Event Report

CloudSEK

[GTI] CloudSEK: Global Threat Landscape Report 2025

Category

Adversary Intelligence

Region

Global

Executive Summary

In 2025, the global cyber threat landscape remained **highly active, fast-moving, and heavily driven by profit**. Threat actors continued to scale attacks using **stolen identities, leaked credentials, and access brokerage**, while major breaches and supply chain-style incidents showed that compromise at a shared platform layer can create **large downstream impact across thousands of organisations**.

A major driver of global exposure was the **dark web economy**, where stolen data and unauthorised access were traded openly at scale. Activity remained concentrated on a few dominant forums. **DarkForums emerged as the most active platform worldwide**, fuelled by threat actor migration after **BreachForums faced law-enforcement disruption in 2025**. This reinforces a key reality: when one platform goes down, the ecosystem does not stop, threat actors simply move to new forums and continue selling **leaks, credentials, and corporate access**.

The report also highlights how the **threat actor ecosystem** is structured, ranging from high-impact operators who enable access resale and large-scale exposure, to high-volume data sellers who repeatedly monetise leaks across forums. It also observed the steady rise of **newer actors**, many of whom are quickly building reputation through frequent postings, large dataset leaks, and continuous underground activity. These patterns show that the global underground market is not driven by one single group, it is powered by **a wide pipeline of actors supporting each other's monetisation models**.

Across global incidents, the most common entry points remained **repeatable and scalable**. Most intrusions began with **phishing and social engineering, stolen credentials from infostealer logs**, and **exploitation of internet-facing vulnerabilities** especially on edge devices and remote access services **(VPN/RDP/Citrix)**. This trend confirms that many successful attacks still rely on **weak identity controls, exposed infrastructure, and delayed patching** rather than advanced or rare techniques.

The global breach landscape in 2025 was shaped by multiple high-impact incidents that highlighted **platform-level and third-party risk**. Key cases included a large exposure tied to **cloud identity infrastructure**, a **major perimeter device configuration leak affecting 15,000+ systems**, and a breach of a **centralised consulting development environment**, raising concern over engineering repositories storing sensitive customer-linked material. The report also observed a major compromise theme where attackers targeting **shared communications infrastructure**, including SMS ecosystems, where access can enable **OTP interception, account takeover attempts, and downstream fraud**.

Ransomware remained one of the most disruptive global threats. The ecosystem continued to fragment, with multiple groups operating at scale instead of one dominant leader. Activity remained consistent throughout the year, with visible spikes driven by bulk leak-site victim disclosures and data extortion campaigns. The report also observed that ransomware outcomes are increasingly shaped by **identity compromise and perimeter exposure**, with threat actors repeatedly abusing **stolen credentials, weak remote access controls, and exposed public-facing systems**.

Finally, the vulnerability environment continued to favour attackers. 2025 saw sustained publication and discussion of **high-severity vulnerabilities**, including trending CVEs with mass exploitation potential. The speed at which vulnerabilities move from disclosure to exploitation remains a critical risk factor, especially for organisations with **large external attack surfaces** or complex patching cycles.

Overall, the 2025 global threat landscape confirms a clear pattern of **modern cybercrime operating like a supply chain**. Stolen identities, exposed access, and shared platform weaknesses continue to power **large-scale compromise, extortion, and disruption worldwide**. Organisations that prioritise **identity protection, rapid patching of internet-facing systems, stronger vendor controls, and continuous threat monitoring** will be best positioned to reduce risk in 2026

Overview of Dark Web Activity

Dark web activity observed over the past 12 months highlights a highly active and organised underground ecosystem where stolen data and unauthorised access are traded at scale. The overall pattern shows that the global cybercrime economy remains strongly driven by identity abuse (PII + credentials), access resale, and supply-chain style exposure that enables follow-on attacks such as fraud, extortion, and ransomware.

Underground forum activity remained concentrated across a small number of dominant platforms. DarkForums emerged as the most active forum globally, supported by a major shift in threat actor behaviour after BreachForums was taken down and disrupted in 2025. Instead of slowing down, many actors migrated quickly and continued posting leaks and access listings on alternative forums. This confirms a key trend in the underground market: when one platform is disrupted, threat actors simply relocate and continue operations elsewhere.

Across global incidents, the most common initial attack vectors remained consistent and repeatable. The majority of intrusions were enabled through stolen credentials, infostealer-driven access, exploitation of internet-facing vulnerabilities, and abuse of exposed remote access services (VPN/RDP). Supply chain compromise and SaaS integration abuse also stood out as major global risks, particularly where attackers exploited shared platforms or vendor connections to create a wide downstream impact.

Finally, sector-wise exposure confirms that threat actors are not targeting randomly—they focus on industries with strong monetisation value. Technology, government, finance, telecom, and e-commerce recorded the highest dark web exposure globally, showing continued preference for data-rich environments and systems that can be abused for identity fraud or access resale. Other sectors such as education, healthcare, crypto, and social media also remain consistently targeted, reinforcing that dark web risk has become cross-industry and global in nature.

Key trends shaping global dark web activity

- **Forum migration is constant:** when platforms face disruption, threat actors quickly shift to alternatives rather than stopping.
- **Identity and credentials remain the most traded assets:** PII and login datasets continue to drive downstream phishing, fraud, and takeover attacks.

- **Access resale is a major enabler:** VPN/RDP and admin-level access sales continue feeding ransomware and extortion operations.
- **Supply-chain exposure is rising:** attacks increasingly target shared vendors, SaaS platforms, and aggregators to maximise impact.
- **Technology and government remain top exposure sectors:** these environments enable large-scale identity abuse and downstream compromise.

Dark Web Forum Activity Analysis

The global underground forum ecosystem remains highly active and concentrated, where a small number of platforms account for the majority of observed cybercrime activity. This distribution reflects a mature underground market where threat actors continuously migrate, re-post, and trade across multiple platforms depending on accessibility, trust level, and enforcement pressure.

Screenshot showing Bar Chart of Prominent Underground Forums Active Worldwide Over The Past Year

DarkForums is now the dominant global underground platform, accounting for approximately **37%** of monitored incidents with over **9,000 listings**. This rise followed the **2025 law enforcement takedown of BreachForums**, causing threat actors to migrate and establish DarkForums as a high-volume hub for data leaks, stealer logs, and access sales. However, this surge has been accompanied by a significant increase in fake listings and scammers, due to the platform's lack of active moderation—a feature that made the defunct BreachForums a preferred choice.

BreachForums accounts for about **20%** of global activity with over **5,000 listings**, making it the second-largest platform. Despite law enforcement disruptions in 2025, its influence remains significant. The platform was a major venue for disclosing breaches, distributing leaked data, and was used by threat actors to advertise datasets and establish credibility. Its sustained activity is linked to credible threat actor endorsements and it being successor to the popular Raidforums.

ExploitForum and **LeakBase** form the next core tier of underground platforms, contributing **around 15%** and around **14%** of total activity respectively. ExploitForum is typically associated with more technical and higher-trust discussions, including exploit sharing and detailed access listings. LeakBase continues to function as a steady marketplace for identity datasets, credential leaks, and structured database sales. While their overall volumes are lower than DarkForums and BreachForums, the content on these forums is often more targeted and monetisation-driven.

XSS accounts for around 8% of observed global activity, with just over 2,000 incidents. The forum has historically operated as a more controlled, higher-trust platform compared to open leak forums, often hosting listings from access brokers, malware sellers, and financially motivated operators. Posts on XSS typically involve verified access offers, corporate compromise listings, and advanced tooling trade, making even lower-volume activity high risk.

In 2025, **law-enforcement action reportedly led to the shutdown of XSS**, including the alleged arrest of its administrator ("toha"). Following this disruption, threat actor activity began shifting toward alternative platforms — most notably **DamageLib**, which emerged as a replacement-style forum and gained visibility as actors migrated away from XSS.

Smaller platforms such as **BreachStars, DamageLib, Rehub, Ramp4u, UmbraForums, and Ransomed Forums** contribute lower overall volume but remain important for monitoring. These forums frequently host opportunistic leaks, reposted databases, and early-stage actors building reputation. While activity is limited compared to major forums, they often act as **entry points for new threat actors and alternate distribution channels for stolen data**.

Key Threat Actors Shaping the Global Dark Web Ecosystem

The global dark web ecosystem includes thousands of threat actor handles involved in data leaks, access sales, and underground trading. For this report, we shortlisted notable threat actors based on a combination of **repeat activity, operational impact, and visibility across underground forums and monitoring sources**. The final list includes a mix of **high-impact access brokers, large-scale data leak actors**, and **emerging handles** that show signs of growth. Together, these actors reflect how the global dark web market enables both sophisticated and opportunistic cyber threats, especially through stolen credentials, exposed remote access services, and sale of unauthorised access.

Tier 1 Actors (High Impact & Consistent Operations)

This list has actors involved in high-risk access sales, large-scale data exposure, or high-impact extortion activity,

- **miyako** is a highly active access broker known for selling privileged and VPN-level access to organisations across underground forums. The actor typically exploits exposed systems and compromised remote services, then resells this access to support wider intrusion activity. miyako has also been linked to ransomware ecosystems such as Hellcat, highlighting the strong connection between access brokerage and large-scale cyberattacks.

CloudSEK Threat Actor Directory - miyako Profile Showing Top Targeted Countries and Industries

- **Belsen_Group** gained significant visibility after leaking **configuration files and VPN credentials linked to over 15,000 FortiGate devices**. This exposed firewall rules, keys, and plain-text credentials, creating wide-scale downstream risk by enabling other criminals to reuse this access for intrusions and ransomware operations. The incident reinforces how delayed patching and exposed perimeter infrastructure can create large-scale compromise opportunities.

CloudSEK Threat Actor Directory - Belsen_Group Profile Showing Top Targeted Countries and Industries

- **Sentap** is a financially motivated actor known for repeated activity across dark web forums, with operations linked to **data theft, access brokering, and extortion**. Their targeting patterns span multiple industries, including healthcare, government, telecom, engineering, construction, and other operationally important sectors. Sentap is also associated with broader underground ecosystems that support ransomware and extortion-style monetisation.

CloudSEK Threat Actor Directory - Sentap Profile Showing Top Targeted Countries and Industries

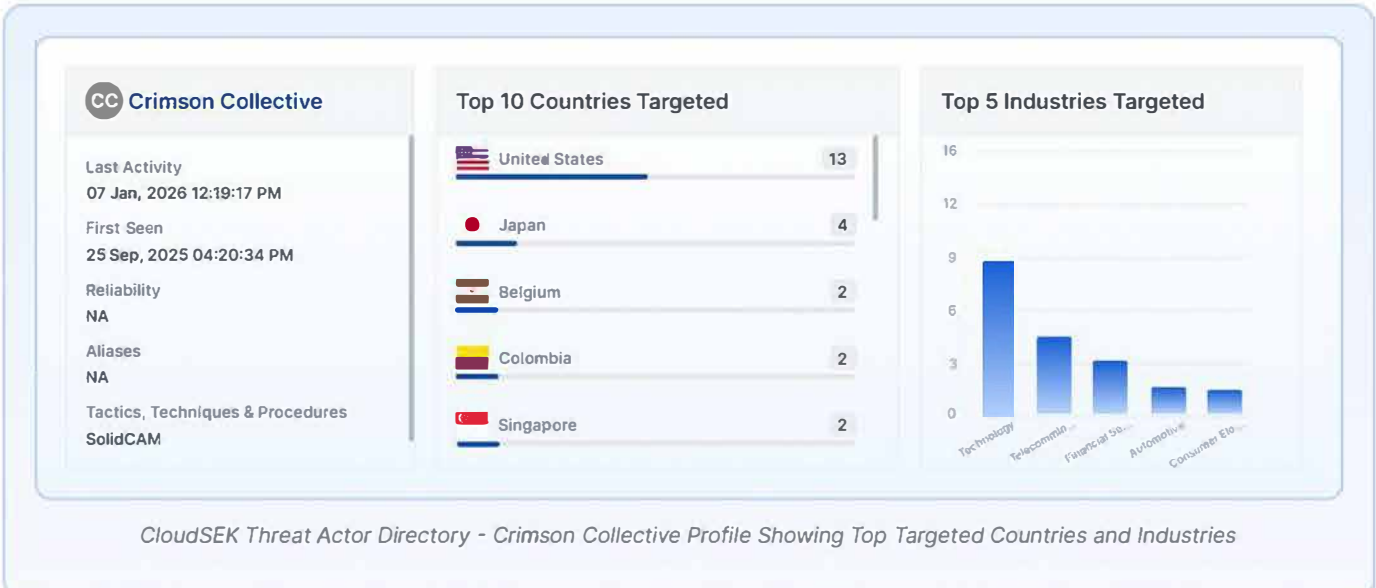
- **Machine1337** has been linked to high-impact activity involving compromise of administrative access related to a **third-party communications/SMS service provider**. The actor reportedly monetised this access by intercepting sensitive messages such as OTPs and transaction alerts, and selling the intercepted data through underground channels. This highlights a serious global risk: **supply-chain compromise enabling real-time data interception**, which can directly support fraud and account takeover.

CloudSEK Threat Actor Directory - Machine1337 Profile Showing Top Targeted Countries and Industries

- **Handala represents an ideologically motivated hacktivist actor**, where operations focus on political messaging combined with sensitive data exposure. The group is primarily associated with data exfiltration, public leaks, and disruptive campaigns rather than financial extortion. Their activity often involves targeting government-linked, technology, and institutional environments to maximise political and reputational impact. Handala's operations create elevated reputational and operational risk because victims are selected for symbolic or geopolitical reasons, with stolen data frequently used for public pressure, narrative shaping, and disruption rather than direct monetisation.

CloudSEK Threat Actor Directory - Handala Profile Showing Top Targeted Countries and Industries

- Scattered Spider / Scattered Lapsus$ Hunters ecosystem reflects a highly capable intrusion cluster known for **identity-driven compromise**, including social engineering and manipulation of enterprise access workflows. This ecosystem is strongly associated with "access-as-a-service" style operations, where compromised identities and third-party integrations can be abused at scale. Their relevance is global because the approach is not sector-specific, it targets organisations with complex support processes, SaaS dependence, and high exposure to identity compromise. We wrote an in-depth analysis of the parent group called the COM, which can be found here.
- **Crimson Collective** gained major attention after publicly claiming responsibility for breaching **Red Hat's consulting-related internal development environment**. The breach involved exposure of internal repositories and consulting-related datasets, raising concern because such material can contain client-facing documentation, infrastructure details, and embedded secrets that may be reused for follow-on attacks. This case highlights how threat actors increasingly target environments that aggregate sensitive customer and enterprise data.



CloudSEK Threat Actor Directory - Crimson Collective Profile Showing Top Targeted Countries and Industries

Tier 2 Threat Actors (Notable High-Activity & Specialised Actors)

The list has actors involved in high-volume data leaks, access sales, or opportunistic exploitation

- **grep is a data-focused threat actor** widely linked to credential abuse, brute-force activity, and high-volume data harvesting. Their operations are largely leak-driven, with repeated exposure of customer databases and large datasets across underground forums. The actor has also been associated with the Hellcat leak collective, which is known for mass database disclosures and public data dumping. In addition, grep has been linked to supply-chain style data exposure activity, showing how their impact can extend beyond single organisations and affect connected platforms or services.

CloudSEK ThreaCloudSEK Threat Actor Directory — grep Collective Profile Showing Top Targeted Countries and Industriest Actor Directory - miyako Profile Showing Top Targeted Countries and Industries

- **kazu** is an access-oriented threat actor known for exploiting vulnerable systems and selling **high-risk administrative access**. Their listings commonly include control over panels, servers, or internal systems — making their activity particularly dangerous because buyers can use the access for deeper intrusion, data theft, or ransomware deployment.

