

Threat Intel Report: January 13-26, 2025

Countries



Top Tags

Gsocket

Codefinger

OAuth

ALPHV

b0nd

Executive Summary

Actionable Information:

- **Exploitation of Zero-Day Vulnerabilities:** Attackers are leveraging previously unknown vulnerabilities to gain unauthorized access to systems, emphasizing the importance of proactive vulnerability management.
 - *Recommendation:* Regularly update and patch systems, prioritize vulnerability assessments, and monitor for unusual activity to mitigate zero-day exploitation risks.
- **Advanced Malware and Botnet Campaigns:** There is an uptick in the use of sophisticated malware and botnets to compromise servers and deploy malicious payloads, affecting various sectors.
 - *Recommendation:* Implement robust intrusion detection systems, conduct regular security audits, and ensure timely updates of web applications and plugins to defend against such campaigns.
- **Cloud Service Exploitation:** Threat actors are targeting cloud environments, exploiting misconfigurations and weak access controls to compromise data integrity.
 - *Recommendation:* Enforce strict access controls, monitor cloud environments for unauthorized activities, and regularly back up data to prevent and respond to such attacks.
- **Significant Data Breaches:** Recent incidents have resulted in the exposure of sensitive information of millions of individuals, highlighting vulnerabilities in data protection practices.
 - *Recommendation:* Enhance data encryption, implement comprehensive monitoring, and establish incident response plans to mitigate the impact of data breaches.

Outlook:

The cybersecurity landscape is witnessing a surge in sophisticated attacks exploiting both known and unknown vulnerabilities across various platforms and services. The increasing complexity of malware, coupled with targeted data breaches affecting millions, indicates that threat actors are becoming more adept and resourceful. Organizations must

adopt a proactive security posture, emphasizing regular system updates, continuous monitoring, and comprehensive incident response strategies to safeguard against these evolving threats.

Threat Activity in Imperva

Top CVE Growth This Week:

[Imperva customers are protected against these CVEs.](#)

📈 689% [CVE-2024-20767](#)

- ColdFusion versions 2023.6, 2021.12 and earlier are affected by an Improper Access Control vulnerability that could result in arbitrary file system read. An attacker could leverage this vulnerability to access or modify restricted files.

📈 80% [CVE-2024-45195](#)

- Direct Request ('Forced Browsing') vulnerability in Apache OFBiz.

📈 19% [CVE-2024-38856](#)

- Incorrect Authorization vulnerability in Apache OFBiz.

US Beverage Company Targeted in 13.5M RPS DDoS Attack

[+DDoS](#) [+US](#) [+Food & Beverage](#)

- A massive application-layer (layer 7) distributed denial-of-service (DDoS) attack targeted a US company in the Food & Beverage industry, with 13.5 million requests per second (RPS)—the largest we've seen this year. The attack, which came from over 7,000 unique IP addresses, lasted just 8 minutes.

Australian Government Site Hit In Attempted Command Injection Attacks

[+Australia](#) [+Government](#) [+Singapore](#)

- Recently, an Australian government website was hit by automated attacks targeting API sites, and attempting to conduct command injection attacks. Attacks came from Singapore and within Australia.

Recent Cyber Threats

Python Bots Exploit PHP Servers to Promote Gambling Sites

[+Python](#) [+Bad Bots](#) [+Gsocket](#) [+Indonesia](#) [+Gambling](#) [+Education](#)

- Imperva researchers have uncovered a campaign where Python-based bots compromise PHP servers to promote Indonesian gambling platforms. Attackers leverage tools like [GSocket](#) to establish persistent access, deploying PHP files that redirect users to gambling sites. This campaign has resulted in millions of malicious requests targeting web applications, particularly those running the Moodle learning management system.

Fortinet Firewalls Exploited via Suspected Zero-Day Vulnerability

[+Firewall](#) [+Zero-day](#)

- Attackers have conducted a mass exploitation campaign targeting [Fortinet FortiGate](#) firewalls with exposed management interfaces. Researchers believe a zero-day vulnerability was used to gain unauthorized access, alter configurations, and establish persistent connections through SSL VPN tunnels. This breach allowed the theft of credentials and potential lateral movement within affected networks.

'Codefinger' Group Encrypts AWS S3 Data Without Ransomware

+Codefinger +AWS

- The ['Codefinger'](#) cybercriminal group is encrypting data in AWS S3 buckets using AWS's server-side encryption with customer-provided keys (SSE-C). By leveraging compromised AWS keys, they encrypt data without exfiltration and demand ransom for the decryption key. The attackers also set encrypted files for deletion within seven days to pressure victims into paying.

