2025

ThreatMon
Under Cyber Wings

MID-YEAR CYBER THREAT REPORT

EXECUTIVE SUMMARY & KEY FINDINGS

The first half of 2025 has witnessed a significant intensification of global cyber threats. According to the IBM X-Force Threat Intelligence Index 2025, 70% of cyberattacks in 2024 exploited known but unpatched vulnerabilities, a trend that has continued into 2025. Valid credentials were the initial attack vector in 30% of all incidents, underlining persistent identity and access management failures.

The WEF Global Cybersecurity Outlook 2025 further warns that a growing "confidence gap" exists between cyber leaders and business executives — with only 31% of business leaders believing their organizations are cyber-resilient, compared to 67% of security leaders. This misalignment has translated into slow incident response and underinvestment, despite clear and present risks.

Meanwhile, ransomware attacks jumped 49%, with over 4,000 leak-site incidents, increasingly enabled by Ransomware-as-a-Service models. Europe emerged as the most attacked region, overtaking North America, with manufacturing, finance, and healthcare topping the list of impacted sectors.

AI-powered automation continues to reshape threat operations, from vulnerability scanning to phishing attacks. Infostealers and dark web credential dumps are accelerating the speed and volume of breaches. Geopolitical cyber operations—especially from Iran, Russia, and North Korea—also saw a notable rise in sophistication and scope.

- ***Ransomware attacks rose by 49%, with 4,198 incidents tracked via leak sites.***

- ***Europe became the top-targeted region globally, making up 32% of all cyberattacks.***

- ***70% of attacks involved known vulnerabilities, emphasizing the ongoing failure in timely patching.***

- ***Valid credentials used in 30% of breaches, often stolen through infostealers and phishing kits.***

- ***Only 31% of business executives believe their organization is cyber-resilient, compared to 67% of security leaders.***

- ***Manufacturing remains the most attacked sector, followed by financial services and healthcare.***

- ***AI-powered attacks accelerating: organizations face automated vulnerability scanning, phishing, and evasion tactics.***

- ***Infostealers surge, serving as primary access points for credential-based attacks.***

- ***Telegram becomes a primary dark web channel for leaking breached data.***

- ***Cyber investment misalignment: security budgets remain low despite growing threats; only 29% of organizations report being "mature" in cyber governance.***

TIMELINE OF INCIDENTS

Significant Cyber Incidents

January

US Treasury Breach

- Attack Type: Cyber-espionage (APT)
- Details: Computers of senior U.S. Treasury officials were accessed via third-party compromise.
- Actors: China-linked “Flax Typhoon” group

Frederick Health Ransomware Attack

- Attack Type: Ransomware
- Details: Affected ~934,000 patient records, including sensitive health data.
- Actors: Likely part of coordinated healthcare-sector campaign

February

Genea IVF Clinic Breach (Australia)

- Attack Type: Ransomware
- Details: Termite ransomware group exfiltrated 940GB of sensitive medical data.
- Impact: Legal intervention halted data publication; national media attention.

Volt Typhoon Targeting Guam Infrastructure

- Attack Type: State-sponsored infiltration
- Details: Critical telecom and power infrastructure in Guam targeted for potential wartime disruption.
- Impact: U.S. military preparedness review triggered.

From the corridors of government to hospital networks and global supply chains, the first seven months of 2025 have revealed the expanding scope, scale, and sophistication of cyber threats. Ransomware groups, state-sponsored actors, and criminal collectives alike have escalated their operations — often targeting critical infrastructure, healthcare providers, and multinational brands with increasing precision. This timeline captures two high-impact incidents per month that shaped the global cybersecurity narrative, reflecting how vulnerabilities in one region can reverberate worldwide.

Significant Cyber Incidents

March

Oracle Healthcare Breach

- Attack Type: Data breach
- Details: Patient-related records in Oracle Health environment accessed.
- Impact: FBI opened a probe due to potential exposure across hospital systems.

Zoomcar (India) Credential Theft & Exposure

- Attack Type: Credential stuffing
- Details: PII of Indian mobility-tech startup Zoomcar leaked on Telegram.
- Impact: Customer trust eroded; signals spread of retail/mobile targeting.

April

Iberian Peninsula Power Outage (Spain & Portugal)

- Attack Type: Initially suspected cyberattack
- Details: Affects energy, telecom, and transit sectors; ruled out as cyber but spotlighted resilience gaps.
- Impact: Raised cybersecurity preparedness discussions in EU.

Harrods, M&S, Co-op Ransomware Campaign (UK)

- Attack Type: Ransomware
- Actors: Scattered Spider, DragonForce
- Impact: M&S online presence disabled for 7 weeks; suspects arrested in July.

May

City of Dallas – Government Ransomware

- Attack Type: Ransomware
- Details: Operational disruptions to police, court, and citizen service systems.
- Impact: Public safety delayed, sensitive documents leaked.

DaVita Dialysis Data Leak (USA)

- Attack Type: Data exfiltration
- Details: Medical records exposed from U.S. dialysis network.
- Impact: Undermined trust in U.S. healthcare infrastructure resilience.

June

JBS Meatpacking Ransomware (USA/Australia)

- Attack Type: Ransomware
- Details: Shut down meat processing in multiple countries for two days.
- Impact: Supply chain disruption with global food sector implications.

Lee Enterprises Ransomware (USA)

- Attack Type: Ransomware
- Details: 40,000 SSNs and financial records stolen by Qilin group.
- Impact: Journalistic operations and publishing systems halted.

January 2025

In early January, the U.S. Department of the Treasury fell victim to a sophisticated cyber-espionage campaign linked to the Chinese APT group known as Flax Typhoon. The breach was traced to a vulnerability in a third-party platform, BeyondTrust, which provided a backdoor into the email systems of senior Treasury officials. While the technical intrusion was quickly detected and contained, the incident sparked significant geopolitical fallout. The U.S. government responded with sanctions against Beijing-based Integrity Technology Group, underscoring the growing risk posed by vendor-based access points and the strategic targeting of federal institutions by nation-state actors.

Later in the month, Frederick Health, a regional hospital network in Maryland, disclosed a major ransomware attack that compromised the sensitive data of approximately 934,000 patients. The breach included protected health information, social security numbers, and detailed clinical records. Although the identity of the ransomware group behind the attack remains unconfirmed, it is widely suspected to be part of a broader campaign affecting U.S. healthcare systems. The attack forced the network to revert to manual systems temporarily, raising alarms about the fragility of healthcare infrastructure in the face of increasingly targeted ransomware threats.

February 2025

In February, the Australian healthcare sector faced a devastating blow when Genea, a major fertility clinic network, was targeted by the ransomware group Termite. The attackers claimed to have exfiltrated nearly 940 GB of highly sensitive medical data, including reproductive health records, patient identities, and internal communications.

The situation escalated quickly, prompting the New South Wales Supreme Court to issue an injunction preventing the public release of the stolen data. While the court order helped contain reputational damage, the incident raised serious concerns about the preparedness of private healthcare providers to handle complex extortion threats and the ethical stakes of cyberattacks on reproductive care services.