CloudSEK Threat Actor Directory — kazu Collective Profile Showing Top Targeted Countries and Industries

- **888** gained visibility after being linked to multiple public breach claims involving well-known brands. The actor has appeared in incidents tied to exposed datasets and misconfigured cloud assets, making them a notable leak handle in the global breach ecosystem.

CloudSEK Threat Actor Directory — 888 Collective Profile Showing Top Targeted Countries and Industries

- **ByteToBreach** is a financially motivated and opportunistic actor that shows a wide range of initial access methods, including **exploitation of internet-facing vulnerabilities, cloud misconfigurations, file-inclusion techniques, and password attacks**. The actor is also known for actively monetising stolen data and access through underground platforms, and shifting toward extortion or public leaks if buyers do not engage.

CloudSEK Threat Actor Directory — ByteToBreach Collective Profile Showing Top Targeted Countries and Industries

- **Agency9** stands out as a high-volume data seller with repeated listings involving large consumer datasets. The actor has been linked to major mobile/contact database sale activity, including TrueCaller-related listings, highlighting continued risk of mass identity exposure and secondary fraud enablement.

- **BIGBROTHER** is a high-volume seller linked to large dataset sales and access-style listings. Their activity includes public-facing data sale claims involving major entities and large record volumes, showing how some actors operate as consistent "data merchants" rather than one-time hackers.

CloudSEK Threat Actor Directory — BIGBROTHER Collective Profile Showing Top Targeted Countries and Industries

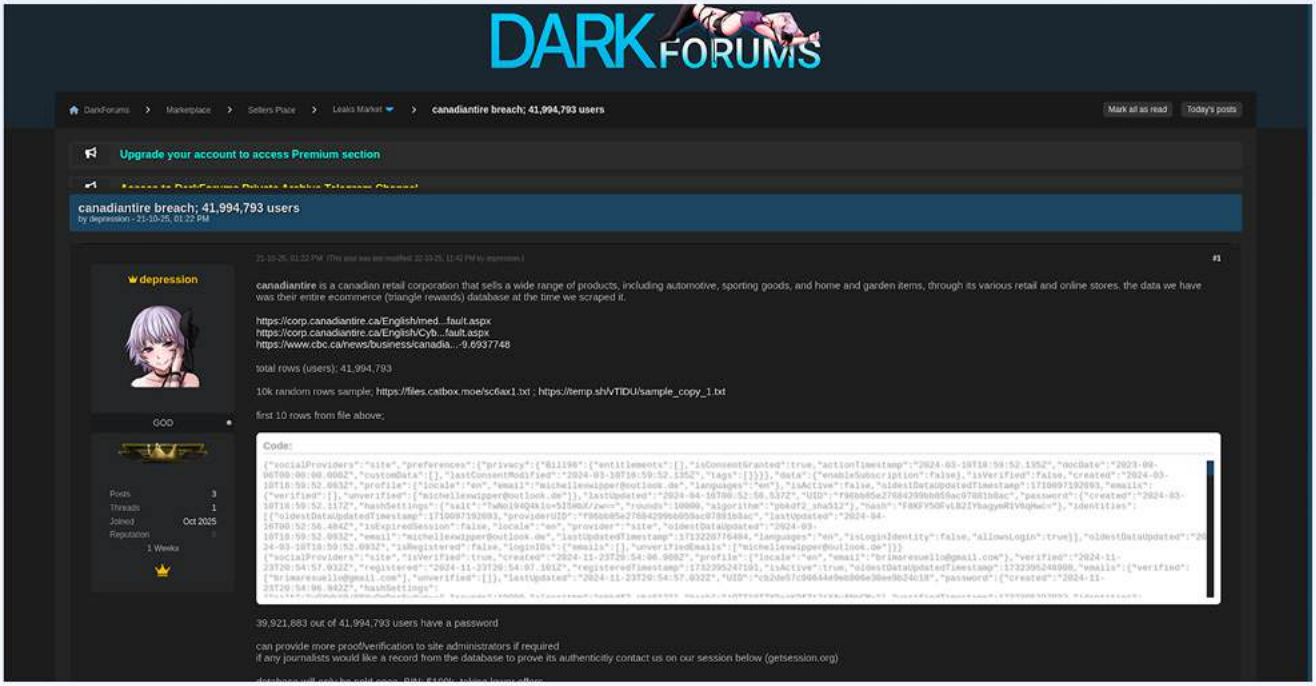
- **Victim** is an established underground actor associated with web exploitation and scraping-led breaches. The actor has been discussed in threat research due to claims of control over victim infrastructure and continued data extraction, reflecting a blend of ideological exposure and financial monetisation.

CloudSEK Threat Actor Directory — victim Collective Profile Showing Top Targeted Countries and Industries

Emerging Threat Actors (Rising Operators & New Entrants)

The list has actors involved in high-volume breach postings, aggressive monetisation activity, or early signs of advanced capability. While many of these actors may not yet have long-term credibility like top-tier operators, their activity is important because they often show fast learning curves, repeat listings, and scaling behaviour across underground forums.

- **depression** is an emerging data seller linked to monetising stolen databases rather than running ransomware or long-term access operations. The actor appears to focus on **web application attacks** to obtain large datasets and then sells the extracted records through underground forums. Although still early-stage, the actor gained visibility after advertising a **high-volume consumer dataset**, which shows potential for rapid escalation in underground reputation and repeat breach activity.



Screenshot of the forum post by depression captured in Threat Intelligence section of CloudSEK platform

- **STEPBRO** is a highly active leak-focused handle observed across multiple underground platforms. The actor demonstrates consistent operational activity and is frequently linked to **database dumps, lead sales, and occasional admin access listings**. STEPBRO commonly leverages techniques such as **SQL injection, credential stuffing, web shell deployment, phishing, and stealer-driven credential harvesting**. Their activity spans multiple regions and industries, including retail, financial services, government, transportation, and healthcare. The actor is also known for selling “lead lists” and breached login datasets, highlighting their strong focus on monetisation and repeat victimisation at scale.

CloudSEK Threat Actor Directory — STEPBRO Collective Profile Showing Top Targeted Countries and Industries

- **ransom** is an emerging access broker and tooling seller operating on higher-tier underground forums. The actor is notable for advertising **high-value corporate access (such as remote access entry points)** and also selling **advanced offensive tooling designed to help attackers evade detection**. While direct victim attribution is not consistently public, their combination of access brokering and malware/tool trade activity suggests strong alignment with ransomware affiliate ecosystems and broader intrusion markets, making them strategically relevant in the global threat landscape.

Initial Attack Vectors

Threat actors operating globally continue to rely on a mix of high-volume, low-cost entry methods and high-impact exploitation techniques:

- Phishing & Social Engineering (Email, Vishing, Smishing)
  - **How:** Fake login pages, malicious links/attachments, invoice scams, HR/lure emails, or help-desk impersonation calls that trick employees into sharing credentials or approving MFA.
  - **Why prevalent:** Still the cheapest and most scalable method. AI-written lures and phishing kits make campaigns faster and harder to detect.
  - **Mitigation:** Phishing-resistant MFA (FIDO2), email filtering/sandboxing, block risky attachments, verify helpdesk requests, targeted training for high-risk roles (finance/IT).
- Credential Compromise & Valid Account Abuse (Infostealers + Reuse)
  - **How:** Threat actors reuse stolen credentials from infostealer logs, breached databases, password spraying, or credential stuffing to log in directly (VPN, O365, RDP, SaaS).
  - **Why prevalent:** The access economy is thriving—stealer logs and credential markets provide ready-made entry without technical exploitation.

- **Mitigation:** Enforce MFA everywhere, block legacy authentication, monitor leaked credentials, conditional access policies, abnormal login detection.

- Remote Access Abuse (RDP / VPN / Citrix / SSH)
  - **How:** Brute force, password spraying, stolen credentials, misconfigurations, or appliance exploitation of remote access services.
  - **Why prevalent:** Remote work + exposed services remains one of the most reliable entry paths. Many organisations still leave management portals reachable from the internet.
  - **Mitigation:** Remove public RDP, enforce MFA, restrict portals to allow-lists, use jump servers, monitor remote logins and session behaviour.

- Supply Chain & Third-Party Compromise (MSPs, SaaS, Vendors)
  - **How:** Threat actors compromise a vendor/MSP, software update system, third-party integrations, or vendor credentials and pivot into customers.
  - **Why prevalent:** One compromise can impact many downstream victims. This is increasingly attractive for extortion campaigns.
  - **Mitigation:** Strong vendor access controls, least privilege, segmentation for third-party connections, monitoring of supplier accounts, SBOM/code-signing controls.

- Cloud Misconfiguration & IAM Abuse (Token/API Key Theft)
  - **How:** Exposed buckets, over-permissioned IAM roles, leaked API keys, insecure OAuth tokens, weak cloud policies, and lack of visibility.
  - **Why prevalent:** Cloud adoption is accelerating faster than security maturity. Attackers exploit exposed secrets and misconfigured access controls.
  - **Mitigation:** CSPM, least privilege IAM, rotate keys, short-lived tokens, centralised logging, alerting on risky permission changes.

- Web Application Logic Flaws & API Abuse
  - **How:** Auth bypass, weak session handling, insecure APIs, rate-limit bypass, business logic manipulation, and poor validation.
  - **Why prevalent:** Modern services expose many APIs and endpoints—automation makes it easy to discover and exploit weaknesses.
  - **Mitigation:** Secure SDLC, regular app/API testing, WAF with API protection, rate limiting, schema validation and strong authentication.

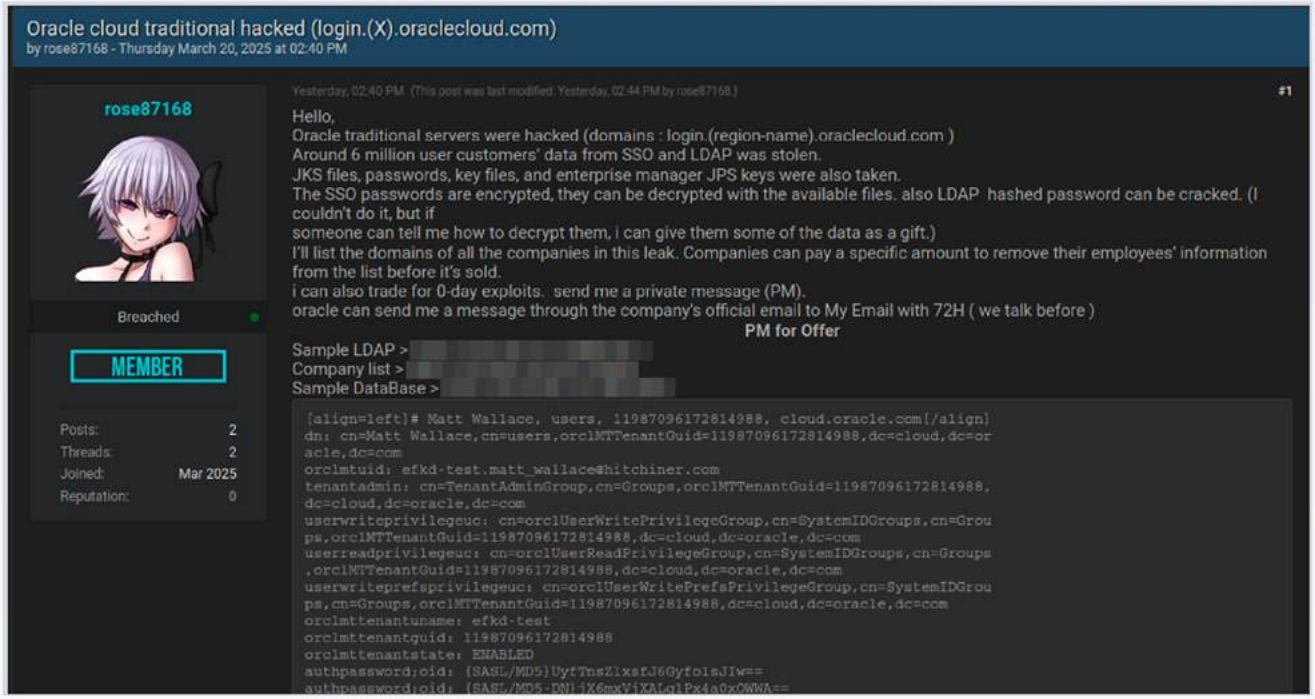
- Exposed Secrets in Repositories & Public Files (Git/Paste Sites)
  - **How:** Developers accidentally expose credentials, API keys, tokens, configs, and environment files which attackers harvest automatically.
  - **Why prevalent:** CI/CD pipelines and modern cloud development create more chances for accidental exposure.
  - **Mitigation:** Secrets scanning in repos, security gates in CI/CD, vault-based secrets management, enforce rotation and alerts.

- Insider Risk & Compromised Employee Devices
    - **How:** Insider misuse, coerced employees, compromised BYOD devices, or session hijacking enables direct access to internal resources.
    - **Why prevalent:** Hybrid work and unmanaged devices increase attack surface as well as outsourced services like customer support. Access often bypasses perimeter controls.
    - **Mitigation:** Device compliance policies, endpoint management, DLP controls, behavioral analytics, privileged action monitoring.
- IoT / OT & Weakly Secured Network Devices (as Pivot Points)
    - **How:** Exposed device interfaces, outdated firmware, weak default passwords, poorly segmented OT environments exploited as a foothold.
    - **Why prevalent:** Many organizations still run legacy devices that cannot be patched quickly and lack modern security controls.
    - **Mitigation:** Asset inventory, firmware patching, removing internet exposure, segmentation between OT/IT, strict monitoring of device traffic.
- Hybrid Credential Theft + Authenticated Exploitation (IDORs, API Abuse)
    - **How:** Threat actors first steal valid user credentials through phishing, infostealer logs, or credential stuffing. Once logged in as legitimate users, they abuse weak access controls, insecure APIs, and logic flaws such as IDORs (Insecure Direct Object References) to extract large volumes of sensitive data or escalate access.
    - **Why prevalent:** Many modern applications rely heavily on APIs and user-based permissions. After authentication is bypassed using stolen credentials, attackers can operate without triggering traditional security alerts, making this method stealthy and highly effective.
    - **Mitigation:** Strong MFA everywhere, continuous monitoring for abnormal authenticated behaviour, API security testing, proper access control enforcement, rate limiting, and regular application logic reviews.

