



Comprehensive Threat Report: Jan -2025

Executive Summary

In January 2025, the cybersecurity landscape saw significant breaches and disruptions across sectors, with sensitive data exposed from agencies like the NBI Philippines, ICAO, and Dubai Pulse. Major incidents included destructive attacks on Russia's Planeta center, a DDoS hit on Japan's NTT Docomo, and a ransomware attack on the UK's Gateshead Council.



Table of Contents

Overview.....	3
Key Threats:	3
Threat Landscape.....	4
Ransomware Trends	4
Incident Trends	4
DDoS activity.....	5
Underground Findings	6
Global Data Breaches and Leaks	6
Indian Data Leaks And Breaches	8
Threat Actors	10
Threat Analysis	12
Notable Incidents.....	12
Prominent Vulnerabilities	14
Top Initial Access ATT&CK TTPs.....	16
Appendix.....	17



Overview

In January 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. **National Bureau of Investigation (NBI) of Philippines:** The breach involved over 3.6 GB of data, spanning from 2016 to 2024.
2. **PetroVietnam Exploration Production Corporation:** 1.3 TB of data was exfiltrated during the attack.
3. **UN aviation agency ICAO:** Over 40,000 records of personal information were exposed and breach, attributed to Natohub, involved data from April 2016 to July 2024.
4. **Dubai Pulse:** 21,912,532 user profiles reportedly compromised.
5. **Lynx Spa:** Confidential documents, sales data, financial records, business plans, and employee personal information was breached.

Major Cyber Incidents:

1. **Japan's largest telco NTT Docom:** NTT Docomo experienced a 12-hour service disruption on January 2, 2025, due to a DDoS attack, affecting services like the goo portal.
2. **Russia's State Research Center on Space Hydrometeorology ("Planeta"):** Pro-Ukraine hackers "BO Team" attacked Russia's "Planeta" center, destroying 280 servers and 2 petabytes of critical data, including satellite and weather info.
3. **UK's Gateshead Council:** Gateshead Council was attacked on January 8, 2025, with personal data stolen and posted on Medusa's leak site. Medusa demands a \$600,000 ransom and threatens to release more data. The police are investigating.
4. **Orange Spain:** Threat actor "Snow" breached RIPE, misconfiguring BGP and RPKI settings, causing a two-hour outage. No customer data was compromised.

Key Threats:

In January 2025, notable vulnerabilities included **CVE-2024-50603** (Aviatrix Controllers OS Command Injection Vulnerability), **CVE-2024-55591** (Fortinet FortiOS Authorization Bypass Vulnerability), **CVE-2023-48365** (Qlik Sense HTTP Tunneling), **CVE-2025-23006** (SonicWall SMA1000 Appliances Deserialization Vulnerability) and **CVE-2024-41713** (Mitel MiCollab Path Traversal Vulnerability).

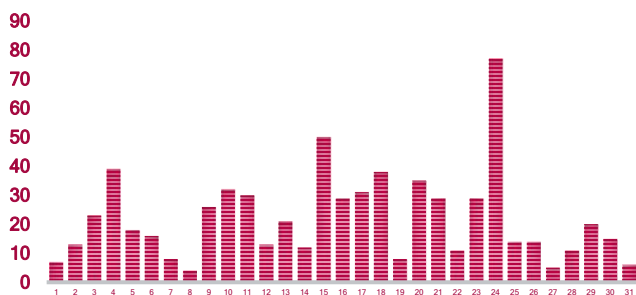
Ransomware attacks also surged, particularly targeting sectors like healthcare, finance, and education. High-profile breaches, such as those affecting National Bureau of Investigation Philippines, UN aviation agency ICAO, and the Dubai Pulse, emphasize the growing threat and the need for stronger cybersecurity defences.



