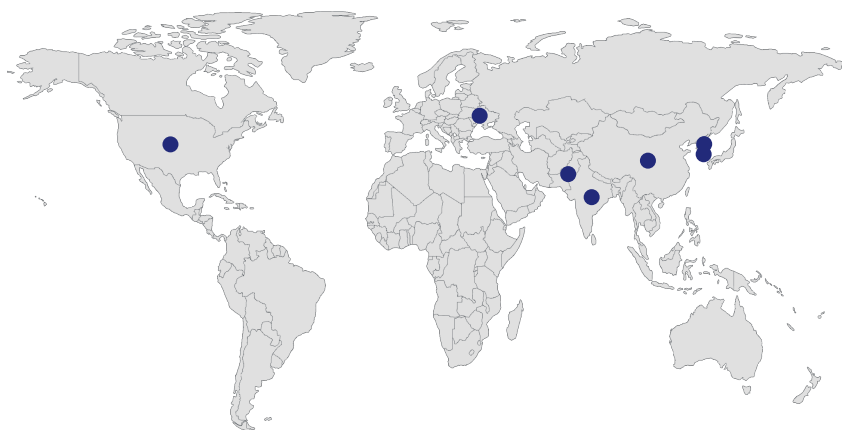


IMPERVA THREAT RESEARCH

Threat Intel Report: March 2-8, 2026

Countries



Top Tags

OpenClaw

BadPaw

UAT-9244

APT37

FulcrumSec

Executive Summary

Actionable Information:

- **Threat actors are increasingly abusing trust in developer ecosystems and emerging technologies.** The OpenClaw malware campaign shows how attackers can weaponize search results and legitimate platforms such as GitHub to distribute malware. By impersonating popular AI tools and repositories with large developer communities, attackers increase the likelihood that victims will execute malicious installers without suspicion. Organizations should monitor software supply chains and encourage verification of code sources and hashes before installation.
- **Nation-state espionage activity remains persistent and geographically diverse.** Multiple campaigns this week involved state-aligned actors including China-linked UAT-9244 targeting telecom infrastructure in South America, North Korea's APT37 expanding espionage tooling, and Pakistan-linked APT36 targeting Indian government networks using malware disguised as AI utilities. These operations highlight continued strategic targeting of telecommunications providers, government agencies, and policy organizations to enable surveillance and intelligence collection.
- **Social engineering continues to drive initial compromise across both targeted and mass campaigns.** Spear-phishing lures in the BadPaw campaign used credible government-themed messages related to border crossings, while large-scale tech-support spam campaigns deployed remote access malware. Additionally, the HungerRush extortion emails demonstrate attackers leveraging brand recognition and fear tactics to pressure victims, even when no breach occurred.
- **Credential exposure and sensitive data mismanagement remain high-impact risk factors.** The theft of \$48 million in cryptocurrency following exposure of a wallet seed phrase demonstrates how a single leaked secret can result in immediate financial loss. Similarly, breaches affecting Madison Square Garden and LexisNexis highlight continued targeting of organizations storing large volumes of personally identifiable information (PII), increasing downstream risks such as identity theft and fraud.

- **Operational disruption attacks against public infrastructure continue to pose risk.** The malware incident affecting Cumberland County, New Jersey, disrupted government phone systems, including communications tied to emergency services. Even when data theft is not confirmed, such incidents highlight how cyberattacks can directly impact service availability and public-sector operations.

Outlook:

This week's activity reflects a convergence of two persistent cyber trends: the continued expansion of nation-state espionage operations and the growing exploitation of trusted platforms and social engineering techniques to deliver malware at scale. Threat actors are increasingly leveraging the popularity of emerging technologies, particularly AI tools, and widely trusted infrastructure such as GitHub repositories or legitimate brands to disguise malicious activity. At the same time, state-sponsored groups continue to prioritize strategic sectors such as telecommunications, government networks, and policy organizations, seeking long-term access for intelligence collection. Looking ahead, organizations should expect continued weaponization of developer ecosystems, supply chains, and AI-related tools alongside persistent credential exposure risks and data breaches targeting large data aggregators. Strengthening identity protection, monitoring for anomalous account creation or credential exposure, and validating software sources will be critical as attackers increasingly combine traditional social engineering with modern technology ecosystems to scale their operations.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

274% [CVE-2025-55182](#)

- A pre-authentication remote code execution vulnerability exists in React Server Components versions 19.0.0, 19.1.0, 19.1.1, and 19.2.0 including the following packages: react-server-dom-parcel, react-server-dom-turbopack, and react-server-dom-webpack. The vulnerable code unsafely deserializes payloads from HTTP requests to Server Function endpoints.

