Comprehensive Cyber Threat Report – April 2025: Emerging Risks, Attack Trends, and Security Insights

Date: April 30, 2025
Saptanglabs.com

Executive Summary

In April 2025, global cybersecurity faced a surge in data breaches, ransomware attacks, and critical vulnerabilities. High-profile incidents hit sectors like government, healthcare, aviation, and e-commerce—most notably breaches at TAV Havalimanları, WooCommerce, and DaVita Inc. Public institutions in Indonesia, Nepal, and Malaysia also suffered major data leaks. Critical software flaws in platforms like Apache Tomcat and Cisco Smart Licensing added to the threat landscape. The month underscored the growing scale and impact of cyberattacks, reinforcing the urgent need for stronger security measures and rapid vulnerability management.

Table of contents

Overview

In April 2025, the cybersecurity landscape experienced notable data breaches, leaks, and vulnerabilities. High-profile incidents across various sectors revealed significant risks and exposed sensitive information.

Key Data Breaches:

1. **TAV Havalimanları —Turkey**: The breach involved 75 GB of data, including airport blueprints, personnel records, contracts worth €2.4 million.
2. **Ministry of Transportation of Indonesia**: The breach exposed a database 14,271 employees 6.51MB CSV.
3. **Province Public Service Commission of Nepal**: Over 800,000+ sensitive files, including facial images, signatures, and ID cards.
4. **WooCommerce - USA**: The breach exposed 4.4 million customers and businesses, including emails, addresses, social media profiles, financials, and employee details.
5. **Jabatan Perdana Menteri of Malaysia:** Leaks 270GB of Data Including Logistics Files.

Major Cyber Incidents:

1. **DaVita Inc. Hit by Ransomware Attack**: Hacker stole 510GB of Data Compromised, Disrupts 2,600 U.S. Outpatient Centers.
2. **Manchester Credit Union Breached**: Hackers stole 6GB of Data Exfiltrated, including files and SQL databases.
3. **SK Telecom Suffers Cyberattack**: Stole Sensitive Customer Data, Target USIM Information.
4. **Ransomware Attack on Municipality of Ardon**: A ransomware attack exposed 30 GB of Data.

Key Threats:

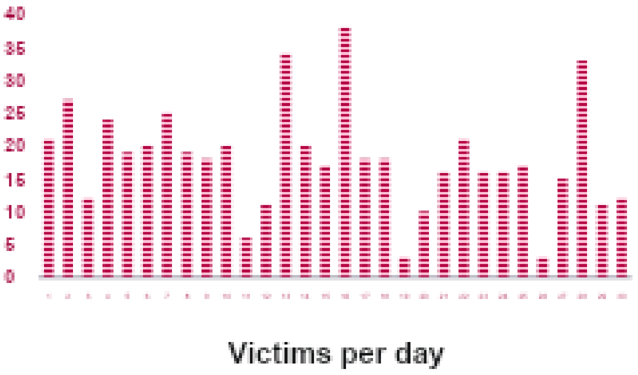
In April 2025, notable vulnerabilities included **CVE-2025-1316** (Edimax IC-7100 IP Camera OS Command Injection Vulnerability), **CVE-2024-20439** (Cisco Smart Licensing Utility Static Credential Vulnerability), **CVE-2025-24813** (Apache Tomcat Path Equivalence Vulnerability), **CVE-2025-22457** (Ivanti Connect Secure, Policy Secure and ZTA Gateways Stack-Based Buffer Overflow Vulnerability) and **CVE-2025-30406** (Gladinet CentreStack and Triofox Use of Hard-coded Cryptographic Key Vulnerability).

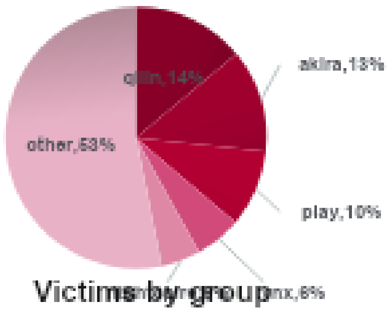
Ransomware attacks also surged, particularly targeting sectors like government administration, airlines & aviation, and e-commerce & online stores. High-profile breaches, such as those affecting Ministry of Transportation, WooCommerce, and the TAV Havalimanları, emphasize the growing threat and the need for stronger cybersecurity defences.

