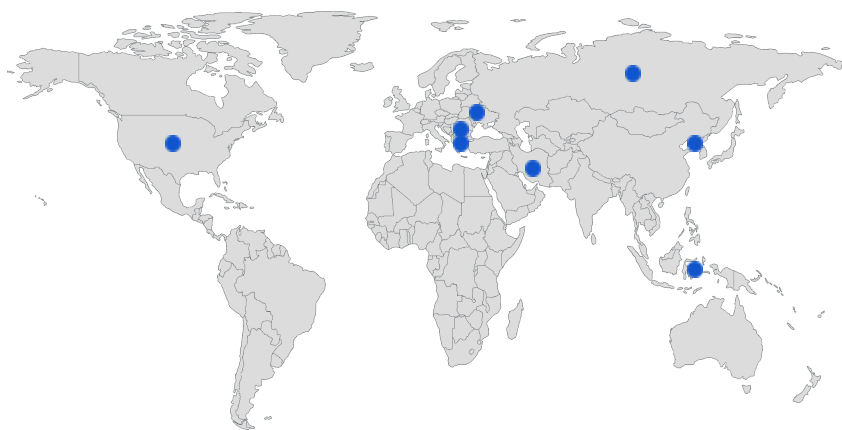


Threat Intel Report: January 29 - February 4, 2024

Countries



Top Tags

DarkGate

PurpleFox

Starcruft

Cactus

ALPHV

Executive Summary

Actionable Information:

- *Supply Chain and Software Repository Attacks:* Malicious packages in software repositories (e.g., PyPI) and vulnerabilities in container environments (e.g., Docker) emphasize the need for rigorous software supply chain security and regular vulnerability assessments.
- *Cryptocurrency and Financial Sector Targets:* Attacks on Bitcoin ATMs and financial organizations like Schneider Electric reveal the attractiveness of financial targets for cybercriminals, necessitating enhanced security measures in these sectors.
- *Use of Legitimate Platforms for Malware Distribution:* The exploitation of platforms like Microsoft Teams for malware distribution (e.g., DarkGate malware) indicates a trend towards using legitimate services for malicious purposes, highlighting the importance of securing communication tools.
- *Nation-State Cyber Operations:* Activities by groups like Scarcruft and ALPHV, as well as Iran-linked hackers, demonstrate the ongoing cyber espionage and sabotage efforts by nation-states, stressing the need for heightened cybersecurity awareness and defense in critical sectors.
- *Ransomware and Data Breaches:* High-profile ransomware attacks (e.g., ALPHV's breach of Technica) and data exposures (e.g., Mercedes-Benz source code leak) continue to pose significant risks, underscoring the importance of robust incident response plans and data protection strategies.

Outlook:

The landscape of cyber threats is increasingly complex, with adversaries leveraging a mix of technical sophistication, social engineering, and exploitation of public and private sector vulnerabilities. The trend towards targeting critical infrastructure, financial systems, and leveraging supply chain vulnerabilities is likely to persist, driven by both financial

motives and geopolitical tensions. Organizations across all sectors must prioritize cybersecurity resilience, adopting a proactive and comprehensive approach to security that includes regular vulnerability assessments, employee training, and collaboration with cybersecurity agencies and partners. As the digital and physical worlds become more interconnected, the stakes for protecting sensitive data and critical infrastructure from cyber threats will only continue to rise.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

⬆ 63% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB

⬆ 24% [CVE-2023-35078](#)

- A remote unauthenticated API access vulnerability in Ivanti Endpoint Manager Mobile

⬆ 26% [CVE-2023-35082](#)

- A remote unauthenticated API access vulnerability in Ivanti Endpoint Manager Mobile

4.7M RPS DDoS Attack Targets Indonesian Gaming Site

+Indonesia +Gaming +DDoS

- The largest DDoS attack we've seen since September occurred this week, with a 4.7M requests per second (RPS) onslaught targeting an Indonesian gaming site. The attack came from 1,700 Canadian, Indian, and US IPs, and mainly leveraged the Nessus vulnerability scanner.

US Retail Site Hit With Path Traversal and XSS Attacks

+US +Retail +Path Traversal +XSS

- A US retail site was targeted this week in an attack leveraging path traversal and XSS. The attack came from only 2 US-based IPs, suggesting a focused and possibly localized threat actor.

Recent Cyber Threats

Stealthy PyPI Packages Deploy WhiteSnake Malware

+PyPI +Stealer Malware +WS

- Researchers discovered malicious PyPI packages that install [WhiteSnake Stealer](#) malware on Windows systems. The malware, hidden in packages uploaded by a threat actor named "WS," targets data from web browsers, cryptocurrency wallets, and various applications, demonstrating the ongoing risk of supply chain attacks in software repositories.

Compromising Bitcoin ATMs with New Vulnerabilities

+Bitcoin +Cryptocurrency

- Researchers identified vulnerabilities in [Lamassu's Douro Bitcoin ATMs](#) that allow attackers to gain full control over the machines. By exploiting these flaws, attackers could potentially manipulate transactions and access sensitive information, raising concerns about the security of cryptocurrency ATMs.

