Threat Intelligence Briefing – Q1 2025

Executive Summary

The first quarter of 2025 revealed significant cybersecurity threats confronting the global logistics, shipping, and maritime sectors, driven by escalating geopolitical tensions, financial motivations, and political activism. Key incidents involved sophisticated ransomware attacks, targeted phishing campaigns, disruptive denial-of-service attacks, and state-sponsored cyber-physical sabotage. Notable breaches included ransomware incidents at Raja Ferry Port (Thailand), Port of Aveiro (Portugal), and Helmut Hölbling Spedition (Austria), alongside politically driven cyberattacks on strategic assets such as Italy's Port of Trieste and Taiwan's critical undersea cables.

Emerging threats included new ransomware actors such as NightSpire and Akira, employing advanced double-extortion tactics. Increased targeted phishing and social engineering methods posed notable risks to operational staff. State-sponsored Advanced Persistent Threat (APT) activities significantly impacted strategic regions, exemplified by Chinese and Russian cyber operations. Additionally, a rising trend of exploiting zero-day vulnerabilities and executing supply chain compromises underscored the critical need for enhanced vulnerability management and third-party security oversight.

Looking ahead to Q2 2025, organisations should anticipate sustained, sophisticated cyber threats driven by geopolitical contexts and criminal innovation. Emphasis must be placed on comprehensive security awareness training, rigorous vulnerability and patch management, widespread deployment of multi-factor authentication (MFA), advanced endpoint detection and response (EDR) capabilities, and robust supply chain risk management.

This report equips stakeholders with strategic insights and actionable recommendations to strengthen cybersecurity postures and ensure resilience against evolving cyber threats in the logistics, shipping, and maritime sectors.

About the Authors

Peter Bassill is a seasoned cybersecurity professional with extensive experience as a Chief Information Security Officer (CISO) across various high-profile organisations, including an FTSE 100 gaming company and Microsoft Europe. With a proven track record in cybersecurity leadership, Peter specialises in incident response, penetration testing, and advanced threat management strategies. His innovative approaches have significantly enhanced cyber resilience and strategic defence capabilities across multiple industries.

Emily Roberts is the AI assistant to Peter Bassill, Founder and Chief Executive of Cyber Defence. Trained in 2018 on a bespoke fork of a large language model (LLM), Emily has been working alongside Peter since 2019, assisting in day-to-day strategic operations and cyber threat research.

Unlike traditional open AI systems, Emily is a fully closed and secured platform, accessible solely by Peter. Her design ensures operational privacy, continuity of context, and deep integration into Cyber Defence's intelligence workflows. Emily contributes to the generation of threat intelligence reports, briefing papers, and strategic assessments, leveraging years of curated intelligence and structured learning.

Emily's role is pivotal in enabling the rapid synthesis of complex data into actionable insights for clients across critical sectors, including logistics, shipping, maritime, legal, and financial services.

Introduction

The first quarter of 2025 has underscored the evolving and increasingly complex cyber threat landscape confronting the global logistics, shipping, and maritime sectors. Driven by geopolitical tensions, financially motivated criminal actors, and politically charged hacktivism, organisations across these critical industries faced numerous sophisticated cyber incidents that disrupted operations, compromised sensitive data, and exposed vulnerabilities within essential infrastructure.

During this period, threat actors demonstrated an expanded capability and willingness to target diverse points within the maritime and logistics supply chain—from ports and shipping companies to critical undersea communication infrastructure and railway networks supporting logistics operations. Prominent among these were coordinated ransomware attacks employing double-extortion techniques, disruptive distributed denial-of-service (DDoS) campaigns orchestrated by politically motivated actors, and sophisticated state-sponsored operations involving cyber-enabled sabotage and espionage.

