

# Threat Intel Report: February 24-March 2, 2025

## Countries



## Top Tags

FatalRat

GRUB2

Auto-Color

Linux

Lazarus

## Executive Summary

### Actionable Information:

- **Authentication Exploits & Password Attacks:** The rise in password-based attacks remains a major concern. The Microsoft 365 botnet campaign demonstrates how attackers continue to abuse Basic Authentication to bypass MFA protections. *Organizations should disable outdated authentication methods and enforce MFA across all accounts.*
- **Supply Chain & Software Integrity Risks:** Malicious VSCode extensions affecting millions of users highlight the growing security risks in third-party software and developer tools. *Regular security audits of installed extensions and application dependencies are crucial to prevent supply chain compromises.*
- **Nation-State Attacks on Critical Infrastructure & Finance:** The Lazarus Group's \$1.5 billion cryptocurrency heist reinforces North Korea's strategic targeting of digital financial assets to fund illicit activities. Concurrently, FatalRAT phishing campaigns targeting APAC industries and the Auto-Color Linux backdoor aimed at government institutions show *persistent threats from well-resourced actors.*
- **Widespread Vulnerabilities in Open-Source and Enterprise Systems:** The Exim MTA and GRUB2 bootloader vulnerabilities expose millions of systems to potential exploitation. These flaws demonstrate the *continued need for proactive patching strategies to prevent attackers from leveraging unpatched weaknesses in widely used software.*
- **Data Breaches & Exposure of Sensitive Information:** The breaches at Zacks Investment Research and Geisinger Health System underscore the financial and healthcare industries' vulnerability to data theft. These incidents highlight the importance of *secure data handling, encryption, and access controls to prevent unauthorized exposure.*

## Outlook:

The ongoing trends indicate that cybercriminals and nation-state actors continue to evolve their attack strategies, targeting both critical infrastructure and financial assets. With increasing reliance on third-party software and cloud-based authentication, enterprises must prioritize supply chain security and robust identity protection measures. As vulnerabilities in commonly used software persist, proactive patching and security hygiene remain key defenses. Expect to see further attacks exploiting weak authentication mechanisms, financial fraud campaigns linked to nation-state actors, and continued data breaches affecting high-value industries. Organizations must enhance threat detection capabilities and enforce stricter security policies to mitigate these emerging risks.

---

## Threat Activity in Imperva

### Top CVE Growth This Week:

**Imperva customers are protected against these CVEs.**

↑ 1,150% [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.

↑ 221% [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/apmcfupload` of the component Web Management Interface. The manipulation of the argument session leads to os command injection. It is possible to launch the attack remotely.

↑ 146% [CVE-2024-53704](#)

- An Improper Authentication vulnerability in the SSLVPN authentication mechanism allows a remote attacker to bypass authentication.

### US Financial Site Targeted by ATO

**+US +Financial Services +ATO**

- A US Financial Services site was attacked last week, leveraging account takeover attacks to target the company's API login portal. The attacks, which were primarily brute force, primarily leveraged bots.

### Brazilian Energy Site Targeted by Path Traversal and Automated Attacks

**+Brazil +Energy**

- A Brazilian energy company was targeted by path traversal and automated attacks, coming from US-based IPs. Attacks attempted to leverage vulnerabilities in CGI scripts and F5 BIG-IP iControl.
- 

## Recent Cyber Threats

### Sitevision CMS Vulnerability Exposes Private Keys

**+Java +Private Keys +CMS**

- A critical vulnerability in [Sitevision](#) CMS versions 10.3.1 and earlier allowed attackers to extract private keys used for signing SAML authentication requests. The flaw stemmed from the use of a Java keystore accessible

via WebDAV, protected by a weak, auto-generated password. By exploiting this vulnerability, attackers could potentially compromise authentication processes, affecting organizations relying on Sitevision for content management. Sitevision addressed the issue in version 10.3.2 by enforcing stronger password complexity.