Around the same time, cybersecurity authorities in the U.S. disclosed alarming details about an ongoing state-sponsored campaign targeting Guam's critical infrastructure, attributed to the Volt Typhoon APT group linked to China. The campaign, which had begun months earlier but intensified in early 2025, focused on infiltrating telecom networks, power grids, and transportation systems on the island — a key hub for U.S. military operations in the Pacific. The attack was widely interpreted as part of a broader geopolitical strategy to develop pre-positioned access for potential conflict scenarios, drawing renewed attention to the cyber vulnerabilities of essential civilian infrastructure in geopolitically sensitive regions.

March 2025

In March, U.S. federal authorities launched an investigation into a breach of Oracle's cloud-based healthcare systems, raising alarms across the medical technology sector. The breach reportedly exposed patient records and healthcare analytics data from several provider networks relying on Oracle's infrastructure. Though the full scale of the data loss remains undisclosed, the FBI's involvement signaled its potential severity. The incident underscored the growing risks tied to centralized data environments and the systemic impact of supply-chain vulnerabilities when core infrastructure providers are compromised.

Meanwhile, in India, mobility-tech startup Zoomcar experienced a data breach that resulted in the leak of user information on Telegram channels frequented by cybercriminals. The attack leveraged credential-stuffing tactics and targeted account-level access, exposing email addresses, phone numbers, and trip histories. While Zoomcar downplayed the scope of the breach, ThreatMon's monitoring indicated rising dark web chatter around the data, suggesting increased threat actor interest in automotive and mobility platforms. The breach highlighted how customer-centric digital platforms remain prime targets for mid-level cybercrime groups exploiting weak authentication practices.

April 2025

April began with disruption across the Iberian Peninsula, where a massive power outage affected millions of residents in Spain and Portugal. Initially feared to be the result of a coordinated cyberattack, the incident triggered emergency responses and cybersecurity investigations across EU agencies. While authorities later attributed the blackout to a critical infrastructure failure rather than direct malicious interference, the event underscored Europe's fragility in responding to systemic disruptions — whether cyber-induced or not. It also reinforced the urgency of bolstering cyber-resilience in the energy and transit sectors, especially amid heightened geopolitical tensions.

Later in the month, a coordinated ransomware campaign struck some of the UK's most recognizable retail brands — Marks & Spencer, Harrods, and Co-op — in what would become one of the most high-profile attacks of the year. Carried out by affiliates of the Scattered Spider and DragonForce groups, the attack took down online storefronts, disrupted inventory systems, and exposed sensitive customer data. Marks & Spencer's website remained offline for nearly seven weeks. UK police arrested multiple suspects by July, but the incident revealed how sophisticated ransomware actors increasingly target legacy systems in retail giants, causing financial, reputational, and operational fallout across entire consumer ecosystems.

May 2025

In May, the City of Dallas became the latest high-profile victim of a ransomware attack that crippled essential public services. The attackers, linked to the RansomHub group, disrupted police communications, court operations, and municipal service portals, effectively paralyzing key city functions for several days. Sensitive law enforcement documents were exfiltrated and later leaked on dark web forums. This attack not only disrupted daily life for millions of residents but also reignited debates around cyber-readiness in local governments, many of which continue to rely on outdated IT systems and lack robust incident response protocols.

Also in May, DaVita, one of the largest dialysis providers in the United States, reported a significant breach involving the unauthorized access and potential exfiltration of patient health information. Though the company offered limited public detail, security analysts observed related datasets circulating across dark web marketplaces in the weeks following the disclosure. Given the company's vast network of care centers and the critical nature of its services, the breach raised questions about the cybersecurity posture of essential healthcare providers and the growing risks tied to electronic medical record systems across the U.S. health sector.

June 2025

June opened with a large-scale ransomware attack on JBS, one of the world's largest meat processing companies, affecting operations across the United States and Australia. Facilities were forced to halt production for two consecutive days, disrupting meat supply chains and triggering price volatility across retail markets. Although JBS did not publicly confirm the ransom demand or payment, the incident reflected the persistent vulnerability of critical food infrastructure to targeted extortion efforts. It also echoed the company's 2021 ransomware episode, raising concerns about recurring weaknesses in industrial cybersecurity across global logistics networks.

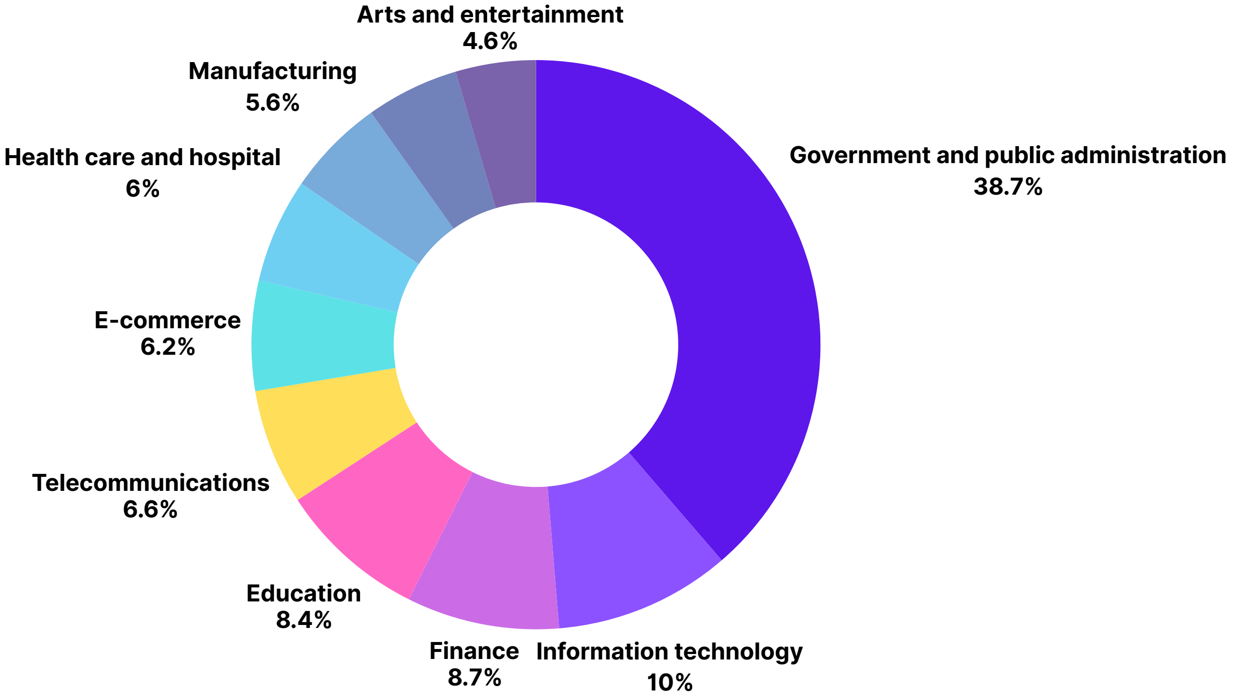
Later in the month, Lee Enterprises, a major U.S. media and publishing conglomerate, was targeted by the Qilin ransomware group. The attackers exfiltrated and published over 40,000 social security numbers, employee records, and internal HR files, disrupting newsroom operations and digital publishing systems in over two dozen local markets. The attack not only impacted business continuity but also threatened the privacy of journalists and staff. It served as a stark reminder that even organizations outside the traditional “critical infrastructure” designation are increasingly in the crosshairs of highly capable ransomware-as-a-service operators.

