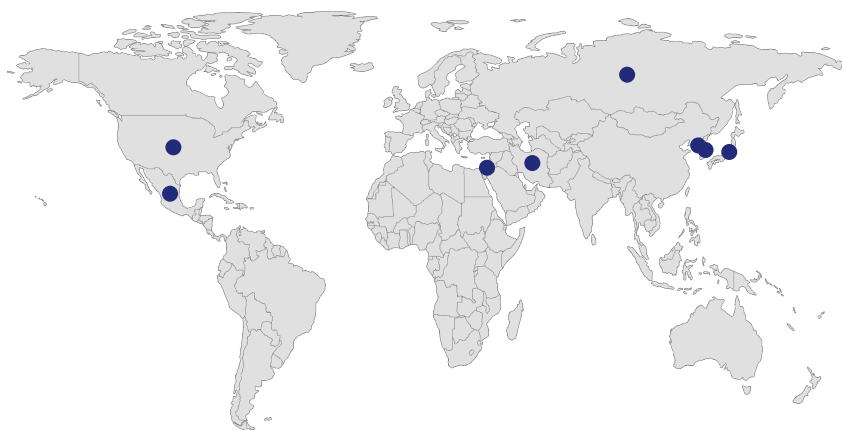


IMPERVA THREAT RESEARCH

Threat Intel Report: February 23-March 1, 2026

Countries



Top Tags

Operation MacroMaze

APT28

Ruby Jumper

APT37

Handala

Executive Summary

Actionable Information:

- **AI-Assisted Attack Development:** Multiple incidents this week (notably the Mexican government breach) demonstrate adversaries leveraging generative AI not merely for phishing or social engineering, but as an active tool to craft exploit code, automate tooling workflows, and scale operational activities. This elevates the baseline skill set required to defend effectively: defenders must anticipate AI-augmented tactics when modeling threat behavior and hardening environments.
- **Data Breaches Targeting Consumer & Health Data at Scale:** The Conduent incident, impacting over 25 million U.S. residents' health and personally identifiable information, combined with the Coupang breach affecting tens of millions in South Korea, highlights persistent systemic weaknesses in large data aggregators and service providers. Attack surface and downstream exposure are amplified when backend processors manage sensitive records for state, healthcare, or e-commerce systems; risk assessments should prioritize these high-impact supply chain tiers.
- **Ransomware & Supply Chain Risks Persist:** The ransomware attack on Advantest, a key supplier in the semiconductor ecosystem, underscores that manufacturing and technology supply chains remain a high-value target for disruptive extortion operations. While attribution remains unclear in that case, the trend of targeting high-value industrial suppliers continues. Concurrently, software supply chain abuse through malicious AI "skills" distributing MacOS stealers indicates adversaries will blend traditional supply chain weaknesses with platform-specific automation techniques.
- **Internal Security Hygiene & Competitive Fallout:** The Coupang breach has not only operational security implications but also competitive and regulatory effects, as scrutiny intensifies over internal safeguards and breach response transparency. This exemplifies the reputational and market risks of inadequate internal controls, especially when breaches are attributed to preventable internal management lapses as opposed to advanced external actors.

Outlook:

The current landscape exhibits a convergence of AI-augmented offensive capabilities with enduring challenges in data protection and supply chain security. Attackers are increasingly operationalizing automation, whether by training AI to generate or adapt exploit code or by embedding malicious logic into tool workflows, which can shorten campaign development cycles and expand scale. Meanwhile, defenders are facing not only technical risks but also amplified business impacts as breaches of large data custodians ripple into regulatory and market pressures. Looking ahead, we should expect a rise in hybrid threat campaigns that blend AI tactics, supply chain abuse, and data exfiltration at scale. Organizations must evolve defenses to include adversarial AI awareness, prioritize secure software and service dependencies, and strengthen governance controls over high-impact data holdings to mitigate both technical and strategic risk.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

 574% [CVE-2025-66039](#)

- FreePBX Endpoint Manager is a module for managing telephony endpoints in FreePBX systems. Versions are vulnerable to authentication bypass when the authentication type is set to "webserver." When providing an Authorization header with an arbitrary value, a session is associated with the target user regardless of valid credentials.

 171% [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.

 135% [CVE-2025-53772](#)

- Deserialization of untrusted data in Web Deploy allows an authorized attacker to execute code over a network.

Recent Cyber Threats

Cyber Front Opens in Iran-Israel Conflict

[+US](#) [+Iran](#) [+Israel](#) [+Government](#)

- A rapidly escalating [conflict](#) between Israel, the United States, and Iran has expanded into cyberspace alongside ongoing military operations, with both sides conducting digital attacks on government, military, and infrastructure targets. Iran-linked hackers—including the Islamic Cyber Resistance Axis and personas tied to the Iranian Ministry of Intelligence and Security— have claimed hits on defense firms and apps like the widely used BadeSaba Calendar, pushing propagandistic messages to millions of users. Concurrent connectivity disruptions and attempted hacks on news outlets signal a coordinated cyber front intended to disrupt communications and erode situational awareness. Analysts warn that this conflict could trigger sustained geopolitical cyberattacks targeting broader digital ecosystems beyond immediate combatants.

Russia's APT28 Looms Over European Targets

[+Russia](#) [+APT28](#) [+Operation MacroMaze](#)

- The Russia-linked threat actor APT28 is running a multi-month campaign named [Operation MacroMaze](#) targeting entities in Western and Central Europe using malicious documents with webhook-based macros to initiate a covert beacon and malware execution chain. The campaign, active from late 2025 into early 2026, abuses legitimate services to evade detection and establishes out-of-band beaconing via HTTP webhook triggers when lure documents are opened. This ongoing operation

highlights APT28's continued focus on credential harvesting and data theft against regional targets, reinforcing persistent espionage objectives across sectors. Analysts have also linked other APT28 activity to critical credential theft and phishing campaigns globally, underlining its capability to blend social engineering and malware deployment.

