CYBLE

TELECOMMUNICATIONS SECTOR

THREAT LANDSCAPE REPORT 2025

TABLE OF CONTENT

Executive Summary

Cyble's sectoral threat landscape report brings to light specific threat activities targeting the Telecommunication sector around the globe in 2025.

In 2025, the Telecommunications sector remained a high-value target for cybercriminals, ransomware operators, and hacktivist groups due to its role as critical national infrastructure and its access to high-volume subscriber data. Threat activity against telecom organizations was driven by the monetization potential of subscriber Personally Identifiable Information (PII), the strategic leverage of telecom operations in geopolitical conflicts, and the sector's frequent exposure through internet-facing infrastructure and third-party service dependencies.

Dominant ransomware groups, notably Qilin, Akira, and Play, were responsible for a significant portion of attacks, impacting major carriers like AT&T and Orange S.A. and extending deep into the technology supply chain.

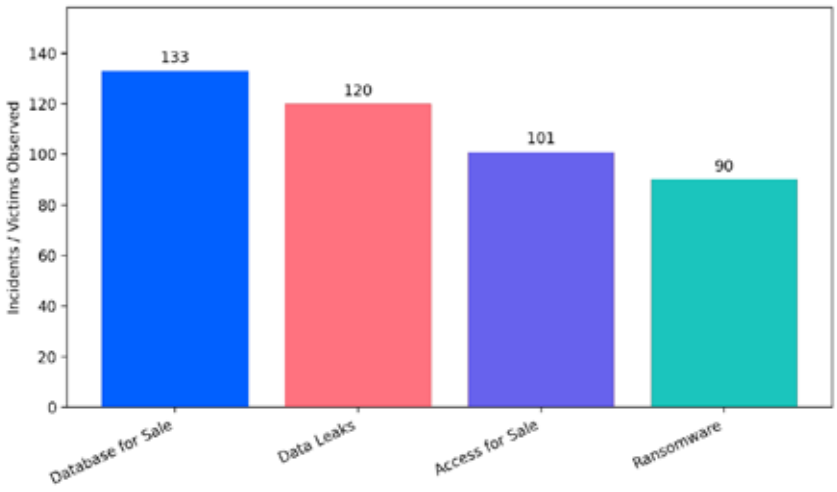
Cybercrime forums featured a continuous trade of compromised network access and extensive customer databases, with notable incidents including SIM swapping-as-a-service targeting T-Mobile customers and alleged data leaks from Telcel and Movistar. Nation-state actors, particularly the China-linked group Salt Typhoon, demonstrated a persistent threat, infiltrating telecom providers for long-term espionage by exploiting critical vulnerabilities in network-edge devices from vendors such as Cisco and Fortinet.

Geopolitically motivated hacktivism also contributed to operational disruption, exemplified by pro-Russian groups claiming successful intrusions against Ukrainian telecommunication infrastructure. To counter these threats, organizations are urged to prioritize the rapid patching of known exploited vulnerabilities and implement robust and enhanced monitoring of critical enterprise gateways and networks.

Key Highlights

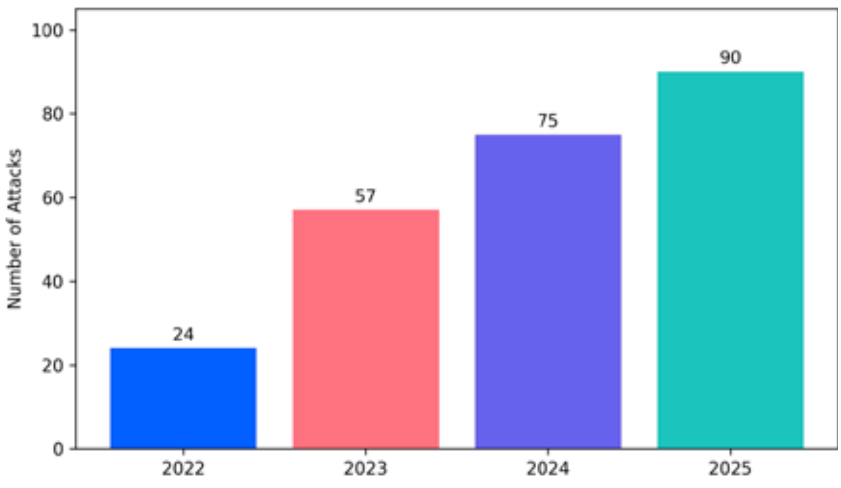
444 Incidents

Stolen telecom data and access continue to circulate as tradeable commodities.



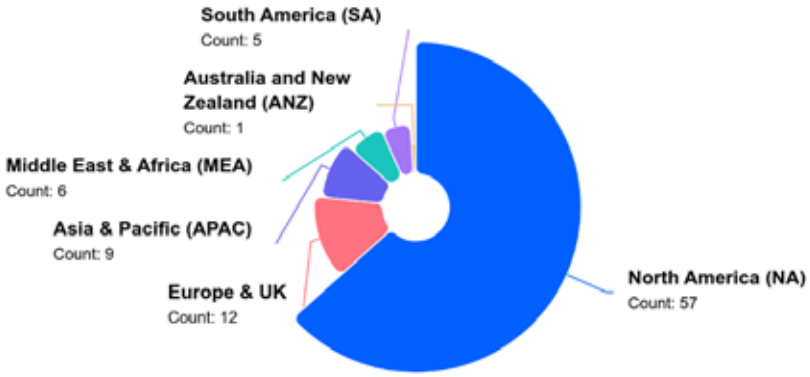
4X

Ransomware attacks have grown four-fold in last four years.



69%

7 out of 10 ransomware attacks were targeted towards Americas.



CVE-2025-0282/0283

Ivanti bugs exploited widely in multiple Telecom attacks.

Key Takeaways

01 Sustained nation-state espionage, exemplified by the Salt Typhoon campaign, targeted global telecommunication providers for long-term network persistence and surveillance, compromising hundreds of companies to steal sensitive call records.

02 The sector faced relentless pressure from ransomware, with a few highly active groups like Qilin and Akira responsible for nearly 40% of the 90 observed attacks, targeting not just major carriers but the entire technology and infrastructure supply chain.

03 A diverse underground economy thrived on monetizing compromised telecommunication assets, featuring a fragmented market of threat actors selling network access, specialized services like SIM swapping, and massive customer databases from major international providers.

04 Geopolitically motivated hacktivism resulted in widespread operational disruptions, with various groups employing Distributed Denial-of-Service (DDoS) attacks, website defacements, and data leaks to target telecommunication infrastructure as part of broader ideological campaigns.

Ransomware Attacks

CRIL observed 90 ransomware attacks targeting the global Telecommunication sector in 2025, indicating a significant and sustained threat to the industry. The year was characterized by a diverse range of threat actors, with 34 distinct ransomware groups identified.

Fig 1. Telecommunications sector ransomware attacks heatmap

Ransomware attacks aimed at the Telecom sector have grown four-fold since 2021. This high volume of attacks shows the sector's appeal to cybercriminals, which is likely due to factors like its critical infrastructure role, ease of espionage once compromised, and the vast amounts of sensitive data it manages.

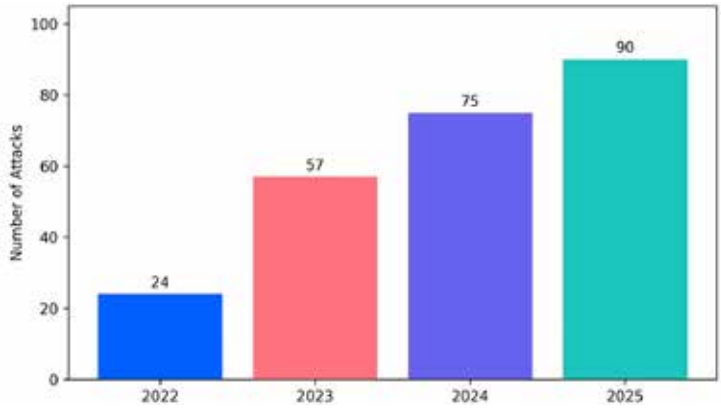


Fig 2. Ransomware attacks in Telecom sector Y-o-Y distribution

Owing to the U.S. (47), Americas topped the list of the most attacked region around the globe. Multiple telecom companies including Verizon, AT&T and Lumen Technologies had already reported breaches in the lead-up to the U.S. elections in the last quarter of 2024. But opportunistic actors even forced monetization of the data that was likely siphoned during these attacks that included hordes of customer PII.

