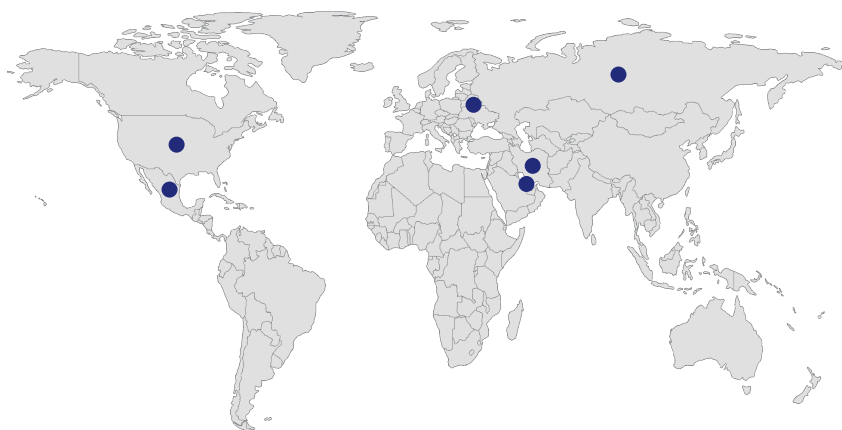


IMPERVA THREAT RESEARCH

Threat Intel Report: March 30-April 12, 2026

Countries



Top Tags

Masjesu

DDoS

SCADA

Handala

ShinyHunters

Executive Summary

Actionable Information:

- **DDoS attacks are both easier to launch and more operationally disruptive:** The continued growth of DDoS-for-hire services, combined with expanding IoT botnet capabilities, is lowering the barrier to entry while increasing the likelihood of widespread, multi-sector service disruption.
- **Critical infrastructure targeting is shifting toward disruption over access:** Adversaries are moving beyond reconnaissance and pre-positioning to actively interfere with industrial systems and government operations, signaling increased willingness to cause tangible operational impact.
- **Identity compromise remains the most reliable initial access vector:** Weak credential hygiene, social engineering, and infostealer data continue to provide attackers with consistent entry points, particularly across SaaS platforms and federated identity environments.
- **Supply chain dependencies are amplifying breach impact at scale:** Compromises within widely used libraries and third-party services are cascading across large ecosystems, allowing attackers to reach multiple organizations through a single point of failure.
- **AI is accelerating attacker capability and lowering skill requirements:** The use of commercial AI tools to assist with reconnaissance, exploit generation, and automation is enabling faster, more scalable attacks without requiring deep technical expertise.
- **Stolen data is increasingly leveraged for secondary attacks rather than immediate monetization:** Attackers are prioritizing the collection of contextual and behavioral data that can be reused in targeted phishing, fraud, and impersonation campaigns, extending the lifecycle and impact of breaches.

Outlook:

This week's activity reflects a clear shift toward asymmetric, efficiency-driven attack models, where attackers maximize impact while minimizing cost and effort. Application-layer DoS, AI-assisted intrusion workflows, and supply chain compromises all point to a landscape where traditional indicators of attack scale (bandwidth, sophistication, time investment) are becoming less relevant. At the same time, identity remains the weakest control plane, consistently bypassing hardened infrastructure through credential abuse and social engineering. Most notably, activity targeting critical infrastructure and government systems is trending toward operational impact, not just access or espionage, increasing the risk of disruptive or destructive events. Going forward, organizations should expect faster exploitation cycles, more indirect attack paths (via dependencies and SaaS), and increased blending of cybercrime and state-aligned tactics, particularly in sectors tied to public services, finance, and industrial operations.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

 31,543% [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.

 1,394% [CVE-2025-30208](#)

- Vite, a provider of frontend development tooling, has a vulnerability in versions prior to 6.2.3, 6.1.2, 6.0.12, 5.4.15, and 4.5.10. `@fs` denies access to files outside of Vite serving allow list. Adding `?raw??` or `?import&raw??` to the URL bypasses this limitation and returns the file content if it exists. This bypass exists because trailing separators such as `?` are removed in several places, but are not accounted for in query string regexes. The contents of arbitrary files can be returned to the browser.

 127% [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.