High-Impact Breaches in 2025

Oracle Cloud Exploitation (Supply-chain scale incident)

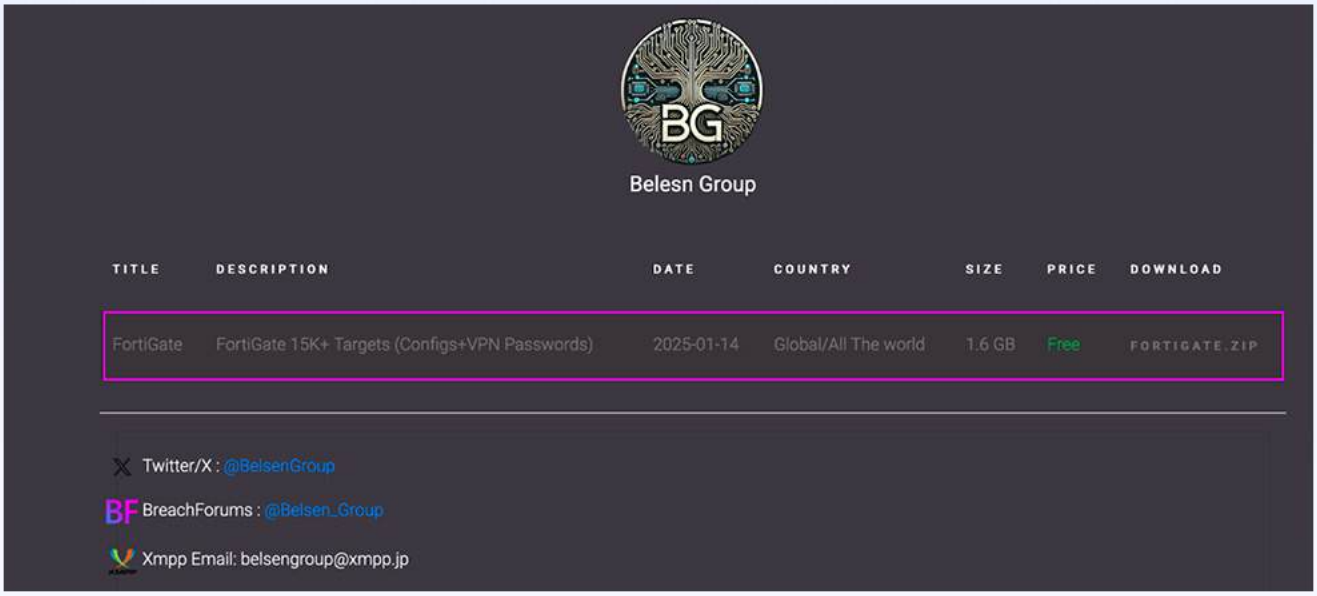
One of the largest supply-chain style incidents reported in 2025 involved a threat actor offering a dataset allegedly exfiltrated from Oracle Cloud identity systems. The exposure reportedly included authentication-related artifacts such as keystores and encrypted password material, with claims of impact spanning a very large number of tenants globally. This incident stood out because it represented platform-level risk, where compromise at a shared cloud layer can create downstream exposure across thousands of organisations. It also reinforced how identity infrastructure (SSO/LDAP-like systems) remains a high-value target for attackers due to its potential for broad access and follow-on compromise.



Threat actor listing 6M records exfiltrated from Oracle Cloud

FortiGate Configuration Leak (Belsen_Group)

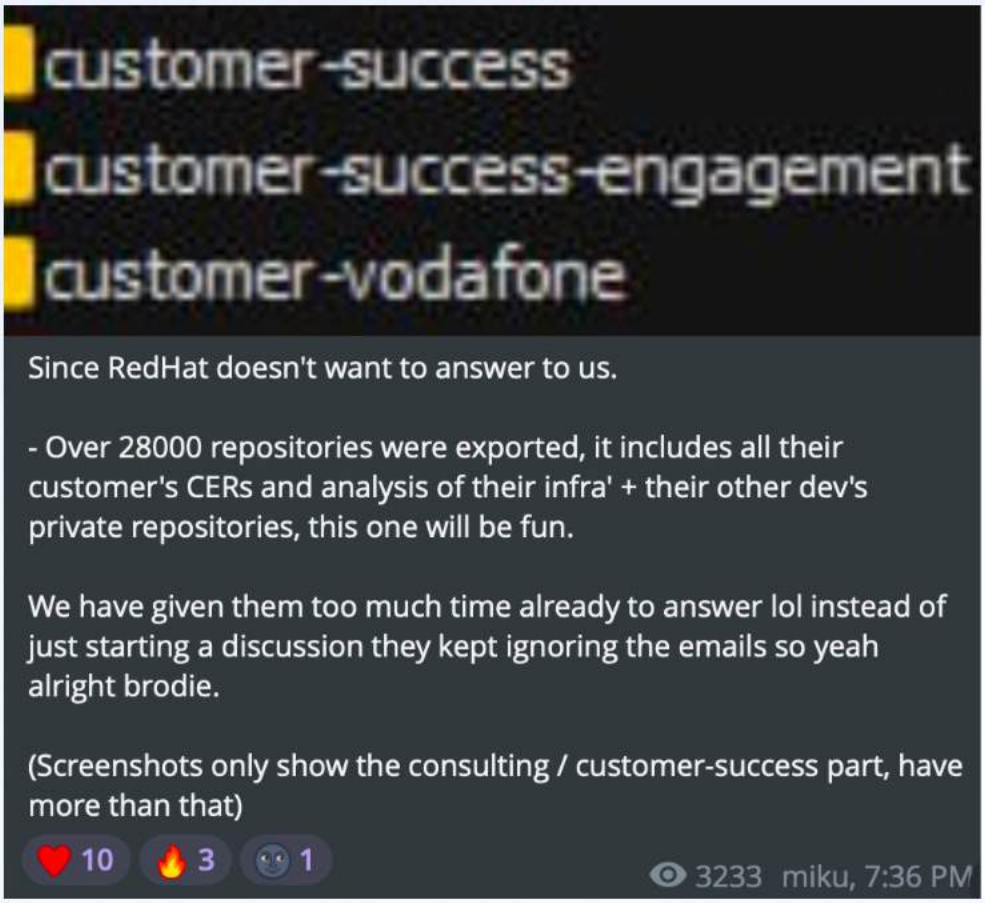
In 2025, the threat actor Belsen_Group gained major attention after leaking configuration files and VPN-related credential data linked to over 15,000 FortiGate devices. The exposed material reportedly included highly sensitive security configuration details such as firewall rules, private keys, and plaintext passwords. The case was high-impact because the leak was released openly, making it easy for other threat actors to reuse the data for follow-on compromise, credential abuse, and network intrusion at scale. It also reinforced a key trend in 2025: perimeter device exposure and delayed patching continue to create long-term risk, even when the original compromise occurred earlier.



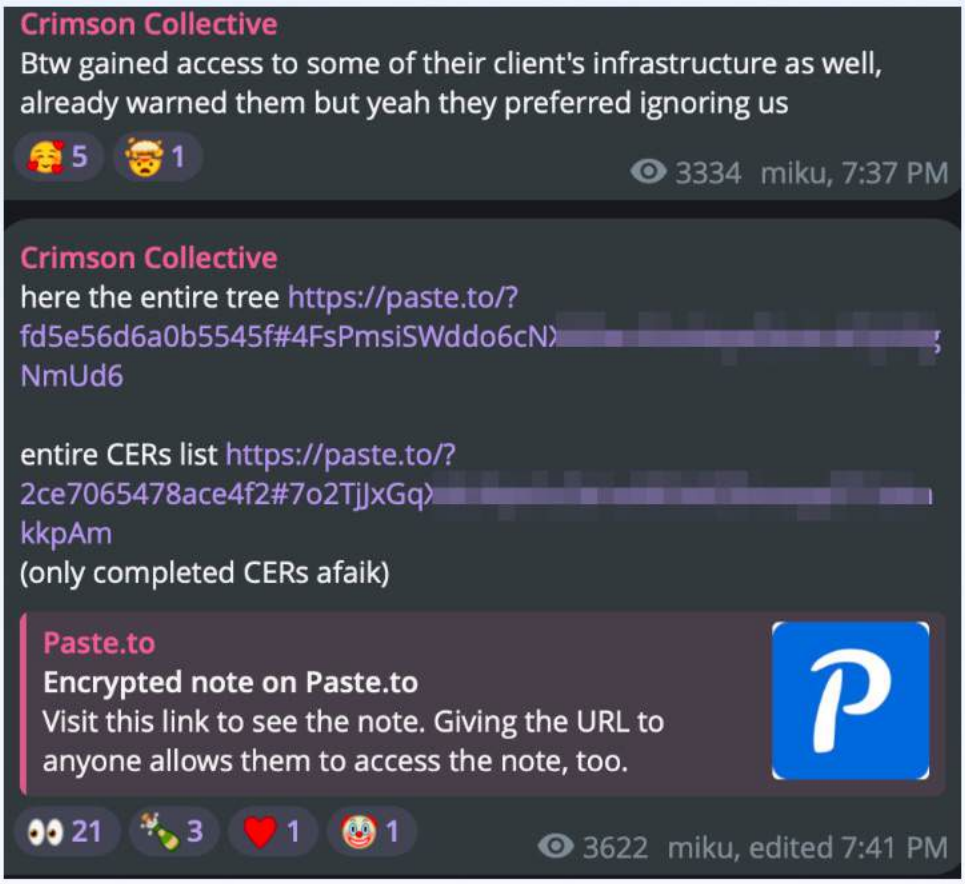
Threat actor leaking configs from over 15k Fortigate firewalls on their onion website for free

Red Hat Consulting GitLab Breach (Crimson Collective)

In late 2025, an extortion group calling itself Crimson Collective publicly claimed a breach of Red Hat's consulting-focused GitLab environment and alleged theft of a very large volume of internal repository data. The incident was significant because consulting repositories often contain aggregated customer-related engineering material, internal documents, and technical project files — creating a "one-to-many" exposure risk. Red Hat publicly confirmed the breach was limited to the consulting GitLab instance and stated there was no impact to core products or the broader software supply chain. The case became a key 2025 example of how attackers increasingly target centralised engineering and consulting environments due to the value of stored customer-linked data and reusable secrets.



Screenshot of the post made by crimson collective



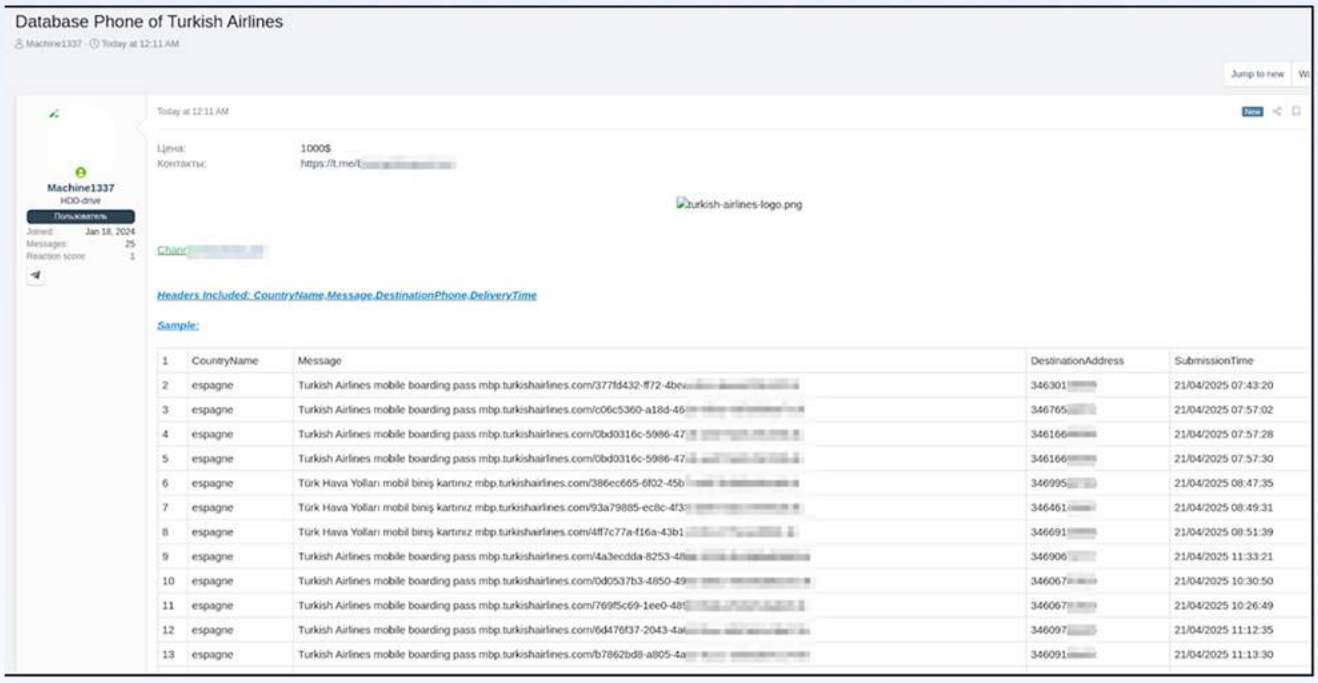
Screenshot of the post made by crimson collective

Screenshot of Threat actor claiming to possess 570 Gb of data

Compromise of a Global SMS Aggregation Ecosystem

In 2025, a major breach was linked to a central SMS aggregation ecosystem, where attackers allegedly obtained partner connectivity credentials (SMPP-type credentials) and used them to intercept or monitor customer messaging traffic. This incident was significant because it showed how compromising a shared communications layer can create large downstream risk, including OTP interception, account takeover attempts, and fraud activity across multiple industries such as banking, aviation, and consumer applications.

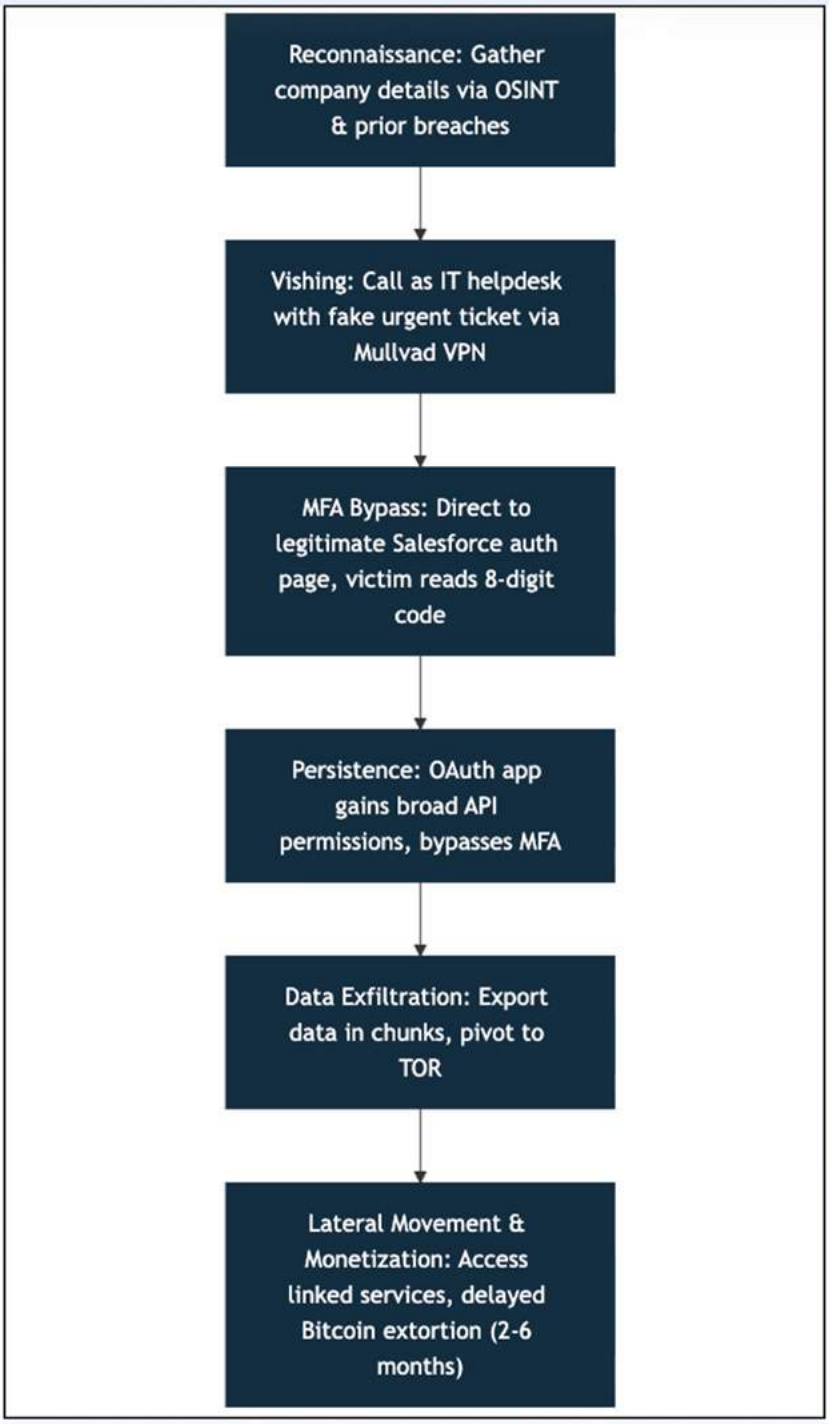
The case gained strong attention due to the high level of third-party dependency in SMS delivery systems and the direct security impact on authentication and transaction messaging.



