SAPTANG™
Proactive Threat Defence

Monthly Threat Report
February 2026

Contents

Executive Summary

February 2026 featured escalating cyber threat activity across ransomware, unprecedented zero-day exploitation, hacktivist-driven DDoS operations, and massive data breaches dominated by social engineering attacks with significant supply chain and telecom sector exposure.

Ransomware disclosures totalled 680 victim postings across 54 active operations, with Qilin leading the month (104 victims) followed by TheGentlemen (78), CL0P (49), Play (44), and INC Ransom (39). Payment rates declined to 20-35% as organizational resilience improved, while healthcare incidents doubled to 93.

Vulnerability exploitation featured sub-24-hour weaponization of critical infrastructure, including BeyondTrust Remote Support unauthenticated RCE (8,500 exposed instances), Dell RecoverPoint CVSS 10.0 hardcoded credentials (18-month state-sponsored campaign), Cisco Catalyst SD-WAN authentication bypass prompting emergency CISA directive, and six Microsoft zero-days within a single Patch Tuesday cycle demonstrating unprecedented attacker speed and sophistication.

Data breach disclosures emphasized social engineering-driven mass exposure, including ShinyHunters' systematic vishing campaign affecting Panera Bread (5.1M), CarGurus (12.4M), Match Group (10M+), and the catastrophic Conduent Business Services breach escalating to 25+ million victims, the eighth-largest U.S. healthcare breach. Third-party compromises at Odido (6M+), Singapore's four major telcos (UNC3886 zero-day campaign), TriZetto (3.4M), and ManoMano (38M) demonstrated that telecom and supply chain vulnerabilities enable attackers to target entire economies rather than isolated organizations.

Key Highlights

- **Ransomware Activity –**
  - **Elevated threat levels**: 680 victim disclosures across 54 active operations, maintaining historically high activity amid ecosystem fragmentation
  - **Top threat actors by victim count**: Qilin (104 victims), TheGentlemen (78), CL0P (49), Play (44), and INC Ransom (39)
  - **Geographic concentration**: United States absorbed 49% of identifiable incidents, followed by Europe (25%), Canada (5%), Thailand (TheGentlemen surge), and Brazil (24 education victims)

- ❖ **Sector targeting**: Manufacturing/industrial leading exposure, healthcare incidents doubled to 93, education and professional services sustaining heavy hits, construction emerging strongly
- ❖ **Top 10 groups captured approximately 65% of victims** amid affiliate shifts and decentralized growth
- ❖ **Payment rates declined to 20-35%** versus prior periods, signalling improved organizational resilience through enhanced backups and response
- ❖ **Median ransom demands stabilized at $1.1–1.4 million**; recovery rates hit 96% for encrypted victims
- ❖ **Attack vectors**: 32% exploited VPN/RDP vulnerabilities, 28% used credential compromise, perpetuating cross-regional risks

- **Vulnerability Exploitation –**
  - ❖ **Unprecedented sub-24-hour weaponization** of remote support infrastructure with state-sponsored multi-year zero-day campaigns culminating in emergency government directives
  - ❖ **Six Microsoft zero-days within single Patch Tuesday cycle** (Office, Word, Windows Shell, Desktop Window Manager, Remote Desktop Services)

- **Distributed Denial-of-Service (DDoS) Activity** –
  - ❖ **Sustained hacktivist-driven geopolitical campaigns:** Pro-Russian NoName057(16) prominently targeting Milan-Cortina Winter Olympics and government infrastructure
  - ❖ **DDoSia platform:** Coordinated volumetric and application-layer floods alongside opportunistic regional groups amplifying claims via Telegram
  - ❖ **Geographic focus:** Europe bore brunt of named operations; Asia-Pacific (including India) saw spillover from multi-nation campaigns
  - ❖ **India-specific activity:** Aligned with regional hacktivist patterns targeting public-facing government and critical services
  - ❖ **Tactical approach:** Brief outages (minutes to hours) prioritizing psychological disruption and media visibility over prolonged outages, often paired with defacements

- **Cyber Incidents** –
  - ❖ **Resurgent ransomware targeting critical infrastructure:** High-profile operational disruptions including:
    - Advantest Corporation semiconductor operations (Japan)
    - University of Mississippi Medical Centre clinic network shutdown
    - France's FICOBA financial registry breach: 1.2 million accounts exposed

  - ❖ **India-specific developments:**
    - Policy responses and strategic risk elevation: India AI Impact Summit high-alert status amid "Agentic AI" threats
    - Heightened national vigilance as AI-enhanced attacks accelerate targeting digital transformation initiatives

- **Global telecommunications as force-multiplier:**
  - ❖ **Odido breach:** 6M+ Dutch telecom customers exposed
  - ❖ **Singapore's four major telcos:** Compromised by Chinese nexus UNC3886 via zero-days
  - ❖ **Strategic implication:** Sustained, undetected carrier infrastructure access enabling downstream targeting of entire economies rather than isolated organizations

- **Global Data Breach Activity –**
  - ❖ **Social engineering replaced technical exploits** as primary threat vector through systematic vishing campaigns
  - ❖ **ShinyHunters' systematic vishing campaign** exploiting single sign-on vulnerabilities:
    - Panera Bread: 5.1 million customers
    - CarGurus: 12.4 million accounts
    - Match Group: 10+ million records
    - Figure: 1 million users

Ransomware Activity of February 2026

Overview

Ransomware continued to pose elevated and persistent threat levels throughout February 2026, with victim postings totaling 680 disclosures across 54 active operations, maintaining historically high activity amid ecosystem fragmentation and competitive pressures. The landscape featured pronounced diversification, with operational extortion groups spanning established volume leaders and rapidly scaling newcomers like TheGentlemen, demonstrating the RaaS model's resilience as affiliates migrate between brands and fill gaps left by disruptions. **Qilin dominated with 104 victims, followed by TheGentlemen (78), CL0P (49), Play (44), and INC Ransom (39),** underscoring how industrialized pipelines enable a handful of actors to drive disproportionate impact while smaller operators gain ground.

Geographically, **the United States remained the primary target at 49% of identifiable incidents, trailed by Europe (25%), Canada (5%), Thailand (notable TheGentlemen surge), and Brazil (24 education victims)**, reflecting attackers' pursuit of high-value density alongside expanding footprints in emerging markets. Critical sectors absorbed the brunt, with manufacturing/industrial leading exposure, **healthcare doubling to 93 incidents**, education and professional services sustaining heavy hits, and construction emerging strongly top 10 groups capturing 65% (approx.) of victims amid affiliate shifts and decentralized growth.

Payment rates trended lower into the 20-35% range versus prior periods, signaling organizational resilience gains through improved backups and response, while median demands stabilized at $1.1–1.4 million amid supply saturation. Recovery rates hit 96% for encrypted victims via tools or restore, though 32% of attacks exploited vulnerabilities (VPN/RDP dominant) and 28% used credential compromise, perpetuating risks across regions and verticals despite defensive progress.

Major Threat Actor Analysis

Qilin – High-Volume Industrial and Food Supply Chain Disruption

The Qilin operation dominated activity with **104 recorded victims**, a commanding performance that solidified its leadership among ransomware operators. The targeting heavily favored manufacturing and food supply chains, with notable victims including **Mount Barker Co-operative**, **regional steel fabricators**, **automotive parts suppliers**, and

logistics providers, demonstrating a pattern of prioritizing production-critical infrastructure were downtime cascades into immediate financial and contractual penalties. Qilin executes aggressive double-extortion with streamlined efficiency, deploying encryption to halt operations while exfiltrating gigabytes of proprietary data for leak-site pressure, exploiting sector-specific sensitivity to force accelerated negotiations.

