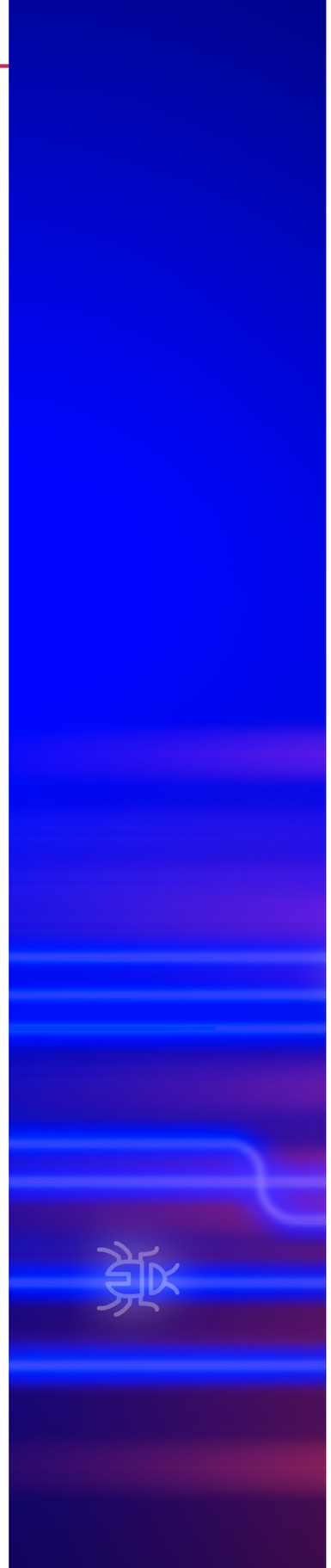
ncc group

FOX IT
part of ncc group

Cyber Threat Intelligence Report

Review of Q3 2025

Contents



Executive Summary

This Quarter, the cyber threat landscape continued to evolve and was marked by high-impact supply chain compromises, persistent ransomware activity, and increasing geopolitical tensions influencing cyber operations. Notable incidents included the exploitation of critical SharePoint vulnerabilities by Chinese state-linked actors, a major breach at Jaguar Land Rover, and the Salesforce–Salesloft Drift breach affecting over 700 organisations.

Ransomware attacks declined slightly by 5% when compared to Q2, with 1125 incidents recorded in our database. Qilin remained the most prominent threat actor for the Quarter, the group continue to demonstrate a heightened level of sophistication through their expansive affiliate network and advanced tooling. The ransomware landscape continues to fragment, with the emergence of several new groups such as Interlock, Gunra, The Gentlemen and Coinbase Cartel, some of which appear to be rebrands or splinters from existing collectives.

Away from the numbers, the ransomware spotlight explores new research by New York University, who released a proof-of-concept (PoC) large language model (LLM) controlled ransomware that can autonomously conduct reconnaissance, execution, and evasion, named “Ransomware 3.0”. The release of PromptLock illustrates new ways in which AI could be exploited by threat actors in their operations and provides considerations for the long-term.

Our Emerging Cyber Trend segment explores Cookie hijacking, the theft and reuse of session cookies or equivalent authentication tokens. As of 2025, this technique has retained its strategic importance, and developments signal that cookie hijacking is a key attack vector shaping the threat landscape in 2025.

Finally, geopolitical developments, including NATO airspace incursions and Middle Eastern tensions, further shaped the threat environment, suggesting increased global tensions.

All in all, the quarter underscores the need for robust third-party risk management, rapid incident response, and proactive security strategies to counter increasingly sophisticated and adaptive threat actors.

Section 1

Timeline of Critical Incidents Q3 2025

01/07/25

The Russian hosting company Aeza Group and four operators were sanctioned by the U.S. Department of the Treasury. The Office of Foreign Assets Control (OFAC) claims that Aeza Group is a bulletproof hosting service (BPH), who are hosting companies that ignore abuse complaints and takedown requests.

OFAC claims that it was used by BianLian ransomware, Redline, and BlackSprut. The other four operators sanctioned are, Penzev, Bozoyan, Gast and Knyazev.

07/07/25

Multiple vulnerabilities in SharePoint were exploited, CVE-2025-49704, CVE-2025-49706, CVE-2025-53770, and CVE-2025-53771, known collectively as ToolShell.

Chinese state-linked actors Linen Typhoon, Violet Typhoon, and Storm-2603 were observed exploiting the engineering flaws to gain initial access to target organisations.

10/07/25

The U.K National Crime Agency (NCA) arrested four people for their part in the attacks on Marks & Spencer, the Co-op, and Harrods - three men and one woman aged 17-20 were apprehended in the West Midlands for participating in the activities of an organised crime group.

