

IMPERVA THREAT RESEARCH

Threat Intel Report: March 9-22, 2026

Countries



Top Tags

ClickFix

Camaro Dragon

ShinyHunters

Payload

LAPSUS\$

Executive Summary

Actionable Information:

- **Social engineering is a dominant initial access vector.** Attackers are increasingly relying on user interaction, like phishing, fake prompts, and malicious instructions, to bypass technical controls and gain execution within trusted environments. This reduces dependence on exploits and allows attackers to scale campaigns across organizations regardless of patching posture.
- **Geopolitical events are consistently being weaponized for cyber operations.** Breaking news and regional conflicts are rapidly incorporated into lures for espionage, fraud, and malware delivery. This creates a dual threat landscape where both nation-state and financially motivated actors exploit the same narratives to target victims at scale.
- **Supply chain and shared platform risk continues to expand.** Attackers are prioritizing widely used ecosystems, such as open-source repositories, SaaS platforms, and third-party vendors, to achieve broad, downstream impact. Misconfigurations and trust relationships are increasingly being exploited instead of platform vulnerabilities.
- **Identity-based attacks are outpacing traditional perimeter threats.** Credential theft, account takeover, and abuse of legitimate access are key drivers of breaches, often enabled through phishing or third-party compromise. These attacks frequently evade detection by blending in with normal user activity.
- **Critical infrastructure and high-impact industries remain priority targets.** Sectors where disruption has immediate operational or safety consequences, such as healthcare and regulated systems, continue to face disproportionate targeting, increasing both financial and societal risk.
- **Cybercrime infrastructure remains globally distributed and resilient.** Despite coordinated takedown efforts, the scale and decentralization of malicious infrastructure enable rapid reconstitution, allowing phishing, malware distribution, and scam operations to persist with minimal disruption.

Outlook:

This week's activity reflects a continued shift toward scalable, low-friction attack methods paired with high-impact targeting. Attackers are increasingly combining social engineering, cloud misconfigurations, and supply chain compromise to bypass traditional defenses and maximize reach, while geopolitical tensions are accelerating both nation-state operations and opportunistic cybercrime. At the same time, the convergence of digital attacks with physical-world consequences—seen in healthcare disruptions and automotive system outages—signals growing risk to operational technology and regulated systems. Looking ahead, organizations should expect sustained growth in conflict-themed phishing campaigns, identity-based breaches, and multi-tenant platform abuse, alongside continued ransomware and extortion activity targeting high-value sectors. While law enforcement efforts will intermittently disrupt infrastructure, the adaptability of threat actors suggests overall attack volume and sophistication will continue to increase.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 549% [CVE-2025-55752](#)

- Relative Path Traversal vulnerability in Apache Tomcat. The fix for bug 60013 introduced a regression where the rewritten URL was normalized before it was decoded. This introduced the possibility that, for rewrite rules that rewrite query parameters to the URL, an attacker could manipulate the request URI to bypass security constraints including the protection for /WEB-INF/ and /META-INF/. If PUT requests were also enabled then malicious files could be uploaded leading to remote code execution.

↑ 178% [CVE-2025-66039](#)

- FreePBX Endpoint Manager is a module for managing telephony endpoints in FreePBX systems. Versions are vulnerable to authentication bypass when the authentication type is set to "webserver." When providing an Authorization header with an arbitrary value, a session is associated with the target user regardless of valid credentials.

↑ 121% [CVE-2025-40598](#)

- A Reflected cross-site scripting (XSS) vulnerability exists in the SMA100 series web interface, allowing a remote unauthenticated attacker to potentially execute arbitrary JavaScript code.
-

Recent Cyber Threats

Velvet Tempest Uses ClickFix Technique in Multi-Stage Ransomware Intrusion

+[Velvet Tempest](#) +[ClickFix](#) +[US](#)

- Researchers observed the ransomware affiliate group [Velvet Tempest](#) using the ClickFix social-engineering technique to gain initial access and deploy malware during simulated attacks against a large U.S. nonprofit network. Victims were tricked into executing malicious commands that downloaded DonutLoader and installed the CastleRAT backdoor using legitimate Windows utilities like PowerShell and cmd.exe. The operation unfolded over 12 days and leveraged credential harvesting and persistence mechanisms before staging ransomware capabilities. Velvet Tempest has previously been linked to major ransomware families including Ryuk, REvil, Conti, LockBit, and BlackCat.

