ncc group

FOX IT
part of ncc group

Cyber Threat Intelligence Report

Review of Q2 2025

Contents

Executive summary

The second quarter of 2025 saw continued activity across the threat landscape, from ransomware targeting major retailers to ongoing tensions in the Middle East. Threat actors continue to exploit global uncertainty and instability, to capitalise on their illegal activities.

In Q2, Hack and Leak numbers dropped to a total of 1180 attacks, a decline of 43% from Q1 2025. This decline could be due to multiple factors, including seasonal fluctuations as we enter the summer period. Equally, as discussed in February and March, the number of attacks earlier this year were heavily skewed due to Cl0p's bulk release of victims, largely inflating the overall numbers. Hence, we are now likely observing more stable numbers with a steady decline.

Our Spotlight this month explores Safepay, a ransomware group first identified in late 2024. Although quiet for much of 2025, many victims were observed in May, prompting curiosity amongst the threat landscape. Commentators researching SafePay's ransomware payload and TTPs have linked the group to several major ransomware gangs such as LockBit, ALPHV, INC ransomware, BlackCat and Play, suggesting a potential rebrand of major players that have since disbanded or were targeted by law enforcement.

Away from ransomware, the Emerging Cyber Security Trend explores the prevalence of API attacks. As digital transformation accelerates, APIs have shifted from being simple tools of integration to critical supports for business operations and innovation which makes them an attractive target for malicious threat actors. As APIs become more deeply embedded in AI, cloud, and mobile systems, understanding and mitigating their associated risks will be vital to safeguarding digital infrastructure in the years ahead. Looking ahead, organisations should prioritise API security to safeguard their systems and unlock the full potential of APIs as key components of business transformation.

Geopolitical tensions rose throughout the Quarter, with the 12 Day War between Israel and Iran being the main event. As such, this Quarter, Geopolitical Developments focus on the events and their wider implications for cyber security, and international security alike. It is considered fair to describe the nature of war as having changed the intractable nature of negotiations over Iran's nuclear programme and provided opportunities for significant geopolitical shifts. Possible outcomes in the areas of regime change, and which we consider, include Iran's nuclear programme, and the US relationship with Israel and Iran individually.

Section 1

Timeline of critical incidents Q2 2025

April 2025

14/04/2025

Suspected 4chan and internal data leaked

The controversial image board 4chan was hacked, with gigabytes of compressed data published online. Leaked screenshots circulating show 4chan's back end, including its source code, user ban templates, and a list of alleged moderators and "janitors" (users who can delete posts and threads).

20/04/2025

Cyber-attack on M&S leads to click and collect delays

Marks & Spencer (M&S), a major British multinational retailer of clothing, beauty products and more, dealt with a major cyber incident over the Easter weekend that affected its online operations and store services for weeks. Marks and Spencer confirmed that personal customer information was breached in the attack.

22/04/2025

SK Telecom sim data leaked in cyber-attack

SK Telecom, South Korea's largest mobile carrier announced that it was hit by a cyber-attack that led to the theft of personal data affecting approximately 23 million customers. 25 different types of personal information, including mobile phone numbers and unique identifiers (IMSI numbers), as well as USIM authentication keys and other USIM data, had been exfiltrated from its central database, known as its home subscriber server.

25/04/2025

Nova Scotia power confirms data breach, customer information compromised

Nova Scotia Power, the primary electricity provider in Nova Scotia, Canada, confirmed a cyber security incident involving unauthorised access into certain parts of its Canadian network and servers. Customer information stored on the impacted servers was accessed and exfiltrated by an unauthorised third party, including names, phone numbers, email addresses, mailing and service addresses, Nova Scotia Power program participation information, dates of birth, customer account history, driver's license numbers, and Social Insurance Numbers.