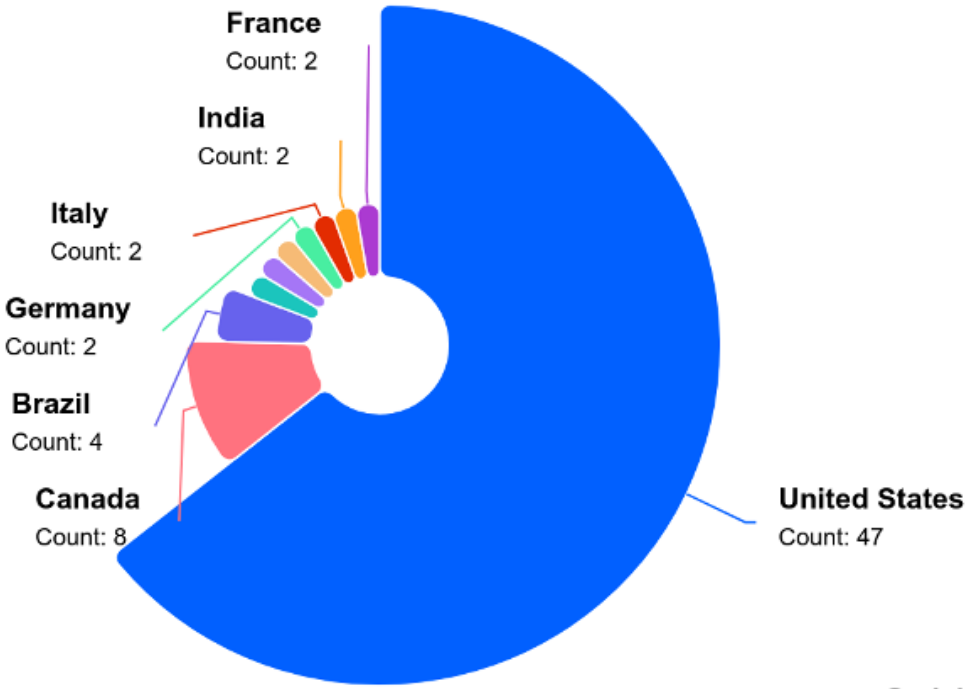


Fig 3. Country-wise targeting of Telecommunications Sector

Dominant Groups

A small number of highly active groups were responsible for the major share of the incidents. The top three most prolific groups—Qilin, Akira, and Play—collectively accounted for 35 out of the 90 attacks, representing nearly 39% of all observed activity.

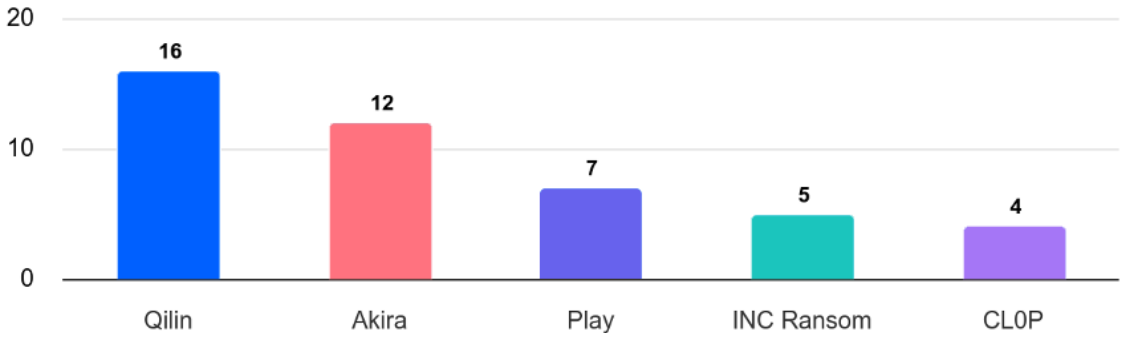


Fig 4. Most active ransomware groups targeting telecommunications sector

Qilin was the most dominant, with 16 recorded incidents, demonstrating a persistent focus on the telecommunications vertical. While U.S. was its primary target, The group spread its attack surface across Europe and Asia by targeting entities in Germany, the UK, Malaysia and Taiwan.

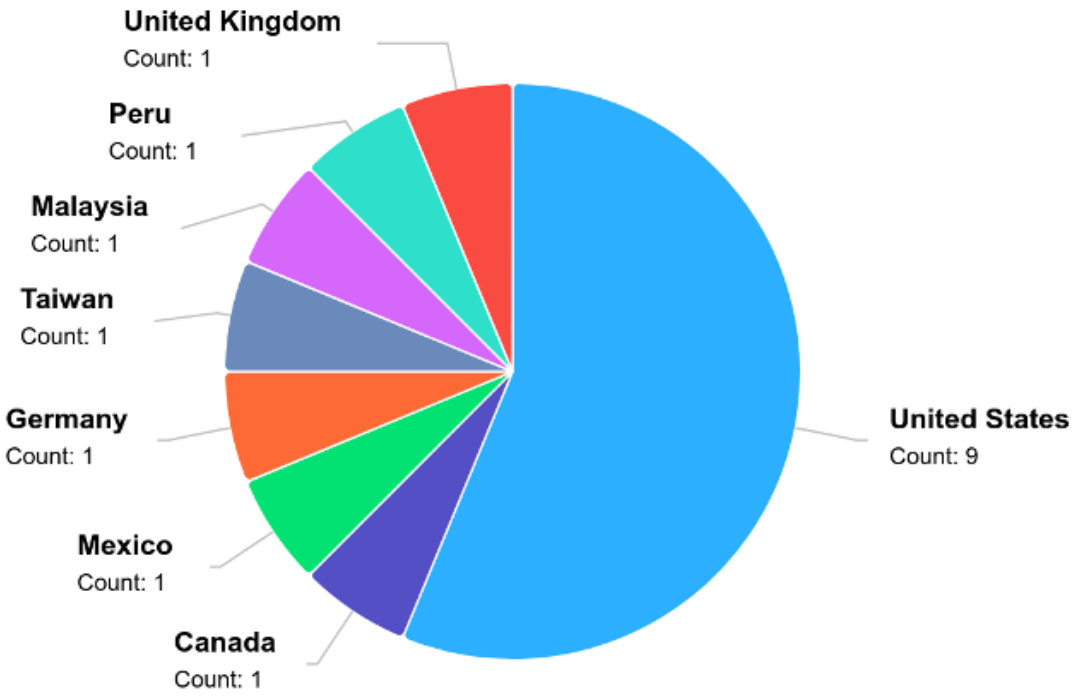


Fig 5. Country-wise targeting of Qilin ransomware group

Akira followed Qilin with 12 attacks, while the Play ransomware group was linked to 7 incidents. Other significantly active groups included INC Ransom with five attacks, and a subsequent tier of groups including Lynx, CL0P, SafePay, and Dragonforce, each responsible for four attacks. This concentration indicates that while the overall ecosystem is fragmented, a few key players pose the most consistent threat.

Impact Analysis

The attacks impacted a wide spectrum of organizations within the telecommunications ecosystem, from multinational carriers to regional service providers and critical technology suppliers. Major industry players such as Orange S.A., and AT&T Carriers were among the high-profile victims, highlighting the threat to core telecommunication services.

While core telecom service providers remained the prime focus for threat actors, those providing Internet infrastructure (15) and manufacturing communications equipment (11) were also targeted.

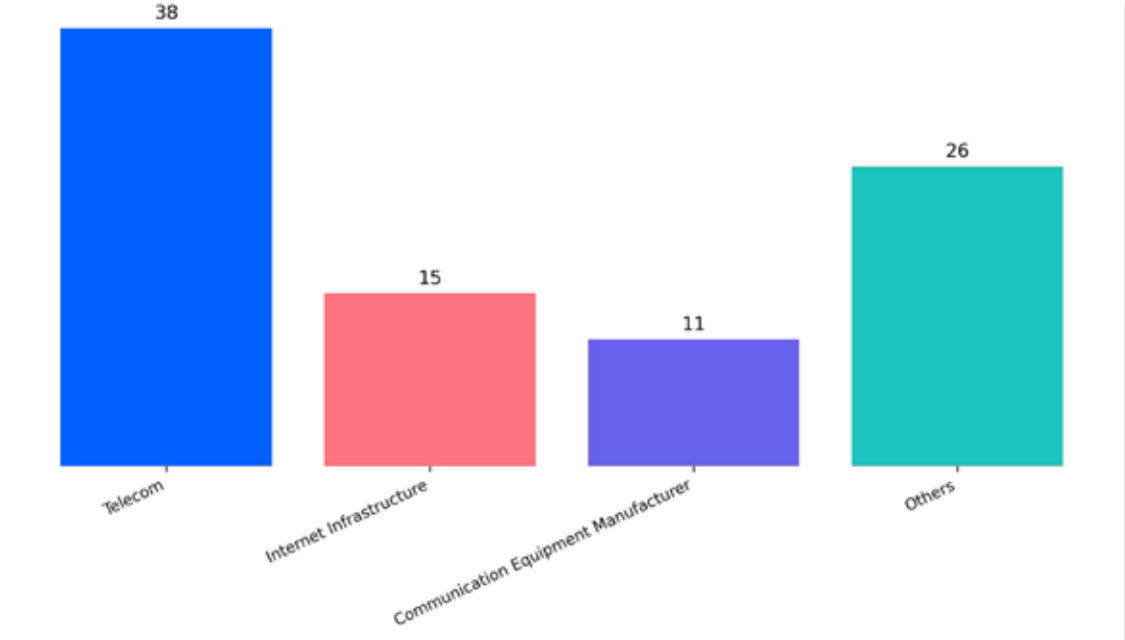


Fig 6. Sub-sectoral breakdown of ransomware attacks on telecommunications sector

The breadth of victims reveals a strategy by ransomware groups to disrupt operations across the entire vertical.