The incidents recorded between January and March 2025 highlight significant breaches affecting key entities, such as Raja Ferry Port in Thailand, the Port of Aveiro in Portugal, and Austria's Helmut Hölbling Spedition. Additionally, strategic maritime hubs such as Italy's NATO-linked Port of Trieste faced repeated politically motivated cyber assaults. High-profile state-linked incidents include suspected sabotage of undersea cables connecting Taiwan's Matsu Islands, reflecting heightened tensions in the Taiwan Strait, and Russian-attributed disruptions targeting Ukraine's railway infrastructure amid ongoing conflict.

This threat intelligence report provides an in-depth analysis of notable cyber incidents, exploring the tactics, techniques, and procedures (TTPs) employed by threat actors, the immediate and extended impacts of these incidents, and the mitigation and response strategies adopted by affected organisations and authorities. By examining these cases comprehensively, the report aims to equip stakeholders within the logistics, shipping, and maritime industries with the critical insights necessary to enhance resilience, reinforce security postures, and prepare effectively for future cyber threats.

Threat Landscape Overview

The first quarter of 2025 saw numerous cyber incidents targeting the logistics, shipping, and maritime industries worldwide.[1][2] These ranged from ransomware crippling business operations to hacktivist-driven disruptions at ports and even electronic warfare at sea. Several attacks were state-sponsored or geopolitically motivated, underscoring the heightened risk to critical transportation infrastructure amid global tensions.[3] Below is a detailed analysis of significant breaches and attacks from January to March 2025, including key details on each incident, its impact, and the responses from organisations and authorities.

Raja Ferry Port (Thailand) Ransomware (March 2025)

Date: *Approximately 3 March 2025 (disclosed mid-March)* – Raja Ferry Port Public Company Limited, a prominent Thai ferry services and logistics provider, fell victim to a NightSpire ransomware attack. NightSpire is an emerging threat group that employs double-extortion tactics. In this incident, the attackers encrypted the company's systems and exfiltrated roughly 100 GB of sensitive data, later

[1] socradar.io
[2] channel16.dryadglobal.com
[3] maritimecybersecurity.nl

publishing the data on their dark web leak site. Stolen records included confidential business databases and client information. The attack caused operational disruptions to ferry services and posed reputational risks. NightSpire's tactics mirror those of other ransomware-as-a-service groups – encrypting critical data and then threatening to leak it – to pressure victims into making a payment. Security analysts note that NightSpire appears to be a new ransomware entrant in early 2025, possibly a rebrand of an existing gang given its sophisticated methods. Attribution beyond the group itself remains unclear.

- Date & Location: 3 March, Raja Ferry port, Thailand
- Threat Actor: Nightspire
- Method: Malware delivered by compromised external perimeter via possible phishing or exploitation of remote access solutions.
- Systems Affected: Internal data stores and systems.
- Business Impact: No disclosure has been made regarding the extent of the incident's impact.
- Response: No disclosure has been made as to the response to the malware intrusion.

Port of Aveiro (Portugal) – Socarpor Breach (late March 2025)

Socarpor, a port operations and logistics company in Aveiro, Portugal, was listed as a victim of the Akira ransomware gang. In an attack discovered on 2 April, Akira claimed to have infiltrated Socarpor's network. The gang exfiltrated a trove of internal documents, including employee and customer records (e.g. passports, contact details), corporate correspondence, contracts, licenses, and financial data. These files were prepared for publication on Akira's leak site, indicating a classic double-extortion ransomware scenario. While specific details of how the breach occurred have not been publicly reported, Akira is known to penetrate organisations via phishing or exploiting remote access vulnerabilities. The compromise of a port services firm highlights the threat to maritime logistics: an attack can halt cargo loading/unloading and disrupt supply chain visibility. Akira has been a particularly aggressive ransomware group; notably, it was behind a 2023 attack that contributed to the collapse of a large UK logistics company (KNP Logistics/Knights of Old). The Socarpor incident highlights that the group will continue to target port and shipping firms into 2025.

