ncc group | FOX IT part of ncc group

Cyber Threat Intelligence Report

Review of Q2 2026

Contents

Section 1
Executive summary

The second quarter of 2026 saw a further escalation in cyber threat activity, with supply chain attacks increasing in frequency and sophistication. Ransomware volumes also continued to rise, while geopolitical tensions increasingly shaped sector-specific and regional risk profiles. These trends indicate that threat actors are scaling operations and becoming more deliberate in how they select targets.

The Ransomware spotlight examines how ransomware operators continue to prioritise VPNs and internet-facing edge devices as high-value initial access vectors. Groups including Akira, Qilin, and The Gentlemen are exploiting software flaws to gain unauthorised entry and deepen network compromise. The volume of VPN-related alerting, alongside recent campaigns affecting Fortinet, SonicWall, and Citrix technologies, highlights threat actor intent and requirement to prioritise patch management.

The Emerging cyber security trends section explores the rapid increase in attacks targeting trusted software development ecosystems. Activity observed in Q2 2026 highlights the abuse of developer platforms and CI/CD workflows to compromise trust at scale. Campaigns linked to TeamPCP, including Mini Shai-Hulud, show how upstream access can drive downstream compromise and expand organisational exposure. These developments reinforce the need for continuous dependency governance, credentials exposure reduction, strengthened CI/CD security, and behaviour-led monitoring across development environments.

The Geopolitical developments section assesses how Belarus' support for Russia, Ireland's EU Council presidency, and China's regional assertiveness may increase cyber threat activity. Politically exposed organisations face heightened risk from state-linked espionage, topical phishing, DDoS activity, disinformation, and potential pre-positioning in sensitive networks. Organisations should monitor activity linked to Russia-, Belarus-, and China-aligned actors, strengthen phishing resilience, and use behaviour-led threat hunting where static indicators are insufficient.

Section 2

Timeline of critical incidents Q2 2026

April

02/04/2026

DigiCert disclosed that attackers infiltrated its support environment through malware delivered via a customer chat channel disguised as a screenshot. The malware infected two internal systems, allowing the attackers to access the company's support portal and abuse limited support functions to obtain EV code signing certificates from approved customer orders. By using initialisation codes and existing requests, the attackers were able to abuse certificates to sign payloads associated with Zhong Stealer. DigiCert identified and revoked 60 affected certificates by 17th April and found no evidence of broader system compromise.

06/04/2026

Winona County in Minnesota was hit by a ransomware attack. This caused a widespread shutdown of Government systems and disrupted public services. The Governor deployed the National Guard's Cyber Unit, alongside the FBI and state authorities, to support response and recovery efforts. It was the county's second cyberattack this year, following the January 2026 attack. Emergency services remained operational and full recovery was achieved by 24th April 2026.

07/04/2026

A ransomware attack on ChipSoft forced its website offline and led healthcare institutions to disconnect from its systems after a data incident involving possible unauthorised access. While most hospital operations continued, some patient portals were temporarily taken offline as Z-Cert coordinated the response. Later, they confirmed that attackers had stolen some patient data, including medical records. However, they stated that the data had not been released and was ultimately destroyed. The incident was linked to Embargo; however, it remained unclear if the ransom had been paid.

13/04/2026

Operation PowerOFF, an ongoing coordinated international law enforcement activity involving 21 countries, targeted the Distributed Denial of Service (DDoS)-for-hire ecosystem, identifying over 75,000 users. They have issued warning notices to administrators and users while executing 25 search warrants, arresting four individuals, and seizing 53 domains tied to illicit services.

23/04/2026

US authorities carried out a major crackdown on cyber-enabled fraud targeting Southeast Asian scam centres, using a coordinated approach led by the Department of Justice with support from the Treasury and State Department. The operation focused on dismantling the full ecosystem behind these scams, targeting trafficking compounds, the online infrastructure, and financial networks used to steal and launder cryptocurrency. At the same time, authorities shut down more than 500 fake investment websites used to scam users and restrained over $700 million in cryptocurrency tied to these activities. As a result, this action demonstrated a clear shift towards not just arresting individuals but also cutting off the financial flows and infrastructure that sustain large-scale fraud operations.

May

11/05/2026

OpenAI disclosed a supply chain attack on the TanStack development framework that deployed malicious packages from infected developer devices, including two used by OpenAI employees. The infection granted the attackers the ability to steal limited credentials and access certain internal code repositories, while no customer data or core intellectual property was compromised. OpenAI responded by rotating credentials, revoking sessions, restricting deployments, and replacing exposed code signing certificates across multiple platforms. The company also required software updates, particularly for macOS users, while coordinating with platform providers to prevent misuse of stolen certificates. The incident was linked to incomplete security upgrades during an ongoing transition to stronger protections following an earlier supply chain attack.

19/05/2026

Delano Public Schools in Minnesota suffered a ransomware attack after attackers acquired access to the district's systems and printed hundreds of pages containing ransom messages. The authorities confirmed that the attack appears to have originated externally, with no involvement from students, phishing, or artificial intelligence, and investigators have identified the access vector but not the attackers. Authorities, including the FBI, were notified, and limited system access helped reduce the impact. Classes resumed on 21st May, with students using Ethernet connections while recovery efforts continued.

June

02/06/2026

Dashlane has reported a cyberattack in which hackers bypassed its two-factor authentication system by brute-forcing codes, allowing them to access around 20 customer accounts and download at least a dozen encrypted password vaults. While the company says its core systems were not compromised and the stolen data remains encrypted and unreadable without each user's master password, it warned that users with weak master passwords could still be at risk. Dashlane added that it has taken steps to prevent future attacks but has not disclosed further details about the breach or the attackers.

12/06/2026

Anthropic has globally disabled access to its Claude Fable 5 and Mythos 5 AI models following a US government order citing national security concerns over a potential method to bypass their safety controls. Anthropic argues that the issue is limited and not a major threat, emphasising that it already uses strong safeguards and layered protections. This highlights the growing tension between regulators seeking tighter control over powerful AI systems and companies pushing to keep these tools broadly available.

19/06/2026

Operation Endgame involved the RCMP and global partners disrupting a Russian-linked network behind SocGholish malware, which spread through compromised WordPress sites disguised as software updates. The operation cleaned 2,488 systems, took action on nearly 15,000 websites, and helped prevent reinfection while alerting affected Canadian organisations.

On the 19th June, Klue confirmed a supply chain breach in which attackers used compromised credentials to access its systems and steal OAuth tokens, enabling unauthorised access to Salesforce data across multiple customers. The incident affected around two dozen organisations, including LastPass and Tanium, and remains active amid ongoing investigation and extortion attempts.

