CYBLE®

TRANSPORT AND LOGISTICS

THREAT LANDSCAPE REPORT 2025

TABLE OF CONTENT

Executive Summary

The transport and logistics industry plays a pivotal role as the foundation of global commerce. It is the lifeblood of international trade, serving as the essential conduit for the movement of goods and services, enabling the seamless flow of products across borders and driving economic activity. Moreover, in the days of global conflict, it also acts as an extremely critical source for not only providing relief goods in areas most impacted but also helps in evacuation and keeping the supply chains running.

As the world becomes increasingly interconnected, the efficiency and reliability of these transport networks are more crucial than ever, underpinning the growth andstability of the global economy.

Ransomware groups, notably CL0P and Qilin, were responsible for the majority of attacks, disrupting operations for major airlines, maritime shipping, and ground logistics providers through both widespread vulnerability exploitation and sustained pressure.

Concurrently, a highly fragmented market for initial access brokers and data leaks thrived, fueled by a long tail of opportunistic actors selling compromised credentials and exfiltrated databases.

High-profile incidents demonstrate the severe impact of these threats, including a destructive attack crippling a major Russian airline, a data breach exposing the personal information of six million Qantas customers, and the complete operational collapse of a UK logistics firm following a ransomware attack that exploited a weak password. Emerging tactics also include cyber-enabled cargo theft using RMM tools and sophisticated SMS phishing campaigns.

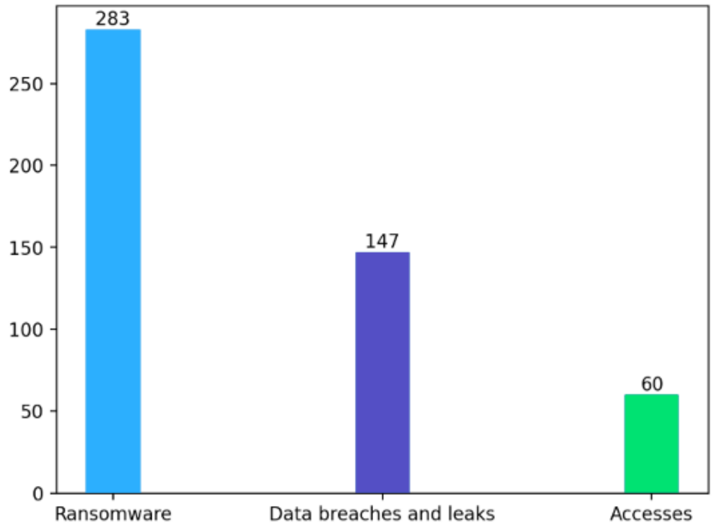


Fig 1: Cybercrime Incidents Impacting Transport and Logistics Sectors

Ransomware Attacks

In 2025, CRIL observed 283 ransomware attack victims (with five remaining unidentified) in the transport and logistics sector, indicating a significant and sustained threat level against this critical infrastructure.

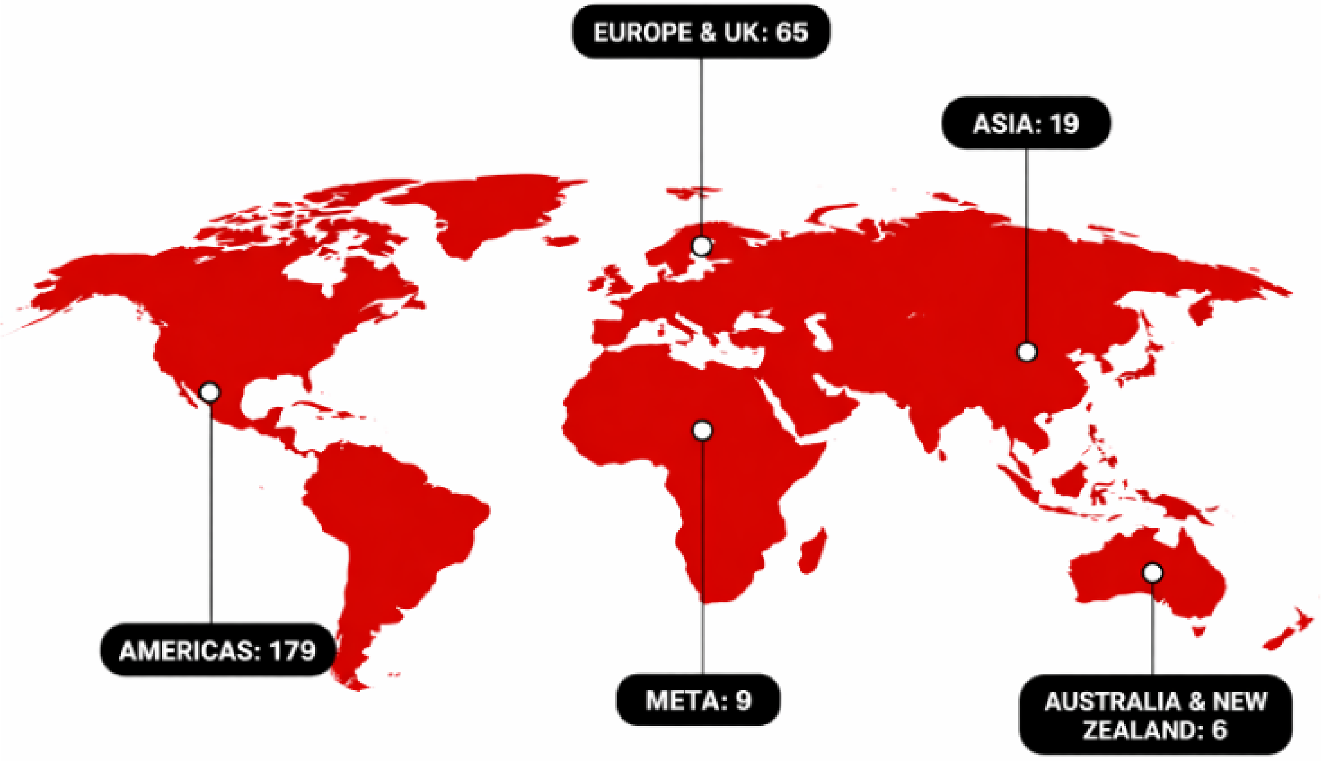


Fig 2: Worldwide Geographic Concentration of Reported Ransomware Incidents

In fact, the ransomware attack numbers this year for the transport and logistics sector are more than the cumulative of the last two years which saw 120 attacks in 2023 and 122 in 2024.

The numbers are alarming to say the least. The consistent volume of incidents throughout the year highlights the sector's appeal to cybercriminals, who leverage operational disruptions for financial gain. This analysis details the most prolific ransomware groups, their targets, and the overarching trends that defined the threat landscape for the sector.

Dominant Groups

The ransomware landscape was heavily concentrated, with a few groups responsible for majority of the incidents. The top four most active groups—CL0P, Qilin, Akira, and Play—were responsible for 160 attacks, representing approximately 57% of all activity observed.

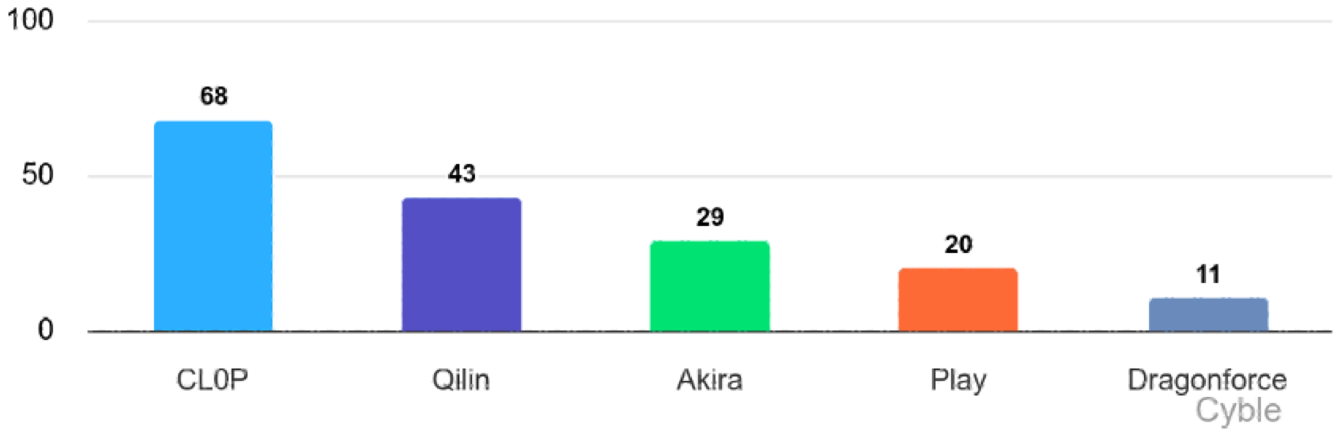


Fig 3: Top Ransomware Actors Targeting the Transport and Logistics Sector

CL0P was exceptionally prolific, launching 68 attacks, or 24% of the total, or one in every four attacks, making it the single most significant threat actor for the sector. Following CL0P, the Qilin group was responsible for 43 attacks (15%), while Akira and Play claimed 29 (10%) and 20 (7%) victims, respectively.

This concentration demonstrates that a limited number of sophisticated Ransomware-as-a-Service (RaaS) operations pose the primary threat to organizations in this industry.

Impact Analysis

The attacks impacted a wide spectrum of sub-sectors within transport and logistics, disrupting operations from global supply chains to local transit. Victims included major airlines, maritime entities, and crucial ground logistics providers like Mainfreight. The data also reveals attacks on specialized services, including cold storage facilities, freight forwarders, and warehousing companies.

When it comes to industry-wide distribution, logistics and freight services were the most targeted businesses by ransomware actors while the trucking, air and railroad were equally targeted through 2025 and took the joint second rank on the list.

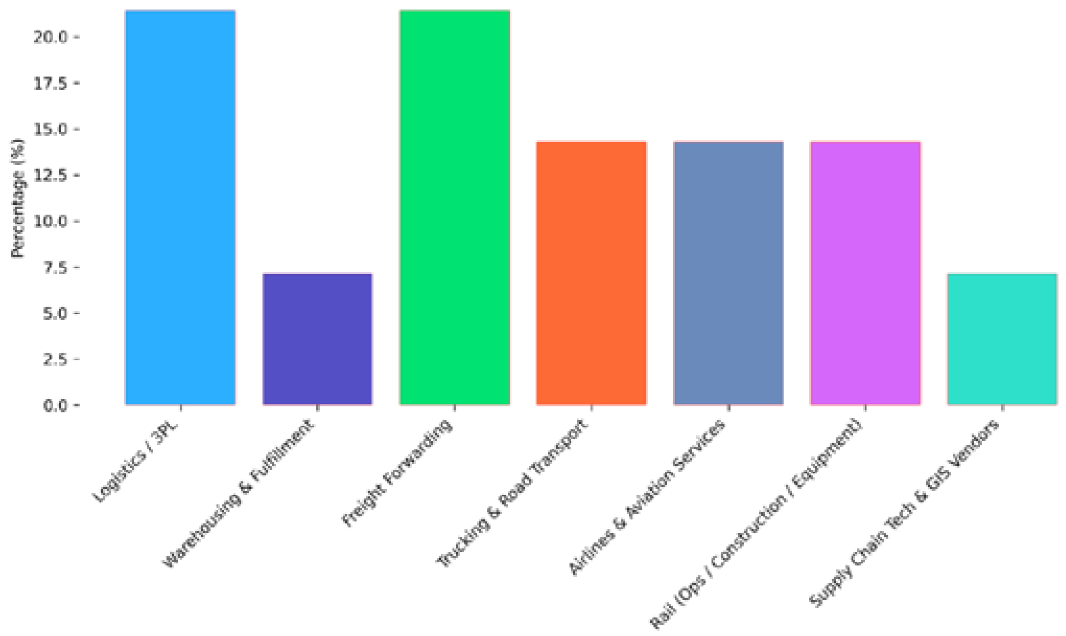


Fig 4: Industry Distribution of Reported Ransomware Incidents

Further analysis of this data from the ransomware victims in the transport and logistics sector indicated that land operations were the primary target with nearly 3 in every 4 attacks targeted at it across the three major sectoral categories – Land, Sea, and Air.

