ncc group

FOX IT
part of ncc group

Cyber Threat Intelligence Report

Review of October 2025

Contents

Section 1
Executive Summary

Ransomware activity throughout October has continued to increase month on month from August, reversing the downward trend we observed from March onwards. Once again, the Industrials sector remains the most targeted, accounting for 28% of all victims in October. Qilin, the most prominent actor last month and throughout Q3, remains the most prolific ransomware actor in October with 29% of all attacks attributable to the group.

This month's Ransomware Spotlight focuses on the emergence of The Gentlemen ransomware group as well as an observed increase in ransomware variants in the landscape. The Gentlemen were first observed in September of this year, and have already launched advanced, and tailored, attacks on organisations across the globe. The emergence of The Gentlemen can be seen as indicative of the rise in ransomware variants seen in 2025, with over 200 different variants observed throughout the course of the year.

The extended Spotlight examines the return of LockBit, with the launch of their 5.0 iteration and apparent alliance with other prominent RaaS groups. The LockBit operation has evolved significantly since its initial observation in 2019, and weathered multiple law enforcement operations. This experience, combined with an apparent alliance with DragonForce and Qilin, makes them a group worthy of continued monitoring.

In geopolitical news, the GTI team has been following continued developments in the Israel-Hamas conflict, particularly relating to ceasefire and exchange of hostage agreements. Additionally, the fluid U.S.-Russia relationship is observed and examines the announcement of sanctions targeting the largest two oil companies in Russia, as well as their subsidiaries. America also signed an agreement with Australia to increase cooperation on critical minerals, whilst Japan saw the swearing in of their first female President, Sanae Takaichi.

The Emerging Cyber Security Trends research conducted by NCC Group's TI function in October explores the growing threat posed by fileless malware, with a focus on a newly observed strain called EggStreme. Fileless techniques have become increasingly prevalent throughout 2025, used by financially motivated criminal groups and state-sponsored APTs alike. The EggStreme tool was reportedly used to compromise a Philippine defence company and used for persistent access with the objective of long-term espionage.

The TI team's Thought Piece for October explores digital ID systems and their associated risks. This is inspired by the UK government's 26th September announcement to launch a digital ID scheme before the end of the current parliament. It is intended to simplify the process of proving identity and right to work, in addition to access to public services and housing. Despite positive intentions, any ambitious scheme like this requiring a national database will encounter significant security risks and opposition from civil liberties groups. Cyber attacks on critical national infrastructure, third party breaches, and concerns over state surveillance have all been raised in response to the government's announcement.

