in inspections and gathering documentary evidence. In modern, increasingly paperless organisations, this is unlikely to be limited to printed documents, providing valuable opportunities for the reconnaissance and even initial access phases of a cyberattack.

The broad scope of the regulations provides Chinese intelligence agencies with effective cover to gather intelligence against organisations of wider interest to the Chinese state with an identifiable footprint within China. Parallel activities to require replacement of foreign software (including cyber security tools) with Chinese alternatives may skew cyber espionage opportunities towards Chinese threat actors.[16]

- Introduction of these measures coincides with US-initiated delays in the planned summit between President Trump and China's leader Xi Jinping and a perceived uptick in Chinese assertion of its interests in multiple areas including; Taiwan[17,18] the South China Sea[19,20] seabed mining[21], public threats of retaliation against the EU[22], and their relationship with North Korea[23]. During the same period, the US and international community have been focused on navigating the impact of Israel and the US war with Iran. It is inferred that China perceives opportunity in the ongoing geopolitical environment. Securing advantage requires an intelligence-led approach via methods including cyber espionage. Defenders in proximity to organisations involved in assessing and informing governments and corporate entities on their response options, in any area China is asserting their interests, may experience increased frequency and breadth of cyberattacks by China-linked threat actors with overlapping objectives.

10/04/2026

NASA successfully completed its second mission in the Artemis programme to orbit the Moon with a four-member crew on 10th April.[24] The 10-day mission represents the first human visit to the Moon since NASA's Apollo programme ended in 1972, the deepest humans have entered space in history, and a necessary step towards astronauts physically returning to the surface of the Moon by 2028.[25] Goals of the Artemis programme include building a 'long-term US presence on the Moon over the next decade and beyond', and supporting broader aspirations in relation to the planet Mars.[26]

So what?

- The Artemis programme is dependent on multiple private sector contracts and collaborations with organisations including Lockheed Martin, Boeing, Northrop Grumman, Elon Musk's SpaceX, and Jeff Bezos' Blue Origin. These companies present high value targets for threat actors seeking to acquire sensitive operational and proprietary information. Complex dependencies extend the threat and potential attack and pivot points throughout specialist and dual use supply chains, support service supply chains, and related government departments. In addition, the implications of the Artemis programme for defence and security, intelligence sharing between Five-Eyes, and wider goals of interoperability and secure communications systems between military allies are anticipated to require a level of intelligence and knowledge sharing, as well as deconfliction. Organisations not involved directly in space programme delivery, but with overlapping or dependent interests may hold communications or information of interest to rival nations and be perceived as softer targets for compromise.

- Since the 1980s, space programmes have typically been focused on space stations, satellite technologies, and developing multi-trip rockets. As in the Cold War period, geopolitical competition is now driving the race to achieve key space milestones first. The potential for weaponisation and targeting of satellite technology in conflict (including within the domain of space), and competition to control natural resources represent only some of the factors motivating the US Artemis programme to return to[27], and establish a presence on the Moon. China's advancing space programme seeks to land astronauts on the Moon[28,29]. As a high value Chinese strategic interest, organisations involved in the Artemis programme should anticipate attempted compromise from the most advanced of Chinese nation-state capabilities (as well as insider threats) for both IP theft, espionage, and where relevant pre-positioning.[30]

- Applied in the broadest terms, the current 'space race' inferred to motivate espionage, IP theft activities, and potentially even destructive attacks, should not be assessed as limited to China and the US. Numerous other well-resourced countries (and private companies) are pursuing high-stakes interests dependent on the domain of space; including but not exclusive to India, Japan, Israel, South Korea, UAE, Russia, Iran, and North Korea.[31,32] Defenders should avoid being too narrow in their assessments of potential threats.

12/04/2026

After 13 years leading Hungary, Viktor Orban's political party Fidesz lost national elections held on 12th April.[33] With record levels of voter turnout, centre-right party Tisza (Respect and Freedom) achieved a two-thirds supermajority in the Hungarian parliament. The results occurred in the context of significant efforts by Orban's government to disadvantage other parties, and support of Orban's campaign by the US and Russia.[34,35] Tisza ran on a positive platform, rejecting fear and nationalist based messaging, and pledging to address existing corruption to improve public services and the national economy.

