SAPTANG™
Proactive Threat Defence

Monthly Threat Report
January 2026

CONTENTS

Executive Summary

January 2026 demonstrated **escalating sophistication and impact** across all cyber threat domains, with notable shifts toward intellectual property theft, state-sponsored zero-day exploitation, and industrialized fraud operations. January 2026 represents a maturation of attacker tactics - state actors exploiting zero-days pre-patch, ransomware affiliates optimizing for downtime-sensitive targets, fraud syndicates industrializing social engineering at scale, and threat actors systematically targeting proprietary IP over consumer databases. The ecosystem's fragmentation, combined with sophisticated supply chain exploitation and perimeter compromise patterns, signals sustained high-threat conditions requiring multilayered defensive strategies.

Key Highlights

- **Ransomware Activity:**
  - **Fragmented ecosystem** with dozens of parallel operations creating persistent elevated threat levels
  - **Top threat actors by victim count**: 0APT (30 victims), Qilin (25), Akira (15), Everest (12), and INC Ransom (10)
  - **Geographic concentration**: North America and United States absorbing largest victim share, followed by Canada and Western Europe; Asia emerged as secondary theatre with supply-chain targeting
  - **Sector targeting**: Manufacturing/industrial supply chains, education/public sector, healthcare, and professional services attackers optimizing for operational paralysis and reputational leverage
  - **Attack pattern**: Perimeter-driven compromise via remote access pathways enabling rapid lateral movement, staged exfiltration, and resilient campaigns through affiliate mobility.

- **Vulnerability Exploitation:** Unprecedented zero-day campaigns targeting enterprise authentication infrastructure
  - Critical flaws exploited:
    - ❖ Maximum CVSS 10.0 vulnerabilities in workflow automation platforms (n8n)
    - ❖ Unauthenticated remote code execution in enterprise systems
    - ❖ Critical SQL injection in SAP S/4HANA ERP systems

        - ❖ State-sponsored zero-day exploitation of Microsoft Office and Windows Desktop Window Manager before patches available
    - DDoS campaigns: Hacktivist operations by pro-Russian NoName057(16) and DDoSia ecosystem targeting UK infrastructure (coordinated 7-day campaign January 5-11).

- **Data Breaches & IP Theft:**
    - **Strategic pivot to intellectual property**: Month dominated by source code and proprietary data theft rather than traditional customer data
    - Major incidents:
        - ❖ Nike: 1.4TB data exfiltration by WorldLeaks ransomware group
        - ❖ Target: 860GB source code exposure via misconfigured public Git server
        - ❖ New Zealand's Manage My Health: 428,337 medical documents compromised (120,000+ patients)
        - ❖ Monroe University: 320,973 individuals affected by year-old breach with comprehensive identity data exposure
    - Delayed disclosures: Multi-month gaps between breach discovery and notification prolonging victim exposure to identity theft risks

- **Supply Chain & Enterprise Impact:**
    - **Third-party compromise as force multiplier**: Attackers leveraging ecosystem vulnerabilities for cascading impact
    - **Trust Wallet incident**: ~$8.5 million theft from 2,500+ wallets linked to "Shai Hulud" npm supply chain campaign demonstrating developer toolchain intrusions converting to direct end-user financial loss
    - **Ledger breach**: Compromise through payment processor Global-e highlighting third-party vendor risks
    - **Cross-sector targeting**: Systematic attacks across retail, technology, healthcare, education, and financial sectors

- **Infrastructure Targeting:**
  - India-specific threats: Industrialized cyber-enabled fraud featuring "digital arrest" authority impersonation scams
    - ❖ Telangana Cyber Security Bureau arrests linked to interstate syndicate with ₹16 crore+ losses
    - ❖ Sophisticated operations combining psychological coercion ("virtual custody" via continuous video calls), forged legal narratives, and rapid multi-state mule account laundering
  - DDoS as geopolitical tool: Low-cost, high-visibility disruption tactics by hacktivist groups targeting national-scale public infrastructure
  - Perimeter vulnerabilities: Ongoing exploitation of remote access pathways, security appliances, and authentication infrastructure enabling repeatable, resilient ransomware campaigns

Ransomware Activity – January 2026

Overview

Ransomware continued to maintain elevated and persistent threat levels across the reporting window, with victim postings concentrated among a crowded ecosystem of active extortion operations and sustained competition between established leaders and emerging brands. The ecosystem remained strongly fragmented, with dozens of groups operating in parallel, while a small set of high-tempo actors produced a disproportionate share of disclosures most **notably 0APT (30 recorded victims) and Qilin (25), followed by Akira (15), Everest (12), and INC Ransom (10**).

Geographically, disclosures remained heavily concentrated in **North America and Western Europe, with the United States continuing to absorb the largest share of identifiable victims** due to its density of high-value enterprises and the high operational cost of downtime, while Canada and parts of Europe saw recurring healthcare, industrial, and construction-related exposure. **Asia remained a consistent secondary theatre through fragmented but repeated supply-chain and industrial victimization**, indicating that affiliate networks continue to operate transnationally rather than remaining region-bound. Critical services and downtime-sensitive sectors bore the heaviest burden, with manufacturing and industrial supply chains, education/public sector entities, healthcare providers, and professional services repeatedly appearing among victim sets reinforcing that attackers are optimizing for operational paralysis plus reputational leverage rather than narrow sector specialization.

The overall pattern continued to point to perimeter-driven compromise at scale particularly exposure and weakness in remote access pathways enabling rapid lateral movement, staged exfiltration, and repeatable campaigns that are resilient to disruption and capable of rapid rebranding through affiliate mobility.

Major Threat Actor Analysis

Qilin – Expansive Industrial and Public-Sector Pressure

The Qilin operation led activity with **25 recorded victims**, sustaining a high-tempo campaign that reinforced its position as a dominant operator. The targeting pattern emphasized

manufacturing, local government, and education, with notable victims including **Muebles Dico**, **Medinah School District 11**, **Workers Health & Safety Centre**, and **SoCal ROC**, indicating a deliberate preference for downtime-sensitive environments where disruption quickly translates into payment pressure. Qilin's playbook remained consistent: rapid compromise of exposed perimeter services, broad lateral movement, and double extortion combining encryption with credible data-leak threats to maximize leverage

Akira – Steady Volume Across Industrial and Services

Akira registered **15 recorded victims**, maintaining steady operational output and a clear focus on industrial supply chains and mid-market services. Targets included **JST Power Equipment**, **Zurflüh-Feller**, **Ferretti Construction**, and **Kilograph**, reflecting a pattern of pursuing organizations where production continuity and contractual delivery obligations amplify ransom urgency. Intrusions frequently align with perimeter access weaknesses (VPN/RDP exposure and credential abuse), followed by staged exfiltration and encryption to enforce double-extortion outcomes.