Section 2

Ransomware Statistics October 2025

41%

Global ransomware attacks increased by 41% in October 2025

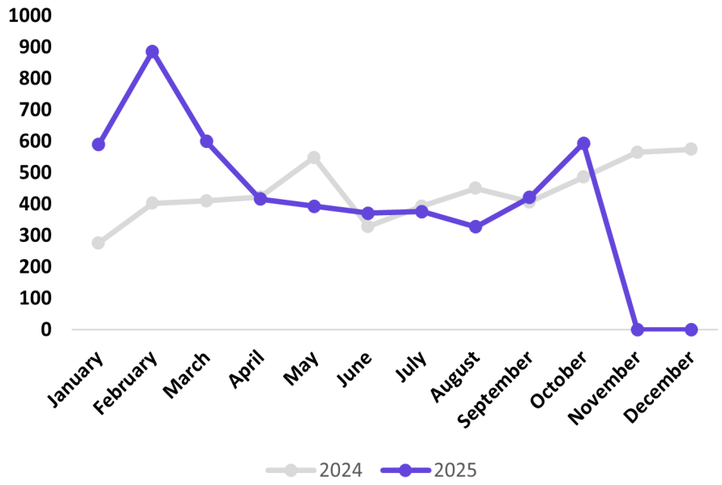


Figure 1 Ransomware Attacks by Month 2024 - 2025

28%

Industrials accounted for 28% of ransomware attacks in October 2025

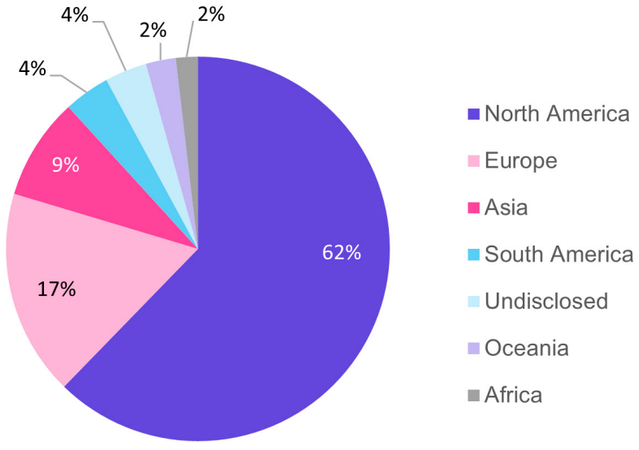


Figure 2 Ransomware Attacks by Region – October 2025

29%

Qilin was responsible for 29% of attacks in October 2025

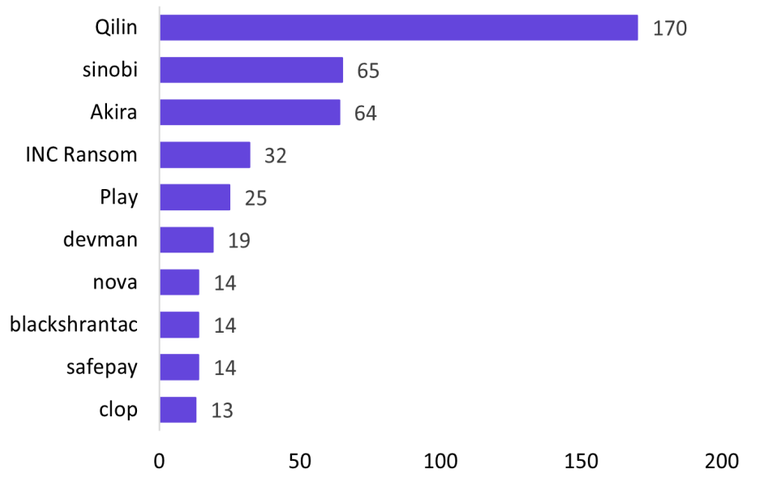


Figure 3 Top Threat Actors – October 2025

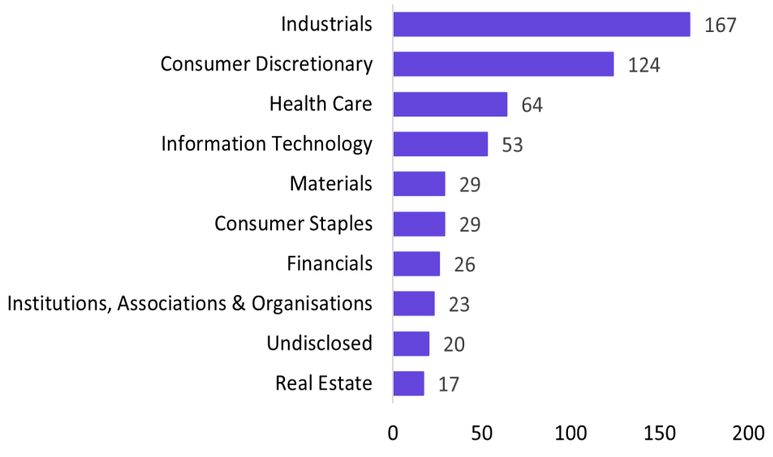


Figure 4 Top Targeted Sectors – October 2025

Key Events

14/10/25

Volkswagen Group France

The company suffered a ransomware attack reportedly carried out by the cybercriminal group Qilin. The attackers claim to have stolen around 150 GB of sensitive data, including personal information of vehicle owners, detailed vehicle data, and internal company documents. To validate their claims, Qilin published six documents online as proof of the breach.

16/10/25

Australian Fluid Power

It was targeted in a cyberattack involving unauthorised access to a limited number of its IT systems, resulting in the compromise of employee, customer, and supplier information. The ransomware group Anubis claimed responsibility and leaked stolen data online.

20/10/25

UK Ministry of Defence

The Russian-linked Lynx Group leaked hundreds of sensitive UK Ministry of Defence contractor files, exposing personal data and operational details of eight military bases, posing serious risks to national security and privacy.

