SAPTANG™
Proactive Threat Defence

Monthly Threat Report November 2025

Contents

Executive Summary

November 2025 marked a **sharp escalation** in global cyber threat activity, driving the threat ecosystem to new operational peaks. The month was dominated by a **record surge in industrialized ransomware attacks** with an increase in disclosures-persistent exploitation of critical enterprise platforms, and a strategic pivot by adversaries toward **intellectual property and source code theft**.

Key Highlights

- **Ransomware Activity: 675 confirmed victim organizations** were publicly disclosed, with the **Qilin** and **Akira** groups driving most of the activity. This surge solidified the transition from simple file encryption to **pure data extortion**, heavily impacting the **Manufacturing, Healthcare, and Construction** sectors globally.
- **Vulnerability Exploitation:** Attackers focused intensely on high-privilege systems, weaponizing critical Deserialization RCE flaws in **Microsoft WSUS** and **Oracle E-Business Suite** within days of disclosure. The **SharePoint "ToolShell"** clusters also persisted as reliable, multi-stage intrusion frameworks.
- **Data Breaches & IP Theft:** Underground marketplaces saw a significant volume of new listings, including a massive **17 million record healthcare data dump (M-TIBA)**. Crucially, incidents at the **Lawrence Berkeley National Laboratory (LBNL)** and **RIPE NCC** confirmed a strategic shift toward targeting high-value **Source Code** and **proprietary tools** from national research and critical internet infrastructure.
- **Supply Chain & Enterprise Impact:** High-profile global incidents, including breaches at **Volkswagen Group France**, **Qantas**, and **Salesforce** (via vendors), underscored the systemic fragility of third-party ecosystems. In India, major exposures at **Dukaan** and other enterprises highlighted persistent risk from configuration weaknesses and targeted extortion.
- **Infrastructure Targeting:** Attacks on ports, logistics, and utilities continued, alongside politically motivated DDoS campaigns, reinforcing the need for defensive resilience across all critical services.

The November threat landscape revealed an increasingly efficient and specialized adversary ecosystem. Attackers favoured exploiting vulnerabilities in core IT systems (like patch management and ERP) to achieve rapid internal compromise, maximizing both financial return and strategic intelligence theft in a single campaign.

Ransomware Activity - November 2025

Overview

Ransomware continued to demonstrate persistent and elevated threat levels throughout 2025, with ransomware victim postings stabilizing at an average of 535 victims per month during Q3 2025, representing a 25% increase compared to the same period in 2024. The ransomware ecosystem witnessed record fragmentation, with the number of active extortion groups rising to 85 in Q3 2025, the highest number observed to date. Despite law enforcement disruptions of major operations including LockBit and RansomHub, the overall attack volume has not declined, instead maintaining historically high levels. Qilin emerged as the most active group, averaging 75 victims per month during Q3, followed by Akira, INC Ransom, and Play, demonstrating how quickly successor groups fill operational gaps left by disrupted organizations within the resilient Ransomware-as-a-Service economy.

Geographically, the United States remained the primary target, accounting for 54% of all ransomware incidents where victim countries could be identified during Q3 2025, followed by Canada, Germany, the United Kingdom, and France. Critical infrastructure sectors continued to bear the brunt of attacks, with nearly 50% of incidents striking manufacturing, healthcare, energy, transportation, and finance sectors, with manufacturing attacks surging 61% year-over-year. The top 10 ransomware groups accounted for only 56% of all published victims in Q3, down from 71% in Q1, reflecting increased fragmentation as affiliates migrate between operations and smaller groups emerging to exploit the decentralized threat landscape.

Despite elevated attack volumes, victim payment rates fell sharply to between 23-49% in 2025 compared to 56% in 2024, indicating improved organizational resilience and incident response capabilities. The median ransom payment decreased to $1,324,439 in 2025 from $2 million in 2024, representing a 50% decline, while 97% of organizations that had data encrypted were able to recover it through backups, decryption tools, or payments, with 53% recovering within one week. However, organizations remain vulnerable to evolving attack methodologies, with 32% of ransomware incidents in 2025 beginning with exploited vulnerabilities, making this the most common technical initial access vector, followed by compromised credentials at 23%, underscoring the persistent threat ransomware poses to organizations across all sectors and geographic regions.

Major Threat Actor Analysis

Qilin - Expansive Industrial and Healthcare Campaigns

The **Qilin** operation dominated the November threat landscape with an astonishing **178 recorded victims**, a massive surge in output that cemented its position as the single most prolific ransomware operator of the month. While the gang's activity was heavily concentrated in the United States, logging ninety-five cases, it also demonstrated significant and alarming reach across Europe and Asia, indicative of a sophisticated and highly industrialized affiliate network. Their targets included multiple major North American manufacturers, mid-sized construction firms across both the US and France, and sensitive healthcare providers in Canada and Spain. Qilin continues to employ aggressive **double-extortion** tactics with notable efficiency, leveraging the dual pressure of robust encryption-which prevents operational recovery-and debilitating data-leak threats-which inflict reputational damage-to maximize victim pressure. This pattern of relentlessly targeting operationally critical sectors like manufacturing and healthcare is a deliberate strategy designed to exploit **downtime sensitivity** and the high public accountability these sectors face, thereby forcing faster payment cycles and negotiations.

