

IMPERVA THREAT RESEARCH

Threat Intel Report: June 15-21, 2026

Countries



Top Tags

FortiBleed

SocGholish

DragonForce

FulcrumSec

ShinyHunters

Executive Summary

Actionable Information:

- **Credential theft is increasingly concentrated around high-trust access points.** FortiBleed, malicious JetBrains plugins, Mastra AI package compromise, and ROKAROLLA all show attackers prioritizing credentials that unlock downstream access: firewall/VPN logins, AI API keys, npm maintainer accounts, banking credentials, crypto wallets, and mobile app sessions. Defenders should treat credential exposure as an infrastructure-level risk rather than a user-level incident, especially when stolen secrets provide access to edge devices, developer environments, cloud services, or financial systems.
- **Trusted infrastructure continues to be abused for stealth and persistence.** DragonForce's use of Microsoft Teams relays for C2, SocGholish's long-running WordPress infection network, and third-party business application breaches show attackers increasingly hiding inside legitimate services, vendor platforms, and commonly allowed traffic. This reduces the effectiveness of blocklist-based controls and raises the importance of behavioral detection, token monitoring, outbound traffic analysis, and vendor integration auditing.
- **Developer and AI ecosystems remain priority targets for supply-chain compromise.** North Korea-linked actors compromised more than 140 Mastra AI npm packages, while malicious JetBrains plugins targeted AI service keys directly. These incidents show that AI development workflows are becoming a high-value extension of the software supply chain, where a single compromised maintainer, plugin, or API token can expose code, credentials, model access, and cloud resources.
- **Extortion groups are targeting data with operational, regulatory, and reputational leverage.** Novo Nordisk, iRhythm, Klue, Nintendo, Kodak, and the Council of Europe incidents all centered on stolen data rather than confirmed operational disruption. The most sensitive exposures involved healthcare data, Salesforce/OAuth-connected business records, employee survey data, intellectual property, HR/payroll files, and intergovernmental documents, reflecting attacker interest in datasets that create maximum pressure through legal, privacy, commercial, and public-trust consequences.

Outlook:

This week's activity points to continued convergence between credential theft, supply-chain compromise, and data extortion. Attackers are increasingly targeting the systems that sit between organizations and their most valuable assets: VPNs and firewalls for access, developer tools and package ecosystems for propagation, AI services for monetizable credentials, and third-party SaaS platforms for concentrated business data. Nation-state and criminal actors alike are expanding across operating systems, mobile devices, cloud services, and vendor environments, making traditional perimeter-centric defense less effective. Organizations should expect continued attacks against trusted platforms and integrations, with the highest near-term risk concentrated in exposed edge devices, developer credentials, SaaS OAuth connections, and third-party-hosted business applications.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 4,247% [CVE-2025-34028](#)

- The Commvault Command Center Innovation Release allows an unauthenticated actor to upload ZIP files that represent install packages that, when expanded by the target server, are vulnerable to path traversal vulnerability that can result in Remote Code Execution via malicious JSP. This issue affects Command Center Innovation Release: 11.38.0 to 11.38.20. The vulnerability is fixed in 11.38.20 with SP38-CU20-433 and SP38-CU20-436 and also fixed in 11.38.25 with SP38-CU25-434 and SP38-CU25-438.

↑ 3,291% [CVE-2025-8943](#)

- The Custom MCPs feature is designed to execute OS commands, for instance, using tools like `npx` to spin up local MCP Servers. However, Flowise's inherent authentication and authorization model is minimal and lacks role-based access controls (RBAC). Furthermore, in Flowise versions before 3.0.1 the default installation operates without authentication unless explicitly configured. This combination allows unauthenticated network attackers to execute unsandboxed OS commands.

↑ 1,073% [CVE-2026-22610](#)

- Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to versions 19.2.18, 20.3.16, 21.0.7, and 21.1.0-rc.0, a cross-site scripting (XSS) vulnerability has been identified in the Angular Template Compiler. The vulnerability exists because Angular's internal sanitization schema fails to recognize the href and xlink:href attributes of SVG <script> elements as a Resource URL context. This issue has been patched in versions 19.2.18, 20.3.16, 21.0.7, and 21.1.0-rc.0.