It is believed that the attacks on the major retailers were perpetrated by the decentralised cybercrime group Scattered Spider who are known for advanced social engineering.

14/07/25

Operation Eastwood struck a significant blow against the pro-Russian group, NoName057(16). The group were targeted by Europol and Eurojust with law enforcement from 12 countries. It was marked as one of the most coordinated cyber crackdowns in recent years. NoName057(16) has been known for targeting NATO countries and other countries supporting Ukraine. The sweeping international effort led to 2 arrests, 7 warrants, 24 house searches, 100 servers being taken offline, and dismantling their main server network.

04/08/25

Bouygues Telecom suffered a data breach, with the personal data of 6.4 million customers compromised.

The company is the largest telco in France with 14.5 million mobile subscribers. The threat actor that perpetrated the attack wasn't disclosed but echoed similar attacks against US-based telcos attributed to Salt Typhoon in late 2024. Stolen customer details included personal contact details, civil status, company details and IBANs.

05/08/25

Pandora confirms third-party data breach - the Danish jewelry company confirmed that it fell victim to a cyberattack that exposed customer data to unauthorised parties.

The breach occurred through a third-party platform used by Pandora, though the company did not disclose which provider was involved. Pandora stated that "some customer information" was allegedly accessed and that their core internal systems were not compromised.

08/08/25

Salesforce-Salesloft Drift Breach - Salesloft disclosed that attackers stole OAuth tokens linked to the Drift chatbot integration used in Salesforce. With these stolen tokens, they accessed hundreds of Salesforce customer environments between August 8–18 and extracted data such as contacts, accounts, opportunities, and cases.

The attackers also scanned the stolen records for sensitive credentials, including AWS and Snowflake keys.

25/08/25

Ransomware takes Swedish municipalities offline for just $168K - About 200 municipalities and regional governments in Sweden were severely disrupted following a ransomware attack on IT systems supplier Miljödata.

CEO Erik Hallén confirmed on August 25th that the disruption was the result of a cyberattack, impacting roughly 200 of Sweden's 290 municipalities. Police later reported that attackers demanded 1.5 Bitcoin, roughly $168,000, to prevent the stolen data from being exposed.

02/09/25

Cyberattack against Jaguar Land Rover stops production for weeks - Jaguar Land Rover was hit by a major cyberattack that forced production to halt across several UK plants and disrupted operations for weeks. Initially, the company said no customer data was affected, but later confirmed some information had been accessed, without specifying details.

The shutdown caused millions in daily losses and highlighted how outdated credentials and weak security controls can leave critical manufacturing operations exposed to crippling breaches.

08/09/25

Hundreds of NPM packages hit in supply chain attack - A sophisticated NPM supply chain attack has emerged as one of the most significant security threats to the Node.js ecosystem in 2025, compromising over 477 npm packages, with billions of weekly downloads.

20/09/25

Cyber-attack disrupts major European airports - A cyberattack on a check-in and boarding systems provider disrupted operations at several major European airports. The disruption was linked to MUSE software developed by Collins Aerospace, which provides systems to several airlines at airports globally. The incident forced airlines to switch to manual processes, resulting in long delays, cancellations, and passenger congestion.

25/09/25

CISA released an emergency directive to identify and mitigate potential compromise of Cisco devices - CISA issued an emergency directive addressing two actively exploited zero-day vulnerabilities, CVE-2025-20333 and CVE-2025-20362, in Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Secure Firewall Threat Defense (FTD). According to the report, the flaw allows unauthenticated remote code execution and persistence through read-only memory (ROM), which poses a serious risk to victim networks.

CISA also noted that the campaign is attributed to a threat actor codenamed UAT4356 (aka Storm-1849) and linked to the cluster dubbed ArcaneDoor, which previously targeted network devices from several vendors, to deploy malware families like Line Runner and Line Dancer.

