

IMPERVA THREAT RESEARCH

Threat Intel Report: May 4-10, 2026

Countries



Top Tags

TrickMo

Cloudzy

Versatile Werewolf

ShinyHunters

MuddyWater

Executive Summary

Actionable Information:

- **Attackers are increasingly abusing trusted platforms and legitimate infrastructure to blend malicious activity into normal enterprise workflows.** Threat actors leveraged Microsoft Teams for malware delivery, GitHub repositories for malware distribution, Phone Link for SMS interception, and blockchain infrastructure for command-and-control communications, reflecting a broader shift away from traditional phishing infrastructure toward attacker-controlled use of legitimate services.
- **AI adoption is accelerating operational efficiency across the threat landscape, particularly for lower-sophistication actors.** Generative AI is being used to streamline exploit research, malware development, reconnaissance, and phishing operations, reducing technical barriers and enabling commodity threat actors to execute more advanced campaigns with greater speed and scale.
- **Software supply chain and developer ecosystem attacks continue to expand beyond enterprise software vendors into consumer and open-source distribution channels.** Compromised installers, trojanized repositories, and malicious developer tooling indicate attackers are prioritizing trusted software ecosystems to maximize infection scale and persistence while exploiting high levels of implicit user trust.
- **Application-layer vulnerabilities are being operationalized rapidly after disclosure, particularly within widely adopted web frameworks and centralized SaaS platforms.** Exploitation activity targeting React Server Components and the Canvas learning platform demonstrates how vulnerabilities in modern shared application ecosystems can quickly create large-scale disruption across thousands of downstream organizations.
- **Critical infrastructure and strategically significant sectors remain priority intelligence and intrusion targets.** Aviation firms, utility technology providers, laboratory testing organizations, and government-related voter systems were all targeted or

impacted this week, reflecting continued adversary focus on sectors tied to national security, operational resilience, and sensitive infrastructure data.

- **Account takeover activity is increasingly centered around bypassing MFA and exploiting identity synchronization workflows rather than direct credential theft alone.** SMS interception, linked-device abuse, and cross-platform identity tooling are becoming central components of financially motivated cybercrime operations seeking persistent access to user accounts.

Outlook:

This week's activity highlights a continued convergence between cybercrime, espionage, and operational disruption tactics, with attackers increasingly prioritizing stealth, scalability, and trusted-platform abuse over traditional malware delivery methods. Legitimate collaboration tools, developer ecosystems, decentralized infrastructure, and synchronization services are becoming core components of intrusion chains because they allow malicious activity to blend into normal enterprise traffic and reduce detection opportunities. At the same time, the rapid exploitation of newly disclosed vulnerabilities and supply chain compromises demonstrates that organizations continue to face shrinking response windows between disclosure and active targeting. The broader threat landscape also indicates that attackers are shifting toward ecosystem-level targeting rather than isolated victims. Campaigns affecting education platforms, software repositories, utility vendors, and infrastructure-adjacent providers show how compromising centralized technologies or trusted intermediaries can create downstream access into thousands of organizations simultaneously. Combined with AI-assisted operational acceleration and increasing focus on identity-based attacks, defenders should expect continued growth in campaigns that emphasize operational scale, indirect access paths, and abuse of legitimate enterprise services rather than overtly malicious infrastructure.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 1,911% [CVE-2026-42208](#)

- LiteLLM is a proxy server (AI Gateway) to call LLM APIs in OpenAI (or native) format. From version 1.81.16 to before version 1.83.7, a database query used during proxy API key checks mixed the caller-supplied key value into the query text instead of passing it as a separate parameter. An unauthenticated attacker could send a specially crafted Authorization header to any LLM API route (for example POST /chat/completions) and reach this query through the proxy's error-handling path. An attacker could read data from the proxy's database and may be able to modify it, leading to unauthorised access to the proxy and the credentials it manages.

↑ 526% [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.

↑ 344% [CVE-2026-39808](#)

- An improper neutralization of special elements used in an os command ('os command injection') vulnerability in Fortinet FortiSandbox 4.4.0 through 4.4.8 may allow attacker to execute unauthorized code or commands.

Recent Cyber Threats

React Components Crash Loops

+CVE +React

- Researchers disclosed [CVE-2026-23870](#), a critical denial-of-service vulnerability affecting React Server Components that could allow attackers to repeatedly crash or exhaust application resources through crafted requests. The flaw impacts applications using affected React and Next.js implementations, raising concerns for high-traffic consumer and enterprise platforms relying on server-side rendering. Imperva reported observing exploit attempts targeting exposed applications shortly after disclosure, highlighting the continued speed at which newly published web vulnerabilities are operationalized. The vulnerability underscores growing risk around modern JavaScript frameworks becoming high-value targets for application-layer disruption attacks.

AI-Assisted Exploit Development Expands

+AI +Malware

- Google's Threat Intelligence Group warned that threat actors are increasingly using [generative AI tools](#) to accelerate exploit research, malware development, phishing content creation, and vulnerability analysis. The report noted that while AI has not fundamentally changed attacker capabilities, it has reduced operational barriers and improved efficiency for both state-backed and financially motivated groups. Researchers observed actors leveraging AI to assist with scripting, reconnaissance, and adapting exploit chains tied to zero-day vulnerabilities. The findings reinforce concerns that commodity attackers can now execute more sophisticated campaigns with less technical expertise.

TrickMo Hides Traffic in TON Network

+TrickMo +Trojan

- The [TrickMo](#) Android banking trojan adopted The Open Network (TON) blockchain infrastructure to conceal command-and-control communications and improve resilience against disruption. Researchers found the malware leveraging decentralized blockchain-based messaging to receive operational commands, complicating traditional takedown and detection efforts. TrickMo continues targeting banking customers through credential theft, device compromise, and MFA interception capabilities. The campaign highlights how financially motivated malware operators are increasingly experimenting with decentralized infrastructure to evade security monitoring and law enforcement disruption.