Everest – Data-Heavy Extortion Against Recognizable Brands

Everest claimed **12 recorded victims**, concentrating on high-value organizations where reputational damage and sensitive datasets increase coercive power. Notable victims included **Iron Mountain, Polycom, Shinwa Co Ltd**, and **Acu Trans Solutions LLC**, illustrating a consistent preference for data-rich enterprises and service providers. The operating pattern emphasizes large-scale data theft, detailed leak-site proofing, and pressure-driven timelines that force victims into accelerated negotiation cycles

INC Ransom – Broad Targeting with Emphasis on Services and SMBs

INC Ransom posted **10 recorded victims**, reflecting persistent mid-tier volume with a strong tilt toward professional services and operationally constrained organizations. Victims included **ChokChey Finance, www.pucobre.cl , Best Attorneys, Foamtec International,** and **Hawk Law Group**, signaling a pattern of targeting entities where legal exposure, customer data, and operational disruption combine into high leverage. The group's campaigns commonly reflect double-extortion pressure, with exfiltration and publication threats used to overcome organizations that can technically restore systems but cannot tolerate data exposure.

DragonForce – Professional Services and Retail Pressure Campaigns

DragonForce recorded **around 8 victims**, frequently selecting targets where public pressure, client trust, and reputational damage can be weaponized effectively. Notable

victims included **Erickson Thorpe & Swainston**, **T & M Electric LLC**, and **Mullinax Ford**, reflecting a pattern of pursuing professional services and consumer-facing businesses. The group's approach blends classic extortion mechanics with high-visibility leak threats, often prioritizing perceived negotiation leverage over pure victim volume.

0APT – Mass-Posting, High-Visibility Multi-National Targeting

0APT exhibited **30 recorded victims**, standing out for unusually high-volume postings and repeated selection of globally recognizable enterprises. Notable victims included **Thermo Fisher Scientific, GlaxoSmithKline, Tetra Pak International,** and **Mayo Clinic**, reflecting a pattern that emphasizes maximum visibility and downstream fear effects across sectors. The operational style suggests a "headline-driven" extortion model where reputation impact and perceived scale are used as primary pressure multipliers.

Play – Opportunistic Mid-Market Disruption

Play disclosed **6 recorded victims**, maintaining a consistent but lower-volume cadence centered on disruption-driven extortion. Notable victims included **Deatak** and **Bar S Services**, reflecting the group's continued tendency to pursue mid-market organizations where business interruption can rapidly force payment discussions. Campaign patterns remain aligned with opportunistic access and double-extortion leverage, with encryption used to create immediate operational paralysis

The Gentlemen – Industrial and Hygiene/Consumer Goods Targeting

The Gentlemen logged **5 recorded victims**, concentrating on mid-sized manufacturers and consumer-linked businesses that are sensitive to downtime and supply disruptions. Notable victims included **Handsome Manufacturing** and **Nobel Hygiene Pvt**, showing a pattern of targeting production-oriented environments where delayed fulfilment and reputational harm create fast-moving negotiations. The group's activity aligns with straightforward double-extortion operations designed for repeatable execution across similar-sized targets.

Interlock – Education and Community-Oriented Organizations

Interlock recorded **4 victims**, with activity that favoured community-facing entities where service disruption and local reputational impact intensify pressure. A notable victim included **Odyssey Academy**, consistent with a pattern of targeting organizations that often lack robust security staffing and incident-response depth. The operating approach appears geared toward fast coercion steal, threaten, and disrupt rather than prolonged stealth.

Linkc – Smaller-Scale Targeting of Specialized Technology Firms

Linkc recorded **around 3 victims**, focusing on niche technology and industrial-adjacent targets. Notable victims included **Sajet Products (Senior Aerospace)** and **StrongLink**, indicating a pattern of selecting specialized organizations where sensitive operational or customer data can provide disproportionate extortion leverage. The activity suggests a lower-volume model optimized for targeted pressure rather than broad spraying across sectors.

Sectoral & Geographic Impact

Geographic Distribution

Targeting remained heavily concentrated in North America and Western Europe, with the United States continuing to absorb the largest share of victim disclosures due to its density of high-value enterprises and the high operational cost of downtime. This concentration is reflected in repeated hits against U.S.-based manufacturing, professional services, and public-facing organizations such as **Medinah School District 11, SoCal ROC,** and **Mullinax Ford**. Canada also remained a frequent theatre for healthcare exposure, consistent with continued targeting of medical providers and imaging services in prior periods, while Europe saw sustained activity against industrial and construction organizations such as Zurflüh-Feller and other mid-sized manufacturers. Asia showed continued but more fragmented exposure, largely tied to supply-chain and industrial targets, indicating that affiliate networks are maintaining multi-region reach rather than operating purely domestically.

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:** Industrial firms stayed a top target set, reflecting attackers' preference for environments where production downtime produces immediate economic loss and contractual penalties; examples include **JST Power Equipment**, **Zurflüh-Feller**, and **Muebles Dico.**

- **Healthcare and Public Health:** Healthcare exposure persisted due to the sensitivity of patient data and regulatory pressure, with attackers using reputational damage and privacy impact as coercive multipliers; examples include **Mayo Clinic** and other medical providers listed among high-visibility victims.

- **Professional Services (Financial/Legal/Advisory):** Law and advisory firms remained attractive due to client PII, case files, and financial documents that can trigger secondary impacts beyond IT recovery; examples include Best Attorneys and Hawk Law Group.

- **Public Sector and Education**: Schools, training institutes, and public-facing community entities continued to face repeated targeting due to limited cyber resources and high sensitivity to service disruption; examples **include Medinah School District 11, SoCal ROC, and Odyssey Academy**.

- **Retail and Automotive/Franchise Businesses**: Consumer-facing organizations were targeted for brand leverage and customer data exposure, with examples such as Mullinax Ford indicating continued interest in reputation-driven extortion.

Trends & Strategic Assessment

- **Escalating Victim Volume**: The prior period marked a sustained high posting tempo, and the current window continued to show broad multi-group activity rather than a meaningful slowdown, indicating that ecosystem capacity remains high and resilient to disruption.

- **Dominance of High-Volume Actors**: A small set of actors continued to account for a disproportionate share of disclosures, with high-output groups repeatedly surfacing across industrial, public-sector, and services victims consistent with industrialized affiliate pipelines and repeatable intrusion playbooks.

- **Persistent Targeting of Critical Services**: Education, construction/field services, and industrial supply chains remained under sustained pressure because downtime directly halts revenue or essential delivery, while healthcare and professional services were repeatedly leveraged for the regulatory and reputational impact of sensitive-data exposure.