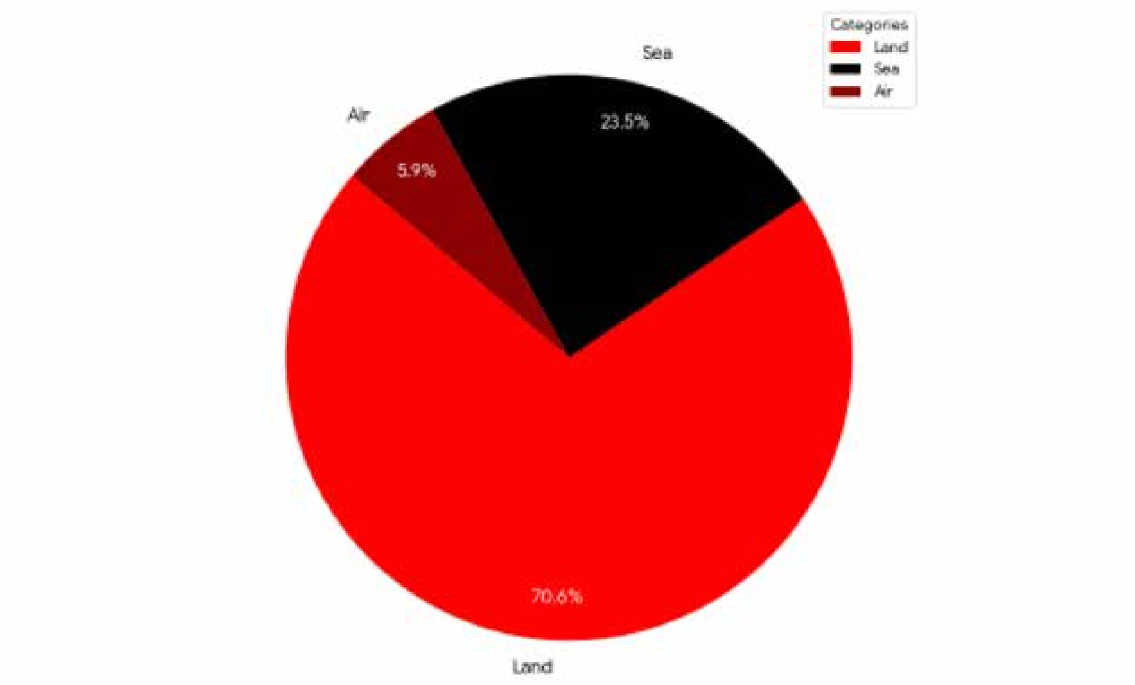


Fig 5: Distribution of Reported Ransomware Incidents Across Land, Sea and Air

Furthermore, public transit authorities, such as Ohio Transportation Company were also targeted, showing the direct risk to public services and infrastructure.

Notable Incidents/Trends

A significant trend observed was the campaign-style approach of the CL0P group. The data reveals concentrated bursts of activity, with dozens of organizations listed as victims on the same day, particularly on January 15 and February 24.

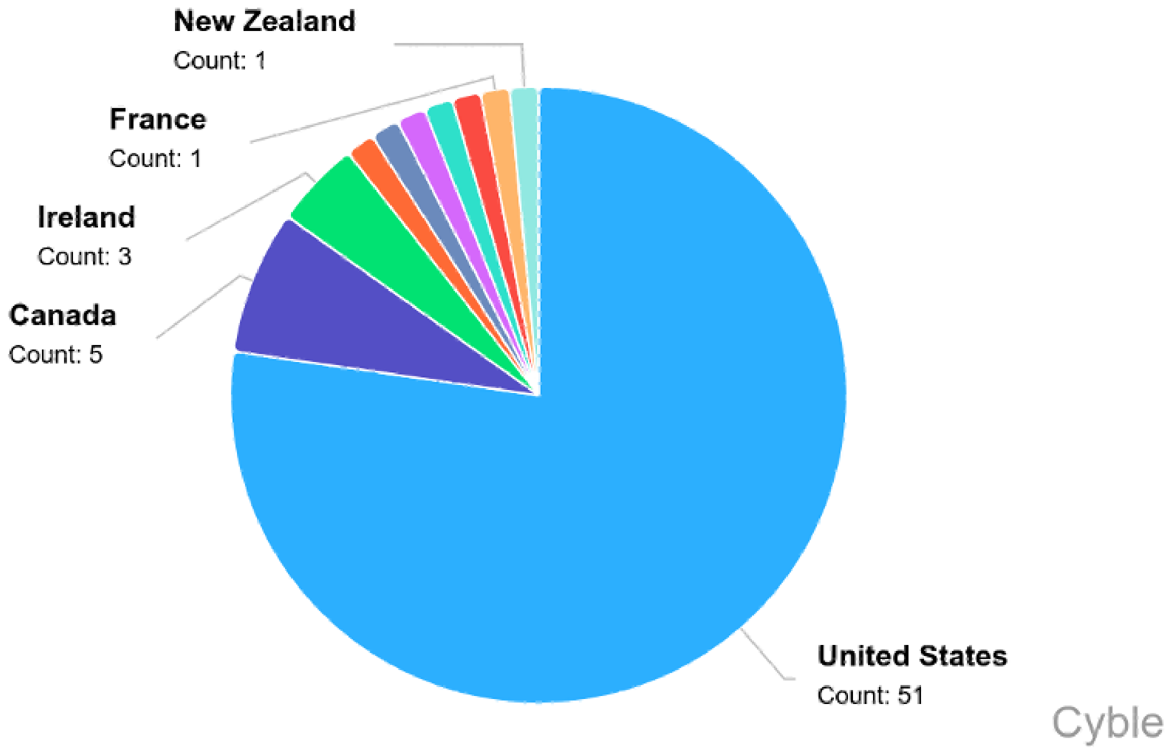


Fig 6: Country-wise Attacks by Cl0P

This pattern suggests the widespread exploitation of a common vulnerability across multiple organizations, enabling CL0P to compromise a large number of victims in a short period and most of them were from the U.S.

In contrast, the Qilin group demonstrated a more sustained operational tempo, maintaining a steady pace of attacks throughout the year that escalated in the final quarter, with 19 of its 43 total attacks occurring in November and December.

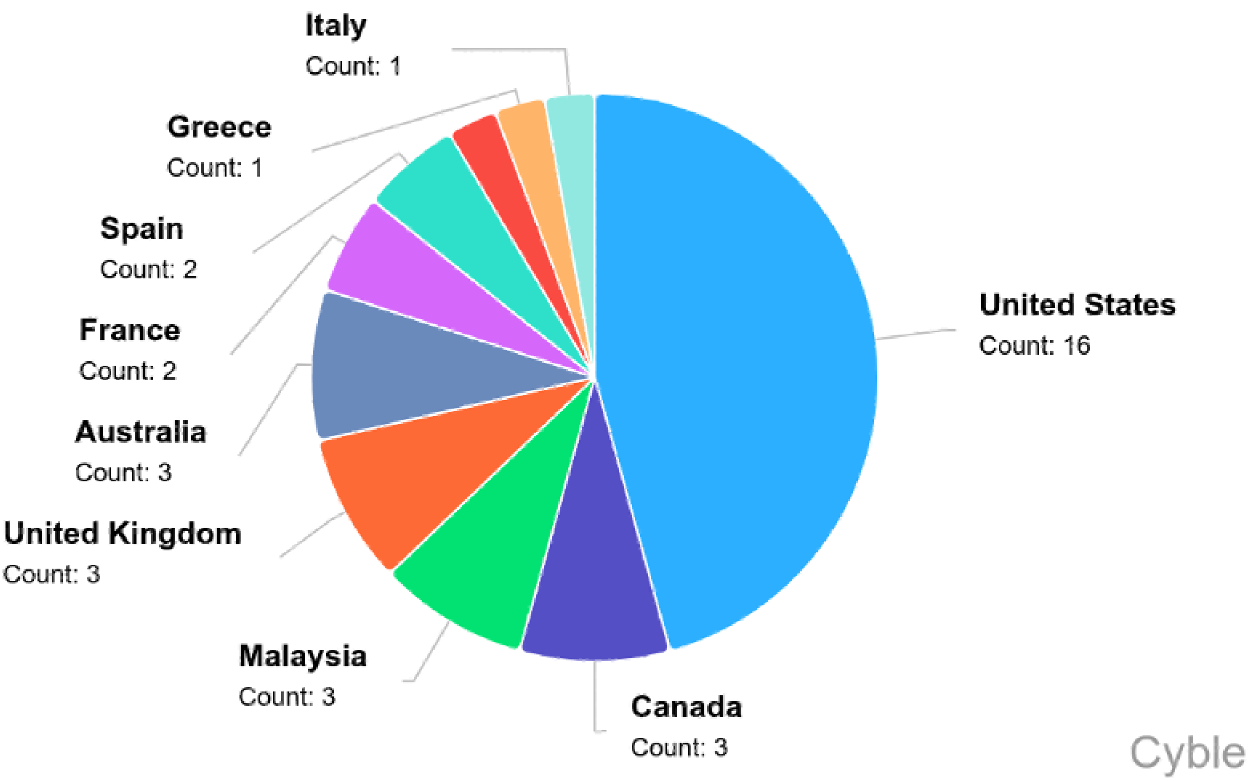


Fig 7: Country-wise Attacks by Cl0P

Apart from North America, Qilin highly targeted the European transport and logistics sector that is currently stretched due to the ongoing invasion of Russia on Ukraine.

Ultimately, the 2025 threat landscape for the transport and logistics sector was defined by the outsized impact of a few highly active ransomware groups, particularly the campaign-driven attacks by CL0P and the sustained pressure from Qilin.

These actors demonstrated the capability to disrupt a diverse range of critical services, from global aviation and maritime shipping to local warehousing and public transportation, underscoring the systemic risk ransomware poses to the interconnected logistics ecosystem.

Regional Trends

As evident by now, majority of the attacks were targeted at the American continent where North and South America together represented more than half of the attack volume (64%).

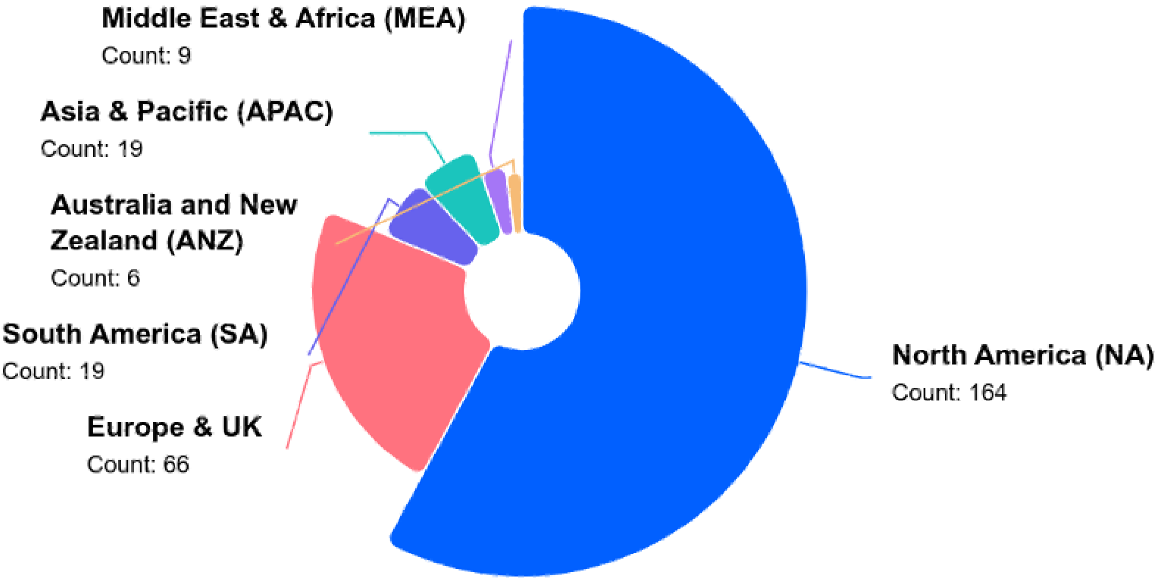


Fig 8: Region-wise Ransomware Attacks Distribution

Americas

After U.S., Canada was the most targeted country in the American continent. The lesser known for transport and logistics, the South American countries like Brazil, Colombia, Chile and Peru were also on the radar of ransomware actors, this year. This shows a marked shift in interest towards smaller nations and economies that are already fragile but also highly vulnerable.