Notable Trends

Throughout 2025, a key trend was the persistent, year-long campaigns conducted by the most active groups. Qilin, for example, maintained a consistent operational tempo with attacks recorded in nearly every quarter.

A particularly noteworthy incident involved a west shore-based telecom company, which appeared on the leak sites of both INC Ransom and Qilin in September 2025. This instance of double victimization in the same month shows the severe and relentless pressure faced by organizations in this sector. Furthermore, the appearance of a single attack by the historically prominent LockBit group in late December may suggest residual activity from its affiliates following earlier law enforcement disruptions.

The ransomware landscape for the telecommunications sector in 2025 was defined by concentrated aggression from a few dominant groups, particularly Qilin and Akira, who executed sustained campaigns. The threat was not limited to major carriers but extended deep into the supply chain, impacting technology vendors, infrastructure providers, and regional operators.

The persistent nature of these attacks, coupled with instances of multiple groups targeting the same victim, signals a highly opportunistic and hostile environment, making robust cybersecurity defenses a critical priority for all organizations within the sector.

Notable Incidents

Orange Telecom Confirms Targeted Attack on "Information Systems"

French telecom giant Orange issued red alert as it responds to a cyberattack targeting its "information systems." Certain services and platforms, of both corporate and regular consumers, facing disruptions due to ongoing response. Orange first detected the cyberattack on Friday, July 25, when its security team saw intrusion on one of its information systems.

The telecom provider dialed in its Orange Cyberdefense team who sprung in action "to isolate the potentially affected services and limit the impacts," Orange said in a press statement. "However, these isolation operations resulted in the disruption of certain services and management platforms for some of our corporate customers and some consumer services, primarily in France," it added.

Read more: Telecom Giant Orange Responding to Cyberattack on 'Information Systems'

FBI Decoding China-links to US Telecoms' Breach

The FBI has issued a public appeal for information concerning an ongoing cyber campaign targeting US telecommunications infrastructure, attributed to actors affiliated with the People's Republic of China (PRC). This cyber operation, tracked under the moniker Salt Typhoon, compromised networks at multiple US telecommunications companies and resulted in the theft of sensitive data.

Read more: Salt Typhoon Cyberattack: FBI Investigates PRC-linked Breach of US Telecoms

SK Telecom Breach Shakes Consumer Trust

SK Group Chairman Chey Tae-won issued a public apology at the SK Telecom headquarters, following a SK Telecom cyberattack that affected millions of users. The cyberattack, which came to light in April, raised concerns over data security, especially among SK Telecom's 24 million customers. The data breach, which involved the suspected leakage of SIM card-related data due to malware planted by hackers, has not resulted in confirmed secondary damage, as of yet.

Read more: A Breach, an Apology, and a Pledge to Change: SK Chairman Breaks Silence on Telecom Cyberattack

U.S. Telecom, Zero-Day Attacks Call for Better Cyber Hygiene

As China-backed threat groups have been linked to recent attacks on telecom networks, the U.S. Treasury and other high-value targets, one issue has become increasingly clear: Good cyber hygiene could have limited damage from many of the attacks. Organizations have little in the way of defenses against advanced persistent threats (APTs) exploiting unknown zero-day vulnerabilities – at least until there's an available patch – but they can make it harder for those threat actors to move laterally once inside their network.

Read more: U.S. Telecom, Zero-Day Attacks Show Need for Cybersecurity Hygiene

Initial Accesses on Sale

Analysis of the compromised access market targeting the telecommunication sector shows that the threat actors ‘h4tr3dw0rld’ and ‘alpha-wmr’ were the most prolific sellers by post volume. These two actors, along with ‘yrrrr’ and ‘psych1c’, were collectively responsible for nearly 25% of all identified access listings.

Despite this concentration of activity among the top sellers, the market remains highly fragmented. The overall landscape is characterized by a significant long tail of threat actors observed posting only once, indicating a broad and opportunistic marketplace with a low barrier to entry for selling compromised network accesses.

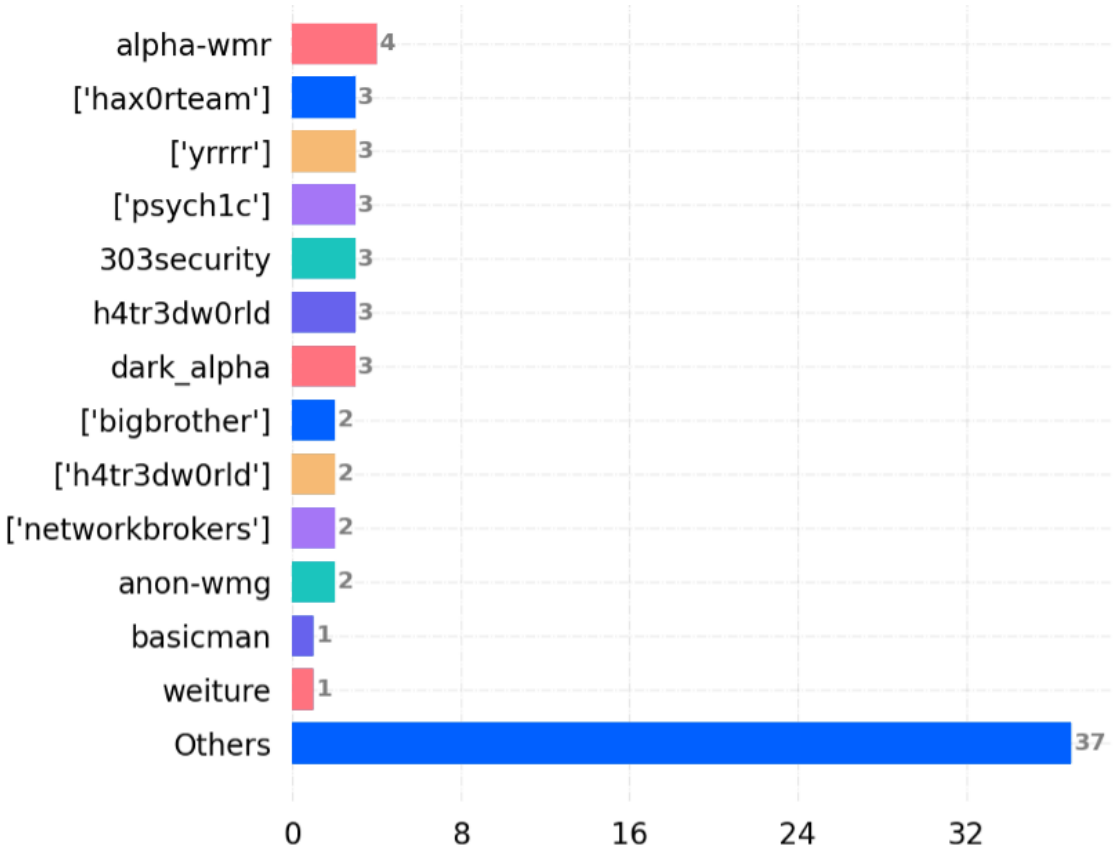


Fig 7: Active threat actors selling compromised access

Notable Accesses on Sale

Alleged Turkish Telecom Vulnerability for Sale on Cybercrime Forum

In early August 2025, the threat actor 'masterseller' advertised a critical vulnerability allegedly impacting a Turkish Telecom provider on the nuovo BreachForums. The actor claimed the exploit allowed complete takeover of a customer's account using only their phone number by leveraging a refresh token to generate unlimited access tokens.

This persistent, unauthorized access could allegedly expose a wide range of personal information, including full names, national ID numbers, addresses, and modem details, and allow an attacker to view internet records and change modem passwords. The threat actor offered details of the vulnerability for US$10,000, but a provided link meant to serve as evidence was inaccessible, leaving the claims unconfirmed.