### Exim MTA Vulnerability Permits SQL Injection Attacks

[+SQLi](#) [+MTA](#)

- A critical SQL injection vulnerability ([CVE-2025-26794](#)) has been identified in the Exim mail transfer agent (MTA), potentially allowing attackers to compromise email systems and manipulate underlying databases. This flaw affects versions prior to the latest patch, underscoring the urgency for administrators to update their Exim installations to mitigate potential exploitation.

### Botnet Exploits Basic Authentication in Microsoft 365

[+Microsoft 365](#) [+Botnet](#) [+Password Spray](#)

- A botnet comprising over 130,000 compromised devices is conducting password-spray attacks against [Microsoft 365](#) accounts worldwide. By leveraging Basic Authentication, the attackers bypass Multi-Factor Authentication (MFA) protections, gaining unauthorized access without triggering security alerts. This method exploits non-interactive sign-ins, commonly used for legacy protocols, highlighting the need for organizations to disable Basic Authentication and monitor non-interactive sign-in attempts to mitigate such threats.

### FatalRAT Targets APAC Industries via Phishing

[+FatalRAT](#) [+APAC](#)

- Industrial organizations in the Asia-Pacific region have been targeted by phishing attacks distributing [FatalRAT](#) malware. Attackers utilized legitimate Chinese cloud services like myqcloud and Youdao Cloud Notes for their infrastructure, employing a sophisticated multi-stage payload delivery framework to evade detection. The campaign targeted sectors including manufacturing, construction, IT, telecommunications, healthcare, and energy across countries such as Taiwan, Malaysia, China, Japan, and others.

### GRUB2 Bootloader Flaws Threaten Millions of Linux Systems

[+GRUB2](#) [+Linux](#) [+Bootloader](#)

- Multiple critical vulnerabilities have been discovered in the [GRUB2](#) bootloader, widely used across Linux distributions. These flaws, including heap overflows and use-after-free errors, could allow attackers to bypass security measures, potentially compromising millions of systems globally. Administrators are advised to update GRUB2 and related components promptly to address these security issues.

### Auto-Color Linux Backdoor Targets North American Entities

[+Auto-Color](#) [+Linux](#) [+Backdoor](#) [+Government](#)

- A previously undocumented Linux backdoor, dubbed [Auto-Color](#), has been detected targeting universities and government organizations in North America and Asia between November and December 2024. The malware is highly evasive, capable of maintaining persistent access, and poses significant challenges for detection and removal.

### Malicious VSCode Extensions with Millions of Installs Removed

[+Microsoft](#) [+VSCode](#)

- Microsoft has removed two popular [Visual Studio Code](#) (VSCode) extensions, 'Material Theme – Free' and 'Material Theme Icons – Free,' from the marketplace after discovering malicious code within them. These extensions had amassed nearly 9 million downloads, potentially exposing a vast number of developers to security risks. Users are advised to uninstall these extensions and review their development environments for any signs of compromise.

---

## Data Breaches

### Lazarus Group Implicated in \$1.5 Billion Bybit Cryptocurrency Theft

[+Lazarus](#) [+Crypto](#) [+North Korea](#)

- North Korea's [Lazarus Group](#) has been implicated in the theft of over \$1.5 billion worth of Ethereum from the cryptocurrency exchange Bybit. The hackers exploited a routine transfer process, redirecting funds from Bybit's cold wallet to an address under their control. This incident marks the largest cryptocurrency heist to date, with stolen assets potentially funding North Korea's missile programs.

#### Data Breach at Investment Research Firm Exposes 12 Million Records

##### +Financial Services

- [Zacks Investment Research](#) suffered a data breach compromising 12 million customer records. A cybercriminal initially claimed to have stolen 15 million records, but investigations confirmed 12 million were affected. Exposed information includes sensitive customer and client records, highlighting vulnerabilities within financial research firms.

#### Geisinger Health System Data Breach Discovered on California Laptop

##### +Healthcare

- Personal information from a significant data breach at [Geisinger Health System](#) was found on a personal laptop in California. The discovery raises concerns about the extent of the breach and the potential misuse of sensitive patient data. Authorities are investigating the incident to determine how the information was obtained and to mitigate further risks to affected individuals.

---

## 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.