Section 3

Ransomware Spotlight: The Gentlemen Ransomware's Emergence and the Increase in Variants

The Gentlemen ransomware group emerged in September 2025, and by October's end had made 21 public ransomware attack claims targeting organisations across Asia, South America, Europe, and Africa. The Gentlemen were recently highlighted by Trend Micro for their ability to launch advanced and tailored attacks targeting enterprise systems, making them a notable new group to add to the watchlist.[1] The emergence of the group is part of the ongoing trend in which new variants continue to appear across the ransomware landscape. Often, ransomware attack claims by new groups are subject to scepticism as new and copycat actors may make claims based on data that was present in a previous breach. The Gentlemen, however, appear to be a legitimate new group, making their mark on the threat landscape.

Who are The Gentlemen Group?

So far, information regarding The Gentlemen primarily originates from their public attack activity and the September attack investigation report produced by Trend Micro. In September 2025, The Gentlemen ransomware group emerged and made 21 attack claims by the end of October. These organisations appeared to be operating in a range of sectors from healthcare, financials, IT, and consumer discretionary. These claims were uploaded to their Data Leak Site (DLS) which listed their attack claims and corresponding timers threatening the leaking of exfiltrated data.[2] The Gentlemen are likely engaging in double extortion ransomware activity which focuses on encrypting and exfiltrating the data of their victims.

New to the scene, The Gentlemen appear to be keeping a relatively low profile as they have not made a high volume of claims in a short period of time, a tactic often observed with newer groups who attempt to draw media attention and magnify their image to pressure their victims. In terms of individual attack incidents, the group began leaking data from 2GO in October 2025, a large logistics company based in the Philippines. NCC Group assesses that the data is likely legitimate as 2GO does not have any previous record of being breached in the past.[3]

A broader review of all the public claims by The Gentlemen showed that there was no overlap with claims from other groups between 2021 to 2025.

New variants within the threat landscape often produce little evidence of a new breach and rely on old breach data to extort their victims. Ransomware variants such as Funksec and Babuk both made a high volume of claims that were assessed to be recycled data.[4,5]

To ensure accuracy, security teams can compare behavioural data between new ransomware groups to identify indicators such as recycled data and an unusually high volume of attack claims to assess if the group's activity is legitimate. Organisations must be able to verify and assess a threat's capability when conducting defensive efforts and using security resources to ensure accuracy.

Final Thoughts

The 2025 ransomware landscape is likely seeing threat actors evolve based on external pressures. Notably, threat actors are undertaking a diverse range of strategies to increase the likelihood of being paid. Some like The Gentlemen have taken a low-profile approach by making a relatively low number of ransomware attack claims whilst conducting legitimate attacks.

This trend is likely to continue as record numbers of variants have proliferated. Moreover, threat actors will continue to engage in activities that make attribution through TTPs and Indicators of Compromise (IoCs) difficult for defenders. Organisations may be become unprepared or dismiss such groups entirely as fraudulent. Once core ransomware mitigations are implemented, organisations should consider refining or adding intelligence-based mitigations that identify threats that may have been missed.

Section 4

Extended Spotlight: LockBit's Return: Launch of Version 5.0 and Alliance with Prominent RaaS Groups

LockBit first emerged in 2019 and has made a significant return with the launch of LockBit 5.0 in early September 2025.[6] The announcement, first reported on the Ransom Anon Market Place (RAMP) dark web forum, marks the group's re-entry following a period of inactivity due to law enforcement actions in 2024.

LockBit 5.0 is the latest expansion of their ransomware, building from the LockBit 4.0 structure whilst introducing refinements that decrease the detectability.[7] This variant features modular architecture so affiliates can add components per campaign with speed optimisation, stronger anti-analysis and Dynamic Link Library (DLL) reflection capabilities. LockBit continues to offer Windows, Linux and ESXi versions, which confirms the continuation of a cross-platform strategy. Consequently, this enables simultaneous attacks across enterprise networks with the capability of encrypting entire virtualised environments.

Unlike previous versions, LockBit 5.0 grants affiliates permission to target critical infrastructure, including nuclear, thermal, and hydroelectric power plants.[8] This is a change from earlier guidance that discouraged such attacks, which were introduced after the widespread backlash following high-profile incidents such as the Colonial Pipeline attack in May 2021.