Google OAuth Flaw Allows Account Takeover via Expired Domains

+Google +OAuth +ATO

- A vulnerability in Google's [OAuth](#) implementation permits attackers to take over accounts by acquiring expired domains of defunct startups. By recreating email addresses associated with these domains, attackers can access various SaaS applications, including HR systems containing sensitive personal information.

WP3.XYZ Malware Compromises Over 5,000 WordPress Sites

+WordPress +Malware

- A [malware campaign](#) has breached more than 5,000 WordPress websites, creating rogue admin accounts and installing a malicious plugin. The malware exfiltrates sensitive data, including administrator credentials and logs, to the attacker's server disguised as image requests. Website owners are advised to block the 'wp3[.]xyz' domain to prevent further infections.

Critical Flaws in LTE and 5G Networks Could Disrupt City-Wide Communications

+Telecommunications

- Researchers have identified 119 security vulnerabilities across various [LTE and 5G implementations](#), particularly in the Radio Access Network-Core interfaces. Exploiting these flaws could allow attackers to disrupt cellular services on a city-wide scale, track user locations, and exfiltrate connection details for targeted attacks. Many of these vulnerabilities were found in Mobile Management Entity implementations, with 25 enabling pre-authentication attacks using arbitrary devices.

ChatGPT API Vulnerability Enables Potential DDoS Attacks

+AI +ChatGPT +DDoS

- A severe vulnerability in [ChatGPT's](#) API allowed attackers to initiate distributed denial-of-service (DDoS) attacks by sending a single HTTP request containing numerous hyperlinks. This flaw, resulting from inadequate input validation, enabled the API to overwhelm target websites with excessive traffic. OpenAI has since addressed the issue by disabling the vulnerable endpoint.

Unsecured Tunneling Protocols Expose Millions of Hosts to Attacks

+DoS +Routers

- Research indicates that over [4.2 million hosts](#), including VPN servers and routers, are vulnerable due to unsecured tunneling protocols like IP6IP6, GRE6, 4in6, and 6in4. These vulnerabilities allow attackers to hijack systems for anonymous attacks, unauthorized network access, and denial-of-service (DoS) attacks. The issue stems from a lack of authentication and encryption in these protocols, underscoring the need for implementing security measures.

Data Breaches

UnitedHealth Data Breach Affects 190 Million Americans

+Healthcare +ALPHV +US

- UnitedHealth Group recently revealed that the February 2024 data breach experienced by its subsidiary, Change Healthcare, compromised the personal information of approximately 190 million individuals—1 in 2 Americans. The breach, attributed to BlackCat (ALPHV) exposed sensitive data, including health insurance details, medical records, billing information, and Social Security numbers. This incident is considered the

largest healthcare data breach in U.S. history, leading to significant disruptions in insurance claim processing and an estimated financial impact of \$3.09 billion for UnitedHealth.

AT&T Data Breach Exploited to Target Political Figures

+Government +Telecommunications +US

- Hackers breached [AT&T's](#) data systems, accessing call and text metadata of nearly all customers between May and October 2022. They specifically searched for records associated with prominent individuals, including members of the Trump family, Vice President Kamala Harris, and Senator Marco Rubio's wife. The breach not only compromised personal communications but also posed significant national security risks.

Crunchyroll Confirms Data Breach Involving Premium Accounts

+Streaming +Entertainment

- Anime streaming service [Crunchyroll](#) confirmed a data breach where an anonymous individual posted login credentials of premium users on social media. The company stated that its systems were not compromised and advised users to change their passwords regularly and monitor their accounts for suspicious activity. No financial information was reported as exposed.

TalkTalk Investigates Alleged Customer Data Breach

+UK +Telecommunications +b0nd

- UK telecom company [TalkTalk](#) is investigating claims of a data breach after a hacker, known as "b0nd," alleged the theft of data from approximately 18.8 million current and former customers. The exposed information reportedly includes names, email addresses, IP addresses, and phone numbers. TalkTalk has stated that no billing or financial information was compromised and is working with a third-party supplier, CSG Ascendon, to assess the situation.

Otelier Data Breach Exposes Marriott and Hilton Guest Information

+Travel

- Hotel management platform [Otelier](#) suffered a data breach, exposing sensitive customer data from major hotel chains, including Marriott and Hilton. Hackers reportedly exfiltrated 7.8 terabytes of data, encompassing hotel guest reservations, employee emails, transaction information, and other internal data. Hundreds of thousands of email addresses were compromised, with some records also revealing guests' names, addresses, and phone numbers.

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.