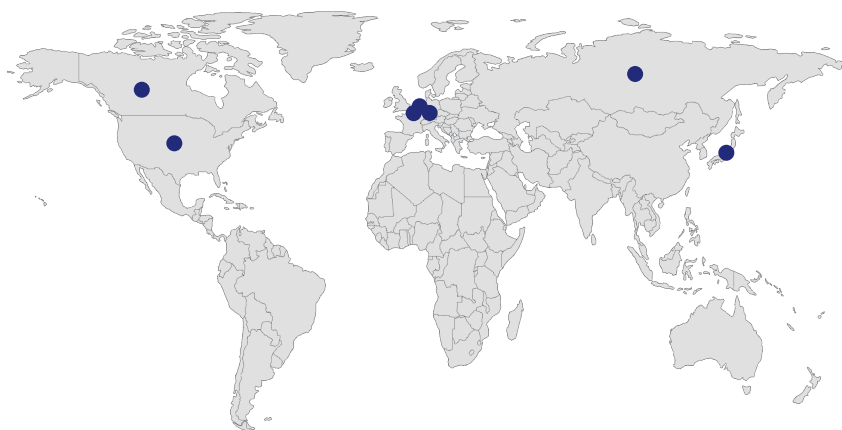


IMPERVA THREAT RESEARCH

Threat Intel Report: July 6-13, 2026

Countries



Top Tags

Forg365

GhostCommit

RedHook

CrashStealer

888

Executive Summary

Actionable Information:

- **Identity-based attacks continue to mature and industrialize.** This week saw multiple examples of attackers shifting away from malware-centric intrusions toward scalable identity compromise. Microsoft 365 users face increasingly sophisticated phishing-as-a-service offerings that combine adversary-in-the-middle (AiTM) techniques, AI-generated lures, and legitimate cloud infrastructure, while vishing campaigns demonstrate that attackers are successfully bypassing technical controls by targeting help desks and end users directly. Organizations should prioritize phishing-resistant MFA, conditional access policies, help-desk verification procedures, and continuous monitoring for session hijacking rather than relying solely on credential protection.
- **Attackers are increasingly abusing trusted technologies instead of exploiting traditional vulnerabilities.** Rather than relying exclusively on software flaws, recent campaigns leveraged legitimate router management features, Apple-notarized applications, Android Wireless ADB, and AI development tools to gain or maintain access. The emergence of Ghostcommit also demonstrates that AI-assisted software development introduces new supply chain risks, with prompt injection capable of manipulating coding agents into exposing sensitive repository secrets. Organizations should expand security reviews to include trusted administrative features, AI-assisted workflows, and software development pipelines.
- **Large-scale breaches continue to emphasize credential and third-party risk over ransomware disruption.** Several of the largest incidents—including KDDI, AssuranceAmerica, Accenture, and Lidl—centered on the theft of credentials, source code, cloud access keys, or sensitive customer information rather than operational disruption. The Odido investigation further highlights that social engineering remains an effective entry point into enterprise environments, while third-party service providers continue to represent high-value targets capable of exposing millions of customer records through a single compromise. Organizations should inventory third-party data exposure, rotate potentially exposed credentials, and monitor for downstream credential-stuffing activity following major breach disclosures.

Outlook:

The dominant trend this week is the continued shift toward identity, trust, and automation as primary attack surfaces. Rather than developing increasingly complex malware, threat actors are investing in scalable services that compromise identities, abuse legitimate administrative functionality, and exploit emerging technologies such as AI-assisted development tools. At the same time, data breach activity demonstrates that attackers continue to prioritize the theft of credentials, cloud secrets, and personally identifiable information over disruptive ransomware operations, recognizing the long-term value of stolen data for follow-on attacks. Organizations should expect identity-centric attacks, AI-enabled social engineering, and supply chain compromises targeting trusted software and service providers to remain the defining threats through the second half of 2026.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

📈 2,013% [CVE-2025-3248](#)

- Langflow versions prior to 1.3.0 are susceptible to code injection in the `/api/v1/validate/code` endpoint. A remote and unauthenticated attacker can send crafted HTTP requests to execute arbitrary code.

📈 370% [CVE-2026-35273](#)

- Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Updates Environment Management). Supported versions that are affected are 8.61 and 8.62. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools.