Alliances with Other Ransomware Groups

Recent reports suggest that LockBit has entered a strategic alliance with two other ransomware groups, DragonForce and Qilin.[9] They are said to be sharing tools, infrastructure, and tactics to make their attacks more effective.

As a result, this partnership could increase the number of double-extortion schemes and accelerate the scale and sophistication of attacks, particularly against critical and traditionally low-risk sectors such as consumer services, public sector, and education.[10] The partnership is also likely aimed at rebuilding LockBit's reputation within the cybercrime community, reassuring affiliates of its continued relevance and operational capacity following the 2024 law enforcement disruptions.

The alliance between LockBit, DragonForce and Qilin combines technical expertise, resources and infrastructure, creating a network capable of sustaining large-scale ransomware operations whilst complicating attribution and response for organisations and law enforcement.

Although LockBit, Qilin, and DragonForce have discussed collaboration and appear to share similar objectives, there is currently no independent verification of joint operations. Currently, no confirmed joint attacks have been detected, and the extent of their actual cooperation remains unclear. This reported alliance may also serve as a marketing strategy by LockBit to restore trust and attract affiliates for future versions.

Final Thoughts

The reported partnership between LockBit, DragonForce, and Qilin highlights a significant shift in the ransomware landscape. By joining their resources and tactics, the groups can potentially coordinate more complex attacks as seen in recent incidents with Lapsus$, Scattered Spider, and ShinyHunters.

Although the duration of this alliance is unclear, it suggests that ransomware groups are adapting to share knowledge and operate without triggering law enforcement action. Many alliances that are formed are short-term, aimed at specific goals, and then split up due to internal issues or changes in the threat landscape, much like alliances of the Lapsus$, Scattered Spider, and ShinyHunters. However, the developing skills and resilience of these groups suggest that future partnerships could last longer and have a greater impact than previously seen.

Section 5
Geopolitical Developments

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

09/10/25

On Thursday 09/10/25 Israel and Hamas signed an agreement to implement a ceasefire, partial withdrawal of Israeli troops within Gaza, and exchange of Israeli hostages for Palestinian prisoners.[11] Brokered by the USA with President Trump personally involved, the development was described by the USA as the end of a 2-year period of war between Israel and Hamas and 'the historic dawn of a new Middle East'.[12]

Having initiated the ceasefire on 10/10/25, on 13/10/25 the 20 remaining living hostages were released by Hamas and returned to Israel.[13] In parallel, nearly 2,000 Palestinian prisoners were released by Israel. Separately the USA and regional allies Egypt, Turkey, and Qatar formally agreed to moderate the agreement and implement a wider US-authored 20-point plan for long-term peace.[14] At the time of writing, remains of 21 of 28 deceased hostages have been returned.[15] Aid delivery into Gaza has increased, however it continues to be limited by remaining Israeli restrictions, security challenges, and damaged infrastructure.[16]

Despite reported violations of the ceasefire in October and concerns over the long-term capabilities of the 20-point plan to achieve peace, efforts to establish elements of the framework required for the next stage are being actively discussed and progressed.[17] Key areas are security, governance, reconstruction and the role/presence of Hamas.

20/10/25

On 20/10/25 the USA and Australia signed an agreement to increase cooperation in the area of critical minerals.[18] The deal includes short term commitments for each country to invest $1 billion into related mining and processing capabilities within Australia and minimum pricing levels. The White House reported overall investment commitments totaling $5 billion to realise natural resources valued at $53 billion.[19] The agreement recognises the strategic importance of reliable access to both the raw materials and refined products of specific natural resources to the USA's manufacturing goals and strategic interests. Currently, China dominates control of rare earth supply chains globally, and has demonstrated increased willingness to leverage - and arguably weaponise - this control as part of the ongoing US-China trade war, and to respond to broader geopolitical tensions. Separately, additional trade and cooperation were reported in the areas of defence, space and other advanced technologies, and investment funds.

