SAPTANG™
Proactive Threat Defence

# Monthly Threat Report
# December 2025

## Contents


Executive Summary ..... 2
Key Highlights ..... 2
Ransomware Activity – December 2025 ..... 4
  Overview ..... 4
  Major Threat Actor Analysis ..... 5
  Sectoral & Geographic Impact ..... 8
  Trends & Strategic Assessment ..... 10
Most Exploited Vulnerabilities – December 2025 ..... 10
  Overview ..... 10
  Key Highlights ..... 11
  Top CVEs Actively Exploited ..... 12
    Enterprise Deserialization & Authentication Issues ..... 12
    Network Appliances & Gateways ..... 13
    Browser & Runtime Exploits ..... 14
    Consumer IoT & Legacy Devices ..... 14
  Observations & Trends ..... 14
  Impact Profile ..... 15
Distributed Denial-of-Service (DDoS) Activity ..... 16
  Overview ..... 16
  Key Threat Groups Observed ..... 17
  Targeted Regions and Sectors ..... 17
  Key takeaways ..... 18
Cyber Incidents - December 2025 ..... 18
  Overview ..... 18
  India incidents ..... 19
  Global incidents ..... 20
Global Data Breach Intelligence Summary - December 2025 ..... 22
  Overview ..... 22
  Major Data Breaches of December 2025 ..... 23
  Strategic Assessment ..... 27
Adversary Simulation Services from Saptang Labs ..... 30
  What We Deliver ..... 30

# Executive Summary

December 2025 featured sustained high cyber threat activity across ransomware, active exploitation of critical vulnerabilities, hacktivist-driven DDoS operations, and multiple high-impact cyber incidents and data breaches with significant downstream/supply-chain exposure.Ransomware disclosures averaged ~724 victim postings across 40+ active operations, with Qilin leading the month (22 victims) followed by Akira (14), Everest (9), SafePay (8), and Warlock (7).

Vulnerability exploitation accelerated around authentication bypass and pre-auth RCE affecting perimeter and enterprise infrastructure, with multiple high-severity issues (including several CVSS 10.0) described as exploited in the wild during the month and Data breach disclosures emphasized third-party compromise and misconfiguration-driven exposure, including multi-million victim impacts (e.g., University of Phoenix ~3.5M; 700Credit ~5.6M) and supplier incidents affecting healthcare and financial ecosystems.

## Key Highlights

### Ransomware Activity:

- Activity remained elevated with ~724 disclosures and an extortion ecosystem described as fragmented across 40 active operations, reinforcing the resilience of the RaaS model.
- Initial access drivers cited included exploited vulnerabilities (30%) and credential compromise (25%), alongside observations of declining payment rates (low 20–40 range) and high recovery success via backups/tools (95% for encrypted victims).

### Vulnerability Exploitation:

- The month’s exploitation narrative centred on rapid weaponization and high-impact compromise of network security appliances and enterprise platforms (Fortinet FortiOS/FortiProxy, Cisco Secure Email Gateway, WatchGuard Firebox, HPE OneView).

## Distributed Denial-of-Service (DDoS) Activity:

- DDoS activity was described as dominated by highly visible hacktivist-style operations, led globally by NoName057(16) and its DDoSia ecosystem.
- India-specific DDoS reporting in the file emphasized sustained DDoS plus defacements against public-facing services, with THE GARUDA EYE and HellR00ters cited for claimed incidents and narrative amplification.

## Cyber Incidents:

- December 2025 marked by sustained ransomware operations, large-scale consumer/service-provider breaches, and systemic downstream impact from supply chain and third-party compromise.
- India's incidents are concentrated on law enforcement actions dismantling cross-border fraud operations (e.g., fake call centres in Mumbai/Noida/Delhi; tech support scams; betting fraud; "digital arrest"/impersonation scams), including references to VoIP tooling, victim datasets, mule accounts, and crypto movement of proceeds.
- Global incidents cited include ransomware disruption at Romania's national water authority ("nearly 1,000 computers"), an IT supplier incident affecting UK GP software provider office systems.

## Data Breaches:

- The multiple significant breach disclosures and attributes a strong share of December impact to third-party compromise and misconfiguration rather than direct, sophisticated intrusion at the end organization.
- Interestingly, Telecom third-party credential compromise (Freedom Mobile) and emphasize detection/reporting gaps (months between compromise and discovery) as a recurring factor increasing breach severity and victim counts.

# Ransomware Activity – December 2025

## Overview

Ransomware continued to pose elevated and persistent threat levels throughout December 2025, with victim postings averaging approximately 724 disclosures across more than 40 active operations, representing sustained high activity compared to prior months. The ecosystem exhibited pronounced fragmentation, with the number of operational extortion groups reaching 40+ including established leaders and emerging affiliates rapidly filling competitive gaps. Despite ongoing law enforcement actions against major players, overall attack volume held firm at record levels, with Qilin leading at 22 victims, followed by Akira (14), Everest (9), SafePay (8), and Warlock (7), illustrating the resilience of the Ransomware-as-a-Service model as disrupted groups cede ground to successors.

Geographically, the United States dominated as the primary target, comprising 55% of incidents where locations were identifiable, trailed by Europe at 25%, Canada at 8%, Asia at 7%, and other regions at 5%. Critical infrastructure and supply-chain sectors absorbed the heaviest impacts, with nearly 55% of attacks hitting manufacturing, healthcare, professional services, and IT/cloud providers, manufacturing surging notably due to Qilin's focus. The top 10 groups captured about 65% of published victims, down slightly from prior periods amid affiliate migrations and smaller operators gaining traction in the decentralized landscape.

Payment rates appeared to decline further into the low 20-40% range compared to earlier 2025 figures, signalling bolstered organizational resilience, while median demands hovered around $1.2–1.5 million amid market saturation. Recovery success reached 95% for encrypted victims via backups or tools, though 30% of incidents stemmed from exploited vulnerabilities like VPN flaws, followed by credential compromise at 25%, highlighting enduring risks across sectors and regions despite defensive gains.