216% [CVE-2025-59718](#)

- A improper verification of cryptographic signature vulnerability in Fortinet FortiOS 7.6.0 through 7.6.3, FortiOS 7.4.0 through 7.4.8, FortiOS 7.2.0 through 7.2.11, FortiOS 7.0.0 through 7.0.17, FortiProxy 7.6.0 through 7.6.3, FortiProxy 7.4.0 through 7.4.10, FortiProxy 7.2.0 through 7.2.14, FortiProxy 7.0.0 through 7.0.21, FortiSwitchManager 7.2.0 through 7.2.6, FortiSwitchManager 7.0.0 through 7.0.5 allows an unauthenticated attacker to bypass the FortiCloud SSO login authentication via a crafted SAML response message.

176% [CVE-2025-32432](#)

- Craft is a flexible, user-friendly CMS for creating custom digital experiences on the web and beyond. Starting from version 3.0.0-RC1 to before 3.9.15, 4.0.0-RC1 to before 4.14.15, and 5.0.0-RC1 to before 5.6.17, Craft is vulnerable to remote code execution. This is a high-impact, low-complexity attack vector. This issue has been patched in versions 3.9.15, 4.14.15, and 5.6.17, and is an additional fix for CVE-2023-41892.

Authentication Infrastructure Targeted by Prolonged Application-Layer DDoS

+DDoS +Telecommunications

- Attackers targeted a telecommunications company's authentication infrastructure this week, launching an application-layer DDoS attack against its remote access gateway that peaked at nearly 8 million requests per second and persisted for 16 hours. The targeted endpoint appears to support RADIUS-based authentication, which organizations commonly use for VPN, Wi-Fi, and network access control. Attacks against authentication services can disrupt employee connectivity and remote access, highlighting how adversaries increasingly target identity infrastructure to cause operational disruption.

Brute-Force ATO Campaign Targets US Retail Platform

+ATO +US +Retail

- A US-based retail site experienced a concentrated account takeover (ATO) campaign this week, with attackers generating nearly 1.5 million malicious login attempts within a single hour. The activity was largely driven by brute-force login attempts originating entirely from US-based IP addresses, suggesting the use of compromised domestic infrastructure or proxy networks to blend in with legitimate traffic. Retail platforms remain attractive targets for credential attacks due to stored payment methods, loyalty accounts, and resale value of compromised accounts, highlighting the continued need for strong bot mitigation and login abuse protections.

Recent Cyber Threats

Malicious OpenClaw Installers Spread via AI Search Results

+OpenClaw +AI +Malware

- Attackers distributed malware through fake installers for the [OpenClaw](#) AI agent after poisoning search results with a malicious GitHub repository. Users searching Bing AI for “OpenClaw Windows” were directed to the repository, which delivered information-stealing malware and the GhostSocks proxy tool when executed. The campaign leveraged trust in GitHub and the popularity of the OpenClaw project, which has tens of thousands of forks, to appear legitimate. Researchers discovered the activity in February, and the malicious repositories were later removed.

BadPaw Malware Campaign Targets Ukrainian Entities

+BadPaw +Malware +Ukraine

- Researchers uncovered a multi-stage malware campaign dubbed [BadPaw](#) targeting Ukrainian organizations using spear-phishing lures referencing government border-crossing appeals. The campaign delivered malicious documents designed to appear credible by leveraging Ukrainian email infrastructure and government-themed content. Once opened, the files executed multiple stages of malware designed to establish persistence and enable further compromise. The operation highlights continued cyber activity aligned with geopolitical tensions involving Ukraine.

Self-Propagating Worm Vandalizes Wikipedia Pages

+Worm +JavaScript

- [Wikipedia](#) experienced a security incident when a self-propagating JavaScript worm modified user scripts and vandalized pages on Meta-Wiki. The malicious code injected itself into user and global JavaScript files, allowing it to spread automatically as editors loaded affected pages in their browsers. Approximately 3,996 pages were modified and about 85 user scripts altered before the incident was contained. Wikimedia temporarily restricted editing while engineers removed the code and restored affected content; no evidence of data theft was found.

