

Threat Intel Report: March 31-April 6, 2025

Countries



Top Tags

Triton

ClickFix

Qakbot

PowerShell

API

Executive Summary

Actionable Information:

- **Crypto Phishing Campaigns on the Rise:** This week, over 500 phishing domains targeting Bybit users highlight the continuing trend of cybercriminals focusing on the cryptocurrency sector. As seen with other attacks, crypto platforms remain a prime target for credential theft and fund exfiltration.
- **Exploitation of Legacy and Unsecured APIs:** Several breaches, including the X (Twitter) data leak and the Verizon Call Filter API vulnerability, demonstrate attackers' increasing use of outdated or poorly secured APIs to access sensitive user data. These API-based attacks are becoming a preferred method of data exfiltration due to their stealthy nature and widespread use in modern applications.
- **Social Engineering and RATs:** The widespread use of Remote Access Trojans (RATs), such as the Triton RAT targeting Roblox credentials, underscores the increasing sophistication of social engineering tactics. These attacks use familiar platforms like Microsoft Teams and Roblox to deliver malware, evading traditional security defenses and exploiting user trust.
- **Exploits in Popular Software Platforms:** Critical vulnerabilities, such as those in WordPress plugins, Apache Parquet, and CrushFTP, highlight ongoing risks in widely-used software. Attackers are consistently targeting these platforms for remote code execution or unauthorized access, taking advantage of unpatched flaws in a variety of industries, including e-commerce, telecommunications, and legal sectors.

Outlook:

Looking ahead, attackers are expected to continue exploiting vulnerabilities in widely-used platforms and applications, particularly targeting APIs and third-party integrations. As seen with the massive data leak from X (Twitter) and the breach of various pension funds and automotive platforms, cybercriminals are honing in on high-value sectors with significant personal data, often leveraging social engineering and advanced malware tactics to

bypass security measures. Financial institutions and large corporations will need to increase their focus on securing APIs, patching vulnerabilities promptly, and enhancing employee awareness of phishing and RAT risks. Additionally, as the exposure of private and sensitive data remains a top concern, industries managing personal data, such as legal, healthcare, and social media, must prioritize strengthening their security posture against both external and internal threats.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 16,800% [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.

↑ 2,500% [CVE-2024-51568](#)

- CyberPanel (aka Cyber Panel) before 2.3.5 allows Command Injection via `completePath` in the `ProcessUtilities.outputExecutioner()` sink. There is `/filemanager/upload` (aka File Manager upload) unauthenticated remote code execution via shell metacharacters.

↑ 2,294% [CVE-2024-53675](#)

- An XML external entity injection (XXE) vulnerability in HPE Insight Remote Support may allow remote users to disclose information in certain cases.

Recent Cyber Threats

Over 500 Phishing Domains Targeting Bybit Users

+Bybit +Crypto +Phishing

- Cybercriminals have set up over 500 phishing domains mimicking [Bybit](#) to steal user credentials. These domains target unsuspecting cryptocurrency investors by impersonating the exchange, compromising both individual and institutional accounts. The phishing efforts are part of a larger trend of targeting crypto platforms, aiming to steal funds and personal information.

Critical WordPress Plugin Vulnerability Affects 90,000 Sites

+Tags

- A critical vulnerability in a widely-used [WordPress](#) plugin, with over 90,000 active installations, allows attackers to exploit a lack of proper input validation. The flaw, tracked as CVE-2025-2294, lets malicious actors gain unauthorized access by bypassing security controls, potentially allowing them to alter or control vulnerable websites.

Triton RAT Targets Roblox Credentials

+Triton +RAT +Gaming

- A Python-based Remote Access Trojan (RAT), [Triton](#), is being used to steal credentials from Roblox users. The RAT is distributed through social engineering tactics, infecting systems with malicious payloads that allow attackers to gain control of users' accounts, potentially leading to the theft of in-game assets or personal data.

Malicious Code Hidden in WordPress MU-Plugins

[+WordPress](#) [+Malware Injection](#)

- Attackers are exploiting the [Multi-User \(MU\) Plugin](#) functionality in WordPress to inject persistent malicious code into websites. This tactic involves hiding malicious scripts within the MU-Plugin, which is typically overlooked by security systems due to its deep integration within WordPress configurations.

ClickFix CAPTCHA Distributes Malware

[+Malware](#) [+CAPTCHA](#) [+ClickFix](#) [+Qakbot](#) [+PowerShell](#)

- Hackers are using a fake CAPTCHA system called [ClickFix](#) to distribute infostealers, ransomware, and Qakbot malware. The technique tricks victims into executing malicious commands that lead to PowerShell scripts downloading and executing payloads. This attack primarily targets Windows users and relies on social engineering to bypass traditional security mechanisms.