TheGentlemen – Rapidly Scaling Multi-Sector Attacks

TheGentlemen registered **78 recorded victims**, nearly doubling prior output and establishing itself as a fast-growing force with broad opportunistic targeting. The group hit manufacturing, education, and business services, including **mid-tier construction firms**, **regional schools**, and **professional consultancies**, reflecting a pattern of pursuing mid-market entities where disruption yields quick leverage without requiring highly sophisticated access. Affiliates favor common perimeter exposures and credential abuse, followed by rapid exfiltration and encryption to enforce classic double-extortion against resource-constrained defenders.

CL0P – Enterprise Vulnerability Exploitation

CL0P claimed **49 recorded victims**, maintaining high-impact focus on enterprise software and supply-chain compromises. Targets included **organizations hit via Oracle EBS flaws**, **file-transfer platforms**, and **large-scale manufacturing**, illustrating a signature pattern of mass data harvesting through zero-day or recently patched vulnerabilities. The strategy centers on pure data extortion with auction-style leaks, bypassing widespread encryption to maximize downstream effects across affected customer bases.

Play – Consistent Global Mid-Market Pressure

Play disclosed **44 recorded victims**, sustaining steady cadence across engineering, IT services, and logistics with a pattern of targeting mid-sized organizations sensitive to operational interruption. Notable victims included **aerospace engineering firms**, **regional IT consultancies**, and **transportation providers**, where business continuity demands amplify ransom urgency. Campaigns align with opportunistic RDP/VPN intrusions, staged data theft, and encryption to create immediate paralysis and negotiation leverage.

INC Ransom – Persistent Public and Services Targeting

INC Ransom posted **39 recorded victims**, reflecting mid-tier reliability with emphasis on public sector, education, and professional services. Victims included **municipal governments**, **K-12 districts**, and **law firms**, signaling a pattern of hitting under-resourced entities where service disruption combines with data exposure for high pressure. The group leverages double-extortion through exfiltration threats and operational lockout, optimized for organizations with limited recovery options**.**

Akira – VPN-Driven Industrial and Services Compromises

Akira registered **39 recorded victims**, delivering consistent volume through attacks on industrial firms, professional services, and IT providers. Notable targets included **power equipment manufacturers**, **construction companies**, and **consulting firms**, demonstrating a pattern capitalizing on production and delivery obligations for rapid coercion. Affiliates heavily exploit misconfigured VPN/RDP endpoints, using credential weaknesses and poor patching hygiene to enable widespread opportunistic compromises.

LockBit – Resurgent Affiliate-Driven Operations

LockBit logged **34 recorded victims**, showing marked resurgence through its mature RaaS ecosystem targeting manufacturing, services, and government. Victims encompassed **European manufacturers**, **U.S. municipalities**, and **service providers**, reflecting a pattern of broad affiliate deployment against downtime-sensitive targets. The group deploys advanced encryption kits with data leaks, focusing on operational recovery pressure while maintaining high negotiation efficiency.

DragonForce – Reputation-Focused Services and Retail

DragonForce claimed **30 recorded victims**, blending data extortion with high-visibility pressure on professional services and consumer businesses. Notable victims included **law firms**, **electrical contractors**, and **auto dealerships**, illustrating a pattern prioritizing reputational damage alongside operational disruption. The approach mixes classic mechanics with public shaming and leak threats to maximize leverage beyond technical recovery.

INSOMNIA – Emerging Steady Growth Across Sectors

INSOMNIA recorded **25 recorded victims**, emerging as a reliable mid-tier actor with broad targeting across construction, education, and finance. It involves **mid-sized construction**, **financial Small and Medium-Sized Businesses (SMBs)**, and **service providers**, showing a pattern of scalable double-extortion against mid-market targets. The model leverages ransomware encryption plus leak threats, exploiting public-facing apps and credential access for repeatable campaigns.

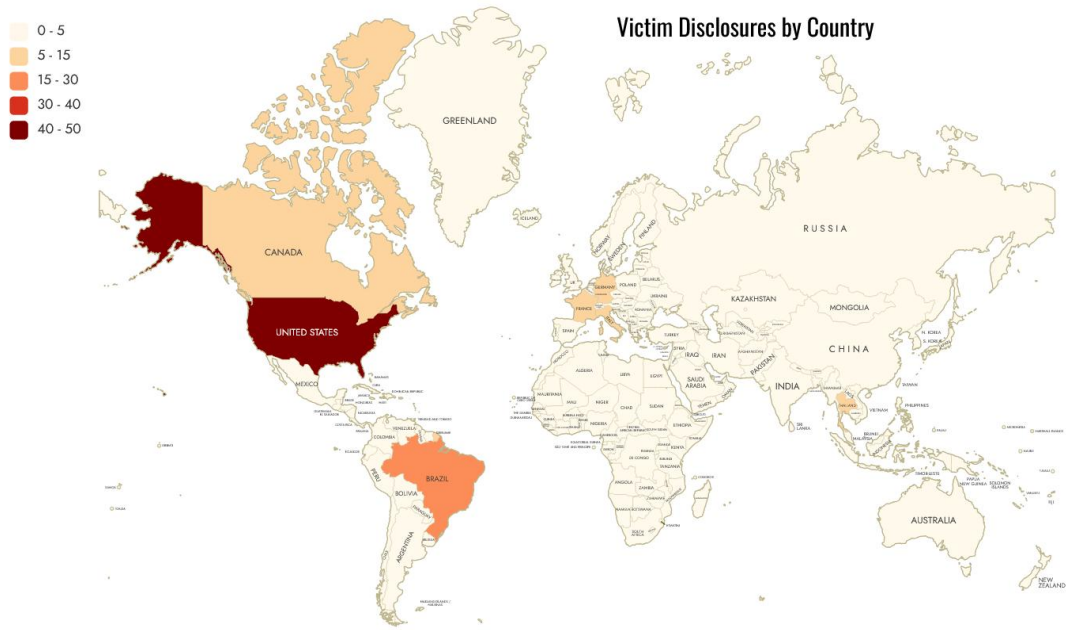
NightSpire – Newcomer Multi-Sector Expansion

NightSpire posted **25 recorded victims**, rapidly scaling as a newer entrant focused on healthcare, manufacturing, and education. Victims included **regional hospitals**, **schools**, and **construction firms**, reflecting an aggressive pattern of disruption against time-sensitive sectors. The group combines file encryption, backup deletion, and leak-site threats to position itself as a high-pressure newcomer in competitive ecosystems.

