Comprehensive Threat Report – May 2025

Executive Summary

By - Saptang Labs

In May 2025, the cybersecurity landscape saw a surge in hacktivist-driven cyberattacks, including data breaches, ransomware incidents, and widespread DDoS campaigns. Targets spanned sectors such as industrial manufacturing, insurance, aviation, and government ministries across Europe, Asia, and North America. DDoS attacks notably disrupted key government services in Lithuania, Poland, France, and India. The rise in politically and financially motivated attacks highlights growing risks to critical infrastructure and underlines the need for enhanced defense strategies.

Table of contents

Key Data Breaches: 3
Major Cyber Incidents:.. 3
Key Threats: 3
Threat Landscape.. 4
Ransomware Trends 4
DDOS 5
Underground Findings 6
Global Data Breaches and Leaks 6
Indian data leaks and breaches.. 8
Threat Actors 11
Threat Analysis 13
Notable Incidents 13
Prominent Vulnerabilities 16
Appendix.. 19
Glossary.. 19

Key Data Breaches:

1. **Iraq Ministry of Interior**: Selling over 4TB of personal and professional data of 650,000+ employees, including IDs, contact info, and job details from critical departments.
2. **CENEPRED-Peru**: The breached leaked a 4GB SQL database.
3. **Kenya National Social Security Fund**: Ransomware attack exposed around 2.5TB of sensitive data from the government agency managing social security and financial records.
4. **Avid Technology — USA**: The breach exposed over 10 million user records including contact details.
5. **Frisco Police Department — USA:** Selling detailed records of 90,000 law enforcement personnel, including personal info, contacts, IP addresses, supervisors, and training history.

Major Cyber Incidents:

1. **Coinbase Cyber Atatck**: Unauthorized access to internal systems and customer data confirmed; threat actor demands $20 million ransom.
2. **South African Airways Cyber Incident:** Disrupted website, mobile app, and internal systems causing temporary outages; confirmed by the airline.
3. **Uttar Haryana Bijli Vitran Nigam Cyberattack**: Website disruption stalled 50,000+ new electricity connection applications and affected technical services.
4. **INDIGO Group Cyberattack**: 1.5TB of data compromised, including sensitive business and customer info.

Key Threats:

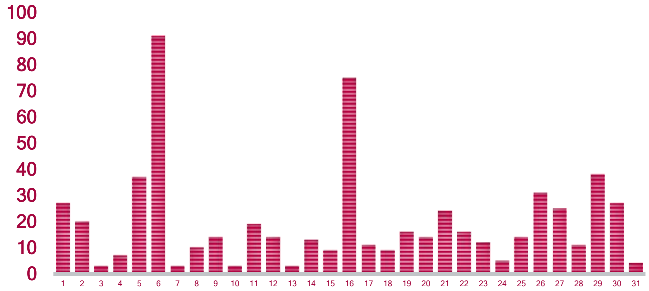
The key threats identified include critical vulnerabilities such as the path traversal and remote code execution flaw in Commvault Command Center (CVE-2025-34028), OS command injection in GeoVision devices (CVE-2024-6047) and DrayTek Vigor routers (CVE-2024-12987), and a stack-based buffer overflow affecting multiple Fortinet products (CVE-2025-32756). Additionally, a deserialization vulnerability in SAP NetWeaver (CVE-2025-42999) poses significant risks to system integrity.

Ransomware attacks also surged, particularly targeting sectors like government, airlines & aviation, and e-commerce & online stores. High-profile breaches, such as those affecting Ministry of Interior, Avid Technology, CENEPRED, and the National Social Security Fund, emphasize the growing threat and the need for stronger cybersecurity defences.

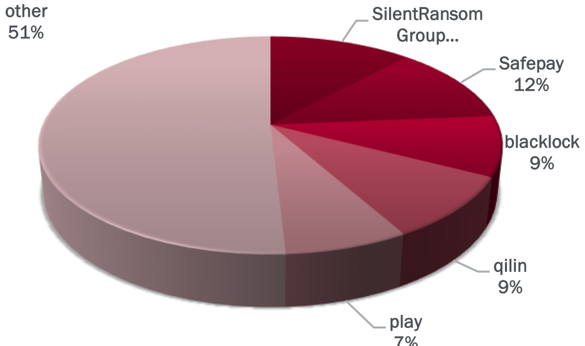
Threat Landscape

Ransomware attacks are happening more often and causing more trouble, while mobile malware takes advantage of how many people use smartphones and tablets. Both threats show that there is an urgent need to improve security measures.

