ncc group | FOX IT part of ncc group

Cyber Threat Intelligence Report

Review of February 2026

Contents

Section 1
Executive Summary

For February's edition of the Threat Pulse, there were 635 recorded ransomware listings, with the Industrials sector being the most targeted, consistent with previous reporting patterns. Qilin remains the most active ransomware group, with 15% of recorded listings. The emergence of The Gentlemen group among the top three most active threat actors is notable as it demonstrates how a relatively new group can scale operations rapidly.

Beyond the numbers, this month's Ransomware Spotlight explores the newly identified Reynolds ransomware group. While the group's reported activity remains limited, its integration of a Bring-Your-Own-Vulnerable-Driver (BYOVD) component within its payload is uncommon and warrants attention. Reynolds' innovation is indicative of attempts to increase their competitiveness.

Geopolitical Developments for this month highlights the increasing cyber risk globally as a result of the escalating geopolitical tensions and heightened economic competition. Key developments include US pressure to remove Chinese operators from Panama Canal ports and US and Israeli strikes on Iran. Cyber risk, including espionage operations and retaliatory threat activity targeting entities linked to Western governments, is likely to increase as a result of these events.

Finally, the Emerging Cyber Security Trend for this month examines the inherent security risks associated with Low-code/No-Code (LCNC) AI agents and automation platforms. The effectiveness of these tools often relies on highly permissive integrations while lowering the technical barrier to use, a combination that introduces amplified security risks that organisations should monitor closely.