# Major Threat Actor Analysis

## Qilin – Expansive Industrial and Healthcare Campaigns

The Qilin operation dominated the threat landscape with **22 recorded victims**, a strong performance that reinforced its position as one of the most prolific ransomware operators. The activity concentrated heavily in the United States while extending across Europe and Asia, revealing a sophisticated affiliate network with global reach. Targets included major North American manufacturers, mid-sized industrial firms in Germany and France, and healthcare providers in Canada, demonstrating a pattern of prioritizing operationally critical infrastructure for maximum disruption. Qilin employs **aggressive double-extortion tactics** with high efficiency, using robust encryption to block recovery and data-leak threats to inflict reputational damage, creating a deliberate strategy that exploits downtime sensitivity in manufacturing and healthcare to force rapid payment negotiations.

## Akira – Sustained U.S. and Global Operations

Akira registered **14 victims**, successfully sustaining the operational momentum seen previously through globally dispersed attacks spanning North America, Europe, and Asia, with a particular emphasis on the United States. The group targeted a diverse mix of professional services, industrial firms, and IT providers, including law firms in the U.S., manufacturing companies in Germany, and consultancies in Canada and India. Akira affiliates heavily favor intrusion through **misconfigured or weakly secured VPN and RDP endpoints**, a pattern that capitalizes on poor patching hygiene and lack of Multi-Factor Authentication (MFA) to enable opportunistic compromises across varied organizations.

## Everest – High-Visibility Healthcare and Professional Services

Everest claimed **9 victims**, focusing on data-rich organizations where public exposure and sensitivity provide strong extortion leverage, with a clear pattern of targeting healthcare and accounting entities primarily in North America. Notable victims included Gramercy Surgery Center, Cukierski & Associates LLC, Pureform Radiology Center, and Rundle Eye Care, all featuring extensive medical and financial data thefts. The group's strategy revolves around **double-extortion with large-scale exfiltration (400+ GB)**,

detailed leak site publications, and countdown timers designed to exploit reputational risks and patient privacy concerns for accelerated compliance.

## SafePay – Opportunistic Industrial and Services Attacks

SafePay disclosed **8 victims**, following an opportunistic pattern across manufacturing, IT services, and healthcare, with strong U.S. and European representation. Targets included mid-sized manufacturers, regional medical centers, and logistics Small and Medium-sized Businesses (SMB), reflecting a broad-net approach to mid-market disruption. SafePay's tactics emphasize classic **double-extortion with rapid exfiltration** and leak site pressure, capitalizing on common perimeter weaknesses to maintain consistent volume against resource-constrained defenders.

## Warlock – Cross-Border SMB and Manufacturing Focus

Warlock registered **7 victims**, showing a pattern of targeting Small and Medium-sized Businesses (SMB) and manufacturing in Russia and allied regions alongside global outreach. Victims encompassed Russian-based manufacturing firms and international SMBs, an unusual concentration suggesting evolving motivations or regional broker networks. The group deploys standard encryption with data leaks, focusing on **operational recovery pressure** for smaller entities lacking advanced defenses.

## Interlock – Financial and Community Services Pressure

Interlock logged **6 victims**, exhibiting a pattern of targeting small financial institutions and community organizations where operational and reputational pressure yields quick results. Victims included Issaqueena Pediatric Dentistry, Pocono Farms Country Club, and regional SMBs with exposed financial records, concentrated in the U.S. This focuses on niche, under-resourced entities allow Interlock to employ **efficient data-theft-first operations**, leveraging Personally identifiable information (PII) leaks and "shaming" narratives to coerce payments without needing extensive encryption infrastructure.

## Leaknet – Multi-Sector Data Exposure Operations

Leaknet accounted for **5 victims**, demonstrating a pattern of pure data-extortion across logistics, healthcare, and Small and Medium-sized Businesses (SMB) retail, with

geographic spread in Europe and North America. Notable victims comprised regional logistics firms, healthcare providers with **50,000+ patient records**, and SMBs with customer financial data. The group prioritizes investigative-style leak narratives highlighting victim vulnerabilities like **outdated defenses and poor segmentation**, amplifying damage through public storytelling rather than traditional encryption to drive compliance.

## Direwolf – Emerging Multi-Sector Extortion

Direwolf claimed **6 victims** as a newer actor, displaying a broad multi-sector pattern including construction, education, and finance across the U.S. and Europe. Notable hits involved mid-tier construction companies and financial services Small and Medium-sized Businesses (SMB). Direwolf's double-extortion model leverages **crypto-ransomware with leak threats**, targeting mid-sized businesses through exploited public-facing apps and credential abuse to build its operational footprint.

## PayoutsKing – Newcomer Disruption Focus

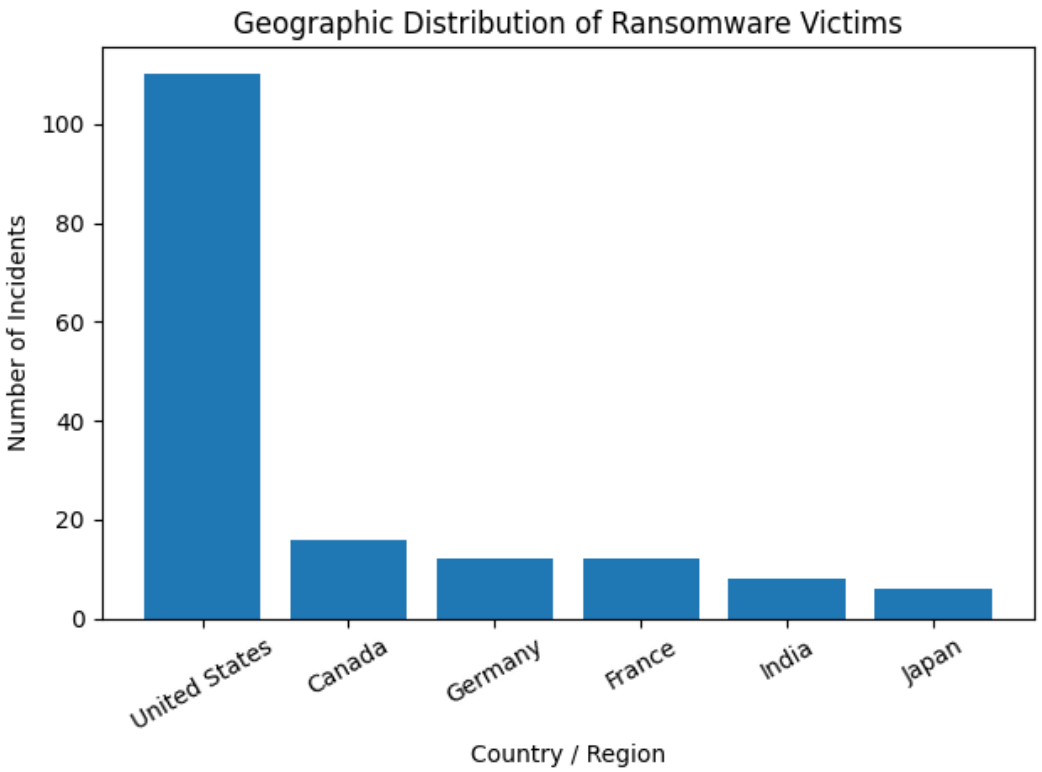
PayoutsKing emerged with **5 victims**, targeting healthcare, construction, and education with a pattern of rapid encryption and backup deletion for maximum disruption. Victims included hospitals, regional schools, and construction firms in North America. The group maximizes damage by combining **file encryption ([.]payoutsking extension)**, ransom notes, and leak site threats, positioning itself as an aggressive newcomer against time-sensitive sectors.