Sectoral & Geographic Impact

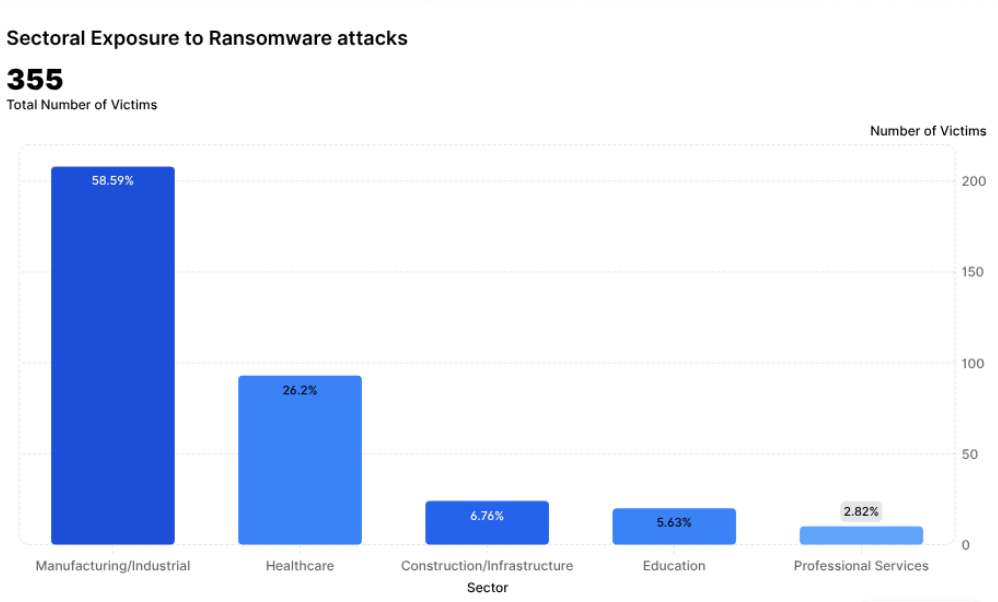
Geographic Distribution

The United States continued to dominate as the primary target, accounting for approximately 49% of tracked victim disclosures, driven by dense concentrations of manufacturing, healthcare, and professional services across Qilin, TheGentlemen, and Akira campaigns. Canada maintained a strong secondary position at around 5%, particularly for healthcare and industrial targets, while Europe led by Germany, France, and Italy captured 25% through repeated industrial and government hits. Asia and Latin America showed expanding exposure, with Thailand (11 TheGentlemen victims), Brazil (24 total), and Japan featuring in supply-chain attacks, signaling affiliate diversification beyond traditional North American/European strongholds.



Sectoral Exposure

Targeting exhibited strategic emphasis on sectors with acute downtime intolerance and high data/regulatory sensitivity, amplifying extortion effectiveness. Manufacturing/industrial supply chains topped exposure with sustained high volume from Qilin and LockBit, while healthcare surged dramatically (40 to 93 victims), reflecting attackers' exploitation of PII and service-criticality. Education and professional services faced persistent pressure due to public accountability and client data value, with construction/infrastructure emerging as a recurring mid-tier target.



Trends & Strategic Assessment

- **Escalating Victim Volume :** February marked a stable but elevated posting rate at 680 victims across 54 groups (slight drop from 58), with healthcare doubling to 93 incidents signalling attackers' sharpened focus on high-leverage sectors rather than raw volume expansion.

- **Dominance of High-Volume Actors :** Qilin (104, 15.3%) and TheGentlemen (78, 11.5%) commanded 27% of total victims, their scaling pipelines (TheGentlemen nearly doubling) highlighting industrialized RaaS enabling rapid affiliate growth.

- **Persistent Targeting of Critical Services:** Manufacturing, healthcare (surge to 93), and education endured disproportionate hits due to downtime costs, PII exposure, and regulatory fallout, with attackers improving double-extortion for maximum coercion.

- **Evolving Geopolitical Distribution:** U.S. primacy (49%) held, but countries hit rose to 72 (+20%), with Thailand/Brazil/Italy gaining prominence showing affiliates broadening footprints to evade saturation and law enforcement focus.

- **Fragmentation and Affiliate Overlap :** 54 active groups (down 7%) showed tooling overlap (VPN/RDP common), affiliate crossover fuelling TheGentlemen's doubling, and scam exposures (0APT's 183 fake claims) complicating attribution while sustaining ecosystem resilience.

Most Exploited Vulnerabilities of February 2026

Overview

February 2026 exploitation activity was defined by unprecedented sub-24-hour weaponization of remote support infrastructure, state-sponsored multi-year zero-day campaigns culminating in emergency government directives, and concentration of six Microsoft zero-days within a single Patch Tuesday cycle. The month was dominated by critical unauthenticated remote code execution flaws in privileged access management (BeyondTrust Remote Support), hardcoded credentials in disaster recovery systems (Dell RecoverPoint), and authentication bypass vulnerabilities in network infrastructure (Cisco Catalyst SD-WAN, Ivanti EPMM).

The Exploitation Landscape Highlights Three Dominant Vectors:

1. **Remote Support & Privileged Access Infrastructure Exploitation:** The BeyondTrust Remote Support/Privileged Remote Access platform became the month's most rapidly weaponized target, with unauthenticated RCE exploited within 24 hours of proof-of-concept release affecting approximately 8,500 internet-exposed instances. This was joined by Dell RecoverPoint hardcoded credential vulnerability (CVSS 10.0) representing an 18-month state-sponsored zero-day campaign, giving attackers root-level persistent backdoor access to enterprise disaster recovery and privileged session management infrastructure. Ransomware operators immediately incorporated BeyondTrust exploits into active campaigns, deploying VShell, SparkRAT, SimpleHelp, and AnyDesk for persistence and lateral movement across compromised environments**.**

2. **Network Appliance & Government Infrastructure Targeting:** Cisco Catalyst SD-WAN authentication bypass vulnerability prompted emergency CISA directive to federal agencies requiring patches by February 27, 2026, at 5:00PM Estimated time, reflecting active exploitation against government infrastructure. Attackers demonstrated sophisticated multi-stage methodology, chaining authentication bypass for initial access with deliberate firmware downgrade to reintroduce previously patched privilege escalation vulnerabilities for root access. Ivanti Endpoint Manager Mobile (Ivanti EPMM) bash script injection saw widespread automated exploitation with web shell, crypto miner, and persistent backdoor deployment, continuing patterns of network appliance targeting for perimeter compromise and persistent access establishment.

3. **Microsoft Zero-Day Concentration & Browser Runtime Exploitation**: Six actively exploited zero-days in Microsoft products within single Patch Tuesday cycle (Office, Word, Windows Shell, Desktop Window Manager, Remote Desktop Services) demonstrated persistent attacker investment in Windows exploitation frameworks. Chrome CSS use-after-free zero-day with 143 tracked sightings enabled arbitrary code execution inside sandbox via crafted HTML pages, requiring emergency browser update within 48 hours of discovery. The concentration of zero-day exploitation across document processing, shell operations, desktop windowing systems, and browser rendering engines indicates coordinated research efforts and pre-positioned exploitation capabilities across multiple platform subsystems.

Key Highlights

- **BeyondTrust Remote Support Sub-24-Hour Weaponization**: Critical unauthenticated RCE (CVSS 9.9) in BeyondTrust Remote Support/Privileged Remote Access exploited within 24 hours of public PoC release on February 10, affecting approximately 8,500 internet-exposed instances. CISA confirmed active use in ransomware campaigns deploying VShell, SparkRAT, SimpleHelp, and AnyDesk for persistence, demonstrating AI-enabled variant analysis accelerating PoC-to-operational-exploit timelines.

- **Dell RecoverPoint 18-Month State-Sponsored Campaign**: Maximum severity hardcoded credential vulnerability (CVSS 10.0) exploited by state-nexus threat actors since mid-2024, deploying BRICKSTORM, GRIMBOLT backdoors and SLAYSTYLE web shell for root-level persistent access to disaster recovery infrastructure. Added to CISA KEV February 18 with 3-day remediation deadline, representing longest zero-day exploitation window before disclosure in February disclosures.

- **Cisco SD-WAN Emergency Government Directive**: Critical authentication bypass vulnerability in Cisco Catalyst SD-WAN Controller and Manager exploited in the wild against government infrastructure, prompting CISA emergency directive requiring federal agency patches by February 27, 2026, at 5:00PM ET. Attackers demonstrated firmware downgrade methodology to re-enable historical privilege escalation vulnerabilities for root access, bypassing current patch status through version manipulation.