- **Evolving Geopolitical Distribution**: While the U.S. remained the financial center of gravity, recurring victims in Western Europe and Asia indicate diversification of target geographies, suggesting affiliates are expanding into additional jurisdictions to broaden opportunity and reduce dependency on a single market.

Most Exploited Vulnerabilities – January 2026

Overview

January 2026 exploitation activity was defined by unprecedented zero-day campaigns targeting enterprise authentication infrastructure, maximum CVSS 10.0 workflow automation vulnerabilities, and state-sponsored exploitation of Microsoft Office and Windows kernel components before patches became available. The month was dominated by unauthenticated remote code execution flaws in enterprise workflow platforms (n8n automation), critical SQL injection in ERP systems (SAP S/4HANA), and zero-day exploitation of Microsoft Office and Windows Desktop Window Manager by state-aligned threat actors.

The exploitation landscape highlights three dominant vectors:

1. **Enterprise Workflow & ERP Platform Exploitation:** The n8n workflow automation platform emerged as the month's most critical target, with dual CVSS 10.0 vulnerabilities enabling unauthenticated administrative access and arbitrary command execution affecting over 103,000 exposed instances globally. This was joined by newly weaponized SAP S/4HANA SQL injection enabling full database compromise, and Microsoft SharePoint SQL injection/RCE vulnerabilities continuing enterprise targeting patterns. Attackers demonstrated systematic focus on business-critical automation and ERP infrastructure where single vulnerabilities provide cascading access to interconnected enterprise systems managing financial, supply chain, and operational data.

2. **Zero-Day Office & Windows Kernel Exploitation:** State-sponsored threat actors executed coordinated zero-day campaigns against Microsoft Office OLE protection bypass and Windows Desktop Window Manager information disclosure before patches became available. The Office vulnerability was weaponized within 72 hours of emergency patch release through phishing campaigns delivering backdoors via RTF files, while the Desktop Window Manager flaw enabled ASLR bypass commonly chained with privilege escalation exploits. Both vulnerabilities were added to CISA KEV catalog on disclosure day, reflecting immediate exploitation timelines that eliminate traditional patch deployment windows.

3. **Network Appliance & Server Infrastructure Targeting:** Fortinet FortiOS SSO zero-day exploitation, Palo Alto GlobalProtect denial-of-service with public proof-of-concept, and Windows Server Update Service unauthenticated RCE demonstrated persistent attacker focus on perimeter security devices and patch management infrastructure. The rapid weaponization of network appliance vulnerabilities, combined with targeting of patch distribution systems, reflects sophisticated understanding that compromising security infrastructure and update mechanisms provides persistent access points and widespread distribution capabilities across enterprise environments.

Key Highlights

- **n8n Workflow Automation "Ni8mare" Exploit:** Dual CVSS 10.0 vulnerabilities in n8n platform enabling unauthenticated file access, administrator credential forgery, and arbitrary command execution through Content-Type confusion and unrestricted file upload. Over 103,000 potentially vulnerable instances globally with public proof-of-concept available, observed in targeted intrusion campaigns against enterprise automation infrastructure.

- **Microsoft Office Zero-Day Emergency Response:** Office OLE protection bypass vulnerability exploited as zero-day by state-sponsored threat actors before patch availability, triggering emergency out-of-band patch release on January 26. Weaponized within 72 hours through phishing campaigns delivering backdoors via RTF files, added to CISA KEV catalogue with 21-day remediation deadline reflecting critical exploitation risk.

- **SAP Enterprise Platform Critical Flaws:** SAP S/4HANA SQL injection (CVSS 9.9) enabling arbitrary SQL command execution and full system compromise, combined with Wily Introscope RCE (CVSS 9.6) and Landscape Transformation code injection (CVSS 9.1), demonstrated systematic targeting of SAP enterprise infrastructure managing critical business operations and financial data.

- **Windows Desktop Window Manager Zero-Day ASLR Bypass:** Information disclosure vulnerability enabling extraction of sensitive memory addresses from ALPC ports, commonly chained with privilege escalation exploits for full system compromise. Actively exploited in the wild as zero-day, added to CISA KEV catalog on Patch Tuesday with 21-day remediation deadline, demonstrating zero-day discovery and weaponization before vendor awareness.

- **Fortinet FortiOS SSO Zero-Day Continuation:** FortiOS SSO zero-day vulnerability (CVSS 9.8+) actively exploited in the wild during January 2026, continuing patterns of network appliance authentication bypass exploitation enabling persistent perimeter access and configuration file harvesting containing credential material.
- **Palo Alto GlobalProtect Proof-of-Concept Disruption:** Denial-of-service vulnerability in GlobalProtect with public proof-of-concept exploit enabling unauthenticated attackers to disrupt firewall operations, with repeated exploitation potentially forcing devices into maintenance mode. Affects all PAN-OS 10.1+ deployments with GlobalProtect enabled, creating operational continuity risk for enterprise perimeter security.

Top CVEs Actively Exploited

Enterprise Deserialization & Authentication Issues

- **CVE-2026-21858 (n8n "Ni8mare" Unauthenticated RCE)** - *CVSS 10.0*: Content-Type confusion vulnerability in n8n workflow automation platform allowing unauthenticated attackers to access files, forge administrator access, and execute arbitrary commands on the server through manipulation of form-based workflow.

- **CVE-2026-0501 (SAP S/4HANA SQL Injection)** - *CVSS 9.9* : Critical SQL injection vulnerability in S/4HANA impacting Remote Function Call-enabled module relying on ABAP Database Connectivity framework for native SQL statement execution, allowing attackers to execute arbitrary SQL commands and fully compromise the system.

- **CVE-2026-0500 (SAP Wily Introscope RCE)** - *CVSS 9.6*: Remote code execution issue in Wily Introscope Enterprise Manager enabling attackers to execute arbitrary code on SAP monitoring infrastructure.

- **CVE-2026-0491 (SAP Landscape Transformation Code Injection)** - *CVSS 9.1*: Code injection defect in Landscape Transformation shipped as separate DMIS add-on, allowing unauthorized command execution.

- **CVE-2026-20947 & CVE-2026-20963 (Microsoft SharePoint SQL Injection/RCE) -** CVSS *8.1*: Critical vulnerabilities affecting Microsoft Office SharePoint enabling SQL injection and remote code execution

Network Appliances & Gateways

- **CVE-2026-24858 (Fortinet FortiOS SSO Zero-Day)** - *CVSS 9.8*: Fortinet Multiple Products Authentication Bypass. The flaw exploits improper access control in FortiCloud SSO authentication

- **CVE-2026-24061 (11-Year-Old Telnetd Authentication Bypass)** - *CVSS 9.8*: Authentication bypass flaw allowing root access via Telnet, actively weaponized by actors like 'rwxrwx'.

