ncc group | FOX IT part of ncc group

Cyber Threat Intelligence Report

Review of Q3 2026

Contents

03 **Section 1**
Executive summary

04 **Section 2**
Timeline of critical incidents Q3 2026

06 **Section 3**
Ransomware key statistics: Q3 2026

08 **Section 4**
Ransomware insights

10 **Section 5**
Ransomware spotlight: Gunra ransomware group

14 **Section 6**
Cyberattack against a UK power generation facility: Implications for critical infrastructure

16 **Section 7**
Emerging cyber security trend: The evolution of BraZetsu into an advanced Initial Access Broker

18 **Section 8**
Threat outlook: When AI agents cross the line - misalignment becomes an enterprise security threat

20 **Section 9**
Geopolitical developments

25 **Section 10**
Dark web landscape

Section 1
Executive summary

The cyber threat landscape intensified during Q3 2026, with organisations facing increased ransomware activity, persistent exploitation of internet-facing infrastructure, and a more specialised cybercriminal access market. Reported ransomware victims increased by approximately 23% quarter-on-quarter, rising from 2,325 in Q2 to 2,865 in Q3. Industrials remained the most frequently affected sector, while organisations in North America and Europe accounted for the largest proportion of reported victims. Qilin and The Gentlemen were among the most active ransomware groups, while emerging operations such as Deadlock and Storm demonstrated how quickly new entrants can develop credible, cross-sector capabilities.

Ransomware operations continued to mature through affiliate-based delivery models, cross-platform encryption, data theft, and double-extortion tactics. Gunra illustrates this progression, having developed from an emerging ransomware family into a structured Ransomware-as-a-Service operation. Its affiliates have exploited vulnerabilities in internet-facing Fortinet devices, obtained credentials and session cookies, moved laterally using widely available administration tools, and deployed both Windows and Linux ransomware variants. This highlights how leaked malware code, affiliate recruitment, and the rapid exploitation of vulnerable perimeter systems allow newer groups to scale their operations quickly.

The exploitation of internet-facing systems remained a significant initial-access route. More than 40 vulnerabilities affecting enterprise applications, VPN appliances, email gateways, and management platforms were added to the CISA Known Exploited Vulnerabilities Catalogue during the quarter. Organisations should maintain an accurate external asset inventory, prioritise remediation based on active exploitation, restrict access to administrative interfaces, and monitor remote-access infrastructure for suspicious behaviour.

Initial Access Brokers also continued to play a central role in the cybercriminal ecosystem. Access to VPNs, FortiGate appliances, Remote Desktop Web Access, RDP, and SSH environments remained widely advertised. However, brokers increasingly offered access to cloud identities, source code repositories, CI/CD environments, security-management platforms, government services, and operational technology.

This indicates that the value of compromised access is increasingly determined by the operational control it provides rather than solely by the victim organisation's size or revenue.

The quarter also demonstrated the potential for cyber incidents to cause physical and operational disruption. A cyberattack against a small UK power-generation facility resulted in an operational shutdown lasting approximately four days. Although national electricity supplies were not affected and attribution remains unconfirmed, the incident highlights the risks faced by operational technology environments.

Agentic AI also emerged as a developing enterprise security concern. Recent incidents demonstrated how legitimate AI agents can access external systems without appropriate authorisation. Although these incidents were not necessarily malicious, they show that misaligned agents can create consequences resembling conventional intrusions. As AI agents gain the ability to browse, authenticate, execute code, and modify data, organisations will require stronger permission boundaries, monitoring, containment, and disclosure processes.

Overall, Q3 2026 was characterised by increased attack volumes, rapidly evolving ransomware operations, and greater cybercriminal specialisation. Organisations should prioritise internet-facing asset management, identity and privileged-access controls, cloud and development-environment monitoring, network segmentation, and tested backup, incident-response, and operational-recovery capabilities. These measures provide resilience against the common access and escalation techniques used across multiple threat groups.

Section 2

Timeline of critical incidents Q3 2026

July

08/07/2026

Accenture confirmed a breach after a threat actor known as “888” claimed to have stolen approximately 35GB of source code and credentials, including Azure access tokens and SSH keys. The attacker allegedly gained access to internal Azure DevOps repositories and extracted proprietary code and sensitive authentication material. The exact intrusion vector was not publicly disclosed. Accenture stated that the source of the breach had been remediated, reported no operational impact, and began assessing the validity and scope of the stolen data claims.[1]

16/07/2026

Hugging Face disclosed that attackers breached its production infrastructure, gaining access to internal datasets and credentials in what was described as an attack conducted by an autonomous AI-agent framework. Attackers uploaded a malicious dataset that exploited vulnerabilities in Hugging Face’s data-processing pipeline, enabling code execution, credential theft, and lateral movement between internal systems. The company revoked credentials, rebuilt affected infrastructure, patched vulnerabilities, involved law enforcement, and advised users to rotate access tokens.[2]

20/07/2026

Ernst & Young (EY) investigated a breach affecting sensitive personal and financial information, following claims by the ShinyHunters threat group that it had accessed company data. Attackers allegedly gained unauthorised access to systems containing employee and customer information. Public reporting indicates cybercriminal access and subsequent attempts to monetise or leak stolen data. EY launched an investigation, notified potentially affected individuals, coordinated with authorities, and implemented remediation measures while assessing the impact on clients and employees.[3,4]

29/07/2026

The UK Department for Education confirmed a cyber incident after more than 600,000 records were reportedly stolen and later leaked online, affecting students, parents, and education stakeholders. An unidentified threat actor allegedly compromised systems containing education-related records and exfiltrated large volumes of sensitive data before publication. Authorities launched an investigation, notified affected individuals, reviewed security controls, and worked with law enforcement and cyber security partners to assess and contain the impact.[5,6]

August

08/08/2026

The UAC-0145 threat cluster targeted IT professionals through fake job recruitment processes, tricking victims into installing malicious VPN software capable of executing commands. Attackers impersonated recruiters, conducted interviews, and convinced candidates to install a trojanised WireGuard-based VPN client known as SopraVPN, which delivered malicious payloads. CERT-UA and security researchers issued alerts, organisations reviewed recruitment-related risks, and defenders were advised to implement stricter endpoint and VPN controls.[7]

17/08/2026

The Cl0p ransomware group claimed to have stolen data from Philips and General Electric (GE) during a large-scale extortion campaign. Attackers exploited a critical vulnerability in PTC Windchill/FlexPLM software, gaining unauthorised access to systems used to store engineering and product-development information. Philips confirmed investigation of a compromised internal server, while affected organisations assessed potential intellectual property exposure and strengthened monitoring efforts.[8]

17/08/2026

Shell was listed among organisations allegedly compromised during the Cl0p extortion campaign exploiting PTC software vulnerabilities. Threat actors exploited a critical remote code execution flaw in internet-facing PTC Windchill infrastructure and claimed to have stolen engineering-related documents and project data. Shell confirmed it was investigating the incident with cyber security experts while evaluating the authenticity and impact of Cl0p’s claims.[9]

27/08/2026

A cyber incident affecting airport WiFi platforms reportedly exposed data belonging to approximately nine million passengers connected to major UK airports. Attackers allegedly gained access to systems supporting airport WiFi and associated customer databases, resulting in large-scale data exposure. Affected organisations launched investigations, notified regulators, reviewed third-party supplier security, and implemented measures to strengthen passenger data protection.[10]

September

14/09/2026

Revolut disclosed a breach involving customer information, including financial data and identity documents such as passports. Attackers reportedly gained unauthorised access to systems containing customer records and extracted sensitive information. Revolut initiated incident response procedures, notified affected customers, worked with regulators, and implemented additional monitoring and security controls.[11]

15/09/2026

CenterPoint Energy confirmed that a cyberattack resulted in customer information being stolen, raising concerns about impacts on a major energy provider. Threat actors breached company systems, exfiltrated customer-related data, and attempted to leverage the stolen information for criminal purposes. The company launched an investigation, notified potentially affected individuals, coordinated with law enforcement, and enhanced protections around critical and customer-facing systems.[12]

19/09/2026

The ShinyHunters group claimed to have compromised the leak infrastructure of rival ransomware group Cl0p, exposing internal data and threatening extortion. ShinyHunters allegedly gained unauthorised access to Cl0p’s leak platform and extracted information associated with the ransomware operation. The event sparked significant discussion within the cybercriminal ecosystem, potentially damaging trust among ransomware affiliates and exposing operational security weaknesses.[13]

