Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

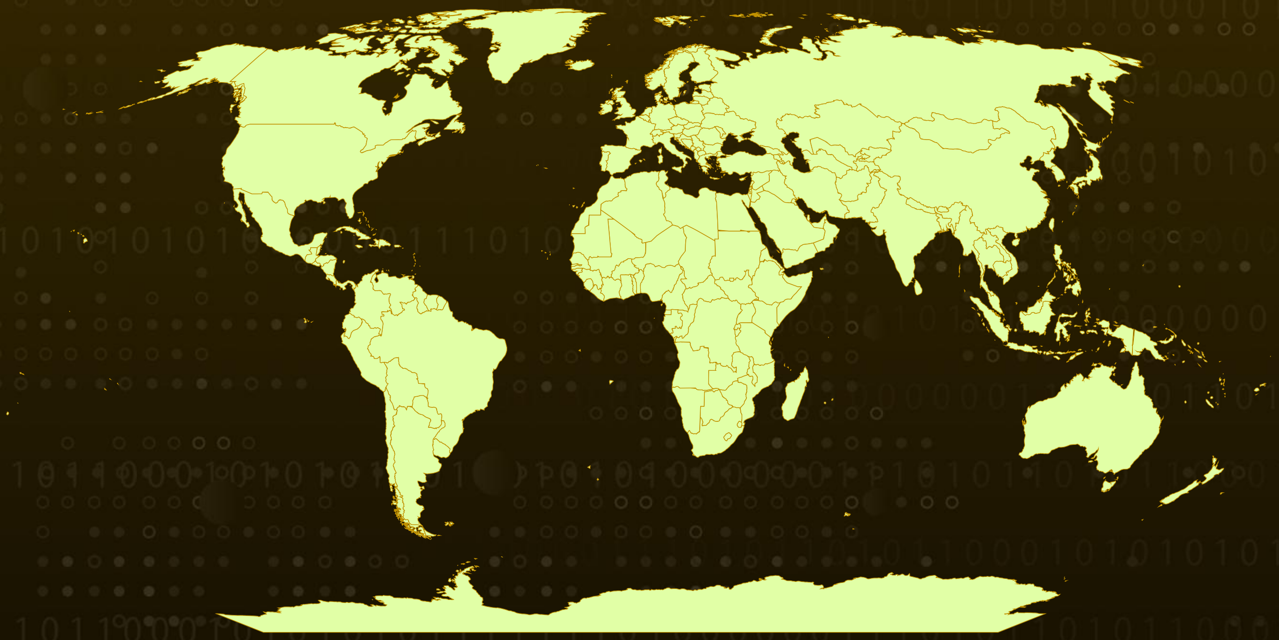
VVS Stealer Exposed: Inside a Stealthy Discord Credential Theft Operation

Date of Publication	Admiralty Code	TA Number
January 6, 2026	A1	TA2026003

Summary

First Seen: April 2025
Targeted Region: Worldwide
Affected Platform: Windows
Malware: VVS Stealer (also styled as VVS $tealer)
Attack: VVS Stealer is a Python-based information stealer that targets Discord users to exfiltrate sensitive credentials, tokens, and browser data. The malware has been marketed for sale on Telegram since April 2025 at various pricing tiers ranging from €10 weekly to €199 for lifetime access. The stealer employs advanced obfuscation through Pyarmor to evade static analysis and signature-based detection mechanisms. It is distributed as a PyInstaller package, enabling execution without additional dependencies. Key capabilities include Discord token theft, session hijacking via JavaScript injection, browser credential harvesting, screenshot capture, and persistence through Windows Startup folder installation. The malware displays fake error messages to distract victims during installation and exfiltrates stolen data via Discord webhooks.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Attack Details

#1 Discord, widely used for real-time communication, has increasingly become an attractive target for information-stealing malware. One such threat is VVS Stealer, a stealthy malware strain designed to harvest Discord credentials alongside sensitive browser data. It operates quietly in the background, ensuring persistence by automatically installing itself at system startup, displaying deceptive error messages, and even capturing screenshots to monitor user activity. Its primary objective is to hijack active Discord sessions by stealing authentication tokens, while also siphoning cookies, saved passwords, and browsing history from popular web browsers.

