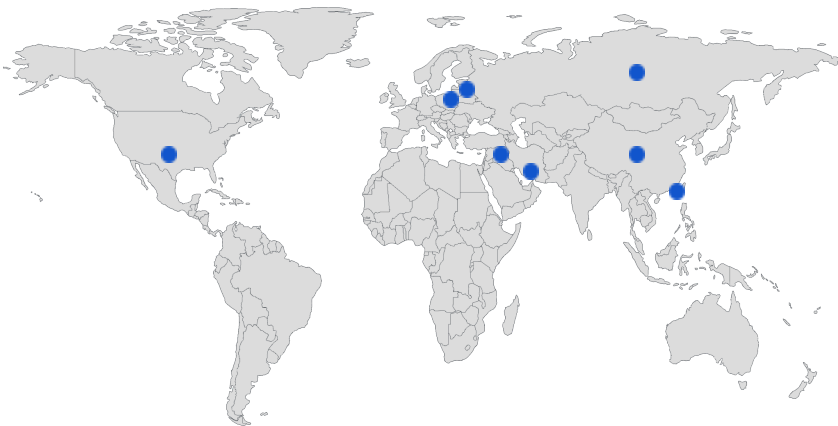


Threat Intel Report: September 9-15, 2024

Countries



Top Tags

APT34

Crimson Palace

TiDrone

Rambo

Pixhell

Executive Summary

Actionable Information:

- **Emerging AI and Automation Threats:** The use of AI and bots for fraudulent activities, as seen in the \$10 million streaming royalties fraud case, highlights an increasing trend of exploiting automated systems for financial gain. This underscores the need for enhanced detection and mitigation strategies for AI-driven fraud in digital platforms.
- **Geopolitical Cyber Espionage:** Iranian-linked APT34 and the Chinese Crimson Palace group are intensifying cyber-espionage operations, targeting government entities and strategic sectors in Iraq and Asia respectively. This trend emphasizes the ongoing geopolitical tensions and the strategic importance of cyber defense in protecting national and industrial secrets.
- **Critical Vulnerabilities and Zero-Day Exploits:** Several critical vulnerabilities have been disclosed this week, including those affecting Apache OFBiz, GeoServer, and Cursor AI. These vulnerabilities enable remote code execution and data exfiltration, stressing the importance of timely patching and securing software development environments.
- **Data Breaches and Third-Party Risks:** High-profile data breaches affecting organizations like 23andMe, Fortinet, and Capgemini demonstrate the persistent risk of third-party vendor vulnerabilities. This highlights the need for robust third-party risk management and comprehensive security assessments to protect sensitive data.

Outlook:

The cybersecurity landscape is increasingly defined by sophisticated, AI-driven attacks and critical software vulnerabilities. The escalation of cyber-espionage activities from state-sponsored actors suggests a growing threat to national security and industrial integrity, particularly in sectors like aerospace and telecommunications. With data breaches affecting high-profile companies and critical infrastructure, organizations must prioritize proactive threat detection and response strategies. As cyber threats continue to evolve, maintaining robust security practices, including

regular vulnerability assessments and strengthening third-party controls, will be crucial for mitigating risks and protecting sensitive information.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

📈 5133% [CVE-2023-40044](#)

- In WS_FTP Server, a pre-authenticated attacker could leverage a .NET deserialization vulnerability in the Ad Hoc Transfer module to execute remote commands on the underlying WS_FTP Server operating system.

📈 113% [CVE-2023-38035](#)

- A security vulnerability in MICS Admin Portal in Ivanti MobileIron Sentry, which may allow an attacker to bypass authentication controls on the administrative interface due to an insufficiently restrictive Apache HTTPD configuration.

📈 87% [CVE-2023-34960](#)

- A command injection vulnerability in the wsConvertPpt component of Chamilo allows attackers to execute arbitrary commands via a SOAP API call with a crafted PowerPoint name.

German Sites Targeted in WS_FTP CVE Attack

+Germany +CVE

- Two German sites were targeted this week with attacks attempting to exploit CVE-2023-40044, a .NET deserialization vulnerability in WS_FTP server. Attacks came from bots and tools written in Go.

US Technology Company Targeted by Automated Attacks

+US +Technology

- A US-based technology site was targeted this week by automated attacks, coming from IPs with an average risk score of 51%. The attacks, which reached 2.7M requests, came from US-based IPs, and targeted the site's subscriptions portal.

Recent Cyber Threats

Musician Accused of \$10M Fraud Using AI and Bots for Streaming Royalties

+AI Fraud +Music +Streaming

- A musician has been charged with a \$10 million [fraud scheme](#) in which AI and bots were used to artificially inflate streaming numbers to collect royalties. The artist allegedly created thousands of fake accounts and used automated systems to simulate streams on platforms like Spotify and Apple Music. This incident raises concerns about the vulnerability of digital music platforms to AI-driven fraud.

Iran-Linked Hackers Target Iraq Government Agencies

+Iran +Iraq +Government +APT34

- Iran-linked threat actors are targeting government agencies in [Iraq](#), aiming to gather intelligence on political and military operations. The hacking campaign, attributed to a group known as APT34 (OilRig), focuses on stealing sensitive government documents and exploiting vulnerabilities in Iraqi networks. This marks an escalation in cyber espionage activities between the two countries.

