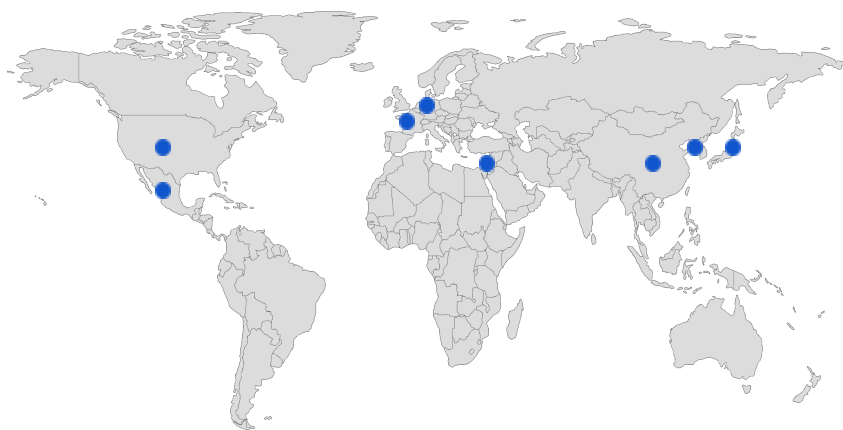


Threat Intel Report: February 5-11, 2024

Countries



Top Tags

Mispadu

OV3R_Stealer

Kimsuky

Coyote

Black Basta

Executive Summary

Actionable Information:

- **Exploitation of Vulnerabilities:** Several attacks, such as those involving the Mispadu banking Trojan and the critical flaw in Airbus' FlySmart system, leveraged vulnerabilities to gain unauthorized access or to steal sensitive information. This trend highlights the importance of timely patching and vulnerability management.
- **Ransomware and Malware Campaigns:** The Black Basta ransomware attack on Hyundai Motor Europe and the distribution of OV3R_Stealer malware via phishing highlight the continued prevalence of ransomware and malware. These incidents demonstrate threat actors' focus on both financial gain and espionage.
- **Insider Threats:** The Verizon insider breach incident reveals the significant risk posed by insider threats, emphasizing the need for robust access controls and monitoring.
- **Sector-Specific Targeting:** Attacks on specific sectors, such as healthcare (Lurie Children's Hospital and Viamedis) and financial services (Coyote malware targeting banking apps), indicate that threat actors are tailoring their campaigns to exploit sector-specific vulnerabilities and maximize impact.

Outlook:

Looking ahead, the cyber threat landscape is expected to remain dynamic, with threat actors continuing to refine their tactics, techniques, and procedures (TTPs). The diversity of this week's incidents suggests that no sector is immune to cyber threats, and the sophistication of attacks is likely to increase. Organizations across all industries must remain vigilant and proactive in their cybersecurity efforts, prioritizing the identification and remediation of vulnerabilities, enhancing detection and response capabilities, and fostering a culture of security awareness among employees. Additionally, the rise in insider threats and API security issues calls for a more comprehensive approach to security,



encompassing both technological solutions and human factors. As threat actors increasingly leverage social engineering and sophisticated malware to bypass traditional security measures, organizations must adopt a multi-layered defense strategy to protect against the evolving threat landscape.

Threat Activity in Imperva

Top 3 CVEs Targeted This Week:

Imperva customers are protected against these CVEs.

📈 36% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB

📈 21% [CVE-2023-35078](#)

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

📈 20% [CVE-2023-35082](#)

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

Israeli Insurance Company Targeted in Second Largest DDoS Attack Of The Year

+Financial Services +Israel +DDoS

- An Israeli insurance company was targeted this week in an almost 4M requests per second (RPS) application-layer DDoS attack. This attack came from over 3,000 IPs, mostly based within Israel. This attack is the second largest DDoS attack we've seen so far in 2024.

US Rewards Site Hit With Multi-Vector Attack

+US +Financial Services +RCE +XSS +Path Traversal

- A US-based rewards site was hit with path traversal, cross-site scripting (XSS), and remote code execution (RCE) this week. This is the first time this site has experienced an attack in 2024.

Recent Cyber Threats

The New Mispadu Banking Trojan Variant

+Mispadu +Financial Services +Mexico +Trojan

- Researchers have uncovered a new variant of the [Mispadu](#) banking Trojan, initially reported in 2019, which now employs sophisticated techniques to evade detection and steal information. This variant exploits the CVE-2023-36025 vulnerability to bypass Windows SmartScreen and target users primarily in Mexico, focusing on stealing banking credentials and sensitive information. The impact of this campaign is significant due to its stealthy nature and the potential financial losses for victims.