June 2025

In early July, Qantas, Australia’s flagship airline, confirmed a significant customer data breach affecting up to 6 million individuals. The breach originated from a compromise in a third-party loyalty program provider, allowing attackers to access passenger profiles, travel histories, and frequent flyer credentials. While financial data remained uncompromised, the exposure of personally identifiable information raised serious privacy concerns. The breach was widely attributed to affiliates of the Scattered Spider group, marking yet another example of attackers exploiting supply chain weaknesses to target national-scale consumer platforms.

In parallel, a wave of credential-stuffing attacks struck major consumer-facing brands, including The North Face and Optima Tax Relief. By reusing credentials leaked from prior data breaches, cybercriminals gained unauthorized access to thousands of customer accounts, some of which were later advertised on Telegram and dark web forums. The attacks triggered password reset campaigns and forced both companies to enhance multi-factor authentication protocols. These incidents reinforced a persistent challenge in the cybersecurity landscape: the long tail of weak password hygiene and the ease with which threat actors weaponize reused credentials at scale.

DARK WEB INSIGHTS



The first half of 2025 has seen a steep intensification in dark web activity, marked by the evolution of threat actor coordination, expansion of Telegram as an operational hub, and growing sector-specific targeting. Our analysis of over 9,000 incidents tracked across marketplaces, ransomware sites, and Telegram-based ecosystems reveals an increasingly professionalized cybercrime landscape — one that is no longer confined to traditional dark web forums but thrives in real-time, accessible platforms.

A clear trend this year has been the disproportionate targeting of public institutions. As seen in the chart above, government and public administration sectors alone accounted for nearly 39% of tracked incidents, followed by information technology (10%), finance (8.7%), and education (8.4%). This prioritization of public-facing, high-data-value systems aligns with a broader strategic shift among threat actors who now seek maximum disruption and visibility over pure financial gain.

Emerging and existing threat actors — including NoName057(16), Qilin, Dark Storm Team, and Arabian Ghosts — played a significant role in shaping this ecosystem. These groups operate in complex environments where ransomware and hacktivism often blur, merging ideological motives with financial models. In parallel, dark web vendors and info-stealer operators such as those distributing Lumma and Raccoon Stealer logs have created an easily accessible entry point for low-skill actors to wreak corporate-level damage.

From a geographical lens, Israel, India, and the U.S. remain top targets and sources of chatter. Meanwhile, rising volumes of cyber incidents targeting or originating from Indonesia, Turkey, and Morocco point to the decentralization of cybercrime operations, with new players entering the stage and often participating in ransomware-as-a-service (RaaS) campaigns, defacements, or political hacktivism.

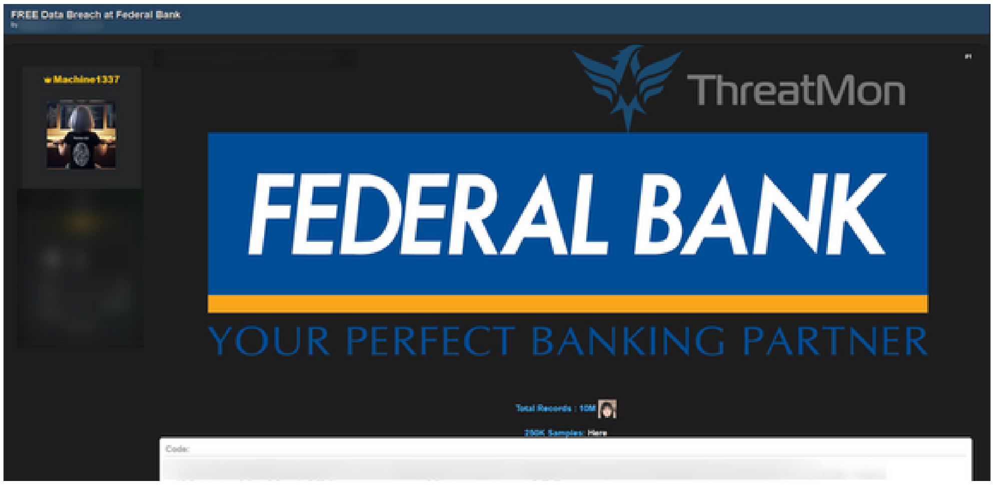
Looking ahead to the second half of 2025, we anticipate three key shifts:

1. Increased targeting of Tier-2 markets — especially in MENA and Southeast Asia — as cybercrime operators diversify their attack surface to evade saturated defenses in the West.
2. Refinement of Telegram-based market operations, with threat actors offering bundled services (e.g., phishing kit + email list + log parsing bot) under monthly subscription models.
3. Elevated ransomware public relations tactics, including real-time leaks, interactive extortion bots, and AI-generated fake “victim” messages to amplify pressure campaigns.

In response, organizations must think beyond perimeter defense. Proactive threat intelligence — especially dark web monitoring — has become non-negotiable. ThreatMon continues to infiltrate closed channels, decode actor patterns, and issue early-warning alerts to help organizations move from reactive defense to anticipatory resilience.

Dark Web Exposures:
A Glimpse into Some Alarming Breaches of 2025

Federal Bank (India) – Alleged Dark Web Data Breach



FREE Data Breach at Federal Bank

Machine1337

Total Records : 10M

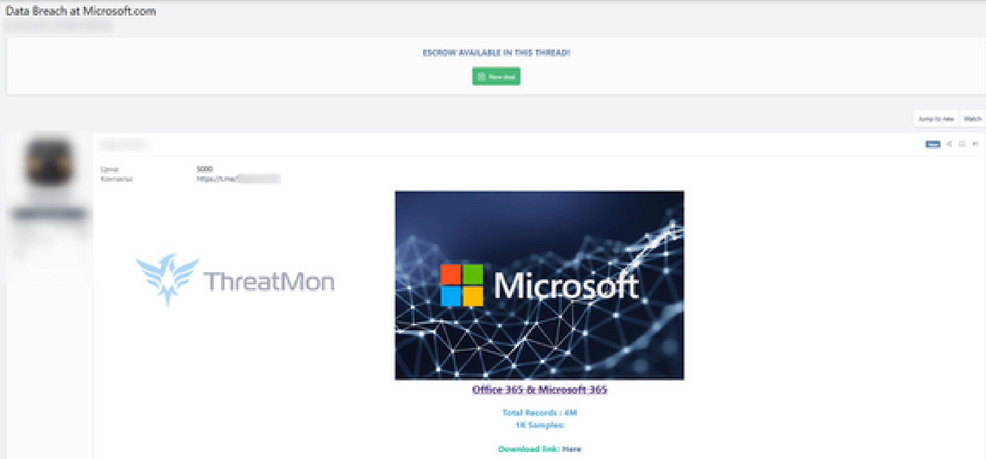
250K Samples: Here

Code:

In one of the most notable dark web exposures of early 2025, a user going by the alias Machine1337 posted a thread on a well-trafficked underground forum claiming access to sensitive data from The Federal Bank Limited, one of India's most prominent banking institutions. The actor alleges the leak includes over 10 million records, offering 250,000 as a sample, and suggests the breach originated from internal banking SMS communication systems. The exposed data reportedly includes fields such as clientaccountname, messageId, destinationaddress, submissiontime, statusreason, and raw message content — raising severe concerns about customer privacy and possible regulatory violations under Indian financial data laws. Although no ransomware demand was attached, the free release of such a large dataset indicates a desire for notoriety or disruption rather than financial gain, aligning with patterns observed in hacktivist-linked breaches earlier this year.