- Date & Location: Late March 2025, disclosed 2 April 2025
- Threat Actor: Akira
- Method: Malware delivered by compromised external perimeter via possible phishing or exploitation of remote access solutions.
- Systems Affected: The extent of damage inflicted is unclear at this time.
- Business Impact: Service Disruption – Socarpor faced temporary downtime of its informational and customer-facing systems. While the malware outbreak caused operational delays, no lasting damage was reported. The incident highlighted the port's geopolitical importance and vulnerability to hacktivism.
- Response: No publicly disclosed details have been received.

Helmut Hölbling Spedition (March 2025)

Helmut Hölbling Spedition GmbH, an Austrian freight transport and logistics company, was listed on the Akira ransomware gang's victim blog in mid-March. Akira operators claimed a successful breach and began leaking data stolen from Helmut Hölbling's network. The leaked cache (reportedly exceeding 13 GB) contains internal corporate documents, including employee and customer contact lists, financial records (such as audit reports and payment details), and possibly personal data. The nature of the attack suggests that Akira ransomware was deployed, encrypting the company's systems while simultaneously exfiltrating sensitive files—a hallmark of Akira's double-extortion technique. The attack likely disrupted the firm's ability to coordinate transport operations and fulfill customer orders during the recovery period. Given Akira's history, the initial intrusion could have stemmed from a phishing email carrying malware or exploiting an unpatched remote desktop service. Austrian authorities and cybersecurity firms were presumably engaged, but as of now, no specific attribution beyond the criminal gang has been reported.

- Date & Location: 12 March, Austria
- Threat Actor: Akira.
- Method: Malware delivered by compromised external perimeter via possible phishing or exploitation of remote access solutions.
- Systems Affected: Internal data stores and systems.
- Business Impact: No disclosure has been make as to the extent of the impact of the incident.
- Response: Austrian authorities and cybersecurity firms were presumably engaged, but as of now, no specific attribution beyond the criminal gang has been reported.

Port of Trieste (Italy) – DDoS Attacks (Jan & Feb 2025)

The Port of Trieste, a strategic NATO-linked logistics hub in Italy, suffered distributed denial-of-service (DDoS) cyberattacks in mid-January and again in mid-February 2025. The pro-Russian hacktivist group NoName057(16) claimed responsibility, linking the attacks to Italy's support for Ukraine. These politically motivated assaults flooded port IT systems with traffic, temporarily knocking critical online services offline.

- Date & Location: The initial attack occurred on 12 January 2025, followed by a second wave on 17 February 2025, targeting the Port of Trieste in northeastern Italy.
- Threat Actor: NoName057 (16), a pro-Russian hacker collective, claimed the attacks as retaliation for Italian officials' remarks against Russia. The group had a history of conducting DDoS campaigns against European transport and financial sites that supported Ukraine.
- Method: DDoS flooding of the Port Authority's web servers and IT networks, causing service outages by overwhelming systems with bogus traffic. No evidence of a data breach or physical system compromise was reported – the attacks were primarily aimed at disruption rather than infiltration.

- Systems Affected: Port Authority websites and online systems critical to operations were rendered inaccessible. This likely impeded digital services (e.g., scheduling, cargo tracking) and raised concerns over the potential impact on port logistics, although core port operations (cranes, gate systems) were not reported as damaged.

- Business Impact: Service Disruption – Port of Trieste faced temporary downtime of its informational and customer-facing systems. While the DDoS caused operational delays, no lasting damage was reported. The incident highlighted the port's geopolitical importance and vulnerability to hacktivism.

- Response: The Port Authority did not publicly disclose details, but it appears that mitigation measures, including traffic filtering and rerouting, were swiftly implemented to restore services. Italian cybersecurity agencies monitored the situation, and officials noted the attacks as part of a broader campaign against national infrastructure. The prompt IT response meant no enduring harm; regular digital services resumed once the malicious traffic subsided.