## Cl0p – Enterprise Software Zero-Day Exploitation

Cl0p posted **4 high-impact victims**, adhering to its signature pattern of exploiting enterprise software vulnerabilities for mass data harvesting, primarily in manufacturing and tech sectors globally. Victims included organizations compromised via Oracle EBS and similar platforms. Cl0p favors pure extortion through **auction-style leaks over encryption**, focusing on supply-chain leverage to affect numerous downstream entities efficiently.

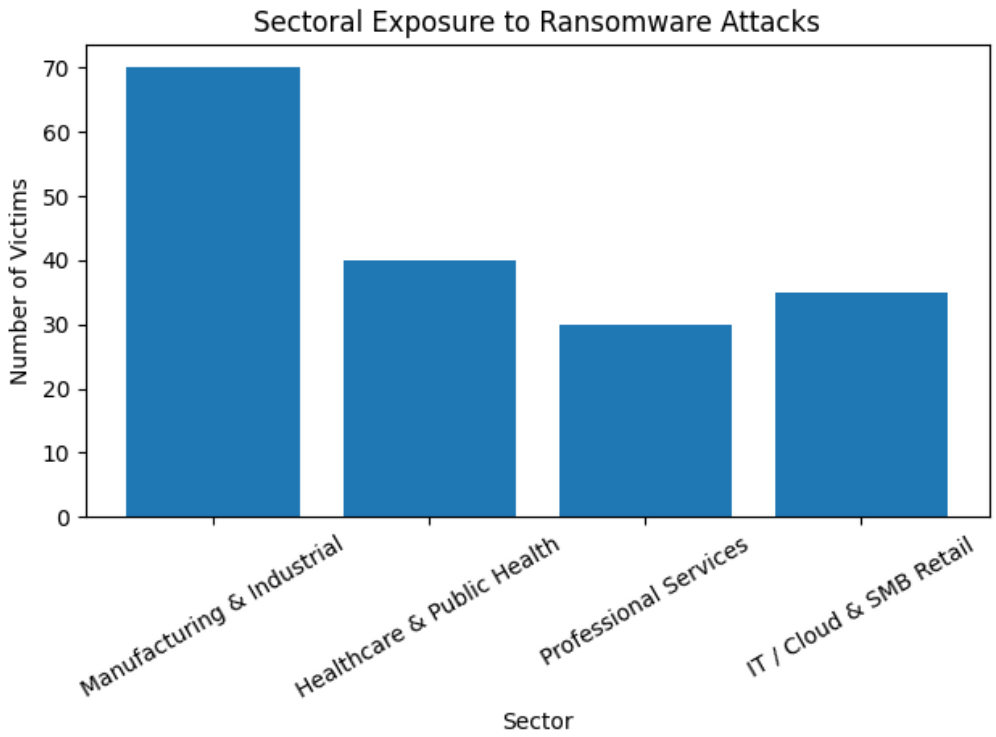
## Sectoral & Geographic Impact

### 1) Geographic Distribution




The **United States** remained, by a substantial margin, the primary target theatre, accounting for **55% of tracked victims with over 110 incidents driven by Qilin, Akira, and Everest operations.** This concentration reflects the density of high-value industrial and healthcare targets alongside perceived ransom payment willingness. Significant activity also appeared in Canada (8%), Germany and France (combined 12%), and scattered cases across India and Japan (7%), with newer groups like Direwolf expanding European footprints and underscoring the transnational nature of Ransomware-as-a-Service (RaaS) affiliate networks.

## 2) Sectoral Exposure




The targeting pattern reveals a calculated emphasis on sectors exhibiting low tolerance for operational disruption and high data sensitivity

- **Manufacturing and Industrial Supply Chains:** Leading with **approximately 70 victims**, this sector faced relentless pressure from Qilin and SafePay due to legacy OT/ICS systems and immediate downtime costs.
- **Healthcare and Public Health:** Approximately **40 breaches** targeted patient data networks, exploiting fragmented infrastructure for humanitarian and regulatory leverage.
- **Professional Services:** Around **30 victims** including accounting and law firms hit by Akira, valued for client PII and financial records.
- **IT/Cloud Services and SMB Retail:** Combined **~35 victims** from VPN exploits and data theft, pursued for customer databases and IP re-sale.

## Trends & Strategic Assessment

### Escalating Victim Volume

December showed sustained high attack rates with 724 disclosures, indicating aggressive scaling among top RaaS groups like Qilin and persistent affiliate success, as defenses fail to outpace offensive tooling evolution.

### Dominance of High-Volume Actors

A handful of elite operators accounted for 60%+ of incidents, their industrialized pipelines blurring lines between syndicates and professional services, enabling consistent global efficiency.

### Persistent Targeting of Critical Services

Manufacturing, healthcare, and professional services endured disproportionate hits due to downtime intolerance and cascading financial/safety risks, amplifying double-extortion effectiveness.