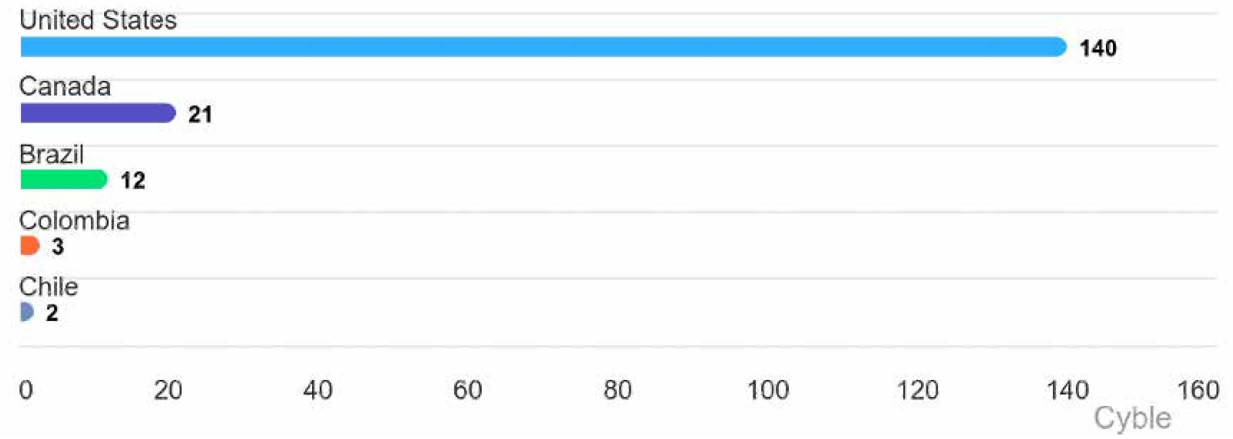


Fig 9: Most Ransomware Attacked Countries in Americas

While Cl0p led the charge here too, other threat actors like Play and Akira were equally active along with Qilin, who was the second most active in this region.

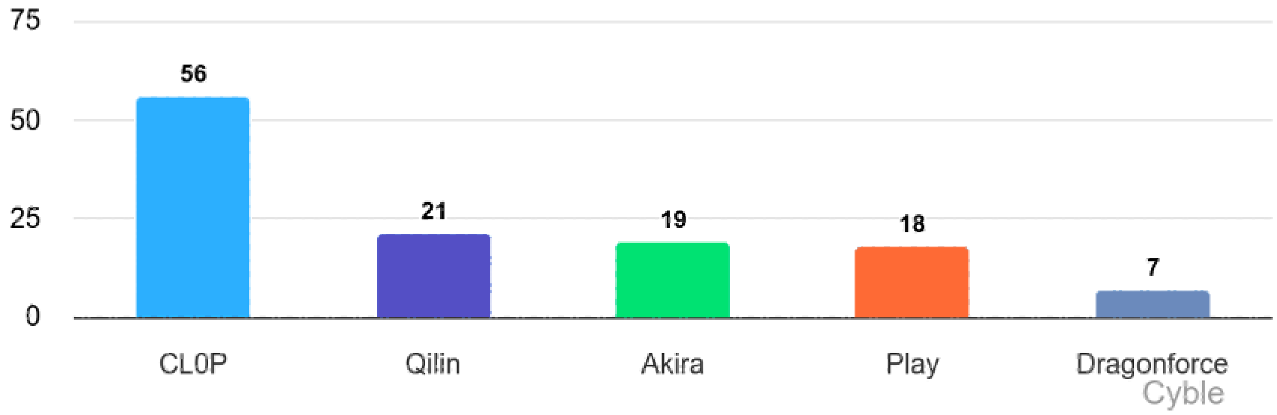


Fig 10: Top Ransomware Actors in Americas

Europe and UK

The region emerged as the second-most targeted this year after America. From aviation to shipping, all industries were targeted through 2025. And while Germany and the UK accounted for nearly 50% of the transport and logistics sector in Europe, France, Ireland, Italy, Norway and Denmark were all equally targeted.

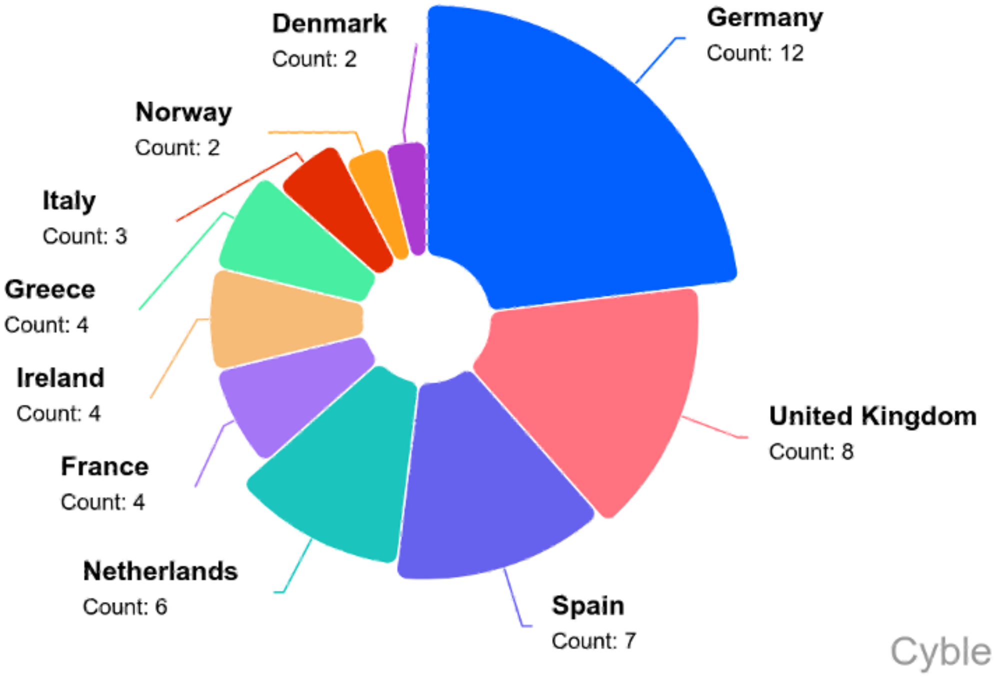


Fig 11: Most Ransomware Attacked Countries in Europe and UK

This region saw a heavy presence of Qilin, who was a dominant threat actor targeting the sector in nearly all major European nation.

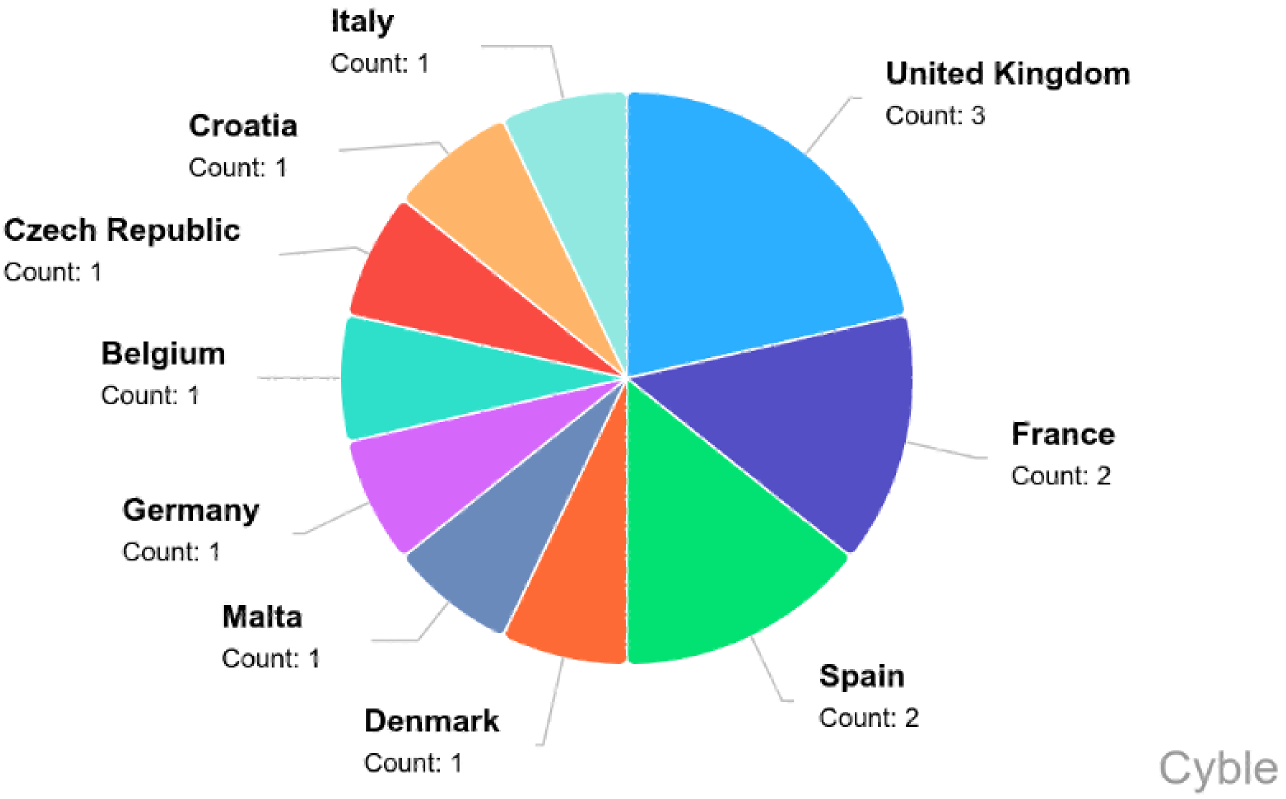


Fig 12: Most Attacked Countries in Europe and UK by Qilin Ransomware

And while Qilin led the race, other prominent players like Akira and SafePay also emerged in the region in the second half of the year, going after the transport and logistics sector.

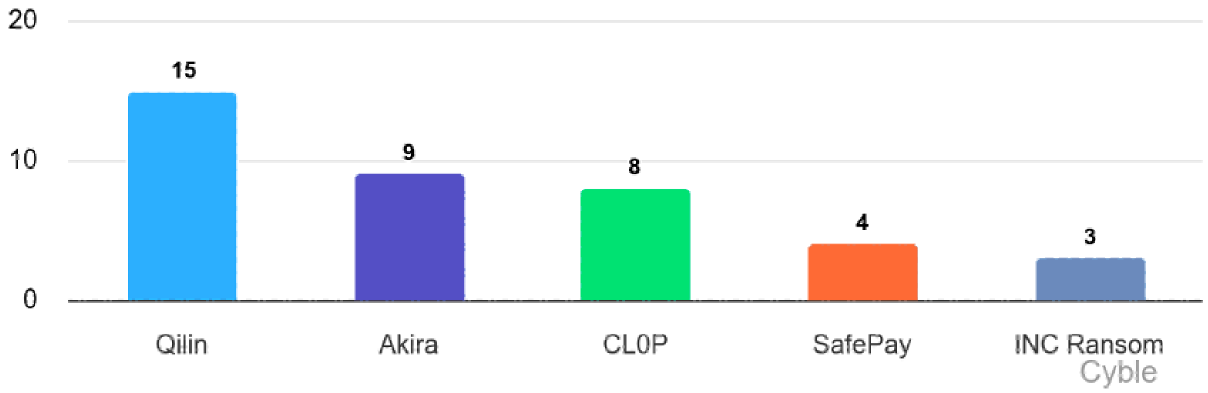


Fig 13: Top Ransomware Actors in Europe and UK

Asia

In Asia, the South-Eastern countries were the prime target with Malaysia and Thailand accounting for half of the attacks. The Transport and Logistics sector that is considered to be one of the vast in the region and across the world in countries like China and India, remained nearly untouched or likely beyond the grasp of the ransomware actors.

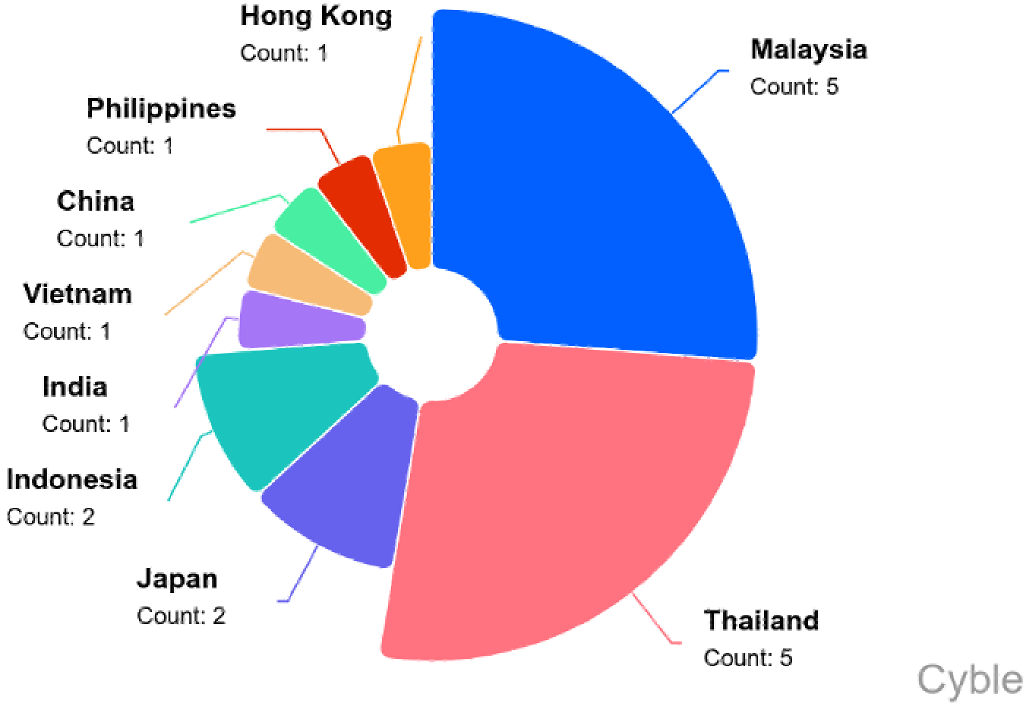


Fig 14: Most Ransomware Attacked Countries in APAC

The top ransomware actors list although led by Qilin, remained fragmented and equally targeted by others such as The Gentleman, NightSpire and Ransomhub.