Threat Landscape

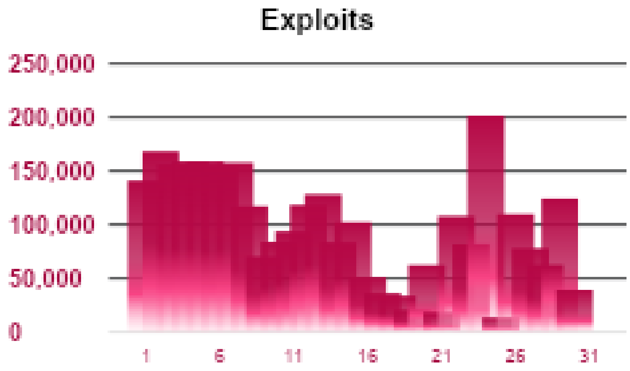
Ransomware attacks are happening more often and causing more trouble, while mobile malware takes advantage of how many people use smartphones and tablets. Both threats show that there is an urgent need to improve security measures.

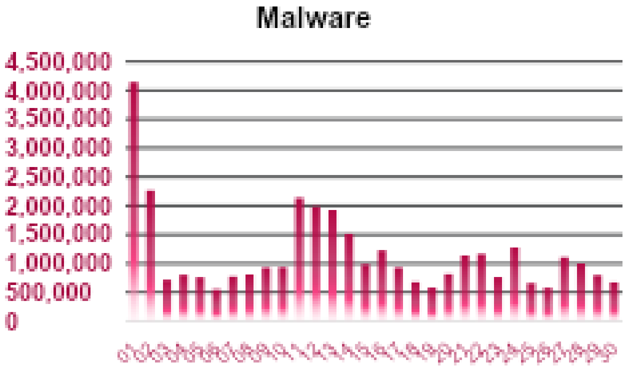
Ransomware Trends

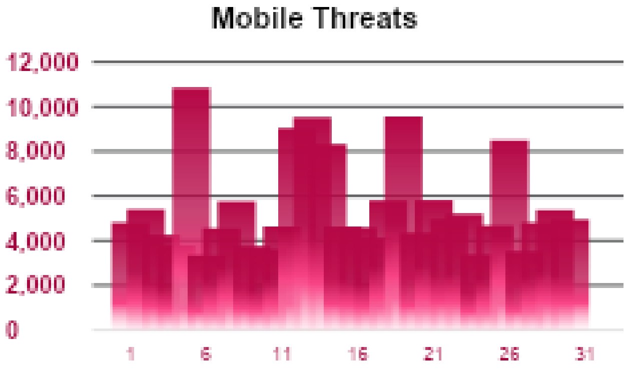


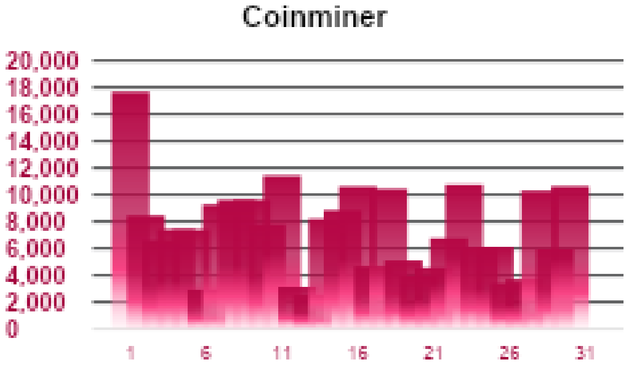


Incident Trends

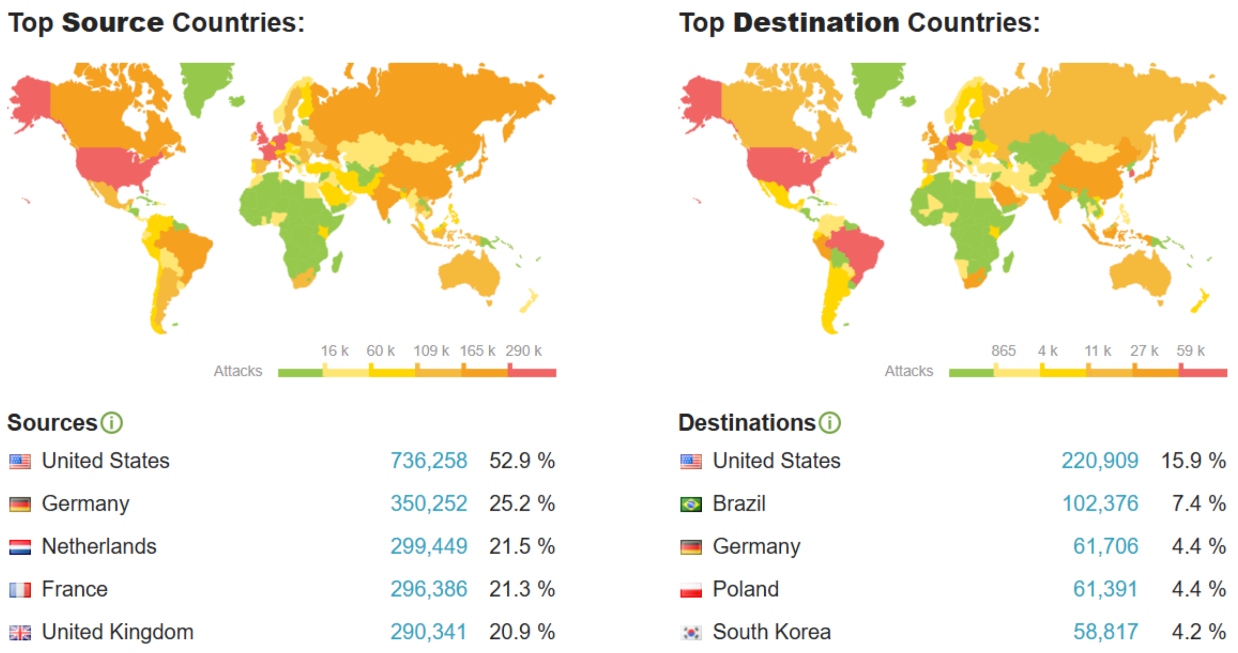








DDoS activity



Top **Source** Countries:

Sources		
United States	736,258	52.9 %
Germany	350,252	25.2 %
Netherlands	299,449	21.5 %
France	296,386	21.3 %
United Kingdom	290,341	20.9 %

Top **Destination** Countries:

Destinations		
United States	220,909	15.9 %
Brazil	102,376	7.4 %
Germany	61,706	4.4 %
Poland	61,391	4.4 %
South Korea	58,817	4.2 %

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
🇹🇷	TAV Havalimanları	The threat actor known as **Sentap** breached the systems of TAV Havalimanları, resulting in the exfiltration of 75 GB of highly sensitive data connected to the Esenboğa Airport Expansion Project in Ankara, Turkey. The dataset includes technical and operational documents such as official correspondences between TAV and DHMİ, blueprints for airport infrastructure (including taxiways, aprons, and technical blocks), and structural test results conforming to international standards (e.g., ACI 318, NFPA, ICAO Annex 14). Additionally, the leak contains sensitive personnel data (IDs, medical records, and addresses), financial and legal contracts (including project agreements exceeding €2.4 million for electrical and IT works), full Gantt charts and progress reports (up to