### Evolving Geopolitical Distribution

U.S. primacy persists, but expansion into Canada/Europe signals diversifying affiliates and C2 hosting to counter law enforcement disruptions.

### Fragmentation and Affiliate Overlap

Shared RDP/VPN tactics across Qilin, Akira, and Play suggest tooling overlapping and affiliate crossover, hindering attribution while fueling rapid rebranding under pressure.

# Most Exploited Vulnerabilities – December 2025

## Overview

December 2025 exploitation activity was defined by unprecedented weaponization speed and targeting of critical network security infrastructure, enterprise authentication systems, and modern web application frameworks. The month was dominated by authentication bypass vulnerabilities, zero-day exploitation of network perimeter devices, and framework-level remote code execution flaws affecting enterprise infrastructure and cloud-native applications.

**The exploitation landscape highlights three dominant vectors:**

1. **Network Perimeter & Security Appliance Exploitation**: Critical authentication bypass and zero-day vulnerabilities in Fortinet FortiOS/FortiProxy (CVE-2025-59718), Cisco Secure Email Gateway (CVE-2025-20393), WatchGuard Firebox (CVE-2025-14733), and HPE OneView (CVE-2025-37164) gave attackers unauthenticated administrative access to enterprise security infrastructure. These compromises enabled persistent backdoor establishment, configuration file exfiltration, and lateral movement capabilities across protected networks.

2. **Framework & Runtime Infrastructure Targeting**: A critical pre-authentication RCE in React Server Components (CVE-2025-55182) moved from disclosure to active exploitation within hours, triggering state-sponsored mass scanning campaigns. This was joined by serialization injection flaws in LangChain (CVE-2025-68664) and workflow automation vulnerabilities in n8n (CVE-2025-68613), demonstrating attackers' strategic pivot toward compromising development frameworks and automation platforms that affect thousands of downstream applications.

3. **Mobile & Supply Chain Compromise**: Zero-day exploitation of Android Framework vulnerabilities (CVE-2025-48633, CVE-2025-48572) by commercial spyware vendors and supply chain compromise of ASUS Live Update (CVE-2025-59374) revealed sophisticated targeting of consumer endpoints and software distribution mechanisms for persistent access and surveillance capabilities.

## Key Highlights

- **Fortinet FortiOS SAML Authentication Bypass**: A critical SAML signature verification flaw in Fortinet FortiOS/FortiProxy (CVE-2025-59718) was actively exploited in the wild starting December 12, allowing unauthenticated attackers to bypass FortiCloud SSO and immediately download system configuration files containing credentials.

- **React Server Components "React2Shell" Zero-Day**: A maximum CVSS 10.0 pre-authentication RCE in React Server Components (CVE-2025-55182) affecting Next.js and related frameworks was exploited within hours of December 3 disclosure by state-aligned threat actors, enabling arbitrary code execution through malicious HTTP requests via insecure deserialization.

- **Cisco Secure Email Gateway Zero-Day Campaign**: A CVSS 10.0 remote command execution vulnerability (CVE-2025-20393) in Cisco AsyncOS was exploited as a zero-day on December 10, allowing attackers to execute root-level commands and plant persistence mechanisms. Cisco attributed attacks to state-aligned actors.

- **WatchGuard Firebox VPN Zero-Day**: An out-of-bounds write vulnerability (CVE-2025-14733) in WatchGuard Fireware OS was actively exploited in the wild, with threat actors encrypting and exfiltrating VPN configuration files from mobile user and branch office VPN deployments.

- **HPE OneView Unauthenticated RCE**: A CVSS 10.0 unauthenticated remote code execution vulnerability (CVE-2025-37164) in HPE OneView infrastructure management platform allowed attackers to execute arbitrary code via /rest/id-pools/executeCommand endpoint without authentication.

- **Android Framework Targeted Exploitation**: Two Android Framework vulnerabilities (CVE-2025-48633 information disclosure, CVE-2025-48572 privilege escalation) were exploited in limited, targeted attacks affecting Android 13-16, likely by commercial spyware vendors.

## Top CVEs Actively Exploited

### Enterprise Deserialization & Authentication Issues

- **CVE-2025-55182 (React2Shell - React Server Components RCE)** - CVSS 10.0 Critical pre-authentication remote code execution vulnerability affecting React Server Components, Next.js, and related frameworks allowing attackers to execute arbitrary code through malicious HTTP requests via insecure deserialization.

- **CVE-2025-68664 (LangChain Core Serialization Injection)** - CVSS 9.3 Serialization injection vulnerability in LangChain's dumps() and dumpd() functions enabling secret theft and prompt injection through unsafe serialization when user-controlled data contains 'lc' keys.
- **CVE-2025-68613 (n8n Workflow Automation RCE)** - CVSS 9.9 Authentication-based vulnerability allowing authenticated attackers to execute arbitrary code with privileges of the n8n process due to insufficient isolation of expression evaluation context, affecting 103,476 potentially vulnerable instances globally.

## Network Appliances & Gateways

- **CVE-2025-20393 (Cisco Secure Email Gateway Zero-Day)** - CVSS 10.0 Remote Command Execution vulnerability in Cisco AsyncOS Software for Secure Email Gateway and Secure Email and Web Manager, exploited as zero-day on December 10, 2025, allowing attackers to execute root-level commands and plant persistence mechanisms.
- **CVE-2025-37164 (HPE OneView Unauthenticated RCE)** - CVSS 10.0 Critical unauthenticated remote code execution vulnerability in HPE OneView affecting versions before 11.0, allowing attackers to execute arbitrary code on infrastructure management platforms. Exploitable via /rest/id-pools/executeCommand endpoint reachable without authentication
- **CVE-2025-59718 (Fortinet FortiCloud SSO Authentication Bypass)** - CVSS 9.8 Improper verification of cryptographic signature vulnerability in Fortinet FortiOS, FortiProxy, and FortiSwitchManager allowing unauthenticated attackers to bypass FortiCloud SSO login authentication via crafted SAML response message
- **CVE-2025-14733 (WatchGuard Firebox VPN Zero-Day)** - CVSS 9.3 Out-of-bounds write vulnerability in WatchGuard Fireware OS iked process allowing remote unauthenticated attackers to execute arbitrary code, affecting mobile user VPN with IKEv2 and branch office VPN configurations.

