ThreatMon
Under Cyber Wings

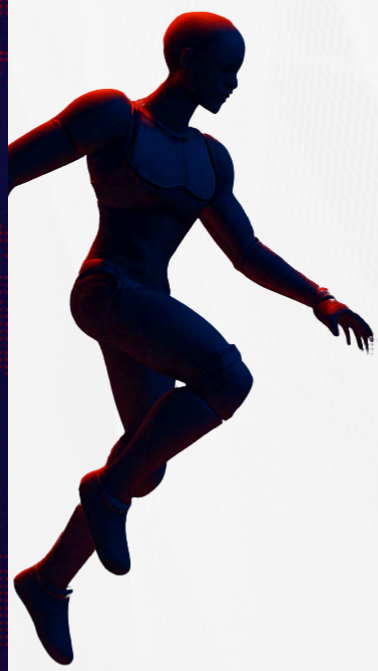
Global Government Sector

CYBER THREAT INTELLIGENCE REPORT

threatmon.io

ThreatMon
Under Cyber Wings

Table of Contents



Executive Summary

By 2025, the cyber threat landscape affecting public institutions has expanded significantly in terms of both diversity and intensity. DDoS attacks were the most common type of attack throughout the year, accounting for 68.6% of all incidents. These attacks were typically operations directed by hacktivist groups, targeting service disruption and concentrated in conflict zones such as Israel and Ukraine.

However, the real critical risk lies in the more silent threats focused on identity and access. The rapid spread of infostealer software, which transfers stolen identity information to Initial Access Brokers, forms the basis for data breaches and ransomware cases. The increase in such activities in regions such as India, Indonesia, and Turkey shows that weaknesses in identity management in public infrastructure remain a significant problem.

State-sponsored APT groups continue to be the most strategic and long-term impactful side of these attacks. SideWinder's operations throughout 2025 were a striking example of this. Targeting South Asian countries, this campaign infiltrated networks via phishing emails launched through vulnerable office documents and conducted persistent espionage activities against diplomatic and military institutions using multi-stage loaders and identity theft modules. Such operations demonstrate once again how difficult it is to detect when classic attack methods are combined with modern concealment techniques.

Ransomware groups also continued to view the public sector as a high-value target throughout 2025. The Qilin group spread rapidly by exploiting both leaked credentials and unpatched services, becoming involved in over 700 incidents worldwide. At least 31 of these attacks directly targeted public institutions, often resulting in both service disruptions and significant data breaches.

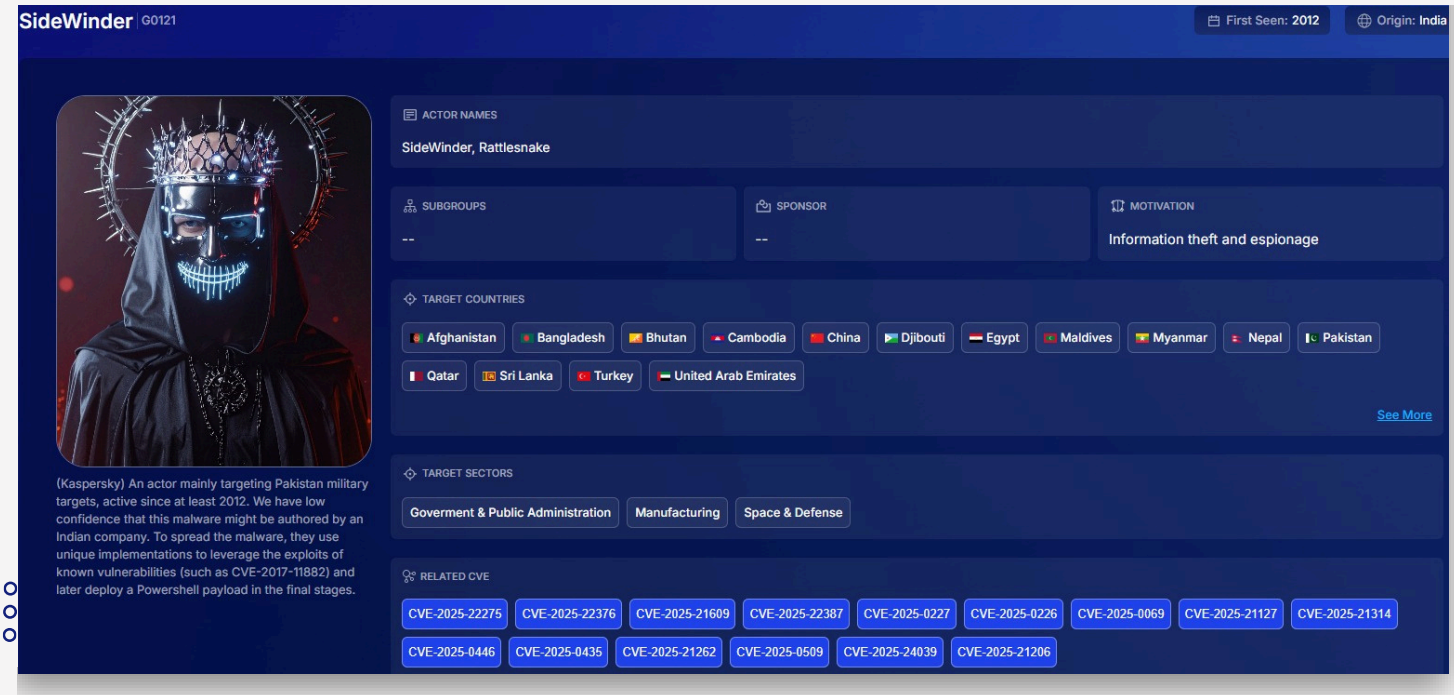
Looking at the overall picture, intense DDoS pressure, identity-based intrusion attempts, advanced APT operations, and increasingly planned ransomware campaigns have left the public sector facing a multidimensional and constantly evolving threat environment in 2025. This environment highlights the importance of robust defense strategies on both the operational resilience and identity security fronts more than ever before.

Threat Actor Trends Targeting Government Entities

The global government sector in 2025 continues to face an increasingly diverse and rapidly evolving threat actor ecosystem driven by geopolitical tensions, the commoditization of cyber tools, and the expansion of the cybercrime economy.
Across this period, three primary adversary classes—state-aligned Advanced Persistent Threat (APT) groups, financially motivated ransomware operators, and ideologically driven hacktivist collectives—have shaped the overall risk landscape for public-sector entities worldwide.

STATE-SPONSORED APT THREATS

ThreatMon Threat Actor Page



State-aligned APT groups remain the most strategically impactful threat to government institutions due to their long-term intelligence objectives, sophisticated tradecraft, and ability to persist undetected within high-value networks. Throughout 2025, multiple APT campaigns targeted ministries, diplomatic missions, defense institutions, and critical public services.

One of the most notable cases was the SideWinder APT campaign observed between March and September 2025, which focused on government organizations across Sri Lanka, Pakistan, Bangladesh, and other South Asian states. The group initiated operations through advanced spear-phishing emails delivering malicious RTF and Word documents exploiting CVE-2017-0199 and CVE-2017-11882. SideWinder then deployed a multi-stage loader equipped with polymorphic payloads, server-side obfuscation, and geofenced execution. The final payload included credential theft modules for persistent espionage against diplomatic, military, and financial government bodies. This campaign exemplifies how APT actors continue to combine classic exploitation vectors with modern stealth techniques—making early detection increasingly difficult for government defenders.

RANSOMWARE GROUPS

Although ransomware incidents represent a smaller percentage of total public-sector cyber events compared to DDoS, their operational and financial impacts remain disproportionately high. Ransomware groups in 2025 demonstrated enhanced targeting accuracy, leveraging Initial Access Brokers (IABs), infostealer data, and unpatched external services to compromise government systems.

A leading example is the Qilin ransomware group, which escalated its global activity throughout 2025. Qilin was attributed to over 700 attacks, with at least 31 confirmed intrusions involving government agencies.
These attacks primarily targeted ministries, municipal administrations, public service providers, and citizen-data platforms. Qilin consistently applied double-extortion tactics, combining rapid encryption of core systems with large-scale data exfiltration to pressure government institutions into payment. Their operations highlight how ransomware actors increasingly treat public-sector organizations as high-leverage victims due to their operational dependency on service continuity and sensitive citizen information.

RANSOMWARE GROUP	VICTIM	COUNTRY	SECTOR	DATE	TAG
qilin	www.williamson-county.org	United States	Government & Public Administration	28/11/2025	--
qilin	fayettecountypa.org	--	Government & Public Administration	20/11/2025	--
qilin	www.scouts.ca	Canada	Government & Public Administration	08/11/2025	--
qilin	www.newlenox.net	--	Government & Public Administration	07/11/2025	--
qilin	www.villemontlaurier.qc.ca	Canada	Government & Public Administration	06/11/2025	--
qilin	www.sarpc.org	United States	Government & Public Administration	26/10/2025	--
qilin	sede.agenciatributaria.gob.es	Spain	Government & Public Administration	15/10/2025	--
qilin	www.catawbacountync.gov	United States	Government & Public Administration	14/10/2025	--
qilin	www.rivierabch.com	United States	Government & Public Administration	14/10/2025	--
qilin	www.hautsdefrance.fr	France	Government & Public Administration	10/10/2025	--
qilin	www.sugarlandtx.gov	United States	Government & Public Administration	09/10/2025	--
qilin	www.ville-saintclaude.fr	France	Government & Public Administration	03/10/2025	--
qilin	sagchip.org	United States	Government & Public Administration	02/10/2025	--
qilin	www.heparks.org	United States	Government & Public Administration	25/09/2025	--
qilin	lakehaven.org	United States	Government & Public Administration	25/09/2025	Announcement
qilin	orpp.or.ke	Kenya	Government & Public Administration	14/09/2025	--

ThreatMon Ransomware Attacks Page

In 2025, the Medusa ransomware group intensified its focus on government and public-administration entities, particularly those managing large volumes of citizen and operational data.

A notable example occurred on 21 February 2025, when Medusa claimed responsibility for a targeted intrusion against bentonpolice.org,

a United States government and public administration domain.

The attack reportedly resulted in the exfiltration and publication of sensitive administrative records, demonstrating Medusa's continued use of double-extortion tactics against public-sector institutions.

RANSOMWARE GROUP	VICTIM	COUNTRY	SECTOR	DATE	TAG
medusa	pacga.org	United States	Government & Public Administration	03/07/2025	--
medusa	northprovidenceri.gov	United States	Government & Public Administration	30/05/2025	Announcement
medusa	--	United States	Government & Public Administration	24/04/2025	--
medusa	--	Canada	Government & Public Administration	19/04/2025	Exposed
medusa	--	United States	Government & Public Administration	26/02/2025	--
medusa	mundeleinparks.org	United States	Government & Public Administration	24/02/2025	Exposed
medusa	bentonpolice.org	United States	Government & Public Administration	21/02/2025	--
medusa	gateshead.gov.uk	United Kingdom	Government & Public Administration	21/02/2025	--
medusa	--	United States	Government & Public Administration	12/02/2025	Exposed

ThreatMon Ransomware Attacks Page

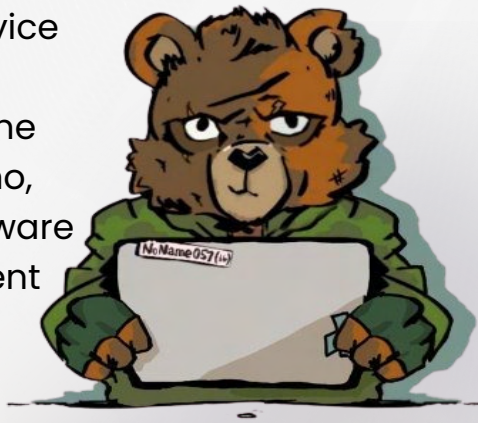
Hacktivist and Geopolitical Threat Groups

Hacktivist collectives—often aligned with regional or geopolitical agendas—continued to orchestrate high-volume disruptive attacks against government institutions. The majority of these operations consisted of large-scale DDoS campaigns, website defacement, and opportunistic data leaks intended to influence public opinion or destabilize political environments. In regions experiencing active conflict or heightened political tension, such as Israel and Ukraine, hacktivist-driven DDoS attacks accounted for a dominant percentage of all government-sector incidents in 2025. While these groups lack the sophistication of APTs or ransomware operators, their ability to rapidly mobilize, coordinate large botnets, and target public-facing systems creates significant short-term operational pressure on government digital infrastructure.

One notable group in 2025 was NoName057(16), a pro-Russian hacktivist collective known for sustained DDoS activity against government and public-service institutions. According to Radware's threat intelligence reporting, the group was responsible for a significant portion of hacktivist-driven attacks in Q1 2025, with the United States representing 13.5% of all observed hacktivist targets during that period. Their operations primarily focused on disrupting public-facing government portals, transportation authorities, and municipal service infrastructures through large-scale botnet-driven DDoS waves.

Throughout 2025, NoName057(16) and similar politically aligned hacktivist groups continued to prioritize government and public-sector organizations globally.