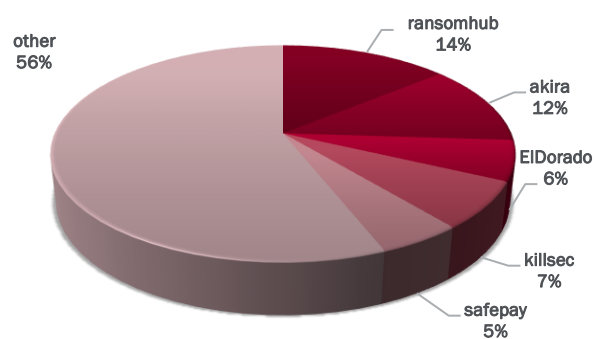
Threat Landscape

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



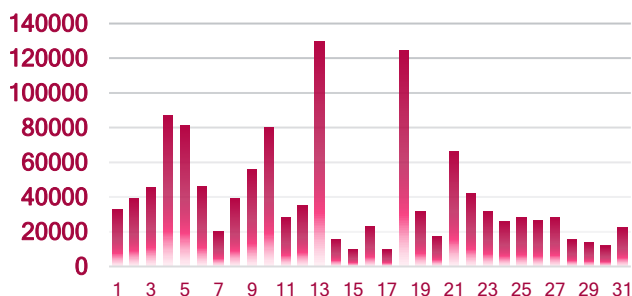
Victims per day



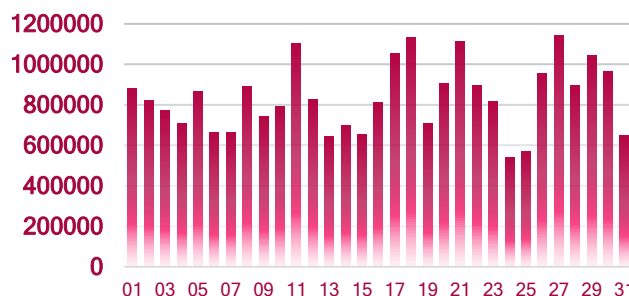
Victims by group

Incident Trends

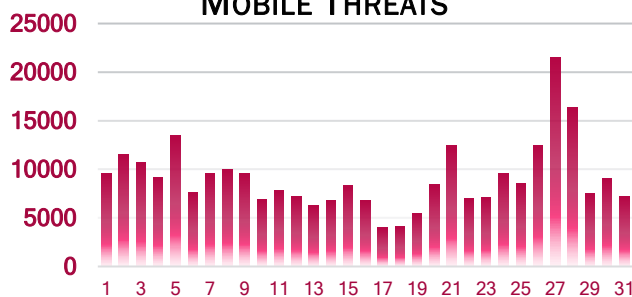
EXPLOITS



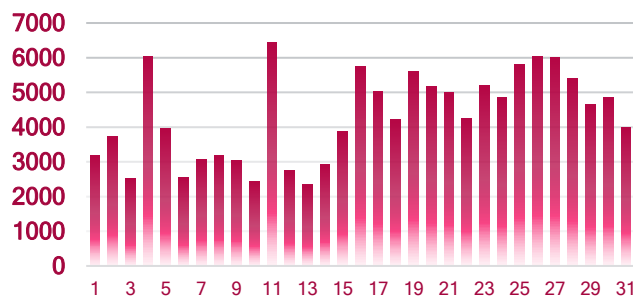
MALWARE



MOBILE THREATS



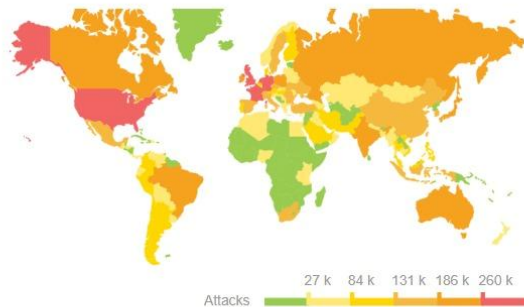
COINMINER





DDoS activity

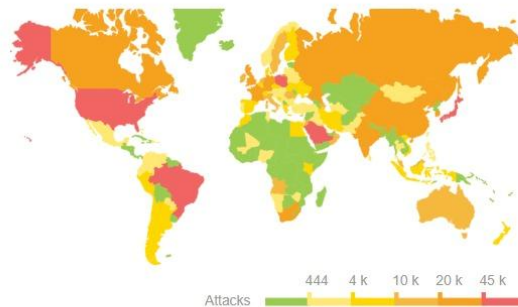
Top Source Countries:



