ncc group | FOX IT part of ncc group

Cyber Threat Intelligence Report

Review of January 2026

Contents

Section 1
Executive Summary

For January's edition of the Threat Pulse, there were 741 recorded ransomware listings, with the Industrials sector being the most targeted, consistent with previous reporting patterns. Notably, suspected scam operations accounted for 12% of claimed attacks. These attacks were excluded from this month's statistics. Given this proportion, this month's Ransomware Spotlight examines the structure of the ransomware ecosystem and the inherent limitations of interpreting ransomware data feeds. It also outlines how the threat intelligence team addresses these constraints through iterative processing and contextual enrichment to produce a high-fidelity dataset that informs trend analysis.

Our Geopolitical Developments section assesses recent instability, including US intervention in Venezuela, a prolonged internet blackout in Iran during mass protests, and rising US-Europe tensions over Greenland. These events reshape the geopolitical environment and elevate risks of cyber espionage, influence operations, and insider threats. The US, Russia, and China are likely to intensify cyber activity, increasing exposure across Europe and Latin America.

The section of Emerging Cyber Security Trends for this month examines the evolution of messaging platforms into primary attack vectors for phishing, malware delivery, spyware deployment, and account compromise at scale. Threat actors exploit trusted features, encryption, automation, and bring-your-own-device environments to bypass traditional perimeter controls.

Finally, the January 2026 opinion piece explores why cyber threat intelligence is becoming increasingly central to reducing organisational risk. As attack surfaces continue to grow, adversaries refine their tradecraft, and geopolitical tensions rise, organisations can no longer afford to be reactive. An intelligence-led, forward-looking approach is now essential. Effective CTI depends on cross-domain integration and data-driven insight to reduce uncertainty, prioritise risk, and support defensive action.