Ransomware Trends



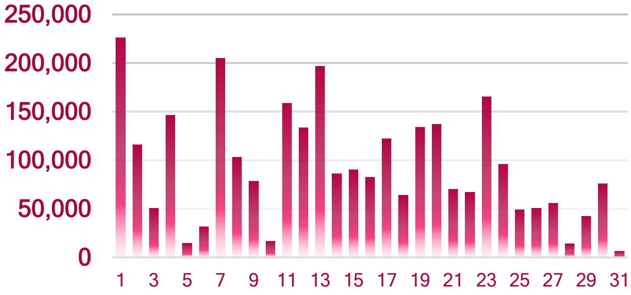
Victims per day



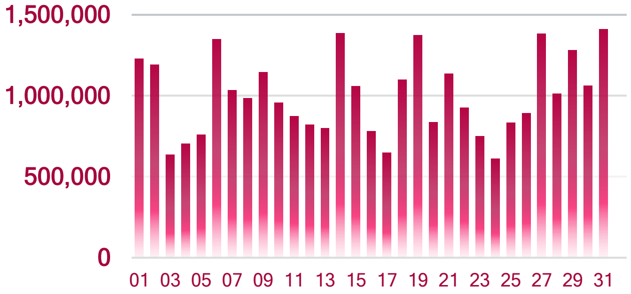
Victims by group

Incident Trends

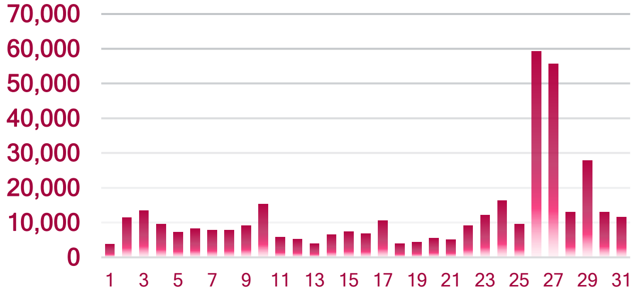
Exploits



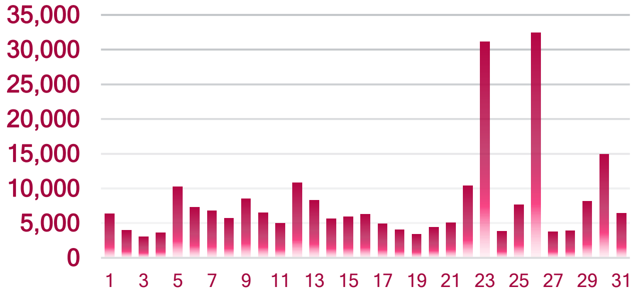
Malware



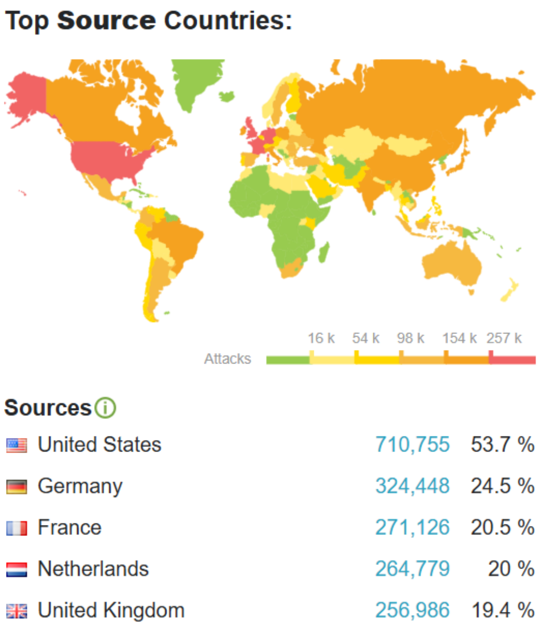
Mobile Threats



Coinminer



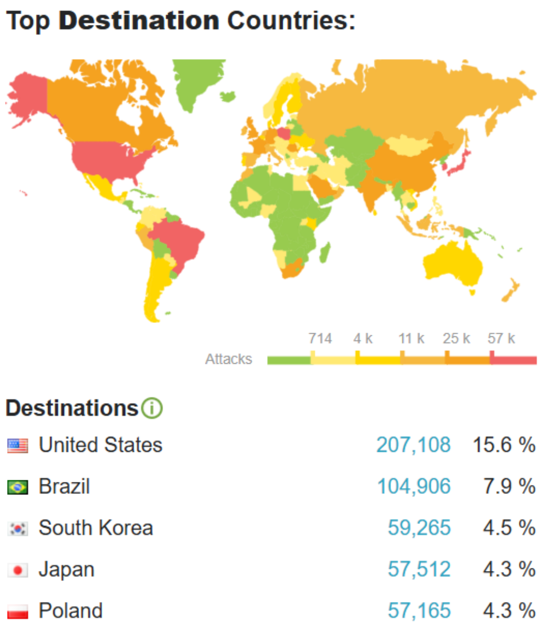
DDoS activity



Top **Source** Countries:

Sources

Sources		
United States	710,755	53.7 %
Germany	324,448	24.5 %
France	271,126	20.5 %
Netherlands	264,779	20 %
United Kingdom	256,986	19.4 %



Top **Destination** Countries:

Destinations

Destinations		
United States	207,108	15.6 %
Brazil	104,906	7.9 %
South Korea	59,265	4.5 %
Japan	57,512	4.3 %
Poland	57,165	4.3 %

Underground Findings

The findings listed below are among the critical datasets discovered on underground forums in April, 2025. Additionally, several threat actors are noted based on their prominent activities during this period.

Global Data Breaches and Leaks

Region	Organisation	Significant data
🇺🇸	US Bank	A threat actor known as **info_usa** is allegedly involved in the sale of a CSV file linked to a significant data breach affecting US Bank. The actor claims to have compromised approximately 12.1 million customer records spanning all U.S. states. The exposed data reportedly includes a wide range of sensitive personal and financial information, such as full names, Social Security Numbers, dates of birth, phone numbers, IP addresses, email addresses, physical addresses, banking details, and employment information.
🇸🇦	Technical and Vocational Training Corporation	A data breach has reportedly compromised the entire database of Saudi Arabia's Technical and Vocational Training Corporation, affecting 338,703 individuals linked to institutions such as technical colleges, industrial and construction institutes, prison training centers, and strategic partnership institutes. The exposed data includes national ID numbers, full names, dates of birth, email addresses, mobile numbers, and even plaintext passwords intended for use on the official TVTC portal. The breach was allegedly carried out by a threat actor identified as **NO8LO**, who claims to have directly extracted the data from TVTC systems and is promoting it for reconnaissance and exploitation purposes.
🇮🇶	Ministry of Interior	A threat actor known as **Q8300** is allegedly selling a massive dataset containing the personal and professional information of over 650,000 employees from Iraq's Ministry of Interior. The data, reportedly totaling more than 4TB and sourced directly from government systems, includes full names, national ID numbers, dates of birth, addresses, high-resolution ID and residency card images, contact details, emails, phone numbers, and extensive job-related information such as rank, department, work location, and hire dates. The breach affects personnel across key departments, including Counter Terrorism, Federal Police, Intelligence, Immigration, and Border Security. The dataset is being marketed for sale at a price of 10 BTC.

🇮🇩	Ciputra Group	Ciputra Group, a major player in the real estate industry in Indonesia, has reportedly become the latest victim of a cyberattack. A threat actor identified as **Betway** claims to have exfiltrated a dataset containing the personal information of approximately 600,000 users. The compromised data includes names, phone numbers, email addresses, and cities, and is currently being offered for sale for $500.
🇪🇸	Audax Renovables	Audax Renovables, a company operating in the civil engineering and construction sector in Spain, has reportedly suffered a significant data breach. A threat actor known as **Brainfuck** is claiming to sell the complete database of the organization, which allegedly contains around 300,000 personal records. The leaked data reportedly includes personally identifiable information such as names, addresses, phone numbers, email addresses, IBANs, and detailed contract data. Additionally, the actor claims to possess 1.2TB of highly sensitive documents, including electricity and gas contracts, scanned IDs and passports, bank account information, and tax documentation digitally signed via Logalty.
🇵🇪	CENEPRED	A threat actor known as **Cypher404x** has reportedly leaked a 4GB SQL database allegedly belonging to CENEPRED (Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres), a critical Peruvian government agency responsible for disaster risk estimation and prevention. The leaked data appears to contain SQL insert statements and structured content such as internal administrative documents and submission records extracted from the agency's system.
🇺🇸	Avid Technology	Avid Technology, a U.S.-based company in the content and collaboration software industry, has allegedly suffered a significant data breach, resulting in the exposure of over 10 million user records. The compromised dataset, reportedly extracted in May 2025, includes a wide range of sensitive information such as contact details, birthdates, departments, communication history, account roles, financial metrics, and mailing addresses. A threat actor known as **betway** has claimed responsibility for the breach, stating they accessed and exported the entire dataset from avid.com.
🇰🇪	National Social Security Fund	Kenya's National Social Security Fund (NSSF), the state agency tasked with delivering social security protection to the nation's workforce, has suffered a ransomware attack attributed to the threat actor **Devman**. The breach resulted in the compromise of approximately 2.5 terabytes of sensitive data, highlighting a major cybersecurity incident affecting a key government institution responsible for managing citizen welfare and financial records.