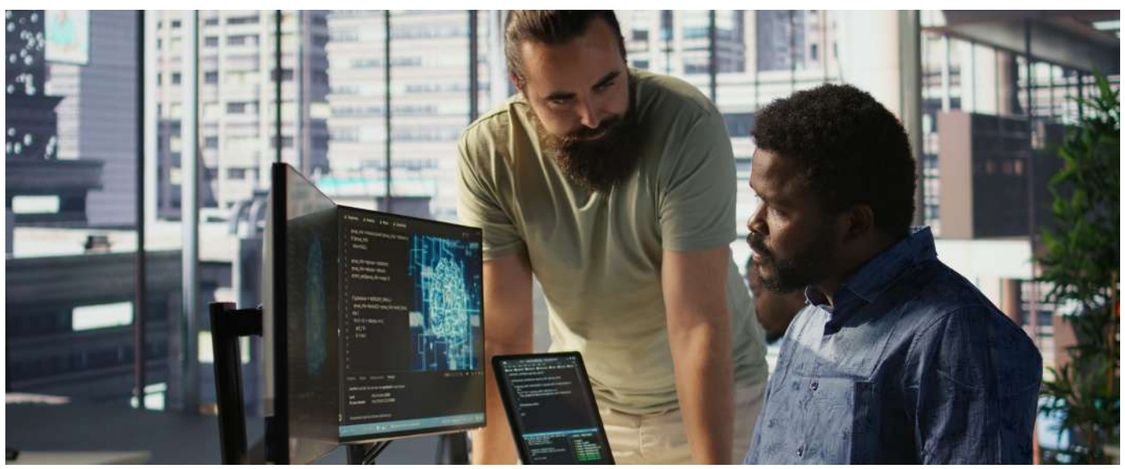
Despite not being due to be sworn in as prime minister until 9th May, Tisza leader Peter Magyar has already begun negotiating over the necessary changes required to release EU funding frozen in 2022 over concerns regarding corruption and erosion of the rule of law under Orban's government.[36,37] Tisza's parliamentary majority provides the new Hungarian government with sufficient political power to reverse changes made by Orban's government at pace.

So what?

- Already, the election result has had significant implications for Russia's war with Ukraine, a notable driver for the cyber threat landscape. Hungary's veto to a €90 billion EU loan to Ukraine, previously in place since February 2026, has been lifted.[38] The loan is intended to meet two thirds of Ukraine's fiscal needs for 2 years. The timing is particularly significant, as Ukraine had expected to run out of funding by June 2026. Approximately €56 billion is anticipated to be used for military spending. Securing the funding reduces Russia's leverage in shaping the terms of any future peace agreement.

- Beyond Ukraine, the result is a setback to Russia's broader European interests. Orban was a valuable strategic ally of Russia: as a member state, Orban had an ability to undermine EU goals from within. Publicly, Russia declared respect for the result and that it sees a pragmatic relationship with the new government.[39] In practice, the Tisza government is not anticipated to be actively opposed to Russian interests, but delivering their mandate will inevitably require disrupting Russian influence in Hungarian political and civic infrastructure. Efforts will need to be balanced with dependencies on Russia for energy. Organisations with links to Hungarian foreign and economic policy, particularly EU members, may experience increased exposure to Russian cyber capabilities seeking short-to-medium term intelligence.

- The potential geopolitical impact of national elections in countries retaining legitimate vote counting capabilities reinforces the value of influence operations. Election outcomes can determine how engaged a country is in seeking membership or delivering EU and/or NATO strategic goals. Each nation's election cycles present an opportunity for capable nations to skew public voting patterns in their favour; overtly as the US did in Hungary, or more covertly as is typically associated with Russian and Chinese regimes. Whilst highly significant countries may attract sustained attention, limited (and specialist) resources often move from country to country with the election calendar. In 2026, Cyprus, Estonia, Kosovo, Malta, Armenia, Sweden, Russia, Czechia, and Kazakhstan have planned national elections. Due to recent political fragmentation, Romania may call an early election.[40]



Section 5

Emerging Cyber Security Trend: Is Claude Mythos a game changer or just marketing hype?