May 2025

21/05/2025

Europol and Microsoft disrupted the world's largest infostealer Lumma

Microsoft's Digital Crimes Unit (DCU), Europol, and international partners have disrupted Lumma's technical infrastructure, cutting off communications between the malicious tool and victims. Over 1300 domains seized by or transferred to Microsoft, including 300 domains actioned by law enforcement with the support of Europol, will be redirected to Microsoft sinkholes.

02/05/2025

Rhysida ransomware gang claims attack on Peruvian government

The Rhysida Ransomware gang claims that it had breached Peru's official digital platform, 'Gob[.]pe'. The group published the images of multiple documents allegedly stolen from the Peruvian government platform and demanded a five-bitcoin ransom, which equals roughly $471,000. This prompted Peru's Ministry of Government and Digital Transformation to publish a statement and deny any hostile takeover of its digital assets.

23/05/2025

Silent Ransom Group targeting law firms

The FBI Cyber Division has issued an advisory warning that the cyber threat group known as Silent Ransom Group (SRG), also known as Luna Moth, Chatty Spider, and UNC3753, is actively targeting law firms. The group employs IT-themed social engineering phone calls and callback phishing emails to gain remote access to systems or devices, enabling them to steal sensitive data for extortion.

27/05/2025

US Department of Justice seizes domains supporting crypting services

The U.S. Department of Justice (DoJ) took down an online cybercrime syndicate that offered services to threat actors to ensure that their malicious software stayed undetected from security software. The operation, in partnership with Dutch and Finnish authorities, seized four domains, and their associated server facilitated the crypting service. These include AvCheck[.]net, Cryptor[.]biz, Cryptor[.]live, and Crypt[.]guru, all of which now display a seizure notice.

28/05/2025

Connectwise hit by cyber-attack

ConnectWise, the developer of remote access and support software ScreenConnect, has disclosed that it was the victim of a cyber-attack that it said was likely perpetrated by a nation-state threat actor. ConnectWise stated that only a small number of ScreenConnect customers were affected, and that they have already been contacted. ConnectWise also confirmed that it has coordinated with law enforcement regarding the incident.

June 2025

10/06/2025

EU launches its own DNS service with practical functions

The European Union has officially launched its own DNS resolver, promising to be more privacy-compliant and cyber resilient. Known as DNS4EU, the service will be an alternative to major US-based public DNS services (like Google and Cloudflare). It includes built-in protection against malicious domains, such as hosting malware, phishing, or other cybersecurity threats. For home users, DNS4EU offers optional filters to block ads and adult content.

11/06/2025

Interpol's infostealer crackdown

More than 20,000 malicious IP addresses or domains linked to information stealers have been taken down in an INTERPOL-coordinated operation against cybercriminal infrastructure. Working with private sector partners Group-IB, Kaspersky and Trend Micro and sharing critical intelligence with cyber teams across Asia. They have seized 41 servers, over 100 GB of data, and arrested 32 suspects linked to illegal cyber activities.

17/06/2025

Pro-Israel hacktivist group claims attack on Iran's Nobitex exchange, destruction of $90m in crypto, and Bank Sepah hack

The pro-Israeli hacktivist group 'Gonjeshke Darande' (Predatory Sparrow) has claimed to have stolen over $90 million in cryptocurrency from Nobitex, Iran's largest crypto exchange, and burned the funds in a politically motivated cyber-attack. Prior to this, the group also took credit for disrupting Bank Sepah on June 17, alleging the destruction of its internal data. Iran's Bank Sepah is one of Iran's oldest financial institutions with ties to the Islamic Revolutionary Guard Corps (IRGC) and the Army. This attack reportedly caused a country-wide shutdown of ATMs and digital banking services.

25/06/2025

Iranian APT35 hackers targets Israeli tech experts in spear-phishing campaigns

The Iranian threat group Educated Manticore (APT35), linked to the Islamic Revolutionary Guard Corps (IRGC), has launched spear-phishing campaigns targeting Israeli journalists, high-profile cyber security experts and computer science professors from leading Israeli universities, according to a report by Check Point. The attacks began in mid-June 2025 following the outbreak of the Iran-Israel war that targeted Israeli individuals using fake meeting decoys, either via emails or WhatsApp messages tailored to the targets.