🇺🇸	Social Security	A threat actor known as Shinchan is selling a stolen database containing 1 million U.S. Social Security records along with associated driver's license information. The data includes highly sensitive personal and financial information such as full names, addresses, dates of birth, Social Security Numbers (SSNs), driver's license details, emails, phone numbers, income types, employer names, banking information (including routing and account numbers), and more. The seller claims the dataset totals one million records and is actively seeking buyers.
🇺🇸	Frisco Police Department	A dataset allegedly containing detailed records of approximately 90,000 U.S. law enforcement personnel has been listed for sale, with a particular focus on individuals affiliated with the Frisco Police Department in Texas. The exposed data reportedly includes extensive personal and professional information such as names, email addresses, alternate contact numbers, IP addresses, supervisor details, training history, and more. The breach was allegedly carried out by a threat actor known as Shinchan.

Indian data leaks and breaches

Organisation	**Significant data**
planet-itservices	A ransomware incident targeting the Indian technology company planet-itservices.com resulted in the compromise of two user accounts and the extraction of sensitive operational data. The attack, linked to the Raccoon infostealer malware, was publicly disclosed on May 21, 2025. A leak page included a screenshot of compromised internal content and a public claim URL, suggesting an avenue for potential negotiation or further data exposure. The breach has been attributed to the threat actor **safepay**.
TeamLease	TeamLease, an India-based business services provider, has reportedly been breached by the threat actor **NightSpire**, which claims to have exfiltrated about 100 GB of internal data. The leak now posted online contains information stolen with multiple infostealer tools, including Azorult, Raccoon, and RedLine, suggesting extensive data-exfiltration activity. According to the threat actor, the compromise affects more than 7,000 users and 54 third-party entities, undermining both employee privacy and partner security across associated domains and revealing a significant loss of operational integrity for the organization.
Ratna Sagar P Ltd	Indian publishing house Ratna Sagar Pvt. Ltd. has reportedly suffered a data breach allegedly carried out by the threat actor **J hacking**, which claims to have exfiltrated 38 GB of data. The company, known for producing educational books for children, is reported to have a revenue of approximately $64.9 million.

D'Decor Exports	On May 5, 2025, Indian home décor brand D'Decor fell victim to a ransomware attack executed by the **BrainCipher** threat actor. The breach led to the compromise of 350 GB of data, reportedly including internal documents and databases. Known for its premium textiles and furnishings, D'Decor's operations may face disruption due to file encryption and possible ransom demands.
Wilson International	Wilson International, an India-based global commodities trading firm specializing in the supply chain for fertilizer and petrochemical manufacturing, has suffered a major data breach following a cyberattack by the threat actor **Dire Wolf**. The breach resulted in the exposure of 159GB of sensitive data related to the chemicals and related products sector. Compromised files include legal documents, insurance contracts, claims history, business contracts, supplier files, email backups, and other confidential records.
Mizoram PSC	On the evening of May 15, 2025, a suspected cyberattack briefly disrupted the official website of the Mizoram Public Service Commission (MPSC). Around 10:00 PM, attackers defaced the MPSC homepage, displaying pro-Pakistan imagery and mocking Indian national symbols. The cyberattack was claimed by a group known as **Team Insane PK**. The MPSC website, a critical platform for civil service recruitment in Mizoram, hosts job notifications, application forms, exam schedules, and results. This temporary breach triggered concern among aspirants preparing for competitive examinations, highlighting vulnerabilities in state-level digital infrastructure.
I Paid A Bribe	I paid a bribe, a prominent Indian anti-corruption platform managed by the non-profit Janaagraha, has allegedly suffered a data breach attributed to the threat actor **frog**. The platform enables citizens to report incidents of bribery anonymously, making the breach especially serious due to the sensitive and potentially identifying information it holds. The exposed dataset reportedly contains 12,773 records in CSV format, including email addresses, timestamps, and other user identifiers.
Choksi Laboratories Limited	Choksi Laboratories Limited, a listed analytical testing and R&D laboratory firm based in Madhya Pradesh, has fallen victim to a ransomware attack. A threat actor breached the company's main server, encrypted all stored data, and left a ransom note stating: “Your data has been stolen. If you do not pay the ransom, then your data will be published by me.” The breach rendered all systems inoperable and exposed the organization to the risk of sensitive data being leaked if the ransom is not paid.
Saarathi.ai	Saarathi.ai, a fintech company providing digital onboarding and lending solutions to financial institutions in India, has allegedly become the target of a threat actor who exploited a misconfigured and publicly accessible storage bucket. The breach reportedly exposed around 500 GB of highly sensitive data, including Know Your Customer (KYC) documents and client records. This data leak has compromised the personal information of millions of individuals associated with public and private banks, insurance firms, and non-banking financial companies (NBFCs).