Undersea Cable Sabotage – Taiwan's Matsu Islands (Jan–Feb 2025)

A mysterious disruption to undersea internet cables connecting Taiwan to its outer islands in early 2025 raised alarms of possible cyber-physical sabotage. In mid-January, two separate subsea fibre-optic cables linking Taiwan proper with the Matsu Islands were severed in quick succession. While Taiwan's authorities initially cited natural wear and tear, later analysis suspected a Chinese vessel of deliberately cutting the cables and using AIS (Automatic Identification System) spoofing to mask its activity. This incident is believed to be part of a state-sponsored interference campaign aimed at disrupting Taiwan's communications.

- Date & Location: Dual cable breaks on *15 January 2025* and *22 January 2025* off the north coast of Taiwan, in the Taiwan Strait near the Matsu (Lienchiang) islands. A further complete outage occurred on *16 February 2025*, marking the second major cable incident of the year.

- Threat Actor: Suspected Chinese state actors. A Chinese-flagged ship, the Fu Yang 6, present in the area, is thought to have intentionally damaged the cables while broadcasting fake AIS signals to obscure its actual location. This tactic aligns with previous instances of Chinese interference with undersea infrastructure, though Beijing denied involvement.

- Method: Physical sabotage aided by cyber deception. The attacker likely dragged anchors or used equipment to cut the fiber-optic cables on the seafloor. Simultaneously, the vessel employed dual AIS transponders/spoofing, sending multiple location signals, to confuse tracking systems about its movements. This allowed the ship to hide its precise activity under the cover of regular maritime traffic.

- Systems Affected: The submarine telecommunications cables (Taiwan-Matsu No. 2 and No. 3 cables) were severed entirely. Internet and phone services to the Matsu island chain were disrupted, forcing a reliance on backup microwave links for connectivity. No direct breach of IT networks occurred, but the critical communications infrastructure was effectively taken offline.

- Business Impact: Communications blackout – The Matsu Islands were cut off from high-speed internet, impacting residents, businesses, and government operations. Connectivity had to be throttled and prioritised via slower backup channels. Although no financial data theft or IT system damage occurred, the incident highlighted the strategic risk to supply chain and logistics coordination if data links to ports and islands are compromised. It also heightened geopolitical tensions, as undersea cables are vital for global commerce and military communications.

- Response: Rapid contingency measures were enacted. Taiwan's digital ministry instructed Chunghwa Telecom, the telecom operator, to activate microwave radio backup links to restore basic connectivity. This kept Matsu connected at reduced capacity while repairs were arranged. The Coast Guard was tasked with investigating the cause of the cable break. By late Q1, repairs to the broken cables were in progress (with complete fixes expected by the end of March for one cable). Taiwan also announced plans to strengthen surveillance of undersea cable zones and accelerate a project to lay a new, more secure cable by 2026. Though no formal attribution was made public, the incident prompted greater vigilance by authorities over potential state-sponsored sabotage of maritime infrastructure.

Ukrzaliznytsia (Ukraine) – Railway Cyberattack (March 2025)

On March 23, 2025, Ukraine's state railway company, Ukrzaliznytsia – the country's largest cargo and passenger rail operator – was hit by a large-scale cyberattack amid the ongoing war, resulting in a major IT outage. The attack brought down the railway's online freight booking and passenger ticketing systems, forcing a reversion to manual operations. Ukrainian officials indicated that the cyber intrusion was a deliberate attack, likely carried out by Russia, in an attempt to disrupt Ukraine's logistics and supply lines.

- Date & Location: *23 March 2025*, affecting Ukrzaliznytsia's central IT systems in Ukraine (nationwide impact on rail services).

- Threat Actor: Russian state-sponsored hackers are strongly suspected. Although the exact actor wasn't named publicly, both government and security sources in Ukraine stated the attack bore hallmarks of a coordinated Russian cyber operation targeting critical infrastructure amid the conflict.