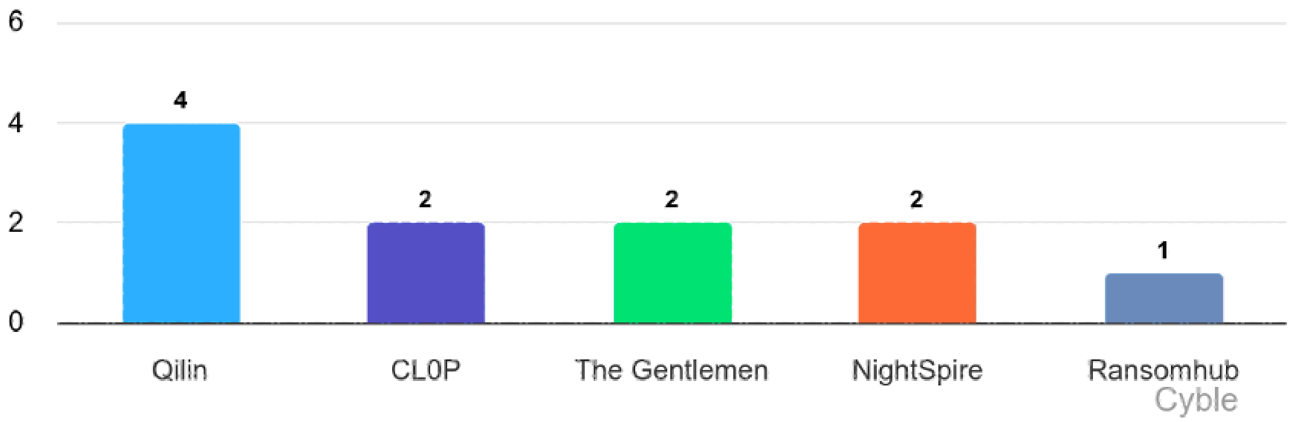


Fig 15: Top Ransomware Actors in APAC

Australia and New Zealand

The Australia and New Zealand region saw the least number of attacks but probably the most impactful as one of the attacks led to the data leak of 6 million customer records. As compared to last year, the number of ransomware attacks aimed at the Transport and Logistics sector in the ANZ region remained same for Australia but for the first time a T&L organization has appeared on the attacked list, highlighting the shifting targets and motivations of ransomware actors.

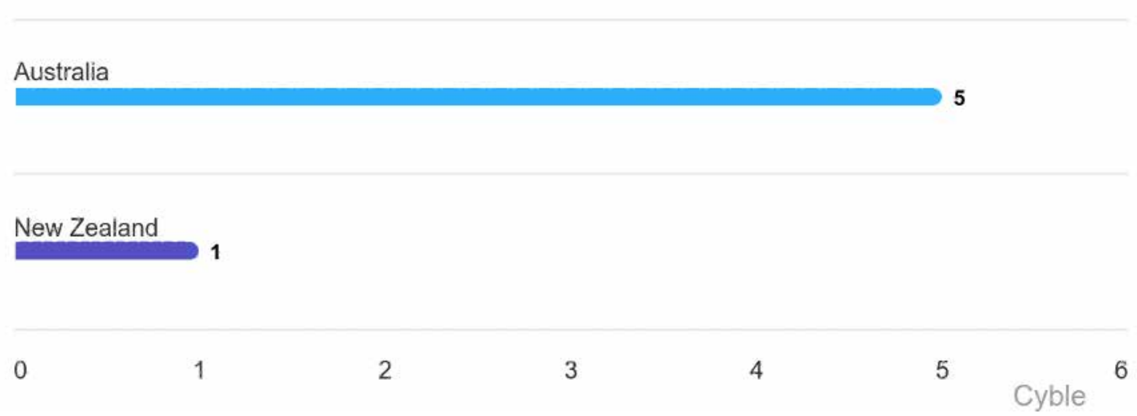


Fig 16: Ransomware Attack Statistics for ANZ

The space was owned by only three ransomware actors who targeted the Transport and Logistics sector in this region in a decremental manner.

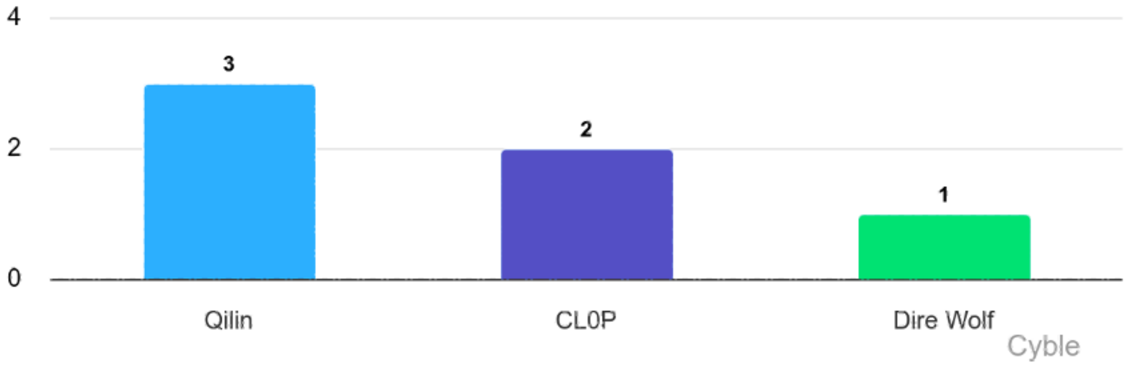


Fig 17: Top Ransomware Actors in ANZ

Middle East and Africa

The most fragmented threat landscape when it comes to the ransomware attacks on the Transport and Logistics sector is the Middle East and Africa, also known as MEA region.

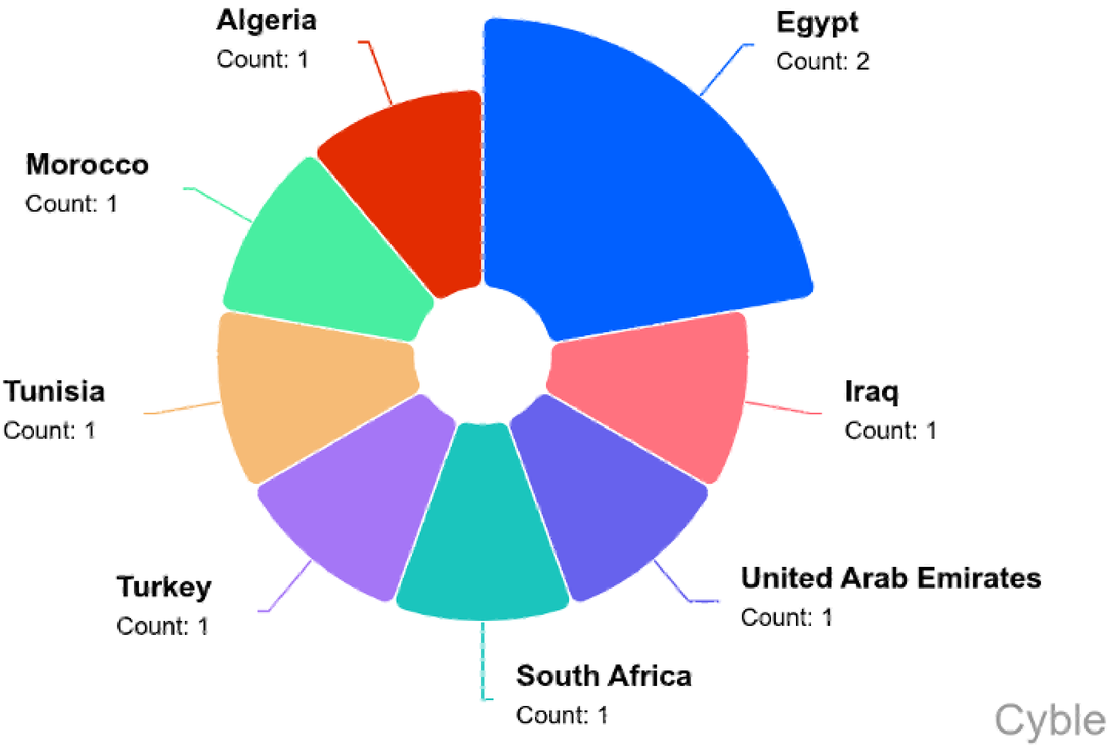


Fig 18: Most Ransomware Attacked Countries in MEA

The number of attacks were equally distributed with Egypt being the leader by a tiny fraction. At the same time, while INC had two attacks under its name, there was a longtail of other actors that were seen targeting this sector in the region.

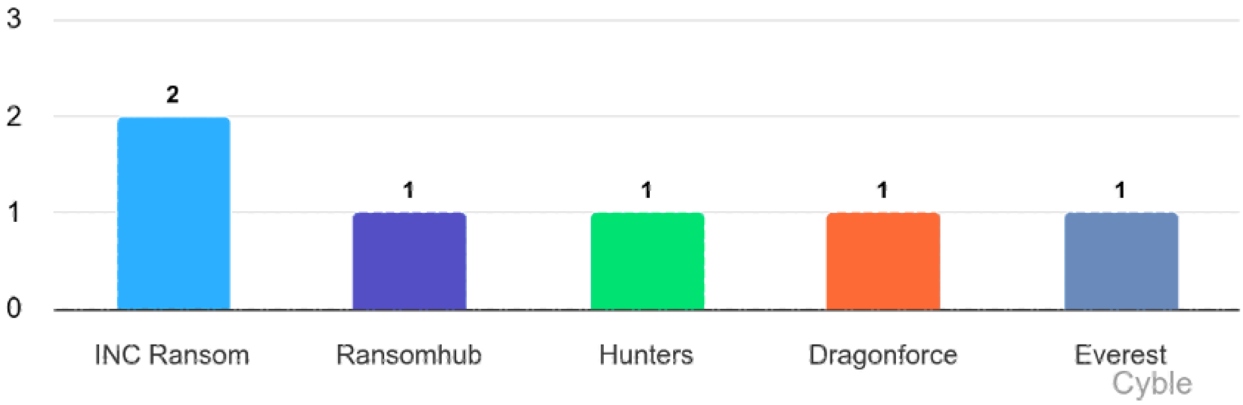


Fig 19: Top Ransomware Actors in MEA

Data Breaches and Leaks

Analysis of threat actor activity revealed that two actors going by the name ‘privilege’ and ‘bytetobreach’ were the most prolific sources of data leaks targeting the transport and logistics sector in 2025. A secondary tier of active threat actors, including ‘gloomer’ and ‘bigbrother’, also maintained a consistent presence with four posts each.

While this small group of actors accounts for a significant share of the activity, the overall threat landscape for data breaches was highly fragmented. A vast number of actors, constituting a long tail, were observed posting leaked data only once or twice throughout the year. This distribution suggests that the sector is targeted not only by a few persistent threat actors but also by a wide array of opportunistic individuals and groups, highlighting a broad and diverse threat environment where data exfiltration and leakage are common and accessible attack vectors.

