Comprehensive Threat Report: Feb -2025

Executive Summary

In February 2025, cybersecurity incidents surged globally, with major data breaches, ransomware attacks, and critical vulnerabilities impacting government, healthcare, finance, and tech sectors, highlighting urgent gaps in digital defenses.

Table of content

Overview

In February 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. **Military Saudi Arabia and Government**: The breach involved over 590 GB of internal documents allegedly stolen from officials' emails.
2. **Swiss Medical**: More than 2 million patient records exposed during the attack.
3. **Israel Police**: A reported 2.1TB data leak exposed personnel records, case files, and sensitive law enforcement data.
4. **Bank Central Asia (BCA)**: Alleged breach exposed 4.9 million records, including 890K account details, login credentials, and transaction histories.
5. **Investing.com Breach:** 6.5 million user records, including emails and user IDs, allegedly compromised due to an IDOR vulnerability.

Major Cyber Incidents:

1. **Bybit Crypto Heist – UAE**: Hackers stole 401,347 ETH from Bybit's cold wallet during a routine transfer, exposing major security risks.
2. **Unimicron Ransomware Attack – Taiwan**: A ransomware group claims to have stolen 377GB of data from Unimicron.
3. **HCRG Care Group Ransomware Attack – UK**: Medusa ransomware operators claim to have stolen 2TB of sensitive data from HCRG Care Group, demanding a $2 million ransom.
4. **OmniGPT**: A cyberattack exposed data of 30,000+ users, including chatbot conversations, emails, and sensitive documents.

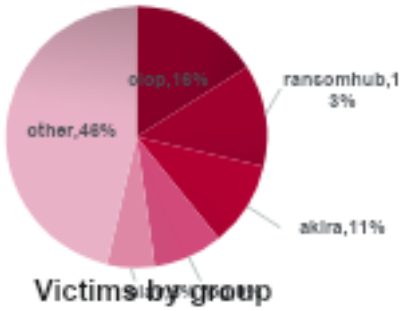
Key Threats:

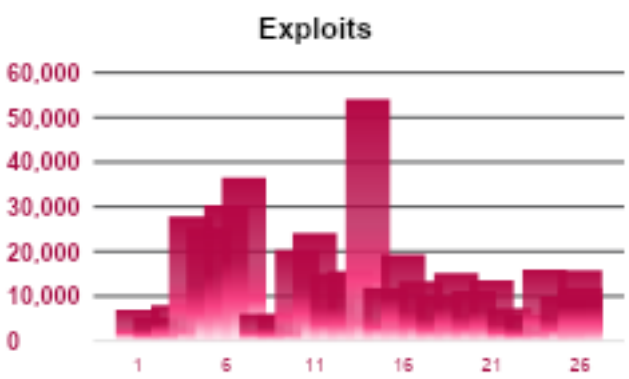
In February 2025, notable vulnerabilities included **CVE-2024-53704** (SonicWall SonicOS SSLVPN Improper Authentication Vulnerability), **CVE-2024-40890** (Zyxel DSL CPE OS Command Injection Vulnerability Vulnerability), **CVE-2025-0411** (7-Zip Mark of the Web Bypass Vulnerability), **CVE-2025-0994** (Trimble Cityworks Deserialization Vulnerability Vulnerability) and **CVE-2018-19410** (Paessler PRTG Network Monitor Local File Inclusion Vulnerability). Ransomware attacks also surged, particularly targeting sectors like healthcare, manufacturing, and education. High-profile breaches, such as those affecting Swiss Medical, military Saudi Arabia and government, and the Israel Police, emphasize the growing threat and the need for stronger cybersecurity defences.