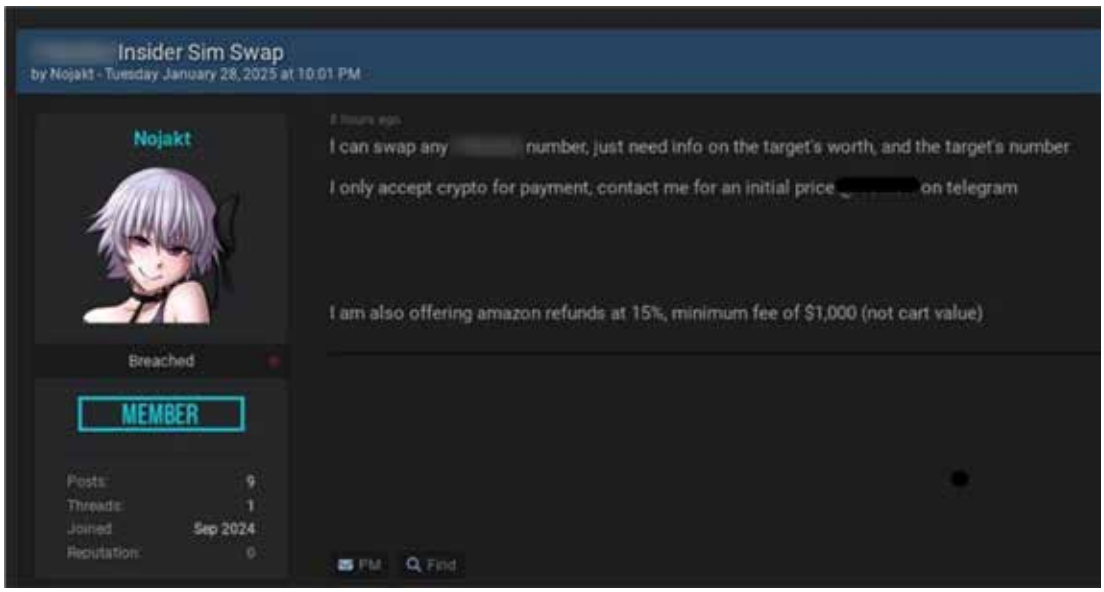
KillNet Affiliate UserSec Claims Breach of Ukrainian Telecom Infrastructure

In mid-June 2025, the pro-Russian hacktivist group UserSec, an affiliate of KillNet, claimed responsibility for a large-scale cyber operation against a Ukrainian telecommunications provider. The group alleged that it had scanned over 400,000 IP addresses, uncovering the company's backend infrastructure by bypassing Web Application Firewall (WAF) protections and capturing FTP access credentials.

To support its claims, UserSec published screenshots as visual evidence, which appeared to show direct access to administrative interfaces, FTP uploads across multiple Ukrainian IP ranges, and access to various HTML-based control panels and backend systems on non-standard ports.

Threat Actor Advertises SIM Swapping as a Service

In late January 2025, the threat actor 'Nojakt' advertised a SIM swapping service on BreachForums, specifically targeting subscribers of the US-based telecommunications company. The actor claimed to require only the victim's phone number to perform the swap, suggesting they may possess unauthorized access to an internal portal or are leveraging an insider threat. The service was offered for a percentage of the buyer's earnings, indicating its intended use in financially motivated attacks such as account takeovers.



Threat Actor Sells Alleged Mail Access to Major UK ISP

In early May 2025, threat actor Anon-WMG advertised the sale of unauthorized mail access for a UK-based internet service provider on the Russian-language Exploit forum. The actor claimed the access, priced at US$1,100, would allow a buyer to read the account's inbox and send emails. The victim was not explicitly named. The threat actor did not supply proof to validate their claims, leaving the alleged compromise unconfirmed at the time of reporting.

Alleged US Telecom Giant's Network Admin Access For Sale on Cybercrime Forum

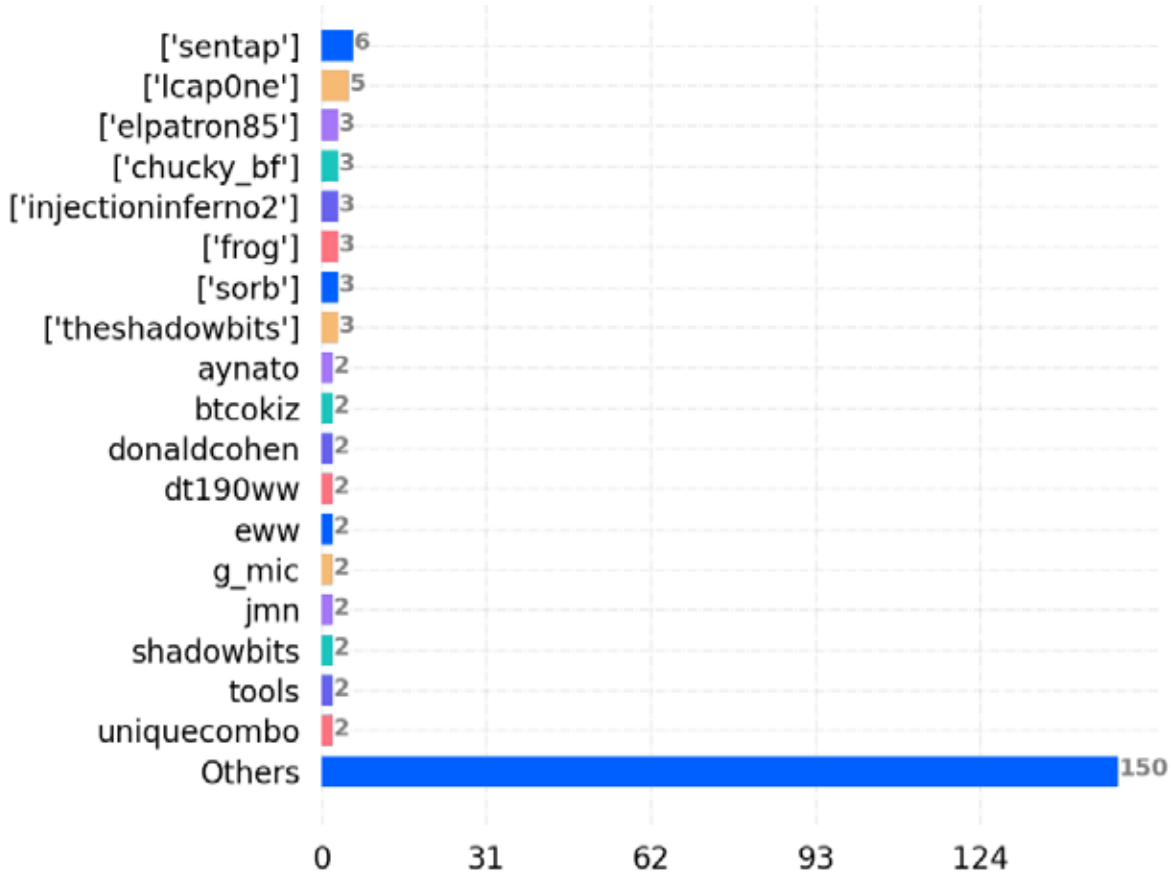
In late November 2025, the threat actor 'capton' advertised the sale of unauthorized administrative access to network infrastructure allegedly belonging to a major US telecommunications company, on the DarkForums cybercrime forum.

The threat actor claimed to be offering persistent, admin-level Secure Shell access to a Cisco IOS XE router with Full Privilege 15 administrative rights for US$4,000, requesting interested buyers to contact them privately. The claims remained unconfirmed at the time of reporting, as the threat actor did not provide any proof-of-concept to support their assertions.

Data Breaches and Leaks

An analysis of threat actor activity reveals that ‘sentap’ and ‘lcap0ne’ were the most prolific actors involved in data breaches and leaks, with six and five related posts, respectively. A secondary tier of consistently active threat actors, including ‘theshadowbits’, ‘frog’, ‘elpatron85’, and ‘injectioninferno2’, were each responsible for three posts.

