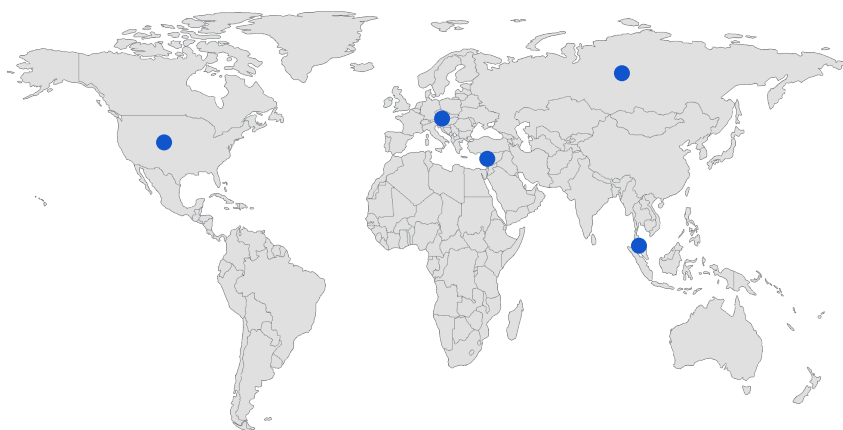


Threat Intel Report: February 3-9, 2025

Countries



Top Tags

Time Bandit

Tiny.FUD

Sector 16

Handala

Paragon

Executive Summary

Actionable Information:

- **AI Exploitation & Supply Chain Risks:** Threat actors are increasingly targeting AI ecosystems, with techniques such as the Time Bandit jailbreak bypassing ChatGPT safeguards and infostealer malware impersonating AI tools on PyPI. These incidents highlight the growing risk of AI-powered social engineering and supply chain attacks affecting developers.
- **Evolving Ransomware & Insider Threats:** Cybercriminals are now actively recruiting insiders to facilitate ransomware attacks, making them more damaging and harder to detect. Organizations must implement strict access controls and behavioral monitoring to mitigate this rising threat.
- **Critical Infrastructure & Government Targets:** Russian-linked threat actors continue to target U.S. energy infrastructure (Sector 16 campaign) and major corporations (HPE breach), signaling ongoing cyber espionage efforts. Meanwhile, the Handala Hackers breach of Israeli police data underscores the persistent cyber threats against government institutions.
- **Financial & Retail Attacks on the Rise:** Web skimming attacks, such as the Casio breach, continue to evolve, making payment data theft harder to detect. Additionally, the emergence of cryptocurrency-stealing apps on Apple's App Store highlights vulnerabilities in mobile financial security, even within tightly controlled ecosystems.
- **Healthcare Data Exposure Concerns:** The massive healthcare data breach affecting 8.9 million individuals demonstrates the risks posed by third-party security gaps. Organizations handling sensitive health information should prioritize data segmentation, access restrictions, and stronger vendor security assessments.

Outlook:

Cyber threats are evolving in complexity, with a notable shift towards AI exploitation, insider recruitment, and targeted cyber espionage against critical sectors. The increasing frequency of nation-state attacks against infrastructure and corporations suggests that geopolitical tensions will continue to drive cyber operations in 2024. Meanwhile, financial cybercrime remains a persistent challenge, with fraudsters refining their methods in mobile, retail, and cryptocurrency-related attacks. Moving forward, organizations must adopt a proactive security posture, integrating AI-aware threat defenses, supply chain risk management, and robust insider threat detection strategies.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

📈 1,083% [CVE-2024-12987](#)

- A vulnerability, which was classified as critical, was found in DrayTek Vigor2960 and Vigor300B 1.5.1.4. Affected is an unknown function of the file /cgi-bin/mainfunction.cgi/apmcfgupload of the component Web Management Interface. The manipulation of the argument session leads to os command injection.

📈 128% [CVE-2024-25600](#)

- Improper Control of Generation of Code ('Code Injection') vulnerability in Codeer Limited Bricks Builder allows Code Injection.

📈 68% [CVE-2024-7593](#)

- Incorrect implementation of an authentication algorithm in Ivanti vTM other than versions 22.2R1 or 22.7R2 allows a remote unauthenticated attacker to bypass authentication of the admin panel.

Austrian Sports Site Targeted by ATO

+Austria +Sports +ATO

- An Austrian sports site was targeted by account takeover (ATO) attacks over four days, averaging almost 1 million logins per day. The attacks, which were almost entirely brute force, targeted the site's Single Sign-On page and came from 1,100 France-based IPs.