Geopolitical Tensions Drive Surge in Conflict-Themed Cyber Campaigns

+[Geopolitical](#) +[Backdoor](#) +[Phishing](#) +[Scams](#)

- Security researchers reported a wave of cyber activity exploiting the ongoing [Middle East conflict](#), including phishing campaigns, malware distribution, and fraud operations themed around regional events. Analysts identified more than 8,000 newly registered domains referencing the conflict, many likely intended for scams or malware delivery. Observed campaigns included

fake news or conflict reports used to deliver backdoors, phishing sites impersonating government services, and donation scams designed to steal financial information. Researchers noted that geopolitical crises frequently trigger opportunistic cybercrime as attackers exploit public interest and urgency around breaking events.

China-Linked Hackers Target Qatar with War-Themed Malware Lures

+China +Qatar +Camaro Dragon

- China-linked hackers associated with the [Camaro Dragon](#) group targeted organizations in Qatar using malware disguised as breaking war news. The campaign distributed files referencing missile strikes and regional conflict to lure victims into opening infected documents. Once executed, the malware installed the PlugX backdoor and leveraged tools like Cobalt Strike to enable espionage activities such as keystroke logging, file theft, and remote control of compromised systems. Researchers believe the campaign focused on military and energy sector targets amid rising geopolitical tensions in the region.

Global Operation Shuts Down Tens of Thousands of Cybercrime Servers

+Operation Synergia III +INTERPOL

- An INTERPOL-led international law enforcement effort, [Operation Synergia III](#), dismantled more than 45,000 malicious IP addresses and servers used for cybercrime infrastructure across 72 countries and territories. The campaign targeted infrastructure supporting phishing, malware distribution, and online scams, and resulted in 94 arrests linked to cybercriminal activity. Investigators coordinated with private-sector cybersecurity partners to identify malicious infrastructure and issue alerts to affected organizations. Authorities say the operation highlights the scale of globally distributed cybercrime infrastructure and the importance of cross-border intelligence sharing.

Al-Qaeda-Aligned Hacktivists Call for Global “Cyber Jihad”

+Cyber Jihad Movement +Al-Qaeda +US +Israel +Pakistan +India +DDoS

- A hacking collective known as the [Cyber Jihad Movement \(CJM\)](#), aligned with Al-Qaeda, released a statement calling for a global “cyber jihad” targeting government systems in the United States, Israel, Pakistan, India, and several Arab states. The manifesto, circulated on encrypted jihadist platforms, urged supporters to participate in cyber operations as part of broader geopolitical conflicts involving Iran, the U.S., and regional actors. CJM has previously conducted distributed-denial-of-service (DDoS) attacks and website defacements against government and infrastructure targets. Analysts warn the announcement could encourage hacktivist activity and digital propaganda campaigns tied to extremist networks.

Glassworm Supply Chain Campaign Infects Hundreds of Dev Repositories

+Glassworm +Code Repository

- Researchers uncovered a large-scale supply chain campaign dubbed [Glassworm](#), which compromised over 400 code repositories across GitHub, npm, VSCode Marketplace, and OpenVSX. The malicious packages were designed to appear legitimate while delivering backdoor functionality capable of data exfiltration and remote command execution. The campaign specifically targeted developers by poisoning widely used open-source ecosystems, increasing the likelihood of downstream compromise in enterprise environments. The breadth of platforms affected highlights the growing risk of software supply chain attacks at scale.