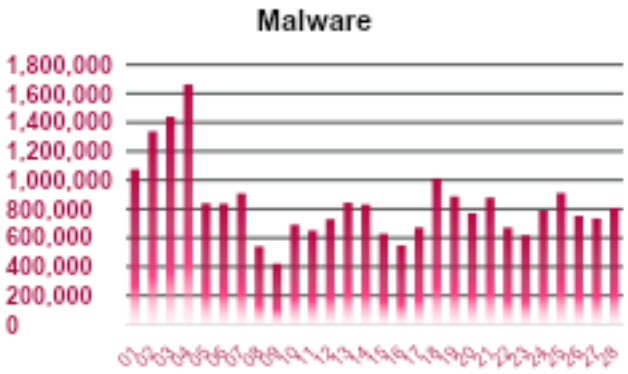
Threat Landscape

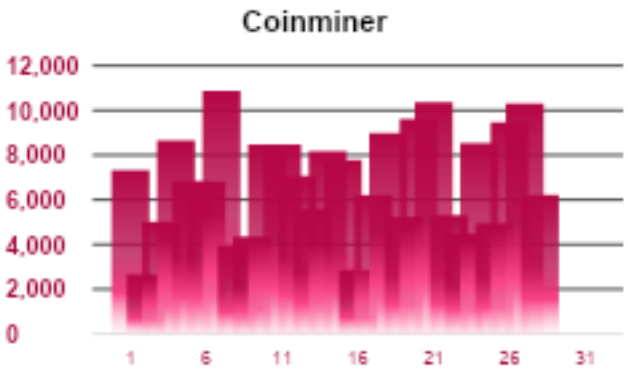
Ransomware attacks are happening more often and causing more trouble, while mobile malware takes advantage of how many people use smartphones and tablets. Both threats show that there is an urgent need to improve security measures.

Ransomware Trends



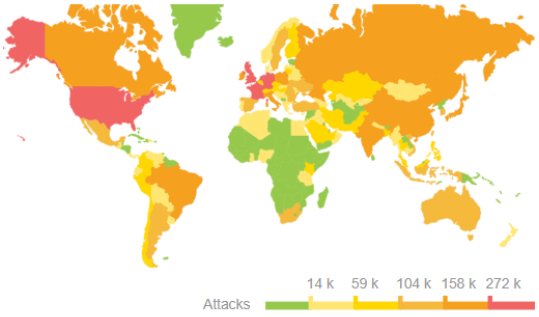






DDoS activity

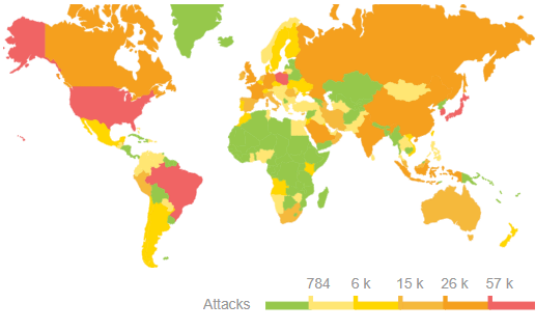
Top Source Countries:



Sources

United States	676,052	40.9 %
Germany	330,083	20 %
Netherlands	288,695	17.5 %
France	280,807	17 %
United Kingdom	272,188	16.5 %

Top Destination Countries:



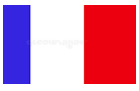
Destinations

United States	248,278	15 %
Brazil	119,510	7.2 %
Poland	75,081	4.5 %
Japan	72,249	4.4 %
South Korea	56,589	3.4 %

Underground Findings

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

Global Data Breaches and Leaks

Region	Organisation	Significant data
	Swiss Medical	The threat actor “rufusdomando” has allegedly breached Swiss Medical, a leading healthcare provider in Argentina, exposing 2,045,608 records containing sensitive patient and customer data. The leaked information reportedly includes user credentials (potential login details and passwords), physical addresses, social security and healthcare-related data, and other personally identifiable information.
	Infolaft	A threat actor claims to have obtained a 1.2TB database from Infolaft, a corporate office based in Colombia, and is offering it for sale. The leaked data is said to contain important information, including Infolaft's customer and employee login details, customer folders, and Infolaft-specific folders.
	NAGA	NAGA, a company in the Architecture, Engineering & Design industry based in the United Arab Emirates, has allegedly been breached by the threat actor “RansomHub”. Allegedly, 118GB of data were exfiltrated, and a sample has been leaked.
	Military Saudi Arabia and Government	A threat actor known as “SkyWave” claims to be selling 590GB of data, including military and government internal documents from Saudi Arabia. The alleged exfiltrated data is said to have been stolen from the email accounts of several military officials.
	Chronopost	A threat actor claims that Chronopost, a Freight & Logistics Services company in France, has a database of over 7.3 million users, including both individual customers and businesses, and is putting it up for sale. This data is said to include Customer Profile, Credentials, Address Information, and Additional Information for corporate clients.
	Unique Personnel	“Al-Sheikh”, a prominent threat actor, claims to have access to the Unique Personnel South Africa database and offers it for sale. This data is said to include 1,001,427 Authorized User Information (Username, Password, Email Address), 11,474 Customer Information (Name, Surname, Username, Password, etc.), and 968,580 Candidate Personal