Dark Web Exposures:
A Glimpse into Some Alarming Breaches of 2025

Microsoft 365 – Database Sale on the Dark Web



Data Breach at Microsoft.com

ESCROW AVAILABLE IN THIS THREAD!

Цена: 5000
Контакты: https://t.me/[redacted]

Office 365 & Microsoft 365

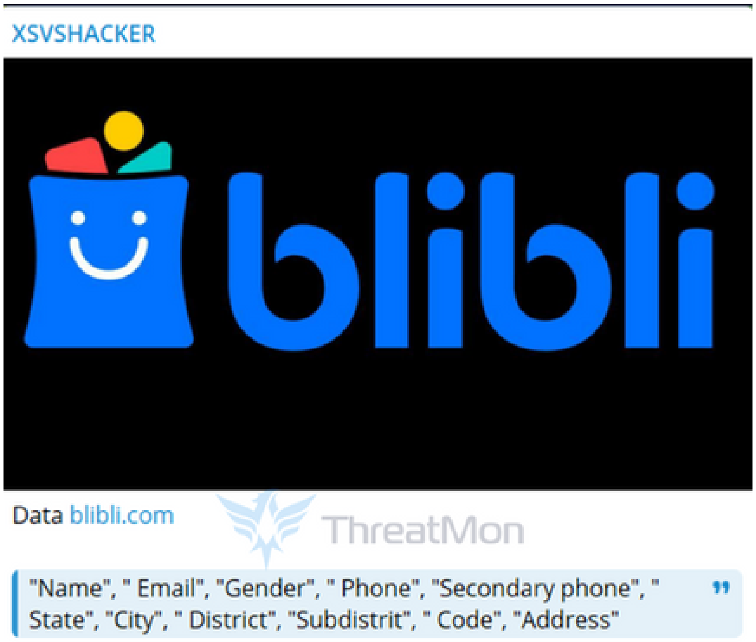
Total Records : 4M
1K Samples:

Download link: Here

A threat actor recently listed a 4-million-record dataset allegedly linked to Microsoft's Office 365 and Microsoft 365 services for sale on a known dark web marketplace. Priced at $5,000, the database was advertised with professional-level formatting, escrow options, and limited-time download links, suggesting the involvement of an experienced and organized threat group. The post lacks specific exploit details but claims to contain usernames, account metadata, and credential fragments. While Microsoft has not confirmed any related compromise, this mirrors a trend seen across 2025 where attackers increasingly bundle business software credential leaks for resale — creating risks for corporate espionage, supply chain intrusion, and targeted phishing at scale. This also highlights the vulnerability of SaaS-based enterprise environments, which remain high-value targets for data brokers and ransomware affiliates alike.

Dark Web Exposures:
A Glimpse into Some Alarming Breaches of 2025

Blibli (Indonesia) – Customer PII Dump by XSVSHACKER

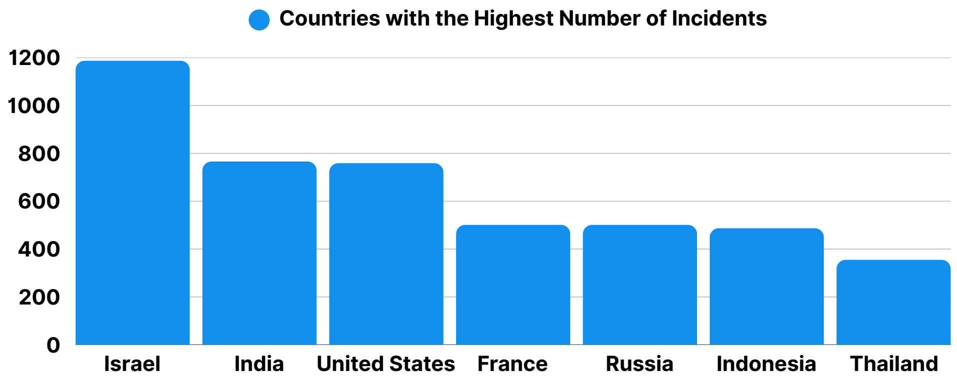

XSVSHACKER

Data blibli.com

"Name", " Email", "Gender", " Phone", "Secondary phone", " State", "City", " District", "Subdistrit", " Code", "Address"

The Indonesian e-commerce giant Blibli became the subject of an alleged data breach when the actor XSVSHACKER shared a sample dataset on Telegram and dark web forums. The dump is claimed to include highly sensitive personally identifiable information (PII) such as full names, gender, email, mobile and secondary phone numbers, as well as complete addresses down to district and subdistrict levels. Although the scale of the breach remains unverified, the structure of the leaked data aligns with customer onboarding information, indicating a likely database-level intrusion. With Indonesia emerging as a top-10 geography in cyber incident targeting, this attack underscores the country's growing digital surface area — and the challenges of securing fast-scaling consumer tech platforms. Moreover, the breach could carry consequences for both national privacy enforcement and customer trust in local e-commerce ecosystems.

Countries with the Highest Number of Incidents



In the first half of 2025, dark web activity has revealed clear geographic concentrations, with certain countries facing a disproportionate share of underground targeting, data leaks, and chatter. According to ThreatMon's monitoring of high-traffic dark web channels and actor groups, Israel stands out with the highest number of associated incidents — accounting for 16.5% of all activity tracked among the top 20 countries. This spike likely reflects the broader geopolitical context and persistent hacktivist operations targeting the region, particularly those tied to state-linked campaigns and ideological actors.

India and the United States follow closely, each representing just over 10% of total tracked activity. In India's case, the surge is fueled by increasing attacks on the financial sector, such as the recent Federal Bank breach, and by the nation's growing digital infrastructure footprint. The U.S., a perennial target for cybercrime due to its global enterprise ecosystem, continues to face steady exposure — with corporate credential leaks, Microsoft 365 database sales, and ransomware posts frequently emerging in underground forums.

France, Russia, and Indonesia each hold a notable share of dark web mentions, ranging from 6.8% to 7%, showing the globally distributed nature of threat actor activity. Indonesia's inclusion reflects rising breaches in the consumer tech space, including the widely publicized Blibli e-commerce data leak, while Russia's presence reflects both external targeting and internal actor operations. Thailand, with nearly 5% of mentions, rounds out the top seven — a reminder that Southeast Asia's digital rise brings corresponding cyber exposure.