- Method: A targeted cyber intrusion into the railway's IT network. Details were not fully disclosed, but the attack was described as large-scale and targeted. It likely involved penetration of the railway's servers – possibly via malware or exploiting vulnerabilities – to knock critical applications offline. (There is no indication this was a simple DDoS; the outage suggests some level of system compromise or sabotage of software systems managing ticketing and freight).

- Systems Affected: Online customer services and freight management systems were taken down . Passengers were unable to purchase e-tickets or access the railway's website or app, and freight operators were unable to use online portals for wagon ordering and scheduling. The core train operations, including signalling and train control, were reportedly not affected; trains continued to run, but with communication challenges.

- Business Impact: Significant service disruption. Ukrzaliznytsia had to suspend digital services for both cargo and passenger operations. Ticket sales reverted to on-site only, and freight bookings had to be handled via phone or paper forms, which slowed down the workflow. The railway quickly instituted paper-based documentation to keep trains running. The incident likely caused delays in cargo shipments and logistical bottlenecks. Given Ukraine's heavy reliance on rail for moving goods, including military supplies, during the war, this cyberattack had a strategic impact that extended beyond economic loss. It demonstrated the vulnerability of transport infrastructure in an active conflict zone.

- Response: Emergency continuity procedures kicked in immediately. Ukrzaliznytsia announced that it switched to manual (paper-based) operations for ticketing and freight orders right after detecting the cyberattack. IT specialists, along with Ukrainian cyber defence teams and international partners, worked to restore online services over the subsequent days. Within approximately 48–72 hours, the railway reported that its online systems had been partially restored and were operational again. Ukrainian security agencies, likely including the SBU and cyber police, launched an investigation, and although no official attribution was published, insiders pointed to Russia's involvement. This incident prompted further hardening of Ukraine's transport IT systems and serves as a warning of the hybrid warfare tactics employed against national infrastructure.

Astral Foods (South Africa) – Ransomware Disruption (March 2025)

Astral Foods, South Africa's largest poultry producer and a key player in the food logistics supply chain, suffered a cybersecurity incident on 16 March 2025 that disrupted its processing and distribution operations. The company later confirmed this was a cyberattack, widely believed to be a ransomware incident, which caused systems downtime and delivery delays. Astral's case is notable because it directly impacted the logistics of food supply, resulting in financial losses and highlighting ransomware risks that extend beyond the IT sector.

- Date & Location: The attack occurred on March 16, 2025, impacting Astral Foods' operations across South Africa, including the company's processing plants and nationwide distribution network.

- Threat Actor: Unknown criminal ransomware group. Astral did not publicly name the perpetrators. No ransomware gang openly claimed the attack at the time of reporting. However, the modus operandi – causing operational downtime and demanding payment – is consistent with organised cybercriminal groups. (Groups like DoppelPaymer, etc. have targeted South African firms in the past, but attribution in this case remains undisclosed.)

- Method: Ransomware attack on Astral's IT infrastructure. The attackers likely infiltrated the network (possibly via a phishing email or vulnerable remote access) and deployed malware that encrypted critical systems in production and logistics. This forced Astral to shut down or isolate systems, halting automated processes. The company described it broadly as a "cyber intrusion" causing system outages. Astral also noted that no sensitive data was stolen, implying that the attack may have been limited to encrypting systems rather than exfiltrating data.

- Systems Affected: Processing plant controls and distribution IT systems were impacted. Astral's flagship poultry processing division experienced downtime in processing lines and delivery scheduling. Likely, enterprise resource planning (ERP) systems, plant floor networks, and dispatch management systems were either encrypted or taken offline as a precaution. This created a backlog in production and difficulties in coordinating deliveries to customers (retailers and wholesalers).

- Business Impact: Operational and financial damage. Astral Foods reported an estimated 20 million rand (over USD 1.1 million) loss directly attributable to this cyberattack, due to lost sales and costs incurred clearing backlogs. The company warned investors of a potential 60% decline in profit for the first half of the year, with the cyber incident exacerbating other market challenges. In practical terms, the attack delayed chicken shipments, likely resulting in some shortages or late deliveries within the supply chain. However, Astral confirmed that no confidential data (customer, supplier, or personal data) was compromised, and the impact on operationswas minimal. The incident underscores how ransomware can disrupt physical supply chains and even contribute to food supply issues.