India Steel Expo	A threat actor is selling a database allegedly stolen from the India Steel Expo, containing detailed personal and professional information of attendees. The leaked dataset includes multiple .xlsx files such as registration_2015.xlsx, registration_2019.xlsx, registration_2020.xlsx, and electrical_invoice.xlsx, and exposes sensitive fields like full name, email address, phone and mobile numbers, fax, company name, designation, city, state, country, website, zip code, visitor number, registration date, and address details. Some records reference individuals from companies in Japan and India, including roles like "Assistant Manager" and "Owner." The database is being offered for $250.

Threat Actors

1. ThreeAM

ThreeAM is a ransomware threat actor behind a series of cyberattacks targeting organizations across various sectors in the United States. Notable victims include KKP.law, a legal services firm known for its client-focused solutions; Industrial Service Solutions, operating in the consumer services sector; Interstate Commercial Glass & Door, part of the commercial and residential construction industry; Desert Behavioral Health, a healthcare provider; and Texas Industrial Control Manufacturing, a company in the electronics industry. These attacks reflect ThreeAM's broad targeting strategy and continued activity across critical U.S. sectors.

2. Akira

Akira is a prolific threat actor linked to numerous high-impact data breaches across multiple sectors and countries. In the United States, AKIRA targeted Insight Pipe Contracting, a company specializing in trenchless maintenance services, exfiltrating approximately 7 GB of sensitive data including employee files, client information, financial audits, and internal agreements. In Belgium, construction firm Ghent Dredging suffered a breach resulting in the exposure of 16 GB of corporate and personal data. German manufacturing company Delignit AG was hit with a 24 GB data leak, including confidential client data, financial records, and documents tied to major clients like Mercedes Benz. In another major incident, U.S.-based law firm Murphy Pearson Bradley & Feeney faced a breach involving over 182 GB of sensitive data, including personal identification documents of employees and clients. Akira's campaign spans various industries globally, emphasizing its reach and aggressive targeting of high-value corporate data.

3. Qilin

Qilin is a threat actor linked to cyberattacks across a wide range of industries and countries. Victims include Elit'Avia, a major business aircraft services provider in Slovenia; Berko Pharmaceuticals and Chemical Industry Inc., a manufacturing firm in Turkey; Bestop, an automotive parts company in the United States; and Scelltech, a French company specializing in signage and maintenance services. Qilin's attacks span multiple sectors globally, reflecting a broad and persistent threat campaign.

4. NightSpire

NightSpire is a threat actor associated with a wave of targeted intrusions across diverse European industries. Its victims include Calçada Wines, a legacy winery in Portugal; Valentin Hotels & Resorts, a family-run hospitality group in Spain; Ertl Elektro Feldbach, an Austrian electronics specialist; and SIMALGA, a Spanish facility services company. These incidents highlight NightSpire's deliberate targeting of organizations holding extensive and valuable operational data.

5. STORMOUS

STORMOUS is a prolific cyber threat actor targeting the global hospitality and service sectors across various countries and industries. In the United Kingdom, they compromised The Watermans Arms, a riverside restaurant and bar, leaking 1 GB of data. In Turkey, they breached Crystal Hotels, a 5-star beachfront resort chain, and Nirvana Hotels, a luxury hotel brand, each with 40 GB of stolen data that included full names of hotel guests, internal and external email addresses, booking references, customer feedback, and internal communications. In the Czech Republic, AXXOS Hotels & Resorts, a national hospitality group managing multiple hotels and spas, suffered a breach involving 33 GB of data, including 2025 booking records and identity cards. These incidents highlight STORMOUS's widening attack surface across the hospitality, food services, and tourism industries in Europe, exploiting businesses where customer data and operational continuity are crucial.

6. Direwolf

In May 2025, threat actor Direwolf claimed responsibility for a series of cyberattacks targeting companies across various sectors. Victims include Singapore-based DataPost Pte Ltd, a secure data handling provider; Taiwan's kiwi86, an insurance database service; Italy's Qualitas Commercialisti Associati, a finance audit firm with 350GB of leaked data including customer and bank records; and SMV Thailand, a jewelry retailer hit with a 265GB breach exposing design files, financials, and customer data.

7. Safepay

Threat actor SafePay claimed responsibility for multiple cyberattacks targeting companies across the U.S. and Argentina. Victims include Labbeemint Inc., a Washington-based global mint exporter (15GB data leaked); Service Center Metals, a major U.S. aluminum products manufacturer (120GB leak); Ozarkah2o, the official site for Texas-based bottled water brand Ozarka; and Estudio LM from Argentina, an architectural and engineering firm, with 20GB of project-related data exposed.

