H1 2026 Global Threat Landscape Report

By Cyble Research and Intelligence Labs

TABLE OF CONTENT

TABLE OF CONTENT

Executive Summary

The first half of 2026 confirms that the cyber threat landscape has entered a phase of sustained, high-tempo operations rather than episodic spikes. Cyble Research and Intelligence Labs (CRIL) tracked 3,836 ransomware attacks, 367 data breach and leak incidents, and 129 initial access listings worldwide between January and June 2026 — an operational cadence that puts real, continuous pressure on security teams across every region and sector.

Ransomware remained the most consequential threat category. A small cohort of Ransomware-as-a-Service (RaaS) operators — Qilin, Akira, Dragonforce, INC Ransom, and The Gentlemen — accounted for a disproportionate share of claimed victims, with Manufacturing, Professional Services, Construction, and Healthcare bearing the brunt. Double extortion is now the default operating model: encryption is frequently a secondary lever behind the threat of publishing exfiltrated data.

The underground economy that feeds ransomware and data-theft campaigns continues to mature. Initial access brokers such as 'sanguine' and 'dark_alpha' concentrated on Technology and Retail organizations, while data-leak brokers like 'tanaka' ran industry-agnostic operations disproportionately impacting BFSI and Government & Law Enforcement entities. This division of labor — access brokers, data brokers, and ransomware affiliates operating semi-independently — is now a structural feature of the cybercrime ecosystem rather than an anomaly.

Vulnerability exploitation remains the connective tissue between these threats. Of the 146 CVEs CRIL analyzed as part of this reporting cycle, nearly 90% were rated critical or high severity, and repeat offenders — SmarterTools, SolarWinds, Fortinet, Ivanti, and Cisco — continued to appear in both the CISA Known Exploited Vulnerabilities (KEV) catalog and active zero-day campaigns. Two zero-days in particular, affecting Ivanti Endpoint Manager Mobile and Palo Alto Networks Cloud NGFW, illustrate the continued attacker preference for network and device management platforms as an entry point into enterprise environments.

Hacktivism, meanwhile, has become difficult to separate cleanly from geopolitics or from financially motivated cybercrime. Groups operating under hacktivist branding claimed over 32,400 unique domains and approximately 9,825 data leak and dump posts worldwide, with DDoS attacks and defacements concentrated on Government, Technology, BFSI, and Healthcare targets. In several regions, channels marketed as "hacktivist" are functionally cybercrime marketplaces trading in stolen credentials, DDoS-for-hire services, and access brokerage.

The remainder of this report breaks these trends down at the worldwide level and across five regional groupings — Americas (North America and South America), Europe & UK, Asia-Pacific, Middle East & Africa, and Australia & New Zealand — before closing with forward-looking recommendations for security leaders.

Key Highlights

3,836	367	129	32,400+
Ransomware Attacks. U.S. Most Attacked.	Data Breach & Leak Incidents. BFSI was Worst Hit.	Initial Access Listings	Hacktivist-Impacted Domains

- **Ransomware operated at record scale** — 3,836 attacks globally, averaging over 630 incidents per month, with Qilin, Akira, Dragonforce, and INC Ransom as the most prolific operators and Manufacturing as the single most targeted sector.
- **Double extortion is now the baseline ransomware model.** Data exfiltration, not just encryption, is the primary leverage point used to compel ransom payment — a trend consistent across every region covered in this report.
- **A thriving initial access brokerage market** (129 listings worldwide) continues to serve as a precursor market for ransomware and espionage operations, with Technology and Retail the most frequently listed sectors.
- **Data breaches and leaks (367 incidents) disproportionately hit BFSI, followed by Government & Law Enforcement and Technology** — a pattern driven by the direct monetization value of financial data and PII.
- **Vulnerability exploitation is concentrated in a recurring set of vendors** — Ivanti, Fortinet, Cisco, SolarWinds, and SmarterTools — with nearly 90% of the 146 CVEs analyzed rated critical or high severity, underscoring the value of prioritized, risk-based patching over blanket patch cycles.
- Hacktivism and geopolitically motivated cyber activity blurred further into financially motivated cybercrime, with **over 32,400 domains and roughly 9,825 data leak posts tied to hacktivist-branded channels worldwide.**
- **Regional variation is significant.** North America and Europe/UK carry the highest absolute ransomware volumes, while Middle East & Africa and parts of Asia-Pacific show heavier concentration around a single dominant group ("The Gentlemen" in MEA, Qilin/The Gentlemen elsewhere) — a signal that regional threat models should not be treated as a single global average.

Overview

CRIL's worldwide dataset for H1 2026 spans 3,836 ransomware attacks, 367 data breach and leak incidents, and 129 initial access sale listings, layered on top of a highly active hacktivism landscape and a steady drumbeat of critical vulnerability disclosures. Read together, the data shows a threat landscape organized around a small number of highly capable, highly active actors operating at industrial scale, rather than a long tail of low-skill opportunists.

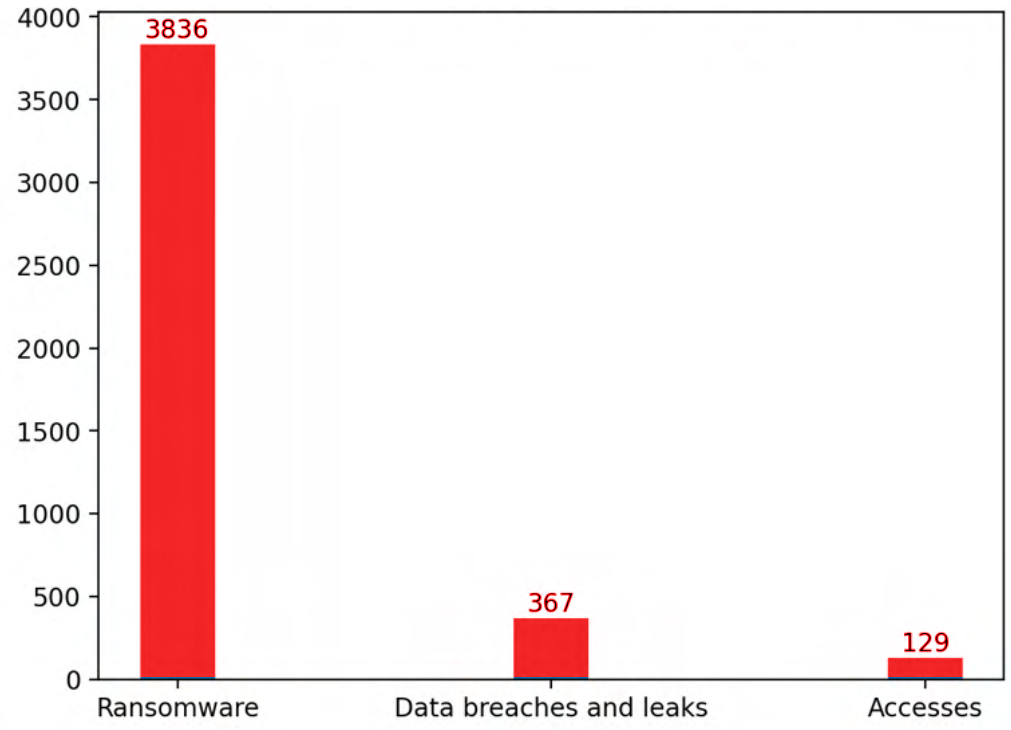


Fig 1: Worldwide Cybercrime Incidents, H1 2026

Data Breach and Leaks

Between January and June 2026, CRIL observed 367 data breach and leak incidents worldwide. These numbers have remained almost the same as compared to H1 2025 which saw 372 such incidents.

The Banking, Financial Services, and Insurance (BFSI) sector was the most heavily impacted, with 38 incidents — just over 10% of all observed breaches — followed by Government & Law Enforcement Agencies (LEA) at roughly 5.7% and Technology at approximately 4.9%.

BFSI's exposure is driven by the direct monetization value of financial data and PII; Government and Technology breaches skew more toward espionage, theft of state secrets, and acquisition of intellectual property or source code.

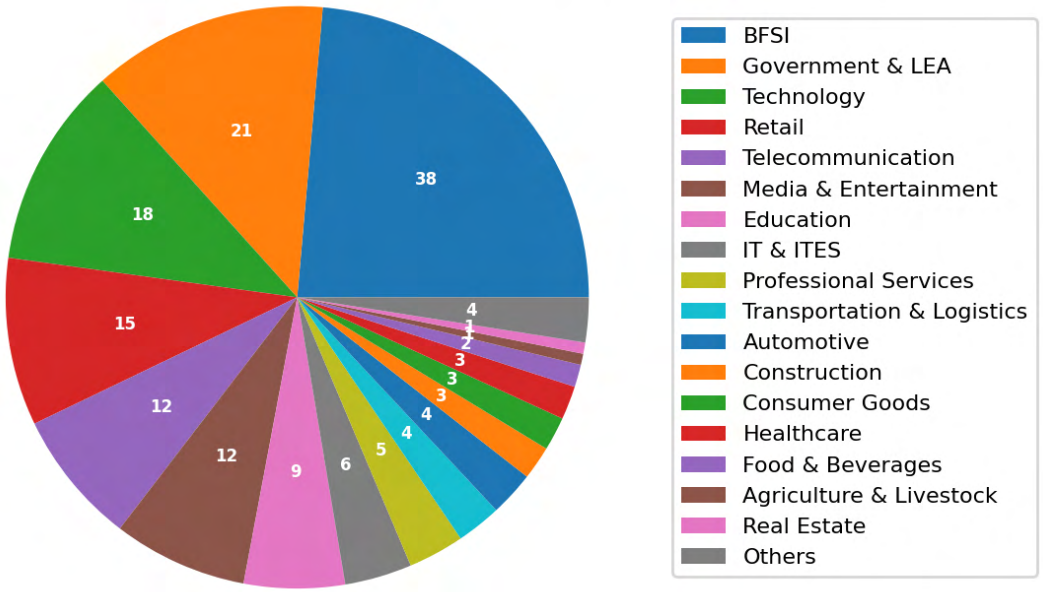


Fig 2: Worldwide Data Breaches Across Industries

The data breach and leak landscape was concentrated around a small number of highly prolific actors. ‘tanaka’ was the single most active, responsible for 25 distinct leak posts — more than double the volume of the next-most-active entities, ‘frog’ and ‘evnrnd’ (11 posts each), followed by ‘cryptix’ with 10. A long tail of dozens of opportunistic actors contributed one or two posts each, producing a broad but top-heavy ecosystem for trading and leaking compromised data.

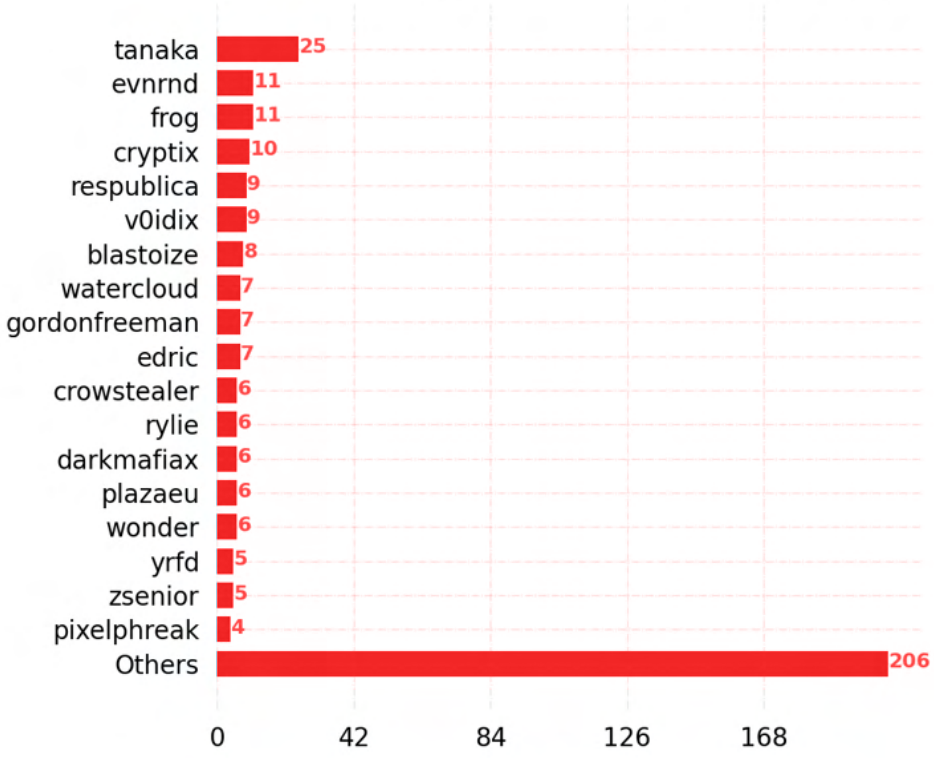


Fig 3: Most Active Threat Actors Selling Data Breaches

Targeting strategies varied by actor. ‘tanaka’ ran an industry-agnostic, global-scale operation, while newer entrants like ‘Cryptix’ focused specifically on technology and service-based industries across North America, Europe, and APAC, and ‘ResPublica’ concentrated almost exclusively on BFSI and Professional Services within the Americas — evidence that deliberate, sector-specific targeting is now coexisting with broad-spectrum campaigns.

Online Access Sale

CRIL observed 129 distinct initial access sale incidents worldwide during H1 2026. Technology and Retail were the most frequently targeted sectors, each accounting for 8 incidents, followed by Agriculture & Livestock with 6. Technology's exposure is driven by intellectual property value and supply-chain attack potential; Retail is targeted for its concentration of customer PII and payment data. Initial access remains a critical precursor to ransomware deployment and corporate espionage, and this distribution shows threat actors deliberately favoring data-rich, monetizable industries.

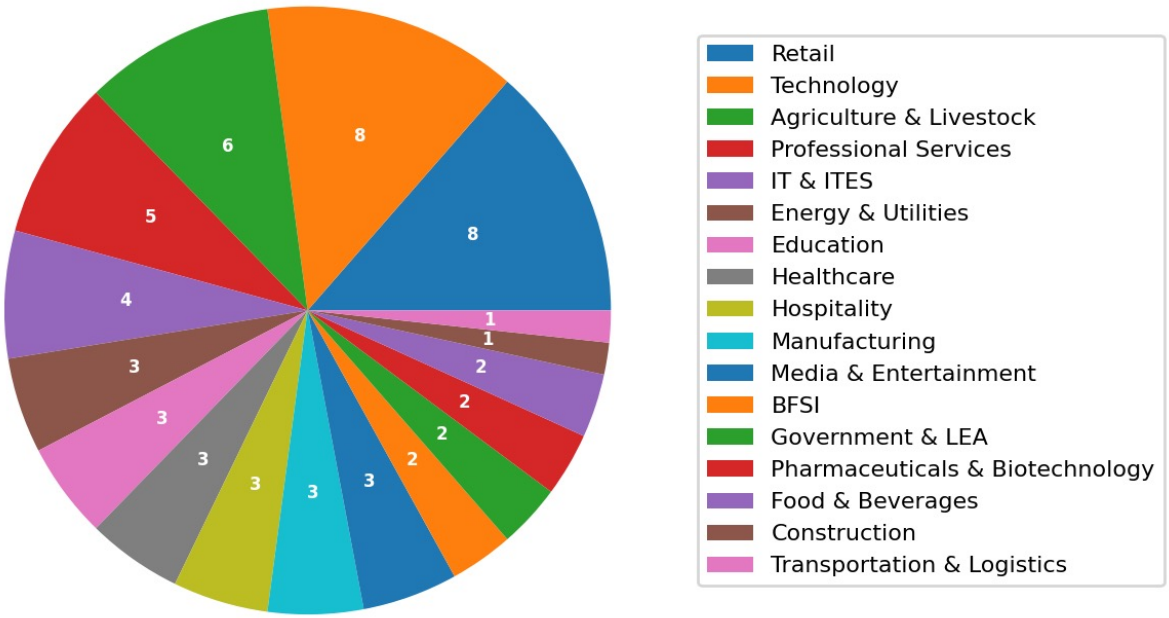


Fig 4: Compromised Accesses Across Industries

The market was led by a small cohort of highly active sellers: 'sanguine' (12 listings), 'dark_alpha' (10), and 'karuhunters' and 'redpin' (9 each) — together responsible for roughly 30% of all observed listings. Beneath this concentrated top tier, the market remains fragmented, with a long tail of sellers posting only once or twice, indicating both established brokers and opportunistic, lower-volume participants operating side by side.

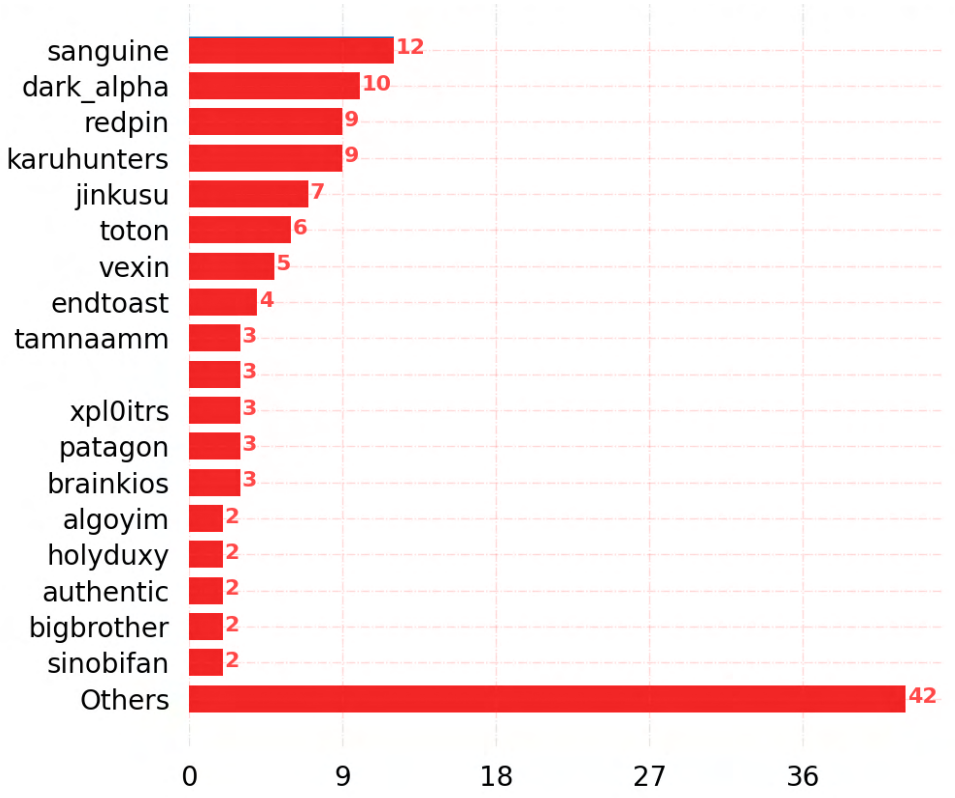


Fig 5: Active Threat Actors Selling Compromised Access

Ransomware

Overview

CRIL recorded 3,837 ransomware attacks globally in H1 2026, averaging over 630 incidents per month — a pace that confirms ransomware as the most consistently damaging cyber threat organizations face today.

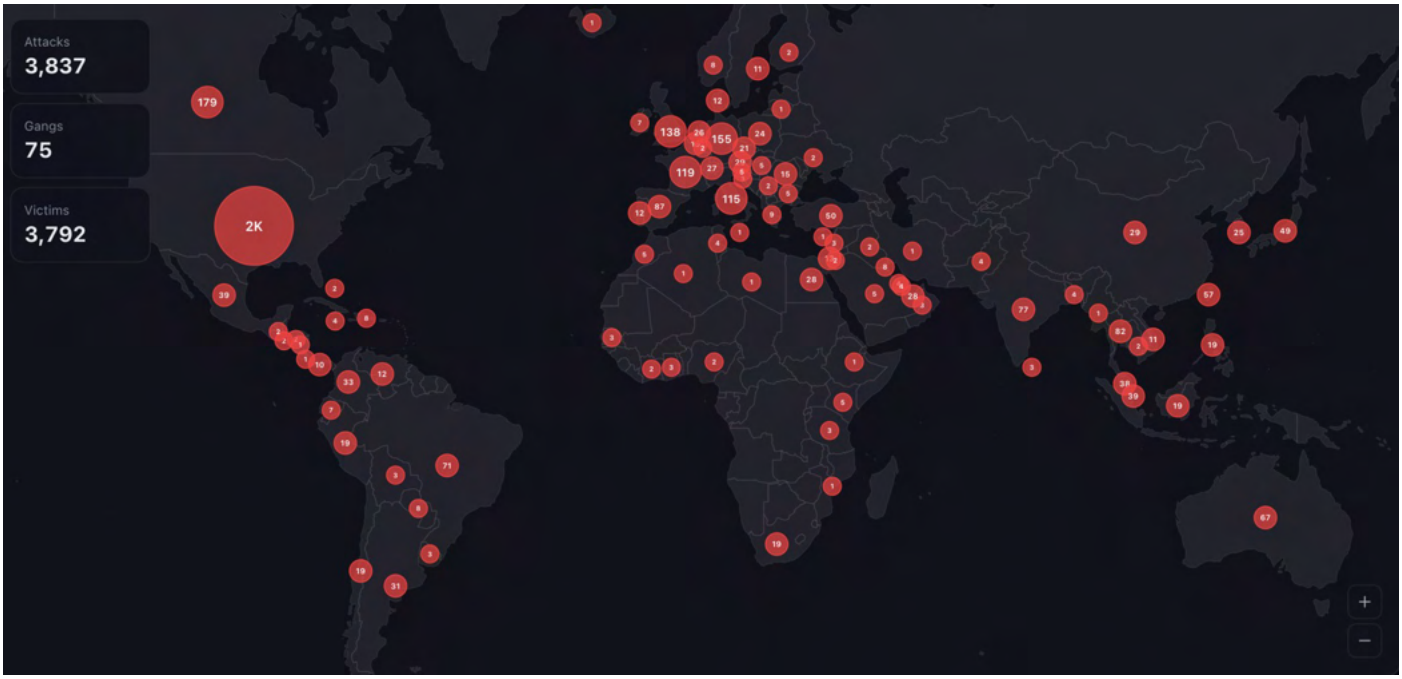


Fig 6: Global Distribution of Ransomware Attacks

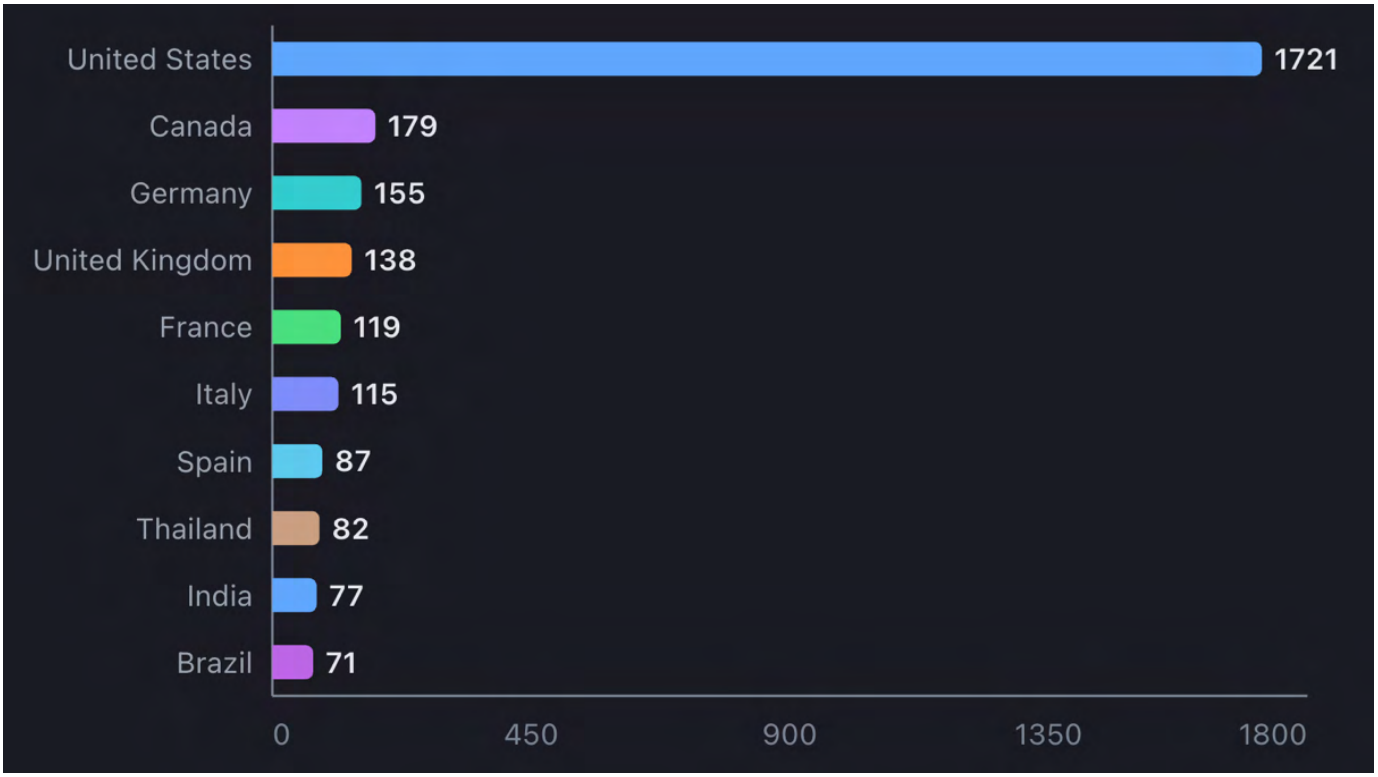


Fig 7: Top 10 Most Attacked Countries by Ransomware Actors

The landscape was dominated by a mix of established and aggressively emerging RaaS groups, led by Qilin, Akira, Dragonforce, and INC Ransom, who collectively accounted for a significant share of observed attacks.

Construction was the single most targeted sector, prized for its low tolerance for downtime and valuable intellectual property, followed by Professional Services, Manufacturing, and Healthcare — evidence of broad, largely opportunistic targeting across operationally sensitive industries.

Monthly Attack Trends

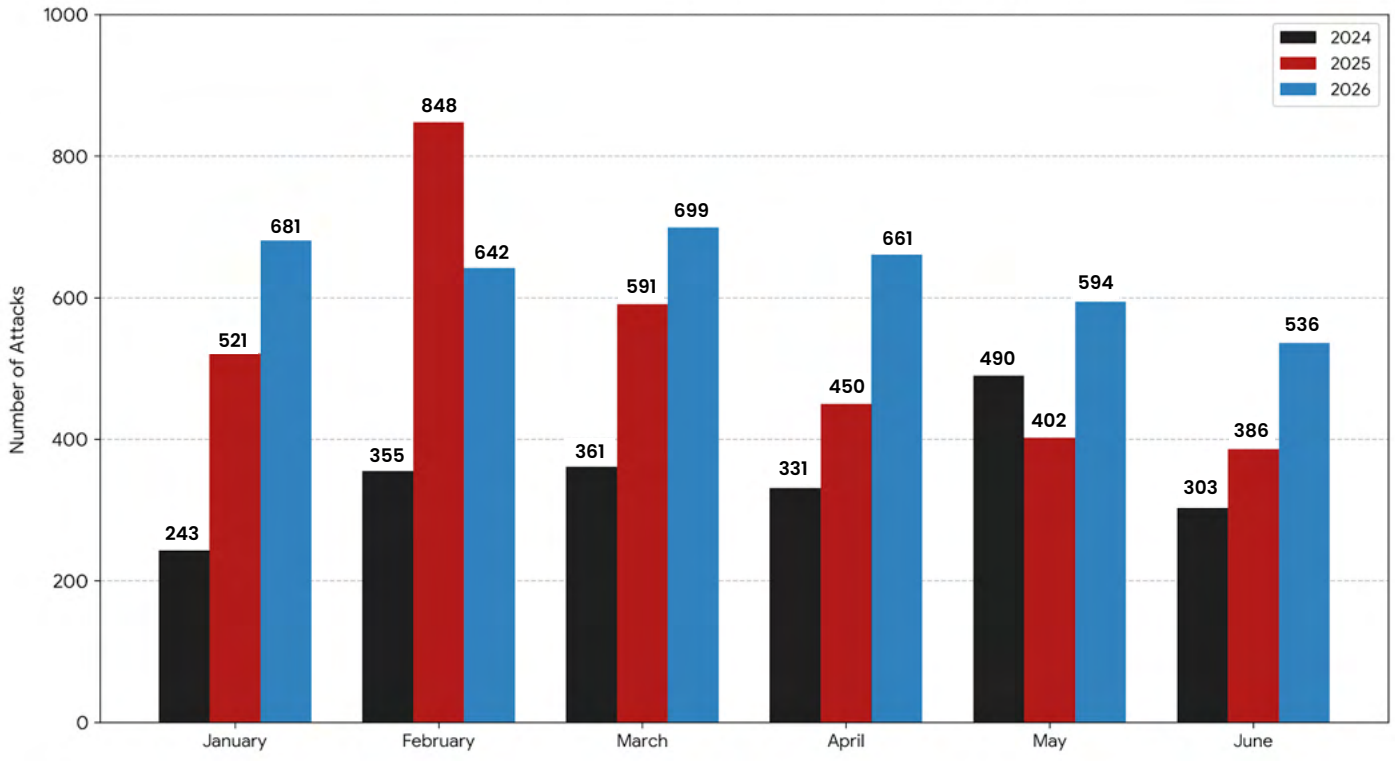


Fig 8: Comparison of Ransomware Attacks by Month (2024-2025-2026)

Quick Takeaways from YoY Comparison

- **New Peaks:** While February 2025 still holds the absolute record high (848), 2026 shows a significantly higher sustained volume across the board.
- **The Spring Shift:** In 2024 and 2025, ransomware attacks generally began a downward trend heading into May and June. In 2026, the numbers stay aggressively high as compared to previous years, with March and April seeing massive surges compared to previous years.