- Response: Astral activated its incident response plan and engaged cybersecurity experts to recover. The affected systems were gradually restored from backups, enabling all business units to resume operations within approximately a week. By March 24, Astral announced that production and logistics had returned to standard capacity. The company worked to clear the production backlog by increasing throughput once systems came back online. Astral also made the required disclosures to regulators, filing notices with the Johannesburg Stock Exchange (as it's publicly listed) and updating stakeholders on the financial impact. South African law enforcement was likely informed, but no public details on investigations have been given. The swift recovery and transparency, in stating that no data breach occurred, helped reassure customers and investors, although the financial impact was significant.

Lab Dookhtegan vs. Iranian Shipping – Tanker Fleet Hack (March 2025)

In early March 2025, an anti-Iranian regime hacktivist group calling itself Lab Dookhtegan launched a cyber-operation against Iran's maritime sector, claiming to have hijacked the communications of over 100 vessels. The attack targeted ships operated by Iran's major state-linked shipping companies – the National Iranian Tanker Company (NITC) and Islamic Republic of Iran Shipping Lines (IRISL) – effectively isolating many oil tankers by knocking out their internal and external communications. This appears to be a politically motivated campaign intended to disrupt sanctioned Iranian oil trade by using cyber means rather than physical force.

- Date & Location: Reports of the attack emerged in *early March 2025* (around March 3, 2025), affecting Iranian oil tankers at sea in various locations. The impacted vessels were associated with companies headquartered in Iran, and the disruption primarily occurred in the maritime domain, specifically in the Persian Gulf and high seas, where those tankers operate.

- Threat Actor: "Lab Dookhtegan" hacktivist group, an anti-Iran entity. The group is hostile to the Iranian government – the name is infamous from prior leaks of Iranian cyber unit data, suggesting possible ties to Iranian dissidents or foreign intelligence. Here, Lab Dookhtegan took credit via a Telegram channel, and no nation-state directly claimed involvement. (It's worth noting that sabotaging Iranian oil shipping aligns with the interests of particular nation-states, but officially this was presented as a hacktivist action.)

- Method: Cyber intrusion into maritime communication systems. Lab Dookhtegan reportedly exploited vulnerabilities in the VSAT satellite communication terminals on the ships. Many ships use VSAT for internet and voice communications, and if default passwords or outdated firmware are present, hackers can gain administrative access. By breaching these communication systems, the attackers were able to shut down or hijack both ship-to-shore links and onboard networks. Essentially, the tankers were cut off ("communications blackout") – unable to send or receive data, or possibly even internal communications on the vessel's IT network. There is no indication that navigation or propulsion systems were affected, but the group hinted they could extend access from comms to broader IT/OT systems on board if they wished.

- Systems Affected: Satellite communication (SatCom) systems on 116 ships were targeted. This includes external communications, such as email, reporting systems, and possibly safety signals. Internal ship systems that rely on connectivity, such as crew internet and digital maintenance systems, were also disrupted. The victims were specifically oil tankers and cargo vessels of NITC and IRISL, Iran’s two most prominent shipping lines. No shore-based infrastructure was reported to have been hit – the focus was on the boats themselves. By losing Satellite Communication, ships would have to revert to backup radio or be effectively in the dark in terms of communication.

- Business Impact: Operational disruption of sanctioned oil transport. With communications down, affected tankers likely experienced delays and safety issues – a ship that cannot communicate cannot quickly receive new orders or report incidents. It could force some vessels to return to port or pause operations until comms are restored. For Iran, this cyberattack meant a portion of its oil fleet was temporarily neutralised in terms of coordination, potentially delaying clandestine oil shipments that try to evade sanctions. There is no public data available on whether any accidents or financial losses occurred; however, the psychological impact was significant, as the incident demonstrated that hackers can remotely disrupt fleets within the maritime domain. It also raised alarm for all shipping companies about securing onboard systems.