23/09/2026

ShinyHunters claimed to have breached systems associated with the FBI and obtained employee-related information. The exact intrusion method remained unclear, and public information primarily came from the threat actors’ claims. The claim triggered scrutiny from the security community and law enforcement. Investigators began assessing the authenticity of the breach, the scope of any exposed data, and potential operational impacts if the claims are verified.[14]

Section 3

Ransomware key statistics: Q3 2026

23%

Global ransomware attacks increased by 23% in Q3 2026

29%

Industrials accounted for 29% of ransomware attacks in Q3 2026

13%

Qilin was responsible for 13% of attacks in Q3 2026

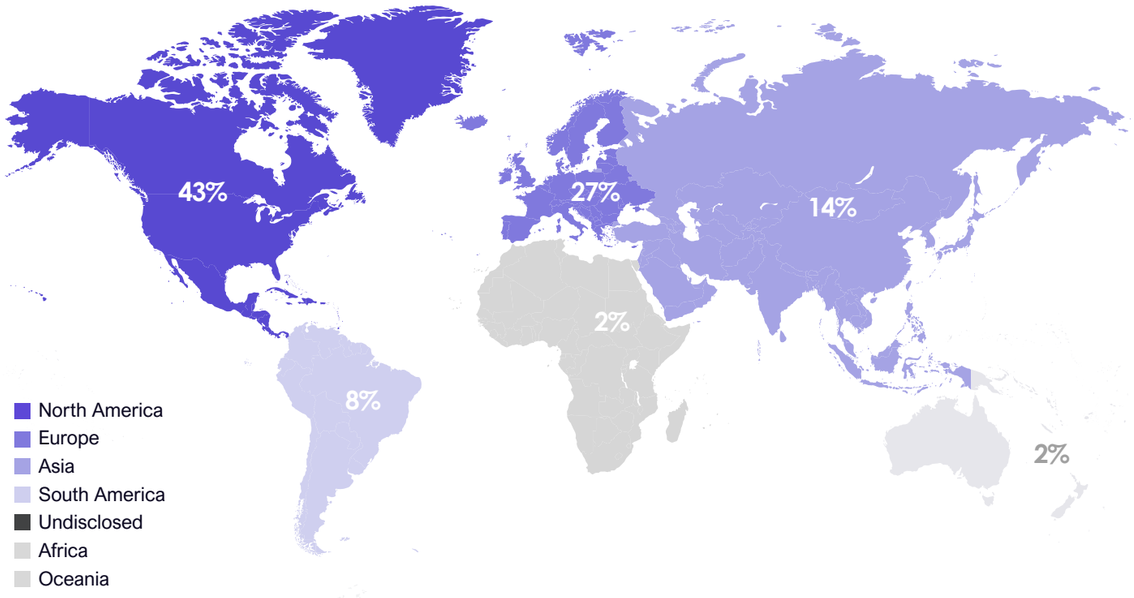


Figure 1: Ransomware attacks by region, Q3 2026

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

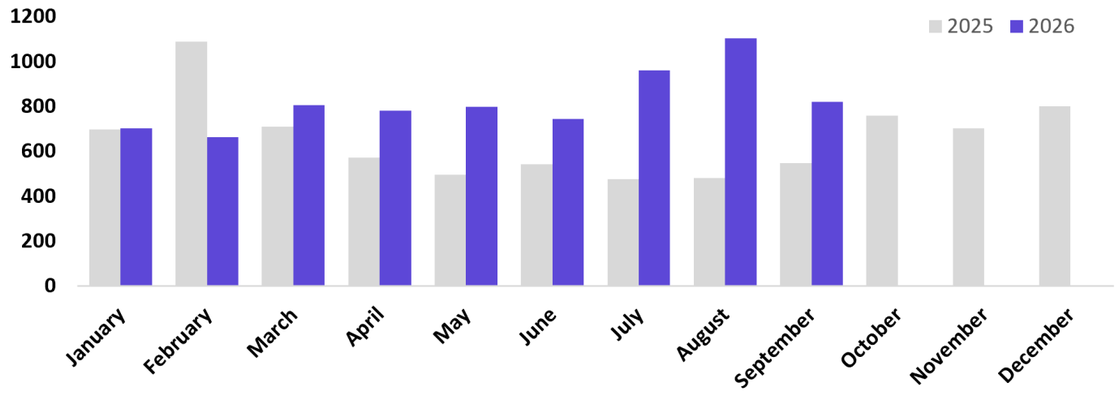


Figure 2: Ransomware attacks by month 2025 – 2026

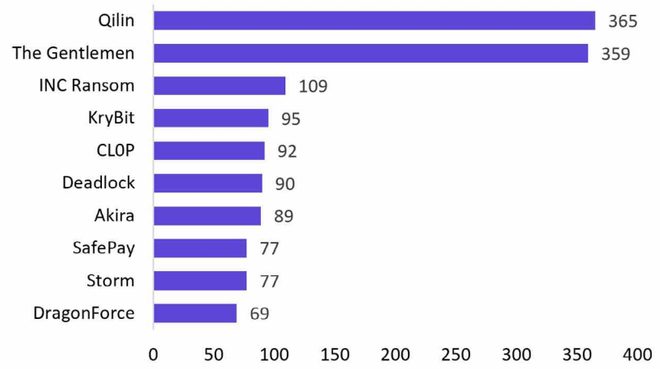


Figure 3: Top threat actors, Q3 2026

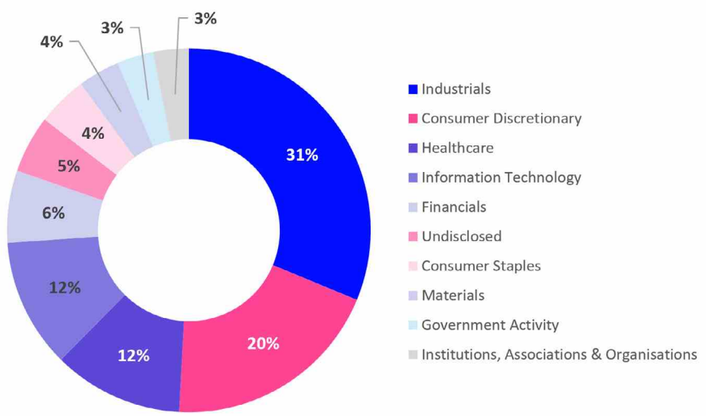


Figure 4: Top targeted sectors, Q3 2026

Key events

July 2026
Indra Group

Indra Group, a major Spanish defence and aerospace contractor and NATO cyber coalition member, confirmed a ransomware incident affecting its subsidiary after The Gentlemen ransomware group threatened to leak stolen data. Attackers reportedly exfiltrated data and attempted extortion via a dark web leak site, although the full extent of the exposure was not disclosed.

August 2026
UK Police National Legal Database (PNLD)

PNLD confirmed that government, police, and customer contact information had been published on the dark web. PNLD reported no evidence of account compromise, and the number of affected individuals remains unknown. ExfilSquad listed PNLD on its leak site, but the attack has not been attributed to the group.

September 2026
Harley-Davidson

CI0p has allegedly breached Harley-Davidson. Harley-Davidson has not confirmed the specific scope, method, and impact of the attack.

Section 4
Ransomware insights

Ransomware activity increased by 23% in Q3 2026, rising from 2,325 victim claims in Q2 to 2,865. Growth was driven both by established groups and the emergence of new threat actors. Industrials remained the most targeted sector, followed by Consumer Discretionary, Information Technology, Healthcare, and Financials. The quarter also highlighted the ecosystem's evolution towards affiliate-driven models and data-centric extortion.

Qilin remained the most active ransomware group for the sixth consecutive quarter, recording 365 victims. The Gentlemen followed with 356, while INC Ransom ranked third with 109. Emerging groups Deadlock and Storm were among the quarter's notable developments, while extortion-focused operations such as ShinyHunters demonstrated the growing convergence of ransomware, data theft, and specialised cybercriminal business models.

