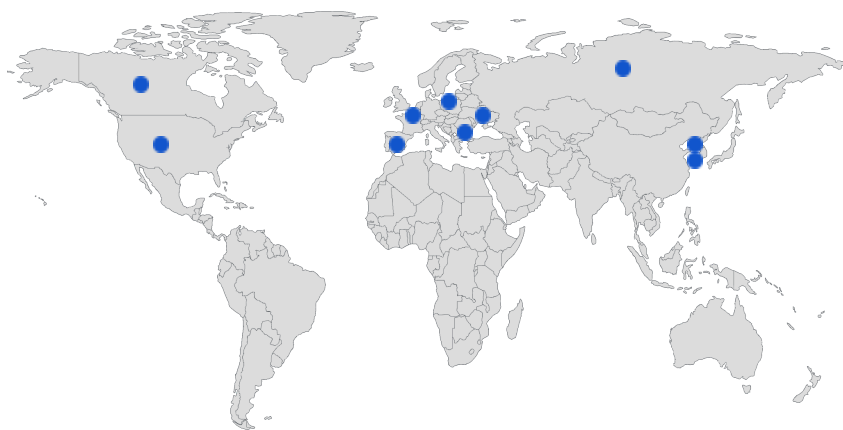


Threat Intel Report: February 12-18, 2024

Countries



Top Tags

Volt Tycoon

IntelBroker

Black Basta

AlphV

Turla

Executive Summary

Actionable Information:

- **Vulnerability Exploitation:** Immediate patching of known vulnerabilities in software products, including those disclosed in Ivanti's security products and the DNSSEC protocol, is crucial to prevent unauthorized access and potential service disruptions.
- **Ransomware Vigilance:** Organizations, especially in healthcare and critical infrastructure, must enhance their ransomware defense mechanisms and backup strategies to mitigate the impact of data encryption attacks.
- **Phishing Defense:** Strengthening defenses against phishing campaigns, particularly those targeting senior executives to compromise corporate clouds, is essential for protecting sensitive information.
- **Spyware Awareness:** Increased awareness and preventive measures against spyware targeting mobile devices, especially those involving cryptocurrency wallets, are necessary to safeguard financial assets.
- **Third-Party Risk Management:** Rigorous assessment and monitoring of third-party vendors and contractors are required to address security risks posed by external entities managing sensitive data.

Outlook:

The diversity of cyber threats observed this week indicates a persistent and evolving challenge for cybersecurity professionals. Ransomware continues to be a significant threat to both public and private sectors, with healthcare and critical infrastructure being particularly vulnerable due to their essential services. The exploitation of software vulnerabilities remains a favored tactic, highlighting the importance of timely patch management and the need for continuous vigilance in monitoring for new threats. Additionally, the targeting of high-value individuals through phishing and the misuse of legitimate tools for espionage activities demonstrate the sophistication of threat actors. Looking



ahead, it is imperative for organizations to adopt a proactive and comprehensive cybersecurity posture, incorporating both technological solutions and human vigilance to anticipate and mitigate emerging threats. The collaboration between public and private sectors and international cooperation will be key in addressing the global nature of cyber threats and enhancing the overall resilience of cyberspace.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 10% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB

↓ 12% [CVE-2023-35078](#)

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

↓ 10% [CVE-2023-35082](#)

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

UK Grocery Chain Hit With 3M RPS DDoS Attack

+UK +Retail +DDoS

- This week, a UK grocery chain was targeted in an almost 3M requests per second (RPS) attack. The attack came from 2,000 IP addresses, and could potentially have targeted the site for extortion or competition.

ATO Attack on Italian Telecommunications Site

+Italy +Telecommunications +ATO

- An Italian telecommunications company saw attempted account takeover (ATO) attacks this week, coming from thousands of IPs. Sites like this, which see financial and personal data and transactions, are frequent targets for ATO attempts.

Recent Cyber Threats

ExpressVPN Feature Leak Compromises User Privacy

+ISP

- A critical bug in [ExpressVPN's](#) split tunneling feature led to the unintended exposure of DNS requests to ISPs, breaching user privacy by revealing visited domains. This flaw, present in versions from May 2022 to February 2024, was addressed by removing the feature in the latest update, with promises of a future fix to reintroduce it securely.

Hackers Deploy DSLog Backdoor via Ivanti SSRF Vulnerability

+CVE *Imperva customers are protected against [CVE-2024-21893](#) and [CVE-2024-22024](#).*

- Vulnerabilities in Ivanti's security products, known as [CVE-2024-21893](#) and [CVE-2024-22024](#), allow attackers to bypass authentication and access restricted resources, compromising the security of Connect Secure, Policy Secure, and ZTA gateways.

KeyTrap DNSSEC Flaw Endangers Internet Infrastructure

+DNS

- Researchers uncovered a severe flaw in the [DNSSEC](#) protocol, dubbed KeyTrap (CVE-2023-50387), that could allow attackers to disable DNS servers with a single malicious packet. This vulnerability, affecting a significant portion of the internet's infrastructure, prompted urgent patching efforts to prevent potential widespread service disruptions.

