Hive Pro

Threat Level

Red

Hiveforce Labs

# THREAT ADVISORY

## ATTACK REPORT

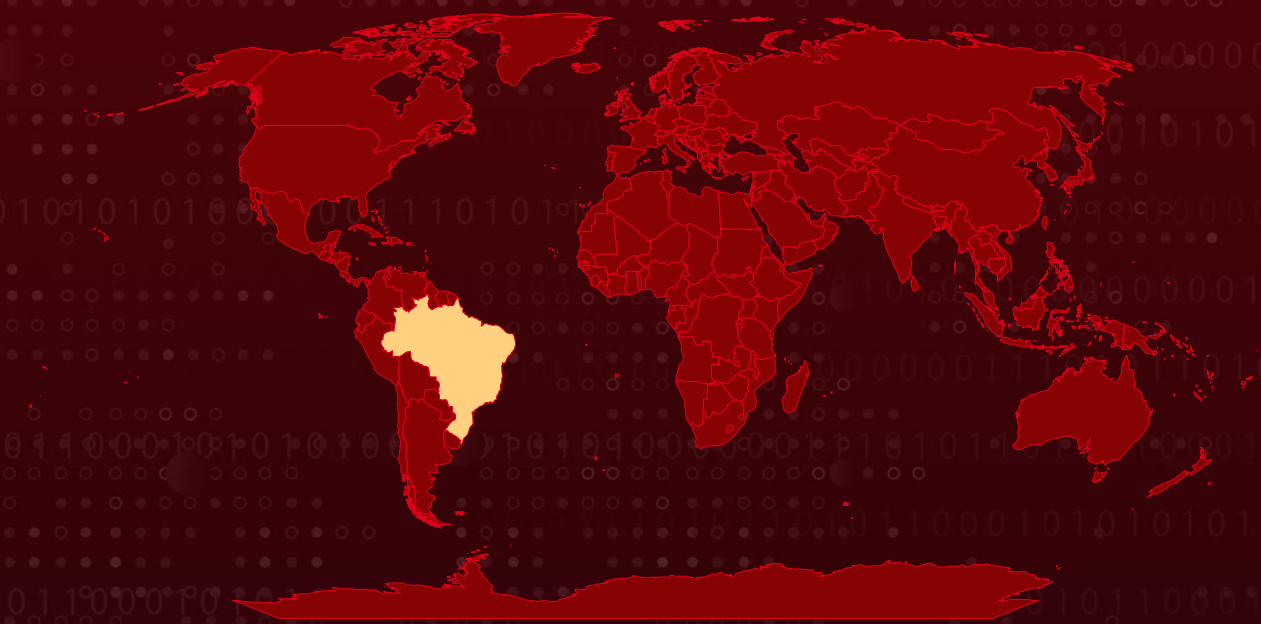
# VENON Trojan Targets 33 Brazilian Financial Platforms


| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| March 13, 2026 | A1 | TA2026070 |

# Summary

**First Seen:** February 2026
**Targeted Region:** Brazil
**Targeted Platform:** Windows
**Targeted Products:** Itaú Unibanco, Santander Brasil, Caixa Econômica Federal, Banco do Brasil, Nubank, Banco Inter, Sicoob, Sicredi, Banco Original, Banco Safra, BTG Pactual, PagBank/PagSeguro, PicPay, Mercado Pago, Bling ERP, Receita Federal, Binance, Coinbase, Kraken, Bybit, Mercado Bitcoin, Foxbit, Gemini, Nexo, Ripio, MetaMask, Trust Wallet, Phantom, Ledger Live, Rabby Wallet, Cake DeFi
**Targeted Industries:** Financial Services, Cryptocurrency, Banking, Government
**Malware:** VENON
**Attack:** VENON is a Rust-based banking RAT that targets 33 Brazilian financial institutions and cryptocurrency platforms. It employs DLL sideloading via a legitimate NVIDIA binary, nine anti-analysis evasion techniques, state-of-the-art encryption, and credential-stealing banking overlays. The malware also deploys VBScript-based shortcut hijacking specifically targeting the Itaú banking application. Evidence suggests AI-assisted development was used to rewrite classic Latin American banking Trojan functionality from Delphi into Rust.

