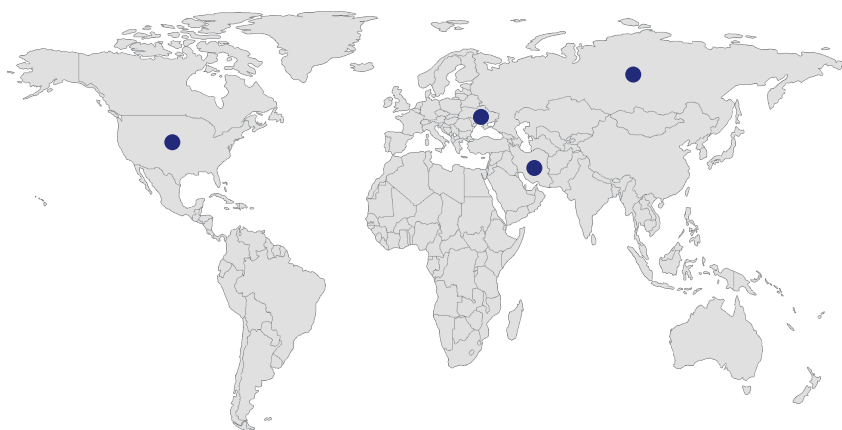


IMPERVA THREAT RESEARCH

Threat Intel Report: January 5-11, 2026

Countries



Top Tags

UAC-0184

MuddyWater

PHALT#BLYX

TridentLocker

Crimson Collective

Executive Summary

Actionable Information:

- **Scale and automation continue to dominate attacker tradecraft.** High-velocity credential spraying and ransomware-as-a-service operations demonstrate that attackers are prioritizing breadth, speed, and resilience over bespoke intrusion paths. Default credentials, exposed services, and weak identity hygiene remain primary enablers, with attackers rapidly monetizing access through crypto theft or extortion.
- **Social engineering is evolving toward “assisted compromise.”** Campaigns leveraging messaging platforms, browser-based deception, and trusted enterprise communication channels show attackers increasingly relying on user participation rather than pure exploit chains. This trend lowers technical barriers while maintaining high success rates, particularly in travel, financial services, and government-adjacent environments.
- **AI and automation tooling are becoming a new attack surface.** From malicious Chrome extensions exfiltrating AI prompts to critical workflow automation vulnerabilities, attackers are exploiting the rapid adoption of AI and low-code platforms, often abusing trusted integrations and insufficient isolation controls rather than zero-days.
- **Sensitive data exposure now spans consumer PII, government records, and critical infrastructure design.** Breaches affecting gas station operators, federal contractors, telecom providers, utilities engineering firms, and even cybercrime forums underscore that both regulated industries and attacker ecosystems themselves are leaking at scale, expanding identity theft risk, regulatory exposure, and intelligence value for adversaries.

Outlook:

This week's activity reinforces that 2026 is shaping into a year where trust boundaries, not perimeter exploits, are the primary battleground. Attackers are increasingly successful by abusing legitimate access paths: credentials instead of exploits, extensions instead of malware loaders, contractors instead of insiders, and notifications instead of phishing emails. As organizations accelerate adoption of AI assistants, automation platforms, and third-party service providers, the attack surface is broadening faster than governance and monitoring controls are maturing. Expect continued growth in campaigns that blend automation with low-friction social engineering, alongside heightened interest in data sets that offer downstream leverage, whether for fraud, extortion, or strategic intelligence, rather than immediate disruption alone.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

 723% [CVE-2025-55752](#)

- Relative Path Traversal vulnerability in Apache Tomcat. The fix for bug 60013 introduced a regression where the rewritten URL was normalized before it was decoded. This introduced the possibility that, for rewrite rules that rewrite query parameters to the URL, an attacker could manipulate the request URI to bypass security constraints including the protection for /WEB-INF/ and /META-INF/.

 293% [CVE-2025-12101](#)

- Cross-Site Scripting (XSS) in NetScaler ADC and NetScaler Gateway when the appliance is configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) OR AAA virtual server.

 280% [CVE-2025-47227](#)

- In the Production Environment extension in Netmake ScriptCase through 9.12.006 (23), the Administrator password reset mechanism is mishandled. Making both a GET and a POST request to login.php is sufficient. An unauthenticated attacker can then bypass authentication via administrator account takeover.