Cyble's analysis highlights that these collectives expanded their operational scope beyond DDoS activity, incorporating service disruption campaigns, opportunistic data leaks, and coordinated influence operations. This trend underscores the growing impact of ideologically motivated cyber actors who, despite limited sophistication compared to APT or ransomware groups, exert significant operational pressure on government digital services during periods of geopolitical tension.



Cybercrime Ecosystem and Initial Access Brokers

Supporting all major threat actor categories is the expanding underground ecosystem of Initial Access Brokers and infostealer-driven credential marketplaces. Millions of compromised government-domain credentials were observed across infostealer logs in 2025, providing cost-effective entry points for both ransomware affiliates and espionage groups. The commodification of access—where attackers can purchase session tokens, VPN credentials, or administrative logins for minimal cost—has significantly lowered the barrier to launching impactful operations against government systems. This trend amplifies the importance of identity security, MFA enforcement, and continuous credential monitoring across public-sector environments.

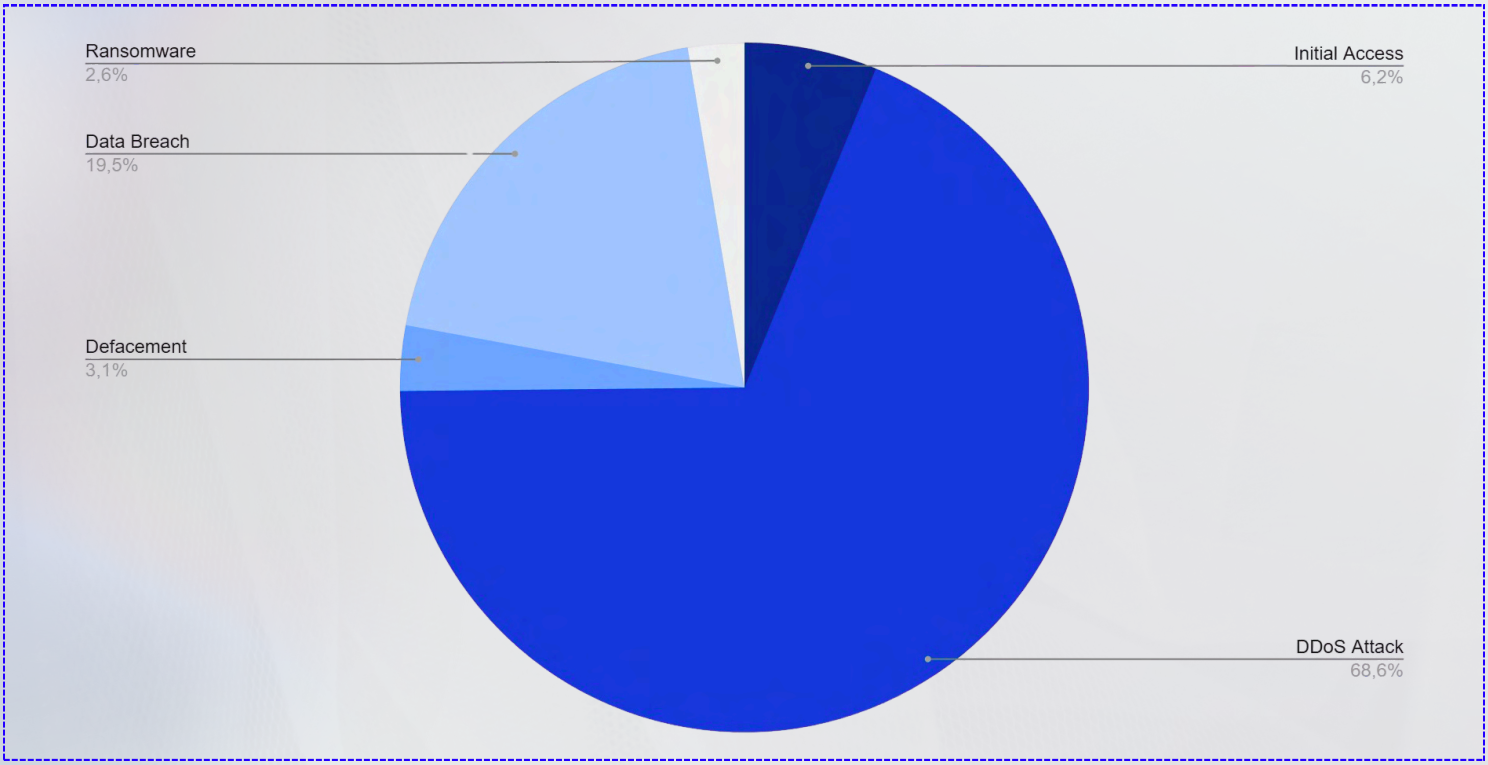
OVERALL ASSESSMENT

The threat actor landscape impacting government institutions in 2025 is characterized by a clear bifurcation:

- High-volume disruption driven by hacktivist collectives and DDoS-focused actors, and
- Low-frequency but high-impact compromise driven by APT and ransomware groups.

The integration of APT-level stealth techniques with ransomware monetization strategies, coupled with widespread credential leakage and the proliferation of IAB services, indicates that government networks face sustained strategic and operational risk. As adversaries continue to refine their techniques—particularly around identity compromise, supply-chain infiltration, and stealthy lateral movement—the ability of public-sector institutions to maintain resilience increasingly depends on proactive detection, continuous monitoring, and identity-centric security architectures.

Cyber Incident Analytics and Attack Vector Breakdown



In 2025, DDoS attacks accounted for 68.6% (6,055 incidents) of all recorded cyber incidents targeting the public sector, making them the most prevalent threat vector. This trend indicates a strong emphasis on large-scale service disruption aimed at public-facing government systems.

Data breach incidents represented 19.5% (1,718 cases), underscoring persistent risks to sensitive governmental and citizen-related data. Initial access activities comprised 6.2% (550 incidents), reflecting continued exploitation of exposed services, weak credentials, and misconfigurations to establish initial footholds.

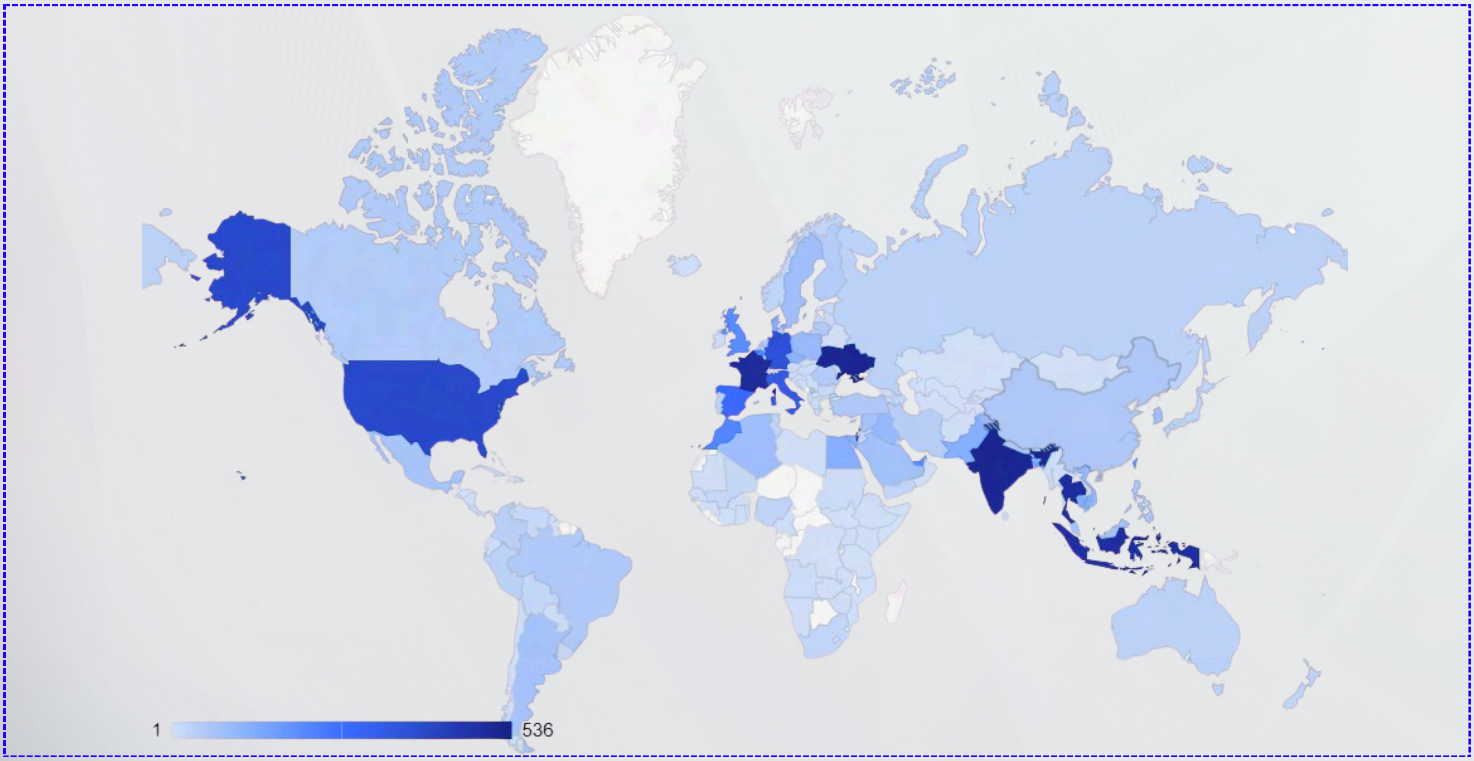
Defacement attacks accounted for 3.1% (270 incidents), primarily impacting public trust and institutional reputation, while ransomware incidents remained comparatively lower at 2.6% (233 incidents) but posed high operational and financial impact despite their lower frequency.

Government Sector Victimology and Statistical Distribution

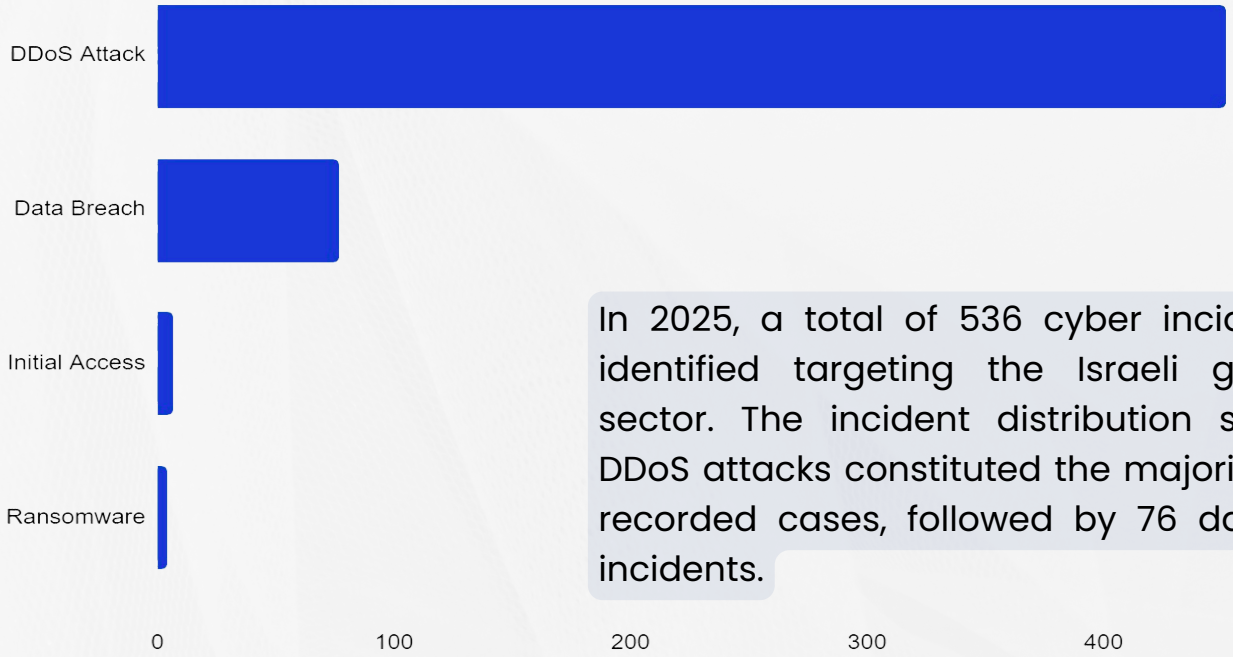
In 2025, DDoS attacks accounted for 68.6% (6,055 incidents) of all recorded cyber incidents targeting the public sector, making them the most prevalent threat vector. This trend indicates a strong emphasis on large-scale service disruption aimed at public-facing government systems.

Data breach incidents represented 19.5% (1,718 cases), underscoring persistent risks to sensitive governmental and citizen-related data. Initial access activities comprised 6.2% (550 incidents), reflecting continued exploitation of exposed services, weak credentials, and misconfigurations to establish initial footholds.

Defacement attacks accounted for 3.1% (270 incidents), primarily impacting public trust and institutional reputation, while ransomware incidents remained comparatively lower at 2.6% (233 incidents) but posed high operational and financial impact despite their lower frequency.

