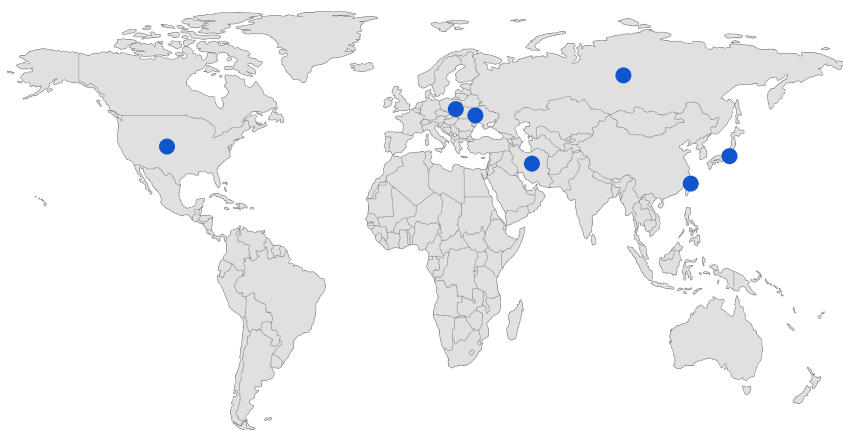


Threat Intel Report: March 3-9, 2025

Countries



Top Tags

Space Pirates

Lumma Stealer

ClickFix

Eleven11Bot

Qilin

Executive Summary

Actionable Information:

- **State-Backed and Geopolitical Cyber Operations:** Several cyber incidents this week highlight persistent threats against government and critical infrastructure. Attacks on Poland's space agency (POLSA) and Ukraine's Ministry of Foreign Affairs, likely linked to nation-state actors or politically motivated groups, demonstrate the ongoing targeting of government entities. Additionally, the Iran-linked Eleven11bot is actively launching DDoS attacks on telecommunications and gaming sectors.
- **Ransomware and Financial Data Breaches on the Rise:** The Qilin ransomware attack on Ukraine and the Bank of America data breach underscore the continued targeting of financial institutions and government entities. These attacks highlight the importance of third-party security assessments, as the Bank of America incident was linked to a vendor's mishandling of sensitive data.
- **Phishing and Malware Campaigns Expanding Scope:** Attackers continue to refine phishing techniques, as seen in the ClickFix campaign abusing SharePoint and the Lumma Stealer malware using fake CAPTCHA pages. Organizations should enforce multi-factor authentication (MFA), educate employees on phishing tactics, and monitor for unusual activity in cloud environments.
- **Web-Based and IoT Exploits Continue to Grow:** More than 1,000 WordPress sites were infected with JavaScript backdoors, and 49,000 misconfigured building access systems were discovered online. The exposure of API keys in AI training datasets also highlights a growing risk in cloud and machine learning security. Organizations must prioritize proper credential management, apply web security best practices, and assess IoT vulnerabilities to mitigate these risks.
- **Widespread Data Breaches Affecting Businesses and Schools:** High-profile breaches at Chicago Public Schools (CPS) and NTT Communications demonstrate that both public and private institutions continue to

struggle with data protection. The CPS incident, affecting 700,000 students, and the NTT breach, impacting 18,000 corporate clients, emphasize the necessity of vendor risk management and strict data handling policies.

Outlook:

The trends observed this week indicate a continued escalation in cyberattacks targeting both government institutions and private enterprises. The increasing sophistication of phishing campaigns, such as ClickFix, and the persistence of ransomware groups like Qilin suggest that cybercriminals are adapting their tactics to bypass traditional defenses. As state-backed cyber operations grow more aggressive, critical infrastructure sectors—including space, telecommunications, and financial services—will likely remain high-priority targets. Additionally, the discovery of sensitive credentials within AI training datasets highlights emerging security concerns in the machine learning and API security landscape. Organizations must strengthen their cybersecurity posture through proactive threat intelligence, improved access controls, and rigorous third-party security assessments.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

📈 14,064% [CVE-2024-20767](#)

- ColdFusion versions 2023.6, 2021.12 and earlier are affected by an Improper Access Control vulnerability that could result in arbitrary file system read. An attacker could leverage this vulnerability to access or modify restricted files. Exploitation of this issue does not require user interaction. Exploitation of this issue requires the admin panel be exposed to the internet.

📈 1,168% [CVE-2024-2879](#)

- The LayerSlider plugin for WordPress is vulnerable to SQL Injection via the `ls_get_popup_markup` action in versions 7.9.11 and 7.10.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.

📈 485% [CVE-2024-21893](#)

- A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication.

Brazilian Dating Site Targeted by 1.6M RPS DDoS Attack

+Brazil +Society +DDoS

- A Brazilian online dating site was targeted by DDoS this week, reaching 1.6 million requests per second (RPS) in just under an hour. The attack came from just 313 US and India-based IP addresses.

Japanese Site Hit by Automated Attacks

+Japan +Automated Attack +Path Traversal

- A Japanese site was attacked by automated attacks and path traversal recently, reaching almost 7 million requests in one day. The attacks came exclusively from within Japan.

Recent Cyber Threats

Cyberattack Hits Polish Space Agency

+Poland +Government +POLSA

- Poland's space agency ([POLSA](#)) experienced a cyberattack, prompting an investigation. In response, the agency disconnected its network from the internet, and its website remained inaccessible as of Monday. Poland's digital minister, Krzysztof Gawkowski, confirmed that state cybersecurity services had detected unauthorized access to POLSA's IT infrastructure and secured the affected systems. Cyber specialists are now working to identify the attackers behind the breach.