Akira - Sustained U.S. and Global Operations

Akira registered a substantial **fifty-five victims** in November, successfully maintaining the strong operational momentum observed in the prior month. The group's attacks were globally dispersed, spanning North America, Europe, and Asia, though they maintained a particularly strong presence in the United States, targeting a diverse mix of professional services and industrial firms. Specifically, notable victims included law and accounting firms in the U.S., manufacturing companies in Germany and Spain, and consultancies and IT service providers across Canada and India. Akira affiliates heavily favour intrusion through **misconfigured or weakly secured VPN and RDP endpoints**. This persistent reliance on exploiting perimeter exposure starkly highlights affiliates who are capitalizing on poor patching hygiene and a critical lack of Multi-Factor Authentication (MFA), allowing their opportunistic and unspecialized targeting models to result in frequent and widespread compromises.

Sinobi - Healthcare and Infrastructure Focus

Sinobi emerged as a key mid-tier actor in November, documenting **fifty-two victims**, many of which fell within the sensitive healthcare and critical services domains. The group executes a hybrid strategy, blending traditional file encryption campaigns with strategic, selective data exfiltration. Their focus is clearly on organizations where operational downtime directly affects service delivery and human safety. Noteworthy breaches included regional healthcare systems in the U.S. and Canada, as well as logistics providers and local utilities across Europe. Sinobi’s sustained pressure on healthcare entities points to the continued exploitation of inherently **under-resourced networks** and the weak segmentation often common in public-service infrastructure. This pattern suggests a deliberate willingness to pursue targets with high ethical and operational sensitivity for maximum leverage.

ShinyHunters - Data Exfiltration and Retail Exposure

ShinyHunters accounted for **forty-two victims** this month, steadfastly maintaining its specialization in data-theft-centric operations rather than relying purely on encryption. Its preferred targets included large retail chains, distribution companies, and e-commerce platforms-sectors all extremely sensitive to regulatory penalties and **customer-data exposure**. Specific breaches involved large North American retail franchise operators and European wholesale distributors. The group’s established focus on high-volume **data**

exfiltration and aggressive public leak-site pressure aligns precisely with its longstanding reputation for monetizing stolen databases and credentials on underground forums, positioning it more as a specialized data broker than a traditional encryption-focused RaaS.

Incransom - Persistent Targeting of SMBs and Nonprofits

With **twenty-nine recorded victims**, **Incransom** continued its steady and predictable presence in the lower-tier ransomware ecosystem. Most of its attacks consistently struck smaller, resource-limited entities, including schools, local healthcare providers, municipal services, and small-to-medium enterprises (SMBs). Incransom's persistence highlights the chronic exposure of community institutions and smaller businesses that frequently operate with minimal dedicated security staff, making them prime candidates for quick-turnaround, smaller ransom payments due to a critical lack of mature backup or segmentation strategies.

Play - Structured Global Activity

Play recorded **twenty-four confirmed attacks**, yet again demonstrating continued operational discipline and methodical global reach. The group's preferred victims included engineering, logistics, and IT service firms across the United States, Germany, and Brazil. Play is known for meticulous planning, consistently leveraging **credential abuse** and known vulnerabilities in remote access services. They often conduct extensive reconnaissance and establish significant dwell time before executing the final payload, suggesting a more process-driven and less opportunistic approach than groups like Akira.

Devman and Clop - Moderate but Strategic Activity

Devman, with **eighteen victims**, and **Clop**, with **sixteen victims**, sustained moderate but strategically selective campaigns throughout November. **Clop**, a group historically associated with zero-day exploitation of secure file transfer appliances and large-scale data leaks, showed a notable renewed interest in consulting and higher-education sectors, potentially signalling the testing or deployment of new initial access vectors.

Devman targeted a specific mix of technology and construction entities, often focusing on victims within Europe, suggesting specialized, targeted affiliate operations focused on exploiting vulnerabilities within those regional industrial supply chains.