- **Microsoft Zero-Day Concentration**: Six actively exploited zero-days within single February Patch Tuesday (Office, Word, Windows Shell, Desktop Window Manager, Remote Desktop Services) with three publicly disclosed, addressing 54-59 total

CVEs. Concentration across document processing, shell operations, and desktop windowing systems indicates coordinated exploitation framework maintenance targeting Windows subsystems for privilege escalation to SYSTEM and security feature bypass.

- **Chrome CSS Zero-Day Emergency Response**: Use-after-free vulnerability in Chrome CSS component (CVSS 8.8) actively exploited in the wild as zero-day before patch availability, discovered and reported February 11 with emergency update released February 13. Tracked 143 sightings in February, enabling arbitrary code execution inside sandbox via crafted HTML pages.

- **Ivanti EPMM Widespread Automated Exploitation**: Critical RCE vulnerabilities (CVSS 9.8) in Ivanti Endpoint Manager Mobile allowing unauthenticated bash arithmetic expansion exploitation, added to CISA KEV catalog with observed widespread automated deployment of web shells, crypto miners, and persistent backdoors across vulnerable instances.

Top CVEs Actively Exploited

Enterprise Deserialization & Authentication Issues

- **CVE-2026-1731 (BeyondTrust Remote Support/Privileged Remote Access RCE)** - CVSS 9.9 ~ Critical pre-authentication remote code execution vulnerability allowing unauthenticated attackers to execute arbitrary OS commands via crafted WebSocket messages . Discovered January 31, patched February 2 for SaaS, exploited as zero-day starting February 10 within 24 hours of public PoC release. CISA confirmed active use in ransomware campaigns, with attackers deploying VShell, SparkRAT, SimpleHelp, and AnyDesk for persistence. Approximately 8,500 on-premises instances exposed to internet.

- **CVE-2026-22769 (Dell RecoverPoint for Virtual Machines Hardcoded Credentials)** - CVSS 10.0 ~ Maximum severity hardcoded credential vulnerability enabling unauthenticated remote attackers to gain root-level access and establish persistent backdoors. Exploited as zero-day by China-nexus threat actor UNC6201 since mid-2024, deploying BRICKSTORM, GRIMBOLT backdoors and SLAYSTYLE web shell.

- **CVE-2026-21514 (Microsoft Word Security Feature Bypass)** - CVSS 7.8 ~ Security feature bypass vulnerability in Microsoft Word requiring attackers to convince user to open crafted Office file, publicly disclosed and exploited as zero-day.

- **CVE-2026-21510 (Windows Shell Security Feature Bypass)** - CVSS 8.8 ~ Security feature bypass affecting Windows Shell, publicly disclosed and exploited in the wild as zero-day, allowing attackers to bypass SmartScreen and Shell warnings through malicious links or shortcut files.

Network Appliances & Gateways

- **CVE-2026-1281 & CVE-2026-1340 (Ivanti EPMM Bash Script Injection)** - CVSS 9.8 ~ Critical remote code execution vulnerabilities in Ivanti Endpoint Manager Mobile allowing unauthenticated attackers to remotely execute arbitrary code via bash arithmetic expansion exploitation in legacy Apache RewriteMap scripts. It observed widespread automated exploitation with web shell, crypto miner and persistent backdoor deployment.

- **CVE-2026-20127 (Cisco Catalyst SD-WAN Authentication Bypass)** - CVSS 10.0 ~ Critical authentication bypass vulnerability in Cisco Catalyst SD-WAN Controller and Manager exploited in the wild, allowing attackers to gain initial access then downgrade firmware to exploit *CVE-2022-20775* for privilege escalation to root.

- **CVE-2026-24300 (Azure Front Door Privilege Escalation)** - CVSS 9.8 ~ Critical elevation of privilege vulnerability affecting Azure Front Door allowing remote attackers with no privileges to elevate privileges through improper access control, proactively remediated by Microsoft within Azure infrastructure without customer intervention.

Browser & Runtime Exploits

- **CVE-2026-2441 (Google Chrome CSS Use-After-Free)** - CVSS 8.8 ~ High-severity use-after-free vulnerability in Chrome CSS component allowing remote attackers to execute arbitrary code inside sandbox via crafted HTML pages.

- **CVE-2026-21519 (Desktop Window Manager Privilege Escalation)** - CVSS 7.8 ~ Elevation of privilege vulnerability affecting Desktop Window Manager allowing local

authenticated attackers to elevate to SYSTEM privileges, exploited in the wild as zero-day.

- **CVE-2026-21513 (Microsoft Office Zero-Day)** – CVSS 8.8 ~ Zero-day vulnerability in Microsoft Office, Protection mechanism failure in MSHTML Framework allows an unauthorized attacker to bypass a security feature over a network.

- **CVE-2026-21533 (Windows Remote Desktop Services EoP)** - CVSS 7.8 ~ Elevation of privilege vulnerability affecting Windows Remote Desktop Services allowing local authenticated attackers to elevate to SYSTEM privileges, actively exploited in the wild with no user interaction required

Consumer IoT & Legacy Devices

- **CVE-2026-24061 (GNU InetUtils Telnetd Authentication Bypass)** - CVSS 9.8 ~ 11-year-old argument injection vulnerability in GNU InetUtils allowing authentication bypass and root access via Telnet.

- **CVE-2026-20700 (Apple OS Zero-Day)** - CVSS 7.8 ~ Apple macOS, iOS, iPadOS, tvOS, watchOS, and visionOS zero-day flaw weaponized to execute arbitrary code on susceptible devices

- **CVE-2026-20841 (Windows Notepad Remote Code Execution)** – CVSS 7.8 ~ Improper neutralization of special elements used in a command (command injection) in Windows Notepad App allows an unauthorized attacker to execute code locally.

Observations & Trends

- **Remote Support & Privileged Access Infrastructure Targeting**: Attackers heavily concentrated on remote access platforms like BeyondTrust Remote Support/Privileged Remote Access and Dell RecoverPoint for Virtual Machines. Compromising these systems provides extraordinary payoff, enabling unauthenticated remote code execution across approximately 8,500 internet-exposed instances, root-level persistent backdoor establishment, and administrative control over enterprise disaster recovery and privileged session management infrastructure managing credentials and remote access to critical systems.

- **Long-Duration Zero-Day Exploitation Campaigns**: The Dell RecoverPoint hardcoded credential vulnerability demonstrated state-sponsored threat actors' capability to maintain operational security during 18+ month zero-day exploitation campaigns before public disclosure. This persistent exploitation pattern, with ***deployment of BRICKSTORM and GRIMBOLT backdoors plus SLAYSTYLE web shell***, reveals sophisticated long-term access maintenance strategies where attackers prioritize stealth and persistence over rapid exploitation, indicating zero-day stockpiling and selective deployment against high-value targets.

- **PoC-Driven Weaponization Acceleration**: The BeyondTrust Remote Support vulnerability highlighted unprecedented weaponization speed, with exploitation beginning within 24 hours of public proof-of-concept release on February 10. Attackers demonstrated systematic capability to analyze PoC code, develop operational exploits, and deploy ransomware campaigns (VShell, SparkRAT, SimpleHelp, AnyDesk) faster than organizations could emergency-patch internet-exposed instances, compressing exploitation timelines to sub-24-hour windows.

- **Chaining and Firmware Downgrade as Standard Practice**: Attackers demonstrated sophisticated multi-stage exploitation methodology, with Cisco Catalyst SD-WAN campaigns chaining authentication bypass for initial access with deliberate firmware downgrade to reintroduce previously patched privilege escalation vulnerabilities for root access. This reflects advanced operational tradecraft where attackers deliberately regress system security posture to re-enable historical vulnerability exploitation, bypassing current patch status and creating persistent access through version manipulation.