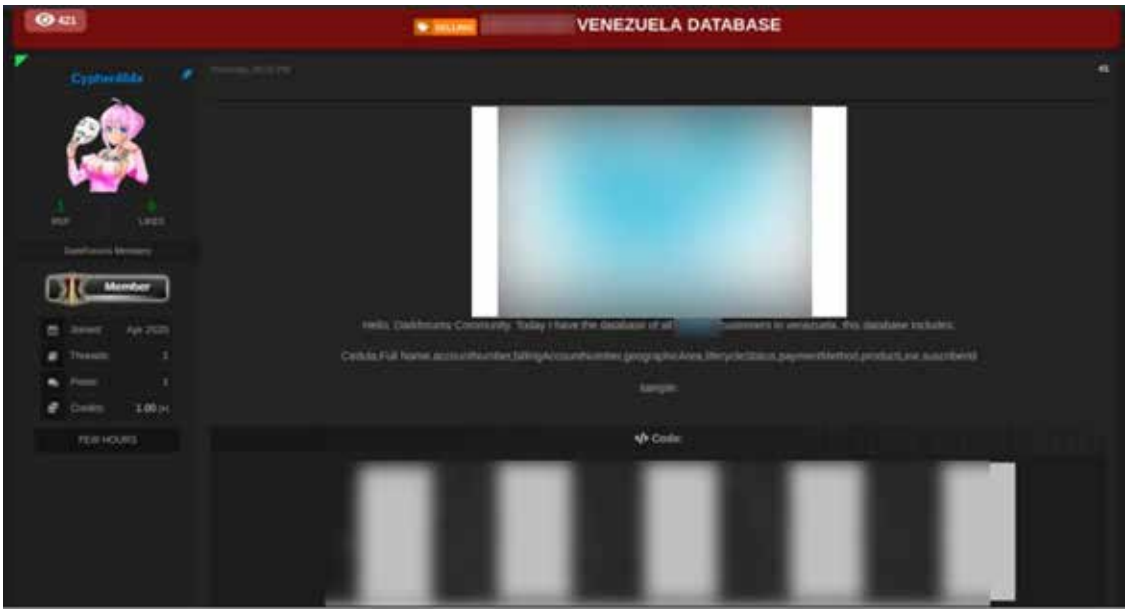
Beyond these more active entities, the overall threat landscape is highly fragmented, characterized by a long tail of numerous actors contributing only one or two posts each. This distribution suggests a dual-pronged threat environment where a small number of specialized actors drive a significant portion of high-volume breach disclosures, while a much larger, more diffuse group of opportunistic actors contributes to the broader landscape of data compromise within the telecommunications sector.



Notable Data Breaches and Leaks

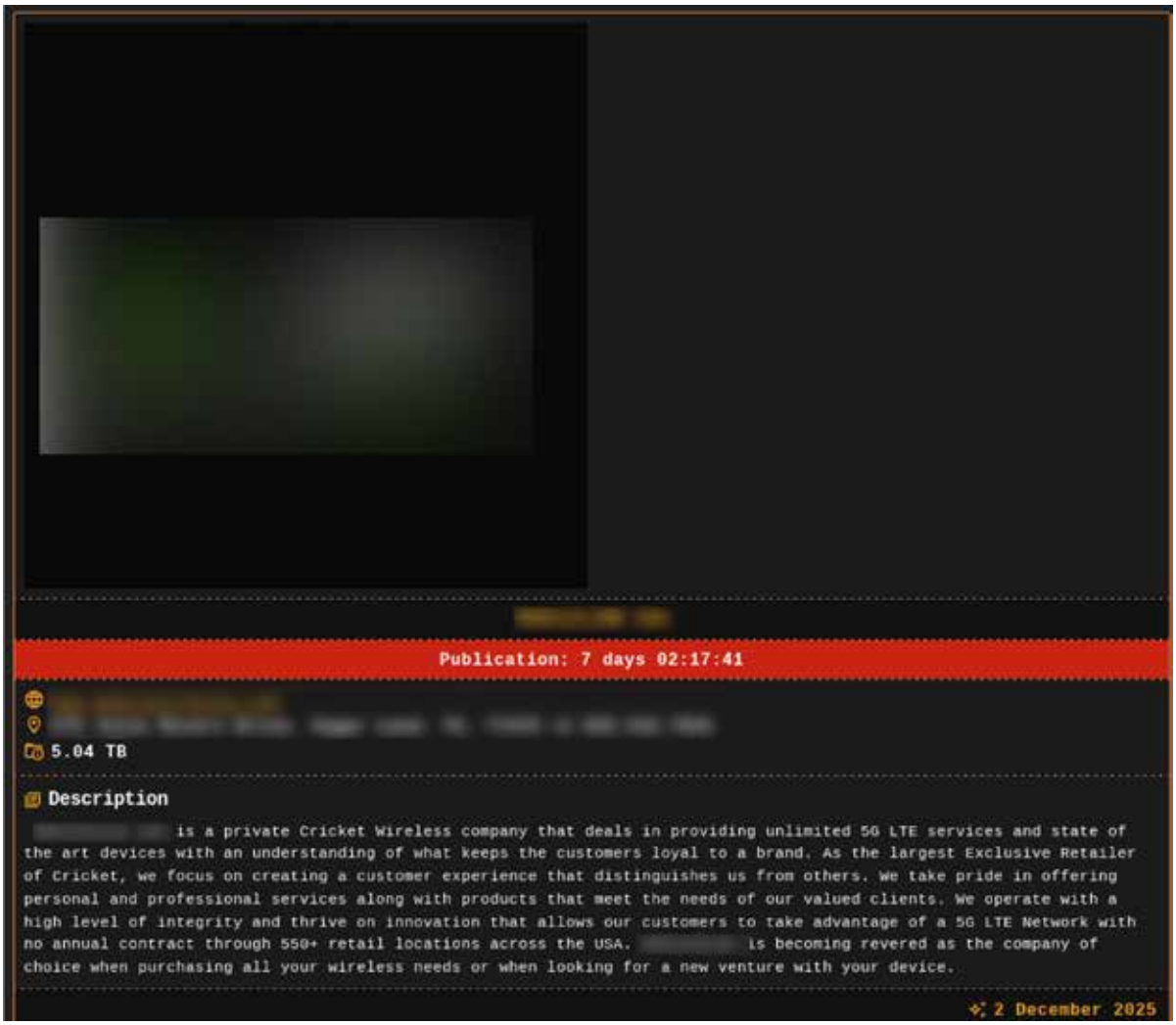
Threat Actor Puts Alleged Venezuela Customer Database Up For Sale

In April, the threat actor 'Cypher404x' advertised a database for sale on the English-language cybercrime forum, Darkforums. The actor claimed the database belongs to a major Venezuelan telecommunications provider and contained 5 million records allegedly exfiltrated the same month. The compromised data reportedly included sensitive customer information such as full names, Cedula (national ID numbers), account numbers, billing details, and geographic areas. To validate their claims, the threat actor shared sample records and invited interested buyers to negotiate a price privately.



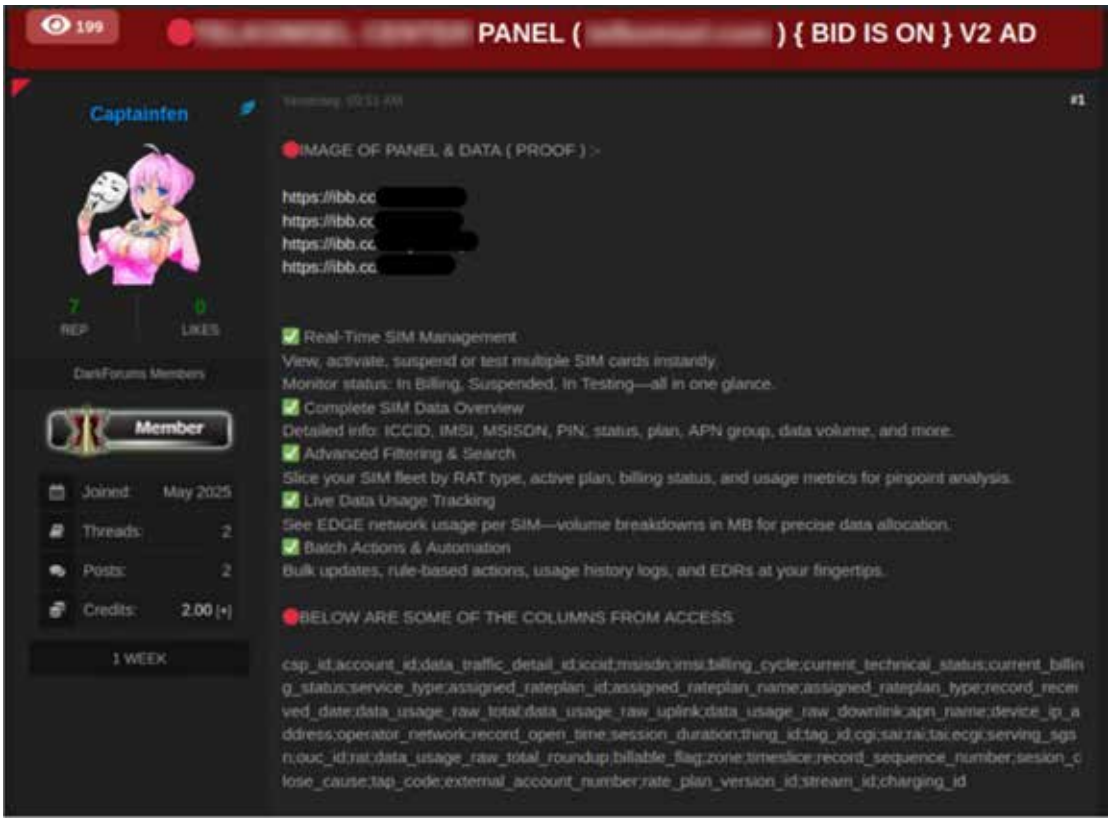
DragonForce Ransomware Claims Major Data Breach at US Mobile Service Provider

In early December 2025, the DragonForce ransomware group claimed responsibility for a cyberattack against a prominent U.S. wireless retail and telecommunications services provider. The threat actor alleged the exfiltration of 5.04 TB of company data and set a seven-day deadline before threatening a public release of the information. The group has did not provide any samples or proof to substantiate its claims, leaving the extent of the breach unverified.