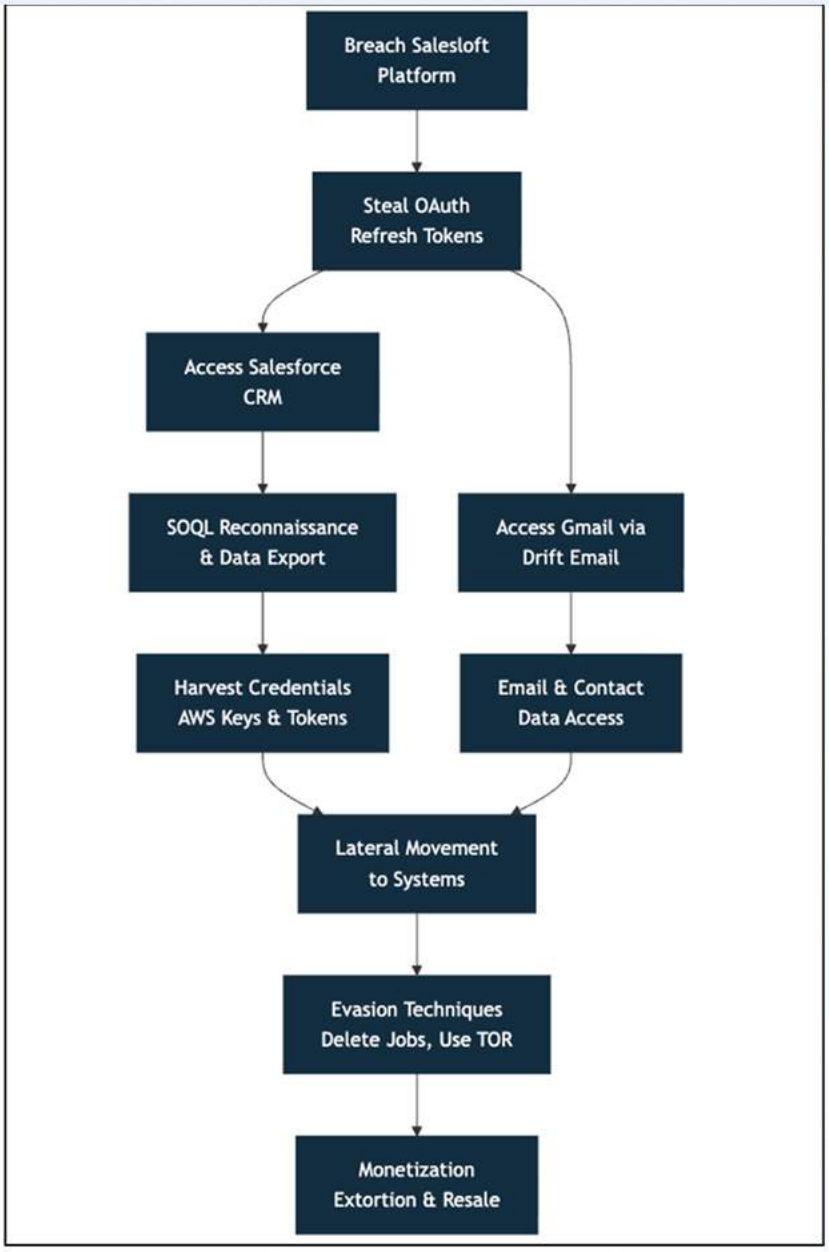
Dark Web Post Advertising Sale of Airline Messaging Records Linked to SMS Aggregation Abuse

ShinyHunters / "The Com" Ecosystem — Multi-vector Attacks on SaaS + Integrations

In 2025, multiple incidents reinforced the growth of a large cybercrime ecosystem often associated with "The Com" umbrella, where groups combine credential theft, social engineering, access brokering, and extortion. Activity linked to the ShinyHunters-style branding showed an evolution from single-company breaches to integration and partner exploitation where compromise of one SaaS connector or workflow can expose many downstream environments. This stood out as a major breach theme because it reflects scale through trust relationships, not just direct exploitation.



Flow chart representing the attack chain for the Salesforce Vishing Campaign



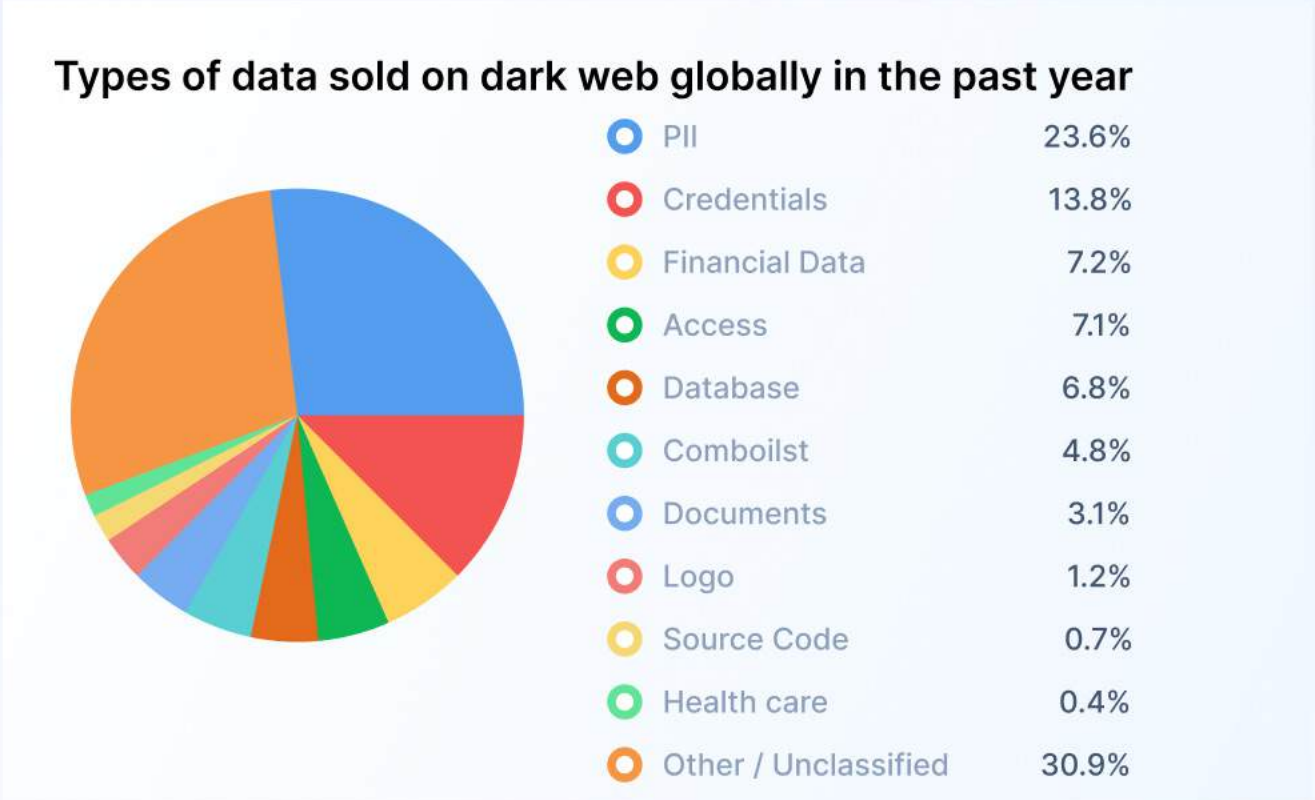
Flow chart representing the attack chain for the Salesloft Drift Supply Chain Attack

Supply-chain Focused Data Exfiltration

Threat actor grep remained notable in 2025 due to incidents tied to large-scale data harvesting and supply-chain style exposure in the QSR ecosystem. Reporting highlighted a case where the actor targeted a platform connected to high-volume retail operations, enabling theft of sensitive operational and potentially customer-linked data at scale. This case matters because QSR and retail ecosystems rely heavily on connected service providers, which makes them highly vulnerable to indirect compromise.

Screenshot of the X post made by the TA

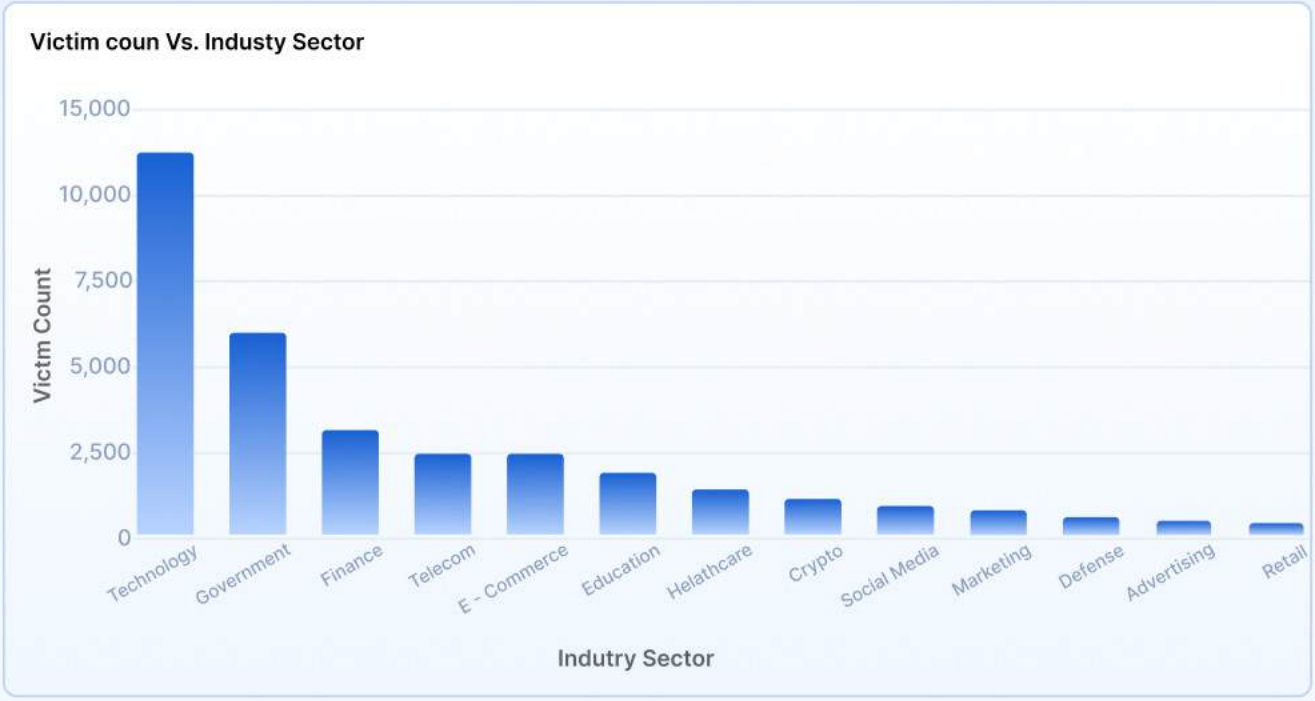
Data Types Circulated on the Dark Web



Screenshot showing Pie Chart for the types of data sold on dark web globally in the past year

The distribution of data types circulating across global dark web forums shows a clear pattern of what cybercriminals steal and sell most often. Over the past 12 months, the underground market was heavily driven by **identity-based data, account takeover material**, and **access listings**, all of which directly enabled fraud, intrusion, and ransomware campaigns. The dataset also shows a large portion of listings grouped under "Other / Unclassified", reflecting the wide variety of mixed and non-standard data sold on forums.

Industry-wise Distribution of Global Dark Web Incidents



Screenshot showing Pie Chart for Industry-wise Distribution of Global Dark Web Incidents in the past year

The global dark web ecosystem shows clear industry targeting patterns, where threat actors consistently focus on sectors that provide the best value for monetisation. The distribution of global dark web incidents indicates that attackers are prioritising industries with large user bases, high volumes of personal or financial data, and environments where stolen access can be resold to other criminals. The dataset also reflects how cybercrime has become highly commercial, with access brokers and data sellers actively feeding fraud, extortion, and ransomware ecosystems.

Information Technology recorded the highest exposure globally, with **over 13,000 incidents**, making it the most impacted sector in the dataset. This reflects how technology organisations sit at the center of digital ecosystems and often act as downstream enablers for compromise. Dark web listings linked to this sector commonly include leaked credentials, access to SaaS environments, cloud data exposure, and compromised developer or admin accounts. The high volume also highlights the risk of third-party and supply-chain exposure, where compromise of one tech provider can impact many connected customers.

The Government sector recorded **nearly 7,000 incidents**, showing continued threat actor focus on public infrastructure and citizen-facing systems. Government entities remain attractive because they store large volumes of sensitive personal data and often operate legacy systems. Dark web

activity in this sector commonly includes leaked citizen databases, internal documents, compromised portals, and access listings linked to public agencies.

Finance remains one of the most sensitive and consistently targeted sectors, with **over 4,000 incidents** recorded globally. Even when the volume is lower than technology or government, financial organisations provide high-value data and strong leverage for fraud. The most common exposures linked to this sector include banking credentials, identity records, customer PII, and access to internal systems that can later support account takeover or financial theft.

High activity was also observed across **Telecom** and **E-commerce**, with **over 3,000 incidents each**. Telecom is repeatedly targeted due to the value of subscriber data, SIM-swap enabling information, and internal access that can support wider abuse. E-commerce listings commonly include customer databases, loyalty data, purchase history, and admin panel access, which are often reused for fraud and large-scale credential stuffing operations

A steady volume of incidents was also observed across **Education** (over **2,000**) and **Healthcare** (around **1,500**). These sectors remain exposed because they contain high volumes of identity-linked data and often have uneven security maturity.

Emerging but consistent activity was recorded across **Crypto, Social Media**, and **Marketing**, with each sector showing **hundreds to over a thousand incidents**. Crypto incidents often involve exchange credentials, user databases, and wallet-linked data. Social media related incidents typically include stolen accounts, scraped user data, and access resale, which are frequently used to amplify scams. Marketing and advertising breaches often expose campaign systems, email lists, and customer engagement data, supporting phishing operations and lead monetisation.

Lower-volume but notable exposure was also observed in **Defense, Advertising**, and **Retail**, showing that dark web exposure is not limited to only high-volume consumer industries. While these sectors appear in smaller numbers, incidents in these categories often carry high operational or reputational.