22/10/25

In October 25, the US administration was observed to change its approach towards Russia. The media reported on 21/10/2025 that plans for President Trump to meet again personally with President Putin of Russia had been placed on hold.[20] The following day, the USA imposed economic sanctions targeting Russia's two largest oil companies: Lukoil and Rosneft, and their subsidies.[21,22] The US Treasury explained the measures as aiming to reduce Russia's available funding to continue the war, 'given President Putin's refusal to end this senseless war' in Ukraine. In parallel, the EU extended Russian restrictions, including a two-stage ban on Russian liquified natural gas (LNG).[23]

What NCC are watching

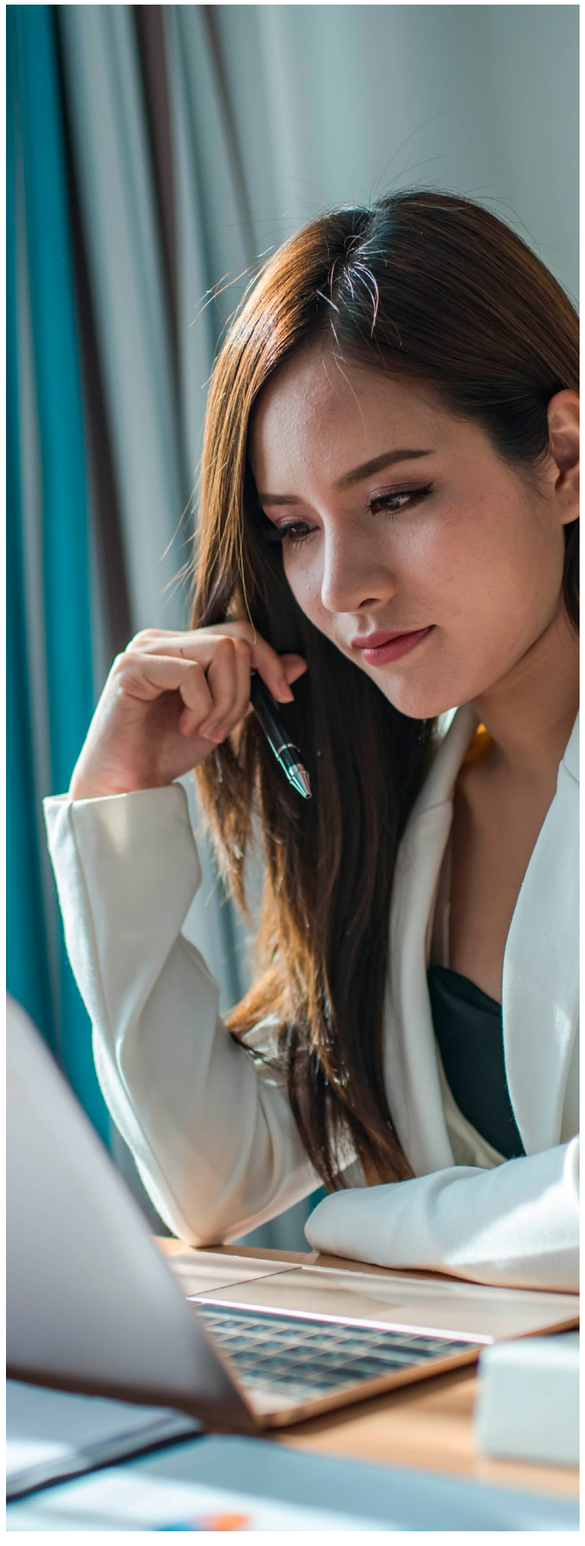
In Japan's national parliamentary elections on 04/10/25 the ruling Liberal Democrat Party (LDP) won the largest proportion of seats.[24] Leader of the LDP, Sanae Takaichi was sworn in as Japan's first female President on 21/10/25. Japan will be governed by a coalition of the LDP, supported by a right-wing party known as Ishin.[25] The coalition remains 2 votes short of a majority.[26] Analysts assessed the LDP's appointment of Takaichi as party leader in the run up to the election as a reaction to high cost of living coinciding with growing public support for opposition parties promising economic growth and anti-immigration policies.

The impact of Japan's new leadership is both framed as a political shift to the right, with uncertain outcomes during challenging geopolitical times and also as a potential return to the approaches of Shinzo Abe – Takaichi's mentor – during his time as Prime Minister between 2012-2020.[27] Japan's role in the global economy, regional security, and within Western alliances provides a new layer of uncertainty to the geopolitical landscape which influences the cyber threat landscape.