Sectoral & Geographic Impact

Geographic Distribution

The **United States** remained, by a substantial margin, the primary target theatre, accounting for a stark **358 of the 675 global victims**-representing well over **53%** of all global incidents. This overwhelming concentration is directly driven by the country's immense density of high-value targets and the perceived willingness of U.S. organizations to pay ransoms quickly. Beyond the U.S., other significant concentrations of incidents were observed in Canada (38), France (33), Germany (17), and Australia (15). While the major groups, Qilin and Akira, were predominant across North America, smaller, focused groups such as Sinobi and ShinyHunters visibly expanded their operational footprint into European markets, which explicitly underlines the truly transnational reach of the RaaS ecosystem and the increasing diversification of their affiliate networks.

Sectoral Exposure

The analysis of targeting reveals a calculated, strategic focus on sectors with low tolerance for downtime.

- **Manufacturing and Industrial Supply Chains:** Manufacturing topped the victim count with **forty-six organizations** breached. The sector remains highly vulnerable due to its extensive use of **legacy systems, including Operational Technology (OT) and Industrial Control Systems (ICS)**, and the tangible, immediate monetary impact of operational downtime, which consistently pressures quick negotiation and payment.
- **Healthcare and Public Health:** Healthcare entities suffered **thirty-two confirmed breaches**. Attacks are often tragically successful due to fragmented networks and outdated infrastructure, frequently targeting patient-care networks and hospital

management systems, thereby magnifying both humanitarian and regulatory consequences for the victims.

- **Construction and Infrastructure:** With **32 victims**, construction firms and contractors emerged as a recurring and significant target set-due to their project-based, decentralized IT structures and heavy reliance on third-party vendors for critical systems management.
- **Technology and Retail Sectors:** Technology firms (**24 victims**) and retail/distribution companies (**20 victims**) endured sustained campaigns focused on data-exfiltration and double-extortion. These sectors are targeted specifically for their large customer databases, proprietary source code, and intellectual property, directly reflecting attackers' pursuit of data-rich environments for secondary monetization on underground markets.

Trends & Strategic Assessment

Escalating Victim Volume

November marked a substantial month-over-month rise in successful attacks, suggesting an aggressive and successful operational scaling among top RaaS groups-most notably evidenced by **Qilin's explosive growth**-and a corresponding growing number of active, successful affiliates. This alarming trend clearly signals that organizational defences are not improving quickly enough to match the sustained pace and sophistication of offensive tooling being deployed.

Dominance of High-Volume Actors

A clear pattern shows that a few top-tier RaaS groups now account for most observed global incidents. Their highly industrialized attack pipelines and centralized RaaS management infrastructure blur the critical distinctions between loose criminal syndicates and professionally managed service operations, allowing for greater attack consistency, operational efficiency, and overall effectiveness.

Persistent Targeting of Critical Services

Healthcare, manufacturing, and construction sectors remain under disproportionate and sustained pressure because of their inherent, low tolerance for operational downtime and the cascading safety and financial risks associated with disruption. This factor makes them extremely sensitive targets for aggressive **double-extortion** tactics.

Evolving Geopolitical Distribution

While the United States remains the primary financial battleground, the expanding campaigns into Europe and Asia indicate a noticeable **diversification of affiliate networks** and shifts in hosting and command-and-control infrastructure strategies designed to evade coordinated international disruption efforts by law enforcement agencies.

Fragmentation and Affiliate Overlap

The observed overlap of initial access tactics (such as RDP/VPN exploitation) among groups like Qilin, Akira, and Play strongly suggests potential **shared tooling** or active affiliate crossover between different RaaS platforms. This interchangeability of operators complicates accurate threat attribution and simultaneously enables rapid campaign rebranding when law enforcement pressure targets a specific operational entity.

Most Exploited Vulnerabilities – November 2025

Executive Summary

November 2025 exploitation activity was defined by high-impact, rapid weaponization of vulnerabilities in core enterprise and internet infrastructure. The month was dominated by critical remote code execution (RCE) and deserialization flaws in patch management (Microsoft WSUS), ERP systems (Oracle E-Business Suite), and enterprise collaboration platforms (Microsoft SharePoint).

The exploitation landscape highlights three dominant vectors:

1. **Enterprise Platform Exploitation (ToolShell & ERP):** The persistent SharePoint "ToolShell" cluster (CVE-2025-53770) continued to be a primary vector for ransomware. It was joined by newly weaponized, critical flaws in Oracle EBS (CVE-2025-61882) and Microsoft WSUS (CVE-2025-59287), giving attackers direct, privileged access to critical business systems.
2. **Infrastructure-Level Flaws (DNS & Endpoints):** A critical BIND 9 cache-poisoning flaw (CVE-2025-40778) moved from disclosure to public proof-of-concept, triggering widespread scanning and renewing the risk of large-scale DNS redirection. A zero-day in Motex Lanscope Endpoint Manager (CVE-2025-61932) also saw active in-the-wild use.
3. **Appliance & Open-Source Exploitation:** Externally facing appliances (FortiWeb, Cisco ISE) and popular open-source platforms (XWiki) remained prime targets for unauthenticated RCE and initial access.