Section 2

Ransomware Statistics: February 2026

8%

Global ransomware attacks decreased by 8% in February 2026

31%

Industrials accounted for 31% of ransomware attacks in February 2026

15%

Qilin was responsible for 15% of attacks in February 2026

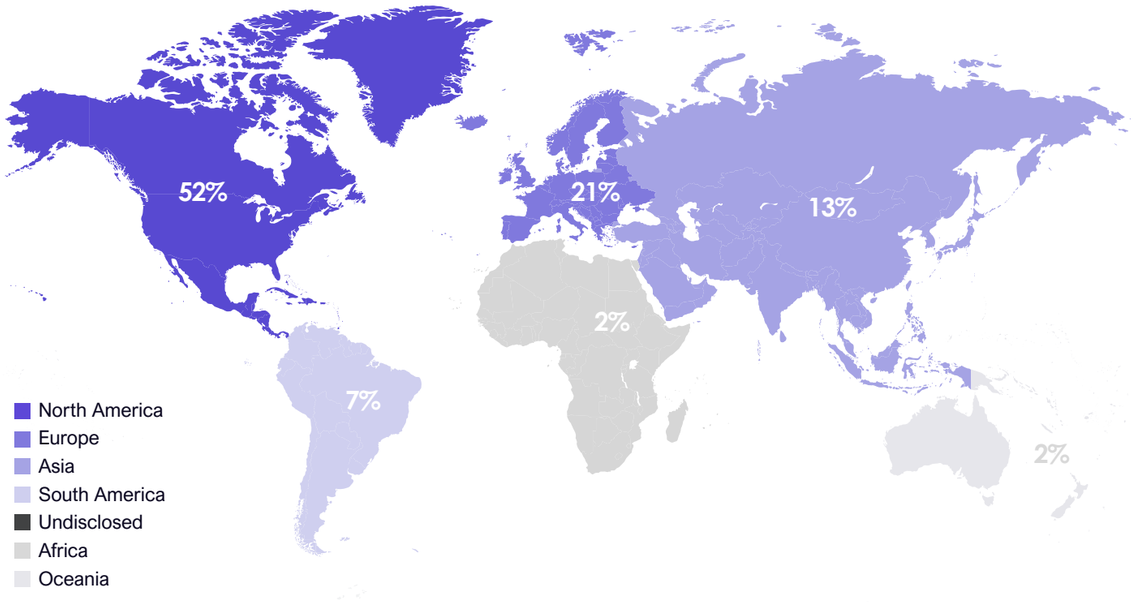


Figure 1 Ransomware Attacks by Region – February 2026

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

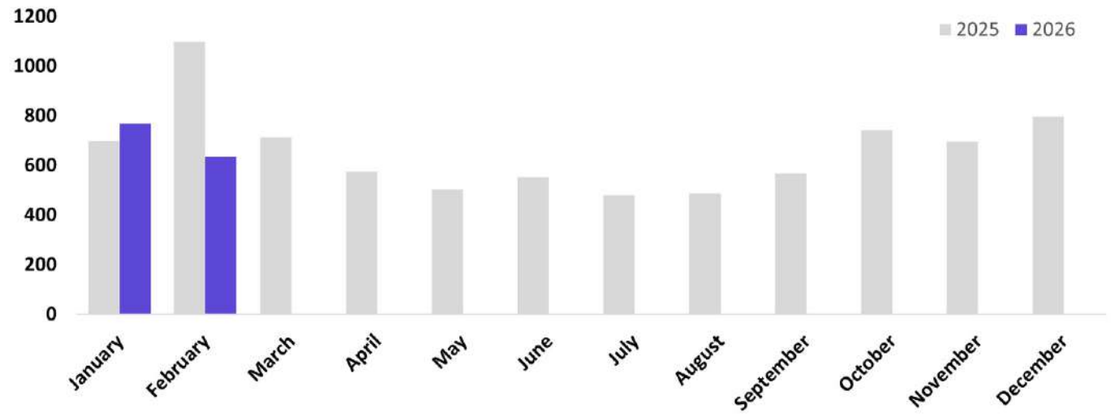


Figure 2 Ransomware Attacks by Month 2025 - 2026

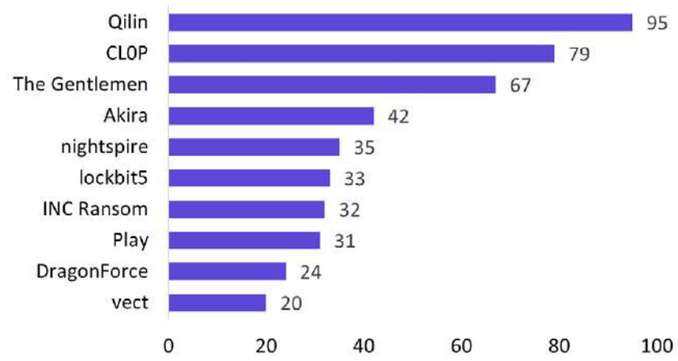


Figure 3 Top Threat Actors – February 2026

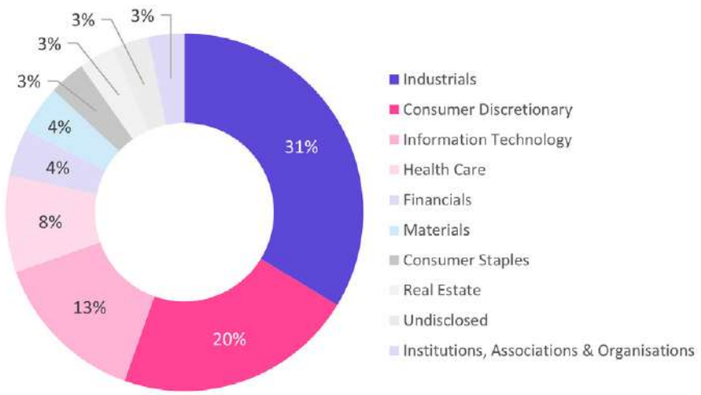


Figure 4 Top Targeted Sectors – February 2026

Key Events

02/02/2026

La Sapienza University

Rome's La Sapienza University was hit by ransomware (BabLock) linked to Russian cybercrime group Femwar02. Major IT systems were knocked offline for days, disrupting services and forcing recovery via backups.