Section 2

Ransomware Statistics: January 2026

17%

Global ransomware attacks decreased by 17% in January 2026

32%

Industrials accounted for 32% of ransomware attacks in January 2026

17%

Qilin was responsible for 17% of attacks in January 2026

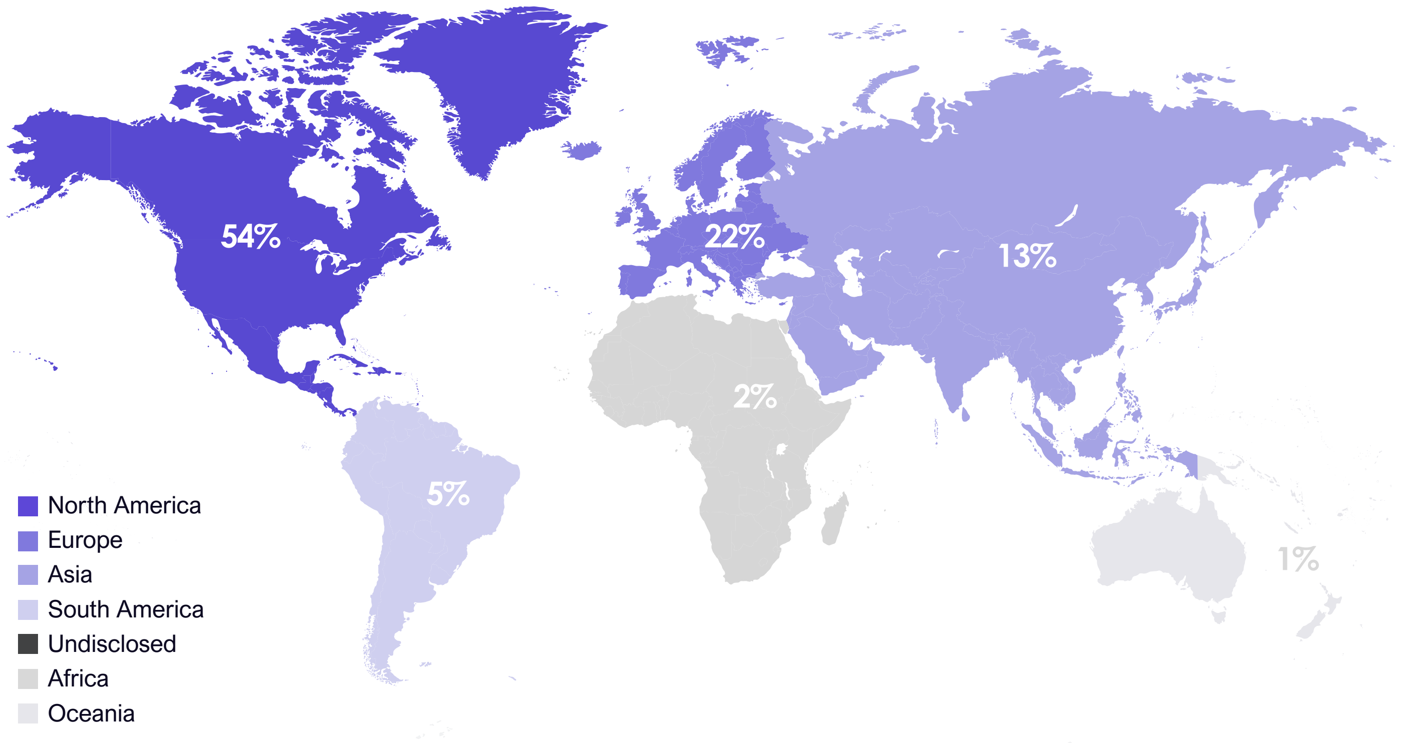

Figure 1 Ransomware Attacks by Region – January 2026

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

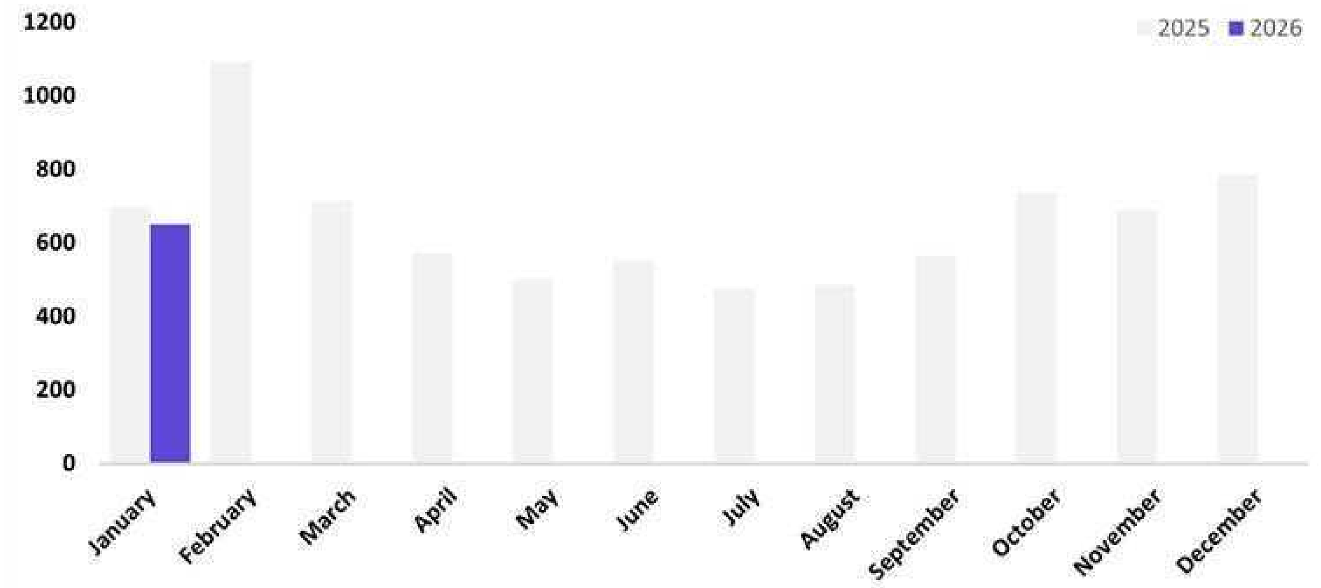

Figure 2 Ransomware Attacks by Month 2025 - 2026

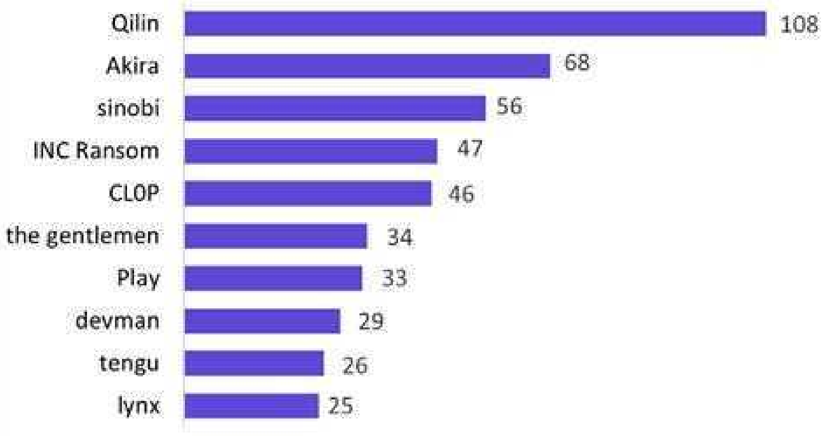

Figure 3 Top Threat Actors – January 2026

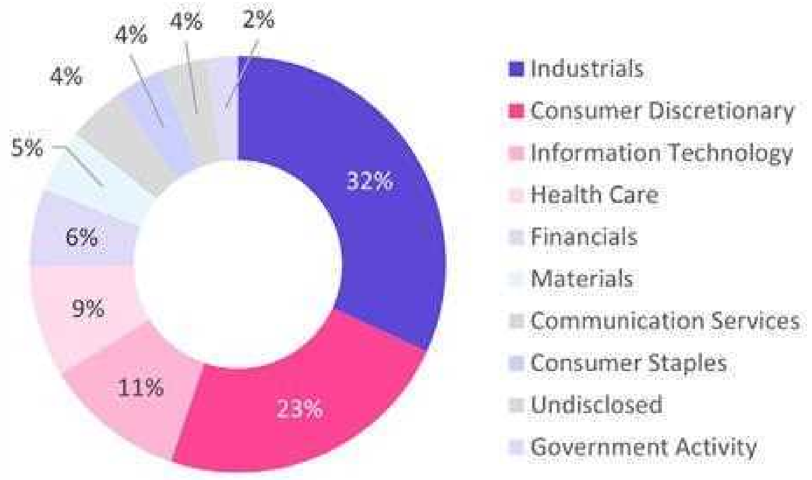

Figure 4 Top Targeted Sectors – January 2026

Key Events

02/01/2026

Covenant Health

Covenant Health was attacked by Qilin Ransomware, exposing sensitive personal and medical data of about 478,188 patients and disrupted hospital operations.