The speed of weaponization for both enterprise and infrastructure flaws was a key feature of the month. Attackers demonstrated a clear focus on chaining vulnerabilities, such as pairing authentication bypasses with RCEs, to achieve full, unauthenticated compromise of high-value targets.

Key Highlights

- **WSUS Deserialization Flaw:** A critical deserialization flaw in Microsoft WSUS (CVE-2025-59287) was rapidly weaponized, allowing unauthenticated RCE and full server takeover. High-volume scanning was observed, with attackers using compromised WSUS servers to deploy infostealers.
- **Oracle E-Business Suite RCE:** A multi-stage, unauthenticated RCE in Oracle EBS (CVE-2025-61882) saw high-visibility exploitation, triggering emergency vendor advisories due to its critical impact on enterprise financial and processing components.
- **SharePoint "ToolShell" Persistence:** The ToolShell cluster of deserialization and auth-bypass flaws (CVE-2025-53770, -53771) continued to be a favoured tool for ransomware groups and targeted intrusion campaigns.

- **BIND 9 Cache-Poisoning PoC:** Public proof-of-concept code for a critical BIND 9 cache-poisoning vulnerability (CVE-2025-40778) was released, leading to immediate, large-scale scanning of exposed DNS resolvers.
- **Motex Lanscope Zero-Day:** A zero-day RCE in Motex Lanscope Endpoint Manager (CVE-2025-61932) was confirmed to be actively exploited in the wild, leading to its addition to curated exploit lists.

Top CVEs Actively Exploited

Enterprise Deserialization & Authentication Issues

- **CVE-2025-59287 (Microsoft WSUS Deserialization)** - CVSS 9.8 Unauthenticated deserialization of untrusted data allowing full RCE. Rapidly weaponized for infostealer and payload delivery.
- **CVE-2025-61882 (Oracle E-Business Suite RCE)** - CVSS 9.8 Unauthenticated, multi-stage flaw in BI Publisher. Chained to achieve RCE and takeover of critical EBS components.
- **CVE-2025-53770 (SharePoint ToolShell RCE)** - CVSS 9.8 Unsafe deserialization enabling unauthenticated RCE. Continued heavy use in ransomware and targeted intrusion campaigns.
- **CVE-2025-53771 (SharePoint ToolShell Patch-Bypass)** - Critical Authentication-spoofing variant used to bypass previous patches and enable RCE chains against on-prem servers.
- **CVE-2025-24893 (XWiki Platform Template Injection)** - CVSS 9.8 Unauthenticated server-side template injection in the SolrSearch macro. Actively exploited to deliver coinminers.
- **CVE-2025-41244 (VMware Aria / Tools LPE)** - CVSS ~7.8 Local privilege escalation from guest to host root. Added to KEV after confirmed in-the-wild use by sophisticated actors.
- **CVE-2025-5086 (Dassault DELMIA Apriso RCE)** - CVSS ~9.0 Unsafe deserialization in industrial/PLM software. Targeted exploitation observed against manufacturing environments for data theft.

- **CVE-2025-2746 / -2747 (Kentico Xperience Auth Bypass)** - CVSS 9.8 Authentication bypass in the Staging Sync Server. Exploited to gain administrative control over CMS content.
- **CVE-2025-49704 / -49706 (SharePoint Deserialization Chain)** - CVSS 6.3-8.8 Related deserialization and auth-spoofing flaws chained together to achieve code injection as part of ToolShell activity.

Network Appliances & Gateways

- **CVE-2025-61932 (Motex Lanscope RCE)** - CVSS ~9.3 Zero-day RCE in endpoint manager. Actively exploited in the wild for token misuse and follow-on compromise.
- **CVE-2025-40778 / -40780 (BIND 9 Cache-Poisoning)** - CVSS ~8.6 Resolver logic flaws allowing acceptance of unsolicited records, enabling remote DNS cache-poisoning. Public PoC led to mass scanning.
- **CVE-2025-20282 (Cisco ISE Unauth File-Upload → RCE)** - CVSS 9.8 Internal API allowed unauthenticated file upload and execution as system. Public PoCs and targeted exploitation observed.
- **CVE-2025-25257 (FortiWeb Fabric Connector SQLi → RCE)** - CVSS ~9.6 Pre-authentication SQL injection escalating to command execution. Used for initial access in opportunistic scanning campaigns.
- **CVE-2025-54309 (CrushFTP Admin Access)** - CVSS ~9.0 AS2 validation bypass allowing unauthenticated elevation to administrative functions. Exploited for full server takeover.

Browser & Runtime Exploits

CVE-2025-6558 (Chromium ANGLE / GPU Sandbox Escape) - CVSS ~8.8 Input-validation weakness in the GPU path allowing browser sandbox escape. Continued in-the-wild exploitation reports.