Section 2

Ransomware Key Statistics Q3 2025

5%

Global ransomware attacks decreased by 5% in Q3 vs Q2 2025

30%

Industrial sector accounted for 30% of attacks in Q3 2025

13%

Qilin was responsible for 13% of attacks in Q3 2025

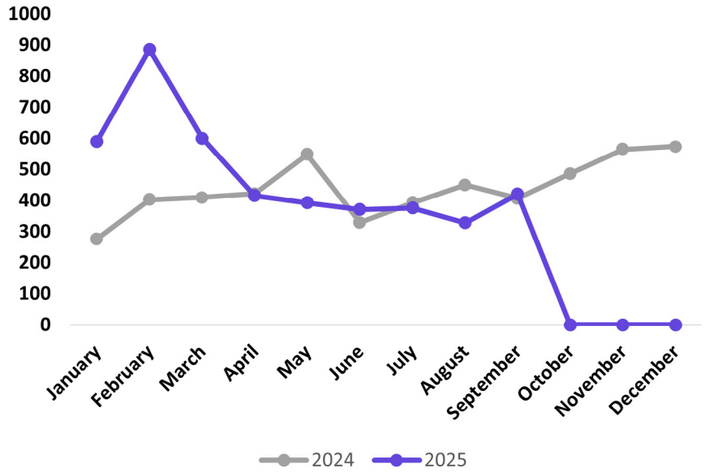


Figure 1 Ransomware Attacks by Month 2024 - 2025

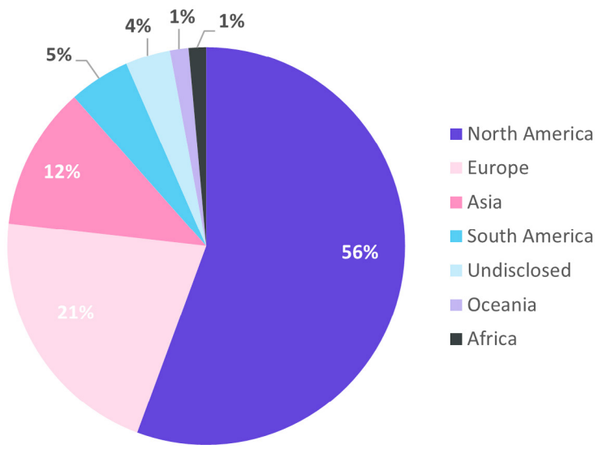


Figure 2 Ransomware Attacks by Region Q3 2025

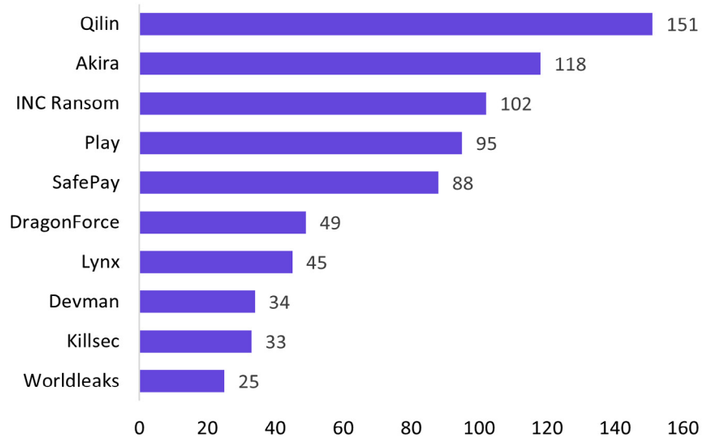


Figure 3 Top Threat Actors Q3 2025

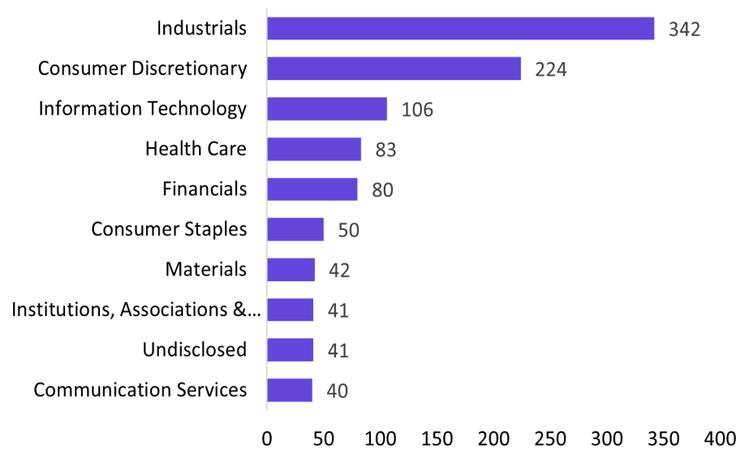


Figure 4 Top Targeted Sectors Q3 2025

Key Events

July 02, 2025
Ingram Micro

The global IT distribution giant suffered a major ransomware attack that led to a worldwide outage of its internal systems and customer platforms. The attack was attributed to the SafePay ransomware group, which infiltrated Ingram Micro's network via its GlobalProtect VPN.

August 11, 2025
St. Paul's City Government

The Interlock ransomware group infiltrated the government systems of St. Paul's City, compromising around 43 GB of internal data and primary files related to employees. The breach severely disrupted essential digital services, prompting the governor to deploy the National Guard in response.