- Takaichi is described as a 'conservative nationalist' and 'pro-business politician'. Takaichi campaigned on increased spending and a more relaxed monetary policy, seeking to stimulate Japan's shrinking economy.[28]
- After one week in office, on 28/10/25 Japan hosted US President Trump and closing a trade deal between the two countries, leveraging; $550 billion investment opportunities, pledges to accelerate defence spending increases to 2% of GDP, natural resource supply chain cooperation, nuclear power opportunities, the historic relationship the former Prime Minister Abe, and a commitment to nominate President Trump for the Nobel Peace Prize.[29]
- On 24/10/25 in her first speech to Parliament as Prime Minister, Takaichi highlighted security concerns relating to China, North Korea and Russia and committed to restoring a role for Japan in global diplomacy and reinforcing the 'deterrence and response capabilities of the Japan-U.S. Alliance', as a 'cornerstone of Japan's diplomacy and securities policies'.[30]
- One area in which Takaichi is distinguished from her mentor Abe is Russia.[31] Takaichi has been consistently critical of Russia's war in Ukraine, calling for stronger Japanese sanctions against Russia in her campaign. As Prime Minister, Takaichi has already highlighted both Russia's 'aggression against Ukraine' and continuing territorial disputes in relation to four Japanese islands occupied by Russia since World War Two.[32]
- Hours before Takaichi's first address to Parliament on 24/10/25, Japan reported the triggering of a military air escort response to Russian warplanes travelling in close proximity to the edge of Japanese airspace. A Russian official described its activities as routine patrol activity. The Sea of Japan separates Russia's eastern border from Japan's western border.
- Takaichi maintains strong support for Taiwan as an 'extremely important partner and a valued friend for Japan' and is quoted as having considered a 'quasi-security alliance' between Japan, Taiwan and other regional and European partners.

Section 6

Emerging Cyber Security Trend: Emergence of EggStreme and the Growing Threat of Fileless Malware



Introduction and Overview

Fileless malware has rapidly evolved into one of the most challenging threats in modern cyber security. Unlike traditional malware that relies on malicious files written to disk, fileless attacks execute their payload entirely in memory.[33] It leverages legitimate systems and trusted processes to evade detection. This “living off the land” (LOTL) approach makes conventional signature-based defences nearly useless. This forces organisations to rethink their detection and response strategies ahead.

In 2025, fileless techniques have become increasingly prevalent in targeted attacks, particularly among advanced-persistent-threat (APT) groups and financially motivated cybercriminals. Attackers exploit trusted tools such as PowerShell, Windows Management Instrumentation (WMI) and mshta to perform malicious actions without leaving a footprint.[34,35] These methods are often combined with polymorphic or reflective loading mechanisms. This enables malware to continuously alter its in-memory structure and bypass behavioural analytics.[36] The technique’s stealth and adaptability have made it one of the most persistent cyber security challenges this year.

Traditional malware relied on files stored on disk, making them detectable through hash-based or heuristic scans. Over time, threat actors have shifted to memory-resident attacks, using scripts and legitimate binaries to deploy payloads dynamically. This reflects a move forward where attackers use built-in operating system tools to blend into normal network activity.