Consumer IoT & Legacy Devices

- **CVE-2025-9377 (TP-Link Router RCE)** - High/Critical Authenticated RCE in Parental Control module of EOL firmware. Ongoing exploitation for botnet recruitment.

Observations & Trends

- **Dominance of Patch-Management/ERP Vectors:** Attackers heavily focused on platforms like WSUS and Oracle EBS. Compromising these systems provides a high payoff, enabling widespread internal payload distribution and access to critical business data.
- **Persistence of "Exploitation Families":** The SharePoint "ToolShell" cluster remains a reliable and persistent framework for attackers, demonstrating that complex, multi-stage exploits are maintained and reused long-term.
- **PoC-Driven Exploitation Spikes:** The BIND 9 vulnerability highlighted the speed of weaponization. Public PoC disclosure led to immediate, observable, large-scale scanning as attackers raced to find unpatched resolvers.
- **Chaining as Standard Practice:** Attackers are rarely relying on a single flaw. The most effective campaigns (e.g., SharePoint, FortiWeb) chained authentication, spoofing, or injection flaws with RCEs to achieve unauthenticated compromise.
- **Supply-Chain Cascade Effects:** Several incidents involved compromised credentials or maintenance tools being used to propagate malicious artifacts, highlighting a trend of attackers targeting CI/CD pipelines and package ecosystems to amplify their reach.

Impact Profile

- **Severity:** Most high-priority items carried Critical (9.0-9.8) or High (7.8-8.8) severity ratings, associated with RCE, privilege escalation, or infrastructure manipulation.
- **Exploitation Outcomes Observed:**
  - Initial access and administrative takeover (WSUS, EBS, Cisco ISE)
  - Ransomware deployment (SharePoint, FortiWeb)
  - Credential and token harvesting
  - DNS manipulation and traffic interception (BIND 9)

  - Deployment of infostealers and coinminers (WSUS, XWiki)
  - Botnet recruitment (TP-Link)
- **Threat Type Balance:** Activity showed a mix of highly targeted intrusions (DELMIA Apriso, Oracle EBS) and widespread, opportunistic scanning (BIND 9, WSUS, XWiki).

Cyber Incidents - November 2025

Executive summary

November 2025 was defined by a massive and coordinated surge in high-impact ransomware campaigns, significant data leaks from major global consumer brands, and persistent supply-chain extortion. The month's activity, particularly the explosive spikes in ransomware victims attributed to groups like Qilin (with 178 victims) and Akira (55 victims), signals a new peak in industrialized cybercrime. These groups demonstrated a clear capability to successfully breach major industrial, automotive, and healthcare chains at scale.

In India, the threat landscape's most significant events shifted from last month's focus on fraud-and-arrest operations to the consequences of large-scale data exposures. The discovery of a major data leak at the e-commerce platform **Dukaan**, coupled with numerous Indian enterprises (such as **Future Generali** and **Rasi Laboratories**) appearing on public ransomware leak sites, indicates a growing and dual-pronged risk from both critical data misconfigurations and targeted, successful extortion campaigns.

Globally, high-profile incidents at **Volkswagen**, **Qantas**, and **Salesforce** highlighted the severe and lasting reputational and financial damage stemming from data theft. These events underscore a critical vulnerability: attackers are increasingly gaining initial access not by direct assault, but through the softer target of third-party vendors and supply-chain partners.

India incidents (November 2025)

- **Dukaan e-commerce platform data exposure** A significant and highly concerning data exposure was discovered at the Indian e-commerce platform Dukaan. Reports in November confirmed that the incident involved a large, unsecured dataset of merchant and customer records. Most alarmingly, this included sensitive payment gateway tokens. The discovery of this exposed data highlighted significant and immediate privacy and financial risks, potentially enabling attackers to impersonate merchants or customers, siphon funds, and severely undermine trust in the platform.
- **Ransomware extortion incidents (Future Generali, Rasi Labs)** Multiple Indian corporations were publicly named and shamed on ransomware leak sites in November, indicating successful, unmitigated breaches. Notable victims included **Future Generali (India)**, a major insurance provider, which appeared on extortion trackers early in the month. This was followed by **Rasi Laboratories**, which was publicly listed as a victim of the prolific Qilin ransomware group in mid-November, confirming that top-tier global threat actors are actively and successfully targeting Indian industry.
- **Hospitality sector breaches (Laxmi Niwas Palace, Indian Spring)** The hospitality sector saw several confirmed compromises, a popular target due to its high volume of transient customer PII and often-fragmented IT systems. **The Laxmi Niwas Palace** in Bikaner was listed on a leak tracker with a November discovery date, indicating a data breach. Similarly, the **Indian Spring Country Club** was publicly named as a Qilin victim, reflecting a broader trend of ransomware groups targeting hospitality providers for their valuable customer data and operational reliance on IT systems.
- **Regional business and real estate attack** the impact of cybercrime was also felt at a regional level. A Kolkata-based real-estate firm reported a targeted cyberattack and ransomware incident in November, escalating the matter by filing a formal complaint with local police. Concurrently, international ransomware trackers showed numerous other small hospitality firms and businesses, such as **BRDSoft (India)**, being posted on leak sites. This demonstrates a high-volume, opportunistic campaign against small-to-medium enterprises, which are often less resilient to such attacks.