## Browser & Runtime Exploits

- **CVE-2025-48572 (Android Framework Privilege Escalation)** - CVSS 7.4 Elevation of privilege vulnerability in Android Framework affecting Android 13-16, allowing local attackers to gain higher-than-intended privileges through improper input validation.
- **CVE-2025-48633 (Android Framework Information Disclosure)** – CVSS 5.5 Information disclosure vulnerability in Android Framework affecting Android 13-16, exploited in limited, targeted attacks allowing local applications to access sensitive information through improper input validation

## Consumer IoT & Legacy Devices

- **CVE-2025-59374 (ASUS Live Update Supply Chain Compromise)** - CVSS 9.3 Embedded malicious code vulnerability in ASUS Live Update client stemming from supply chain compromise where certain Live Update versions were distributed with embedded malicious code targeting specifically identified devices

## Observations & Trends

- **Critical Infrastructure & Network Perimeter Focus**: Attackers heavily concentrated on network security appliances and enterprise infrastructure platforms like Fortinet FortiOS/FortiProxy, Cisco Secure Email Gateway, WatchGuard Firebox, and HPE OneView. Compromising these perimeter devices provides high payoff, enabling persistent backdoor access, lateral movement capabilities, and administrative control over enterprise security infrastructure.

- **Framework & Runtime Exploitation Surge**: The React Server Components "React2Shell" vulnerability demonstrated attackers' strategic pivot toward modern web frameworks and JavaScript runtime environments. Targeting Next.js, React, and n8n workflow automation platforms enables widespread application compromise through single framework vulnerabilities affecting thousands of downstream applications.

- **Zero-Day Weaponization Speed**: Multiple vulnerabilities were exploited as zero-days before patches became available, with Cisco Secure Email Gateway, SonicWall SMA1000, and WatchGuard Firebox all experiencing active exploitation during patch development. State-aligned threat actors demonstrated capability to discover and weaponize vulnerabilities before vendor awareness, compressing traditional vulnerability lifecycle timelines.

- **Authentication Bypass as Primary Vector**: Authentication-related flaws dominated the threat landscape, with SAML signature verification bypass (Fortinet), unauthenticated RCE (HPE OneView, Cisco), and cryptographic signature validation failures enabling attackers to achieve administrative access without credential compromise. This represents a shift from credential-based attacks toward exploiting authentication protocol weaknesses.

- **Supply Chain & Development Tool Targeting**: Exploitation of ASUS Live Update supply chain compromise, LangChain serialization vulnerabilities, and n8n workflow automation demonstrates attackers' recognition that compromising development tools, CI/CD pipelines, and automation platforms provides multiplicative impact across downstream customers and internal operations.

## Impact Profile

- **Severity:** Majority carried Critical (9.0-10.0) or High (7.4-9.9) severity ratings, with four vulnerabilities achieving maximum CVSS 10.0 scores, associated with unauthenticated RCE, authentication bypass, and root-level privilege escalation.
- **Exploitation Outcomes Observed:**
    - **Initial access and administrative takeover** (Fortinet FortiOS SAML bypass, HPE OneView unauthenticated RCE, Cisco Secure Email Gateway root access)
    - **Ransomware deployment** (Fortinet appliance compromise, react framework exploitation enabling application-layer access)

- **Credential and configuration file harvesting** (FortiOS configuration downloads, WatchGuard encrypted file exfiltration)
- **Persistent backdoor establishment** (Cisco Email Gateway implant deployment, SonicWall root-level persistence)
- **Framework-wide application compromise** (React2Shell affecting Next.js deployments, n8n workflow automation exploitation)
- **Android device compromise** (Targeted spyware deployment via Android Framework vulnerabilities)
- **Supply chain malware distribution** (ASUS Live Update embedded malicious code affecting specifically targeted devices)

**Threat Type Balance**: Activity revealed a bimodal distribution of highly targeted, state-sponsored intrusions (Cisco Email Gateway, Android Framework spyware, ASUS supply chain compromise) and widespread opportunistic scanning (React2Shell mass exploitation, Fortinet FortiOS authentication bypass campaigns, HPE OneView appliance targeting). State-aligned actors demonstrated strategic patience with zero-day development while opportunistic groups raced to exploit publicly disclosed vulnerabilities within hours of disclosure. The prevalence of maximum CVSS 10.0 scores and authentication bypass vectors indicates attackers achieved unprecedented access levels with minimal complexity requirements.

# Distributed Denial-of-Service (DDoS) Activity

## Overview

December 2025 DDoS activity was dominated by highly visible hacktivist-style operations, led globally by NoName057(16) and its DDoSia ecosystem, alongside India-focused actors leveraging disruption for propaganda and reputational impact. In parallel, India experienced intensified DDoS and defacement activity against public-facing services, with groups such as THE GARUDA EYE and HellR00ters explicitly cited as claiming incidents and amplifying narratives via social platforms.

## Key Threat Groups Observed

- **NoName057(16) / DDoSia** remained the most visible global DDoS operator in December reporting, with weekly intelligence tracking coordinated campaigns.
- **NoName057(16) / DDoSia (Denmark-focused week)** was reported as conducting a coordinated campaign (15–21 Dec) resulting in “4,559 recorded attack entries,” targeting “148 unique domains” and “137 unique IP addresses” across multiple countries.
- **THE GARUDA EYE** and **HellR00ters** were specifically cited in December reporting as claiming multiple DDoS/defacement incidents impacting India, using social channels to publicize activity and amplify impact narratives.

## Targeted Regions and Sectors

- **Europe and international domains** were repeatedly targeted by the NoName057(16) campaigns (from 22–28 December).
- **India** experienced intensified hacktivist-driven disruption activity, with reporting emphasizing sustained DDoS and defacements against public-facing services.
- In **NoName057(16) target distribution**, government/public sector targets formed the largest share in one referenced dataset (41.09%), followed by sectors such as transportation/logistics and telecommunications.

## Attack Characteristics and Motivation

- **NoName057(16)’s / DDoSia** model relies on a Go-based client that enables low-skill volunteers to participate, recruited via Telegram and incentivized with cryptocurrency rewards, aligning activity to political “information operation” goals while scaling volume.
- Observed techniques described for DDoSia include both volumetric and resource-exhaustion methods (e.g., SYN/ACK floods, HTTP GET floods, Slow Loris “nginx_loris”), typically aimed at **ports 443/80** to disrupt web-facing services.