Global Ransomware Activity Overview

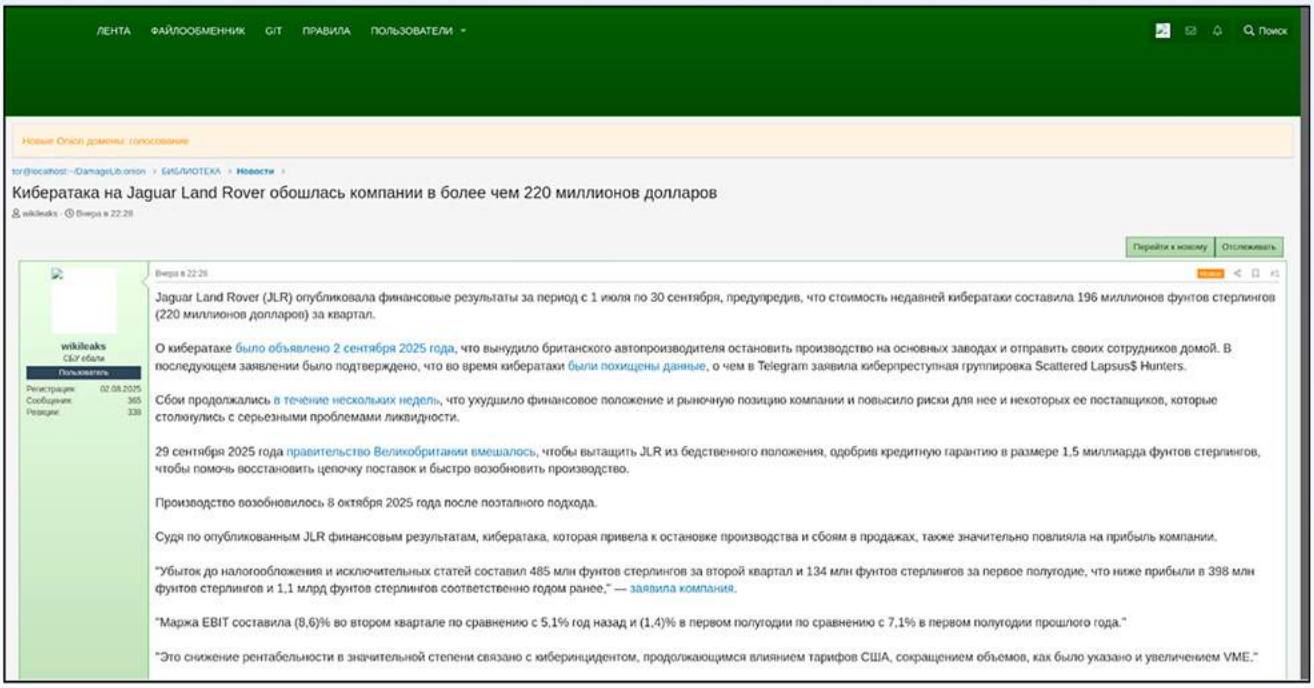
Ransomware remains a top global cyber threat, driven by financial motives and widespread activity. The fragmented landscape sees numerous groups profiting from extortion. This report details key groups, common initial access methods (credential exposure, insecure remote access, exploiting internet-facing systems), and most affected sectors/countries. Steady year-round pressure confirms ransomware's non-regional nature, impacting critical infrastructure, commercial industries, and public services, with attackers increasingly combining disruption and data theft to maximize pressure.

Significant Ransomware & Extortion Attacks Worldwide

Jaguar Land Rover (JLR) suffered a significant cyber incident in late August/September 2025 that disrupted production across multiple sites and caused broader supply-chain impact. Public reporting indicates JLR temporarily shut down key systems as part of containment and recovery, resulting in factory downtime and operational disruption. Scattered Lapsus$ Hunters claimed

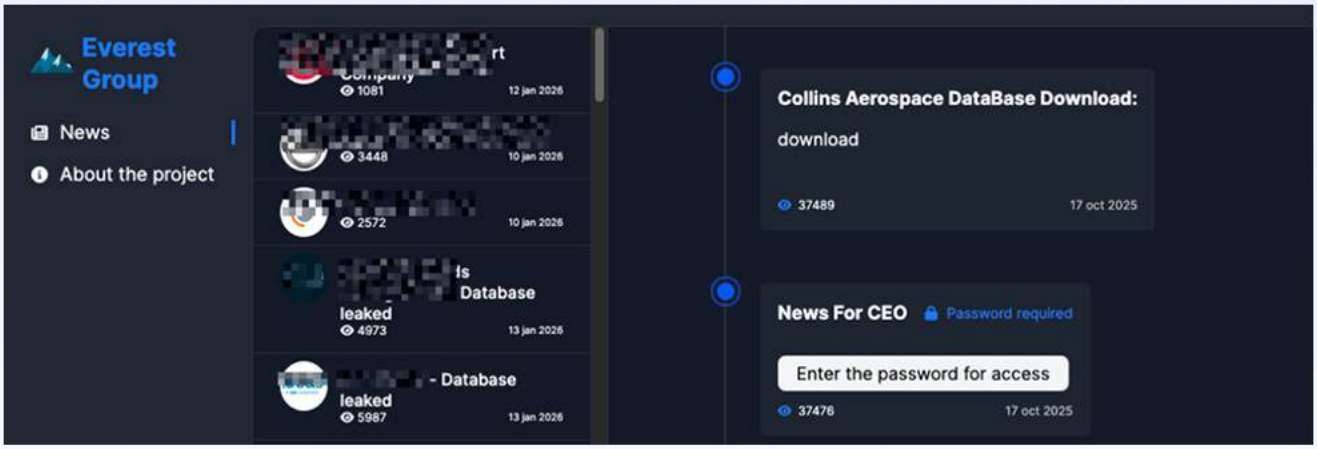
responsibility, and the incident was linked in reporting to Scattered Spider/Lapsus$/ShinyHunters-style intrusion activity, which is commonly associated with identity-driven access and social engineering-led compromise.

While JLR did not publicly disclose detailed technical findings or the full intrusion chain, the incident remains a high-impact example of how ransomware and extortion-linked operations can disrupt industrial environments where operational downtime creates strong pressure. Earlier in 2025, the Hellcat ransomware group also claimed involvement in a separate JLR-related data leak, indicating sustained adversary interest in the organisation during the year.



Dark Web Post Detailing Jaguar Land Rover Cyberattack (2025)

In **September 2025**, Collins Aerospace (an RTX subsidiary) suffered a ransomware-linked cyber incident that disrupted passenger processing services across multiple European airports, including **London Heathrow, Brussels**, and **Berlin**. The attack impacted Collins Aerospace's **airport check-in/ boarding systems**, forcing airlines and airports to shift to manual procedures and causing delays and operational disruption. This incident is a notable example of **third-party concentration risk**, where a ransomware event affecting a single technology provider creates cascading impact across multiple airports and airline operations. Public sources described the incident as ransomware-related, and the **Everest** ransomware group later **claimed responsibility** for the attack. Overall, the event highlights how ransomware operators can generate large-scale disruption by targeting shared service providers supporting critical infrastructure.



Collins Aerospace (RTX) Mention on Everest Ransomware Leak Site

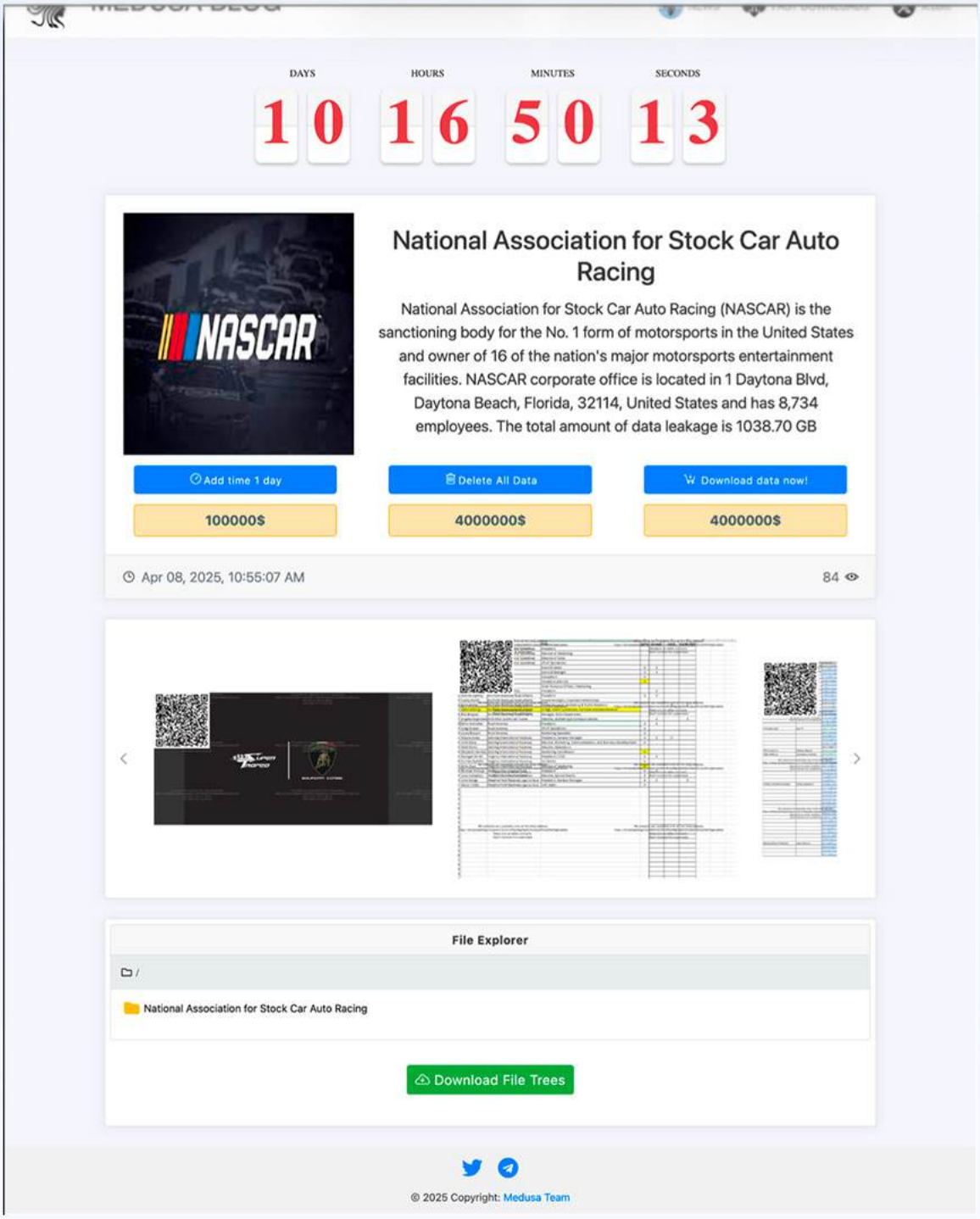
Several high-impact ransomware incidents over the past 12 months gained global attention due to the scale of disruption, brand visibility, and downstream impact. **Ingram Micro** was reportedly impacted by the **SafePay** ransomware group, drawing attention due to its role as a major global IT distributor and the potential supply-chain implications for downstream customers.

SafePay Ransomware Leak Site Listing for Ingram Micro

In the manufacturing sector, **Asahi Group Holdings (Japan)** was claimed by **Qilin**, with public reporting indicating disruption concerns and data theft claims. Another major trend was the **Cl0p-led Oracle E-Business Suite exploitation wave**, which highlights exploit-at-scale extortion activity impacting multiple large organisations, notable victims linked to this campaign include **Harvard University, American Airlines (Envoy Air)**, and **The Washington Post**, underscoring the broad reach of third-party software exploitation

The education sector also saw high-profile impact through the **PowerSchool** incident, which drew wide attention due to the scale of education ecosystem exposure and follow-on consequences. Additionally, **NASCAR** was listed on the **Medusa** leak site, reflecting continued ransomware targeting of globally recognised brands where reputational pressure increases extortion leverage.

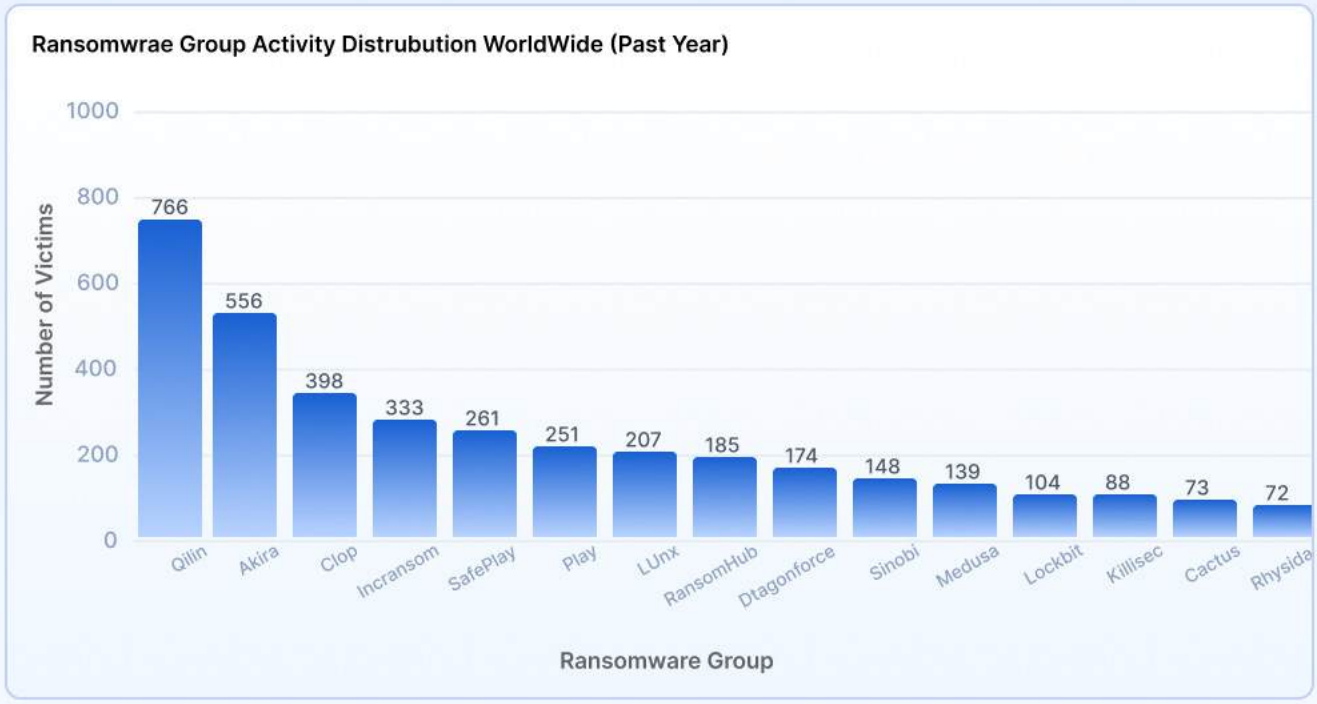
Overall, these incidents reinforce that ransomware operations continue to generate widespread impact by targeting high-value enterprises, education platforms, and widely used enterprise software to maximise disruption and extortion pressure.



Medusa Ransomware Leak Site Post Showing NASCAR as a Victim

Most Active Ransomware Groups Worldwide

Global ransomware activity over the past 12 months remained highly fragmented, with multiple groups competing at scale rather than a single dominant leader. As reflected in the below chart, **Qilin** emerged as the most active ransomware group globally with around **700 victims**, followed by **Akira** with **well over 500 victims**, and **Cl0p** with **close to 400 victims**. Beyond the top three, several groups sustained strong operational output, including **Incransom** with **over 300 victims**, **SafePay** and **Play** with around **250 victims each**, and **Lynx** with just **over 200 victims**. This distribution highlights how rapidly scaling and high-output ransomware groups continue to gain traction through affiliate-driven models, shared tooling, and consistent access broker support.



Most active ransomware group worldwide (Past Year)

The global ransomware threat is segmented into three tiers. The most active groups—**Qilin, Akira**, and **Cl0p**, followed by **Incransom, SafePay, Play, Lynx, RansomHub**, and **Dragonforce**—drive the majority of attacks. They typically use credential abuse, exploit internet-facing systems, and buy initial access, leading to data theft, rapid lateral movement, and double extortion.

A second-tier, including **Sinobi, Medusa, LockBit, Killsec, Babuk-bjorka, Cactus, Rhysida, Sarcoma, World Leaks, Nightspire, Everest, FunkSec, and Interlock**, operates with steady but lower victim counts. They target mid-sized organizations, exploiting weak remote access (RDP/VPN), unpatched applications, and poor network segmentation for fast intrusions.

The long-tail consists of **low-volume and emerging groups like Pear, Fog, Nova, DireWolf, Kairos, RansomHouse, and devman**. Collectively, these groups signal a decentralizing ecosystem, with new brands constantly appearing through rebranding or splintering. This resilience means the overall ransomware threat persists despite disruptions to high-profile operators.