- **Gujarat hospital CCTV privacy breach** A major privacy scandal emerged in Gujarat in late November involving a large-scale breach of hospital CCTV feeds. Reports indicated that the breach was not a sophisticated hack but stemmed from a basic security failure: the use of default or weak credentials on the camera systems. This allowed attackers to access highly sensitive live feeds, leading to widespread public and media reporting on the critical failure to protect patient privacy, and opening the door for potential blackmail.
- **Ayushman Bharat (NHA) data tampering investigation** Investigations were reported in November after suspicious data tampering was detected within the Ayushman Bharat (National Health Authority) systems. This incident was treated as a significant breach of public health data integrity, as unauthorized modification of health records could lead to fraudulent claims, denial of service for legitimate beneficiaries, or disruption of the national health scheme. FIRs were filed, and investigations were launched.
- **Aadhaar PII data leak investigation** November saw widespread and alarming reporting of an alleged, massive data leak involving the Personally Identifiable Information (PII) of hundreds of millions of Indian citizens, purportedly from the Aadhaar system. The claims, while actively and publicly disputed by authorities, are being investigated as a high-priority, national-scale data security event due to the sheer potential impact on citizen privacy and national security.
- **Increased targeting of financial sector (NSE)** The National Stock Exchange (NSE) issued public statements in November noting an "extremely high volume" of probing and cyberattacks targeting India's financial sector. This official advisory confirmed that financial institutions are on high alert due to a measurable and sustained increase in threat activity, indicating a concerted effort by attackers to find weaknesses in critical economic infrastructure.
- **Law enforcement actions and fraud-related arrests** in response to the growing threat, police in various regions reported actions related to ongoing cybercrime. This included arrests in Coimbatore for a specific security breach and proactive actions in Varanasi related to number-blocking and the takedown of fraud rings. These actions,

all stemming from November investigations, highlight the reactive law enforcement pressure being applied to combat these criminal enterprises.

Global incidents (November 2025)

- **Volkswagen Group France - Qilin ransomware claim,** The Qilin ransomware group, in line with its documented focus on the manufacturing sector, claimed responsibility for a significant intrusion against **Volkswagen Group France** in mid-November. The group backed up its claims by posting exfiltrated data to its dark-web leak site. This public leak indicated a successful breach and data theft operation, targeting a high-value industrial corporation as part of Qilin's massive surge in activity.
- **Qantas customer data leak,** The Australian airline Qantas faced a major customer impact and reputational crisis in November as attackers released a trove of customer data. This data was acquired during an earlier, previously undisclosed breach. The incident resurfaced, causing significant damage as customers learned of the breach from threat actors, prompting renewed regulatory and public scrutiny of the airline's data protection and transparency practices.
- **Salesforce supply-chain extortion attempt,** A major supply-chain extortion event involving Salesforce and its vendors (like Drift and Salesloft) came to light in November. Attackers, reportedly linked to the ShinyHunters extortion group, leveraged exposed authentication tokens from third-party vendors to access data. The incident highlighted the systemic risk of interconnected SaaS platforms. In a significant move, Salesforce confirmed it had been targeted but had **refused the ransom demand**, a stance that is critical but not universal.
- **Multiple U.S. municipalities hit by outages,** Several U.S. municipal and county governments reported crippling IT outages and system disruptions during November, grinding public services to a halt. Confirmed incidents in **Kaufman County, TX**, **La Vergne, TN**, and **DeKalb County, IN**, pointed to a widespread, opportunistic campaign of ransomware or other cyber incidents targeting local government services, which often lack the security budgets of federal or private-sector entities.
- **SimonMed Imaging - Medusa ransomware attack,** The Medusa ransomware group claimed a major healthcare breach against **SimonMed Imaging**, one of the largest

outpatient imaging providers in the U.S. The full impact of the attack, which involved the theft of a large volume of sensitive patient data (Protected Health Information or PHI), was fully surfaced in mid-November, highlighting the continued and relentless threat of ransomware to the healthcare sector.