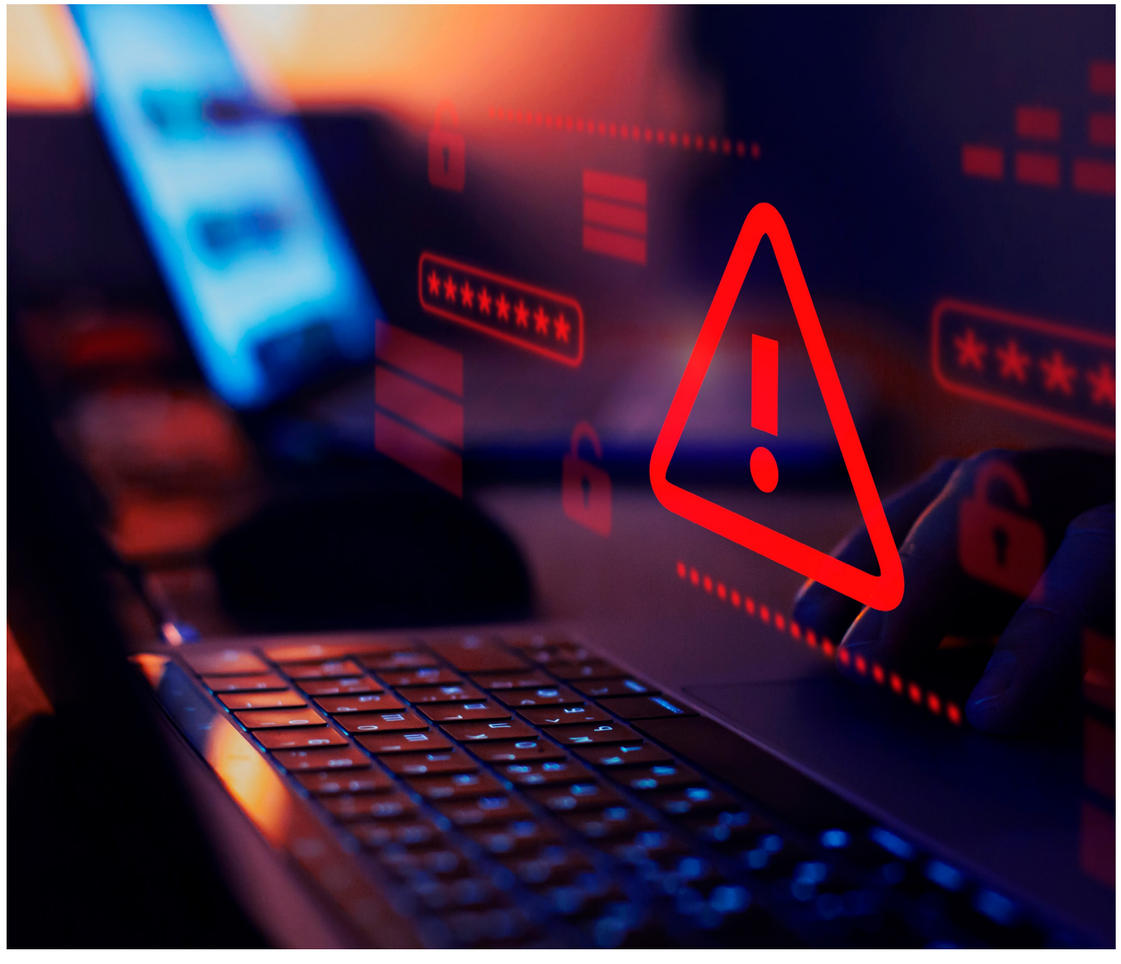
In early 2025, a new fileless framework named EggStreme was identified. The malware targeted a Philippine military company and used Dynamic-Link Library (DLL) sideloading and in-memory execution to achieve persistence and control. EggStreme features modular components such as keylogger and EggStremeAgent, a backdoor capable of encrypted command and control (C2) communications via HTTPS and DNS tunnelling.[37] This has also been reported to be linked to a Chinese APT, suggesting an espionage-driven objective.

EggStreme’s discovery underscores how threat actors continue to refine fileless tactics for stealth and persistence.

The campaign serves as a reminder that defenders must focus on behavioural detection, memory forensics and telemetry correlation rather than relying solely on file-based signatures.

Mitigating fileless malware like EggStreme requires a shift from traditional, file-based detection to a more behavioural and memory-centric defence strategy. Since these attacks live and operate in volatile memory and leverage legitimate system tools, defenders must harden every layer from endpoint configuration to network monitoring. This will improve visibility into in-memory and live execution activity.[38,39]

It’s important to understand the capabilities of these fileless malware, and to ensure that appropriate mitigations are consistently implemented. Defensive strategies must be operational and integrated into daily processes rather than treated as one-time actions. The sustained application of these practices will determine whether organisations can detect such threats early or remain exposed to evolving variants.