Recent Cyber Threats

Credential Spray at Internet Scale

+[GoBruteforcer](#)

- A rapidly evolving botnet dubbed [GoBruteforcer](#) is brute-forcing weak and reused credentials to compromise internet-facing Linux servers at scale, with an estimated 50,000+ exposed servers at risk. The exposure is amplified by millions of services reachable on default ports and by predictable usernames/password patterns that appear in copied (including AI-generated) config examples. The 2025 variant is rewritten in Go and adds obfuscation, persistence, and process-masking (e.g., renaming to "init"), plus resilient fallback C2 paths. In multiple intrusions, operators escalated into crypto theft tooling while infected hosts can scan ~20 IPs/second to keep throughput high.

Viber-Lured ZIPs Drop Remcos on Ukraine Targets

+[Russia](#) +[Ukraine](#) +[UAC-0184](#) +[Viber](#)

- Russia-aligned activity attributed to [UAC-0184](#) targeted Ukrainian military and government entities using Viber to deliver malicious ZIP archives. The ZIPs contain LNK files masquerading as Word/Excel documents; opening them triggers a decoy while

a PowerShell script retrieves a second archive (“smoothieks.zip”) to deploy Hijack Loader. The loader is reconstructed in-memory and uses evasion (including DLL side-loading/module stomping) and security-product checks before persisting via scheduled tasks. Final-stage delivery executes Remcos RAT (injected into “chime.exe”), enabling remote control and data theft.

RustyWater: MuddyWater’s Quiet RAT Upgrade

+MuddyWater +RustyWater +Iran

- The Iran-linked actor [MuddyWater](#) was tied to a spear-phishing campaign across Middle East sectors, including diplomatic, maritime, financial, and telecom, delivering a Rust implant dubbed RustyWater. Emails posing as cybersecurity guidance attach a malicious Word document that prompts victims to “Enable content,” triggering a VBA macro to install the Rust payload. RustyWater collects host details, checks installed security tools, establishes persistence via registry keys, and connects to a C2 to support file ops and command execution. Reporting characterized the shift to Rust as a tooling evolution toward more modular, lower-noise RAT capability.

N8scape: Workflow Editors to Host Command Execution

+AI +CVE

- A critical n8n flaw ([CVE-2025-68668](#), CVSS 9.9) allows an authenticated user who can create/modify workflows to execute arbitrary OS commands on the host running n8n. The issue is described as a sandbox bypass in the Python Code Node using Pyodide, effectively running attacker code with the same privileges as the n8n process. It affects versions 1.0.0 to <2.0.0 and is fixed in 2.0.0; n8n also pointed to a task-runner based native Python implementation introduced earlier (and made default in 2.0.0) to improve isolation. Suggested mitigations include disabling the Code node or Python support via environment variables and enabling the sandboxed runner configuration.

Fake Booking Cancellations Push “ClickFix” Malware in Hotels

+PHALT#BLYX +Travel +Russia

- A campaign tracked as [PHALT#BLYX](#) targets European hospitality organizations using fake reservation cancellation emails that impersonate booking sites and route victims through a staged browser-error flow. Victims are shown a fake “Blue Screen of Death” page and instructed to copy/paste commands (a ClickFix technique) that ultimately downloads malware. The infection chain uses MSBuild project files and culminates in DCRat, enabling keystroke logging and broader remote actions; researchers said the script chain can disable Windows Defender and open a legitimate booking page as a decoy while the malware executes. Indicators cited (including Russian debug strings and Russia-geolocated infrastructure) suggest a Russian nexus, and the lures used Euro-denominated charges (often >€1,000) to drive urgency.

Prompt Poaching via “ChatGPT Sidebar” Impostors

+AI

- Two [Chrome Web Store](#) extensions (with over 900,000 users collectively) have been reported, that exfiltrate ChatGPT and DeepSeek conversations plus browsing telemetry to attacker-controlled infrastructure. The add-ons masquerade as a legitimate AI chat extension and request “analytics” permissions, but then scrape DOM elements to capture chat content and upload it, along with all open tab URLs, every 30 minutes to C2 domains. Researchers also observed the actors using the Lovable AI web-development platform to host privacy-policy and infrastructure components to blur attribution and intent. The net impact is high-risk leakage of sensitive prompts, files, and context that can be weaponized for corporate espionage, targeted phishing, and downstream account compromise.

