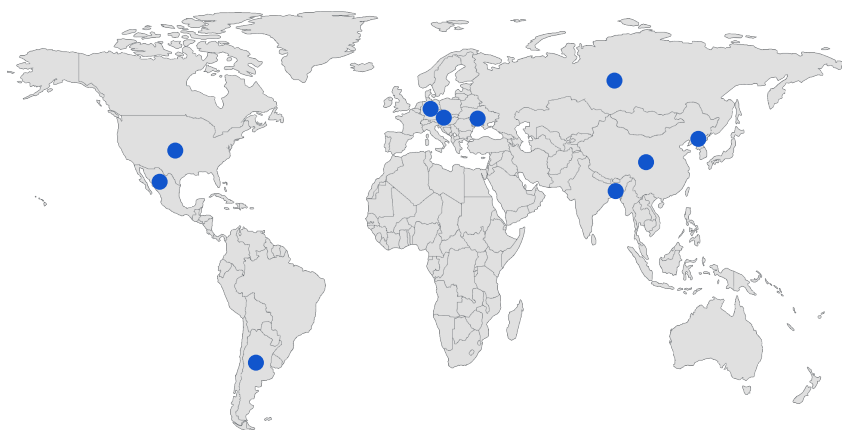


Threat Intel Report: December 30, 2024-January 5, 2025

Countries



Top Tags

OtterCookie

TrueNAS

NGate

Tor

Salt Typhoon

Executive Summary

Actionable Information:

- **Rising Complexity of Cyber Attacks:** The trend toward more sophisticated, multi-faceted cyber-attacks is clear. Attackers are increasingly leveraging social engineering tactics combined with technical exploits, making these threats harder to detect and prevent. As the methods used by threat actors evolve, organizations must adapt their security measures to address the growing complexity of these campaigns.
- **Vulnerability Management and Patching:** There is an ongoing need for robust vulnerability management. A critical trend in the current threat landscape is the exploitation of unpatched vulnerabilities in both software platforms and hardware systems. Ensuring timely patching and the adoption of proactive security measures remains crucial in mitigating risks from these persistent weaknesses.
- **Email and Data Encryption Gaps:** A significant trend in data security is the widespread lack of encryption in basic communication channels, such as email. The absence of essential security protocols like TLS for mail servers is exposing sensitive data to interception. Organizations should prioritize encryption across all communication platforms to prevent the leakage of sensitive information.
- **Targeted Attacks on High-Value Targets:** Cybercriminals and state-sponsored actors continue to focus on high-value industries, such as healthcare, finance, and telecommunications. These sectors are particularly vulnerable due to the sensitive nature of their data and the potential for large-scale disruption. Strengthening defenses in these critical sectors is essential to preventing breaches and service interruptions.

Outlook:

The outlook for the cybersecurity landscape points toward a continuation of current trends, with cyber-attacks becoming more complex and targeted. As threat actors refine their methods, organizations will need to place greater emphasis on advanced threat detection, encryption, and vulnerability management. The increasing focus on high-value industries suggests that these sectors will be prime targets for future attacks, making cybersecurity a top priority. As

attackers continue to exploit technical flaws and human vulnerabilities, organizations must adopt a holistic approach to security, integrating proactive defenses and employee education to stay ahead of the threat curve.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

📈 357% [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.

📈 255% [CVE-2024-45195](#)

- Direct Request ('Forced Browsing') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 18.12.16.

📈 244% [CVE-2024-21893](#)

- A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication.

Argentinian Financial Site Targeted in 3.2M RPS DDoS Attack

[+Argentina](#) [+Financial Services](#)

- An Argentinian financial services site was hit by a 3.2M requests per second (RPS) application-layer DDoS attack. The attack came from just under 2,500 IP addresses.

Attackers Try to Scrape Mexican Retail Sites

[+Mexico](#) [+US](#) [+Czechia](#) [+Business Logic](#)

- A Mexican retail site was targeted by business logic attacks attempting to scrape inventory and product data. The attack came from primarily United States- and Czechia-based IP addresses.

Recent Cyber Threats

North Korean Hackers Deploy OtterCookie Malware

[+North Korea](#) [+Contagious Interview](#) [+OtterCookie](#)

- North Korean hackers, operating under the [Contagious Interview](#) campaign, have deployed a new JavaScript malware named OtterCookie to steal sensitive data. The malware, often disguised as a legitimate job interview process, targets cryptocurrency wallet keys, clipboard content, and files. It's spread through malicious videoconferencing apps and npm packages, continuing a broader social engineering campaign associated with North Korea's cyber-espionage operations.

Critical Vulnerability in TrueNAS CORE Allows Remote Code Execution

[+TrueNAS](#) [+RCE](#)

- A critical vulnerability (CVE-2024-11944) in [TrueNAS CORE](#), an open-source storage operating system, enables network-adjacent attackers to execute arbitrary code on affected systems. This flaw results from improper validation in the tarfile.extractall method, allowing directory traversal attacks. Without authentication

or user interaction, this vulnerability could give attackers root privileges, compromising system confidentiality, integrity, and availability. A patch has been released to address the issue.

