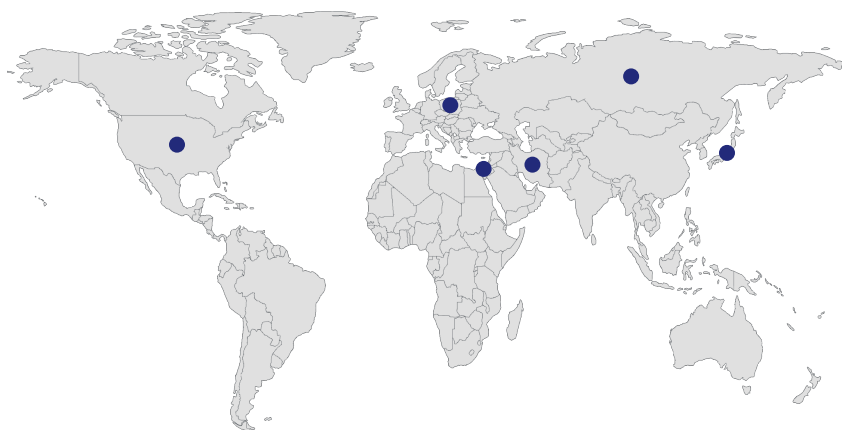


IMPERVA THREAT RESEARCH

# Threat Intel Report: May 11-17, 2026

## Countries



## Top Tags

Static Tundra

Nitrogen

ALPHV

ShinyHunters

## Executive Summary

### Actionable Information:

- **AI ecosystems are rapidly becoming operational attack surfaces rather than isolated developer tooling.** Recent activity showed attackers targeting AI workflow infrastructure, developer frameworks, and package ecosystems simultaneously through sandbox escapes, cross-tenant exposure, malicious dependency distribution, and token theft. The convergence of AI orchestration platforms with CI/CD pipelines and cloud-native development environments is creating highly interconnected attack paths where compromise of a single component can expose source code, credentials, or downstream enterprise systems.
- **Critical infrastructure targeting continues shifting toward disruption and psychological impact over pure destruction.** Activity linked to Russian and Iranian state-aligned actors focused on fuel distribution, energy production, and civilian morale operations, demonstrating sustained interest in generating economic pressure and public uncertainty through cyber operations. Notably, several campaigns relied on exposed remote-access systems, operational technology weaknesses, and information operations rather than advanced zero-day exploitation, reinforcing that basic segmentation and access control failures remain high-impact national security risks.
- **Software supply chain and developer-environment compromises remain one of the highest-leverage attack vectors.** Incidents involving TanStack, Grafana, and Foxconn illustrate how attackers increasingly prioritize trusted development ecosystems, GitHub environments, manufacturing partners, and package repositories to maximize downstream impact. Stolen tokens, compromised dependencies, and third-party vendor breaches allow threat actors to reach thousands of organizations indirectly while avoiding direct perimeter defenses. This trend continues to blur distinctions between traditional data breaches, supply-chain attacks, and extortion operations.
- **Identity-rich datasets and biometric information are becoming central extortion and fraud targets.** Healthcare, hospitality, and retail breaches exposed medical records, fingerprints, passports, driver's licenses, and customer CRM data, reflecting growing

attacker interest in long-lived identity data that supports fraud, impersonation, and secondary phishing operations. Several incidents also reinforced the shift from encryption-based ransomware toward pure data theft and extortion, where attackers reduce operational complexity while maintaining monetization opportunities through leaks, resale, and public pressure campaigns.

## Outlook:

This week's activity highlights a broader transition toward ecosystem-centric cyber operations, where attackers increasingly target the connective tissue between organizations rather than isolated endpoints. AI development platforms, CI/CD environments, cloud storage, manufacturing partners, and operational technology networks are all being treated as scalable access layers capable of producing downstream compromise across multiple industries simultaneously. At the same time, nation-state and financially motivated actors continue converging around similar operational goals: maximizing disruption, public pressure, and long-term leverage through data theft, supply chain compromise, and critical infrastructure targeting. Organizations should expect continued growth in attacks against trusted third-party environments, identity repositories, and AI-integrated applications, particularly as threat actors capitalize on weak segmentation, overprivileged development systems, and rapidly deployed AI tooling that often matures faster than its security controls.