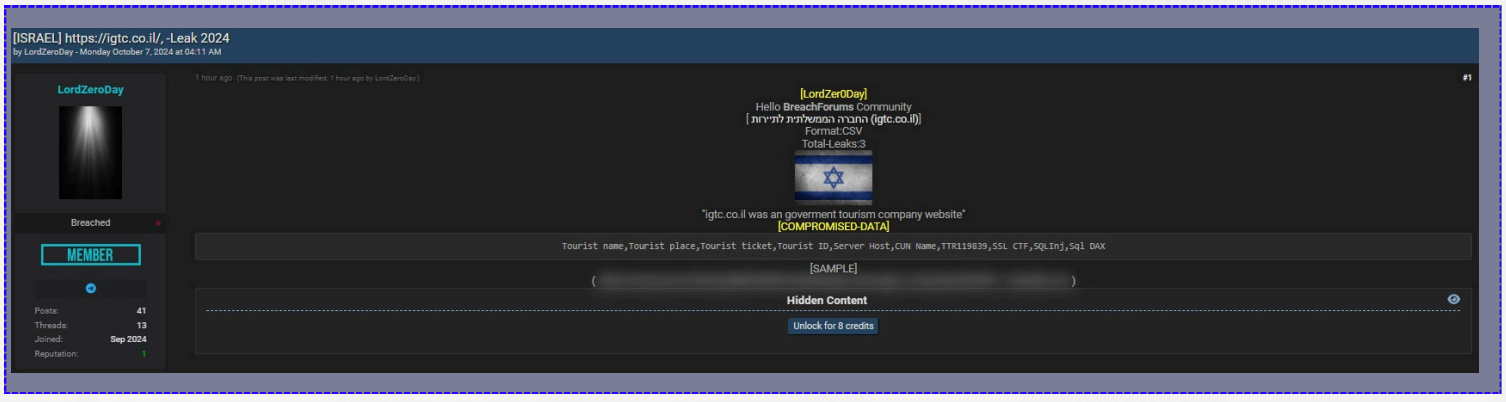


ISRAEL



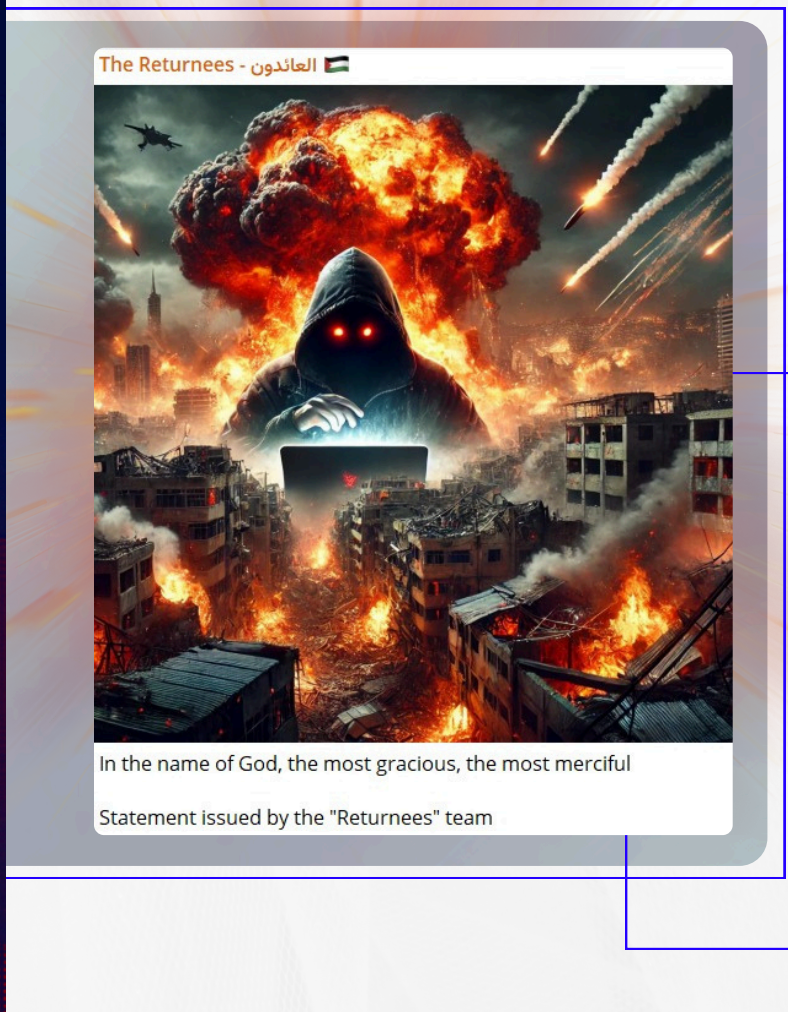
In 2025, a total of 536 cyber incidents were identified targeting the Israeli government sector. The incident distribution shows that DDoS attacks constituted the majority, with 451 recorded cases, followed by 76 data breach incidents.

Initial access (6 cases) and ransomware incidents (3 cases) were observed at significantly lower frequencies when compared to disruptive and data exposure–related activity. Overall, the majority of recorded incidents fell within the DDoS attack category.



On October 7, 2024, a threat actor claimed to have leaked the data of the Israel Government Tourist Corporation (IGTC), a government entity responsible for promoting Israel as a global tourist destination.

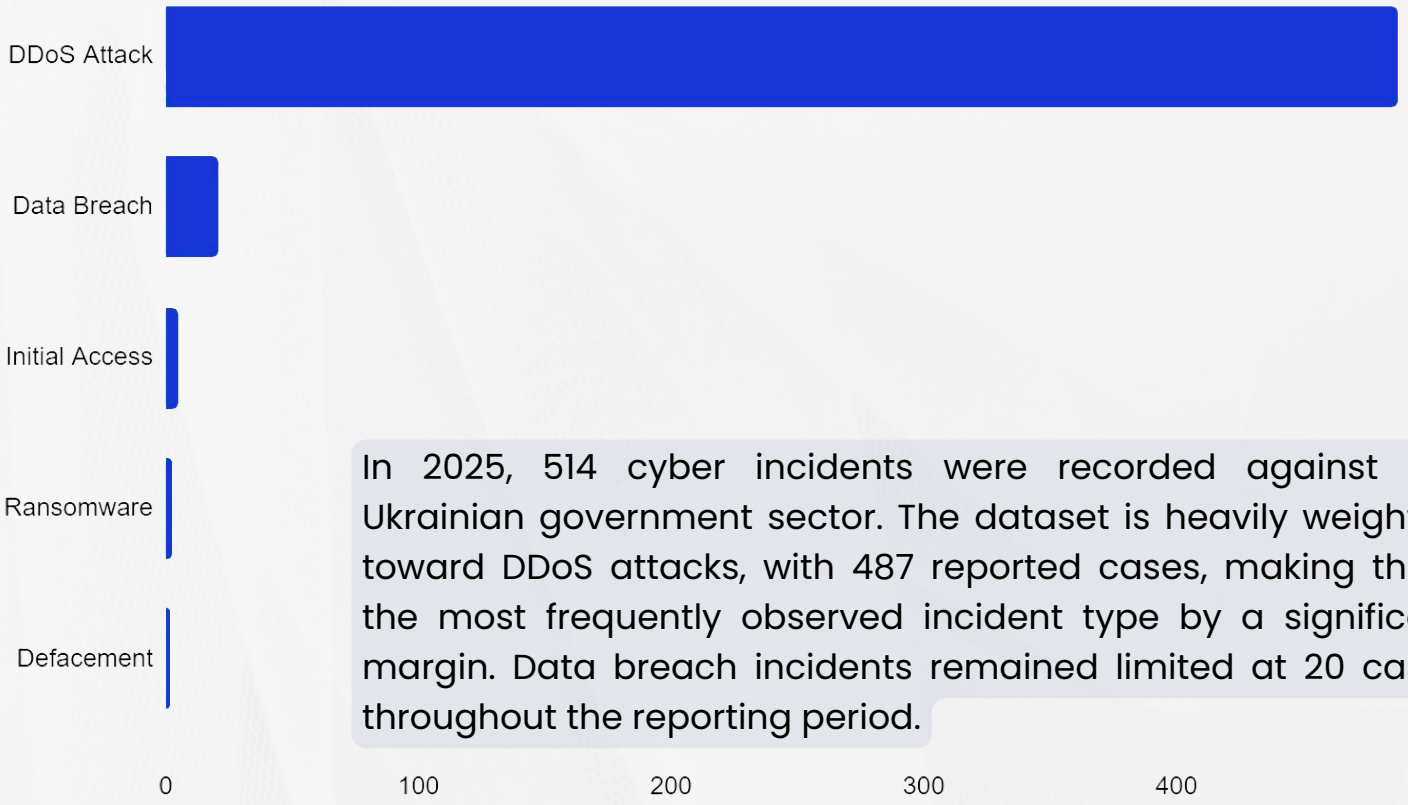
The leaked data reportedly contains information such as names, locations, ID numbers, ticket details, and other personal information.



On October 7, 2024, The Returnees group claimed to have breached The Israeli Ministry of Finance, extracting 30 GB of sensitive files related to the Ministry's activities and various projects.

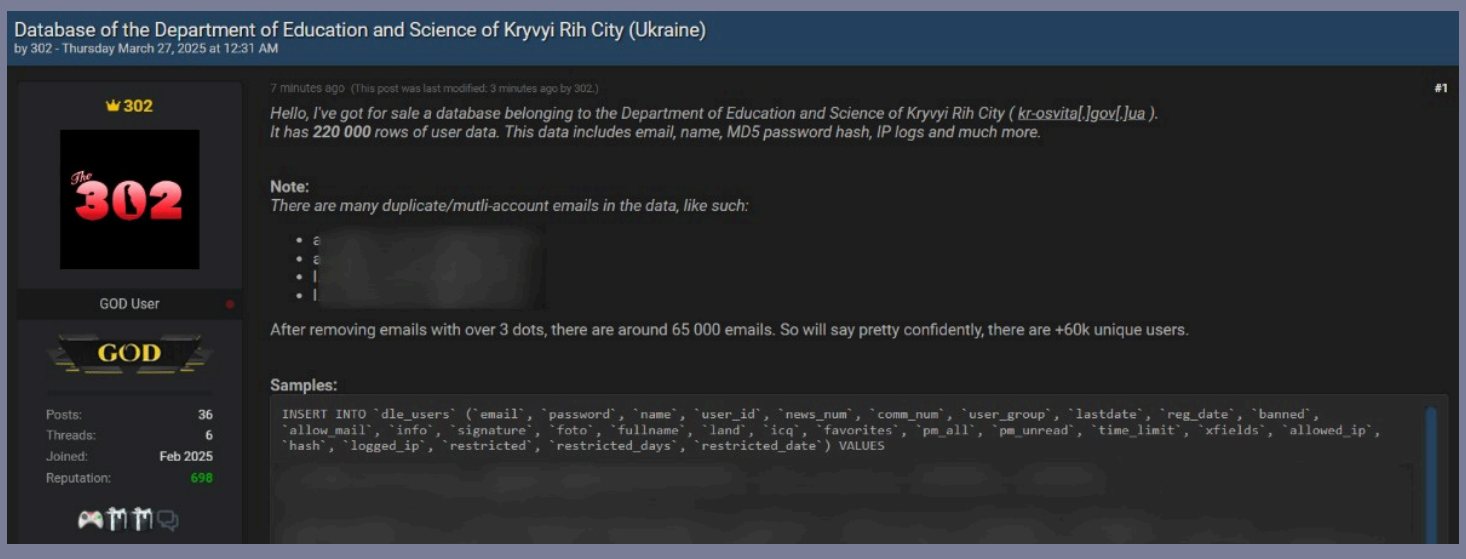
The compromised data reportedly includes detailed information on 4,000 publishers, including personal and employment data.

UKRAINE



In 2025, 514 cyber incidents were recorded against the Ukrainian government sector. The dataset is heavily weighted toward DDoS attacks, with 487 reported cases, making them the most frequently observed incident type by a significant margin. Data breach incidents remained limited at 20 cases throughout the reporting period.

Other activity types, including initial access (4 cases), ransomware (2 cases), and defacement (1 case), were observed only sporadically within the overall dataset. The incident distribution therefore reflects a pronounced imbalance across attack categories, with disruptive activity comprising the majority of recorded events.


