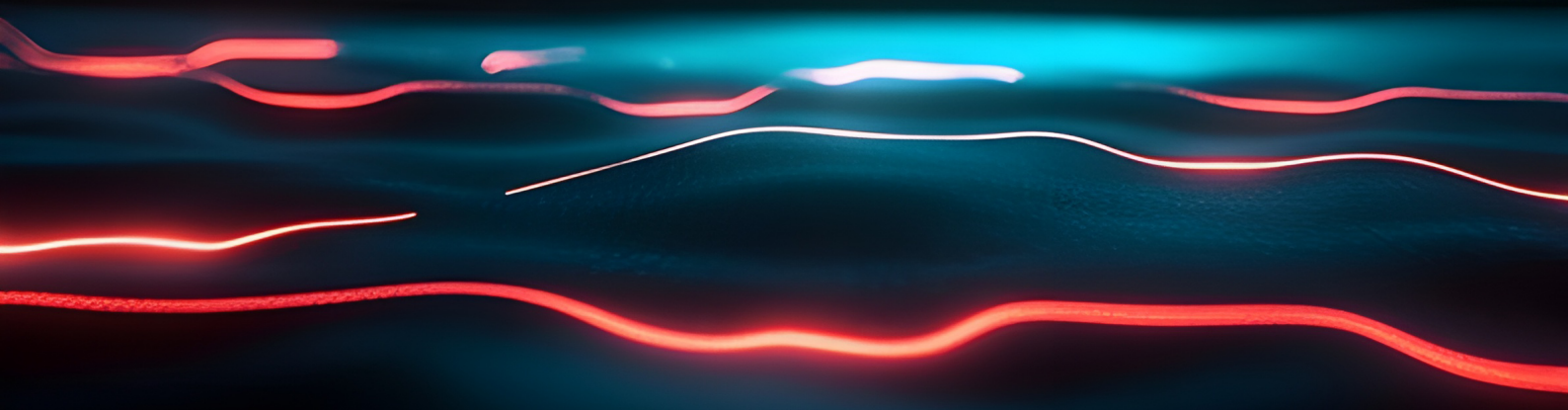
CyberProof®
A UST Company

Better Security,
Together.

CyberProof 2025 Mid-Year Cyber Threat Landscape Report

H1 2025 ANALYSIS

August 2025



cyberproof.com

Executive Summary

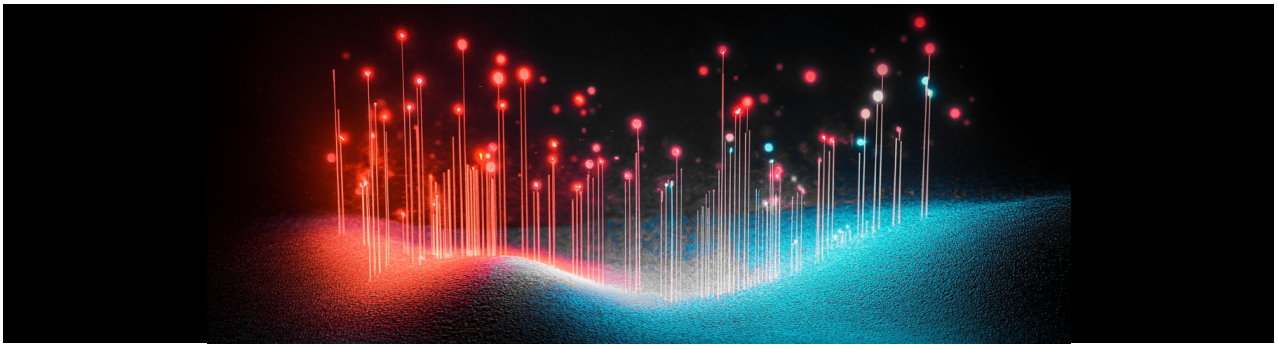
The first half of 2025 has witnessed a significant evolution in the cyber threat landscape, characterized by the emergence of sophisticated AI-powered ransomware groups, intensified targeting of critical infrastructure, and the continued blurring of lines between nation-state actors, cybercriminals, and hacktivists.

The period has been marked by several high-profile campaigns, including the persistent activities of Scattered Spider targeting the retail sector, the emergence of AI-centric ransomware groups, and the continued dominance of established players like Akira ransomware.