Based on the ransomware activity distribution and the victim counts observed across the year, three key trends were identified:

- **Ecosystem fragmentation is increasing**: While a few groups such as **Qilin and Akira** remained highly active, a significant portion of activity came from numerous mid-tier and smaller groups. This indicates that ransomware has become a highly competitive marketplace rather than a few dominant "cartels."
- **Fast-scaling operators gained significant traction**: Groups such as **Incransom, SafePay, Lynx, and RansomHub** recorded strong victim volumes during the year, indicating that ransomware crews can rapidly scale operations through affiliate recruitment, shared tooling, and brokered access.
- **Rebranding and naming variants remain common**: Multiple ransomware brands appear in different naming formats and variants (e.g., LockBit and Babuk variants, etc.). These differences may reflect rebranding, affiliate branding, or inconsistencies in how groups are tracked, and should be treated as potential duplicates rather than confirmed distinct entities.

Overall, the ransomware group distribution highlights a **fast-moving and monetized threat environment**, where both established operators and new entrants continue to target victims across all major sectors, enabled by credential exposure, insecure remote access, and supply of initial access from underground markets.

Initial Access Vectors (IAVs) Used by Top Ransomware Groups & Opportunistic Players Globally

Group Name	IAVs
Qilin	Phishing / social engineering to harvest credentials or deliver loaders
	Use of stolen credentials (often sourced from infostealer logs)
	Exploitation of exposed services (RDP/VPN) where authentication controls are weak
	Purchase of access from Initial Access Brokers (IABs)
Akira	Exploitation of VPN / firewall vulnerabilities (commonly edge appliances)
	Use of compromised remote access (VPN/RDP) credentials
	Leveraging insecure or exposed remote services and weak MFA configurations
	Opportunistic targeting of exposed enterprise environments (including hypervisors and backup infrastructure observed in campaigns)

Group Name	IAVs (Indicators and Vulnerabilities)
Cl0p	Exploitation of managed file transfer (MFT) platforms and mass-exploitation campaigns
	Leveraging vulnerabilities in internet-facing applications to access file stores and databases
	Data theft-focused intrusions (extortion often driven by exfiltration rather than broad encryption)
Incransom	Exploitation of internet-facing vulnerabilities, particularly enterprise appliances
	Credential abuse (VPN/RDP), including reuse of valid leaked credentials
	Phishing-delivered initial payloads
	Opportunistic access via externally exposed services
SafePay	Use of weak / compromised credentials (VPN access is repeatedly noted)
	Exploitation of exposed remote services (VPN/RDP)
	Opportunistic targeting of organizations with exposed perimeter access
	Rapid execution post-entry
Play	Exploitation of internet-facing systems and public vulnerabilities
	Credential theft / credential reuse (VPN/RDP)
	Access purchased through brokers or harvested from previous compromises
	Abuse of exposed remote services with weak authentication
Lynx	Credential theft and reuse (infostealer-sourced credentials)
	Exploitation of exposed RDP/VPN services
	Use of access sourced through brokers / prior compromises
	Double-extortion approach (data theft prior to encryption)

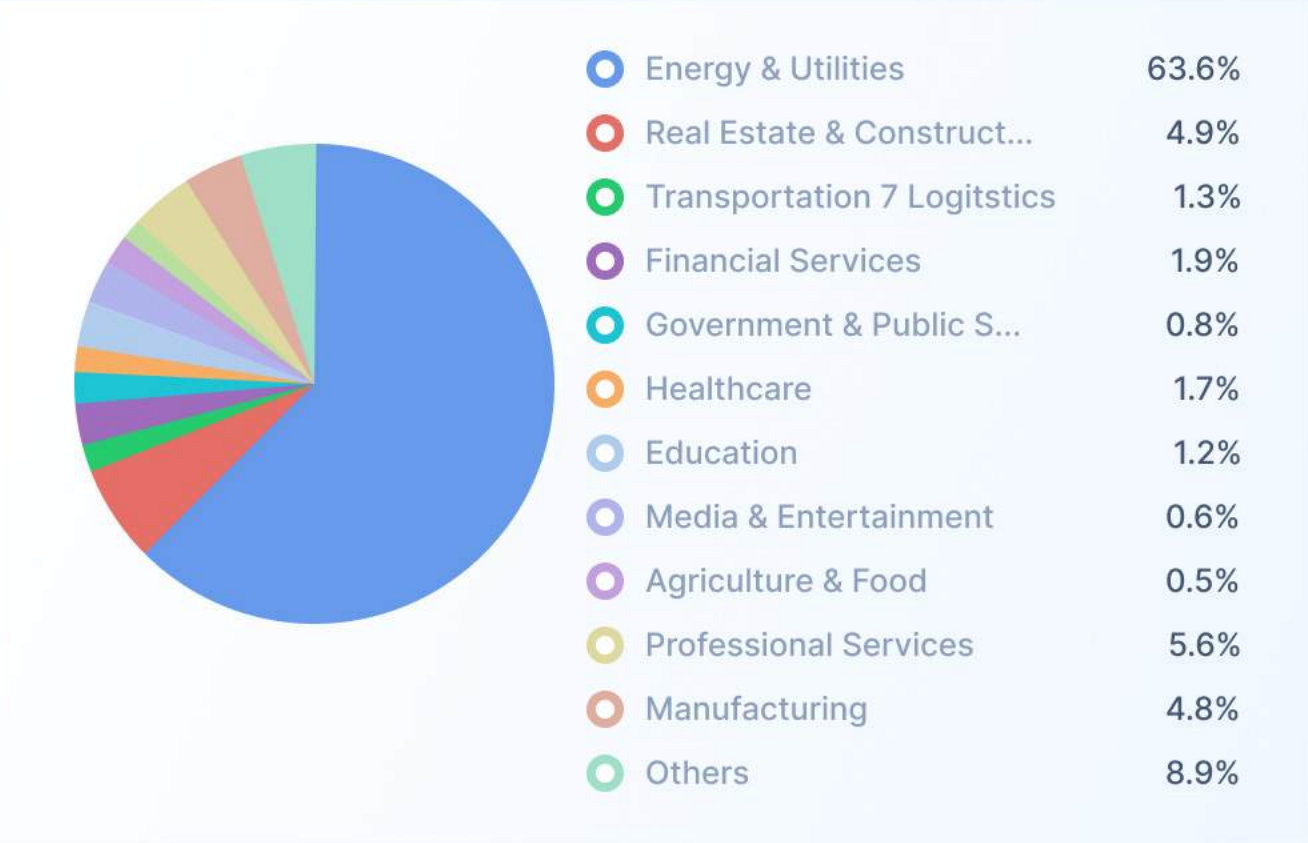
Group Name	IAVs (Indicators and Vulnerabilities)
RansomHub	Phishing and social engineering for initial foothold
	Exploitation of vulnerabilities after gaining access
	Exploitation of vulnerabilities after gaining access
	Use of tooling aimed at disabling security controls prior to execution
Dragonforce	Network scanning + exploitation of exposed services
	Credential brute forcing / password attacks
	Abuse of remote admin tooling once access is established
	Opportunistic exploitation of weak external exposure
Sinobi	Credential-based access (including compromised VPN credentials)
	Exploitation of edge appliance exposure (SSL VPN-type)
	Stealth-led intrusion behavior (quiet access → expansion → extortion)
	Likely affiliate-style operations observed (campaign patterns consistent with RaaS models)

Across the top 10 ransomware groups, the most consistent initial access patterns were:

- **Credential abuse remains the dominant entry vector** (stolen VPN/RDP credentials, password spraying, and credential reuse from infostealer logs).
- **Perimeter exposure continues to drive ransomware scale**, especially via VPN/firewall/ remote access appliances.
- **IAB-driven access enables rapid expansion**, helping high-activity groups scale without running full intrusion chains themselves.
- **Exploit-at-scale models remain high-impact**, particularly visible through Cl0p-style campaigns targeting third-party platforms.

Industry-Wise Breakdown of Ransomware Attacks Worldwide

The global ransomware threat landscape shows clear sector targeting patterns, with threat actors consistently focusing on industries that are either operationally critical or have high leverage for financial and data extortion. As shown in the chart below, the distribution reflects both concentrated targeting of high-impact industries and continued expansion into a wide range of other sectors.



Industry-wise Distribution of Ransomware Attacks Globally (Past 12 Months)

The **Energy & Utilities** sector was the most affected globally, with around **2,600 victims**, indicating ransomware operators prioritize essential services for faster negotiation. This sector's vulnerability is exacerbated by legacy systems and complex dependencies.

Professional Services, Real Estate & Construction, and Manufacturing followed, each with around **200 victims**. These are targeted for sensitive data, business dependency, and the immediate impact of downtime.

Technology saw **around 170 victims**, while **Financial Services** had **close to 80**. Technology firms offer wider disruption potential, and financial services remain a high-leverage target due to data sensitivity and reputational risk.

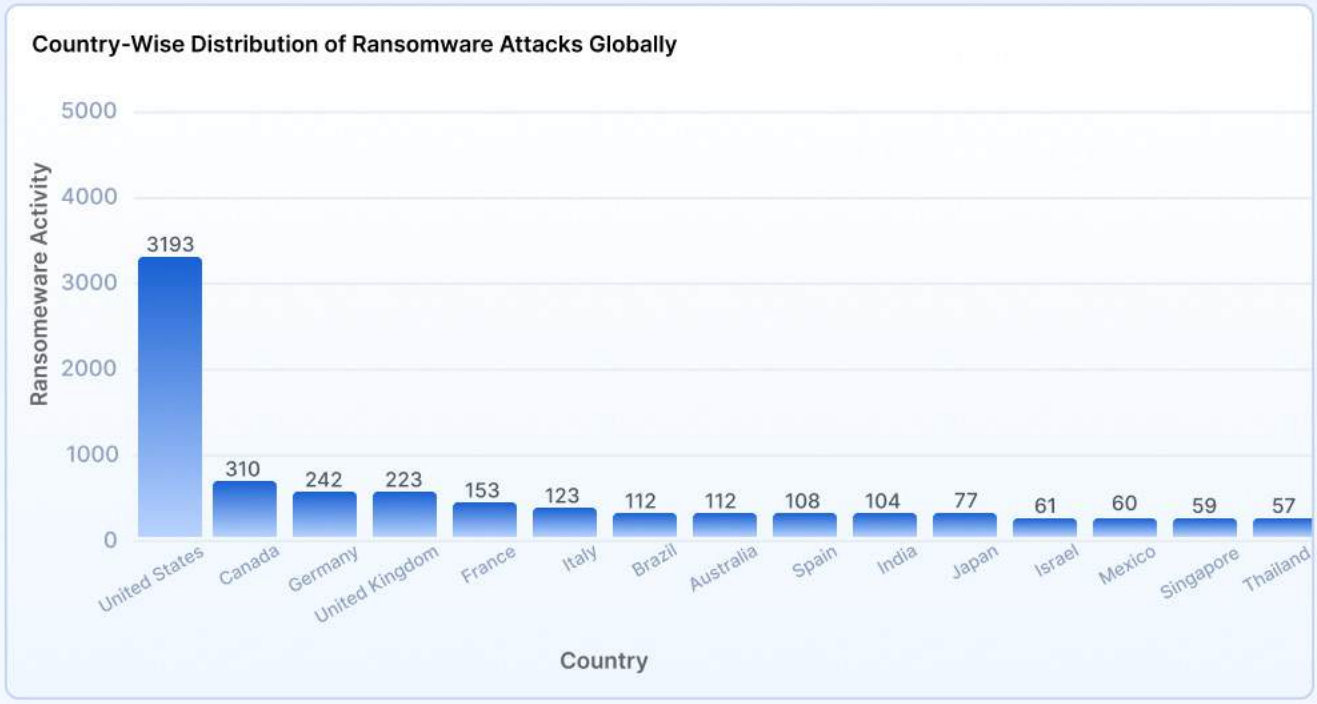
Lower, consistent activity was observed in **Healthcare (around 70 victims)**, **Transportation & Logistics (around 50 victims)**, and **Education (around 50 victims)**. These are vulnerable due to service urgency, time-sensitive operations, and often weaker security controls.

The Government & Public Sector, Media & Entertainment, and Agriculture & Food each recorded **roughly 20–30 victims**, highlighting growing diversification. These incidents exploit outdated infrastructure and time-sensitive operations.

Finally, "Others" accounted for about 360 victims, showing ransomware is expanding beyond traditional high-value targets by exploiting weak security across diverse verticals.

Most Affected Countries by Ransomware Activity

The global ransomware victim distribution shows a strong concentration in a small set of countries, reflecting where ransomware operators find the best combination of **high-value targets, large digital footprints, and widespread exposure of remote access infrastructure**. As highlighted in the country-wise charts, ransomware activity remains heavily concentrated in a few key markets, with the leading countries consistently targeted by multiple ransomware groups.



Country-wise Distribution of Ransomware Attacks Globally (Past 12 Months) – Top 20 Countries

The United States remained the most affected country with **just over 3,000 victims**, significantly higher than others, reflecting its extensive enterprises, tech adoption, and high system exposure. **Canada** followed with **around 300 victims**, showing continued focus on large, digitally connected economies.

Europe saw consistently high ransomware activity, with **Germany** and the **United Kingdom** each recording **over 200 victims**, due to targeting of large, high-value business ecosystems. **France** and **Italy** were also impacted, confirming exploitation of environments with dense commercial activity and broad third-party dependencies.

Globally, **Brazil and Australia** recorded just **above 100 victims**, while **Spain and India** saw around **100 victims**. Moderate but persistent activity was noted in countries including **Japan, Israel, Mexico, Singapore, Switzerland, Taiwan, Thailand, Malaysia, the UAE, and Argentina**. This confirms ransomware operators are targeting victims beyond traditional hotspots, pursuing both advanced and rapidly digitizing markets.