September 11, 2025
Panama's Ministry of Economy and Finance

Panama's Ministry of Economy and Finance experienced a cyber-attack attributed to the INC Ransom group. The theft resulted in 1.5 TB of sensitive data, including emails, financial documents and budgeting details. The core systems vital to its operation remained unaffected.

NCC Service

NCC Group can support you to mitigate against the ransomware threat. Please see our contact details at the end of this report should you require assistance.

Section 3

Ransomware Insights Q3 2025

As we close out the third quarter of 2025, ransomware activity experienced a 5% decline compared to the previous quarter. This drop is slightly higher compared to the 3% drop in Q3 2024, which suggests a temporary stabilisation rather than a sustained downward trend. Despite this drop, established threat actors such as Qilin, Akira, and INC Ransom sustained a high level of operational activity, underscoring their continued influence in the threat landscape.

Qilin Takes Top Spot

Qilin remains the most active ransomware group in Q3 2025, accounting for 151 out of 1125 recorded ransomware incidents, and maintaining their position as the most prominent threat actor in Q2. The group continue to demonstrate a heightened level of sophistication through their expansive affiliate network and advanced tooling. Qilin affiliates have been observed to leverage multi-stage loaders that decrypt the ransomware payload at runtime using dynamically generated AES keys, enabling stealthy execution and detection evasion.[1] Additionally, their ransomware binaries support cross platform attacks on Windows, Linux and ESXi environments, and include features like automated safe mode execution, network propagation and customisable encryption modes.[2]

Based on our ransomware statistics, Qilin primarily focused their attacks on the Industrials (29%), Financials (21%), and Consumer Discretionary (15%) sectors. This is largely like Q2 where they mainly focused their attacks on Industrials (28%) and Consumer Discretionary (19%), but with Information Technology (15%) ranking in third. Targets thus continue to reflect an interest in data-centric, financially lucrative, and supply-chain dependent industries, suggesting an intent to maximise operational disruption and leverage extortion.

In Q3, Qilin targeted companies in the Industrial sector, such as Quaser Machine tools and Chinup Technology Co, disrupting operations and exfiltrating large volumes of sensitive data.[3,4] Within the Consumer Discretionary sector, Nissan Creative Box, a subsidiary involved in branding and design was targeted. Targets in the Financials sectors include South Korean investment firms such as Welcome Financial Group and Mobidic Asset Management, as well as the compromise of financial records from Mecklenburg County Public Schools in the US.[5,6] This indicates a prominent interest in financial data and a focus on attacks that seek to maximise financial gain.

From a Tactics, Techniques, and Procedures (TTP) perspective, Qilin affiliates have exploited vulnerabilities such as Fortinet's CVE-2024-21762 and CVE-2024-55591, in addition to credential theft, phishing, and use of purchased access from Initial Access Brokers.[7] Once inside networks, affiliates deploy custom loaders, parallel encryption routines, and data exfiltration scripts. This enables multi-layered extortion combined with encryption, leaks, and reputational coercion.[8] Notably, Qilin maintains collaborative links with groups such as Scattered Spider, Devman, Moonstone, and FIN12, leveraging their advanced social engineering and cloud intrusion capabilities to enhance their initial access capabilities and operational reach.[9,10]

Looking ahead, Qilin is expected to maintain their dominance into Q4 2025, with further development of their extortion mechanisms and increased focus on high-value targets, including managed service providers and supply chain dependent organisations.

New Threat Actors Continue to Emerge

Meanwhile, the ransomware landscape continues to fragment with the emergence of several new groups such as Interlock, Gunra, The Gentlemen and Coinbase Cartel. Some of these appear to be rebrands or splinters from existing collectives such as BlackLock, Conti, and Babuk.[11,12] New groups continue to suggest a maturing underground economy where smaller actors leverage shared infrastructure and leaked builder kits to establish their presence.

The Gentlemen ransomware group targeted multiple industries including manufacturing, construction, and healthcare, with confirmed incidents reported in at least 17 countries.[13] The group operates a traditional ransomware model of data theft, encryption, and extortion. However, their highly adaptive evasion techniques are what makes them dangerous. They have been abusing legitimate signed drivers to bypass security tools, deploying "KillAV" utilities to disable antivirus and EDR, and leveraging Group Policy Objects (GPOs) for domain wide deployment.[14] The Gentlemen can also alter tooling mid-campaign, which is a sign of a sophisticated and flexible operation. With their adaptability and willingness to target operational technology environments, this makes them a serious risk to critical infrastructure.