JDownloader Supply Chain Compromise

+Malware +Trojan

- Attackers breached the [JDownloader](#) website and replaced legitimate installers with trojanized versions containing Python-based remote access malware. Users downloading the compromised installers unknowingly executed malware capable of remote command execution and persistent access on infected systems. The malicious installers remained available for several days before discovery and removal, potentially exposing a large number of users due to JDownloader's popularity. The incident reflects continued attacker focus on trusted software distribution channels to maximize malware delivery at scale.

Malicious OpenAI Repository Gains Traction

+AI +Malware

- A fake [GitHub repository](#) impersonating an OpenAI privacy-focused tool accumulated more than 1,000 stars while distributing hidden malware to developers. The repository used AI branding and privacy-themed messaging to build legitimacy and lure victims into downloading malicious payloads disguised as developer utilities. Researchers warned that attackers are increasingly exploiting interest in AI tooling and open-source ecosystems to distribute malware through seemingly legitimate repositories. The campaign demonstrates how trust in widely recognized AI brands is being weaponized for developer-focused social engineering attacks.

Phone Link Abuse Enables Account Takeovers

+Cloudzy +ATO +SMS Interception

- Researchers identified abuse of Microsoft's Phone Link application by the [Cloudzy](#) cybercrime operation to facilitate large-scale SMS interception and account takeover activity. The campaign exploited linked-device functionality to capture authentication messages and bypass multi-factor authentication protections tied to victim accounts. Investigators tied the activity to infrastructure associated with mobile proxy and cybercrime services previously linked to Cloudzy. The abuse highlights growing attacker focus on legitimate cross-device synchronization tools as a method for credential theft and identity compromise.

Data Breaches

Aviation Contractors Targeted for Strategic Mapping Data

+Aviation +GPS +Versatile Werewolf

- Researchers uncovered a cyber-espionage campaign targeting [aviation and aerospace organizations](#) to steal sensitive geographic and mapping data tied to flight operations and infrastructure. The attackers, tracked as Versatile Werewolf, reportedly focused on firms involved in aeronautical charting and navigation technologies, suggesting intelligence-gathering objectives rather than immediate financial gain. Analysts believe the stolen datasets could support military planning, surveillance operations, or future targeting activity. The campaign reflects continued interest by advanced persistent threat actors in transportation and aviation ecosystems with national security relevance.

Canadian Voter Records Leak Fuels Political Tensions

+Canada +Government +Voting

- Officials in [Alberta](#) disclosed a voter data breach affecting individuals connected to a separatist referendum initiative, exposing personal information tied to political organizing efforts. The compromised data reportedly included names, addresses, and voter registration-related records collected during petition activities. The incident intensified political tensions surrounding the referendum movement and raised concerns about the protection of politically sensitive datasets. The breach highlights growing risks around election-related data collection outside traditional government election infrastructure.

Canvas Portal Defacements Spread Across Schools

+ShinyHunters +Education

- [Instructure](#) confirmed attackers exploited a vulnerability in the Canvas learning platform to deface portals used by schools and universities. The activity impacted educational institutions during a critical academic period, with attackers replacing portal content and disrupting access for students and faculty. Researchers linked the broader campaign to ongoing ShinyHunters-associated extortion and intrusion activity targeting educational organizations. The attacks demonstrated how centralized education technology platforms can create large-scale operational disruption across thousands of institutions simultaneously.

Retail Customer Records Exposed in Zara Incident

+Retail

- Fashion retailer [Zara](#) disclosed a data breach affecting approximately 197,000 individuals after unauthorized access exposed customer personal information. Exposed data reportedly included contact details and order-related information, though payment card data was not believed to be impacted. The breach adds to ongoing targeting of global retail brands holding large volumes of consumer and loyalty-program data. Researchers noted that retail organizations remain attractive targets due to the combination of customer data, transaction systems, and seasonal operational pressure.

MuddyWater Turns Teams Into Initial Access Channel

+Iran +MuddyWater +Malware

- Iran-linked threat actor [MuddyWater](#) was observed using Microsoft Teams messages to deliver malware and establish initial access into targeted environments. The campaign leveraged impersonation tactics and direct communication through trusted enterprise collaboration tools to bypass traditional phishing defenses. Researchers said the operation targeted organizations across government, telecom, and infrastructure sectors, continuing MuddyWater's long-running espionage-focused activity. The campaign highlights growing abuse of legitimate workplace collaboration platforms as attacker-controlled intrusion channels.

Australian Testing Giant Restores Systems After Cyber Incident

+Australia +Scientific

- [ALS Limited](#), a major Australian laboratory and scientific testing company, restored most services after a cyber incident disrupted operations and affected portions of its data environment. The company said investigations were ongoing to determine the scope of impacted information and whether customer data had been compromised. ALS supports industries including pharmaceuticals, food safety, mining, and environmental testing, making the incident significant from a broader supply-chain resilience perspective. The disruption demonstrates how attacks against laboratory and testing providers can create downstream operational risk across multiple critical industries.

Utility Vendor Breach Raises Infrastructure Access Concerns

+US +Utilities

- Hackers breached utility technology provider [Itron](#) and gained access to systems connected to critical infrastructure operators, raising concerns about downstream exposure across the energy sector. Itron provides smart grid, metering, and utility management technologies used by energy providers globally, giving attackers potential visibility into operational environments and customer networks. Investigators stated there was no evidence of disruption to utility operations, but the breach highlighted risks associated with trusted vendor access into critical infrastructure ecosystems. The incident reinforces ongoing concerns around third-party compromise as a pathway into operational technology and utility environments.

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.