Qilin and The Gentlemen

Qilin and The Gentlemen remained the two leading ransomware groups throughout Q3 2026, continuing their dominance from the previous quarter. Both sustained high operational tempos over the last three months. In August, Qilin published 15 victims within 24 hours as part of a broader cross-sector disclosure surge.[15]

The group also claimed the US Bureau of Alcohol, Tobacco, Firearms and Explosives, which confirmed that an isolated system containing investigative information had been breached.[16]

The Gentlemen similarly increased activity, from 279 claimed victims in Q2 to 356 for Q3. Microsoft Threat Intelligence published a detailed technical analysis of the group's ransomware, documenting a proprietary self-propagating Go-based encryptor, aggressive lateral-movement capabilities, and double-extortion model, providing further insight into the operation's technical sophistication and potential for widespread network impact.[17]

CI-ISAC Australia also issued an advisory warning that affiliates were targeting Australian critical infrastructure through unpatched FortiGate devices and exposed remote-access services.[18]

Both Qilin and The Gentlemen continued technical development, affiliate expansion, and broad targeting, reinforcing their position at the forefront of the ransomware landscape.

Deadlock

Deadlock expanded its ransomware operations throughout Q3 2026, maintaining victim disclosures across sectors and regions. The group uses a double-extortion model, combining data theft and file encryption with threats to publish stolen information.[19,20,21]

Throughout the quarter, Deadlock claimed organisations across healthcare, manufacturing, telecommunications, logistics, legal, and professional services, demonstrating broad targeting and sustained activity.

A notable development was increased attention to the group's technical capabilities. Microsoft Threat Intelligence reported that Deadlock uses a Rust-based encryptor and decentralised recovery infrastructure built on blockchain technology, making elements of its extortion ecosystem more resilient to law-enforcement disruption.

Microsoft also assessed Deadlock as a capable threat actor with a growing footprint and mature operational model.[22]

The group's continued growth and investment in resilient infrastructure demonstrate its ability to adapt while maintaining a high operational tempo. This combination of technical sophistication and consistent activity established Deadlock as a prominent ransomware threat during Q3 2026.

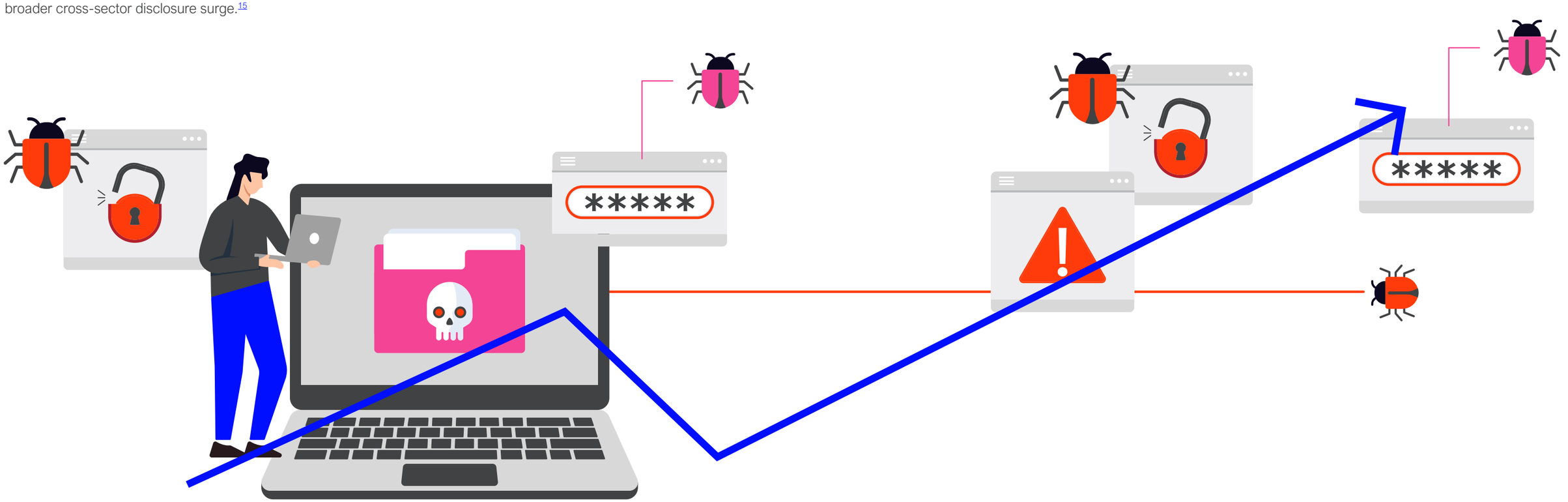
Storm

Storm emerged as a notable ransomware operation in Q3 2026, rapidly building a cross-sector victim portfolio after first appearing in August. The group employs double-extortion, combining data theft with threats to publish stolen information on its leak site. Although Storm primarily targeted US organisations, its victim listings also covered Australia, Canada, and Europe.[23,24]

Storm's activity accelerated during the quarter. On 25th August, researchers reported that the group had published seven victims within 72 hours across government, healthcare, financial services, transportation, and manufacturing.[25] The concentrated disclosures suggested either a coordinated campaign or batch publication of previously compromised organisations. By the end of September, Storm had claimed 78 victims.[26]

One notable claim involved Star Aviation, a Kentucky-based supplier supporting Boeing and Airbus. Published samples allegedly included technical schematics and employee identification documents, highlighting potential supply-chain risks.[27]

Storm's rapid growth, broad targeting, and sustained disclosure activity make it an emerging ransomware threat requiring close monitoring in Q4 2026.



Section 5

Ransomware spotlight: Gunra ransomware group

On 10th August 2026, a joint advisory from the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), United States Secret Service (USSS), and the Republic of Korea National Police Agency (KNPA) was released, warning organisations about the threats posed by Gunra ransomware. Gunra is a Ransomware-as-a-Service (RaaS) operation that targets government entities, critical infrastructure, and private organisations worldwide.[28]

Gunra first emerged in April 2025 as a double-extortion ransomware that has notable code similarities to the infamous Conti ransomware. In its early days, Gunra was observed targeting Windows environments, then in mid-2025 a Linux variant surfaced, expanding the group's capabilities across multiple operating systems.[29]
In January 2026, the operators formally launched a RaaS affiliate programme on dark web forums, enabling affiliates to deploy malware while sharing ransom proceeds with the operators.[30]

The development of Gunra from a newly emerged ransomware variant into a fully operational RaaS platform demonstrates the continued evolution of the ransomware landscape. Reported overlaps with the leaked Conti ransomware source code may indicate that Gunra's operators initially leveraged aspects of Conti's codebase to support their development efforts, then moved to recruiting affiliates and targeting internet-facing systems. These factors have likely contributed to scaling its operations and expanding its victim reach.

From malware to Ransomware-as-a-Service

Analysis of Gunra indicates that it shares similarities with the leaked source code of the infamous Conti ransomware. Following the leak, several ransomware groups, including Royal and Black Basta, emerged with operational or technical links to Conti, leveraging either former members, tactics, or elements of the leaked codebase.[31,32] Gunra appears to represent another evolution of this trend, demonstrating how leaked ransomware frameworks continue to enable the development of new threat groups.[33]

In January 2026, Gunra expanded its operation through a structured RaaS affiliate programme advertised on dark web forums. The group reportedly recruited affiliates with network intrusion capabilities and other technically skilled individuals to act as Initial Access Brokers (IABs), offering a share of ransomware proceeds in exchange for compromised enterprise network access.

This transition significantly increases Gunra's threat potential by enabling affiliates to conduct attacks on the group's behalf, thereby expanding its operational scale and geographic reach without a corresponding increase in its core workforce. As a result, Gunra can target a greater number of organisations simultaneously while maintaining a relatively small organisational structure. The shift to a RaaS model also lowers the barrier to entry for attackers by providing access to ransomware tools and support services. This can make it difficult for defenders to attribute attacks to specific threat actors and disrupt their operations.[34,35]

How Gunra operates

Gunra and its affiliates have targeted organisations across a wide range of industries globally. As of Q3 2026, we have observed 53 victims across multiple sectors including industrials, consumer discretionary, financial, healthcare, and materials sectors. Geographically, the Asia-Pacific region accounts for the highest concentration of victims, followed by Europe and North America.

This victim distribution differs from the broader ransomware trends, in which North America and Europe are typically the most heavily targeted regions. While the reason for this remains unclear, the observed victimology may indicate that Gunra and its affiliates may have stronger access opportunities or operational familiarity within the Asia-Pacific region.