05/02/2026

Conpet S.A.

Romanian's national oil operator Conpet was hit by a cyberattack by Qilin. It disrupted parts of its technology infrastructure and knocked its website offline, while oil transport operations were not affected.

20/02/2026

BeyondTrust

Attackers have been actively exploiting a critical BeyondTrust remote access vulnerability to gain unauthorisedcontrol, deploy malicious tools and carry out ransomware related intrusions against organisations.

Section 3

Ransomware Spotlight: Reynolds Ransomware

On the 5th of February 2026, a joint report by Symantec and Carbon Black disclosed the details of a threat activity initially attributed to Black Basta. However, the report was later updated to confirm the payload was a new ransomware variant named Reynolds.[1] The report noted that the malware includes a built-in Bring-Your-Own-Vulnerable-Driver (BYOVD) component within its primary executable. The ransomware abuses a vulnerable Windows driver to disable security tools and evade detection before encrypting systems. As of this writing, publicly available information on the Reynolds ransomware campaign remains limited.

Embedded BYOVD for Defence Evasion

Bring-Your-Own-Vulnerable-Driver (BYOVD) has been used increasingly by threat actors due to its reliability and stealthiness. Attackers use BYOVD because it leverages the inherent trust given by the operating system to legitimate kernel-mode drivers.

Since these drivers are signed, the operating system loads them without suspicion. It does not recognise that they are vulnerable, enabling actors to execute malicious actions with elevated privileges.

The Reynolds ransomware variant is a notable shift in how threat actors use BYOVD. Instead of relying on a separate EDR-killer component, Reynolds embeds the vulnerable NsecSoft NSecKrnl driver directly within the ransomware payload to impair the target's defences.

The NSecKrnl driver contains a known medium-severity vulnerability, CVE-2025-68947, that enables attackers to send specially crafted requests to the driver and force it to terminate processes belonging to other users. This includes highly privileged SYSTEM processes and Protected Processes, which are normally shielded from interference.[2] During execution, the Reynolds payload drops the vulnerable NsecSoft NSecKrnl driver and attempts to create an NSecKrnl service. Once loaded, the driver is used to terminate multiple Endpoint Detection and Response (EDR) processes, including, among others, Avast, CrowdStrike Falcon, Palo Alto Networks Cortex XDR, Sophos, and Symantec Endpoint Protection. After disabling these defences, the ransomware payload then appends the '.locked' extension to the files that it encrypts.[3]

Built-in BYOVD: Key Risks and Limitations

Embedding a BYOVD component directly into ransomware provides several operational advantages while simultaneously introducing certain limitations. With the driver packaged inside the payload, the ransomware could disable the security tools immediately after launch, thereby reducing defender reaction times. The lack of a gap between driver drop and payload execution limits defenders' ability to intervene before encryption begins.

Delivering a single combined payload can also reduce the noise in comparison to staging multiple tools. Packaging the vulnerable NSecKrnl driver directly within the ransomware payload makes the attack flow much more straightforward for the operators. By having the vulnerable driver embedded in the ransomware itself, they no longer need to manage a separate BYOVD tool or stage additional files on the target. It reduces the number of steps in the kill chain, resulting in a quieter attack.

This feature likely aims to simplify affiliate deployment and improve operational efficiency. From a commercial perspective, streamlining the required steps is a potential selling point to attract affiliates. The observed activity coincides with reduced ransomware revenues in 2025, despite a rise in publicly reported attacks. The ransomware ecosystem remains competitive, with more than 85 active RaaS operations seeking to strengthen their position through new capabilities and features that increase their advantage.

However, this technique also has real constraints. Loading a vulnerable driver can be blocked by security vendors. Defenders can maintain blocklists of vulnerable drivers, which can prevent driver loading and undermine the attack, putting attackers at a tactical disadvantage by creating a single point of failure.[4] Merging BYOVD with ransomware encryption into one payload risks breaking the entire execution chain once the driver is detected by security software.