Since the start of 2026, generative AI has come up in almost every monthly Pulse, and for good reason. That trend continued in April 2026, marked by the emergence of Claude Mythos. On 7th April 2026, Anthropic announced its new and most capable LLM, Claude Mythos. Anthropic claims the model can not only identify thousands of zero-days across major operating systems and browsers, but also autonomously develop exploit chains.[41] A preview version of Claude Mythos has been released to a limited but growing group of organisations through Project Glasswing, a cyber security initiative focused on securing critical systems using Anthropic's frontier model.[42]

Unsurprisingly, the announcement sparked a debate, with some suggesting this model could mark the end of cyber security as we know it. Sceptics, on the other hand, have framed the announcement as marketing hype, arguing that Mythos may not be as capable as it is portrayed. In the meantime, the model remains unavailable to the public and the closest we can get to the truth, likely lies somewhere between these two claims.

Hype vs. reality

As of today, the claim that Mythos represents a capability shift rests largely on Anthropic's data and tests conducted in simulated environments. The most notable of these is a technical assessment published by the UK AI Security Institute (AISI), a research organisation within the UK government's Department for Science, Innovation and Technology, confirming that Mythos was the first AI model to complete an end-to-end simulated corporate network attack challenge. However, the limitations of these simulated tests were acknowledged by AISI, who noted that the evaluation of Mythos was carried out in controlled lab settings.

The test environment lacked defensive security tooling that would typically trigger alerts. In the words of AISI, their test cannot confirm "whether Mythos Preview would be able to attack well-defended systems", pointing to the challenges of drawing comparisons with real-world scenarios.[43]

With access to Claude Mythos remaining restricted, the full implications for the future of cyber security remain uncertain. Early reporting suggests that Mythos represents a meaningful capability shift in AI-assisted vulnerability research. Looking ahead, AI-assisted cyber operations are expected to evolve beyond LLM-supported reconnaissance and deepfakes to autonomous, agentic kill chains. However, as noted by a Technical Director at NCC Group, this development is better understood as "an evolution, not a revolution".[44] Rather than fundamentally changing how cyberattacks are carried out, the shift appears to lie in enhanced reach and velocity of offensive capabilities.