Section 3

Ransomware key statistics: Q2 2026

3%

Global ransomware attacks increased by 3% in Q2 2026

30%

Industrials accounted for 30% of ransomware attacks in Q2 2026

14%

Qilin was responsible for 14% of attacks in Q2 2026

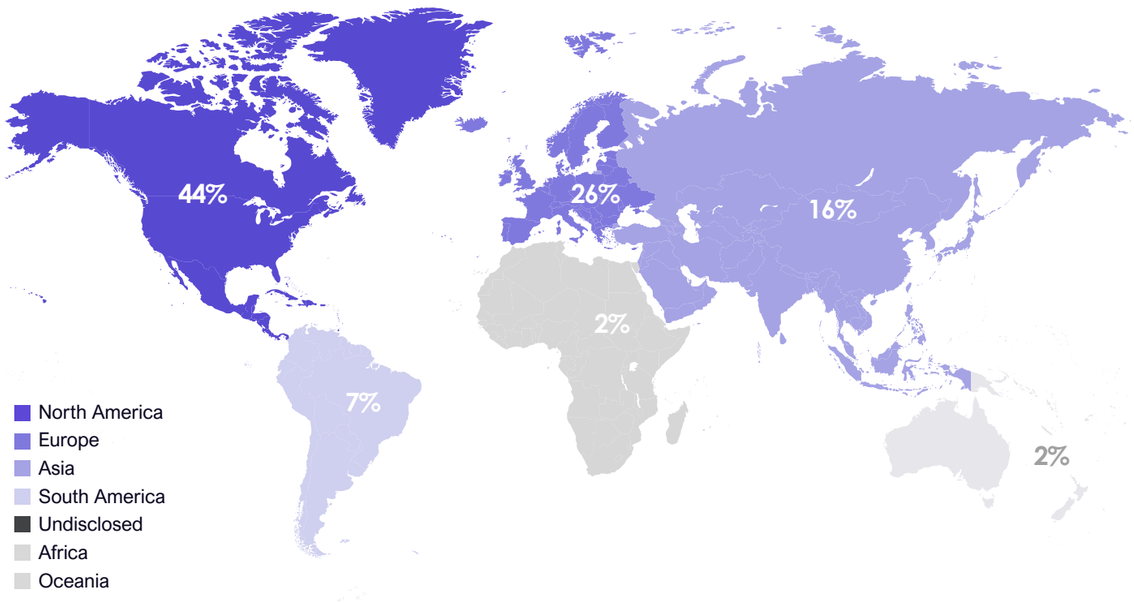


Figure 1: Ransomware attacks by region, Q2 2026

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

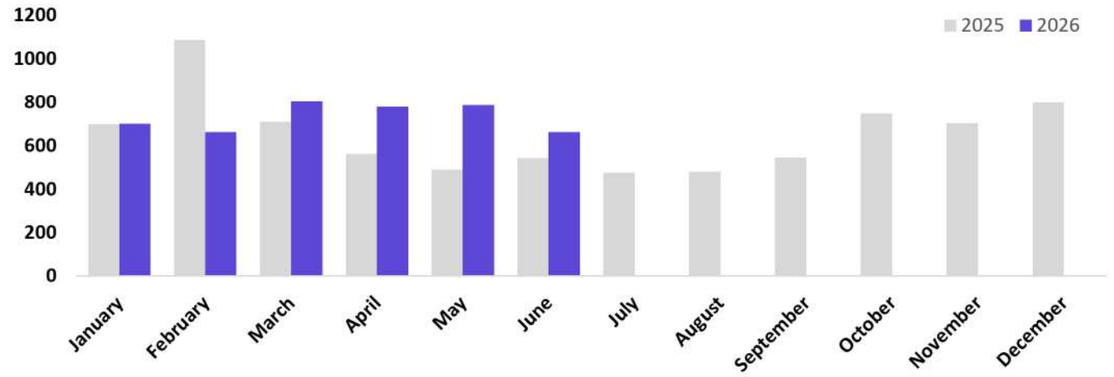


Figure 2: Ransomware attacks by month 2025 - 2026

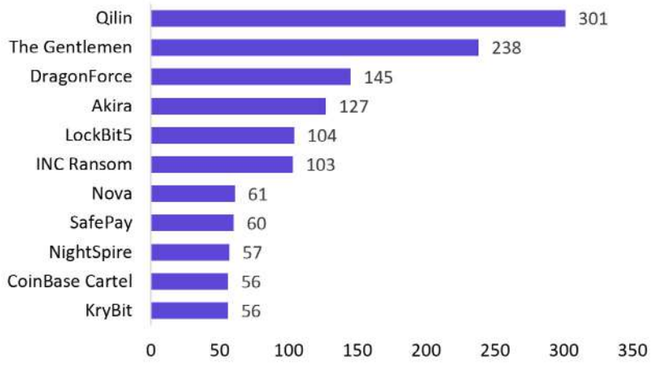


Figure 3: Top 10 threat actors, Q2 2026

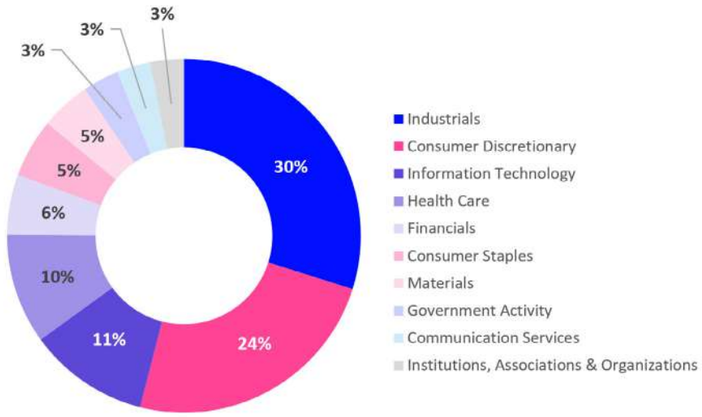


Figure 4: Top 10 targeted sectors, Q2 2026

Key events

April 2026
Signature Healthcare

Signature Healthcare was hit by a ransomware attack that disrupted operations at Brockton Hospital, Massachusetts, forcing staff to switch to manual processes while critical systems went offline.

May 2026
Baker Distributing

The Baker Distributing breach involved ShinyHunters listing the company with claims of over 260,000 stolen Salesforce records, then releasing the data in early June after failed negotiations, exposing about 103,000 customer contact records along with support tickets and internal SharePoint documents.

June 2026
Liberty University

Akira claimed a June 2026 attack on Liberty University that encrypted systems, caused a campus-wide outage, and involved a USD 4.5 million ransom demand, with possible exposure of data from up to 250,000 students and staff.

Section 4

Ransomware insights

In Q2 2026, ransomware activity increased slightly compared to Q1 2026, increasing by 3% from 2,165 to 2,229. While the increase was relatively small, ransomware activity remained consistently high across all industries throughout the quarter. The Industrial sector remained the most targeted, followed by Consumer Discretionary, Information Technology, Health Care, and Financials. The quarter also demonstrated that leading ransomware groups maintained their positions, while several threat actors continued to mature and expand their operations by adopting sophisticated tactics and techniques.

Qilin remained the most active ransomware threat actor for the fifth consecutive quarter, recording 301 victims in Q2 2026. The Gentlemen followed with 238 victims, while DragonForce ranked third with 145 victims. The continued success of these groups highlights the effectiveness of their tradecraft and operational maturity.

Qilin

Qilin continued to dominate the ransomware landscape in Q2 2026, maintaining the top position since Q2 2025. The group consistently demonstrated advanced technical capabilities and willingness to adopt new techniques to improve operational performance.

Recent reports show that Qilin affiliates have leveraged Bring Your Own Vulnerable Driver (BYOVD) techniques to disable security tools on compromised systems. In some cases, Qilin has deployed malware which can neutralise endpoint detection and response (EDR) solutions, capable of disabling more than 300 EDR drivers across a wide range of security vendors.[1,2] This significantly reduces defenders' ability to detect and respond to the group's activity. Qilin has also continued to adapt to broader ransomware trends, including the exploitation of vulnerabilities in internet-facing edge devices.[3,4] This continued investment in defence evasion and initial access capabilities demonstrates the group's technical maturity and likely contributes to its sustained success and high victim volumes.

The Gentlemen

The Gentlemen has rapidly emerged as one of the most active ransomware groups in 2026.

Despite being active for less than a year, the group has demonstrated a level of operational maturity typically associated with more established ransomware operations.

In May 2026, a reported breach of the group's internal infrastructure provided researchers with insight into its operations, revealing discussions around attack techniques, credential abuse, EDR-disabling tools, and access to compromised networks. One of the more interesting insights resulting from this breach highlighted the typical dwell time the group spent inside a victim's network before encrypting and extracting valuable data and issuing ransom notes, with an average of between 2 and 6 weeks.[5]

Despite this exposure, The Gentlemen has remained highly active. The group has allegedly entered an official partnership with a new version of BreachForums, allowing it to advertise on the platform while receiving infrastructure and operational support.[6] This development highlights the growing professionalisation of ransomware operations and the increasing role of cybercriminal partnerships in sustaining their growth.