July 2023), and quality assurance documents for materials like epoxy and polyurethane coatings. Applications of this data span reverse engineering, targeted exploitation, competitive intelligence, and system vulnerability assessments. Data samples for verification include blueprints, concrete test reports, medical records, and financial documents. Sentap has offered 20% of the dataset for sample access.
🇺🇸	WooCommerce	WooCommerce, an open-source e-commerce plugin for WordPress, is widely adopted by small to large-sized merchants and powers over 4.4 million websites globally as of April 2025. Known for its flexibility and ease of use, WooCommerce supports a substantial share of the online retail ecosystem. A recent data breach linked to WooCommerce has been claimed by the threat actor known as **Satanic**. The actor alleges unauthorized access to a vast trove of over 4.4 million unique customer records and detailed data from more than 4.4 million businesses. The compromised dataset includes emails, phone numbers, physical addresses, social media profiles, and LinkedIn IDs of customers, along with comprehensive company information such as SEO metrics, domain and hosting details, financial figures (revenue, net income, operating income), and employee details. This data, reportedly sourced through a third-party breach, is being sold via private Telegram channels, with samples provided to potential buyers.
🇪🇸	Naturgy Energy Group	Naturgy Energy Group S.A., a leading energy and utilities provider in Spain, has been linked to an alleged data breach involving the sale of a sensitive customer database. The threat actor **Crocs** has claimed responsibility, stating that the database

