

IMPERVA THREAT RESEARCH

Threat Intel Report: August 18-24, 2025

Countries



Top Tags

Silk Typhoon

Chaos

Warlock

Qilin

Interlock

Executive Summary

Actionable Information:

- **Protocol and Standards Exploitation:** Attackers are identifying ambiguities and overlooked behaviors in common protocols, using them to bypass controls and inject malicious activity.
- **Persistence of Infostealers:** Credential-harvesting malware remains a dominant threat, with campaigns using phishing, malvertising, and fake software to achieve long-term access to sensitive systems and data.
- **Cloud and SaaS Exposure:** Adversaries increasingly exploit cloud trust relationships, identity infrastructure, and third-party integrations to expand access and move laterally across environments.
- **Escalating Data Theft and Ransomware Impact:** Criminal groups continue to exfiltrate and monetize large volumes of sensitive data, impacting multiple industries and millions of individuals.
- **Supply Chain and Third-Party Risk:** Breaches are frequently initiated through weaker partners, vendors, and SaaS dependencies rather than direct targeting of primary organizations.
- **Credential Market Expansion:** The underground economy for credentials continues to thrive, fueled by large infostealer datasets and widespread demand for account access.

Outlook:

The threat landscape is trending toward greater convergence between nation-state sophistication and cybercriminal monetization models. While state actors refine stealthy access through cloud and identity exploitation, cybercriminals scale their operations with data theft, ransomware, and credential markets. Organizations should anticipate broader cross-domain attacks, where weaknesses in identity, third-party providers, or emerging platforms like AI-driven tools are exploited in tandem. Proactive defenses must emphasize identity security,

vendor risk management, and continuous monitoring of credential exposure, as attackers increasingly seek to weaponize trust and interconnectedness as their primary entry points.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 1,165% [CVE-2025-22457](#)

- A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.6, Ivanti Policy Secure before version 22.7R1.5, and Ivanti ZTA Gateways before version 22.8R2.2 allows a remote unauthenticated attacker to achieve remote code execution.

↑ 535% [CVE-2024-12987](#)

- A critical OS Command Injection vulnerability in DrayTek Vigor2960, Vigor300B, and Vigor3900 routers running firmware v1.5.1.4. The flaw resides in the Web Management Interface, specifically in the /cgi-bin/mainfunction.cgi/apmcfgupload handler. Because the session parameter is not properly sanitized, an unauthenticated attacker can inject arbitrary system commands that the device executes with root privileges.

↑ 217% [CVE-2025-54253](#)

- Adobe Experience Manager versions 6.5.23 and earlier are affected by a Misconfiguration vulnerability that could result in arbitrary code execution. An attacker could leverage this vulnerability to bypass security mechanisms and execute code. Exploitation of this issue does not require user interaction and scope is changed.

Recent Cyber Threats

Chunk-Extension Trick Enables HTTP Desync Attacks

+HTTP +Request Smuggling

- Researchers recently discovered a novel variant of [HTTP request smuggling](#) that abuses an ambiguous syntax: ending a chunk size line with just a semicolon. The front-end proxy skips this malformed extension, while the back-end treats it as the end of one request, allowing attackers to inject a second, unauthorized HTTP request and bypass security controls.

Noodlophile Infostealer Lures Victims with Legal-Threat Phishing

+Legal +Spear-phishing +Noodlophile

- In a spear-phishing spree, attackers impersonate law firms to threaten organizations with copyright or IP infringement claims, prompting recipients to click links to fake PDFs (actually ZIPs or MSI installers). Using DLL side-loading within legitimate, signed applications, the attackers establish a multi-stage payload that ultimately deploys the [Noodlophile](#) infostealer. The stealer extracts credentials, browser data, credit card info, system details, and maintains persistence while self-deleting to evade detection.

“Shamos” Mac Malware Spread via Fake Fixes

+Shamos +COOKIE SPIDER

- A new macOS infostealer dubbed “[Shamos](#)” is propagated by the COOKIE SPIDER group. Victims are duped through malvertising or bogus GitHub repos offering “fixes” that prompt terminal commands. These commands install a Base64-decoded Bash script, disabling Gatekeeper and executing Shamos, which then harvests keychain data, browser credentials, crypto wallets, Apple Notes, and more, sometimes achieving persistence via LaunchDaemons.

China-Linked Silk Typhoon Exploits Zero-Days to Breach Cloud Environments

+China +Silk Typhoon

- The Chinese state-linked espionage group [Silk Typhoon](#) (also tracked as Murky Panda) is compromising cloud service providers to access downstream customer data. By exploiting zero-days and vulnerable tools (Citrix, Ivanti, etc.), the group has breached SaaS providers, acquired Entra ID service secrets, and gained Global Admin privileges to infiltrate tenant environments. Their stealth is aided by trusted-relationship abuse, web shells (China Chopper, Neo-reGeorg), and custom Linux RATs like CloudedHope.