Database of the Department of Education and Science of Kryvyi Rih City (Ukraine)
by 302 - Thursday March 27, 2025 at 12:31 AM

302

GOD User

GOD

Posts: 36
Threads: 6
Joined: Feb 2025
Reputation: 698

7 minutes ago (This post was last modified: 3 minutes ago by 302.) #1

Hello, I've got for sale a database belonging to the Department of Education and Science of Kryvyi Rih City (kr-osvita[.]gov[.]ua).
*It has **220 000** rows of user data. This data includes email, name, MD5 password hash, IP logs and much more.*

Note:
There are many duplicate/mutli-account emails in the data, like such:

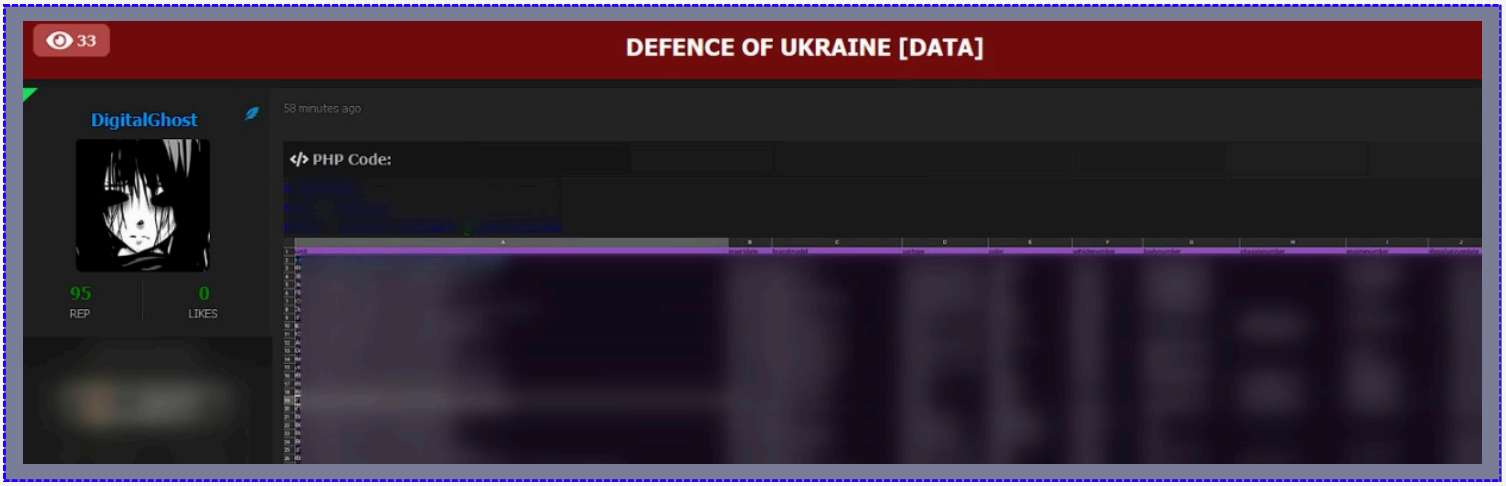
After removing emails with over 3 dots, there are around 65 000 emails. So will say pretty confidently, there are +60k unique users.

Samples:

```
INSERT INTO `dle_users` (`email`, `password`, `name`, `user_id`, `news_num`, `comm_num`, `user_group`, `lastdate`, `reg_date`, `banned`,
`allow_mail`, `info`, `signature`, `foto`, `fullname`, `land`, `icq`, `favorites`, `pm_all`, `pm_unread`, `time_limit`, `xfields`, `allowed_ip`,
`hash`, `logged_ip`, `restricted`, `restricted_days`, `restricted_date`) VALUES
```

On March 27, 2025, a threat actor claimed to be selling data from the Department of Education of the Kremenchuk City Council.

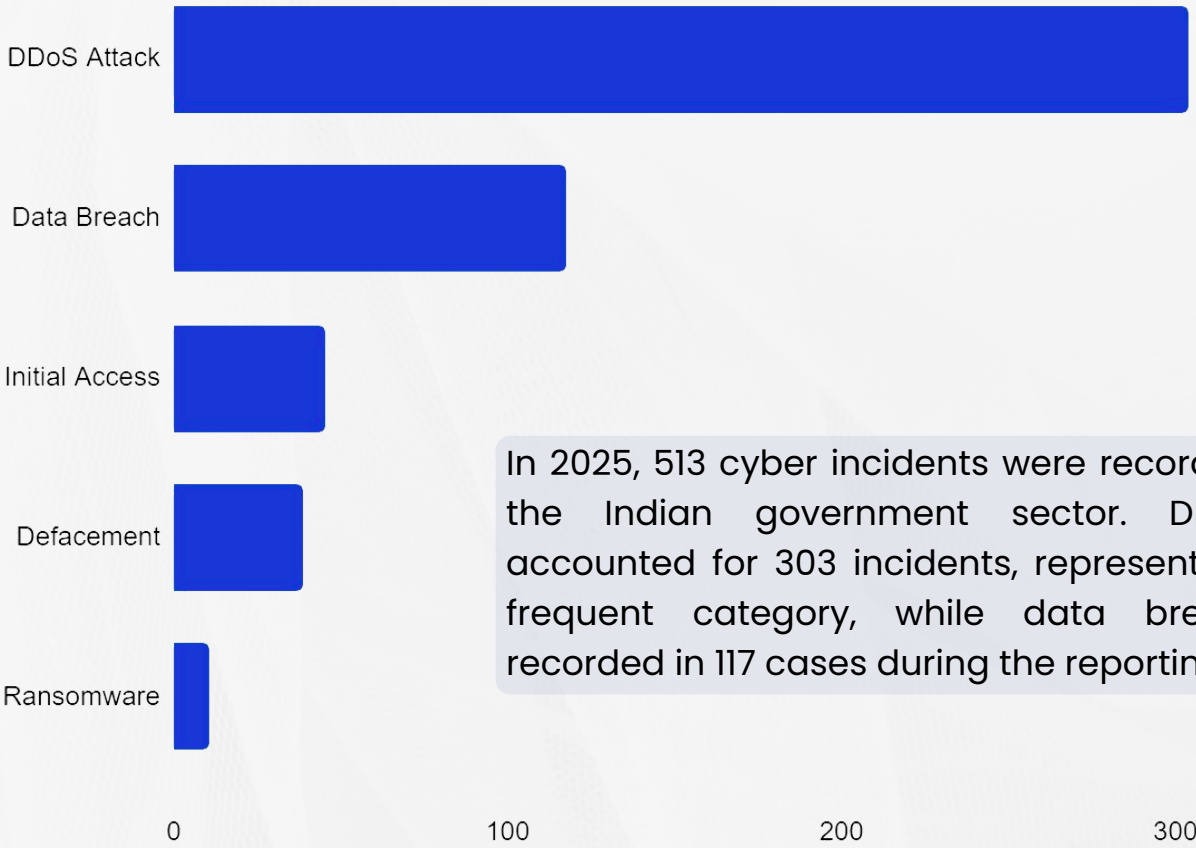
The compromised data reportedly contains 220,000 rows of user data, including email addresses, names, MD5 password hashes, IP logs, and other related information.



On June 10, 2025, a threat actor claimed to have breached four databases of the Ministry of Defense of Ukraine.

The exposed data reportedly includes unit, engine number, date, car type, chassis number, body number, and additional related information.

INDIA

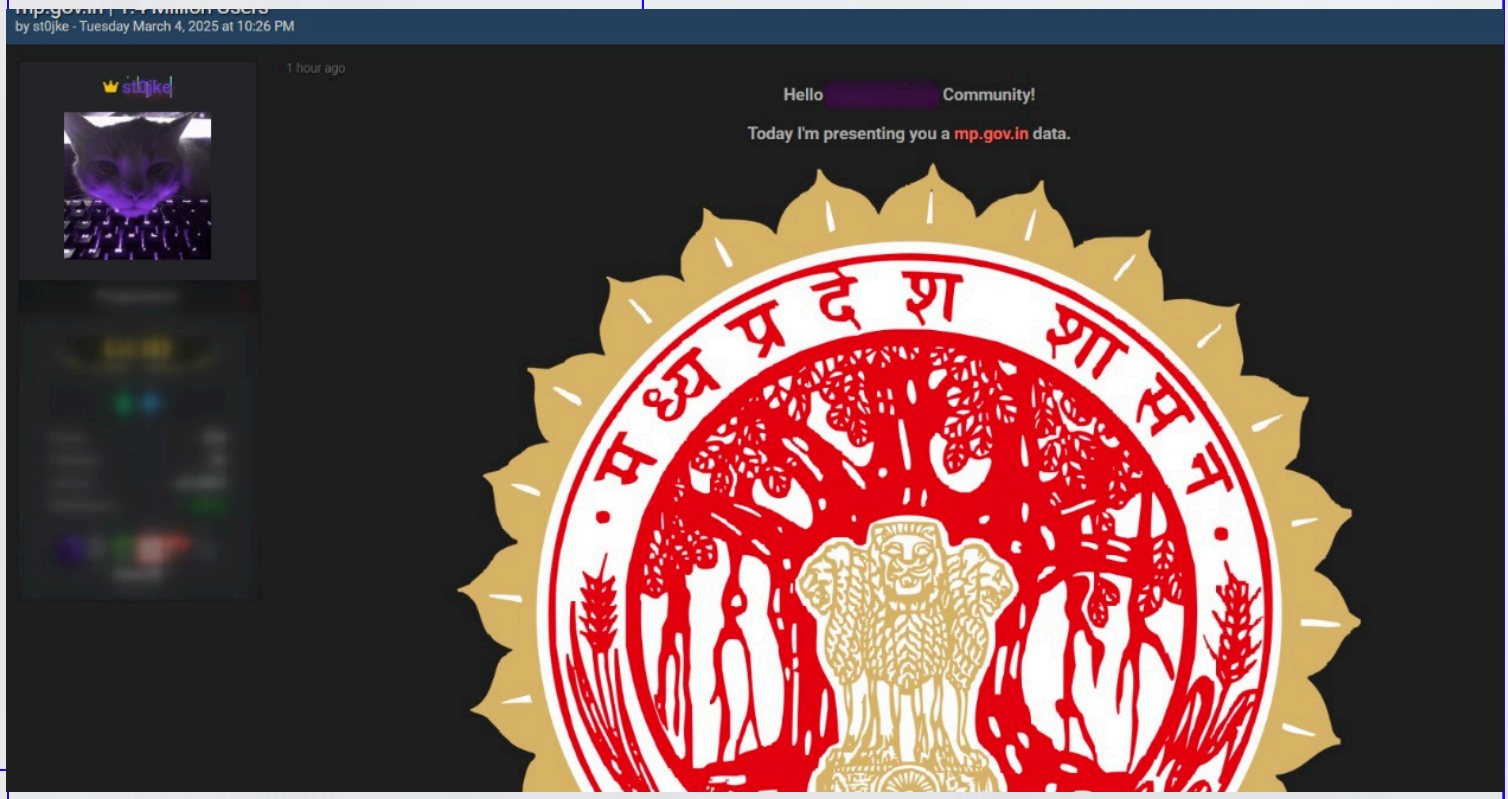


In 2025, 513 cyber incidents were recorded targeting the Indian government sector. DDoS attacks accounted for 303 incidents, representing the most frequent category, while data breaches were recorded in 117 cases during the reporting period.

Additional activity was observed across multiple categories, including initial access (45 cases), defacement (38 cases), and ransomware (10 cases). Compared to other country profiles within the dataset, the incident distribution in India spans a wider range of attack categories, reflecting a more diversified pattern of recorded events.

On February 19, 2025, a threat actor claimed to be selling data from the Ministry of Culture, Government of India.

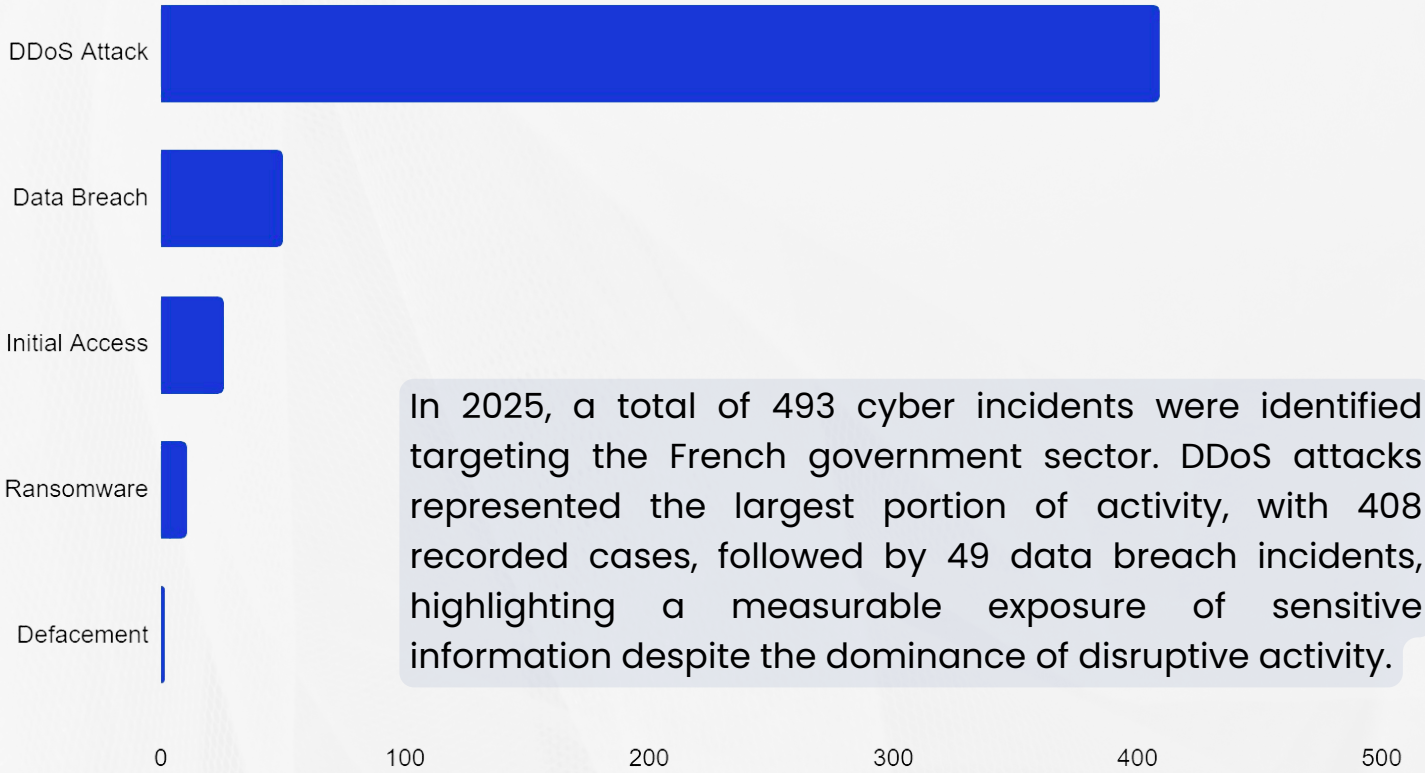
The leaked data reportedly includes name, sex, gender, job, phone number, and other related information.



