

Countries



Top Tags

dCRAT

Plugin

Salt Typhoon

PyPI

Telecommunications

Executive Summary

Actionable Information:

- **Increase in Telecom and Critical Infrastructure Breaches:** Recent breaches at Comcast, AT&T, Verizon, and American Water Works indicate a rising trend in targeting critical infrastructure sectors. These attacks expose sensitive customer data, compromise national security, and highlight the importance of robust cybersecurity measures in critical services like utilities and telecommunications.
- **Growing Threat from Nation-State Actors:** Chinese hackers have been implicated in a major breach involving U.S. telecom companies, stealing wiretap and sensitive data. This reinforces concerns about espionage and the national security risks posed by advanced persistent threats (APTs), particularly from adversarial nation-states.
- **Expanding Threat to Open-Source Ecosystems:** A series of incidents involving malicious packages on the PyPI repository continues to reveal vulnerabilities within the open-source community. These attacks, which involve stealing cryptocurrency wallet keys and distributing malware to developer environments, emphasize the need for enhanced vetting and monitoring in open-source software repositories.
- **Ransomware and Data Theft on the Rise:** Ransomware, such as the INC ransomware targeting U.S. healthcare systems, continues to be a major concern. Healthcare remains a high-value target due to the sensitive nature of the data it handles. Additionally, large-scale data thefts, such as the Comcast and American Water Works breaches, underscore the need for more stringent data protection strategies across industries.

Outlook:

The cybersecurity landscape continues to evolve with a sharp rise in attacks on critical infrastructure, telecoms, and open-source ecosystems. Nation-state actors, particularly from China, are increasingly involved in highly sophisticated breaches aimed at stealing sensitive data and conducting espionage. Meanwhile, ransomware groups are broadening

their scope, particularly within the healthcare sector, to exploit vulnerable systems and demand high ransom payments. In the coming months, organizations should prepare for more frequent and targeted attacks, particularly in sectors involving critical services, and should prioritize security measures to protect sensitive data, enhance monitoring of open-source code, and improve incident response strategies.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

📈 175% [CVE-2023-26009](#)

- Improper Privilege Management vulnerability in favethemes Houzez Login Register allows Privilege Escalation.

📈 151% [CVE-2023-6553](#)

- The Backup Migration plugin for WordPress is vulnerable to Remote Code Execution.

📈 71% [CVE-2024-3400](#)

- Command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software.

Indonesian Government Site Targeted by 12-Hour DDoS Attack

+Indonesia +Government +DDoS

- An Indonesian government site was targeted by DDoS this week, reaching 1.3 million Requests per Second (RPS) in an almost 12-hour attack. This site has been frequently targeted by DDoS in the past few months, with attacks reaching up to 5 million RPS.

Travel Site Hit By 15M Request Business Logic Attack

+Travel +Business Logic +US +France

- A global travel site was targeted by business logic attacks, totaling almost 15M requests over two days. The attacks primarily came from the US and France, and used bots and the Chrome browser.

Recent Cyber Threats

VSCode Exploit Enables Remote Access on Compromised Systems

+VSCode +RCE

- Attackers are exploiting the popular Visual Studio Code ([VSCode](#)) to gain remote access to developer systems. The attack leverages malicious extensions that enable threat actors to control machines by executing arbitrary code. Researchers warn of potential widespread impact due to VSCode's popularity among developers.

First Mobile Crypto Drainer Targeting Google Play Users

+Crypto +Android

- Security researchers uncovered the first known [mobile crypto drainer](#) targeting Android devices via Google Play. The malicious app mimics legitimate services to drain cryptocurrency wallets of unsuspecting users. This new type of attack highlights the need for stronger protections on mobile platforms to defend against cryptocurrency theft.

dCRAT Malware Leveraging HTML Smuggling Techniques

[+dCRAT](#) [+Malware](#) [+HTML Smuggling](#) [+RAT](#)

- [dCRAT](#) malware is deploying HTML smuggling techniques to infect systems and steal sensitive information. This technique allows attackers to bypass security filters by embedding malicious payloads directly into web content. The campaign is targeting users across multiple industries, posing a significant risk to enterprises.

Severe SQL Injection Vulnerability in WooCommerce Wishlist Plugin

[+SQLi](#) [+WordPress](#) [+Plugin](#) [+WooCommerce](#)

- A critical SQL injection vulnerability ([CVE-2024-43917](#)) has been identified in the WooCommerce Wishlist plugin, impacting over 100,000 websites. The flaw, with a CVSS score of 9.3, remains unpatched and could allow attackers to steal sensitive data or take control of affected sites. Site administrators are urged to apply protective measures.

New Phishing Campaign Lures Victims with P. Diddy Scandal

[+Phishing](#) [+RAT](#)

- A sophisticated phishing campaign is using the recent P. Diddy scandal as bait to distribute a [remote access trojan](#) (RAT). The malicious emails trick users into downloading the RAT, which can steal data, monitor activities, and control infected devices. The attack is targeting individuals and organizations globally.

Infected PyPI Packages Target Roblox Cheaters with Malware

[+PyPI](#) [+Roblox](#) [+Gaming](#)

- Malicious actors are exploiting infected PyPI packages to target [Roblox](#) cheaters, deploying malware through fake cheat tools. These packages, once installed, deliver backdoors that allow attackers to control compromised systems and steal sensitive information. The gaming community, especially those using cheat tools, is at heightened risk.

PyPI Malware Steals Crypto Wallet Private Keys

[+PyPI](#) [+Crypto](#)

- New malware hosted on the [PyPI](#) repository is stealing private keys from cryptocurrency wallets. The malware is embedded in seemingly harmless packages, which, once installed, extract sensitive wallet information and send it to the attackers. This highlights the continued risk of malicious software in open-source ecosystems.

LiteSpeed Cache Plugin Vulnerability Puts Millions of WordPress Sites at Risk

[+Plugin](#) [+RCE](#) [+WordPress](#)

- A severe vulnerability ([CVE-2024-47374](#)) in the LiteSpeed Cache plugin affects millions of WordPress sites globally. Exploiting this flaw could allow attackers to execute arbitrary code, potentially leading to data breaches and website defacements. Site administrators are urged to update their plugins immediately to mitigate the risk.

Data Breaches

Comcast Faces Data Breach, Exposing SSNs and Personal Data

[+Telecommunications](#) [+US](#)

- [Comcast](#) has suffered a significant data breach, exposing sensitive personal information, including Social Security Numbers and names of customers. The compromised data could potentially be used for identity theft or fraud. Comcast is investigating the breach, but it underscores the vulnerabilities faced by large telecom companies in protecting customer data.

Chinese Hackers Breach AT&T and Verizon, Steal Sensitive Data

[+China](#) [+Telecommunications](#) [+Salt Typhoon](#)

- Chinese hackers, known as [Salt Typhoon](#), have reportedly infiltrated the networks of AT&T, Verizon, and Lumen Technologies, stealing sensitive wiretap data in a massive breach. The attack poses a significant threat to U.S.



national security, as the stolen data could be used for surveillance and espionage. Both telecom giants are working with federal authorities to assess the damage and tighten security.

American Water Works Hit by Security Breach, Impacting Critical Systems

+US +Utilities

- [American Water Works](#), one of the largest water utility companies in the U.S., has been targeted in a cyberattack that compromised sensitive operational data. The breach could potentially disrupt water services or expose critical infrastructure vulnerabilities. Investigations are underway to determine the extent of the damage and ensure the safety of the nation's water supply systems.

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.