- **Askul (Japan) retail and logistics disruption,** The Japanese retail and logistics firm Askul reported a significant ransomware event in late November. The attack caused widespread outages and system paralysis, disrupting operations for several major Japanese retailers that depend on Askul's services. This incident served as a powerful reminder of the cascading, real-world impact of supply-chain attacks, where a single breach can halt operations for numerous dependent businesses.
- **Nintendo - Alleged intrusion and data leak,** the "Crimson Collective" threat group claimed an intrusion against gaming giant Nintendo. To prove their access, screenshots and files of alleged internal asset data were leaked in November. This prompted urgent investigations by the company into the extent of the breach, a critical event given the high value of its intellectual property, trade secrets, and unreleased game content.
- **WestJet and travel sector data leaks** The Canadian airline WestJet was among several travel industry companies that appeared in data leak postings and security trackers during November. These incidents were not isolated; they pointed to a correlated, sector-wide targeting of airline and hospitality data, which is highly valuable to threat actors for fraud and resale.
- **Massive surge in ransomware activity (Qilin, Akira)** Underpinning many of these specific incidents, security trackers and threat intelligence firms (e.g., ransomware.live, LevelBlue) confirmed a major, 56% month-over-month surge in ransomware activity, with **675** new victims posted. Groups like **Qilin** and **Akira** dominated the disclosures, being responsible for hundreds of these victims and demonstrating a focus on industrial, utility, and manufacturing targets.
- **Scattered and ShinyHunters extortion campaigns** Affiliates and variants of the **ShinyHunters** and **Scattered** groups remained highly active. These groups, which often focus on data theft for extortion rather than encryption, were linked to several large corporate data leaks and extortion postings on their dedicated leak sites

throughout November. Their activity focused on high-profile enterprise targets and, crucially, their supply-chain partners.

Global Data Breach Intelligence Summary - November 2025

Overview

Major Data Breaches: November 2025

November 2025 witnessed a series of significant data breach disclosures spanning technology, financial services, healthcare, education, and food delivery sectors. The month was dominated by the Cl0p ransomware group's exploitation of Oracle E-Business Suite zero-day vulnerabilities, with over 100 organizations reportedly compromised, alongside major supply chain attacks targeting Salesforce customers through third-party integrations.

The following intelligence summary highlights the most significant verified breach incidents from November 2025, reflecting a continued trend toward supply chain compromises, zero-day exploitation, and social engineering attacks that demonstrate the evolving sophistication of threat actor operations.

1. Oracle E-Business Suite Mass Exploitation Campaign (Cl0p)

Threat Actor: Cl0p Ransomware Group
Vulnerability: CVE-2025-61882, CVE-2025-61884
Estimated Victims: 100+ organizations globally
Timeline: August-November 2025

- In a 24-hour period between November 20 and November 21, the Cl0p group reportedly exploited breaches and exfiltrated data from 29 additional companies, marking one of the most aggressive phases of this campaign. The cybercriminal organization exploited a zero-day vulnerability in Oracle's E-Business Suite, leading to critical data breaches for dozens of large corporations including allegedly Broadcom, Estée Lauder, Mazda, and Canon

Confirmed Major Victims:

- **Cox Enterprises:** 9,479 individuals notified, with data exfiltration occurring between August 9-14, 2025
- **The Washington Post:** Nearly 10,000 employees and contractors affected, with exposed data including names, bank account numbers, Social Security numbers, and tax ID numbers
- **Dartmouth College:** Over 32,500 individuals affected (1,500 in Maine, 31,000+ in New Hampshire), with 226 GB of data leaked including Social Security numbers and bank account details
- **Harvard University:** Confirmed as victim with undisclosed impact
- **Logitech:** Confirmed data breach linked to Oracle campaign
- **Potential Impact:** CVE-2025-61882 is easily exploitable by unauthenticated attackers with network access via HTTP, and may lead to remote code execution, affecting Oracle E-Business Suite versions 12.2.3 through 12.2.14. The campaign demonstrates how zero-day vulnerabilities in widely used enterprise software can enable mass data theft operations affecting critical financial and personal information across multiple industries.

2. Salesforce/Gainsight Supply Chain Attack (ShinyHunters)

Threat Actor: ShinyHunters (UNC6240) / Scattered Lapsus$ Hunters
Attack Vector: Compromised OAuth tokens
Estimated Victims: 200+ Salesforce instances
Discovery Date: November 19-20, 2025

- Google confirmed that hackers have stolen the Salesforce-stored data of more than 200 companies in a large-scale supply chain hack following a breach of Gainsight-published apps. ShinyHunters claimed they used credentials stolen from an earlier attack on Salesloft (where Gainsight was also a victim) to compromise Gainsight, affecting almost 1,000 organizations.