		contains 2.5 million rows of personally identifiable information (PII) along with detailed energy usage data. The dataset is being offered under a one-time sale condition, with the actor demanding $7,500 worth of cryptocurrency for exclusive ownership.
	3ipe	3ipe, a prominent infrastructure engineering firm with operations across Peru, Chile, Brazil, and Uruguay, has reportedly been targeted in a major cyberattack by the threat actor **Sentap**. The threat actor claims to be selling a 568 GB dataset allegedly exfiltrated from the company's internal systems. The data reportedly includes technical documentation, bidding contracts, airport and civil infrastructure project files, HR archives, geospatial maps, and marketing media, with contents in both English and Spanish. Marketed as exclusive and never-before-leaked, the dataset is being offered for $12,000 in Monero.
	Indonesian Ministry of Transportation	A threat actor known as **BanyuwangiXploit** claims to have leaked the personal data of 14,271 employees from the Ministry of Transportation of the Republic of Indonesia. The alleged dataset, reportedly shared for free, is described as an act of defiance against the government. According to the claims, the data is in CSV format, totals 6.51MB in size, and is linked to the official website of the ministry.
	Jabatan Perdana Menteri	An alleged data breach has targeted Malaysia's Prime Minister's Department (Jabatan Perdana Menteri), with the threat actor **R00TK1T** ISC CYBER TEAM claiming responsibility. The threat actor asserts that it has breached the department's network and exfiltrated over 270GB of data. As part of the disclosure, a folder related to the logistics and facilities sector has already been leaked, with the threat actor announcing plans to release the remaining files throughout the week.
	Asiacell	A threat actor known as **None0fyourbuS** has claimed to have shared a massive database allegedly exfiltrated from Asiacell, a major telecommunications provider in Iraq. The alleged leak reportedly exposes the personal records of over 10 million individuals, including full names, phone numbers, ID numbers, and other sensitive information.
	Province Public Service Commission	A threat actor named **kazu** is selling access to over 800,000 sensitive files from the Province Public Service Commission (PPSC) of Bagmati Province, Nepal. The breach reportedly includes facial images, signatures, and front/back copies of citizenship ID cards, impacting more than 200,000 users. The asking price for the stolen data ranges from $0 to $2000.
	Wolters Kluwer	Wolters Kluwer, a Dutch financial software giant generating nearly $7 billion annually and serving numerous US accounting firms, banks, and Fortune 500 companies, has reportedly been targeted in a data breach. The leaked data, estimated to range between 3GB and 6GB, allegedly includes full names, email addresses, phone numbers, residential addresses, job and university details, social media accounts, and tokens.

🇲🇾	Construction Industry Development Board	The threat actor **R00TK1T** claims to have breached the Construction Industry Development Board (CIDB) Malaysia, compromising 482GB of sensitive data. The stolen information reportedly includes confidential documents, sensitive accounts, and internal blueprints.

Indian data leaks and breaches

Organisation	**Significant data**
Zed Pay	A threat actor claims to have obtained a database from zbazaarsolutions.com, the online platform of Zed Pay, an India-based financial services provider. The alleged breach reportedly exposes personal information of approximately 1.5 million unique users, with account activation dates spanning January 2024 to December 2024. The leaked data is said to include full names, email addresses, phone numbers, and plaintext passwords. The database is being offered for $900 USD.
DealPlexus	DealPlexus is an Indian financial marketplace platform that connects individuals, businesses, and financial professionals. A threat actor identified as **RuskiNet** claims to have breached the platform's database, allegedly compromising records of 28,830 users. According to the actor, the stolen data includes identity details, names, email addresses, phone numbers, educational and professional qualifications, organization details, verification codes, and more. The threat actor has reportedly demanded a ransom and set a three-day deadline for compliance.
State Bank of India	The threat actor **mr_jack311** claims to have leaked sensitive personal information belonging to 15 million customers of State Bank of India (SBI), one of the country's largest banking institutions. The alleged breach reportedly includes data such as dates of birth, contact information, and Permanent Account Numbers (PANs).
BajajCapital	BajajCapital is one of India's oldest and most established fintech companies, offering a wide range of financial services including investment, insurance, and wealth management solutions. A threat actor known as **GreyMan** has allegedly claimed to possess and sell a vast collection of sensitive data from the company. According to the actor, the stolen data includes multiple databases, customer Know Your Customer (KYC) records, insurance policy documents, source code, internal documents, and third-party vendor credentials. The leak reportedly contains around 2 million KYC records featuring Aadhaar numbers, PANs, and cancelled cheques, along with 1 million car and bike insurance policy PDFs. The threat actor also claims to have access to the source code of all BajajCapital projects.
Mapaex	Mapaex, an India-based CDMO (Contract Development and Manufacturing Organization) specializing in healthcare and wellness products, has reportedly fallen victim to a ransomware attack carried out by the Qilin threat actor. The compromised data, totaling 143 GB, allegedly includes financial records, employee details, and other confidential information. The stolen data is expected to be published on April 20, 2025.