- **Microsoft Zero-Day Concentration**: Six actively exploited zero-days in Microsoft products (Office, Word, Windows Shell, Desktop Window Manager, Remote Desktop Services) within single Patch Tuesday cycle demonstrates persistent attacker investment in Windows and Office exploitation frameworks. The concentration of zero-day exploitation across document processing, shell operations, and desktop windowing systems indicates coordinated research efforts and pre-positioned exploitation capabilities across multiple Windows subsystems.

Impact Profile

- **Severity:** Majority carried Critical (9.0-10.0) or High (7.8-8.8) severity ratings, with Dell RecoverPoint achieving maximum CVSS 10.0 for hardcoded credentials enabling root access, BeyondTrust scoring CVSS 9.9 for unauthenticated RCE, and Azure Front Door

reaching CVSS 9.8 for privilege escalation. These ratings associated with unauthenticated remote code execution, hardcoded credential exploitation, privilege escalation to SYSTEM/root, and authentication bypass across privileged access infrastructure.

- **Exploitation Outcomes Observed:**
    - **Initial access and administrative takeover** (BeyondTrust unauthenticated RCE affecting 8,500 exposed instances, Dell RecoverPoint hardcoded credentials providing root access, Cisco SD-WAN authentication bypass enabling firmware downgrade)
    - **Ransomware deployment** (BeyondTrust exploitation in active ransomware campaigns deploying VShell, SparkRAT, SimpleHelp, AnyDesk for persistence and lateral movement)
    - **Persistent backdoor establishment** (Dell RecoverPoint 18-month campaign deploying BRICKSTORM, GRIMBOLT backdoors and SLAYSTYLE web shell for long-term access)
    - **Privilege escalation to SYSTEM/root** (Desktop Window Manager and Remote Desktop Services elevation enabling SYSTEM privileges, Cisco SD-WAN firmware downgrade for root access, Azure Front Door privilege escalation)
    - **Credential and session management compromise** (BeyondTrust privileged remote access infrastructure managing enterprise credentials, Dell RecoverPoint disaster recovery systems)
    - **Web shell and crypto miner deployment** (Ivanti EPMM bash script injection exploitation with widespread automated deployment of web shells, crypto miners, and persistent backdoors)
    - **SmartScreen and security feature bypass** (Windows Shell security feature bypass enabling attackers to circumvent SmartScreen warnings via malicious links/shortcuts, Microsoft Word security feature bypass)
    - **Browser sandbox escape attempts** (Chrome CSS use-after-free enabling arbitrary code execution inside sandbox environment via crafted HTML pages)

- **Threat Type Balance:** Activity showed clear polarization between patient state-sponsored campaigns maintaining multi-year persistence (Dell RecoverPoint 18-month exploitation, Cisco SD-WAN prompting CISA emergency directive) and aggressive opportunistic weaponization occurring within 24 hours of PoC release (BeyondTrust affecting 8,500 instances, Ivanti EPMM automated exploitation, Chrome 143 sightings). The concentration of six Microsoft zero-days within single Patch Tuesday, combined with maximum CVSS 10.0 scores and unauthenticated RCE vectors, indicates defenders face simultaneous pressure from both strategic long-term intrusions and sub-24-hour exploitation timelines, with hardcoded credentials and authentication bypass fundamentally challenging traditional credential-based security models.

Distributed Denial-of-Service (DDoS) Activity of February 2026

Overview

February 2026 saw sustained hacktivist-driven DDoS campaigns globally, with pro-Russian group NoName057(16) prominently targeting high-profile events like the Milan-Cortina Winter Olympics and government infrastructure amid ongoing geopolitical tensions. In India, activity aligned with regional hacktivist patterns, focusing on public-facing government and critical services amid broader Asia-Pacific disruptions.

Key actors included NoName057(16) leveraging its DDoSia platform for coordinated volumetric and application-layer floods, alongside opportunistic regional groups amplifying claims via Telegram for propaganda effect. Targets span government entities, event infrastructure, and telecoms, where brief outages maximized media visibility.

Europe bore the brunt of named operations, but Asia-Pacific including India saw spillover from multi-nation campaigns. Technical impacts remained short-lived (minutes to hours), prioritizing psychological disruption over prolonged outages, often paired with defacements.

Key Threat Groups Observed

NoName057(16)

Remained the most prolific actor, launching DDoS attacks on Milan-Cortina 2026 Winter Olympics websites, hotels, and Italy's Foreign Ministry offices early February, using DDoSia (*Distributed Denial of Service [DDoS] attack toolkit*) for sustained pressure. The campaign aligned with pro-Russian opposition to Western-hosted events, extending prior NATO (North Atlantic Treaty Organization) / EU (European Union) targeting patterns.

Pro-Russian hacktivist clusters

Supported NoName057(16) in broader European operations, including Spanish government websites, emphasizing ideological disruption of public services.

Regional actors (India / APAC [Asia-Pacific] focus)

Unnamed multi-nation hacktivists contributed to 149 attacks hitting 110 organizations across 16 countries, with **India-facing claims on government portals and telecoms mirroring late-2025 patterns like THE GARUDA EYE/HellR00ters**.

Targeted Regions and Sectors

Regions most affected:

- **Europe:** Italy (Olympics infrastructure, Foreign Ministry), Spain (government sites), with spillover to UK/NATO allies.
- **Asia-Pacific (including India):** Part of 16-country hacktivist wave, targeting Indian government digital assets and telecoms amid regional tensions.
- **North America/International:** Opportunistic hits on event-related domains.

Sectors most frequently targeted:

- **Government and municipal services:** Ministries, Olympics organizing bodies, public portals (+41% historical NoName share).
- **Critical infrastructure:** Telecoms, event logistics (hotels/transport).
- **Private corporations:** Media/event platforms, Internet Service Provider (ISP).

Attack Characteristics

- **Types of Attacks:** Predominantly DDoSia-driven volumetric floods (TCP SYN/ACK, UDP) mixed with application-layer HTTP GET floods and Slow Loris (nginx_loris) variants exhausting web ports 80/443. Multi-vector waves hit clustered targets simultaneously.
- **Duration & Impact:** Short bursts (minutes-hours) causing service degradation; no prolonged outages reported, but Olympics/event disruptions amplified via claims.
- **Tactics & Infrastructure:** Volunteer-recruited botnets via Telegram/crypto incentives, rapid target rotation (daily waves), propaganda via social channels exaggerating "total collapse."

Threat Actor Motivation

Motivations mirrored hacktivist norms:

- **Political Alignment:** Pro-Russian backlash against Olympics/NATO (NoName057(16)), regional grudges in India/APAC.
- **Propaganda & Visibility:** Telegram claims project power, timed to events like Winter Games for global headlines.
- **Psychological Effect:** Erode trust in hosts (e.g., Italy's event security), coinciding with geopolitical flashpoints.

Key Takeaways

- **Event-tied targeting demands proactive surge capacity**: High-profile disruptions like Milan-Cortina Winter Olympics show hacktivists timing campaigns for maximum media amplification organizations hosting public events must pre-stage DDoS mitigation scaling and rapid incident communication to counter visibility-driven attacks.

- **Government portals remain prime targets globally and in India**: NoName057(16)'s focus on ministries/Foreign Offices (Italy, Spain) plus APAC/India spillover reinforces public sector as +41% priority, prioritize origin shielding, WAF tuning for HTTP/Slow Loris, and volumetric scrubbing on 80/443.