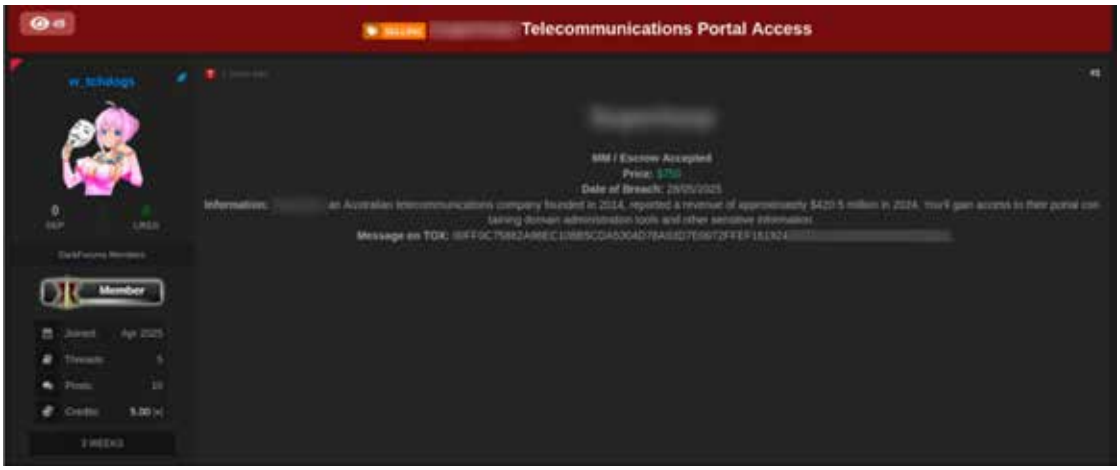
Cybercriminal Offers Alleged Access to SIM Panel

In June, the threat actor Captainfen advertised the sale of alleged unauthorized access to a SIM management panel belonging to an Indonesian telecommunications operator on the DarkForums cybercrime forum. The actor claimed the compromised panel provides real-time control over SIM cards, including the ability to view, activate, suspend, and monitor their status. Furthermore, the access allegedly exposes detailed SIM data such as ICCID, IMSI, MSISDN, plan details, APN group, and data usage. To substantiate their claims, Captainfen provided screenshots of the panel and a database header purportedly obtained through the illicit access.



Threat Actor Sells Alleged Access to Australian Telecom Company

In May 28, 2025, the threat actor 'w_tchdogs' advertised the sale of unauthorized access to an Australian telecommunications company. The post, made on the English-language cybercrime forum Darkforums, claimed the company was breached and offered access to a portal for US$750. According to the threat actor, this portal provides access to domain administration tools and other critical network information.



Critical Vulnerabilities observed as Zero days and CISA KEV

Known Exploited Vulnerabilities

The 2025 threat landscape was defined by a significant volume of critical, industry-agnostic, and region-agnostic vulnerabilities, with a substantial number of CVEs scoring 9.0 or higher, indicating a trend toward highly severe security flaws. Analysis of the CISA Known Exploited Vulnerabilities (KEV) catalog reveals a persistent focus by threat actors on internet-facing devices and enterprise software.

Fig 8: CISA KEV catalog-based Vulnerability Mapping

Vendors such as Fortinet, Microsoft, Apple, and Cisco appeared frequently, with multiple critical vulnerabilities in their respective product lines, including FortiOS, Office, macOS, and security appliances. The targeted products often included network security devices like VPN gateways and firewalls, as well as widely used enterprise platforms for collaboration and business analytics, underscoring their high value to attackers for gaining initial access and lateral movement.

Several vulnerabilities garnered significant attention due to active exploitation, including those in Fortinet devices (CVE-2025-59718), Cisco security products (CVE-2025-20333), and Oracle's E-Business Suite (CVE-2025-61882), which was leveraged in widespread extortion campaigns. The consistent addition of such vulnerabilities to the KEV catalog throughout the year highlights the urgency for rapid patching, as threat actors demonstrated the capability to quickly weaponize newly disclosed flaws.

The recurrence of critical vulnerabilities in similar product categories from the same vendors points to systemic weaknesses and the persistent interest of attackers in these targets. To mitigate these threats, organizations are strongly advised to prioritize patching of KEV-listed vulnerabilities, implement network segmentation to limit attack surfaces, and enhance monitoring of perimeter devices and critical enterprise applications.

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-2025-59374	Live Update Client	Asus	9.8
CVE-2025-20393	Secure Email	Cisco	10
CVE-2025-14733	Fireware Os	Watchguard	9.8

Zero-Day Vulnerabilities

The 2025 threat landscape was defined by a significant number of critical, industry-agnostic, and region-agnostic zero-day vulnerabilities, with a notable concentration of CVSS scores above 9.0.

A recurring trend was the targeting of edge network devices and enterprise software, with vendors like Apple, Fortinet, and Ivanti repeatedly featured. The active exploitation of these flaws underscores intense threat actor interest in gaining initial access to corporate networks through widely used products such as VPN gateways, mobile operating systems, and enterprise platforms.

The frequency of zero-days in these categories highlights systemic weaknesses that attackers are quick to weaponize. Consequently, organizations must move beyond periodic patching and adopt a more proactive security posture, emphasizing rapid patch deployment, robust network segmentation to limit lateral movement, and continuous monitoring to detect anomalous activity.

Table showing zero-days exploited in 2025 by threat actors against the Telecom sector:

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-2024-58136	Yii2	Yii2	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-2025-53690	Experience Manager	Sitecore	9.0
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-2025-14611	Centrestack	Gladinet	9.8
CVE-2025-20393	Secure Email	Cisco	10.0
CVE-2025-14733	Fireware Os	Watchguard	9.8

Hacktivism

During the 2025 period, the hacktivism landscape was characterized by high-volume, geopolitically and ideologically motivated campaigns. A diverse array of threat groups and channels, including 'Save Palestina 🇮🇹', 'GANOSECTEAM PALESTINA', 'SOLDADOS DIGITALES - UNIÓN AMERICANA', and 'MINIONS CYBER CRIME HACKTIVIST', were prominent in orchestrating these operations.

The primary tactics employed included disruptive Distributed Denial-of-Service (DDoS) attacks, widespread website defacements, and a significant volume of data exposure events, with **CRIL observing approximately 3,461 data leak and dump posts.** These campaigns were extensive in scale, impacting over 20,600 unique domains across a broad spectrum of industries. Targets ranged from Government and Law Enforcement agencies to Technology, BFSI, and critical Telecommunication infrastructure, including VoIP and SIP service domains.

KREMLIN BR GROUP < HACKING TOOLS AND COURSE FREE />

The Portuguese-language channel **'KREMLIN BR GROUP'** functions as a marketplace for cybercrime tools, services, and stolen data, indicating a financial motivation rather than a hacktivist agenda. The group does not claim responsibility for any specific attacks but instead advertises a range of illicit goods for sale. These include malware such as info-stealers, Android RATs, and ransomware; tools for financial fraud like phishing kits ('Telas Fakes') and credit card information ('InfoCCs'); and services like email/SMS spamming and access to panels for querying personal information. The channel also offers "blackhat" hacking courses and sells compromised data, as seen in a January 2025 post advertising a database of Hotmail, Outlook, and Live email accounts, which included a sample of compromised credentials belonging to a user in Brazil. While the channel name references free tools and courses, its primary focus is the commercial sale of cybercriminal products.