13/01/2026

Kyowon Group

South Korean education company Kyowon Group detected abnormal system activity, which led to shutdown to parts of its internal networks and caused disruptions across multiple subsidiaries. This incident potentially compromised up to 9.6 million user accounts, with an estimated 600-800 servers being affected.

30/01/2026

Tulsa Airport

Qilin ransomware group attacked Tulsa International Airport, leaking internal documents such as financial records and employee identification data, after breaching the airport's network.

Section 3

Ransomware Spotlight: The State of Ransomware Reporting

During 2025, the ransomware landscape has remained decentralised, with frequent rebranding and an expanding number of claimed attacks. These factors introduce noise into ransomware datasets, reducing the reliability and precision of trend analysis.

This month's Ransomware Spotlight discusses how the NCC Group Threat Intelligence team continues to refine its processes to overcome these limitations and keep pace with this constantly evolving landscape. To ensure the highest level of data fidelity, our methodology goes beyond numbers by categorising and enriching recorded listings with additional contextual data.

The Ransomware Ecosystem

Ransomware-as-a-Service (RaaS) is a subscription-based model. The developers of the malware typically lease their product to affiliates for a share of the profit. This business model reflects the ongoing industrialisation of the cybercrime ecosystem, in which threat actors specialise in different functions, including Initial Access Brokers (IABs), malware developers, and data brokers, among other specialisations.

According to the RaaS model, multiple threat actors can conduct operations under the same brand, while affiliates may work with several RaaS operations simultaneously.[1] Additionally, the fluid nature of RaaS also leads to frequent rebranding and splintering. When operators exit or face pressure, groups may reinvent themselves under a new brand. Reporting indicates that rebranding accelerated over the past year, driven by law enforcement pressure, operational security, and the growing competitiveness of the RaaS market. Examples include Sinobi, assessed as a rebrand of Lynx and the World Leaks brand, shifting from encryption-based to an extortion-only group. By the end of 2025, there were 127 recorded RaaS brands, a 35% increase from 2024, showing the expansion and fragmentation of the ransomware landscape.

The Limitations of Ransomware Threat Data Feeds

Recorded listings have inherent limitations and biases that influence the measurement of ransomware prevalence. Ransomware Data Leak-site (DLS) aggregators, while useful, are often incomplete and inconsistent, which complicates accurate victim counting.[2] Recorded listings derived from data leak sites only include organisations that declined to pay the ransom and were subsequently named-and-shamed by the ransomware groups.[3] Organisations that chose to pay the ransom are far less likely to appear on these sites, which can skew the perceived distribution of targeting.

It is also worth noting that relying on victim breach notifications provides limited visibility into the true scale of ransomware activity. Disclosure requirements are not enforced consistently across industries or jurisdictions.[4] As such, not all incidents make their way into these databases due to weak or poorly enforced reporting mechanisms, and certain industries or geographies may remain underrepresented in the data.

Furthermore, each ransomware data feed has its own collection and inclusion criteria, resulting in fragmented and contradictory views of the threat landscape across different vendors. Addressing these limitations, NCC Group has consolidated multiple threat feed aggregators into a single, high-fidelity database with detailed annotations. Our database undergoes repeated cycles of processing and enrichment to build a more accurate picture of the ransomware threat landscape. Each listing is validated, enriched, and assigned a confidence level to distinguish between confirmed, reported, fraudulent, and recycled listings.

The discrepancy between the actual attack date and the discovery or disclosure date presents another challenge when conducting nuanced analysis. Ransomware groups often publish victims on their leak sites days, weeks, or even months after the intrusion occurred. Organisations may not disclose an attack until long after initial compromise. To preserve analytical nuance, ransomware listings data is treated as a moving target that requires continuous updating and contextualisation.

This multilayered approach enables us not only to quantify the volume of activity more accurately but also to contextualise the observed threat behaviours at a more granular level. Despite these figures representing the best assessment based on available evidence, they should always be interpreted as high confidence estimates rather than exact measurements of the scale of ransomware activity.

Unvalidated Threat Reports

The volume and speed of threat activity at times exceeds the capacity of threat intelligence teams to track and report on rapidly evolving and emerging threat activities. A relevant example from this reporting period is the case of the 0APT ransomware group. Several vendors rushed into publishing blog posts in late January 2026 describing 0APT as a new ransomware threat actor.[5] Early claims reported 71 intrusions across multiple sectors within 48 hours and assessed the group as operating at an unprecedented scale and speed for an emerging ransomware threat actor. A week later, other researchers questioned the legitimacy of their claims and identified 0APT as a fraudulent operation that relied on fabricated victim listings.[6] The group created fictitious AI-generated companies and mixed them with a limited number of real organisations to increase the perceived legitimacy of their claims.