GStreamer Vulnerabilities Threaten Linux Systems

+GStreamer +Linux

- A series of 29 vulnerabilities in the [GStreamer](#) multimedia framework threatens millions of Linux systems, including those running Ubuntu, Fedora, and openSUSE. These vulnerabilities, primarily affecting MP4 and MKV formats, could allow attackers to execute arbitrary code, cause crashes, or leak sensitive data. GStreamer, integral to applications like Nautilus and GNOME Videos, is widely used in Linux environments, making these flaws critical to address. A custom fuzzing method was used to identify these vulnerabilities, and users are urged to update their systems immediately.

NGate Trojan Drains Bank Accounts Using NFC

+NGate +Trojan +Russia +Czechia

- The [NGate](#) banking trojan is exploiting Near Field Communication (NFC) capabilities to steal funds from victims' accounts via ATMs and contactless payments. The trojan, which spreads through social engineering and phishing, prompts victims to install malicious apps disguised as official government or bank services. Once installed, NGate uses NFC to capture sensitive card data, which attackers then use to withdraw cash or make purchases. The malware targets Russian users but has previously affected other regions, including Czechia.

LLM Jailbreak Technique Exploits Evaluation Capabilities

+LLM +AI

- Researchers have identified a novel multi-turn technique, [Bad Likert Judge](#), that exploits large language models' (LLMs) evaluation capabilities to bypass safety measures. By prompting LLMs to act as judges scoring the harmfulness of responses using the Likert scale, attackers can generate content that aligns with higher harmfulness scores, potentially leading to the production of unsafe or inappropriate content. This technique has demonstrated an increased attack success rate by more than 60% compared to plain attack prompts across various LLMs.

Over 3 Million Mail Servers Exposed to Sniffing Attacks

+Mail +TLS

- Over three million POP3 and IMAP mail servers [lack TLS encryption](#), rendering them vulnerable to network sniffing attacks. Without TLS, email contents and credentials are transmitted in plaintext, allowing attackers to intercept sensitive information. This widespread exposure underscores the critical need for implementing encryption protocols to safeguard email communications.

Critical Active Directory Flaw Threatens Microsoft Servers

+Microsoft

- A critical vulnerability in Active Directory's [LDAP protocol](#) can be exploited to crash multiple unpatched Windows servers simultaneously. The attack chain could be used by a threat actor to achieve RCE or exploited to crash any Windows server, if the target system's domain controller has a DNS server connected to the Internet. This flaw poses a significant risk to organizations that have not applied the latest security patches.

Stealthy Malware Targets Ukrainian Military via SSH Over Tor

+Tor +Ukraine +Government

- A sophisticated malware campaign is targeting Ukrainian military personnel by distributing a malicious installer disguised as the legitimate [ArmyPlus](#) application. The installer extracts the Tor browser and configures it for covert operations, establishing a backdoor via SSH over the Tor network. This enables attackers to execute arbitrary commands with high privileges, posing a severe security threat.

Data Breaches

Volkswagen Data Breach Exposes 800,000 Electric Vehicle Owners' Data

+Germany +Automotive

- A data breach at [Volkswagen](#) exposed location data and personal information of approximately 800,000 electric vehicle owners, including those of Audi, Seat, and Skoda brands. The leak, originating from Volkswagen's software division, Cariad, allowed unauthorized access to sensitive driver data stored on Amazon's cloud service. The company has since addressed the issue, assuring customers that no passwords or payment details were compromised.

New York Hospital Ransomware Attack Affects 670,000 Individuals

+US +Healthcare

- [Richmond University Medical Center](#) in New York has been investigating a ransomware attack that occurred in May 2023, leading to a data breach impacting over 670,000 individuals. The attack caused significant disruptions, with the hospital taking several weeks to restore affected services. The compromised data included personal and health information, prompting the hospital to offer credit monitoring services to affected individuals.

City Bank Data Breach: Client Financial Statements Sold on Underground Forums

+Bangladesh +Financial Services

- [City Bank PLC](#) in Bangladesh suffered a data breach where client financial statements were exposed and sold on underground forums. The breach was discovered in December 2024, with unauthorized access to client statements identified. The bank has since resolved the issue, stating that no transactions or unauthorized activities were performed by the hacker.

Chinese Hackers Breach Multiple U.S. Telecom Networks

+China +Telecommunications +Salt Typhoon

- Chinese hackers, operating under the group [Salt Typhoon](#), were found to have breached networks of several more telecommunications companies, including Charter Communications and Windstream. The attacks, which also included previously reported breaches into AT&T, Verizon, and T-Mobile, compromised private communications of government officials and sensitive customer data. The U.S. government has acknowledged the breaches, with agencies like CISA and the FBI confirming the incidents.

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.