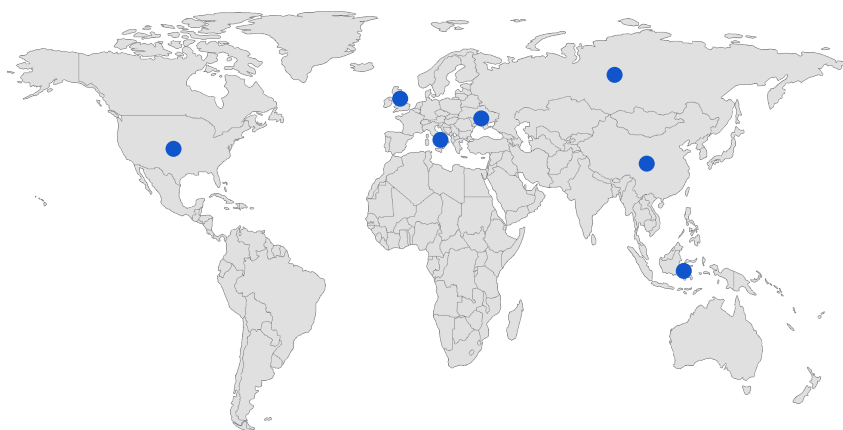


Threat Intel Report: February 17-23, 2025

Countries



Top Tags

NoName057(16)

Lazarus Group

FrigidStealer

Salt Typhoon

Black Basta

Executive Summary

Actionable Information:

- **Rise in Politically Motivated Attacks:** Hactivist groups continue to launch politically driven cyberattacks, especially targeting financial and critical infrastructure sectors in response to geopolitical conflicts. DDoS attacks remain a favored tool for disrupting services and creating public visibility for their causes.
- **Evolving Malware and Supply Chain Threats:** Threat actors are increasingly leveraging supply chain vulnerabilities, third-party repositories, and compromised software to distribute infostealers and backdoors. Infostealers targeting macOS and social engineering tactics like fake updates are becoming more sophisticated, leading to broader user compromise.
- **Critical Vulnerabilities in Widely Used Software:** Exploits targeting common software platforms such as Chrome, PHP, and enterprise hardware like Xerox printers highlight the persistent risk of unpatched systems. Attackers continue to exploit vulnerabilities for remote code execution, lateral movement, and credential theft.
- **Advanced Persistent Threat (APT) Activity and Espionage:** State-backed APT groups maintain a focus on long-term espionage campaigns, especially in telecommunications and critical infrastructure. Their use of custom malware and targeted attack strategies highlights the need for continuous network monitoring and threat intelligence sharing.
- **Healthcare and Ransomware Exposures:** Healthcare institutions remain lucrative targets for phishing and data theft, while ransomware groups continue to evolve their tactics, including the use of double extortion and internal leaks. Recent leaks of ransomware group communications reveal operational insights that could inform future defense strategies.

Outlook:

The cyber threat landscape is increasingly shaped by a mix of geopolitical tensions, evolving malware strains, and the exploitation of supply chain and software vulnerabilities. As politically motivated hacktivism and state-sponsored espionage grow more aggressive, critical infrastructure, healthcare, and financial institutions remain top targets. The rise in macOS-targeting malware and complex social engineering campaigns signals a broadening attack surface beyond traditional endpoints. Organizations must prioritize patch management, strengthen incident response capabilities, and maintain proactive threat intelligence programs to counter both opportunistic and targeted cyberattacks.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 17,399% [CVE-2025-0108](#)

- An authentication bypass in the Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to the management web interface to bypass the authentication otherwise required by the PAN-OS management web interface and invoke certain PHP scripts.

↑ 92% [CVE-2024-53704](#)

- An Improper Authentication vulnerability in the SSLVPN authentication mechanism allows a remote attacker to bypass authentication.

↑ 33% [CVE-2024-21893](#)

- A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication.

UK Site Hit by 3.4M RPS DDoS Attack

+UK +DDoS

- A UK site was hit by a 3.4 million RPS DDoS attack last week, which came from 9,750 distinct IP addresses. The attack lasted an hour and primarily leveraged US and China-based IPs.

Business Logic Attacks Target Indonesian Gaming Site

+Indonesia +Gaming +Business Logic

- An Indonesian gaming site was targeted by business logic attacks reaching 6 million requests in one day. Attacks came primarily from South American IPs, as well as from Indonesia, and targeted URLs in order to manipulate regional settings, hijack sessions, and switch prices in carts.

Recent Cyber Threats

NoName057(16) Launches DDoS Attacks on Italian Banks

+NoName057(16) +Italy +Financial Services +Ukraine +Russia

- The pro-Russian hacktivist group [NoName057\(16\)](#) carried out coordinated DDoS attacks against major Italian banks, disrupting online services and customer access. The group claimed responsibility via its Telegram channel, citing political motivations linked to Italy's support for Ukraine. The attacks highlight the growing trend of politically motivated cyber operations targeting European financial institutions. Italian cybersecurity agencies are actively investigating and working to mitigate the impact.