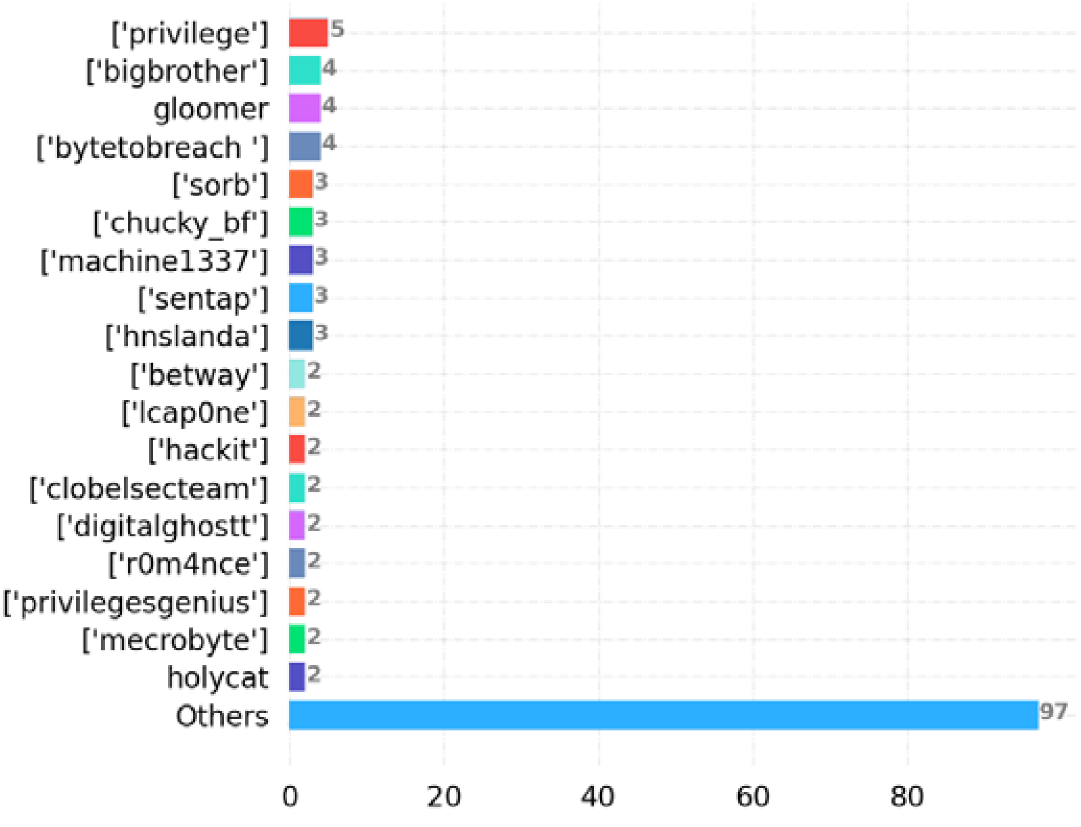


Fig 20: Active Threat Actors Selling Data Breaches

Notable Data Breaches and Leaks

Termite Ransomware Leaks Data from UK Supply Chain Firm

Earlier this February, the Termite Ransomware group leaked 129.36GB of archived data allegedly stolen from a global supply chain management and logistics firm based in the UK. The threat actor published a file tree revealing that the exfiltrated data contains sensitive internal financial and operational documents.

The exposed files include budget reports for key markets like the UK, USA, Australia, and China, profit and loss statements, financial forecasts, business plans, customer data, and strategic initiatives, creating potential financial and operational risks for the company and its partners.

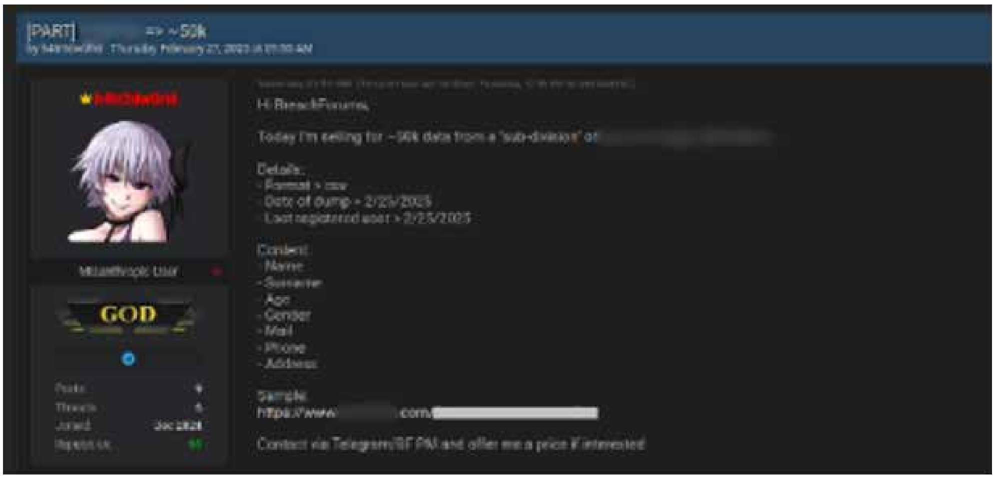
[redacted]

Description

[redacted] provides freight forwarding and supply chain management solutions. The company was founded in 1996 and is headquartered in Leeds, United Kingdom

Partial Database of French Postal Service Leaked Online

In February, the threat actor 'h4tr3dw0rld' posted on the nuovo BreachForums claiming to have a partial database stolen from a French postal service company. The threat actor alleged that the data was exfiltrated on February 25 and contained 50,000 records of Personally Identifiable Information (PII) in [.]csv format. The exposed data fields reportedly included full names, age, gender, email addresses, phone numbers, and physical addresses. A small data sample was provided to support the claim, and while no price was quoted, the threat actor invited interested buyers to make contact privately.



[PART] [redacted] => ~50k

Hi BreachForums,

Today I'm selling for ~50k data from a 'sub-division' of [redacted]

Details:
- Format > csv
- Date of dump > 2/25/2025
- Last registered user > 2/25/2025

Content:
- Name
- Surname
- Age
- Gender
- Mail
- Phone
- Address

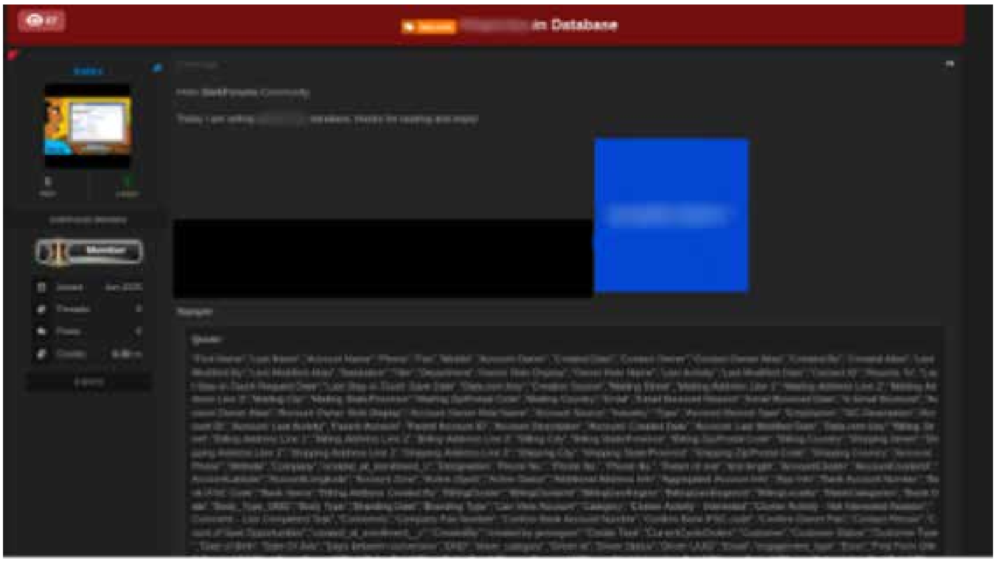
Sample:
https://www.[redacted].com/[redacted]

Contact via Telegram/BF PM and offer me a price if interested

Alleged Logistics Firm Data Breach Puts 7 Million User Records Up For Sale

Around July this year, a threat actor named 'index' advertised a database for sale on the DarkForums cybercrime forum. The threat actor claimed the database contains personally identifiable information (PII) for approximately 7.09 million users of an India-based logistics and transportation platform, allegedly stolen during a data breach in May 2025.

To support the claim, the seller shared sample records appearing to originate from a CRM system, which included account names, phone numbers, mailing addresses, account types, and industry designations. The data was offered as a one-time sale with no public price, inviting buyers to a private chat. It remains unclear if this data is connected to a previously reported breach at the company in September 2024.



[redacted] in Database

Hello DarkForums Community

Today I am selling [redacted] database, thanks for reading and enjoy!

[redacted]

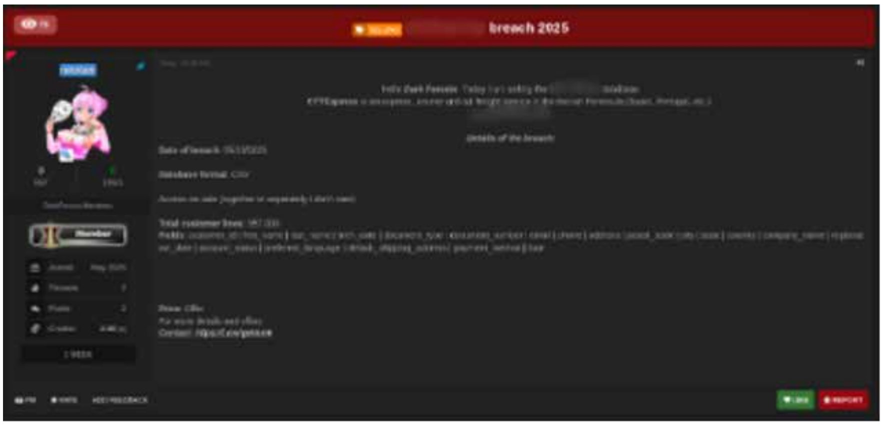
Sample

Quote

[illegible]

Alleged Spanish Courier Company Data Breach Exposes 357000 Customer Records

Earlier this May, threat actor ‘retolam’ advertised a database on the DarkForums cybercrime forum, allegedly stolen from a Spanish courier company. The actor claimed a data breach on May 19, stating he had exposed approximately 357,000 lines of customer records in CSV format, including personally identifiable information such as names, birth dates, document numbers, emails, phone numbers, addresses, and IBANs. In the post, ‘retolam’ also claimed to possess access to the company’s network. However, no supportive evidence or a price was provided, and the claim remains unverified.



[redacted] breach 2025

Hello Dark Forums! Today I am selling the [redacted] database

Details of the breach

Date of breach:

Database format: CSV

Total customer lines:

Fields:

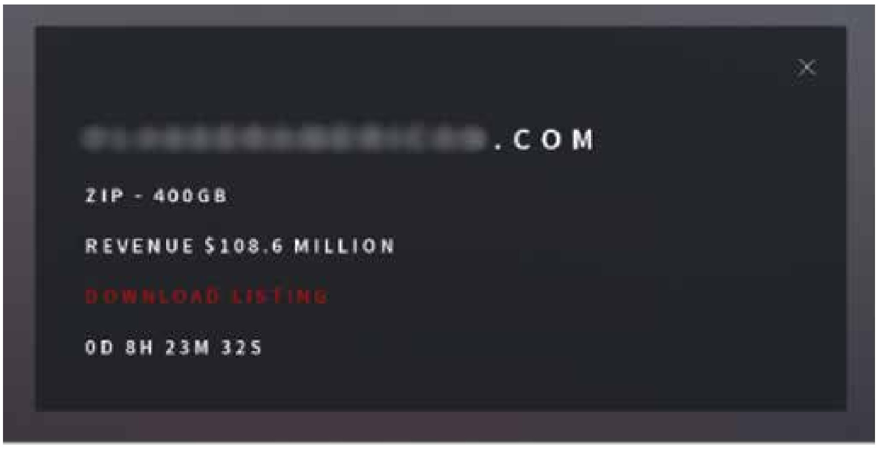
Price: Offer

For more details and offers

Contact:

US Rail Equipment Firm Targeted by SAFEPAY Ransomware

Around February, the SAFEPAY ransomware group claimed to have compromised a U.S.-based manufacturer of rail track maintenance machinery. The threat actors alleged the theft of 400GB of internal documents and imposed a tight 8-hour deadline for the company to respond. To substantiate their claim, the group published a file tree of the purportedly stolen data. As of the time of this report, the equipment company has not publicly acknowledged the breach.



[redacted].COM

ZIP - 400GB

REVENUE $108.6 MILLION

DOWNLOAD LISTING

0D 8H 23M 32S

Initial Accesses on Sale

Analysis of threat actor activity reveals that 'budda12' and 'stepbro' were the most prolific vendors of compromised accesses impacting the transport and logistics sector in 2025. These two actors alone were responsible for approximately 13% of the observed listings.

Below this top tier, a small group of moderately active threat actors posted two listings each, but the market's structure is predominantly defined by a long tail of transient or opportunistic sellers. The vast majority of listings originated from a diverse set of dozens of individual actors who only posted a single time. This distribution indicates a highly fragmented and decentralized marketplace for compromised access, rather than one controlled by a few dominant players.

