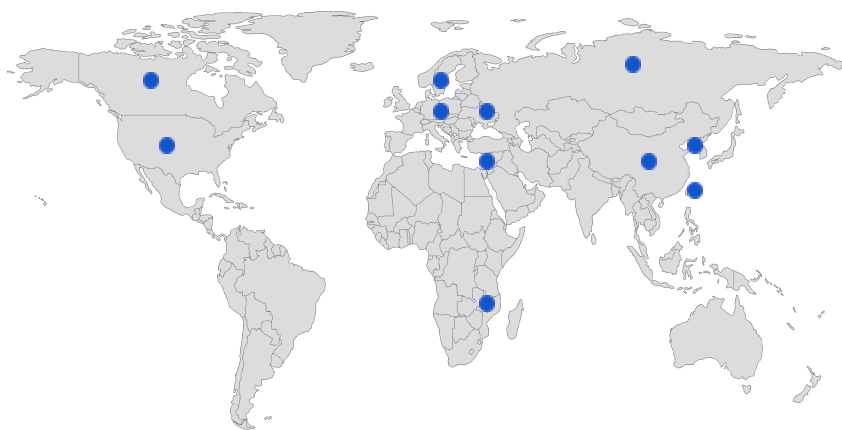


Threat Intel Report: February 26-March 10, 2024

Countries



Top Tags

IntelBroker

Akira

Rhysida

Play

Golang

Executive Summary

Actionable Information:

- *Implement stringent validation processes for software dependencies:* The discovery of malicious npm packages by North Korean hackers underscores the need for organizations to vet third-party libraries thoroughly.
- *Update and secure web applications:* The vulnerability in the Ultimate Member plugin for WordPress and other similar vulnerabilities highlight the importance of keeping web applications up-to-date and secured with additional measures like web application firewalls.
- *Prioritize IoT and endpoint security:* The global hack of Anycubic 3D printers and the targeting of MacOS users by the AMOS Stealer malware variant emphasize the need for robust security practices for IoT devices and endpoints.
- *Enhance supply chain security:* Incidents involving pre-installed malware on consumer electronics and attacks targeting the software supply chain call for enhanced security checks and vetting processes.
- *Stay vigilant against social engineering and phishing attacks:* The Tesla authentication flaw and the Facebook account takeover exploit demonstrate the effectiveness of social engineering tactics, necessitating ongoing education and awareness efforts.

Outlook:

Looking ahead, the cybersecurity landscape is expected to face continued challenges from a variety of fronts. The increasing reliance on digital technologies across all sectors, coupled with the rapid advancement of cybercriminal techniques, suggests that threats will become more sophisticated and potentially damaging. State-sponsored activities, particularly those involving espionage and intellectual property theft, are likely to persist, with geopolitical tensions playing a significant role in targeting patterns. Ransomware attacks are expected to remain a significant threat,

especially to public sector entities and critical infrastructure, as evidenced by the incidents in Malawi, Sweden, and the United States. The role of artificial intelligence and machine learning in both enhancing cybersecurity defenses and being exploited by attackers is poised to grow, indicating a dual-edged trajectory for these technologies. Overall, this week's highlights underscore the importance of proactive and comprehensive cybersecurity strategies to mitigate the evolving threats.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 30% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB

↑ 1% [CVE-2023-35078](#)

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

↓ 3% [CVE-2023-35082](#)

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

Israeli Financial Institutions Targeted in Coordinated DDoS Attacks

+Israel +DDoS

- Several Israeli financial institutions were targeted in DDoS attacks this week, with several attacks reaching over 1M requests per second (RPS). Although all of these institutions have been targeted before, the rate and frequency of overlapping attacks is unique. Over 3200 IPs overlapped among all attacks, so this was almost certainly a coordinated attack.

US Entertainment Site Sees Path Traversal and RCE Attacks

+US +Entertainment

- A US-based entertainment site was targeted this week in path traversal and remote code execution attacks. The attacks, which reached over 10M requests per day, came from US-based IPs as well, which could point to a regional botnet or an attempt to mask the true origin of the attack.