Another emerging ransomware group, Coinbase Cartel, operates more as a data broker and extortion focused collective. The group concentrates on exfiltrating sensitive information and leveraging it for extortion, using public leak threats to pressure victims into payment.

Their campaigns have targeted major firms such as NTT Data, Desjardins Group, and CEVA Logistics, spanning sectors from Finance to Telecommunications.[15] Their affiliate model offers revenue shares or fixed payments for access or data that mirrors a RaaS structure, but without deploying encryption payloads. They appear to be more focused on reputational damage and data exposure instead of operational damages as their tactics follow a double extortion pattern, where encryption is not considered as a main weapon.[16]

Whilst unconfirmed, in August, Scattered Spider also teased a ransomware service. The group shared an image of a ransom note on their Telegram channel, with the caption, 'RaaS Soon Boys'. If true, this could mark a shift in the landscape with an English-led RaaS, facilitating Western cybercriminals in conducting ransomware attacks, where having traditionally relied on Russian-speaking providers.[17]

Ransomware Continues to Have a Detrimental Impact

Several major incidents occurred this Quarter, including:

July 1, 2025 – Welthungerhilfe, a major German humanitarian aid organisation was attacked by Rhysida ransomware. The attackers accessed and encrypted sensitive data, including donor information and demanded a ransom of 20 bitcoin.

July 18, 2025 – Russia's largest alcohol retailer, WineLab was forced to shut down over 2,000 stores due to a ransomware attack that crippled its IT infrastructure and customer service.

August 5, 2025 – DaVita confirmed a ransomware attack by Interlock group, compromising the sensitive data of nearly 2.6 million patients. This triggered data breach notifications, regulatory scrutiny and the widespread exposure of about 1.5TB of data from internal files'.

August 18, 2025 – Colt Technology Services was targeted by WarLock group which exploited a SharePoint vulnerability to steal customer and employee data. This knocked out its Colt Online customer portal and Voice API systems that was initially framed as technical issues.

August 26, 2025- Swedish IT service provider Miljödata suffered a ransomware attack that disrupted operations of over 200 municipalities and public-sector clients. Attackers exfiltrated around 1.2 terabytes of employee and citizen data, including PII and payroll records.[18] They also demanded a ransom estimated at $168,000 for data deletion and decryption keys. This highlights the growing risk of supply chain compromise.[19]

September 17, 2025 – Insight Partners disclosed a breach that affected approximately 12,600 individuals, stemming from a months-long social engineering campaign.[20]

September 20, 2025 – Collins Aerospace's MUSE check-in/boarding system was compromised causing widespread flight delays across Europe, following a HardBit ransomware attack.[21]

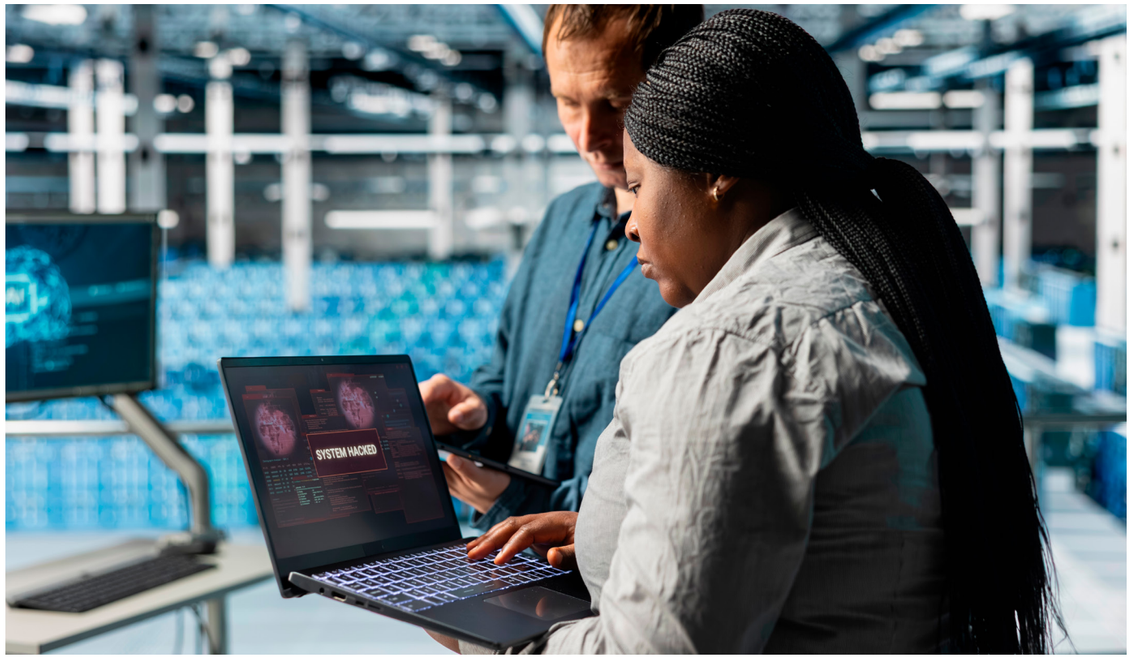
In sum, Q3 2025 reflects an evolving ransomware landscape, with established players like Qilin strengthening their dominance, while new entrants such as Coinbase Cartel and The Gentlemen redefine extortion tactics and flexibility. As organisations face increasingly fragmented, yet sophisticated adversaries, reliance on traditional defences is no longer sufficient. Intelligence-driven security strategies, stronger third-party risk management and rapid incident response frameworks are required to mitigate financial and reputational damage. Moving into the last quarter of 2025, the key challenge will be anticipating how hybrid ransomware and data extortion models continue to evolve as well as collaborate.