8. Datacarry

Threat actor DataCarry has claimed responsibility for cyberattacks on several European companies. Victims include La Maison Liégeoise, a Belgian seller of Carlina tapioca; Executive Jet Support, a UK-based aviation services firm; Mammut Sports Group, a Swiss outdoor gear company; and Balcia Insurance, a Latvia-based insurer offering various non-life insurance products.

9. Play

Threat actor Play has claimed responsibility for cyberattacks targeting organizations across the U.S., Canada, Japan, and Sweden. Victims include Frederick's Machine & Tool Shop (Industrial Machinery & Equipment, US), WAT Supplies (Chemicals, Canada), Media Links (Communications Equipment, Japan), and AKJ Energiteknik AB (Heating Contractor, Sweden), with the latter breach including screenshots potentially showing internal documents or technical data related to operations.

10. Dark Storm

The threat actor Dark Storm Team has claimed responsibility for a wave of distributed denial-of-service (DDoS) attacks targeting multiple government and public websites across several countries. In Lithuania, they allegedly disrupted websites of 14 ministries including the Ministries of Defence, Foreign Affairs, Justice, and Health, as well as the Panevėžys City Municipality. Additional targets include the National Portal of India, SoundCloud, Rouen and Chalon Airports in France, and the Polish Prime Minister's site along with gov.pl, Poland's official government portal.

Threat Analysis

Notable Incidents

- **Coinbase Faces $20M Ransom Demand:** On May 11, 2025, Coinbase, the largest cryptocurrency exchange in the United States, received an unsolicited email from an unknown threat actor. The email claimed access to internal systems and sensitive personally identifiable information (PII) of a subset of customers. Coinbase confirmed the breach, stating that unauthorized users accessed internal company documents and customer data. The threat actor demanded a $20 million ransom in exchange for not publicly leaking the stolen information.

- **Pearson Suffers Global Data Breach:** Pearson, a UK-based education giant and one of the world's largest providers of academic publishing and digital learning tools, has suffered a cyberattack. The incident resulted in unauthorized access to corporate data and customer information. Pearson, which serves schools, universities, and individuals in over 70 countries, confirmed the breach impacted both internal systems and clients across its global network.

- **Cyberattack Disrupts South African Airways' Services and Internal Systems:** On May 3, 2025, South African Airways (SAA), the national flag carrier of South Africa, experienced a significant cyber incident that disrupted its website, mobile application, and several internal operational systems. The breach caused temporary service outages and prompted immediate response measures by the airline. The company officially confirmed the incident on May 6, 2025.

- **Legal Aid Agency Cyberattack:** On May 19, 2025, the UK's Legal Aid Agency (LAA) confirmed that a recent cyberattack was significantly more severe than initially believed. An investigation revealed that threat actors had accessed and stolen a substantial amount of sensitive data belonging to legal aid applicants dating back to 2010. The compromised information includes criminal records, personal details (such as addresses, dates of birth, and national ID numbers), and financial data (including contributions, debts, and payment records). The breach forced the agency to shut down its online services to mitigate further risk.

- 🇩🇰 **Arla Foods Disrupts Production at German Facility:** Arla Foods, a Danish multinational dairy cooperative, has confirmed a cyberattack that disrupted production operations at its facility in Upahl, Germany. The incident, which impacted the local IT network, has caused delays and potential cancellations in product deliveries. Arla Foods, a farmer-owned cooperative with 7,600 members and 23,000 employees across 39 countries, produces well-known brands including Arla, Lurpak, Puck, Castello, and Starbucks dairy products. The company generates an annual revenue of €13.8 billion and serves customers in 140 countries.

- 🇮🇳 **Cyberattack Disrupts UHBVNL:** On May 7, 2025, the official website of Uttar Haryana Bijli Vitran Nigam Limited (UHBVNL) was targeted in a cyberattack, severely disrupting services for new electricity consumers. As a result of the incident, over 50,000 new connection applications have been stalled, and other technical services remain non-functional. The breach has caused significant inconvenience to consumers.

- 🇻🇪 **GlobalX Charter Airline Hit by Cyberattack:** Charter airline GlobalX, known for its role in deportation flights during the Trump administration—particularly involving Venezuelan migrants—has suffered a cyberattack allegedly carried out by individuals claiming affiliation with Anonymous. The attackers defaced a GlobalX subdomain, condemning the airline's involvement in controversial deportations. Beyond defacement, the breach involved the theft of sensitive data, including flight logs, passenger lists, and itinerary details spanning from January 19 to May 1. The leaked data reportedly aligns with official ICE flight logs and court documents, exposing deportation operations that included individuals actively contesting removal orders mid-flight. The breach was allegedly enabled by the discovery of a GlobalX developer's token, which led to the compromise of AWS access and secret keys, granting entry to the firm's cloud storage.