KryBit

A notable development in Q2 was the emergence of KryBit among the top 10 most active ransomware groups, with the group claiming 56 victims during this quarter. First observed in March 2026, KryBit is an emerging Ransomware-as-a-Service (RaaS) operation that employs an affiliate-based business model. Under this model, cybercriminal partners conduct intrusions and deploy ransomware while sharing ransom proceeds with the operators, reportedly on an 80/20 revenue split. The group's ransomware is capable of targeting multiple environments, including Windows, Linux, VMware ESXi, and NAS devices, and employs a double-extortion strategy.[7,8,9]

Since its emergence, KryBit has claimed victims across numerous industries and countries. The group gained significant attention due to a public conflict with rival ransomware group 0APT, during which both groups reportedly breached and exposed elements of each other's infrastructure and operational data. Despite this exposure, KryBit has remained active and continues to advertise ransomware services and publish victim claims on its leak site.[10]

Section 5

Ransomware spotlight: Targeting and exploiting VPNs and edge devices

Multiple ransomware actors have been observed targeting VPNs and edge devices as part of their campaigns, specifically Akira, Qilin, and The Gentlemen. The targeting of VPNs by these groups, and others, has made them the most exploited entry point for ransomware operators in 2026 so far.[11] As discussed in last month's Threat Pulse, the increasing ubiquity of AI presents a threat to defenders as well as a boon. Threat actors are using AI to accelerate the timeline of exploit development. Exploits developed for publicly known but as-yet-unpatched vulnerabilities, can now be described as "n-hours" due to the swiftness with which attackers are developing working exploits.[12]

NCC TI alerts focus on VPNs:

Of these 150+ alerts issued by NCC so far in 2026, vulnerabilities affecting specific VPNs or their manufacturers have been among the most common, representing 15% of the total issued to date. Not only are these vulnerabilities frequently rated either High or Critical severity, but they are also often being actively exploited in the wild by threat actors. Though ransomware groups are not always behind the active exploitation campaigns, this trend does highlight the attractiveness of VPNs as a target for network intrusion by threat actors.

Ransomware gang exploitations:

Akira:
Akira is one of the more prominent ransomware groups which actively targets VPNs. It does this both through exploiting vulnerabilities in flawed software and also through abusing legitimate credentials. These are sometimes bought on the dark web from data brokers, phished, or stolen through the use of infostealers such as Lumma Stealer. Starting in July 2025, Akira engaged in a campaign which involved exploiting vulnerabilities in SonicWall SSL VPN devices via CVE-2024-40766 which had been initially disclosed over a year prior. In addition to the exploitation of CVE-2024-40766, Akira was also assessed to be leveraging other flaws within SonicWall technology, enabling the group to maintain access even in instances where the vulnerability was patched in the victim's network.[13]

Using similar methods, Akira was estimated to have earned nearly $50 million in its first year of operations, and approximately a quarter of a billion dollars in ransom payments by 2026.[14,15]

Qilin:
Qilin, the most prominent ransomware threat group so far in 2026 according to NCC's own ransomware tracking data, is another group known to target VPNs. Similar to Akira, Qilin exploits vulnerabilities in VPNs to gain initial access. Notably, the group has exploited CVE-2023-27997 and CVE-2024-21762 in Fortinet's FortiGate products as well as CVE-2023-4966, known as the Citrix Bleed vulnerability, in Citrix NetScaler in order to hijack authenticated sessions and bypass MFA through the theft of session tokens.[16]

One recent campaign by Qilin which involved targeting VPNs was the May - June 2026 targeting of Check Point Remote Access VPN and Mobile Access deployments in an authentication bypass attack. This campaign exploited CVE-2026-50751 and enabled Qilin to exploit a logic flaw in the certificate validation process and establish a VPN session without the need for a valid password, and thus bypassing authentication requirements.[17] This is a particularly impactful campaign as 4 of the 9 affected products have reached End-of-Life status, and therefore cannot be patched. Full migration to a new and supported release is a significantly more complex operation than simply installing an update patch.

The Gentlemen:
The Gentlemen is another ransomware group which actively targets VPNs and other edge devices to gain access to its victims' networks. A leak of The Gentlemen's own internal backend database, Rocket, in May 2026 highlighted a rare and valuable end-to-end view of the group's operations. These included details on initial access paths, the division of roles within the group, what toolsets are used, and how the group tracks and evaluates CVEs for potential exploitation.

The group's main method of gaining initial access is through exposed edge devices in their victims' networks, such as firewalls, VPNs, and other internet-facing systems. It is particularly known for targeting Fortinet's FortiGate product line as well as a range of Cisco products. In addition to exploiting known vulnerabilities, The Gentlemen uses brute-forcing tactics against web and VPN panels, as well as purchasing legitimate credentials from access brokers on the dark web. These footholds are then used as pivots in order to move laterally and deeper within their victims' networks.[18]

What to expect:
FortiBleed facilitates future attacks
FortiBleed is the name being given to a massive credential compromise incident affecting Fortinet and FortiGate firewalls and VPN gateways which was uncovered in June 2026. Security researchers found an open directory that a threat actor had unintentionally left exposed on the public internet, which contained compiled data affecting approximately half of all publicly exposed FortiGate devices. This directory contained a range of sensitive data on tens of thousands of FortiGate environments including cleartext credentials.[19]

What the existence of this directory tells us, is that multiple actors find high value to be gained from accessing VPNs and edge devices, and that many major organisations around the globe are at risk of compromise through this attack vector. It is expected that many threat actors will seek to take advantage of this directory, even those who may otherwise not have targeted these types of entry vectors.

All organisations using Fortinet and FortiGate products should familiarise themselves with the guidance issued by Fortinet, as well as the NCSC, to defend against future attacks.[20,21]

Mitigation advice:
Despite being a valuable target for threat actors, VPNs are simply not something that we can do without in the modern age. Thus, it is important that they are secured and properly managed to defend against unwanted threat actor attention. Most VPN providers will provide advice on how to secure their products and release advisories in the event of exploitation or compromise. These advisories should be monitored, and patches installed as soon as practicable to stay secure. Strong authentication measures such as MFA, though possible to be bypassed, are still invaluable measures in defending one's network and should not be ignored.

Regular security audits and consistent monitoring can help detect anomalous behaviour, particularly from legitimate accounts if their credentials are compromised and being abused, and enable defenders to minimise the impact from network intrusions. Threat intelligence, whether done internally or provided by a third party such as NCC, is also invaluable in assisting defenders as it can alert teams to vulnerabilities and trends in attacker behaviour before they are targeted.

Section 6
Extended ransomware spotlight: The Gentlemen

Since NCC Group's April 2026 Pulse assessment, further analysis has shown that The Gentlemen is not simply an emerging ransomware group but a mature and increasingly scalable RaaS operation.

A major turning point came in May 2026 with the leak of an internal backend database known as Rocket, which exposed internal communications, operational records, negotiation activity, and affiliate coordination. This reinforced earlier assessments that The Gentlemen's rapid success is driven by experienced leadership, proven enterprise-focused attack techniques, and highly effective affiliate-driven operations.

Evidence gathered since April has strengthened links between The Gentlemen and the cybercriminal identity hastalamuerte, believed to play a central role in the organisation.[22]

Insights from the Rocket leak

The Rocket leak provided unprecedented insight into the group's structure. It revealed a core team of approximately nine members with clearly defined responsibilities, supported by a broader network of affiliates.[23] This hybrid model combines centralised oversight with decentralised execution, allowing the group to maintain operational consistency while scaling activity through affiliates.

Operators actively target vulnerabilities affecting internet-facing infrastructure, particularly Fortinet and Cisco devices, while also using credential harvesting, NTLM relay attacks, and compromises of Microsoft 365 and Outlook Web Access environments. Rather than relying on a single access technique, the group opportunistically combines multiple methods depending on target conditions. Internal coordination around vulnerability exploitation, tooling, and access development demonstrates a disciplined and systematic approach to intrusion operations.