The brief emergence of 0APT group demonstrates how easily fabricated activity can circulate in the intelligence ecosystem, highlighting a structural issue within parts of the industry. Therefore, our approach prioritises validation before reporting any activity. Our team correlates dark-web claims with technical artefacts to assess confidence levels and avoid prematurely categorising emerging actors or behaviours as credible threats. Following this rigorous process, while time- and resource-intensive, ensures that consumers only receive intelligence that has been verified.

Final Thoughts

The production of ransomware threat reports presents several methodological challenges that affect trend analysis. Threat data feeds are noisy and often lack supporting detail, with many alleged incidents being fraudulent or lacking sufficient information. Additionally, the ransomware ecosystem is intricate and constantly evolving, and some vendors do not fully capture its subtleties. These constraints can skew metrics and misrepresent actual targeting patterns.

To mitigate this, our threat intelligence team applies rigorous, structured collection and verification processes that combine iterative data processing with analytical enrichment. This approach allows us to produce a dataset that more accurately reflects real-world ransomware activity to support reliable trend analysis across threat actors, industries, time, and regions.

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.

03/01/2026

The US military carried out Operation Absolute Resolve in Venezuela on 03/01/26: using military strikes in support of troops who forced entry into President Nicolás Maduro's residential compound, removing him and his wife to transport them to US territory.[7]

Following the operation, President Trump confirmed intentions to "run [Venezuela] until such time as we can do a safe, proper and judicious transition".[8] Developments throughout January indicate the US will allow Maduro's former leadership team to continue to administer the country, with the USA exerting influence and control through a combination of incentives and coercive measures.[9,10,11,12,13]

Intense activities have been reported to facilitate the restoration and expansion of Venezuela's oil sector; including lifting of US sanctions, new oil trade agreements with non-US rival countries, and domestic oil reform measures.[14,15] The US navy continues to maintain a significant presence in the region, including enforcing restrictions on oil tankers carrying Venezuelan oil through vessel seizures.[16,17]

On Monday 05/01/2026 Maduro and his wife pleaded not guilty in a New York federal court to offences linked to drug trafficking, specifically cocaine.[18] The case will continue in court on 17/03/26.

IMPLICATIONS:

- Tensions in the region remain high. Despite initial celebrations, displaced Venezuelans remain cautious of returning to the country.[19,20] Regionally, numerous Latin American countries condemned US activities.[21] Threats against Colombia, US willingness to use military power, and the threat of US tariffs create challenging conditions for Latin American leaders and organisations operating in the region.[22,23] In this context, threat actors may be presented with increased opportunities to compromise networks through malicious insiders or social engineering.
- Recognising the high-profile media coverage and controversial nature of developing events large quantities of related false information and propaganda were quickly observed being distributed online.[24] This included content attributed to Russian and Chinese-linked influence operations seeking to shape (or confuse) the narrative and undermine US interests.
- Indirectly, US intervention disrupts Russian regional influence. In addition to removal of Russia's ally Maduro, the US is obstructing critical support to another of Russia's strategic regional allies, Cuba.[25] As in Syria, loss of influence in Latin America reduces Russian ability to physically project power. Russia may expand its interests in West Africa, and/or strategically pivot away from opposing the USA to re-enforcing power and influence in Europe. An indicator of such a strategic change may include greater focus of Russia-linked cyberactivity towards Europe.
- Chinese influence in Latin America is assessed as less easy for the USA to reverse due to their links to large-scale infrastructure projects and formal bi-lateral agreements with countries less vulnerable to US influence; such as Brazil, Chile, and Peru.[26,27] Indicators suggest Chinese APT activity in Latin America is unlikely to reduce: Chinese technology supports expansive telecommunication infrastructure, and Venezuelan themed spear phishing campaigns have been observed against US government and policy targets.[28,29]
- These inconsistencies between the international response to Russia's invasion of Ukraine and the US taking control of Venezuela have been highlighted.[30] Canadian Prime Minister Mark Carney described the current geopolitical situation as a "rupture in the world order".[31] Major powers actively competing for global influence – the USA, China, and Russia – all possess advanced cyber capabilities. Greater cooperation between at least some middle powers – as Carney proposed in his speech – and efforts to distribute dependencies across multiple great powers are already being observed.[32,33] This sets the conditions for increased risk of pre-positioning, espionage, and influence operations against middle powers. Greater targeting of EU institutions to mitigate the risk of the world's largest trading bloc and democratic political union leveraging its potential power more effectively.