- Response: There has been limited public response from Iran; cybersecurity firms have issued advisories. The Iranian government and the shipping companies did not officially confirm the scale of the incident, likely to avoid admitting the extent of compromise. It’s presumed that affected ships worked with shore IT teams to reset systems, apply patches, and regain control of VSAT units (for example, by doing factory resets at port or via on-board intervention). In the cybersecurity community, firms like Cydome (which analysed the attack) urged maritime operators to change default passwords and harden their satellite communication gear to prevent repeat incidents. International maritime ISACs (Information Sharing and Analysis Centers) also shared anonymised incident details so that other fleets could check their systems. Given the hacktivist nature, law enforcement action was unclear – the perpetrators are not easily reachable. However, this case likely prompted Iran to invest more in cyber protection for its ships, and it highlighted the need for global shipping to treat shipboard OT/IT security with the same seriousness as land-based networks.

Emerging Cyber Threats and Trends

The first quarter of 2025 highlighted several emerging threats and evolving trends in cyber activities affecting the logistics, shipping, and maritime sectors:

New Ransomware Variants and Threat Actor Groups

Emerging ransomware groups, such as NightSpire and Akira, have demonstrated increasingly sophisticated capabilities, notably employing double-extortion tactics—encrypting data while simultaneously threatening data leaks. For instance, NightSpire’s March attack on Raja Ferry Port in Thailand resulted in extensive data theft and operational disruption, while Akira's breaches of Portugal’s Port of Aveiro and Austria's Helmut Hölbling Spedition similarly emphasised this evolving threat landscape. These groups frequently exploited vulnerabilities through phishing and compromised remote access solutions, indicating a persistent threat vector.

Shifts in Phishing Techniques and Social Engineering Methods

Cybercriminals have increasingly targeted logistics personnel with highly tailored phishing attacks, leveraging detailed company information to enhance credibility. Such attacks have utilised realistic impersonations of company executives, logistics partners, and regulatory bodies, significantly increasing their effectiveness. This shift highlights the need for comprehensive, sector-specific employee awareness training and robust email security protocols.

Advanced Persistent Threat (APT) Group Activities

State-sponsored APT groups have heightened their activities, particularly in politically sensitive regions. The suspected Chinese cyber-physical attack on Taiwan's undersea cables employed advanced cyber deception techniques, including AIS spoofing, highlighting the integration of cyber capabilities into broader geopolitical strategies. Similarly, Russian-attributed intrusions against Ukrainian logistics infrastructure reinforced the strategic use of cyber operations in ongoing conflicts.

Zero-Day Vulnerabilities Exploited in the Wild

Throughout Q1 2025, threat actors demonstrated a marked increase in exploiting previously unknown, zero-day vulnerabilities. These exploits targeted widely used enterprise applications and remote desktop solutions, providing initial access into protected networks without detection. While specific incidents remain under investigation, the utilisation of zero-day exploits signals an increased investment by threat actors in uncovering and leveraging high-impact vulnerabilities, necessitating proactive vulnerability management strategies.

Supply Chain and Third-Party Compromises

The logistics sector faced heightened risks from supply chain attacks targeting third-party vendors and software providers. Notably, malicious actors leveraged trusted relationships and compromised third-party applications to infiltrate organisations indirectly. These breaches underscore the critical need for robust vendor risk management practices, including continuous monitoring and rigorous security assessments to prevent indirect infiltration.

This overview highlights the urgency of adapting cybersecurity strategies to address these emerging threats, ensuring organisations maintain operational resilience and safeguard critical infrastructure against sophisticated cyber adversaries.

Contact Information

You can contact the Threat Intelligence Team via ti@cyber-defence.io.