Quick Takeaways from 2026 MoM Analysis

- **January:** The year began with a high baseline of activity, driven by established groups like Akira and CL0P.
- **February:** A slight dip in overall attack volume, potentially reflecting operational shifts or law enforcement disruption affecting smaller players.
- **March – May:** A significant escalation in attack frequency, peaking in May and primarily fueled by the hyperactivity of Qilin, Dragonforce, and INC Ransom, who launched numerous campaigns in quick succession.
- **June:** Activity remained high despite a marginal decrease from the May peak — still well above the H1 average.
- The overall trend indicates that lulls in ransomware activity are temporary; threat actors adapt and rescale operations quickly to capitalize on new vulnerabilities and targets.

Dominant Ransomware Groups: The Key Players of H1 2026

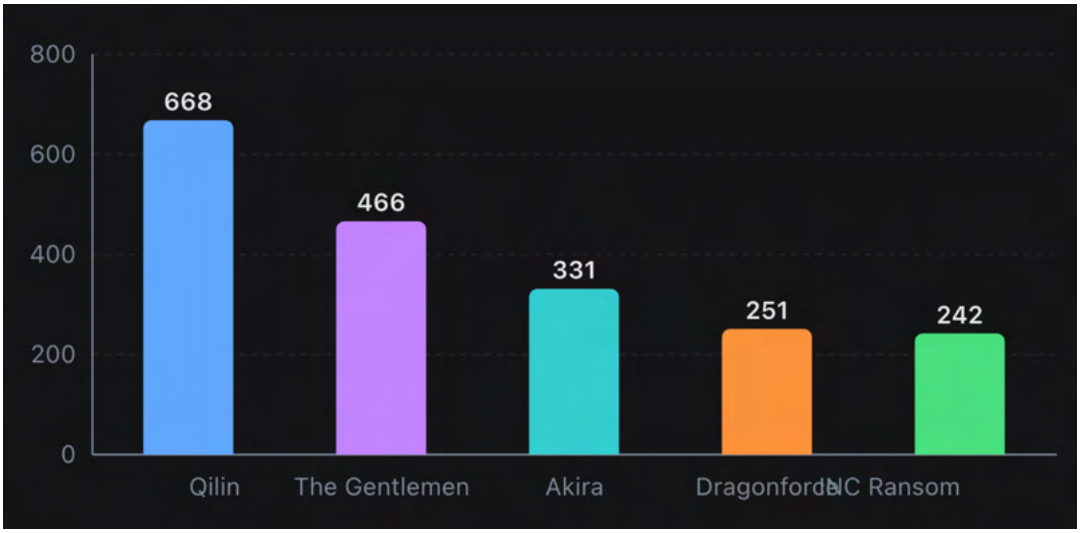


Fig 9: Top Five Ransomware Actors Worldwide

1. Qilin: Emerged as the single most prolific threat actor in H1 2026, demonstrating a remarkable capacity for targeting a diverse range of industries — from Construction and Manufacturing to Healthcare and Professional Services. Its widespread activity points to a highly effective affiliate network and a focus on rapid, large-scale exploitation.

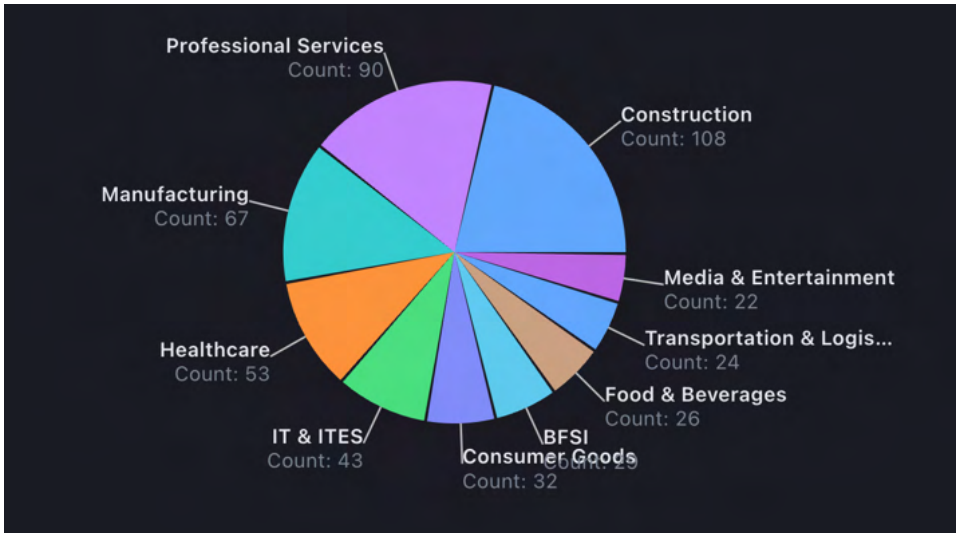


Fig 10: Top Sectors Targeted by Qilin

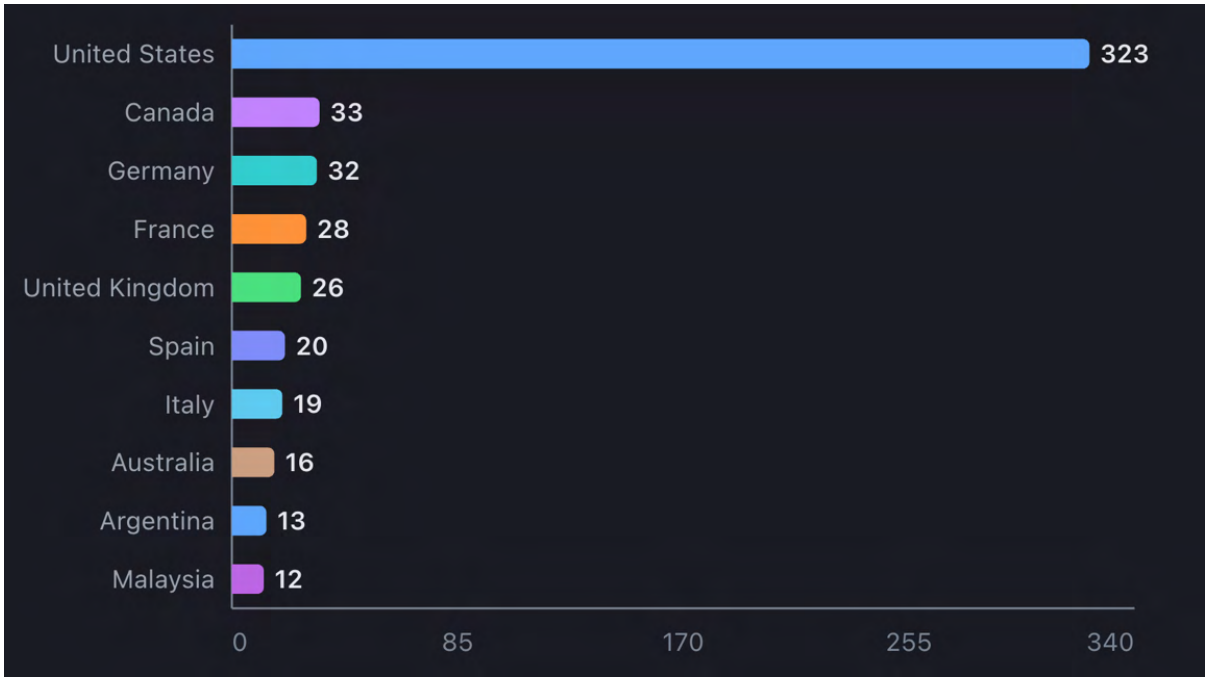


Fig 11: Top Countries Targeted by Qilin

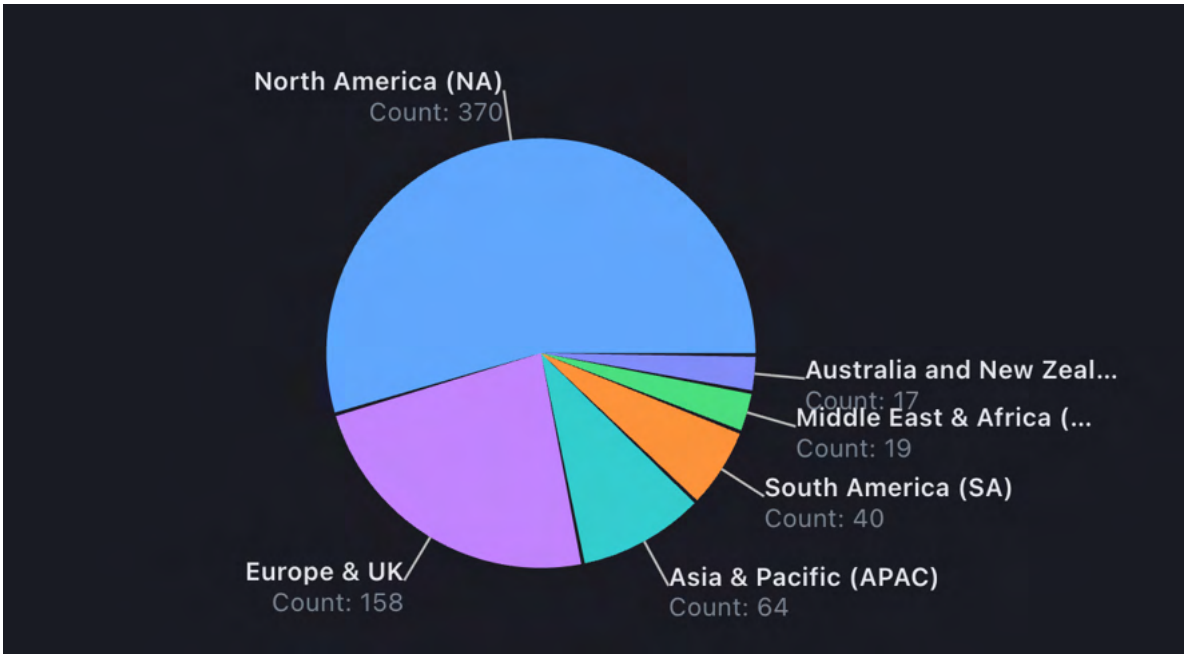


Fig 12: Regional Attack Patterns of Qilin

2. The Gentleman: A newer ransomware group as compared to the other established players but is making its presence felt with its focus on Manufacturing, Construction, Healthcare and IT industries. This threat actor also gained spotlight in South Asia particularly for the extensive targeting of Thailand where it accounted for nearly 50% of all ransomware attacks. The European region, however, remained the group's primary focus with a 144 entities targeted.

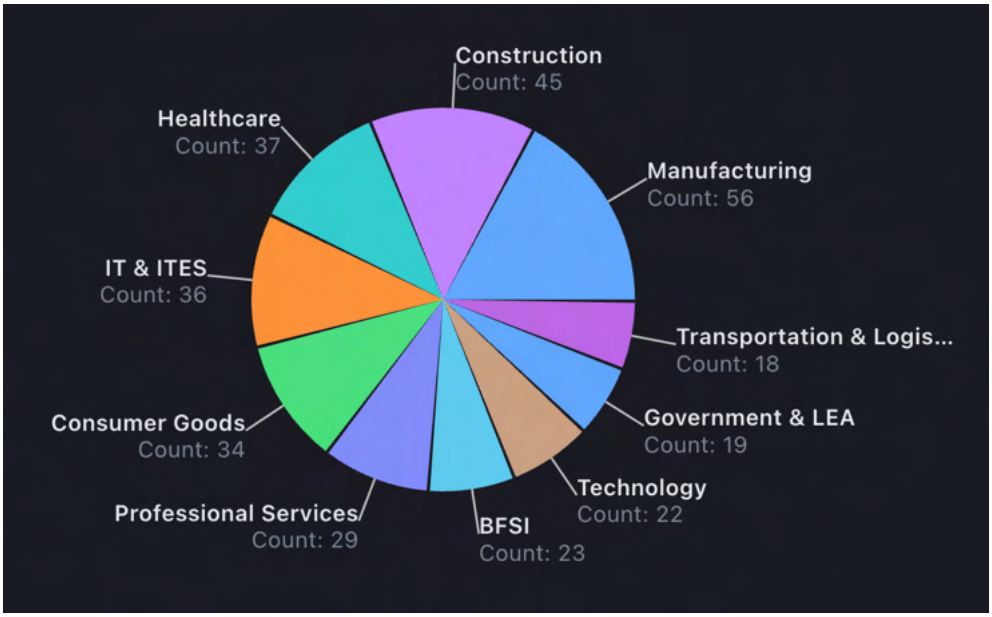


Fig 13: Top Sectors Targeted by The Gentleman

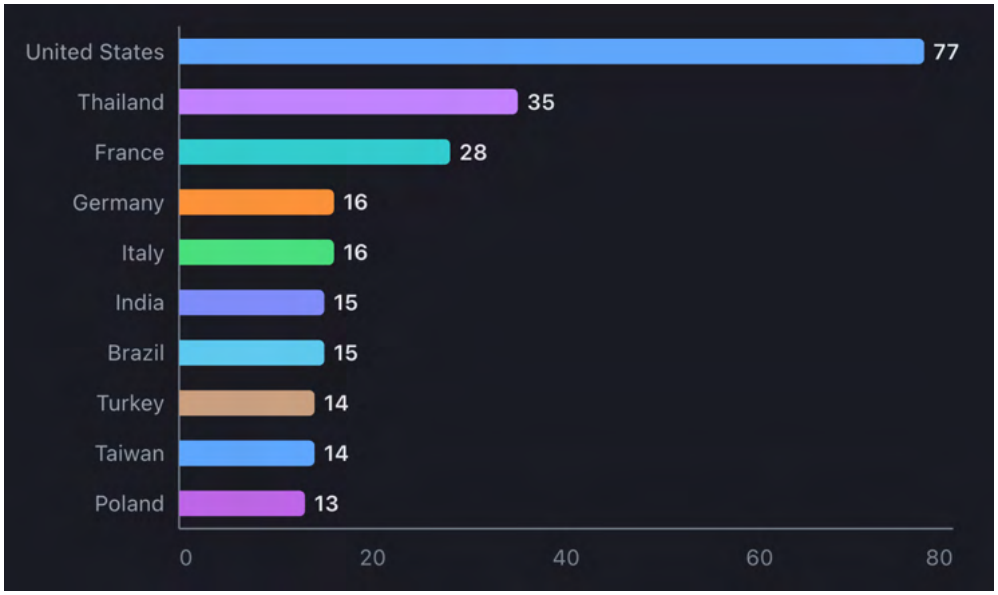


Fig 14: Top Countries Targeted by The Gentleman

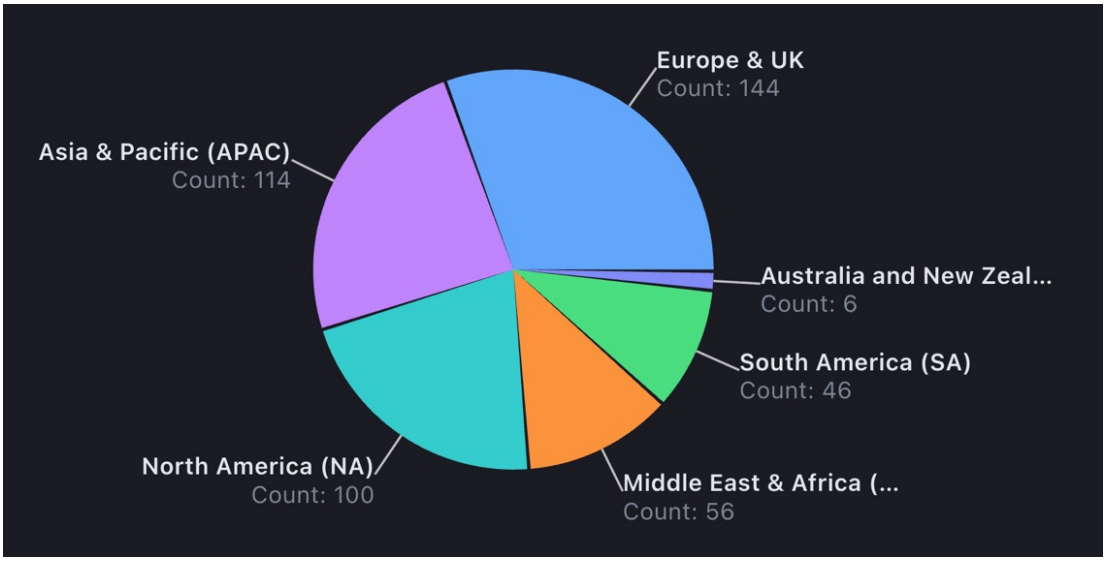


Fig 15: Regional Attack Patterns of The Gentleman

3. Akira: A persistently formidable threat responsible for a substantial number of attacks throughout the period, with a clear preference for Manufacturing, Construction, and Professional Services. Akira's continued success reflects a robust operational model and consistent ability to compromise small-to-medium-sized businesses across North America and Europe. Its primary focus were U.S.-based entities where it carried out 247 attacks.

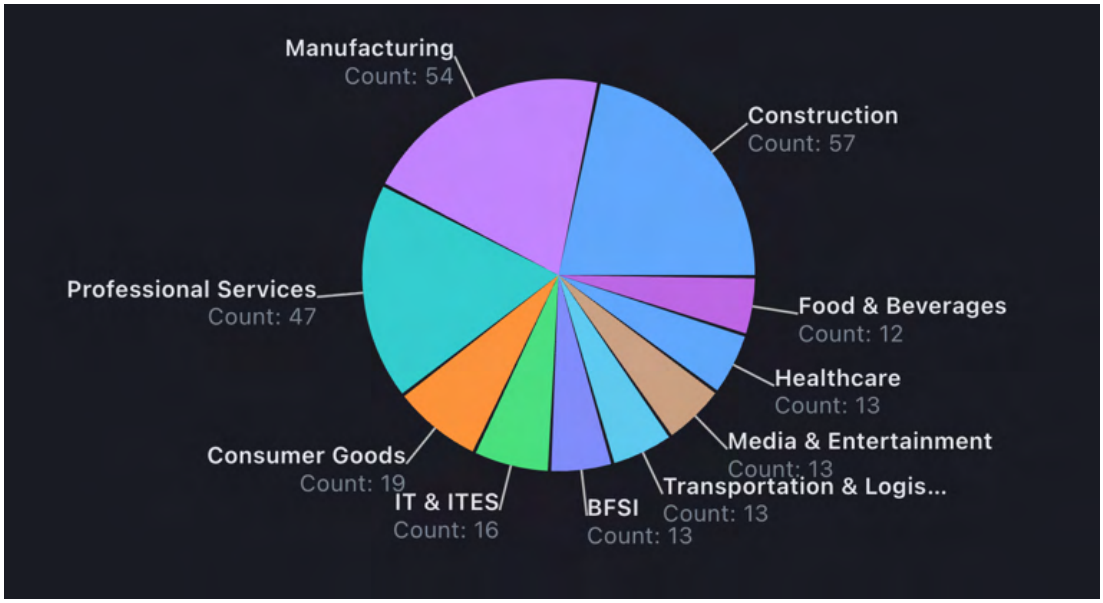


Fig 16: Top Sectors Targeted by Akira

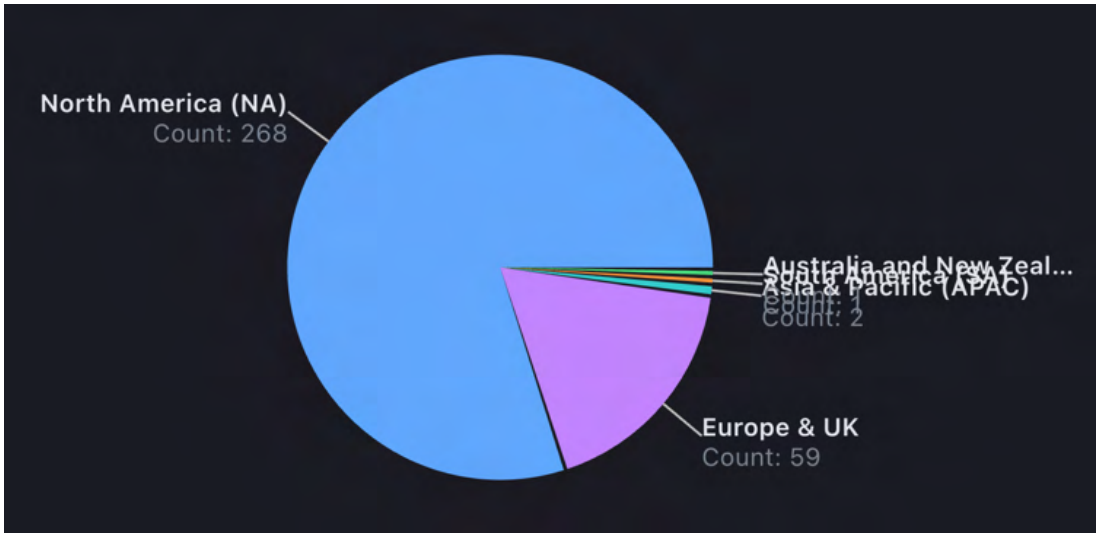


Fig 18: Regional Attack Patterns of Akira

4. Dragonforce: Maintained an aggressive operational tempo, consistently ranking among the top three most active gangs, with significant focus on Construction, Manufacturing, and Professional Services. The volume of its attacks reflects a mature RaaS platform capable of supporting numerous concurrent affiliate campaigns.

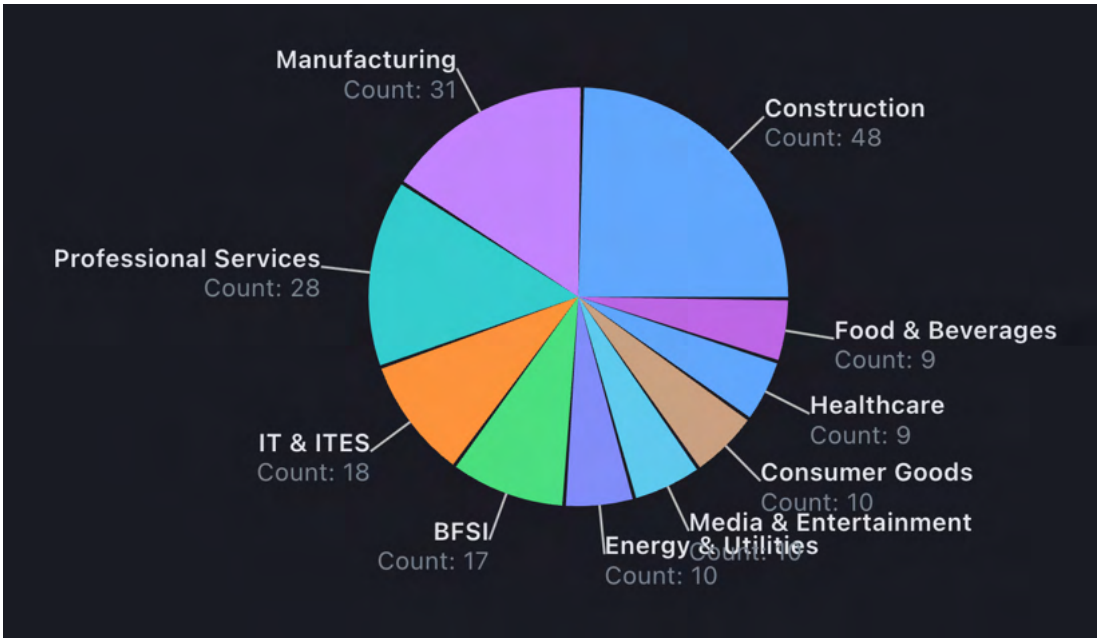


Fig 19: Top Sectors Targeted by Dragonforce

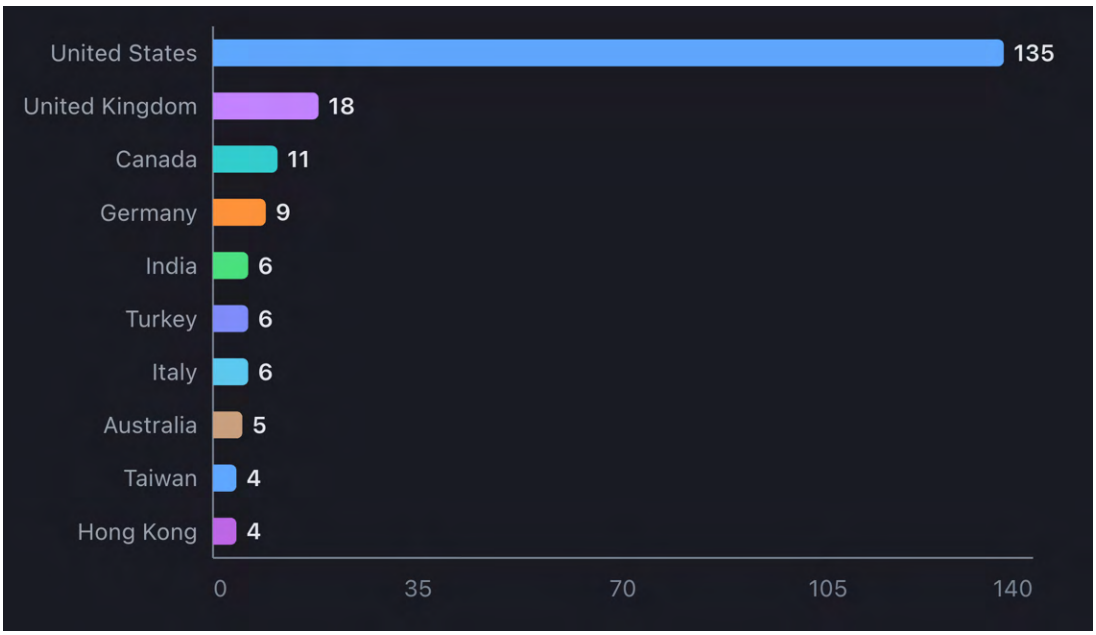


Fig 20: Top Countries Targeted by Dragonforce

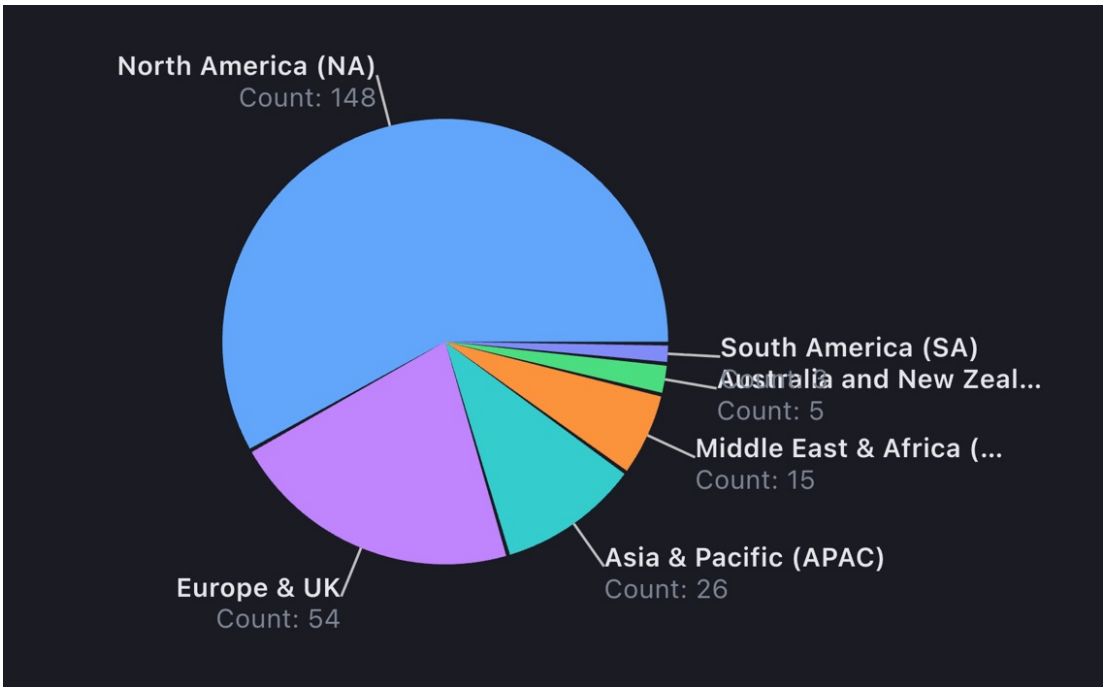


Fig 21: Regional Attack Patterns of Dragonforce

5. INC Ransom: Known for its rapid pace, with a distinct focus on Healthcare, Manufacturing, and Professional services entities, alongside consistent targeting of Transportation and Energy sectors — leveraging the sensitive client data these organizations hold for double extortion.