Key findings from H1 2025 include a 60% surge in ransomware attacks compared to the previous period, with Akira alone responsible for 72 attacks in January. The manufacturing sector emerged as the most targeted industry with 75 incidents globally, while the United States remained the primary target geography with 259 incidents. Notably, new threat actors have leveraged artificial intelligence to lower barriers to entry in ransomware operations, while established groups have adopted increasingly sophisticated supply chain attack methodologies.

The threat landscape in H1 2025 was further shaped by a series of high-impact infrastructure attacks, particularly involving China-aligned APT groups. Notably, Salt Typhoon compromised at least nine major U.S. telecommunications providers, signaling a renewed focus on critical communications infrastructure. In parallel, groups such as Silk Typhoon shifted toward targeting IT supply chain providers—demonstrating a strategic pivot aimed at exploiting trusted third-party relationships to access downstream victims.

Major Threat Trends in H1 2025



The first half of 2025 also revealed several defining threat trends that shaped the global cyber landscape. These developments reflect a broader shift toward more targeted, scalable, and collaborative attack methods.

AI-Powered Ransomware Operations

The emergence of AI-assisted ransomware development has fundamentally altered the threat landscape. FunkSec represents the first major ransomware group to extensively leverage AI for code development, creating barriers-to-entry reduction for less technically sophisticated actors. The group's use of GenAI for creating encryption capabilities and their rapid iteration cycles demonstrate how AI can accelerate threat actor capabilities.[1]

Supply Chain Infiltration Strategies

Chinese APT groups have significantly evolved their targeting strategies, with Silk Typhoon shifting focus to IT supply chain providers including remote management tools, cloud applications, and privileged access management platforms. This approach leverages trusted relationships to access downstream customers, making detection and mitigation more challenging.[2]

[1] https://www.infosecurity-magazine.com/news/new-ransomware-group-uses-ai/
[2] https://www.darkreading.com/remote-workforce/china-silk-typhoon-it-supply-chain-attacks

High-Impact, Low-Resilience Targeting

Threat actors are increasingly focusing on organizations that provide essential services but lack the defensive maturity to withstand sustained attacks. One prominent example is municipal governments, which have become frequent ransomware targets due to limited cybersecurity budgets and operational fragility. Adversaries are exploiting the digital transformation of local governments, taking advantage of cloud adoption and third-party dependencies to expand the attack surface. These incidents often disrupt critical public services and include data exfiltration to increase extortion pressure, reflecting a broader shift toward targets where even limited disruption creates significant leverage.

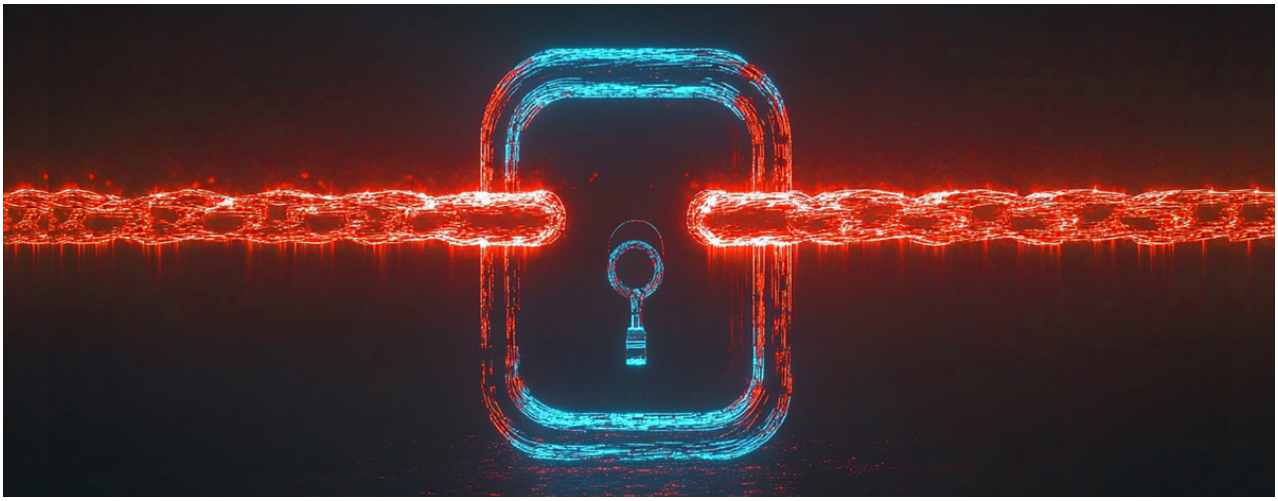
Infrastructure-as-a-Service for Cybercrime