On March 4, 2025, a threat actor claimed to have leaked data from the Government of Madhya Pradesh.

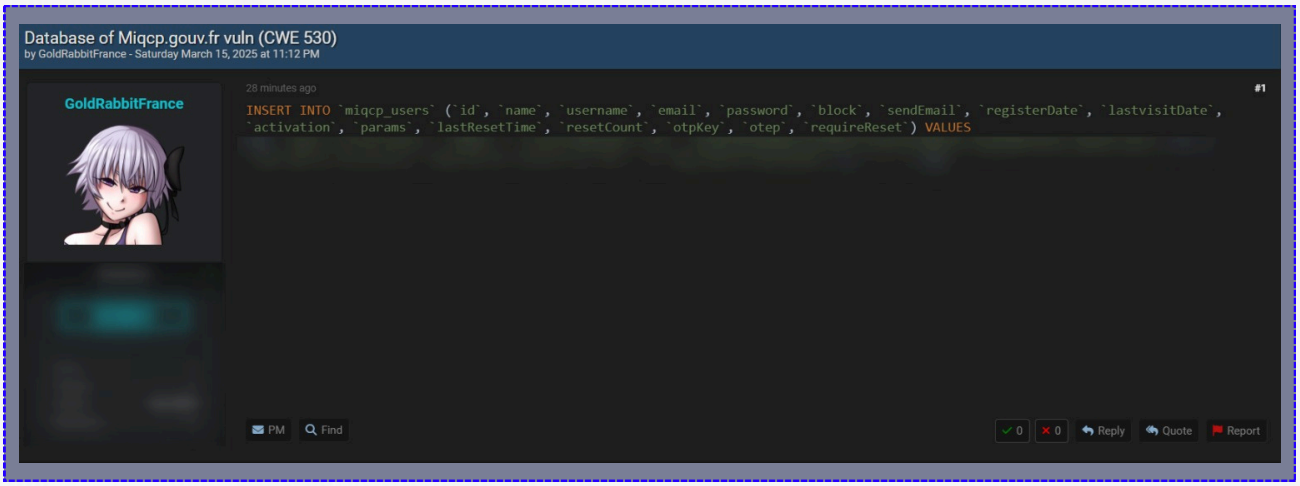
The leaked information reportedly contains over 1.4 million records, with the actor also claiming to be selling access to the affected data.

FRANCE



In 2025, a total of 493 cyber incidents were identified targeting the French government sector. DDoS attacks represented the largest portion of activity, with 408 recorded cases, followed by 49 data breach incidents, highlighting a measurable exposure of sensitive information despite the dominance of disruptive activity.

Additional categories included initial access (25 cases), ransomware (10 cases), and defacement (1 case), which were observed less frequently but remain part of the overall incident profile. The distribution of incidents across these categories demonstrates both a concentration in service disruption attacks and the presence of lower-volume activities targeting data compromise, access establishment, and limited website defacement. This detailed statistical distribution provides a comprehensive view of the types of attacks affecting the government sector within France for the year 2025.



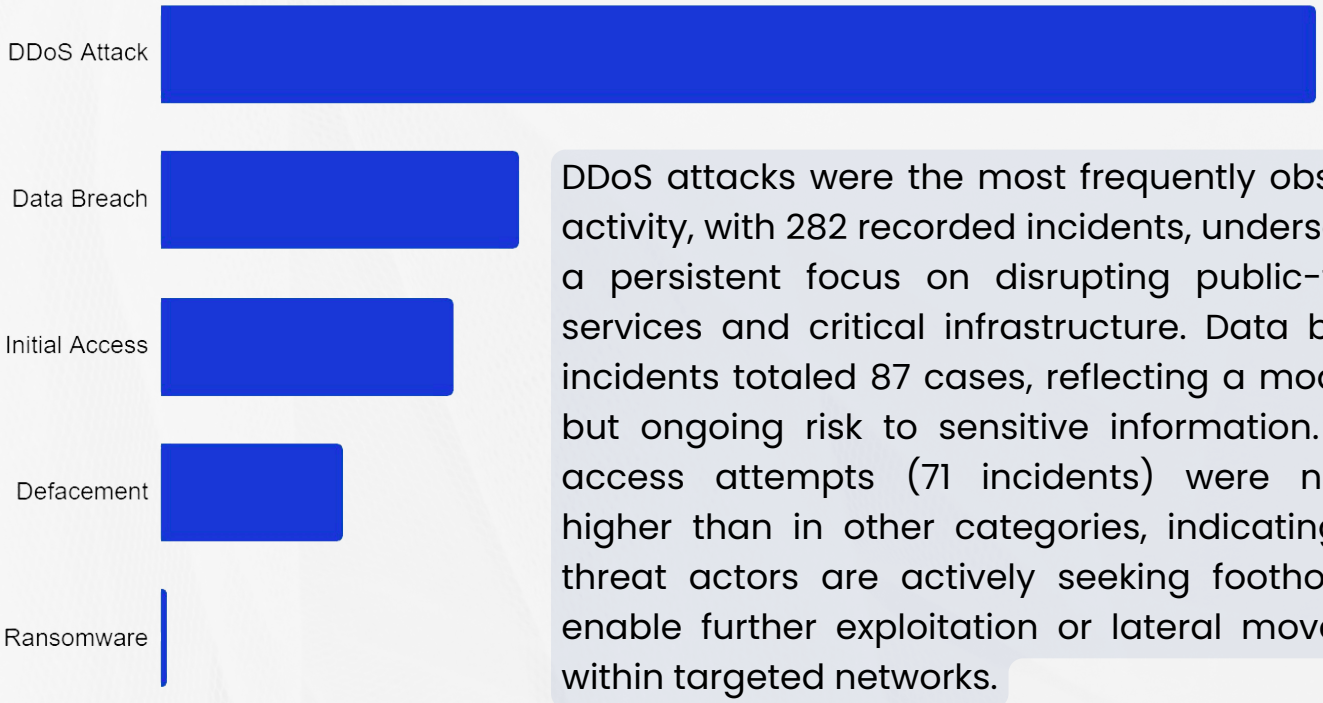
On March 15, 2025, a threat actor claimed to have leaked a database from the Interministerial Mission for the Quality of Public Constructions (MIQCP) in France.

The compromised data reportedly includes ID, name, username, email address, password, and other related information.

On March 22, 2025, a threat actor claimed to be selling data from the Agence Nationale des Titres Sécurisés (ANTS).

The compromised data reportedly contains approximately 12 million rows, including name, sex, email address, phone number, and other related information.

THAILAND

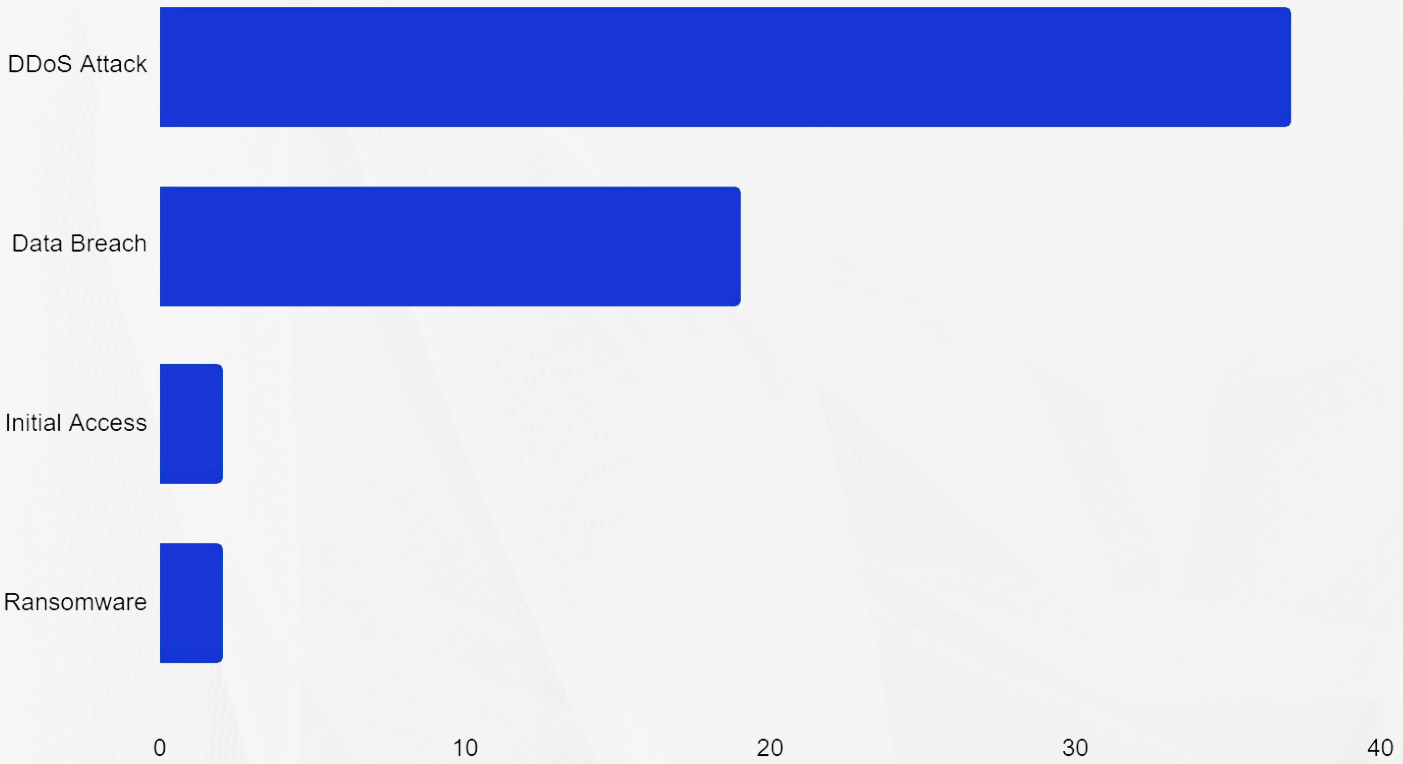


DDoS attacks were the most frequently observed activity, with 282 recorded incidents, underscoring a persistent focus on disrupting public-facing services and critical infrastructure. Data breach incidents totaled 87 cases, reflecting a moderate but ongoing risk to sensitive information. Initial access attempts (71 incidents) were notably higher than in other categories, indicating that threat actors are actively seeking footholds to enable further exploitation or lateral movement within targeted networks.

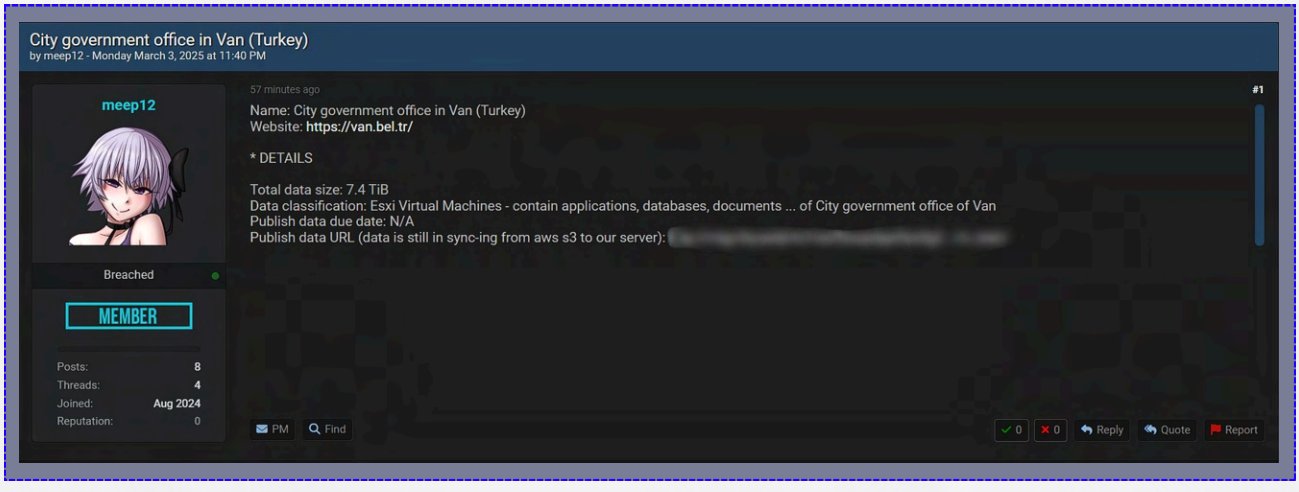
Defacement activity (44 incidents) suggests a visible trend in low-complexity, reputation-impacting attacks. Ransomware incidents remained minimal, with only 1 recorded case, highlighting that availability disruption and defacement are currently prioritized over long-term compromise or extortion campaigns.

