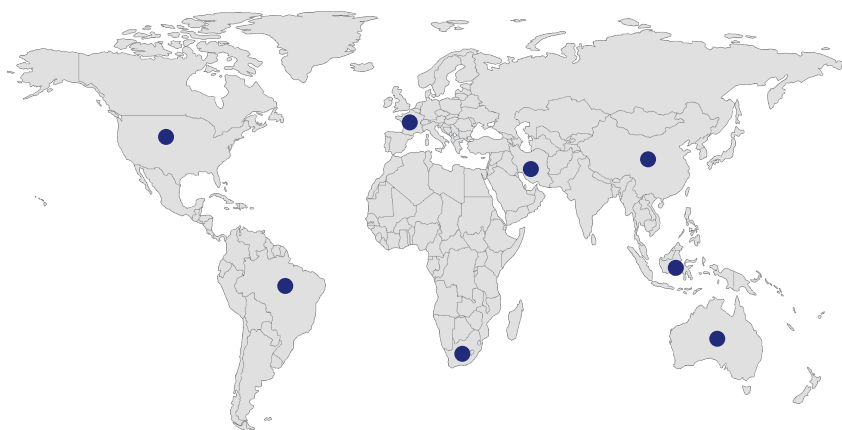


IMPERVA THREAT RESEARCH

Threat Intel Report: July 21-27, 2025

Countries



Top Tags

PoisonSeed

MuddyWater

Coyote

Qilin

Lynx

Executive Summary

Actionable Information:

- **Attackers continue to diversify abuse of trusted protocols and platforms**, including downgrading FIDO2 MFA, abusing Microsoft UI Automation, and exploiting Telnet defaults in VoIP routers—highlighting the need to harden authentication flows and legacy infrastructure.
- **Healthcare, financial, and government sectors face persistent targeted threats**, including high-volume DDoS campaigns, ransomware, and phishing-based CRM compromises. Attackers are also exploiting geopolitical unrest (e.g., Iran-Israel tensions) to launch espionage and defacement attacks.
- **Ransomware operations are increasingly sophisticated and widespread**, with double-extortion tactics, tool abuse (e.g., ToolShell), and botnet expansion through brute-force and social engineering. Multiple ransomware strains (Gunra, Qilin, Warlock, LockBit, Lynx) were active across industries.
- **Misconfigured databases and cloud services are fueling large-scale data leaks**, as seen in breaches at Tea, SABO, Allianz Life, and France Travail. Exposed personal data—especially from sensitive platforms like dating and jobseeking apps—poses escalating risks for identity theft and targeted phishing.

Outlook:

This week's activity reinforces the evolving threat landscape where attackers blend advanced technical tactics with simple misconfiguration exploitation. While state-aligned actors weaponize zero-days and deploy malware tied to geopolitical conflict, financially motivated groups are exploiting soft targets across industries with increasing operational scale. We expect continued ransomware diversification, phishing innovations targeting AI and identity systems, and higher scrutiny on platforms that mishandle user data—especially those in high-trust or safety-centric sectors. Strengthening endpoint defenses, cloud hygiene, and identity protections remains critical moving into Q3.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 192% [CVE-2024-0012](#)

- An authentication bypass in Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to the management web interface to gain PAN-OS administrator privileges to perform administrative actions, tamper with the configuration, or exploit other authenticated privilege escalation vulnerabilities.

↑ 132% [CVE-2025-29891](#)

- Bypass/Injection vulnerability in Apache Camel. This vulnerability is present in Camel's default incoming header filter, that allows an attacker to include Camel specific headers that for some Camel components can alter the behaviors such as the camel-bean component, or the camel-exec component.

↑ 43% [CVE-2024-13159](#)

- Absolute path traversal in Ivanti EPM before the 2024 January-2025 Security Update and 2022 SU6 January-2025 Security Update allows a remote unauthenticated attacker to leak sensitive information.

Automated GeoServer Attacks Target South African Healthcare

+[South Africa](#) +[Healthcare](#) +[Bots](#)

- A South African healthcare provider was targeted this week by automated attacks reaching almost 1.5 million requests in one day. Attacks came from IPs located in the Netherlands, and targeted GeoServer instances.

Prolonged App-Layer DDoS Hits Indonesian Financial Site

+[Indonesia](#) +[Financial Services](#) +[DDoS](#)

- An Indonesian financial services site was hit by an application-layer DDoS attack this week totaling 6 million requests per second (RPS). The attack lasted 10 hours.

Recent Cyber Threats

FIDO2 MFA Downgrade via Cross-Device Phish

+[PoisonSeed](#) +[FIDO2](#)

- Threat group [PoisonSeed](#) staged a phishing campaign abusing WebAuthn's cross-device login feature to trick users into approving weaker MFA flows via QR codes. Though the FIDO2 protocol isn't broken, attackers achieved credential compromise by downgrading authentication strength and intercepting user sessions. No direct system compromise occurred in observed cases, but this technique undermines high-assurance authentication workflows.

DCHSpy Android Spyware Expands in Middle East Conflict

+[MuddyWater](#) +[Iran](#) +[DCHSpy](#)

- Iran-linked APT [MuddyWater](#) deployed four new variants of DCHSpy, disguised as fake VPN apps (including Starlink, EarthVPN, Comodo VPN), that now also harvest WhatsApp, SMS, location, and files, and can record audio and photos. The campaign aligns with escalating Iran-Israel tensions, leveraging surging VPN adoption in affected regions. Lookout researchers warn the attacks illustrate evolving mobile surveillance sophistication.