The leak revealed insight into negotiation and extortion practices. In one case, an initial ransom demand of $250,000 was negotiated down to $190,000, reflecting a commercially aware approach to victim engagement. The group has demonstrated a willingness to reuse stolen information across campaigns, leveraging data from one victim to enable access or exert pressure on others.

This indicates growing confidence in applying multi-party and downstream extortion strategies.

Tooling and intrusion model

Technical analysis shows that The Gentlemen employs a Go-based, multi-platform ransomware encryptor targeting Windows, Linux, and ESXi.[24,25] Strong encryption capabilities are combined with automated propagation mechanisms using harvested credentials, administrative tools, and remote services to spread across networks with minimal operator involvement.

The Gentlemen also provides affiliates with a comprehensive suite of endpoint detection and response (EDR) bypass tools.[26] Central to this toolkit is GentleKiller, complemented by tools such as HexKiller, HavocKiller, and ThrottleBlood. Many appear to have been acquired externally and modified for consistent use. These tools employ advanced obfuscation techniques and are often disguised as legitimate cyber security software. Leaked communications indicate that group leadership actively manages the development and distribution of these capabilities, reflecting a deliberate strategy to standardise affiliate operations and lower technical barriers to entry.

Assessment

Overall, The Gentlemen's success is rooted in operational maturity rather than innovation. For defenders, the greatest opportunity for disruption remains the early stages of attack activity, including credential abuse, initial access, privilege escalation, and lateral movement. As automation and self-propagation continue to reduce response windows, early detection and containment become increasingly critical. The Gentlemen should therefore be viewed as a professionally managed ransomware ecosystem led by experienced actors, with the Rocket leak providing evidence of both its organisational maturity and growing operational effectiveness.

Section 7

Emerging cyber security trend: Supply chain attacks

During Q2 2026, multiple campaigns targeted the software development ecosystem, prompting renewed scrutiny of how these environments are integrated and secured. Recent reporting indicates a marked escalation in the scale and sophistication of supply chain compromises.[27] These campaigns increasingly targeted widely trusted platforms, creating cascading effects across multiple environments. Affected ecosystems included GitHub Actions, Docker Hub, npm, PyPI, Open VSX, the Visual Studio Code Marketplace, and other developer tooling environments, where threat actors embedded infostealer functionality into trusted development dependencies and automation workflows.

Among the most significant supply chain threats observed during the reporting period was 'Mini Shai-Hulud'. Researchers attributed the self-propagating worm to the financially motivated threat actor TeamPCP, although other unidentified threat actors were also linked to related activity.

This section of the report discusses the implications of supply chain campaigns observed between April and June 2026 and the measures organisations can take to mitigate these risks. To minimise the likelihood and impact of upstream compromise, organisations need to implement continuous dependency governance and monitoring, harden their CI/CD environments, reduce credential exposure, and prioritise behavioural detection over static indicators. Given the observed increased use of this attack vector, organisations should reassess the implementation and security of their development pipelines.

Key implications

The series of supply chain attacks demonstrates key structural weaknesses in the development ecosystem. TeamPCP and related activity show that maintainer accounts, GitHub Actions runners, npm tokens, OIDC tokens, and cloud credentials are now primary targets. The main risk is no longer limited to a compromised endpoint or exploitable software vulnerability, but extends to the compromise of the ecosystems that publish, attest, analyse, and release software. The key issue with this type of threat activity is the compromise of "transitive trust".[28]

Across these campaigns, the attackers utilised legitimate and trusted pipelines and distribution channels to deliver their payloads and harvest victim credentials. As such, the threat model shifts from vulnerability and malware to trust-chain exploitation.

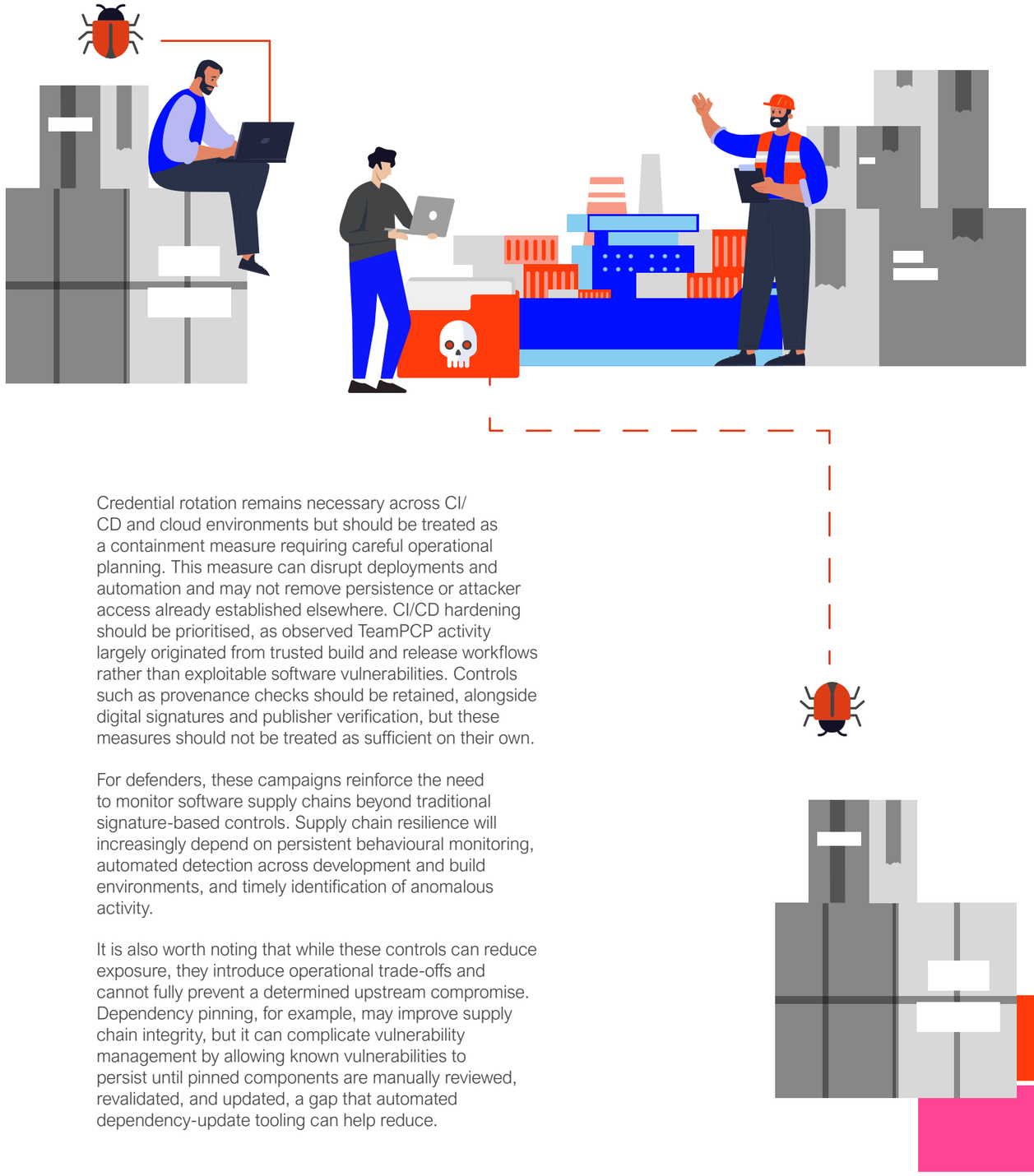
Assurance mechanisms themselves can be co-opted, expanding both the scale of downstream exposure and the ambiguity of post-compromise trust. In fact, the blast radius of this threat activity is also of note, as these compromised systems accelerate the spread of infection across multiple environments. Such attacks often yield credentials that enable attackers to move to the next target. For instance, stolen credentials linked to the March Trivy compromise were used to access Cisco's development environment, resulting in the exfiltration of more than 300 internal repositories, including source code associated with Cisco AI Assistant and AI Defense.[29]

These campaigns demonstrate the cascading effect of supply chain compromise, where the organisation ultimately breached may be distinct from the initial point of compromise. They also show that downstream victims can suffer irreversible data loss before exposure is detected, and that credential rotation at the original entry point may be insufficient once access has already been exploited. TeamPCP and similar threat activity indicate that CI/CD pipelines have become primary intrusion targets. By compromising build actions and release workflows, the actor demonstrated that automation layers can provide privileged access to secrets, tokens, repositories, and downstream environments at scale.

