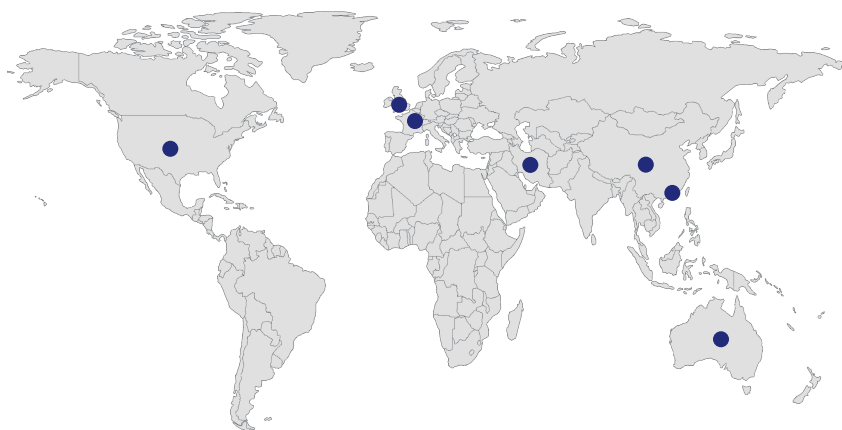


IMPERVA THREAT RESEARCH

Threat Intel Report: June 8-14, 2026

Countries



Top Tags

ShinyHunters

JDY

Volt Typhoon

AudiA6

Handala

Executive Summary

Actionable Information:

- **Enterprise access platforms remain the week's highest-priority exposure point.** Threat actors exploited or targeted Oracle PeopleSoft, ServiceNow, Check Point VPN, and other high-trust enterprise systems that sit close to identity, workflow, remote access, and administrative operations. These platforms often contain sensitive business data while also providing privileged paths into enterprise environments, making them attractive both for ransomware affiliates and data-extortion groups.
- **Financially motivated actors are increasingly combining zero-day exploitation with extortion.** ShinyHunters' exploitation of Oracle PeopleSoft before public disclosure, followed by reported leak threats, demonstrates a continued shift from opportunistic credential theft toward faster operationalization of critical enterprise flaws. This pattern raises the risk that organizations may face extortion pressure before standard patch-management cycles can begin, especially when exposed systems are tied to universities, business applications, or large identity datasets.
- **Nation-state and hacktivist activity continues focusing on reconnaissance, critical infrastructure, and public-pressure operations.** China-linked JDY activity shows long-term use of compromised SOHO and IoT devices to map exposed services and prepare future operations, while Iran-linked Handala's claimed Cal Water intrusion blended data theft with retaliatory messaging against a U.S. utility. These cases show that strategic cyber activity is increasingly aimed at persistence, visibility, and psychological leverage, not only immediate disruption.
- **Third-party platforms and account compromise remain central breach drivers.** The SoFi Hong Kong, Oxford CareerConnect, and Tchao incidents show how attackers can expose sensitive data by compromising vendors, platform providers, or individual accounts rather than breaking core infrastructure directly. Organizations relying on SaaS, education platforms, secure messaging tools, and fintech vendors should prioritize vendor access reviews, segmentation, SSO enforcement, and monitoring for anomalous queries or account activity.

Outlook:

This week's activity points to a continued convergence of ransomware, data-extortion, state-aligned reconnaissance, and hacktivist operations around the same core targets: exposed enterprise platforms, remote-access systems, third-party services, and identity-rich repositories. Attackers are moving quickly from vulnerability discovery to exploitation, while also using stolen data and public claims to generate pressure even when operational impact remains unverified. Critical infrastructure and public-sector-adjacent organizations should expect continued targeting from both nation-state and ideologically motivated actors, particularly where compromise can create symbolic or psychological effects. Across sectors, the most important defensive priority is reducing exposure across trusted systems, like SaaS platforms, VPNs, enterprise applications, vendors, and privileged accounts, because these environments increasingly provide attackers with the fastest path to both access and leverage.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

 1,458% [CVE-2025-5394](#)

- The Alone – Charity Multipurpose Non-profit WordPress Theme theme for WordPress is vulnerable to arbitrary file uploads due to a missing capability check on the `alone_import_pack_install_plugin()` function in all versions up to, and including, 7.8.3. This makes it possible for unauthenticated attackers to upload zip files containing webshells disguised as plugins from remote locations to achieve remote code execution. CVE-2025-54019 is likely a duplicate of this.