The TAG-124 traffic distribution system (TDS) is a malicious infrastructure service used to redirect victims to malware payloads based on detailed profiling—including browser type, IP geolocation, and behavioral patterns. It functions as a "smart router" for cybercriminals, ensuring that malware is delivered only to high-value or relevant targets while avoiding detection. TAG-124 has been adopted by multiple threat actors, including FIN7, ransomware groups like Interlock and Rhysida, and state-sponsored entities, demonstrating how shared, professional-grade tools are streamlining cybercrime operations. Its growing use reflects the broader trend of cybercrime-as-a-service, where specialized infrastructure is commercialized and reused across different campaigns.[3]

Ransomware Cartel Models

DragonForce's "cartel" operation model represents an evolution in ransomware business structures, allowing interested actors to create their own brands while utilizing shared infrastructure and resources. This approach differs from traditional RaaS models by providing greater operational flexibility while maintaining centralized technical capabilities.

Major Cyber Events that Shaped H1



Various events shaped the threat landscape in the first half of 2025. From the ripple effects of geopolitical tensions manifesting as cyber spillovers, to a surge in major ransomware incidents and the widespread exploitation of critical vulnerabilities, these developments collectively affected cyber operations. The following details several pivotal global events that had a profound impact on threat activity during this period.

Geopolitical Conflicts and Cyber Spillover

India-Pakistan - In May 2025, heightened India–Pakistan border tensions sparked a surge in cyber activity, with over 650 confirmed DDoS and defacement incidents attributed to hacktivist campaigns like #OpIndia and #OperationSindoor.

[3] https://gbhackers.com/threat-actors-leverage-tag-124-infrastructure/

Pakistan-aligned groups such as APT36 and SideCopy targeted India's defense, government, telecom, and education sectors, while the Bitter APT group (TA397) launched spear-phishing attacks against Pakistan Telecommunication Company Limited (PTCL), focusing on high-value technical personnel. Malware like WmRAT was deployed to conduct signals intelligence and network mapping. In total, at least 45 hacktivist groups became active—pro-Pakistan and pro-India ones—highlighting how geopolitical tensions continue to fuel large-scale cyber operations.

Israel, US-Iran - In June 2025, amid rising Iran–Israel tensions, Iranian state-sponsored group APT35 (Educated Manticore) launched AI-enhanced spear-phishing campaigns targeting Israeli tech experts, cybersecurity professionals, and academics. Using fictitious personas over WhatsApp and email, attackers lured victims to fake Gmail and Google Meet pages under the guise of urgent AI-related security assistance. The campaign employed advanced phishing kits built with modern web frameworks, including 2FA bypass via relay attacks and passive keylogging. In parallel, U.S. agencies issued alerts warning of potential Iranian cyber operations targeting critical infrastructure, reinforcing concerns that the digital front would escalate alongside geopolitical conflict.

UK Retail Sector Targeted by Ransomware

In 2025, the UK retail sector faced a coordinated wave of ransomware attacks, with Scattered Spider identified as the initial access broker behind several major breaches, including those at Co-op, Marks & Spencer, and Harrods. Using advanced social engineering, the group posed as employees to deceive IT helpdesk staff to reset passwords and gain internal access, ultimately delivering DragonForce ransomware, which was used to encrypt systems and extort victims. The attacks caused significant operational disruption, including data breaches and service outages, with M&S believed to have been compromised as early as February. Additional high-profile incidents at Dior, Adidas, and Victoria's Secret were also reported during the same period, though attribution in those cases remains unconfirmed.

Widespread Exploitations in the Wild

One such example is CVE-2025-31324, a critical zero-day vulnerability in SAP Visual Composer with a CVSS score of 10.0, which was widely exploited in the wild during April and May 2025. Affecting SAP NetWeaver Visual Composer Framework 7.1x and above, the flaw allows unauthenticated attackers to upload arbitrary files and execute remote code, resulting in full system compromise.

Despite SAP issuing patches and mitigation guidance, many organizations hesitated to apply them due to the operational risks of disrupting mission-critical environments—leaving systems exposed for weeks. Exploitation occurred in successive waves, with early activity linked to Chinese state-aligned APTs conducting espionage, followed by ransomware groups leveraging the same vulnerability for initial access and lateral movement. The repeated and opportunistic abuse of CVE-2025-31324 shows how high-impact vulnerabilities continue to attract a broad range of threat actors, especially when patching delays persist across enterprise networks.[4]

Top Attack Indicators Identified in H1 2025

[4] https://thehackernews.com/2025/05/china-linked-apts-exploit-sap-cve-2025.html

Top attack indicators are specific pieces of data or observations that strongly point to potential or confirmed malicious activity within a system or network. These can include unusual network traffic patterns, suspicious file executions, unauthorized access attempts, or connection to known malicious IP addresses or domains.