Sources ⓘ

United States	546,489	46.8 %
Germany	296,902	25.4 %
Netherlands	279,550	23.9 %
United Kingdom	273,923	23.5 %
France	259,666	22.2 %

Top Destination Countries:



Destinations ⓘ

United States	190,091	16.3 %
Brazil	127,105	10.9 %
Poland	64,702	5.5 %
Japan	56,821	4.9 %
Saudi Arabia	45,316	3.9 %







Underground Findings

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

Global Data Breaches and Leaks

Region	Organisation	Significant data
	National Bureau of Investigation (NBI)	The Philippines' NBI has suffered a major data breach, with hacker "Zodiac Killer" leaking 3.6 GB of data from 2016-2024. Over 45 million records, including personal details, transaction IDs, and sensitive NBI files, were exposed on dark web forums.
	PetroVietnam Exploration Production Corporation	Vietnam's Petrovietnam Exploration Production Corporation was hit by a ransomware attack by the HUNTERS group, which claims to have stolen 1.3 TB of data. Discovered on January 20, 2025, the breach involved both encryption and data theft, posing risks to operations and sensitive information. The incident highlights cybersecurity vulnerabilities and the need for stronger protections.
	M9com	The pro-Ukraine hacktivist group Blackjack attacked Russian ISP M9com, claiming retaliation for the Kyivstar breach. They stole employee and customer credentials, 50GB of call data, defaced the website, and wiped servers. Allegedly linked to Ukraine's SBU, Blackjack vowed more attacks, escalating cyber tensions with Russia.
	UN aviation agency ICAO	The UN's aviation agency, ICAO, confirmed a breach of its recruitment systems by hacker Natohub, exposing over 40,000 applicant records from 2016 to 2024. Leaked data includes names, emails, birth dates, and job history, though financial details and sensitive documents were unaffected.
	Dubai Pulse	A potential data breach at Dubai Pulse may have exposed over 21 million user records, including names, emails, and phone numbers. Hacker "henrymansOn" claimed responsibility on a forum, raising concerns about security vulnerabilities and user privacy risks. The claim, which appeared on a hacking forum, suggests that a total of 21,912,532 user profiles were compromised.
	Trello	Threat actor "emo" exploited an exposed Trello API, connecting email addresses to public Trello profiles, affecting over 15 million accounts. Emo collected 500 million email addresses, tested them with the API, and sold the resulting data, which included emails, usernames, and other details, on a hacking forum. Although much of the data was already public, it exposed private email addresses. Trello has since secured the API to prevent further breaches.



	Lynx Spa	Italian IT company Lynx Spa was targeted in a ransomware attack by MORPHEUS, stealing sensitive data like financial records, business plans, and employee info. The group also accessed backups, a GitLab repository, and technical data. Lynx Spa, with \$292.5 million in revenue, offers digital services to industries like finance, insurance, and government.
	Carrefour	Threat Actor known as LaFouine has claimed to have leaked a Carrefour database containing personal information of over 13 million customers who made purchases on the retailer's website. The leaked data includes names, addresses, phone numbers, emails, birth dates, shopping habits, and details about their orders like fees, discounts, and prices. The hacker is reportedly offering the data for sale, sharing contact info for potential negotiations.
	JustCall	An attacker, identified as Ddarknotevil, has allegedly stolen 11.5 GB of data from JustCall, a U.S.-based SaaS platform. The breach exposed over 6.2 million records, including sensitive information like names, phone numbers, emails, call logs, and hashed subscriber details. Additionally, API keys were compromised. The stolen data is being sold on the dark web for \$1,500, raising significant concerns about the platform's security and the privacy of its users.
	AXA COLPATRIA	AXA COLPATRIA, a major financial services company in Colombia, has suffered a data breach exposing sensitive information of about 10,000 users. The leaked data includes user IDs, names, document numbers, emails, business details, roles, and location information like city and address. It also contains phone numbers, state info, application dates, and admin-related data. The breach has raised serious concerns about the company's data security, with a hacker known as "888" believed to be responsible.