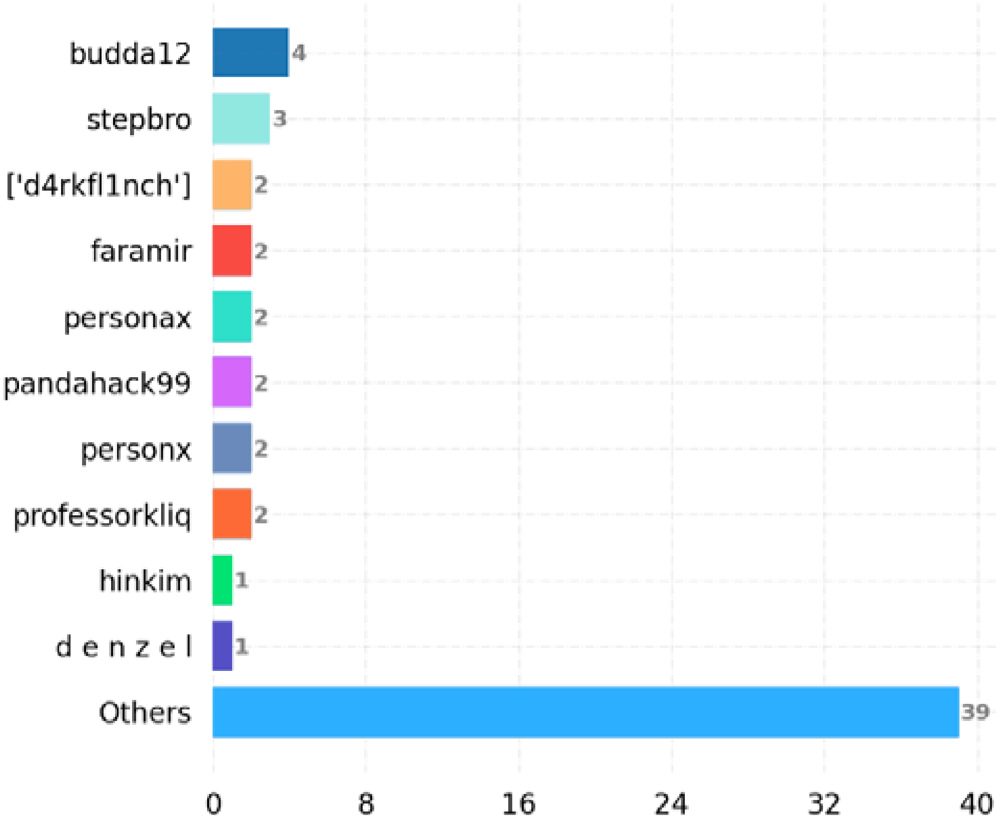
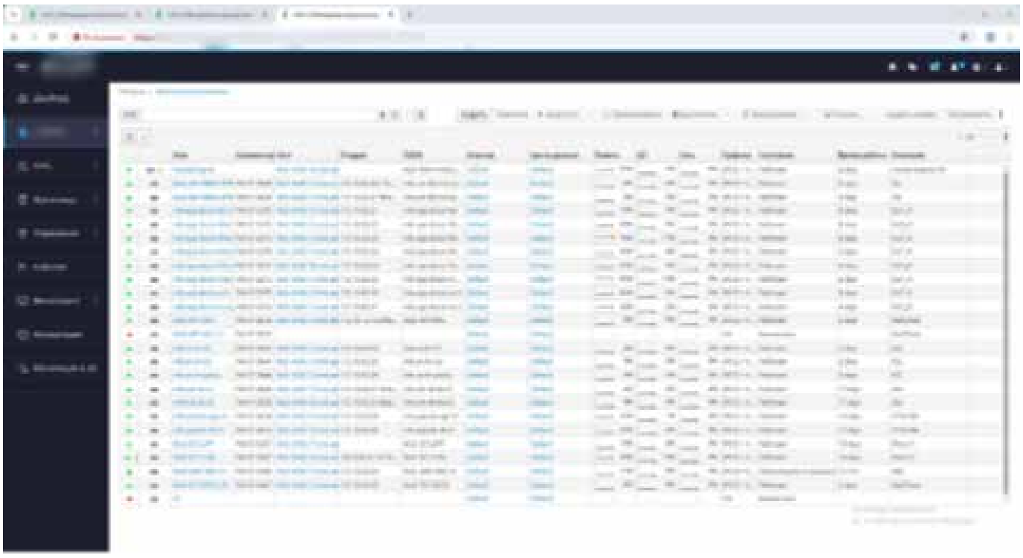


Fig 21: Active Threat Actors Selling Compromised Access

Notable Accesses on Sale

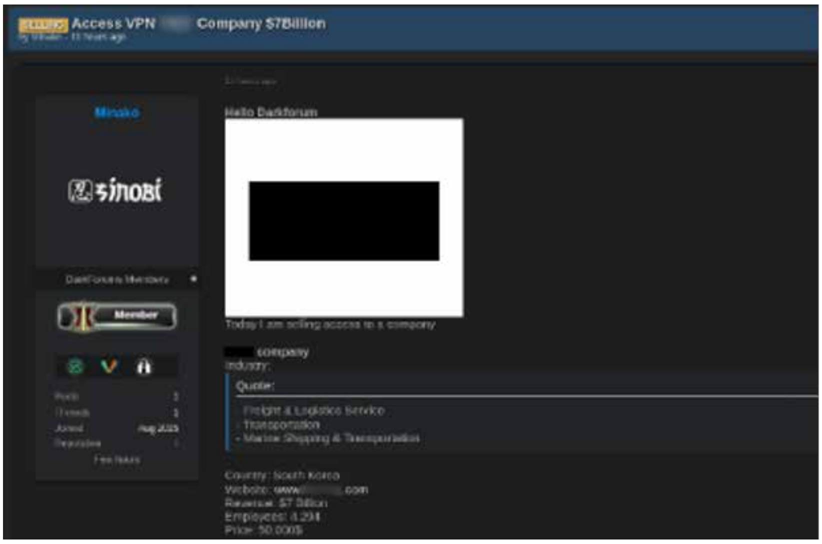
Hacktivist Groups Cripple Russian Airline in Destructive Cyberattack

In late July, the pro-Ukrainian hacktivist groups Cyber Partisans BY and Silent Crow claimed a destructive cyberattack against the Russian state-owned airline, Aeroflot. The groups alleged they utilized year-long Tier-0 access to compromise and sabotage the airline's IT infrastructure, reportedly destroying approximately 7,000 servers. Core operational systems, including CREW, Sabre, and Exchange, were impacted, and the attackers claimed to have exfiltrated 12TB of databases, 8TB of file shares, and 2TB of email data. The incident, which Russia's General Prosecutor confirmed was a cyberattack, resulted in significant operational disruption, including over 40 flight cancellations and delays at Sheremetyevo Airport.



Threat Actor Sells VPN Access to South Korean Shipping Firm HMM

In mid-August, the threat actor Minako advertised the sale of unauthorized VPN access to a major South Korean shipping and logistics company on the English-language cybercrime forum, DarkForums. The threat actor listed the access for USD 50,000. As proof of the compromise, Minako provided a screenshot displaying the output of an internal network reconnaissance scan performed with the NetExec tool. The scan results detailed reachable Windows systems on the compromised company's network, substantiating the threat actor's claim of having established a foothold within the company's infrastructure.



SELLING Access VPN Company $7Billion

Hello Darkforum

[redacted]

Today I am selling access to a company

[redacted] company

Industry:

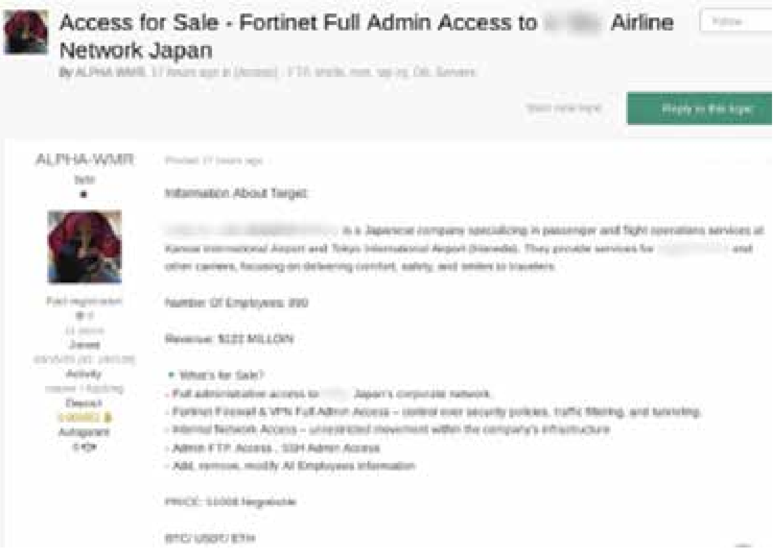
Quote:

- Freight & Logistics Service
- Transportation
- Marine Shipping & Transportation

Country: South Korea
Website: www. .com
Revenue: $7 Billion
Employees: 4,234
Price: 50,000$

Alleged Network Access to Japanese Flight Operations Firm Offered on Cybercrime Forum

In early April, the threat actor known as ALPHA-WMR offered alleged network access to a Japanese flight operations service provider, for sale on the Exploit cybercrime forum. The actor claimed the access included control over the company's Fortinet Firewall and VPN, allowing for the management of security settings and network traffic. Additionally, ALPHA-WMR asserted they had unrestricted movement within the internal network and administrative privileges for FTP servers and SSH, which would enable the modification of employee information. While no evidence was provided publicly in the post to substantiate these claims, the threat actor stated they would share proof privately with potential buyers.



Access for Sale - Fortinet Full Admin Access to Airline Network Japan

Information About Target:

is a Japanese company specializing in passenger and flight operations services at Kansai International Airport and Tokyo International Airport (Haneda). They provide services for and other carriers, focusing on delivering comfort, safety, and smiles to travelers.

Number Of Employees: 890

Revenue: $122 MILLION

- What's for Sale?
- Full administrative access to Japan's corporate network.
- Fortinet Firewall & VPN Full Admin Access – control over security policies, traffic filtering, and tunneling.
- Internal Network Access – unrestricted movement within the company's infrastructure
- Admin FTP Access , SSH Admin Access
- Add, remove, modify All Employees information

PRICE: 5100$ Negotiable

BTC/ USDT/ ETH

Scattered Spider Suspected in Qantas Data Breach Affecting 6 Million Customers

Suspected threat actor group Scattered Spider gained unauthorized access to a customer service portal belonging to the Australian airline Qantas. The breach exposed the personally identifiable information (PII) of approximately 6 million customers. The compromised data includes customer names, email addresses, phone numbers, birth dates, and frequent flyer numbers.

According to the airline, more sensitive information such as credit card details, financial data, and passport information was not impacted, as it was not stored on the affected system. Furthermore, no account passwords, PINs, or login credentials were accessed. This incident is potentially linked to a broader campaign by the threat actor targeting the aviation sector.

Critical Vulnerabilities observed as Zero days and CISA KEV

Known Exploited Vulnerabilities

The 2025 cyber threat landscape, as reflected in the CISA Known Exploited Vulnerabilities (KEV) catalog, is characterized by a prevalence of critical and high-severity vulnerabilities across a wide range of products, irrespective of industry or region.

A significant majority of the listed Common Vulnerabilities and Exposures (CVEs) possess CVSS scores of 9.0 or higher, indicating a persistent trend of highly impactful security flaws being actively exploited. Notably, vendors such as Microsoft, Apple, Cisco, and Fortinet appear multiple times. This is due to the continued targeting of widely deployed enterprise technologies, including network security appliances, operating systems, and productivity software.

The inclusion of several vulnerabilities with perfect 10.0 CVSS scores, such as those affecting Adobe Experience Manager, Commvault Command Center, and Cisco Identity Services Engine, highlight the severe risk posed by unauthenticated, remote code execution flaws. For instance, the critical vulnerability in Adobe Experience Manager (CVE-2025-54253) was actively exploited, allowing attackers to take full control of vulnerable systems. Similarly, vulnerabilities in Cisco's Identity Services Engine (CVE-2025-20281 and CVE-2025-20337) were subject to in-the-wild exploitation attempts, posing a significant threat of complete system compromise.

The recurrence of vulnerabilities in similar product categories, such as VPN gateways and enterprise management platforms, suggests a continued focus by threat actors on these high-value targets.

To mitigate these risks, organizations must implement a robust vulnerability management program that includes prompt patching, network segmentation to limit lateral movement, and continuous monitoring for signs of compromise.