Here are some of the top threat signals that the CyberProof Threat Research Team observed in breaches and attacks in the first half of 2025:

Top 5 Attack Vectors

- Email Attacks
- Fake Captcha
- Vulnerability Exploitations
- Identity based attacks
- Authenticode Stuffing

Top Active Ransomware Groups

- Qilin
- Akira
- SafePay
- INC
- Play

Top 5 Malwares

- LummaStealer
- RedLine
- Amadey
- AgentTesla
- XWorm

Top 5 LOLBINs

- Powershell
- mshta
- Cmd
- Sc.exe
- msiexec

Top 5 RMMs Abused

- ScreenConnect
- PDQDeploy
- AnyDesk
- VNCViewer
- SimpleHelpRMM

Top 5 Tools Used in Attacks

- Impacket
- Advanced IP Scanner
- Psexec
- ADRecon
- NetPass

Top 5 Malicious File extensions

- .exe
- .js
- .mp3/.mp4
- .pdf
- .lnk

Top 5 malicious TLDs (Top Level Domains)

- .top
- .shop
- .ru
- .site
- .icu

Top abused Third-Party Platforms

- WhatsApp
- Telegram
- Discord
- Pastebin
- Transfer.sh

Top MITRE IDs

- T1217
- T1140
- T1562
- T1555.001
- T1219.002

2024 Predictions vs. 2025 Reality

The first half of 2025 has largely validated the core threat predictions outlined in The CyberProof Annual Cyber Threat Intelligence Report: Mapping 2025 Threats & Trends, with several trends in the 2024 summary not only materializing but escalating beyond expectations. While some forecasts have yet to fully take shape, emerging developments suggest they may still be on track. This section examines where our expectations have aligned with current events, where gaps remain, and how the threat landscape is continuing to evolve.

Increased Targeting of Critical Sectors: CONFIRMED

The prediction of intensified targeting of critical sectors has been validated throughout H1 2025. Activity attributed to Chinese APT Salt Typhoon has included a focused campaign against Canadian telecommunications networks, resulting in the compromise of core systems and exfiltration of sensitive data. It follows additional attacks on critical communications and defense infrastructure in the U.S., including intrusions affecting AT&T, Verizon and components of the U.S. Army and National Guard.[5] These attacks compromised sensitive and exposed government communications, demonstrating the predicted focus on sectors where downtime is intolerable and information exposure carries national security implications.

The manufacturing sector bore the brunt of attacks with 75 incidents globally in January 2025 alone, confirming the prediction of precision attacks on operationally dependent sectors.

Adoption of Advanced Ransomware Tactics: CONFIRMED AND EXCEEDED

The prediction of enhanced ransomware tactics has been not only confirmed but exceeded expectations. Multiple threat actors have adopted AI-assisted development, with FunkSec representing a new paradigm of AI-centric ransomware operations. The group uses GenAI to create ransomware code and has implemented sophisticated auction systems through their FunkBID platform.

DragonForce has evolved into a large-scale financial extortion operation, adopting a cartel-style model that enables affiliates to develop their own brands while leveraging shared infrastructure. The core group provides the payloads, infrastructure, and negotiation support, while affiliates retain up to 80% of ransom proceeds—making the model both attractive and highly scalable. The group leverages leaked ransomware builders from established groups including LockBit and Conti, demonstrating the interconnected nature of modern cybercriminal ecosystems.

Enhanced Regulation and Cybersecurity Standards: PARTIALLY CONFIRMED

While there has been visible progress on cybersecurity regulation, particularly around critical infrastructure protection, the anticipated shift in attacker behavior toward smaller, less-protected entities has only been partially observed. While smaller organizations are increasingly targeted, large critical infrastructure

[5] https://www.securityweek.com/chinas-salt-typhoon-hacked-us-national-guard/

operators remain frequent victims of both ransomware and state-aligned operations. At the same time, in the United States, the disbanding of key DHS cybersecurity advisory committees has complicated public-private collaboration, potentially weakening collective response capabilities against major cyber threats.[6] As a result, although regulatory development continues, the broader systemic shifts in both adversary focus and defensive coordination have not fully materialized.