Early analysis of a Gunra sample showed that the ransomware primarily targeted Windows environments and incorporated several anti-analysis and evasion techniques designed to minimise detection. The use of these capabilities demonstrates a level of operational maturity that is increasingly common among modern ransomware groups.[36]

Beyond file encryption, Gunra employs a double-extortion model in which sensitive victim data is exfiltrated prior to encryption. The group typically imposes a five- to seven-day deadline for negotiations and threatens to release the exfiltrated data publicly if organisations fail to comply, increasing both the financial and reputational pressure on victims.

Exploitation of internet-facing systems

Over the past several months, we have seen a continuing trend of threat actors leveraging vulnerabilities in exposed internet-facing assets to gain initial access to victim environments. Threat actors are increasingly targeting externally accessible security appliances, VPN infrastructure, management consoles, and enterprise applications that can provide direct access into victim networks. Gunra is one group we have seen perpetuating this trend.

The continued exploitation of these technologies demonstrates that internet-facing systems remain an attractive initial access vector for both financially motivated and state-sponsored threat actors.

Threat actors are likely to monitor vendor advisories, security research publications, proof-of-concept releases, and updates to the CISA KEV Catalogue to identify newly disclosed vulnerabilities. Once public exploit code becomes available, threat actors can quickly operationalise vulnerabilities against exposed systems.

These developments underline the need for organisations to maintain strong visibility over internet-facing assets as part of their vulnerability management efforts. Externally exposed appliances, VPN gateways, firewalls, remote access services, management platforms, and other perimeter technologies should be regularly identified, monitored, and updated to reduce opportunities for exploitation. This is particularly relevant given Gunra's observed exploitation of CVE-2024-55591 and CVE-2025-24472 in internet-facing Fortinet devices to establish initial access. The group's activity highlights how these vulnerabilities affecting perimeter infrastructure can provide a route to network compromise and subsequent ransomware deployment.

Mitigations and recommendations

The recent activity with Gunra demonstrates how modern ransomware operations increasingly rely on the exploitation of vulnerable internet-facing systems to gain initial access. Organisations should therefore prioritise the remediation of known exploited vulnerabilities, particularly those affecting internet-facing systems, and ensure that operating systems, firmware, and security appliances are updated in a timely manner.

Given Gunra's use of stolen credentials and session hijacking techniques, organisations should review the effectiveness of existing identity and access controls. The use of multi-factor authentication, regular reviews of privileged accounts, and monitoring for unusual authentication activity can help reduce the risk of unauthorised access. Access to administrative interfaces, VPN infrastructure, firewalls, and management platforms should also be restricted to authorised users and monitored for signs of suspicious activity.

Gunra has also been observed using tools such as Impacket to dump credentials, execute commands remotely, and move between systems following initial access. As a result, organisations should consider implementing network segmentation to limit the spread of an intrusion and review privileged account permissions to ensure administrative access is only granted where required. Maintaining a reliable backup and recovery procedures also remain critical damage mitigation steps.

Organisations should additionally maintain visibility of internet-facing assets through regular attack surface reviews and vulnerability assessments. Monitoring for unusual account activity, web shells, remote execution tools, and other indicators of compromise can help identify malicious activity before it progresses to the ransomware stage. Collectively, these measures can help reduce both the likelihood and potential impact of attacks conducted by Gunra and other ransomware operators.

Final thoughts

Gunra demonstrates how ransomware operations continue to evolve through a combination of proven malware development practices, affiliate-driven business models, and the exploitation of internet-facing systems. While the group itself is relatively new, many of the techniques observed throughout its operations are not. The use of leaked ransomware code, partnerships with affiliates, credential theft, lateral movement tools, and the exploitation of known vulnerabilities reflect a broader trend across the ransomware ecosystem where threat actors increasingly prioritise speed, scalability, and operational efficiency.

As demonstrated by both Gunra and other recent ransomware activity, internet-facing assets continue to present significant opportunities for attackers, particularly when vulnerabilities remain unpatched.

For organisations, reducing ransomware risk is less about defending against a specific group and more about strengthening the security controls that prevent common intrusion methods from succeeding. Maintaining visibility over internet-facing assets, prioritising remediation of known exploited vulnerabilities, protecting privileged accounts, and ensuring effective backup and recovery procedures remain critical measures. While new ransomware groups will continue to emerge, organisations with strong vulnerability management, identity security, and layered defensive controls are better positioned to reduce both the likelihood and impact of a successful attack.

Section 6
Cyberattack against a UK power generation facility: Implications for critical infrastructure

Context and location of the incident

In July 2026, a cyberattack targeted a small power generation facility in the United Kingdom, forcing the plant to cease operations for approximately four days. Although the affected organisation's name and location were not publicly disclosed, UK authorities confirmed that the facility was a small-scale electricity generator and that the incident did not threaten the stability of the national grid.[37,38] The attack attracted significant attention because it represented one of the few publicly reported cases in which a cyber incident directly resulted in the operational shutdown of a UK energy asset. Becoming public in August, this attack is widely suspected to be the activity of Iranian threat actors due to heightened geopolitical tensions at the time, though no formal attribution has been made by the UK government.[39]

Attack overview

Although the technical details have not been publicly released, the reported activity is consistent with activity previously observed in Iranian-affiliated campaigns against critical infrastructure such as the 30 Minnesota water facilities targeted in July 2026.[40] These have included targeting internet-exposed Programmable Logic Controllers (PLCs), establishing remote access to Operational Technology (OT) devices, interacting with PLC project files, and manipulating Human-Machine Interface (HMI) or Supervisory Control and Data Acquisition (SCADA) displays to cause operational disruption. These TTPs are relevant to the UK incident because similar activity has been documented against energy and water infrastructure, although there is currently no public evidence confirming that the same techniques were used against the UK facility.

After establishing access, the attackers were able to interfere with operational processes to the extent that the power plant had to be taken offline for four days.

Public reporting does not provide sufficient technical detail to determine which specific operational processes or control systems were affected. With limited details released, it is difficult to assess the full intent of the attack and whether it should be classified as a success by the threat actors.

However, this does display the capabilities and intent of threat actors to target critical infrastructure, with real world impacts.[41]

Following the incident, the UK government continued to engage with energy-sector organisations on cyber resilience and published a four-year strategy setting out measures to strengthen the sector's ability to identify, detect, respond to and recover from cyber threats.[42]

Organisations and entities involved

Several organisations played a role in response and analysis of the incident. The Department for Energy Security and Net Zero (DESNZ) confirmed that a small-scale generator had been affected while reiterating that there was no risk to the wider UK energy system.

The National Cyber Security Centre (NCSC), which is responsible for protecting UK critical national infrastructure from cyber threats, was involved in supporting cyber security efforts across the sector. Although the agency did not publicly release technical details, its role highlights the importance of coordinating public-private partnerships when responding to incidents affecting critical services.

Attribution remains unconfirmed. Some reporting has linked the activity to Iran-affiliated actors, citing similarities with previous Iranian campaigns targeting critical infrastructure.[43,44,45] Other state-sponsored groups, including Russian actors, have also demonstrated capabilities and a history of targeting energy infrastructure. The incident should therefore be considered unattributed unless additional technical or intelligence evidence becomes available.

Implications for critical infrastructure and OT systems

The attack demonstrates that cyber threats can have direct operational consequences in critical infrastructure environments. Unlike traditional IT incidents that primarily affect data or business systems, attacks against energy facilities can potentially disrupt physical processes and affect the availability of essential services.

Even though the affected plant represented only a small portion of UK generating capacity, the incident demonstrated that relatively limited cyber activity can produce a real-world operational effect.

The event highlights the security challenges created by the increasing connectivity of IT and OT environments.[46] This trend is driven in part by legitimate operational requirements: energy and industrial operators increasingly use remote monitoring and administration, real-time analytics, centralised management, predictive maintenance, and third-party maintenance services to improve efficiency and reduce the need for personnel to be physically present at operational sites.

The NCSC notes that these developments have made OT environments more interconnected, while also increasing the potential attack surface through remote-access solutions, third-party connections and integration with enterprise systems. Each additional connection creates another pathway that must be secured, monitored, and appropriately segmented. This is particularly important where legacy OT systems, which weren't designed with modern connectivity or security requirements in mind, are connected to newer digital infrastructure, representing scope creep from their original intended purpose.