08/01/2026

A nationwide internet blackout has been reported to be effective in Iran since 08/01/2026.[34,35] The blackout coincided with the largest protest activity observed in Iran for 3 years. Protests began on 28/12/25 - triggered by the falling value of the Iranian currency and the impact on domestic trade. In addition to the tactical use of an internet blackout, the Iranian government's response has included the use of lethal force, mass arrests and detainment to dispel, disrupt, and suppress protest activity.[36] Human rights group HRANA cited 6,305 confirmed protester deaths and 17,091 cases ongoing on 31/01/26.[37,38] Despite threats made by the USA and the mobilisation of military assets into the region, the USA has so far not directly intervened.[39]

IMPLICATIONS:

- Affecting 92 million citizens and extending for 4 weeks at the time of writing, this blocking of internet access (and some phone and SMS communication) by the Iranian government was described by the BBC as one of the most 'extreme internet shutdowns in history'.[40]
- An investigation by the digital rights organisation Filterwatch concluded the current blackout is more expansive and being achieved through more advanced strategic methods than those previously imposed.[41] Through removal of infrastructure (including selective removal of over 98% IPv6 address space – see their technical report for more details), the state is "aggressively implementing a "Selective Whitelist" model" to establish a framework which removes public access to the internet whilst allowing government-controlled entities privileged access. If accurate, generalised public internet access may not be restored without regime change, and Iran may demonstrate that internet isolation can be achievable and advantageous to autocratic regimes with fewer cyber resources than China and Russia.
- Despite the risks, Iranians are assessed to have smuggled ~50,000 Starlink terminals capable of accessing the internet through satellite-based communication.[42,43] In addition to the use of satellite signal jammers, Iranian officials are reported to have confiscated identifiable equipment, which is illegal in Iran and reportedly being offered during this period for free by Starlink and supplied through a sanctions exemption.[44,45] Reporting indicates the Iranian regime is contracting private sector companies with advanced capabilities to design systems capable of detecting Starlink traffic.[46]
- Changing internet access within Iran has the potential to highlight cyber activity originating in, or dependent on, Iranian infrastructure. For example, social media accounts presenting as Scottish independence supporters have again become inactive.[47] In contrast, the pro-Iranian threat actor Handala Hack, linked to Iranian intelligence service MOIS, was reported by Check Point Research on 20/01/26 to have resumed activity but using Starlink networks for attacks.[48]

17/01/2026

Tensions between the USA and Europe experienced a dramatic increase when President Trump used social media to notify Denmark, Norway, Sweden, Germany, the Netherlands, Finland, and the United Kingdom that additional 10% retaliatory tariffs would be imposed from 01/02/26, and increase to 25% in June 2026.[49]

European countries responded negatively to the US articulating their desire to buy Greenland. As a Danish territory, Greenland is part of the Kingdom of Denmark and NATO. EU leaders responded robustly, leveraging economic power and diplomacy.[50] In parallel, European nations undertook military reconnaissance in Greenland and proposed a new NATO mission.[51,52]

On 21/01/26 at the annual World Economic Forum event hosted in Davos, Switzerland, President Trump withdrew the threat of use of force to acquire Greenland; crediting NATO Secretary General Mark Rutte with a negotiated deal to de-escalate the situation.[53] Related diplomatic talks between the USA, Greenland, and Denmark were reported to have begun on 28/01/26.[54]

IMPLICATIONS:

- The unpredictable nature of the current US Administration and their preferred approach to foreign policy undermines the stability of the current resolution, and is anticipated to have a long term, negative impact on relations between the USA and the rest of the world. China, Russia, Iran, and North Korea all strategically benefit from divisions between the USA and NATO member countries. Cyber capabilities available to all four countries may be used to inflame the situation further. For example, espionage and data leaks can expose new pressure points, and disruptive and/or hybrid attacks can highlight security weakness in Greenland, Denmark, or NATO.
- The USA defends its position on Greenland using national security arguments, including an unevidenced Chinese and Russian presence, and claims of Europe's "weakness".[55] Citing NATO's own intelligence, Nordic diplomats refuted US claims of an existing or recent level of Chinese or Russian presence around Greenland.[56] Influence campaigns on this particular issue have the potential to trigger new actions from the US administration.
-

Section 5
Emerging Cyber Security Trend: Messaging Platforms as Emerging Attack Vector

In 2026, messaging applications have become a critical communication infrastructure worldwide, but they have also been increasingly used as emerging attack vectors for cybercriminals and threat actors. Platforms such as WhatsApp, Telegram, Discord, Signal, LinkedIn, and Gmail-integrated messaging are increasingly being exploited for phishing, malware delivery, social engineering, account takeover, and spyware-based compromises.

A major campaign detected in 2025 was using Meta's WhatsApp as part of a large-scale scam and fraud operation. In this campaign, threat actors initiated contact with victims through WhatsApp using AI-generated messages, made with platforms like ChatGPT, to promote fake "like for pay" schemes, pyramid schemes, and fraudulent cryptocurrency investment opportunities. WhatsApp later reported the removal of over 6.8 million accounts linked to global scam networks that used coordinated multi-platform tactics and criminal infrastructure to lure and defraud users.[57] These campaigns are often blended with messaging apps with social media, SMS, and even AI tools to evade detections.

At the same time, zero-click malware and spyware delivery through messaging apps is being actively documented. US CISA has issued alerts noting that threat actors have been observed leveraging encrypted messaging platforms to deliver commercial spyware and other advanced malware to high-value targets, including executives and non-profit leaders.[58]

The mobile threat landscape experienced an increase in mobile attacks in 2025. A rise of 29% in Android device attacks was observed, encompassing threats that leverage messaging deliveries for malware, credential theft, and data exfiltration.[59] In April 2025, South Korea's largest mobile carrier, SK Telecom, detected abnormal outbound traffic involving the BPFDoor backdoor, exposing nearly 27 million IMSI and USIM records which affected nearly half of South Korea's population.[60] This trend underscores how mobile networks and devices are becoming increasingly attractive targets to threat actors.