SOLDADOS DIGITALES - UNIÓN AMERICANA

Based on the provided channel content, 'SOLDADOS DIGITALES - UNIÓN AMERICANA' did not claim responsibility for disruptive cyberattacks such as DDoS, data breaches, or website defacements during the specified period. Instead, the group's primary activity consisted of information operations focused on disseminating geopolitical narratives and conspiracy theories. The channel frequently reposted content from Russian state-affiliated media outlets, including Sputnik Mundo and RT, alongside extensive posts detailing QAnon-adjacent themes.

These narratives centered on a covert global military operation led by Donald Trump against a “Deep State” or “Cabal,” an impending global financial reset (GCR/QFS), and the activation of programs like NESARA/GESARA. The group’s stated motivation is to support Donald Trump and inform followers of a “silent war” to restore a global republic, indicating a clear ideological and political alignment rather than a focus on technical cyber intrusions.

Ghost Princess™

During the observation period, the '*Ghost Princess*' channel operated primarily as an information operations platform with a stated pro-Palestinian motivation, framing its activities as a response to an ongoing “genocide” in Gaza. The channel’s main function was the curation and dissemination of “News Bulletins,” casualty reports, and graphic content from the conflict zone to shape a specific narrative critical of Israel, the United States, and their allies. In addition to these narrative operations, the channel served as an aggregator for cyberattacks claimed by associated hacktivist entities such as ‘Op Israel Hackers,’ ‘RuskiNet,’ and ‘AnonGhost.’

These claimed activities primarily consisted of website defacements and DDoS attacks targeting Israeli commercial, defense, and infrastructure entities, including the national water company Mekorot. Notably, the channel also amplified DDoS attacks and data breaches against Egyptian targets, such as the National Telecommunication Institute (nti.sci.eg) and various banks, explicitly to exert pressure to open the Rafah border crossing. The channel’s content also included geopolitical commentary relevant to the report’s scope, such as highlighting a reported weapons deal between the Israeli defense firm Elbit Systems and Albania.

Industry Insights and Analysis

Mitel MiCollab VoIP Software: Zero-Day Vulnerability Alert

The article discusses a zero-day vulnerability in the Mitel MiCollab VoIP software, which is being actively exploited by threat actors. The vulnerability poses a significant risk as it allows attackers to gain unauthorized access to systems. The threat group known as Salt Typhoon, attributed to China's foreign intelligence service, has been breaching U.S. telecommunications firms' networks, including Verizon, AT&T, and Lumen. The attackers have been targeting sensitive information and high-value targets for surveillance. The U.S. government has issued warnings about ongoing compromises to communications and the need for companies to address cybersecurity gaps. The threat group has also breached telecommunication networks in dozens of countries worldwide, highlighting the global impact of the cyber attacks.

Salt Typhoon hackers exploited stolen credentials and a 7-year-old software flaw in Cisco systems

The article discusses how the threat actor group known as Salt Typhoon, a Chinese hacking collective, exploited stolen credentials and a 7-year-old software flaw in Cisco systems. They have targeted telecom providers in the U.S. and overseas by leveraging vulnerabilities in communications infrastructure. This cyber attack highlights the ongoing threat posed by sophisticated threat actors to critical industries like telecommunications.

AT&T Confirms Data Breach Affecting Nearly All Wireless Customers

The article discusses a major data breach affecting AT&T's wireless customers where threat actors accessed call records and text interactions. The threat actors managed to exfiltrate files containing customer call and text data, potentially compromising customer privacy. The breach involved a third-party cloud platform and impacted various MVNOs using AT&T's network. The attackers demanded a ransom from AT&T, which was reportedly paid in cryptocurrency. The malicious cyber campaign targeting Snowflake involved a financially motivated threat actor group named UNC5537. The fallout from the cybercrime spree is expanding, with law enforcement agencies investigating the incident. The breach highlights the importance of implementing robust security measures to protect customer data and prevent future attacks.

Three-Year Intrusion: SK Telecom Breach Exposes 27 Million User Records

A three-year intrusion at SK Telecom compromised 27 million user records, including sensitive information like IMSI numbers, USIM authentication keys, and text messages. The breach was detected in April 2025, with attackers maintaining a covert presence within the infrastructure for as long as three years. The attackers implanted backdoors tailored to different malicious functions and were able to exfiltrate data without detection. The breach affected 26.95 million SK Telecom users, leading to the suspension of new customer onboarding and the issuance of replacement SIM cards with enhanced security measures.

Salt Typhoon likely to remain in US telco networks forever, experts say

The article discusses how multiple U.S. telecommunications providers have been compromised by the Chinese state-backed threat group Salt Typhoon. Experts believe that the threat posed by Salt Typhoon is likely to remain in the networks of these providers indefinitely. The challenges in expunging the threat stem from the complexities of modern telecommunications networks and their identity solutions, as well as inadequate cybersecurity measures. The founder of Nemesis Global, Gentry Lane, emphasized the importance of early identification in combating such threats. The lack of sufficient indicators of compromise for Salt Typhoon has made it difficult for threat hunters to effectively detect and remove the malicious activity. Overall, the article highlights the persistent and challenging nature of the cyber threat posed by Salt Typhoon to U.S. telco networks.

Bouygues Telecom Data Breach Exposes 6.4 Million Customer Records

Bouygues Telecom, one of France's largest telecom providers, experienced a cyber-attack resulting in the exposure of personal data of 6.4 million customers. The compromised data included contact details, contractual data, civil status details, and international bank account numbers. The attackers accessed certain personal information associated with Bouygues Telecom subscriptions. The incident was detected on August 4, and the company has taken measures to block malicious access and enhance system monitoring. The compromised customers have been notified to watch out for fraudulent emails and calls. The incident has been reported to the national data protection agency in France, CNIL, and a complaint has been filed with judicial authorities. The attack on Bouygues Telecom follows a similar cyber-attack on Orange, France's leading telecom provider, which isolated potentially impacted systems without compromising corporate or customer data. The article highlights the vulnerability of telecom providers to cyber threats, referencing a past cyber espionage campaign by the Chinese state-sponsored group Salt Typhoon targeting major US telecoms providers in late 2024.

FBI says China's Salt Typhoon hacked at least 200 US companies

The FBI has identified a Chinese-backed hacking group known as Salt Typhoon that has targeted at least 200 American companies and breached companies in 80 countries. The hackers have focused on stealing call records of senior American politicians and officials, leading to concerns about surveillance. The FBI has warned about the ongoing threat from China and provided guidance on identifying intrusions. The group primarily targets company routers to siphon sensitive network traffic.

Year-Long Nation-State Hack Hits US Telecom Ribbon Communications

Ribbon Communications, a US telecom firm, disclosed a major security breach where nation-state hackers infiltrated their systems and remained undetected for almost a year. The breach was discovered in September 2025, with evidence suggesting the initial compromise occurred in December 2024. While no 'material information' was accessed, older customer files were compromised. The incident highlights the ongoing trend of nation-state actors targeting telecom companies for espionage, aligning with campaigns like Salt Typhoon. The breach underscores the importance of preparedness among critical infrastructure providers in the face of escalating cyber threats.

FCC guts post-Salt Typhoon telco rules despite ongoing espionage risk

The article discusses the Federal Communications Commission (FCC) revoking telecom cybersecurity rules introduced after the Salt Typhoon espionage campaign, which was linked to China. The FCC scrapped the rules meant to prevent state-backed snoops from infiltrating US networks, citing voluntary cooperation from carriers as a reason for the rollback. The Salt Typhoon group had breached multiple US telecom companies, including gaining access to lawful intercept systems.

The new FCC leadership decided to remove the obligations, arguing the previous order was impractical. However, dissenting voices warn that abandoning enforceable requirements could leave the country less secure, especially with hostile states probing telecom networks.

The Electronic Privacy Information Center (EPIC) criticized the FCC's move, stating it could create a safe harbor for insecure cybersecurity practices. The FCC claims it is not stepping back from cybersecurity but adopting a more agile approach, pointing to targeted rules and a Council on National Security. The decision to rely on voluntary cooperation raises concerns about monitoring and enforcing cybersecurity practices, especially for smaller carriers. The article highlights the ongoing risk of state-sponsored cyber threats and questions whether industry goodwill alone can safeguard the nation's communications infrastructure.

Conclusion

The telecommunications sector in 2025 faced a severe and multi-faceted threat landscape characterized by a few dominant and highly impactful trends. Prolific ransomware groups, particularly Qilin, Akira, and Play, were responsible for a significant portion of attacks, systematically targeting the entire industry supply chain from major carriers to technology suppliers.