		Information (Birthday, Ethnic Group, ID Number, Address, etc.). Unique Personnel operates in the Business Services industry in South Africa.
	Israel Police	“Handala”, a threat actor, has allegedly breached and leaked 2.1 terabytes of sensitive data from Israel Police, which operates in the Government Administration sector in Israel. The leaked data reportedly includes personnel records, armory inventories, medical and psychological profiles, case files, weapon permits, and identity documents. This breach could have severe security implications, potentially exposing sensitive law enforcement operations and compromising the privacy of police personnel and civilians associated with these records.
	Lantiqx	Lantiqx, an IT services company based in the United Kingdom, has allegedly suffered a data breach involving 128GB of stolen data, including database dumps and various company files, with full access being offered for $1,000. Screenshots of SQL database files and JSON-formatted employee data were shared as proof, exposing sensitive company information. The leaked data is said to include employee working status, full names, email addresses, task descriptions, task names, project release codes, and other IT-related internal data. The breach is claimed by the threat actor “Arikos”.
	Bank Central Asia (BCA)	Bank Central Asia (BCA), a leading bank in Indonesia operating in the Banking & Mortgage industry, has allegedly suffered a data breach with access to 890,000 accounts and a database containing 4.9 million records being offered for sale. The leaked data is claimed to include account login credentials, usernames and passwords, account balances, transaction histories, and personal identifying information (PII). The breach is attributed to the threat actor “SkyWave”.
	Investing.com	A threat actor claims to be selling a database containing 6.5 million user records from Investing.com, a data collection and internet portal company based in Israel. The compromised data reportedly includes user IDs, registration times, platforms, emails, registration sources, and more, allegedly due to an Insecure Direct Object Reference (IDOR) vulnerability.

Indian data leaks and breaches

Organisation	Significant data
Vision IAS	A massive database allegedly stolen from Vision IAS, a well-known educational institution in India specializing in UPSC Civil Services Examination preparation, has been put up for sale. The breach reportedly includes 1,486,000 user records in a 47GB MySQL dump, exposing personally identifiable information (PII) of students and users. The leaked data is claimed to include full names, email addresses, MD5-hashed passwords, phone numbers, dates of birth, work locations, father's names, and father's employment details. The threat actor behind this claim is “Sorb”.
QBurst	QBurst, a software development firm in India, has allegedly fallen victim to a ransomware attack, with the threat actor “Fog” claiming responsibility. QBurst, a full-service software solutions provider specializing in mobile, web, cloud, and analytics solutions for enterprises worldwide, has reportedly suffered a 7GB data leak as a result of the breach.
SkilloVilla	Bangalore-based edtech company SkilloVilla has allegedly suffered a major data breach, resulting in the unauthorized exposure of over 30GB of sensitive data. The leaked dataset reportedly includes personal information of SkilloVilla’s customers and potential customers, with over 80 million records across 10 databases compromised. This incident highlights the growing cybersecurity risks faced by startups and small businesses globally. The breach is claimed by the threat actor “FutureSeeker”.
PW (PhysicsWallah)	A threat actor claims to be selling the database of PhysicsWallah (PW), an edtech platform, allegedly exposing 2,882,135 customer records. The leaked data reportedly includes full names, email addresses, mobile phone numbers, Twitter handles, company details, addresses, and more.
Maxvy Technologies Pvt	Maxvy Technologies Pvt, an India-based technology company, has allegedly become the latest target of a ransomware attack and data breach. The well-known threat actor “Fog” claims responsibility for the attack, potentially exposing sensitive company data.
Indian State Department's	“NanC”, a prominent threat actor, claims to have panel access to a government ministry in India and is offering it for sale. The actor promoted the ministry access on Telegram channels frequented by cybercriminals. Screenshots of the post reveal offers to provide privileged entry points to backend systems, though the specific ministry remains unnamed. The $80,000 price tag aligns with previous dark web valuations of Indian government datasets, such as the 750 million mobile subscriber records