AI-Supply Chain Abuse Delivers macOS Data Stealer

+AI +OpenClaw +AMOS

- Researchers have uncovered a sophisticated supply chain technique where malicious [OpenClaw](#) "skills" are used to manipulate AI agent workflows to install a new variant of the Atomic macOS Stealer (AMOS). This campaign abuses documentation files to prompt AI helpers into fetching a fake installer, tricking both automated agents and users into executing the payload which exfiltrates credentials, browser data, keychains, crypto wallets, and user documents. This evolution reflects an increasing trend of attackers targeting AI tooling and repository ecosystems to broaden infection vectors beyond traditional malware distribution methods. Organizations are advised to scrutinize untrusted AI "skills" and enforce rigorous supply chain security and endpoint defenses on macOS devices.

North Korean APT37 Malware Bridges Air-Gaps

+North Korea +APT37 +Ruby Jumper

- Security analysts report that North Korean state-linked APT37 has developed a malware suite, dubbed [Ruby Jumper](#), capable of infecting and bridging air-gapped networks through removable media. The toolkit includes multiple malicious components that can exfiltrate data and create bidirectional covert channels via USB drives, undermining the physical isolation of sensitive systems typically used in critical infrastructure and defense environments. While specific targets have not been publicly confirmed, the campaign underscores a strategic shift toward penetrating even highly isolated environments by leveraging physical media and sophisticated loader/backdoor chains. This technique presents a significant risk to organizations that rely on air-gap segregation as a primary defense.

Iranian Cyber Retaliation Claims Hit Gulf Energy Sector

+Iran +Energy +Handala

- In the wake of escalating military and cyber strikes by U.S. and Israeli forces, pro-Iranian and aligned hacktivist groups have begun signaling a broader digital counter-offensive targeting Western and Gulf energy infrastructure. One group, [Handala](#), claimed a breach of an oil and gas exploration firm's network, posting on leak sites and warning of "massive cyber attacks." Analysts observe an expansion in the number of active groups and the geographic breadth of threats, with some allied pro-Russian actors expected to join operations. While independent verification of operational impact remains limited, warnings have intensified for energy and OT-linked critical infrastructure owners to harden defenses against correlated and asymmetric cyber threats.

Israeli Forces Unleash Historic Cyber Strike on Iran

+Israel +Iran +Government

- Israeli forces, in parallel with kinetic strikes against Iranian targets, reportedly executed one of the [largest cyberattacks in history](#) against Iran, disrupting critical infrastructure, official news websites, and government digital communications. Internet connectivity within Iran plunged to near total blackout levels as critical services and regime communications systems were taken offline or severely degraded, compounding the impact of ongoing physical military operations. The offensive appears designed to prevent coordinated Iranian responses and to isolate leadership digitally, even affecting state media platforms. Independent analysts and network measurement groups confirmed severe connectivity drops consistent with large-scale cyber interference.

Data Breaches

AI-Driven Exploits Shake Mexican Government Networks

+AI +Mexico +Government

- Hackers abused Anthropic's [Claude Code](#) AI assistant, along with prompts passed to OpenAI's GPT-4.1, to write exploits, build tools, and automate data exfiltration from multiple Mexican government systems, including the tax authority and civil registry. Over 150 GB of sensitive data was taken across at least ten government bodies and a financial institution, potentially exposing hundreds of millions of identity records. The attack bypassed AI guardrails by convincing the model that its actions were

authorized, illustrating a new breed of AI-assisted operational tradecraft. This incident underscores how generative AI can supercharge exploit development, automation, and scale for attackers.

Conduent Exposes Health & ID Data in Potential Largest US Breach

+US +Business

- A massive breach at [Conduent Business Services](#), a backend services provider for state Medicaid and administrative programs, has exposed personal and health information for over 25 million Americans, including Social Security numbers, addresses, and health data. State filings and attorney general statements suggest the number of affected records continues to rise, potentially making this the largest-ever U.S. data breach. Texas and other states are among the hardest hit, triggering legal demands and a high-profile investigation into whether security lapses violated data protection laws. The sheer volume of exposed sensitive consumer data has alarmed regulators and privacy advocates nationwide.

Coupang Faces Competitive Backlash After Massive Data Leak

+South Korea +Retail

- South Korea's largest e-commerce platform, [Coupang](#), is bracing for stronger competition and regulatory scrutiny after disclosure of a major data breach affecting around 34 million users, exposing names, phone numbers, and shipping addresses (no payment or login credentials). Consumer trust dipped as rival platforms saw user gains, and analysts say the breach contributed to weaker quarterly performance and a downward revision of growth forecasts. Investigations by Korean authorities attribute the incident to management lapses rather than sophisticated external attack vectors, deepening concern about internal security practices. Coupang's recovery now hinges on rebuilding trust amid rising competitive pressure and calls for tighter data security reform.

Advantest Semiconductor Supplier Hit by Ransomware

+Japan +Technology

- Tokyo-based semiconductor test equipment maker [Advantest](#) confirmed a ransomware attack after detecting unusual network activity on February 15, 2026, deploying incident response and isolating affected systems. While it remains unclear which group is responsible or whether data exfiltration occurred, the firm engaged external cybersecurity experts to contain the intrusion and investigate impact. Advantest serves major global chipmakers, and this incident highlights ongoing ransomware targeting across the semiconductor supply chain, which has seen similar attacks in recent years. The company pledged to notify stakeholders if evidence of compromised customer or employee data emerges as investigations continue.

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.