Data Breaches

Gas Station Operator Data Breach Exposes Consumer PII

+Retail +Travel

- [Gulshan Management Services, Inc.](#), which operates 150+ gas stations under Handi Plus/Handi Stop, reported a breach that exposed personal data tied to ~377,000 individuals, including names, addresses, Social Security numbers, driver’s licenses and financial account information. Unauthorized access occurred between mid- and late-September 2025 and was not publicly disclosed until January 5, 2026. The delay in notification has spurred class-action lawsuits and regulatory scrutiny, with potential identity theft and fraud risks elevated for affected individuals.

Ransomware Disrupts Federal Contractor Files

+TridentLocker +US

- [Sedgwick Government Solutions](#)—a subsidiary of claims administrator Sedgwick that supports multiple U.S. federal agencies—confirmed a cybersecurity incident after the TridentLocker ransomware group claimed to have stolen ~3.4 GB of data from an isolated file transfer system. TridentLocker, a relatively new ransomware-as-a-service operator, posted samples to its leak site as part of a double-extortion campaign. Sedgwick says the incident did not affect broader corporate systems or mission-critical platforms, but the exposure of sensitive government service data underscores persistent threats to contractors handling federally entrusted information.

Title Utility Engineering Data Offered for Sale After Alleged Breach

+US +Utilities

- A hacker alleges they have exfiltrated and are selling 139 GB of engineering and operational data from [Pickett and Associates](#), a U.S. firm that provides planning and design services for major electric utilities including Tampa Electric, Duke Energy Florida, and American Electric Power. The claimed stolen files reportedly include LiDAR point clouds, orthophotos, design files, and control settings that could support infrastructure mapping and risk analysis; the data was posted for sale on a dark web forum for ~6.5 BTC (~\$585,000). Duke Energy has confirmed an investigation into the claims, while Pickett and Associates has not commented. If validated, the breach could impact millions of utility customers and raise concerns about the exposure of critical infrastructure design information.

Broadband Provider Faces Data Theft Claims

+Crimson Collective +Telecommunications

- The extortion group [Crimson Collective](#) claimed it has obtained over 1 million customer records from U.S. fiber broadband provider Brightspeed and posted a data sample to pressure the company. Brightspeed acknowledged it is investigating the alleged breach, though the company has not confirmed the scope or impact publicly. The claimed data exfiltration reflects ongoing targeting of communications infrastructure providers, with potential regulatory, reputational, and customer protection implications if verified.

EEOC Portal Data Exposed by Contractor Misuse

+US +Government

- The [U.S. Equal Employment Opportunity Commission](#) (EEOC) disclosed a security incident in its Public Portal system involving unauthorized handling of agency data by contractor staff, first identified in early 2025. The incident may have exposed personally identifiable information submitted to the portal, prompting the EEOC to require password resets and work with law enforcement as it assesses the scope. The breach highlights risks tied to third-party contractor access in sensitive public sector systems.

Instagram ‘Leak’ Stemmed from Credential-Reset Abuse

+Social Media

- Reports of a major [Instagram](#) breach affecting ~17.5 million accounts were attributed to a scraped data set from 2022 that resurfaced, leading to password reset email waves for users. Meta has stated no breach occurred, asserting that account data was not stolen through a new intrusion, and that reset emails reflect abuse of a password reset request mechanism rather than direct exposure of credentials or PII. Security professionals recommend users ignore unsolicited resets and secure accounts directly.

Crime Forum Compromised, 324K Accounts Exposed

+Cybercrime

- A massive database leak from the notorious cybercrime forum [BreachForums](#) exposed roughly 323,000–324,000 user accounts, including usernames, email addresses, hashed passwords, IP metadata, private messages, and potentially PGP keys tied to forum signatures. The breach reportedly occurred during a site restoration process in August 2025, prior to the forum’s October takedown, and the data was later published by unknown actors alongside a lengthy manifesto claiming responsibility. The exposure undermines trust in the platform, especially for users relying on anonymity, and presents forensic opportunities for law enforcement and researchers tracking cybercriminal networks.

Fake Crypto Scam Notification Hits Betterment Users

+Financial Services +Crypto

- Fintech platform [Betterment](#) confirmed a security incident after hackers used unauthorized access to its third-party messaging infrastructure to send fraudulent crypto scam messages through both email and the mobile app. The messages, appearing to offer a “crypto giveaway” promising tripled returns for deposits into specified BTC/ETH wallets, caused confusion among users; blockchain records show some funds were sent before alerts were issued to disregard the offer. Betterment states that no customer accounts or credentials were directly accessed, and the incident response team has revoked the unauthorized access and launched an ongoing investigation.

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.