JKwerlo Ransomware Campaign Hits European Targets

+JKwerlo +France +Spain

- The [JKwerlo](#) ransomware, a Go-based variant, has been actively targeting users in France and Spain through sophisticated phishing emails disguised as legal notices. This campaign leverages social engineering and advanced technical methods to encrypt victims' data, demanding ransom for decryption keys.

SpyNote Android Spyware Targets Cryptocurrency Wallets

+SpyNote +Crypto

- The notorious [SpyNote Android](#) spyware has evolved to target cryptocurrency wallets, exploiting the Accessibility API to initiate unauthorized transfers. By masquerading as legitimate crypto wallet apps, it deceives users into granting permissions that allow it to replace transaction details with the attacker's wallet address, leading to financial losses.

Volt Typhoon APT Expands Targets to Electric Utilities

+Volt Tycoon +Critical Infrastructure

- The [Volt Typhoon](#) advanced persistent threat (APT) group, particularly its Voltzite subset focusing on operational technology networks, has been observed conducting reconnaissance on electric utilities in the US and Africa. Although currently limited to IT network breaches, their activities hint at potential preparations for future disruptive attacks against critical infrastructure.

Data Breaches

Facebook Marketplace Data Leak Exposed

+IntelBroker +algoatson

- The [Facebook Marketplace](#) database was partially leaked by the threat actor IntelBroker, with data stolen by another hacker named "algoatson." The leak involved around 200,000 entries including sensitive personal information like full names, Facebook IDs, phone numbers, and more.

Ransomware Disrupts Romanian Healthcare

+Romania +Healthcare

- A ransomware attack targeted the [Hippocrate Information System](#) used by 100 Romanian hospitals, encrypting databases and forcing systems offline. The attack, which began over a weekend, affected hospitals' ability to manage medical activities and patient data digitally, reverting to paper-based systems.

Azure Account Takeover Targets Executives

+Microsoft Azure +Business

- An ongoing campaign has compromised numerous [Microsoft Azure](#) corporate clouds, targeting senior executives with phishing attacks to steal Microsoft 365 login credentials. The attackers, focusing on high-value targets within organizations, have engaged in data exfiltration, financial fraud, and impersonation.

Hackers Mint Billions from PlayDapp Platform

+Gaming +Crypto

- Hackers exploited a stolen private key to mint and steal over 1.79 billion PLA tokens from the [PlayDapp](#) gaming platform, causing significant financial impact. The attack led to the unauthorized creation of tokens valued at millions of dollars, demonstrating the vulnerabilities present in blockchain-based platforms and the challenges in securing digital assets.

Jet Engine Dealer Hit by Cyber Attack

+Black Basta +Aviation

- [Willis Lease Finance Corporation](#), a major jet engine dealer, disclosed a cybersecurity incident after data was leaked by the Black Basta ransomware group. The attack compromised sensitive information, including customer and employee data.

GAO Breach Linked to Atlassian Vulnerability

+US +Government

- https://cyberscoop.com/atlassian-vulnerability-at-fault-in-gao-breach/?&web_view=true
- The US [Government Accountability Office](#) (GAO) experienced a data breach affecting thousands of employees due to a vulnerability in an Atlassian collaboration tool used by a contractor. The breach, which exposed sensitive information, highlights the risks associated with third-party software vulnerabilities and the need for timely patch management and incident response.

Trans-Northern Pipelines Ransomware Attack

+AlphV +Canada +Infrastructure

- Canada's [Trans-Northern Pipelines](#) confirmed a ransomware attack by the AlphV group, which claimed to have stolen 183 GB of data. Despite the cyberattack, the company maintained that pipeline operations and fuel delivery were not disrupted.

US Military Cloud Email Leak Affects 20,000

+US +Government

- The U.S. [Department of Defense](#) notified approximately 20,600 individuals of a data breach resulting from an unsecured cloud email server leak. The breach, which exposed sensitive military emails, was attributed to a misconfiguration on Microsoft's cloud platform.

North Korean Hackers Target South Korean President's Office

+North Korea +South Korea +Government

- Suspected North Korean hackers breached the private email account of an official in the [South Korean President's Office](#), accessing information about state visits and communications. The breach, facilitated by the official's use of a private email for work, underscores the persistent cyber espionage efforts by North Korea.

TinyTurla Malware Targets Polish NGOs

+Turla +Russia +Poland +Ukraine +Government

- Researchers have uncovered a new backdoor, [TinyTurla-NG](#), used by the Russian Turla APT group to target Polish NGOs supporting Ukraine. This malware, designed for espionage, demonstrates Turla's continued focus on political and strategic targets and highlights the cybersecurity risks faced by organizations involved in geopolitical conflicts.

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