This distribution is not only a reflection of attack volume but also a window into what threat actors value: data-rich sectors, politically symbolic targets, and infrastructure with exploitable vulnerabilities. As the second half of the year unfolds, regional tensions, elections, and global events may shift this ranking, but the early signals are clear — cybercriminal activity is increasingly strategic, globally diverse, and ideologically varied.

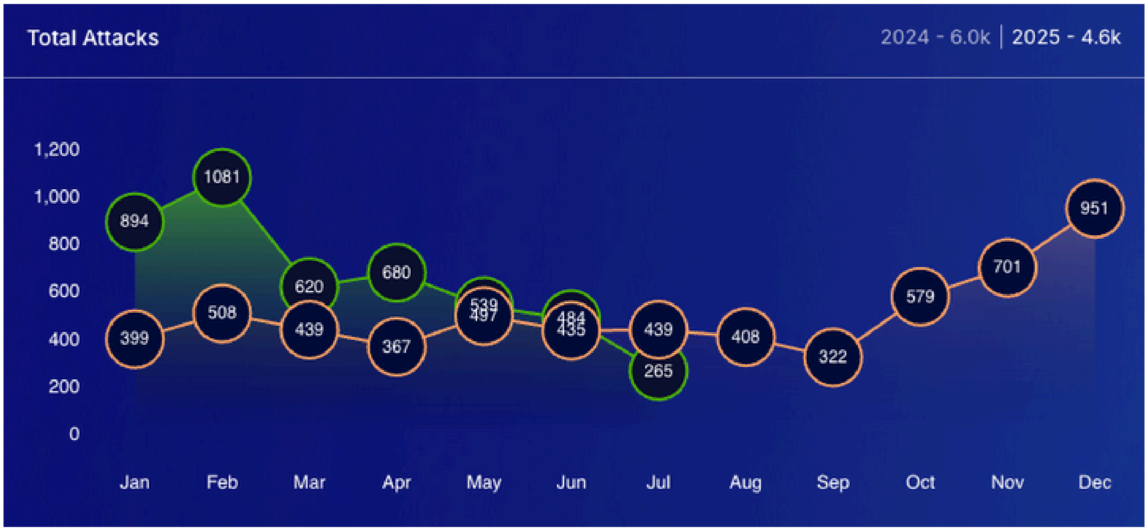
Top Threat Actors in 2025:

As we reached the midpoint of 2025, several prominent threat actor groups have remained consistently active across the dark web and underground forums. Their activities range from targeted ransomware operations to politically motivated hacktivism and commercial data sales. These groups are not only geographically diverse, but also technologically sophisticated—often collaborating across borders, adopting multi-vector attack strategies, and regularly shifting their infrastructure to avoid detection.

At the top of the list is **NoName057(16)**, responsible for an extraordinary number of operations (682 reported instances), largely associated with politically charged campaigns, often targeting critical infrastructure across Eastern Europe. Close behind, groups such as **Dark Storm Team** (273) and **Keymous+** (266) have ramped up ransomware campaigns, targeting enterprise systems globally. **Mr Hamza** (231) and **TEAM FEARLESS** (169) have also been actively involved in data leaks and financial sector breaches.

Meanwhile, **WOLF CYBER ARMY** (128) and **Market Exchange** (122) have gained prominence for orchestrating large-scale credential dumps and malware-as-a-service offerings. Threat actors like **Akira** (82), previously linked to ransomware campaigns against mid-size enterprises, and **Mysterious Team Bangladesh** (77), known for ideological attacks and web defacements, continue to pose regional and sector-specific risks.

RANSOMWARE INCIDENTS



This year's threat landscape shows a dynamic shift in cyberattack patterns, as visualized in the chart above. The green line represents 2025, while the orange line reflects the same months in 2024, offering a side-by-side comparison of total attacks reported across both years. While January and February 2025 witnessed a sharp surge in cyberattacks — peaking at over 1,000 incidents in February — the numbers gradually declined throughout the spring and reached their lowest in July. In contrast, 2024 experienced a more consistent attack frequency across the year, with notable spikes toward the end.

Despite 2025 showing a lower total attack count at the midpoint (4.6k vs. 6.0k in 2024), the early months paint a picture of intensifying campaigns, possibly driven by geopolitical motivations and the rise of new threat actors. The drop-off post-February suggests either enhanced mitigation efforts or a strategic pause by some actor groups. As we move into the second half of 2025, the question remains: will we see a resurgence similar to the late-year climb observed in 2024? The evolving tactics of ransomware groups, hacktivist collectives, and data brokers will play a decisive role in shaping that trajectory.

Ransomware Incidents: A Strategic Shift in Targeting

Ransomware attacks in 2025 have followed a volatile trajectory, with a dramatic spike in Q1 followed by a steady decline through mid-year. This diverges from 2024’s more gradual pace, where monthly attacks built up toward a high-volume Q4. The data suggests that threat actors in 2025 may have front-loaded their campaigns, either due to opportunistic geopolitical tensions or in anticipation of counteractive cyber-defense strategies. February 2025 saw the highest attack volume with over 1,080 incidents, making it the most aggressive month so far this year.

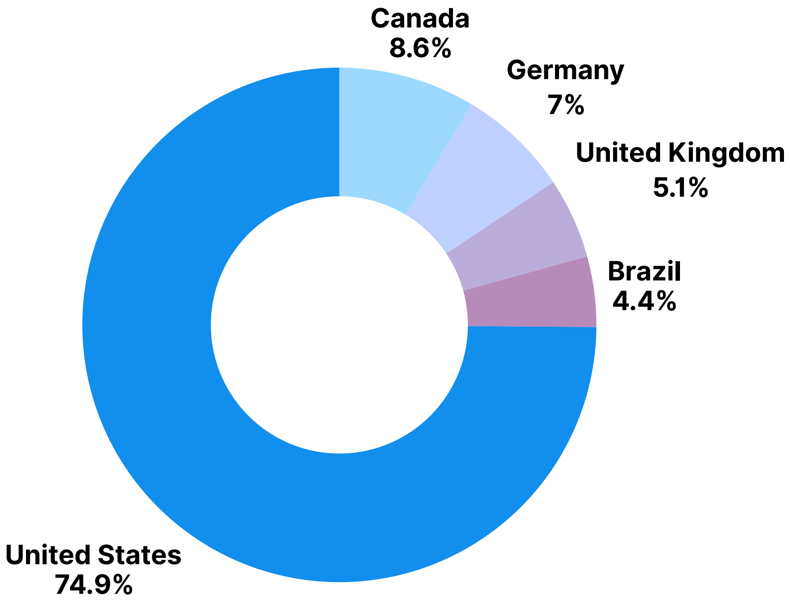
What stands out is not just the volume, but who and what sectors were targeted. Government and public institutions remained the most attacked vertical, accounting for over 30% of all dark web incidents, followed by the IT sector, finance, and education. The healthcare industry, while slightly less targeted than others, still saw a significant number of breaches — underscoring its continued vulnerability despite increased investment in cyber hygiene.