The operational value lies in the pipeline's position between code, identity, and deployment. CI/CD security has therefore shifted from an engineering-control concern to a core threat intelligence priority, requiring continuous monitoring and compromise assessment across build dependencies.

Mitigations and recommendations

Going forward, organisations should move beyond the conventional guidance to disable auto-update and instead pin dependencies, third-party actions, and build components to verified safe versions using immutable references.



Credential rotation remains necessary across CI/CD and cloud environments but should be treated as a containment measure requiring careful operational planning. This measure can disrupt deployments and automation and may not remove persistence or attacker access already established elsewhere. CI/CD hardening should be prioritised, as observed TeamPCP activity largely originated from trusted build and release workflows rather than exploitable software vulnerabilities. Controls such as provenance checks should be retained, alongside digital signatures and publisher verification, but these measures should not be treated as sufficient on their own.

For defenders, these campaigns reinforce the need to monitor software supply chains beyond traditional signature-based controls. Supply chain resilience will increasingly depend on persistent behavioural monitoring, automated detection across development and build environments, and timely identification of anomalous activity.

It is also worth noting that while these controls can reduce exposure, they introduce operational trade-offs and cannot fully prevent a determined upstream compromise. Dependency pinning, for example, may improve supply chain integrity, but it can complicate vulnerability management by allowing known vulnerabilities to persist until pinned components are manually reviewed, revalidated, and updated, a gap that automated dependency-update tooling can help reduce.

Section 8
Geopolitical developments

03/06/2026

Around 3rd June, China imposed 1-year travel bans on four New Zealand back-bench MPs following their parliamentary visit to Taiwan in May, a practice framed as routinely occurring over decades for New Zealand lawmakers.[30] New Zealand's government described the ban as 'entirely inappropriate' and planned to raise the matter with the Chinese Government.[31] On 11th June, China imposed sanctions which include a travel ban on the Defence Secretary of the Philippines and his family.[32] China justified the decision based on his repeated 'erroneous remarks concerning China'.

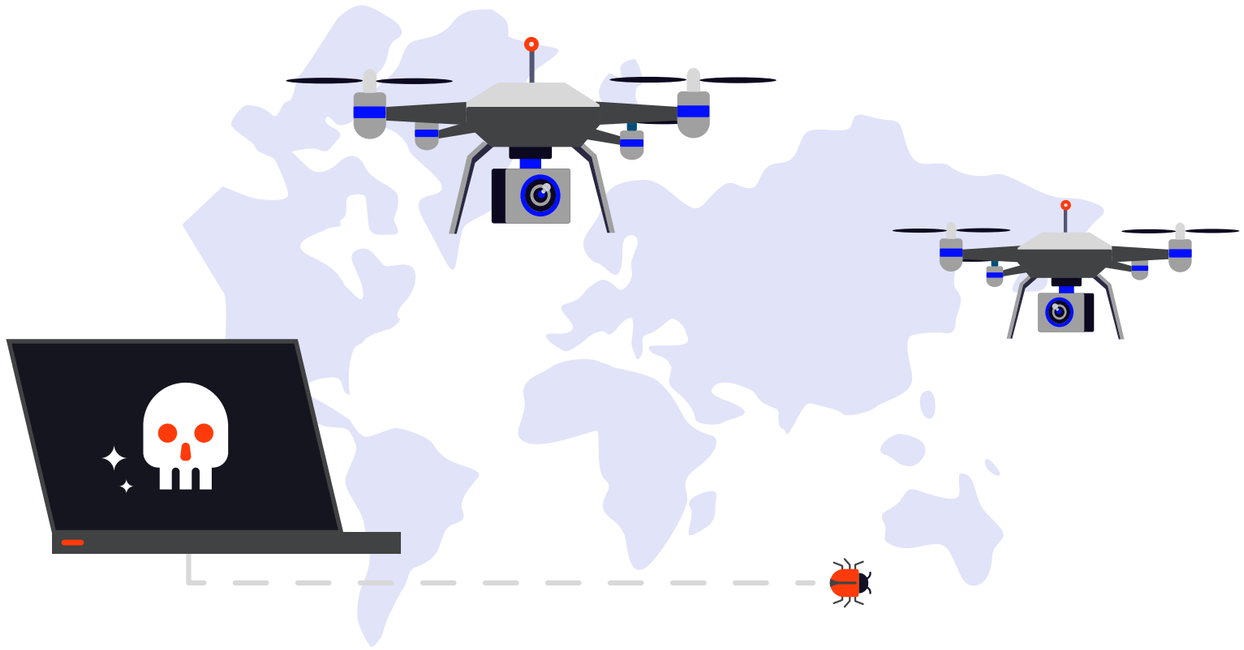
So what?

- China's regional territorial claims are significant drivers of geopolitical tensions and cyber activity in the global threat landscape. China's use of sanctions over diplomatic visits to Taiwan is rare, but not unprecedented.[33] The timing of China's decision to oppose now what appears to have been a regular occurrence in New Zealand, and long-running tensions with the Philippines, is inferred to be significant. Deliberately pushing boundaries with Western powers (and their allies) provides insight to China (and observing nations) into the willingness and limitations of countries (and the international community) to respond.

- These travel bans follow a series of acts reported in April, notably in the weeks before President Trump's visit to China on 13th May, which indicated Chinese confidence in taking a more assertive posture over regional strategic interests, particularly regarding Taiwan.

For example, public and active engagement with Taiwan's opposition government, imposing export bans on dual-use technology for specific European entities supplying weapons to Taiwan, and disrupting travel plans for Taiwanese officials through influence on African nations.[34,35,36] There is a risk of comparable shifts in China's decision-making over the use of its cyber capabilities.

- Broad espionage campaigns have the potential to identify new opportunities for China to test boundaries in other areas and assert its interests. Prepositioning in communications and defence networks may provide a layer of contingency planning, if risk taking creates outcomes assessed as less likely. Organisations involved in public, political, and policy activities relating to China, particularly where they overlap with efforts to limit Chinese interests or activities, are assessed as being at elevated risk during this ongoing period of Chinese assertiveness. China's proven advanced capabilities and history of adapting techniques and procedures once exposed require defenders to recognise the limitations of static IOCs, consider behaviour-based threat hunting, and pay attention to indicators of network activities at the margins of 'normal'.