Blurred Lines Between Threat Actor Types: STRONGLY CONFIRMED

The convergence of hacktivists, APTs, and cyber criminals has been dramatically evident in H1 2025. SideCopy, a Pakistani linked APT has expanded beyond traditional espionage to incorporate hacktivist elements, mimicking government personnel while targeting Indian government sectors including railway, oil & gas, and external affairs ministries. The group demonstrates hybrid motivations combining state-sponsored espionage with broader political messaging.

Also, North Korean hackers associated with Moonstone Sleet have begun deploying Qilin ransomware, marking a shift from custom-built software to utilizing Ransomware-as-a-Service models. This demonstrates nation-states leveraging cybercriminal infrastructure for their operations.[7]

Supply Chain Trust Erosion: CONFIRMED

The prediction of supply chain vulnerabilities has been validated through multiple campaigns. Silk Typhoon has shifted focus to IT service providers, using their privileged access to infiltrate downstream customers and abuse trusted relationships within the ecosystem. Simultaneously, British retailers have faced a wave of sophisticated intrusions, where attackers leveraged federated identity systems, remote management platforms, and inadequate internal segmentation to bypass defenses. At Marks & Spencer, access was likely gained through a compromised third-party service deeply integrated into internal infrastructure.

These incidents go beyond operational disruption—they undermine confidence in the integrity of interconnected systems, accelerating the erosion of trust at the core of modern digital business.

What to Expect in H2 2025

Building on the trends and incidents observed in the first half of the year, the following points outline how the threat landscape is likely to evolve in H2 2025.

- **AI-Driven Threat Operations Will Mature:** The adoption of generative AI in cybercrime is expected to accelerate, with threat actors refining their use of AI for malware development, evasion techniques, and social engineering. The early examples seen in H1 suggest that more groups will follow, adopting AI to lower technical barriers and increase attack scale and speed.
- **Critical Infrastructure Will Remain a Prime Target:** The Salt Typhoon and Silk Typhoon campaigns demonstrated a strategic interest in communications and IT infrastructure. As defensive efforts strengthen at top-tier providers, threat actors may pivot toward regional or second-tier infrastructure—where visibility and protection are often weaker, but the operational impact remains high.
- **Supply Chain Targeting Will Deepen:** H1 saw a shift in Chinese APT activity toward exploiting IT service providers and privileged access platforms. In H2, we expect to see more intricate supply chain attacks that exploit third-party integrations, cloud ecosystems, and managed service relationships to move laterally across trusted networks.
- **Threat Actor Collaboration and Consolidation:** Hybrid models seen in groups like DragonForce point to a broader trend of collaboration between politically and financially motivated actors. This will likely drive the emergence of more structured affiliate programs and shared toolsets that blur the line between ideologically driven and profit-focused campaigns.

[6] https://www.axios.com/2025/03/18/dhs-cisa-cyber-council-industry-trust
[7] https://securityaffairs.com/175178/apt/north-korea-linked-apt-moonstone-used-qilin-ransomware.html

- **Regulatory and Public-Private Shifts:** Following high-profile incidents involving telecoms and the supply chain, H2 may bring regulatory tightening, especially in sectors deemed critical. At the same time, structural changes in how governments coordinate with private entities could reshape how threat intelligence is shared and acted upon.
- **Geographic Rebalancing of Threat Activity:** As Western organizations enhance their cyber defenses, threat actors may increasingly shift focus to underregulated or undersecured regions, such as Latin America and parts of Southeast Asia, seeking softer entry points for monetization and espionage.

Conclusion

The first half of 2025 has shown how quickly the cyber threat landscape is changing. Attackers are using new tools—like AI and advanced phishing kits—and are focusing more on critical infrastructure and trusted third-party services. Ransomware groups are becoming more organized, and several incidents showed how political motives and financial gain are starting to overlap. From telecom providers to retailers, no sector has been off-limits.

In the second half of the year, we expect many of these trends to continue. Threat actors are likely to go after less protected targets, especially in regions with weaker oversight or defenses. Organizations will need to adapt quickly—both to new attacker techniques and to evolving regulations. Staying ahead will require more than just better tools—it will take faster detection, better internal coordination, and closer cooperation between public and private sectors.

About CyberProof

CyberProof delivers threat-led, co-managed security operations with the belief that better security is achieved through the right partnerships, technology and client experiences. Our threat-led, cloud-first, and AI-powered approach to security, delivers industry-leading security services which drives real and measurable business outcomes. We believe that working closely with our clients and partners through a better security, together model, jointly empowers us to defend against the greatest threats.

To learn more visit, www.cyberproof.com.

CyberProof® A UST Company | Better Security, Together.