	that leaked in January 2024. This incident underscores persistent weaknesses in India's digital infrastructure.
Intelliswift	A threat actor, "Louhunter", claims that Intelliswift has a database of 574,000 Indian job seekers and is offering it for sale for $200. This data is said to contain critical details, including personal information, career history, education background, and location data of job seekers on Intelliswift. The compromised information reportedly includes names, contact details, employment history, and social media profiles such as LinkedIn, GitHub, and Twitter.
BC Jindal Group	The threat actor "RansomHub" claims to have carried out a ransomware attack on BC Jindal Group, a leading company in the building materials industry in India. Allegedly, 140 GB of data were exfiltrated.
Interjet	A significant data breach has allegedly impacted the Indian company Interjet, with claims that a vulnerability in its systems has exposed around 5GB of sensitive personal and business-related information. The compromised data reportedly includes identity-confirming images and various business transaction documents, raising concerns about potential misuse. This claim has been made by the threat actor "wewiy15632".
Ministry of Culture	"NanC", a threat actor, has claimed to possess a database allegedly linked to the Ministry of Culture, Government of India, containing personal details of approximately 300,000 individuals. The leaked data reportedly includes names, gender, occupations, and phone numbers, with the dataset formatted as HTML and convertible into CSV for buyers. Shared sample records suggest that a significant portion of the exposed individuals are farmers.

Threat Actors

1. Salt Typhoon

The Salt Typhoon hacking group from China continues to target telecoms globally, successfully infiltrating additional U.S. telecommunications providers through unpatched Cisco IOS XE network devices.they compromised over 1,000 Cisco devices, with more than half located in the U.S., South America, and India. Using internet scanning data. They primarily gained access to targeted networks through stolen credentials, although the exact method of acquiring them is unclear. Once inside, they escalated their access by extracting additional credentials from network device configurations and intercepting authentication traffic such as SNMP, TACACS, and RADIUS.

2. Lazarus

The Lazarus Group, a North Korean state-sponsored cyber threat actor, has remained active throughout February 2025, with notable breaches including the theft of 400,000 Ethereum from the Bybit cryptocurrency exchange, valued at approximately $1.5 billion. This breach, along with other sophisticated attacks, is attributed to the Lazarus Group due to their history of targeting cryptocurrency platforms. Additionally, the group is suspected of exploiting vulnerabilities in Palo Alto firewalls to gain unauthorized access to systems. These recent activities demonstrate their continued focus on financially motivated attacks, particularly in the cryptocurrency sector

3. IntelBroker

Serbian hacker IntelBroker continued his cyberattacks, notably breaching Hewlett Packard Enterprise (HPE) and exposing sensitive data. The stolen information included product source codes, certificates, and private keys. IntelBroker offered to sell this data on BreachForums, claiming access to HPE's API, WePay, and GitHub repositories. HPE initiated an investigation but reported no operational impact or evidence of compromised customer data.

4. Rey

In February 2025, the threat actor known as "Rey" was responsible for several cyberattacks, including breaching Orange Group's Romanian operations by exploiting vulnerabilities in Jira software. Over a month, Rey exfiltrated around 12,000 files, including employee records and project documents, though Orange confirmed no impact on customer operations. Rey also claimed responsibility for a data breach at Zurich Insurance Group, allegedly stealing over 1,400 sensitive files, though Zurich has not publicly confirmed the incident. Additionally, Rey attempted to leak employee data from CrowdStrike, but the company refuted the claims, stating the data was publicly sourced.

5. GhostWriter

Belarusian-linked cyber threat actor known as Ghostwriter intensified its operations, primarily targeting Ukrainian governmental bodies and Belarusian opposition figures. Utilizing sophisticated techniques, Ghostwriter distributed Microsoft Excel documents embedded with Macropack-obfuscated macros to deploy a new variant of PicassoLoader malware.