CVE ID	Product	Vendor	CVSS(V3)
CVE-2020-2883	Weblogic Server	Oracle	9.8
CVE-2024-41713	Micollab	Mitel	9.1
CVE-2025-0282	Ivanti Connect Secure	Ivanti Connect Secure	9
CVE-2023-48365	Qlik Sense	Qlik	9.9
CVE-2024-55591	Fortios	Fortinet	9.8
CVE-2024-50603	Controller	Aviatrix	9.8
CVE-2025-23006	Sma1000	Sonicwall	9.8

CVE-2025-24085	Visionos	Apple	10
CVE-2018-19410	Prtg Network Monitor	Paessler	9.8
CVE-2020-29574	Cyberoamos	Sophos	9.8
CVE-2024-21413	Office	Microsoft	9.8
CVE-2020-15069	Xg Firewall Firmware	Sophos	9.8
CVE-2024-53704	Sonicos	Sonicwall	9.8
CVE-2025-0108	Cloud Ngfw	Paloaltonetworks	9.1
CVE-2025-24989	Power Pages	Microsoft	9.8
CVE-2017-3066	Coldfusion	Adobe	9.8
CVE-2023-34192	Collaboration	Zimbra	9
CVE-2024-49035	Partner Center	Microsoft	9.8
CVE-2022-43939	Vantara Pentaho Business Analytics Server	Hitachi	9.8
CVE-2024-4885	Whatsup Gold	Progress	9.8
CVE-2025-24201	Visionos	Apple	10
CVE-2025-1316	Ic 7100 Ip Camera	Edimax	9.8
CVE-2019-9874	Cms	Sitecore	9.8
CVE-2024-20439	Smart License Utility	Cisco	9.8
CVE-2025-24813	Tomcat	Apache	9.8
CVE-2025-22457	Connect Secure	Ivanti	9.8
CVE-2025-31161	Crushftp	Crushftp	9.8
CVE-2025-30406	Centrestack	Gladinet	9.8
CVE-2025-31200	Ipados	Apple	9.8
CVE-2025-31201	Macos	Apple	9.8
CVE-2025-42599	Active Mail	Qualitia	9.8
CVE-2025-31324	Netweaver	Sap	9.8
CVE-2024-38475	Http Server	Apache	9.1
CVE-2024-58136	Yii2	Yii2	9.8
CVE-2025-34028	Command Center Innovation	Commvault	10
CVE-2025-3248	Langflow	Langflow Ai	9.8
CVE-2024-6047	Gv Vs14 Vs14	Geovision	9.8
CVE-2024-11120	Gv Dsp Lpr	Geovision	9.8
CVE-2025-32756	Forticamera	Fortinet	9.8

CVE-2024-12987	Vigor300B	Draytek	9.8
CVE-2025-42999	Netweaver	Sap	9.1
CVE-2025-4632	Magicinfo 9 Server	Samsung Electronics	9.8
CVE-2021-32030	Gt Ac2900 Firmware	Asus	9.8
CVE-2024-56145	Cms	Craft	9.8
CVE-2025-32433	Otp	Erlang	10
CVE-2024-42009	Webmail	Roundcube	9.3
CVE-2025-24016	Wazuh	Wazuh	9.9
CVE-2024-0769	Dir 859	D Link	9.8
CVE-2024-54085	Megarac Spx	Ami	9.8
CVE-2025-6543	Netscaler Application Delivery Controller	Citrix	9.8
CVE-2014-3931	Multi Router Looking Glass	Multi Router Looking Glass Project	9.8
CVE-2016-10033	Phpmailer	Phpmailer Project	9.8
CVE-2025-47812	Wing Ftp Server	Wftpserver	10
CVE-2025-25257	Fortiweb	Fortinet	9.8
CVE-2025-53770	Sharepoint Enterprise Server	Microsoft	9.8
CVE-2025-2776	On Prem	Sysaid	9.8
CVE-2025-54309	Crushftp	Crushftp	9.8
CVE-2025-20281	Identity Services Engine	Cisco	10
CVE-2025-20337	Identity Services Engine	Cisco	10
CVE-2025-54948	Apex One	Trendmicro	9.8
CVE-2025-7775	Netscaler Application Delivery Controller	Citrix	9.8
CVE-2025-57819	Freepbx	Freepbx	9.8
CVE-2025-53690	Experience Manager	Sitecore	9
CVE-2025-5086	Delmia Apriso	Dassault Syst Mes	9
CVE-2025-10585	Chrome	Google	9.8
CVE-2025-20333	Adaptive Security Appliance	Cisco	9.9
CVE-2025-10035	Goanywhere Mft	Fortra	9.8
CVE-2015-7755	Screenos	Juniper	9.8
CVE-2017-1000353	Jenkins	Jenkins	9.8
CVE-2025-21043	Devices	Samsung	9.8

CVE-2010-3765	Firefox	Mozilla	9.8
CVE-2025-61882	Concurrent Processing	Oracle	9.8
CVE-2016-7836	Skysea Client View	Skygroup	9.8
CVE-2025-54253	Experience Manager	Adobe	10
CVE-2025-2746	Xperience	Kentico	9.8
CVE-2025-2747	Xperience	Kentico	9.8
CVE-2025-61932	Lanscope Endpoint Manager And Detection Agent	Motex	9.8
CVE-2025-54236	Commerce	Adobe	9.1
CVE-2025-59287	Windows Server 2012	Microsoft	9.8
CVE-2025-6205	Delmia Apriso	Dassault Syst Mes	9.1
CVE-2025-24893	Xwiki Platform	Xwiki Platform	9.8
CVE-2025-48703	Centos Web Panel	Centos Webpanel	9
CVE-2025-21042	Devices	Samsung	9.8
CVE-2025-9242	Fireware Os	Watchguard	9.8
CVE-2025-12480	Triofox	Triofox	9.1
CVE-2025-64446	Fortiweb	Fortinet	9.8
CVE-2025-61757	Identity Manager	Oracle	9.8
CVE-2025-55182	React Server Dom Parcel	Meta	10
CVE-2022-37055	Go Rt Ac750 Firmware	Dlink	9.8
CVE-2025-66644	Arrayos Ag	Array	9.8
CVE-2025-58360	Geoserver	Geoserver	9.8
CVE-2025-14611	Centrestack	Gladinet	9.8
CVE-2025-59718	Fortios	Fortinet	9.8
CVE-2025-20393	Secure Email	Cisco	10

Zero-Day Vulnerabilities

The 2025 threat landscape was defined by a surge in high-severity, industry-agnostic, and region-agnostic zero-day vulnerabilities, with a significant concentration of CVSS scores in the critical (9.0-10.0) range. This trend underscores the widespread and immediate risk posed by actively exploited flaws, as threat actors rapidly weaponized vulnerabilities in perimeter devices and widely used enterprise software.

Notably, vendors such as Apple, Fortinet, and Ivanti experienced multiple critical zero-day events, indicating systemic challenges in securing internet-exposed products like VPN gateways and network security appliances. The active exploitation of these vulnerabilities, particularly in products from Cisco, Citrix, and Microsoft, highlights intense threat actor interest in gaining initial access to corporate networks.

The prevalence of critical vulnerabilities in enterprise platforms like SAP and Sitecore further illustrates the broad attack surface available to adversaries. Organizations must prioritize rapid patching, robust network segmentation, and continuous monitoring to mitigate the significant risk posed by this escalating wave of zero-day threats.

CVE ID	Product	Vendor	CVSS(V3)
CVE-2025-0282	Ivanti Connect Secure	Ivanti Connect Secure	9
CVE-2024-55591	Fortios	Fortinet	9.8
CVE-2025-23006	Sma1000	Sonicwall	9.8
CVE-2025-24085	Visionos	Apple	10
CVE-2025-22457	Connect Secure	Ivanti	9.8
CVE-2025-30406	Centrestack	Gladinet	9.8
CVE-2025-31200	Ipados	Apple	9.8
CVE-2025-31201	Macos	Apple	9.8
CVE-2025-42599	Active Mail	Qualitia	9.8
CVE-2025-31324	Netweaver	Sap	9.8
CVE-2025-32432	Cms	Craft	10
CVE-2025-32756	Forticamera	Fortinet	9.8
CVE-2025-6543	Netscaler Application Delivery Controller	Citrix	9.8
CVE-2025-53770	Sharepoint Enterprise Server	Microsoft	9.8
CVE-2025-54948	Apex One	Trendmicro	9.8
CVE-2025-25256	Fortisiem	Fortinet	9.8
CVE-2025-43300	Macos	Apple	9.8
CVE-2025-7775	Netscaler Application Delivery Controller	Citrix	9.8
CVE-2025-57819	Freepbx	Freepbx	9.8
CVE-2025-21042	Devices	Samsung	9.8
CVE-2025-21043	Devices	Samsung	9.8
CVE-2025-10585	Chrome	Google	9.8
CVE-2025-61932	Lanscope Endpoint Manager And Detection Agent	Motex	9.8
CVE-2025-64446	Fortiweb	Fortinet	9.8
CVE-2025-20393	Secure Email	Cisco	10.0

Hacktivism

The hacktivism landscape in 2025 was characterized by a high volume of activity, primarily fueled by geopolitical conflicts and ideological agendas. The primary attack vectors included high-volume Distributed Denial-of-Service (DDoS) campaigns, website defacements, and a significant number of data leak incidents, with CRIL observing approximately 40,865 data leak and dump posts throughout the year. This activity impacted a vast digital footprint, with attacks directed at over 44,540 unique domains.

The targeting was largely opportunistic and widespread, affecting organizations across more than two dozen industries, including government, technology, media, and the transport and logistics sector. Numerous hacktivist collectives, often organized via social media and messaging channels, were responsible for these campaigns. Prominent groups and channels observed during this period include Русский Легион Z, GANOSECTEAM PALESTINA, Malaysia Hacktivist - Official, and Anonymous Italia 🇮🇹, reflecting the global and multifaceted nature of these threat actors.

הימין הלא מתנצל של הצל קבוצת דיוני השכל

Analysis of the Telegram channel 'הימין הלא מתנצל של הצל קבוצת דיוני השכל' (The Unapologetic Right of The Shadow - The Intellect Discussion Group) indicates its function as a political discussion forum rather than an operational hacktivist group. Content within the channel consists primarily of pro-Israeli, right-wing political commentary, internal criticism of Israeli government officials and military leadership, and hostile rhetoric directed at Palestinians, Arabs, and the Israeli left. Throughout the observation period, the group did not claim responsibility for, nor did it discuss conducting, any specific cyber operations such as DDoS attacks, data breaches, or website defacements. The channel's activities are centered on information dissemination and ideological discourse aligned with a nationalist Israeli perspective.

KREMLIN BR GROUP < HACKING TOOLS AND COURSE FREE />

The 'KREMLIN BR GROUP' channel is a Brazilian Portuguese-speaking marketplace for financially motivated cybercrime, rather than a traditional hacktivist collective. The channel's primary activities involve the advertisement and sale of malicious tools, stolen data, and illicit services to its members. Advertised offerings include ransomware, information stealers, Android Remote Access Trojans (RATs), phishing pages ('telas fake'), stolen credit card information ('infoCCs'), compromised databases, and access to money mule accounts ('laras').

Within the scope of the transport and logistics sector, members advertised phishing pages targeting the online travel agency '123 Milhas' and pages designed to intercept payments for vehicle taxes and fines (IPVA). Additional targets included major e-commerce platforms with extensive logistics networks, such as Mercado Livre and Magazine Luiza. All observed activities and discussions on the channel point to a purely financial motivation, with no discernible political or ideological agenda.

MINIONS CYBER CRIME HACKTIVIST

Based on an analysis of its channel content, 'MINIONS CYBER CRIME HACKTIVIST' functions as a financially motivated entity advertising a broad portfolio of cybercriminal services for hire, rather than a traditional hacktivist group. The channel's posts, a mix of English and Spanish, consistently market illicit services targeting both individuals and organizations without specifying victims or claiming responsibility for attacks.

Advertised capabilities include compromising social media, email, and mobile device accounts; conducting DDoS attacks; website database extraction; and deploying malware, spyware, and ransomware. A significant portion of their offerings is dedicated to financial fraud, including the sale of cloned credit cards (carding), cryptocurrency wallet hacking, and fraudulent fund recovery services. The group's motivation is explicitly commercial, with numerous posts emphasizing that services are not free and often demanding payment in cryptocurrency.

𝐍𝐨𝐂𝐫𝐲 𝐓𝐄𝐀𝐌 < ʜᴀᴄᴋɪɴɢ ᴛᴏᴏʟs ᴀɴᴅ ᴄᴏᴜʀsᴇ ғʀᴇᴇ />

Analysis of the '𝐍𝐨𝐂𝐫𝐲 𝐓𝐄𝐀𝐌' channel indicates its primary function is a service for querying sensitive and personally identifiable information (PII) through an automated bot. The observed activities are predominantly focused on data retrieval rather than disruptive attacks like DDoS or defacements.

