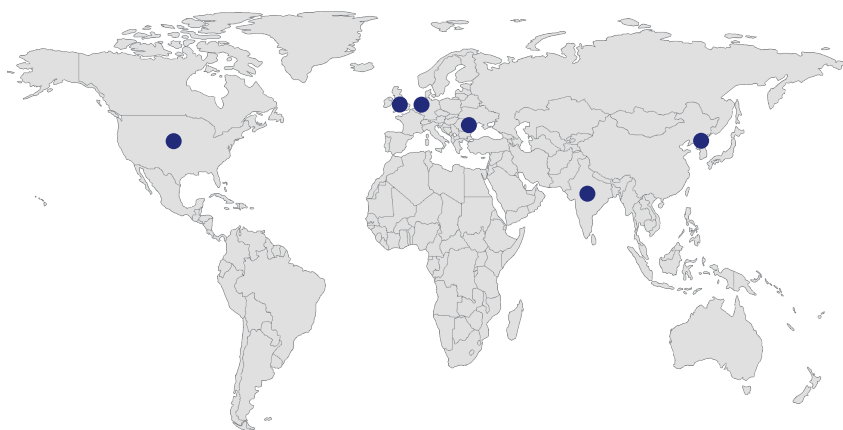


IMPERVA THREAT RESEARCH

# Threat Intel Report: February 9-22, 2026

## Countries



## Top Tags

---

Lazarus Group

---

OpenClaw

---

Global Group

---

SafePay

---

Qilin

## Executive Summary

### Actionable Information:

- **Attackers are prioritizing stealth, persistence, and low-dependency execution.** Offline-capable ransomware (Phorpiex/Global Group), botnets like Prometei, and infostealers targeting AI agent configs all reduce reliance on live C2 infrastructure, allowing attacks to succeed even in segmented or monitored environments. This increases dwell time and complicates detection and response.
- **Identity, credentials, and authentication workflows are the primary battleground.** From SMS/OTP bombing and mobile RATs harvesting MFA codes to infostealers targeting AI agent tokens and supply-chain malware stealing developer credentials, attackers are consistently bypassing traditional perimeter controls by abusing identity and trust relationships.
- **Third-party and supply-chain exposure remains a dominant breach driver.** The Conduent breach impacting Volvo employees and Lazarus's abuse of npm/PyPI demonstrate how attackers increasingly compromise upstream providers and ecosystems to achieve scale, often with delayed detection and downstream victims learning of exposure months later.
- **Critical services and financial infrastructure face increasing disruption risk.** ATM jackpotting campaigns, payment processor ransomware (BridgePay), and ransomware against energy infrastructure (Conpet) show attackers targeting systems where availability and operational continuity are as damaging as data loss.
- **Automation is accelerating abuse at scale.** SMS/OTP bombing has evolved from nuisance attacks into API-driven, automated exploitation capable of inducing MFA fatigue, service degradation, and account takeover across telecom, financial, and government platforms.

## Outlook:

The threat landscape continues to shift toward quiet, scalable, and trust-abusing attacks rather than noisy exploits or single-point intrusions. Expect further growth in malware that operates offline or blends into legitimate tooling, deeper targeting of identity systems (MFA, tokens, AI agents), and increased use of third-party compromise to reach large victim populations with minimal effort. As attackers increasingly monetize disruption and access, rather than just data theft, organizations should expect more incidents where availability, operational continuity, and downstream liability are the primary impacts—particularly in financial services, energy, healthcare, and telecom.

---

## Threat Activity in Imperva

### Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 2,971% [CVE-2026-22610](#)

- Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to versions 19.2.18, 20.3.16, 21.0.7, and 21.1.0-rc.0, a cross-site scripting (XSS) vulnerability has been identified in the Angular Template Compiler. The vulnerability exists because Angular's internal sanitization schema fails to recognize the href and xlink:href attributes of SVG <script> elements as a Resource URL context.

↑ 1,092% [CVE-2025-40598](#)

- A Reflected cross-site scripting (XSS) vulnerability exists in the SMA100 series web interface, allowing a remote unauthenticated attacker to potentially execute arbitrary JavaScript code.

↑ 1035% [CVE-2025-54309](#)

- CrushFTP 10 before 10.8.5 and 11 before 11.3.4\_23, when the DMZ proxy feature is not used, mishandles AS2 validation and consequently allows remote attackers to obtain admin access via HTTPS, as exploited in the wild in July 2025.

---

## Recent Cyber Threats

### Offline Ransomware Hitchhikes via Phorpiex Phishing

+Global Group

- Researchers have identified a [low-noise phishing campaign](#) using deceptive .LNK shortcut files that, when opened, trigger PowerShell to deploy Global Group ransomware locally. This ransomware variant can operate offline, encrypting victim machines without reaching out to its C2 infrastructure, and deletes backups/evidence after encryption. The method highlights that even basic phishing attachments continue to be effective vectors for serious ransomware impacts across industries.

### ZeroDayRAT Mobile Spyware Gives Full Remote Control

+ZeroDayRAT +Android +iOS

- A new cross-platform Remote Access Trojan ([ZeroDayRAT](#)) is being sold on underground forums and Telegram, offering attackers full remote control of both Android and iOS devices once installed. Capabilities include intercepting communications, stealing credentials and SMS/2FA codes, tracking location, and even accessing camera/microphone streams. Its commercialization and ease of spread (via phishing links, fake apps, smishing) lower the barrier for mobile espionage and fraud, making mobiles as risky an endpoint as PCs.