- **CVE-2026-20856 (Windows Server Update Service RCE)** - *CVSS 8.1*: Improper input validation in Windows Server Update Service allowing unauthenticated remote code execution via machine-in-the-middle attacks.

- **CVE-2026-20868 (Windows Routing and Remote Access Service RCE)** - *CVSS 8.1*: Critical remote code execution vulnerability impacting Windows Routing and Remote Access Service.

- **CVE-2026-0227 (Palo Alto GlobalProtect DoS)** - *CVSS 7.7*: Denial-of-service vulnerability in GlobalProtect PAN-OS software caused by improper check for exceptional conditions, allowing unauthenticated attackers to disrupt firewall operations, with repeated exploitation potentially forcing devices into maintenance mode.

Browser & Runtime Exploits

- **CVE-2026-20952 & CVE-2026-20953 (Microsoft Office RCE)** - *CVSS 8.4*: Critical remote code execution vulnerabilities in Microsoft Office exploiting use-after-free conditions, requiring no user interaction in worst-case scenario with preview pane as attack vector.

- **CVE-2026-20944 (Microsoft Word RCE)** - *CVSS 8.4*: Critical out-of-bounds read vulnerability in Microsoft Office Word enabling remote code execution through malicious files, with preview pane as attack vector.

- **CVE-2026-21509 (Microsoft Office OLE Bypass Zero-Day)** - *CVSS 7.8*: Security feature bypass vulnerability in Microsoft Office 2016-2024 and Microsoft 365 Apps allowing attackers to bypass OLE mitigations and COM/OLE control protections through malicious Office files. Russian state-sponsored Fancy Bear (APT 28) exploiting via phishing campaign delivering backdoors through weaponized RTF files, observed January 29, 2026.

- **CVE-2026-20876 (Windows VBS Enclave Privilege Escalation)** - *CVSS 6.7*: Critical privilege escalation flaw in Windows Virtualization-Based Security Enclave enabling attackers to obtain Virtual Trust Level 2 privileges, subvert security controls, establish deep persistence, and evade detection.

- **CVE-2026-20805 (Windows Desktop Window Manager Zero-Day)** - *CVSS 5.5*: Information disclosure vulnerability in Windows Desktop Window Manager allowing authenticated local attackers to extract sensitive memory addresses from ALPC ports, enabling ASLR bypass. Commonly chained with privilege escalation exploits for full system compromise.

Consumer IoT & Legacy Devices

- **CVE-2023-31096 (Windows Agere Modem Driver EoP)** - *CVSS 7.8*: Two-year-old local privilege escalation flaw in Agere Soft Modem drivers allowing attackers to gain SYSTEM permissions through stack-based buffer overflow. Microsoft removed Agere Soft Modem drivers in January 2026 cumulative update, rendering affected modem hardware non-functional.

- **CVE-2026-20926 (Windows SMB Server Privilege Escalation)** - *CVSS 7.5*: Race condition vulnerability in Windows SMB Server caused by improper synchronization when handling concurrent access to shared resources, allowing authorized attackers to elevate privileges over a network through Time-of-Check Time-of-Use (TOCTOU) exploitation. The vulnerability allows authenticated users with low-level privileges to send specially crafted requests designed to trigger the race condition, exploiting the synchronization gap between security checks and resource usage to bypass authorization controls without requiring user interaction.

Observations & Trends

- **Workflow Automation & ERP Platform Dominance**: Attackers heavily concentrated on enterprise workflow systems (n8n automation platform achieving maximum CVSS 10.0 with unauthenticated RCE) and SAP S/4HANA ERP infrastructure. Compromising these platforms provides exponential payoff, enabling administrative control over business-critical workflows, arbitrary SQL command execution against enterprise databases, and lateral movement across interconnected business systems managing financial, supply chain, and operational data.

- **Microsoft Office Weaponization Renaissance**: The Office Object Linking and Embedding (OLE) bypass zero-day demonstrated persistent attacker investment in document-based exploitation chains, with Russian state-sponsored Fancy Bear (APT 28) weaponizing the vulnerability within three days of emergency patch release through phishing campaigns delivering backdoors via RTF files. This reflects long-term maintenance of Office exploitation frameworks across multiple vulnerability families (OLE bypass, use-after-free RCE, out-of-bounds read vulnerabilities) that remain effective against organizations with delayed patch deployment cycles.

- **Zero-Day Exploitation Before Disclosure**: Windows Desktop Window Manager information disclosure and Office OLE bypass were both exploited as zero-days. This compressed timeline demonstrates sophisticated threat actors' capability to discover and weaponize vulnerabilities before vendor awareness, eliminating traditional patch deployment windows and requiring organizations to implement detection-based controls rather than prevention-only strategies.

- **Privilege Escalation Chaining as Standard Practice**: Multiple vulnerabilities were specifically designed for chaining, with Windows Desktop Window Manager information disclosure commonly paired with privilege escalation exploits for full system compromise, and Windows VBS Enclave privilege escalation enabling attackers to achieve Virtual Trust Level 2 permissions for deep persistence and security control subversion. The most sophisticated campaigns demonstrated multi-stage exploitation combining Address Space Layout Randomization (ASLR) bypass, privilege escalation, and persistence mechanisms within single attack chains.

- **Legacy Driver Removal as Mitigation Strategy**: Microsoft's unprecedented removal of Agere Soft Modem drivers in cumulative updates reflects a strategic shift toward eliminating vulnerable legacy components rather than patching them, rendering affected

hardware non-functional but eliminating persistent privilege escalation attack surface. This demonstrates recognition that some vulnerability classes cannot be effectively mitigated without fundamental architectural changes or component removal.

- **State-Sponsored Rapid Weaponization**: Russian APT 28 exploitation of Office OLE bypass within 72 hours of emergency patch release, combined with attribution of network appliance targeting to state-aligned actors, demonstrates nation-state threat groups maintain pre-positioned exploitation frameworks capable of adapting to newly disclosed vulnerabilities faster than enterprise patch deployment processes can respond.

Impact Profile

- **Severity:** Majority carried Critical (9.0-10.0) or High (7.5-8.9) severity ratings, with multiple vulnerabilities achieving maximum CVSS 10.0 scores (n8n unauthenticated RCE, n8n authenticated file upload), associated with unauthenticated remote code execution, SQL injection enabling full database compromise, and privilege escalation to SYSTEM-level or Virtual Trust Level 2 permissions.

