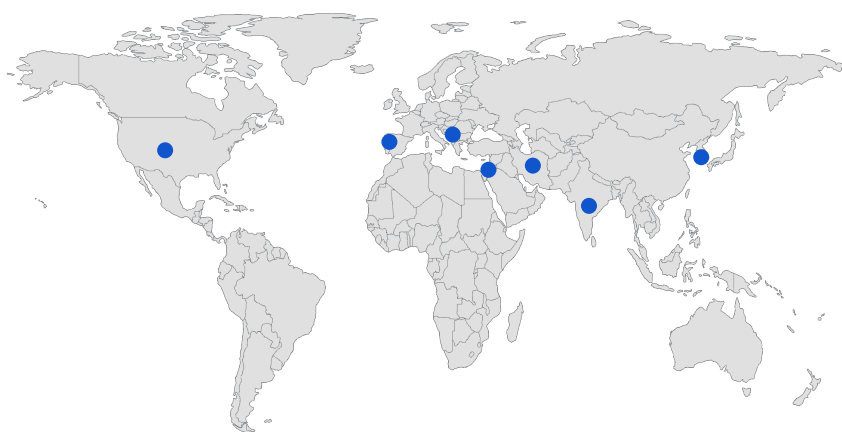


Threat Intel Report: June 9-15, 2025

Countries



Top Tags

NICKNAME

Warlock

Handala

Black Basta

Chaos

Executive Summary

Actionable Information:

- **Ransomware Expands Global Reach with Diverse Tactics:** Warlock, Black Basta, and Chaos have collectively targeted over 20 organizations in the past month, exploiting healthcare, finance, and government verticals. Warlock's return to aggressive extortion mirrors previous campaigns from Black Basta and REvil, suggesting recycled or rebranded playbooks. Double-extortion and public data leaks remain key tools.
- **Surveillance-Grade Exploits Used in Espionage Campaigns:** The NICKNAME zero-click iMessage exploit is a clear example of high-end, stealthy mobile surveillance likely deployed by a nation-state. Victims included journalists, politicians, and AI researchers. Lack of public disclosure from Apple leaves a gap in defensive posturing for at-risk individuals.
- **Consumer and Mobile Threats Grow More Sophisticated:** Over 20 malicious crypto wallet apps bypassed Google Play protections, while Myth Stealer, a Rust-based infostealer, used pirated game lures to compromise browser credentials. Both attacks reveal the persistence and evolution of cybercriminals exploiting user trust in everyday platforms.
- **Credential-Based Intrusions Undermine Public Infrastructure:** Multiple incidents—including those at NHS Professionals, TxDOT, and Thomasville's city government—originated with credential misuse or basic remote access abuse. These highlight continued weaknesses in account hygiene, access controls, and threat detection in public sector networks.
- **Data Breaches Amplify Regulatory Pressure on Organizations:** Episource, Optima Tax Relief, McLean Mortgage, and Zoomcar reported breaches exposing hundreds of thousands to millions of records. Affected data includes PII, financial accounts, healthcare records, and crash report details. Legal scrutiny and consumer trust implications are expected to rise.

Outlook:

The volume and variety of attacks this week suggest a widening threat surface, with threat actors simultaneously exploiting systemic weaknesses (unpatched software, weak credentials) and high-value vulnerabilities (zero-click mobile exploits). As ransomware groups evolve and rebrand, and nation-states invest in stealthy surveillance campaigns, defenders must strengthen detection and response strategies, particularly around credential management, software supply chains, and endpoint monitoring. Regulatory scrutiny—especially in finance, healthcare, and mobility sectors—is likely to intensify in the wake of large-scale data breaches affecting millions. Expect continued pressure on mobile platforms and SaaS providers to improve vetting, disclosure, and transparency as attackers increasingly target their ecosystems.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

542% [CVE-2025-22457](#)

- A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.6, Ivanti Policy Secure before version 22.7R1.4, and Ivanti ZTA Gateways before version 22.8R2.2 allows a remote unauthenticated attacker to achieve remote code execution.

327% [CVE-2025-34026](#)

- The Versa Concerto SD-WAN orchestration platform is vulnerable to an authentication bypass in the Traefik reverse proxy configuration, allowing at attacker to access administrative endpoints. The internal Actuator endpoint can be leveraged for access to heap dumps and trace logs. This issue is known to affect Concerto from 12.1.2 through 12.2.0.