Section 4

Ransomware Spotlight: NYU Researchers Release AI Ransomware Proof-of-Concept

On the 28th of August 2025, New York University researchers released a proof-of-concept (PoC) large language model (LLM) controlled ransomware that can autonomously conduct reconnaissance, execution, and evasion, named “Ransomware 3.0”. This was achieved by deploying modules to a victim system that enables interaction with a server hosting an LLM, which sends dynamic code based on the target environment.[22]

Ransomware groups are actively using Artificial Intelligence (AI) in different areas of their operations, such as malware development and code optimisation in the wild. The release of PromptLock illustrates new ways in which AI could be exploited by threat actors in their operations. That said, the requirement for privileged initial access, unmonitored outbound connectivity, and common user level security controls, are a significant barrier to seeing similar activities in the wild.



PromptLock Proof-of-Concept

The experimental LLM ransomware payload was initially named “Ransomware 3.0”, later dubbed “PromptLock” by ESET security researchers, who discovered samples of the payload on VirusTotal. ESET then reported that PromptLock is the first example of AI ransomware found in the wild. However, NYU researchers clarified that PromptLock was a PoC that cannot be used by threats in its current state.

The payload uses LLMs to autonomously plan, adapt, and execute a ransomware attack. Initial access is assumed to a level where attackers can deploy three core modules on the victim system. Once the Lua interpreter, public key, and HTTP transport modules are deployed, the victim machine can begin interacting with the attacker controlled LLM server. The payload contains four prompt sets which enumerate files and obtains system information.

Once sensitive files are identified, the HTTP transport module sends Lua code to the victim system, which is executed by the interpreter. Identified files are encrypted, exfiltrated, and sometimes if ransoms aren’t paid, destroyed, using three different payloads. The researchers attempted to realistically mimic core ransomware threat objectives. Each payload is tailored to the target system based on information found during the reconnaissance phase. Once complete, the fourth prompt generates a personalised ransom note. LLM-generated Lua code is sent from the LLM server to the target system, adapting and executing code, depending on what is found in the target environment. PromptLock achieved a 100% success rate when identifying sensitive file systems during testing across PC, server, and controller platforms. The success rate slightly decreased during the exfiltration and encryption phases, which was attributed to policy refusals on the LLM side.[23]

PromptLock is a functional PoC designed to work in a lab environment. Researchers stated that an LLM orchestrated ransomware attack is “feasible”.[24] Recon, execution, encryption, and exfiltration can be achieved, which are key components of most ransomware attacks. PromptLock demonstrates many capabilities that are common today, but lacks advanced techniques used by sophisticated threat actors. Threat actors cannot directly use the code without significant modifications. However, researchers demonstrated it is possible to minimise human input in a ransomware attack. The overall lowering of the technical barrier through source code leaks has allowed less technically proficient threat actors to conduct attacks. PromptLock’s release could be viewed in a similar nature. However, the limited capability and controlled environment is a possible short-term barrier to seeing attacks in the wild.