 647% [CVE-2026-42271](#)

- LiteLLM is a proxy server (AI Gateway) to call LLM APIs in OpenAI (or native) format. From version 1.74.2 to before version 1.83.7, two endpoints used to preview an MCP server before saving it — `POST /mcp-rest/test/connection` and `POST /mcp-rest/test/tools/list` — accepted a full server configuration in the request body, including the `command`, `args`, and `env` fields used by the stdio transport. When called with a stdio configuration, the endpoints attempted to connect, which spawned the supplied command as a subprocess on the proxy host with the privileges of the proxy process. The endpoints were gated only by a valid proxy API key, with no role check. Any authenticated user — including holders of low-privilege internal-user keys — could therefore run arbitrary commands on the host. This issue has been patched in version 1.83.7.

 325% [CVE-2025-59718](#)

- A improper verification of cryptographic signature vulnerability in Fortinet FortiOS 7.6.0 through 7.6.3, FortiOS 7.4.0 through 7.4.8, FortiOS 7.2.0 through 7.2.11, FortiOS 7.0.0 through 7.0.17, FortiProxy 7.6.0 through 7.6.3, FortiProxy 7.4.0 through 7.4.10, FortiProxy 7.2.0 through 7.2.14, FortiProxy 7.0.0 through 7.0.21, FortiSwitchManager 7.2.0 through 7.2.6, FortiSwitchManager 7.0.0 through 7.0.5 allows an unauthenticated attacker to bypass the FortiCloud SSO login authentication via a crafted SAML response message.

Recent Cyber Threats

Oracle PeopleSoft Zero-Day Exploited by ShinyHunters

+[ShinyHunters](#) +[RCE](#)

- ShinyHunters exploited [CVE-2026-35273](#), a critical unauthenticated RCE vulnerability in Oracle PeopleSoft Enterprise PeopleTools, before Oracle issued its June 10 advisory. Mandiant tracked exploitation between May 27 and June 9, making the

bug a zero-day during the observed campaign. Attackers reportedly targeted PeopleSoft Environment Management Hub exposure, with more than 100 organizations alerted and higher education making up 68% of potentially vulnerable endpoints identified by Google. Victims reportedly received extortion demands threatening to leak stolen data unless payment was made.

ServiceNow Flaw Exploited Against Customer Instances

+Australia

- [ServiceNow](#) warned that unknown actors exploited a security issue that allowed unauthenticated users, under certain circumstances, to gain more access to customer instances than intended. The company applied a security update to hosted instances on June 5 and said anomalous activity began June 2, with evidence of successful table queries against a subset of customers. The issue affected customers on the Australia platform release or customers with certain configuration changes on earlier releases. The incident highlights continued attacker focus on enterprise SaaS platforms that contain high-value workflow, ticketing, HR, IT, and business data.

Check Point VPN Zero-Day Linked to Ransomware Activity

+Ransomware +VPN

- [Check Point](#) warned that a vulnerability affecting Remote Access VPN and Mobile Access deployments had been exploited since early May and was tied to ransomware activity. The flaw was targeted by a ransomware affiliate, reinforcing continued attacker interest in VPN infrastructure as an initial-access vector. Edge-access systems remain especially high risk because successful exploitation can bypass normal perimeter controls and place attackers directly inside enterprise networks. The activity follows a broader pattern of ransomware groups rapidly operationalizing VPN and security-appliance flaws once reliable access paths emerge.

China-Linked JDY Botnet Expands Reconnaissance Network

+China +JDY +Volt Typhoon

- Black Lotus Labs reported a resurgence of [JDY](#), a covert botnet associated with China-nexus state-sponsored activity. The network now includes more than 1,500 compromised SOHO and IoT devices and functions as a centrally controlled scanner for discovering, fingerprinting, and continuously mapping exposed services at scale. JDY was first identified as a cluster within the KV-botnet ecosystem in December 2023 and has been linked to Chinese groups including Volt Typhoon. The activity underscores the strategic value of compromised edge devices for stealthy reconnaissance and long-term operational preparation.