Recent Cyber Threats

FortiBleed Exposes 86,644 Fortinet Firewall and VPN Credentials

+FortiBleed +Credential Theft

- CISA urged Fortinet customers to harden internet-exposed FortiGate appliances after the [FortiBleed](#) campaign produced a verified database of 86,644 working credentials across 194 countries. Generic admin accounts made up 35% of exposed credentials, built-in Fortinet system accounts made up 28.3%, and organization-specific accounts accounted for 36.7%. Researchers said the campaign involved roughly 1.16 billion credential attempts against more than 320,000 FortiGate targets, with telecom, government, and education among the most impacted sectors.

SocGhosh Botnet Disrupted; Nearly 15,000 WordPress Sites Cleaned

+SocGholish +WordPress +Netherlands +Canada +US +Germany

- Law enforcement agencies in the Netherlands, Canada, the U.S., and Germany, with Europol support, disrupted [SocGholish](#) infrastructure and removed malware from 14,971 infected WordPress sites. Authorities also took down 106 command-and-control servers and domains linked to the operation. SocGholish, also known as FakeUpdates, has operated since 2017 as a JavaScript-based loader used for drive-by malware delivery, including ransomware, banking trojans, spyware, AsyncRAT, NetSupport RAT, LockBit, and RansomHub.

DragonForce Abuses Microsoft Teams Relays for C2 Evasion

+DragonForce +Backdoor.Turn +RAT

- [DragonForce](#) ransomware operators used a custom Go-based RAT called Backdoor.Turn to hide command-and-control traffic inside legitimate Microsoft Teams TURN relay infrastructure. The malware obtained anonymous Teams visitor tokens, connected through Microsoft relay infrastructure, and then established QUIC sessions to the attacker's real C2 server. The backdoor was deployed against a major U.S. services firm, where attackers reportedly maintained access for one to two months.

Mastra AI npm Supply Chain Attack Linked to North Korea

+North Korea +AI +Sapphire Sleet +Crypto

- Microsoft attributed the [Mastra AI](#) supply-chain attack to Sapphire Sleet, also known as BlueNoroff, after attackers hijacked an npm maintainer account and pushed malicious updates to more than 140 Mastra-related packages. The compromised packages belonged to a JavaScript and TypeScript framework used to build AI applications, making the attack especially relevant to developer and AI workflow environments. The campaign reflects continued North Korean targeting of cryptocurrency and developer ecosystems through package compromise and stolen maintainer access.

Malicious JetBrains Plugins Steal AI API Keys From Developers

+JetBrains +AI +API

- Researchers found at least 15 malicious [JetBrains Marketplace](#) plugins designed to steal AI provider API keys from developers. The campaign targeted development environments directly, where exposed OpenAI, Anthropic, and other AI service credentials can support unauthorized usage, resale, or follow-on attacks against AI-enabled workflows. The activity shows continued attacker focus on IDEs, extensions, and developer tooling as high-value credential repositories.

Rokarolla Android Malware Targets 217 Banking and Crypto Apps

+Rokarolla +Crypto +Financial Services

- A new Android banking trojan named [Rokarolla](#) is targeting 217 banking and cryptocurrency apps using 137 supported commands. The malware is distributed through malicious sites impersonating Google Chrome and TikTok downloads and can gain extensive administrative control over infected devices. Its targeting of both banking and crypto applications reflects continued convergence between mobile banking fraud and cryptocurrency theft.

Windows SprySOCKS Variant Targets Government Organizations

+SprySOCKS +China +Government +Earth Lusca

- Researchers identified Windows variants of [SprySOCKS](#), malware previously associated with Linux systems and linked to Chinese threat group Earth Lusca. The malware has been used against government organizations in at least four countries, particularly entities connected to foreign affairs, technology, and telecommunications. The activity suggests continued cross-platform expansion by Chinese espionage operators targeting public-sector and strategic industry networks.