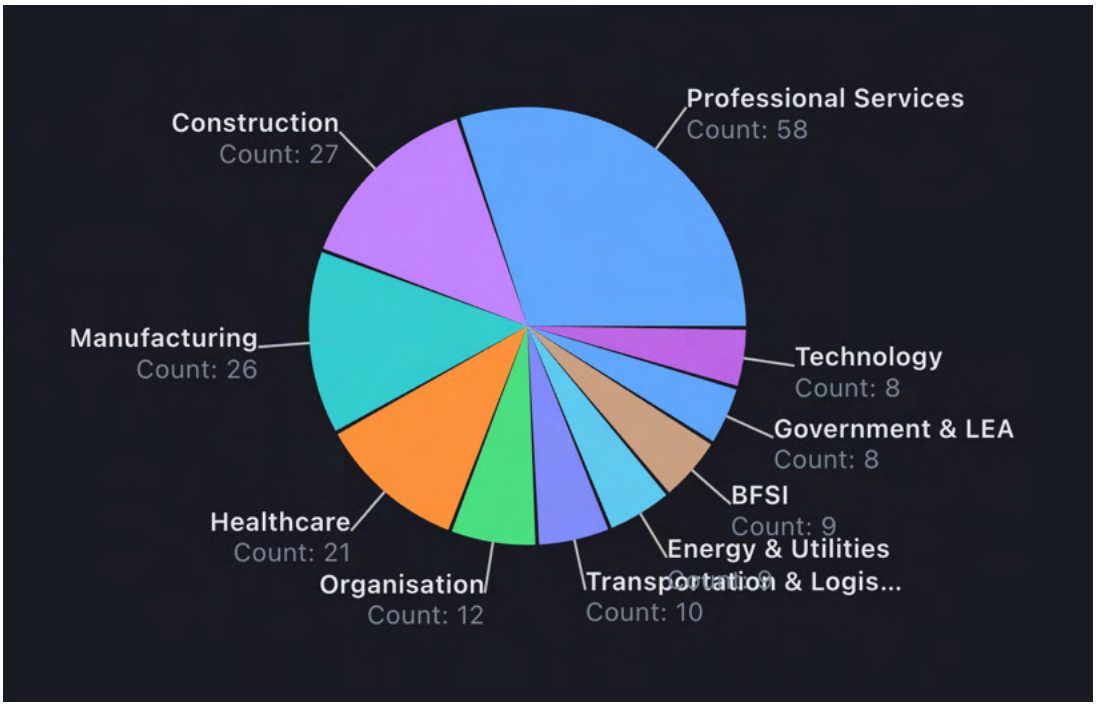


Fig 22: Top Sectors Targeted by INC Ransom

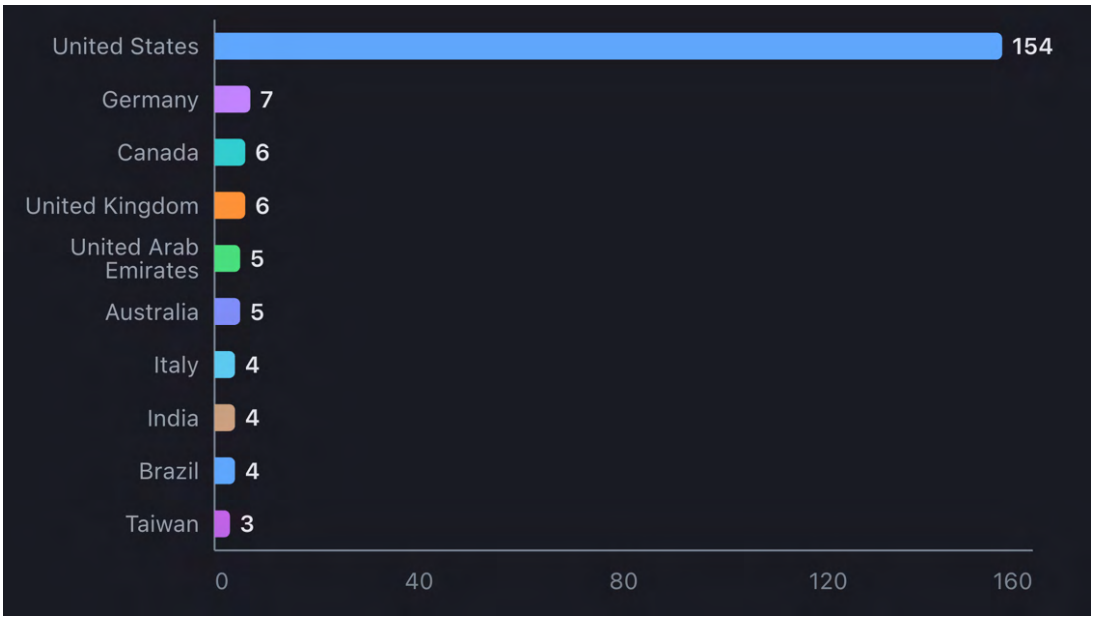


Fig 23: Top Countries Targeted by INC Ransom

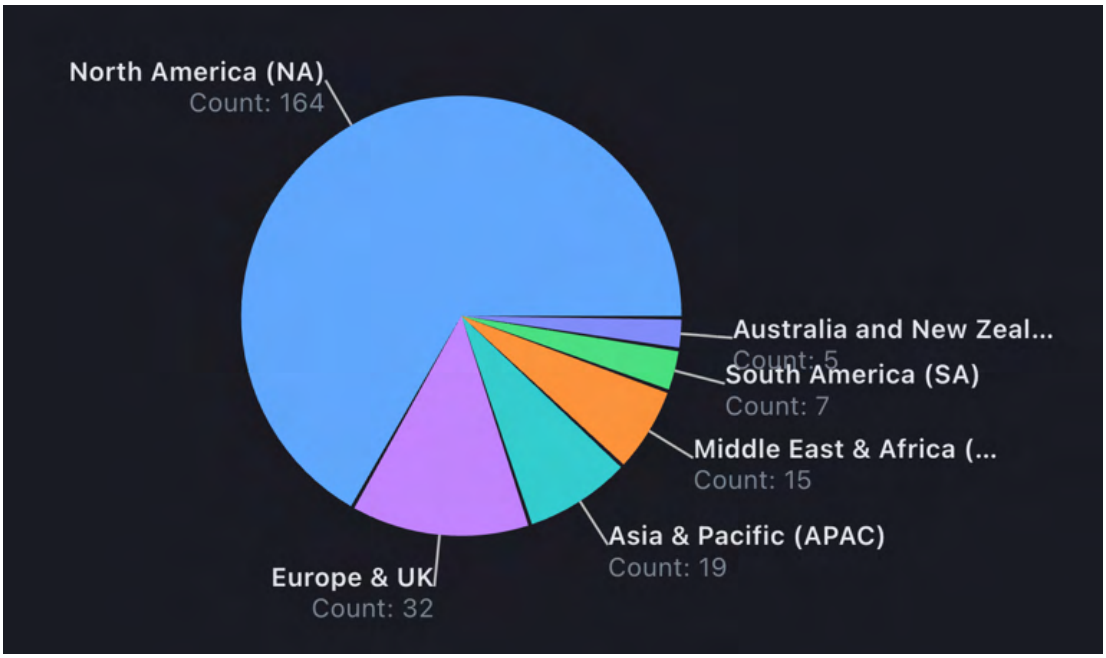


Fig 24: Regional Attack Patterns of INC Ransom

6. LockBit: Despite significant law enforcement action in prior years, LockBit's operation has proven resilient. While not the most prolific group in H1 2026, it remained a constant, dangerous presence — underscoring the decentralized, hard-to-disrupt nature of top-tier RaaS operations.

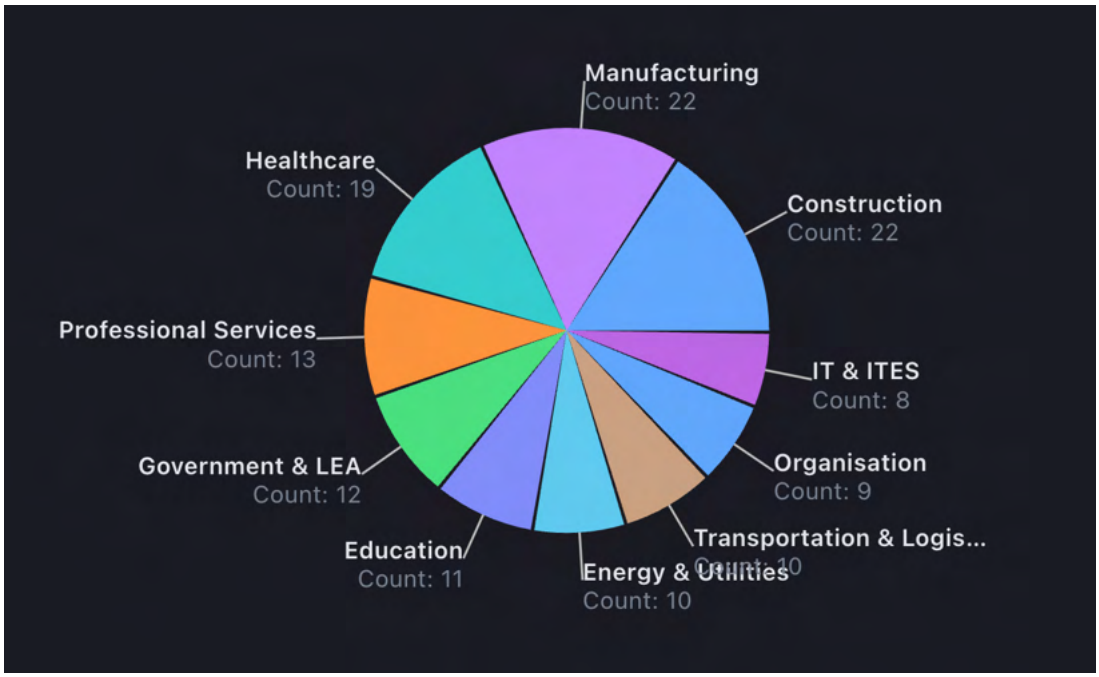


Fig 25: Top Sectors Targeted by LockBit

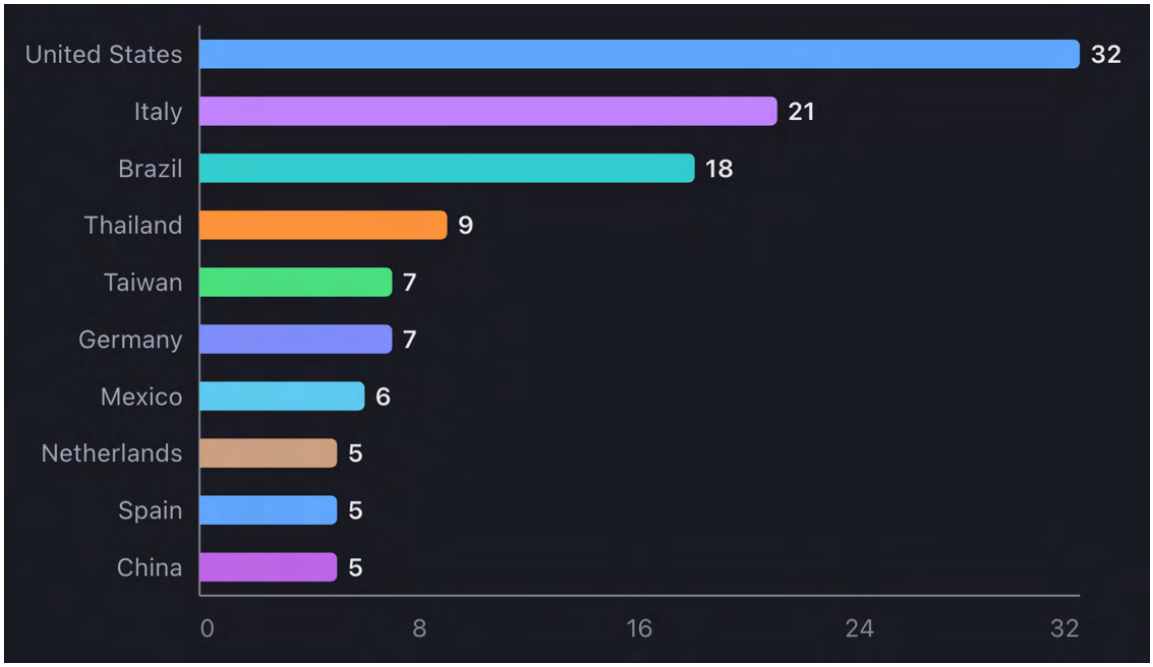


Fig 26: Top Countries Targeted by LockBit

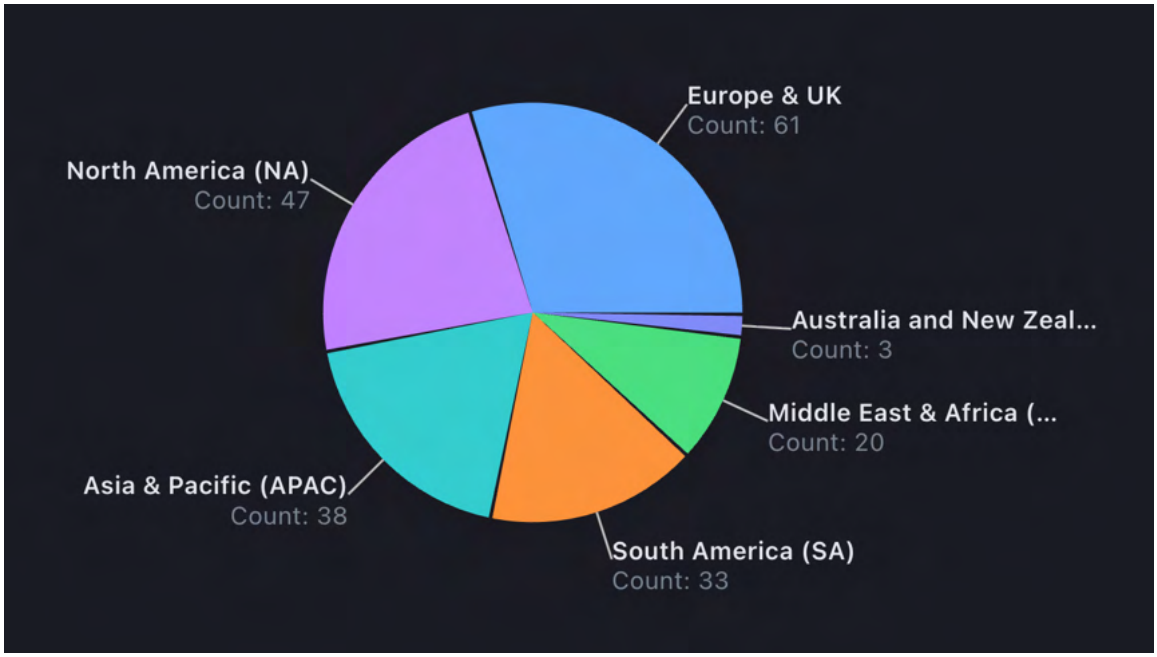


Fig 27: Regional Attack Patterns of LockBit

7. Play: Continued its "Big Game Hunting" approach, supplemented by a high volume of SMB attacks. Primary targets were in Construction, Professional Services, and Manufacturing, frequently via unpatched public-facing network devices. Its sole focus remained on North American entities in these sectors with some low lying attempts on European and Australian businesses.

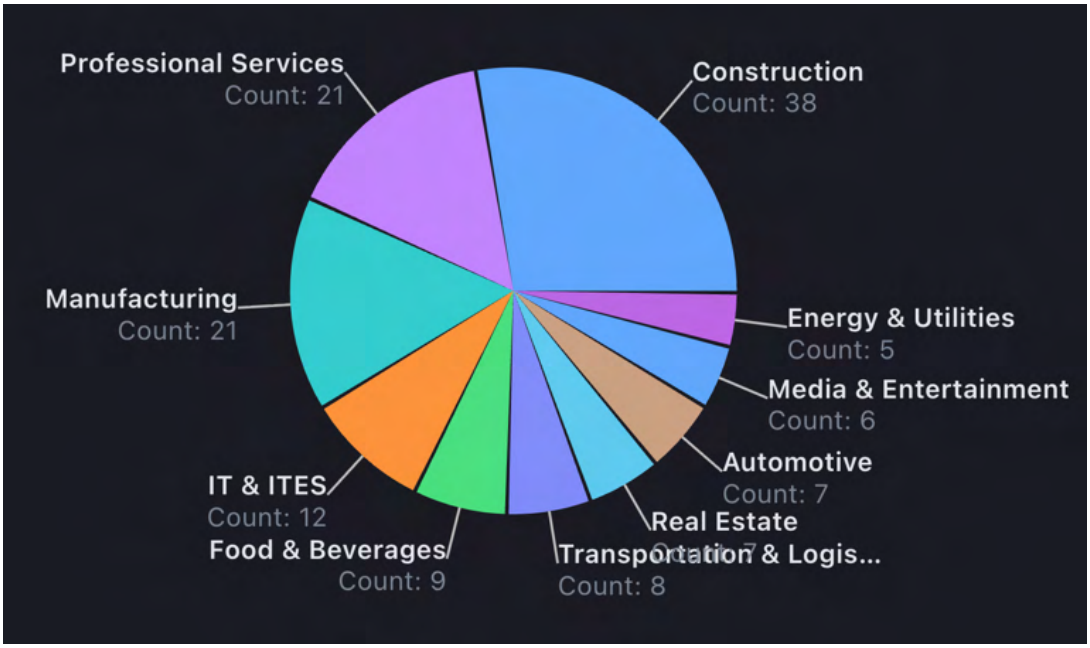


Fig 28: Top Sectors Targeted by Play

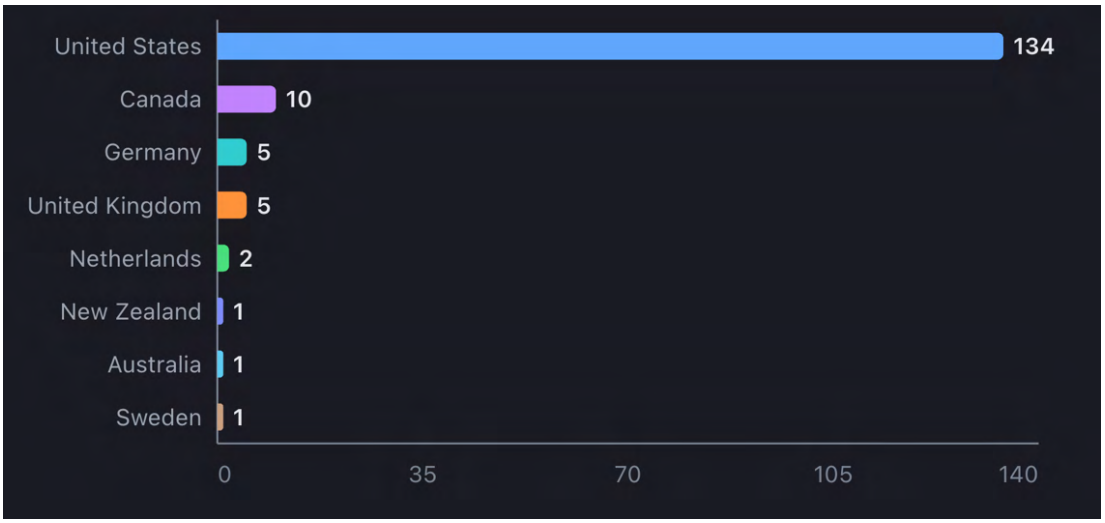


Fig 29: Top Countries Targeted by Play

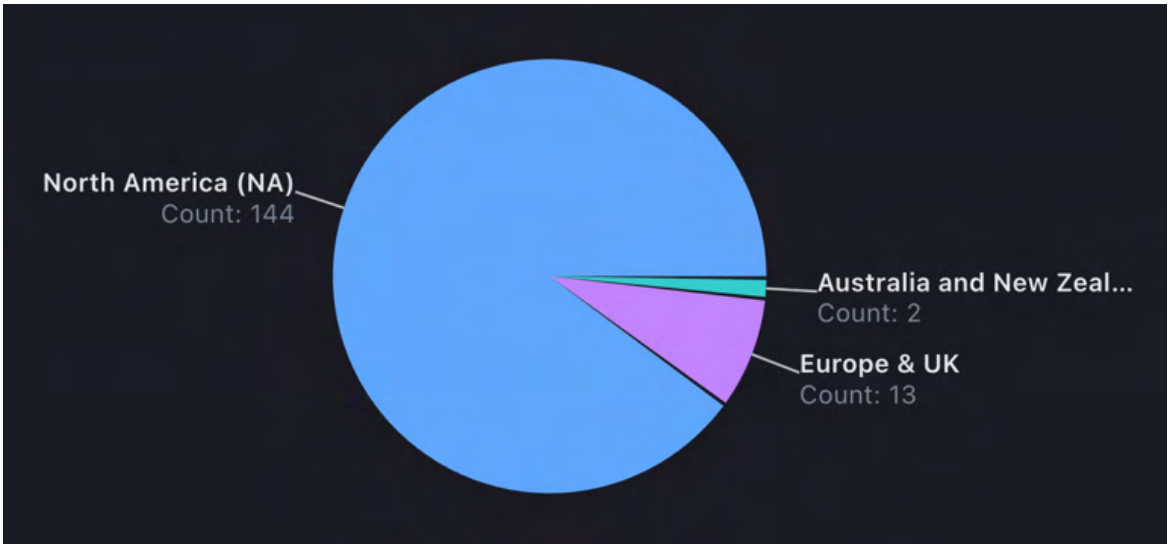


Fig 30: Regional Attack Patterns of Play

8. CL0P: Operated differently from its peers — rather than a high volume of disparate attacks, CL0P executed a large-scale campaign concentrated in January and February, characteristic of its strategy of exploiting a single zero-day vulnerability across hundreds of organizations at once (reminiscent of the MOVEit campaign). Primary targets were IT, Professional Services, and BFSI.