## Attack Regions



Targeted  Non-Targeted

# Attack Details

**#1**

VENON is a banking malware campaign targeting users in Brazil. Unlike most malware used in the Latin American cybercrime ecosystem typically written in Delphi, VENON is built in Rust. The malware spreads through phishing emails, fake websites that imitate legitimate portals, and sponsored online advertisements. Infection begins when a user downloads a seemingly legitimate installer containing a trusted executable named NVIDIANotification.exe. The malware abuses Windows' DLL search order to load a malicious file named libcef.dll instead of the real Chromium Embedded Framework library. No technical exploit is required, the attack relies entirely on the victim launching the installer.

**#2**

Once executed, a small obfuscated batch script rebuilds hidden commands, file paths, and URLs during runtime to avoid signature detection. The script restarts itself with administrator privileges using PowerShell, then adds an exclusion in Microsoft Defender Antivirus to avoid detection. It downloads a ZIP file from Amazon Web Services storage, extracts the legitimate executable alongside the malicious DLL, and creates a Registry Run key to maintain persistence. The script deletes itself and forces a system reboot within seconds. After the restart, the Run key launches the program, the malicious DLL loads through sideloading, and the original infection evidence disappears.

**#3**

The malware then activates a chain of defensive evasion techniques. It bypasses Antimalware Scan Interface and Event Tracing for Windows, replaces the in-memory code of the Windows library ntdll.dll with a clean version from disk, and executes system calls indirectly to avoid security monitoring. It hides threads from debuggers, blocks external processes from accessing its memory, performs sandbox detection checks, prevents screenshots of its window, and verifies whether Windows Defender security identifiers are present.

**#4**

The malware then creates a scheduled task named "NVIDIA Notification Service" that runs at logon with elevated privileges. Communication with the command server occurs through encrypted WebSocket traffic over TLS using Rust networking libraries. Each infected system is uniquely identified through a hardware fingerprint derived from the computer name and disk serial number.

**#5**

VENON focuses on financial theft. It monitors activity across 33 banking and digital-asset platforms, including traditional banks, fintech services, government portals, cryptocurrency exchanges, and crypto wallets. The malware watches active window titles and browser domains. When a targeted site or application appears, it deploys credential-stealing overlays designed to capture login details. The campaign also includes a specialized attack against the Itaú banking application. Two embedded scripts replace legitimate desktop shortcuts with altered versions that redirect victims to attacker-controlled web pages while preserving the official bank icon. A remote restoration script allows operators to revert the system later, helping conceal the compromise.

# Recommendations

**Monitor for DLL Sideloading via NVIDIA Binaries:** Deploy detection rules to identify NVIDIANotification.exe or renamed variants (particularly those using Unicode characters like ®) executing from non-standard directories such as C:\ProgramData\USOShared\. Alert on any instance of libcef.dll being loaded from ProgramData paths rather than legitimate Chromium or NVIDIA installation directories.

**Audit Windows Defender Exclusions:** Regularly review and audit Windows Defender exclusion paths configured via Add-MpPreference. Flag any exclusions under C:\ProgramData\USOShared\ or similar paths mimicking legitimate Windows Update directories. Unauthorized exclusions should be immediately removed and investigated.

**Detect Registry Run Key Persistence:** Monitor HKCU\Software\Microsoft\Windows\CurrentVersion\Run for newly created entries, especially those referencing executables with Unicode characters in their filenames or located in typical directories. Correlate with process creation events for enhanced detection confidence.

**Implement WebSocket Traffic Inspection:** Deploy network monitoring capable of identifying WebSocket connections to unknown or recently registered domains. Since VENON uses WebSocket over TLS 1.3 for C2 communication, TLS inspection or DNS-based detection of C2 domains is critical for visibility into malware communications.