---

## Threat Activity in Imperva

### Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 814% [CVE-2025-55752](#)

- Relative Path Traversal vulnerability in Apache Tomcat. The fix for bug 60013 introduced a regression where the rewritten URL was normalized before it was decoded. This introduced the possibility that, for rewrite rules that rewrite query parameters to the URL, an attacker could manipulate the request URI to bypass security constraints including the protection for /WEB-INF/ and /META-INF/. If PUT requests were also enabled then malicious files could be uploaded leading to remote code execution. PUT requests are normally limited to trusted users and it is considered unlikely that PUT requests would be enabled in conjunction with a rewrite that manipulated the URI.

↑ 524% [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. Only apps explicitly exposing the Vite dev server to the network (using `--host`` or `server.host`` config option) are affected.

↑ 63% [CVE-2025-8085](#)

- The Ditty WordPress plugin before 3.1.58 lacks authorization and authentication for requests to its `displayItems` endpoint, allowing unauthenticated visitors to make requests to arbitrary URLs.

---

## Recent Cyber Threats

### Dify Bugs Enable Account Takeover and Cross-Tenant Code Exposure

+AI +ATO

- Imperva researchers disclosed two vulnerabilities in [Dify](#): a file-handling flaw enabling one-click account takeover and a sandbox isolation weakness that could expose other tenants' application source code. In the first issue, malicious SVG files uploaded through workflow tool nodes could execute JavaScript from Dify's trusted application origin because [upload.dify.ai](#) and [cloud.dify.ai](#) shared the same origin boundary. The second issue affected [dify-sandbox](#), where Python executions shared filesystem paths and a static runtime identity, allowing attackers to sample temporary wrapper files from other tenants and recover encrypted source code using weaknesses in the repeating-key XOR scheme. Dify patched the issues in versions 1.13.1 and 1.13.3, though Imperva said the vendor patched silently and did not respond to disclosure messages.

### 18-Year-Old NGINX Flaw Revives RCE Concerns

+RCE +DoS

- Security researchers disclosed [CVE-2026-42945](#), a critical heap-based buffer overflow vulnerability affecting NGINX Open Source and NGINX Plus deployments dating back nearly two decades. The flaw exists in the `ngx_http_rewrite_module` and can be exploited through crafted HTTP requests under specific rewrite configurations, potentially enabling denial-of-service conditions or remote code execution where protections such as ASLR are disabled. Because NGINX powers a substantial portion of internet-facing infrastructure, the vulnerability carries broad exposure across enterprise and cloud environments. Imperva customers are protected out of the box.

### Polish Energy Sector Hit in Coordinated Destructive Campaign

+Poland +Russia +Government +Utilities +Static Tundra

- [CERT Polska](#) detailed coordinated cyberattacks conducted against more than 30 wind and photovoltaic farms, a manufacturing company, and a major combined heat and power plant in late December 2025. The attacks attempted to disrupt industrial operations and remote management systems, with investigators linking activity to destructive tactics associated with Russian state-aligned threat groups. Reporting indicated attackers leveraged exposed infrastructure and weak remote-access security controls rather than novel zero-days, highlighting persistent operational technology security gaps. Although power generation continued, the incident marked one of the most significant destructive cyber campaigns targeting Polish critical infrastructure to date.

### OpenAI Responds After AI Ecosystem Supply Chain Breach

+AI +Supply Chain

- [OpenAI](#) addressed concerns tied to the compromise of the TanStack ecosystem after attackers reportedly leveraged the software supply chain to distribute malicious packages affecting developers and downstream users. The incident renewed concerns around the growing intersection of AI tooling, developer frameworks, and package repository trust, where a single compromised dependency can rapidly propagate across thousands of environments. Researchers noted that threat actors increasingly target developer ecosystems supporting AI and modern web applications due to their broad downstream reach. The attack reflects continued evolution of software supply chain operations from niche intrusions into scalable ecosystem-level compromises.

### Iran-Linked Intrusions Target U.S. Fuel Operations

+Iran +US +Automotive

- U.S. officials and researchers believe Iran-linked hackers were connected to cyber activity affecting [gas station operations](#) across multiple states, disrupting payment systems and fuel availability at some locations. The incidents followed a broader pattern of escalating cyber tensions involving Iranian actors targeting operational technology and critical infrastructure sectors. Analysts warned that even limited disruptions against fuel distribution networks can create outsized public impact due to supply-chain dependencies and consumer panic buying. The activity reflects continued interest by state-aligned groups in targeting civilian infrastructure for psychological and economic pressure rather than purely destructive effects.