UI Automation Malware Steals Brazilian Bank Credentials

+Coyote +Brazil +UIA

- A new variant of the banking trojan [Coyote](#) has become the first malware observed abusing Microsoft's UI Automation framework (UIA) in the wild. Targeting Brazilian users, it silently reads browser tabs and UI elements to harvest credentials from 75 banking and crypto services. This marks a notable escalation in malware tactics by weaponizing Windows accessibility tools.

Chinese Groups Launch Ransomware via SharePoint Zero-Days

+China +ToolShell +LockBit

- Chinese-affiliated groups (Storm-2603, Linen Typhoon, and Violet Typhoon) are exploiting [SharePoint](#) zero-day vulnerabilities—dubbed "ToolShell"—to deploy Warlock and LockBit ransomware on unpatched on-prem servers. Hundreds of enterprise and government systems, including U.S. agencies, have been impacted. Organizations are urged to install updated patches, rotate machine keys, and enhance monitoring systems.

VoIP Routers Co-opted into Telnet-Powered Botnet

+Mirai +Telnet

- Researchers uncovered a new VoIP-based botnet exploiting default [Telnet](#) credentials in routers—initially traced to New Mexico—which quickly expanded to hundreds of devices. The compromised routers are being recruited into a Mirai-style botnet for potential DDoS or proxy misuse. Security professionals should enforce Telnet hygiene and decommission exposed legacy hardware.

Gunra Ransomware Targets Windows in Double-Extortion Campaign

+Gunra

- [Gunra](#), a newly identified ransomware family, is targeting Windows environments worldwide across sectors like real estate, pharmaceuticals, and manufacturing. It uses double-extortion tactics—encrypting files and stealing sensitive data to pressure victims within a five-day window. Advanced anti-analysis features and deletion of shadow copies highlight its sophistication.

Data Breaches

Tea App Breach Exposes Photos and 1.1M Private Chats

+Adult

- Two unsecured databases tied to the women-only dating safety app [Tea](#) have leaked sensitive user content, including 72,000 images—such as 13,000 ID/selfies and 59,000 dating-related posts—and 1.1 million private chat messages from 2023 through mid-2025. The photo archive was linked to legacy accounts created before February 2024 and did not include emails or phone numbers, while the second leak revealed deeply personal conversations discussing topics like abortion and infidelity. Both datasets, totaling over 59 GB, were publicly accessible and circulated on hacking forums, triggering widespread backlash over the platform's poor storage hygiene and failure to protect users of a service marketed as safety-first.

Allianz Life CRM Compromise via Social Engineering

+Financial Service

- [Allianz Life](#) confirmed a breach on July 16 where attackers used social engineering to gain access to a third-party, cloud-based CRM system. The data stolen reportedly covered personally identifiable information for the majority of its 1.4 million U.S. customers, financial professionals, and some employees, though no internal systems were affected. The company engaged regulators and the FBI and plans to offer identity protection to those impacted.

Morgan County 911 Hit by Qilin Ransomware Gang

+Government +Qilin +US

- [Morgan County 911](#) in Alabama suffered a ransomware incident in May 2025, claimed by the Qilin group. While administrative systems were disrupted for several days, critical dispatch services remained functional. According to officials, the attack was driven by brute-force methods rather than phishing, and the agency disconnected networks as a precaution.

French Jobseeker Agency Breach Exposes 340K Records

+France +Government

- [France Travail](#), the French national employment agency, disclosed that an infostealer compromised a user account tied to a training organization, exposing personal data of roughly 340,000 jobseekers—names, addresses, phone numbers, and job status. No financial or password data was affected, but the breach fuels concerns about phishing risks following repeated data exposures from this agency.

Massive Customer Records Leak at SABO

+Australia +Retail

- A misconfigured, unencrypted online database tied to Australian fashion brand [SABO](#) exposed over 3.5 million customer records, including names, email addresses, phone numbers, addresses, invoices, and order histories spanning from 2015 to mid-2025. The 292 GB dataset contained multiple orders per PDF, suggesting the true number of affected individuals may exceed file counts. While the breach was secured within hours, the company has not responded publicly, leaving uncertainty over whether the data was accessed by malicious parties. This leak poses serious risks for targeted phishing and social engineering against customers.

Gaming PC Maker Compromised by Lynx Ransomware

+Lynx +Computing

- Ransomware group [Lynx](#) claimed responsibility for a June 2025 network breach impacting gaming PC manufacturer iBUYPOWER and its sister brand HYTE. The incident disrupted internal systems including ERP, accounting, production, and customer service, although no payment data is believed to have been stored internally.

Pro-Iranian Defacement of Arizona Candidate Portal

+Iran +US +Government

- In late June, pro-Iranian actors defaced [Arizona's online political candidate portal](#)—replacing candidate photos with images of Ayatollah Khomeini and linking to a Telegram message threatening retaliation after U.S. strikes in Iran. The portal remained offline for several days before state authorities resolved the incident without federal support. Arizona officials criticized CISA for alleged lack of election-security assistance from the federal government.

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.