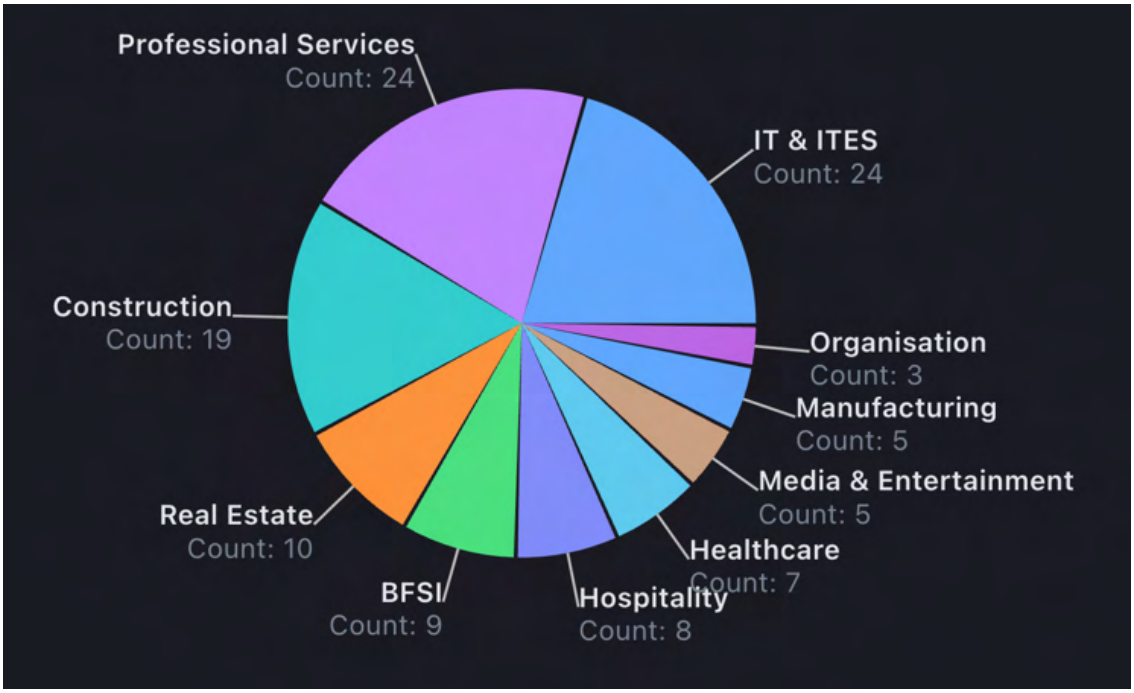


Fig 31: Top Sectors Targeted by CL0P

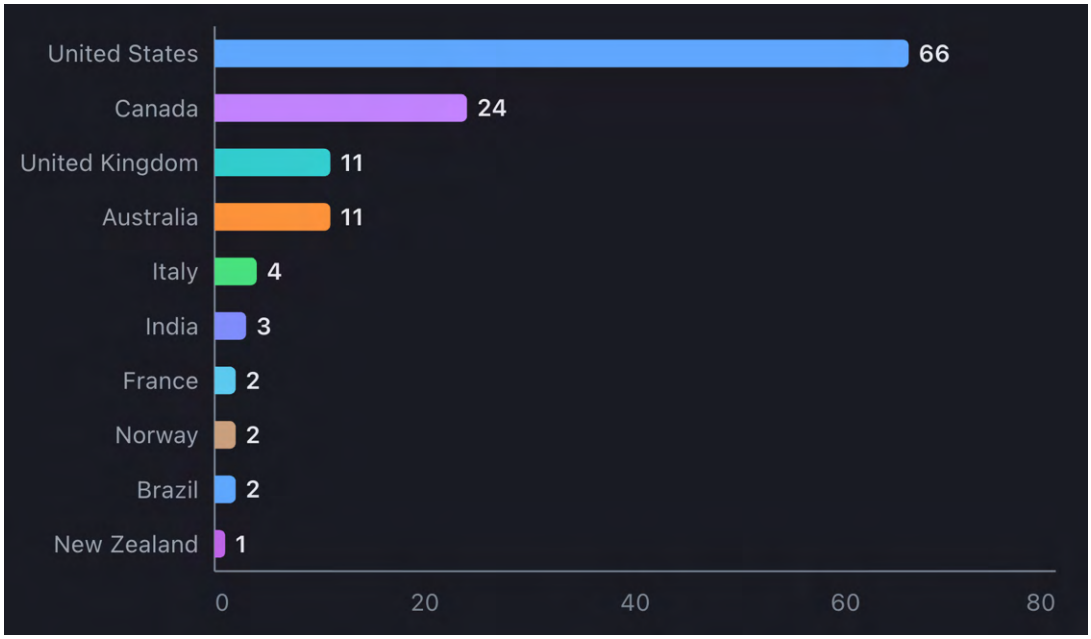


Fig 32: Top Countries Targeted by CL0P

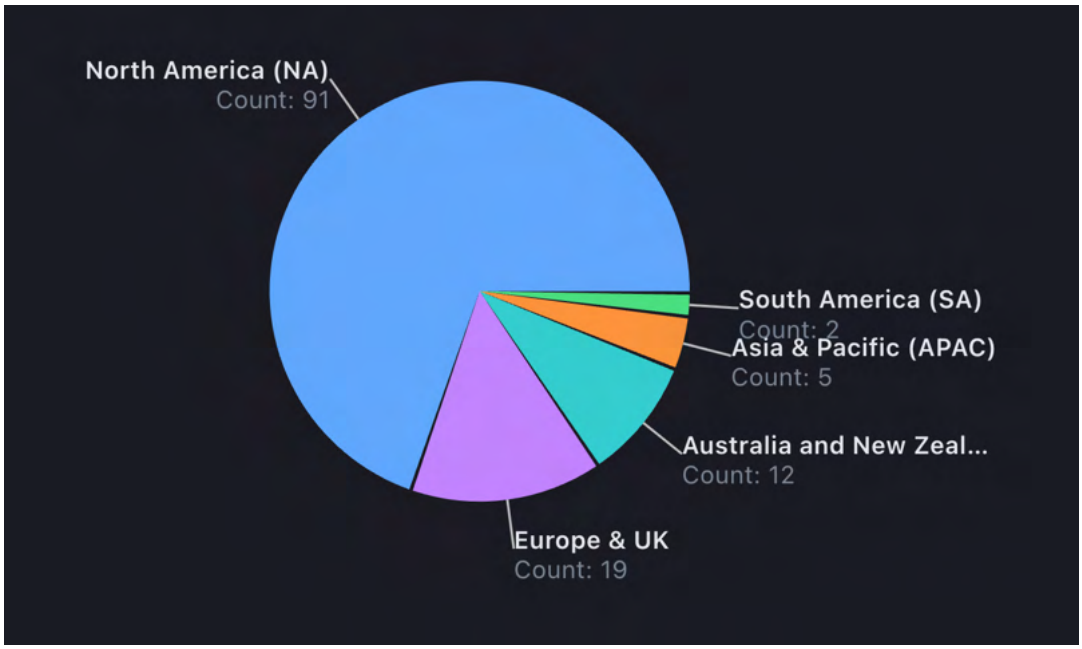


Fig 33: Regional Attack Patterns of CL0P

Most Targeted Industries/ Sectors

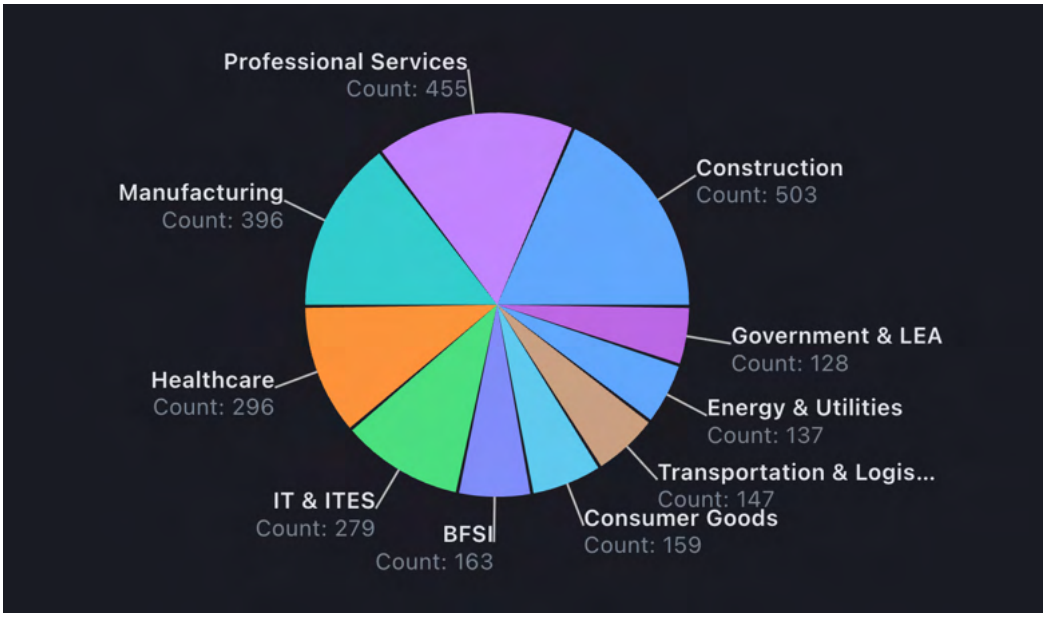
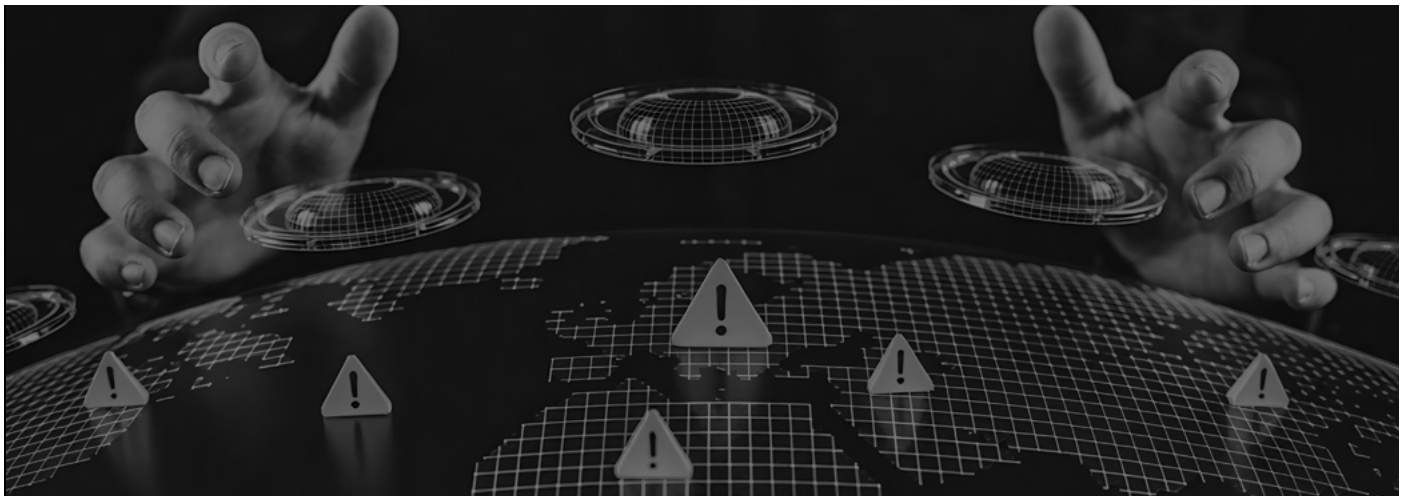


Fig 34: Top 10 Industries/Sectors Attacked by Ransomware Actors

Rank	Industry	Analysis
1	**Construction**	Targeted for time-sensitive projects, valuable bid data, and an interconnected network of contractors and subcontractors that can be exploited for wider access.
2	**Professional Services**	Legal, accounting, and consulting firms hold vast amounts of sensitive client data, making them ideal for double extortion and supply-chain attacks.
3	**Manufacturing**	The premier target due to reliance on OT/ICS environments, complex supply chains, and valuable intellectual property. Downtime translates directly into massive financial loss, increasing pressure to pay.
4	**Healthcare**	A perennial target given the critical nature of its services and the high value of Protected Health Information (PHI); ethical and regulatory pressure to restore services quickly is a key leverage point.
5	**IT & ITES**	Compromising an IT or Managed Service Provider (MSP) can provide access to dozens of downstream client networks, magnifying the impact of a single breach.
6	**BFSI**	Banks, insurers, and financial services firms are consistently targeted for direct access to financial assets and sensitive customer financial data.

Outlook and Strategic Recommendations

- **Increased competition:** The RaaS market will remain highly competitive, with groups like Qilin and Dragonforce challenging established players for affiliate loyalty and market share.
- **Continued focus on in-demand vulnerabilities:** Groups will keep rapidly weaponizing N-day and zero-day vulnerabilities in widely used enterprise software and hardware.
- **Data exfiltration as primary leverage:** The "double extortion" model is now standard practice, and the threat of public data leakage — not just the encryption itself — will remain the primary driver for ransom payments.
- **Attack surface management:** Maintain a comprehensive inventory of internet-facing assets and ensure timely patching of known vulnerabilities.
- **Identity and access control:** Enforce phishing-resistant multi-factor authentication (MFA) across VPNs, RDP, and cloud consoles, and apply the principle of least privilege.
- **Network segmentation:** Segregate critical networks to prevent lateral movement, and isolate IT and OT environments to protect industrial processes.
- **Resilient backups:** Maintain offline, immutable, and regularly tested backups to enable recovery without paying for a decryptor.
- **Incident response:** Develop and regularly test an incident response plan to ensure a swift, effective reaction that minimizes downtime and impact.



Hacktivism

The first half of 2026 saw a highly active and volatile hacktivism landscape, predominantly fueled by geopolitical conflict and nationalistic ideology.

A diverse set of actors — including IT ARMY OF RUSSIA, "BLAZER TEAM ATTACK", and various Indonesian-affiliated collectives — ran widespread campaigns combining DDoS attacks, website defacements, and data breaches, evidenced by approximately 9,825 data leak and dump posts.

The operational scale was significant: over 32,400 unique domains were impacted across a broad spectrum of industries, with Government, Technology, BFSI, and Healthcare entities most frequently targeted — a pattern consistent with a strategic focus on disrupting critical services for political messaging.

Notably, several channels marketed as hacktivist collectives function as hybrid operations: alongside DDoS logging and defacement claims, they broker stolen data and offer DDoS-for-hire services, blurring the line between ideological activism and financially motivated cybercrime.

Blazer Team Attack

The hacktivist channel 'Blazer Team Attack' primarily served as a coordination and proof-sharing platform for Distributed Denial-of-Service (DDoS) attacks. The group's activity centered on launching and logging Layer 4 and Layer 7 attacks, with numerous posts detailing attack statistics such as traffic volume (Gbps/PPS) and request rates against targets, many of which were protected by Cloudflare. In addition to DDoS operations, channel discussions also included website defacements and the potential sale of data belonging to Indonesian government entities. Targeted sectors were diverse, including Indonesian government websites like the Ministry of Foreign Affairs, educational institutions, financial services, and various online gambling sites. The communications, predominantly in Indonesian, did not indicate a singular ideological motivation; rather, the activity suggested a focus on demonstrating technical prowess, targeting rivals, and offering DDoS-for-hire services.

Hatzel's Unapologetic Right-Wing Group

Based on an analysis of the channel "Hatzel's Unapologetic" from January to June 2026, the group's activity focused on information operations and political discourse rather than technical hacktivism. The channel served as a forum for disseminating content aligned with a pro-Israel, right-wing nationalist ideology. Its primary activities involved sharing news, political commentary, propaganda, and inflammatory rhetoric.

The content did not contain claims of conducting DDoS attacks, data breaches, or website defacements. Instead, the group's targeting was rhetorical, focusing on domestic political opponents such as Israeli left-wing figures and the judiciary, as well as geopolitical adversaries including Iran, Hamas, and Hezbollah. The observed methods were centered on shaping narratives and mobilizing online political discussion, with no evidence of direct cyberattacks being claimed or coordinated through the channel during this period.

Legion Null

Analysis of the "Legion Null" channel indicates that it operates primarily as a Turkish-language marketplace for financially motivated cybercrime rather than as a hacktivist group. Threat actors within the channel focus on trading, renting, and creating accounts for money muling purposes, heavily targeting the Turkish financial sector, including banks like Akbank, ING, and QNB Finansbank, and fintech/payment services such as Paycell, Papara, Uption, and Colendi.

Activities also include the brokerage of sensitive data, with actors claiming to possess large datasets of Turkish citizen PII and government employee information. The channel serves as a hub for cybercrime-as-a-service, where members offer tools and services including SMS verification for bypassing 2FA, phishing scripts for various platforms, stolen credit card data, and services for paying off debts and bills with illicit funds. All observed communications and activities are centered on financial profit.

Brotherhood Capung BCI (Cyber)

Based on channel analysis, "Brotherhood Capung BCI (Cyber)", an Indonesian-speaking hacktivist collective, primarily focused on opportunistic website defacements and Distributed Denial-of-Service (DDoS) attacks. Their targeting was heavily concentrated on Indonesian entities, particularly within the government and education sectors, as evidenced by numerous posts claiming compromises of `.go.id`, `.ac.id`, and `.sch.id` domains. Claimed victims included subdomains related to regional Indonesian governments and the Indonesian Cyber and Crypto Agency (BSSN). The group's tactics involved exploiting web vulnerabilities like SQL injection, uploading web shells for defacement, and running DDoS scripts. Beyond these attacks, the channel was also used for sharing allegedly leaked databases, including one from an Indian educational institution, and promoting the sale of various hacking tools and doxing services. The group's activities appear to be driven by a desire for reputation, with various members claiming attacks under individual aliases.

Lystic Team #ID

The Indonesian-speaking group 'LYSTIC TEAM #ID' operated primarily as a marketplace and social hub for various low-level cybercriminal activities. The channel's content indicates a focus on selling malicious tools and services rather than conducting coordinated hacktivist campaigns. Prominently advertised offerings included DDoS-for-hire services, with members boasting about targeting online gambling and news websites. The group also claimed to have compromised and offered webshell access to multiple websites, including the Indonesian media outlets transnews.co.id and realitas.web.id. A significant portion of their activity involved the commercial trade of tools and services for banning and unbanning accounts on social platforms like WhatsApp, as well as selling virtual phone numbers (nokos) and various malicious scripts. The group's motivations appear financial, and they claim affiliation with other Indonesian cyber groups, such as 'KELELAWAR CYBER TEAM KCT'.

Most Active Threat Actors of H1 2026

Beyond the incidents and campaigns catalogued elsewhere in this report, CRIL maintains an ongoing census of the threat actors behind them. In H1 2026, CRIL tracked 261 distinct threat actor profiles active worldwide — spanning nation-state Advanced Persistent Threat (APT) groups, ransomware operators, hacktivist collectives, cybercriminal groups, and specialized extortion gangs. The composition of this population, and how it shifts from region to region, is itself a signal. A region dominated by APT activity points to geopolitical and espionage pressure, while a region skewed toward ransomware and cybercriminal groups points to purely financial targeting. The breakdown below — worldwide and across five regional groupings — is intended to help security leaders calibrate which actor types deserve the most attention in their specific operating geography.

Worldwide

261

Total Threat Actor Profiles Observed

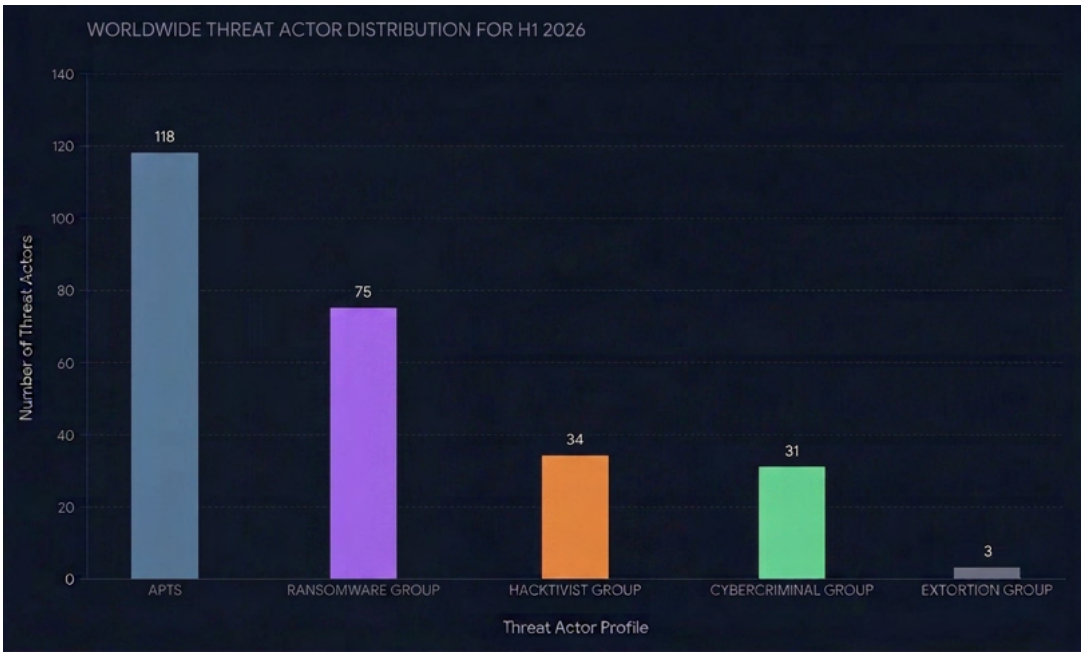


Fig 35: Worldwide Threat Actor Distribution, H1 2026

Nation-state APT groups were the single largest category tracked worldwide, accounting for 118 of the 261 profiles observed (over 45%) — a reflection of the sheer number of state-sponsored programs China, North Korea, Iran, and Russia alone field across espionage, IP theft, and pre-positioning operations. Ransomware groups were the second-largest category at 75 profiles (29%), consistent with the high-volume attack data covered elsewhere in this report. Hacktivist (34) and cybercriminal (31) groups made up a smaller but still substantial share, while dedicated extortion-only groups remained a niche category (3) — most extortion activity today rides on top of ransomware infrastructure rather than operating as a standalone business model.

Threat Actors to Watch

Name	Origin	Target Countries	Target Sectors
Bluenoroff	**North Korea (Lazarus Group subgroup)**	Global — targets individuals in the cryptocurrency sector worldwide	Cryptocurrency, Financial Services
UNC6508	**China (PRC-nexus espionage cluster)**	United States, Canada	Education & Academic Research, Healthcare & Medical Research, Government/Regulatory, Aerospace & Defense
Volt Typhoon	**China (state-sponsored)**	United States (incl. Guam) and allies	Communications, Manufacturing, Energy & Utilities, Transportation, Construction, Maritime, Government, IT, Education
Desert Falcons	**Palestine**	UAE, Albania, Algeria, Egypt, Israel, Jordan, Kuwait, Lebanon, Libya, Iraq, Qatar, Syria, Turkey, Yemen, Zimbabwe	Aerospace & Defense, Education, Government, Law Enforcement, Media, Transportation & Logistics
SideCopy	**Pakistan**	India, Afghanistan	Government, Defense (military and armed personnel)

- **Bluenoroff:** A financially motivated subgroup of the Lazarus Group (also tracked as Hidden Cobra and Labyrinth Chollima), Bluenoroff funds North Korean state operations by targeting individuals in the cryptocurrency space — typically impersonating established investors and planting malicious links inside victims' Calendly scheduling accounts as an entry point for fraud.
- **UNC6508:** A PRC-nexus espionage cluster targeting North American academic, medical, regulatory, and military research organizations. The group compromises externally accessible REDCap environments, deploys web shells and custom malware, and has been observed creating malicious mail-forwarding rules to silently exfiltrate strategically relevant correspondence — all routed through US-based residential proxies and compromised routers to obscure attribution.
- **Volt Typhoon:** A Chinese state-sponsored actor focused on espionage against US critical infrastructure, notably in Guam. Volt Typhoon favors "living off the land" techniques to blend into normal network activity, prioritizing long-term, undetected access over rapid data theft — a profile consistent with pre-positioning for potential future disruption of critical communications.

- **Desert Falcons:** A native Arabic-speaking group running politically themed spear-phishing campaigns against influential individuals across the Middle East, using professionally produced lures tied to current political events to gather intelligence or extort targeted victims.
- **SideCopy:** A Pakistan-based group targeting Indian and Afghan government and defense personnel since 2019. SideCopy deliberately mimics the infection chains of SideWinder and shares links to Transparent Tribe (APT36), frequently updating its malware modules and borrowing other groups' TTPs to complicate attribution.

Regional Threat Actor Distribution

The regional splits below show how the worldwide threat actor population documented above is distributed geographically, and how that mix shifts from an APT-heavy profile in some regions to a ransomware-dominated one in others.

Asia and Pacific

123

Total Threat Actor Profiles Observed

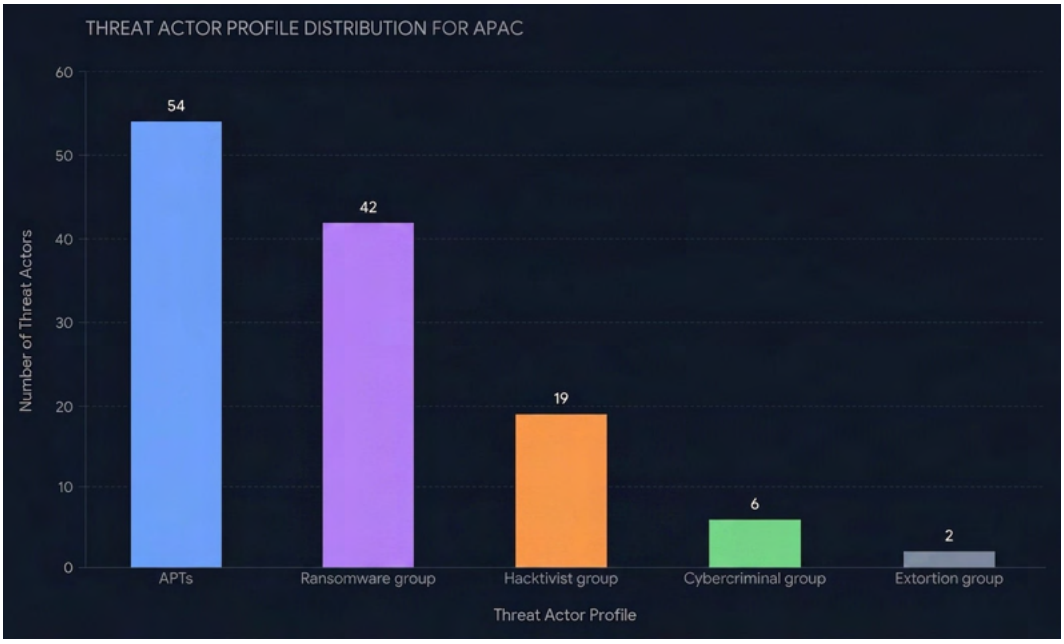


Fig 36: Threat Actor Distribution for Asia and Pacific

Asia-Pacific recorded the highest APT-to-total ratio of any region in this report — 54 of 123 profiles (44%) — underscoring the region's position at the center of state-sponsored cyber activity, with China-, North Korea-, and Iran-linked groups (SharpPanda, Kimsuky, MuddyWater) running sustained espionage campaigns against regional governments and critical sectors. Ransomware groups (42) were the second-largest category, while a comparatively small cybercriminal footprint (6) suggests the region's underground economy remains less developed than its state-sponsored threat landscape.

Threat Actors to Watch

Name	Origin	Target Countries	Target Sectors
SharpPanda	**China**	Indonesia, Malaysia, Thailand, Vietnam	Government
Kimsuky	**North Korea**	Japan, South Korea, Thailand, Vietnam	Aerospace & Defense, Education, Energy & Utilities, Government, Healthcare, Manufacturing
MuddyWater	**Iran**	Middle Eastern countries, India, Thailand, Laos, Russia, and more	Aerospace & Defense, Education, BFSI, Energy & Utilities, Government, Healthcare, Manufacturing, Telecommunication, Transport, Media, IT
Yemen Cyber Army	**Yemen**	India, Malaysia, Philippines, Pakistan	BFSI, Education, Government, Manufacturing, Media, Retail

Australia and New Zealand

48

Total Threat Actor Profiles Observed

Fig 37: Threat Actor Distribution for Australia and New Zealand

Australia and New Zealand show the most financially skewed threat actor profile in this report: ransomware groups account for 30 of 48 profiles (63%), by far the highest ransomware-to-total ratio of any region, while hacktivist (2) and extortion-only (1) groups are almost negligible. This concentration reflects ANZ's attractiveness as a high-value, high-paying ransomware target rather than a focus of ideological or geopolitical cyber activity — though the region still hosts a meaningful APT presence (12), led by China-linked UNC3886.

Threat Actors to Watch

Name	Origin	Target Countries	Target Sectors
UNC3886	**China**	Australia, New Zealand, European countries, India, Trinidad and Tobago, Thailand, and more	Aerospace & Defense, Agriculture, Automotive, BFSI, Construction, Healthcare, Education, Energy & Utilities, Government, Manufacturing, Media, Telecommunication, Transport, IT, Pharmaceuticals
People's Cyber Army of Russia	**Russia**	Australia, United Kingdom, United States, Poland, France, Japan, Taiwan	Critical Infrastructure, Energy & Utilities, Government, Media, Transport
Silence APT	**Unconfirmed (Russian-speaking)**	Australia, New Zealand, United Kingdom, United States, India, Italy, Spain, Denmark, Singapore, and more	BFSI, Government, Manufacturing, Pharmaceuticals
Vanilla Tempest	**Unconfirmed (Russian-speaking)**	Australia, United Kingdom, United States, and more	Automotive, Education, Healthcare, BFSI, Construction, Government, Manufacturing, Pharmaceuticals, Professional Services, Telecommunication, Transport, Retail, Technology

Europe and UK

124

Total Threat Actor Profiles Observed

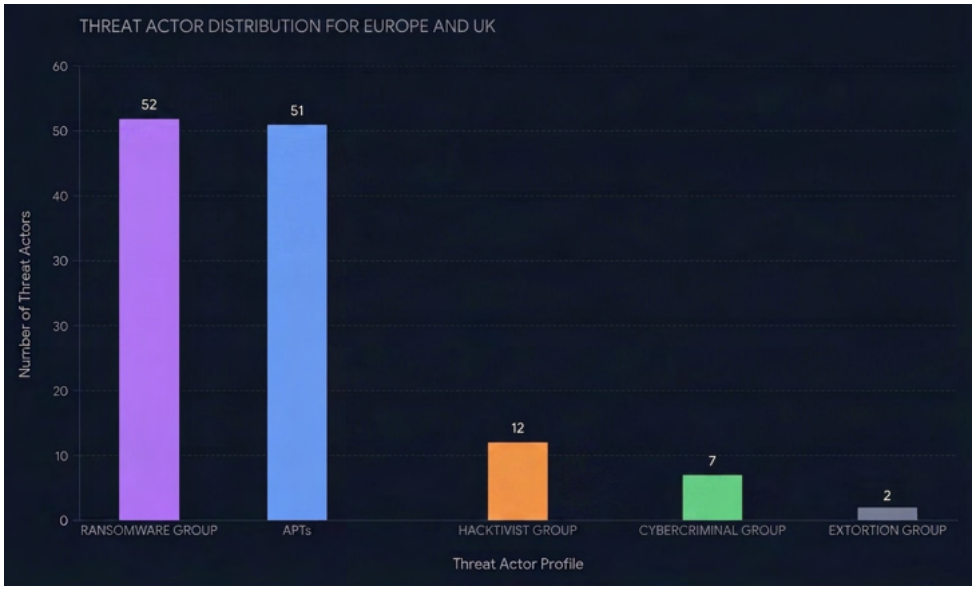


Fig 38: Threat Actor Distribution for Europe and UK

Europe and the UK show the most evenly balanced threat actor profile of any region, with ransomware groups (52) and APTs (51) almost at parity — evidence that the region is targeted equally by financially motivated ransomware affiliates and by state-sponsored espionage operators (China, Russia, and Vietnam-linked groups among them). The region's hacktivist count (12) is elevated relative to its overall size, driven substantially by pro-Russian collectives such as NoName057(16) operating in direct response to the Russia-Ukraine conflict and broader regional tensions.

Threat Actors to Watch

Name	Origin	Target Countries	Target Sectors
Volt Typhoon	**China**	United Kingdom, United States, Australia, India	Construction, Education, Energy & Utilities, Government, Manufacturing, Telecommunication, Transport, IT
Cobalt Group	**Russia**	Estonia, United Kingdom, Ukraine, Spain, Moldova	BFSI, Retail, Media, Technology
NoName057(16)	**Russia**	Estonia, United Kingdom, Ukraine, Italy, Spain, France, Poland, Norway, Denmark, Lithuania, Latvia, Czech Republic, Germany, Moldova	Agriculture, BFSI, Consumer Goods, Retail, Media, Manufacturing, Professional Services, Telecommunication, Transport, Hospitality
APT32	**Vietnam**	Germany, Denmark, United Kingdom, India, and more	Aerospace & Defense, BFSI, Government, Hospitality, Manufacturing, Media, Retail, Technology, Telecommunications

Middle East and Africa

94

Total Threat Actor Profiles Observed

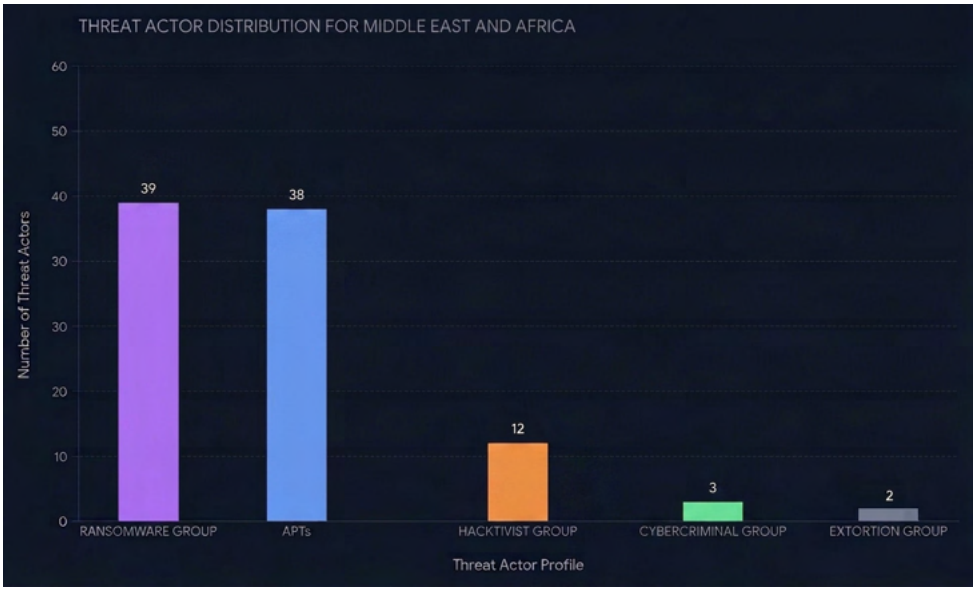


Fig 39: Threat Actor Distribution for Middle East and Africa

Middle East & Africa mirrors Europe's near-parity pattern between ransomware (39) and APT (38) activity, reflecting a region shaped simultaneously by financially motivated ransomware gangs and by intense state- and ideologically-driven cyber activity tied to ongoing regional conflicts. The region's hacktivist count (12) is disproportionately high relative to its overall actor population, consistent with the geopolitically charged hacktivism documented in this report's regional hacktivism sections — much of it tied to Israel-Iran tensions and broader Middle East conflict dynamics.