On March 31, 2025, a threat actor claimed to have obtained a substantial amount of data, approximately 5 terabytes, from the Ministry of Finance (MOF) of Thailand, which oversees public finance, taxation, treasury, government property, and revenue-generating enterprises.

TURKIYE

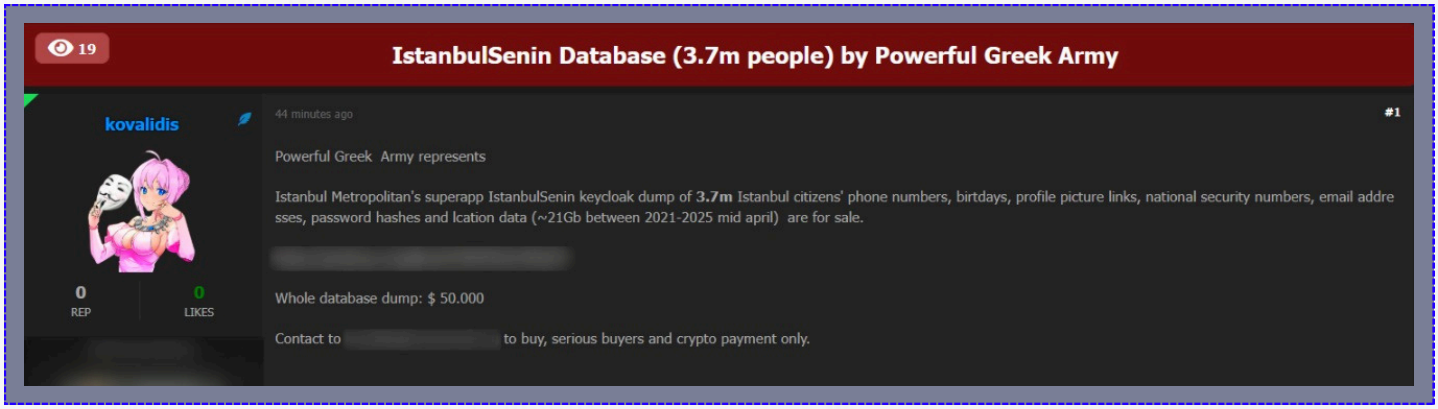


DDoS attacks represented the majority of observed activity in Turkey, with 37 recorded incidents, highlighting a continued emphasis on disrupting public-facing services. Data breach incidents totaled 19 cases, indicating a moderate risk to sensitive information. Initial access attempts (2 incidents) and ransomware activity (2 cases) were minimal, suggesting limited efforts to establish persistent footholds or deploy extortion-based attacks. Overall, the threat landscape in Turkey is currently dominated by availability-focused operations rather than long-term compromise or high-impact intrusion campaigns.



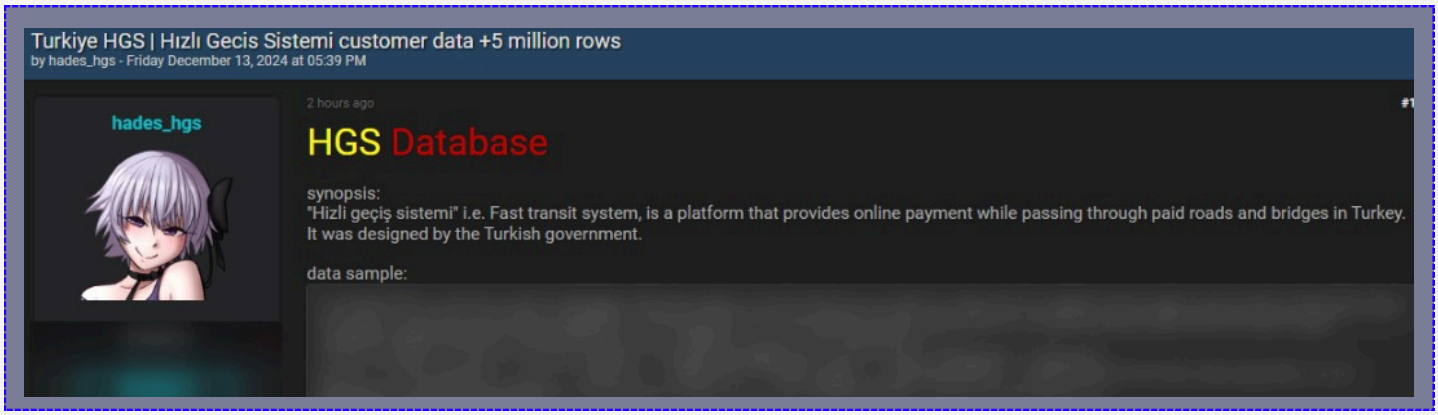
On March 3, 2025, a threat actor claimed to be selling data from Van Büyükşehir Belediyesi.

The compromised data reportedly contains approximately 7.4 TiB of information.



On May 26, 2025, a threat actor claimed to have breached the data of İstanbul Senin.

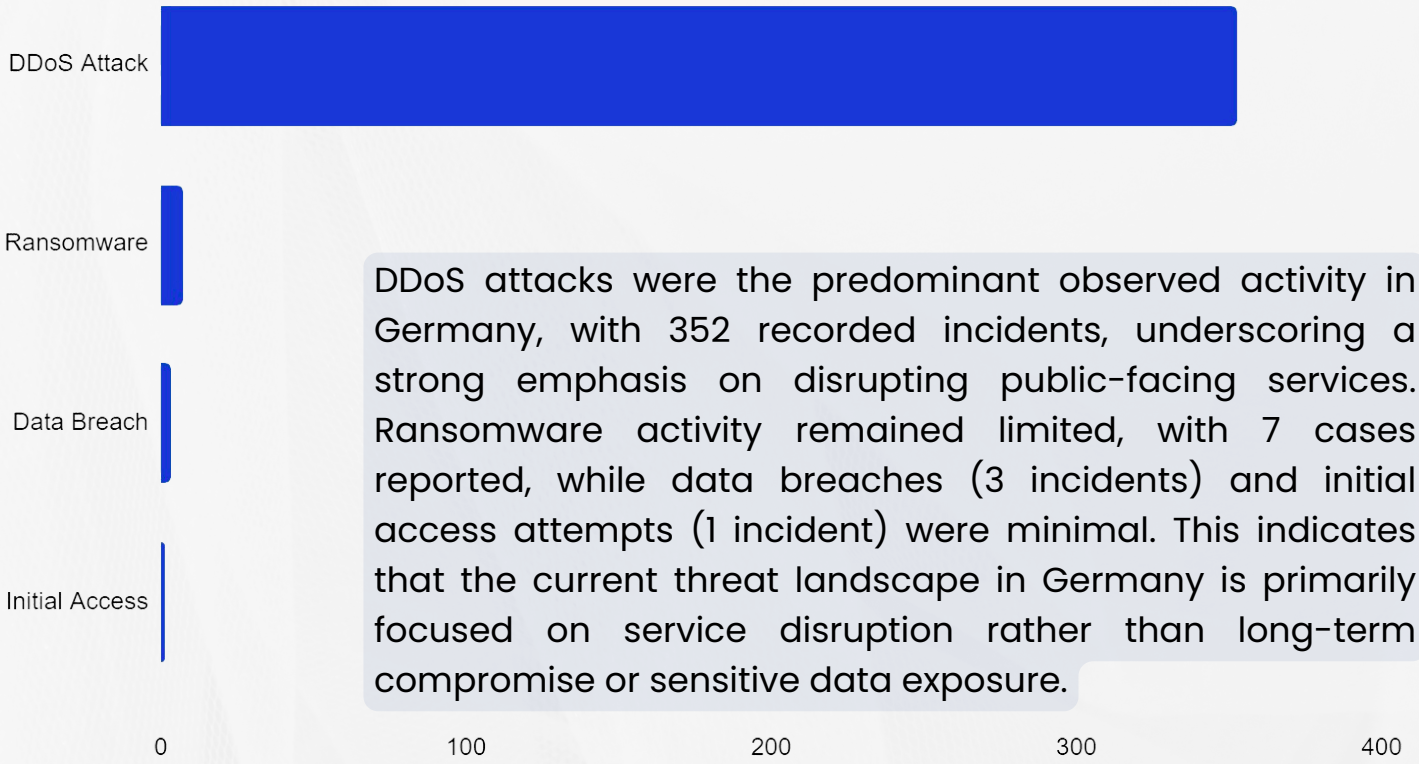
The compromised data reportedly consists of photos, phone numbers, email addresses, passwords, and other related information.



On December 13, 2024, a threat actor claimed to have leaked the database of HGS.

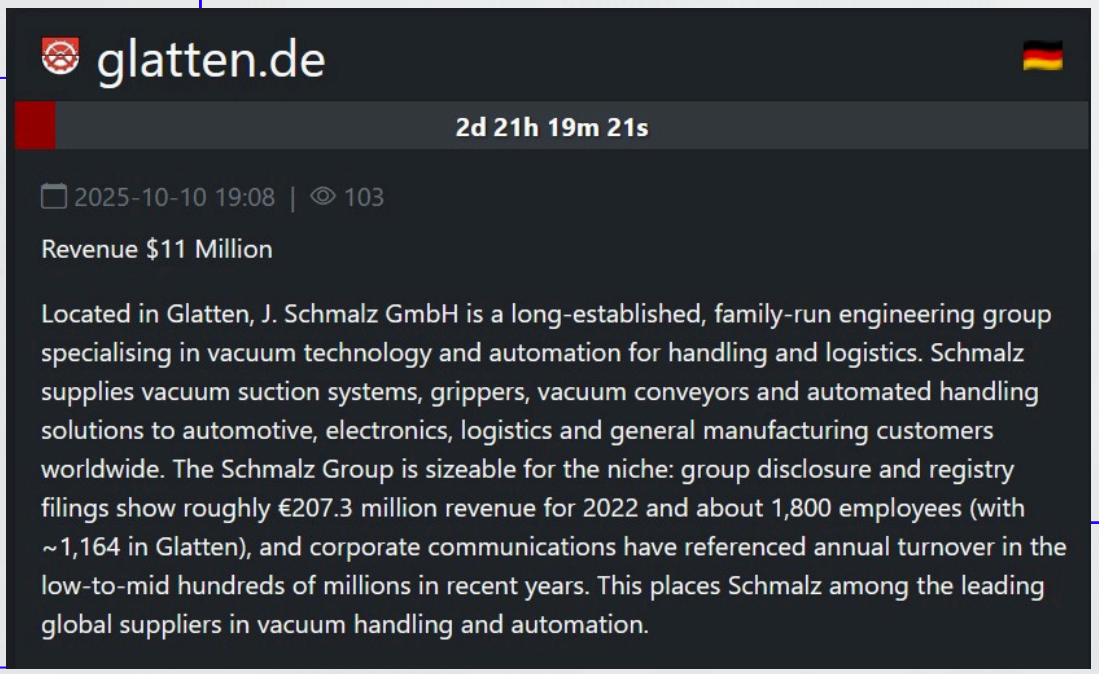
The leaked data reportedly includes user IDs, email addresses, device details, activity logs, location data, IP addresses, personal information, and other related information.