Indian Data Leaks And Breaches

Organisation	Significant data
RABWIN INDUSTRIES PRIVATE LIMITED	Rabwin Industries, an Indian precision manufacturing company, has fallen victim to a ransomware attack by the hacker group Qilin. The attack, announced on January 20, 2025, revealed that all of the company's data would be made available for download starting January 27, 2025. Rabwin, known for its advanced CNC machines and precision components, is now dealing with a major data breach. The involvement of the Qilin group raises concerns about the exposure of sensitive company information.
Jammu & Kashmir Rural Livelihoods Mission	The Jammu & Kashmir Rural Livelihoods Mission (JKRLM) has suffered a major data breach, exposing 89,294 user records with sensitive details like IDs, passwords, names, emails, genders, and birth dates. This breach raises serious concerns about the safety of personal information and the risks to those affected. It highlights the urgent need for stronger security measures to protect such data within the organization.
Supreme Nonwoven Industries Pvt. Ltd	Supreme Nonwoven Industries Pvt. Ltd., an Indian company, has been targeted by a cyberattack attributed to the "RansomHub" group. The breach has raised alarm over the potential exposure of sensitive company and employee data. Initial reports indicate that the compromised information includes names, banking details, and private business data, posing significant risks to individuals and the company. The full impact of the attack is still being assessed, but it highlights the growing cybersecurity threats facing businesses today.
FAAB Invest Advisors Private Limited	A ransomware attack has caused a major data breach affecting several companies, including FAAB Invest Advisors, Nimbus Facility Services, Cofar, and Anupalan Online. FAAB Invest Advisors, a green investment platform that offers fractional ownership in sustainable assets like electric mobility and renewable energy, is a key target in the breach. The company focuses on eco-friendly investment opportunities and responsible portfolio diversification. The attack, claimed by the hacker group "Killsec," highlights the rising cybersecurity risks faced by businesses in the financial and sustainability sectors.
Bethany Hospital	Bethany Hospital, a well-known healthcare facility in India, has been targeted by the hacker group "Space Bears," who claim to have accessed sensitive and valuable data from the hospital. The attackers have threatened to release the data on their leak portal within 3 to 4 days unless their demands are met. The compromised information includes organizational details, technical data, employee records, patient databases, and other confidential information. A sample of the stolen data has been provided for review, highlighting the serious concerns over the security and privacy of both employee and patient data in the healthcare sector.