- 🇷🇺 **4B1D Target Russian Lecardo Clinic:** In May 2025, Lecardo Clinic, a private hospital in the Russian republic of Chuvashia, suffered a major cyberattack that disrupted operations for three days. The attack, claimed by the pro-Ukraine hacker group 4B1D, targeted the clinic's patient management software, allegedly gaining access through the compromised account of the clinic's director. The hackers reported wiping servers, deleting backups, encrypting and exfiltrating patient data, and disabling over 100 computers. They also leaked sensitive records, including an X-ray and personal data of approximately 52,000 patients and staff, with around 2,000 records reportedly sold.

- 🇫🇷 **Indigo Group Data Breach:** In May 2025, INDIGO Group, a prominent company engaged in parking management and urban mobility services in France, suffered a significant cyberattack that reportedly compromised 1.5TB of data. The breach, discovered on May 19 at approximately 23:17, was claimed by the threat actor Worldleaks, who alleged the exfiltration of over 1.14 million files. The stolen data likely includes sensitive business information and personal customer details. Leaked materials may feature internal documents, system screenshots, and operational data.

- 🇰🇷 **Dior South Korea Website Hit by Cyber Attack:** The House of Dior, the renowned French luxury fashion brand, has reported a cybersecurity incident affecting its South Korean website. An unauthorized external party gained access to customer data, prompting breach notifications. Reports indicate that Chinese customers may also be impacted. Exposed data includes full names, gender, phone numbers, email addresses, postal addresses, and purchase histories.

Prominent Vulnerabilities

These are the prominent and most exploited vulnerabilities in the month of March.

1. **CVE-2025-34028 | Commvault Command Center Path Traversal Vulnerability CVSS: 10.0**

   CVE-2025-34028 is a path traversal vulnerability in Commvault Command Center Innovation Release versions 11.38.0 to 11.38.20. It allows an unauthenticated attacker to upload ZIP files containing malicious JSP install packages, which when expanded by the server, can lead to remote code execution. The issue is fixed in versions 11.38.20 (with SP38-CU20-433 and SP38-CU20-436) and 11.38.25 (with SP38-CU25-434 and SP38-CU25-438).

2. **CVE-2024-6047 | GeoVision Devices OS Command Injection Vulnerability CVSS: 9.8**

   CVE-2024-6047 affects certain End-of-Life (EOL) GeoVision devices that improperly filter user input in specific functionality. This vulnerability allows unauthenticated remote attackers to inject and execute arbitrary system commands on the affected devices.

3. **CVE-2025-32756 | Fortinet Multiple Products Stack-Based Buffer Overflow Vulnerability CVSS: 9.8**

   CVE-2025-32756 is a stack-based buffer overflow vulnerability (CWE-121) affecting multiple Fortinet products, including FortiVoice, FortiRecorder, FortiMail, FortiNDR, and FortiCamera. A remote, unauthenticated attacker can exploit this flaw by sending specially crafted HTTP requests with a malicious hash cookie, potentially leading to arbitrary code or command execution. Affected versions include FortiVoice 7.2.0, 7.0.0–7.0.6, 6.4.0–6.4.10; FortiRecorder 7.2.0–7.2.3, 7.0.0–7.0.5, 6.4.0–6.4.5; FortiMail 7.6.0–7.6.2, 7.4.0–7.4.4, 7.2.0–7.2.7, 7.0.0–7.0.8; FortiNDR 7.6.0, 7.4.0–7.4.7, 7.2.0–7.2.4, 7.0.0–7.0.6; and FortiCamera 2.1.0–2.1.3, all 2.0 and 1.1 versions.

4. **CVE-2024-12987 | DrayTek Vigor Routers OS Command Injection Vulnerability CVSS: 9.8**

   CVE-2024-12987 is a critical vulnerability in the Web Management Interface of DrayTek Vigor2960 and Vigor300B running firmware version 1.5.1.4. It allows remote attackers to perform OS command injection via the session parameter in the /cgi-bin/mainfunction.cgi/apmcfgupload endpoint. The flaw can be exploited remotely, and public exploit code is available.

5. **CVE-2025-42999 | SAP NetWeaver Deserialization Vulnerability CVSS: 9.1**

   VE-2025-42999 is a vulnerability in SAP NetWeaver Visual Composer Metadata Uploader that allows a privileged user to upload untrusted or malicious content. When this content is deserialized, it can potentially compromise the confidentiality, integrity, and availability of the host system.