**Monitor for Evasion Technique Indicators:** Implement EDR rules to detect AMSI bypass attempts, ETW patching, ntdll .text section overwrites from disk, indirect syscall construction, and ThreadHideFromDebugger flag usage. These behaviors are strong indicators of advanced malware evasion activity.

**Protect Itaú Application Shortcuts:** For organizations with Brazilian banking exposure, monitor for modifications to .lnk files associated with Itaú banking application across user desktops, Start Menu, and public desktop directories. Alert on VBScript execution (wscript.exe) that accesses or modifies shortcut files targeting banking applications.

# Potential MITRE ATT&CK TTPs

| Tactic | Technique | Sub-technique |
|---|---|---|
| Initial Access | T1566: Phishing | |
| Execution | T1059: Command and Scripting Interpreter | T1059.001: PowerShell |
| | | T1059.005: Visual Basic |
| | T1204: User Execution | T1204.002: Malicious File |
| Persistence | T1547: Boot or Logon Autostart Execution | T1547.001: Registry Run Keys / Startup Folder |
| | T1053: Scheduled Task/Job | T1053.005: Scheduled Task |
| Privilege Escalation | T1548: Abuse Elevation Control Mechanism | T1548.002: Bypass User Account Control |
| Defense Evasion | T1574: Hijack Execution Flow | T1574.001: DLL |
| | T1562: Impair Defenses | T1562.001: Disable or Modify Tools |
| | | T1562.004: Disable or Modify System Firewall |

| Tactic | Technique | Sub-technique |
|---|---|---|
| Defense Evasion | T1027: Obfuscated Files or Information | |
| | T1036: Masquerading | T1036.005: Match Legitimate Name or Location |
| | T1070: Indicator Removal | T1070.004: File Deletion |
| | T1622: Debugger Evasion | |
| | T1497: Virtualization/Sandbox Evasion | |
| | T1106: Native API | |
| Command and Control | T1071: Application Layer Protocol | T1071.001: Web Protocols |
| | T1573: Encrypted Channel | T1573.001: Symmetric Cryptography |
| | T1102: Web Service | T1102.001: Dead Drop Resolver |
| | T1568: Dynamic Resolution | |
| Collection | T1115: Clipboard Data | |
| | T1113: Screen Capture | |
| Impact | T1565: Data Manipulation | T1565.002: Transmitted Data Manipulation |

# Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| Domains | brasilmotorsvs14[.]com,<br>lazybearpottery[.]net,<br>digitalmoineyp[.]com,<br>portalhondihs[.]com,<br>storage[.]googleapis[.]com |
| URLs | hxxps[:]//s3[.]sa-east-1[.]amazonaws[.]com/8151218-25[.]2025[.]7[.]12[.]5178/modmarco2026-2[.]zip,<br>hxxps[:]//storage[.]googleapis[.]com/mydns2026/startabril2026,<br>hxxps[:]//storage[.]googleapis[.]com/mydns2026/startmarco2026_1_,<br>hxxps[:]//storage[.]googleapis[.]com/mydns2026/startjaneiro_1_,<br>hxxps[:]//storage[.]googleapis[.]com/mydns2026/startabril_2,<br>hxxps[:]//pastebin[.]com/raw/2qEMcLsD,<br>hxxps[:]//digitalmoineyp[.]com/v2/cloudflare/avsmail/recive[.]php |
| IPv4 | 104[.]21[.]7[.]106,<br>188[.]114[.]96[.]3,<br>206[.]0[.]29[.]58,<br>51[.]222[.]75[.]250,<br>51[.]222[.]75[.]248,<br>192[.]99[.]226[.]117,<br>212[.]69[.]5[.]84,<br>34[.]227[.]229[.]85,<br>34[.]117[.]59[.]81,<br>142[.]251[.]140[.]187,<br>142[.]251[.]141[.]67,<br>142[.]251[.]140[.]163 |
| File Path | C:\ProgramData\USOShared\NuPLihaOH\,<br>C:\ProgramData\USOShared\NuPLihaOH\NVIDIANotification.exe,<br>C:\ProgramData\USOShared\NuPLihaOH\®mjtgr.exe,<br>C:\ProgramData\USOShared\NuPLihaOH\qYogBt.zip |
| Registry Key | HKCU\Software\Microsoft\Windows\CurrentVersion\Run |
| Filename | libcef.dll,<br>modmarco2026.zip,<br>DocumentReclamaAQUI_56b2ca9811.cmd.bin,<br>Itau_swap_install.vbs |
| MD5 | 427ccfa456ed27a819aa152708212ff4,<br>2d1c4778094ba0e1a6e13bb67ce1b631,<br>a99cb35768489b7aacf2d31d33d8f541 |