Recent Cyber Threats

Expanding Threats from North Korean npm Package Impersonations

+North Korea +npm

- [North Korean](#) hackers have been identified as the perpetrators behind a series of malicious npm packages, designed to impersonate legitimate libraries. These packages, once integrated into software projects, deploy scripts that steal cryptocurrency and user credentials, posing a significant risk to the integrity of the software supply chain. Organizations are advised to implement stringent package validation processes and educate developers on the risks of third-party dependencies.

Ultimate Member Plugin Vulnerability Endangers WordPress Sites

+SQLi +WordPress

- A severe SQL injection vulnerability has been uncovered in the [Ultimate Member](#) plugin for WordPress, impacting over 200,000 installations. This flaw allows attackers to execute unauthorized SQL commands, potentially leading to data breaches or complete site compromise. Web administrators should urgently update to the latest plugin version and consider additional security measures such as web application firewalls (WAFs) to mitigate potential exploitation. Imperva customers are protected against this vulnerability.

AI Model Hijacking Risk Through Hugging Face Vulnerability

+AI

- A critical vulnerability in the [Hugging Face](#) platform's model conversion service could allow attackers to hijack AI models, leading to potential supply chain attacks. This flaw underscores the importance of securing AI development and deployment environments against unauthorized access.

Worldwide Anycubic 3D Printer Hack Exposes IoT Security Flaws

+3D Printers +IoT

- An orchestrated hack of [Anycubic 3D printers](#) globally has highlighted a critical security flaw, with devices receiving a warning message about their vulnerability. This incident serves as a stark reminder of the security risks associated with IoT devices. Manufacturers and users alike must prioritize security updates and adopt best practices for device management to prevent unauthorized access and potential exploitation.

MacOS Under Threat: AMOS Stealer Variant Targets Safari and Crypto

+MacOS +Stealer Malware

- A sophisticated variant of the [AMOS Stealer malware](#) is actively targeting MacOS users, focusing on the theft of Safari browser cookies and cryptocurrency wallet information. Organizations should enhance endpoint security measures, encourage the use of hardware wallets for cryptocurrency, and educate users on phishing and other social engineering attacks.

Pre-Installed Malware Found in Acemagic PCs Raises Supply Chain Security Concerns

+Malware +Supply Chain

- The discovery of [pre-installed malware](#), including Bladabindi and Redline, on Acemagic PCs has raised significant concerns about supply chain security within the consumer electronics industry. This incident highlights the need for rigorous security checks and vetting processes for manufacturers and suppliers. Businesses are advised to conduct thorough security assessments of devices before integration into their IT environments.

Facebook Vulnerable to Zero-Click Account Takeover Exploit

+Meta +ATO

- A critical rate-limiting issue within [Facebook's](#) password reset flow was discovered, allowing for a zero-click account takeover exploit. The issue was discovered by researchers, who found that the issue impacts Facebook's password reset procedure when the user selects "Send Code via Facebook Notification." Meta has since patched the vulnerability.

New Golang Malware Automates Attacks on Misconfigured Servers

+Golang +Malware

- A sophisticated campaign utilizing Golang-based malware targets [misconfigured servers](#) running Apache Hadoop YARN, Docker, Confluence, or Redis. This automated attack mechanism exploits known vulnerabilities and configuration weaknesses, underscoring the critical need for proper server configuration and timely patching.

Tesla's Vulnerability to MiTM Phishing Attacks Highlights Authentication Flaws

+MITM +Tesla

- A demonstrated Man-in-the-Middle phishing attack reveals significant vulnerabilities in [Tesla's](#) authentication process for adding new phone keys, potentially allowing attackers to unlock and steal vehicles. This vulnerability calls for an immediate review of authentication protocols by automotive manufacturers. Tesla owners and

organizations utilizing Tesla fleets should remain vigilant for phishing attempts and prioritize the use of physical keys for sensitive operations.