Recent Cyber Threats

Recursive Flight Bug Turns React Into a DoS Lever

+DoS

- Imperva's Threat Research team recently disclosed [CVE-2026-23869](#), a high-severity unauthenticated remote denial-of-service flaw in React Server Components. The issue sits in the Flight protocol's map/set deserialization logic, where crafted recursive references can force disproportionate computation; a single request can trigger work that lasts minutes, and repeated requests can cause full denial of service. The research found the payload becomes more effective than the earlier CVE-2026-23864 CPU-exhaustion issue after only a few kilobytes, and several orders of magnitude stronger at payloads in the hundreds of kilobytes. React fixed the issue in 19.2.5, and Imperva says versions 19.2.4 and below are affected.

Masjesu Quietly Scales a Telegram-Sold DDoS Service

+ [Masjesu](#) +[DDoS](#) +[synmaestro](#)

- [Masjesu](#) is a stealth-focused botnet marketed on Telegram as a DDoS-for-hire service since 2023. It targets a broad set of IoT routers and gateways across multiple architectures, while an observed later variant added 12 command-injection and code-execution exploits aimed at devices from vendors including D-Link, Huawei, NETGEAR, TP-Link, and others, plus new DDoS flood modules. The botnet also self-propagates by scanning random IPs for exposed services, including Realtek router infrastructure, and it appears built for longevity by avoiding blocklisted ranges such as U.S. Department of Defense IP space. The operation has previously been linked to an actor named “synmaestro.”

DDoS on Rostelecom Ripples Across Russian Essential Services

+[Russia](#) +[DDoS](#) +[Telecom](#)

- A large-scale DDoS attack on state-run carrier [Rostelecom](#) knocked parts of the internet offline in 30 Russian cities. The disruption spilled into internet access, government services, online banking, telecom operators, and satellite companies, leaving people unable to transfer money, withdraw cash, or make card payments for several hours; some impact was also reported in Belarus. Affected organizations included Alfa-Bank, Gosuslugi, Telecom T2, NTV Plus, Tricolor, and Mosenergosbyt, and some outages persisted into Tuesday after Rostelecom said the intrusion had been neutralized. Russia’s regulator recorded a jump from a normal average of 350 attacks per week to 949 during the February 26 to March 4 peak period.

Marimo Bug Was Weaponized Within Hours of Disclosure

+[CVE](#) +[Marimo](#)

- Attackers began exploiting [CVE-2026-39987](#) in Marimo less than 10 hours after disclosure. The flaw affects Marimo 0.20.4 and earlier and stems from the /terminal/ws WebSocket endpoint exposing an interactive terminal without authentication, giving remote attackers a shell with the same privileges as the Marimo process. 125 IPs were observed performing reconnaissance within the first 12 hours, followed by hands-on exploitation focused on stealing .env secrets, cloud credentials, and SSH-related data; the credential-access phase took less than three minutes. Marimo released version 0.23.0 to fix the issue and warned that editable notebooks exposed on shared networks are at particular risk.

Exposed U.S. PLCs Raise the Stakes in Iran-Linked OT Campaigns

+[Iran](#) +[US](#) +[PLC](#) +[SCADA](#)

- U.S. agencies warned that Iranian state-backed groups have targeted [Rockwell Automation/Allen-Bradley PLCs](#) since March 2026, causing operational disruption and financial losses. The FBI said the activity included extracting project files and manipulating HMI and SCADA displays, pointing to direct interference with industrial operations rather than simple reconnaissance. 5,219 internet-exposed Rockwell/Allen-Bradley hosts are exposed globally, with 74.6% of them, or 3,891 devices, located in the United States. Exposure is a major OT risk surface for U.S. critical infrastructure as Iran-linked activity escalates.

Data Breaches

Booking Platform Breach Fuels Targeted Travel Scam Risk

+[Travel](#)

- [Booking.com](#) disclosed that unauthorized third parties accessed customer reservation data after detecting suspicious activity tied to specific bookings. Exposed information includes names, email addresses, phone numbers, addresses, and booking details, though financial data was not accessed. The company reset reservation PINs and warned users about follow-on phishing and impersonation scams leveraging stolen travel data. The scale of impact remains undisclosed, but the incident reinforces ongoing targeting of travel platforms where contextual booking data enables highly convincing fraud.