Chinese 'Crimson Palace' Hacking Group Targets Asian Countries

+China +Crimson Palace +Government

- The Chinese cyber-espionage group known as [Crimson Palace](#) continues to target governments and organizations in Asia. Active for several years, this group specializes in exploiting vulnerabilities in government networks to steal sensitive data. Their operations have been linked to geopolitical objectives, primarily focusing on strategic intelligence collection across the region.

Poland Dismantles Russian-Belarusian Cyber Sabotage Group

+Poland +Belarus +Russia +Energy +Government +Transportation

- Poland's Internal Security Agency has dismantled a [cyber sabotage group](#) with links to Russia and Belarus. The group had been planning cyberattacks on critical infrastructure, including energy and transport sectors, as part of a broader campaign of political and military disruption. The arrest of several members highlights the ongoing cyber tension between Eastern European countries.

Critical Apache OFBiz Vulnerability Allows RCE

+CVE +RCE

- Recently, a critical vulnerability in the widely used [Apache OFBiz](#) framework was disclosed, designated CVE-2024-45195. This vulnerability allows an attacker without valid credentials to exploit missing view authorization checks in the web application, bypassing previous patches, and ultimately executing arbitrary code on the server.

Cursor Trust Setting Vulnerability Exposes Applications to Attacks

+AI +Code Assistant

- Imperva Threat Research has discovered a security vulnerability in the [Cursor](#) AI code assistant tool, which disables a trust setting for managing third-party code execution. This missing feature exposes developers using Cursor to potential malicious activity, as the tool can inadvertently run untrusted or harmful code snippets.

Critical GeoServer Vulnerability Fuels Global Hack Campaigns

+Geospatial

- A critical vulnerability in [GeoServer](#), an open-source software for geospatial data management, is being actively exploited in global hack campaigns. Attackers are leveraging this flaw to gain unauthorized access to sensitive geospatial data, impacting organizations worldwide. This vulnerability has sparked widespread concern, especially in industries relying on accurate geospatial information for operations.

Rambo Attack Steals Data from Air-Gapped Systems via RAM

+Rambo +Data Exfiltration

- A new attack method called [Rambo](#) has been developed to steal sensitive data from air-gapped computers using RAM. This technique allows attackers to extract data from isolated systems by exploiting the physical properties of RAM to transmit signals covertly. The method poses a significant risk to highly secure environments where air-gapped systems are traditionally viewed as safe from remote attacks.

Gallup Website XSS Bugs Expose Visitors to Attacks

+XSS +Polling

- Multiple cross-site scripting (XSS) vulnerabilities have been discovered on [Gallup's](#) website, potentially exposing visitors to attacks. These flaws could allow malicious actors to inject malicious code into the site, leading to the theft of sensitive user information or session hijacking. Gallup is working on patching the vulnerabilities to prevent exploitation and ensure user safety.

Pixhell Acoustic Attack Extracts Data from LCD Screens

+Pixhell +Acoustic Attack

- Researchers have developed the [Pixhell](#) acoustic attack, which can leak sensitive data from LCD screens by analyzing the sounds generated by the display's operations. This novel method allows attackers to extract information without needing physical access to the target system, presenting a new threat to environments where visual data confidentiality is crucial.

Data Breaches

23andMe Faces Lawsuit Over Genetic Data Breach

+Healthcare

- [23andMe](#), a DNA testing company, is facing a class-action lawsuit following a breach where hackers accessed user genetic data. The data breach, which occurred in October 2023, compromised sensitive health and ancestry information of nearly 7 million customers. The lawsuit alleges negligence and lack of security protocols, raising concerns about personal and genetic data privacy.

Fortinet Customer Data Exposed by Third-Party Breach

+Cybersecurity +Third-Party

- [Fortinet](#), a global cybersecurity firm, disclosed a data breach impacting customer information due to a third-party supplier compromise. The breach exposed personal data, including names, emails, and encrypted passwords of some customers. Fortinet has assured that its systems were not compromised and has notified affected users while working to enhance third-party security measures.

Capgemini Data Breach Exposes T-Mobile VM Logs

+Telecommunications +Third-Party

- A data breach involving Capgemini, a global consulting firm, has exposed virtual machine (VM) logs belonging to [T-Mobile](#). The 20 GB of leaked logs included sensitive data, such as customer information and configurations. This breach adds to a series of cybersecurity incidents targeting T-Mobile, raising concerns about the security of telecom infrastructures.

Platinum Mining Company Suffers Data Breach

+US +Mining

- [Stillwater Mining Company](#), one of Montana's largest platinum mining firms, disclosed a data breach that affected sensitive corporate and employee data. The breach, which occurred in 2024, has raised concerns about the security of industrial operations and supply chain vulnerabilities in the mining sector. Stillwater is currently investigating the incident with cybersecurity experts.

Taiwan Drone Manufacturer Hit by 'TiDrone' Cyberattackers

+Aerospace +Manufacturing +Taiwan

- A cyber-espionage group named [TiDrone](#) has been targeting Taiwan's aerospace industry. This advanced persistent threat (APT) group specializes in stealing sensitive information related to drone manufacturing and military applications. The attacks have raised serious concerns about national security and industrial espionage, as Taiwan's drone industry is crucial to its defense and technological infrastructure.

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.