## Psychological Cyber Campaign Targets Israeli Civilians

+Iran +Israel

- Iranian-linked operators reportedly conducted a personalized [cyber-enabled influence campaign](#) targeting Israeli civilians with tailored intimidation and morale-focused messaging. The operation blended cyber intrusion techniques with psychological operations, using personal information and direct communications to amplify fear and uncertainty during ongoing regional tensions. Researchers noted that these campaigns increasingly blur the line between cyberattacks and influence operations, prioritizing psychological disruption over technical destruction. The activity demonstrates how state-linked actors are integrating cyber capabilities into broader information warfare strategies aimed at civilian populations.

---

## Data Breaches

### Supply Chain Giant Faces Multi-Terabyte Extortion Threat

+Nitrogen +US +ALPHV

- [Foxconn](#) confirmed a cyberattack affecting several North American factories after the Nitrogen ransomware group claimed to have stolen roughly 8TB of sensitive data. The attackers alleged the breach included schematics and project information tied to major technology customers including Apple, Google, Dell, and Nvidia, highlighting the downstream impact a compromise of a manufacturing partner can create. Foxconn stated affected facilities were resuming operations, but the incident reinforces how ransomware groups increasingly target organizations positioned deep within global supply chains. Researchers also noted Nitrogen has links to the ALPHV/BlackCat ecosystem and has historically focused on manufacturing and technology victims.

### Grafana Rejects Extortion After GitHub Environment Breach

+GitHub

- [Grafana](#) disclosed that attackers obtained a GitHub token that allowed unauthorized access to the company's GitHub environment and enabled downloads of portions of its codebase. The threat actors reportedly attempted to extort the company following the intrusion, though Grafana stated there was no evidence customer environments or hosted services were compromised. The incident highlights growing attacker focus on developer infrastructure, where stolen tokens and CI/CD access can expose proprietary code and create opportunities for downstream supply-chain abuse. Security researchers warned that developer platforms continue to represent high-value targets because a single credential compromise can provide broad internal visibility.

### Massive NYC Healthcare Breach Exposes Biometric Data

+US +Healthcare +Biometric

- [NYC Health + Hospitals](#) disclosed that hackers accessed and copied sensitive patient and employee information affecting at least 1.8 million individuals after maintaining access to systems for several months. Exposed information reportedly included medical records, Social Security numbers, insurance data, and biometric information such as fingerprints, significantly increasing long-term identity and fraud risks for victims. Investigators determined attackers had access to portions of the network between late 2025 and February 2026 before suspicious activity was detected. The breach underscores continued targeting of healthcare organizations, where large concentrations of sensitive identity and medical data make institutions attractive ransomware and extortion targets.

### ShinyHunters Expands Retail Data Leak Campaign

+ShinyHunters +Salesforce +Retail

- [7-Eleven](#) confirmed a data breach after the ShinyHunters group claimed it stole more than 600,000 Salesforce records containing personal and corporate information. The attackers initially threatened to release the stolen data unless a ransom was paid before later attempting to sell the dataset on cybercriminal forums for approximately \$250,000. Researchers noted the campaign reflects ShinyHunters' continued shift away from disruptive encryption operations toward pure data theft and extortion, a model that lowers operational risk while maximizing monetization opportunities. The incident adds another major retail brand to a broader wave of mass data exposure campaigns tied to the group in recent months.

## Misconfigured Hotel Platform Exposes Over 1 Million IDs

+Japan +Hospitality

- Researchers discovered that a publicly accessible Amazon cloud storage bucket tied to the Japanese hotel [Tabiq's](#) check-in platform exposed more than one million sensitive identity documents and selfie verification images. The exposed data reportedly included passports, driver's licenses, and facial verification photos collected from guests using automated hotel check-in systems across Japan. The incident was attributed to a cloud misconfiguration rather than an active intrusion, but security experts warned the exposed biometric and identity data could facilitate fraud, impersonation, and targeted phishing campaigns. The breach highlights the growing security risks associated with hospitality-sector identity automation and facial recognition platforms.

---

## 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.