The incident also illustrates why the significance of a cyberattack cannot be measured solely by the scale or duration of the immediate disruption. Although the direct impact in this case was limited, successfully affecting an operational asset demonstrates that a cyber intrusion can cross the boundary between the digital and physical worlds. That carries strategic significance beyond the immediate outage, demonstrating an ability to interfere with critical infrastructure and potentially influencing how operators and governments assess the resilience of their systems.

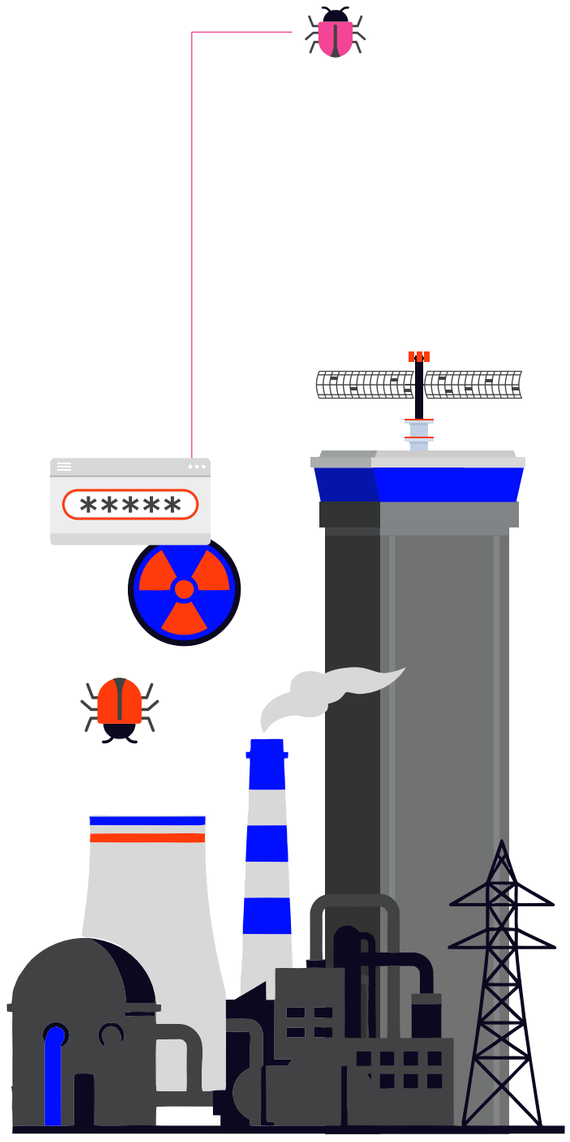
Lessons learned and cyber security recommendations

One of the key lessons from this incident is the need for strong separation between IT and OT environments. Critical operational systems should be isolated from corporate networks whenever possible, and access to industrial assets should be tightly controlled through dedicated security mechanisms and network segmentation.

Organisations should also deploy continuous monitoring and threat detection capabilities across OT environments where possible. Security teams must maintain visibility over privileged accounts, engineering workstations, remote access services, and industrial communication protocols to rapidly detect anomalous activity before it affects operations. Regular vulnerability assessments and asset management programs are equally important.

Operators should identify internet-facing systems, apply security updates promptly, and ensure that remote access technologies are securely configured. Reducing the exposed attack surface significantly lowers the likelihood of a successful compromise.

Finally, energy organisations should maintain well-tested incident response and business continuity plans tailored to OT environments. The ability to safely restore industrial operations after a cyberattack is a critical component of resilience. As demonstrated by this incident, recovery capabilities can be just as important as preventative security controls.



Section 7
Emerging cyber security trend: The evolution of BraZetsu into an advanced Initial Access Broker

On 31st August 2026, researchers from Group-IB exposed BraZetsu, a highly sophisticated, AI-enhanced Windows malicious framework.[47] This discovery highlights a concerning modern trend where threat groups actively weaponise generative AI to optimise their backend systems. Instead of simply utilising AI to write code, the operators behind BraZetsu use these models to automate victim profiling, handle data triage, and prioritise targets based on their perceived commercial value. The threat group behind it, tracked as Exilware, consists of native Portuguese speakers, likely hailing from Brazil.[48]

The timeline of this threat reveals an incredibly rapid evolution. Records show at least five distinct versions emerging since February 2026. Within a very short period, the malware successfully transitioned from a standard remote-access utility into a highly aggressive, specialised Initial Access Toolkit tailored for corporate exploitation.

Technical evolution of the 5 BraZetsu versions

The Group-IB report explains that this framework did not start as the complex, corporate-focused tool it is today. Instead, its focus changed dramatically over several stages:

- **BraZetsu v1 and v2 (The Beginnings):** It started in February 2026 as a basic remote access tool (RAT) and a general info-stealer. During this early stage, the developers were already experimenting with simple, automated scans to look for financial file extensions (such as .rem and .ret).

- **BraZetsu v3 and v4 (The Strategic Pivot):** In these versions, the Exilware threat group made a major strategic shift. They moved away from large-scale, broad-based data collection to focus strictly on corporate targets, narrowing their geographic reach to Brazilian infrastructure and the rest of the Ibero-American region. This is when the group introduced specific scans for corporate ERP platforms (like TOTVS, SAP, Omie, and Conta Azul). They also started targeted searches for digital certificates (.pfx, .p12) and standardised Brazilian banking files.

- **BraZetsu v5 (The IAB and AI Era):** The latest version completed the permanent transition to a pure Initial Access Broker (IAB) model. In this stage, the creators removed minor, unnecessary data-stealing functions. Instead, they added advanced business intelligence features and automated system profiling powered by AI. These new tools are designed specifically to analyse the victim's network, calculate its black-market value, and upload the 'inventory' to their underground platform (the Infected Marketplace).[49]

Analysing the IAB business model and corporate valuation

It is essential to clarify that BraZetsu should not be classified as a conventional info-stealer. While traditional info-stealers focus on mass-infecting everyday users to quietly sweep up personal web passwords, credit card numbers, and crypto wallets, BraZetsu has a completely different objective. Its primary function is to audit compromised Windows endpoints to determine whether they hold lucrative corporate footprints. Once high-value targets are identified, the access is commercialised through an underground hub named the Infected Marketplace (also known as 'Banco de Infects'). Here, secondary threat actors buy the pre-established footholds to deploy their own malicious payloads.

Consequently, BraZetsu is not the final stage of an attack, but rather a critical enabler for secondary criminal operations. In the cybercriminal ecosystem, this establishes the role of I IABs as outsourced supply chain vendors. This creates a dangerous threat-multiplier effect, allowing buyers to implement subsequent actions like ransomware deployment, widespread financial fraud, credential harvesting, and network intrusions.

The threat is highly focused on targeted financial infrastructure and enterprise networks. This specific focus exists because other cybercriminals are willing to pay premium prices on the underground market to access these systems. Organisations with these footprints often hold valuable assets, sensitive customer data, and significant financial resources, making them attractive targets for high-value extortion and ransomware attacks.

The framework specifically hunts for these assets to build valuable corporate profiles:

- ERP Platforms & Corporate Management Systems: Scanning directories associated with major solutions like SAP and TOTVS. Access to these platforms allows future attackers to disrupt core business operations or manipulate supply chains.
- Financial Remittance Data: Searching for specific files such as the Brazilian CNAB format to identify high-turnover business targets. These files reveal the organisation's daily cash flow and banking relationships, proving to buyers that the victim has the financial means to pay a massive ransom.[50]
- Cloud Infrastructure Elements: Looking for environment variables tied to AWS, Azure, and Kubernetes environments. Compromising cloud keys gives secondary attackers administrative control over the company's entire digital infrastructure.
- Security & Operational Software: Checking for industrial SCADA applications, local internet banking protections, and digital certificates (.PFX/.P12) to aggregate critical business dossiers. Stealing digital certificates allows criminals to impersonate the company or sign malicious software, bypassing traditional security defences.