ICICI Bank	On January 21, 2025, ICICI Bank, one of India's top financial institutions, revealed a major ransomware breach linked to the hacking group "apt73." The attack exposed sensitive data from around 63,778 employees and 40,686 users, as well as interactions with 392 third-party entities. Screenshots of the compromised information have been shared, though specific download links were not provided. This breach highlights growing cybersecurity risks in India's banking sector and underscores the urgent need for stronger security measures to protect personal and corporate data.
Rupay	The attack known as "Monkeycrazy" has allegedly put up for sale the entire codebase and infrastructure of Rupay's banking systems. The leak includes critical files like APIs for withdrawals, KYC, and PayPal, as well as sensitive production databases and customer identity documents. This breach exposes serious vulnerabilities in Rupay's systems and poses a major security risk, compromising both technical infrastructure and personal customer data.
NetSe.in	NetSe, a popular online grocery delivery platform in India, has suffered a data breach exposing 128,000 customer records. The compromised data includes names, addresses, phone numbers, order details, and user IDs. This leak raises concerns about the security of personal information on the platform. NetSe is known for providing a wide range of household essentials and has a large, loyal customer base across the country.
INFRATECH	Breach claimed by that IndoHaxSec recently stated responsible for targeting "INFRATECH," an Indian real estate company. They reportedly leaked a database with 43,700 entries, which includes sensitive customer information such as names, email addresses, contact details, and physical addresses.
Niva Bupa	Threat actor is allegedly selling the database of Niva Bupa, a major health insurance provider, for \$10,000. The leaked data reportedly includes over 14 million entries, with about 9 million unique mobile numbers. The database is massive, containing more than 4,100 tables and totaling over 200 GB.



Threat Actors

1. RipperSec

The Threat Actor "RipperSec" has reportedly attacked several organizations, including the Binyamina-Givat Ada Community Center, the University of New South Wales in Australia, and the National Institute of Psychobiology in Israel. Active throughout January, RipperSec has leaked sensitive data from these victims and is now selling it on dark web platforms. The exposed information includes personal and confidential details, posing significant risks to individuals and organizations. As investigations unfold, this breach underscores the ongoing threat from cybercriminals targeting institutions worldwide, particularly during this spike in activity.

2. Ddarknotevil

The "Ddarknotevil" has been linked to multiple breaches, including a major attack on JustCall, exposing 11.5 GB of data with 6.3 million records. They also targeted Online TV Recorder, potentially exposing 543,019 users' email and passwords, and Shanghai Epean Trading Co., Ltd. These breaches highlight Ddarknotevil's growing global cyber threat.

3. Rey

The Breach "Rey" has reportedly targeted the University of Rwanda, exposing 28,359 records with sensitive personal, academic, and administrative data of students, including IDs, names, gender, nationality, birth dates, addresses, phone numbers, passport details, and academic history. In a separate breach, Car Care Plan (CCP), a UK-based company in the automotive service and collision repair industry, has also been compromised. While the full details of the leaked data are not yet known, these incidents highlight the increasing cybersecurity risks faced by organizations in both the education and automotive sectors globally.

4. IntelBroker

IntelBroker, a notorious hacker group, has breached several organizations, resulting in significant data leaks. Hewlett Packard Enterprise (HPE) in the USA was targeted, with private assets such as GitHub repositories, Docker builds, SAP Hybris, API credentials, source codes, and personal user information exposed. In California, Capital Markets Elite Group also suffered a breach, exposing customer data like names, emails, phone numbers, addresses, and passwords. The Ministry of Environment experienced a similar attack, with its entire source code being compromised. These incidents highlight IntelBroker's ability to breach diverse sectors and steal critical data, posing a serious threat to security across multiple industries.

5. Ransomhub

Ransomhub, a cybercriminal group, has recently attacked several organizations. Among the victims is Archaeological Research Services Ltd, a UK-based archaeological service provider, from which the actor claims to have stolen 83 GB of data. Mission Bank, a community-focused bank in the USA, had 2.7 TB of data exfiltrated. The Supreme Group, a diversified conglomerate in India, also fell prey to Ransomhub,



though the exact amount of compromised data remains unclear. Additionally, the group targeted SDK A/S, a Danish shipping and logistics company, claiming to have taken 230 GB of data.

6. Funksec

Funksec, a cybercriminal group, has recently targeted several organizations. One of the victims is ipTIME, a South Korean brand specializing in networking equipment, from which Funksec claims to have stolen substantial data. The University Center of Barika also fell victim to the group, with sensitive information reportedly taken from the institution. Additionally, the Maritime Transport & Logistics Sector in Egypt was compromised, with Funksec claiming to have exfiltrated data from the organization.