The widespread use of Bring Your Own Device (BYOD) policies and the hybrid use of personal devices increases organisational exposure to messaging-based attacks, as these platforms are frequently accessed outside traditional enterprise controls.[61] Personal and hybrid-use devices often lack consistent security controls, enabling attackers to exploit these apps for account compromise and malware delivery.[62]

While corporate-managed mobile devices typically enforce security policies, they can still introduce risk due to messaging applications operating outside many enterprise monitoring solutions, especially when the device is used off-network or relies on mobile data. As a result, even managed devices may provide attackers with vectors that bypass traditional enterprise visibility and control.

Collectively, these developments illustrate a rapidly evolving threat environment in which messaging applications and mobile devices have become intertwined with modern cyber threats. The urgent need for strengthened mobile security governance, adaptive detection capabilities, continuous user awareness, and robust endpoint detection highlights the importance of addressing the rising threats associated with messaging-based attacks in 2026 and beyond.

Messaging Platforms as Attack Vector

Messaging platforms are being leveraged as attack vectors by serving as initial access points, delivery channels, and coordination infrastructure within modern attack chains. Threat actors have used these to deliver phishing links, malicious attachments, QR codes, and fake invitations that exploit legitimate platform features.[63] Even encrypted messaging services are being used to distribute mobile malware and spyware, either through direct user interaction (such as opening files or links) or through feature abuse that enables silent account access.[64] In parallel, platforms such as Telegram are being utilised to host phishing infrastructure, malware repositories, stolen data, and automated bot-based services that support large scale fraud and intrusion campaigns.[65]

The use of messaging platforms as an attack vector is expected to increase further as these services continue to expand in functionality and integrate with other digital ecosystems. Some messaging apps are increasingly converging with payments, cloud storage, authentication, and enterprise services. This creates new opportunities for abuse beyond simple message delivery.

At the same time, attackers are refining their techniques that exploit platform-specific features and user behaviour rather than vulnerabilities in underlying encryption. As messaging platforms replace email and SMS as the primary mode of communication in many regions and organisations, threat actors are likely to treat them as a default vector for initial access, malware delivery, and campaign coordination.

Emerging Attacks Using Messaging Applications

From 2025 to early 2026, emerging attack techniques using messaging applications have been dominated by platform abuse, account compromise, and delivery of mobile malware, rather than exploiting encrypted messaging protocols.

Russian threat actors have been observed exploiting Signal, a messaging application widely used among activists, journalists, politicians, and even military personnel. Attackers abused device-linking features and created phishing pages and fake Signal group invites using malicious links or QR codes to trick victims into linking an attacker-controlled device to their Signal account, which bypassed encryption and gave direct access to messages. APT44 targeted the Signal desktop application by extracting message data through scripts on compromised computers.[66]

Another attack involves WhatsApp-based malware propagation on devices. The WhatsApp malware was identified as SORVEPOTEL and is most active in Brazil. This malware spreads through WhatsApp by sending victims a malicious ZIP file from compromised contacts. When opened on a Windows desktop, the ZIP triggers a shortcut that launches a PowerShell script, downloads the main payload, establishes persistence and then hijacks the victim's active WhatsApp Web session. It automatically sends the same ZIP file to all contacts and groups for rapid propagation.[67]

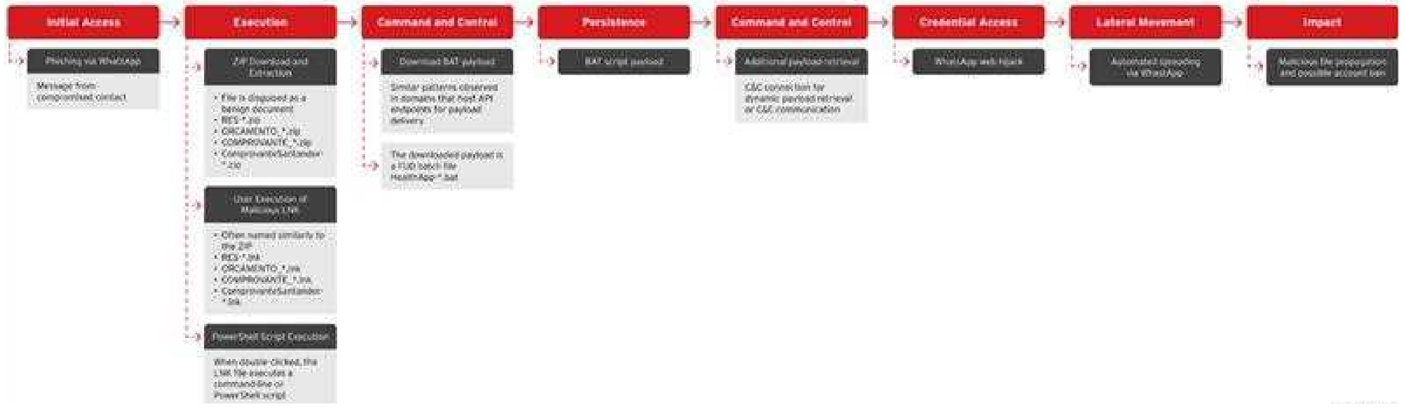
Initial Access
Phishing via WhatsApp
Message from compromised contact
Execution
ZIP Download and Extraction
• File is disguised as a benign document
• RES-*.zip
• ORCAMENTO_*.zip
• COMPROVANTE_*.zip
• ComprovanteSantander-*.zip
User Execution of Malicious LNK
• Often named similarly to the ZIP
• RES-*.lnk
• ORCAMENTO_*.lnk
• COMPROVANTE_*.lnk
• ComprovanteSantander-*.lnk
PowerShell Script Execution
When double-clicked, the LNK file executes a command-line or PowerShell script
Command and Control
Download BAT payload
Similar patterns observed in domains that host API endpoints for payload delivery
The downloaded payload is a FUD batch file HealthApp-*.bat
Persistence
BAT script payload
Command and Control
Additional payload retrieval
C&C connection for dynamic payload retrieval or C&C communication
Credential Access
WhatsApp web hijack
Lateral Movement
Automated spreading via WhatsApp
Impact
Malicious file propagation and possible account ban