Space Pirates Target Russian IT Firms with 'LuckyStrike' Malware

+Russia +Space Pirates +LuckyStrike Agent

- The threat actor known as [Space Pirates](#) has launched a campaign against Russian IT organizations, deploying a new malware dubbed LuckyStrike Agent. Detected in November 2024, the group infiltrated networks using tools like Deed RAT and a modified Stowaway proxy. Over 19 months, they expanded their presence within compromised systems, utilizing Microsoft OneDrive for command-and-control operations.

WinOS 4.0 Malware Targets Taiwanese Companies via Phishing

+Taiwan +Government +WinOS 4.0

- In January 2025, attackers targeted [Taiwanese](#) companies by impersonating official Ministry of Finance communications. They distributed emails with attachments purportedly listing enterprises scheduled for tax inspections, urging recipients to forward the information internally.

Fake CAPTCHA PDFs Distribute Lumma Stealer Malware

+Lumma Stealer

- A widespread phishing campaign has been identified, involving over 5,000 PDF files across 260 domains. These PDFs, hosted on platforms like Webflow and GoDaddy, contain fake CAPTCHA images that trick users into executing malicious PowerShell commands, resulting in the installation of the [Lumma Stealer](#) malware. Since mid-2024, this campaign has affected more than 7,000 users across sectors including technology, financial services, and manufacturing, primarily in North America, Asia, and Southern Europe.

Massive Exposure of Building Access Systems

+AMS +Business

- Researchers have identified over 49,000 misconfigured [Access Management Systems](#) (AMS) globally, spanning various industries. These systems, lacking proper authentication, expose sensitive employee data such as personal details, biometric information, and access logs. The vulnerabilities could allow malicious actors to manipulate building entry protocols, posing significant physical security risks.

ClickFix Phishing Campaign Deploys Havoc C2 via SharePoint

+ClickFix

- A sophisticated phishing campaign, termed [ClickFix](#), tricks users into executing malicious PowerShell commands under the guise of fixing system errors. By exploiting Microsoft SharePoint, attackers deploy the Havoc post-exploitation framework, granting remote access to compromised devices.

Iran-Linked Botnet Targets Telecom and Gaming Sectors

+Iran +Eleven11Bot

- The [Eleven11bot](#) botnet, comprising over 30,000 compromised devices, predominantly security cameras and network video recorders, has been launching DDoS attacks against telecommunications providers and gaming platforms. Originating mainly from Iran, the botnet exploits weak or default passwords on IoT devices, leading to significant disruptions in targeted sectors.

Over 1,000 WordPress Sites Compromised with JavaScript Backdoors

+WordPress +Backdoor

- More than 1,000 [WordPress](#) websites have been infected with malicious JavaScript code, resulting in the installation of multiple backdoors. These backdoors allow persistent unauthorized access, enabling attackers

to execute commands, inject malicious scripts, and maintain control over compromised sites. Website administrators are advised to review and secure their installations to mitigate potential threats.

Data Breaches

12,000+ API Keys and Passwords Exposed in Public Datasets

[+API](#) [+LLM](#)

- Security researchers discovered that [datasets](#) used to train large language models (LLMs) contained over 12,000 active API keys and passwords. These credentials, embedded in public code repositories, pose significant security risks as they can grant unauthorized access to various services. The exposure underscores the importance of sanitizing training data to prevent inadvertent leakage of sensitive information.

Qilin Ransomware Gang Breaches Ukrainian Ministry

[+Ukraine](#) [+Qilin](#) [+Government](#)

- The [Qilin](#) ransomware group claimed responsibility for a cyberattack on Ukraine's Ministry of Foreign Affairs. They allege to have exfiltrated sensitive data, including private communications and official documents, some of which have reportedly been sold to third parties. This incident highlights the persistent threat of ransomware groups targeting government entities.

Chicago Public Schools Data Breach Exposes Student Information

[+US](#) [+Education](#)

- A cyberattack on a vendor of [Chicago Public Schools](#) (CPS) resulted in unauthorized access to personal information of over 700,000 current and former students dating back to the 2017-2018 school year. Exposed data includes names, dates of birth, genders, CPS student ID numbers, and, for Medicaid-enrolled students, Medicaid ID numbers and eligibility dates. No Social Security numbers, financial information, or health data were compromised. CPS is collaborating with law enforcement and has notified affected families.

Bank of America Alerts Customers to Data Breach

[+US](#) [+Financial Services](#)

- [Bank of America](#) has notified a select group of customers about a data breach resulting from improper handling of confidential documents by a third-party vendor. The breach, occurring on December 30, potentially exposed sensitive information, including names, addresses, Social Security numbers, and financial account details. Impacted customers have been offered complimentary identity theft protection services for two years.

Data Breach at Japanese Telecom Giant NTT Affects 18,000 Companies

[+Japan](#) [+Telecommunications](#)

- [NTT Communications Corporation](#) experienced unauthorized access to its 'Order Information Distribution System,' compromising data of approximately 17,891 corporate customers. Exposed information includes company names, representative details, contact numbers, email addresses, physical addresses, and service usage specifics. The breach did not affect individual consumer data.

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.