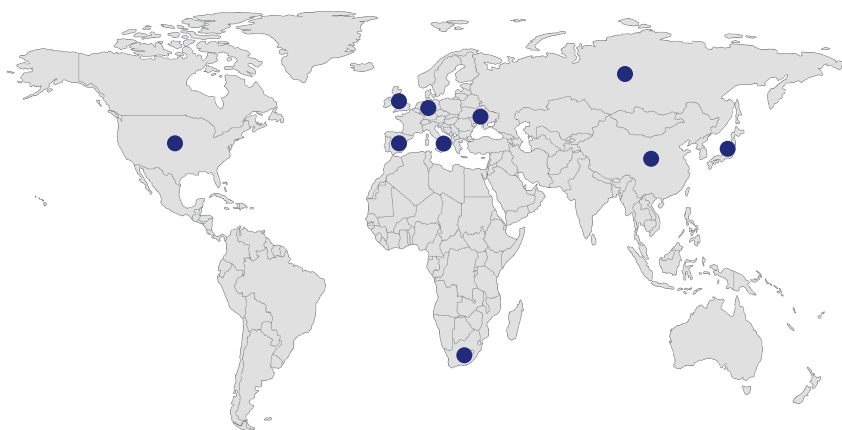


IMPERVA THREAT RESEARCH

Threat Intel Report: June 1-7, 2026

Countries



Top Tags

Gamaredon

HTTP/2 Bomb

IronWorm

TA4922

ShinyHunters

Executive Summary

Actionable Information:

- **Attackers continue prioritizing trusted platforms and legitimate infrastructure to hide malicious activity.** Recent campaigns abused widely used services including Stripe, Google Tag Manager, Steam Community profiles, Polyfill infrastructure, and public cloud environments to host payloads, store stolen data, or communicate with infected systems. By embedding malicious operations inside normal traffic flows and recognizable services, threat actors are reducing detection opportunities and forcing defenders to inspect trusted third-party integrations with the same scrutiny as unknown infrastructure.
- **Software supply chain and developer ecosystems remain high-value targets for credential theft and downstream compromise.** Activity targeting npm packages, WordPress environments, and open-source dependencies demonstrates continued attacker focus on developer workflows as scalable access points. Campaigns increasingly combine stolen publishing credentials, compromised CI/CD processes, malicious packages, and hidden command-and-control mechanisms to reach organizations indirectly through trusted tools and dependencies rather than direct intrusion attempts.
- **Critical infrastructure and public-facing systems remain vulnerable due to exposed services, legacy dependencies, and configuration weaknesses.** Threat actors targeted fuel monitoring systems, major web servers, CMS platforms, and widely deployed technologies through both new vulnerabilities and long-standing security gaps. These incidents reinforce that attackers continue to gain operational impact by exploiting overlooked internet-facing assets and third-party components that support essential business functions.
- **Data theft operations are increasingly focused on sensitive identity information with long-term exploitation value.** Recent breaches exposed healthcare records, government personnel information, humanitarian aid recipient data, and personal user metadata, highlighting attacker interest in datasets that enable fraud, surveillance, targeting, and extortion beyond the initial

compromise. Misconfigurations and unauthorized access continue to create large-scale exposure risks, especially for organizations managing vulnerable populations or highly sensitive personal information.

Outlook:

This week's activity highlights a continued shift toward ecosystem-level compromise, where attackers increasingly target the platforms, services, and relationships organizations depend on rather than isolated systems. Trusted third-party services, developer environments, and administrative tools are becoming central attack paths because they provide broad reach, built-in legitimacy, and access to valuable credentials or data. At the same time, threat actors are blending traditional exploitation with more sophisticated evasion techniques, including decentralized command-and-control, abuse of legitimate platforms, and supply-chain propagation. Organizations should expect continued growth in attacks against software dependencies, cloud-connected services, and exposed infrastructure, requiring stronger visibility into external integrations, identity access, and the full lifecycle of third-party components.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 1,228% [CVE-2026-8732](#)

- The WP Maps Pro plugin for WordPress is vulnerable to Privilege Escalation via Administrator Account Creation in all versions up to, and including, 6.1.0. This is due to the `wpgmp_temp_access_ajax` AJAX action being registered with `wp_ajax_nopriv_` and protected only by a nonce check using the `fc-call-nonce` nonce, which is publicly embedded into every frontend page via `wp_localize_script` as the nonce field of the `wpgmp_local` JavaScript object, rendering the check ineffective as an access control mechanism. This makes it possible for unauthenticated attackers to invoke the `wpgmp_temp_access_support` handler with `check_temp=false`, which unconditionally creates a new WordPress user with the hardcoded role of administrator via `wp_insert_user()` and returns a magic login URL that, when visited, calls `wp_set_auth_cookie()` to fully authenticate the attacker as the newly created administrator, resulting in complete site takeover.