Despite these limitations, Reynolds ransomware remains a credible threat. The single-payload design lowers the technical barrier for affiliates, requiring fewer steps and less expertise to deploy effectively against unpatched environments with outdated vulnerable driver blocklists.

Mitigations and Recommendations

Defending against Reynolds ransomware and other ransomware families that abuse Bring-Your-Own-Vulnerable-Driver (BYOVD) techniques requires a layered and proactive approach. To prevent unapproved drivers from loading, organisations should enforce strict driver loading policies, making use of driver-allowlisting so that only approved drivers can be loaded within the environment.

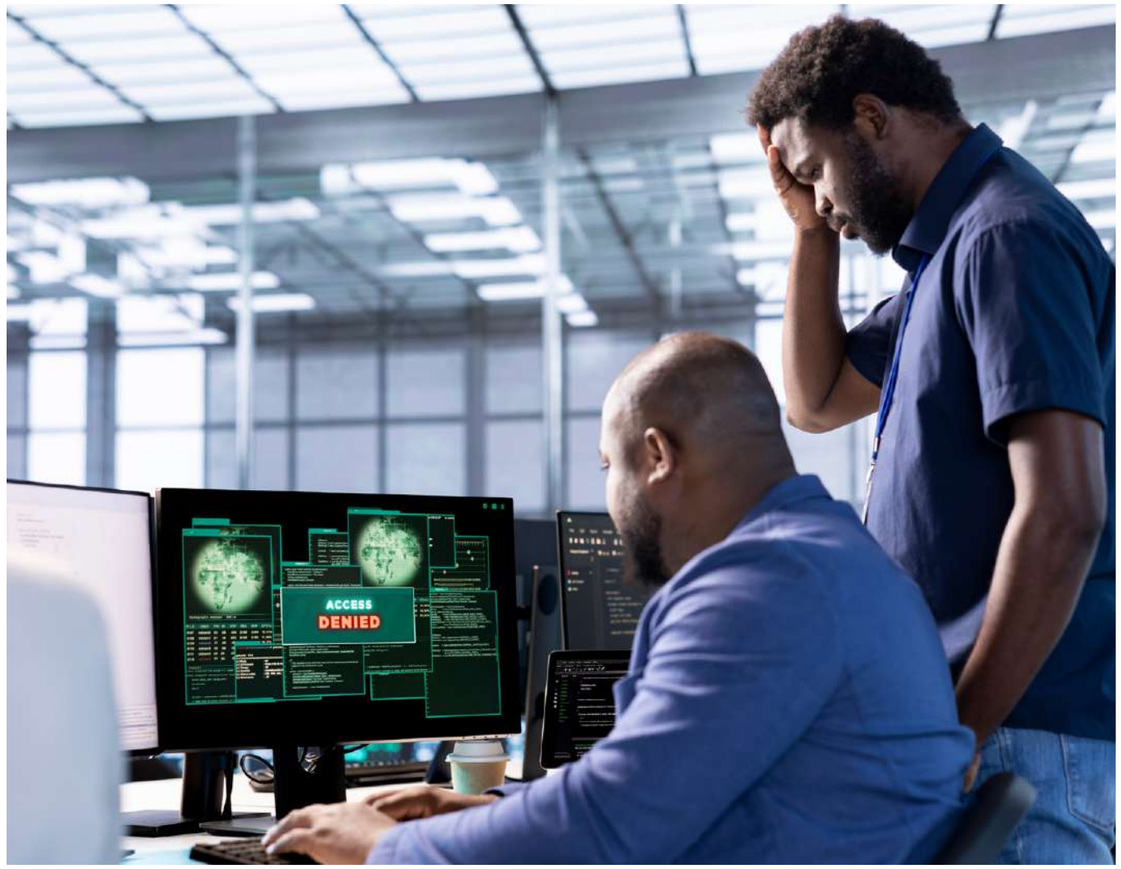
Organisations are advised to leverage threat intelligence feeds to track indicators associated with Reynolds ransomware, including vulnerable driver artifacts and related infrastructure. Integrating these indicators into EDR or XDR platforms can support proactive detection and response.