BuyAntiVirusKey	A threat actor claims to be selling a database allegedly exfiltrated from BuyAntiVirusKey.com, an India-based platform. The reported breach includes over 360,000 user records and more than 500,000 antivirus license keys—both used and unused. The exposed data consists of emails, MD5-hashed passwords, full license keys, registration dates, and customer names, raising concerns over software piracy, credential-stuffing attacks, and potential fraud.
Dhoot Transmission	Dhoot Transmission, an India-based manufacturer and supplier of automotive components to OEMs, has reportedly been targeted in a ransomware attack by the **Qilin** threat actor. The compromised data, amounting to 319 GB across 228,438 files, was listed on April 7, 2025. The exposed files allegedly include internal documents and proprietary manufacturing data related to wire harnesses, electronics, copper wire enamelling, tooling components, stamping components, moulding parts, and cable components used in two-wheelers and other vehicles.
Panjab University	Panjab University, a prestigious higher education institution located in Chandigarh, India, has allegedly been breached by the threat actor **RuskiNet**. The actor claims to have accessed and is now selling over 30 folders of sensitive institutional data, reportedly obtained from the university's official website puchd.ac.in.
Health Level Seven International	Health Level Seven International, an independent, non-profit, membership-based organization operating in India, has allegedly suffered a data breach. A threat actor has claimed to have compromised 1,423,429 patient records, exposing sensitive details such as full names, dates of birth, gender, addresses, emails, mobile numbers, occupations, and other personal identifiers.
DELOPT	DELOPT, an India-based company specializing in defense electronics, electro-optics, and in-store retail technology solutions, has reportedly fallen victim to a ransomware attack carried out by the Akira threat actor. The compromised data, totaling around 70 GB, allegedly includes corporate NDAs, contact numbers and email addresses of employees and customers, corporate licenses, agreements and contracts, financial records (audits, payment details, reports), passports, and other sensitive employee and customer documents.

Threat Actors

1. ## DragonForce

The DragonForce ransomware group has launched a widespread campaign, claiming responsibility for attacks across multiple sectors and regions. Their victims include the City of Grove (78.92 GB of data breached), Iris ID Systems Inc (204.66 GB), Setpoint Systems Corporation (149.8 GB), and RRS Foodservice (25.94 GB), all based in the United States. In addition to these, DragonForce has also targeted numerous other organizations globally, leaking sensitive data and operational information. The group's activities highlight their aggressive expansion across government, technology, automation, and foodservice industries, demonstrating a strategic focus on both public and private sector entities.

2. ## Dark Storm Team

Dark Storm Team is an emerging threat actor known for defacing and disrupting websites of high-profile organizations and government entities. The threat actor has claimed responsibility for attacks on the websites of The Jerusalem Post, InfraGard, Mediacom Communications Corporation, and even Netflix, Inc. Additionally, Dark Storm Team launched a broad campaign Against Kosovo, targeting multiple government ministries including Internal Affairs, Finance, Health, Justice, and Education, among others.

3. ## Qilin

Qilin is a threat actor responsible for a string of recent cyberattacks across multiple sectors. The threat actor has allegedly attacked MonaghanGroup, a grocery retail company in Ireland, and Farmacias Del Pueblo, a pharmacy chain in Argentina. In the United States, victims include 1st Health Inc., a provider of medical care for automobile accident victims; Bertie County Public Schools in North Carolina; Yankee Trails, a travel company; and Universal Window and Door LLC, a manufacturer of residential and commercial window and door solutions.