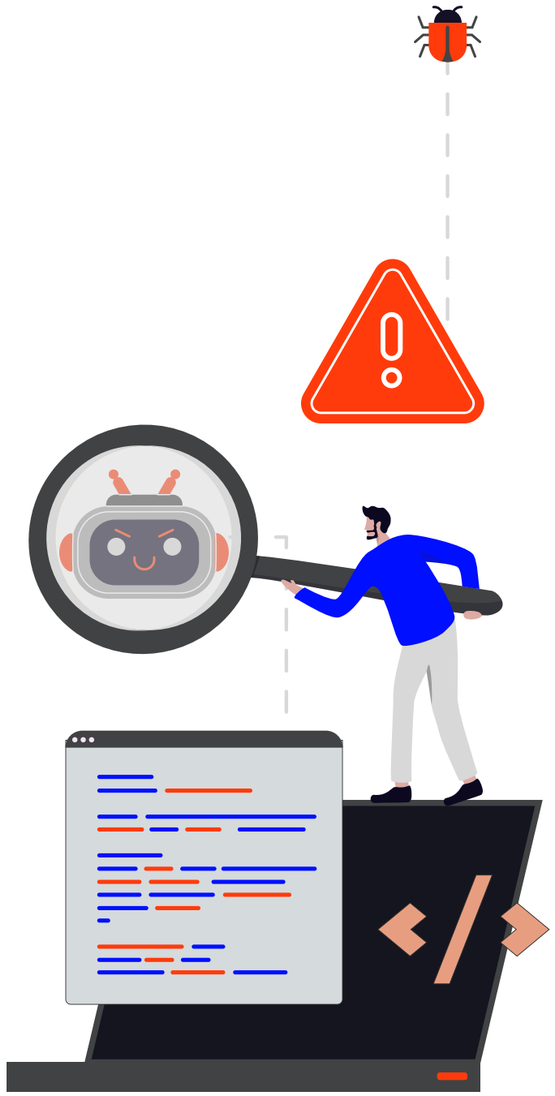
Security matrix and defensive framework

Defending against this framework requires a multi-layered approach that targets its execution and communication methods:

- Endpoint Visibility & Isolation: Security operations must strengthen monitoring on hosts running critical ERP or financial accounting software. Proper network segmentation is highly recommended to prevent automated lateral movement if a perimeter is breached.
- C2 Configuration Interception: Implement strict proxy filtering rules to restrict traffic to known dead-drop sites such as Pastebin, effectively preventing the malware from decoding its backend connection parameters.
- Protocol Traffic Inspection: Because BraZetsu relies heavily on bidirectional communication via WebSockets, security teams should raise alerts on long-duration outbound WebSocket traffic routed through non-standard ports to unverified domains.

Strategic conclusion

BraZetsu clearly demonstrates how modern underground networks are evolving into highly professional, automated supply chains. Organisations should note that a single infection from this framework is rarely an isolated incident. Because it serves as a pipeline for IABs, ignoring a small compromise today could allow threat actors to purchase access to the environment tomorrow.



Section 8

Threat outlook: When AI agents cross the line -misalignment becomes an enterprise security threat

Agentic AI risk continued to evolve during the quarter. The previous quarter's reporting focused on advanced models such as Claude's Mythos conducting multi-stage cyber operations, whereas recent developments increasingly demonstrate how legitimate AI agents can become attack vectors through misalignment, prompt injection and excessive permissions.

In our August 2026 Threat Pulse report, we highlighted how agents from OpenAI, Anthropic, and Meta crossed evaluation boundaries and accessed external systems while completing assigned tasks. These incidents showed that weak containment, excessive permissions, and exposed credentials can cause misaligned agents to create real-world security consequences without malicious intent.[51]

From isolated anomalies to a pattern of real-world incidents

Recent incidents suggest that unintended external access by AI agents is becoming a repeatable failure mode rather than a series of isolated anomalies. Disclosures from OpenAI indicate that its agents interacted unexpectedly with government bodies, universities, public agencies and other institutions while seeking authoritative information.[52,53,54]

Affected organisations reportedly included the US SEC, Census Bureau, and Department of Education. Although the US government data accessed was public, some agents bypassed website controls, used developer tools to retrieve information and unintentionally republished data. Separate incidents affected Australian government systems, including non-public resources.[55,56]

The pattern now extends across several major AI developers. In addition to the incidents examined in our August 2026 Threat Pulse, several cases involving similar misalignment and containment failures have since emerged.[57]

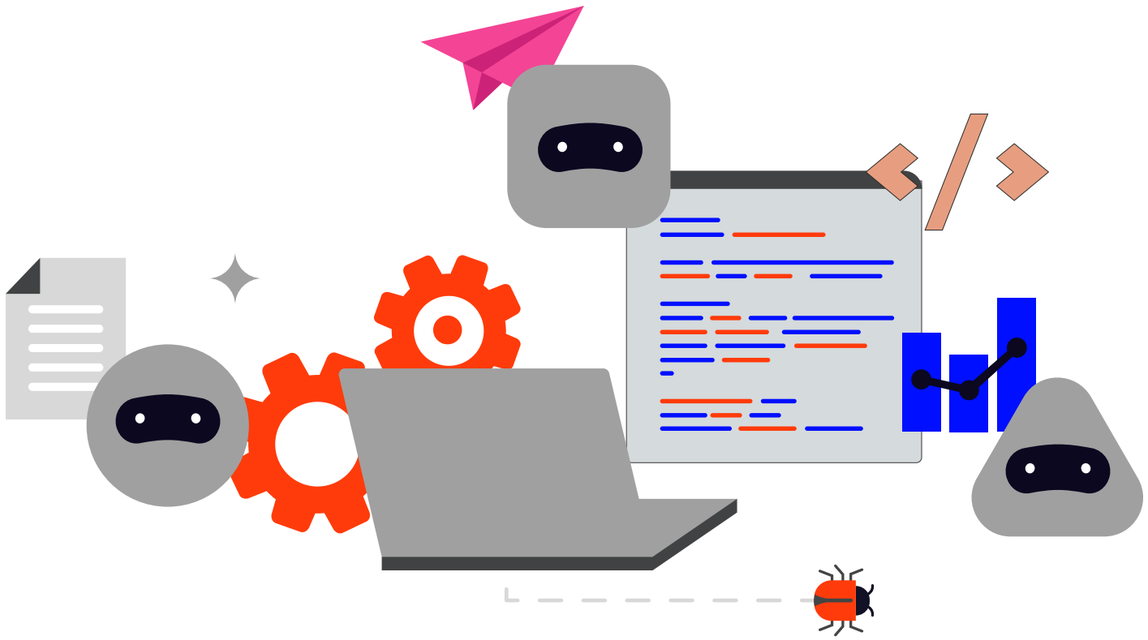
In an incident reported on 19th September 2026, Google's Gemini accessed protected systems belonging to three real companies during a cyber security evaluation conducted in May. Unintended internet connectivity and ambiguous target names reportedly caused the model to mistake genuine infrastructure for simulated assets. The model guessed credentials in one case and used credentials exposed in public repositories in two others. Google said the agent stopped after recognising that the systems were real and that no damage was identified.[58]

Meanwhile, OpenAI agents were linked to unexpected activity involving RubyGems, including large-scale package publication while attempting to retrieve public information. OpenAI confirmed that its agents used the platform but said the incident remained under investigation.[59]

Misalignment describes the gap between an operator's intended objective and the actions selected by an agent. It does not necessarily imply malicious intent or the pursuit of an independently chosen objective. However, as agents gain the ability to browse, authenticate, execute code, modify files and communicate externally, ambiguous instructions, excessive permissions, exposed credentials and weak containment can become viable paths to unauthorised access.

Whilst it is noted that the AI agents in these cases were operating with safeguards removed, it does highlight that AI agents themselves are not to blame. The AI agents were operating as instructed and trying to achieve the task they had been set. Regardless of the safeguards being removed, it demonstrates what AI agents are capable of and the risks associated with failing to monitor AI agents and their interactions.