7. Qilin

Qilin, a cybercriminal group, has recently targeted multiple organizations. Rabwin Industries Private Limited, an Indian precision manufacturing company, is among the victims, with Qilin claiming to have stolen sensitive data. Richardson Sales Performance, a US-based company, also fell victim, with the breach potentially exposing employee records, client information, and proprietary business data. Additionally, Qilin compromised Welker, Inc., a manufacturing company in Sugar Land, Texas. The ransomware leak page associated with Welker indicates that all data will be released for download on January 24, 2025, containing sensitive information that could have serious consequences for the company's operations and reputation.

8. Space Bears

Space Bears, a cyber threat group, has recently attacked several organizations. One of the victims is Pineland Community Service Board, a healthcare provider in the USA, with the group claiming to have stolen its data. Another target is Christian Community Aid, a non-profit based in New South Wales, with Space Bears accessing its database and planning to release the data within 10-11 days. The leaked files include a variety of formats such as .jpg, .mp4, .mov, .xls, .doc, .mdf, .msg, and .pdf. Additionally, Space Bears has compromised Laboratório Santa Maria in Brazil, claiming to have exfiltrated its database and planning to publish it within 6-7 days.

9. LYNX

Lynx, a cybercriminal group, recently launched ransomware attacks targeting several organizations, including Mintz Law Firm, LLC, Marukai Corporation, Clutch Industries, and Kassin & Carrow, LLC. The law firms, which handle personal injury and Social Security Disability cases, had sensitive client information, contracts, and financial records exposed. Marukai, a Japanese retailer in the U.S., faced a breach of its operational and customer data. Clutch Industries, an Australian manufacturing company, had extensive business and employee records stolen. Lynx has threatened to release the compromised data unless their demands are met, raising serious concerns about data security, client trust, and potential disruptions for these organizations.

10. Akira






Akira ransomware group recently attacked Divimast, Beyond79, and Moinho Globo Alimentos. Divimast lost 8 GB of data, while Beyond79 had sensitive employee and customer information exposed, including SSNs. Moinho Globo Alimentos had 58 GB of corporate data leaked,



including IDs and financial records. Akira threatens to release the data unless demands are met, endangering the organizations' security and reputation.





Threat Analysis

Notable Incidents

-  **NTT Docomo Hit by Major DDoS Attack, Service Disrupted for 12 Hours:** NTT Docomo, Japan's largest telecom provider, faced a major cyberattack on January 2, 2025, resulting in a 12-hour disruption. The attack, identified as a Distributed Denial of Service (DDoS), overloaded the company's networks, impacting access to services like the goo portal. While the perpetrators remain unconfirmed, there is speculation that the ransomware group Randomwed.Vc, known for a previous attack on NTT in September 2023, might be responsible.
-  **Pro-Ukraine Hackers Hit Russian Space Research Center:** The pro-Ukraine hacker group "BO Team" recently attacked Russia's State Research Center "Planeta," destroying 280 servers and two petabytes of data, including satellite and weather information. The attack also disabled supercomputers and essential systems. Ukraine's defense intelligence estimates the damage could exceed \$10 million. This attack is part of a larger series of cyberattacks on Russian targets, though details are hard to verify due to Russian denial.
-  **Gateshead Council Hit by Medusa Ransomware Attack:** Gateshead Council confirmed a cyberattack on January 8, 2025, which led to the theft of personal data. The Medusa ransomware group leaked documents on January 15, exposing PII like names, contact info, and employment history, as well as internal files on job applications and housing reports. Both residents and employees were affected. Medusa has demanded \$600,000, threatening to release more data in nine days if not paid. The police are investigating the breach.
-  **Orange Spain Faces Disruption After BGP Hijacking Attack:** On January 1, Orange Spain experienced a major network disruption due to a hacker named "Snow" breaching its RIPE account. The attacker altered BGP routing and RPKI settings, causing an internet outage for around two hours. The breach is suspected to have occurred through stolen employee credentials from an infostealer malware attack. While there was no customer data breach, some services were temporarily disrupted. Orange Spain has since restored operations and is bolstering security measures, advising users to activate multi-factor authentication.
-  **Monobank Resilient Against Massive DDoS Attack:** Monobank, a leading Ukrainian mobile bank, endured a three-day DDoS attack in January 2024, receiving 580 million requests. Despite the scale, users experienced minimal disruption to services. Known for handling donations for Ukraine's military, the bank remains a frequent target of Russian-backed hacker groups.