Threat Actors to Watch

Name	Origin	Target Countries	Target Sectors
Gonjeshke Darande	**Israel**	Iran, Syria	Energy & Utilities, Transportation & Logistics
Desert Falcons	**Palestine**	UAE, Albania, Algeria, Egypt, Israel, Jordan, Kuwait, Lebanon, Libya, Iraq, Qatar, Syria, Turkey, Yemen, Zimbabwe	Aerospace & Defense, Education, Government, Law Enforcement, Media, Transportation & Logistics
Eclipse Hacktivists	**Russia**	Israel, Ukraine	Government, Law Enforcement, Transportation & Logistics
Banished Kitten APT	**Iran**	Israel, United States and Allies	Education, Government, Law Enforcement, Healthcare, Media, Technology

Americas

120

Total Threat Actor Profiles Observed

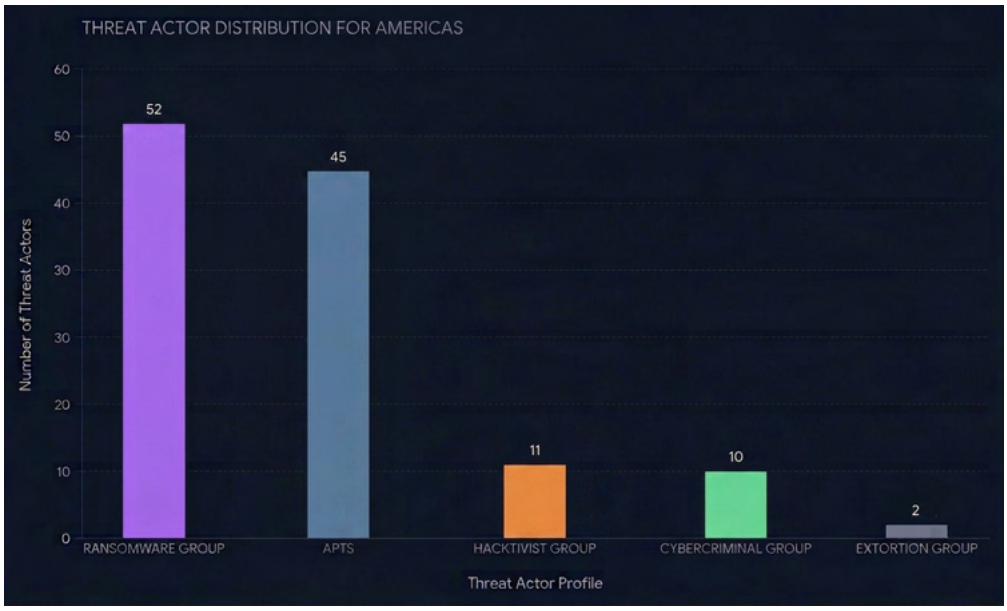


Fig 40: Threat Actor Distribution for Americas

The Americas show a ransomware-led profile (52 groups, 43%) consistent with the region's outsized share of global ransomware attack volume documented elsewhere in this report, closely followed by a substantial APT presence (45) led by China-linked espionage actors such as UNC6508 and Hammer Panda. Notably, the Americas recorded the highest cybercriminal group count of any region (10) — including Brazil-originated Lapsus$ — pointing to a maturing, home-grown cybercriminal ecosystem in South America that operates alongside, rather than purely in service of, the region's dominant ransomware economy.

Threat Actors to Watch

Name	Origin	Target Countries	Target Sectors
UNC6508 Espionage Group	**China**	Canada, United States	Government, Law Enforcement, Healthcare
Lapsus$	**Brazil**	Argentina, Brazil, United States, France, Portugal, and more	Government, Law Enforcement, IT, Retail, Technology
Doppel Spider	**Russia**	Barbados, Brazil, Chile, United States, India, Mexico, Portugal, Canada, and more	Agriculture, Automotive, Manufacturing, Metals, Minerals & Mining, Government, Law Enforcement, IT, Retail, Technology, Healthcare, Media, Real Estate, Education, Food & Beverages
Hammer Panda	**China**	Canada, United States, Chile, India, Hong Kong, Spain, Iran, Jordan, South Korea, Qatar, Morocco, Greece, Ukraine, and more	Aerospace & Defense, Energy & Utilities, Government, Law Enforcement

Read together, these regional splits reinforce a consistent theme: no single actor-type model applies globally. Asia-Pacific, Europe/UK, and MEA carry meaningful — in some cases near-equal — APT exposure alongside ransomware, meaning security programs there should weight threat intelligence and detection investment toward espionage tradecraft (living-off-the-land techniques, credential harvesting, long-dwell-time access) in addition to ransomware defenses. The Americas and, especially, Australia & New Zealand are comparatively ransomware-dominated, meaning defenses there should continue to prioritize the attack-surface, identity, and backup controls outlined in this report's ransomware sections. In every region, the specific named groups in the watchlists above represent the highest-confidence, highest-activity threats security teams should track for indicators of compromise, TTP updates, and targeting shifts through the remainder of 2026.

Regional Trends

CRIL researchers broke the worldwide activity down across five regional groupings — Americas, Europe & UK, Asia-Pacific, Middle East & Africa, and Australia & New Zealand — each covering initial access sales, data breaches, ransomware, and hacktivism specific to that region to provide granular and region-specific analysis of threats and actors.

Americas

The Americas grouping covers North America and South America separately below, given differing threat actor concentration, sector targeting, and regional geopolitics.

North America

1,981	35	9
Ransomware Attacks	Data Breach Incidents	Access Listings

Key Highlights

- A small number of prolific threat actors and RaaS groups dominate the landscape: **'redpin' and 'xpl0itrs' account for the near entirety of initial access listings, while Qilin and Akira alone are responsible for over half of all recorded ransomware attacks.**
- **Threat actors persistently exploit zero-day and known vulnerabilities in internet-facing enterprise platforms** — including Ivanti and Palo Alto Networks products — as a primary initial access vector.
- **Technology and BFSI are the leading targets for data breaches**, while operationally sensitive sectors — Professional Services, Manufacturing, and Healthcare — bear the brunt of ransomware; Agriculture & Livestock industry has emerged as a notable initial-access target, pointing to growing risk in the food supply chain.
- Ransomware activity carries direct regional relevance: **The Gentlemen group targeted entities in Central America and the Caribbean**, including Panama's social security agency, while geopolitical hacktivism channels focus specifically on events in El Salvador and Costa Rica.

Overview

The North American cyber threat landscape in H1 2026 was defined by a high volume of ransomware activity, a concentrated initial access market, and sustained data breach activity concentrated in Technology, BFSI, and Agriculture & Livestock. CRIL recorded 1,981 ransomware attacks, 35 data breach and leak incidents, and 9 initial access sale listings impacting the region during the period — figures that place North America among the most heavily targeted geographies in this report.

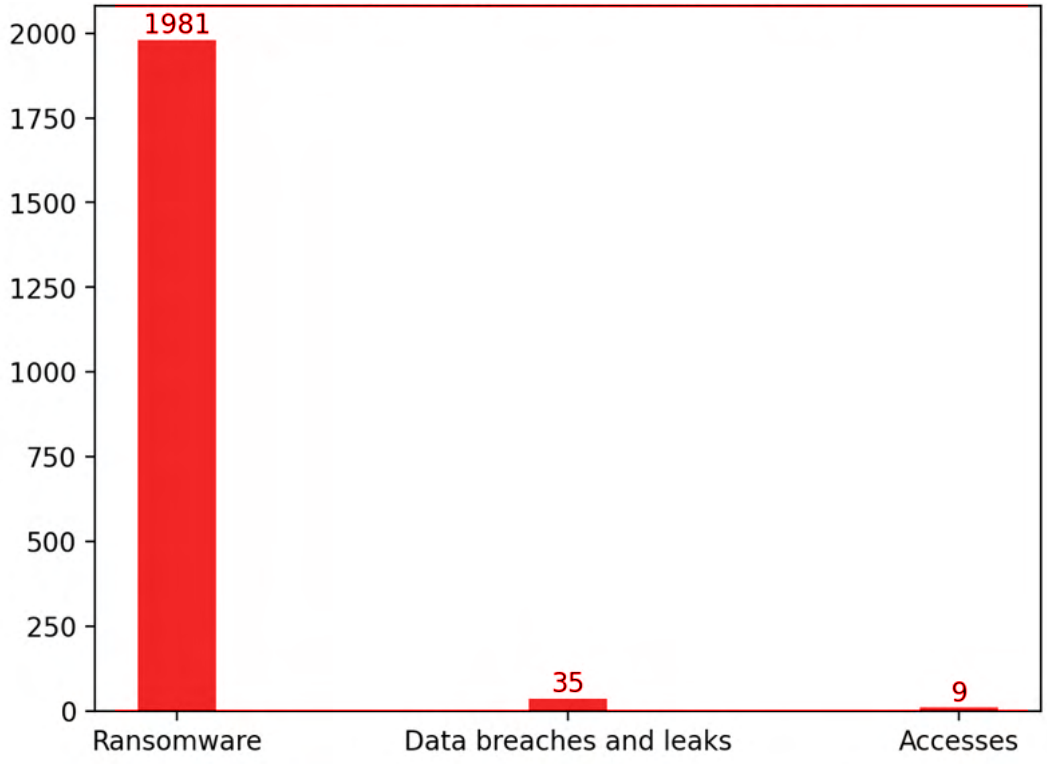


Fig 41: Cybercrime Incidents in North America in H1 2026

Data Breach and Leaks

CRIL observed 35 data breach and leak incidents in North America during H1 2026. Technology and BFSI were the most frequently targeted, together accounting for approximately 43% of incidents (Technology ~23%, BFSI ~20%) — driven by threat actor interest in intellectual property, customer PII, and monetizable financial data.

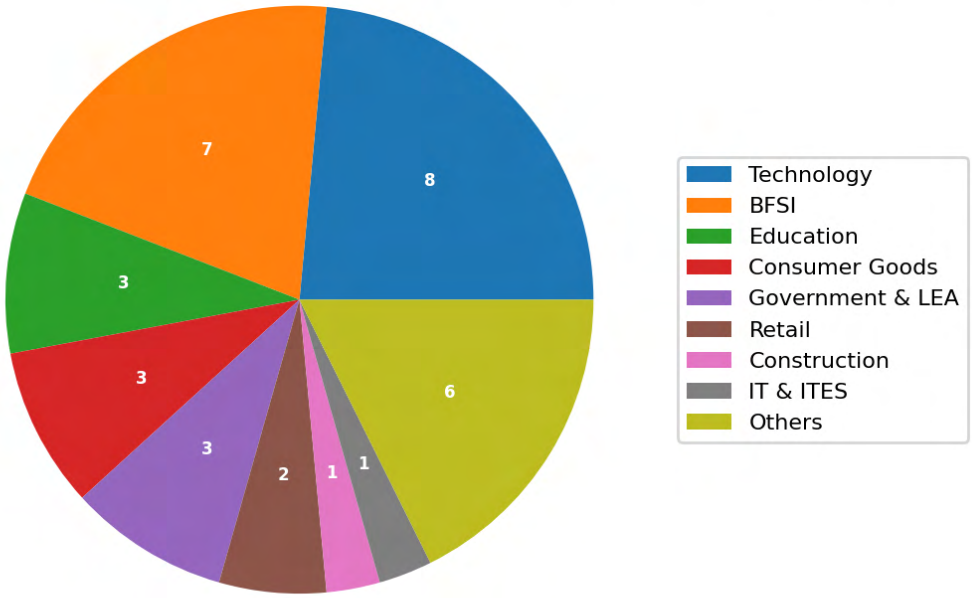


Fig 42: Data Breaches Across Industries

The threat actor 'tanaka' was the most active (7 posts), followed by 'respublica' (5) and 'frog' (4) — together responsible for nearly half of all observed activity. A long tail of single-post actors rounds out a broad, opportunistic ecosystem.

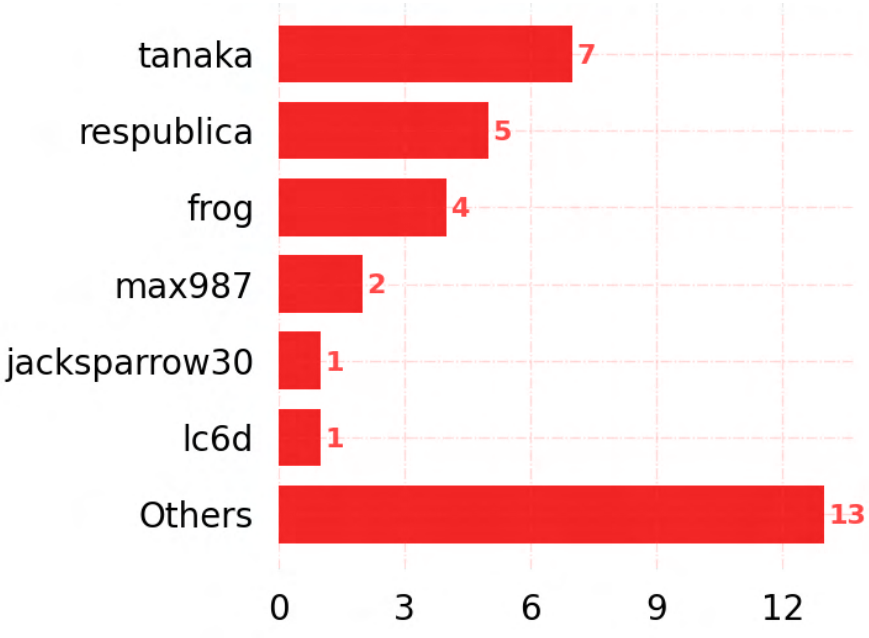


Fig 43: Active Threat Actors Selling Data Breaches

Online Access Sale

CRIL identified 9 initial access sale incidents targeting the region. Technology accounted for roughly 56% of listings, followed by Agriculture & Livestock at 33% — reflecting both the value of technology-sector IP and growing threat actor interest in food-supply-chain disruption.

The market was highly concentrated. 'redpin' alone was responsible for approximately 67% of listings, with 'xpl0itrs' accounting for the remaining third — a structure dominated by a very small number of key sellers rather than a fragmented marketplace.

Ransomware

Overview

CRIL observed 1,981 ransomware attacks impacting North America during H1 2026, reflecting a mature, persistently active RaaS ecosystem operating at high volume across a wide range of industries and geographies within the region.

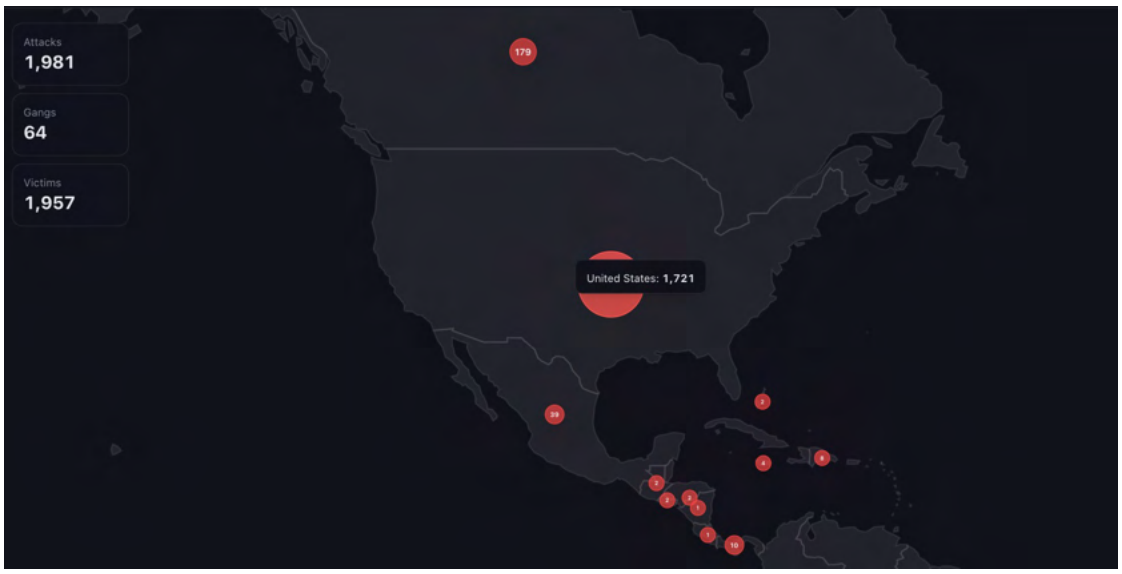


Fig 44: Distribution of Ransomware Attacks in North America (H1 2026)

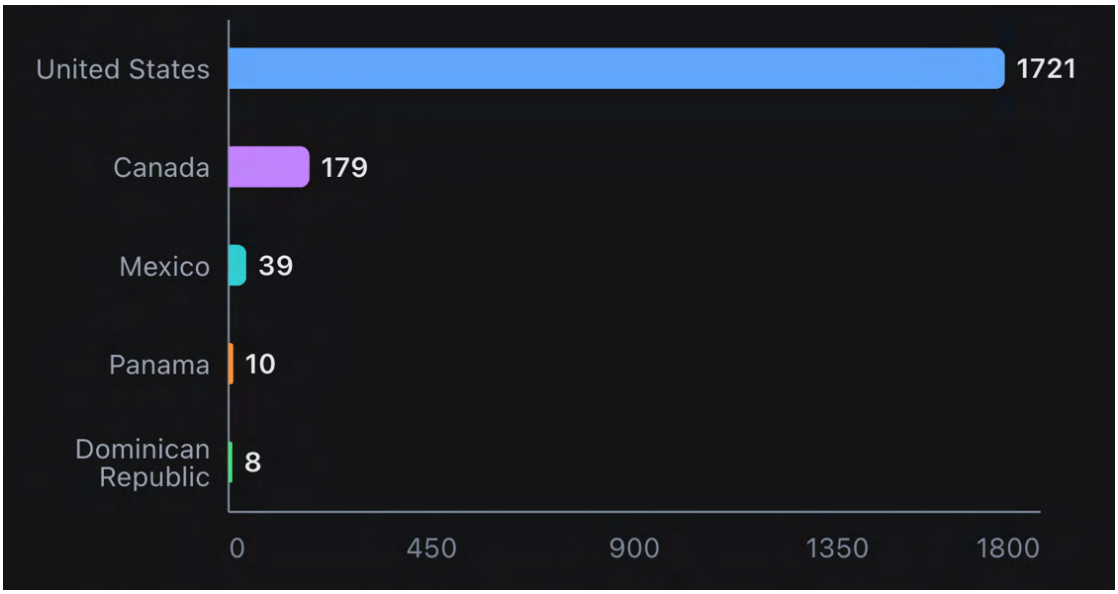


Fig 45: Top Five Countries Targeted in North America

Dominant Ransomware Groups

Qilin, Akira, INC Ransom, Dragonforce, and Play — the top five most active groups — collectively accounted for approximately 55% of all observed incidents. Qilin was the single most prolific, responsible for 370 attacks (nearly 19% of the total), followed by Akira (268 attacks) and INC Ransom (164 attacks).

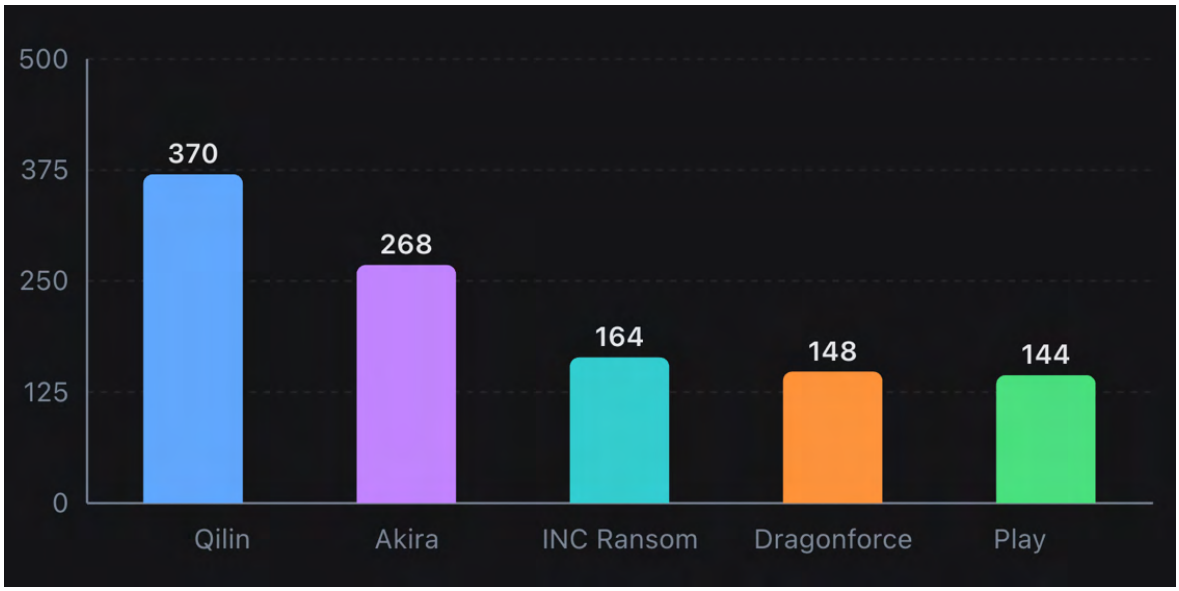


Fig 46: Most Active Ransomware Actors Targeting North America

Impact Analysis

Professional Services was the most heavily impacted sector, followed by Construction, Manufacturing, and Healthcare. INC Ransom and AiLock drove much of the Professional Services impact (including a clear preference by INC Ransom for law firms), while high-tempo groups like Akira and Play concentrated on Construction and Manufacturing. AiLock's activity stood out for a coordinated wave of victim disclosures on a single day (March 3, 2026), and LockBit maintained a steady tempo against public and educational sector targets.

Hacktivism

Hacktivist activity in North America was driven by a mix of geopolitical and socio-political motivations, with collectives including SOLDADOS DIGITALES – UNIÓN AMERICANA, Anonymous #FreeTurtleIsland, KERALA HACKERS, and LYSTIC TEAM #ID among the most prominent. DDoS attacks, defacements, and data leaks were the primary tactics, with approximately 56 data leak or dump posts observed and roughly 360 unique domains impacted. Targeting spanned Government & LEA, Technology, BFSI, and Telecommunication, with additional activity against Aerospace & Defense and Energy & Utilities entities.

South America

207	8	11
Ransomware Attacks	Data Breach Incidents	Access Listings

Key Highlights

- Three ransomware gangs — **The Gentlemen, Qilin, and LockBit — were responsible for over 57% of all observed attacks**, and three initial access brokers accounted for roughly 63% of listed access sales, reflecting a highly concentrated regional threat ecosystem.
- **Government, Healthcare, and Financial Services were relentlessly targeted** across ransomware, data breaches, and state-sponsored activity, pointing to significant risk for the region's critical infrastructure and public data.
- **Brazil emerged as a focal point for sophisticated financial malware, with new Android trojan families** — TCLBANKER and BTMOB RAT — using self-propagation, evasion, and Malware-as-a-Service (MaaS) distribution to target banking and cryptocurrency users.
- Threat actors consistently exploited critical and zero-day vulnerabilities in enterprise products from Ivanti, Cisco, and Fortinet as a primary route to initial network access.

Overview

South America's H1 2026 threat landscape was shaped by high-volume ransomware campaigns from The Gentlemen, Qilin, and LockBit; a concentrated initial access brokerage market; and a more fragmented data breach landscape highlighted by the alleged 250-million-record Serasa breach in Brazil and an access sale allegedly targeting the Central Bank of Brazil. CRIL recorded 207 ransomware attacks, 8 data breach and leak incidents, and 11 initial access sale listings for the region during the period.

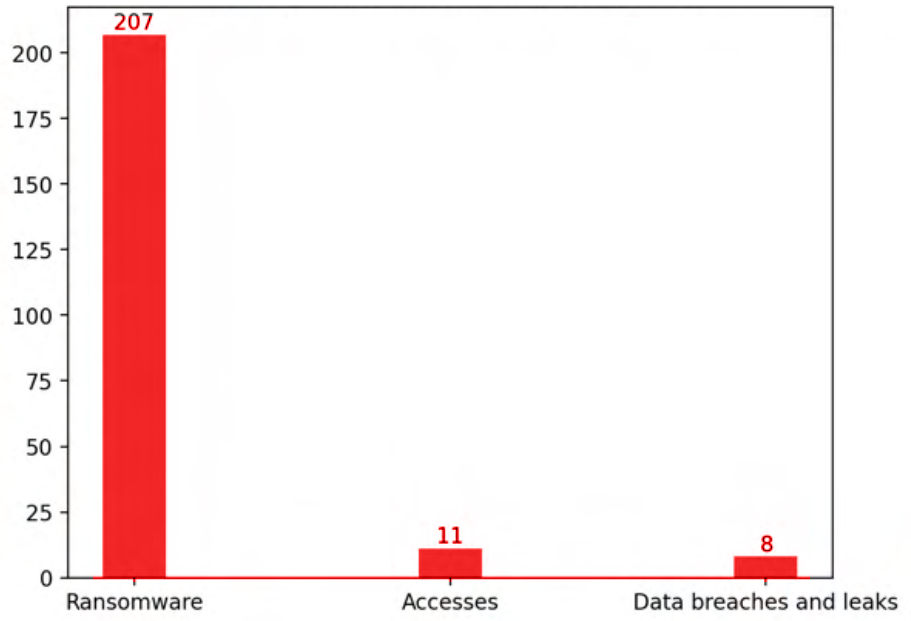


Fig 47: Cybercrime Incidents in South America (H1 2026)

Data Breach and Leaks

CRIL identified 8 significant data breach and leak incidents. Government & Law Enforcement was the most frequently targeted sector (25% of incidents), with the remainder distributed across BFSI, Retail, Transportation & Logistics, and Technology.

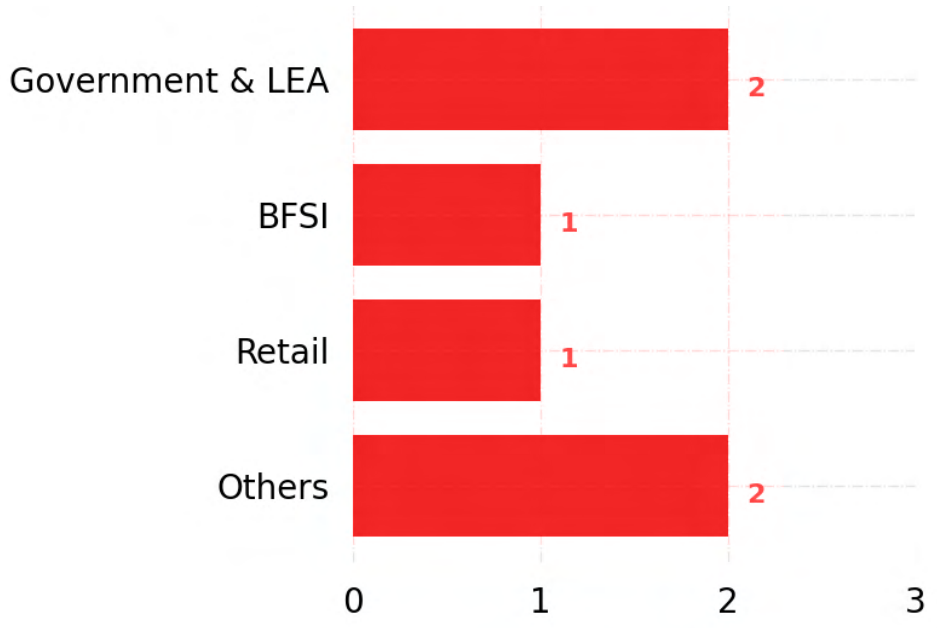


Fig 48: Data Breaches Across Industries in South America

'xorcat' was the most prolific actor with two incidents; the remainder of activity was spread thinly across actors including 'pijush507', 'saofurtencio', 'gordonfreeman', 'tanaka', and 'blastoize' — a fragmented landscape with no single dominant actor.