GERMANY

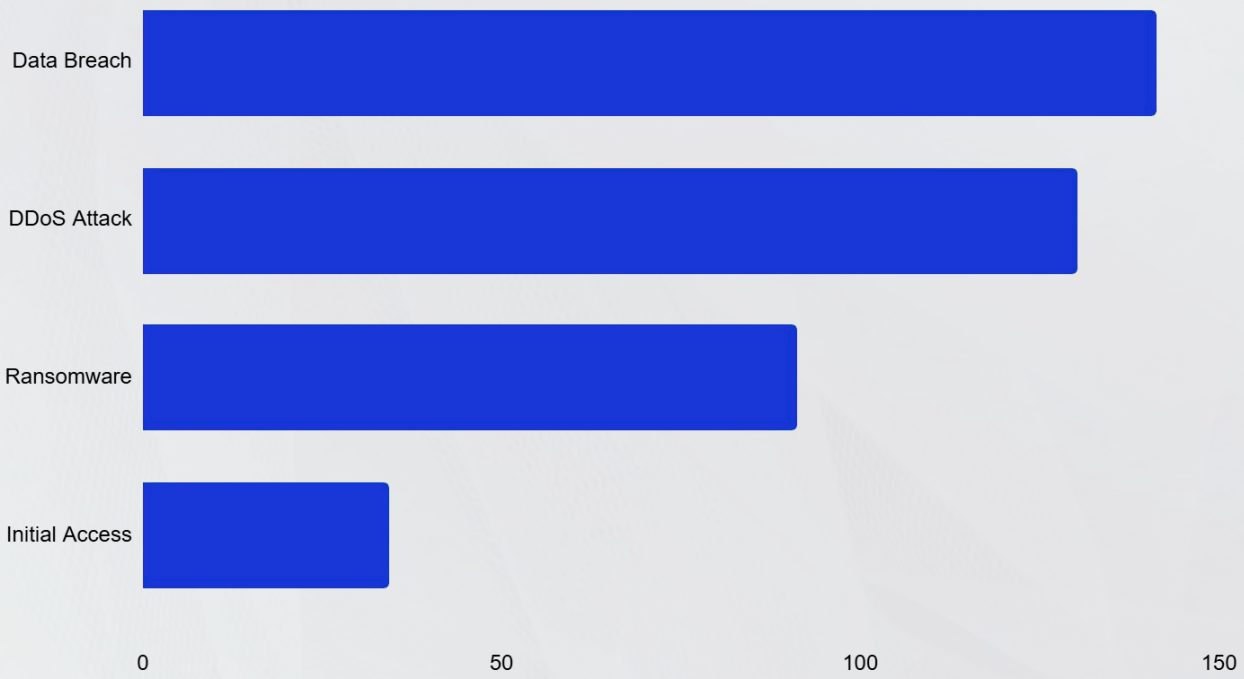


DDoS attacks were the predominant observed activity in Germany, with 352 recorded incidents, underscoring a strong emphasis on disrupting public-facing services. Ransomware activity remained limited, with 7 cases reported, while data breaches (3 incidents) and initial access attempts (1 incident) were minimal. This indicates that the current threat landscape in Germany is primarily focused on service disruption rather than long-term compromise or sensitive data exposure.

On October 10, 2025, the SAFEPAY ransomware group claimed to have obtained data from Glatten.de.



UNITED STATES



Data breach incidents represented the most prominent category with 141 recorded cases, highlighting sustained pressure on sensitive governmental and institutional data. DDoS attacks followed closely with 130 incidents, indicating continued attempts to disrupt availability of public-facing services.

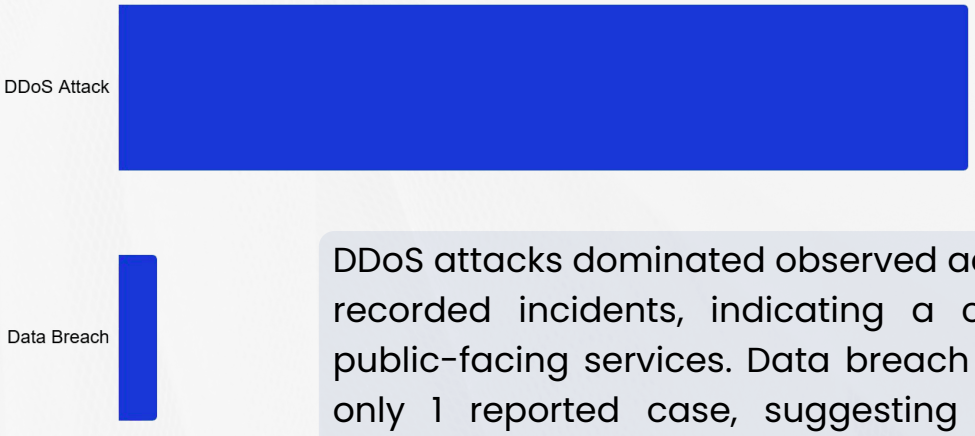
Ransomware incidents (91 cases) were observed at a meaningful level, reflecting a comparatively stronger presence of financially motivated threat activity. Initial access activities (34 incidents) remained less prevalent but continued to play a role in facilitating downstream attacks. Overall, the distribution suggests a more diversified threat landscape compared to predominantly disruption-focused environments.

On February 13, 2025, the ransomware group Medusa claimed to have obtained 84.40 GB of data from the Central District Health organization.

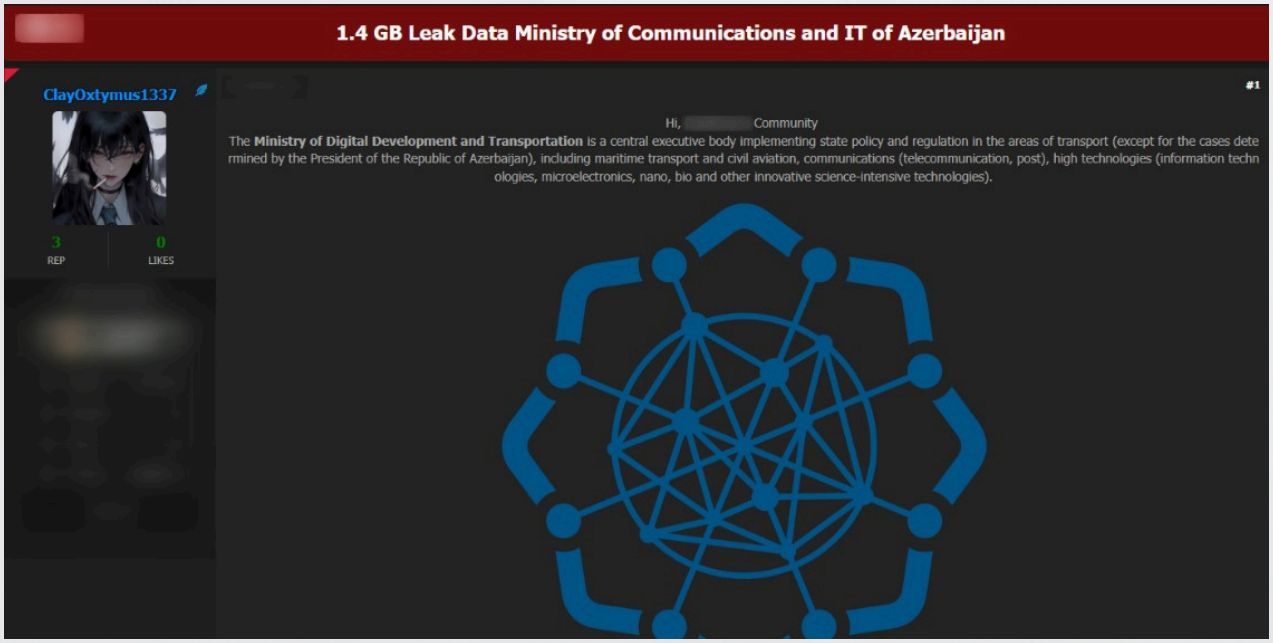
On March 13, 2025, a threat actor claimed to have leaked the database of the Department of Government Efficiency.

The compromised data reportedly includes last name, first name, display name, email address, and other related information.

AZERBAIJAN

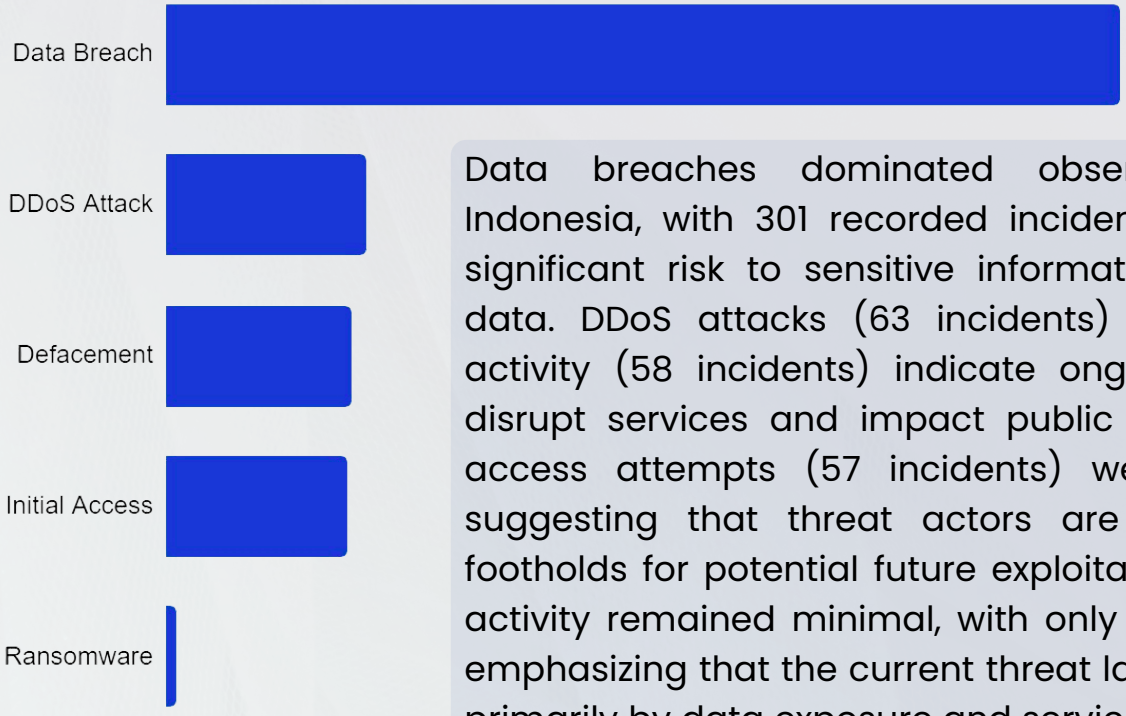


DDoS attacks dominated observed activity in Azerbaijan, with 23 recorded incidents, indicating a clear focus on disrupting public-facing services. Data breach activity was minimal, with only 1 reported case, suggesting that threats to sensitive information remain limited. Overall, the current threat landscape in Azerbaijan is primarily driven by availability-focused operations rather than data exfiltration or long-term compromise.



On June 10, 2025, a threat actor claimed to have breached 1.4 GB of data from the Ministry of Digital Development and Transport of Azerbaijan.

INDONESIA



Data breaches dominated observed activity in Indonesia, with 301 recorded incidents, highlighting a significant risk to sensitive information and personal data. DDoS attacks (63 incidents) and defacement activity (58 incidents) indicate ongoing attempts to disrupt services and impact public perception. Initial access attempts (57 incidents) were also notable, suggesting that threat actors are actively seeking footholds for potential future exploitation. Ransomware activity remained minimal, with only 3 cases reported, emphasizing that the current threat landscape is driven primarily by data exposure and service disruption rather than extortion campaigns.

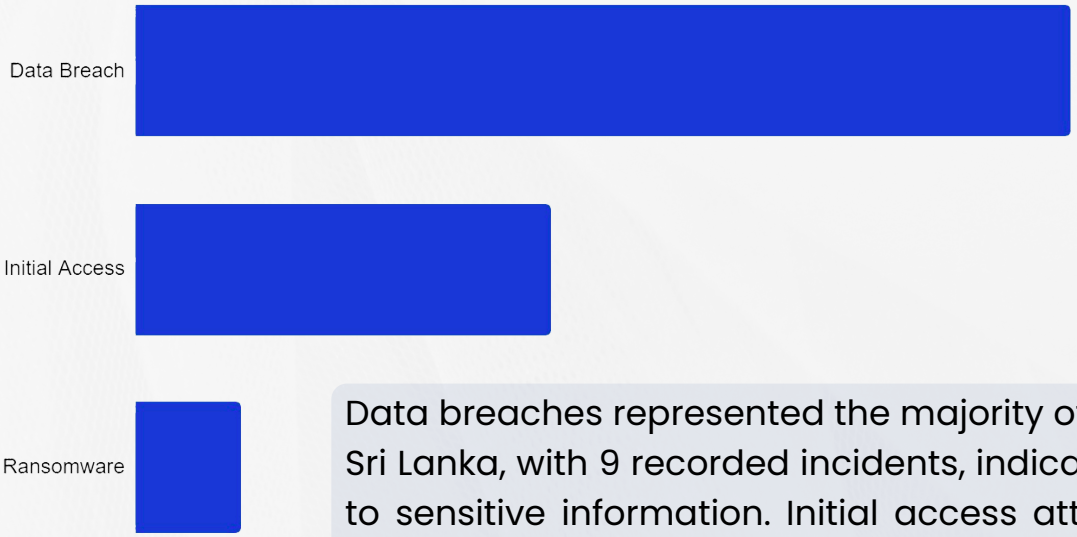
On November 20, 2025, a threat actor claimed to have leaked 1.56 GB of data from the Ministry of Cooperatives of the Republic of Indonesia.

The compromised data reportedly includes sensitive documents, such as financial reports, meeting records, and other related information.