Key Ransomware Trends Observed Globally

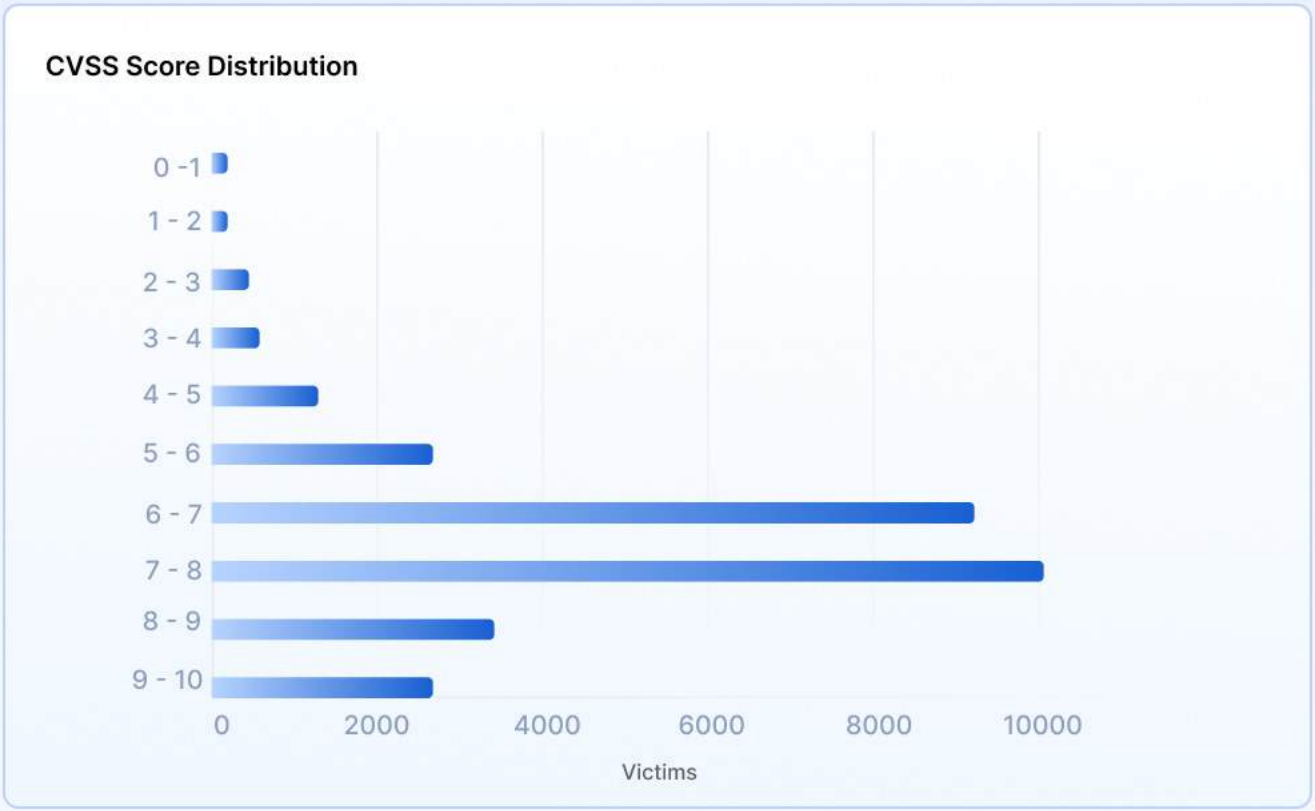
Threat actors operating globally continue to rely on a mix of high-volume, low-cost entry methods and high-impact exploitation techniques:

- **Ransomware remains highly active and widespread:** Victim disclosures stayed consistently high throughout the year, confirming ransomware as a continuous global threat rather than isolated campaigns.
- **The ecosystem is fragmented and competitive:** Multiple ransomware groups operated at scale, with high-output operators leading activity while many mid-tier and small groups continued to contribute to global victim volume.
- **Credential abuse continues to be a primary entry route:** Stolen credentials, password reuse, and weak access controls remain heavily exploited, often combined with exposed RDP/VPN services.
- **Internet-facing infrastructure remains a key risk:** VPN/firewall exposure and exploitation of public-facing systems continue to enable rapid compromise and wide targeting.
- **Energy & Utilities remains the most affected sector:** Essential services continue to attract ransomware operators due to disruption impact, high pressure to restore services, and complex environments.
- **Ransomware targeting is global, but concentrated in key markets:** The United States remains the most affected country, with consistent targeting also observed across major economies in Europe and other digitally connected markets.
- **Activity spikes are often driven by leak-site publishing waves:** Month-wise surges were influenced by increased victim postings from major groups, showing that public disclosures may occur in batches rather than evenly over time

Overview of Dark Web Activity

Key Takeaways (Vulnerabilities & Exploitation Trends)

- Attackers are exploiting public-facing systems first (VPNs, firewalls, web apps) because they give fast entry into networks.
- Patch delays remain one of the biggest reasons for breaches scale, especially for edge appliances.
- Many high-impact incidents are now linked to exploit-at-scale campaigns, where one vulnerability leads to many victims.
- Credential theft + vulnerability exploitation is a common combo (steal access → exploit exposed services → ransomware/extortion).
- Organisations with large digital footprints and weak asset visibility are more likely to be hit, even without being directly targeted.



Weighted Average CVSS Score 7.34

Months	Vulnerability Count
January 2025	3074
February 2025	2187
March 2025	2390
April 2025	1870
May 2025	1241
June 2025	2065
July 2025	2198
August 2025	2171
September 2025	2139
October 2025	2196
November 2025	1811
December 2025	1493

Most Affected Countries by Ransomware Activity

CVE ID and Product Name	CVSS v3 Score	Description	Count of Discussions
CVE-2025-55182React, Next.js, next.js, react	10.0	A pre-authentication remote code execution vulnerability exists in React Server Components versions 19.0.0, 19.1.0, 19.1.1, and 19.2.0 including the following packages: react-server-dom-parcel, react-server-dom-turbopack, and react-server-dom-webpack. The vulnerable code unsafely deserializes payloads from HTTP requests to Server Function endpoints.	2865
CVE-2025-53770SharePoint Server,sharepoint_server	9.8	Deserialization of untrusted data in on-premises Microsoft SharePoint Server allows an unauthorized attacker to execute code over a network. Microsoft is aware that an exploit for CVE-2025-53770 exists in the wild. Microsoft is preparing and fully testing a comprehensive update to address this vulnerability. In the meantime, please make sure that the mitigation provided in this CVE documentation is in place so that you are protected from exploitation.	1738
CVE-2025-61882concurrent_processing, Oracle Concurrent Processing	9.8	Vulnerability in the Oracle Concurrent Processing product of Oracle E-Business Suite (component: BI Publisher Integration). Supported versions that are affected are 12.2.3-12.2.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Concurrent Processing. Successful attacks of this vulnerability can result in takeover of Oracle Concurrent Processing. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	735

CVE ID and Product Name	CVSS v3 Score	Description	Count of Discussions
CVE-2025-59287Windows Server 2012, Windows Server 2019, Windows Server 2022 23H2, windows_server_2025, Windows Server 2025, windows_server_2022_23h2, Windows Server 2016, windows_server_2022, windows_server_2012, Windows Server 2022, windows_server_2019, windows_server_2016	9.8	Deserialization of untrusted data in Windows Server Update Service allows an unauthorized attacker to execute code over a network.	620
CVE-2025-14847mongodb, MongoDB	7.5	Mismatched length fields in Zlib compressed protocol headers may allow a read of uninitialized heap memory by an unauthenticated client. This issue affects all MongoDB Server v7.0 prior to 7.0.28 versions, MongoDB Server v8.0 versions prior to 8.0.17, MongoDB Server v8.2 versions prior to 8.2.3, MongoDB Server v6.0 versions prior to 6.0.27, MongoDB Server v5.0 versions prior to 5.0.32, MongoDB Server v4.4 versions prior to 4.4.30, MongoDB Server v4.2 versions greater than or equal to 4.2.0, MongoDB Server v4.0 versions greater than or equal to 4.0.0, and MongoDB Server v3.6 versions greater than or equal to 3.6.0.	396

CVE ID and Product Name	CVSS v3 Score	Description	Count of Discussions
CVE-2025-8088winrar, WinRAR, Dtsearch, dtsearch	8.8	A path traversal vulnerability affecting the Windows version of WinRAR allows the attackers to execute arbitrary code by crafting malicious archive files. This vulnerability was exploited in the wild and was discovered by Anton Cherepanov, Peter Kosinar, and Peter Strycek from ESET.	372
CVE-2025-43300iPad OS, iPhone OS, ipados, macos, macOS, iphone_os	10.0	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 15.8.5 and iPadOS 15.8.5, iOS 16.7.12 and iPadOS 16.7.12. Processing a malicious image file may result in memory corruption. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals	368
CVE-2025-32463enterprise_linux, leap, linux_enterprise_desktop, linux_enterprise_real_time, sudo, ubuntu_linux, Linux Enterprise Server for SAP, Debian Linux, debian_linux, Leap, Linux Enterprise Desktop, Enterprise Linux, Sudo, Ubuntu Linux, Linux Enterprise Real Time, linux_enterprise_server_for_sap	9.3	Sudo before 1.9.17p1 allows local users to obtain root access because /etc/nsswitch.conf from a user-controlled directory is used with the --chroot option.	316

CVE ID and Product Name	CVSS v3 Score	Description	Count of Discussions
CVE-2025-5777netscaler_gateway, Netscaler Application Delivery Controller, netscaler_application_delivery_controller, Netscaler Gateway	7.5	Insufficient input validation leading to memory overread when the NetScaler is configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) OR AAA virtual server	264
CVE-2021-26829scadabr, Scadabr	5.4	OpenPLC ScadaBR through 0.9.1 on Linux and through 1.12.4 on Windows allows stored XSS via system_settings.shtm	246

APT Activity

Overview

This section provides a chronological overview of major cyber threat activities and security developments throughout 2025, highlighting the evolving tactics, targets, and geopolitical implications of advanced persistent threat (APT) groups and cybercriminal organizations.

Across the year, multiple nation-state–aligned groups such as Salt Typhoon, Lazarus Group, Sandworm, Volt Typhoon, Kimsuky, BITTER, Silver Fox, Muddy Water, RomCom, and APT36 were linked to high-impact incidents. These ranged from sanctions and government advisories to large-scale cryptocurrency thefts, destructive wiper attacks against critical infrastructure, satellite system intrusions, and sustained espionage campaigns targeting telecommunications, government, defense, and private industry. Financially motivated attacks, particularly against cryptocurrency exchanges, reached record levels, underscoring the convergence of cyber espionage and revenue generation.

Q1 2025

On January 17, 2025, the United States imposed sanctions related to the Salt Typhoon cyber campaign, as detailed in a U.S. State Department press statement. The sanctions targeted Yin Kecheng and Sichuan Juxinhe for their roles in conducting and supporting malicious cyber activities attributed to the Salt Typhoon threat actor. In February 2025, the Lazarus Group was linked to a record-breaking **$1.5 billion cryptocurrency theft from the Bybit exchange**. TRM Labs provided an in-depth analysis of the incident, tracing blockchain movements and attributing the Ethereum theft, while The Hacker News confirmed Bybit's acknowledgment of the breach.

Shortly after, between March and April 2025, Sandworm conducted destructive cyber operations involving the **"ZeroLot"** wiper malware. According to a joint BankInfoSecurity and ESET report, researchers identified both ZeroLot and the related PathWiper malware actively targeting Ukrainian critical infrastructure, reinforcing Sandworm's role in disruptive and destructive cyber campaigns.

Q2 2025

Between April and May 2025, the RomCom threat actor carried out **"Operation Deceptive Prospect,"** marking a notable evolution in its operational focus. As outlined in Picus Security's RomCom Threat Actor Evolution (2023–2025) report, the group shifted from primarily regional espionage activities to targeting private industry organizations in the United Kingdom and Canada. On June 20, 2025, a critical WinRAR zero-day vulnerability, tracked as CVE-2025-6218, was disclosed. Wiz.io's vulnerability database provided a technical breakdown of the path traversal flaw, which was discovered by researcher whs3-detonator under the Zero Day Initiative (ZDI). Just one day earlier, on June 19, 2025, reports emerged that the China-linked Salt Typhoon group had breached satellite communications firm Viasat. According to Security Affairs, citing Bloomberg and Reuters, the attackers gained access to satellite telemetry systems, highlighting the group's continued focus on strategic infrastructure targets.

Q3 2025

In August 2025, CloudSEK uncovered an active malware campaign attributed to APT36 that leveraged Linux desktop entry files and Google Drive for payload delivery. The campaign involved phishing ZIP archives containing malicious **".desktop" shortcut files, which, once executed, downloaded additional payloads from Google Drive**. The malware established persistence, evaded detection mechanisms, and communicated with a WebSocket-based command-and-control server. Later that month, on August 27, 2025, U.S. authorities issued a joint advisory from CISA, the FBI, and the NSA warning of widespread Salt Typhoon intrusions into telecommunications backbones.

ExtraHop's Anatomy of an Attack – CISA Alert provided analysis of the advisory, emphasizing the scale and depth of the infiltration. In September 2025, Kimsuky was observed conducting AI-enabled social engineering operations. According to research from the Genians Security Center and reporting by eSecurity Planet, North Korean actors used ChatGPT to generate **highly realistic fake personas and deepfake military identification documents**, significantly enhancing the credibility and effectiveness of their credential fraud and espionage activities.

Q4 2025

In November 2025, the BITTER threat group, also known as APT-C-08, was observed exploiting the WinRAR zero-day vulnerability CVE-2025-6218. SecPod's report, Archive Terror – Dissecting the WinRAR CVE-2025-6218 Exploit, detailed how the group weaponized the flaw against South Asian government targets. Around the same time, on November 27, 2025, the Upbit cryptocurrency exchange suffered a **cyber heist** resulting in the theft of approximately $30–$32 million. SC Media reported that the attack was linked to a private key vulnerability and attributed to the Lazarus Group. Separately, reporting in April 2025 revealed details of what became known as the "Geneva Acknowledgement," in which Chinese officials, during a secret December meeting, indirectly admitted to Volt Typhoon cyber operations, framing them as a form of strategic deterrence, as discussed by SecurityWeek.

Additionally, CloudSEK's TRIAD team documented a sophisticated phishing campaign by the Chinese Silver Fox APT targeting Indian entities using income-tax-themed lures. The campaign, initially misattributed to SideWinder, employed DLL hijacking and the modular Valley RAT to maintain persistence. Finally, CloudSEK's TRIAD also identified an evolved **spear-phishing campaign by the Muddy Water APT group** targeting diplomatic, maritime, financial, and telecom sectors across the Middle East. The campaign delivered a new Rust-based implant, "RustyWater," via malicious Word documents and icon spoofing, representing a significant advancement in the group's tooling.

Hacktivist Activity

Hacktivist activity accelerated globally throughout 2025, driven by sustained geopolitical tensions, ideological polarization, and the widespread exposure of public-facing digital infrastructure. Analysis of 17,700+ verified hacktivist incidents reveals a threat landscape increasingly shaped by campaign-style operations, often synchronised with international political flashpoints, military escalations, and diplomatic developments.

Rather than isolated or spontaneous actions, hacktivist operations demonstrate **reactive coordination**, with attack waves emerging rapidly in response to global events. These campaigns primarily aim to generate **visibility, disruption, and psychological impact**, leveraging cyberspace as a platform for influence rather than long-term compromise.

Ideological drivers remain central to global hacktivist operations, with **pro-Palestinian narratives being one among many**, including **Support for Palestine, OPIndia, and OpIsrael** - emerging as the most prominent motivators across campaigns. S**trong uptick in activity during the event of the border conflict between Thailand and Cambodia was observed**. These themes demonstrate a strong correlation between geopolitical developments and attack intensity, with activity levels frequently spiking in response to military escalations, diplomatic developments, and international political events. Hacktivist operations consistently align with global flashpoints, reinforcing their role as a reactive instrument of political signaling and influence.

Groups such as **SKYNET, ITZ ZERO-DAY, DXPLOIT, and KillNet-aligned networks** emerged as recurring actors within the global ecosystem, regularly engaging in **synchronized DDoS operations, data exposure claims, and propaganda-driven campaigns**. These activities targeted high-visibility sectors and countries - including government institutions, financial services, telecommunications providers, and technology platforms, across multiple regions. Campaign timing frequently coincided with geopolitical milestones, suggesting deliberate coordination intended to maximize **psychological impact, public disruption, and narrative amplification**, rather than achieve sustained technical compromise.

Countries with high geopolitical visibility, strong financial ecosystems, and extensive digital infrastructure - including the United States, Israel, India, Indonesia, and multiple European and Middle Eastern nations, consistently emerged as focal points for hacktivist targeting.

Attack Distribution :

- **Data Leaks & Credential Dumps (~7,900 incidents)** - A growing volume of incidents involve exposed credentials, scraped databases, and previously leaked datasets. These are primarily leveraged for **reputational damage and narrative amplification**, rather than enabling downstream intrusion.
- **Distributed Denial-of-Service (DDoS) (~3,570 incidents)** - The dominant disruption method, widely used against government portals, financial platforms, telecommunications providers, and media outlets. Operations frequently rely on coordinated **"call-to-action"** campaigns on Telegram.
- **Website Defacement (~1,320 incidents)** - Continues to function as a symbolic messaging tool, targeting education, small enterprises, NGOs, and public-sector sites with weak security postures.

The remaining **~4,910 incidents** consist of **propaganda-only operations, secondary or supporting actions, low-confidence events, and multi-vector overlaps**, reflecting the increasingly blended and narrative-driven nature of modern hacktivist campaigns.

Overall, attack distribution highlights a shift toward **visibility-driven, multi-vector operations**, prioritising disruption and messaging over destruction or persistence.