- **Exploitation Outcomes Observed:**
  - **Initial access and administrative takeover** (n8n Content-Type confusion enabling administrator access forgery, SAP S/4HANA SQL injection achieving full system compromise, Windows Server Update Service unauthenticated RCE)
  - **State-sponsored intelligence collection** (Office OLE bypass exploited by Russian APT 28 for backdoor deployment, Windows Desktop Window Manager information disclosure for ASLR bypass in targeted intrusions)
  - **Credential and memory address harvesting** (Desktop Window Manager extracting sensitive memory addresses from ALPC ports, SMB Server race condition privilege escalation)
  - **Enterprise workflow manipulation** (n8n unauthenticated file access and command execution affecting business automation workflows)
  - **Database infrastructure compromise** (SAP S/4HANA arbitrary SQL command execution, SharePoint SQL injection vulnerabilities)
  - **Privilege escalation to kernel/hypervisor level** (Windows VBS Enclave enabling Virtual Trust Level 2 access, Agere Modem driver stack-based buffer overflow for SYSTEM permissions)

    - **Network infrastructure disruption** (Palo Alto GlobalProtect DoS potentially forcing firewalls into maintenance mode through repeated exploitation)
    - **Legacy persistence mechanisms** (11-year-old Telnetd authentication bypass actively weaponized for root access by 'rwxrwx' threat actor)

- **Threat Type Balance:** Activity revealed stark polarization between highly targeted, state-sponsored intrusions (Russian APT 28 Office exploitation campaigns, Windows Desktop Window Manager zero-day in selective targeting) and widespread opportunistic scanning (n8n unauthenticated RCE affecting 103,000+ exposed instances, Fortinet FortiOS SSO zero-day exploitation at scale, legacy Telnetd vulnerability weaponization for mass compromise). State-aligned actors demonstrated operational focus on Office document exploitation chains and Windows kernel-level privilege escalation for long-term persistence, while opportunistic groups prioritized maximum CVSS 10.0 unauthenticated RCE vectors in enterprise workflow automation platforms.

Distributed Denial-of-Service (DDoS) Activity

Overview

January 2026 DDoS activity was dominated by hacktivist-style, geopolitically aligned campaigns, with pro-Russian actor NoName057(16) and its DDoSia ecosystem repeatedly highlighted in weekly reporting as conducting coordinated operations against national-scale targets.

The United Kingdom emerged as a focal point in early January, with a seven-day campaign from 5 to 11 January assessed as intensive and tightly coordinated, reinforcing the continued use of DDoS as a low-cost, high-visibility disruption and propaganda tactic. India-related January 2026 DDoS specifics are less consistently documented in the same openly accessible weekly sources referenced here; however, the broader pattern of hacktivist disruption affecting public-facing services and critical sectors remains consistent with late-2025 activity and is likely to persist into early 2026.

Key Threat Groups Observed

- **NoName057(16) / DDoSia:** Maintained prominence in January 2026 reporting, with an intensive coordinated campaign from 5 to 11 January.The activity showed operational coordination through repeated “target list updates” across the week, suggesting sustained planning rather than one-off floods.

- **Pro-Russia hacktivist ecosystem:** UK government reporting described continuing pro-Russia-aligned hacktivist activity targeting UK organizations, emphasizing that motivations were ideological rather than financial and reflecting an evolving DDoS threat environment

Targeted Regions and Sectors

- **United Kingdom** was the dominant target geography in the 5–11 January dataset, representing 85.2% of recorded attacks in that reporting period.

- “Unknown/International” targets were also present (14.8%) within the same dataset, consistent with spillover targeting beyond a single country.

Attack Characteristics and Motivation

The January (5 – 11) campaign was reported with measurable scale 1,812 recorded attack entries, 86 unique domains, and 87 unique IP addresses indicating multi-target pressure rather than a single-victim event. The persistence over seven consecutive days plus repeated target-list updates indicates coordination and a structured campaign cycle (plan → execute → amplify → retarget).

Key takeaways

- Prioritize resilience for public-facing national services (especially government and critical “infrastructure” domains) against sustained multi-day campaigns, as demonstrated by the UK-focused operation.

- Treat DDoS as part of an influence/attention strategy: build a “claim-driven” response loop (monitoring + fast comms), because ideologically motivated actors optimize for visibility and public trust effects.

- Ensure mitigations cover campaign persistence (not just peak volume): automate detection of repeated waves and rotating targets, since the January operation showed repeated updates and sustained cadence.

Cyber Incidents - January 2026

Overview

January 2026 was defined by the continued industrialization of cyber-enabled fraud in India, renewed momentum in supply-chain-enabled compromise affecting consumer crypto users, and urgent patch-driven risk tied to actively exploited perimeter and security-appliance vulnerabilities. India's most consequential developments cantered on "digital arrest" and authority-impersonation scams operating at scale, exemplified by Telangana Cyber Security Bureau arrests tied to an interstate syndicate linked to losses of over ₹16 crore and multi-state mule-account facilitation.

In India, the month reinforced that fraud operations are no longer purely low-value, high-volume schemes; they increasingly combine sustained psychological coercion ("virtual custody" via continuous video calls), forged legal narratives, and rapid fund movement through layered accounts to enable crore-level theft from individual victims. The operational pattern impersonation + remote surveillance + fast laundering suggests that enforcement gains will hinge on disrupting mule-account supply, improving bank-side velocity checks, and accelerating cross-state coordination rather than only victim awareness messaging.

Globally, high-impact incidents illustrated how third-party and ecosystem compromise remains the attacker's preferred force multiplier: Trust Wallet attributed an approximately $8.5 million theft from 2,500+ wallets to activity linked to the "Shai-Hulud" npm supply-chain campaign, showing how developer-toolchain intrusions can convert into direct end-user financial loss.

India incidents : January 2026

- **Telangana Cyber Security Bureau busts ₹16-crore "digital arrest"/interstate fraud network** - Telangana Cyber Security Bureau arrested six people described as CA aspirants/MBAs for allegedly running a sophisticated interstate fraud network with losses reported at around ₹16 crore. Reporting tied the operation to "digital arrest" scam tradecraft (authority impersonation, coercive pressure, and forced transfers), reflecting the continued scale-up of impersonation-led financial crime in India.

- **Delhi "digital arrest" case: doctor couple allegedly defrauded of ~₹14.85 crore; e-FIR registered** - Delhi Police investigated a case in which an elderly doctor couple in Greater Kailash was allegedly kept under "digital arrest" for over two weeks and coerced into transferring nearly ₹14.85 crore after scammers impersonated law enforcement/telecom officials. The incident window reported in January culminated in an e-FIR and ongoing cybercrime unit investigation, illustrating high-value victim targeting through prolonged psychological control.