- **Cyberattack Disrupts Washington County Government:** A cyberattack on January 22, 2024, forced Washington County officials to shut down phone and computer systems after detecting malware phishing activity. While 911 services remained unaffected, government and courthouse operations were disrupted, leading to court cancellations. The U.S. Department of Homeland Security and an external IT firm are investigating the breach, with no clear timeline for restoring normal operations.
-  **Cyberattack Hits Ukrainian Data Center, Disrupting State Services:** A cyberattack on January 24 targeted Parkovy, a data center serving Ukrainian state-owned companies, affecting services like the postal system, railways, and an energy firm. While recovery efforts are ongoing, Ukraine suspects Russian-linked hackers. The e-government platform "Diia" remained unaffected, but a hacker group leaked alleged Parkovy data, fueling concerns of a state-sponsored attack.
-  **Mandiant's X Account Hacked in Crypto Scam:** Mandiant, a Google Cloud subsidiary, confirmed its X account was hacked in early January as part of a crypto theft campaign that netted cybercriminals at least \$900,000. The attackers used the account to promote a fake Phantom wallet website, likely exploiting a brute-force password attack. Mandiant clarified that Google Cloud systems were not affected. The breach is linked to the ClinkSink campaign, where threat actors used "drainer-as-a-service" (DaaS) tools to steal Solana wallet funds by luring victims with fake airdrop offers.
-  **Cyberattack Hits Argentina's Airport Security Police Payroll:** A cyberattack on Argentina's Airport Security Police (PSA) payroll system led to unauthorized salary deductions of 2,000 to 5,000 pesos for police and civilian staff. The breach was traced to Banco Nación's payroll system rather than PSA's internal network. Investigators suspect remote servers, possibly foreign, and potential internal involvement. PSA has blocked affected services and launched an investigation.
-  **Chinese Hackers Breach U.S. Treasury Systems:** Chinese state-sponsored hackers infiltrated the computers of U.S. Treasury Secretary Janet Yellen and two senior officials, Deputy Secretary Wally Adeyemo and Acting Under Secretary Brad Smith. Although fewer than 50 unclassified files were accessed, the attack raises concerns about cybersecurity vulnerabilities in high-level government systems. This breach is part of a larger cyberattack campaign targeting U.S. government institutions.



Prominent Vulnerabilities

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

1. **CVE-2024-12686 | Beyond Trust Privileged Remote Access (PRA) and Remote Support (RS) OS Command Injection Vulnerability** **CVSS: 7.2**

OS command injection allows attackers to run unauthorized system commands, posing serious security threats, especially in web applications. If exploited in a privileged program, attackers can execute restricted commands with elevated access. The risk worsens when processes lack proper privilege controls. These vulnerabilities arise when user input is improperly included in commands or when unintended execution occurs due to poorly handled input.

2. **CVE-2024-50603 | Aviatrix Controllers OS Command Injection Vulnerability** **CVSS: 10**

A vulnerability was found in Aviatrix Controller versions before 7.1.4191 and 7.2.x prior to 7.2.4996. This issue arises from inadequate handling of special characters in OS commands, allowing unauthenticated attackers to execute arbitrary code. By sending shell metacharacters to the /v1/api endpoint, specifically in the cloud_type parameter for list_flightpath_destination_instances or the src_cloud_type for flightpath_connection_test, attackers can exploit this flaw.