As with other ransomware threats, organisations should also implement standard defensive measures such as maintaining offline backups, applying timely security patches, and deploying behaviour-based detection mechanisms to reduce the potential impact of an attack.

Final Thoughts

The Reynolds campaign shows how the ransomware landscape continues to evolve as threat actors compete to attract affiliates. Within a highly competitive ransomware ecosystem, groups are increasingly incorporating features that intend to streamline the attack chain and improve the operational efficiency of their products. By embedding a vulnerable driver within the ransomware payload, Reynolds removes operational steps between execution and defence evasion. The consolidated design reduces the window for detecting pre-encryption activity.

While the Reynolds ransomware family shows functional limitations and limited reported activity, it demonstrates the growing use of BYOVD techniques to obtain privileged access with a small operational footprint.



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.

20/02/2026

Via a majority decision, the US Supreme Court ruled against President Trump's administration on 20/02/26 to declare a subsection of US tariffs introduced as unlawful.[5] The court determined that the 1977 International Emergency Economic Powers Act (IEEPA) relied upon by the President did not create a legal basis to impose tariffs. IEEPA-based tariffs include tariffs imposed on China, Canada and Mexico in relation to the fentanyl drug trade in February and March 2025, and individualised 'reciprocal tariffs' imposed on countries with a trade deficit with the USA on 'Liberation Day' (02/04/25).[6] Tariffs imposed using other legal powers remain unaffected.

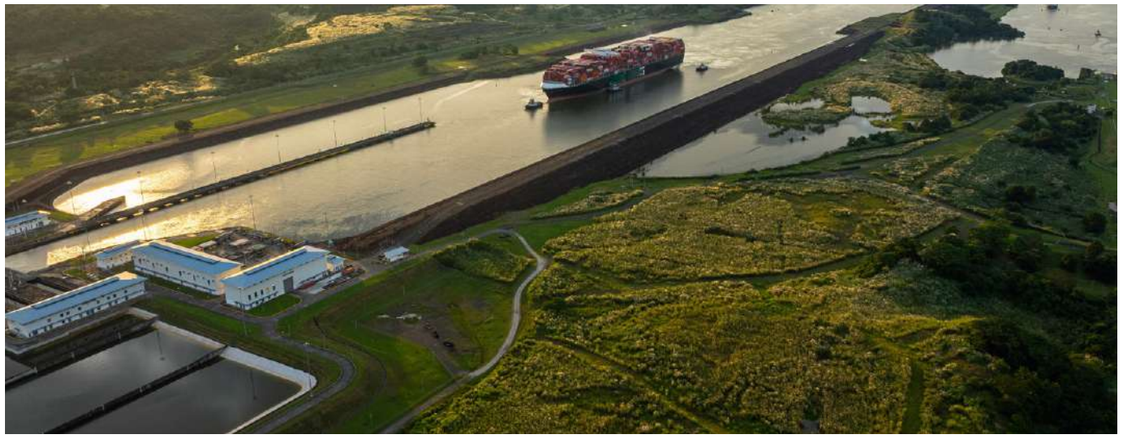
At the time of the ruling, analysts assessed that revenue collected under IEEPA-based tariffs exceeded $175 billion, revenue which appears to be eligible for a refund.[7] The status of trade agreements and broader concessions made by countries seeking to reduce tariff rates against their countries is unknown.[8] President Trump has stated his intention to seek an alternative legal basis for his tariffs, drawing on different legislation to authorise a temporary universal tariff level of 10% for an interim period of 5 months, effective 24/02/26.

