Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

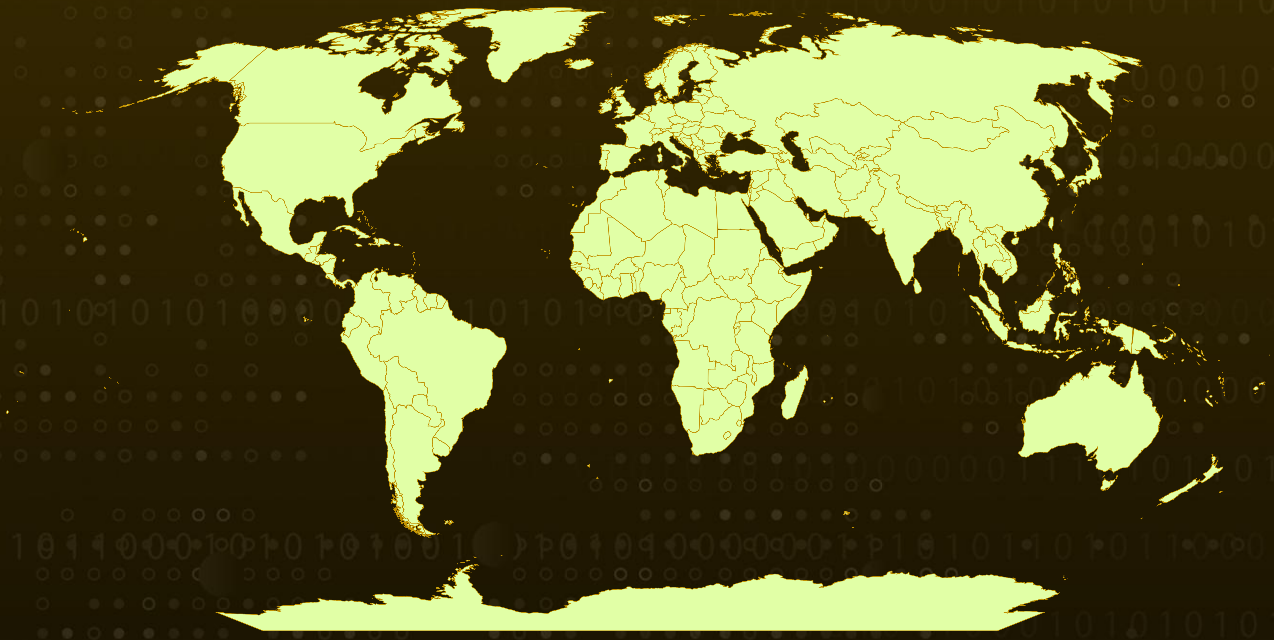
Vidar Stealer 2.0 Distributed via Fake Game Cheats on GitHub and Reddit

Date of Publication	Admiralty Code	TA Number
March 19, 2026	A1	TA2026077

Summary

First Seen: October 2025
Targeted Regions: Global
Targeted Platform: Windows
Targeted Industry: Gaming
Malware: Vidar Stealer 2.0
Attack: Threat actors are distributing Vidar Stealer 2.0 through hundreds of fake game cheat repositories hosted on GitHub and promoted via Reddit posts. The malware masquerades as free cheating software for popular online games such as Counter-Strike 2, Fortnite, Valorant, and Call of Duty. Victims are lured into downloading and executing PowerShell-based loaders compiled into .NET binaries, which then deploy the Themida-packed Vidar 2.0 infostealer. The malware exfiltrates browser credentials, cookies, autofill data, Azure tokens, cryptocurrency wallets, FTP/SSH credentials, Telegram and Discord session data, and local files to attacker-controlled C2 infrastructure concealed behind Telegram bots and Steam profiles used as dead drop resolvers.

Attack Regions



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

■ Targeted ■ Non-Targeted

Attack Details

#1

What starts as a tempting shortcut for gamers quickly turns into a full-scale compromise. Threat actors are actively targeting players hunting for free cheat tools, seeding malicious links across Reddit threads and Discord servers dedicated to titles like Counter-Strike 2, Fortnite, Valorant, and Call of Duty. These posts promise high-performance cheats but quietly redirect users to fake GitHub repositories or polished GitHub Pages that convincingly mimic legitimate software hubs. By abusing the trust associated with well-known platforms, the attacker lowers suspicion and makes the malicious downloads appear credible.

#2

Once on these pages, victims are guided through a seemingly professional installation process designed to feel familiar. The instructions deliberately ask users to disable antivirus protections, extract password-protected archives, and run executables with administrative privileges. Because cheat tools often require deep system access, these steps don't immediately raise red flags. The payloads themselves are cleverly disguised, packed in nested or encrypted archives, and labeled with gaming-themed names, helping them slip past automated detection and casual scrutiny.

#3

Behind the scenes, the execution chain is far more sophisticated. The initial payload is typically a PowerShell-based loader compiled into a .NET binary using PS2EXE, allowing it to blend in as a standard executable. Once launched, it weakens system defenses by adding exclusions in Windows Defender, then reaches out to attacker-controlled infrastructure, often via Pastebin, to fetch secondary payloads hosted on GitHub. The loader establishes a hidden foothold in the %AppData% directory, drops additional components, and ensures persistence through scheduled tasks that trigger at user logon. In some variants, heavily obfuscated scripts and multi-stage extraction chains are used to reconstruct the final malware in memory, making detection even harder.