- **Hybrid DDoS + propaganda requires claim-driven response**: Telegram-amplified claims often exceed technical impact build monitoring for social channels + automated playbooks blending tech mitigation with public statements to neutralize psychological effects.

- **Regional India context demands telecom/gov hardening**: Amid 16-country hacktivist waves, sustain defences on public-facing services mirroring Dec-Jan patterns (THE GARUDA EYE-style actors) add rate limiting and connection controls for multi-vector L3/L4 + L7 floods.

- **Volunteer botnets evolve faster than isolated mitigations**: DDoSia's Telegram/crypto recruitment model enables rapid pivots adopt intel-sharing platforms (e.g., MISP) and AI anomaly detection to track campaign waves pre-emptively.

Cyber Incidents of February 2026

Overview

February 2026 was defined by resurgent ransomware campaigns targeting critical infrastructure and healthcare, massive Personally Identifiable Information (PII) exposures from national registries and telecom providers, and sophisticated state-sponsored telecom sector compromises demonstrating persistent strategic access. High-profile disruptions included Advantest Corporation's semiconductor operations in Japan and the University of Mississippi Medical Centre's clinic network shutdown, alongside France's FICOBA financial registry breach affecting 1.2 million accounts revealing attackers' dual focus on operational paralysis and mass identity theft at national scale.

In India, confirmed cyber incidents cantered on policy responses and strategic risk elevation rather than individual operational breaches. The India AI Impact Summit's high-alert status amid "Agentic AI" threats illustrated emerging risks to flagship technology events, signalling heightened national vigilance as AI-enhanced attacks accelerate targeting of digital transformation initiatives.

Globally, incidents at Odido (6M+ Dutch telecom customers exposed) and Singapore's four major telcos (compromised by Chinese nexus UNC3886 via zero-days) highlighted telecommunications as the ultimate force-multiplier for both financial crime and intelligence operations. These events underscore a maturing attacker calculus where sustained, undetected access to carrier infrastructure enables downstream targeting of entire economies rather than isolated organizations.

India Incidents

- **India AI Impact Summit 2026 placed on high cyber alert (New Delhi) -** India's cybersecurity agencies issued high-alert warnings during the India AI Impact Summit 2026 (Feb 16-17) at Bharat Mandapam, New Delhi, amid threats from advanced "Agentic AI" autonomous hacking systems. The event featuring global tech leaders like Jensen Huang (NVIDIA), Sam Altman (OpenAI), and Sundar Pichai (Google) triggered massive security operations to protect critical digital infrastructure. This incident highlights emerging risks to high-profile national tech gatherings from AI-powered threat actors.

Global Incidents

- **Advantest Corporation ransomware attack (Japan)** - Japanese semiconductor testing equipment maker Advantest Corporation confirmed unauthorized access by a third party on February 15, leading to ransomware deployment across portions of its network. The company reported potential impacts on internal systems while customer and employee data exposure remains under investigation. This incident highlights ongoing industrial sector targeting by ransomware operations seeking both operational disruption and data extortion.

- **University of Mississippi Medical Center ransomware disruption (US)** - The academic healthcare system suffered a ransomware attack forcing clinic network closures and electronic medical record access disruptions across Mississippi. Elective procedures were canceled and operations shifted to manual processes as systems were taken offline, with no ransomware group publicly claiming responsibility. The event demonstrates healthcare's continued vulnerability to ransomware despite extensive regulatory focus and sector-specific guidance.

- **Odido telecom breach exposing 6+ million customer records (Netherlands)** -Dutch telecom provider Odido confirmed a cyberattack first detected on February 7, resulting in unauthorized access exposing personal data from over six million customer accounts. Stolen information included names, phone numbers, email addresses, bank account numbers, and passport numbers before access was terminated. The breach underscores telecom sector exposure to mass Personally Identifiable Information (PII) theft enabling downstream fraud campaigns.

- **Singapore telecom sector coordinated compromise (Chinese nexus UNC3886)** - Singapore's Cyber Security Agency disclosed that Chinese-linked group UNC3886 had compromised all four major telecom providers (Singtel, StarHub, M1, Simba) using zero-day exploits and rootkits. Attackers maintained persistent hidden access for nearly a year, enabling strategic intelligence collection rather than immediate disruption. This state-sponsored operation represents peak telecom sector risk where network dominance provides downstream targeting of all dependent digital services.

Global Data Breach Activity of February 2026

Overview

February 2026 was dominated by ShinyHunters' systematic vishing campaign exploiting single sign-on vulnerabilities across major corporations, resulting in massive data exposures at Panera Bread (5.1 million customers), CarGurus (12.4 million accounts), Match Group (10+ million records), and Figure (1 million users).

The month revealed the catastrophic scale of the Conduent Business Services breach, escalating from initial estimates to over 25 million victims across 30+ states, making it the eighth-largest healthcare breach in U.S. history and triggering Texas Attorney General investigation. Social engineering attacks replaced technical exploits as the primary threat vector, with attackers impersonating IT staff through voice phishing to obtain legitimate credentials and bypass multifactor authentication at organizations including Choice Hotels and Optimizely. International incidents included France's FICOBA national bank registry breach exposing 1.2 million accounts through compromised civil servant credentials, while third-party compromises at TriZetto (3.4 million), ManoMano (38 million), and multiple financial service providers demonstrated continued supply chain vulnerabilities.

February disclosures revealed persistent delayed breach notifications spanning over a year between discovery and victim notification while ransomware groups including Genesis, Interlock, Qilin, and INC maintained sustained attacks across healthcare, legal services, and critical infrastructure sectors.

Major Data Breaches

1. Panera Bread Data Breach

- **Threat Actor:** ShinyHunters extortion group
- **Vulnerability:** Microsoft Entra Single Sign-On (SSO) compromise through vishing (voice phishing) attack
- **Estimated Victims:** 5.1 million unique customers
- **Timeline / Discovery Date:**
  - **Breach occurred**: Late December 2025 - January 2026

- **Data leaked**: Late January/Early February 2026 (760MB archive)
- **Public disclosure:** February 3-6, 2026

- **Description:** ShinyHunters targeted Panera Bread's identity infrastructure by impersonating IT staff and convincing employees to enter their credentials into a phishing site, capturing valid login information and session tokens to access customer data repositories. This was Panera's second major breach in two years following a 2024 incident affecting 150,000 employees.

- **Attack Methodology:** ShinyHunters called employees at Panera, impersonated IT support or Microsoft staff, and talked them into revealing multi-factor authentication codes or SSO credentials through voice phishing. The attackers used custom real-time phishing kits capable of capturing credentials and session tokens during vishing calls.

- **Confirmed Major Victims:** Panera Bread customers across the United States

- **Claimed Victims Include:** ShinyHunters initially claimed 14 million customer records, but analysis confirmed 5.1 million unique email addresses.

- **Response Measures:** Panera CEO Paul Carbone confirmed a social engineering incident resulted in unauthorized access to a third-party SaaS application, and the company engaged independent security experts who quickly identified the cause and strengthened controls. When extortion attempts failed, ShinyHunters released a 760-megabyte archive containing millions of customer records on its leak site. At least seven class action lawsuits were filed in federal court by late February.

- **Potential Impact:** Exposed data includes names, email addresses, phone numbers, physical addresses, and account-related information. While payment information was not included, the exposed data creates heightened risks for phishing, identity theft, and targeted social-engineering scams.