Figure 5 SORVEPOTEL attack chain[68]

These techniques show a clear shift toward low-complexity, high-impact methods that exploit legitimate messaging workflows and trusted infrastructure. By abusing legitimate messaging features and trusted cloud infrastructure, threat actors avoid relying on their own servers or specialised tools.

This reduces the number of places that defenders or law enforcement can directly disrupt their operations. Because defenders cannot block or disable widely used services without causing major collateral damage, attackers gain stronger operational resilience. As multi-device support, automation features, and integration with cloud services become more common in messaging platforms, threat actors will increase the likelihood of abusing these capabilities to support both opportunistic and highly targeted intrusion or surveillance campaigns.

We expect attacks leveraging messaging platforms to increase in frequency and sophistication, as these platforms expand multi-device support, automation features, and cloud integrations. Attackers are likely to incorporate features such as AI-assisted social engineering and malware delivery, embedding malicious actions deeper into routine communication flows and making detection increasingly challenging.

For organisations, these developments significantly expand the attack surface beyond email and traditional network boundaries. The abuse of trusted platforms and encrypted messaging apps reduces the effectiveness of perimeter-based controls and increases reliance on user behaviour and endpoint security posture. Organisations face increased risks of account compromise, sensitive conversation exposure, and malware ingress via unmanaged messaging channels, particularly where messaging apps are used for business communications or installed on BYOD devices.

Mitigations and Recommendations

As messaging platforms continue to be leveraged and exploited, organisations must recognise that these threats operate largely within legitimate communication workflows. Effective mitigation, therefore, requires layered controls that address identity, endpoints, monitoring, governance, and user behaviour rather than reliance on traditional perimeter defences alone.

Having a strong authentication method remains one of the most effective countermeasures against messaging-based abuse.[69] Many campaigns rely on account takeover or session hijacking rather than exploitation of software vulnerabilities. Enforcing multi-factor authentication that is resistant to phishing attacks significantly reduces the success of credential theft and impersonation.

Lastly, incident response planning must explicitly include messaging-app scenarios. Traditional playbooks often focus on email and web threats, but successful incidents involving spyware targeting messaging platforms demonstrate the need for actionable procedures specific to messaging account compromise and device exploitation. Building and testing playbooks for disconnecting compromised sessions, unlinking devices, and remediating infected endpoints, improves resilience when attacks occur.

Final Thoughts

The leveraging and exploitation of messaging platforms has become an important initial attack vector in modern environments. Threat actors are leveraging trusted features and user behaviour to bypass traditional detection and gain access through legitimate channels.

Strengthening the human layer of defence with continuous training and workshops remains essential as users are consistently targeted through seemingly legitimate AI-enabled phishing attacks. Organisations must take decisive steps and address the risks that arise from unmanaged usage, mobile access, and blurred boundaries between personal and corporate communication.

Acting now is critical to maintaining control as messaging platforms continue to evolve and expand their role within enterprise environments.

Section 6

January Thought Piece: Why Cyber Threat Intelligence Matters More Than Ever in 2026

Cyber threat intelligence (CTI) is often misunderstood and undervalued because, unlike other operational functions in cyber security that deliver immediate results, its impact is typically long-term. Yet, without reliable threat intelligence, the effectiveness of cyber defence is significantly reduced. The lack of intelligence often creates blind spots and leads to slower, less accurate response efforts. Industry surveys indicate that organisations leveraging threat intelligence have improved their detection and response times by 54% and experienced a 40% decrease in the number of incidents.[70] These figures are indicative of CTI's measurable value to effective defensive action.

Looking ahead to 2026, organisations are facing rapid technological evolution, sophisticated threat actors, and increased geopolitical conflicts. These factors are driving up both the volume and complexity of threats. In addition, mounting regulatory pressure is driving the adoption of a proactive defensive approach. CTI is becoming more critical than ever. However, ensuring threat intelligence delivers operational value requires the integration of cross-domain expertise, handling of data feeds, and effective management of information overload.