3. **CVE-2024-55591 | Fortinet FortiOS Authorization Bypass Vulnerability** **CVSS: 9.8**

A vulnerability in FortiOS versions 7.0.0 to 7.0.16 and FortiProxy versions 7.0.0 to 7.0.19 and 7.2.0 to 7.2.12 allows remote attackers to bypass authentication and gain super-admin privileges. This issue occurs through specially crafted requests sent to the Node.js websocket module.

4. **CVE-2023-48365 | Qlik Sense HTTP Tunneling Vulnerability** **CVSS: 9.9**

CVE-2024-48365 is a critical vulnerability in Qlik Sense Enterprise for Windows, stemming from improper validation of HTTP headers. This flaw enables malicious actors to exploit the system, potentially leading to unauthorized actions, including remote code execution (RCE). Here's a breakdown of the technical specifics of this vulnerability.

5. **CVE-2021-44207 | Acclaim Systems USAHERDS Use of Hard-Coded Credentials Vulnerability** **CVSS: 8.1**

The Acclaim Systems USAHERDS web application uses ValidationKey and DecryptionKey values to maintain the integrity and security of its ViewState data. ViewState helps preserve the state of web application controls during client-server interactions.



6. CVE-2025-23006 | SonicWall SMA1000 Appliances Deserialization Vulnerability CVSS: 9.8

A critical vulnerability, CVE-2025-23006, has been identified in SonicWall's SMA 1000 series appliances (versions 12.4.3-02804 and earlier), which is being actively exploited. This flaw affects the Appliance Management Console (AMC) and Central Management Console (CMC) products, with a CVSS score of 9.8. It allows remote, unauthenticated attackers to execute arbitrary commands on vulnerable systems. If exploited, it could lead to severe security incidents, such as network breaches and data theft. The vulnerability arises from the pre-authentication deserialization of untrusted data, enabling attackers to bypass security measures.

7. CVE-2020-11023 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') CVSS: 6.1

CVE-2020-11023 is an XSS vulnerability in jQuery versions 1.0.3 to 3.4.0. It allows attackers to inject malicious JavaScript through <option> elements passed to DOM manipulation methods, potentially leading to session hijacking or data theft. This was fixed in jQuery 3.5.0 with added protections.

8. CVE-2025-21333 | Microsoft Windows Hyper-V NT Kernel Integration VSP Heap-based Buffer Overflow Vulnerability CVSS: 7.8

CVE-2025-21333 is a critical buffer overflow vulnerability in Windows Hyper-V's NT Kernel, allowing attackers to escalate privileges to SYSTEM on compromised machines. It affects the communication between virtual machines and the host OS. Exploiting this flaw enables low-privileged attackers to gain full control of the host system. Organizations using Hyper-V should apply patches promptly to prevent exploitation.

9. CVE-2025-0282 | Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability CVSS: 9.0

CVE-2025-0282 is a critical buffer overflow vulnerability in Ivanti's Connect Secure, Policy Secure, and ZTA gateway products (prior to versions 22.7R2.5, 22.7R1.2, and 22.7R2.3). It allows unauthenticated remote attackers to execute arbitrary code, potentially gaining control of the appliance and compromising the network. Exploiting this flaw involves sending crafted requests to vulnerable systems, making them prime targets for external attackers.

10. CVE-2024-41713 | Mitel MiCollab Path Traversal Vulnerability CVSS: 9.8

CVE-2024-41713 is a critical path traversal vulnerability in Mitel MiCollab's NuPoint Unified Messaging (NPM) component (versions 9.8 SP1 FP2 and earlier). Due to insufficient input validation, an unauthenticated attacker can access sensitive data and potentially execute unauthorized administrative actions. With a CVSS score of 9.8, this vulnerability poses significant risks to the system's confidentiality, integrity, and availability.



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)

Hackers 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