## Key takeaways

- Treat **government and education portals** (additionally telecom/retail-facing services) as primary DDoS pressure points in India, given sustained hacktivist disruption and defacement emphasis in this month.
- Build defences for **web-layer exhaustion** (rate limiting, WAF tuning, origin shielding, connection-limit protections) in addition to volumetric scrubbing, since DDoSia-style operations explicitly mix L3/L4 floods with L7 and Slow Loris variants.
- **Operationalize "claim-driven" response**: strengthen the monitoring and rapid communications playbook because adversaries actively amplify incidents via social channels, and reported campaigns show repeated multi-target waves across countries/domains in this month.

# Cyber Incidents - December 2025

## Overview

December 2025 was characterized by sustained ransomware operations, large-scale data breaches at consumer-facing and service-provider organizations, and an ongoing pattern of supply-chain and third-party compromise driving downstream impact across multiple sectors. Prominent incidents included major breaches at education, retail, and financial data processors such as the University of Phoenix, 700Credit, and Petco. where exposed records numbered in the millions and were often traced back to misconfigurations or weaknesses in vendor environments rather than direct attacks on end organizations.

In India, December's activity centred on dismantling cross-border fraud infrastructures, with enforcement actions against fake call centres in Mumbai, Noida, and Delhi that were defrauding foreign nationals through tech-support scams, online betting schemes, and authority-impersonation tactics. These operations alongside continued national focus on "digital arrest" scams and impersonation-based financial crime,

highlighted India's dual role as both a target and an operational hub for high-volume cyber-enabled fraud.

Globally, incidents at healthcare and public-service suppliers, including an NHS GP software provider in the UK and multiple US service providers, underscored the fragility of critical services when upstream vendors are compromised. Taken together, December's events reinforce a strategic shift where configuration errors, third-party weaknesses, and service-provider breaches are increasingly the preferred paths for attackers, amplifying systemic cyber risk well beyond the initially compromised organizations.

## India incidents

- **Mumbai fake call center's defrauding US citizens busted -** Mumbai Police Crime Branch raided two fake call centers in Andheri (East) that were impersonating US government officials and threatening foreign nationals with legal action to extort money. Officers arrested nine suspects and seized 11 laptops, 18 phones, VoIP infrastructure, and victim data used in scripted scam calls. The case highlights India's role as an operational base for cross-border intimidation and "digital arrest"-style fraud against overseas victims.

- **Noida sham call centre running betting and fraud schemes -** Noida Police arrested two people from Sector 9 for running a bogus call centre that lured victims into online betting and related schemes. More than 10 bank accounts opened with forged documents were linked to the fraud, with lakhs of rupees already frozen during the investigation. The incident underscores continued misuse of fake KYC and mule accounts for organised cyber fraud in the NCR region.

- **North Delhi flat used to cheat US citizens via tech-support scam -** Delhi Police exposed an illegal call-centre-style operation from a flat in north Delhi, where seven operatives posed as technical support staff to defraud US citizens. Victims were coerced into making payments that were later moved through cryptocurrency

channels, illustrating the blending of classic tech-support fraud with crypto-based money laundering.

- **Ongoing action against "digital arrest" and authority-impersonation scams -** Central agencies and CBI advanced cases and chargesheets in major "digital arrest" scams where victims were confined on video calls and coerced into high-value transfers by fake law-enforcement officials. Public advisories and analysis at the end of 2025 identified digital arrest, phishing/OTP fraud, and identity-theft-based scams as leading typologies in India's cyber fraud surge.

## Global incidents

- **Romania's national water authority hit by ransomware (Romanian Waters) -** Romania's national water management authority (Romanian Waters) suffered a ransomware attack that reportedly impacted nearly 1,000 computers and disrupted some internal operations. Authorities confirmed service disruption and incident response activity, highlighting the growing risk to environmental and public-utility bodies in Europe.

- **Right Power Technology (Malaysia) -** Malaysian company Right Power Technology Sdn Bhd was listed by the Space Bears ransomware group, which claimed to have exfiltrated internal data and published it on their leak site. The incident underscores the spread of newer ransomware operations targeting Asian critical infrastructure and energy-related firms.

- **NHS GP software supplier cyber-attack (UK) -** An IT supplier providing software to General practitioners (GPs) practices in the UK disclosed a "security incident" in a stock exchange filing on 18 December 2025, affecting its office IT systems. While clinical systems were reported as mostly resilient, the incident raised concerns about supply-chain exposure in national healthcare delivery.

- **University of Phoenix : third-party breach (~3.5 million affected) -** The University of Phoenix announced a data breach after a third-party provider detected unauthorised access to systems holding student, applicant, and staff records. Around 3.5 million individuals were affected, with exposed data including personal identifiers and contact details, driving regulatory scrutiny and large-scale notification obligations.

- **Inotiv pharmaceutical firm (ransomware data breach disclosure) -** Inotiv confirmed in December that a ransomware incident earlier in the year resulted in unauthorised access and theft of personal information for 9,542 individuals. Exposed data included names, addresses, dates of birth, and social security numbers, reinforcing the persistent targeting of pharma and research entities by extortion groups.

- **700Credit : automotive credit data breach (~5.6 million individuals) -** Credit data provider 700Credit disclosed a breach that exposed information for approximately 5.6 million individuals tied to automotive credit checks and dealer services. Investigations pointed to weaknesses in third-party controls and data access governance rather than exotic exploits, amplifying concern over downstream risk in financial services supply chains.

- **Petco security lapse exposing customer data -** Petco reported that a misconfiguration in one of its software applications allowed certain customer files to be publicly accessible on the internet until corrected. The incident illustrated how simple configuration errors in retail environments can expose sensitive customer data without any direct intrusion by threat actors.

- **Coupang data breach fallout : CEO resignation (South Korea) -** South Korean e-commerce giant Coupang continued dealing with the fallout of a major data breach revealed in December, culminating in the resignation of CEO Park Dae-jun reported on 10 December 2025. The breach and leadership change underlined the

regulatory and reputational impact that large-scale customer data exposures can have in Asia’s digital retail sector.