New Prinz Eugen Ransomware Prioritizes Recent Files

+Prinz Eugen +Ransomware

- A new ransomware operation named [Prinz Eugen](#) was observed prioritizing recently modified files for encryption, likely to maximize operational pressure by targeting the most business-relevant data first. Unlike many ransomware families, the malware reportedly leaves no ransom note on the system, complicating incident response and victim communication. The behavior suggests experimentation with ransomware impact optimization rather than standard broad encryption workflows.

Data Breaches

Novo Nordisk Extortion Group Claims 1.3 TB Theft and \$25M Demand

+Healthcare +FulcrumSec

- [FulcrumSec](#) claimed it stole more than 1 TB of data from Novo Nordisk after spending more than two months inside the pharmaceutical company's networks and unsuccessfully demanding \$25 million. The group said the stolen data includes source code, proprietary information on released and unreleased drugs, clinical trial data, employee, doctor and patient data, production-facility information, and internal AI model information. Reuters could not verify the full authenticity of the claims, while Novo Nordisk confirmed unauthorized access to a limited number of internal IT systems and said operations continued.

iRhythm Data Stolen From Third-Party-Hosted Business Applications

+Healthcare

- Digital health company [iRhythm](#) disclosed that attackers stole data from third-party-hosted business applications after unauthorized activity was detected on June 8. The threat actor contacted the company on June 9, claimed to have stolen sensitive information including proprietary data and patients' protected health information, and demanded a ransom. iRhythm said clinical systems, medical device systems, manufacturing and distribution operations, patient safety, and financial reporting systems were not impacted.

Clue Supply Chain Attack Exposes Salesforce Data at Cybersecurity Firms

+Clue +Salesforce +OAuth

- A supply-chain attack against market intelligence platform [Clue](#) began on June 11 and resulted in unauthorized commands against Clue backend servers, a code update to harvest OAuth tokens, and Salesforce data exposure for affected customers. Clue deactivated OAuth tokens and disabled integrations with Salesforce, HubSpot, SharePoint, Zoom, Gong, Chorus, Clari, Google Drive, and Slack; Salesforce later disabled the Clue Battlecards app after detecting unusual activity.

Nintendo Confirms Third-Party TinyPulse Survey Data Theft

+Gaming +Shadowbyt3

- [Nintendo of America](#) confirmed that threat actors stole survey information from TinyPulse, a third-party service used internally, while stating that Nintendo systems and customer accounts were not compromised. Shadowbyt3\$ claimed it stole close to 1 GB of data and demanded \$2 million, alleging the cache included names, email addresses, analytics and survey data, bank statements, W-9 forms, employee IDs, progress plans, and reports spanning 2016 to 2026. The group later said the breach affected a small number of Nintendo employees who used TinyPulse and began leaking alleged employee conversations after ransom negotiations failed.

Kodak Confirms Breach Claimed by ShinyHunters

+ShinyHunters

- [Kodak](#) confirmed it is working with external cybersecurity experts to investigate a breach after attackers gained access to some company data. ShinyHunters claimed responsibility for the incident, adding Kodak to the group's expanding list of extortion targets across legacy enterprise, technology, education, and SaaS-connected environments. Kodak's scale, with the company holding 79,000 worldwide patents, makes even limited data exposure significant because of the company's intellectual property, commercial print, advanced materials, and chemical product footprint.

Council of Europe Investigates ShinyHunters Data Theft Claims

+ShinyHunters +Government

- The [Council of Europe](#) opened an investigation after ShinyHunters claimed to have stolen more than 429,000 documents from multiple departments. The threat actor claimed the files included HR and payroll data and threatened to leak the data unless the organization responded by June 16. The incident is notable because it targets an intergovernmental institution and fits ShinyHunters' continued focus on large identity-rich repositories used for extortion rather than disruptive malware deployment.

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.