- **Everest ransomware group claim against McDonald's India -** A weekly threat brief reported that the Everest ransomware group claimed it breached McDonald's India and exfiltrated 861 GB of data, posting "evidence" on its leak portal around 20 January 2026. As of the brief's noted timeframe, McDonald's India had not publicly confirmed the incident, so this should be tracked as a **leak-site claim pending independent confirmation.**

- **Alleged dark-web listing of Indian fintech "Rmoney India" with claimed production database exfiltration** - CYFIRMA reported that "Rmoney India" was allegedly listed on a dark-web forum on 8 January 2026, with a threat actor claiming theft of a 1.5 GB SQL dump including KYC-related data and other schemas. Treat this as an allegation until corroborated by victim disclosure or regulator/forensic confirmation, but it signals continued targeting of fintech/KYC ecosystems in India.

Global incidents : January 2026

- **Trust Wallet crypto theft (~$8.5M) tied to "Shai-Hulud" npm supply-chain activity** - Trust Wallet linked an approximately $8.5 million theft affecting 2,500+ wallets to a supply-chain compromise associated with the "Shai-Hulud" npm malware campaign, described as involving a malicious browser extension used to drain funds. This incident reinforced how developer-ecosystem compromises can translate directly into consumer crypto losses at scale.

- **Sedgwick Government Solutions confirms cyber incident; ransomware gang claim (TridentLocker)** - Sedgwick's federal contractor subsidiary confirmed a cyber incident in early January, with reporting noting a ransomware claim by TridentLocker and alleged theft of ~3.4 GB of data from an isolated file transfer system. The event highlights continued targeting of government-adjacent service providers and the persistence of data-theft extortion even when core networks are segmented.

- **Kyowon Group (South Korea) disruption from suspected ransomware; large-scale account exposure risk** - A suspected ransomware incident disrupted systems at Kyowon Group, a major South Korean education company, prompting incident response and investigation. Separate reporting stated Kyowon confirmed a ransomware attack with an external data leak and that investigators estimated up to 9.6 million accounts may be exposed, demonstrating high-impact risk in the education services sector.

- **eScan update-server breach used to push malicious update** - Security vendor eScan confirmed its update server was breached and used to distribute a malicious software update to customers. This is a high-risk scenario because compromised update channels can rapidly propagate malware across many downstream endpoints.

Global Data Breach Intelligence Summary - January 2026

Overview

January 2026 marked a pivotal shift in cybersecurity incidents with high-profile corporate intellectual property breaches overshadowing traditional customer data compromises. The month was dominated by WorldLeaks ransomware group's 1.4TB Nike data exfiltration and Target's massive 860GB source code exposure through a misconfigured public Git server. Healthcare systems faced continued ransomware assaults with New Zealand's Manage My Health suffering compromise of 428,337 medical documents affecting 120,000+ patients, while Monroe University disclosed a year-old breach impacting 320,973 individuals with comprehensive identity data exposure. January demonstrated attackers' strategic pivot toward proprietary source code, manufacturing blueprints, and intellectual property rather than consumer databases, alongside persistent third-party supply chain vulnerabilities exemplified by Ledger's breach through payment processor Global-e. The month revealed systematic targeting across retail, technology, healthcare, education, and financial sectors, with **ransomware groups including Qilin, Akira, Shinobi, and Clop claiming hundreds of victims through dark web leak sites**, while delayed breach disclosures some spanning months between discovery and notification continued exposing victims to prolonged identity theft and fraud risks.

Major Data Breaches: January 2026

1) Nike Data Breach (Nike, Inc.)

- **Threat Actor:** WorldLeaks ransomware group (rebrand of Hunters International)
- **Vulnerability:** Unauthorized access to internal systems (attack vector not publicly disclosed)
- **Estimated Victims:** Unknown (no customer data confirmed exposed); internal data exposure
- **Timeline / Discovery Date:**
    - **Disclosed:** January 22-26, 2026
    - **WorldLeaks listing:** January 22, 2026
    - **Later removed from leak site:** January 27, 2026

- **Description:** Nike confirmed it is investigating a potential data breach after the ransomware group WorldLeaks claimed to have published **1.4 terabytes of data** from the sportswear giant. The group published files with names pointing to design and manufacturing workflows, including directories labeled Women's Sportswear, Men's Sportswear, Training Resource Factory, and Garment Making Process

- **Attack Methodology:** The scale of the extraction **1.4TB equivalent to 280 million pages of documents** signals sustained access to Nike's internal network long enough to locate, collect, and transfer a massive volume of files The attack methodology remains undisclosed, though experts suspect third-party access or compromised credentials.
- **Claimed Victims Include:** WorldLeaks alleges it has stolen 188,347 files from Nike's systems , primarily focused on product development, manufacturing processes, and internal operational documentation.

- **Response Measures:** Nike has engaged cybersecurity experts to conduct detailed forensic investigation, and legal teams are reportedly preparing for potential regulatory notifications. The company has not confirmed whether any ransom was paid. WorldLeaks removed the Nike entry from its leak site before publication, suggesting possible negotiation with the company

- **Potential Impact:** Based on available analysis, the leaked data does not appear to include customer personal information such as names, addresses, payment details, or Social Security numbers. However, the exposed data reportedly includes product designs, manufacturing details, pricing information, materials specifications, factory audits, and intellectual property that could benefit competitors and undermine Nike's competitive advantage.

2) Target Source Code Breach

- **Threat Actor:** Unknown (Initial Access Broker or insider threat suspected)

- **Vulnerability:** Exposed internal Git server (git.target.com) accessible from public internet without VPN requirement

- **Estimated Victims:** Unknown (source code breach, not customer data)

- **Timeline / Discovery Date:**

  - **Breach discovered:** Early January 2026
  - **Sample posted:** January 13, 2026
  - **Target locked down Git server:** January 9, 2026
  - **Disclosure:** January 13, 2026

- **Description:** A threat actor published a **14MB** preview of stolen repositories on Gitea serving as advertisement for a gargantuan 860GB dataset allegedly containing the retailer's core business logic and internal documentation. Multiple current and former Target employees confirmed that leaked source code samples match real internal systems.

- **Attack Methodology:** The attackers allege to have exfiltrated the trove from Target's self-hosted Gitea development server. The leaked repositories contain Target's source code, configuration files, and documentation with files referencing Target's internal systems such as wallet services, identity management systems, networking tools, and gift card systems.

- **Confirmed Major Victims:** Target Corporation

- **Claimed Victims Include:** The threat actor claims about 860 GB of internal source code and developer documentation were stolen, including digital wallet systems, gift card platforms, networking tools, and identity services.

- **Response Measures:** Target rolled out an accelerated lockdown of its Git server requiring VPN access a day. The company made its repositories private and restricted git.target.com to only be accessible from Target's internal network or corporate VPN. Target has not responded to media inquiries or confirmed the breach officially.