### Lazarus Exploits npm & PyPI in Fake Recruiter Supply Chain Attack

+North Korea +Lazarus Group +npm +PyPI

- Security researchers uncovered malicious npm and PyPI packages tied to a [fake recruitment campaign](#) attributed to the North Korea-linked Lazarus APT. The operation, active since mid-2025, uses fake job interview tasks and recruiter outreach to lure developers into installing tainted packages that drop malware. This technique blends social engineering with software supply chain compromise, targeting developers and potentially any organizations using infected packages.

## Infostealer Targets OpenClaw AI Agent Secrets

+OpenClaw +Infostealer +Malware +AI

- For the first time, live infections show infostealer malware targeting [OpenClaw](#) AI assistant configuration files, exfiltrating API keys, authentication tokens and persistent memory artifacts. Researchers warn that as AI agents store sensitive credentials and integration tokens, malware targeting these environments could compromise broader linked services. This marks an evolution from typical credential theft to harvesting AI agent identities and capabilities.

## Malware-Driven ATM Jackpotting Surges, Millions Stolen

+ATM Jackpotting +Financial Services +Ploutus

- The FBI warns that [ATM jackpotting](#), a cyber-physical attack where malware forces ATMs to dispense cash without customer authorization, has surged, with over 700 incidents in 2025 resulting in >\$20 M in stolen cash. Attackers exploit both physical access (generic keys) and malware like Ploutus to bypass bank systems and directly command cash dispensers. The trend underscores the growing threat at the intersection of physical security and malware compromise.

## SMS & OTP Bombing Abuse Matures Into Automated API Exploits

+SMS-bombing +OTP-bombing +API

- Research into [SMS- and OTP-bombing](#) tactics shows a shift from manual scripts to coordinated, automated tooling exploiting vulnerable API endpoints across sectors like telecommunications, financial services and government portals. Attacks repeatedly trigger one-time password requests, overwhelming services, incurring costs and creating MFA fatigue that may lead to account takeover. Techniques include API automation, SSL bypass, and voice-bombing, reflecting the maturation of this vector beyond nuisance spam.

---

## Data Breaches

### Prometei Botnet Squats on UK Construction Server

+Prometei +UK

- In January 2026, a UK construction firm's Windows Server was found compromised by the long-running [Prometei](#) botnet after weak or default RDP credentials were abused to gain access. Once inside, Prometei installed persistent components, routed command traffic through TOR, mined Monero, and used tools like Mimikatz to harvest passwords across the network. The malware even blocked other attackers to maintain exclusive control and evaded analysis with sandbox-bait behavior.

### BridgePay Ransomware Halts Payments Nationwide

+Financial Services

- U.S. payment gateway [BridgePay Network Solutions](#) confirmed a ransomware attack on February 6, 2026, that knocked its core transactional systems offline, leading to a nationwide outage affecting merchant card processing. Forensic findings reported that files were encrypted but there is no current evidence of payment card data loss, and federal authorities (FBI, Secret Service) are involved in the investigation. Dependent services including APIs, virtual terminals, and hosted payment pages were disrupted, forcing some businesses to revert to cash-only operations.

### Third-Party Breach at Conduent Exposes Volvo Employee Data

+Automotive +Safepay

- A large-scale cyberattack against business services provider [Conduent](#) exposed personal data belonging to nearly 17,000 Volvo Group North America employees, as part of a breach now impacting at least 25 million individuals across multiple U.S. states. Attackers accessed Conduent's network between October 2024 and January 2025, stealing highly sensitive data including names, addresses, dates of birth, Social Security numbers, and health and insurance information. The Safepay ransomware group claimed responsibility for the attack in February 2025, which also caused service outages affecting state payment and customer

support systems. Volvo was not directly breached and stated it only became aware of the incident in January 2026, highlighting prolonged detection delays and systemic third-party risk exposure.

## Romania's National Oil Pipeline Operator Confirms Data Theft

+Romania +Qilin +Energy

- Romania's national oil pipeline company [Conpet](#) disclosed it suffered a cyberattack in which the Qilin ransomware gang stole company data and likely exfiltrated files. The company confirmed that sensitive information was taken during the incident, which also disrupted business systems. This adds to increasing ransomware activity against energy infrastructure in Europe.

## Odido Breach Exposes Personal Info of 62M Users

+Netherlands +Telecommunications

- Dutch mobile operator [Odido](#) suffered a data breach affecting roughly 62 million customers, exposing personal information such as names, addresses, and potentially ID numbers and contact details. The incident raised concerns about data protection practices within large telecom operators and has potential privacy implications for users across its markets.

## DavaIndia Pharmacy Flaw Allowed Customer Data Access

+India +Healthcare

- A security flaw at [DavaIndia's](#) online pharmacy platform permitted attackers to access customer data and potentially more internal records, due to improper access controls and application design weaknesses. Exploiters could harvest personal information and order histories, highlighting risks in e-commerce healthcare systems that handle sensitive customer details.

---

## Imperva Protection

Imperva provides comprehensive digital security solutions, including protection against threats to web applications and APIs— including security vulnerabilities, fraud, and bad bots, data security solutions, and security against disruptive network- and application-level DDoS attacks.