Critical Vulnerability in Airbus' FlySmart System Exposed

+Aviation

- A critical flaw was discovered in [Airbus' FlySmart](#) system, potentially allowing hackers to manipulate flight data and endanger flight safety. The vulnerability, if exploited, could lead to unauthorized access to flight systems, posing a

significant risk to aircraft operations worldwide. The issue underscores the critical need for robust cybersecurity measures in the aviation sector.

OV3R_Stealer Malware Campaign Unveiled

+OV3R_Stealer +Malware +Phishing

- Researchers have identified a phishing and Facebook advertising campaign distributing the [OV3R_Stealer](#) malware. This malware is designed to steal personal information from infected devices, leveraging social engineering tactics to spread.

Canon Printers Vulnerable to Critical Bugs

+Technology +Business

- Critical vulnerabilities in [Canon's](#) small office printers could allow attackers to execute arbitrary code or launch DDoS attacks. These flaws pose a significant risk to businesses relying on these devices, emphasizing the need for timely updates and cybersecurity awareness in the technology sector.

Kimsuky's New Disguise Targets with Valid Certificate

+Kimsuky +North Korea

- The North Korean hacking group [Kimsuky](#) has been reported to disguise itself as a Korean company, using a valid certificate to distribute the Troll Stealer malware. This tactic represents a significant escalation in the group's efforts to target individuals and organizations, bypassing traditional security measures.

Urgent Warning Issued for New Ivanti Vulnerability

+CVE

- [Ivanti](#) has issued an urgent warning regarding a new vulnerability affecting its products. Tracked as CVE-2024-22024 with a severity score of 8.3, this vulnerability could allow attackers to compromise systems, highlighting the need for immediate patching and the continuous monitoring of software vulnerabilities.

Imperva customers are protected against CVE-2024-22024.

Coyote Malware Targets Banking Apps

+Coyote +Malware +Financial Services

- A new malware, dubbed [Coyote](#), has been found preying on 61 banking apps, stealing credentials and financial information from unsuspecting users. This malware's widespread targeting of banking apps points to the persistent threat cybercriminals pose to the financial industry, and the importance of secure banking practices.

Data Breaches

Cyberattack Forces Pediatric Hospital to Take Systems Offline

+US +Healthcare

- [Lurie Children's Hospital](#) in Chicago experienced a cyberattack that forced the hospital to take its IT systems offline, causing disruptions and delays in medical care. Scheduled procedures were delayed, and the hospital had to revert to manual processes for prescriptions and prioritize emergency situations. No ransomware demands have been made public.

Classified Japanese Diplomatic Documents Leaked

+Japan +China +Government

- Classified [Japanese diplomatic documents](#) have been leaked following cyberattacks by Chinese hackers on Japan's Ministry of Foreign Affairs in 2020. The exact content and magnitude of the leaked information was not specified, but the breach underscores Japan's digital vulnerabilities and the geopolitical implications of cyber espionage.

Chinese Hackers Infiltrate Dutch Defence Ministry's Network

+China +the Netherlands +Government

- Chinese state-sponsored hackers infiltrated the [Dutch Ministry of Defence's](#) network via FortiGate vulnerabilities, deploying malware for espionage. This incident highlights the strategic targeting of military and governmental networks by nation-state actors.

Verizon Insider Breach Exposes Employee Data

+Telecommunications +Insider Threat

- An unauthorized access incident at [Verizon](#) led to the exposure of sensitive information belonging to over 63,000 employees. The breach, discovered nearly three months after the initial access, included full names, physical addresses, Social Security numbers, national IDs, gender, union affiliations, dates of birth, and compensation information.

Cyberattack on Viamedis Affects Millions in France

+France +Healthcare +Financial Services

- [Viamedis](#) suffered a cyberattack that exposed the data of policyholders and healthcare professionals. The company manages payments for 84 healthcare organizations covering 20 million insured individuals, all of whom could be at risk.

Spoutible Social Media Platform's API Leak

+API Security +Social Media

- [Spoutible](#), a social media platform, faced a security issue where its publicly exposed API allowed for the potential scraping of 207,000 user records. Security consultant Troy Hunt highlighted the leak, which included usernames, first and last names, user IDs, bios, emails, IP addresses, verified phone numbers, bcrypt hashes of passwords, seeds for generating one-time passwords for 2FA, bcrypt hashes of 2FA backup codes, and password reset tokens.

Black Basta Ransomware Targets Hyundai Motor Europe

+Black Basta +Automotive

- [Hyundai Motor Europe](#) was hit by a ransomware attack orchestrated by the Black Basta group, which claimed to have stolen three terabytes of corporate data. Initially described by Hyundai as IT issues, the company later confirmed the cyberattack and stated that an unauthorized third party accessed a limited part of its network. This incident is part of a series of attacks by Black Basta, which has been known for its double-extortion tactics since its operation began in April 2022.

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