IMPLICATIONS:

- The weaponisation of tariffs for revenue generation and as a coercive tool is now well established within President Trump's administration and contributes to high levels of geopolitical tension globally. The current environment of unpredictable change, and the related harm to national interests capable of being caused by tariffs, provide strong drivers for cyber-espionage activity. This effect is most notable in relation to China-linked APTs, due to the trade war which tariffs have triggered and the broader strategic rivalry between the two superpowers. In September 2025, the US House Select Committee on China described persistent efforts to compromise the systems of individuals involved in US-China trade engagements.[9]

  Reconnaissance activities and cyber-attacks by suspected Chinese APTs targeting Latin American government networks involved in trade were reported in February 2026.[10] APT41 and APT31 specifically have been attributed to attacks on organisations capable of influencing trade negotiations.[11,12]

- Outside of nation-state activity, uncertainty and confusion around the cost of global trade with the USA set ideal conditions for social engineering based cyber-crime such as phishing, fraud, and scams using tariff-themed lures. Organisations impacted by changing tariff systems should re-iterate the risks internally, and review mitigations against malicious communications beyond email-based methods to include increasingly prevalent mobile device-based methods using QR-codes, SMS, and messaging apps as vectors. Assisted by AI technology, voice and video-based social engineering also present accidental insider risks where gaps in robust verification processes and controls exist.



23/02/2026

Authorities physically removed personnel of Panama Ports Company (PPC) from ports on the Panama Canal on 23/02/26, following a legal annulment process initiated by the Panamanian government which cancelled PPC's contract to operate container terminals at each end of the canal since 1997.[13,14] PPC is a subsidiary of the Hong Kong-based company CK Hutchison. At the time of the annulment, CK Hutchison was in the process of finalising a broader sale of 43 ports globally to US-led consortium BlackRock, which would have included the 2 ports in Panama.

Panama has issued temporary licences to subsidiaries of Maersk and the Mediterranean Shipping Company (MSC) to operate the former PPC ports, and declared an intention to prevent awarding control of the two ports to a single company in future.

Separately, Panamanian police conducted a search of CK Hutchison locations on 26/02/26, seizing property.[15]

IMPLICATIONS:

- Whilst the legal basis of the annulment decision was based on public interest and the nature of the privileges and exemption awarded to PCC, which were determined as unconstitutional, the case coincides with sustained and significant pressure applied by the USA under President Trump's administration to remove alleged Chinese influence from the canal; which forms a critical part of Western hemisphere trade and strategic infrastructure. The subsequent police investigation into CK Hutchison suggests Panama may perceive (or be experiencing) continued pressure from the USA to create more hostile conditions for China-linked interests in Panama.

- Despite being privately owned, Hong Kong based companies are subject to Chinese national security laws and susceptible to state-influence.[16] Loss of Chinese involvement in the operations of the canal is perceived as a strategic win for the USA, which seeks to dominate in the Western Hemisphere.

- The Chinese government have condemned the activities and warned of 'heavy prices' to pay.[17] The President of Panama was quoted as saying he believed there would be no retaliation due to the dependency the Chinese have on the use of the canal for both energy imports and manufacturing exports. Whilst in the short-to-medium term this may be true, China continues to develop alternative infrastructure to the Panama Canal in Latin America. Pre-positioning activity in Panama's infrastructure may allow China to delay retaliation until a more strategically secure time.

- Although China has the capability and resources to conduct retaliatory destructive cyberattacks on Panama, there are strategic reasons to avoid attributable attacks. Panama's critical infrastructure or proxy interests, or the digital assets of Danish Maersk or Swiss/Italian MSC now operating the terminals, are assessed to be at higher risk of cyber-attacks which present as criminal acts such as ransomware, but may be geopolitically motivated.