Ransomware remains the most financially damaging tool among cybercriminals, responsible for 1,047 dark web incidents reported so far. Many of these attacks were tied to high-profile actors such as Qilin, Akira, and Team Fearless, whose tactics now increasingly involve double extortion: stealing data and encrypting systems, then threatening public exposure unless a ransom is paid. This shift has blurred the lines between data breaches and ransomware, creating a hybrid threat model that multiplies reputational and financial risks for targeted entities.

The majority of ransomware-related activity was concentrated in countries with dense digital infrastructure. The United States, India, and France saw disproportionately high targeting, with threat actors exploiting regional infrastructure gaps and, in some cases, political motivations. Nation-state-aligned groups and hacktivist collectives, including NoName057(16) and WOLF CYBER ARMY, played a significant role in ramping up ransomware activity with ideological objectives in mind.

Looking ahead, the latter half of 2025 is likely to witness tactical evolution over sheer volume. With cybersecurity teams hardening defenses, ransomware groups may pivot toward supply chain vulnerabilities and software exploits (as seen in several CVE disclosures across forums), aiming for maximum lateral spread with minimal exposure. Organizations, especially those in critical infrastructure and financial services, must prioritize proactive threat intelligence and simulated response drills to mitigate the risks ahead.

Global Distribution of Ransomware Attacks in 2025 (YTD)



The ransomware landscape in 2025 has been heavily concentrated in a few key regions, with the United States alone accounting for over 69% of all recorded incidents. This dominant share reflects both the country's high digital footprint and its attractiveness as a target for financially motivated actors. Canada and Germany follow with more modest shares, while other major economies like the United Kingdom and Brazil also report notable activity. The data reinforces how ransomware operations remain sharply focused on countries with robust enterprise and public-sector infrastructures, making preparedness and cross-border coordination more critical than ever.

Top Ransomware Groups in 2025

RansomHub – From Dominance to Disappearance

RansomHub began 2025 as one of the most aggressive ransomware collectives, quickly overtaking many of its peers. Capitalizing on a well-coordinated structure and incorporating former LockBit affiliates, the group executed hundreds of attacks globally during Q1. However, by April, the group vanished from dark web forums, sparking speculation that it may have faced disruptions or internal collapse possibly linked to ties with other high-profile threat networks like Evil Corp. Its sudden disappearance leaves a power vacuum that other groups have swiftly moved to fill.

RansomHub – From Dominance to Disappearance

Akira has sustained high levels of activity in the first half of 2025, launching widespread campaigns that affected both public and private sector entities. Its strategy involves leveraging stolen credentials and known vulnerabilities to gain access to networks before deploying ransomware payloads. With nearly 350 documented victims this year, Akira remains a persistent threat and has become increasingly sophisticated in its use of social engineering tactics.

Qilin – The Q2 Front-Runner

Emerging as the most active group in Q2, Qilin executed over 300 attacks in the first half of 2025, with a significant portion occurring in healthcare and municipal sectors. The group’s hallmark is the use of its “Agenda” ransomware variant, coupled with aggressive extortion tactics. Notably, Qilin was linked to major disruptions in the UK’s National Health Service, signaling its willingness to target critical infrastructure.

Top Ransomware Groups in 2025

SafePay – The Newcomer Making Waves

SafePay is a relatively new player that has quickly climbed the ranks. Despite surfacing only in early 2025, it managed to carry out over 200 known attacks by mid-year. Its rise can be attributed to a streamlined affiliate program and a wide array of targeted industries. SafePay's approach reflects a new generation of ransomware groups that blend technical capability with organizational agility.

Play – Quiet but Dangerous

Though not as publicly visible as some peers, Play has maintained a consistent level of activity throughout 2025. A major point of concern is the group's exploitation of a Windows zero-day vulnerability (CVE-2025-29824), allowing it to gain elevated privileges undetected. Play's operations demonstrate that even lower-profile actors can cause severe damage when leveraging advanced tactics and persistent vulnerabilities.

Clop – Continuing Its High-Impact Campaigns

Clop has long been known for its large-scale data breach operations, and 2025 is no exception. The group continues to orchestrate double-extortion campaigns, stealing data before encrypting systems. Notable for its previous MOVEit exploit campaign, Clop remains active with hundreds of new victims in various sectors, particularly finance and logistics.

Emerging Actors and Tactical Shifts

Ghost

Flagged by U.S. federal agencies, Ghost has gained momentum in 2025 by exploiting unpatched software vulnerabilities. The group targets hospitals, government bodies, and universities—relying on stealthy infiltration and minimal dwell time before executing encryption.

DragonForce

DragonForce has drawn attention not only for its ransomware campaigns but also for its feud with rival group RansomHub. This internal conflict in the cybercriminal ecosystem could lead to overlapping attacks on the same targets, raising risks for organizations caught in the crossfire.

Scattered Spider

Known for its audacity, Scattered Spider focuses on large corporations and tech firms. The group often bypasses security through SIM-swapping and impersonation of internal help desks, demonstrating the increasing blend of cyber and social engineering.

Vice Society

This group continues to target vulnerable institutions in education and healthcare, where defenses are typically weaker. Vice Society's hallmark is a double-extortion model that pressures victims with both data encryption and public leaks.

Strategic Takeaways

The ransomware landscape in 2025 is increasingly characterized by agility, specialization, and collaboration among cybercriminals. Ransomware-as-a-Service (RaaS) remains a dominant model, lowering barriers for new entrants like SafePay. Meanwhile, the use of zero-day exploits by groups like Play and Ghost underscores a shift toward more technically advanced campaigns. The disappearance of RansomHub and the rise of turf wars, such as the one between DragonForce and other actors, also signal growing instability and unpredictability in the underground ecosystem.

DATA BREACHES

From healthcare systems and consumer platforms to global tech giants, 2025 has already been a turbulent year for data privacy. Massive breaches have affected millions worldwide — not just due to sophisticated attacks but often stemming from weak configurations, overlooked credentials, and third-party vulnerabilities. ThreatMon's cyber intelligence data highlights both high-profile incidents and long-tail breaches affecting a wide range of sectors.

Compromised Records

14.986.167.586

Organization	Pwned Accounts	Breach Date	Data Types Included
Operation Endgame 2.0	15,436,844	May 22, 2025	Emails, Passwords
ALIEN TXTBASE Stealer Logs	284,132,969	Feb 14, 2025	Emails, Passwords
Stealer Logs Jan 2025	71,039,833	Jan 12, 2025	Emails, Passwords
Thermomix Recipe World (Germany)	3,123,439	Jan 29, 2025	Personal data including BIOS and addresses
Scholastic (US)	4,247,768	Jan 7, 2025	Emails, names, physical addresses, phone numbers
Orange Romania	556,557	Feb 23, 2025	Emails, phone numbers, partial credit card data
Ualabee (Argentina)	472,296	May 22, 2025	Profile data and personal identifiers

Selected 2025 Data Breach Highlights

Yale New Haven Health System (April 11)

One of the largest U.S. healthcare systems disclosed a data breach potentially impacting 5.6 million patients. The compromised information is believed to include medical records, insurance details, and personal identifiers — underscoring the growing vulnerabilities in large-scale hospital IT networks.