📈 297% [CVE-2025-54068](#)

- Livewire is a full-stack framework for Laravel. In Livewire v3 up to and including v3.6.3, a vulnerability allows unauthenticated attackers to achieve remote command execution in specific scenarios. The issue stems from how certain component property updates are hydrated. This vulnerability is unique to Livewire v3 and does not affect prior major versions. Exploitation requires a component to be mounted and configured in a particular way, but does not require authentication or user interaction. This issue has been patched in Livewire v3.6.4. All users are strongly encouraged to upgrade to this version or later as soon as possible. No known workarounds are available.

Recent Cyber Threats

Russian FSB Hackers Target Critical Infrastructure Through Weak Routers

+Russia +US +Government +Energy +Communications +Healthcare +Financial Services

- Cybersecurity agencies from the United States and eight partner countries warned that Russia's [FSB Center 16](#)—tracked as Static Tundra, Berserk Bear, Energetic Bear, and related names—is compromising vulnerable and poorly configured routers to penetrate critical-infrastructure networks. The actor scans for devices using default or weak SNMP community strings, spoofs source IP addresses, extracts configuration files, and transfers them to attacker infrastructure over TFTP. Targeted sectors include energy, communications, healthcare, financial services, government, defense, and the defense industrial base.

Forg365 Industrializes Microsoft 365 Device-Code Phishing

+Forg 365 +AITM +AI

- A new phishing-as-a-service platform called [Forg365](#) is combining device-code phishing, adversary-in-the-middle session theft, antibot controls, AI-generated lures, and post-compromise mailbox operations against Microsoft 365 users. The service is advertised through Telegram for \$400 per month or \$3,800 per year and uses legitimate delivery providers, including Amazon SES and Twilio SendGrid, to make malicious redirect chains resemble normal email traffic. Its operator panel supports automated invitations, OAuth application configuration, SVG generation, SMTP rotation, AI-assisted email creation, token storage, keyword alerts, account intelligence, and browser-extension integration. The platform reflects the continuing commoditization of identity attacks in which less-skilled operators can purchase infrastructure capable of stealing both credentials and active sessions.

Ghostcommit Hides Prompt Injection in Images to Steal Repository Secrets

+Ghostcommit +AI +Prompt Injection

- Researchers demonstrated an attack called [Ghostcommit](#) that embeds malicious instructions inside a PNG submitted with a software pull request. AI code-review tools that do not inspect image contents can approve the request, while a downstream coding agent later interprets the concealed prompt, reads sensitive files such as .env, and writes repository secrets into source code as an apparently innocuous list of numbers. Testing involved AI reviewers CodeRabbit and Bugbot, and the researchers published a proof of concept after notifying affected vendors. A survey of 6,480 pull requests across 300 highly active public repositories found that 73% of merged changes reached the default branch without substantive human or bot review, creating a substantial opening for similar AI-assisted supply-chain attacks.

RedHook Malware Abuses Wireless ADB for Android Shell Access

+RedHook +Malware +Wireless ADB

- A new [RedHook](#) Android malware variant uses the platform's Wireless Debugging functionality to establish shell-level access without requiring a physical computer connection. Abuse of Wireless ADB can provide significantly broader control than ordinary application permissions, enabling command execution and access to device functions outside the malware's standard sandbox. The technique illustrates attackers' continuing shift toward legitimate administrative and debugging features that may evade controls focused on conventional Android exploits. Users must still enable or approve portions of the debugging workflow, making social engineering and deceptive setup instructions important components of the attack chain.

CrashStealer Uses Apple-Notarized Dropper to Target macOS Credentials

+CrashStealer +macOS +Infostealer

- Researchers identified [CrashStealer](#), a native C++ macOS infostealer distributed through a signed and Apple-notarized application posing as a crash-reporting utility. The malware validates the victim's macOS password locally before harvesting data from browsers, password managers, cryptocurrency wallets, and the Apple Keychain. Stolen information is encrypted with AES-GCM and exfiltrated using libcurl, while persistence is established by copying and re-signing the malware. The use of a notarized dropper allows the initial application to pass Apple Gatekeeper checks and increases the likelihood that users will trust and execute it.

Okta Warns of Vishing Campaigns Targeting Microsoft 365 Accounts

+Vishing

- Okta warned that attackers are calling employees and directing them to phishing pages that closely reproduce [Microsoft Entra ID](#) authentication interfaces. The live telephone interaction allows operators to guide victims through authentication steps, capture credentials, and potentially overcome uncertainty or security warnings in real time. These attacks reinforce the shift from static email phishing toward interactive identity attacks combining social engineering, realistic login infrastructure, and session-token theft. Organizations relying primarily on user recognition of suspicious emails remain exposed when the attacker controls the conversation through voice calls.