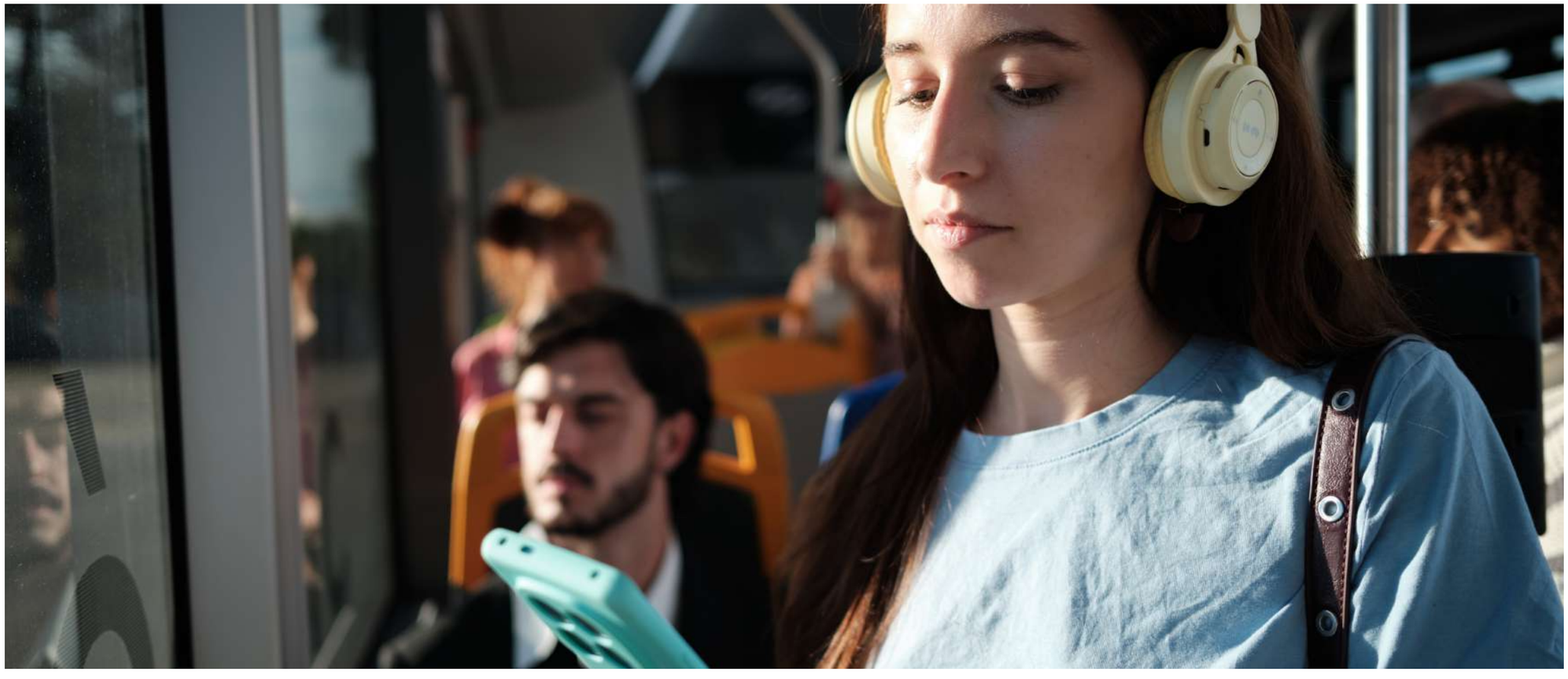
Claude Mythos does not represent an entirely novel breakthrough. Current AI systems do not independently originate research in the way human experts do. Their capabilities are primarily derived from learning, recombining, and scaling existing human knowledge. As such, AI could accelerate threat actors' ability to compromise vulnerable endpoints, with organisations that fall short of basic security practices facing a heightened level of risk.

Defensive posture in the era of AI-assisted vulnerability research

The democratisation of this AI capability, through access to Mythos or the emergence of an equivalent model, is likely to put more pressure on organisations to rethink their defensive model. With vulnerability alert volumes rising, defenders must shift from periodic to continuous vulnerability and attack surface management. In an environment shaped by AI-driven vulnerability discovery and exploitation, traditional remediation cycles are becoming increasingly ineffective as disclosure-to-exploitation timelines continue to compress towards near-zero intervals. Patching prioritisation models must also move beyond static severity scores and account for specific organisational contexts.

Each security environment presents a unique risk profile, shaped by factors such as internet exposure, network architecture, supply chain dependencies, authenticated attack paths, and threat profile. Context-aware remediation strategies can therefore help organisations manage the expected flood of findings by prioritising those that pose the greatest risk.

More broadly, organisations need to embrace structural change by shifting from reactive practices to proactive, secure-by-design approaches that eliminate risks at their source. Although this approach may drive up implementation costs and potentially slow innovation, these trade-offs must be weighed against the long-term benefits of stronger, more resilient cyber security architecture. At the same time, the inherently dual-use nature of AI technology also offers defensive opportunities. The same capabilities driving offensive operations can be leveraged for code security testing, alert triage, and automated response mechanisms that help contain or remediate threats. Such measures may allow organisations to better keep pace with AI-driven cyber threats.