Scholastic (January 7)

The U.S.-based education publishing giant revealed that over 4.2 million user records were exposed. The breach included names, phone numbers, addresses, and other sensitive details. Scholastic later confirmed that the incident originated from a third-party vendor vulnerability.

Adidas (May 23)

A breach at a third-party customer service provider allowed hackers to gain access to customer contact data. While no financial or password information was exposed, the incident highlighted persistent risks in outsourced systems.

McDonald's AI Chatbot Leak (July 14)

In July 2025, McDonald's faced major scrutiny after its AI chatbot "Olivia," used for screening job candidates, was found to have exposed over 64 million records. The cause? A critical security oversight where the admin account retained the default password "123456." This led to chat logs — containing personal information of years of applicants — being accessible to outside actors. The vendor, Paradox.ai, responded quickly with fixes and introduced a bug bounty program, but the incident served as a cautionary tale about lax default settings in third-party AI deployments.

Conclusion: An Expanding Threat Landscape

So far in 2025, data breaches have been driven by a mix of careless misconfigurations, third-party service vulnerabilities, and large-scale credential-stealing malware. Notably, healthcare, education, and telecom sectors remain the hardest hit. As AI-powered systems proliferate, attackers are increasingly targeting weakly secured automation tools and data-rich backends. The sheer scale and frequency of breaches suggest that organizations must move beyond reactive cybersecurity and adopt proactive threat intelligence, better vendor vetting, and stricter access controls to stay ahead of evolving risks.

CRITICAL VULNERABILITIES

The cybersecurity landscape in 2025 has been marked by a surge in highly critical vulnerabilities that cut across hardware, firmware, cloud infrastructure, web applications, and AI systems. These aren't just theoretical risks—several have been actively exploited in the wild, targeting everything from consumer-grade devices to enterprise infrastructure and government systems. What makes this year particularly alarming is the convergence of two troubling trends: a deeper integration of insecure systems (like AI containers and embedded firmware) and a higher pace of zero-day discoveries and weaponizations. As threat actors evolve and detection windows shrink, patching critical vulnerabilities swiftly is now a foundational component of cyber resilience for organizations of all sizes. Below is a curated list of the most dangerous vulnerabilities revealed in 2025 so far.

Featured Critical Vulnerabilities (Jan–July 2025)

UEFI Firmware Backdoors in Gigabyte Motherboards

CVE-2025-7026 through 7029

Security researchers uncovered four high-severity flaws in Gigabyte motherboard firmware that expose the system to persistent firmware-level attacks. Exploited via System Management Mode (SMM), these bugs allow attackers to bypass Secure Boot and install stealth malware that survives reboots or reinstalls. Affected systems include numerous consumer and enterprise devices. Given the difficulty in detecting and removing such implants, BIOS updates have been issued and are strongly recommended.

Featured Critical Vulnerabilities (Jan–July 2025)

CitrixBleed 2 – Citrix NetScaler ADC/Gateway

CVE-2025-5777

A follow-up to the infamous 2023 CitrixBleed vulnerability, this 2025 variant allows attackers to extract sensitive data from memory through a buffer over-read vulnerability. Exploitation doesn't require authentication, and several organizations have already reported compromises via this bug. Due to its ease of exploitation and widespread use of Citrix appliances in critical sectors, CISA issued an emergency directive requiring immediate patching.

NVIDIAScape – AI Container Escape

CVE-2025-23266

A severe vulnerability in the NVIDIA Container Toolkit has raised concerns within the AI community. The bug enables privilege escalation and allows an attacker inside a container to break isolation and gain root access on the host. With NVIDIA's tools underpinning many ML workloads, especially in cloud-hosted AI services, this vulnerability poses a systemic risk to the AI development and deployment pipeline.

Featured Critical Vulnerabilities (Jan–July 2025)

Chrome Zero-Day Sandbox Escape

CVE-2025-6558

Google patched a zero-day exploit in its Chrome browser that targeted the ANGLE graphics engine. The vulnerability allows attackers to escape the browser sandbox and execute code on the underlying OS. The flaw was observed being exploited in the wild, which prompted Google to fast-track a stable release update. All users have been urged to update their browsers immediately.

VMware ESXi Hypervisor Escape

CVEs: 2025-41236 through 41239

VMware issued a critical advisory in mid-2025 after researchers demonstrated that malicious VMs could break out of the hypervisor environment, potentially compromising host servers and adjacent virtual machines. With virtualization forming the backbone of many corporate and government IT stacks, this vulnerability has been classified as one of the highest risks of the year so far.

Conclusion & Forward Outlook

What 2025 has made strikingly clear is that critical vulnerabilities are no longer limited to the traditional software stack. We're seeing flaws originate deep within firmware, containers, and even hardware-level abstractions—challenging conventional detection and response models. This has serious implications:

- Firmware and BIOS threats, as seen in the Gigabyte case, highlight the risk of long-term persistent attacks that evade OS-level monitoring tools.

- AI systems, once considered niche, now represent a growing attack surface, particularly in container orchestration environments.

- Web-facing infrastructure and edge services, like Citrix and VMware products, continue to be high-priority targets due to their visibility and privilege levels.

- Consumer-facing software, such as Chrome, remains vulnerable to zero-day exploits, showing that even highly resourced vendors can't eliminate all threat vectors.

Going forward, organizations need to adopt a more proactive, layered approach to vulnerability management. This includes:

- Applying firmware and microcode updates—not just application patches.

- Using sandboxing and behavioral isolation tools more effectively.

- Integrating automated patch management and threat intelligence into DevSecOps workflows.

- Prioritizing attack surface reduction via network segmentation and hardened baselines.

Additionally, with the increasing overlap between cloud-native architecture and on-device processing (especially in AI and IoT), expect more complex vulnerabilities that involve cross-system interactions and privilege escalations through obscure APIs. CISOs and security teams must treat vulnerability intelligence as a strategic asset, not just an IT hygiene task.

2025 is shaping up to be a pivotal year in cybersecurity—not for the sheer number of bugs disclosed, but for how deep and systemic they are. The organizations that win will be those that don't just react fast, but prepare smart.

Infostealer Analysis

As of mid-2025, the cybersecurity landscape continues to face a steady onslaught from infostealer malware, malicious software designed to covertly harvest sensitive user information from infected systems. These stealers target credentials, financial data, browser histories, and session tokens—serving as a foundational weapon for broader cybercrime activity including fraud, identity theft, and follow-on ransomware attacks. From January through July, the ThreatMon system captured detailed logs of infostealer activity, allowing us to analyze the top malware families in circulation and their month-by-month footprint.

Leading Infostealer Families

The most active infostealer families in 2025 so far include well-known strains such as RedLine, LummaC2, Raccoon Stealer, and Vidar. These families have proven persistent across different geographies and attack vectors, often spreading via phishing campaigns, malvertising, and cracked software sites. RedLine, in particular, continues to dominate in both prevalence and adaptability, frequently incorporating anti-VM and anti-analysis features to evade detection.