AudiA6 Crypto Laundering Service Disrupted by Europol

+Europe +AudiA6

- European authorities disrupted [AudiA6](#), a cryptocurrency laundering service used by ransomware groups and cybercriminal networks to cash out stolen digital assets. Europol said the platform laundered more than €336 million since launching in 2021 and also linked its operators to Dark2Web, a dark web cybercrime forum. The June 10 operation included two arrests in Georgia, three property searches, takedown of 25 domains, seizure of more than 30 servers, freezing of €692,000 in crypto assets, and seizure of €86,000 in cryptocurrency. The operation targeted ransomware monetization infrastructure rather than a single malware family.

Data Breaches

Cal Water Hack Claimed by Iran-Linked Handala

+Iran +Handala +US +Utilities

- Iran-linked group [Handala](#) claimed it hacked California Water Service and published 5 GB of allegedly stolen data. The leak included customer personal information and credentials for the RTKBase platform. The group framed the intrusion as retaliation for recent U.S. actions in Iran and claimed it could have disrupted water access but chose not to. Even if operational disruption is unverified, the incident is significant because it blends data theft, hacktivist messaging, and claimed access to a U.S. water utility.

University of Nottingham Breach Exposes Student and Alumni Data

+UK +Education +ShinyHunters

- The [University of Nottingham](#) confirmed that attackers accessed its Campus Solutions student records system, affecting current students and alumni. ShinyHunters claimed responsibility and leaked more than 450,000 email addresses and other information, while other reporting said exposed data included contact details, National Insurance numbers, protected characteristics, course information, student and staff IDs, and financial records. The university took the system offline and launched a forensic investigation with external experts, Action Fraud, the ICO, and regulators. The breach adds to sustained targeting of higher education institutions with large identity datasets and complex third-party technology environments.

French Government Tchap Messaging Platform Breached

+France +Government +misere

- France's interministerial digital directorate DINUM disclosed that [Tchap](#), the French government's secure messaging platform, was breached after attackers used a compromised account to access public chat rooms. Reporting said more than 73,000 government accounts were affected, while a threat actor calling itself "misere" claimed to have stolen 13.5 GB of data, including more than 640,000 messages, nearly 60,000 media files, and data from 876 chat rooms. ANSSI detected the intrusion, and private conversations were reportedly encrypted while public rooms were exposed. The breach shows how even sovereign government communication platforms can be compromised through account hijacking rather than a break in core cryptography.

SoFi Hong Kong Confirms Third-Party Data Breach

+Hong Kong +Financial Services

- [SoFi Hong Kong](#) warned customers that attackers accessed a database at a third-party vendor containing customer information. The company detected the incident on April 30 after unauthorized access to a SoFi Securities Hong Kong database through one of its vendors and engaged a third-party cybersecurity firm to respond. SoFi said the investigation was ongoing and that it did not yet have complete information about the scope, impact, or categories of personal data involved. The incident reinforces third-party risk in fintech and securities environments where vendors may hold regulated customer data.

Oxford University Discloses CareerConnect Platform Breach

+UK +Education

- The [University of Oxford](#) disclosed a breach after third-party provider Group GTI informed it that the CareerConnect careers platform had been compromised. Attackers accessed users' first names, last names, email addresses, and encrypted passwords for users who do not authenticate with SSO, including alumni, research staff, and employer users. Oxford said passwords were invalidated by GTI and affected users would be required to reset them on next login. The platform is also used by other UK education organizations, including King's College London and the University of Manchester, raising broader third-party exposure concerns.

Novo Nordisk Reports Clinical Trial Patient Data Breach

+Healthcare +Pharma

- [Novo Nordisk](#) disclosed unauthorized access to limited patient data from certain clinical trials. Copied data may include patient ID, birth year, sex, and health or immunogenicity details, but not names or direct identifiers. The company brought in external cybersecurity experts, coordinated with authorities, temporarily shut down some internal IT systems, and said core operations continued. The breach is significant because even pseudonymized clinical trial data can carry regulatory and trust implications for pharmaceutical research 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.