Section 2

Ransomware key statistics

43%

Global ransomware attacks decreased by 43% in Q2 2025

30%

Industrials accounted for 30% of ransomware attacks in Q2 2025

13%

Qilin was responsible for 13% of attacks in Q2 2025

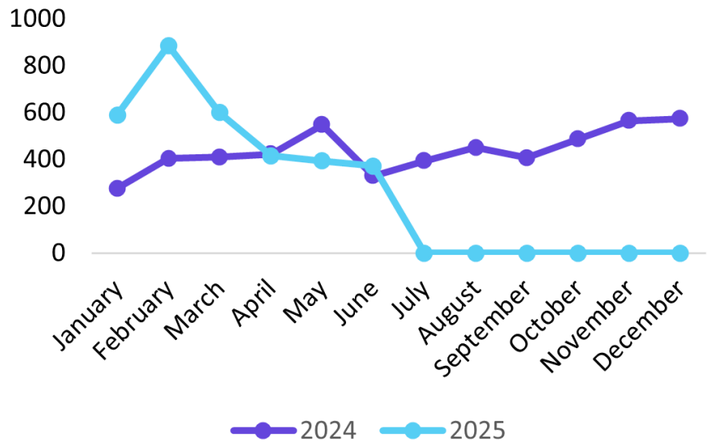

Figure 1 Ransomware Attacks by Month 2024 - 2025

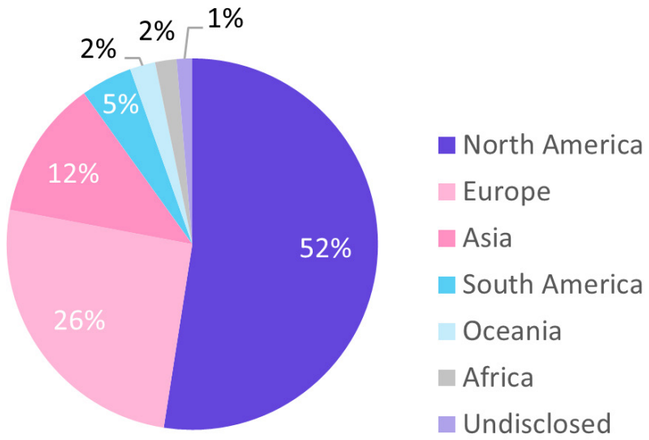

Figure 2 Ransomware Attacks by Region Q2 2025

Qilin ransomware group exploits Fortinet flaws for stealthy takeover

In mid-2025, Qilin ransomware exploited Fortinet flaws CVE-2024-21762 and CVE-2024-55591 to hijack FortiGate devices, bypassing authentication and executing remote code. This allowed them to deploy ransomware without phishing, marking a shift to automated, infrastructure-level attacks—faster, stealthier, and harder to stop.