6. Cl0p

Clop ransomware group continued its operations with notable activity, particularly exploiting the CLEO vulnerability. This vulnerability led to a surge in ransomware attacks, with Clop responsible for 115 public incidents in January alone. The group targeted organizations across various sectors, including the U.S. multinational IT services firm DXC Technology and Chicago Public Schools. Despite these claims, some companies, like Home Depot, denied being impacted by Clop’s ransomware. Additionally, Clop adapted its tactics by exploiting flaws in Cleo file-transfer software, affecting companies such as Blue Yonder.

7. Storm-237

In February 2025, Microsoft identified a phishing campaign conducted by the threat actor Storm-2372, believed to align with Russian interests. Active since August 2024, Storm-2372 targeted sectors including government, NGOs, IT services, defense, telecommunications, health, education, and energy across Europe, North America, Africa, and the Middle East. The campaign employed device code phishing, deceiving users into entering authentication codes that allowed the actors to harvest access tokens for unauthorized account access. Attack vectors included fake messaging app interfaces resembling WhatsApp, Signal, and Microsoft Teams, delivered via email invitations.

8. Black Basta

Black Basta ransomware group gained attention due to the leak of over a year's worth of internal chat logs, revealing that they extorted approximately $107 million in Bitcoin from victims in 2023. The logs also highlighted their tactics, which included exploiting vulnerabilities in Microsoft, Citrix, and network edge devices like those from Fortinet and Cisco. The group primarily targeted exposed RDP and VPN services, using weak credentials to deploy malware.

9. LockBit

LockBit ransomware group attempted to resume operations after a significant disruption in February 2024, when international law enforcement seized their infrastructure. An individual associated with LockBit teased the release of LockBit 4.0, a new locker malware variant, with a countdown to February 3, 2025. However, the group's activities remained limited, possibly due to the previous takedown and ongoing law enforcement pressure. In a coordinated effort, the U.S., U.K., and Australia imposed sanctions on Zservers, a Russia-based bulletproof hosting provider supporting LockBit attacks.

10. FIN7

FIN7, also known as Carbanak, has continued its operations, adapting and evolving its tactics. In mid-2024, researchers uncovered new infrastructure linked to FIN7, with servers located in Russia and Estonia, indicating the group's evolving network strategy. They have also developed and sold tools like AvNeutralizer, designed to tamper with security solutions, showcasing their adaptability and technical expertise. Furthermore, FIN7 has been implicated in ransomware operations, with analyses suggesting connections to groups like Black Basta, highlighting their involvement in diverse cybercrime activities.

Threat Analysis

Notable Incidents

-  **Cyberattack Disrupts Raymond Lifestyle's IT Infrastructure:** On Wednesday, February 19, Raymond Lifestyle, a division of Raymond Limited, a leading textile and clothing company, suffered a cybersecurity attack affecting multiple IT assets. The breach reportedly disrupted parts of the company's IT infrastructure, raising concerns about potential data exposure and operational impact.

-  **zkLend Suffers DeFi Exploit, $9.5M Stolen:** On February 12, 2025, decentralized money-market protocol zkLend, built on Starknet, fell victim to a major cyberattack. Threat actors exploited a smart contract vulnerability to steal 3,600 Ethereum, valued at $9.5 million at the time. Intelligence from the SlowMist Security Team confirmed nearly $10 million in asset losses, raising concerns about security weaknesses in DeFi protocols.

-  **Finastra Discloses Unauthorized Access:** Finastra, a global financial technology provider, has disclosed that an unauthorized third party accessed portions of its IT network. The incident, which occurred between October 31, 2024, and November 8, 2024, involved the compromise of a Secure File Transfer Platform (SFTP) used for technical support. The affected data includes names and financial account information of customers. In response, Finastra engaged cybersecurity experts and law enforcement to investigate the situation. Meanwhile, a threat actor known as "abyss0" has claimed responsibility, alleging possession of 400GB of stolen data and offering it for sale.

-  **Security Incident at NABCO Raises Data Exposure Concerns:** On February 20, 2025, NABCO, a California-based electrical wholesale company, informed the Attorney General of Texas about a security incident involving unauthorized access to its systems. The company revealed that sensitive personal identifiable information (PII) and protected health information (PHI) might have been compromised. The potentially exposed data includes names, Social Security numbers, driver's license numbers, medical records, and health insurance details. The full extent of the breach and the number of affected individuals remain under investigation.