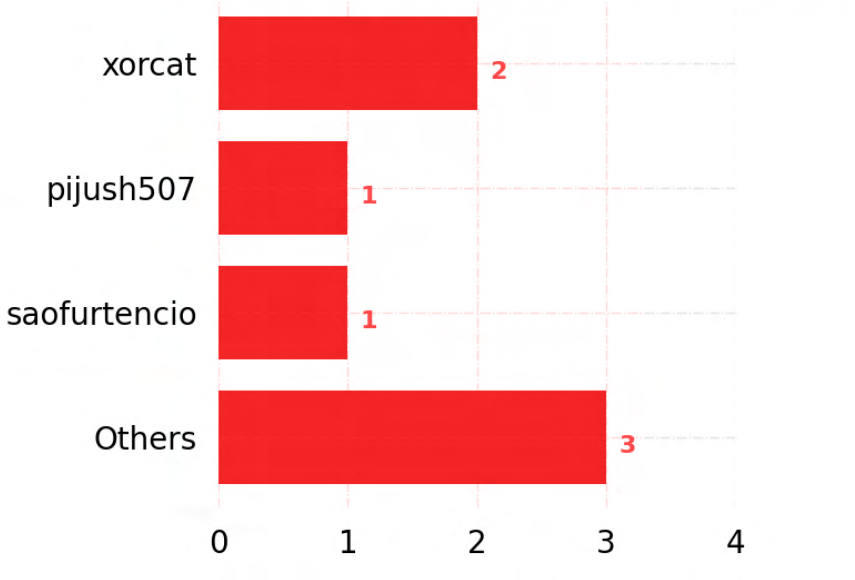


Fig 49: Active Threat Actors Selling Data Breaches

Online Access Sale

CRIL observed 11 initial access sale incidents. Retail and Professional Services were the most frequently targeted, each accounting for four listings (40% combined) — reflecting broker interest in both customer payment data and corporate client information.

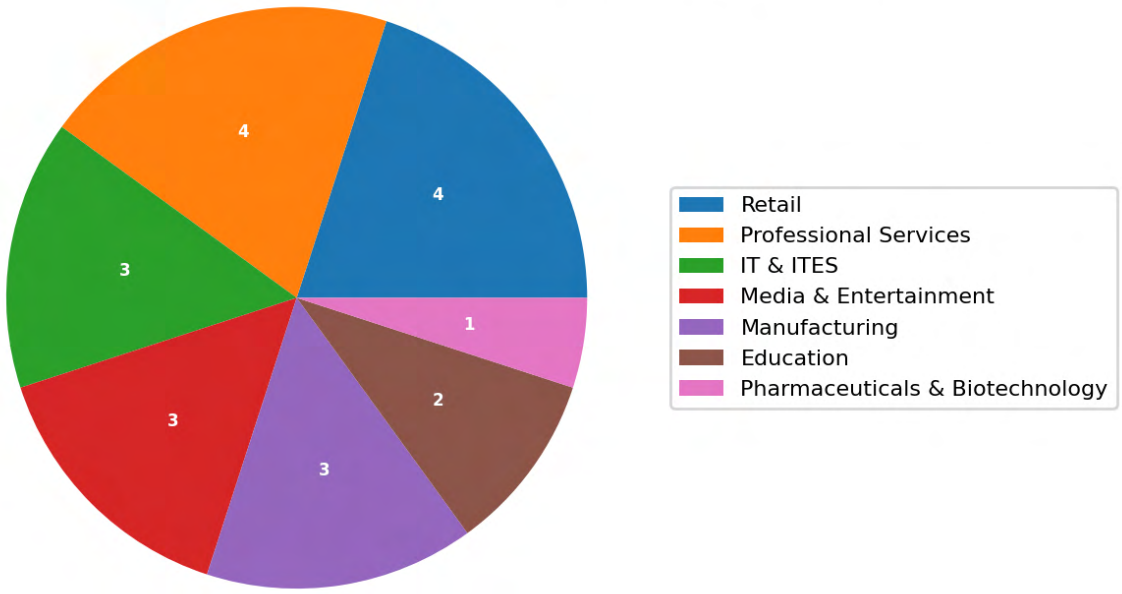


Fig 50: Compromised Accesses Across Industries in South America

'sanguine' led the market with three listings, followed by 'holyduxy' and 'vexin' with two each; together the top three accounted for over 63% of observed offerings, with the remainder fragmented among opportunistic single-post sellers.

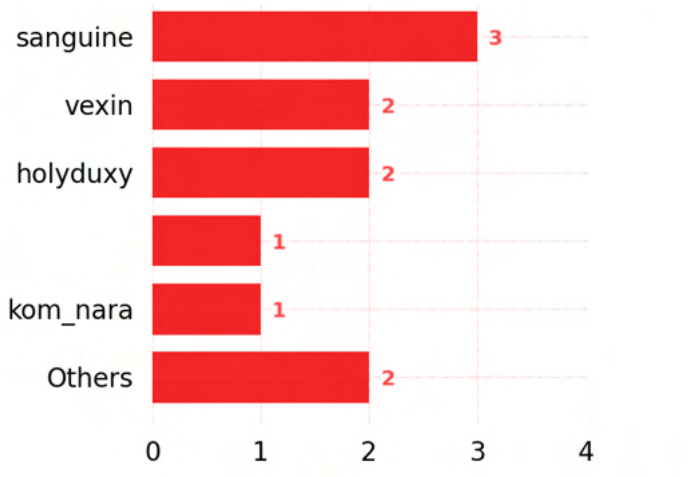


Fig 51: Active Threat Actors Selling Compromised Access

Ransomware

Overview

CRIL recorded 207 ransomware attacks impacting the region, with more than 30 distinct groups active — evidence of a dynamic ecosystem with a low barrier to entry alongside a small set of dominant operators.

Fig 52: Distribution of Ransomware Attacks in North America (H1 2026)

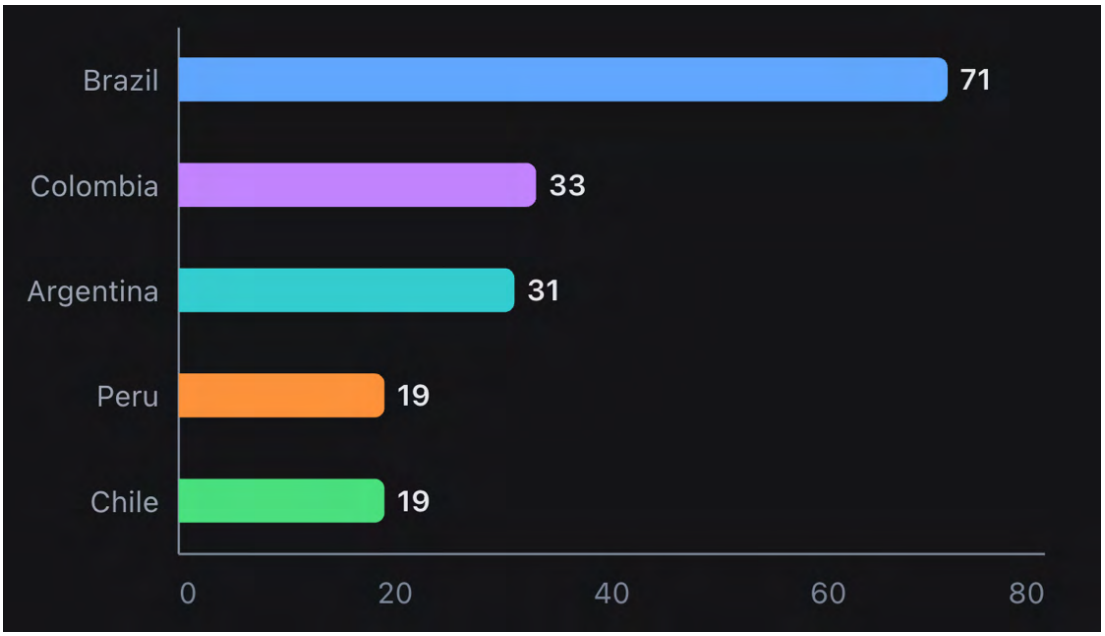


Fig 53: Top Five Countries Targeted in South America

Dominant Ransomware Groups

The Gentlemen, Qilin, and LockBit collectively accounted for 119 incidents (approximately 57.5% of all attacks): The Gentlemen led with 46 attacks, followed by Qilin (40) and LockBit (33). A second tier of active groups — RALord/Nova, Vect, and Krybit — contributed consistent, if lower-volume, pressure.

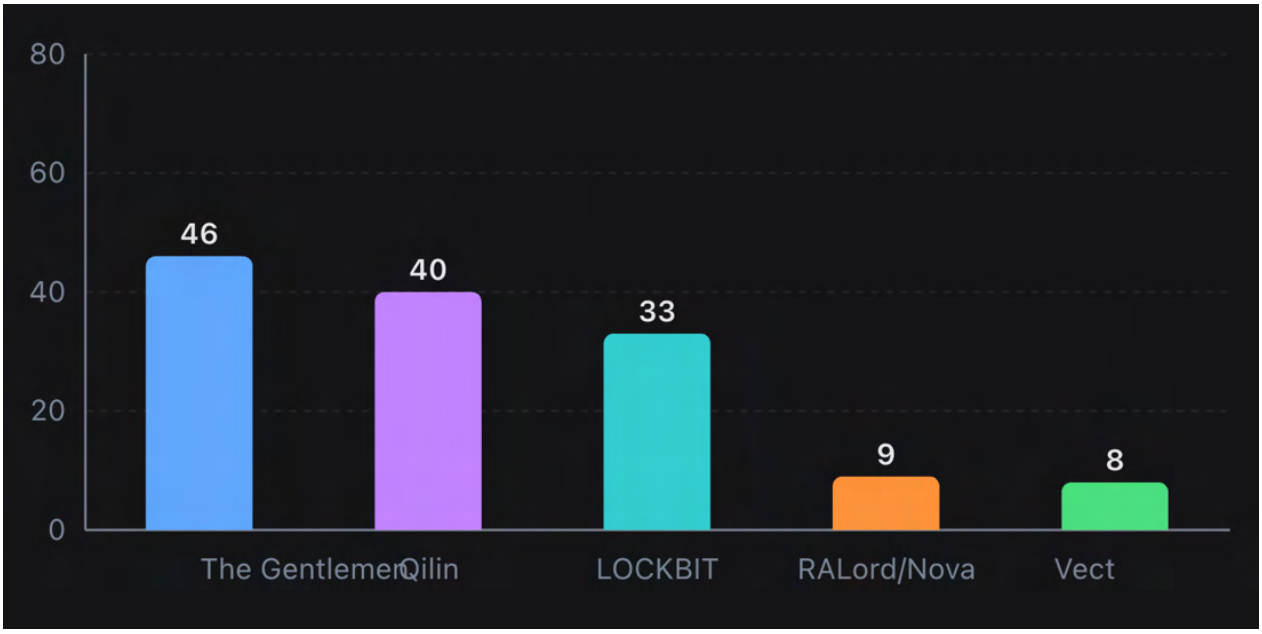


Fig 54: Most Active Ransomware Actors Targeting South America

Impact Analysis

IT & ITES, Healthcare, Professional Services, and Energy & Utilities were the most heavily impacted sectors. Healthcare incidents included The Gentlemen's attack on Primero Medicina Privada and LockBit's compromise of Clínica Dávila; government and law enforcement bodies were also frequently targeted, as in RALord/Nova's attack on Peru's SUNASS and CoinbaseCartel's attack on Ecuador's Superintendencia de Ordenamiento Territorial.

Hacktivism

Hacktivism in South America was dynamic and high-volume, fueled by geopolitical and socio-political agendas. SOLDADOS DIGITALES – UNIÓN AMERICANA, Anonymous Colombia (#OpColombia) Y.A.N, and "BLAZER TEAM ATTACK" were among the most prominent collectives, with website defacements and DDoS attacks as the predominant tactics, supplemented by approximately 84 data leak or dump posts. The campaigns impacted at least 572 unique domains, with a notable concentration of attacks against Government & LEA, Education, Technology, and BFSI.

Europe and UK

866	51	7
Ransomware Attacks	Data Breach Incidents	Access Listings

Key Highlights

- The cybercrime landscape was **dominated by a concentrated set of highly prolific actors** — Qilin in ransomware and 'tamnaamm' in initial access sales — underscoring a top-heavy ecosystem.
- **Rapid weaponization of critical zero-day vulnerabilities** in internet-facing enterprise products, particularly network and security appliances, served as a primary initial access vector for both state-sponsored and financially motivated actors.
- **Geopolitically motivated hacktivism, driven primarily by pro-Russian groups**, evolved beyond disruptive DDoS attacks to include targeting of Industrial Control Systems (ICS) and critical infrastructure — blending cyber operations with hybrid-warfare objectives.
- Threat actors demonstrated clear sector-based targeting logic: **ransomware groups favored Manufacturing and Construction for their low downtime tolerance**, while data breaches concentrated on BFSI and Telecommunication for their PII and financial data value.

Overview

Europe and the UK experienced a high-tempo threat landscape in H1 2026, driven by a concentrated set of threat actors operating across ransomware, data breaches, and initial access sales.

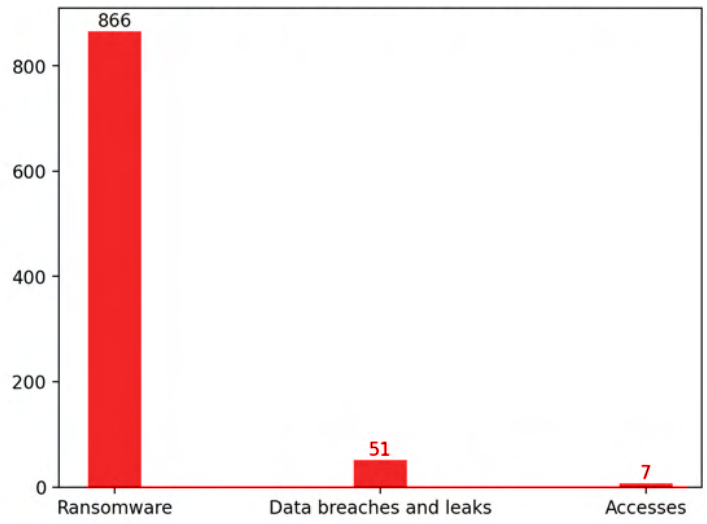


Fig 55: Cybercrime Incidents

CRIL recorded 866 ransomware attacks, 51 data breach and leak incidents, and 7 initial access sale listings for the region — with Qilin and LockBit heavily targeting Manufacturing, Construction, and Professional Services, and BFSI, Telecommunication, and Retail bearing the brunt of data breaches. Geopolitically motivated hacktivism, led by pro-Russian groups such as NoName057(16), continued to disrupt European critical infrastructure and government agencies through DDoS campaigns.

Data Breach and Leaks

CRIL observed 51 data breach and leak incidents impacting the region. BFSI and Telecommunication were each responsible for roughly 17.6% of incidents, with Retail close behind at nearly 15.7% — together these three sectors accounted for over half (51%) of all observed breaches, reflecting the high value of the PII, financial records, and payment data they hold.

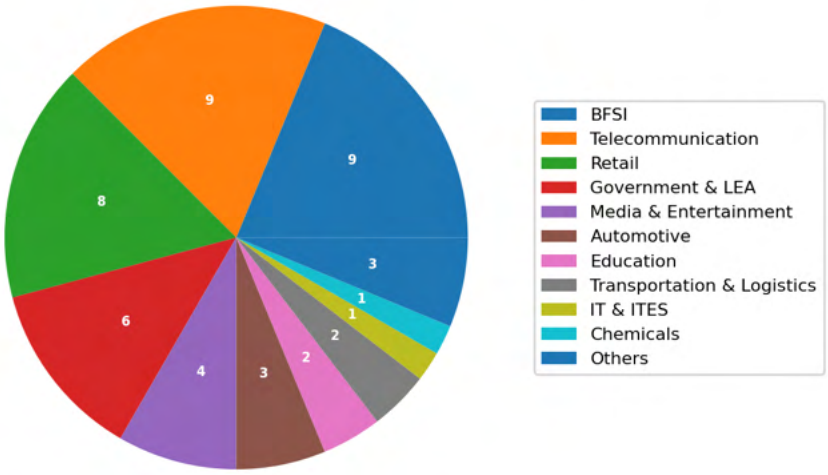


Fig 56: Data Breaches Across Industries

'tanaka' was the most prolific actor (6 posts), followed by 'kazutlg' (4); a secondary tier — 'ken6k', 'zoozkooz', 'aslan1', and 'darkcybervault' — each posted twice. 'ken6k' ran a sustained, six-month campaign against BFSI targets in the UK and Belgium, while 'aslan1' ran a short, highly focused operation against Telecommunication in the Netherlands.

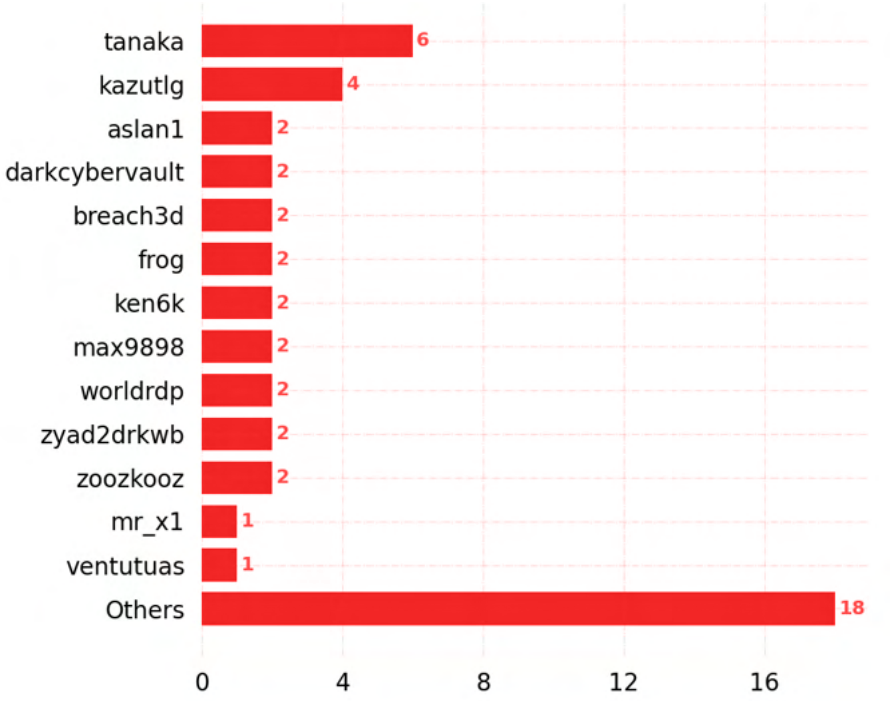


Fig 57: Active Threat Actors Selling Data Breaches

Online Access Sale

CRIL identified 7 initial access sale incidents. Agriculture & Livestock was the most frequently targeted sector, followed by a notable concentration against IT & ITES, Professional Services, and Government & LEA — reflecting strategic interest in both critical infrastructure and high-value supply-chain entry points.

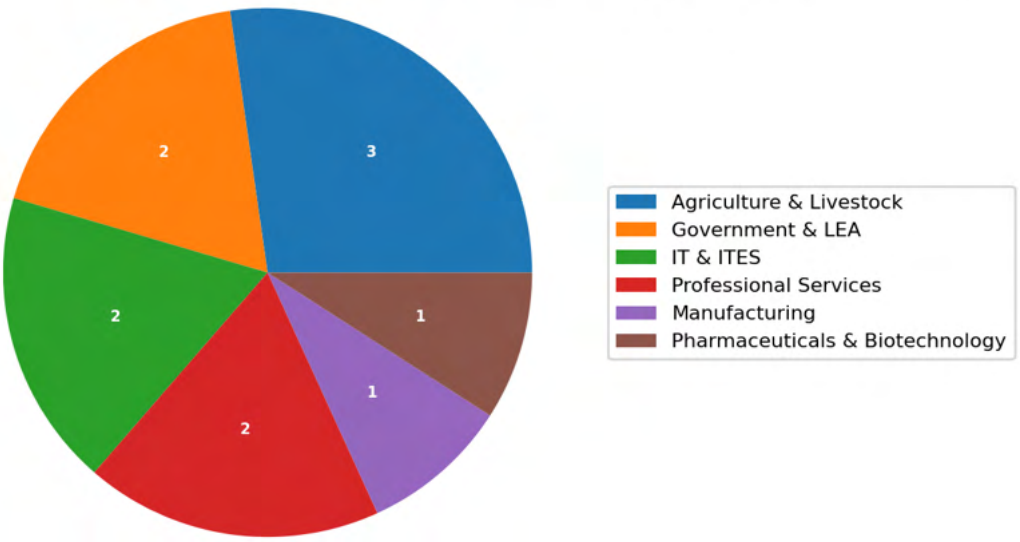


Fig 58: Compromised Accesses Across Industries

'tamnaamm' and 'algoyim' together accounted for approximately 71% of listings, with 'holyduxy' contributing at a lower volume — a market structure dominated by a very small number of key players.

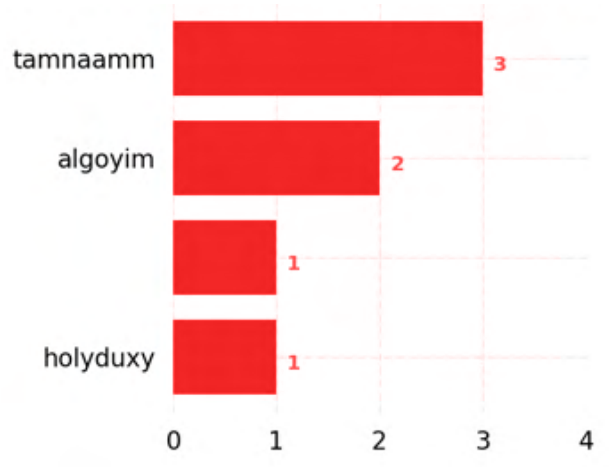


Fig 59: Active Threat Actors Selling Compromised Access

Ransomware

Overview

CRIL observed 866 publicly claimed ransomware attacks across Europe and the UK in H1 2026 — the highest regional total covered in this report — underscoring the persistent, evolving threat ransomware poses across the region's diverse economies.

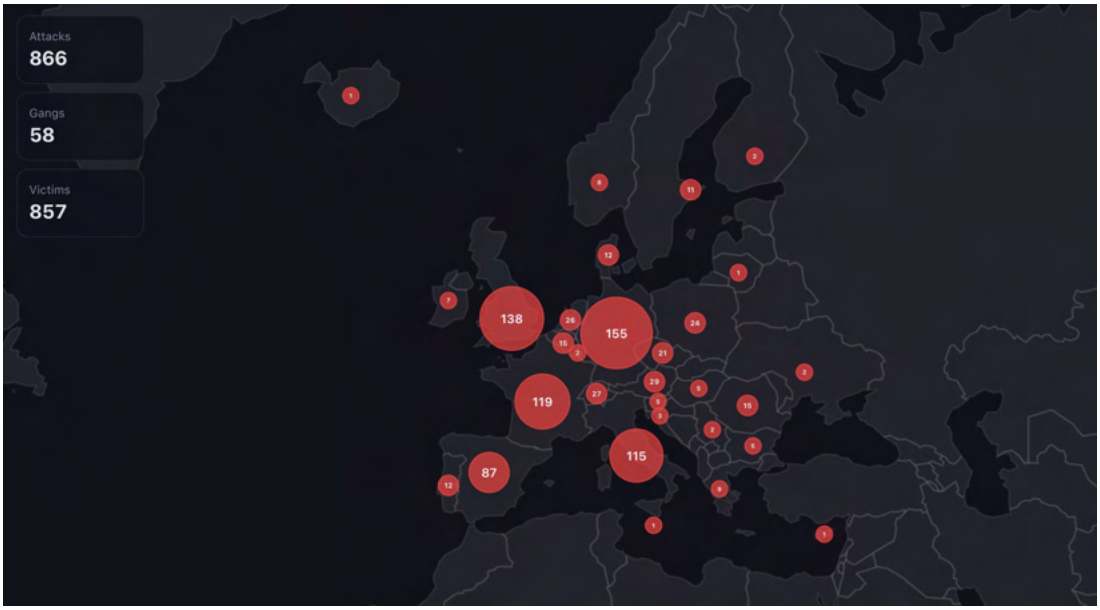


Fig 60: Distribution of Ransomware Attacks in Europe and UK (H1 2026)

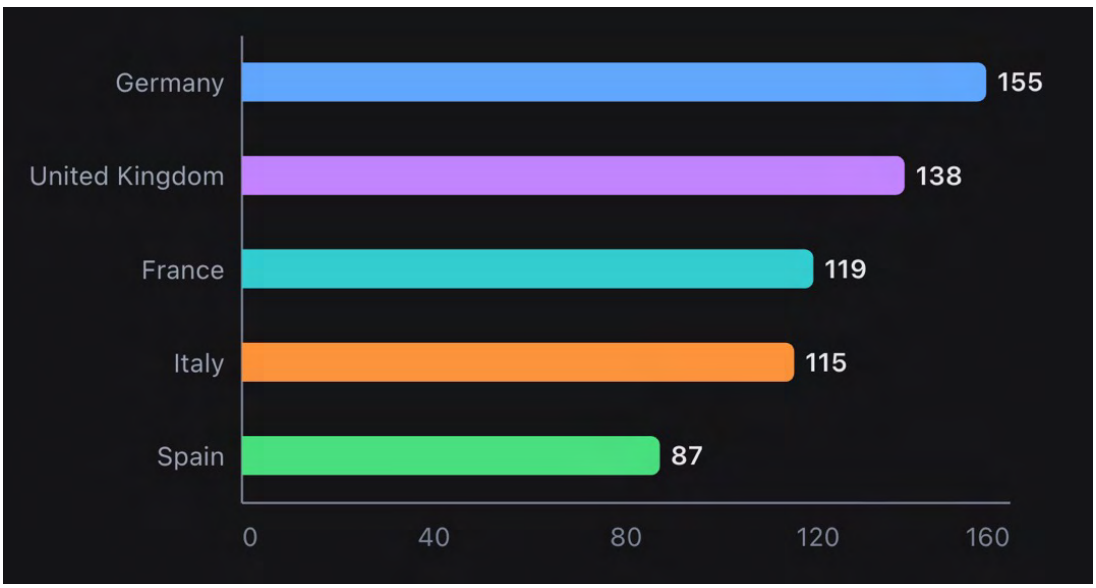


Fig 61: Top Five Countries Targeted in Europe and UK

Dominant Ransomware Groups

Qilin (158 attacks), The Gentlemen (144), and LockBit (61) accounted for over 41% of all activity; extending to Akira (59) and DragonForce (54) brings the top five to nearly 55% of all incidents. Beyond these leaders, a long tail of over 30 groups recorded only a single attack each, pointing to a dynamic ecosystem of smaller affiliates, rebrands, and new entrants.