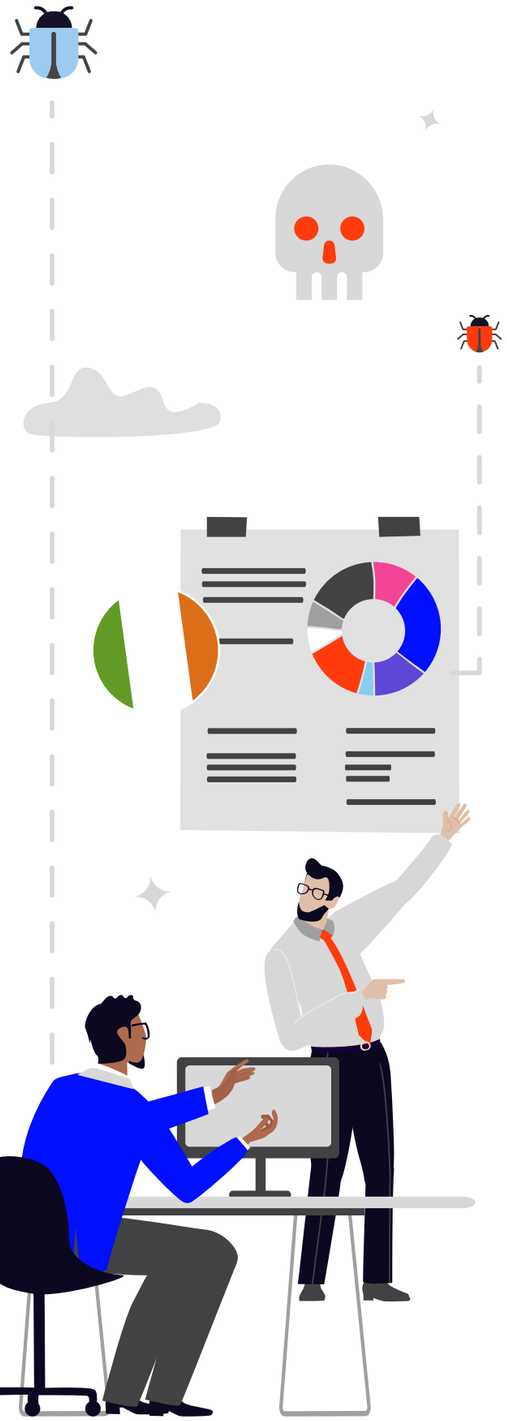
19/06/2026

On 19th June Ukrainian President Volodymyr Zelensky publicly issued an ultimatum to Belarus: remove military equipment used by Russia to guide drone attacks against Ukraine, or Ukraine would respond.[37] Multiple signal relay stations located close to the Belarus-Ukraine border were referenced, and a one-week deadline was set. On 24th June, Zelensky stated that the relay stations were no longer active. Speaking to the media, Belarusian President Lukashenko claimed to have reached an agreement with Ukraine.[38] Russian officials criticised the threat.[39]

So what?

- While Belarus has supported Russia since the start of the war against Ukraine in 2022, this incident falls within wider Ukrainian public accusations of Belarus increasing support to Russia's war effort. Recently, Zelensky described Belarus' 'development of border infrastructure for aggression', referring to upgraded roads and ammunition/fuel storage capabilities.[40] Additional criticism described Belarus' supply chain role, including refining Russian oil and manufacturing weapons components. It is unclear if Ukraine's increasing pressure on Belarus reflects a changing intelligence picture regarding the threat, or Ukraine's increasing confidence in its offensive capabilities.

- The concession suggests Belarus is reassessing both the domestic risk of supporting Russia's war against Ukraine, and Russia's capabilities as a protector. Despite recent attempts to establish relations with the US, Belarus remains politically isolated and dependent on its alliance with Russia for domestic stability.[41] Strategically, Belarus is important to Russia as a physical buffer to NATO's eastern border, for access to northern Ukraine, and for its role in Russia's oil economy.[42] If opportunities to support Russia without being drawn into the active military conflict become more limited, Belarus may extend support through other means, for example through its cyber capabilities. The most well-described threat is the Belarus-linked espionage threat tracked as Ghostwriter.[43] Historically, researchers have highlighted overlaps between Ghostwriter and the Russian nation-state cyber threat, although the nature and extent of these connections are not well understood.[44,45] Organisations exposed to Russian espionage threats should consider broadening their monitoring to include indicators associated with Ghostwriter activity. Reporting from June 2026 by Poland's CERT and multiple security vendors highlights both technical evolutions in this threat actor's phishing activity, and broader targeting observed in campaign activity.[46,47]



30/06/2026

Cyprus' six-month term as President of the Council of Europe (EUCO) ends on 30th June, passing to Ireland for the rest of 2026.[48] As part of the role, Irish representation will be highly visible in Brussels, deliver specific EU programmes, and host '22 informal ministerial meetings, two Leaders' Summits, and around 250 conferences and stakeholder engagements'.[49] Ireland intends to prioritise the themes of EU Competitiveness, Values and Security during its Presidential term.[50] Specific stated areas of planned focus include continued 'unwavering support for Ukraine', EU enlargement, advancing 'positive relations with the UK' and – within the current 'complex' geopolitical landscape – strengthening the 'EU's role as a principled global actor'.

So what?

- EUCO, as the EU institution comprising of government ministers from across EU member states, plays a key role in implementing EU strategy and seeking to coordinate alignment between member states on key issues and activities. As President, Ireland becomes a key influencer of action by member state governments and a high-profile representative of EU interests. This visibility temporarily elevates Irish risk of cyber threats by identifying Ireland as a specific proxy target for malicious activities driven by anti-EU sentiment or other geopolitical themes involving the EU. As reported in Cyprus, organisations across Ireland may experience higher levels of geopolitically motivated attack activity during the presidency period.[51] Beyond DDoS attacks, entities supporting Ireland's EU activities – or even just capable of being perceived to be involved – should consider increasing their awareness of and monitoring for indicators of compromise by actors linked to Russian and Chinese espionage activities; both well-established threats such as APT28 and APT29, returning threats such as Mustang Panda, and recently reported threats such as Sidewinder and Webworm.[52,53,54]

- Hacktivist claims or disinformation campaigns can coincide, or expressly reference, specific developments or announcements with geopolitical implications; for example targeting EU leadership members with deepfake content, or falsely claiming disruptive events were retaliation for sanctions against Russia.[55] Leaders of the EUCO are vulnerable as targets within the EU, due to their specific role adopting sanctions.[56]

- More broadly, Ireland's elevated position on the international stage during its presidency may be perceived by activists or threat actors as a six-month window of opportunity to maximise the notoriety or attention gained for their activities. This is not limited to hacktivism: Emerging opportunists or cybercriminal actors may recognise the opportunity to gain more media attention through attacks against targets linked to Ireland's presidential programmes, particularly for disruptive attacks. Finally, the relatively short period of EU-related focus may be leveraged by threat actors who rely on topical lures for phishing activities.

- Within the EU, Ireland (along with Spain) has persistently advocated for Palestinian interests, maintained a critical public narrative of Israel's military campaign and sought opportunities to promote acts of intervention by Ireland and the EU. Under Irelands Presidency, EUCO may facilitate more open debate than has previously occurred. Media investigations allege that Israeli cyber capabilities have been used against Western institutions considering the legality of Israeli activities.[57]

What NCC are watching

As complex strands of geopolitical developments dominate both media reporting and the attention of international governments and diplomatic efforts, low but persistent levels of reporting indicate a shift in posture, economic status, and confidence within North Korea, also known as the Democratic People's Republic of Korea (DPRK). As a country with active and advanced cyber capabilities, NCC continue to monitor DPRK developments to better understand the drivers of the current cyber threat landscape.

- North Korea is experiencing relative prosperity, attributed to weapons supply to Russia and cyber-enabled revenue including nation-state-sponsored crypto-theft.[58]

- Analysts assess North Korea as seeking to achieve tactical nuclear weapon and precision strike capabilities across South Korea.[59] In April, the US Congress assessed that the pace of ballistic missile tests had increased.[60] Testing activities and declared progress have since been reported monthly.[61,62,63]

- In April 2026, the UN's nuclear technology watchdog, the IAEA, reported "very serious" advances in DPRK's nuclear weapon production capabilities.[64]

- On 19th June, US President Trump was reported to have stated that he intended to now 'pay attention to the North Korea issue'.[65]

- DPRK continues to condemn US support of South Korea and dismiss diplomatic solutions or normalised relations with South Korea.[66,67,68]

- For the first time in 7 years, on 8th June, Chinese leader Xi Jinping visited North Korea and committed to expanding cooperation, including in areas of technology.[69]

- In March, North Korea signed a 'friendship' treaty with Belarus, initiating formal bilateral relations.[70]

Section 9
Dark web

Ongoing law enforcement operations targeting major infostealers including Lumma, Rhadamanthys, and StealC have reshaped the infostealer landscape. Previous disruptions often created market opportunities for competing developers, driving operators to seek alternative tools and contributing to a more competitive market.