4. ## AnonSec

AnonSec has recently claimed responsibility for attacking multiple websites in India. The targeted organizations include high-profile entities such as the Indian Air Force, Income Tax India, Bhubaneswar Municipal Corporation, Shivalik Small Finance Bank, and Mehsana Urban Co Op Ltd. These attacks highlight the group's focus on government and financial institutions, as well as its capability to disrupt critical online services in India.

5. ## Akira

Akira has recently claimed responsibility for targeting multiple organizations across different countries. The newly affected victims include TOPPAN NEXT (Singapore), Hayward Quartz Technology (United States), and Tänzer GmbH (Germany). Additionally, the group has added Agencia Browne y Espinoza (Chile), an accounting firm, and Heinz Hammer Vertragswerkstatt GmbH (Germany), a family-owned Mercedes-Benz dealership, to its list of compromised targets. Akira claims to have exfiltrated 37 GB of data from the Chilean accounting firm and 40 GB from the German dealership.

6. ## RALord

RALord has targeted multiple organizations across various sectors and countries. In the agricultural sector, Malaysia's Agromate Holdings was attacked with 15 GB of data exfiltrated. In the technology sector, Bettin Soluções in Brazil had 15 GB of data compromised. Bio-Clima Service, an Italian company specializing in laboratory and biomedical equipment, was attacked, with 50 GB of data exfiltrated. Lastly, ARRCO – Lights Sound Magic, a professional event technology company in Norway, was impacted with 5 GB of data stolen.

7. NightSpire

NightSpire has targeted several organizations across different sectors and countries. In Taiwan, Chang Shen Hospital, a healthcare facility, was hit with 800 GB of compromised data. In the U.S., Mid-America POOL RENOVATION, Inc. suffered a breach with 3 GB of data stolen, while Compliance Consulting Group had 150 GB of data exfiltrated. Additionally, Doroshow Pasquale Krawitz & Bhaya, a Delaware-based law firm, experienced a breach involving 182 GB of data.

8. Sarcoma

The recent wave of ransomware attacks has affected several organizations across various countries and industries. In Brazil, Sinalisa Segurança Viária Ltda., a company focused on road safety and urban infrastructure, was hit with 43 GB of data compromised. In Germany, beverage distributor FAKO-M experienced a significant breach involving 446 GB of data. The UK’s Manchester Credit Union, a non-profit financial cooperative, was also impacted. In Australia, TMA Technology, known for its parking and security solutions, suffered a breach that exposed financial reports, passports, and other sensitive documents. These incidents have been attributed to the Sarcoma threat actor.

9. INC RANSOM

INC RANSOM, a threat actor, has recently claimed responsibility for a series of cyberattacks across various sectors and countries. Among the organizations affected is Ahold Delhaize, a Dutch-Belgian multinational retail and wholesale company, with 6 TB of data reportedly compromised. In Germany, ibL – Ingenieurbüro für Landentwicklung GmbH, an engineering consultancy based in Halle (Saale), experienced a data breach involving 230 GB. In the education sector, Trocaire College, a U.S.-based higher education institution, was impacted by a breach involving 310 GB of data. Additionally, Chickenshed Theatre, an inclusive theatre company based in London, and Orthopaedic Specialists of Connecticut, a healthcare provider in the U.S., were also targeted by the threat actor.

10. SAFEPAY

SAFEPAY, a ransomware threat actor, has expanded its attack campaign by listing 12 organizations. These include a range of companies and institutions across Germany, the UK, and Australia. The affected entities include Stadt Heilbronn, Kellermann & Engelhardt ITEC GmbH, Heinrich + Steinhardt GmbH, Hurst + Schröder GmbH, FRAPACK GmbH, Gemeinde Kirkel, Getriebetechnik Magdeburg GmbH, Eichele Bauunternehmung, and Gebr. Förster GmbH — all based in Germany. Additionally, Helix Tool in the UK and Extreme Fire Solutions in Australia were also targeted. Among the most notable entries is WILHELM NIEMANN GmbH & Co, a family-owned German manufacturing company, with 230 GB of data reportedly compromised.