#2 The technical analysis begins with how the VVS malware is packaged and protected. The sample is distributed as a PyInstaller executable, which bundles Python applications and their dependencies into a single binary. Using PyInstaller's built-in utility, key components such as the compiled Python bytecode, the Pyarmor runtime files, and the Python 3.11 dynamic library are extracted. Initial inspection of the bytecode reveals deliberate manipulation of internal headers, requiring analysts to restore missing metadata, such as the Python magic number, before the file can be processed by standard decompilation tools.

#3 Once the bytecode is repaired, the focus shifts to decompilation. Tools like Pycdc are used to translate the Python 3.11 bytecode back into readable source code, allowing deeper inspection of the malware's logic and functionality. This step is crucial for understanding function behavior, parameters, and control flow, often aided by Python's Abstract Syntax Tree (AST). At this stage, analysts can begin to trace how the malware orchestrates data theft and communicates with its command-and-control infrastructure.

#4 A significant hurdle in the analysis is Pyarmor, a commercial code-protection framework used here to heavily obfuscate the malware. Pyarmor employs AES-128 encryption in Counter (CTR) mode and introduces additional complexity through features such as BCC (ByteCode-to-Compilation) mode, which converts Python functions into native C code compiled into ELF binaries. The obfuscated bytecode is marked with special flags and wrapped between distinct entry and exit markers, signaling encrypted regions. By identifying these markers, reconstructing AES keys tied to the Pyarmor license, and disabling specific runtime protections, analysts can gradually peel back the encryption layers to recover meaningful logic and embedded strings.

#5 With the obfuscation removed, the full scope of VVS Stealer becomes clear. The malware aggressively targets Discord by scanning LevelDB files for encrypted tokens, decrypting them using Windows' DPAPI and AES-GCM, and querying Discord's APIs to collect extensive user data, including account details, payment information, and system identifiers. It further injects malicious JavaScript into the Discord application to maintain persistence and monitor sensitive user actions, while also harvesting data from browsers like Chrome, Firefox, and Brave. All stolen information is compressed and exfiltrated via webhooks, ensuring continuous data leakage. Ultimately, VVS Stealer demonstrates how legitimate protection tools like Pyarmor can be repurposed to conceal sophisticated credential-stealing operations, underscoring the need for vigilant monitoring and stronger defenses against account compromise and malware abuse.

Recommendations

Be Cautious With Unknown Files And Links: Avoid opening files or shortcuts received through Discord or other messaging platforms, especially if they appear as PDFs or error-related files. These are commonly used to trick users into running hidden malware.

Protect Your Discord Account with Strong Security Settings: Enable multi-factor authentication (MFA) on Discord and regularly review active sessions and connected devices. This makes it much harder for attackers to hijack your account even if a token is exposed.

Limit Stored Browser Data: Avoid saving passwords and sensitive information in browsers where possible. Clearing cookies and stored data periodically can reduce the amount of information available to data-stealing malware.

Watch for Unusual Discord Behavior: Unexpected logouts, strange messages sent from your account, or sudden password reset prompts may indicate compromise. If observed, change your credentials immediately and revoke all active sessions.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**TA0010** Exfiltration
T1204 User Execution	**T1204.002** Malicious File	**T1059** Command and Scripting Interpreter	**T1059.006** Python
T1059.007 JavaScript	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1027** Obfuscated Files or Information