6. **CVE-2025-4428 | Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability**
CVSS: 8.8

CVE-2025-4428 is a vulnerability in the API component of Ivanti Endpoint Manager Mobile 12.5.0.0 and earlier versions that allows authenticated attackers to execute arbitrary code remotely via specially crafted API requests. The issue affects unspecified platforms and can lead to full remote code execution.

7. **CVE-2023-38950 | ZKTeco BioTime Path Traversal Vulnerability**
CVSS: 7.5

CVE-2023-38950 is a path traversal vulnerability in the iclock API of ZKTeco BioTime v8.5.5 that allows unauthenticated attackers to read arbitrary files on the server by sending specially crafted payloads, potentially exposing sensitive system information.

8. **CVE-2025-30400 | Microsoft Windows DWM Core Library Use-After-Free Vulnerability**
CVSS: 7.8

CVE-2025-30400 is a use-after-free vulnerability in Windows Desktop Window Manager (DWM) that allows a locally authorized attacker to elevate privileges. Successful exploitation could enable the attacker to execute code with higher system privileges.

9. **CVE-2025-30397 | Microsoft Windows Scripting Engine Type Confusion Vulnerability**
CVSS: 7.5

CVE-2025-30397 is a type confusion vulnerability in the Microsoft Scripting Engine that allows an unauthorized attacker to execute code remotely over a network. This flaw enables remote code execution by exploiting improper handling of resource types.VE-2018-9276 is a critical OS command injection vulnerability affecting PRTG

10. **CVE-2025-27920 | Srimax Output Messenger Directory Traversal Vulnerability**
CVSS: 7.2

CVE-2025-27920 is a directory traversal vulnerability in Output Messenger versions before 2.0.63, caused by improper handling of file paths. Attackers could exploit this flaw by using ../ sequences in parameters to access files outside the intended directory, potentially exposing configuration files or enabling arbitrary file access.

Top Initial Access ATT&CK TTPs

1. **Phishing:** ATT&CK Technique: **T1566**, Tactic: **TA0001** (Initial Access)

   Phishing tricks victims into revealing sensitive information or installing malware. It includes:

   T1566.001 - Spearphishing Attachment: Targeted emails with malicious attachments or links.
   T1566.002 - Spearphishing Link: Links to fake sites designed to steal credentials.
   T1566.003 - Spearphishing via Service: Deceptive messages on social media.
   T1566.004 – Spearphishing Voice: Highly targeted attacks on high-profile individuals.

2. **Exploit Public-Facing Application:** ATT&CK Technique: **T1190**, Tactic: **TA0001** (Initial Access)

   Adversaries exploit vulnerabilities in Internet-facing systems, such as web servers, databases, or cloud applications, to gain initial network access. They may also target edge devices with weak defenses or misconfigurations. Exploits can lead to broader access through compromised infrastructure or weak access controls.

3. **Supply Chain Compromise:** ATT&CK Technique: **T1195**, Tactics: **TA0001** (Initial Access)

   Supply chain compromise involves manipulating products or their delivery mechanisms to achieve data or system compromise. This can occur at various stages, including software and hardware, by manipulating development tools, source code, or distribution channels.

   Sub-techniques:
   T1195.001 - Compromise Software Dependencies and Development Tools
   T1195.002 - Compromise Software Supply Chain
   T1195.003 - Compromise Hardware Supply Chain

4. **Trusted relationship:** ATT&CK Technique: **T1199**, Tactic: **TA0001** (Initial Access)

   Malicious actors often infiltrate an organization by targeting its partners and contractors. If a partner is compromised, attackers can use their access points and tools to breach the organization. In practice, they frequently target IT subcontractors (like MSPs, authentication providers, and technical support specialists) who have administrative access to the organization's systems.

5. **Valid Accounts:** ATT&CK Technique: **T1078**, Tactic: **TA0001** (Initial Access)

   It involves attackers using stolen or compromised credentials to gain initial access to systems or networks. They may obtain these accounts through methods like phishing or credential dumping, allowing them to bypass security controls and move laterally within the network.

Appendix

Glossary

DDoS	Distributed Denial of Service
VM	Virtual Machine
POC	Proof of Concept
TIDE	Think-Tank for Information Decision and Execution Superiority
CVE	Common Vulnerabilities and Exposures
ATT&CK TTPs	Adversarial Tactics, Techniques, and Common Knowledge's Tactics, Techniques, and Procedures
IOC	Indicator of compromise
NATO	North Atlantic Treaty Organization
USAID	United States Agency for International Development
SSH	Secure Shell
SNMP	Simple Network Management Protocol