China-Linked Hackers Deploy New Toolkit Against Telecom Providers in South America

+China +UAT-9244 +Telecommunications

- Security researchers identified a Chinese state-linked threat actor tracked as [UAT-9244](#) targeting telecommunications providers in South America using a newly observed malware toolkit. The group is believed to have ties to known Chinese cyber-espionage clusters such as FamousSparrow and Tropic Trooper. The toolkit is designed for stealthy network compromise and persistence, enabling long-term access to telecom infrastructure. The campaign highlights ongoing nation-state interest in telecom networks due to their value for surveillance and intelligence collection.

North Korea's APT37 Expands Malware Arsenal for Espionage Operations

+North Korea +APT37 +Malware

- Researchers report that the North Korean threat group [APT37](#) (ScarCruft) has expanded its malware toolkit to support broader cyber-espionage operations. The group has introduced new backdoors and reconnaissance tools designed to collect sensitive information and maintain persistence within compromised networks. Campaigns have targeted organizations involved in policy, diplomacy, and regional security matters. The activity reflects continued North Korean investment in cyber capabilities to gather intelligence and support geopolitical objectives.

Pakistan-Linked APT36 Targets Indian Government with AI-Themed Malware Campaign

+Pakistan +India +APT36

- The Pakistan-linked threat actor [APT36](#) (Transparent Tribe) has launched a campaign targeting Indian government networks using malware disguised as AI-themed “vibeware” tools. The operation used spear-phishing lures and malicious software masquerading as legitimate AI utilities to trick victims into installing the malware. Once executed, the malware establishes persistence and enables data exfiltration from compromised systems. The campaign appears focused on espionage against Indian government institutions amid ongoing geopolitical tensions in the region.

Tech Support Spam Campaign Deploys Remote Access Malware

+Malware +Spam

- Researchers uncovered a large [spam campaign](#) distributing fake technical support messages that ultimately deliver remote access malware. Victims are tricked into contacting fraudulent support channels or interacting with malicious attachments that install remote access tools on their systems. Once installed, attackers can control infected machines, harvest credentials, and deploy additional payloads. The campaign highlights how tech-support themed social engineering continues to be an effective vector for malware distribution.

Data Breaches

\$48M in Cryptocurrency Stolen After Government Wallet Seed Exposure

+South Korea +Government +Crypto

- Approximately \$48 million in cryptocurrency was stolen after a wallet seed phrase linked to a [South Korean tax agency system](#) was inadvertently exposed online. Attackers were able to use the seed phrase to access and drain funds from the affected crypto wallets. The breach illustrates how improper handling of sensitive cryptographic credentials can result in immediate and irreversible financial loss. Authorities are investigating the incident while attempting to trace the stolen funds through blockchain transactions.

Madison Square Garden Notifies Customers of Data Breach

+US +Entertainment

- [Madison Square Garden Entertainment](#) disclosed a data breach affecting customer records after unauthorized actors gained access to systems associated with the company’s network. Exposed data reportedly includes names and Social Security numbers, raising concerns about identity theft risks for affected individuals. The company has begun notifying impacted customers and offering credit monitoring services. The incident underscores continued targeting of entertainment and hospitality organizations that store large volumes of customer data.

Restaurant Customers Targeted in Mass Extortion Email Campaign

+Technology +Extortion

- Hackers sent mass extortion emails to customers of restaurant technology provider [HungerRush](#), claiming they had stolen sensitive customer information. The messages threatened to publish allegedly compromised data unless victims paid a ransom. HungerRush said the campaign appears to be a fraudulent extortion attempt, with no evidence that its systems were breached or customer data was accessed. The campaign demonstrates how attackers increasingly target end users with scare tactics tied to recognizable brands.

LexisNexis Confirms Data Breach Following Leak of Stolen Files

+FulcrumSec +US +Government +Technology

- [LexisNexis Risk Solutions](#) confirmed a data breach after a threat actor known as FulcrumSec leaked stolen files online, prompting an investigation into the scope of the incident. The exposed data reportedly includes sensitive records linked to individuals and organizations contained within the company’s data services platform. LexisNexis is working to determine how attackers accessed the systems and what information may have been compromised. Given the company’s role in providing large-scale data intelligence services, the breach could have downstream impacts on organizations relying on its datasets.

County Cyberattack Disrupts Emergency Phone Systems in New Jersey

+US +Government

- Officials in [Cumberland County, New Jersey](#) reported that a malware attack disrupted the county's phone systems, temporarily affecting government communications including emergency call infrastructure. The incident forced authorities to shut down parts of their network while responding to the intrusion and restoring services. County officials stated that the disruption impacted internal and public-facing communications but did not confirm whether sensitive data was accessed. The attack highlights how local government infrastructure remains vulnerable to cyber incidents that can disrupt critical services.

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.