DarkGate Malware Distributed via Microsoft Teams

+DarkGate

- Attackers are using Microsoft Teams group chats to distribute [DarkGate](#) malware through phishing attacks. By exploiting compromised accounts, they send malicious attachments to unsuspecting users, demonstrating the increasing use of legitimate platforms for malware distribution and the importance of securing communication tools against external threats.

Cloud Containers' Security Flaws Exposed

+Leaky Vessels +runC

- Researchers have identified four significant vulnerabilities in Docker and other container environments, notably affecting runC, which could allow attackers to escape containers and execute malicious actions on the host system. This set of vulnerabilities, dubbed [Leaky Vessels](#), poses a global threat to cloud-native developers and underscores the critical need for updating container runtime environments.

PurpleFox Malware Rampant in Ukraine

+PurpleFox +Ukraine

- The [PurpleFox](#) malware, also known as DirtyMoe, has infected over 2,000 computers in Ukraine, according to CERT-UA. This modular Windows botnet malware, first identified in 2018, includes a rootkit module for persistence and can deliver second-stage payloads, offer backdoor capabilities, and perform DDoS attacks.

Ukraine's POW Agency Attacked

+Ukraine +Russia +Government

- Ukraine's [agency overseeing prisoners of war](#) experienced a DDoS attack, which the agency attributes to Moscow, linking it to the crash of a Russian transport plane. The attack aimed to disrupt the agency's operations, including negotiations for prisoner exchanges and the return of fallen soldiers' bodies, amidst ongoing cyber warfare between Ukraine and Russia.

FritzFrog Botnet Exploits Log4Shell in Internal Networks

+FritzFrog +Botnet +Log4Shell

- Researchers have discovered a new variant of the [FritzFrog](#) botnet, active since 2020, now exploiting the Log4Shell vulnerability to penetrate deeper into victims' internal networks. This botnet, known for deploying cryptominers through brute-force SSH attacks, has adapted to target Java applications vulnerable to Log4Shell, affecting over 1,500 victims globally.

Data Breaches

Scarcruft Targets Cybersecurity Sphere

+Scarcruft +North Korea +Cybersecurity

- [Scarcruft](#), a North Korean APT group, is preparing to target cybersecurity professionals and businesses, focusing on gathering strategic intelligence and possibly infiltrating non-public cyber threat intelligence. The group has been experimenting with new infection chains, including using a technical threat research report as a decoy, indicating a strategic shift towards targeting individuals consuming threat intelligence.

Massive Data Wipe in Russian Research Center

+Ukraine +Russia +Government

- Pro-Ukrainian hackers reportedly breached the [Russian Center for Space Hydrometeorology](#), wiping 2 petabytes of data and causing an estimated \$10 million in damage. This cyberattack targeted the center's sustainability business division, impacting weather, climate, and natural disaster predictions, and posing a significant setback to Russian state agencies.

Schneider Electric Hit by Cactus Ransomware

+Electricity +Cactus

- [Schneider Electric](#) suffered a data breach due to a Cactus ransomware attack, with the gang claiming to have stolen terabytes of corporate data. The attack specifically impacted Schneider Electric's Resource Advisor cloud platform, causing outages, though the company confirmed that other divisions were not affected.

Mercedes-Benz Source Code Exposed

+Automotive

- [Mercedes-Benz](#) inadvertently exposed internal data, including source code, due to a leaked private key on GitHub. The exposure was discovered when researchers found an employee's authentication token in a public repository, granting full access to the company's GitHub Enterprise Server. This incident highlights the risks associated with mishandling sensitive authentication credentials.

Network Operators' Credentials Circulating in Dark Web

+Cybersecurity

- Hundreds of [credentials](#) belonging to customers of regional internet registries like RIPE, APNIC, AFRINIC, and LACNIC have been found on the dark web. These credentials, compromised through infostealer infections, include access to sensitive network configurations and personal data, posing a significant risk to global internet infrastructure security.

Pentagon Investigates ALPHV Ransomware Breach

+ALPHV +US +Government

- The [Pentagon](#) is investigating a breach by the ransomware group ALPHV, which claims to have stolen 300 gigabytes of data from Technica, a Virginia-based IT services company working with the U.S. military. The stolen data reportedly includes sensitive information related to the Defense Counterintelligence and Security Agency.

Romanian Parliament's Database Hacked

+Romania +Government

- Hackers breached the [Romanian Chamber of Deputies'](#) database, obtaining confidential information including the prime minister's identity documents and medical records. The unnamed attackers demanded a ransom of 0.8 bitcoin, highlighting vulnerabilities in the cybersecurity measures protecting governmental institutions.

Cloudflare Breach Linked to Okta Attack

+Computing & IT

- [Cloudflare](#) disclosed a breach of its internal Atlassian server, attributed to a nation-state attacker using stolen Okta auth tokens. The breach exposed Confluence, Jira, and Bitbucket systems but reportedly did not impact Cloudflare's services or customer data.

Iran-Linked Hackers Target Albania's Census Agency

+Iran +Albania +Government

- Iran-linked hackers claimed responsibility for an attack on [Albania's Institute of Statistics](#), threatening to leak over 100 terabytes of sensitive geographic and population data. This incident underscores the ongoing cyber tensions between Albania and Iran, with previous attacks targeting Albanian state agencies and 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.



By Phone:
650-345-9000

By mail:

Imperva Headquarters
One Curiosity Way, Suite
203 San Mateo, CA 94403