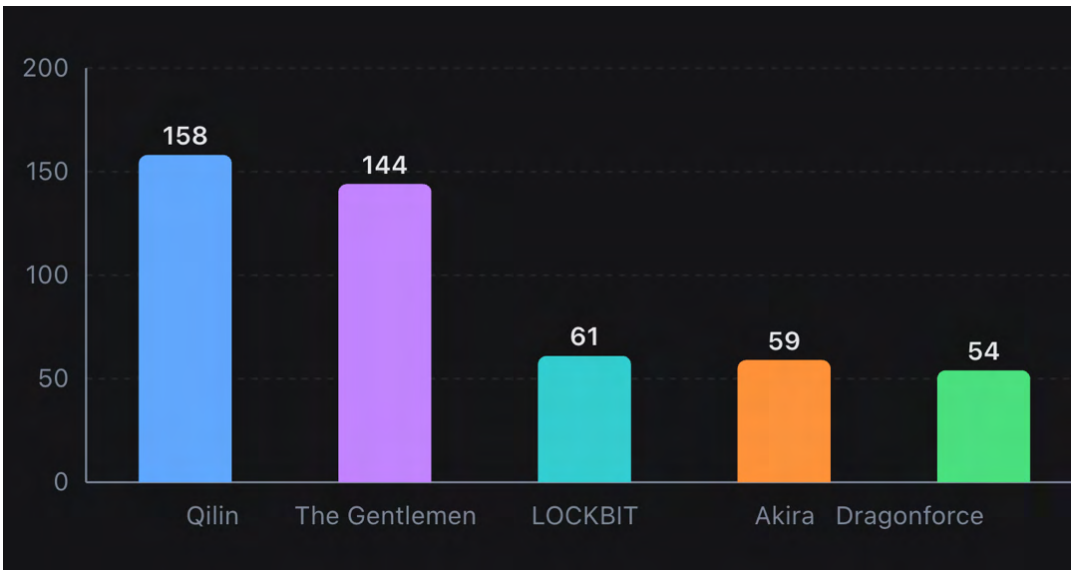


Fig 62: Most Active Ransomware Actors Targeting Europe and UK

Impact Analysis

Manufacturing, Construction, Professional Services, and IT & ITES were the most consistently targeted sectors. Akira showed a strong preference for Construction and Manufacturing (including victims such as MOTORPAL, a.s. and Murnane & O'Shea Ltd), while dominant groups like Qilin and The Gentlemen targeted a diverse range of industries — from Healthcare and Government to Retail and Transportation — reflecting an opportunistic rather than niche approach.

Hacktivism

H1 2026 saw significant, geopolitically charged hacktivism across the region, led by pro-Russian groups NoName057(16) and Russian Legion, alongside Homeland Justice, Anonymous Switzerland, and Darkstormteam. DDoS attacks and data exfiltration were the primary tactics, with approximately 86 data leak and dump posts observed and at least 916 unique domains impacted. Targeting concentrated on Government & LEA, Aerospace & Defense, Energy & Utilities, and BFSI — a pattern consistent with hacktivist operations aligning with broader geopolitical conflict.

Asia and Pacific

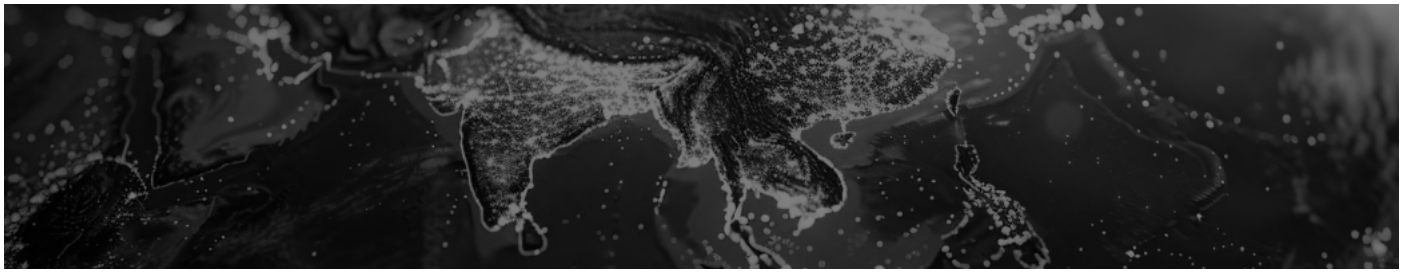
496	19	20
Ransomware Attacks	Data Breach Incidents	Access Listings

Key Highlights

- A small number of highly prolific threat actors and ransomware groups drove a disproportionate share of activity: the top three ransomware gangs accounted for over 43% of all attacks, and a few key actors dominated both the initial access a nd data-leak markets.
- Government and Law Enforcement entities were the leading target for data breaches, while Manufacturing bore the brunt of ransomware, and Retail and Professional Services were most affected by initial access sales.
- Supply chain attacks and evasion techniques grew more sophisticated, with campaigns compromising trusted software updates, weaponizing developer tools like Visual Studio Code for covert access and exploiting AI distribution platforms such as Hugging Face as a new malware delivery vector.
- The network edge remains a critical battleground: threat actors persistently exploited high-severity and zero-day vulnerabilities in widely deployed VPNs, firewalls, and endpoint management systems as a favored initial access route.

Overview

The Asia-Pacific threat landscape in H1 2026 was defined by a high volume of ransomware, sophisticated supply-chain attacks, and a thriving initial access brokerage market. CRIL recorded 496 ransomware attacks, 19 data breach and leak incidents, and 20 initial access sale listings for the region.



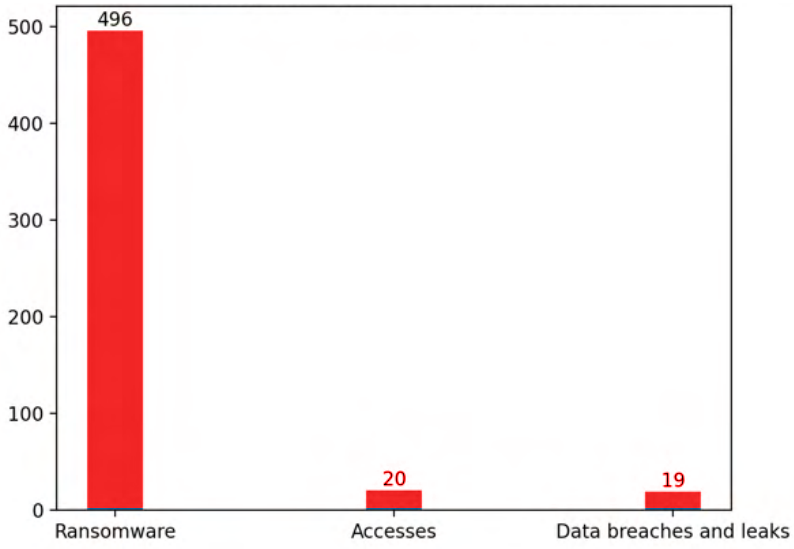


Fig 63: Cybercrime Incidents

Ransomware activity was dominated by The Gentlemen and Qilin, with Manufacturing, IT, and Professional Services the most heavily impacted sectors, while state-aligned actors demonstrated increasing sophistication by weaponizing kernel-mode rootkits, legitimate developer tools, and AI distribution platforms for scalable malware delivery.

Data Breach and Leaks

CRIL observed 19 data breach and leak incidents. Government & Law Enforcement (LEA) was the most frequently targeted, with 4 incidents (approximately 21% of total activity), followed by Media & Entertainment, IT & ITES, Retail, and Education (2 incidents each) — reflecting threat actor interest in both citizen data for intelligence gathering and commercial data for monetization.

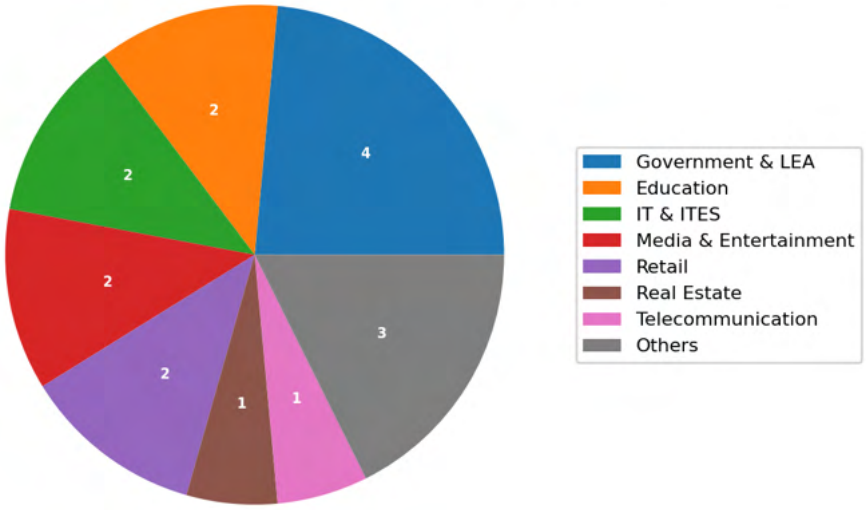


Fig 64: Data Breaches Across Industries

'jxq09' was the most prolific actor, followed closely by 'pixelphreak' and 'crowstealer'. 'jxq09' ran a short-duration, geographically focused campaign against commercial sectors (Real Estate and Retail) in Japan between early February and early March 2026, while 'SpicyRobot' conducted a highly concentrated single-week campaign focused on China in late February.

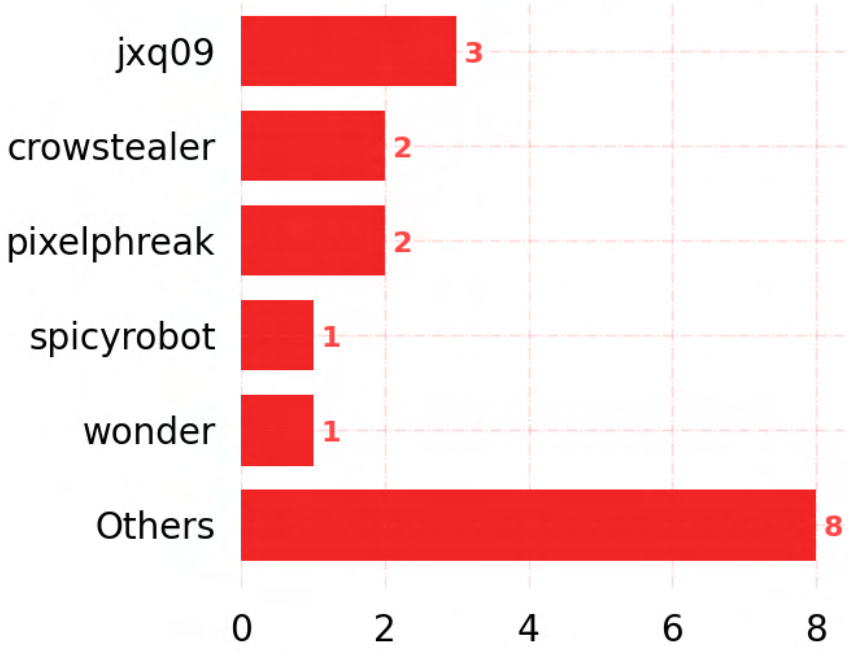


Fig 65: Active Threat Actors Selling Data Breaches

Online Access Sale

CRIL observed 20 initial access sale incidents. Retail and Professional Services were the most frequently targeted, together accounting for 50% of all listings — Retail for its customer and payment data, Professional Services for its sensitive client information and supply-chain potential.

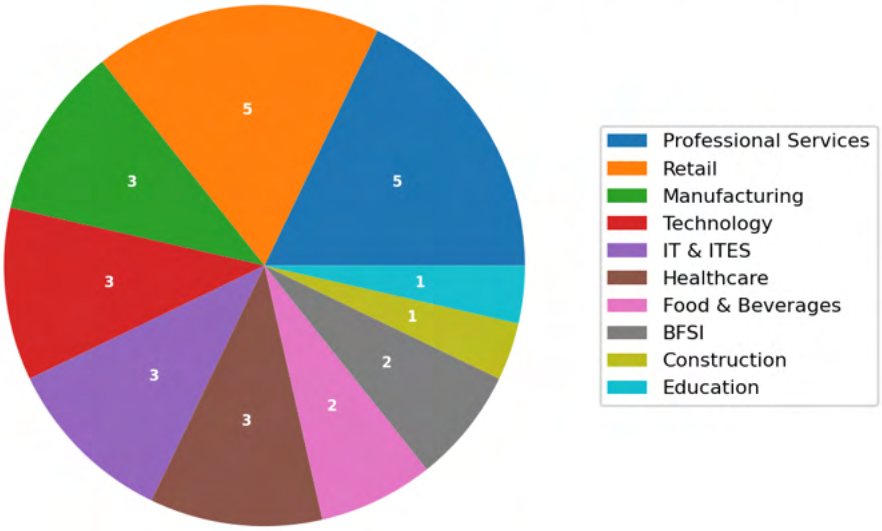


Fig 66: Compromised Accesses Across Industries

'sanguine' led the market with six listings, followed by 'karuhunters' (4) and 'redpin' (3); the top three actors accounted for 65% of all observed listings, with the remainder fragmented among lower-volume, opportunistic sellers.

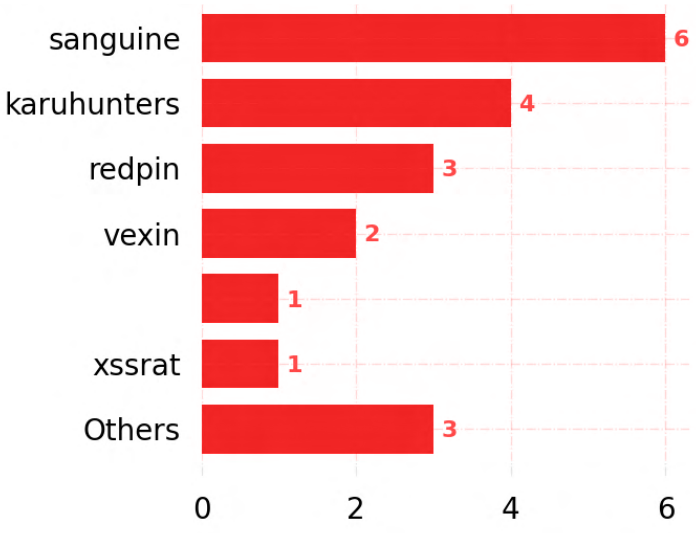


Fig 67: Active Threat Actors Selling Compromised Access

Ransomware

Overview

CRIL recorded 496 ransomware attacks across the region in H1 2026, with activity broadly distributed across Manufacturing and technology-related sectors, alongside concerning campaigns against public sector and critical infrastructure entities.

Fig 68: Distribution of Ransomware Attacks in Asia and Pacific (H1 2026)

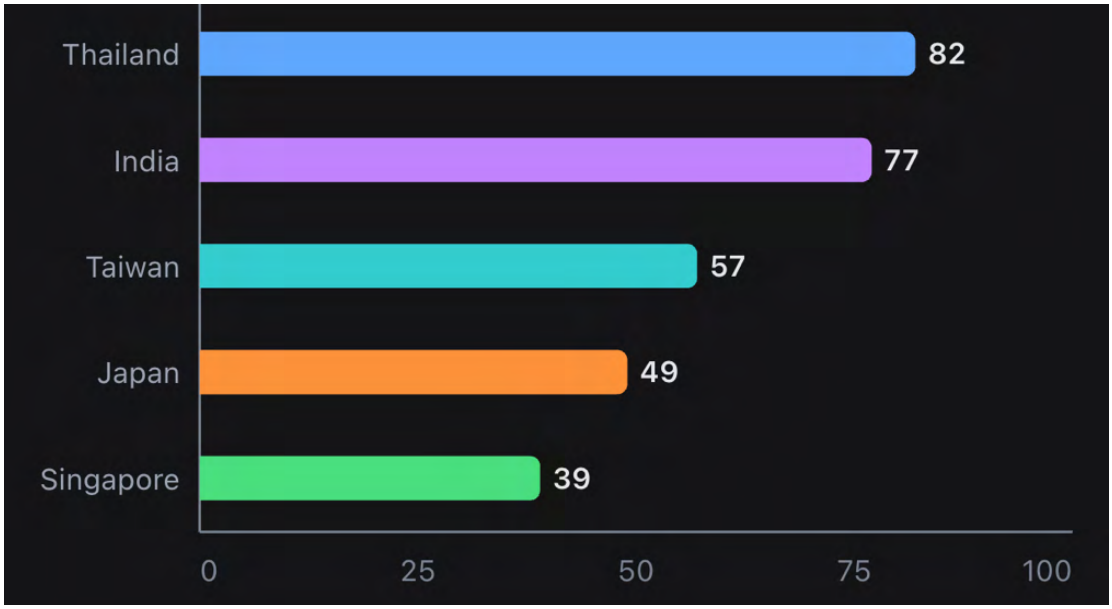


Fig 69: Top Five Countries Targeted in Asia and Pacific

Dominant Ransomware Groups

The Gentlemen, Qilin, and LockBit — the top three most active groups — were responsible for over 43% of all observed incidents. The Gentlemen was exceptionally prolific, claiming 114 victims (approximately 23% of the regional total), followed by Qilin (64 incidents, 13%) and LockBit (38 incidents, 7.7%).

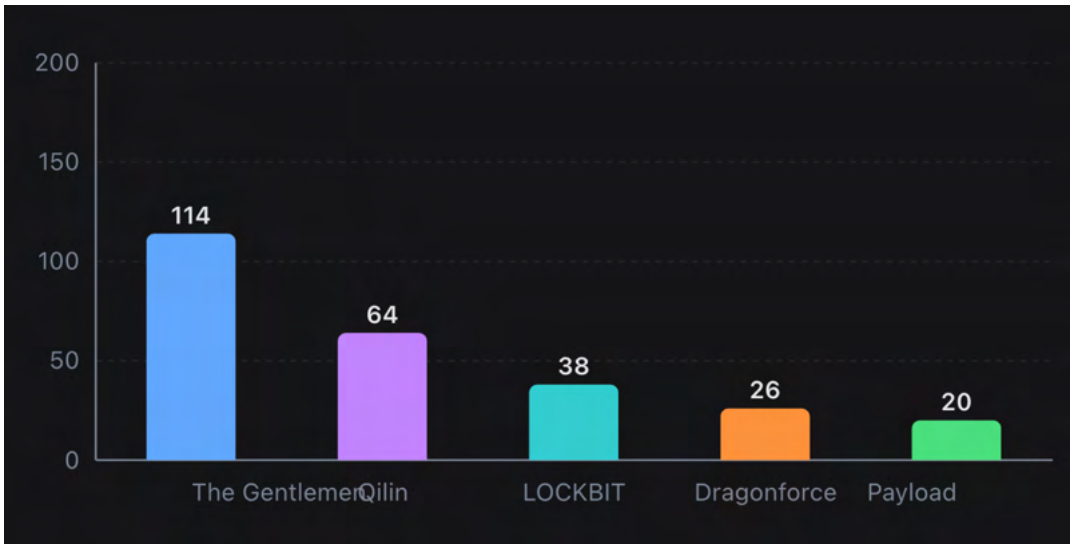


Fig 70: Most Active Ransomware Actors Targeting Asia and Pacific

Impact Analysis

Manufacturing was the most heavily impacted sector (at least 49 publicly claimed attacks), followed by IT & ITES (30), Consumer Goods (26), Professional Services (24), Healthcare (23), Construction (23), and BFSI (22). Notable manufacturing victims included Kawasaki Motors and Foxconn Technology Group. Government and public sector entities were also deliberately targeted — CoinbaseCartel focused on Indonesian ministries and RALord/Nova on multiple government and educational institutions — while the Netrunner group exclusively targeted healthcare organizations, including Shiraume Hospital and Nippon Medical School Musashi Kosugi Hospital.

Hacktivism

Hacktivism in APAC was characterized by a high volume of disruptive and opportunistic activity, primarily driven by collectives based in Southeast Asia — particularly Indonesia and Malaysia. Prominent groups included EXECUTOR NETWORK CO LTD, BROTHEROOD CAPUNG INDONESIA (B.C.I), Malaysia Hacktivist – Official, and Jav4nyM0uzCorp, using website defacements, DDoS attacks, and data exfiltration as primary tactics. CRIL observed over 4,500 unique domains targeted and approximately 700 distinct data leak posts, with victims spanning Government, Education, Technology, and Retail sectors — indicating a largely opportunistic targeting approach.

Middle East and Africa

211	16	1
Ransomware Attacks	Data Breach Incidents	Access Listings

Key Highlights

- Ransomware was dominated by a single highly active group: "**The Gentlemen" alone was responsible for over 26% of all attacks**, strategically targeting critical sectors including Construction, BFSI, and Government.
- State-sponsored and ideologically motivated cyber operations, particularly from **Iran-nexus threat actors, escalated in sophistication and destructive capability — deploying novel malware against government and critical infrastructure targets**, often in direct response to regional geopolitical conflict.
- **Government and Law Enforcement agencies were the most consistently targeted sector across multiple threat vectors** — the primary victims of data breach campaigns and frequent targets of both ransomware attacks and initial access brokers.
- A surge in critical, industry-agnostic vulnerabilities in **widely used enterprise network and security appliances was actively exploited in the wild**, establishing them as a primary initial access vector across the region.

Overview

The Middle East & Africa threat landscape in H1 2026 was dominated by high-volume ransomware activity, with over 211 attacks primarily impacting Construction, BFSI, and Government, concentrated around "The Gentlemen" group. CRIL recorded 211 ransomware attacks, 16 data breach and leak incidents, and 1 initial access sale listing for the region.

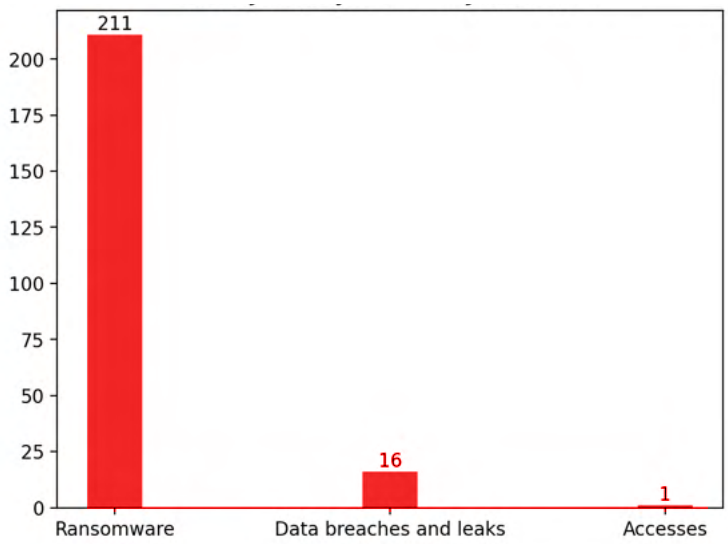


Fig 71: Cybercrime Incidents

Government and Law Enforcement was the most frequent data breach target, while sophisticated state-sponsored operations — particularly from Iran-nexus APT groups like MuddyWater — introduced novel malware such as RustyWater and ZionSiphon against targets in Israel, Iraq, and the broader Middle East.

Data Breach and Leaks

CRIL observed 16 data breach and leak incidents. Government & Law Enforcement (LEA) was the most frequently targeted sector, accounting for 5 incidents (over 31% of total observed breaches), followed by Retail with 3 incidents (nearly 19%) — reflecting threat actor interest in both citizen PII/national security data and monetizable customer data.

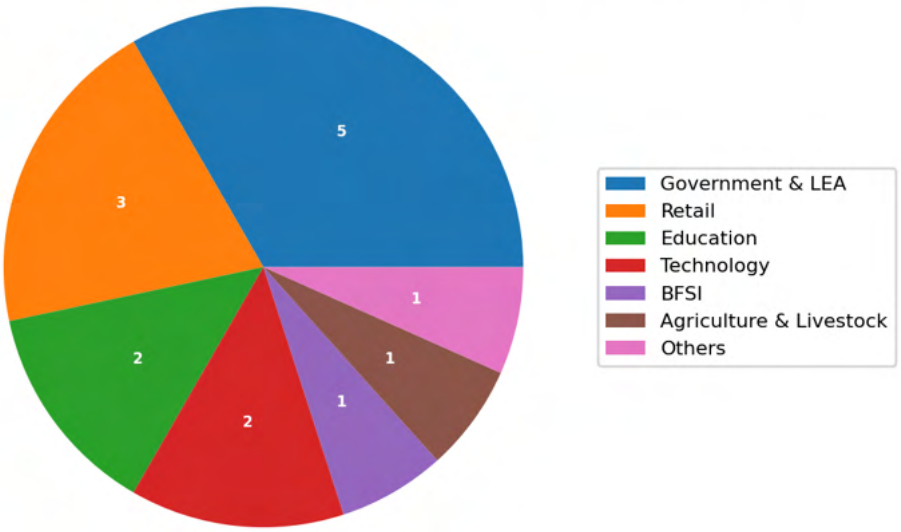


Fig 72: Data Breaches Across Industries

'crowstealer' was the most active, linked to two distinct leak posts; the remainder of the activity was thinly distributed across actors including 'blueex', 'roulettegun', 'frog', and 'bzaari'. 'BlueEx' targeted government entities in Algeria in January 2026, and 'bzaari' targeted the government sector in the Middle East in March — both consistent with espionage or geopolitical, rather than purely financial, motivations.

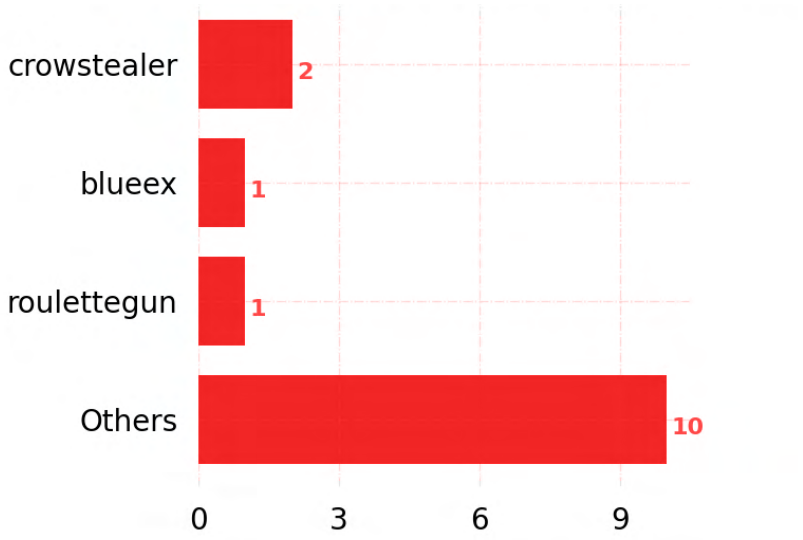


Fig 73: Active Threat Actors Selling Data Breaches

Online Access Sale

CRIL identified a single significant initial access sale incident during H1 2026, exclusively impacting the Transportation & Logistics sector. While limited in volume, this listing is notable for its potential to enable supply-chain disruption and follow-on ransomware attacks. The sole participant observed in this market segment was the threat actor 'xnov', pointing to a currently low-priority but not absent market for regional access brokerage.

Ransomware

Overview

CRIL observed 211 ransomware attacks impacting the region during H1 2026, with more than 30 distinct groups active — indicating a persistent and aggressive threat despite a lower overall regional volume than Europe or North America.