↑ 370% [CVE-2025-32432](#)

- Craft is a flexible, user-friendly CMS for creating custom digital experiences on the web and beyond. Starting from version 3.0.0-RC1 to before 3.9.15, 4.0.0-RC1 to before 4.14.15, and 5.0.0-RC1 to before 5.6.17, Craft is vulnerable to remote code execution. This is a high-impact, low-complexity attack vector. This issue has been patched in versions 3.9.15, 4.14.15, and 5.6.17, and is an additional fix for CVE-2023-41892.

↑ 325% [CVE-2026-1492](#)

- The User Registration & Membership – Custom Registration Form Builder, Custom Login Form, User Profile, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to improper privilege management in all versions up to, and including, 5.1.2. This is due to the plugin accepting a user-supplied role during membership registration without properly enforcing a server-side allowlist. This makes it possible for unauthenticated attackers to create administrator accounts by supplying a role value during membership registration.

Recent Cyber Threats

Gamaredon Exploits WinRAR Flaw Against Ukraine

+Russia +Gamaredon +Ukraine

- Russian state-linked [Gamaredon](#) continued exploiting CVE-2025-8088, a WinRAR path traversal flaw, to deliver GammaPhish, GammaLoad, GammaWorm, and GammaSteel malware against Ukrainian targets. The chain uses malicious RAR archives to launch an HTA payload, retrieve VBScript downloaders, and deploy tools for host fingerprinting, C2 updates, propagation, persistence, and data theft. GammaWorm spreads through network shares and USB drives using malicious LNK files, while GammaSteel exfiltrates targeted files to AWS S3 or attacker-controlled infrastructure. The campaign reflects Gamaredon's continued focus on Ukrainian government, military, and critical infrastructure targets.

Suspicious Polyfill Login Prompts Hit Toshiba and Muji Websites

+Polyfill +Retail +Japan

- Toshiba and Muji warned visitors that [suspicious sign-in prompts](#) appearing on their websites could collect credentials, advising users who entered login data to change passwords. The prompts were generated through the external service hosted at polyfill[.]io, the same domain tied to the 2024 malicious Polyfill incident that affected more than 100,000 websites. Other reported impacted sites included Zojirushi, FINC Technologies, Ishiyaku Publishers, Hobonichi, and Samsung Smart TVs/websites, suggesting lingering Polyfill dependencies remained embedded across public sites.

HTTP/2 Bomb Enables Remote DoS Against Major Web Servers

+HTTP/2 Bomb +DoS

- Researchers disclosed [HTTP/2 Bomb](#), a remote denial-of-service technique affecting NGINX, Apache HTTPD, Microsoft IIS, Envoy, and Cloudflare Pingora. The issue combines HPACK header-compression amplification with a Slowloris-style hold, allowing tiny requests to create large server-side memory allocations that are never released. Researchers said a single client on a 100 Mbps connection could make a vulnerable server inaccessible within seconds, and one client could consume and hold 32 GB of memory against Apache HTTPD and Envoy in roughly 20 seconds. NGINX and Apache have mitigations or fixes available, Cloudflare Pingora requires no action, while IIS and Envoy had no patch at the time of reporting.

Magecart Campaign Abuses Stripe to Store Stolen Payment Data

+Magecart +Retail +Skimming

- Researchers found a [Magecart](#) campaign abusing Google Tag Manager and Stripe API infrastructure to load skimmer payloads and store stolen payment data from checkout pages. The malicious JavaScript targets Magento/Adobe Commerce checkout flows and collects credit card numbers, expiration dates, CVV codes, names, billing and email addresses, and phone numbers. Instead of exfiltrating data to an obvious attacker-controlled domain, each stolen card is stored as metadata in fake Stripe customer records, allowing the operation to blend into traffic to trusted payment infrastructure.

IronWorm Malware Hits 36 npm Packages

+npm +Malware +IronWorm

- A new npm supply-chain attack infected 36 packages with Rust-based infostealer malware called [IronWorm](#). Researchers said the malware targets 86 environment variables and 20 credential files that may contain OpenAI, AWS, Anthropic, npm, vault, SSH, and Exodus wallet secrets. IronWorm hides behind an eBPF kernel rootkit, communicates over Tor, and self-propagates by using stolen publishing credentials, including secrets tied to npm Trusted Publishing workflows, to push trojanized package versions into additional developer and CI environments.