Combined with Operation Endgame's takedown of the infrastructure supporting botnets such as IcedID, SmokeLoader, and Bumblebee, these actions have led to a shift from botnets and loaders as primary access vectors towards the use of stolen credentials, thereby increasing the demand for infostealers. In response, developers are increasingly adopting Software-as-a-Service (SaaS)-like models characterised by frequent updates, feature differentiation, and ongoing efforts to evade defensive measures.

Market overview

Since 1st April 2026, NCC Group has observed 21 distinct infostealer variants being actively marketed, updated, or leaked across multiple dark web forums. Nine new infostealers were announced this quarter, while updates for twelve existing infostealers were released.

Although this level of activity highlights a competitive market, comparison with Q1 2026 suggests that part of the market is characterised by churn, with many previously observed variants showing no visible development activity. This indicates that while numerous new entrants continue to emerge, only a subset achieves sustained adoption and maintenance alongside the established families.

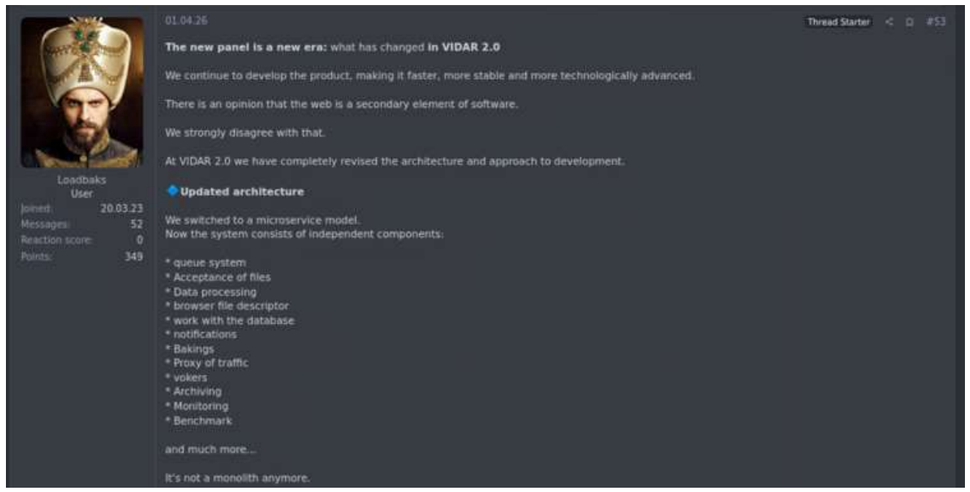


Figure 5: Vidar 2.0 update post showing continued feature development within an established infostealer family (translated from Russian)

Developers promote tools through dark web forums and Telegram channels, emphasising regular updates, technical support, and feature development. Observed offerings ranged from one-off software packages priced between USD 49.99 and USD 2,999 to subscription-based services with team licences, illustrating how infostealer developers are increasingly adopting commercial software business models.

StealC and Remus illustrate these contrasting development approaches. StealC relied on reputation, steady development, and operator trust before its June 2026 law enforcement disruption.

Remus, launched in February 2026, pursued an aggressive development cycle, receiving 44 updates during the quarter.

By comparison, Lumma, which had previously maintained one of the fastest update cadences among prominent infostealers, received only 20 updates in the first quarter of 2025 before its disruption in May 2025. Remus's update cadence therefore rivals or exceeds that of a former market leader, highlighting the increasing importance of rapid iteration and continuous feature delivery as competitive differentiators.

Capability development

Browser credential theft, session cookie harvesting, and cryptocurrency wallet extraction are now standard features across many infostealers and no longer provide meaningful differentiation. As a result, developers are increasingly competing through collection efficiency, flexibility, and stealth rather than the volume of data collected.

Several capabilities highlighted this quarter reflect the continued refinement and commercialisation of existing techniques. Storm Stealer demonstrates an efficiency-focused approach through dynamic browser discovery, scanning for common Chromium- and Gecko-based browser artefacts rather than relying on hard-coded browser lists.

This provides broader compatibility and reduces the need for frequent updates as new browsers or versions emerge. Lunax, meanwhile, differentiates itself through browser extension-based credential theft, enabling real-time credential theft before credentials are submitted while also allowing manipulation of web content without altering the visible URL. These capabilities reduce reliance on stored browser data and improve collection effectiveness.

Collectively, these examples suggest developers are increasingly focused on improving how data is collected rather than expanding what can be collected. Competitive pressure and evolving defensive measures are driving greater investment in stealth, efficiency, and flexibility, contributing to the growing operational maturity of the infostealer market.

Evasion and execution

Across Q2 2026, developers consistently emphasised detection avoidance in advertisements, with many positioning their tools as fully undetectable or resistant to modern endpoint security controls. This focus indicates both increased defensive pressure and the importance of stealth as a selling point. NCC Group has observed multiple stealer variations that adopt distinct approaches to evasion, broadly spanning code obfuscation, execution masking, and behavioural blending.

Aura Stealer demonstrates a code-centric approach, using a virtualisation engine that generates a unique virtual CPU and instruction set for each build. By ensuring that samples do not share identical execution logic, this technique complicates analysis and reduces the effectiveness of signature-based detection.

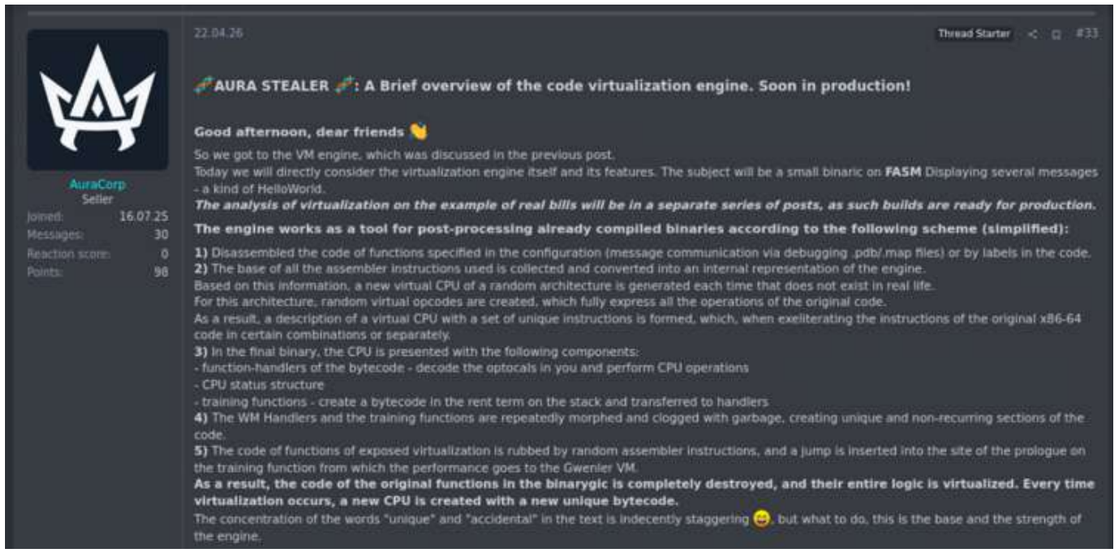


Figure 6: Aura post explaining its code virtualisation engine (translated from Russian)

Xia takes an execution-masking approach, relying on DLL sideloading to execute through trusted applications and employing rootkit-style concealment to hide files, processes, registry keys, and network activity.

The combination of trusted-process abuse and stealth functionality is notable because it more closely resembles tradecraft traditionally associated with higher-end intrusion tooling than commodity infostealers.