- **Marquis Software Solutions ransomware : US banks and credit unions -** Marquis Software Solutions reported a ransomware attack that affected data for more than 780,000 customers of US banks and credit unions relying on its services. The case showcased the systemic risk posed by a single service provider in the financial sector, as multiple institutions faced breach notifications from one upstream incident.

# Global Data Breach Intelligence Summary - December 2025

## Overview

December 2025 saw escalating cybersecurity incidents across multiple sectors, with the Clop ransomware gang's Oracle E-Business Suite zero-day campaign reaching its peak impact. The month was characterized by mass-scale educational institution breaches affecting over 3.5 million individuals at University of Phoenix alone, ransomware attacks on pharmaceutical research organizations, and critical third-party compromise incidents in telecommunications and financial services. Notable patterns included sophisticated supply chain infiltrations through compromised subcontractor credentials, widespread misconfiguration vulnerabilities exposing millions of records, and the continued exploitation of enterprise software platforms. The healthcare sector faced particularly severe impact with Aflac's 22.65 million record breach, while international retail giants like Coupang experienced catastrophic leadership and financial consequences. December disclosures revealed an average detection gap of 3-5 months between initial compromise and discovery, enabling threat actors to exfiltrate sensitive data including Social Security numbers, financial information, and proprietary research across education, healthcare, finance, and technology sectors.

The following intelligence summary highlights the most significant verified breach incidents from December 2025, reflecting a continued trend toward supply chain

compromises and social engineering attacks that demonstrate the evolving sophistication of threat actor operations.

## Major Data Breaches of December 2025

### 1) Petco Data Breach

- **Vulnerability:** Application misconfiguration - incorrect software setting allowed files to be accessible online without proper restrictions (Insecure Direct Object Reference - IDOR)
- **Estimated Victims:** At least 500+ customers (exact number not disclosed; California filing requires disclosure for 500+ residents)
- **Discovery Date:** December 3-5, 2025
- **Description:** Petco's veterinary services company Vetco had a security lapse that allowed anyone on the internet to download customer records without needing login credentials.
- **Attack Methodology:** The security lapse involved an insecure direct object reference, allowing unfettered access to files because proper authentication checks were not in place. Customer numbers were sequential, enabling access to other customers' data by simply changing digits in the web address.
- **Confirmed Major Victims:** Petco/Vetco customers in California (500+), Texas (329), Massachusetts (7), and Montana (3)
- **Response Measures:** Petco immediately corrected the application settings, removed files from online access, and implemented additional security measures and technical controls. The company offered complimentary credit and identity monitoring services to affected individuals.
- **Potential Impact :** Exposed information included Social Security numbers, driver's license numbers, account numbers, credit or debit card numbers, and birth dates.Also included customer veterinary records, visit summaries, medical histories, and prescription/vaccination records for pets.

## 2) University of Phoenix Data Breach

- **Threat Actor:** Clop ransomware gang (Cl0p)
- **Vulnerability:** Oracle E-Business Suite (EBS) zero-day vulnerability (CVE-2025-61882)
- **Estimated Victims:** 3,489,274 individuals (approximately 3.5 million)
- **Timeline / Discovery Date:**
  - **Breach occurred:** August 13-22, 2025
  - **Discovered:** November 21, 2025 (after Clop added university to leak site)
  - **Disclosed:** Early December 2025
- **Description:** An unauthorized third party exploited a previously unknown software vulnerability in Oracle EBS to exfiltrate data from the University's Oracle EBS environment. The breach went undetected for over three months, affecting current and former students, faculty, staff, and suppliers.
- **Attack Methodology:** The Clop ransomware gang exploited a zero-day flaw in Oracle EBS since early August 2025 to steal data from victims' Oracle EBS platforms.
- **Confirmed Major Victims:** University of Phoenix students, staff, faculty, and suppliers
- **Claimed Victims Include:** Part of a wider campaign that also affected Harvard University, University of Pennsylvania, Dartmouth College, Tulane University, and Southern Illinois University, External cybersecurity firms were engaged for investigation.
- **Response Measures:** The university is offering free identity protection services including 12 months of credit monitoring, identity theft recovery assistance, dark web monitoring, and a $1 million fraud reimbursement policy
- **Potential Impact:** Exposed data includes names, contact information, dates of birth, Social Security numbers, and banking details, Bank account and routing numbers were obtained "without means of access" according to the university.

## 3) Inotiv Data Breach

- **Threat Actor:** Qilin ransomware gang (also known as Agenda)
- **Vulnerability:** Ransomware attack with unauthorized system access and encryption
- **Estimated Victims:** 9,542 individuals
- **Timeline / Discovery Date:**
  - **Breach occurred:** August 5-8, 2025
  - **Discovered:** August 8, 2025 (when systems were encrypted)
  - **Data breach dimension disclosed:** December 2025
- **Description:** A ransomware group had access to Inotiv's network between approximately August 5 and August 8, 2025, during which time certain data may have been acquired. The pharmaceutical contract research organization experienced system encryption and operational disruption.
- **Attack Methodology:** Threat actors gained unauthorized access to Inotiv systems, moved laterally to critical servers, exfiltrated data, and then deployed ransomware, encrypting internal systems and forcing network shutdowns
- **Confirmed Major Victims:** Current and former Inotiv employees, their family members, and individuals linked to Inotiv's business or acquisitions
- **Claimed Victims Include:** The Qilin ransomware gang claimed to have stolen about 162,000 files totaling 176GB, including research data collected over the last 10 years
- **Response Measures:** Inotiv secured affected systems, engaged external cybersecurity specialists, notified law enforcement authorities, and offered identity monitoring services to impacted individuals. The company has since restored access to affected networks and systems.
- **Potential Impact:** Exposed data included personal information such as full names, addresses, dates of birth, and Social Security numbers, with no payment card details or banking information involved. The breach also included potentially health-related or employment-related information.