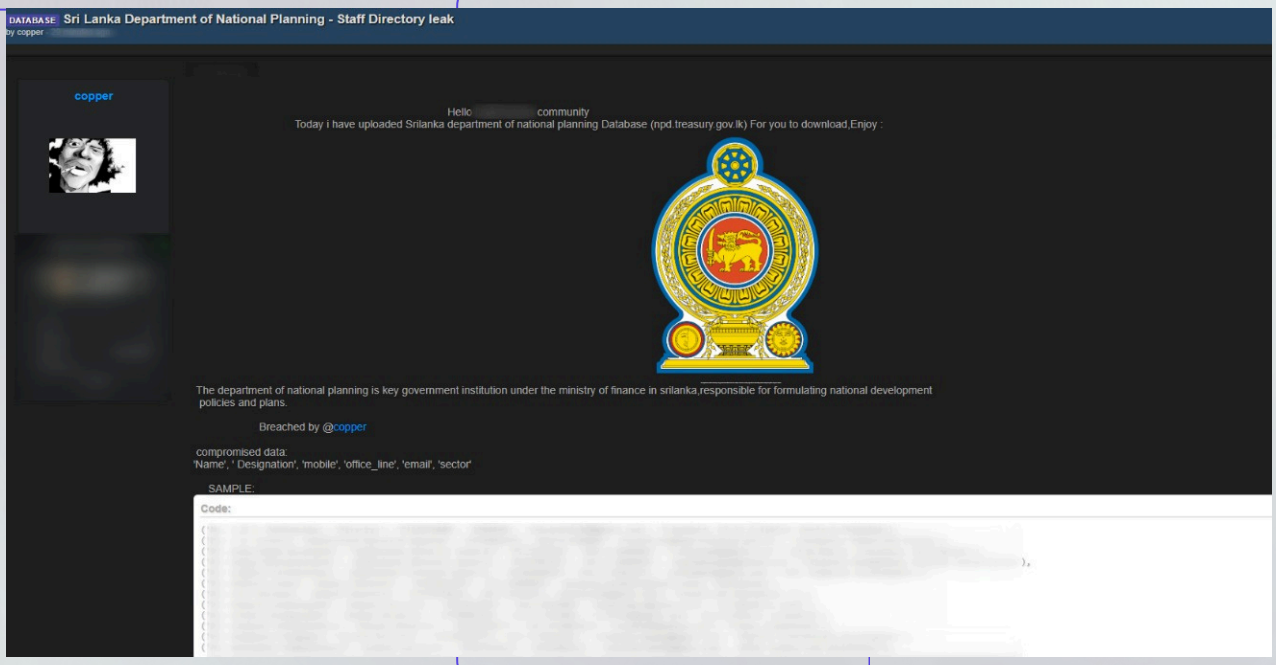
On November 1, 2024, a threat actor claimed to have leaked the database of SIKS (Social Welfare Information System).

The leaked data reportedly contains information such as name, email address, physical address, date of birth, PMKS ID, KK number, NIK, and other related personal information.

SRI LANKA

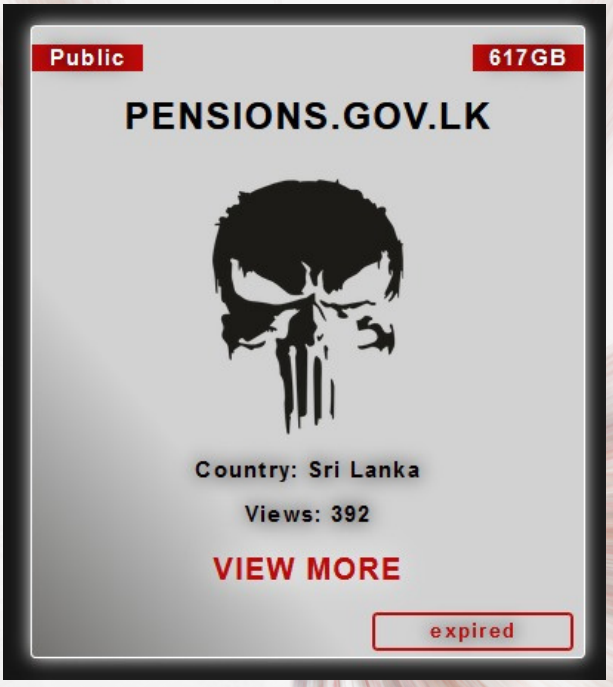


Data breaches represented the majority of observed activity in Sri Lanka, with 9 recorded incidents, indicating a moderate risk to sensitive information. Initial access attempts (4 incidents) were limited, suggesting minimal efforts to establish persistent footholds. Ransomware activity remained very low, with only 1 recorded case, highlighting that the current threat landscape in Sri Lanka is primarily driven by opportunistic data exposure rather than disruptive or extortion-based attacks.



On September 26, 2025, a threat actor claimed to have leaked a database from the National Planning Department (NPD) of Sri Lanka.

The compromised data reportedly includes name, designation, mobile number, office line, email address, and sector information.



On May 27, 2025, the Cloak group claimed to have obtained 617 GB of data from the Department of Pensions.

Government Sector Victimology and Statistical Distribution

When examining the rates at which Government institution accounts and identity information appear in infostealer-related data breaches at a global level, it was determined that the top five countries with the highest visibility are India, Indonesia, Brazil, Mexico, and Turkey, respectively. Differences between countries are significant based on normalized proportional values, and exposure levels within the infostealer ecosystem are directly related not only to the number of users but also to the security maturity of Government networks, identity management practices, and internal access habits within institutions.

This graph shows the frequency of Government institution domain names appearing in infostealer logs over the past year on a normalized scale. The dataset reveals the proportion of Government TLDs (gov, go, mil, gob, pol) from five countries appearing in infostealer-related leaks. According to the records provided, India has the highest density; gov.in domain names are detected significantly more often in infostealer logs compared to other countries. Indonesia ranks second, with go.id and mil.id domain names accounting for a high volume of total visibility.

Although Brazil, Mexico, and Turkey rank lower, the fact that logs belonging to the Government TLDs of these countries are in the millions shows that infostealer-related leaks are not limited to individual users; session, device, and identity information belonging to Government institutions has also become part of this ecosystem. The normalized distribution is used to compare overall visibility between countries, allowing for a more objective assessment of differences in raw data volumes.

This finding shows that infostealer threats affect government agencies on a global scale and that there is no significant geographical difference in the targeting of Government digital assets. Volume differences between countries are influenced by factors such as each country's level of digitalization, the intensity of online use of Government services, and the size of the user base. The analyzed records reveal that infostealer data constitutes a critical vulnerability area for Government institutions and that identity security, session management, and endpoint protection should be priority areas for assessment in the Government sector.

MITRE ATT&CK Techniques

Threat activity observed across the global government sector in 2025 aligns closely with well-defined MITRE ATT&CK techniques, particularly those associated with initial access, credential compromise, lateral movement, and impact. The following TTP patterns were most prominent:

Initial Access (TA0001)

Government networks were frequently targeted through:

- Phishing (T1566) — Highly tailored spearphishing campaigns by APTs and ransomware affiliates targeting ministries, defense institutions, and public service departments.
- Exploiting Public-Facing Applications (T1190) — Zero-day and n-day vulnerabilities in VPN appliances, CMS systems, and authentication platforms.
- Valid Accounts (T1078) — Widespread reuse of infostealer-exposed government credentials significantly enabled unauthorized access attempts.

Execution (TA0002)

Threat actors commonly used:

- PowerShell (T1059.001) and Command Shell (T1059.003) for scripted execution.
- Malicious Office Macros (T1204.002), especially in espionage-motivated campaigns distributing loader malware.

Persistence (TA0003)

Observed persistence mechanisms included:

- Registry Run Keys (T1547.001) in commodity malware deployments.
- Account Manipulation (T1098) through compromised admin and service accounts used by IABs and ransomware groups.

Privilege Escalation (TA0004)

Threat actors leveraged:

- Exploitation for Privilege Escalation (T1068) — Windows kernel and driver vulnerabilities.
- Token Impersonation/Theft (T1134) — Notably used to escalate from user-level access to administrative privileges.

Defense Evasion (TA0005)

Prominent techniques included:

- Obfuscated/Encrypted Files (T1027) for stealthy malware payloads.
- Masquerading (T1036) — Naming malicious binaries to resemble legitimate system files.
- Living off the Land (T1218, T1037) — Abuse of native tools such as CertUtil, WMI, and signed binaries.

Credential Access (TA0006)

Aligned with high infostealer activity:

- Credential Dumping (T1003) — LSASS memory extraction conducted by ransomware operators.
- Input Capture (T1056) — Infostealer families targeting browser-stored credentials and session tokens.

Discovery (TA0007) & Lateral Movement (TA0008)

Threat actors commonly used:

- Network Scanning (T1046) to map government infrastructure.
- Remote Services (T1021) including SMB, RDP, and SSH for lateral propagation.
- Pass-the-Hash (T1550.002) techniques observed particularly in ransomware intrusions.

Collection & Exfiltration (TA0009–TA0010)

- Data Staging (T1074) followed by Exfiltration Over Web Services (T1567.002) such as cloud storage platforms.
- Archive Collected Data (T1560) — Frequently used for preparing large-scale datasets for exfiltration.

Impact (TA0040)

The most prevalent impact techniques were:

- Network Denial of Service (T1498) — Dominant in DDoS-driven geopolitical campaigns.
- Data Encryption for Impact (T1486) — Central to ransomware operations targeting government systems.
- Defacement (T1491) — Used by hacktivists to affect public perception and institutional credibility.

Strategic & Tactical Recommendations

Government sector managers must immediately implement the following architectural and tactical changes to ensure operational continuity and counter identity-based breaches.

DDoS Protection Capacity Enhancement

- Contracts should be made with commercial DDoS mitigation services with network capacities exceeding 400 Tbps.
- This capacity should provide protection against hyper-volumetric attacks above 1 Tbps, and upstream mitigation should be mandatory in this context.

Application Layer (L7) Defense

- To reduce HTTP Flood attacks (59%), specialized Web Application Firewalls (WAF) should be implemented.
- WAFs should be configured with managed rule sets against known malicious bots.
- Aggressive rate limiting should be applied for APIs and login pages.

Network Layer (L3/L4) Automatic Mitigation in Attacks

- BGP Flowspec Implementation: BGP Flowspec, an automatic reduction mechanism in routers, should be used to prevent large-scale network layer attacks and prevent network congestion.
- SYN Protection: To prevent network infrastructure from being overwhelmed, SYN flood protection modes such as SYN cookies or SYN proxies should be enabled on edge devices.

Identity Verification Enhancement (PR-MFA)

- For all corporate accounts, Multi-Factor Authentication (MFA) resistant to phishing attacks, such as FIDO2/WebAuthn, which prevents stolen passwords from being used, should be mandatory.
- Conditional Access policies should be implemented for high-risk actions, requiring re-authentication.

Prevent Session Token Theft

- TPM Protection: Session tokens (e.g., PRTs) must be securely stored using the Trusted Platform Module (TPM) to protect against credential-stealing software.
- Conditional Access: Token Protection should be enabled through Conditional Access policies in solutions such as Microsoft Entra ID, and access should only be permitted from trusted, organization-affiliated devices.

Privileged Access Management Application

- All passwords and secrets for privileged users and systems must be managed in a centralized Privileged Access Management (PAM) solution compliant with FedRAMP or GovRAMP.
- This practice reduces the risk of credentials being compromised by removing them from endpoints.

Zero Trust Architecture and Micro-Segmentation

- The ZTA principles, which assume the network is always at risk, should be adopted quickly.
- To restrict lateral movement:

1. Micro-Segmentation: Strict micro-segmentation should be applied between critical network segments.
2. JIT and Least Privilege: Least Privilege and Just-in-Time Access (JIT) policies should be enforced.

Endpoint Protection and BYOD Management

- All devices accessing corporate resources (including BYOD) must have Endpoint Detection and Response (EDR) solutions enabled.
- Technologies such as Windows Defender Credential Guard should be enabled to isolate and protect credentials from the LSASS memory.

Conclusion

The 2025 data clearly shows that the public sector can no longer maintain its security by focusing on a single threat category. The structure of attacks observed throughout the year revealed that high-volume attacks creating operational pressure and lower-volume but highly effective infiltration campaigns were occurring simultaneously. Hacktivist groups, particularly politically motivated structures such as NoName057(16), targeted public portals, transportation authorities, and critical service infrastructures with large botnet-based DDoS waves. DDoS, as the most intense type of attack, kept the accessibility of public services under constant pressure.

Meanwhile, silent threats targeting identity and access security grew rapidly through Infostealer software and the Initial Access Broker ecosystem. Throughout 2025, millions of public-sector accounts circulating in these markets virtually eliminated the entry barrier for both ransomware groups and espionage-focused APT actors. This chain paved the way for data breaches where data was stolen and leaked, followed by double extortion models implemented by groups such as Medusa.

Additionally, state-sponsored APT groups, particularly actors like SideWinder, have been able to remain undetected in public networks for extended periods by combining classic vulnerability exploitation with modern obfuscation techniques and multi-stage loaders. APT operations continue to conduct persistent intelligence gathering activities across a wide spectrum, from diplomatic missions to defense institutions.

This entire picture—combined with the operational pressure created by high-volume DDoS attacks, the invisible risks posed by identity-centric attack chains, the persistent infiltration capabilities of APTs, and the expanding impact of ransomware operations—has placed the public sector at the center of a multi-layered and constantly evolving threat landscape. The overall assessment for 2025 clearly shows that it is now imperative for public institutions to establish a comprehensive security architecture that integrates identity security, vulnerability management, network resilience, and threat intelligence.

ThreatMon
Under Cyber Wings

More Information About ThreatMon

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*

Contact Us:

Email Address
team@threatmonit.io

https://x.com/MonThreat

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