-  **HCRG Care Group Ransomware Attack:** HCRG Care Group, a major UK-based independent community healthcare services provider, is investigating a cybersecurity incident after reportedly being

compromised by the Medusa ransomware operation. The attackers claim to have stolen over 2TB of sensitive data and are demanding a $2 million ransom. Samples of the purportedly stolen data include employees' personal information, sensitive medical records, financial documents, passports, and birth certificates. The company is assessing the breach's impact while working to secure its systems.

-  **Genea Cyberattack Disrupts IVF Services:** Genea, one of Australia's largest IVF providers, has reported a cyberattack that led to unauthorized access to confidential data. The breach has disrupted patient services and raised concerns about the potential exposure of highly sensitive medical, nursing, and scientific information. Genea is actively investigating the incident and working to contain the threat while assessing the impact on affected individuals.

-  **Unimicron Targeted by Ransomware Attack:** A ransomware group has claimed responsibility for a cyberattack on Unimicron, a leading Taiwan-based printed circuit board (PCB) manufacturer. The attackers allege they have stolen 377GB of SQL files and documents from the company's systems and have threatened to leak the data if a ransom is not paid. Unimicron, a public company with operations in Taiwan, China, Germany, and Japan, specializes in manufacturing rigid and flexible PCBs, high-density interconnection (HDI) boards, and integrated circuit (IC) carriers. The breach reportedly affected Unimicron Technology (Shenzhen) Corp., its China-based subsidiary.

-  **OmniGPT Data Exposure Raises Security Concerns:** Popular AI aggregator OmniGPT, which provides access to multiple AI models including ChatGPT-4, Claude 3.5, Gemini, and Midjourney, has reportedly suffered a significant data breach. The attack is said to have exposed personal data from over 30,000 users, with threat actors offering samples of the stolen information. The leaked data allegedly includes all messages exchanged between users and chatbots, along with links to uploaded files and 30,000 user emails. Among the exposed files were office projects, market analysis reports, university assignments, police verification documents, and other sensitive materials containing credentials and billing details.

-  **SimonMed Imaging Targeted in Ransomware Attack:** SimonMed Imaging, a radiology practice based in Scottsdale, Arizona, has reportedly suffered a ransomware attack attributed to the Medusa ransomware group. The attack was identified and interrupted before file encryption, but some systems were temporarily taken offline, causing delays in services. Medusa has claimed responsibility, listing SimonMed Imaging on its data leak site and alleging the theft of 212 GB of data, including medical records, emails, diagnostic images, and Social Security numbers. The group has provided 45 files as proof and is demanding a $1 million ransom, setting a deadline of February 21, 2025. SimonMed Imaging has not confirmed any data theft at this time.

-  **Bybit Suffers Massive Cryptocurrency Heist:** Bybit, a major cryptocurrency exchange, suffered a massive security breach resulting in the theft of over $1.4 billion worth of Ethereum, marking one of the largest cryptocurrency heists to date. The Dubai-based exchange confirmed that hackers infiltrated one of its Ethereum cold wallets during a routine fund transfer to a warm wallet. Approximately 401,347 ETH was stolen, raising serious concerns about security vulnerabilities in digital asset platforms. The incident has sent shockwaves through the crypto industry, highlighting the ongoing risks associated with centralized exchanges and asset storage methods.

Prominent Vulnerabilities**ent and most exploited vulnerabilities in the month of February.**

1. **CVE-2018-19410 | Paessler PRTG Network Monitor Local File Inclusion Vulnerability CVSS: 9.8**

   CVE-2018-19410 is a critical vulnerability in PRTG Network Monitor versions before 18.2.40.1683, allowing remote unauthenticated attackers to create users with read-write privileges, including administrator access. The flaw exists due to improper handling of the 'include' directive in /public/login.htm, which can be exploited through a Local File Inclusion (LFI) attack. By crafting a malicious HTTP request that includes /api/addusers and supplying manipulated 'id' and 'users' parameters, an attacker can create a new privileged user, potentially gaining full control over the affected system.