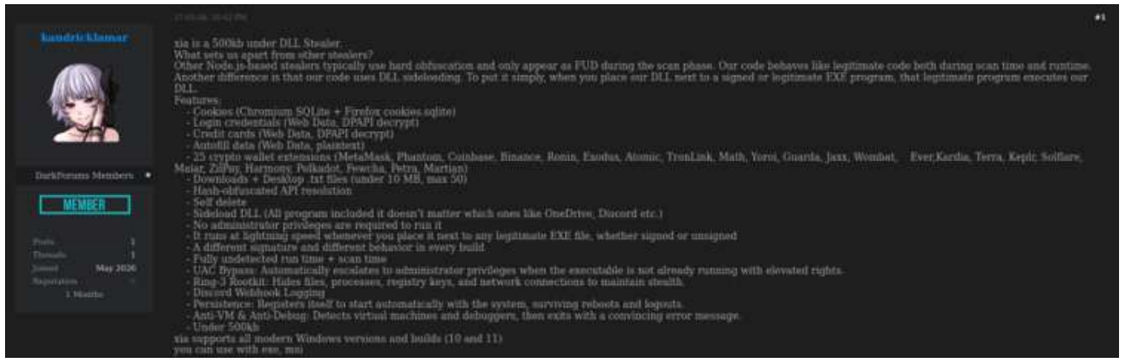


Figure 7: Xia advert highlighting DLL sideloading

Defensive developments

Software vendors and identity providers are beginning to introduce measures aimed at reducing the effectiveness of the access artefacts targeted by infostealers. A notable example is Google's rollout of Device Bound Session Credentials (DBSC), which cryptographically links user sessions to the user's hardware, such as the Trusted Platform Module (TPM) on Windows or the Secure Enclave on macOS, making stolen Google session cookies unusable without access to the underlying hardware-bound key.

Similar trends are emerging across identity control platforms. Okta's use of Secure Enclave-backed keys in its Single Sign-On (SSO) for its Device Access Platform for macOS and Microsoft's promotion of passkey adoption as an alternative to traditional passwords reflect a broader shift towards minimising the dependence on authentication methods that can be stolen or replayed.[71,72]

However, these measures do not significantly reduce the usefulness of stolen credentials, as stolen credentials and session data from platforms without equivalent protections remain valuable. Rather than eliminating the utility of infostealers, these developments are more likely to influence how developers differentiate their tools, encouraging greater focus on enterprise credential theft, cross-platform collection, and alternative access methods.

Assessment

The observed activity in Q2 2026 highlights a more competitive but unevenly mature infostealer market. While a significant number of new variants continue to emerge, earlier observations from Q1 2026 suggest that many of these entrants may be short-lived and show little sustained growth. Meanwhile, a more stable and commercialised subset of the market is distinguishing its tools through efficiency, stealth, and reliability of delivery rather than solely through data collection capability.

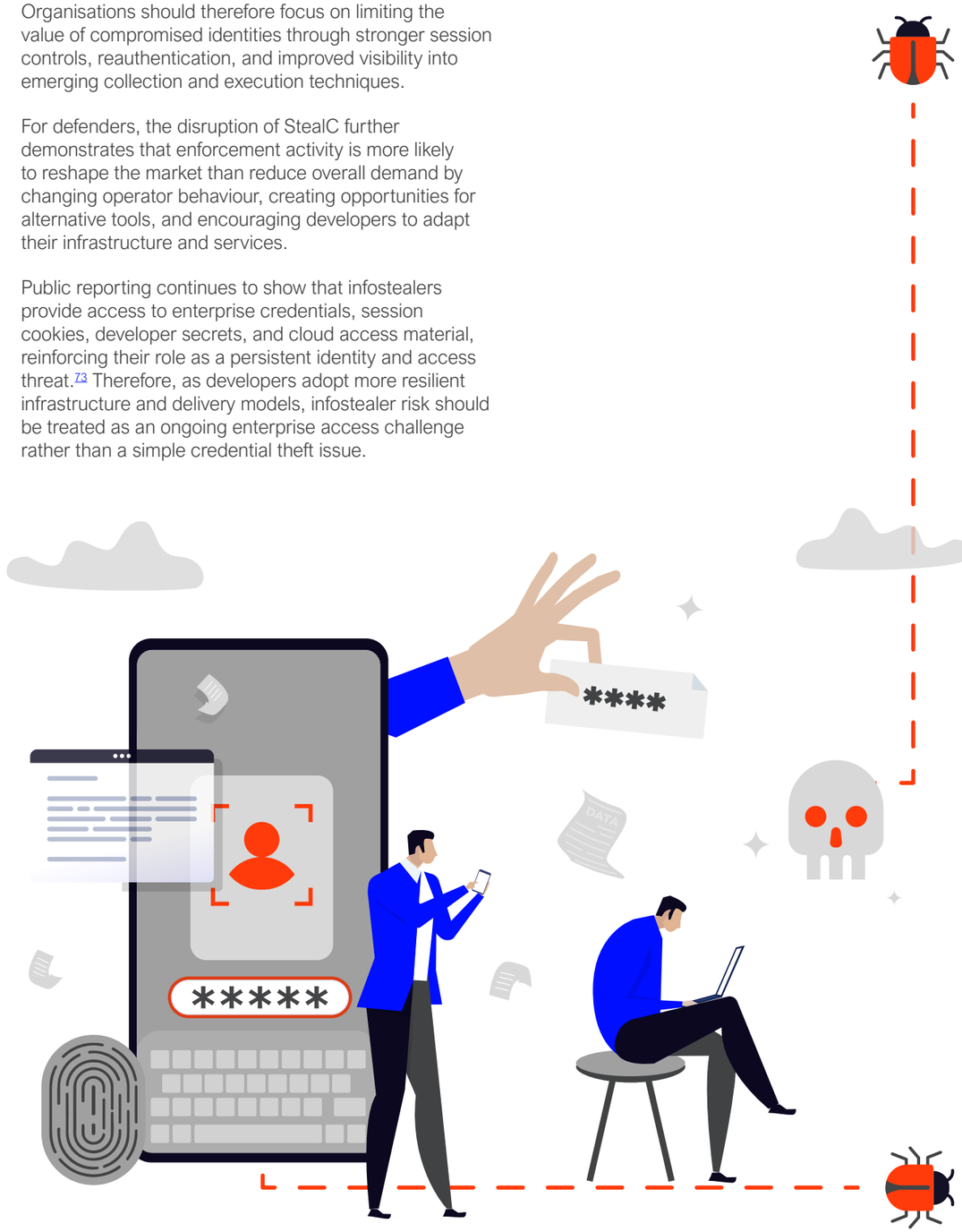
For defenders, the practical challenge is that some of the most marketable improvements now reduce the visibility of malicious activity on the endpoint. Techniques such as off-host processing, trusted-process execution, and browser extension-based collection reduce the effectiveness of detection approaches that rely on identifiable endpoint artefacts. At the same time, the commercialisation of the market enables successful innovations to spread rapidly across competing products.

Additionally, the increasingly commercial nature of the market means that improvements in one successful product can spread quickly as competitors respond with their own updates and feature claims. This is reflected in the frequent updates observed from stealers such as Remus, as well as the pre-disruption maintenance of established families like StealC, which relied on steady development and operator trust to remain competitive.

Defensive measures such as Device Bound Session Credentials are likely to reduce the value of replaying stolen browser sessions in protected environments, but they do not materially reduce the broader utility of stolen credentials and session artefacts from other platforms. Organisations should therefore focus on limiting the value of compromised identities through stronger session controls, reauthentication, and improved visibility into emerging collection and execution techniques.

For defenders, the disruption of StealC further demonstrates that enforcement activity is more likely to reshape the market than reduce overall demand by changing operator behaviour, creating opportunities for alternative tools, and encouraging developers to adapt their infrastructure and services.

Public reporting continues to show that infostealers provide access to enterprise credentials, session cookies, developer secrets, and cloud access material, reinforcing their role as a persistent identity and access threat.[73] Therefore, as developers adopt more resilient infrastructure and delivery models, infostealer risk should be treated as an ongoing enterprise access challenge rather than a simple credential theft issue.



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.

One global business working seamlessly together

Under cyber attack?

Call our 24/7
Incident Response Hotline now.

NCC Group:
+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