Data Breaches

Ransomware Disruption at Malawi Immigration Department

+Malawi +Government

- The [Malawi Immigration Department](#) ceased passport issuance for two weeks due to a ransomware attack. President Lazarus Chakwera confirmed the attack, stating the government's refusal to pay the demanded ransom. The specifics of the ransomware, including the identity of the attackers and whether data was stolen, remain undisclosed. This incident marks a significant disruption in government services, reflecting the increasing threat of ransomware attacks on public sector entities.

Data Breach at Los Angeles International Airport Exposes Private Plane Owners

+US +IntelBroker +Aviation

- Hackers, operating under the alias IntelBroker, claimed to have breached the [Los Angeles International Airport's](#) database, leaking data of 2.5 million private plane owners. The compromised data includes full names, CPA numbers, email addresses, company names, plane model numbers, and tail numbers. The breach was executed by exploiting a vulnerability in one of the airport's CRM systems.

Akira Ransomware Targets Swedish Municipality Bjuv

+Sweden +Akira

- The Akira ransomware group has targeted the municipality of [Bjuv, Sweden](#), threatening to release nearly 200GB of stolen data, including confidential documents, contracts, agreements, and personal HR files. The ransomware group's dark web post indicates the nature of the compromised data. Despite the claim, Bjuv Municipality's official website remains operational, with no immediate evidence of the cyberattack's impact on municipal services or data integrity.

Lurie Children's Hospital Chicago Faces Ransomware Attack

+US +Healthcare +Rhysida

- [Lurie Children's Hospital](#) in Chicago was targeted by the Rhysida ransomware group, demanding a \$3.4 million ransom. The attack forced the hospital to switch to manual processes, affecting patient care. The hospital, a major pediatric healthcare provider in the Midwest, has continued to operate with minimal disruptions, although some appointments and surgeries were canceled. The hospital's MyChart electronic records system remains down as efforts to recover the hospital's systems continue.

Leaky Database Exposes Two-Factor Authentication Codes

+2FA

- [YX International](#), a company specializing in SMS routing, inadvertently exposed a database containing one-time security codes for accounts on platforms such as Facebook, Google, and TikTok. Discovered by security researcher Anurag Sen, the database was accessible without a password, revealing text message contents including two-factor authentication codes and password reset links. The exposure raises concerns about the security of SMS-based two-factor authentication and the risks associated with database misconfigurations.

Suspected Chinese Hackers Breach Taiwan's Largest Telco

+Taiwan +China +Government +Telecommunications

- Taiwan's largest telecom company, [Chunghwa Telecom](#), suffered a data breach, with 1.7TB of data, including government-related information, stolen and subsequently sold on the Dark Web. The Taiwanese Defense Ministry attributed the attack to hackers believed to be backed by the Chinese government. The compromised data includes documents from various government departments, though the ministry assured that no confidential information was leaked.

Ukraine Allegedly Hacks Russian Ministry of Defense Servers

+Russia +Ukraine +Government

- Ukraine's Main Intelligence Directorate claims to have breached the servers of the [Russian Ministry of Defense](#), obtaining sensitive documents including software used for data protection and encryption, secret service documents, and personal information of senior officials. Evidence of the breach was provided through screenshots of database queries and official documents, though the authenticity of these screenshots has not been independently verified.

Canada's FINTRAC Hit by Cyberattack

+Canada

- The [Financial Transactions and Reports Analysis Centre of Canada](#) (FINTRAC) took its corporate systems offline in response to a cyber incident. The nature of the incident has not been disclosed, but the agency is working with federal partners, including the Canadian Centre for Cyber Security, to restore and protect its systems. FINTRAC, responsible for detecting and investigating money laundering and terrorist financing, emphasized that the incident did not involve its intelligence or classified systems.

Swiss Government Data Leaked by Play Ransomware Group

+Switzerland +Play

- Sensitive data from the [Swiss federal government](#) was leaked following a ransomware attack on IT service provider Xplain by the Play ransomware group. The leaked data includes classified documents, login credentials, and around 65,000 documents related to the federal government. The majority of the leaked government files originated from departments such as the Federal Department of Justice and Police and the Federal Office of Justice.

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