T1140 Deobfuscate/Decode Files or Information	**T1036** Masquerading	**T1555** Credentials from Password Stores	**T1555.003** Credentials from Web Browsers
T1528 Steal Application Access Token	**T1552** Unsecured Credentials	**T1552.001** Credentials In Files	**T1082** System Information Discovery
T1113 Screen Capture	**T1005** Data from Local System	**T1071** Application Layer Protocol	**T1071.001** Web Protocols
T1102 Web Service	**T1041** Exfiltration Over C2 Channel	**T1560** Archive Collected Data	**T1560.001** Archive via Utility
T1027.002 Software Packing			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	307d9cefa7a3147eb78c69eded273e47c08df44c2004f839548963268d19dd87, 7a1554383345f31f3482ba3729c1126af7c1d9376abb07ad3ee189660c166a2b, c7e6591e5e021daa30f949a6f6e0699ef2935d2d7c06ea006e3b201c52666e07
URLs	hxxps[://]ptb.discord[.]com/api/webhooks/1360401843963826236/TkFvXfHFXrBIKT3EaqekJefvdvt39XTAxeOIWECeSrBbNLKDR5yPcn75uIqKEzdfs9o2, hxxps[://]ptb.discord[.]com/api/webhooks/1360259628440621087/YCo9eVnIBOYSMn8Xr6zX5C7AJF22z26WljaJk4zr6IiThnUrVyfWCZYs6JjSC12IC8c0

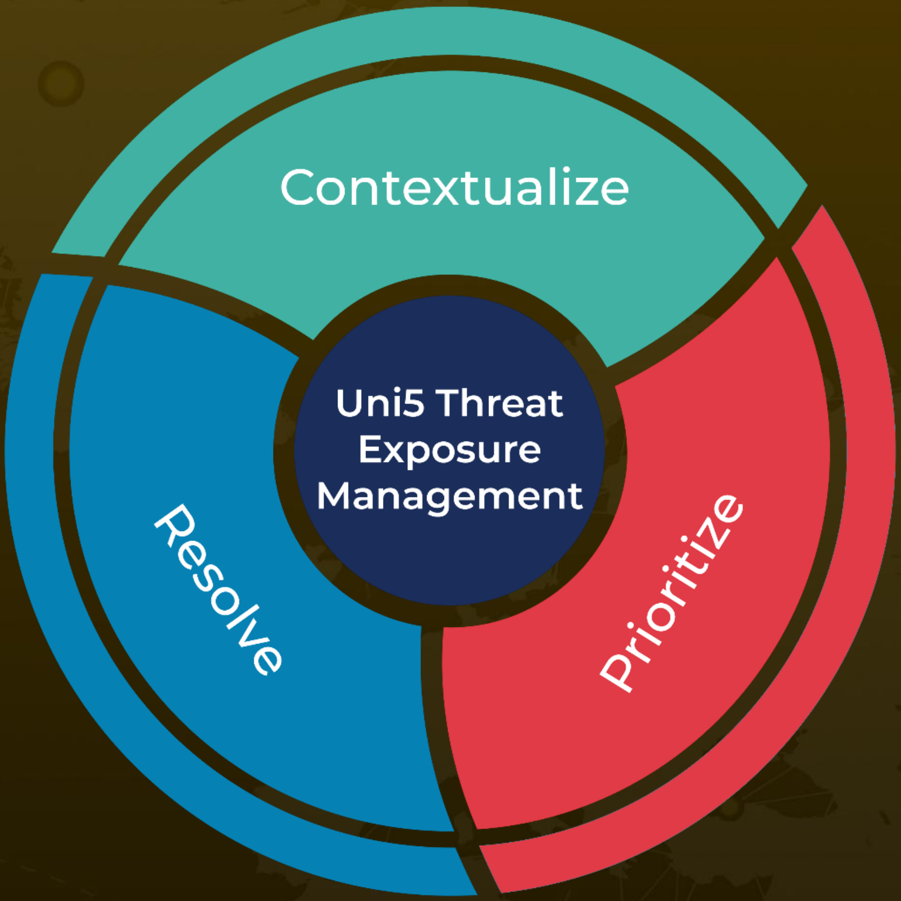
References

https://unit42.paloaltonetworks.com/vvs-stealer/

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

January 6, 2026 • 9:00 AM

More at www.hivepro.com