Channel members frequently query Brazilian PII, including individual taxpayer IDs (CPF), full names, phone numbers, and vehicle license plates. Specific to the transport and logistics sector, members were observed querying for user logins associated with the airline Azul (`azul.com.br`) and the São Paulo Department of Transit (`detran.sp.gov.br`), in addition to numerous queries for individual vehicle license plates. Queries were also directed at Brazilian government and law enforcement portals, such as SINESP and the Civil Police of Minas Gerais. The channel's content lacks any stated political or ideological motivation, with posts instead advertising paid access to private groups and other illicit cybercriminal services.

Key Takeaways

01 The ransomware threat was dominated by a few prolific groups, with CL0P alone responsible for 24% of all attacks through large-scale, campaign-driven exploitation of common vulnerabilities.

02 The line between digital and physical risk blurred as threat actors used remote access tools to orchestrate cargo theft and exploited operational technology vulnerabilities in GPS trackers and rail systems, enabling potential remote vehicle disruption.

03 A diverse array of threat actors targeted the sector, including a fragmented ecosystem of financially motivated access brokers, state-sponsored espionage groups, and politically motivated hacktivists conducting destructive attacks against national carriers.

04 The active exploitation of zero-day and known critical vulnerabilities in widely deployed enterprise technologies, particularly perimeter security devices, served as the primary gateway for major disruptive incidents, including mass ransomware campaigns.

Conclusion

The transport and logistic sector in 2025 faced a severe and multifaceted threat landscape, dominated by a concentrated number of highly active ransomware groups like CL0P and Qilin, who were responsible for the majority of incidents that caused significant operational disruption. Underpinning these attacks was a fragmented but active cybercrime market for initial access and stolen data, which facilitated massive data breaches at companies such as Qantas, exposing the personal information of millions of customers.

Threat actors consistently exploited high-severity zero-day vulnerabilities in perimeter devices and enterprise software, while destructive hacktivism, exemplified by the attack on Aeroflot, and cyber-espionage also posed significant risks.

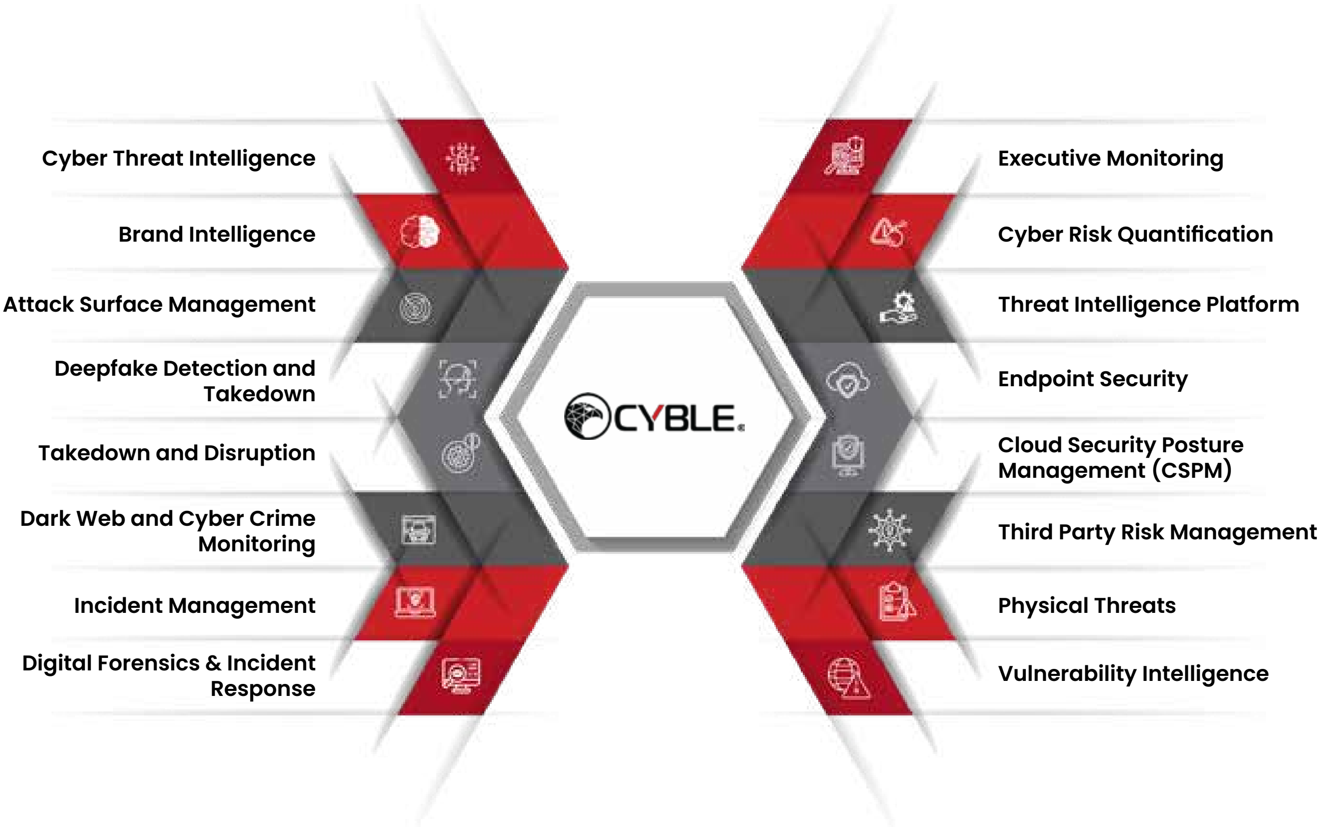
Ultimately, the impact of these cyber activities was profound, ranging from major financial losses to the complete business collapse of a UK logistics firm and the emergence of hybrid threats that blended cyber intrusion with physical cargo theft, highlighting the systemic risk to the global supply chain.

Trust Cyble for All Your Cybersecurity Needs

One Platform. All Threat Surfaces Covered. Real Intelligence.

Cyble gives security teams unified visibility across the adversary ecosystem. From dark web chatter to endpoint compromise, our AI-driven suite delivers intelligence that moves the needle in your favor.

What Cyble Offers...


Cyber Threat Intelligence
Brand Intelligence
Attack Surface Management
Deepfake Detection and Takedown
Takedown and Disruption
Dark Web and Cyber Crime Monitoring
Incident Management
Digital Forensics & Incident Response
CYBLE.
Executive Monitoring
Cyber Risk Quantification
Threat Intelligence Platform
Endpoint Security
Cloud Security Posture Management (CSPM)
Third Party Risk Management
Physical Threats
Vulnerability Intelligence

Industry Recognition

Cyble's capabilities are highly praised by global analysts, industry critics, and cybersecurity leaders

Gartner

Cyble Recognized in **Three Gartner® Hype Cycle™ Reports** for the **Second Consecutive Year 2025, TechScape 2025 & More**

FROST & SULLIVAN

Cyble Named Leader in Frost Radar™ Cyber Threat Intelligence 2024

Y Combinator

Cyble featured among AI startups backed by Y Combinator (YC) 2025

FORRESTER

Cyble has been recognized in Forrester's Q1 2025 report on Extended Threat Intelligence Service Providers (ETISPs) and in the Q2 2024 Forrester Attack Surface Management Landscape report.

QKS Group

SPARK Matrix™ 2025

LEADER

Cyble Named as a Leader in Digital Threat Intelligence Management

AMERICA'S BEST STARTUP EMPLOYERS Forbes 2024

Recognized as one of America's Best Startup Employers by Forbes

GLOBAL INFOSEC AWARDS NOW OPEN CYBER DEFENSE MAGAZINE 2025

Cyble Secures Four Prestigious Honors at the 2025 Global Infosec Awards

Gartner Peer Insights.

Ranked No. 1 among the top Security Threat Intelligence Providers.

4.8/5 ★★★★★

Cyble Named in America's Greatest Startup Workplaces 2025, By Newsweek

TOP INFOSEC INNOVATOR WINNER 2025

Cyble Wins Three Top InfoSec Innovator 2025 Awards

G2

Named a leader in the G2 Grid for Dark Web Monitoring and Threat Intelligence

Cyble, the world's first AI-native cybersecurity company, today announced its commanding presence in the **G2 Fall 2025 Report**, earning **24 prestigious badges across 8 strategic categories**. This unprecedented recognition validates Cyble's breakthrough **Agentic AI architecture** and positions the company as the definitive leader in autonomous cybersecurity intelligence.

FALL 2025 Leader

FALL 2025 Easiest To Use

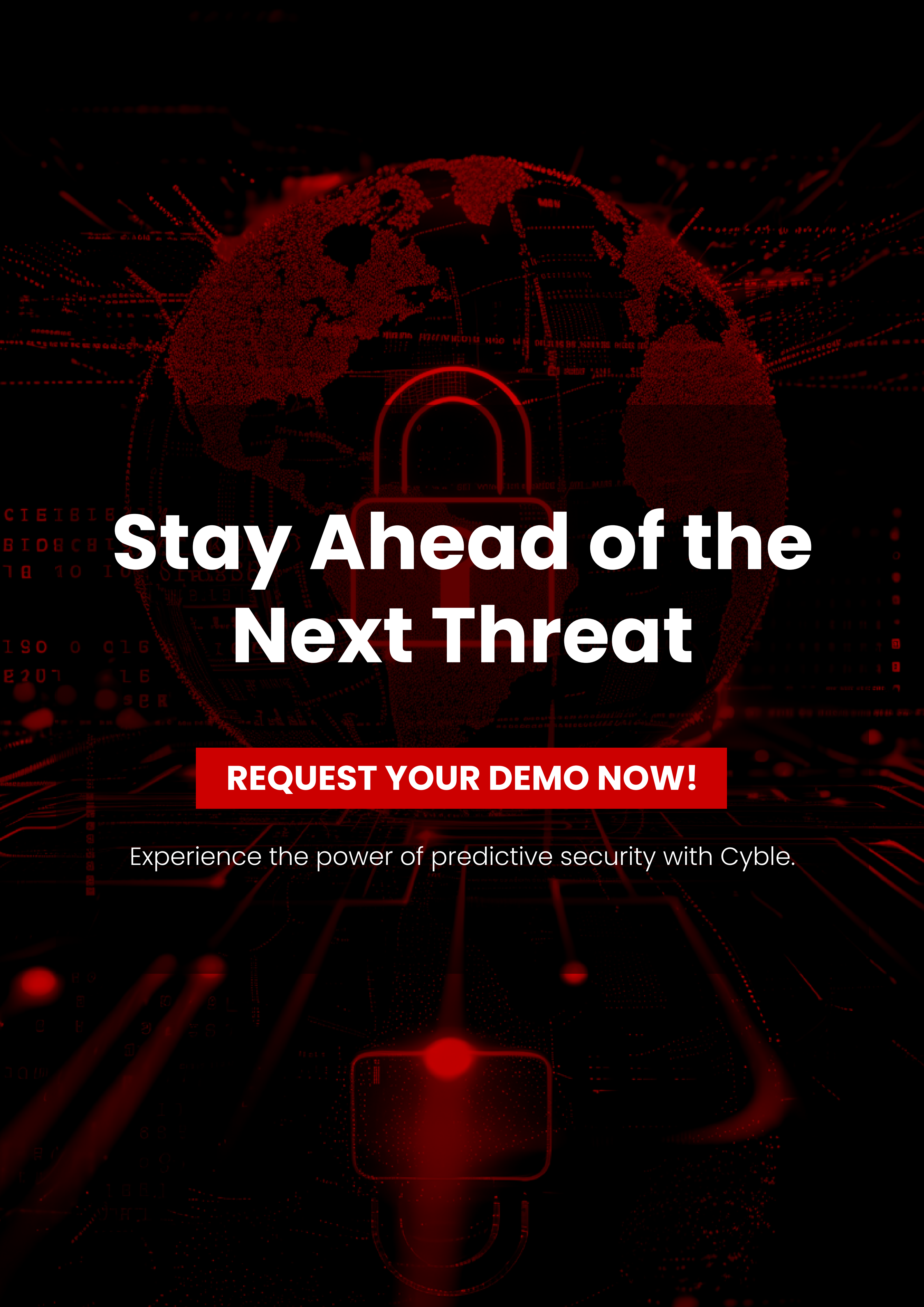
FALL 2025 Leader ENTERPRISE

FALL 2025 ASIA PACIFIC Regional Leader ENTERPRISE

FALL 2025 ASIA High Performer

OUR INVESTORS

BLACKBIRD · KING RIVER · Xoogler.co · SUMMIT PEAK INVESTMENTS · Singtel innov8 · BizLabs · Y Combinator · SPIDER CAPITAL · svb Silicon Valley Bank



Stay Ahead of the Next Threat

REQUEST YOUR DEMO NOW!

Experience the power of predictive security with Cyble.