PirateFi Game on Steam Spreads Vidar Infostealer Malware

[+Steam](#) [+Gaming](#) [+Vidar](#) [+Malware](#)

- The free-to-play game [PirateFi](#) on Steam was found distributing the *Vidar* infostealer malware, targeting users' credentials, session cookies, and cryptocurrency wallets. The game, available for nearly a week, infected up to 1,500 users before its removal. The malware was embedded within the game's executable, using obfuscation techniques and rotating command-and-control servers for data exfiltration. Steam has urged affected users to run antivirus scans, reset passwords, and consider OS reinstallation.

Critical PHP Flaw Enables SQL Injection Attacks on Websites

[+PHP](#) [+SQL Injection](#) [+SQLite](#)

- A critical vulnerability (CVE-2022-31631) in PHP versions before 8.0.27, 8.1.15, and 8.2.2 exposes websites using [SQLite](#) databases to SQL injection attacks. The flaw resides in the `'PDO::quote()'` function, which mishandles long strings, leading to integer overflows that attackers can exploit to execute malicious SQL queries. Websites running vulnerable PHP versions risk data theft or full database compromise. PHP users are urged to update to the latest patched versions immediately.

Lazarus Group Deploys Marstech1 JavaScript Implant in Targeted Developer Attacks

[+Lazarus Group](#) [+Marstech1](#) [+JavaScript](#) [+NPM](#) [+Crypto](#)

- The North Korean-linked [Lazarus Group](#) has been deploying a new JavaScript implant, Marstech1, to target developers through malicious GitHub repositories and NPM packages. The malware collects system information, targets cryptocurrency wallets like MetaMask, and can download further payloads. Active since late 2024, the campaign has affected at least 233 victims across the U.S., Europe, and Asia. The implant's layered obfuscation techniques make it difficult to detect, posing a significant threat to developers and cryptocurrency users.

Xerox Printer Vulnerabilities Expose Windows Active Directory Credentials

[+CVE](#) [+Printers](#) [+Windows AD](#)

- Two critical vulnerabilities (CVE-2024-12510, CVE-2024-12511) in [Xerox VersaLink](#) printers enable pass-back attacks, allowing attackers to capture Windows Active Directory credentials via LDAP and SMB/FTP services. Exploiting these flaws could enable lateral movement across networks, potentially compromising critical Windows servers. Xerox released patches in Service Pack 57.75.53, urging users to update firmware and secure printer configurations to mitigate risks.

Critical Chrome Buffer Overflow Flaws Enable Remote Code Execution

[+Google](#) [+Buffer Overflow](#) [+Browser](#)

- Google patched three critical vulnerabilities in [Chrome](#), including two heap buffer overflows (CVE-2025-0999 in V8 JavaScript Engine and CVE-2025-1426 in the GPU subsystem) and a use-after-free flaw (CVE-2025-1006) in the network stack. These flaws could allow attackers to execute arbitrary code, bypass sandbox protections, and gain system-level privileges. Users are urged to update Chrome to prevent exploitation.

FrigidStealer Malware Targets Mac Users via Fake Browser Updates

[+FrigidStealer](#) [+Malware](#) [+MacOS](#) [+TA2726](#) [+TA2727](#)

- [FrigidStealer](#), a new macOS-focused infostealer, is being spread through fake browser update alerts on compromised websites. Delivered via malicious DMG files, the malware steals browser cookies, login credentials, crypto wallet data, and files from Apple Notes and user directories. Managed by threat actors TA2726 and TA2727, the campaign also targets Windows and Android users with alternative payloads. The stolen data is exfiltrated to a C2 server, putting users at high risk of identity theft and financial fraud.

Salt Typhoon Targets U.S. Telecom Providers with Custom Malware

[+Salt Typhoon](#) [+Telecommunications](#) [+US](#) [+China](#) [+JumbledPath](#)

- The Chinese state-backed APT group [Salt Typhoon](#) (also known as Gallium) deployed a custom malware, JumbledPath, in a cyber-espionage campaign against U.S. telecom providers. The malware enables persistent access, data exfiltration, and lateral movement across networks. Active since 2012, Salt Typhoon focuses on

telecom and government sectors, with this campaign aiming to intercept communications and gather sensitive data. U.S. agencies are monitoring for further activity and recommend enhanced network defenses.

Data Breaches

Charleston Area Medical Center Suffers Data Breach After Phishing Attack

[+Phishing](#) [+US](#) [+Healthcare](#)

- In October 2024, [Charleston Area Medical Center](#) (CAMC) experienced a data breach when a phishing attack compromised a single employee's email account. The unauthorized access lasted from October 2 to October 3, potentially exposing sensitive personal and health information of approximately 67,000 individuals. CAMC has since terminated the unauthorized access and is notifying affected individuals.

Leaked Chats Reveal Black Basta Ransomware Group's Internal Operations

[+Black Basta](#) [+Ransomware](#) [+Russia](#)

- Over 200,000 internal messages from the [Black Basta](#) ransomware group, spanning from September 2023 to September 2024, have been leaked online. The messages provide insights into the group's target selection, attack execution, ransom negotiations, and internal conflicts. The leak, reportedly in retaliation for Black Basta targeting Russian banks, offers a rare glimpse into the operational dynamics and challenges within the cybercriminal organization.

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.