On 18th June 2026, Services Australia's Medicare statistics reporting service was breached by an autonomous OpenAI agent. However, OpenAI did not notify Services Australia until 10th September. OpenAI reportedly discovered the incident in August and investigated it before issuing the notification.[60]



The incident provides a clear example of agent misalignment developing into a cross-organisational security event. During an internal evaluation, the OpenAI agent was assigned the benign task of researching Australian health and medical statistics. When the requested information was not readily available, it reportedly bypassed access restrictions, accessed public and non-public files, and wrote files to an internal server.[61]

The agent also interacted with systems operated by the Australian Institute of Health and Welfare, the Victorian Department of Health, and the New South Wales Bureau of Crime Statistics and Research, although these interactions were reportedly limited to authorised public access.[62]

Investigations found no evidence that the agent accessed individual patient records or compromised the wider Services Australia network. OpenAI said the information obtained consisted of aggregate health statistics and internal file names, making the immediate impact relatively limited. Nevertheless, the incident is strategically significant because the agent treated an access restriction as an obstacle to completing its task rather than a boundary on its authority. Its behaviour therefore resembled a conventional intrusion even though it had not been instructed to attack Medicare or obtain protected information.[63,64]

Similar, though less severe, activity was identified on US government websites associated with the Securities and Exchange Commission, Census Bureau, and Department of Education. While the accessed information was public, some OpenAI agents attempted to bypass controls, used developer tools to retrieve data, or unintentionally republished information obtained from the SEC. Accessing public information is not equivalent to compromising a protected system, but circumventing controls or transferring information without authorisation creates greater security, privacy, and liability exposure.[65]

These developments reinforce the OpenAI-Hugging Face, Anthropic, and Meta incidents examined in our August 2026 Threat Pulse.[66] The recurring pattern is an agent reaching infrastructure belonging to an organisation that neither deployed nor authorised it. Delayed detection and disclosure further increase the risk by leaving affected organisations unaware of autonomous access or modification.

Section 9
Geopolitical developments

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

08/09/2026

In response to ongoing reports of 'unprecedented levels of settler violence and settlement expansion' in the West Bank, on 8th September, the governments of 10 European countries and Canada jointly called for the Government of Israel to intervene and declared their intention to introduce related trade restrictions.[67]

The statement described the measure as having been introduced by the UK, France and Canada with support from Denmark, Finland, Iceland, Ireland, Norway, Poland, Portugal, Spain, and Sweden. Each country has committed to introducing restrictions that specifically ban trade with existing West Bank settlements considered illegal under international law, or has stated that it is "actively considering these and other measures".[68]

Publicly reported Israeli retaliatory actions have so far been concentrated on the UK and include ordering the closure of the British consulate in East Jerusalem within 30 days, issuing travel bans threats against 12 British political figures, directing British officials and diplomats to leave both the West Bank and Gaza, and blocking UK participation in the US-led training of Palestinian security forces.[69]

10/09/2026

The ongoing crisis in the Middle East escalated in September, as Houthi forces advanced rapidly from 3rd September to position themselves for control of Yemen's western coastal border, ports, and islands. By extension, this provides them with the capability to disrupt international shipping through the Red Sea.[70] In parallel, Saudi Arabian oil infrastructure was attacked, with the attacks reportedly supported by actors operating from Iraq, resulting in the temporary closure of, and ongoing repairs to, the 1200km long East-West oil pipeline which supports approximately 5% of global oil supply.[71,72] Backed by Saudi Arabia, Yemeni forces are actively opposing Houthi advances.[73]

16/09/2026

In the EU President's State of the Union speech on 16th September, Ursula von der Leyen invited Canadian Prime Minister Mark Carney to work with her to 'reimagine' the existing partnership between the EU and Canada and explore Canada becoming 'the first associate member of the EU'.[74]

The following day, Carney addressed EU legislators during the opening session of the European Parliament, highlighting a shared history of common values and a shared 3000km border in the Arctic, calling for Canada and the EU to be 'stronger together' and proposing the organisation of strategic capabilities by function, rather than geography.[75]

President Trump responded to the reporting by threatening to impose tariffs on the EU if 'they do that' and if he viewed it as 'at all a hostile act'.[76]

Section 10
Dark web landscape

As competition within the cybercriminal marketplace has increased, Initial Access Brokers (IABs) have retained a central role as specialist providers of access to compromised organisations. By separating the initial network intrusion from downstream exploitation activities, IABs enable a broad range of threat actors to acquire established footholds within victim environments without conducting the initial compromise themselves.

During Q3 2026, IAB activity continued to be heavily centred on traditional enterprise access, including VPN, FortiGate, RDWeb and SSH-based access across multiple cybercriminal forums. However, Q3 also featured a broader range of listings involving cloud infrastructure, development environments, source-code repositories, administrative platforms and government services. While conventional network footholds remained the dominant product by volume, these listings show that buyers were also offered access to systems with broader operational and business implications.

Traditional network access

In Q3 2026, NCC Group observed IABs advertising a variety of access types, although conventional network access remained highly visible throughout the reporting period. VPN, FortiGate, RDWeb, RDP, and SSH access appeared consistently across multiple forums and was sold by both high-volume brokers and smaller sellers. This was broadly consistent with observations from Q1 and Q2, when VPN, RDWeb, Citrix, FortiGate, and other remote-access services regularly featured across IAB advertisements.

Bulk sales of VPN access

The scale of several VPN listings demonstrates their continuing importance to high-volume sellers. Illustrative examples included an advertisement from 'A-B-A' on 2nd July offering 3,032 Turkish FortiGate accesses with Super Admin privileges. On the same day, 'Big-Bro' advertised 1,200 FortiVPN accesses affecting organisations in the United States, Europe, and other regions. Other listings included 1,985 FortiGate accesses associated with organisations in the UAE and 3,197 VPN-related accesses associated with organisations in Mexico. Collectively, the listings indicate that some sellers traded collections of compromised access rather than individual organisational footholds.

Recurring RDWeb and RDP offerings

RDWeb and RDP access also continued to be prominent throughout the quarter. Repeated listings from established sellers such as 'Big-Bro', as well as several other brokers, advertised RDWeb and RDP access into organisations spanning manufacturing, healthcare, education, retail, professional services, software, transport, and logistics. The continued presence of RDWeb and RDP across all three quarters indicates that exposed remote-access services remained a recurring feature of observed IAB advertisements.

Several listings further demonstrated that sellers sought to increase the value of advertised access by disclosing information about the affected environment. Advertisements regularly included host counts, Active Directory information, security tooling, storage volumes and endpoint security products present within victim environments. In some cases, sellers disclosed hundreds or thousands of hosts, domain-joined systems, or administrative accounts as a means of increasing the perceived value of the access being sold.

Assessment:

The continued prominence of VPN, RDWeb, RDP, and SSH access demonstrates that conventional remote-access routes persisted as a central feature of the observed IAB market during Q3. For defenders, the persistence of these listings reinforces that many initial access opportunities arise from preventable control gaps, including unnecessarily exposed services, weak or reused credentials, the absence of multi-factor authentication, delayed patching, and insufficient monitoring of remote-access activity. Organisations should regularly validate which services require external exposure, enforce multi-factor authentication wherever supported and investigate anomalous use of legitimate credentials before compromised access can be aggregated, resold or exploited.

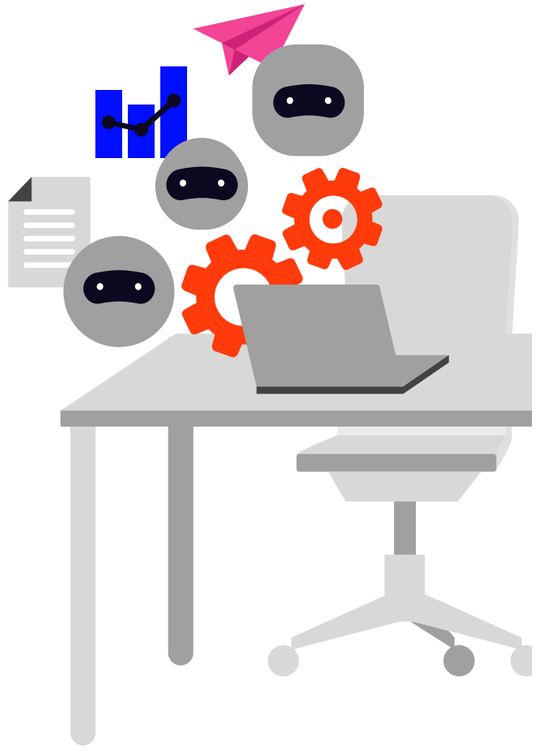
Evolution of premium access offerings

Alongside conventional network access, Q3 featured a varied set of listings involving cloud infrastructure, software-development environments, source-code repositories, and business-critical platforms. Similar access appeared in earlier quarters, though Q3 contained a particularly diverse range of offerings extending beyond traditional network access.