2. Conduent Business Services Data Breach

- **Threat Actor:** SafePay ransomware gang

- **Vulnerability:** Unauthorized network access enabling three-month sustained intrusion

- **Estimated Victims:** Over 25 million individuals (initially reported as 10.5 million, revised upward through February 2026)

- **Timeline / Discovery Date:**
    - **Breach began:** October 21, 2024
    - **Breach discovered:** January 13, 2025
    - **SafePay claim:** February 2025
    - **Victims count escalation:** October 2025 - February 2026
    - **Texas AG (Attorney General) investigation launched:** February 2026

- **Description:** Conduent sits behind the scenes of a major portion of US public services and corporate back-office work, handling state benefit programs such as Medicaid, SNAP, and other government payment disbursements in more than 30 states. What initially appeared to affect approximately 4 million people in October 2025 has ballooned into one of the largest healthcare data breaches in U.S. history, ranking as the eighth largest on record.

- **Methodology:** Investigations confirm that unauthorized actors-maintained access to Conduent's network between October 21, 2024, and January 13, 2025, during which SafePay ransomware group systematically exfiltrated 8 terabytes of files before the intrusion was discovered.

- **Confirmed Major Victims:** Affected parties include Blue Cross Blue Shield plans, Volvo Group North America (17,000 employees), state benefit recipients in Texas (15.4 million), Oregon (10.5 million), and hundreds of thousands across Delaware, Massachusetts, and New Hampshire.

- **Claimed Victims Include:** SafePay boasted of exfiltrating 8.5 terabytes of sensitive data including names, Social Security numbers, addresses, medical histories, and health insurance details.

- **Response Measures:** Texas Attorney General Ken Paxton launched an investigation in February 2026, calling it potentially the largest U.S. healthcare breach ever. At least 10 federal class action lawsuits have been filed and consolidated in U.S. District

Court for the District of New Jersey. Conduent reported approximately $25 million in non-recurring costs related to the response and notifications.

- **Potential Impact:** The stolen data includes full legal names, postal addresses, dates of birth, Social Security numbers, and medical information, health insurance details, and related claims data. These "forever identifiers" cannot be swapped out, leaving victims vulnerable to exploitation for decades, particularly for filing fraudulent insurance claims or obtaining expensive prescription drugs.

3. CarGurus Data Breach

- **Threat Actor:** ShinyHunters extortion group
- **Vulnerability:** Voice phishing (vishing) attack targeting SSO (Single sign-on) credentials
- **Estimated Victims:** 12.4 - 12.5 million user accounts
- **Timeline / Discovery Date:**
  - **Breach occurred:** February 13, 2026
  - **ShinyHunters listing:** February 21, 2026 (initially claimed 1.7 million records)
  - **Data leaked:** February 21, 2026 (6.1GB archive)
  - **Have I Been Pwned confirmation:** February 22, 2026
  - **Public disclosure:** February 24, 2026
  - **Class action lawsuits filed:** Late February 2026
- **Description:** CarGurus is a publicly traded automotive research and shopping company operating in the U.S., Canada, and the U.K., with an estimated 40 million monthly visitors. The incident was disclosed when ShinyHunters added CarGurus to its Tor-based leak site, claiming theft of personally identifiable information and internal corporate data.
- **Attack Methodology:** According to ShinyHunters, the breach occurred on February 13 and was part of a broader code-stealing spree in which they used voice phishing to obtain single-sign-on codes from users of Okta, Microsoft, and Google services.

The attack was executed through vishing, whereby threat actors placed fraudulent telephone calls impersonating trusted entities to obtain access credentials.

- **Confirmed Major Victims:** CarGurus users across United States, Canada, and United Kingdom

- **Claimed Victims Include:** Initially hackers claimed 1.7 million records but subsequently leaked a 6.1GB archive containing information pertaining to approximately 12.5 million accounts.

- **Response Measures:** CarGurus confirmed to media it experienced a cybersecurity incident and stated, "we recently experienced a cybersecurity incident; we quickly secured the impacted environment and engaged an independent cybersecurity firm to conduct a forensic investigation". CarGurus was hit with a flurry of lawsuits in late February 2026 over the data breach.

- **Potential Impact:** Impacted data includes names, phone numbers, physical and IP addresses, email addresses, user account ID mappings, finance pre-qualification application data, dealer account and subscription information, and auto finance application outcomes. The exposed data increases risks of phishing, social engineering attacks, identity theft, financial fraud, and account takeovers.

4. FICOBA (French National Bank Registry) Data Breach

- **Threat Actor:** Unknown malicious actor (impersonated government official)

- **Vulnerability:** Compromised civil servant credentials providing access to interministerial information sharing platform

- **Estimated Victims:** 1.2 million bank accounts (from database containing 300 million accounts for 80 million individuals)

- **Timeline / Discovery Date:**

  - **Breach began:** Late January 2026

  - **Breach detected**: Mid-February 2026

  - **Public disclosure**: February 18-19, 2026
  - **Victim notifications**: February 2026

- **Description:** The French Ministry of Finance disclosed a cybersecurity incident impacting data associated with 1.2 million user accounts after hackers gained access to the national bank account registry (FICOBA) and stole a database containing sensitive information. FICOBA is maintained by the French revenue service, the Direction Générale des Finances Publiques (DGFiP), and all financial institutions across the country are required to submit their customers' banking and personal information to comply with France's tax laws.

- **Attack Methodology**: A threat actor used credentials stolen from a civil servant with access to the interministerial information sharing platform to gain access to part of a database containing all bank accounts opened in French banking institutions. This wasn't a vulnerability exploit—it was authentication, as the system believed the compromised credentials were legitimate.

- **Confirmed Major Victims**: Approximately 1.2 million French bank account holders

- **Response Measures:** The Ministry stated the attacker's access has been terminated and impacted individuals are being notified. The French Data Protection Authority (CNIL) was notified, and cybersecurity teams from the finance ministry and France's national cybersecurity agency ANSSI are assisting with the investigation. The French Banking Federation urged customers to monitor their accounts closely for suspicious direct debit activity.

- **Potential Impact:** Compromised data includes bank account details including RIBs/IBANs, account holder identity, physical address, and in some cases taxpayer identification number. While the exposed data does not grant direct access to bank accounts, the detailed financial and personal information enables business email compromise attacks and highly convincing spear phishing campaigns. Criminals can use IBANs (International Bank Account Number) to set up fraudulent direct debit mandates

Additional February 2026 Breach Disclosures.

Healthcare Sector:

- **Cognizant TriZetto** – 3,433,965 individuals affected; healthcare cost management solutions provider breach discovered in 2024, customer notifications began February 2026, exposed data includes names, addresses, dates of birth, Social Security numbers, financial account information, driver's license/state ID numbers, health insurance information, and medical treatment details
- **BlueCross BlueShield of Tennessee** – 1,670 members affected through Conduent Business Services breach part of the larger 25+ million victim Conduent incident
- **Community Health Action of Staten Island** – Genesis ransomware attack, exposed names, Social Security numbers, driver's license numbers, bank account and routing numbers, medical information, and health insurance information; notifications sent February 25, 2026
- **Emanuel Medical Center (California)** – May 2025 security incident notifications sent in February 2026, unauthorized network access with files containing personal and protected health information exposed
- **San Diego Eye Bank** – Data breach affecting sight restoration services provider disclosed February 2026

Financial Services:

- **Figure (Fintech)** – Approximately 1 million customers affected; ShinyHunters group breach; exposed names, dates of birth, physical addresses, phone numbers, and email addresses; no financial account numbers or Social Security numbers compromised
- **PayPal** – Software error in loan application exposed customer information including Social Security numbers for nearly 6 months in 2025; disclosed February 2026
- **Beacon Pointe** – February 20, 2026, Massachusetts notification; three residents affected with Social Security numbers, financial accounts, and driver's license numbers compromised; ShinyHunters claimed 100,000+ records stolen