28/02/2026

On 28/02/2026, the US and Israel began military strikes against Iran.[18] The attacks followed an extended period of diplomatic activities between the USA and Iran around their nuclear programme, including three rounds of physical negotiations on 5th, 17th, and 26th February.[19,20,21] In parallel, the US increased pressure on Iran through the mobilisation of global military assets to the Middle East, 25% tariffs on countries trading with Iran, new sanctions and restrictions, and rhetoric around the potential consequences of failing to achieve a negotiated resolution.[22]

Israeli officials first announced the activities, as a 'pre-emptive attack against Iran to remove threats to the State of Israel'.[23] In a speech posted on Truth Social, President Trump announced the start of 'major combat operations' in Iran to "defend the American people" against "imminent threats from the Iranian regime".[24] The speech defined the threat in relation to Iran's attempts to 'rebuild their nuclear program and to continue developing the long range missiles that can now threaten' both Europe and US overseas troops.

Described targets included Iran's current missiles and supporting industry, and the Iranian navy. Objectives specified included ensuring 'the region's terrorist proxies can no longer destabilize the region' and that 'Iran does not obtain a nuclear weapon'. The speech concluded with a call to action to the Iranian people to 'take over [their] government' once the US military 'are finished'.

IMPLICATIONS:

- Reporting suggests Supreme Leader Ayatollah Ali Khamenei was killed in early attacks.[25] As Iran's most senior religious cleric, Khamenei has led Iran's political, religious and military structures since 1989. Aged 86 years old, succession planning is understood to have previously been completed, although this may be disrupted by the ongoing conflict. Change in leadership introduces an additional layer of unpredictability to efforts to anticipate how Iran may respond to the attacks.
- Early reporting suggests Iran's retaliatory activities include regional attacks on Israel, US military sites in the region, and widespread attacks on non-military targets of regional US allies. This sort of response risks creating widespread disruption and broadening those involved in the conflict. The risks are particularly high to Israel from Hezbollah in Lebanon, and to the USA and global shipping from the Houthis in Yemen.
- Iran is a country which has demonstrated a level of advanced cyber-capability, and a willingness to conduct attacks outside of the region, including against targets more broadly perceived as being complicit in opposing the regime. Faced with an existential threat and attacks intended to limit kinetic military options, cyber-capabilities may be elevated as a tactical option. It is unclear to what extent limitations imposed on domestic internet access to disrupt the flow of information and coordination of protest activity will either restrict the activities of Iranian threat actors located within the country or assist defenders in detection and/or attribution of attacks.
- Current cyber exposure linked to the conflict with Iran is unlikely to change for organisations outside Iran's previous targeting scope. However, organisations with a presence in Israel, or with commercial or governmental ties to the US government, should expect elevated risk. In the immediate term, Iranian cyber operations are likely to focus on directly supporting objectives in the ongoing conflict with Israel and the US.
- Iran and affiliated cyber threat activity are likely to focus on high-visibility but low-impact operations. These often include hacktivist-style campaigns designed to generate political messaging and public attention rather than sustained and meaningful operational disruption. Distributed denial of service (DDoS) activity is one of the most common tactics to achieve this. Mis and disinformation-related activity is also likely to increase in the short to medium term.

Section 5

Emerging Cyber Security Trend: Security Risks in AI-Enabled Platforms

Automation platforms have emerged as key tools to support the automation of AI-driven workflows. Several Low-Code/No-Code (LCNC) orchestration frameworks have simplified the integration of multiple workflow components with large language models, enabling them to execute complex tasks end-to-end.[26]

Among these tools, n8n and OpenClaw represent two well-known and widely used automation platforms. OpenClaw provides an autonomous AI agent capable of goal-driven task execution, whereas n8n offers workflow automation through a node-based interface that connects services and triggers actions.[27,28]

While these platforms improve operational efficiency and productivity, they introduce security risks and amplify existing ones. In addition to inherent risks associated with their flexible, highly permissive, and easily extensible architecture, recently identified issues in n8n and OpenClaw demonstrate how design gaps may create opportunities for wider system compromise by threat actors.