65% [CVE-2025-34027](#)

- The Versa Concerto SD-WAN orchestration platform is vulnerable to an authentication bypass in the Traefik reverse proxy configuration, allowing at attacker to access administrative endpoints. The Spack upload endpoint can be leveraged for a Time-of-Check to Time-of-Use (TOCTOU) write in combination with a race condition to achieve remote code execution via path loading manipulation, allowing an unauthenticated actor to achieve remote code execution (RCE).

Indian Telecommunications Site Targeted By Business Logic Attacks

+India +Telecommunications

- An Indian telecommunications provider was hit by a surge of business logic attacks totaling nearly 35 million automated requests in a single day. Originating entirely from within India, the requests came from bot traffic rather than human users and targeted application logic, possibly to probe service availability, scrape data, or exploit pricing or authentication workflows.

US Computing Site Hit By 411 Gbps DDoS Attack

+US +Computing

- A U.S.-based computing site experienced a large-scale DDoS attack peaking at 411 Gbps, sustained over a concentrated two-hour period. The assault relied primarily on SYN flood tactics, overwhelming the site's network stack with spoofed TCP handshake requests to exhaust server resources. While brief, the volume and intensity of the attack suggest access to a powerful botnet, likely aimed at temporarily disrupting services or testing defenses ahead of a larger campaign.

Recent Cyber Threats

Malicious Crypto Wallet Apps Harvest Seed Phrases from Google Play Users

[+Cryptocurrency](#) [+Financial Services](#) [+Android](#)

- A wave of over 20 malicious Android apps posing as legitimate cryptocurrency wallets like MetaMask, Trust Wallet, and Phantom were uploaded to Google Play. These apps mimic real wallet interfaces and prompt users to enter their 12-word seed phrases under the guise of account recovery. Once the seed is submitted, attackers can immediately drain the user's assets. Despite takedowns by Google, several of these apps have reappeared under different developer names, showing the resilience of mobile phishing campaigns targeting the crypto sector.

iMessage Exploit Used in Elite Surveillance Operation Tied to China

[+NICKNAME](#) [+Zero-Click](#) [+China](#)

- Security researchers have discovered an advanced zero-click exploit for iMessage, dubbed [NICKNAME](#), which was used in a stealthy campaign targeting political figures, journalists, and AI researchers across the US and Europe. The exploit allows attackers to fully compromise an iPhone without the victim opening any message or file. The campaign shows characteristics of nation-state espionage and coincides with growing tensions over global AI policy and surveillance concerns. Apple has not publicly disclosed the flaw as of mid-June.

New Rust-Based "Myth Stealer" Malware Targets Gamers with Fake Game Downloads

[+Myth Stealer](#) [+Rust](#) [+Malware](#)

- A new info-stealer called [Myth Stealer](#) is being distributed through fraudulent websites offering pirated games and cracked software, particularly targeting gamers. Written in Rust, the malware boasts obfuscation and high performance, with the capability to steal credentials, cookies, and session tokens from Chrome and Firefox. After users download a fake game, a misleading interface is shown while the malware decrypts and runs silently in the background. Myth Stealer highlights a trend toward stealthy, Rust-based malware targeting consumer browsers.

Warlock Ransomware Gang Claims Global Attacks on Government Agencies

[+Warlock](#) [+India](#) [+Croatia](#) [+Portugal](#)

- A newly identified ransomware group called [Warlock](#) has taken responsibility for a growing number of attacks across at least 16 organizations, including government agencies and financial institutions. Victims include Nippon Life India Asset Management, government bodies in Croatia and Portugal, and private companies. The gang reportedly demands average ransoms of \$2.4 million and uses aggressive extortion tactics. The emergence of Warlock may mark the return of tactics used by Black Basta and REvil, though attribution remains uncertain.

Iranian Hackers Ramp Up Aggression Toward Israel with Massive Cyber Wave

[+Iran](#) [+Israel](#) [+Handala](#) [+Defense](#) [+Industrial](#)

- Iranian-aligned hackers, including the hacktivist group [Handala](#), launched a sharp increase in cyberattacks against Israeli targets, with a 700% rise in volume since June 13. Attacks have focused on defense contractors and infrastructure entities, and reports indicate the exfiltration of more than 2TB of sensitive data. These attacks follow recent military tensions and signal the ongoing use of cyber as a tool of asymmetric warfare in the region.