About NCC Group

People powered, tech-enabled cyber resilence

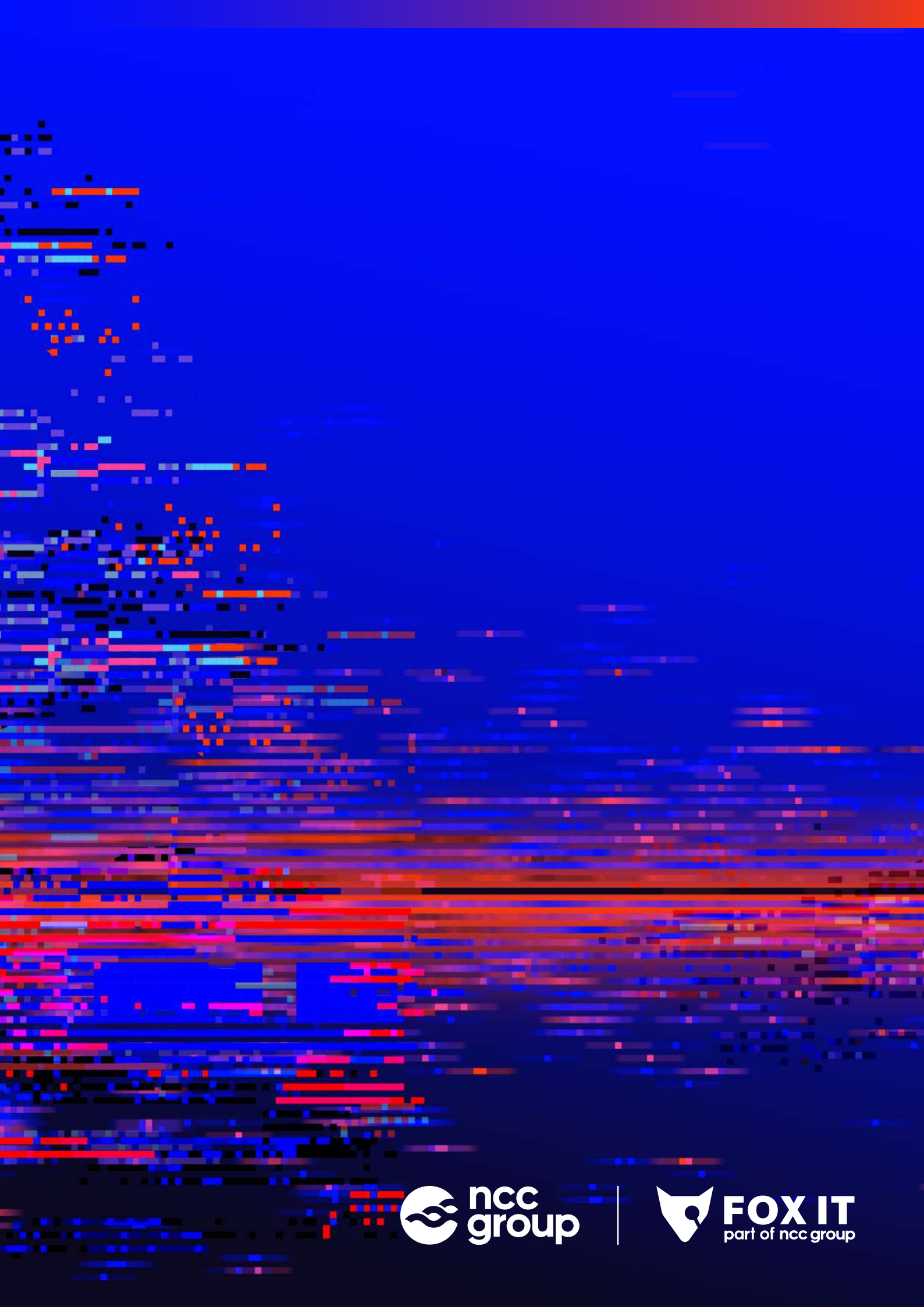
We're a people powered, tech-enabled global cyber security and resilience company with over 2,200 colleagues around the world.

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

Fox-IT:
+31 (0)88 369 23 78
fox@fox-it.com
www.fox-it.com


ncc group
FOX IT
part of ncc group