Section 5

Emerging Cyber Security Trend: Cookie Hijacking in 2025

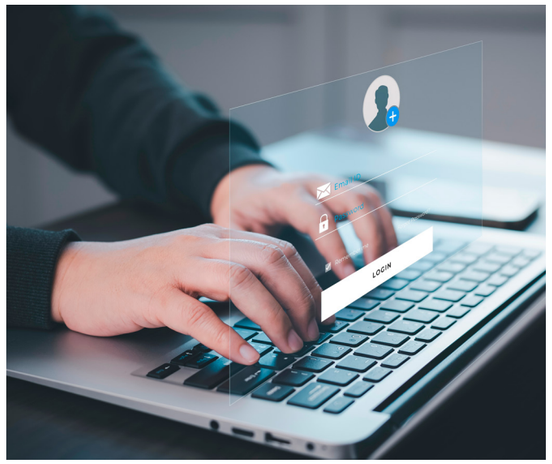
Cookie hijacking, also known as session hijacking, is the theft and reuse of session cookies or equivalent authentication tokens. This is used to impersonate a legitimate user without needing the password or the second authentication mechanism.[25] As of 2025, this technique has retained its strategic importance because attackers can use the stolen sessions to bypass password protections and, in many cases, multifactor authentication (MFA).[26,27]

Sekoia's analysis highlights a surge in adversary-in-the-middle (AiTM) phishing campaigns throughout 2025. A key enabler of these attacks is the theft of session cookies which allowed threat actors to hijack authenticated sessions without any credentials.[28]

This technique, combined with phishing-as-a-service (PhaaS) platforms and widely used AiTM kits like Tycoon 2FA and EvilProxy, has lowered the barrier to entry for attackers. While PhaaS platforms offers a "one-stop shop" for infrastructure, the technique itself is sophisticated since it bypasses MFA without requiring deep technical skill. By relaying the full authentication flow and capturing session tokens, attackers can skip credential harvesting entirely and operate with stolen sessions.

AiTM phishing enables attackers to be in the middle of the authentication process by using a reverse proxy that relays traffic between the victim and legitimate service. This allows them to eavesdrop in real time, capturing credentials, MFA codes and session cookies as the user logs in. These capabilities enable large-scale campaigns that bypass traditional security and exploit trust placed in authentication sessions.

Today, identity-centric intrusions are becoming increasingly prominent as organisations adopt MFA more widely. To bypass MFA, attackers apply techniques such as cookie hijacking. This allows them to capture and reuse authenticated sessions without needing credentials or MFA codes. Of note, Microsoft reported a very large year-on-year increase in AiTM phishing, which specifically targets session tokens and can neutralise MFA when an authenticated session is captured at the time of login.[29] Threat actors have been increasingly exploiting session tokens harvested through infostealer malware, phishing kits, and man-in-the-middle attacks.



In support of this trend, SpyCloud's Annual Identity Exposure Report 2025 revealed that the number of exposed identity records which include cookies and tokens grew by approximately 22% in a single year, surpassing 53 billion unique records.[30] This data confirms a clear and accelerating growth in identity-centric threats, particularly involving session tokens and cookies. The surge is driven not only by the increasing sophistication of attackers, but also by the accessibility of the techniques such as AiTM phishing and token theft, supported by PhaaS platforms.

The growing reliance on cookies and tokens for modern authentication has made these assets highly attractive to attackers.[31] Once obtained, these cookies often remain valid for extended periods due to organisations' long session lifetimes, weak token revocation practices, and limited enforcement of device or location binding. This persistence enables adversaries to maintain access well beyond the initial intrusion, often without triggering immediate detection.

Collectively, these developments signal that cookie hijacking is a key attack vector shaping the threat landscape in 2025. As adversaries capitalise on malware-enabled harvesting and commoditise PhaaS, defenders must treat session security as a first-class concern, recognising that traditional password-centric defences are insufficient.

Section 6

Geopolitical Developments

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

01/09/25

Between 1st and 3rd September 2025, China hosted non-Western global leaders for a regional security summit and Victory Day anniversary event. The events showcased China's willingness and capability to leverage geopolitical shifts largely driven by US domestic and foreign policy activities since the start of President Trump's second term.[32] Challenge to the historically US-led world order was observed with speeches proposing alternative futures, and the public recognition and celebration of warm relations between China and both traditional Western allies such as India, and sanctioned countries such as Russia and North Korea.

09/09/25

On 09/09/25, 21 drones entered Polish airspace across its eastern border. NATO military aircraft responded, shooting down drones perceived as a threat once they crossed the Polish border.[33] The timing of the incursions preceded the start of planned military exercises by Russia and Belarus in proximity to the Polish border with Belarus. Russia maintained a narrative, supported by Belarus, of the incursions being accidental consequences of their active conflict within Ukraine.