- **Potential Impact:** Unlike breaches that focus on customer data, a compromise of development infrastructure exposes the blueprints of how a company's systems operate. Possessing the blueprints of a company's software allows bad actors to conduct deep offline analysis to find hidden vulnerabilities. The breach also exposed names and details of internal engineers, creating targeted lists for spear-phishing or social engineering attacks.

3) Manage My Health (New Zealand) Data Breach

- **Threat Actor:** "Kazu" (hacker forum user) - Ransomware/extortion attack.

- **Vulnerability:** Unauthorized access to "My Health Documents" module within patient portal application

- **Estimated Victims:** 120,000-127,000 individuals (6-7% of 1.8 million registered users); 428,337 medical documents compromised

- **Timeline / Discovery Date:**
    - **Breach discovered: D**ecember 30, 2025 (company notified by partner)
    - **Data posted on hacking forum:** December 30, 2025
    - **Public disclosure:** January 1, 2026
    - **Ransom deadline:** January 15, 2026
    - **Patient notifications:** Mid-January 2026

- **Description:** The ManageMyHealth data breach involved unauthorized access to the ManageMyHealth online patient portal in New Zealand with exfiltration of hundreds of thousands of sensitive medical documents. The investigation identified that one module, Health Documents, within the app was compromised, not the whole app.

- **Attack Methodology:** Ransom hackers accessed and downloaded documents stored in the My Health Documents section of Manage My Health. Hacker Kazu stated precisely 428,337 files totaling 108 gigabytes had been dumped on a hacking forum on December 30 and demanded a ransom of $60,000 by a deadline of January 15.

- **Confirmed Major Victims:** Manage My Health users across New Zealand; 45 general practices in the Northland Region and 355 referral-originating medical practices across several regions

- **Claimed Victims Include:** Sample of leaked data reportedly included clinical notes, lab results, vaccination records, medical photographs and personal information such as names, emails and phone numbers.

- **Response Measures:** Manage My Health secured the affected feature, engaged independent cybersecurity specialists, notified regulators including the Office of the

Privacy Commissioner, New Zealand Police, and Health New Zealand. **ManageMyHealth** applied to the High Court for urgent injunctive relief to prevent access to use of or dissemination of the stolen data. The company commenced legal action and established a dedicated 0800 support helpline.

- **Potential Impact:** Exposed documents included files uploaded by individual users such as correspondence, reports, or results; referrals and discharge summaries from hospitals and specialists; laboratory results and imaging reports; clinical correspondence between providers; and prescriptions or vaccination records. The breach poses risks for medical identity theft, insurance fraud, blackmail, and severe privacy violations particularly for survivors of sexual violence and family harm whose sensitive medical records were exposed.

4) Monroe University Data Breach

- **Threat Actor:** Unknown
- **Vulnerability:** Unauthorized access to university computer systems
- **Estimated Victims:** 320,973 individuals
- **Timeline / Discovery Date:**
    - **Breach occurred:** December 9-23, 2024
    - **Breach discovered:** September 30, 2025
    - **Notification sent:** January 2, 2026
    - **Public disclosure:** January 2026
- **Description:** Monroe University suffered a data breach where cybercriminals gained unauthorized access to the university's computer systems between December 9 and December 23, 2024, and acquired copies of files containing highly sensitive data. Monroe University disclosed the breach following a prolonged forensic investigation that concluded nearly a year after the intrusion took place

- **Attack Methodology:** An unauthorized third party gained temporary access to certain university computer systems and copies of certain files stored on the network may have been acquired without authorization. The specific attack methodology has not been publicly disclosed.

- **Confirmed Major Victims:** Monroe University students, applicants, staff, and affiliated individuals across New York campuses (Bronx, New Rochelle) and Saint Lucia.

- **Claimed Victims Include:** Over **320,000 individuals** including current and former students, applicants, and university-affiliated people.

- **Response Measures:** Monroe University did not notify affected individuals of the breach until January 2, 2026, months after the intrusion occurred. Monroe University offered complimentary one-year credit monitoring and fraud assistance services through Cyberscout to affected individuals. Multiple class action lawsuits have been filed against the university.

- **Potential Impact:** The compromised information included names, dates of birth, Social Security numbers, driver's license and passport numbers, financial account details, student records, and protected health information. Electronic accounts or email usernames and passwords, medical information, and health insurance information were also compromised. The breach places affected individuals at heightened risk of identity theft, financial fraud, medical identity theft, and misuse of credentials.

Additional January 2026 Breach Disclosures

Based on official breach notification records, the following organizations disclosed data breaches in January 2026:

- **Healthcare Sector:**
    - **Alpine Ear, Nose, and Throat (Colorado)** – Notification letters sent January 30, 2026, for breach discovered in November 2024; BianLian ransomware group claimed responsibility; exposed data includes names, dates of birth, medical information, financial account information, credit card numbers with CVC/expiration dates, and Social Security numbers.
    - **The Phia Group, LLC (Massachusetts)** – Healthcare cost containment services provider notified clients about unauthorized access; compromised data included names, addresses, dates of birth, Social Security numbers, financial account information, driver's license/state ID numbers, health insurance information, and medical treatment details.

- **HealthBridge Chiropractic (Philadelphia)** – Targeted by Qilin ransomware group on January 6, 2026; nature and quantity of compromised data under investigation
- **Asian Heart Institute** – Targeted by Shinobi ransomware group; disclosed January 22, 2026
- **Bayside Dental Rowlett** – Targeted by Shinobi ransomware group; disclosed January 22, 2026
- **MIMS (Healthcare Information Service)** – Targeted by Devman ransomware group; disclosed January 22, 2026
- **Chuyang Dental** – Targeted by Qilin ransomware group; disclosed January 29, 2026

- **Financial Services:**
  - **Korol Financial** – Targeted by Clop ransomware group; disclosed January 22, 2026
  - **K&N Kenanga Holdings (Malaysia)** – Targeted by Qilin ransomware group; disclosed January 21, 2026
  - **CPF Financial Services (Kenya)** – Targeted by TheGentlemen ransomware group; disclosed January 21, 2026
  - **Ledger (Cryptocurrency Wallet)** – Customer data exposed after third-party payment processor Global-e was hacked; compromised data includes names and contact information (seed phrases not affected); Global-e also services Netflix, Disney, adidas, and luxury brands
  - **Nomad (Cryptocurrency Platform)** – FTC settlement over lax security that led to hackers stealing $186 million from Nomad customers; company failed to implement adequate security measures despite advertising as "security-first"
  - Ameriprise Financial Services, LLC
  - PNC Financial Services, Inc
  - Eastern Bank
  - Jackson National Life Insurance Company
  - JPMorgan Chase Bank, N.A
  - Needham Bank
  - Dollar Financial Group, Inc (Money Mart)
  - FloatMe, Corp
  - Topstep LLC

