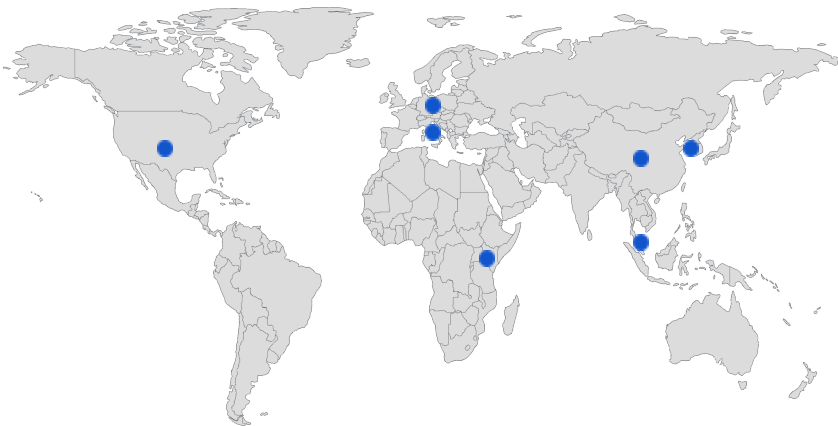


Threat Intel Report: September 23-29, 2024

Countries



Top Tags

Sniper-DZ

Vanir

Salt Typhoon

SambaSpy RAT

AI

Executive Summary

Actionable Information:

- **Critical Infrastructure Vulnerabilities:** Recent attacks on a Kansas water plant, automated tank gauge (ATG) systems, and an unnamed U.S. ISP underscore the continued vulnerability of critical infrastructure. Utilities and energy sectors remain key targets for both criminal and nation-state actors, highlighting the need for heightened defenses and incident response planning in these sectors.
- **Exploitation of Open-Source Platforms:** Malicious actors are increasingly using trusted platforms like PyPI and WordPress to distribute malware or exploit vulnerabilities. Organizations using open-source tools should implement additional security measures to detect compromised libraries and plugins.
- **Evolving Phishing and Ransomware Threats:** The rise of phishing-as-a-service and continued ransomware campaigns point to a growing sophistication in these attack vectors. These threats increasingly target corporations and critical sectors, with phishing attacks evading traditional defenses and ransomware groups being actively pursued by law enforcement.
- **AI-Driven Cybercrime:** The use of AI-written malware and vulnerabilities in AI-powered tools like macOS ChatGPT signals the rise of AI as both an offensive and defensive weapon in cybersecurity. Organizations should prepare for more sophisticated, adaptive malware that can evade standard detection methods.

Outlook:

The cybersecurity landscape is becoming more complex, with critical infrastructure, financial services, and evolving technologies (e.g., AI and IoT) facing increasing threats from both sophisticated nation-state groups and opportunistic cybercriminals. We anticipate that AI-driven malware and phishing-as-a-service platforms will continue to evolve, forcing defenders to adopt more advanced detection techniques. Additionally, the growing number of vulnerabilities in



open-source software and the expanding attack surface of connected devices will push organizations to reassess their security postures, particularly in sectors that are critical to national security and daily operations. Government and industry cooperation in areas like ransomware takedowns and espionage-related breaches will likely increase in response to these growing threats.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

📈 430% [CVE-2024-20767](#)

- ColdFusion is affected by an Improper Access Control vulnerability that could lead to arbitrary file system read.

📈 116% [CVE-2023-34362](#)

- A SQL injection vulnerability in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database.

📈 104% [CVE-2024-23898](#)

- Jenkins does not perform origin validation of requests made through the CLI WebSocket endpoint, resulting in a cross-site WebSocket hijacking (CSWSH) vulnerability that allows attackers to execute CLI commands on the Jenkins controller.

Italian Energy Company Hit By Bot Attack

+Italy +Energy +RCE +Path Traversal +XSS +Bad Bot

- An Italian energy company was targeted in an attack leveraging several intrusion methods, including Remote Code Execution (RCE), Path Traversal, and Cross-Site Scripting (XSS). This attack, which reached over 2M requests, came from US-based bots.

Kenyan Telecommunications Site Targeted by Path Traversal

+Kenya +Telecommunications +Path Traversal

- This week, a Kenyan telecommunications company was targeted by Path Traversal attacks, where attackers exploited vulnerabilities to access restricted directories on the company's servers. The attacks were carried out using tools written in Go, which enabled the attackers to attempt to navigate and manipulate file systems.

Recent Cyber Threats

Federal Investigation Launched into Kansas Water Plant Cyberattack

+US +Government +Utilities

- A federal investigation has been initiated after a cyberattack targeted a [water treatment plant](#) in Kansas. The attack reportedly compromised the facility's operational systems, raising concerns about the vulnerability of critical infrastructure in the U.S. to cyber threats. The plant's operations were disrupted, but no details on the attackers or their motivations have been disclosed yet.

MoneyGram Services Disrupted by Major Cyber Attack

+Financial Services

- A cyber attack severely disrupted [MoneyGram's](#) money transfer services, knocking them offline for several days. The financial services company did not specify the attacker or method used, but this outage caused widespread

service issues across the U.S. and internationally. The incident highlights the financial sector's vulnerability to DDoS attacks and potential operational disruptions.

Sniper-DZ Phishing Platform Targets Businesses with Unique Tactics

+Sniper-DZ +Phishing

- Researchers have uncovered a phishing-as-a-service platform named [Sniper-DZ](#), designed to streamline the creation of targeted phishing campaigns, which is associated with over 140,000 scamming websites this year. The platform employs sophisticated evasion techniques, making it difficult for standard security tools to detect phishing attacks. Sniper-DZ primarily focuses on corporate targets and has impacted businesses globally.