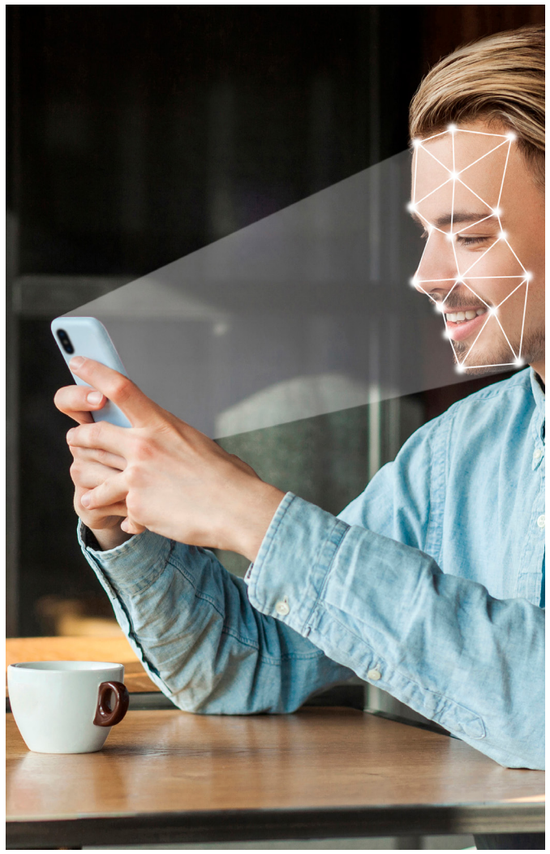


Section 7

October Thought Piece: Digital Identification Systems and Associated Risks

On the 26th of September 2025, the UK Government announced the intention to launch a new digital ID scheme across the UK, with plans for adoption by the end of the current parliament.[40] The aim of this programme is to help combat illegal working, with Digital ID planned to be a mandatory part of Right to Work checks.

With the announcement brings to light several considerations from the privacy and cyber security perspective; these proposals have already received public pushback, petitions, and criticism from public figures.[41]



Implementation Plan For The UK's Scheme And The Global Landscape Of Digital ID

The UK's announced programme would consist of a digital identification held on a smartphone and stored in a digitally encrypted "wallet".[42] These IDs would be authoritative proof of who someone is and their residency status in this country; it will therefore include a name, date of birth, nationality or residency status, and a photo – as the basis for biometric security – similar to an eVisa or passport.

With this, the hope is to simplify the process of proving identity for work, as well as access to public services and housing. Policy-wise, the scheme aims to curb document fraud and block access to formal work for people without status, set against a shadow economy – estimated at 10.8% of GDP – where undocumented labour and identity abuse, including organised crime and human trafficking, persist.[43]

What Are The Privacy And Security Considerations Of These Programmes?

With ambitious national databases like this, there are undoubtedly going to be security risks. For one, this could create a single point of access for nefarious actors who may want to conduct large-scale cyber-attacks including espionage and data theft.

While personal data exists across various government entities, creating a central hub could be a quick and easy one-stop-shop for threat actors, especially if proper safeguards are not in place.

Privacy concerns also escalate dramatically. Such systems can enable mass surveillance, allowing authorities or those who gain illicit access to monitor citizens' activities at a large scale. This, coupled with advanced analytics, opens the door to profiling individuals, potentially influencing access to services or even shaping behavioural patterns.

The aggregation of personal identifiers also increases the risk of identity theft at scale, where a single breach could compromise countless identities and amplify financial and reputational harm.

Gaps In Government Cyber Resilience

Beyond third party attacks, government systems have also fallen victim to cyber-attacks on multiple occasions, with concerns about their cyber resilience posture. Earlier this year, the Ministry of Justice experienced a large scale cyber-attack that compromised millions of pieces of personal data (national insurance numbers, criminal records, employment data) from legal aid applicants.[44]

This shortfall in cyber posture is also felt amongst the public. Survey data from the Institution of Engineering and Technology (and the Cyber Security Breaches Survey) in 2025 shows that 56% of Brits are fearful of being victim to a cyber-attack, with only 24% believing their data is secure.[45] This study also found that two thirds think that the government should prioritise cyber security and invest in public awareness campaigns. This highlights a clear confidence gap among the public, and concern over cyber literacy across the country. Thus, where use is mandatory in certain contexts, successful rollout will depend on trust in the system's security, transparency, and redress mechanisms.

Final Thoughts

This is not just a UK issue; digital identity programmes continue to be advancing globally – for example, the EU anticipate rolling out the Digital Identity (eID) Wallet by the end of 2026.[46] UK organisations can learn practical lessons from these different deployments globally, while multinational firms will face similar requirements across jurisdictions.

If implemented carefully, with input from security experts, this programme has the potential to live up to its aims. However, there are numerous risks and considerations that will need to be taken into account.

Government should set the tone on security and privacy. That means publishing a clear security architecture, data minimisation model, and revocation process. It means independent testing before each major release, transparent reporting of findings, and a live plan for crypto agility and mass re-issue.

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