Technological Development

Rapid technological development has expanded the attack surface. The accelerating adoption of cloud services, Internet of Things (IoT) devices, and other interconnected software has created larger and more complex technology estates for organisations to manage.

At the same time, the widespread adoption of generative AI is introducing new and not yet fully understood risks, particularly where it is deployed quickly or integrated without sufficient oversight. IBM predicts that AI will dominate the threat landscape in 2026, largely because of how deeply it is becoming embedded across business functions and technologies.[71]

Emerging technologies, by their nature, are often misunderstood in their early stages, which can lead to oversimplified or inaccurate reporting in the media and by vendors.

CTI plays an important role in this context. The speed of change across AI, cloud services, and supply chain ecosystems creates uncertainty. Intelligence helps reduce that uncertainty by distinguishing credible threats from speculation and hype. As complexity increases, so too does the need for clear, evidence-based insights that allow security teams to prioritise the risks that matter the most.

Rising Geopolitical Tensions

Geopolitical instability is increasingly reflected in cyberspace, with nation-states targeting critical systems in parallel with real-world conflicts and rising tensions. These developments show that cyber operations have become a routine extension of geopolitical competition and conflict. According to a World Economic Forum survey, 64% of organisations take geopolitically motivated attacks into account in their risk mitigation strategies.[72]

This dynamic is not limited to state-sponsored threat actors; financially motivated threat groups can also become entangled in geopolitical rivalries. These groups may receive support when their activities align with national objectives, blurring the line between crime and espionage operations. An example of this is the permissive operating environment provided to ransomware groups by the Russian government.[73]

During periods of growing geopolitical tension, CTI becomes essential for understanding how global events may shape emerging cyber threats. CTI seeks to contextualise the strategic drivers behind threat activity. By tracking cyber activity in parallel with geopolitical developments such as elections, military clashes, sanctions, and shifting alliances, it informs assessments of how these factors may influence the behaviour and priorities of threat actors.

Behaviour Over Indicators

Threat actors are moving faster than traditional defences by constantly rotating and masking their infrastructure. Advanced Persistent Threat (APT) groups regularly change domains or compromise routers to conceal the origins of their operations.[74] This constant adaptation of infrastructure means that static artefacts such as domains, IP addresses, and file hashes, which defenders have historically relied on for detection, can lose value within hours or days. By the time they are shared or blocked, the threat actor has often pivoted to alternative infrastructure. This presents an even tougher challenge, as threat actors continue to incorporate commonplace IT software and services into their intrusion sets, rendering static detections redundant.

Campaign intelligence captures those longer-term patterns. ATT&CK-mapped playbooks and reoccurring routines reveal how an adversary works over time. Behaviour-focused research also gives detection engineers and SOC analysts practical guides to work with. It can highlight patterns of risk before an activity turns into a compromise. Inspecting the style, capability, victimology, and objectives of threat actors enables defenders to build clearer profiles of their activity and detect emerging threats that may bypass signature-based tools. As threat actors evolve, intelligence clarifies who is behind the activity, why it is occurring, and how defenders should respond, shifting the focus away from static indicators towards behaviour-driven detection.

Overcoming CTI Challenges

In an environment where cyber threats evolve faster than many organisations can respond, separating meaningful intelligence from noise has become critical. Marketing-driven reporting often fixates on buzzwords such as AI, zero-days, and quantum computing, while the real risks frequently stem from far more mundane issues, such as unpatched internet-facing systems. Decision-makers are left overwhelmed by information that does not reduce uncertainty or support practical action. In this oversaturated information space, the importance of mature CTI becomes elevated. At its core, CTI is not about simply describing what has happened; it is about answering the 'So what?' of a threat activity.

That said, a mature CTI capability requires continual improvement to keep pace with the evolving conditions, including the growing volume of threat data with inconsistent quality. Transforming raw data into meaningful intelligence requires disciplined, iterative analysis. To ensure that our intelligence products remain actionable rather than overwhelming, we have introduced additional layers of categorisation and enrichment. These improvements have strengthened both our ransomware incident collection process and our vulnerability reporting workflow.

Another ongoing challenge for any CTI capability is the need to integrate expertise from multiple domains to form a coherent threat picture and ensure outputs align with the strategic, operational, and tactical needs of stakeholders. To strengthen this approach, NCC Group is bringing together incident response, digital forensics, threat hunting, and detection engineering into a unified, intelligence-led capability. By operating as a single, coordinated system, the team is better able to bridge the gap between observed threat activity, operational relevance, and the specific organisational context of each stakeholder.

Final Thoughts

While CTI as a discipline may lack the same standardisation seen in more established cyber security domains, NCC Group is continuously advancing its intelligence capability and addressing its inherent challenges. Through enhanced collection processes, context enrichment, and integration, we reinforce our commitment to improving analytical tradecraft to deliver intelligence products that inform and guide stakeholders.

The need to evolve becomes even more pressing as we move into 2026 and beyond, where CTI is expected to keep pace with rapidly shifting challenges. Advancing technologies, changes in adversary tradecraft, and the increasingly complex geopolitical landscape require intelligence capabilities that are adaptive and well-rounded.

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