CrushFTP Authentication Bypass Exposes Servers

[+File Transfer Program](#)

- A critical vulnerability, CVE-2025-31161 (previously tracked as CVE-2025-2825) in [CrushFTP](#) versions 10 and 11 allows unauthenticated remote access to exposed servers. Disclosed on March 21, 2025, the flaw has been actively exploited, with over 1,500 unpatched instances targeted, primarily from Asia. Users are advised to update to versions 10.8.4 or 11.3.1 promptly to mitigate risks.

Malware Delivered via Microsoft Teams Messages

[+Malware](#) [+PowerShell](#) [+Teams](#)

- Attackers are exploiting [Microsoft Teams](#) by sending malicious PowerShell scripts through crafted messages, leading to credential theft and persistent backdoors. The campaign utilizes social engineering to bypass traditional defenses, highlighting the evolving tactics in malware delivery via trusted platforms.

Exploitation of Legacy Stripe API in Web Skimmer Campaign

[+API](#) [+eCommerce](#) [+Web Skimming](#)

- Cybercriminals are leveraging a deprecated [Stripe API](#) to validate stolen payment card information before exfiltration. Affecting 49 merchants since August 2024, this sophisticated web skimmer ensures only valid card data is stolen, making detection more challenging.

Verizon Call Filter API Flaw Exposes Call Histories

[+US](#) [+Telecommunications](#) [+API](#)

- A vulnerability in [Verizon's](#) Call Filter API allowed unauthorized access to customers' incoming call logs. Discovered on February 22, 2025, and patched the following month, the flaw exposed call histories due to unsecured API endpoints.

Critical Apache Parquet Flaw Enables Remote Code Execution

[+RCE](#) [+Apache](#) [+Java](#)

- A severe vulnerability in [Apache Parquet's](#) Java Library (CVE-2025-30065) allows remote attackers to execute arbitrary code. Affecting versions up to 1.15.0, the flaw has been addressed in version 1.15.1, with a CVSS score of 10.0, or critical severity.

Data Breaches

Massive X (Twitter) Data Leak Exposes Over 200 Million User Records

[+Social Media](#) [+API](#)

- A massive data leak affecting [X \(formerly Twitter\)](#) exposed over 200 million user records, including personal information such as email addresses and phone numbers. This breach was made possible by exploiting a vulnerability in the platform's API, which was discovered in late 2022. Attackers were able to harvest user data, leaving millions of individuals at risk of identity theft and phishing attacks.

Royal Mail Data Leak Blamed on Supplier Spectos

+UK +Government

- A hacker leaked 144GB of data from [Royal Mail Group](#), blaming the breach on its supplier, Spectos. The leaked data includes sensitive information on customers, contracts, and operations, raising concerns about third-party vendor security. The breach has impacted numerous customers and exposed private business details, highlighting the risks associated with relying on external service providers.

Australian Pension Funds Hacked, Millions at Risk

+Australia +Government

- Hackers successfully breached multiple [Australian pension funds](#), compromising sensitive personal and financial data of millions of account holders. The attack was carried out using advanced phishing techniques to gain access to the funds' systems. The breach has prompted an investigation into the adequacy of cybersecurity measures within financial institutions that manage critical pension data.

State Bar of Texas Confirms Data Breach

+US +Legal +Government

- The [State Bar of Texas](#) confirmed a significant data breach after attackers gained unauthorized access to sensitive attorney and client data. The breach affected personal and legal information, with the compromised data including Social Security numbers, birth dates, and contact information. Affected individuals are being notified, and the organization is working to assess the extent of the breach.

Europcar Data Breach and GitLab Hack Affects Up to 200,000 Customers

+Automotive

- [Europcar](#) confirmed a data breach linked to a GitLab hack, exposing personal data of up to 200,000 customers. The breach occurred when an employee's credentials were stolen, allowing attackers to access sensitive customer information. The compromised data included names, addresses, and payment information, highlighting vulnerabilities in supply chain security.

Dating App Data Breach Exposes 1.5 Million Private User Images

+Adult

- A breach affecting five [LGBT dating apps](#) exposed over 1.5 million private and explicit images stored without adequate security measures. The apps had stored these images in unsecured cloud storage, making them vulnerable to access by unauthorized parties. The breach has put users at risk of blackmail and extortion, particularly in regions with anti-LGBT sentiments.

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.