Threat Analysis

Notable Incidents

- 🇺🇸 **DaVita Inc. Hit by Coordinated Ransomware Strike:** On April 12, 2025, kidney care giant DaVita Inc. suffered a ransomware attack that encrypted key elements of its network, disrupting operations across its 2,600 outpatient treatment centers in the U.S. The Fortune 500 company, which employs over 76,000 people in 12 countries and generates more than $12.8 billion in annual revenue, disclosed the incident in an SEC Form 8-K filing. The attack, believed to have been strategically launched over the weekend to exploit reduced IT staffing, underscores the growing threat of ransomware targeting critical healthcare infrastructure.

- 🇸🇦 **Al-Hejailan Group:** On April 14, 2025, the Ralord threat actor claimed responsibility for a ransomware attack on Al-Hejailan Group, a construction company based in Saudi Arabia. The group alleges the exfiltration of 20 GB of data and has uploaded samples as proof. They have threatened to release 5 GB of the stolen data on April 20, 2025, if their ransom demands are not fulfilled.

- 🇫🇷 **Ardon Municipality:** On April 15, 2025, the NightSpire threat actor claimed responsibility for a ransomware attack targeting the Municipality of Ardon in France. The group exfiltrated approximately 30 GB of sensitive data, threatening to release the information publicly if the ransom is not paid by April 30, 2025.

- 🇳🇱 **Ahold Delhaize Cyber Attack:** On April 17, 2025, Ahold Delhaize confirmed that certain files from its U.S. operations were stolen during a November 2024 cyberattack, following a claim by the Inc Ransom threat group. The group alleges it exfiltrated up to 6 TB of sensitive data and has threatened to release the information if ransom demands are not fulfilled.

- 🇹🇼 **Ransomware Targets Taiwan's Ju Percussion Group:** On April, 2025, Ju Percussion Group, Taiwan's pioneering professional percussion ensemble, was reportedly targeted by the Sarcoma ransomware group. The attackers claim to have exfiltrated 1.6 TB of data, with a ransom deadline set for April 26, 2025. Known for its global performances and percussion education system, Ju Percussion Group now faces a serious breach involving a vast archive of internal files.

- 🇵🇹 **Global Media Group Cyber Attack:** On April 18, 2025, Global Media Group, a company operating in Portugal, reportedly fell victim to a ransomware attack by the Nitrogen hacking group. The attackers claim to have exfiltrated financial reports, employee personal information, confidential company data, and contracts.

- **National Social Security Fund in Major Data Breach:** On April 8, 2025, Algerian hackers launched a cyberattack targeting the Ministry of Employment in Morocco—leaving its website inaccessible—and subsequently breached the National Social Security Fund (CNSS). The attackers claim to have exfiltrated over 54,000 PDF files, containing personal data of approximately 500,000 companies and 2 million insured individuals. The incident, which may rank among the largest data breaches in Moroccan history.

- **SK Telecom, Cyber Attack:** On April 19, 2025, SK Telecom, South Korea's largest

mobile network operator with a 48.4% market share and over 34 million subscribers, experienced a significant cyberattack resulting in the compromise of sensitive customer data. The breach, which occurred during the weekend when staffing levels are typically lower, was traced to a malware infection that infiltrated SK Telecom's systems. This malicious activity enabled threat actors to access critical USIM (Universal Subscriber Identity Module) data, including International Mobile Subscriber Identity (IMSI), Mobile Station ISDN Number (MSISDN), authentication keys, network usage logs, and potentially stored SMS or contact details. The exposure of such information raises serious concerns about the potential for targeted surveillance, SIM-swap attacks, and identity-based threats.

- **NASCAR Data Stolen by Threat Actor:** In April 2025, the Medusa ransomware group claimed responsibility for breaching NASCAR, stealing over 1TB of sensitive data, including names, email addresses, job titles, credentials, venue maps, sponsorship info, financial reports, and internal documents. The group demanded a $4 million ransom, threatening to leak the data if unpaid, and released 33 screenshots as proof.

- **Manchester Credit Union, ransomware attack:** On April 17, 2025, Manchester Credit Union, a UK-based financial services provider known for offering ethical loans and savings to over 30,000 members, was reportedly breached in a ransomware attack by the Sarcoma threat actor. The attackers claim to have exfiltrated 6 GB of data, including files and SQL databases, with a ransom deadline set for April 25, 2025.

Prominent Vulnerabilities

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

1. **CVE-2025-1316 | Edimax IC-7100 IP Camera OS Command Injection Vulnerability CVSS: 9.8**

   CVE-2025-1316 is a remote code execution vulnerability affecting the Edimax IC-7100 camera. The device does not adequately sanitize specially crafted requests, allowing an attacker to execute arbitrary code on the system.

