

IMPERVA THREAT RESEARCH

Threat Intel Report: October 13-19, 2025

Countries



Top Tags

[Astaroth](#)[Contagious Interview](#)[RedLine Stealer](#)[ClickFix](#)[ClOp](#)

Executive Summary

Actionable Information:

- **Developer & Open-Source Risk:** Public repos and package ecosystems are being abused for malware delivery and supply-chain attacks.
- **Social Engineering:** Adversaries exploit messaging apps, social media, and ad networks to distribute malware and infostealers at scale.
- **Enterprise & Third-Party Software:** Unpatched or misconfigured enterprise software and cloud services continue to expose sensitive data and enable extortion.
- **Data Exposure & PII Theft:** Misconfigurations and breaches of financial, retail, and marketing platforms are creating mass exposure of PII and financial data.
- **Credential & Wallet Theft:** Malware increasingly targets browser profiles, crypto wallets, and authentication credentials through infostealers and keyloggers.

Outlook:

Threat actors will continue to merge state-level and criminal tactics, exploiting developer tools, social platforms, and cloud misconfigurations to maximize access and profit. Social engineering and supply-chain abuse will remain high-volume vectors, while enterprise software and cloud services misconfigurations will continue to produce large-scale data exposures. Organizations that prioritize supply-chain security, patch management, phishing-resistant MFA, and proactive monitoring of cloud and repo environments will reduce both financial and operational risk in this evolving threat landscape.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

121% [CVE-2024-4885](#)

- In WhatsUp Gold versions released before 2023.1.3, an unauthenticated Remote Code Execution vulnerability in Progress WhatsUpGold. The WhatsUp.ExportUtilities.Export.GetFileWithoutZip allows execution of commands with iisappool\winrmconsole privileges.

110% [CVE-2024-36104](#)

- Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 18.12.14. Users are recommended to upgrade to version 18.12.14, which fixes the issue.

109% [CVE-2024-38856](#)

- Incorrect Authorization vulnerability in Apache OFBiz. This issue affects Apache OFBiz: through 18.12.14. Users are recommended to upgrade to version 18.12.15, which fixes the issue. Unauthenticated endpoints could allow execution of screen rendering code of screens if some preconditions are met (such as when the screen definitions don't explicitly check user's permissions because they rely on the configuration of their endpoints).

Recent Cyber Threats

Astaroth Trojan Adopts GitHub for Resilience

[+Astaroth](#) [+Trojan](#) [+Financial Services](#)

- [Astaroth](#) operators are leveraging GitHub to host malware configurations, enabling the banking trojan to stay operational even after C2 infrastructure takedowns. The campaign uses DocuSign-themed phishing emails to deliver malicious LNK files, leading to credential theft from banking and crypto sites across Latin America. GitHub was used to hide configuration data via steganography, complicating takedown efforts.

WhatsApp Worm Campaign Pushes Malware

[+Worm](#) [+Social Engineering](#)

- A new self-propagating malware is spreading through malicious [WhatsApp](#) messages that lure users into downloading fake updates or APK files. Once installed, the worm forwards itself to the victim's contacts, rapidly expanding its reach. The attack leverages social engineering to compromise mobile devices at scale.

North Korea Targets Developers with npm Supply Chain Attack

[+North Korea](#) [+npm](#) [+Contagious Interview](#)

- Researchers uncovered 338 malicious npm packages tied to North Korea's [Contagious Interview](#) campaign, downloaded over 50,000 times. Attackers posed as recruiters to trick developers into installing malware targeting cryptocurrency and blockchain platforms. The operation highlights increasing abuse of open-source ecosystems for state-backed espionage and theft.

BeaverTail–OtterCookie Merger Supercharges North Korean Malware

[+North Korea](#) [+BeaverTail](#) [+OtterCookie](#) [+Malware](#)

- [North Korean actors](#) are merging BeaverTail and OtterCookie malware capabilities, adding keylogging, clipboard monitoring, and wallet theft modules to enhance their toolkit. The campaign, tied to the Contagious Interview operation, abuses npm, Bitbucket,

and blockchain infrastructure for resilient C2. Recent activity targeted a company in Sri Lanka, indicating ongoing global reach and rapid tool evolution.

Malvertising Campaign Pushes Comet Browser Malware

+RedLine Stealer +AI

- Attackers are distributing fake [Comet Browser](#) installers through malicious Google search ads, delivering a RedLine Stealer variant. The campaign mimics legitimate software pages to infect users' systems and exfiltrate credentials, browser data, and cryptocurrency wallet information. The operation relies on paid search to maximize exposure and trust.

TikTok ClickFix Attacks Drive Infostealer Surge

+ClickFix +LummaC2 +RedLine Stealer

- A growing wave of [ClickFix](#) campaigns on TikTok is luring users with fake account recovery and free service prompts, ultimately dropping infostealers like LummaC2 and RedLine. The malware targets browser data and crypto wallets, exploiting the platform's reach to deliver mass infections. Researchers warn of rising infostealer activity tied to social media lures.

Data Breaches

Invoice Platform Leak Exposes 178K Business Files

+Financial Services

- A publicly accessible, unencrypted database tied to the invoicing-platform [Invoicely](#) (or an associated third-party) contained 178,519 files such as Excel, PDF and image formats, including invoices, tax documents, scanned checks and ride-share receipts. Researchers found names, addresses, tax IDs, bank routing numbers and other PII/financial data. The exposure, discovered by researcher Jeremiah Fowler, was secured after disclosure—but it remains unclear how long the data was open or if malicious actors accessed it.

17.6 M Customers Impacted in Lending-Platform Breach

+Financial Services

- Peer-to-peer lender [Prosper Funding LLC](#) disclosed a breach affecting approximately 17.6 million individuals. The compromised data includes names, addresses, dates of birth, government IDs, email addresses, SSNs and browser details. While no direct account losses or fund thefts have been confirmed, the exposure significantly raises the risk of identity theft and phishing.

Auction House Discloses Breach of Customer Financial Info

+Retail

- [Sotheby's](#) revealed that a July intrusion had stolen certain customer data from its environment. Compromised details include full names, Social Security numbers and financial-account information, though the exact number of affected individuals is not yet public. The incident poses elevated fraud risks for high-net-worth clients and triggers regulatory, legal and reputational consequences.

Misconfigured Marketing Firm Database Leaks 40 Billion Records

+India +Marketing +eCommerce

- India-based marketing firm [NetcoreCloud](#) had an unprotected 13-terabyte database exposed online, allegedly containing ~40 billion records. The dataset included emails, IP addresses, banking notices, healthcare alerts, employment messages and partial account numbers. The firm reportedly locked it down after notification—but the length of exposure and any unauthorized access remain uncertain.

Nation-State Hackers Steal F5 Source Code, Trigger CISA Alert

+BIG-IP +China

- Cyber-attackers, allegedly linked to China, infiltrated [F5 Networks](#), gaining access to proprietary BIG-IP source-code and vulnerability intelligence. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive requiring federal agencies to patch affected devices, warning of an "imminent threat" to the over 260,000 exposed networks worldwide.

Regional Airline Carrier Hit in Oracle EBS Extortion Campaign

+Travel +Airlines +CI0p

- [Envoy Air](#), a regional carrier of American Airlines, confirmed a breach linked to exploitation of zero-day vulnerabilities in Oracle E-Business Suite software by the CI0p group. While no sensitive consumer data has been confirmed stolen, business and contact-list information were accessed. The campaign forms part of a wider wave of third-party software attacks that have hit numerous organizations globally.

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.