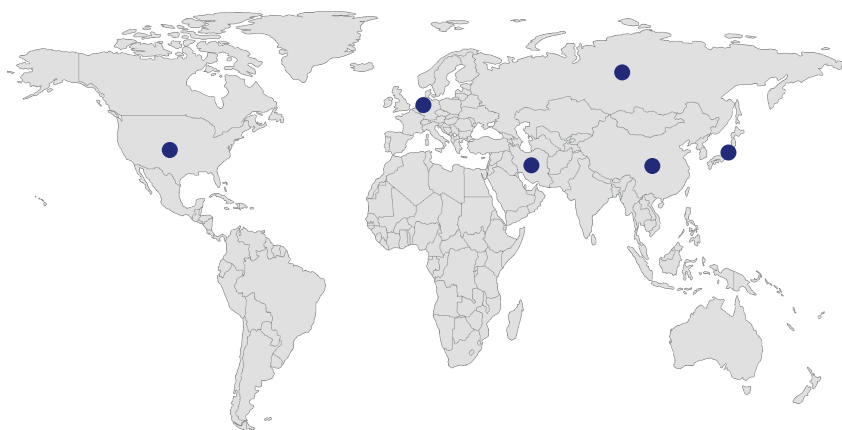


IMPERVA THREAT RESEARCH

Threat Intel Report: March 23-29, 2026

Countries



Top Tags

ClickFix

PyPI

CTRL

Handala

ShinyHunters

Executive Summary

Actionable Information:

- **Cloud and third-party infrastructure are primary entry points:** Attackers are increasingly targeting externally exposed systems, partner integrations, and cloud-hosted environments as lower-friction access points compared to core enterprise networks.
- **Social engineering continues to outperform technical exploitation:** Phishing, user-executed commands, and trusted-platform abuse are consistently enabling initial access, often bypassing traditional security controls without requiring vulnerabilities.
- **Developer and software supply chain ecosystems are increasingly targeted:** Adversaries are embedding malicious code into development workflows and open-source ecosystems, creating scalable opportunities for downstream compromise across multiple organizations.
- **Data exfiltration, not disruption, is the dominant objective:** The majority of activity centers on accessing and extracting sensitive data (e.g., credentials, communications, internal records), indicating a continued preference for intelligence gathering and monetization over operational impact.
- **AI is materially improving attack scale and efficiency:** Automation and AI-assisted tooling are enabling attackers to rapidly generate convincing lures, scale campaigns, and reduce the cost and effort required to execute attacks.
- **Financially motivated attacks remain high-impact and fast-moving:** Attacks against financial platforms are designed for immediate monetization, with rapid exploitation and fund movement reducing the window for detection and response.

Outlook:

The threat landscape continues to shift toward indirect compromise pathways, where attackers prioritize access through cloud services, third-party ecosystems, and user interaction rather than attempting to break hardened perimeter defenses. This reflects a broader evolution in enterprise architecture, where distributed systems and external dependencies expand the attack surface beyond

traditional network boundaries. Looking ahead, organizations should anticipate increased convergence between AI-enabled social engineering and supply chain compromise, particularly targeting identity systems and development environments as high-leverage entry points. Attack operations are becoming more efficient and scalable, relying on automation, trusted platforms, and human behavior exploitation rather than novel technical exploits. As a result, data theft will remain the primary objective, with attackers focusing on persistent, low-noise access to maximize intelligence collection and monetization opportunities.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 507% [CVE-2026-24423](#)

- SmarterTools SmarterMail versions prior to build 9511 contain an unauthenticated remote code execution vulnerability in the ConnectToHub API method. The attacker could point the SmarterMail to the malicious HTTP server, which serves the malicious OS command. This command will be executed by the vulnerable application.

↑ 243% [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.

↑ 189% [CVE-2025-53772](#)

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

Recent Cyber Threats

China-Aligned Clusters Expand Targeting Across Critical Sectors

+China +Government +Critical Infrastructure

- Researchers identified three distinct [China-linked threat clusters](#) conducting coordinated cyber espionage campaigns against government and critical infrastructure organizations worldwide. The groups leveraged overlapping tooling, including custom backdoors and living-off-the-land techniques, to maintain persistence and evade detection. Targeting focused on long-term intelligence collection rather than disruption, with victims spanning multiple regions and industries. The activity highlights continued strategic investment in cyber capabilities to support state-sponsored intelligence objectives.

Apple Moves to Disrupt ClickFix Social Engineering Chain

+ClickFix

- Apple introduced new macOS Terminal warnings designed to prevent [ClickFix](#) attacks, where users are tricked into pasting malicious commands into the terminal. These campaigns rely on social engineering prompts masquerading as fixes for system issues, ultimately executing attacker-controlled code. The update directly targets a growing initial access vector that bypasses traditional malware delivery mechanisms. This reflects a broader shift toward user-driven execution techniques that exploit trust rather than software vulnerabilities.