Vulnerability Disclosures in n8n

On 04 February 2026, six vulnerabilities were disclosed in n8n, following five vulnerabilities found with the platform from earlier in January 2026.[29]

These vulnerabilities could be exploited by attackers through remote code execution, command injection, arbitrary file access, and cross-site scripting.[30] Repeated fixes across multiple functional areas of the platform such as expression evaluation and sandbox boundaries suggests systematic challenges.

Its simple design and flexible integrations drive its popularity, but these features often result in deployments that lack traditional security governance. As n8n becomes more integrated into core workflows, the potential impact of a compromise grows, especially when it connects to sensitive CRMs, identity systems, or AI processing pipelines.

The Emergence of Autonomous AI Assistants

At the same time, the recent emergence of OpenClaw (formerly Clawdbot and Moltbot), an open-source autonomous AI assistant for executing tasks across email, messaging, calendar, and browsers, has similarly introduced new risks. Due to the platform's autonomous design and persistent permissions, OpenClaw instances present significant risks.[31]

OpenClaw's autonomous operation and broad integration make compromised instances especially dangerous, as they often hold sensitive API keys and extensive access.

The ease of deployment for both n8n and OpenClaw platforms, often by non-technical users, increase the probability of shadow AI deployments, where users establish informal integrations and high-privilege workflows without proper oversight.

The Specific Risks Associated with Adopting AI-enabled Platforms

AI-enabled frameworks such as n8n and OpenClaw have revolutionised the automation and integration of complex workflows. By lowering technical barriers, these platforms enable users with limited programming expertise to connect LLMs to organisational systems and third-party applications through simple steps and pre-configured connectors.

Although this accessibility accelerates experimentation with AI-driven processes and provides productivity gains, it introduces new security concerns, particularly for enterprises. By bridging systems and data sources that were previously isolated, these frameworks often collapse boundaries, thereby creating pathways that adversaries can leverage.

A major concern is the increased attack surface resulting from the adoption rate. As more users adopt these tools, configuration mistakes, such as exposing platforms to the internet or leaving permissive defaults unchanged, are increasingly evident.[32]

Another significant risk is the aggregation and centralisation of sensitive credentials. AI-enabled platforms often rely on storing API keys, access tokens, and other secrets to integrate external services. As such, they may become attractive targets for attackers.

The combination of LCNC automation and AI-driven decision-making amplifies the risk of existing AI-specific attack vectors, including prompt injection and data poisoning. A key inherent issue in any LLM-enabled system is that, unlike traditional software architecture, instructions and user data are not logically separated. LLM-based workflows process instructions and user data together, meaning sensitive credentials or prompts can be accidentally exposed if not separated. As a result, architectures that integrate LLM agents with sensitive tokens, credentials, and external databases introduce additional risks, requiring dedicated safeguards for effective mitigation.

Mitigations and Recommendations

To mitigate the risks stemming from the use of n8n and OpenClaw,vendor-released security patches should be implemented immediately. It is highly recommended that AI-enabled frameworks run inside isolated containers or virtual environments with tightly scoped permissions, rather than directly on the host operating system.

If a compromise occurs, such isolation can limit the blast radius and reduce the likelihood of host-level access. Security guidance also recommends the use of short-lived tokens, storing secrets in a managed vault, and segmenting nodes from critical systems.[33] Administrative interfaces should be restricted to trusted networks and never exposed to the internet. Third-party integrations should be vetted prior to deployment. Organisations should maintain an inventory of their AI-enabled workflows and their permissions as part of standard asset management.

Final Thoughts

AI orchestration and automation frameworks not only introduce new risks but also amplify existing vulnerabilities and create new opportunities for lateral movement and privilege escalation. The findings from this research indicate that even small misconfigurations or overlooked permissions can rapidly escalate into major breaches, particularly when these platforms are deeply embedded in business operations. Moving forward, measures such as sandboxing, robust credential management, and strict access controls should be treated as foundational requirements.

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