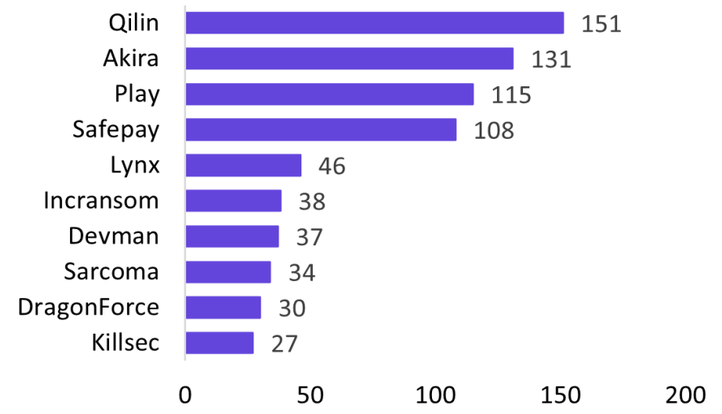

Figure 3 Top 10 Threat Actors Q2 2025

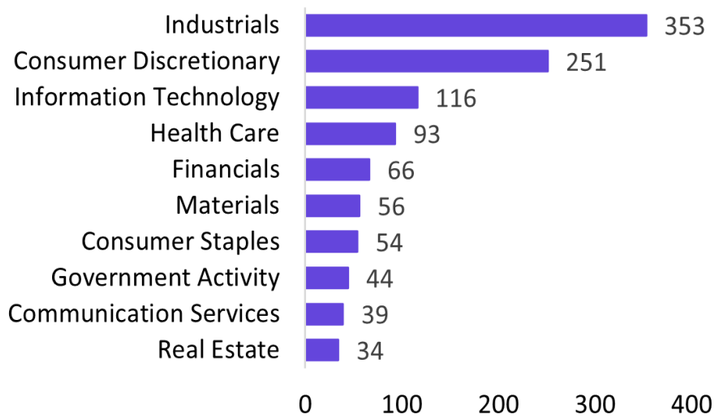

Figure 4 Top 10 Targeted Sectors Q2 2025

Key Events

April 2025

Indian defence and government systems

APT36 launched Operation Sindoor on April 17, 2025, targeting Indian defence and government systems. The campaign peaked May 7–10, using ransomware, espionage tools, and hacktivist support in a coordinated cyber assault.

May 2025

MATLAB

MATLAB services like Cloud Center and License Management, MFA, and SSO were impacted by a ransomware attack. Services were restored, but some issues persist. The attacker remains unidentified, and recovery is ongoing.

June 2025

Aviation sector

Scattered Spider has breached the aviation sector using impersonation and MFA fatigue tactics. Hawaiian Airlines and WestJet reported incidents consistent with the group's methods.

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

In Q2 2025, we observed a 43% decline in attacks, from 2074 attacks in Q1 to 1180 attacks in Q2. This follows a surge in ransomware activity during Q1, which saw unusually high volumes driven by aggressive campaigns from dominant groups such as Cl0p, RansomHub and Akira. The sharp decline in Q2 can be attributed to several factors, including significant law enforcement activity that disrupted key ransomware operators, notably targeting Cl0p and RansomHub affiliates. These disruptions likely caused a ripple effect across the ransomware group's ecosystem, forcing affiliates to regroup or shift to emerging ransomware groups. Additionally, seasonal slowdowns due to global holidays such as Ramadan, Easter and other mid-year observances may have contributed to a temporary dip in operational activity.

At the same time, Cl0p, RansomHub and Babuk2, who were dominant in Q1 disappeared from the Top 10 in Q2. Cl0p alone accounted for 396 attacks in Q1, suggesting that takedowns or affiliate migration significantly disrupted the operations of these groups.[1]

Qilin emerged as the most active ransomware group with 151 attacks, up from 95 in Q1.

This rise reflects a growing trend among ransomware operators targeting industrials and IT sectors, consistent with external reports which highlights Qilin's surge in April and June.[2,3]

Qilin now offers legal assistance to its affiliates through its "Call Lawyer" feature, helping them navigate negotiations to put more pressure on victims to pay up and to provide legal aid to affiliates, should they be caught in law enforcement interventions. This is an unusual feature which reflects the increasing professionalism and support infrastructure within the ransomware-as-a-service operations. This likely also makes them an attractive affiliate to work with.

Groups like Akira and Play remained active despite Akira seeing a decline from 213 to 130 attacks, and while Play amplified their targeting from 81 to 115 attacks. Meanwhile, other groups climbed the Top 10 such as Safepay, DragonForce and Killsec, which could indicate a shift in affiliate loyalty or the rise of new threat actors filling the void left by disrupted groups.