Malicious PyPI Package Hides Payloads in Audio Files

+PyPI

- A compromised PyPI package associated with [Telnyx](#) was found distributing malware concealed within WAV audio files to evade detection. Once installed, the package decoded and executed the hidden payload, enabling unauthorized access and potential data exfiltration. The campaign specifically targeted developers and environments that rely on open-source dependencies. This

demonstrates continued evolution of software supply chain attacks, with attackers leveraging steganography to bypass security tooling.

Fake GitHub VS Code Alerts Infect Developer Environments

+Malware +VSCode +GitHub

- Attackers used fraudulent [Visual Studio Code alerts](#) hosted on GitHub repositories to trick developers into downloading malicious payloads. The campaign mimicked legitimate development warnings, prompting users to install “fixes” that deployed malware on their systems. This approach capitalizes on developer trust in GitHub and common tooling, enabling initial access into development environments. The infections pose downstream risk, including potential compromise of source code and software supply chains.

Russian ‘CTRL’ Toolkit Delivered via Phishing Campaigns

+Russia +CTRL

- A Russia-linked threat actor deployed the [CTRL](#) malware toolkit through targeted phishing campaigns to compromise victim systems. The toolkit provides capabilities for command execution, persistence, and data exfiltration, enabling sustained access to infected environments. Delivery relied on weaponized documents and social engineering to lure victims into execution. The activity aligns with broader Russian cyber operations focused on intelligence gathering and long-term network access.

Data Breaches

Mazda Internal System Breach Exposes Partner Ecosystem Data

+Japan +Automotive

- [Mazda](#) disclosed a breach affecting 692 employees and business partners after attackers exploited vulnerabilities in an internal warehouse management system. Exposed data included names, email addresses, and internal identifiers tied to corporate operations. The compromise did not impact customer data but creates downstream risk for targeted phishing and business email compromise. The incident highlights continued attacker focus on enterprise operational systems rather than customer-facing platforms.

DeFi Platform Resolv Loses \$25M in Smart Contract Exploit

+Crypto +Financial Services

- Attackers breached the [Resolv](#) DeFi platform, stealing approximately \$25 million by exploiting vulnerabilities in its smart contract infrastructure. The attack enabled unauthorized withdrawals of digital assets, underscoring persistent weaknesses in decentralized finance protocols. Incidents like this continue to erode trust in DeFi platforms, where security audits often fail to prevent exploitation. The financial impact was immediate, with funds rapidly moved across blockchain networks to obscure tracing.

FBI Director’s Personal Email Compromised in Targeted Intrusion

+US +Iran +Government +Handala

- Hackers breached the personal email inbox of [FBI Director Kash Patel](#), exposing communications and documents from the account. Pro-Iranian group Handala claimed responsibility and reportedly made portions of the data publicly accessible. The incident demonstrates the continued targeting of personal accounts belonging to high-value government officials as a lower-barrier entry point. Such compromises present intelligence risks even when official systems remain secure.

AI-Driven Phishing Campaign Hits Hundreds via Railway Infrastructure

+AI +Transportation

- A large-scale phishing campaign leveraging AI tooling and [railway hosting infrastructure](#) compromised hundreds of organizations, using dynamically generated phishing pages and automation to scale credential harvesting operations across targets. The campaign highlights how AI lowers the barrier to producing convincing lures and rapidly iterating attack infrastructure. The widespread impact demonstrates increased efficiency and reach of modern phishing operations.

Dutch Police Systems Breached Through Phishing Attack

+Netherlands +Government

- [Dutch police](#) disclosed a security breach after attackers successfully executed a phishing campaign against internal users. The compromise resulted in unauthorized access to internal systems and potential exposure of employee data. Authorities have not disclosed full impact details but confirmed the attack originated through credential theft. The incident reinforces the continued effectiveness of phishing against government organizations despite security awareness efforts.

European Commission Platform Compromised via Cloud Intrusion

+EU +ShinyHunters +Government

- The [European Commission](#) reported a cyberattack involving unauthorized access to one of its web platforms hosted in cloud infrastructure, claimed by ShinyHunters. Initial findings indicate attackers gained entry to backend systems, raising concerns about potential data exposure and broader access risks. The breach highlights the expanding attack surface tied to cloud-hosted government services. Investigations are ongoing to determine scope and attribution.

CareCloud Breach Exposes Patient Data in Healthcare Incident

+Healthcare +US

- Healthcare technology provider [CareCloud](#) disclosed a breach in which attackers accessed and exfiltrated patient data from its systems. The compromised information includes sensitive healthcare-related records, raising risks of identity theft and fraud. The attack underscores the continued targeting of healthcare organizations due to the high value of medical data. Such incidents often lead to regulatory scrutiny and long-term reputational impact for affected providers.

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.