Data Breaches

KDDI Email-Platform Breach Exposes Up to 14.2 Million Accounts

+Japan +Telecommunications

- Japanese telecommunications provider [KDDI](#) said attackers compromised an email platform used by five other ISPs, potentially exposing up to 14.22 million current, former, and inactive accounts. Compromised information included email addresses and passwords, although KDDI said some passwords were hashed or encrypted without specifying the algorithms used or how many credentials may have been stored in plaintext. KDDI discovered the intrusion on June 17, blocked attacker access, and implemented additional defensive measures before publishing an updated impact assessment in July. The concentration of credentials from multiple ISPs creates substantial credential-stuffing, phishing, and account-takeover risk beyond the affected email service itself.

AssuranceAmerica Breach Affects Nearly Seven Million Drivers

+US +Financial Services

- Auto insurer [AssuranceAmerica](#) disclosed that an employee-targeted attack gave an unauthorized party access to portions of its IT environment and exposed records belonging to 6,998,886 individuals. The malicious activity occurred on March 16 and was detected on March 17, after which investigators determined that the attacker had copied data files from company systems. AssuranceAmerica operates through more than 9,500 independent agents and provides coverage across 14 U.S. states, significantly expanding the potential geographic reach of the incident. The scale makes it one of the largest U.S. insurance-sector breach notifications of 2026 to date.

Accenture Confirms Theft of Source Code and Access Keys

+Technology +888

- [Accenture](#) confirmed an isolated security breach after a threat actor using the name “888” offered approximately 35 GB of allegedly stolen company data for sale on a cybercrime forum. The advertised material included source code, RSA and SSH keys, Azure personal access tokens, Azure Storage access keys, and configuration files, creating potential downstream risk if any credentials remained valid or code exposed customer-facing weaknesses. Accenture said it remediated the source of the breach and found no impact to operations or service delivery. Because Accenture provides technology, cloud, engineering, and managed services to major companies and governments, the possible exposure of reusable credentials warrants attention beyond the direct corporate impact.

Centers Laboratory Breach Exposes Health and Identity Data for 542,377 People

+Healthcare

- [Centers Laboratory](#) disclosed that an August 2025 intrusion exposed personal and protected health information belonging to 542,377 individuals. Attackers maintained access from August 9 through August 14 and stole names, dates of birth, Social Security numbers, driver’s license and state ID numbers, passport numbers, health-insurance information, and medical data. WorldLeaks claimed the attack and published more than 1.6 million files totaling approximately 720 GB; the group has listed more than 170 victims after shifting from ransomware encryption to data-theft extortion. The nearly one-year delay between discovery and public impact reporting also leaves affected patients facing an extended period of potential identity and medical-fraud exposure.

Mount Royal University Attackers Steal and Delete Stored Data

+Canada +Education

- [Mount Royal University](#) in Calgary confirmed that attackers accessed its network, stole information from file-storage systems, and subsequently deleted data. The incident combined exfiltration with destructive activity, increasing operational impact beyond a conventional confidentiality breach and complicating recovery efforts. The university began investigating the scope of affected information while a threat actor publicly claimed responsibility for the intrusion. The attack continues a broader pattern of universities being targeted because decentralized storage environments often contain extensive student, employee, research, financial, and identity data.

Dutch Police Link Odido Breach to Help-Desk Social Engineering

+Netherlands +Telecommunications

- Dutch police found strong indications that domestic hackers were involved in the February breach of telecommunications provider [Odido](#), which affected approximately 6.2 million customers. Shortly before the intrusion, a Dutch-speaking man called customer service while impersonating an Odido IT employee, after which personnel were deceived through phishing and attackers accessed the company's customer-contact system. The attackers downloaded millions of records and later contacted the company regarding the stolen data. The investigation highlights the continuing effectiveness of native-language help-desk impersonation, where attackers bypass technical controls by manipulating employees with access to internal identity or customer platforms.

Lidl Customers Exposed Through Third-Party Service Provider

+Food & Beverage +Germany +Belgium +Netherlands

- [Lidl](#) notified online-store customers in Germany, Belgium, and the Netherlands that personal information was stolen following a breach at an external service provider. The incident did not originate within Lidl's primary retail infrastructure but demonstrates how customer data entrusted to marketing, logistics, support, or e-commerce vendors remains exposed to the vendor's security posture. The multinational scope may trigger separate regulatory and notification obligations across affected European jurisdictions. The breach adds to continuing evidence that attackers are prioritizing service providers as aggregation points capable of exposing multiple brands or national customer populations through one compromise.

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.