The motivational landscape stemming from analysis of incidents demonstrates several key trends:

1. **Convergence of ideology and capability** - hacktivist operations are no longer spontaneous but are increasingly integrated with broader political agendas.
2. **Rising cross-group collaboration** - operational overlaps between known collectives indicate shared targeting frameworks and potentially common command structures.
3. **Geopolitical synchronization** - timing of campaigns corresponds closely with conflict events and diplomatic escalations, highlighting intentional influence operations.
4. **Shift to hybridized warfare** - blending psychological, information, and cyber components, hacktivists are leveraging cyberspace as a strategic battlespace rather than a protest medium.

Belgian Tax Declaration Website Defacement Hacktivism

Industry	Datatype	Region
Government	Attack Methodologies	Europe +1 more

Country	Threat Actor	Motivation
Belgium	BD Anonymous	Ideological

Victim Name
Belgian Tax Declarations Website

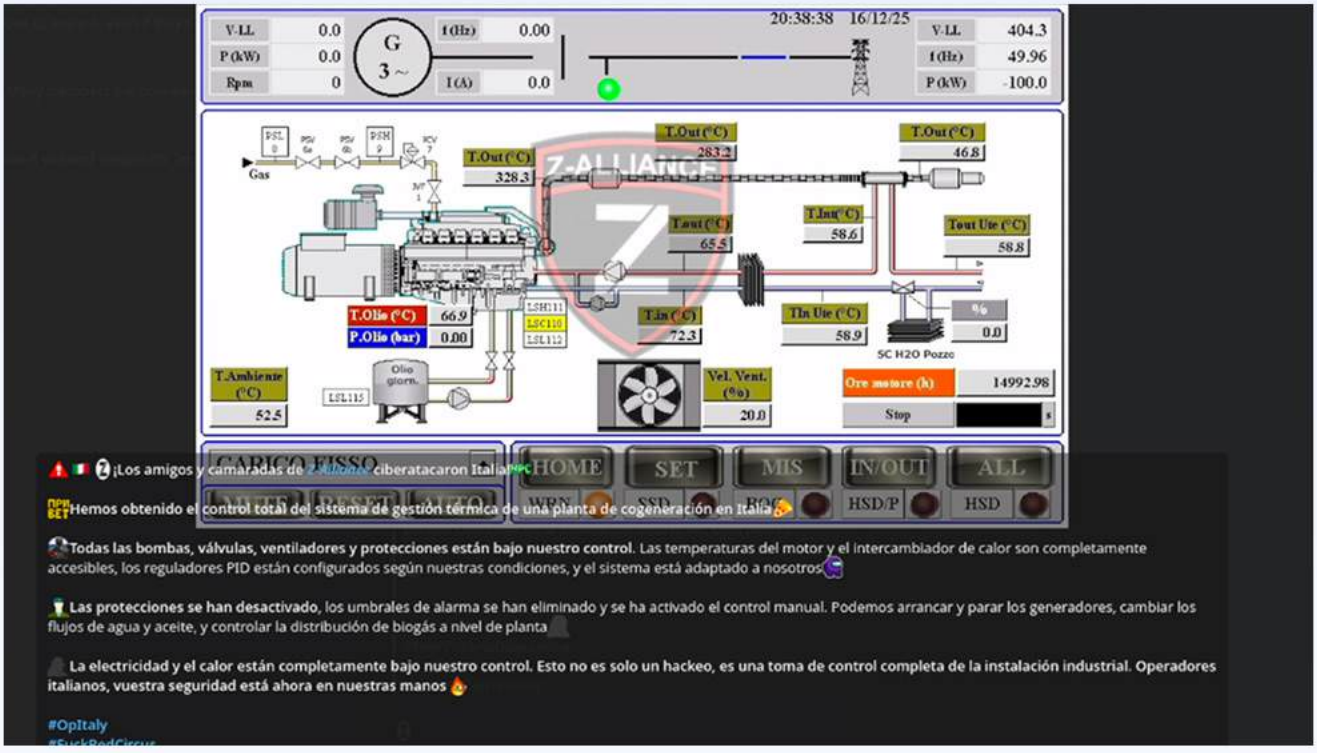
Posted On Source	Posted On CloudSEK
17 Dec, 2025 07:56:25 AM	21 Dec, 2025 04:11:24 AM

Source URL
https://t.me/httpstmemKfsxqmblFkMTlk/1143

Advisory ID: ADV-1945-473264 1 0

Summary
The hacktivist group BD Anonymous claims to have taken down the official website of Belgian tax declarations in response to the Belgian government's support of Zionism. They threaten further actions if the support continues.

Screenshot from CloudSEK's GTI module showing hacktivist Activity by BD Anonymous, upon Belgium's Tax Declaration Portal - via DDOS



Affiliates of Z-Alliance sharing claims of having gained access to an Italian cogenaration plant and it's internal controls

Dominant Hacktivist Group Activity in Timeline

- **KillNet and Affiliates (KillNet, KillNet LATAM)** represents a geopolitically aligned disruption actor, primarily focused on large-scale DDoS campaigns and information operations. Their activity is characterized by persistent targeting of government institutions, financial services, and telecommunications providers, often synchronized with geopolitical or diplomatic developments. While technical sophistication remains moderate, the ecosystem's decentralized affiliate model enables sustained attack volume and rapid mobilization. The primary risk posed by KillNet lies in service disruption and public-facing instability, rather than deep system compromise.

CloudSEK Threat Actor Directory — KillNet Collective Profile Showing Top Targeted Countries and Industries

- **NoName057(16)** operates as a campaign-driven disruption collective, leveraging volunteer-based tooling to conduct repeatable, high-frequency DDoS attacks. Also going by the collective name **DDoSia Project**, their targeting behavior shows a strong emphasis on Western-aligned government and critical infrastructure entities. Operations are tightly coordinated through Telegram tasking and scoring mechanisms, reinforcing participant engagement. The threat profile is centered on availability impact and psychological pressure, with limited evidence of lateral movement or data-centric exploitation.

CloudSEK Threat Actor Directory — NoName057(16) Collective Profile Showing Top Targeted Countries and Industries

- **Handala** represents an ideological actor profile, where operations include political messaging combined with data exposure. Their campaigns show persistent targeting behaviour and are often linked to credential exploitation, phishing-style intrusion, and hybrid extortion tactics. This threat category creates elevated reputational risk because victims are often targeted for symbolic or political reasons, not just financial gain.

CloudSEK Threat Actor Directory — Handala Collective Profile Showing Top Targeted Countries and Industries

- **GhostSec and Anonymous Collectives** - Due to significant operational overlap, shared branding, and decentralized participation, Anonymous and GhostSec activity is assessed collectively as a single ideological hacktivist ecosystem for analytical clarity.

CloudSEK Threat Actor Directory — RipperSec Collective Profile Showing Top Targeted Countries and Industries

They collectively represent a **loosely federated ideological threat ecosystem**, rather than discrete, centralized actors. Operations conducted under these banners typically blend political messaging with disruptive cyber activity, including DDoS attacks, website defacements, and data-exposure claims.

Campaigns are highly **event-driven**, frequently aligning with geopolitical developments, social movements, or conflict-related narratives. Technical sophistication varies widely across cells, with

many operations relying on low-barrier tooling and recycled data rather than novel intrusion capability.

The primary risk posed by this collective stems from **rapid narrative amplification and reputational impact**, as the Anonymous and GhostSec brands enable widespread visibility and media traction even when technical impact is limited. Victims are often selected for **symbolic or political value**, increasing exposure for public-facing organizations and institutions.

- **RipperSec** demonstrates a **hybrid hacktivist–extortion posture**, blending DDoS attacks with data-leak claims and coercive messaging. Campaigns often leverage previously exposed data or low-confidence breach claims to amplify perceived impact. The group's activity introduces **reputational and compliance risk**, particularly where data exposure narratives are used to pressure victims despite limited evidence of deep compromise.

Dominant Hacktivist Tactics, Techniques, and Tooling

Data Leaks & Credential Dumps

Common techniques and tooling observed include:

- Telegram channels for bulk data distribution / amplification. Leaks from forums and ransomware hubs circulate among channels
- Automated scraping tools targeting misconfigured databases, APIs, and cloud storage
- Circulation of Checker scripts and combolists, aiding in **credential stuffing**.

Distributed Denial-of-Service (DDoS)

Dominant techniques and tooling include:

- Usage of low-cost botnets, clubbed with commercial stressers and booter services, lowering **the technical barrier to execution**
- This follows Layer 7 HTTP floods against web applications and CMS-driven sites, leading to temporary operational disruption. Proofs of attacks are documented using third-party website reachability tools and spread, as a means to establish legitimacy.

Distributed Denial-of-Service (DDoS)

Dominant techniques and tooling include:

- Usage of low-cost botnets, clubbed with commercial stressers and booter services, lowering **the technical barrier to execution**
- This follows Layer 7 HTTP floods against web applications and CMS-driven sites, leading to temporary operational disruption. Proofs of attacks are documented using third-party website reachability tools and spread, as a means to establish legitimacy.

Website Defacement

Observed techniques include:

- Exploitation of **unpatched CMS vulnerabilities** (e.g., WordPress, Joomla, Drupal)
- Abuse of **weak or reused administrative credentials**
- **Automated vulnerability scanning tools** used to identify exploitable web assets
- Deployment of **basic webshells** aiding in idealogy based content injection and server compromise.

Line chart depicting the monthly distribution of reported incidents in 202

Industry Impact Analysis

The 2025 hacktivist threat landscape demonstrates a **deliberate concentration of cyber operations on industries with high public visibility, trust dependency, and political or symbolic importance**. Analysis indicates that hacktivist groups consistently prioritize sectors capable of amplifying disruption, public reaction, and narrative impact over those requiring sustained technical compromise.

The **Government & Public Sector (5,640 mentions)** emerged as the most heavily targeted industry in 2025, reflecting attackers' intent to challenge political authority, state legitimacy, and public confidence. This unified category, encompassing government bodies, military institutions, and

public-sector organizations was repeatedly targeted through **DDoS attacks, website defacements, and symbolic data-leak claims**, often synchronized with elections, military escalations, and diplomatic developments.

The Financial Services sector (2,303 mentions) ranked second, underscoring its trust-based operating model and symbolic economic importance. This consolidated category, covering banking, finance, investment, fintech, and insurance, was a frequent focus of **DDoS campaigns and credential-dump operations** aimed at disrupting service availability and undermining confidence in institutional stability, rather than enabling direct financial theft.

The Education sector (1,794 mentions) also remained a consistent target, driven by its extensive online exposure and comparatively low security maturity. Hacktivist activity in this sector primarily involved **defacements and short-duration DDoS attacks**, often leveraged for ideological messaging rather than sustained operational disruption.

Additional frequently targeted industries included **Technology (1,480 mentions)**, **Telecommunications (849 mentions)**, and **Retail & E-Commerce (770 mentions)**, reflecting a continued expansion of hacktivist activity into high-visibility sectors with strong public interaction and symbolic value.

Bar chart depicting the distribution of incidents across different industries, highlighting sectors with higher and lower incident volumes

Conclusion

The global cyber threat landscape in 2025 reflects a highly mature, industrialised, and interconnected adversary ecosystem, where cybercrime, extortion, and strategic targeting increasingly converge. Threat actors now operate within a well-established underground economy that seamlessly links credential theft, access brokerage, data monetisation, and ransomware deployment into a continuous attack pipeline. The dominance of identity-driven compromise - through stolen credentials, infostealer logs, and valid account abuse, highlights a fundamental shift away from purely technical exploitation toward scalable, low-friction intrusion methods.

Dark web activity observed throughout the year underscores the professionalisation of cybercrime. The consolidation of major underground forums, rapid actor migration following law-enforcement disruption, and the central role of initial access brokers demonstrate an ecosystem designed for resilience and efficiency. Stolen access, rather than standalone malware, has become the primary commodity enabling downstream ransomware, fraud, and extortion operations. This access-as-a-service model significantly lowers the barrier to entry for ransomware affiliates and accelerates the speed at which attacks progress from initial compromise to operational impact.

Ransomware activity in 2025 further reinforces this trend. Rather than a small number of dominant groups, the landscape is characterised by fragmentation and rapid scaling, with multiple high-output operators leveraging shared tooling, affiliate networks, and brokered access. High-impact incidents affecting technology providers, critical infrastructure, manufacturing, aviation, and education illustrate how attackers increasingly prioritise targets that maximise downstream disruption and reputational pressure. Supply-chain and third-party compromises have emerged as a defining risk, where a single breach can cascade across thousands of dependent organisations.

Across industries, exposure patterns reveal a consistent focus on sectors that enable scale , such as technology, government, finance, telecom, and cloud-dependent services - reflecting attackers' strategic understanding of digital interdependencies. The continued circulation of PII, credentials, databases, and privileged access listings highlights that cyber risk is no longer confined to individual breaches, but persists as a long-tail threat through credential reuse, access resale, and repeated victimisation.

Looking ahead, the global threat environment is expected to remain persistently high-pressure, driven by the resilience of underground markets, the speed of vulnerability weaponisation, and the growing reliance on shared digital platforms. Organisations must therefore move beyond perimeter-centric security models and adopt intelligence-led, identity-first defence strategies. Continuous attack surface visibility, rapid credential exposure detection, third-party risk management, and disruption of access broker pathways will be critical to reducing real-world impact. As 2026 approaches, cyber threats are no longer episodic events but an ongoing condition - one defined by sustained adversary presence, operational sophistication, and strategic exploitation of trust, identity, and scale.

References

- *Intelligence source and information reliability - Wikipedia
- #Traffic Light Protocol - Wikipedia
- U.S. Takes Action Against PRC-Linked Cyber Actors for Treasury Hack and Salt Typhoon - U.S State Department Press Statement
- The Bybit Hack: Following North Korea's Largest Exploit - TRM Labs
- Bybit Confirms Record-Breaking $1.5 Billion Crypto Heist in Sophisticated Cold Wallet Attack - HackerNews
- Russia's Destructive Wiper Attacks on Ukraine Rise Again - BankInfosecurity
- RomCom Threat Actor Evolution (2023 - 2025) - Picus Security
- CVE-2025-6218: WinRAR vulnerability analysis and mitigation - Wiz
- China-linked group Salt-Typhoon breached Sattelite firm Viasat - Security Affairs
- Investigation Report: APT36 Malware Campaign Using Desktop Entry Files and Google Drive Payload Delivery - CloudSEK
- Anatomy of an Attack : CISA Alert on Salt Typhoon - Extrahop
- AI-Driven Deepfake Military ID Fraud Campaign by Kimsuky APT - Genians Security Center
- North Korean Hackers Weaponize ChatGPT in AI-Driven Phishing Attack - eSecurity Planet
- Archive Terror: Dissecting the WinRAR CVE-2025-6218 Exploit & APT-C-08's Stealth Move - SecPod
- Crypto heist against Upbit linked to private key vulnerability - SCWorld
- China Admitted to Volt Typhoon Cyberattacks on US Critical Infrastructure - SecurityWeek
- Silver Fox Targeting India Using Tax Themed Phishing Lures - CloudSEK
- Reborn in Rust: Muddy Water Evolves Tooling with RustyWater Implant - CloudSEK

CloudSEK

Predict ◆ Protect ◆ Quantify

We **Predict** Cyber Threats **Before They Strike**

Registered Office:

CloudSEK Research Pte. Ltd.
160 Robinson Road, #20-03, Singapore Business Federation Center, Singapore - 068914

Regional Office : India

CloudSEK Information Security Pvt Ltd.
16/1, Cambridge Rd, Halasuru, Cambridge Layout, Jogupalya, Bengaluru, Karnataka - 560008

Regional Office : United States

CloudSEK Inc.
8 The Green, Ste A, Dover, DE - 19901, United States

Regional Office : United Kingdom

CloudSEK, 2 Kingdom Street,
6th Floor London, W2 6BD - United Kingdom

CloudSEK

info@cloudsek.com www.cloudsek.com

Scan for a free Demo of CloudSEK platform