A second major threat vector was persistent nation-state espionage, exemplified by the Chinese-backed actor Salt Typhoon, which executed long-term campaigns against major US telecoms by exploiting critical vulnerabilities to steal sensitive call data. This hostile environment was further compounded by a thriving cybercrime market where threat actors sold initial network access, leaked massive customer databases from providers like SK Telecom and Bouygues Telecom, and offered specialized services such as SIM swapping.

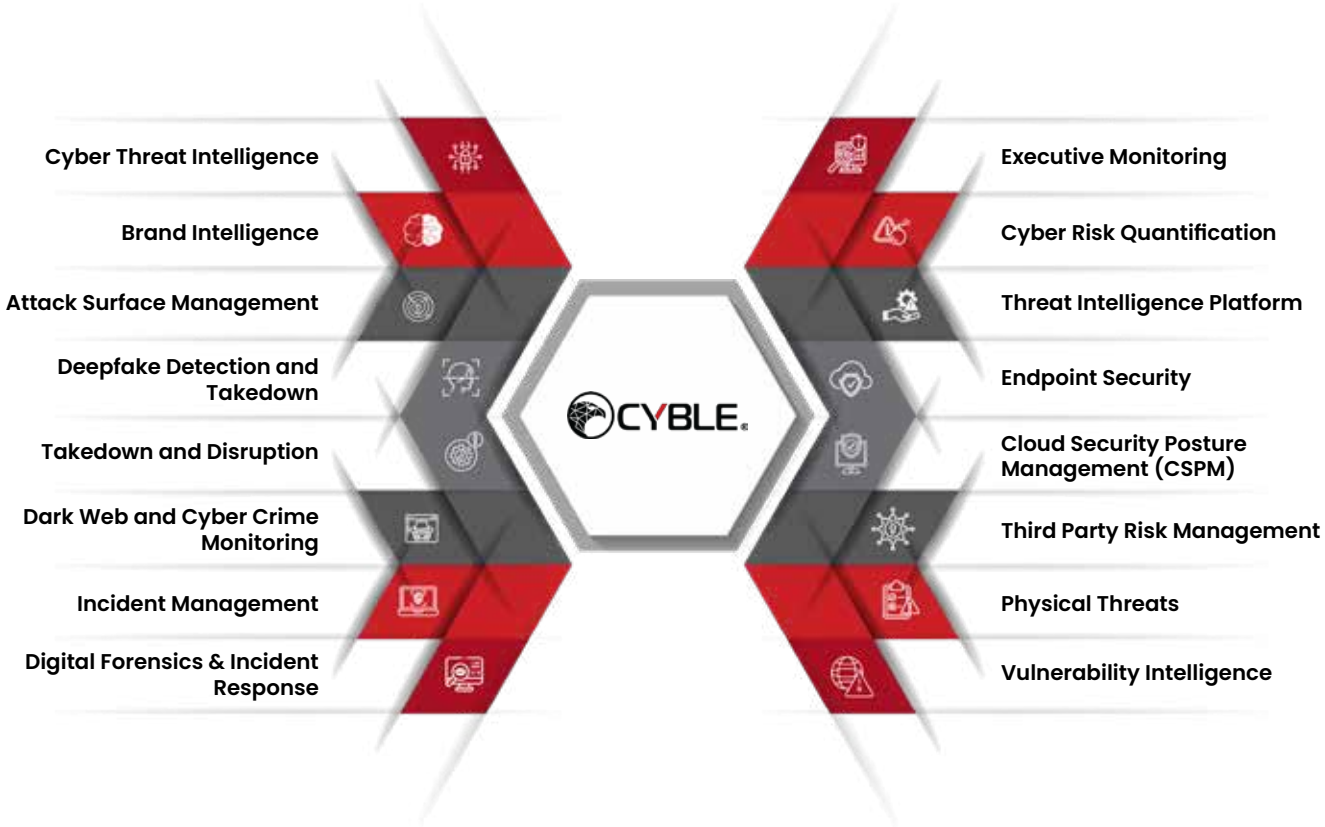
These various attacks were frequently enabled by the rapid weaponization of critical and zero-day vulnerabilities in internet-facing network equipment, while geopolitically motivated hacktivism added another layer of disruption through DDoS attacks and website defacements.

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...



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

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

Cyble Wins Three Top InfoSec Innovator 2025 Awards

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

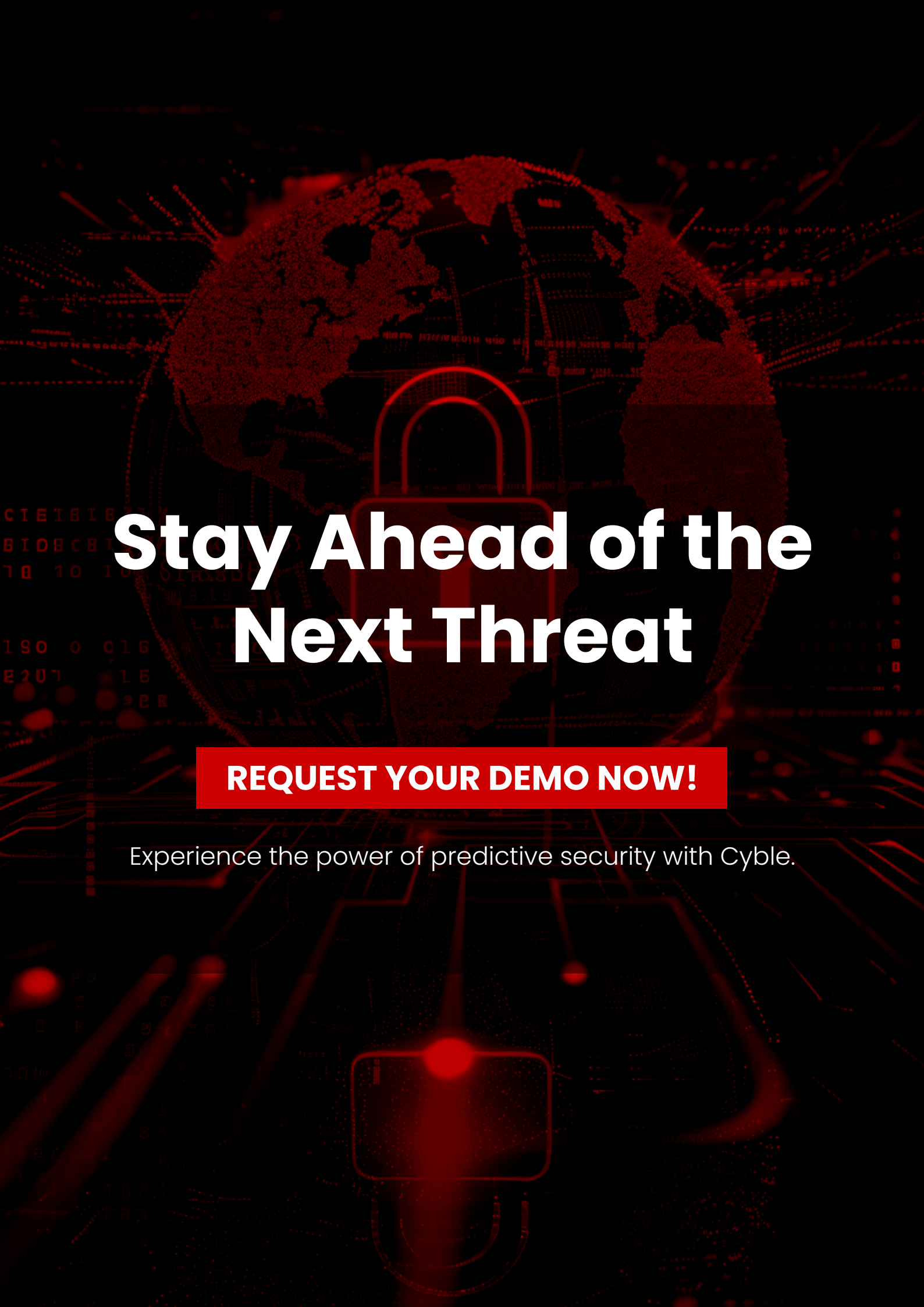
Cyble, the world's first AI-native cybersecurity company, today announced its commanding presence in the **G2 Fall 2025 Report**, earning **24 prestigious badges across 8 strategic categories**. This unprecedented recognition validates Cyble's breakthrough **Agentic AI architecture** and positions the 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 · Singtel innov8 · BizLabs · Y Combinator · SPIDER CAPITAL · svb Silicon Valley Bank

10080 North Wolfe Road, Suite SW3-200, Cupertino, CA 95014 | contact@cyble.com | +1 888 673 2067


Stay Ahead of the Next Threat
REQUEST YOUR DEMO NOW!
Experience the power of predictive security with Cyble.