DragonForce ransomware implicated in the notable Retail attacks in the UK had allegedly evolved from a Malaysian hacktivist collective into a full-fledged ransomware cartel by 2025.[4] In Q2, they targeted high-profile retail and industrial sectors including UK brands like Mark & Spencer and Harrods.[5] The group operates as a ransomware-as-a-service (RaaS) model that allows affiliates to use its infrastructure and tools. Their aggressive campaigns and partnership with social engineering actors, such as Scattered Spider, make them a growing threat globally.

Where considering wider geopolitical tensions, in June, the Handala ransomware group targeted 17 Israeli organisations between the 14th and the 30th of June, coinciding with the 12 day Iran-Israel war.

The group have pro-Palestinian hacktivist motives and are suspected to originate from Iran. It would appear therefore that ransomware attacks are being utilised to push political messaging and signals a growing use of ransomware as a tool for cyber warfare. This may encourage other politically or ideologically driven groups to follow suit. As such campaigns intensify, they may also provoke state-level responses and further complicate the global cyber threat landscape and international security.

Overall, the ransomware landscape in Q2 2025 reflects both continuity and disruption. The decline of dominant players has opened a space for emerging threat actors to rise, whilst increasing global instability contributes to cyber activity. In the months ahead, we may expect disrupted groups to rebrand or return and collaborate with social engineering actors, which may lead to more advanced initial access methods.

Section 4

Ransomware spotlight: SafePay's emergence and connections to major ransomware gangs

SafePay ransomware was first observed in September 2024.[6] In recent months, the group has drawn significant attention to themselves with many claimed attacks and high-profile victims. The ransomware group made 70 attack claims in May 2025, making them the most active threat group for the month. Recently, the threat landscape has seen various threat actors, such as Babuk, falsifying their ransomware attack numbers to pressure victims to pay. This has added challenges to defensive efforts, especially when tracking legitimate threat actor activity. In the case of SafePay, the group's rise in attack numbers in May drew scepticism due to questionable ransomware attack claims from other threat actors. However, various security commentators have identified SafePay as being a likely rebrand of another group.[7]

The group recorded 70 incidents in May 2025, based on NCC's internal data - the largest number of attacks affiliated with the group since their emergence in September 2024. Out of all incidents, the United States (44%) and Germany (26%) were disproportionally represented. In terms of sectors, the group most commonly targets consumer discretionary, industrials, and healthcare.

A notable incident was a confirmed ransomware attack on Microlise, a logistics technology firm, that saw the exfiltration of 1.2TB of company data and the encryption of their virtual machines.[8]

The group likely gains initial access through existing domain account credentials and uses Living-of-the-Land techniques to deploy their ransomware payload. Once SafePay has a solid foothold in the victim environment, data is exfiltrated and encrypted to deny availability to system and network resources.[9] The group also utilises aggressive negotiation tactics by operating a "shame site" where non-paying victims are publicised. Direct phone calls between SafePay threat actors and victims have also been reported.[10]

SafePay appears to operate as a standard double extortion ransomware gang. The observed TTPs and victimology of the group points to the possibility that SafePay is a rebrand of another threat actor, including LockBit. Rebranding can be easily achieved by changing the group's name, data leak site (DLS), and infrastructure; a common tactic used when external pressure mounts.

Section 5

Emerging cyber security trend: Securing the digital backbone; API threats and defences

Application Programming Interfaces (APIs) are the backbone of modern digital infrastructure. They define how software components interact, allowing systems to exchange data and services seamlessly. APIs power everything from mobile banking apps and cloud platforms to IoT devices and AI-driven services.[11] As digital transformation accelerates, APIs have shifted from being simple tools of integration to critical supports for business operations and innovation which makes them an attractive target for malicious threat actors.