Breathalyzer Outage Locks Drivers Out After Cyber Incident

+Automotive

- A cyberattack against a company providing [car breathalyzer](#) (ignition interlock) systems caused widespread outages, preventing drivers from starting their vehicles. The disruption impacted thousands of users who rely on the systems for legal driving compliance, effectively immobilizing vehicles across multiple states. While details of the attack vector were not fully disclosed, the incident demonstrates how cyber disruptions to embedded or regulated systems can have immediate real-world consequences. The event raises concerns around resilience and fail-safes in connected automotive control technologies.

Data Breaches

Hacktivists Claim Disruption of Major Medical Device Firm

+Iran +US +Healthcare

- Pro-Iran hacktivists claimed responsibility for a cyberattack that caused a global network disruption at U.S. medical device manufacturer [Stryker](#). The company reported outages affecting its Microsoft environment and systems used by employees

worldwide, including operations in Ireland. While Stryker said it had no evidence of ransomware or malware and believed the incident was contained, reports indicated some employee devices were wiped and access to corporate systems was disrupted. The company produces critical medical equipment used by hospitals globally, potentially affecting services supporting more than 150 million patients.

Salesforce Data Theft Campaign Targets Hundreds of Companies

+ShinyHunters +Salesforce +Experience Cloud

- The cybercrime group [ShinyHunters](#) claims to have stolen sensitive data from hundreds of companies by targeting poorly secured Salesforce portals and Experience Cloud instances. The attackers reportedly used modified tools to scan public-facing sites and extract data from misconfigured environments, potentially impacting up to 400 organizations. Stolen information is now being used for extortion, with the group threatening to leak the data unless victims pay a ransom. Salesforce stated the activity was not due to a vulnerability in its platform but rather security misconfigurations and external tooling abuse.

Ransomware Gang Claims Breach of Major Bahrain Hospital

+Payload +Bahrain +Healthcare

- The Payload ransomware group claimed responsibility for breaching [Royal Bahrain Hospital](#), one of the country's major healthcare providers. The attackers allege they exfiltrated approximately 110 GB of sensitive data, publishing evidence of compromised systems on their Tor leak site. The gang is threatening to release the stolen data publicly if ransom demands are not met before the announced deadline. Healthcare organizations remain frequent ransomware targets due to the sensitivity and operational importance of patient and clinical data.

Phishing Attack Exposes Starbucks Employee Data

+Phishing +Food & Beverage

- A phishing campaign targeting [Starbucks'](#) Partner Central employee portal resulted in unauthorized access to employee accounts and the exposure of personal data. Investigators found that attackers harvested credentials through fake login pages designed to mimic the legitimate portal before accessing internal systems. The breach impacted approximately 889 Starbucks employees, though no customer payment data was reported compromised. The incident highlights the ongoing risk of credential-theft attacks against corporate employee platforms.

Crunchyroll Users Impacted by Third-Party Telecom Breach

+Entertainment +Third-party

- User data associated with anime streaming service [Crunchyroll](#) was reportedly exposed following a breach linked to telecom provider TELUS. The incident appears to stem from a third-party compromise rather than a direct breach of Crunchyroll systems, highlighting supply chain and vendor risk. Exposed data may include customer information tied to telecom services, though full impact details remain limited. The breach underscores how organizations can be indirectly affected by security failures within partner ecosystems.

LAPSUS\$ Claims Deeper Access in AstraZeneca Data Breach

+LAPSUS\$ +Healthcare

- The LAPSUS\$ hacking group disclosed additional details about its breach of pharmaceutical giant [AstraZeneca](#), claiming access to a broader set of internal data than previously reported. The group alleges it obtained sensitive corporate and potentially research-related information, using its typical extortion tactics of threatening public release. While AstraZeneca has not fully confirmed the extent of the breach, the claims align with LAPSUS\$' history of targeting high-profile organizations through credential theft and social engineering. The incident highlights ongoing risks to intellectual property and sensitive healthcare data.

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.