## 4) Freedom Mobile Data Breach

- **Vulnerability:** Compromised third-party subcontractor account credentials
- **Estimated Victims:** Limited number (exact count not disclosed; company has 3.5 million total customers)
- **Timeline / Discovery Date:**
  - **Discovered:** October 23, 2025
  - **Disclosed:** December 3, 2025
- **Description:** Attackers hacked Freedom Mobile's customer account management platform by using the account of a subcontractor to gain access to personal information. This was Canada's fourth-largest wireless carrier breach affecting customer data.
- **Attack Methodology:** A third party used the account of a subcontractor to gain access to the personal information of customers. The company emphasized this was not a ransomware attack and network operations were not affected.
- **Confirmed Major Victims:** Freedom Mobile customers (limited number, geographically dispersed)
- **Response Measures:** Freedom Mobile quickly identified the incident and implemented corrective measures including blocking suspicious accounts and corresponding IP addresses. The company offered free credit monitoring services for one year to affected customers and enhanced security protocols with multi-factor authentication for third-party accesses.
- **Potential Impact:** Personal information compromised includes names, addresses, phone numbers, dates of birth, and customer account numbers. Payment information and passwords were not affected. The stolen data poses risks for identity theft, phishing scams, and SIM-swapping attacks.

## Strategic Assessment

December 2025 breaches collectively illustrate several critical trends in the cyber threat landscape:

**1) Supply Chain as Primary Attack Vector:**

The overwhelming majority of December breaches originated from third-party vendors and service providers rather than direct organizational compromises. The Oracle EBS zero-day exploitation campaign demonstrated how a single enterprise software vulnerability cascaded across multiple sectors, , affecting universities (Harvard, Dartmouth, Penn, University of Phoenix), healthcare organizations, and corporations globally. The Marquis Software breach affecting 70+ financial institutions through SonicWall vulnerability exemplifies how vendor-managed services create concentrated risk. Third-party breaches at 700Credit, Lockton Companies, and various subcontractors show that organizations no longer control their own security perimeters—they inherit the weaknesses of every partner in their digital ecosystem.

**2) Social Engineering Sophistication:**

Breaches at Freedom Mobile through compromised subcontractor accounts and the Marquis incident demonstrate attackers' evolving use of legitimate credentials rather than malware-based intrusions . The Scattered Spider group's suspected involvement in the Aflac breach highlights social engineering campaigns targeting customer support contractors and help desk personnel. These attacks bypass traditional security controls by exploiting the human element particularly in offshore operations and third-party support centers where security awareness may be inconsistent.

**3) Cross-Sector Impact:**

Financial services experienced cascading failures through fintech intermediaries. Healthcare saw convergence of ransomware, zero-day exploitation, and misconfiguration exposures. Education became the highest-attacked sector with over 4,300 weekly cyberattacks per institution . Retail giants in Asia demonstrated that

geographic location provides no immunity. This cross-sector impact reflects threat actors' business model evolution: rather than specializing by industry, they now exploit common technology platforms, third-party services, and human vulnerabilities that span all sectors.

**4) Underground Marketplace Activity:**

The Qilin ransomware gang claimed to have stolen 162,000 files totaling 176GB from Inotiv, including research data from the last decade. Multiple ransomware-as-a-service (RaaS) groups—including Akira, Medusa, LockBit, and RansomHub—disclosed December victims on dark web leak sites. This demonstrates the maturation of cybercrime into a commoditized service industry with established customer support, affiliate networks, and data marketplaces. Organizations face not just ransomware encryption but permanent data exposure and potential sale to competitors, nation-states, or secondary extortionists.

## Key Takeaways

- **Third-party risk is first-party risk**: Organizations must treat vendor security as extensions of their own infrastructure, with continuous monitoring, contractual breach notification requirements, and API security validation.
- **Detection gaps are exploitation windows**: At least 642 large healthcare data breaches occurred in 2025, with average reporting times of 4.8 months in education. Delayed detection directly correlates with breach severity and victim count.
- **Configuration is as critical as code**: Petco's misconfigured application settings and Blue Shield's Google Analytics exposure demonstrate that security misconfigurations rival zero-day exploits in frequency and impact
- **Ransomware has evolved beyond encryption**: Modern attacks prioritize data exfiltration over encryption, making backup strategies insufficient. Organizations need data loss prevention, network segmentation, and privileged access controls.

- **Compliance does not equal security:** Organizations with robust compliance programs (universities, hospitals, financial institutions) dominated breach disclosures, proving that checkbox security fails against determined adversaries.
- **The human element remains exploitable**: Social engineering targeting contractors, help desk personnel, and administrative staff bypasses billions in security technology investments. Security awareness must extend to the entire supply chain.
- **Disclosure delays compound damage**: Coupang's five-month detection gap led to 33 million exposed records and CEO resignation. Early detection and transparent disclosure limit legal, reputational, and financial consequences.
- **Geographic boundaries are irrelevant**: South Korea's massive breaches, UK manufacturing disruption, Canadian telecom compromises, and U.S. government intrusions prove that cyber threats respect no borders or time zones.

## Adversary Simulation Services from Saptang Labs

The threat landscape outlined in this report makes one reality clear: cyberattacks are no longer limited to opportunistic exploits or isolated incidents. From DDoS campaigns and ransomware operations to advanced espionage and supply-chain intrusions, adversaries are continuously evolving their tactics. Organizations and their vendors face the same exposure, as attackers increasingly exploit third-party connections to bypass strong defenses.

At Saptang Labs, we help enterprises build resilience through adversary simulation services. Our approach goes beyond traditional penetration testing to realistically replicate the tactics, techniques, and procedures (TTPs) of nation-state actors, ransomware gangs, and hacktivist groups. By doing so, we enable organizations to understand how real adversaries would attempt to compromise their infrastructure, data, and people.

### What We Deliver

- **Realistic Threat Testing** - Simulate live attack scenarios including DDoS floods, lateral movement, and exploitation of current CVEs
- **Supply-Chain Validation** - Test vendor ecosystems and third-party integrations before attackers exploit them
- **Maximum Kill Chain Coverage** - From reconnaissance to data exfiltration, identify critical gaps across your entire attack surface
- **Actionable Intelligence** - Prioritized remediation roadmaps mapped to MITRE ATT&CK and NIST frameworks
- **Executive Assurance** - Demonstrate measurable security readiness to leadership and stakeholders

### Ready to test your defence

Contact: sales@saptanglabs.com


SAPTANG
Proactive Threat Defence