- **MV Financial Group** – February 12, 2026, notification;33 Massachusetts residents affected with Social Security numbers, financial accounts, and driver's license numbers exposed
- **Strategic Investment Solutions** – February 12, 2026, notification; 12 Massachusetts residents with Social Security numbers and financial accounts compromised
- **Purus Wealth Management** – February 5, 2026, notification; two Massachusetts residents with financial accounts accessed
- **Mercer** – ShinyHunters group claimed theft of 5 million records: extortion deadline set for February 18, 2026
- **Abu Dhabi Finance Week (ADFW)** – 700 passports and identification cards exposed in unprotected cloud server. global leaders and executives affected including Anthony Scaramucci

Education:

- Education sector continued facing high attack volume with 60-70% of cybersecurity incidents involving compromised credentials.
- 40% of cyber insurance claims in education denied due to incomplete Multi-Factor Authentication (MFA) deployment.
- Multiple K-12 schools and universities targeted by AI-enhanced phishing campaigns impersonating HR and payroll teams

Retail & E-Commerce:

- **ManoMano (France)** – 38 million customers affected by DIY e-commerce chain breach; third-party service provider compromise; exposed full names, email addresses, phone numbers, and customer service communications

Technology & Telecommunications:

- **Optimizely (Ad Tech)** – New York-based company serving 10,000+ businesses including H&M, PayPal, Toyota, Vodafone, Shell, Salesforce, and Nike; vishing attack compromised systems; undisclosed number of customers notified

- **Substack** – February 3, 2026, discovery of unauthorized access; subscriber contact details exposed including phone numbers and email addresses; no passwords, payment cards, or financial records confirmed exposed

- **Flickr** – Third-party provider breach compromised member data including usernames, IP addresses, location data, account types, and Flickr activity; notifications sent February 2026

- **RTL Group** – February 2026 investigation of claims that intranet was breached exposing 27,000+ employee records; sample showed names, work emails, job details, office addresses, work and personal phone numbers; customer data unlikely impacted

Aviation:

- **Japan Airlines** – February 9, 2026, discovery of unauthorized access; customers who used service since July 2024 affected; exposed names, phone numbers, email addresses, departure/arrival airports, hotel names, and flight numbers.

Energy:

- **Conpet (Romania)** – National oil pipeline operator targeted by Qilin ransomware; over 1TB of information compromised including sensitive internal documents, passports, and financial information

Legal Services:

- **Eisenberg Lowrance Lundell Lofgren (Utah)** – INC ransomware group attack; exposed client personal information including government-issued IDs and case-related information

Hospitality:

- **Wynn Resorts** – Attackers claimed theft of PII including Social Security numbers and employee data for over 800,000 records; company has not confirmed details

Government & Other:

- **Volvo Group North America** – February 10, 2026, indirect breach disclosure; approximately 17,000 people affected through Conduent Business Services breach; exposed names, Social Security numbers, dates of birth, health insurance policy details, ID numbers, and medical information

Strategic Assessment

February 2026 breaches collectively illustrate several critical trends in the cyber threat landscape:

1. Supply Chain as Primary Attack Vector: Third-party compromises dominated February disclosures. Cognizant TriZetto's breach affecting 3.4 million individuals occurred through provider systems serving multiple healthcare clients. Volvo Group North America's 17,000 affected individuals resulted from Conduent breach discovered months earlier. ManoMano's 38 million customer exposure stemmed from compromised third-party service provider access. Flickr's breach occurred through a third-party provider affecting member data across the platform. The Conduent incident demonstrates cascading failures at scale. Organizations inherit every vendor's security weakness. Supply chain attacks create concentrated risk affecting hundreds of downstream clients simultaneously.

2. Zero-Day Exploitation at Scale: Voice phishing replaced technical exploits as primary attack vector. ShinyHunters used vishing to obtain SSO codes from users of Okta, Microsoft, and Google services, targeting Panera, CarGurus, and Match Group. Optimizely confirmed breach after threat actors compromised systems through voice phishing attack. Attackers exploit human trust over technical vulnerabilities. Legitimate credentials bypass all technical controls. Organizations cannot patch human decision-making under pressure.

3. Social Engineering Sophistication: Panera attackers impersonated IT staff and convinced employees to enter credentials into phishing sites, capturing valid login information and session tokens. Choice Hotels experienced social engineering attack on January 14, 2026, despite multifactor authentication being in place. AI dramatically increased scale and realism of social engineering attacks with threat actors using AI to automate reconnaissance and generate highly convincing communications. Real-time phishing kits capture credentials and session tokens during vishing calls. MFA provides false security when attackers obtain tokens directly from users. Adversaries exploit urgency and authority to bypass technical safeguards.

4. Cross-Sector Impact: Financial services experienced systematic targeting. Multiple RIAs including Edelman Financial Engines, Beacon Pointe, MV Financial Group, Strategic Investment Solutions, and Purus Wealth Management filed Massachusetts breach notifications in February. Figure's blockchain-based fintech breach affected approximately 1 million customers, demonstrating that even blockchain-native companies must secure entire technology stacks. Healthcare saw delayed disclosures. TriZetto discovered breach in December 2024, but customer notifications began only in February 2026. Healthcare

remained most targeted sector with 27 ransomware incidents in January 2026, followed by government with 11 and manufacturing with 10. No sector remains immune from credential-based attacks.

5. Underground Marketplace Activity: ShinyHunters dominated February extortion landscape. The group targeted Panera (5.1 million records), CarGurus (12.4 million records), Figure (1 million records), Match Group (10+ million records), and Mercer (5 million records). When Panera extortion attempts failed, ShinyHunters released 760MB archive containing millions of customer records. ShinyHunters set February 18, 2026, deadline for Mercer with warning "don't be the next headline". ***Multiple ransomware groups remained active: Qilin (Conpet), Genesis (Community Health Action), Interlock (Apex Spine), Incransom (Hawk Law Group), INC (Eisenberg Lowrance).*** Extortion follows predictable patterns with public deadline pressure and phased data release. Groups operate as professional services with established leak sites and communication protocols.

Key Takeaways

- **Vishing is the new malware**: ShinyHunters systematically exploited voice phishing to obtain SSO credentials from multiple Fortune 500 companies.
- **MFA is not enough**: Choice Hotels breach occurred despite multifactor authentication when social engineering convinced employees to provide access.
- **Delayed disclosure extends victim exposure**: TriZetto's December 2024 breach wasn't disclosed to 3.4 million individuals until February 2026.
- **Supply chain breaches cascade across sectors**: Conduent's single breach exposed over 25 million individuals across healthcare, automotive, and government clients
- **Credential theft targets all sectors**: Financial services faced systematic RIA targeting while healthcare, retail, and technology all experienced credential-based compromises
- **AI accelerates social engineering**: 60-70% of cybersecurity incidents now involve compromised credentials with AI-enhanced phishing bypassing traditional filters.
- **Blockchain doesn't equal security**: Figure's blockchain infrastructure didn't protect traditional databases where customer information was stored.
- **Third-party access creates concentrated risk**: ManoMano, Flickr, and TriZetto breaches all originated from compromised service providers
- **Extortion groups operate transparently**: ShinyHunters publicly lists victims, sets deadlines, and releases data on predictable schedules when ransom demands fail

- **Insurance denials force security improvements**: 40% of education sector cyber insurance claims denied due to incomplete MFA deployment.
- **Detection gaps enable sustained access**: FICOBA breach occurred over weeks before detection; healthcare breaches averaged 4-month discovery delays
- **Session token theft bypasses passwords**: Modern attacks capture live session credentials rather than stealing static passwords requiring separate authentication

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