In late 2024, a global survey by Akamai revealed that 84% of security professionals had experienced at least one API security incident, up from 78% in 2023.[12] This trend is echoed in Salt Security's mid-2024 report, which found a 167% surge in API counts over the last 12 months, alongside a 37% increase in reported API security incidents. Additionally, despite growing API traffic, only 7.5% of organisations have implemented dedicated API testing and threat modelling programs.[13]

The threat landscape is intensifying in 2025. Traceable's industry wide survey reports that 57% of organisations have suffered API related data breaches in the past two years. Yet only 21% feel sufficiently equipped to detect API-layer attacks, and a mere 13% can prevent over half of such attacks.[14] Meanwhile, Cloudflare estimate that APIs now account for 60% of dynamic web traffic, with around a quarter classed as "shadow APIs" which are undocumented and unmanaged endpoints which evade protection.[15]

Additionally, Akamai reports bots now account for 42% of overall web traffic, and 65% of those bots exhibit malicious intent which often targets APIs.[16] As APIs grow more complex, 53% of organisations say that traditional solutions such as WAFs and WAAP are inadequate.[17] The integration of generative AI into APIs is also a contributing factor that widens the attack surface. Despite this high-risk environment, security maturity remains low. This lack of widespread visibility and oversight creates an uneven and volatile security posture. The more APIs organisations deploy without structure or governance, the more opportunities are created for attackers to exploit configuration errors, logic flaws and unmonitored endpoints.

Even though digital systems grow more connected to and dependent on APIs, security capabilities are failing to keep pace.

In 2024, for the first time, more than 50% of all recorded CISA exploited vulnerabilities were API-related.[18] As APIs become more deeply embedded in AI, cloud, and mobile systems, understanding and mitigating their associated risks will be vital to safeguarding digital infrastructure in the years ahead. Looking ahead, organisations should prioritise API security to safeguard their systems and unlock the full potential of APIs as key components of business transformation.

Section 6

Geopolitical developments: 12 Day War creates uncertainty

In this month's edition of Geopolitical Developments, we focus on the 12 Day War between Israel and Iran. We are choosing to share this as a feature piece, given the prominence of the events and ongoing tensions which threaten international security.

13/06/2025

On 13/06/25, Israel began military strikes on Iran, targeting their nuclear programme and military infrastructure.[19] US President Trump called for Iran to negotiate, stating it wasn't 'too late'.[20]

Within 24 hours, Iran retaliated with ballistic missile strikes against Israel, supported by missile attacks by Houthi militia in Yemen.[21]

21/06/2025

On 21/06/25, the US military conducted military strikes on Iran using specialist ground penetrating weapons against 3 Iranian locations with underground infrastructure supporting Iran's nuclear programme.[22]

In a televised speech on 21/06/25, President Trump described the attacks as a 'spectacular military success', describing total obliteration of Iran's nuclear enrichment facility.[23]

23/06/2025

On Monday 23/06/25, Iranian missiles targeted the Al Udeid US air base in Qatar, without casualties. By 12.28 hrs on 24/06/25 a US-mediated ceasefire was in effect, ending what has been referred to as 'The 12 Day War' (12DW).

Now what?

All sides have claimed victory, with individual narratives serving domestic audiences. It is considered fair to describe the nature of 12DW as having changed the intractable nature of negotiations over Iran's nuclear programme and provided opportunities for significant geopolitical shifts.

These developments and their consequences may influence the current cyber-threat landscape, but effects are on a scale of the risk rather than the nature of the threats. Possible outcomes in the areas of regime change, Iran's nuclear programme, the US relationship with Israel and Iran, explored in our full edition of the Pulse.

About NCC Group

“People powered, tech-enabled cyber security”

We’re a people powered, tech-enabled global cyber security and resilience company withover 2200 colleagues around the world.

For over 25 years, we’ve been trusted by the world’s leading companies and Governmentsto 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 client’s challenges. We have a significant market presence in the UK, Europe, North America and APAC, including our global deliveryand operations centre in Manila, the Philippines.

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


ncc
group


FOX IT
part of ncc group