Within Poland, senior officials and military sources have consistently rejected this narrative, describing the incident as deliberate, provocative and strategically focused to test NATO defences around high value targets. Russia accused Estonia of fabricating reports of incursions into Estonian airspace by Russian fighter jets on 19/09/25.[34] A series of subsequent air-related disruptions are described as consistent with hybrid attacks: European air travel was disrupted over multiple days following a ransomware attack on 19/09/25 targeting systems supporting automated check-in systems, whilst air travel was suspended for hours in Norway and Denmark on 22/09/25, due to drone sightings in close proximity to major airports.[35]

09/09/25

On 09/09/2025 Israeli missiles struck buildings used by Hamas leadership as a political base in Doha, the capital of Qatar.[36] The attack followed an armed wing of Hamas claiming a gun attack on Israeli civilians in Jerusalem.

The timing of the attack also coincided with formal negotiation talks with Hamas representatives mediated by Qatari representatives. Israel subsequently confirmed the attack was intended to target senior Hamas leaders. The USA is reported to have provided assurances that no further attacks will occur.

International pressure on Israel (and the USA) grew later in the month with the UK, Canada, Australia and Portugal recognising a Palestinian state on 21/09/25.[37] France, Belgium, Luxembourg, Malta and Andorra added their recognition at the UN General Assembly the following day. Delegates walked out during Prime Minister Netanyahu's address.[38] In the Middle East, the UAE cautioned that Israel's activities risked undermining the Abraham Accords, a diplomatic development achieved during President Trump's first term. In parallel, the US presented a plan for peace in the conflict and President Trump made public statements that it was 'time to stop now'.[39]

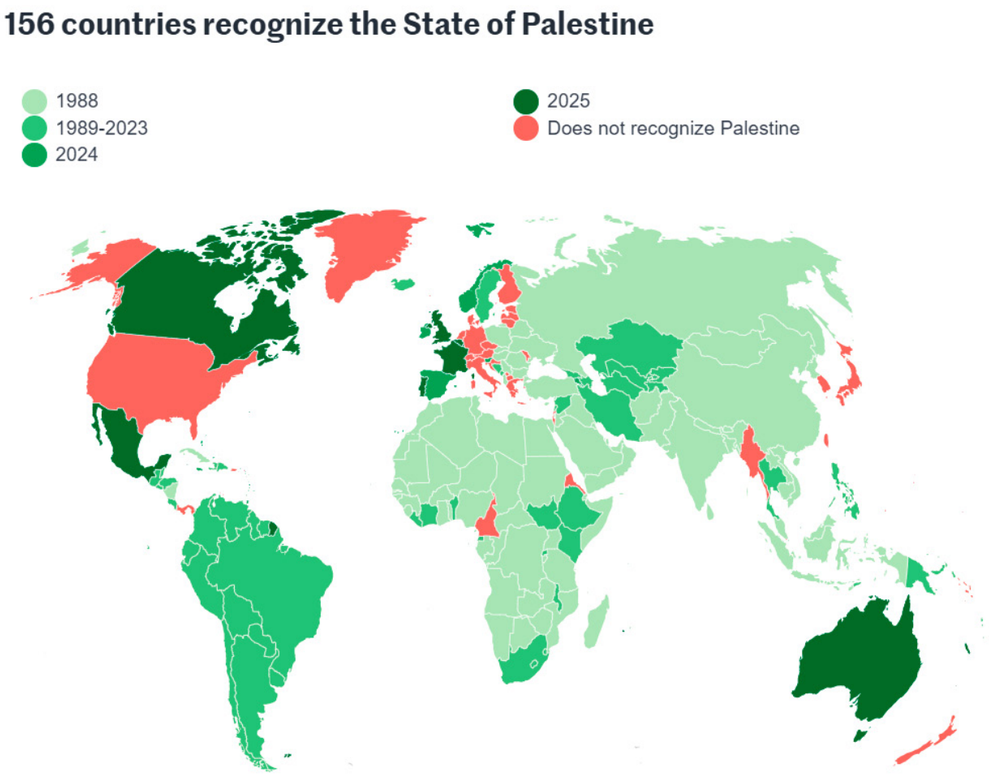


Figure 5 - Expansion of recognition of the State of Palestine over time. (Source: Le Monde)[40]

About NCC Group

“People powered, tech-enabled cyber security”

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

For over 25 years, we’ve been trusted by the world’s leading companies and governments to manage and deliver cyber resilience, working together to create a more secure digital future. We are proud to deliver important and groundbreaking projects for our clients.

We operate as one global business, with in-country delivery tailored to local needs and cultures, as well as a global delivery team to respond quickly to our clients’ challenges. Headquartered in the UK, we also have a significant market presence in Europe, North America and APAC.

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


ncc group
FOX IT
part of ncc group