2. **CVE-2024-20439 | Cisco Smart Licensing Utility Static Credential Vulnerability CVSS: 9.8**

   CVE-2024-20439 is a vulnerability in Cisco Smart Licensing Utility (CSLU) that allows unauthenticated remote attackers to log in using undocumented static admin credentials. Successful exploitation grants full administrative access to the CSLU application API.

3. **CVE-2025-24813 | Apache Tomcat Path Equivalence Vulnerability CVSS: 9.8**

   CVE-2025-24813 is a vulnerability in Apache Tomcat that allows remote code execution or data exposure via path equivalence using internal dot notation in file names. It affects versions 11.0.0-M1 to 11.0.2, 10.1.0-M1 to 10.1.34, and 9.0.0.M1 to 9.0.98.

4. **CVE-2025-22457 | Ivanti Connect Secure, Policy Secure and ZTA Gateways Stack-Based Buffer Overflow Vulnerability CVSS: 9.8**

   CVE-2025-22457 is a stack-based buffer overflow vulnerability affecting Ivanti Connect Secure (before 22.7R2.6), Ivanti Policy Secure (before 22.7R1.4), and Ivanti ZTA Gateways (before 22.8R2.2). This flaw allows a remote unauthenticated attacker to execute arbitrary code on the affected systems, potentially leading to full system compromise.

5. **CVE-2025-30406 | Gladinet CentreStack and Triofox Use of Hard-coded Cryptographic Key Vulnerability CVSS: 9.8**

   CVE-2025-30406 is a deserialization vulnerability in Gladinet CentreStack through version 16.1.10296.56315, fixed in 16.4.10315.56368. The flaw arises from the CentreStack portal's use of a hardcoded machineKey, allowing attackers with knowledge of the key to craft malicious serialized payloads for server-side deserialization and remote code execution.

6. **CVE-2025-30066 | tj-actions/changed-files GitHub Action Embedded Malicious Code Vulnerability CVSS: 8.6**

   CVE-2025-30066 is a vulnerability in tj-actions changed-files where versions before 46 allow remote attackers to discover secrets by reading action logs. A threat actor modified tags v1 through v45.0.7 to point at a malicious commit (0e58ed8) that contained compromised updateFeatures code, enabling unauthorized access to sensitive information.

7. **CVE-2025-31161 | CrushFTP Authentication Bypass Vulnerability CVSS: 9.8**

   CVE-2025-31161 is an authentication bypass vulnerability in CrushFTP, affecting versions 10 before 10.8.4 and 11 before 11.3.1, allowing attackers to take over the crushadmin account unless a DMZ proxy is in place. Exploited in the wild during March and April 2025, the flaw stems from a race condition in the AWS4-HMAC authorization process. Attackers can exploit this by manipulating HTTP headers to bypass authentication, leading to full administrative access.

8. **CVE-2025-29824 | Microsoft Windows Common Log File System (CLFS) Driver Use-After-Free Vulnerability CVSS: 7.8**

   CVE-2025-29824 is a use-after-free vulnerability in the Windows Common Log File System (CLFS) Driver that allows a locally authorized attacker to elevate privileges. By exploiting this flaw, an attacker can gain higher-level access on the affected system, potentially leading to full system compromise.

9. **CVE-2024-53150 | Linux Kernel Out-of-Bounds Read Vulnerability CVSS: 7.1**

   CVE-2024-53150 is a vulnerability in the Linux kernel's ALSA USB-audio driver that could lead to out-of-bounds reads when processing malformed clock source descriptors. The issue stems from the driver's failure to validate the bLength field of USB descriptors during traversal. Malicious or buggy devices could exploit this by providing improperly sized descriptors. CVE-2018-9276 is a critical OS command injection vulnerability affecting PRTG

10. **CVE-2025-27482 | Windows Remote Desktop Services Remote Code Execution Vulnerability CVSS: 8.1**

   CVE-2025-27482 is a vulnerability caused by sensitive data being stored in improperly locked memory within the Remote Desktop Gateway Service. This flaw allows an unauthorized attacker to execute arbitrary code remotely over a network, potentially leading to unauthorized access, data breaches, or full system compromise.

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