Telehealth Breach Exploits SaaS Weak Point via Social Engineering

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

- [Hims & Hers](#) suffered a breach after attackers used a social engineering campaign to access a third-party customer support platform between February 4–7, 2026. The intrusion exposed customer support tickets containing names, contact details, and

limited treatment-related information, but did not impact medical records or provider communications. The attack leveraged compromised SSO credentials, highlighting SaaS and identity-layer weaknesses rather than software vulnerabilities. The company notified regulators and law enforcement and is offering credit monitoring, though the total number of affected users remains undisclosed.

Iran-Linked Handala Claims Destructive Breach of UAE Government Systems

+Iran +UAE +Handala +Government

- The Iran-linked hacktivist group [Handala](#) claims it breached three major UAE entities: Dubai Courts, Dubai Land Department, and Dubai Roads & Transport Authority. The group alleges it exfiltrated 149 TB of sensitive data and destroyed up to 6 petabytes of information, indicating a combined wiper and data-theft operation. Target selection suggests intent to disrupt civil governance and critical infrastructure rather than purely steal data. While claims remain unverified, the scale and destructive nature align with Handala's prior operations and broader Iran-linked cyber activity.

AI Supply Chain Attack Exposes Sensitive Data Across Mercor Ecosystem

+AI +LiteLLM

- AI startup [Mercor](#) confirmed it was impacted by a supply-chain attack on the widely used LiteLLM open-source library, where malicious code was briefly introduced to harvest credentials. The compromise potentially exposed sensitive contractor data, internal communications, and proprietary datasets used to train AI systems, with attackers claiming up to 4 TB of stolen data. The campaign affected thousands of organizations due to LiteLLM's widespread adoption, demonstrating how short-lived package compromises can cascade across ecosystems. The incident has already triggered operational fallout, including paused partnerships and lawsuits tied to exposed personal data.

ShinyHunters Targets Rockstar Again via Third-Party Cloud Breach

+ShinyHunters +Gaming

- [Rockstar Games](#) was targeted in a new breach attributed to the ShinyHunters group, which claims to have accessed company data via a third-party cloud provider. The attackers threatened to publish stolen data unless a ransom was paid, continuing a pattern of extortion-driven intrusions. Rockstar stated the breach involved only limited, non-critical internal information and had no operational impact, though the attackers claim otherwise. The incident marks another high-profile attack by ShinyHunters, known for breaching cloud storage environments and monetizing stolen data.

European Gym Giant Breach Exposes Financial Data at Scale

+Fitness

- [Basic-Fit](#) confirmed a cyberattack impacting approximately 1 million members across Europe, including 200,000 in the Netherlands alone. Attackers accessed a system used to track gym visits and exfiltrated sensitive data including names, addresses, contact details, dates of birth, and bank account information, though passwords and ID documents were not compromised. The breach was detected and stopped within minutes, but not before a significant volume of data was downloaded. The exposure of financial and personal data creates elevated risk of phishing and financial fraud targeting affected users.

Weak Password Hygiene Exposes Hundreds of Hungarian Government Accounts

+Hungary +Government

- An investigation uncovered nearly 800 [Hungarian government](#) email and password combinations circulating in breach datasets, affecting 12 of 13 ministries including defense, foreign affairs, and finance. Many credentials were exposed due to weak or reused passwords, often tied to third-party service breaches rather than direct intrusion. Some records date back years, but newer infostealer logs suggest ongoing compromise of government machines. The exposure includes sensitive roles tied to NATO and national security, highlighting systemic identity security failures across government infrastructure.

AI-Assisted Intrusion Compromises Multiple Mexican Government Agencies

+Mexico +AI +Government

- A single threat actor breached [nine Mexican government agencies](#) between December 2025 and February 2026, stealing hundreds of millions of citizen records. Researchers found the attacker leveraged commercial AI tools, including Claude and ChatGPT, to identify vulnerabilities, generate exploit code, and automate parts of the intrusion. The campaign demonstrates how AI can accelerate reconnaissance and exploitation, enabling large-scale breaches with reduced technical effort. The incident marks a shift toward AI-assisted offensive operations, lowering the barrier for high-impact attacks.

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.