Data Breaches

Municipal Systems Disrupted in Dual Southern Attacks

[+US](#) [+Government](#)

- In recent days, both [Thomasville, North Carolina, and Ogeechee Judicial Circuit in Georgia](#) experienced separate cyber incidents disrupting municipal services and courtroom operations. Thomasville's city systems were taken offline, though essential services reportedly remained functional, while Georgia's DA office suffered phone and internet outages across four counties. Recovery efforts are underway, with Thomasville engaging cybersecurity professionals and Ogeechee halting operations to contain the incidents.

Zoomcar Confirms 8.4 Million Users Exposed in Data Breach

+India +Transportation

- [Zoomcar](#), India's leading car-sharing platform, reported that a hacker accessed personal data of approximately 8.4 million users beginning June 9, including names, phone numbers, addresses, email addresses, and vehicle registration numbers. Although no financial credentials appear compromised, the breach was officially filed via a SEC 8-K on June 13 and is under active investigation. This incident underscores mounting privacy concerns in mobility platforms.

Episource Ransomware Exposes Health Records and Insurance Data

+Healthcare +Technology +US

- [Episource](#), a medical software and coding provider, revealed a January–February 2025 ransomware incident that exposed private health information—including medical records, insurance details, and PII—for at least 24,259 Texas patients and likely thousands more nationwide. The attack impacted Sharp Healthcare's patient base, prompting breach notifications and ongoing legal scrutiny. The firm now faces investigations and potential regulatory fallout.

Black Basta Strikes McLean Mortgage, Exposes 30K Records

+Black Basta +Financial Services

- In an October 2024 ransomware attack claimed by Black Basta, [McLean Mortgage](#) disclosed that over 30,453 individuals had their names, SSNs, driver's license numbers, and financial account info compromised. Black Basta showcased stolen documents to substantiate the breach, though McLean hasn't confirmed if a ransom was paid. The firm is notifying affected parties and may face legal and compliance consequences.

Stealthy AD Theft Hits NHS Professionals Without Public Disclosure

+United Kingdom +Government +Healthcare

- In May 2024, attackers leveraged a compromised Citrix account to infiltrate [NHS Professionals](#) (a staffing organization for NHS trusts), escalated to admin access using tools like Cobalt Strike and WinRM, and stole the Active Directory database containing user credentials. The breach went unreported publicly until recently, raising questions about detection timelines and transparency within UK health services.

Yes24 Ransomware Attack Disrupts South Korea's K-Pop Ticketing Operations

+South Korea

- [Yes24](#), a major South Korean ticketing and online bookstore platform, suffered a ransomware attack on June 9, knocking out its services for over four days. The outage disrupted ticket sales for K-Pop concerts, musicals, and other events; core systems began recovery by June 13, while features like user accounts and comments remained offline. The company has apologized, offered compensation, and pledged improved transparency.

Chaos Ransomware Leaks 69 GB from Optima Tax Relief

+Chaos +Financial Services +US

- U.S. tax resolution firm [Optima Tax Relief](#) was breached by Chaos ransomware in early June, resulting in roughly 69 GB of sensitive legal and tax documentation being leaked via the gang's data site. This double-extortion incident involved both encryption and theft of PII such as SSNs, addresses, and case file details. The breach poses significant risks of identity theft and reputational damage.

Washington Post Confirms Journalist Email Breach Under Investigation

+US +News

- [The Washington Post](#) revealed that attackers gained unauthorized access to the email accounts of several of its journalists in a suspected targeted cyber campaign. While the exact scope and attribution remain under investigation, early signs suggest that the attack may have been politically motivated or linked to a state-

sponsored group. The publication is working with internal security teams and third-party experts to assess and contain the breach.

Texas DOT Crash Reports Breached via Compromised Account

+US +Government +Automotive

- On May 12, hackers used a compromised [Texas Department of Transportation](#) (TxDOT) user account to download nearly 300,000 crash reports, impacting about 423,000 individuals. Exposed data included names, addresses, driver's license and vehicle info, and insurance policy numbers. TxDOT has notified affected individuals, reported the incident to state authorities, disabled the account, and is ramping up security to prevent recurrence.

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.