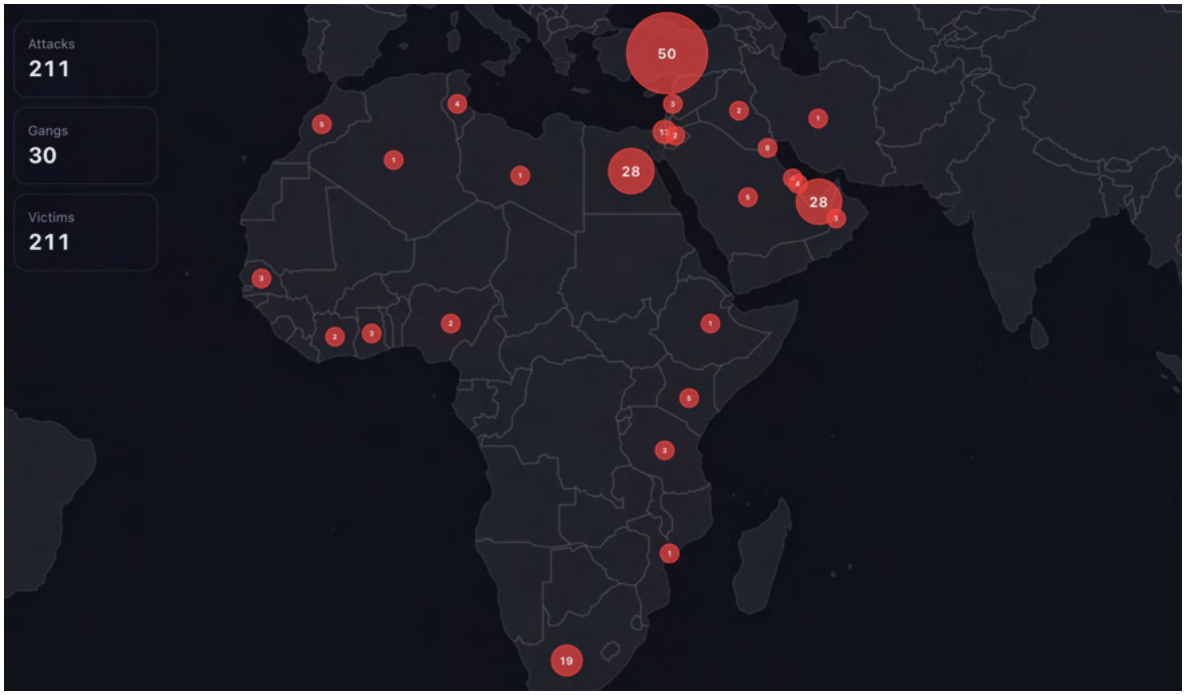


Fig 74: Distribution of Ransomware Attacks in Middle East and Africa (H1 2026)

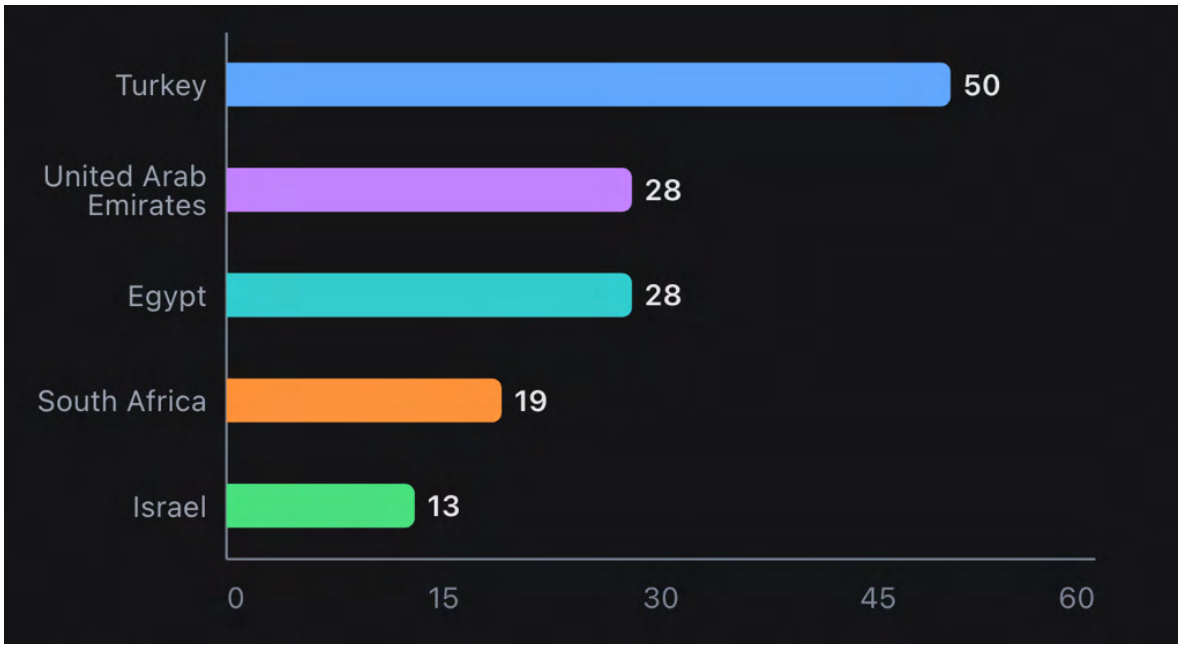


Fig 75: Top Five Countries Targeted in Middle East and Africa

Dominant Ransomware Groups

"The Gentlemen" was the dominant actor, claiming 56 incidents (approximately 26.5% of all attacks), followed by LockBit (20) and Qilin (19). Together, the top three groups accounted for 95 of 211 incidents — over 45% of total regional ransomware activity.

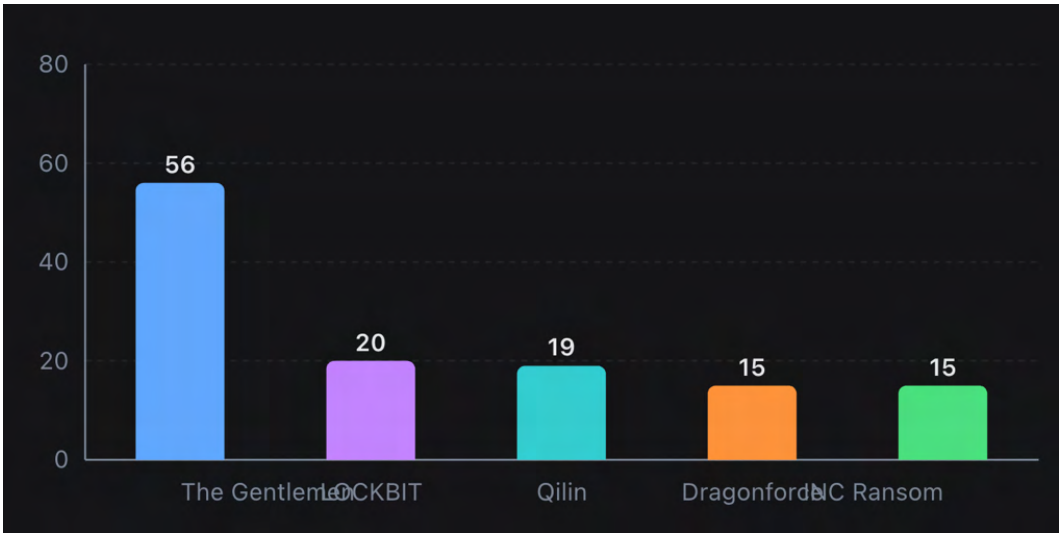


Fig 76: Most Active Ransomware Actors Targeting Middle East and Africa

Impact Analysis

Construction was the most heavily impacted sector (at least 21 organizations targeted), followed by BFSI (13 attacks) and Government & LEA (11 attacks). Notable incidents include the Audit Team group's attack on Direction Générale de la Comptabilité Publique et du Trésor (DGCPT) and Krybit's attack on the Court of Auditors of Senegal, alongside Qilin's targeting of the Central Bank of Libya and INC Ransom's compromise of Namibia Airports Company — showing ransomware groups successfully reaching critical infrastructure and major economic institutions.

Hacktivism

Hacktivist activity across the region was significant and driven primarily by geopolitical and socio-political motivation, involving DDoS attacks, website defacements, and substantial data exfiltration — evidenced by approximately 778 data leak and dump posts. The campaigns impacted at least 3,629 unique domains across Government & LEA, BFSI, Technology, and Healthcare. Prominent groups and channels included SOLDADOS DIGITALES – UNIÓN AMERICANA, Malaysia Hacktivist – Official, BENGKULU CYBER TEAM, and actors associated with campaigns such as #OpIsrael — reflecting a geographically diverse and ideologically varied landscape.

Australia and New Zealand

76	9	Limited
Ransomware Attacks	Data Breach Incidents	Access Listings

Key Highlights

- The ransomware landscape was dominated by a few prolific groups — **Qilin, CL0P, and The Gentlemen were responsible for nearly half of all attacks** — while the data breach and leak ecosystem was comparatively fragmented, driven by a diverse mix of moderately active and opportunistic actors.
- **BFSI was the primary data breach target**, accounting for 44% of observed incidents, while ransomware demonstrated broader impact — most frequently disrupting Healthcare, Professional Services, and IT.
- **Threat actors consistently exploited vulnerabilities in network infrastructure and widely used enterprise applications**, including mass-exploitation of zero-days by ransomware groups and sophisticated social engineering campaigns distributing info-stealing malware such as Vidar.
- The period was marked by **significant data exposure events**, including datasets allegedly from Neighbourly (213 million records) and Ochre Health (700,000 patient records), with a growing trend toward bundling stolen data from multiple breaches for resale.

Overview

Australia and New Zealand's H1 2026 threat landscape was characterized by a high volume of ransomware and significant data breach activity, driven by a diverse ecosystem of financially motivated actors. CRIL recorded 76 ransomware attacks and 9 data breach and leak incidents for the region.

Prolific ransomware collectives Qilin and CL0P dominated, primarily impacting Professional Services, IT, Healthcare, and Construction, while data compromise operations showed a distinct focus on BFSI, with threat actors advertising massive datasets allegedly from entities such as Neighbourly, Ochre Health, and Arrotex Pharmaceuticals. Initial access sale activity in the region was limited during the reporting period, with only isolated, unconfirmed listings observed.

Data Breach and Leaks

CRIL observed nine distinct data breach and leak incidents impacting organizations in Australia and New Zealand during the first half of 2026. The Banking, Financial Services, and Insurance (BFSI) sector was the primary target, accounting for approximately 44% of all observed breaches.

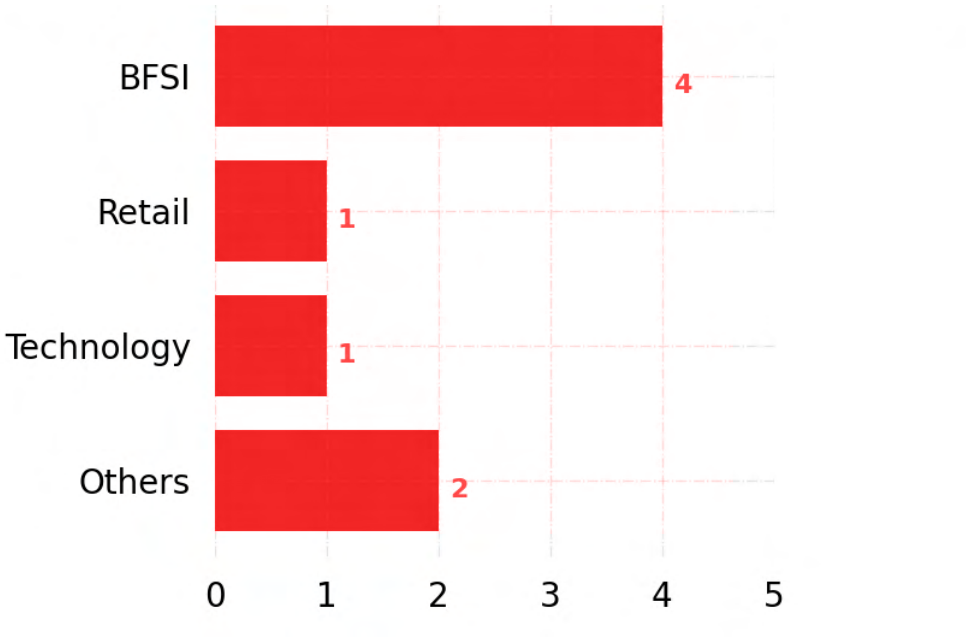


Fig 77: Data Breaches Across Industries

The remaining incidents were distributed across the Technology, Retail, Healthcare, and Consumer Goods sectors. The persistent targeting of the BFSI sector is driven by the high value of its data, as threat actors seek to exfiltrate sensitive financial information, customer Personally Identifiable Information (PII), and account details for illicit monetization and fraud.

This concentration of attacks underscores the significant and persistent threat faced by the financial industry, which remains a lucrative target for data-exfiltrating threat actors in the region.

'kirby' and 'tanaka' were the most prolific actors, each linked to two incidents, in an overall fragmented landscape with no single dominant player. 'motefil1788' exemplified a highly targeted approach, focusing exclusively on Australia's BFSI sector during a short campaign in late February 2026.

Ransomware

Overview

CRIL observed 76 ransomware attacks targeting organizations in Australia and New Zealand during H1 2026, characterized by the dominance of a few highly active collectives supplemented by a diverse array of smaller or emerging groups.

Fig 78: Distribution of Ransomware Attacks in Australia and New Zealand (H1 2026)

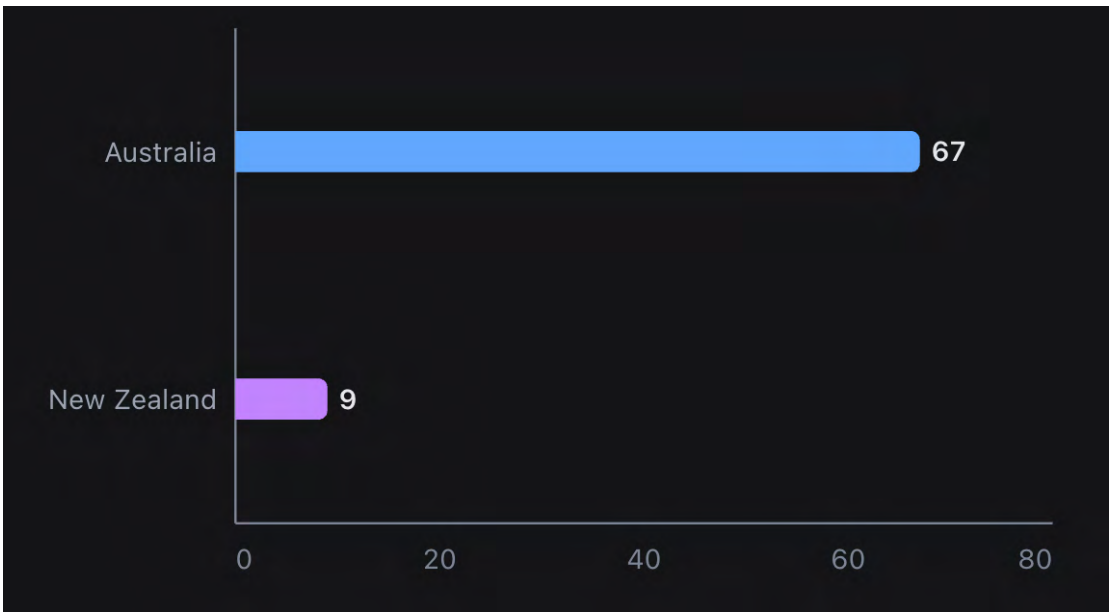


Fig 77: Ransomware Attack statistics for Australia and New Zealand (H1 2026)

Dominant Ransomware Groups

Qilin, CL0P, and The Gentlemen — the top three groups — accounted for approximately 46% of all recorded incidents. Qilin was the most significant threat (17 attacks), followed by CL0P (12 attacks, in a concentrated burst of activity) and The Gentlemen (6 attacks). Lynx, Dragonforce, and INC Ransom were each attributed with 5 incidents.

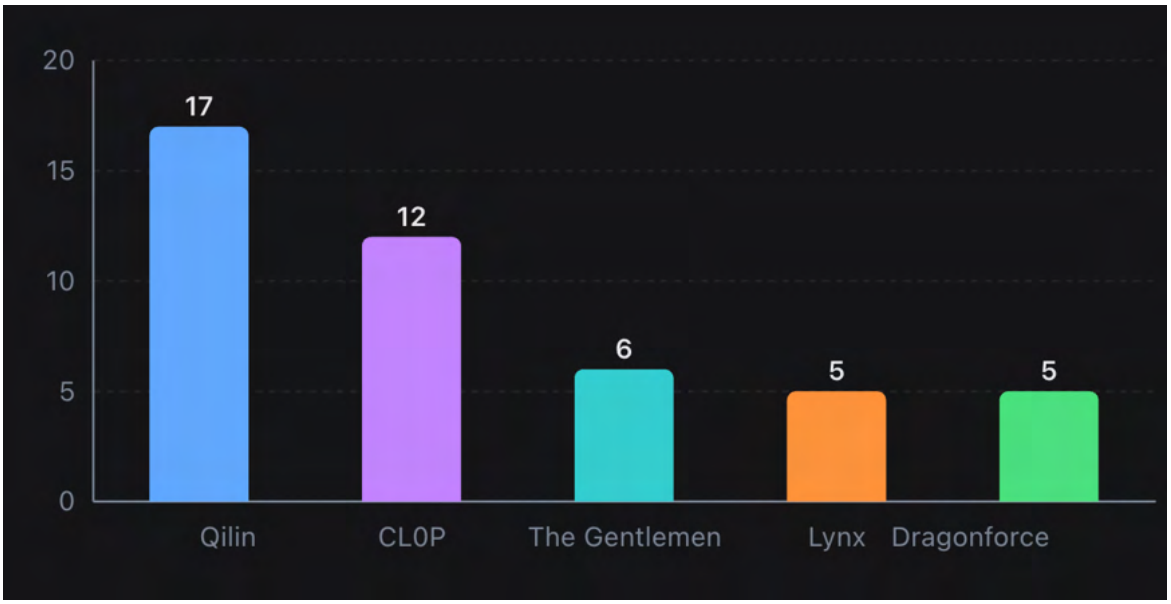


Fig 78: Most Active Ransomware Actors Targeting Australia and New Zealand

Impact Analysis

Professional Services, IT & ITES, Construction, and Healthcare were the most frequently impacted sectors, each recording seven distinct incidents. Notable victims included Menzies Facility Services (Professional Services) targeted by Qilin, ALS Global (IT & ITES) by Aur0ra, Champion Homes Sales Pty Ltd (Construction) by Dragonforce, and Bendigo & District Aboriginal Co-operative (Healthcare) by INC Ransom. CL0P's entire 12-attack campaign occurred on a single day (January 27, 2026) — highly indicative of a mass-exploitation campaign targeting a common zero-day — while RALord/Nova focused on government and educational institutions in June, including the NSW Government's RFS Department and Reynella East College.

Hacktivism

Hacktivism impacting Australia and New Zealand was driven by a mix of geopolitical, ideological, and opportunistic motivations, with GANOSECTEAM PALESTINA, Malaysia Hacktivist – Official, Adams Business Network (ABN), and cyberbrigade212 among the most prominent groups and channels. Website defacements, DDoS attacks, and data exfiltration were the primary tactics, evidenced by approximately 15 data leak posts. Targeting was largely indiscriminate, impacting roughly 104 unique domains across Government & LEA, Healthcare, Technology, Education, and BFSI.

Vulnerabilities

Known Exploited Vulnerabilities

H1 2026 was defined by a significant volume of critical, industry- and region-agnostic vulnerabilities, many of which were added to the CISA Known Exploited Vulnerabilities (KEV) catalog — confirming active exploitation. Of the 146 CVEs CRIL analyzed, nearly 90% were rated critical or high severity.

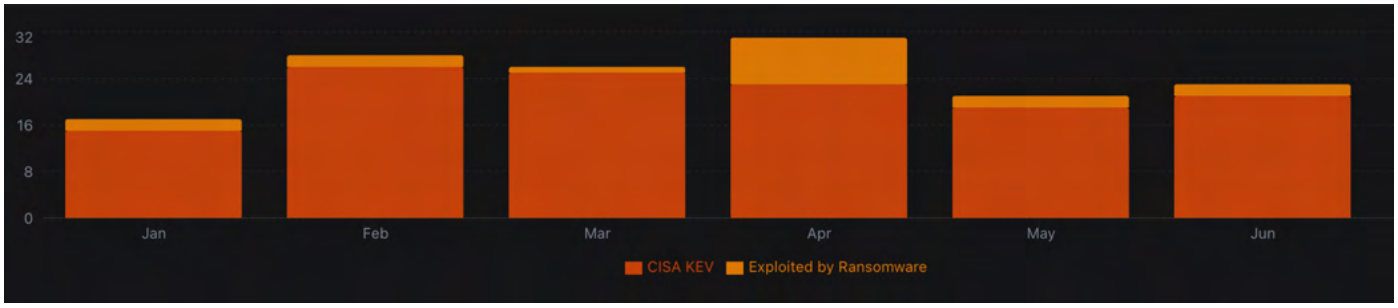


Fig 79: Month-wise CISA KEV and Exploited Vulnerabilities Count in H1 2026

Vendors such as SmarterTools, SolarWinds, Fortinet, Ivanti, and Cisco appeared repeatedly, spanning products from email servers to network management and security appliances. The persistence of older vulnerabilities alongside new disclosures shows attackers continuing to exploit flaws organizations have had ample time to remediate.

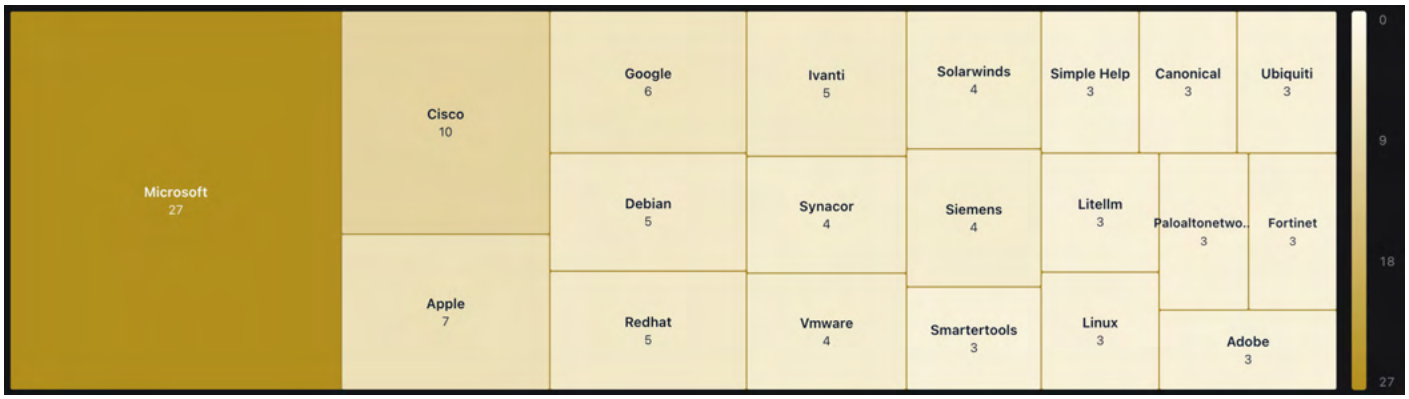


Fig 80: Top Affected Vendors and/or Products Added to CISA KEV Catalog

CVE ID	Product	Vendor	CVSS v3
CVE-2025-52691	SmarterMail	SmarterTools	10.0
CVE-2026-20127	Catalyst SD-WAN Manager	Cisco	10.0
CVE-2026-20131	Secure Firewall Management Center	Cisco	10.0
CVE-2025-32432	CMS	Craft	10.0
CVE-2025-32975	KACE SMA	Quest	10.0
CVE-2026-10520	Sentry	Ivanti	10.0
CVE-2026-34909 / -34908 / -34910	EFG	Ubiquiti	10.0
CVE-2026-48558	SimpleHelp	SimpleHelp	10.0
CVE-2026-1281 / -1340	Endpoint Manager Mobile	Ivanti	9.8
CVE-2026-24858 / -35616 / -21643	FortiAnalyzer / FortiClientEMS	Fortinet	9.8
CVE-2026-20045	Unified Communications Manager	Cisco	9.8
CVE-2025-40551 / -40536 / -26399	Web Help Desk	SolarWinds	9.8
CVE-2026-0300 / -0257	Cloud NGFW	Palo Alto Networks	9.8 / 9.1
CVE-2026-3055	NetScaler Application Delivery Controller	Citrix	9.8
CVE-2026-20963	SharePoint Server	Microsoft	9.8

Table 2: This is a representative selection of the highest-severity CVEs from the full 146-CVE dataset analyzed by CRIL for H1 2026; the complete list is available through Cyble Vision.

Zero-Day Vulnerabilities

H1 2026's zero-day activity was similarly concentrated among critical, high-severity flaws: of the nine major zero-day CVEs tracked, over 88% carried a CVSS score of 7.0 or higher. Two 9.8-rated zero-days stood out — CVE-2026-1340 in Ivanti's Endpoint Manager Mobile and CVE-2026-0300 in Palo Alto Networks' Cloud NGFW — both underscoring sustained attacker interest in network and device management platforms that serve as gateways into broader enterprise networks.

Fig 81: Affected Vendors and/or Products

CVE ID	Product	Vendor	CVSS v3
CVE-2026-1340	Endpoint Manager Mobile	Ivanti	9.8
CVE-2026-0300	Cloud NGFW	Palo Alto Networks	9.8

Table 3: Top Exploited Zero-Days

Organizations are strongly advised to prioritize patching of known exploited vulnerabilities, enhance network segmentation to limit lateral movement, and maintain continuous monitoring for indicators of compromise — with particular urgency for internet-facing network, security, and remote access infrastructure.

Outlook and Strategic Recommendations

1. Prioritize risk-based, not blanket, patching. With nearly 90% of tracked CVEs rated critical or high severity, and repeat exposure concentrated in a recognizable set of vendors — Ivanti, Fortinet, Cisco, SolarWinds, SmarterTools, and Palo Alto Networks — security teams should weight patch prioritization toward internet-facing network, security, and remote access infrastructure rather than treating all vulnerabilities as equal.
2. Treat data exfiltration, not just encryption, as the primary ransomware risk. Double extortion is now the default model across every region in this report. Backup and recovery capability alone is no longer sufficient; data loss prevention, network segmentation to limit exfiltration paths, and a rehearsed public communications plan for breach disclosure are equally important.
3. Assume the initial access market is a leading indicator. Access brokers routinely precede ransomware and espionage operations by weeks or months. Monitoring for organizational exposure in access-broker markets — and treating a confirmed listing as an active incident, not a rumor — can materially shorten dwell time.
4. Calibrate defenses to regional threat concentration, not just global averages. MEA's ransomware activity is dominated by a single group ("The Gentlemen"); Europe/UK and North America face the highest absolute ransomware volumes; APAC and South America show heavier state-aligned and supply-chain activity. Multinational organizations should tailor detection and response priorities by region rather than applying a single global threat model.
5. Expect hacktivism and financially motivated cybercrime to keep converging. Several "hacktivist" channels tracked in this report also broker stolen data and sell DDoS-for-hire services. Treat claims from these channels as credible threat intelligence signals rather than dismissing them as purely ideological noise.
6. Extend MFA and identity controls to third parties. Supply-chain and MSP compromise (IT & ITES ranked among the top-five ransomware targets in nearly every region) means an organization's own control posture is only as strong as that of its most exposed vendor or service provider.

Conclusion

Taken together, the worldwide and regional data in this report describe a threat landscape that is high in volume but increasingly organized: a small number of capable ransomware operators, access brokers, and data-leak actors are responsible for a disproportionate share of global cyber harm, operating with the consistency and specialization of legitimate service industries.

Ransomware remains the most damaging and most consistent threat category across every region, with Manufacturing, Professional Services, Construction, and Healthcare the most exposed sectors globally — though regional concentration varies meaningfully, from the high-volume, multi-group competition seen in Europe and North America to the single-group dominance observed in the Middle East & Africa.

Vulnerability exploitation continues to serve as the connective tissue linking initial access, data breach, and ransomware activity — with a recurring set of enterprise network and security vendors appearing across nearly every regional report. Meanwhile, hacktivism has grown more difficult to separate from financially motivated cybercrime, and geopolitical tension continues to shape both state-aligned espionage and hacktivist targeting.

For CISOs, CIOs, and security practitioners, the practical implication is straightforward: defenses built around rapid, risk-prioritized patching, phishing-resistant MFA, network segmentation, tested offline backups, and active monitoring of the cybercrime underground for organizational exposure remain the highest-leverage investments against the threat patterns documented in this report.

Stay Ahead of the Next Threat

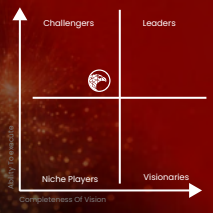
Cyber threats are growing faster than ever. Stay one step ahead with Cyble's real-time threat intelligence — giving you visibility, speed, and confidence to act before attackers do.

REQUEST YOUR DEMO NOW!

Experience the power of predictive security with Cyble.

Industry Recognition

Cyble Recognized as a **Challenger** in the **2026 Gartner® Magic Quadrant ™** for Cyberthreat Intelligence Technologies



QKS Group
SPARK Matrix™ 2026
LEADER
Cyble Named as a Leader in Digital Threat Intelligence Management

FROST & SULLIVAN

Cyble Named Leader in Frost Radar™ Cyber Threat Intelligence 2024

FORRESTER®
Cyble Recognized in Forrester's **External Threat Intelligence** Service Providers Landscape, **Q1 2026 report**

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

AMERICA'S BEST STARTUP EMPLOYERS | Forbes 2026
Recognized as one of America's Best Startup Employers by Forbes

GLOBAL INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2026
Cyble Secures Four Prestigious Honors at the 2026 Global Infosec Awards

Gartner Peer Insights™
Ranked No.1 among the top Security Threat Intelligence and Brand Protection Providers.
4.8/5

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

TOP INFOSEC INNOVATOR WINNER CYBER DEFENSE MAGAZINE 2025
Cyble Wins Three Top InfoSec Innovator 2025 Awards

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

2026 WINNER CYBER SECURITY EXCELLENCE AWARDS

Cyble Earns **36 Badges in G2 Summer 2026** Reports, Highlighting Leadership in AI-Powered Cybersecurity

SUMMER 2026 Leader

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

OUR INVESTORS

BLACKBIRD · KING RIVER · Xoogler.co · SUMMIT PEAK INVESTMENTS · Singtel innov8 · Aditya Birla 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