- **Retail & E-Commerce:**
    - **Under Armour** – Security incident from November 2025; customer dataset released on hacking forum January 21, 2026; exposed data includes names, birthdates, purchase histories, locations, and 72 million email addresses
    - **Hartford (French Fashion Retailer)** – Targeted by Lynx ransomware group; disclosed January 4-5, 2026; double-extortion attack
    - **SoundCloud** – Targeted by ShinyHunters group; member data accessed through internal systems breach with VPN disruption; disclosed January 26, 2026

- **Technology & Manufacturing:**
    - **European Space Agency –** Cyberattack compromised servers used for collaborative engineering solutions; breach forums report over 200GB stolen including API tokens, Bitbucket repositories, and source codes.
    - **Global Shop Solutions –** Data breach involving ANKA manufacturing platform disclosed January 23, 2026; unauthorized access affected multiple client organizations using shared cloud-based platform
    - **CSV Group (Italy) –** Carpentry and fabrication services provider targeted by Qilin ransomware; disclosed January 2, 2026.
    - **3GH Informatica Integral (Spain) –** Data security provider targeted by Incransom ransomware group.
    - **FOX Architects (Washington) –** Targeted by Shinobi ransomware group; data stolen and encrypted.
    - **Venezia Bulk Transport Inc –** Maritime transportation provider experienced unauthorized access to internal IT systems.
    - **Eros (India) –** Elevator manufacturing company breach; over 12GB sensitive data compromised.
    - **M&M Auto Parts –** Targeted by Shinobi ransomware group.
    - **Spector Group (Architecture) –** Targeted by Akira ransomware; disclosed January 26, 2026.

- **Professional Services:**
    - **McMath Woods P.A (Law Firm) –** Targeted by Clop ransomware; disclosed January 22, 2026.
    - **Mettler Partner (Switzerland) –** Targeted by Akira ransomware; disclosed January 22, 2026.
    - **SJL Jimenez Lunz (Legal) –** Targeted by MS13-089 group; disclosed January 16, 2026

  - **Gorlick, Kravitz, & Listhaus, P.C (Law Firm)**
  - **Finnegan, Marks, Desmond & Jones.**

- **Government & Utilities:**
  - **TSU One (Utility Services) –** Targeted by Qilin ransomware; disclosed January 16, 2026
  - **California Tax Data –** Targeted by Play ransomware group; disclosed January 23, 2026
  - **DHS (U.S. Department of Homeland Security) –** Multiple data security incidents reported in January 2026.

- **Telecommunications:**
  - **Claro Chile S.A –** Targeted by STORMOUS ransomware; disclosed January 23, 2026
  - **GMA Network Inc (Philippines) –** Media company targeted by Devman ransomware; disclosed January 21, 2026
  - **Total Wireless**

Strategic Assessment

January 2026 breaches collectively illustrated critical trends in the cyber threat landscape:

1. Supply Chain as Primary Attack Vector: Third-party compromises dominated January incidents. Ledger's breach occurred through Global-e, a payment processor serving Netflix, Disney, and adidas. Global Shop Solutions' platform breach cascaded across multiple manufacturing clients. Healthcare providers suffered repeated vendor-related exposures. Organizations inherit security weaknesses from every third-party connection. Traditional perimeter defenses fail when attackers exploit trusted vendor access

2. Zero-Day Exploitation at Scale: Misconfiguration replaced zero-days as the primary vulnerability. Target's Gitea server was publicly accessible without VPN, enabling 860GB source code theft. Manage My Health's single module exposure led to 428,337 document exfiltration. Configuration errors now rival sophisticated exploits in breach frequency. Attackers target exposed infrastructure over costly zero-day development. Basic security gaps provide easier entry than advanced exploits.

3. Social Engineering Sophistication: Technical exploitation overtook traditional social engineering. European Space Agency attackers stole API tokens from exposed repositories. Manage My Health's attacker "Kazu" demanded precisely $60,000 by January 15,

demonstrating calculated ransom pricing. Threat actors analyze victim financial capacity and regulatory exposure before setting demands. Delayed monetization strategies emerged, with Under Armour's November breach data surfacing in January. Attackers now combine technical access with strategic extortion timing.

4. Cross-Sector Impact: No sector remained immune in January. Education faced 4,388 weekly cyberattacks per organization in 2025. Healthcare, retail, finance, and government all experienced major incidents. Nike and Target breaches exposed intellectual property over customer data. Financial services logged 739 data compromises in 2025, the highest of any industry for the second consecutive year. Attackers exploit common platforms spanning all industries. Shared technology stacks create universal vulnerabilities regardless of sector.

5. Underground Marketplace Activity: Ransomware-as-a-service groups accelerated January operations. Qilin, Akira, Shinobi, Clop, and Play groups claimed multiple victims. WorldLeaks (rebranded Hunters International) published 1.4TB from Nike before removing the listing, suggesting negotiation. Under Armour's dataset with 72 million emails appeared on hacking forums. Multiple dark web leak sites listed hundreds of victims throughout January. Cybercrime operates as a mature service industry with established customer support and data marketplaces. Stolen data faces permanent exposure risk beyond initial ransom negotiations.

Key Takeaways

1) **Vendor security equals organizational security**: Third-party breaches at Global-e and Global Shop Solutions demonstrate supply chain vulnerabilities cascade across entire customer bases.
2) **Misconfiguration rival’s malware**: Target's publicly exposed Git server enabled massive source code theft without sophisticated exploits.
3) **Detection gaps enable sustained access:** Nike's 1.4TB extraction signals prolonged network presence and systematic data collection
4) **Source code breaches escalate risk**: Stolen development blueprints enable deep offline vulnerability analysis by threat actors.
5) **Healthcare remains priority target**: BianLian, Qilin, and Shinobi groups continued systematic healthcare targeting with high-value medical data.
6) **Financial services lead breach counts**: 739 financial sector compromises in 2025 exceeded all other industries for the second year
7) **Ransom strategies evolved:** Attackers now calculate precise demands based on victim capacity rather than data volume

8) **Delayed disclosure compounds damage**: Monroe University's September 2025 discovery wasn't disclosed until January 2026, extending victim exposure.
9) **Intellectual property targeting increased**: Nike and Target breaches prioritized proprietary designs and source code over customer databases.
10) **Education faces relentless assault**: 4,388 weekly attacks per institution demonstrate sustained adversary focus on academic targets.
11) **Multi-year breach trends continue**: Despite record breach counts, victim notifications dropped 79% as attackers shift from mega-breaches to precise, high-value data targeting.

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