German Authorities Seize Vanir Ransomware Leak Site

+Germany +Vanir +Ransomware

- German police have seized the leak site of the [Vanir](#) ransomware group as part of a broader crackdown on cybercriminal activities. The site, used by the group to publish stolen data from ransomware victims, has been taken offline, marking a significant blow to Vanir's operations. The seizure is a part of ongoing efforts by European law enforcement to combat ransomware.

Salt Typhoon Threat Group Breaches U.S. ISP in Espionage Campaign

+China +Salt Typhoon +Telecommunications +US

- [Salt Typhoon](#), a China-linked APT, successfully breached an unnamed U.S. internet service provider, gaining access to critical infrastructure. The attackers exploited vulnerabilities in the ISP's systems, potentially gaining the ability to intercept and manipulate network traffic. This incident adds to growing concerns over Chinese cyber espionage targeting U.S. communication networks.

SambaSpy RAT Targets Italian Users in Malware Campaign

+SambaSpy RAT +Italy +Malware

- A new malware campaign has been uncovered, targeting Italian financial institutions with the [SambaSpy RAT](#) (Remote Access Trojan). This unique malware, designed only to affect Italian-speaking users, utilizes custom phishing emails to gain access to systems and steal sensitive financial data. The campaign is believed to be financially motivated and represents a growing threat to European banking sectors.

Malicious PyPI Packages Target Roblox Cheaters

+Gaming +PyPI +Malware

- Hackers have been distributing malicious Python packages through PyPI, targeting [Roblox](#) users looking for cheat tools. The infected packages contain remote access trojans (RATs) that give attackers control over users' systems, allowing them to steal sensitive data or execute additional malicious actions. This highlights how threat actors exploit popular gaming communities to deliver malware.

Microchip ASF Flaw Exposes IoT Devices to Remote Attacks

+IoT +RCE

- Researchers have discovered a critical vulnerability in MediaTek's Microchip [Advanced Software Framework](#) (ASF), commonly used in IoT devices. The flaw could allow attackers to execute remote code, gaining control over devices. This vulnerability poses a significant risk to industries reliant on IoT technology, making millions of connected devices vulnerable to exploitation.

SQL Injection Found in WordPress Events Calendar Plugin

+SQLi +WordPress

- A critical SQL injection vulnerability (CVE-2024-8275) was discovered in the [Events Calendar](#) plugin, widely used by WordPress websites. Exploiting the flaw allows attackers to manipulate database queries, potentially gaining access to sensitive site information or taking full control of the affected site. The vulnerability affects millions of websites and highlights the ongoing risks to popular web plugins.

Critical Flaws Found in Automated Tank Gauge Systems

+ATG +Critical Infrastructure

- Security researchers have uncovered multiple vulnerabilities in [automated tank gauge](#) (ATG) systems, used by oil and gas companies to monitor fuel levels. These flaws could allow attackers to alter or shut down monitoring capabilities, potentially leading to fuel shortages or safety risks. The vulnerabilities expose critical industrial systems to cyber threats, emphasizing the need for stronger security in the energy sector.

macOS ChatGPT Flaw Opens Doors to Long-Term Exploitation

+spAIware +AI

- A critical flaw, called [spAIware](#), in the macOS ChatGPT application could have enabled attackers to exploit the system for long-term persistence. The vulnerability, which abuses an OpenAI feature called memory, would allow malicious actors to bypass security protections and remain undetected on a victim's device. This flaw underscores the security risks of AI applications and their integrations.

AI-Written Malware Used in Sophisticated Targeted Attacks

+AI +Malware

- Hackers are deploying [AI-written malware](#) in targeted attacks, taking advantage of the speed and sophistication of artificial intelligence to evade traditional detection methods. This new type of malware adapts to its environment, making it more difficult to analyze and defend against. The use of AI in malware creation marks a dangerous shift in the threat landscape.

Kia Portal Flaw Could Let Attackers Control Millions of Cars

+Automotive

- A vulnerability in [Kia's](#) dealer portal could allow attackers to exploit weak security protocols and gain access to millions of cars' systems. By exploiting this flaw, malicious actors could potentially manipulate vehicle settings or track the locations of connected cars. This security lapse highlights the growing cyber risks in the automotive industry as vehicles become more interconnected.

Data Breaches

\$44 Million Stolen from Crypto Platform in Singapore

+Crypto +Financial Services +Singapore

- A cryptocurrency platform in [Singapore](#) suffered a devastating breach, with hackers stealing \$44 million worth of digital assets. The attackers exploited vulnerabilities in the platform's security infrastructure, resulting in significant financial losses. This incident underscores the ongoing challenges of securing cryptocurrency exchanges against increasingly sophisticated cybercriminals.

Meta Fined \$91 Million for Illegally Storing European User Data

+Technology +GDPR

- [Meta](#) was fined \$91 million by European regulators for unlawfully storing user data in violation of the General Data Protection Regulation (GDPR). The social media giant was found to have retained sensitive information without proper consent, leading to a major privacy breach. This penalty reflects the increasing enforcement of data protection laws in the EU.

North Korean Hackers Linked to Breach of German Missile Manufacturer

+North Korea +Germany +Government +Defense

- [North Korean](#) hackers have been linked to a cyber attack on a German missile manufacturer, compromising sensitive defense information. The breach, likely conducted for espionage purposes, raises serious concerns about the security of critical defense infrastructure in Europe. This attack is part of a broader pattern of North Korean cyber operations targeting high-value military assets globally.
-



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.