2. **CVE-2024-53704 | SonicWall SonicOS SSLVPN Improper Authentication Vulnerability CVSS: 9.8**

   CVE-2024-53704 is an improper authentication vulnerability in the SSL VPN authentication mechanism. This flaw allows a remote attacker to bypass authentication and take control of an active SSL VPN session. By exploiting this vulnerability, an attacker can access the user's Virtual Office bookmarks, obtain a client configuration profile for NetExtender, establish a VPN tunnel, and gain access to private networks associated with the compromised account. Additionally, the attacker can forcibly terminate the legitimate user's session, disrupting their connection.

3. **CVE-2025-0994 | Trimble Cityworks Deserialization Vulnerability CVSS: 8.8**

   CVE-2025-0994 is a deserialization vulnerability affecting Trimble Cityworks versions prior to 15.8.9 and Cityworks with Office Companion versions prior to 23.10. The vulnerability allows an authenticated attacker to execute remote code on a customer's Microsoft Internet Information Services (IIS) web server. If exploited, this flaw could enable the attacker to gain control over the affected system, posing a significant security risk.

4. **CVE-2025-0108 | Palo Alto Networks PAN-OS Authentication Bypass Vulnerability CVSS: 8.8**

5. **CVE-2020-29574 | CyberoamOS (CROS) SQL Injection Vulnerability CVSS: 9.8**

CVE-2020-29574 is an SQL injection vulnerability in the WebAdmin interface of Cyberoam OS. This flaw allows unauthenticated attackers to remotely execute arbitrary SQL statements by exploiting improper input validation in the system. A successful attack could lead to unauthorized access to sensitive data, database manipulation, or potential system compromise.

6. **CVE-2024-40890 | Zyxel DSL CPE OS Command Injection Vulnerability CVSS: 8.8**

CVE-2024-40890 describes a post-authentication command injection vulnerability in the CGI program of the legacy Zyxel VMG4325-B10A DSL CPE firmware, specifically version 1.00(AAFR.4)C0_20170615. An authenticated attacker could exploit this flaw by sending a specially crafted HTTP POST request, allowing them to execute operating system (OS) commands on the affected device.

7. **CVE-2022-2374 | Dante Discovery Process Control Vulnerability CVSS: 7.8**

CVE-2022-2374 describes a DLL Sideloading vulnerability in mDNSResponder.exe, where the executable improperly specifies how and from where to load DLL files. This flaw allows an attacker to manipulate the loading process, enabling a legitimate executable to load and execute malicious DLL files. If exploited, this vulnerability can be used to bypass security controls, maintain persistence, and execute arbitrary code on the affected system.

8. **CVE-2024-41710 | Mitel SIP Phones Argument Injection Vulnerability CVSS: 7.2**

CVE-2024-41710 is a vulnerability affecting Mitel 6800 Series, 6900 Series, and 6900w Series SIP Phones, including the 6970 Conference Unit, up to firmware version R6.4.0.HF1 (R6.4.0.136). The flaw exists due to insufficient parameter sanitization during the boot process, allowing an authenticated attacker with administrative privileges to conduct an argument injection attack. If successfully exploited, this vulnerability enables the execution of arbitrary commands within the system's context, potentially compromising the affected devices.

9. **CVE-2018-9276 | Paessler PRTG Network Monitor OS Command Injection Vulnerability CVSS: 7.2**

CVE-2018-9276 is a critical OS command injection vulnerability affecting PRTG Network Monitor versions before 18.2.39. An attacker with administrative privileges and access to the PRTG System Administrator web console can exploit this flaw by sending specially crafted parameters in sensor or notification management scenarios. This vulnerability allows attackers to execute arbitrary commands on both the server and connected devices, potentially leading to system compromise and unauthorized control over the affected environment.

V E-2018-9276 is a critical OS command injection vulnerability affecting PRTG

10. CVE-2025-0411| 7-Zip Mark of the Web Bypass Vulnerability CVSS: 7

CVE-2025-0411 is a vulnerability in 7-Zip that allows remote attackers to bypass the Mark-of-the-Web (MotW) security mechanism. To exploit this flaw, a user must interact with a malicious file or webpage. The issue arises in how 7-Zip handles archived files—when extracting files from a specially crafted archive with the Mark-of-the-Web, the extracted files do not retain this security attribute. As a result, an attacker could leverage this flaw to execute arbitrary code in the context of the current user. This vulnerability was previously tracked as ZDI-CAN-25456.

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