Following closely are LummaC2 and Raccoon, both of which are sold as malware-as-a-service (MaaS) on underground forums, enabling even low-skilled actors to launch attacks. Their popularity stems from ease of use and robust documentation, allowing them to scale fast across victim endpoints. Notably, Vidar has also resurfaced in several campaigns, often distributed through malicious payloads embedded in seemingly benign software installers.

Monthly Activity Trends

Analyzing the data month by month, infostealer activity remained consistent through Q1 and early Q2 of 2025, with January and February registering notable spikes, likely tied to campaigns timed around New Year sales and tax season phishing themes. Although the total number of logs decreased slightly into March and April, June appears to show signs of a resurgence, suggesting a pivot toward summer-themed lures or global events used as bait.

This monthly variance aligns with broader threat intelligence trends, where malware operators time their campaigns to coincide with user behavior cycles, shopping peaks, and global disruptions. As July unfolds, monitoring will continue to determine whether the activity stabilizes or accelerates into the second half of the year.

Summary and Outlook

Infostealers remain a key pillar of the cybercrime economy, acting as precursors to deeper intrusions or financial exploitation. The ongoing dominance of strains like RedLine and LummaC2 highlights the need for proactive defense, including endpoint monitoring, zero-trust architecture, and employee awareness training. For defenders, understanding the tooling and timeline of these malware families is critical—not only to stop breaches in progress but to anticipate future tactics.

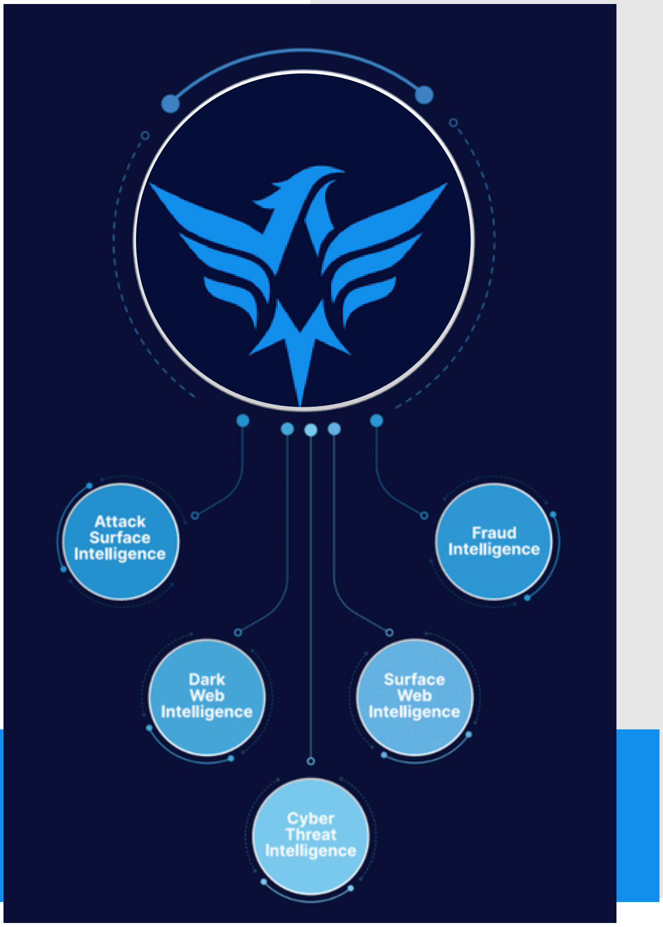
Given current trajectories, we expect infostealer activity to either maintain its level or spike again in Q3, especially around major global events or back-to-school timelines. Enterprises and individuals alike must maintain vigilance, as the commodification of stealer kits makes the threat more scalable than ever.

THREATMON END-TO-END INTELLIGENCE

The ever-changing threat landscape evolves into a more fast-paced environment where threat actors collaborate the most, causing threats to emerge and harm much faster.

Today, it is proven that Businesses of all sizes may suffer from the agility of threat actors.

ThreatMon End-to-End Intelligence consists of multiple modules that enable businesses to obtain collectively exhaustive threat intelligence.



Key Features & Benefits

Holistic Intelligence

Comprehensive approach to threat intelligence covers all your security needs

Proactive Security

Real-time alerts and actionable intelligence

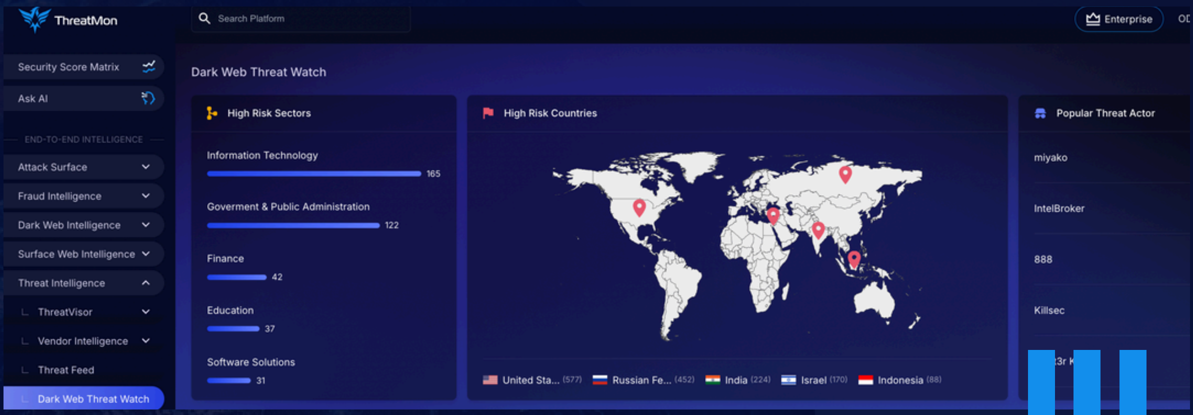
Scalable & Democratized

Flexible pricing options and a user-friendly interface

Enhanced Efficiency

Automated tools and intelligent insights

More Information About ThreatMon



Dark Web Threat Watch

High Risk Sectors

Information Technology	165
Goverment & Public Administration	122
Finance	42
Education	37
Software Solutions	31

High Risk Countries

United Sta... (577) Russian Fe... (452) India (224) Israel (170) Indonesia (88)

Popular Threat Actor

miyako

IntelBroker

888

Killsec

3r K

One Platform for all intelligence needs.

ThreatMon End-to-end intelligence is a cutting-edge, cloud-based SaaS platform that continuously monitors the dark and surface web, providing early warnings and actionable insights into emerging threats.

We are a SaaS platform designed to help businesses proactively detect and address threats before a cyber attack occurs. Unlike traditional cyber threat intelligence, we provide comprehensive and holistic cyber intelligence.

- *Attack Surface Intelligence*
- *Fraud Intelligence*
- *Dark and Surface Web Intelligence*
- *Threat Intelligence*
- *Security Score matrix*
- *ThreatMon AI Agent*

APPLY

FREE ACCESS

Contact Us :

Email Address
info@threatmonit.io

https://x.com/MonThreat

https://www.linkedin.com/company/threatmon