- **Attack Methodology:** The problem lies with the access tokens used by Gainsight's connected applications, which are basically special digital keys allowing the apps to link to Salesforce systems. ShinyHunters claimed they gained access to another 285 Salesforce instances after breaching Gainsight via secrets stolen in the Salesloft Drift breach.
- **Claimed Victims Include:** Atlassian, CrowdStrike, DocuSign, F5, GitLab, LinkedIn, Malwarebytes, SonicWall, Thomson Reuters, and Verizon
- **Response Measures:** Salesforce revoked all active access and refresh tokens associated with Gainsight-published applications and temporarily removed those applications from the AppExchange. Zendesk also revoked its connector access to Gainsight "as a precaution," and the Gainsight app was "temporarily pulled from the HubSpot Marketplace".
- **Potential Impact:** The breach exposes the cascading risks of supply chain attacks where compromising a single third-party integration provider can grant access to hundreds of downstream customer environments, demonstrating the critical importance of OAuth token security and third-party application vetting.

3. DoorDash Social Engineering Breach

Attack Vector: Social Engineering / Employee Compromise
Affected Regions: United States, Canada, Australia, New Zealand
Victims: Undisclosed number (potentially millions)
Disclosure Date: November 13, 2025

- DoorDash disclosed a data breach that exposed the personal information of an unspecified number of users, which included names, email addresses, phone numbers, and physical addresses, after an employee fell for a social engineering attack. The company notified customers that personal information had been compromised after a DoorDash employee fell victim to a social engineering scam, giving an outside actor access to internal systems.

- **Exposed Data:**
  - First and last names
  - Phone numbers
  - Email addresses
  - Physical/delivery addresses
  - Basic order information (for subset of users)
- **Data NOT Compromised:** DoorDash claimed that no sensitive information including passwords, full payment card numbers, bank account numbers, or Social Security numbers was accessed.
- **Context:** According to Palo Alto Networks, social engineering has rapidly become the top cybersecurity threat for companies, accounting for 36 percent of all intrusions from May 2024 to May 2025. This represents DoorDash's third major data breach since 2019.
- **Potential Impact:** While financial data was not compromised, the exposed contact information creates risks for targeted phishing campaigns, address-based harassment, and social engineering attacks. The breach demonstrates how human factors remain the weakest link in cybersecurity defenses despite technological safeguards.

4. Additional November 2025 Breach Disclosures

- Based on official breach notification records, the following organizations disclosed data breaches in November 2025:
- **Healthcare Sector:**
  - Beverly Hills Oncology Medical Group
  - Vibra Hospital of Southeastern Massachusetts
  - St. Anthony Hospital (6,600+ patients and staff potentially exposed)
  - David A. Nover M.D., P.C.

- **Financial Services:**
  - Wells Fargo Bank, N.A.
  - Raymond James Financial
  - The Village Bank
  - SitusAMC (affecting JPMorgan, Citi, Morgan Stanley clients)
- **Education:**
  - President and Fellows of Harvard College (Oracle campaign)
  - Southern Illinois University
  - Tulane University
  - Princeton University
- **Other Sectors:**
  - Logitech (Oracle campaign - reported to SEC)
  - Canon and Mazda (Oracle campaign victims)
  - WEL Companies (logistics)
  - Almaviva hack affecting Italian railway operator Ferrovie dello Stato

Strategic Assessment

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

1. Supply Chain as Primary Attack Vector: The Salesforce/Gainsight and Oracle campaigns demonstrate how compromising widely used enterprise platforms or their integrations can provide access to hundreds of downstream victims simultaneously, creating massive cascading impact.

2. Zero-Day Exploitation at Scale: The Cl0p gang's exploitation of Oracle E-Business Suite zero-day vulnerabilities represents a strategic shift toward targeting enterprise resource planning (ERP) systems that contain comprehensive organizational data

3. Social Engineering Sophistication: Social engineering has rapidly become the top cybersecurity threat, accounting for 36 percent of all intrusions, surpassing both malware incidents and software vulnerability exploits

4. Cross-Sector Impact: From healthcare to financial services, education to logistics, November breaches affected every major industry vertically, with particular emphasis on organizations managing sensitive financial and personal health information.

5. Underground Marketplace Activity: Nearly all major incidents were publicized on cybercrime forums or leak sites, reaffirming the central role of underground marketplaces in monetizing stolen data through extortion and data brokerage models.

Key Takeaways

- **Oracle campaign:** Over 100 organizations compromised through zero-day exploitation, affecting critical ERP systems containing comprehensive organizational and financial data
- **Salesforce supply chain:** 200+ customer instances potentially compromised through third-party OAuth token theft, demonstrating cascading supply chain risks
- **Social engineering dominance:** Multiple major breaches including DoorDash originated from employee manipulation rather than technical vulnerabilities
- **Geographic reach:** Breaches affected organizations across North America, Europe, and Asia-Pacific, underscoring the global nature of cybercrime operations
- **Delayed detection:** Many breaches occurred months before discovery (Oracle campaign began in August, disclosed in October-November), highlighting detection gaps

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