Singaporean Financial Site Attacked by Bots

+Singapore +Financial Services +API +Path Traversal +XSS

- A Singaporean financial company's API portal was attacked using path traversal and cross-site scripting (XSS) in a two-day onslaught, primarily coming from UK-based IP addresses. The attacks, which averaged 1.1 million requests per day, came from bots.

Recent Cyber Threats

Time Bandit ChatGPT Jailbreak Evades AI Safeguards

+AI +LLM +Time Bandit +ChatGPT

- A new jailbreak method called [Time Bandit](#) successfully bypasses OpenAI's safeguards, allowing users to generate harmful and unethical content. By manipulating ChatGPT into thinking it is responding to future prompts, attackers can extract information that is otherwise restricted. This technique could be exploited for social engineering, misinformation, or fraud.

Casio Websites Targeted in Double Entry Web Skimming Attack

+Web Skimming +eCommerce

- Hackers deployed a sophisticated [double entry](#) web skimming attack across 16 Casio websites, injecting malicious scripts to steal payment data. The technique involved loading two skimmers—one for real-time data theft and another for redundancy—making detection harder. Magecart-style attacks like this highlight ongoing threats to e-commerce security.

Deepseek AI Tools Mimicked to Spread Infostealer Malware on PyPI

+AI +PyPI +Python

- Cybercriminals uploaded malicious packages to [PyPI](#), impersonating Deepseek AI tools to distribute infostealer malware. These fake Python libraries were designed to exfiltrate credentials and sensitive data from developers. This highlights the increasing risk of supply chain attacks targeting AI and machine learning ecosystems.

Tiny.FUD: Fully Undetectable macOS Backdoor Emerges

+Tiny.FUD +Backdoor +MacOS

- A new macOS backdoor named [Tiny.FUD](#) has been discovered, capable of operating undetected by security tools. The malware uses sophisticated obfuscation techniques and persistence mechanisms, allowing attackers to maintain access to compromised devices. Researchers warn that this represents an evolving macOS threat landscape.

Cybercriminals Collaborate with Insiders for Ransomware Extortion

+Ransomware +Insider Threat

- A new cybercrime trend sees ransomware groups recruiting [insiders](#) to facilitate attacks, providing access credentials and disabling security measures. These collaborations make attacks more damaging and harder to detect. Security experts urge organizations to implement strict access controls and insider threat monitoring.

Crypto-Stealing Apps Found in Apple App Store for the First Time

+Crypto +Apple +Apps

- For the first time, researchers have identified [cryptocurrency-stealing apps](#) on the Apple App Store, bypassing Apple's stringent security checks. The fraudulent apps trick users into entering wallet credentials, allowing attackers to drain their funds. This incident raises concerns about Apple's app vetting process and the growing threat of mobile crypto theft.

Data Breaches

New Russian Threat Group Hacks U.S. Energy Sector

+Sector 16 +Russia +US +Energy

- A previously unknown Russian threat group known as [Sector 16](#) has compromised multiple U.S. energy organizations in an ongoing cyber espionage campaign. The attackers used custom malware and spear-phishing tactics to infiltrate networks, potentially gathering intelligence for future disruptive operations. The breach raises concerns about critical infrastructure security amid rising geopolitical tensions.

Handala Hackers Leak Israeli Police Data in Major Breach

+Handala +Israel +Government

- The pro-Palestinian hacktivist group [Handala Hackers](#) has leaked sensitive Israeli police data, including personal details of officers and operational documents. The breach, part of a larger cyber campaign, raises concerns about data security in law enforcement agencies. Israeli authorities are investigating the incident and its potential impact on national security.

Paragon Spyware Exploits WhatsApp to Target European Users

+Paragon +Israel +Spyware

- [Paragon](#), an Israeli surveillance firm, has allegedly deployed spyware targeting European users through WhatsApp. The spyware exploits vulnerabilities to gain access to private messages, calls, and device data. This discovery highlights the continued use of commercial spyware for intelligence gathering and surveillance.

Huge Healthcare Data Breach Exposes 8.9 Million Records

+Healthcare +US

- A massive data breach in [Community Healthcare Center](#) has compromised the personal and medical records of 8.9 million individuals, including names, Social Security numbers, and health information. The breach, affecting multiple healthcare providers, was linked to vulnerabilities in a third-party system. The exposure raises concerns about the security of sensitive health data and potential identity theft risks.

HPE Employees Targeted in Russian-Linked Data Breach

+Russia +Business

- [Hewlett Packard Enterprise](#) (HPE) has notified employees of a data breach following a Russian-linked attack on its Office 365 email system. The breach, discovered in December 2023, exposed employee data and internal communications. This incident underscores the continued targeting of Western corporations by nation-state actors.

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.