Agentic AI Browser “Comet” Falls for Fake Shops & Phishing

+Agentic AI +Phishing

- Security researchers tested Perplexity’s [Comet](#) (an agentic AI browser) and found it vulnerable to phishing, fake shop purchases, and prompt injections. In one test, Comet navigated a counterfeit Walmart site, autofilled credit card details, and completed a fake Apple Watch purchase without human oversight. In others, it followed a phishing email to a fake Wells Fargo login and executed hidden instructions in CAPTCHA-like pages to download malware.

Data Breaches

Cloaked CRM Breach at Workday

+Business +Software

- [Workday](#), a leading cloud HR and financial software provider, disclosed a breach where attackers leveraged a social-engineering campaign impersonating HR/IT personnel via phone and SMS to trick employees into divulging credentials or granting access to a third-party CRM platform. The threat actors accessed business contact data—names, email addresses, and phone numbers—but customer tenant data remained secure.

Chaos Ransomware Exposes Tax Relief Clients

+Financial Services +Chaos

- [Optima Tax Relief](#) confirmed a data breach affecting 3,114 individuals after an attack in May 2025. The Chaos ransomware group took responsibility, claiming to have exfiltrated approximately 69 GB of data containing sensitive Social Security numbers and financial account information, though Optima has not independently verified the claim.

Massive ISP Breach at iiNet via Stolen Credentials

+Telecommunications

- [TPG Telecom’s iiNet](#) brand suffered a significant breach due to stolen employee credentials, compromising its order-management system. The attackers accessed around 280,000 active email addresses, 20,000 landline numbers, 10,000 usernames, street addresses, phone numbers, and 1,700 modem setup passwords. No financial or identity documents were exposed. The incident was detected on August 16; TPG activated its incident response, engaged external experts, and began notifying customers.

Orange Breach Sparks SIM-Swapping Alarm

+Warlock +Telecommunications

- [Orange Belgium](#) has suffered a data breach in which approximately 850,000 customer accounts were compromised, including sensitive data such as SIM card numbers and PUK codes. These details can facilitate SIM-swapping attacks, enabling threat actors to hijack mobile identities and potentially bypass multifactor authentication. The intrusion, attributed to the Warlock ransomware group, was detected in late July and publicly disclosed in early August.

Qilin Hits Nissan’s Design Think Tank; Disrupts Pharma Research at Inotiv

+Qilin +Automotive +Healthcare

- The Qilin ransomware group claims to have breached [Nissan Creative Box](#) (CBI), the automaker’s internal design think tank, and exfiltrated over 4 TB of files. The stolen content reportedly includes 3D vehicle design data, VR imagery, reports, photos, videos, and internal documents. Published on Qilin’s leak site, the files remain withheld for now, with the group threatening to release them unless Nissan acknowledges the breach.
- On August 8, 2025, [Inotiv](#), a U.S.-based drug research and development firm, detected a ransomware attack that encrypted parts of its systems, disrupting operations. In an SEC filing, the company confirmed system impacts and initiated forensic

investigations with external experts. The Qilin ransomware gang claimed responsibility, asserting they stole around 176 GB of data—likely including research materials spanning the last decade—by listing Inotiv on their leak site.

DaVita Ransomware Breach Exposes Millions of Patient Records

+Interlock +Healthcare

- A ransomware incident at [DaVita](#), a U.S. dialysis provider, has compromised highly sensitive data from nearly 2.7 million individuals, including personal, medical, and financial information. The attack, attributed to the Interlock gang, occurred between March 24 and April 12, 2025, but was only detected in mid-April. Although patient care continued uninterrupted, DaVita incurred substantial remediation costs and has begun notifying affected patients, offering free identity protection services.

APCS Breach via Upstream Development Partner

+Third-Party

- UK-based [Access Personal Checking Services](#) (APCS), a provider of criminal record checks, has notified customers that their data was compromised due to a breach at a third-party development firm—Hull-based Intradev. While full breach details remain undisclosed, APCS confirmed the incident via direct notification to impacted individuals.

Massive Leak of Plain-Text PayPal Credentials Listed for Sale

+Chucky_BF

- A dubious dataset reportedly containing 15.8 million [PayPal login credentials](#)—emails, plaintext passwords, and associated URLs—is being offered for sale on underground forums by a threat actor called “Chucky_BF.” The dataset may originate from infostealer malware logs rather than a direct PayPal breach, and its authenticity remains uncertain. PayPal denies a new incident.

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.