| TYPE | VALUE |
| --- | --- |
| SHA256 | c482286a7fdfb64d308c197a4deabcd773b8b62d9e74d1d08fcfd02568d75d72, 75d1a2560cf93c6a028aa3573febddaf713014d64b0e8904488111772e4cff49, fd5d9effc1ef77a49b0720d2691bc144f513609760c22fa62bc1e8b84dedf879, 78b62856878cb09602b14104df18ca2bedac8640e09d74b934ff3ea0e15627f3, d61be2b21e135726c547a388ecb47552559e5221894f5005ce35bdb24efc0c26 |

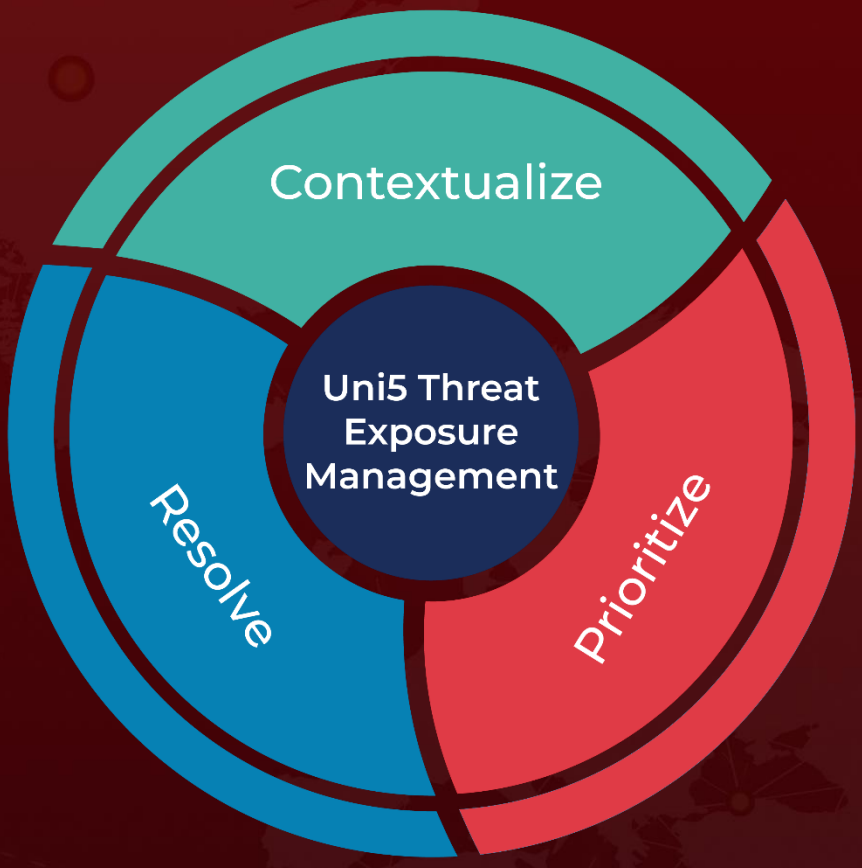
## References

https://zenox.ai/en/venon-the-first-brazilian-banker-rat-in-rust/

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.




REPORT GENERATED ON

**March 13, 2026 • 07:00 AM**



More at www.hivepro.com