Chinese-Speaking TA4922 Expands Atlas RAT Campaigns Into Europe

+TA4922 +China +Atlas RAT +Germany +Italy +US +UK +South Africa

- Researchers report that Chinese-speaking cybercrime group [TA4922](#) has expanded from East Asia into Germany, Italy, the United Kingdom, South Africa, and other regions using localized payroll, tax, VAT, invoice, HR, and government-compliance lures. The group deployed Atlas RAT, which supports system reconnaissance, targeted file theft, plugin/payload downloads, keylogging, screenshots, audio and webcam recording, and shutdown/reboot commands. Researchers also observed RomulusLoader, SilentRunLoader, Winos4.0/ValleyRAT, and possible LLM-assisted development patterns, showing a high-tempo financially motivated actor with malware capabilities that could also support surveillance or resale to espionage groups.

U.S. Agencies Warn of Attacks on Fuel Tank Monitoring Systems

+US +Government +Energy +Chemical +Food +Transportation +ATG

- CISA, the FBI, NSA, Department of Energy, and other U.S. partners warned that threat actors are targeting [internet-exposed automatic tank gauge systems](#) used across energy, chemical, food and agriculture, and transportation sectors. ATG systems monitor fuel and liquid storage tank levels, temperatures, and leaks, making unauthorized access operationally relevant even

when attacks do not directly disrupt industrial control systems. The government said attackers are compromising exposed ATG devices and modifying settings through command execution, though the activity has not yet been attributed to a specific nation-state or threat group.

WordPress Malware Uses Steam Profiles for C2 Payloads

+WordPress +Malware +C2

- Researchers found nearly 2,000 [WordPress websites](#) infected with malware that hides command-and-control data inside Steam Community profile comments. The attacker encoded payloads using invisible Unicode characters to build URLs for malicious scripts, abusing Valve's platform instead of maintaining standalone C2 infrastructure. Researchers said the initial infection vector remains unclear but may include stolen admin credentials, compromised FTP/SFTP access, vulnerable plugins or themes, or supply-chain compromise.

Data Breaches

DentaQuest Breach Impacts 2.6 Million Accounts

+US +Healthcare +ShinyHunters

- ShinyHunters leaked a 234 GB archive allegedly stolen from [DentaQuest](#) after failed negotiations with the dental benefits administrator. Have I Been Pwned reported that the leak affects roughly 2.6 million accounts and includes names, addresses, email addresses, phone numbers, dates of birth, government-issued IDs, and health insurance information. DentaQuest confirmed unauthorized access to a limited portion of its network and said it took action to secure the environment, contain the attack, and work with outside cybersecurity experts. The incident is significant because DentaQuest, a Sun Life subsidiary, serves roughly 35 million people across all 50 U.S. states.

FTF Live Misconfiguration Exposes 22 Million Session Records

+Misconfiguration

- The anonymous video chat platform [FTF Live](#) exposed data from up to 22 million sessions and 3.47 million identifiable users through a publicly accessible Kibana dashboard. The exposed data included usernames, email-like identifiers, device details, gender, IP addresses, country, language, payment-related information, and other metadata tied to sensitive conversations. Researchers also found an unsecured Dozzle instance exposing backend logs, plain-text passwords, session tokens, and internal API requests. Although raw video conversations were not exposed, the leak undermines the platform's anonymity claims and creates stalking, scam, account compromise, and targeting risks for vulnerable users.

UN World Food Programme Breach Exposes Gaza Aid Recipient Data

+UN +Humanitarian

- The [UN World Food Programme](#) disclosed that its Palestine self-registration application was breached, exposing beneficiary data across the Gaza Strip. The stolen data included names, ID numbers, phone numbers, and location information such as neighborhood data recorded during registration. WFP said assistance programs would continue normally while the platform remained temporarily suspended for urgent security improvements; reporting cited by WFP indicated attackers breached the system on May 14 and stole information tied to roughly 600,000 Palestinian households in Gaza.

Spain Arrests Suspected Doxer of Government and Cyber Officials

+Spain +Government +Doxing

- [Spanish National Police](#) arrested a suspected doxer accused of leaking sensitive information belonging to members of key state organizations, including Spain's National Cybersecurity Institute. The case involved personal data tied to government, police, prosecutor, and cyber officials, making it relevant as a targeted exposure of public-sector personnel rather than a conventional enterprise breach. The incident highlights growing risk around doxing and personal-data weaponization against officials involved in law enforcement, prosecution, and cybersecurity functions.

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.