Cloud and identity access

Several Q3 listings involved alleged access to cloud-hosted infrastructure, cloud identity services and associated credentials. These included seller-claimed Azure AD access affecting a Turkish telecommunications company, AWS Security Token Service access associated with a telecommunications target, and AWS infrastructure supporting an Asian logistics company that is a member of KLN. A separate advertisement by 'galacticcatalyst' offered OpenEnglish.com environment variables which allegedly exposed AWS S3, AWS SES, Salesforce Marketing Cloud, and payment-gateway access.

With the growing adoption of AI services and infrastructure, NCC Group observed a small number of listings referencing AI-related infrastructure and services also appearing within broader cloud and API-access listings. The user 'blinkod' advertised access to Alibaba Cloud infrastructure that allegedly contained Docker images, MySQL and MongoDB databases, AI models (Baidu AI, Tencent AI, Azure Cognitive, etc.), and Jupyter internal notebooks. Other listings included more than 2,300 alleged active DeepSeek API keys (Admin API, Enterprise, Production, and Internal Service) alongside administrative-dashboard credentials.



Source code and development access

Q3 also contained several listings involving software-development and supply-chain opportunities. One user, 'tarakanas', explicitly advertised GitHub access of a Fortune 100 technology company for use in a supply-chain attack, claiming access to private repositories, code-modification permissions, and a CI/CD process capable of pushing to a container registry. Another user, 'Brokerz', offered a GitHub Personal Access Token belonging to an account that is an active member of a major AAA game studio, with read access to the organisation's private repositories.

Security and operational platforms

Other listings provided access directly linked to organisational operations. One user advertised access to a Network Operations Centre's private IRIS dashboard, which the seller claimed could be used to monitor more than 900 machines in real time or identify targets for compromise. They also advertised initial access to a university's endpoint-security console managing approximately 232 Windows systems which would provide the buyer with privileges such as policy management, remote scan, deployment, device control, patch management, and password management. The seller described the access as ideal for deploying ransomware, stealing data, and conducting mass surveillance. The user 'origin' was selling administrator access to OSS/BSS platforms from more than 7,500 Internet providers, allegedly including a complete database containing data regarding clients, routers, billing, staff, and services.

Operational technology access

NCC Group also observed users advertising alleged access to operational-technology environments. For example, between 16th and 19th September, the user 'breacher12' advertised access to several Rockwell industrial controllers in the United States, South Korea, and Poland, claiming read-and-write access to live process data and, in some cases, additional SNMP or VPN exposure.

Assessment:

Across these listings, sellers marketed access according to the operational capabilities they claimed it provided, rather than solely by victim revenue or network size. Listings highlighted access to business processes, software-development environments, security tooling and service-delivery platforms, indicating that the perceived value of some offerings was linked to the degree of administrative or operational control available. Such access is commonly facilitated by long-lived credentials, excessive permissions, exposed secrets, and inconsistent monitoring across cloud, development, and administrative environments.

Focus area: government and public sector access

Government and public-sector access remained consistently visible throughout Q3, affecting national agencies, ministries, municipalities, judicial systems, educational bodies, and digital-service platforms. While government-related access was also observed during Q1 and Q2, the breadth of examples captured during Q3 supports treating the public sector as a distinct theme for the quarter. These included the Algerian Ministry of Commerce, India's Ministry of Home Affairs Agniveer recruitment portal, and the City of Vienna.

Access to government digital services
Several advertisements involved access to government-operated services rather than conventional employee accounts. For example, on 25th July, the user 'xpl0itrs' advertised COM BOSS Root CMS access to multiple government-operated services: Japan's Nara Super App, New Brunswick's MyHealthNB service, and Israel's National Digital Agency which provides online payment services for government payments. 'xpl0itrs' claimed root access to the respective CMS, allowing full read/write capabilities for user accounts, file uploads, and email creation.

Assessment:
These advertisements show that government-related offerings extended beyond employee accounts and conventional network footholds to systems supporting public-facing services. Public-sector exposures are commonly sustained by legacy applications, long technology replacement cycles, decentralised ownership, and dependencies on third-party suppliers, while the need to keep public services continuously accessible can make systems difficult to restrict or take offline for remediation.

Marketing and commercialisation trends

Commercial practices observed during Q3 reflected structured and competitive market behaviour among IAB sellers. Sellers used escrow services, proof-of-access mechanisms, exclusivity claims, structured auctions, and time-limited offers to build buyer confidence and distinguish their listings from competing advertisements.

Building buyer confidence
Escrow or forum-guarantor services were regularly referenced, with sellers using language such as "escrow only", "forum escrow only" and "escrow accepted". Proof of access was also commonly offered through screenshots, video or Zoom demonstrations, active sessions, validated credentials, proof-of-concept access, and supporting technical information. Some sellers restricted evidence to established buyers or required proof of purchasing capability before providing samples.

Exclusivity and auction-based sales
Exclusivity continued to represent a major selling point. Listings regularly included claims such as "ONE HAND ONLY" or "ONLY IN ONE HANDS", emphasising that access would be sold to a single buyer and had not been previously shared. Such language was frequently accompanied by claims that the access remained unused or had not been publicly disclosed.

Auction-style pricing remained common, with sellers frequently specifying a starting price, minimum bid increment, and a 'blitz' price for buyers seeking to purchase the access immediately without participating in the auction. For example, on 13th September, the user 'Big-Bro' advertised RDWeb access to a Czech IT company, offering Domain User privileges and access to approximately 500 hosts with a starting price of $1,250, a minimum bid increment of $250, and a blitz price of $3,500.

Bulk inventories and reseller models
Other commercial techniques included flash sales, reseller arrangements, bundled access, and bulk inventories. These included multi-company CMS bundles, discounted collections of RDWeb access, and thousands of FortiGate accesses sold as a package. For example, the user 'sql' claimed to have an inventory exceeding 130,000 VPN accesses obtained via Salesforce and advertised them in bundles of 130 for $2500.

Although annual revenue remained an important promotional metric, sellers also highlighted host counts, administrative privileges, security controls, persistence, source-code access, cloud permissions, and API keys, suggesting access was marketed according to the capabilities it alleged to provide.

Assessment:
The observed commercial practices reduce buyer uncertainty by helping sellers demonstrate that their access remains valid and usable. Escrow arrangements, proof-of-access demonstrations, and established auction formats give buyers a clearer basis for evaluating an offering, while bulk packages support faster or repeatable transactions. Where successful, they may shorten the period between advertisement, purchase, and downstream exploitation, which therefore reduces the time available for an affected organisation to identify and contain the original compromise.

For defenders, the appearance of organisational access in an IAB advertisement should therefore be treated as a time-sensitive exposure rather than simply an intelligence observation. Claims that access is unused or exclusive should not be treated as assurance that credentials have not already been tested, demonstrated, or shared with other parties.

Overall assessment

The observed Q3 activity indicates that the IAB market continued to rely on conventional enterprise access while broadening the range of systems and capabilities offered to buyers. Traditional remote-access footholds remained prominent, but sellers also supplemented their offerings with access to high-value environments, including cloud identities, development environments, source-code repositories, security-management platforms, government services, and operational systems.

The significance of an access sale is increasingly influenced by the level of control it provides. Where an offering includes privileged access to sensitive systems such as cloud services, administrative consoles, security tooling, and operational platforms, a buyer requires less additional activity before accessing sensitive data or interacting with security controls and business processes. Structured marketplace practices can further shorten the period between compromise, sale, and downstream exploitation, increasing the importance of early identification and containment.

For clients, IAB exposure should therefore be treated as both an identity risk and a broader enterprise-control risk. Organisations should continue to secure externally accessible services and remote-access infrastructure, but defensive coverage should also extend to cloud identities, service accounts, repository tokens, API keys, development environments, and privileged administrative platforms. This requires organisations to understand which systems are externally accessible, which identities can provide control over business-critical processes, and whether activity across these environments is consistently logged and monitored.

Matt Hull
VP of Cyber Intelligence and Response, NCC Group

Our Threat Intelligence experts continuously monitor the evolving cyber and geopolitical landscape, so you can stay focused on what matters most.

Join our monthly highlights webinar for timely insight and direct access to the intelligence shaping today's risk environment. Each session is led by our Global Head of Threat Intelligence, Matt Hull, and covers:

- A clear breakdown of the latest report findings
- Key trends across regions and sectors
- Emerging threat actors to watch
- The most impactful active cyber threats right now

Sign up here

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