#4

The final payload is a Themida-packed Vidar Stealer 2.0 binary representing a complete rewrite from C++ to C, a heavily obfuscated and continuously evolving information stealer. It employs polymorphic builds, anti-debugging checks, and virtual machine detection to evade analysis. Its command-and-control infrastructure is deliberately concealed, leveraging Telegram bots and even Steam profiles as indirect channels to resolve real server addresses. Once active, the malware systematically harvests sensitive data, from browser credentials and cookies to cryptocurrency wallets, messaging app sessions, and gaming platform logins, along with files and screenshots from the infected system.

#5

All collected data is staged locally before being exfiltrated to remote servers, completing a highly efficient data theft cycle. What makes this campaign particularly effective is its alignment with user behavior, exploiting both the demand for cheats and the normalization of risky actions within that ecosystem. In essence, the attackers aren't just delivering malware; they're embedding it seamlessly into a workflow that victims already trust.

Recommendations

Deploy Behavioral Endpoint Detection: Implement modern endpoint protection or EDR solutions capable of behavioral and signature-based scanning to detect suspicious process chains, credential access patterns, and data exfiltration behavior characteristic of infostealer infections.

Restrict Execution from Non-Standard Paths: Configure application control policies to block execution of binaries from directories not typically used by legitimate software, including %AppData%, %ProgramData%, and %Temp% subdirectories with randomly generated names.

Monitor Scheduled Task Creation: Implement detection rules for the creation of scheduled tasks with suspicious names such as "SystemBackgroundUpdate" or tasks configured to run at logon with elevated privileges from non-standard executable paths.

Audit Windows Defender Exclusion Modifications: Monitor for unauthorized additions to Windows Defender exclusion paths, particularly those targeting newly created directories in %AppData% or other user-writable locations, as the Vidar loader disables scanning for its payload drop zone.

Enforce Software Download Policies: Educate users on the risks of downloading tools from unofficial sources, particularly game cheats, cracks, and key generators. Enforce policies requiring software to be obtained only from verified vendors or trusted repositories.

Implement Browser Credential Protection: Deploy browser security solutions or enterprise browser configurations that mitigate credential theft via Local State file decryption and browser debug port abuse. Consider disabling remote debugging flags in managed Chromium-based browser deployments.

Monitor for Pastebin and GitHub Payload Staging: Implement network monitoring rules to detect suspicious connections to Pastebin URLs followed by downloads from GitHub repositories, which is the staging pattern used by the Vidar loader to retrieve its secondary payload.

Rotate Credentials After Suspected Compromise: If Vidar infection is suspected, immediately rotate all browser-saved passwords, Azure CLI tokens, FTP/SSH credentials, Telegram and Discord sessions, cryptocurrency wallet keys, and any other credentials that may have been stored on the affected system.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.003: Spearphishing via Service
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.005: Visual Basic
		T1059.003: Windows Command Shell
	T1204: User Execution	T1204.002: Malicious File
Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1574: Hijack Execution Flow	T1574.001: DLL
Privilege Escalation	T1548: Abuse Elevation Control Mechanism	
Defense Evasion	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1027: Obfuscated Files or Information	T1027.002: Software Packing
		T1027.013: Encrypted/Encoded File
	T1497: Virtualization/Sandbox Evasion	
	T1622: Debugger Evasion	
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
	T1070: Indicator Removal	T1070.006: Timestomp

Tactic	Technique	Sub-technique
Defense Evasion	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1102: Web Service	
	T1055: Process Injection	T1055.001: Dynamic-link Library Injection
Credential Access	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
	T1552: Unsecured Credentials	T1552.001: Credentials In Files
	T1539: Steal Web Session Cookie	
Collection	T1005: Data from Local System	
	T1113: Screen Capture	
	T1119: Automated Collection	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1105: Ingress Tool Transfer	
Exfiltration	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	2f416aac027f19f563cc45e3b4b72e992aaafb63da27f968b9a76a391134dc7d, b1cebd305c6aa27048a3673e70f8e1604735b2c06c83452d2935c330b5a3eb58, b6192c05029c8905fcbb88469d712dfdeaf1feb33b0690f8539373f19b6cbf85, fa7eafa65996c325faf2d77cc2d80179daa9228b3c138d2d3365280c79e30820, cbf2218ce316134795c75691f17dfaf02071ff5c369049fbf11ed072cf2103ab, c5e7fab18baee4a6b092e566414f4d2df1afbde35a1d12f518113054f144853f, 4a090e26e285661730dfd0911856c830bd0a44e639237178476ccb4993d7974f, e1979c42cb9e72ba9f9fcae7364887df1edcad38128feefdc3adbc768c51da05, d1721c9adcfa3d16bb4907afccfae64517e6c58a7c6ef058c9f5f543f60240c9, d1258b4c2b9849833651d1e844d1a99a5bc7febbb751548f960e92525afe6c26, bfee57d9e1b68c5c5aa63792b4e67b94f3361749e186531bd01609d9382672f3, 496d15810c25136955dd9aed6d018519380ee431f28c1bca715da59fe1385d12
URLs	hxxps[:]//telegram[.]me/bul33bt, hxxps[:]//telegram[.]me/cego54, hxxps[:]//telegram[.]me/ahnadar, hxxps[:]//steamcommunity[.]com/profiles/76561198765046918, hxxps[:]//steamcommunity[.]com/profiles/76561198761022496, hxxps[:]//steamcommunity[.]com/profiles/76561198780411257

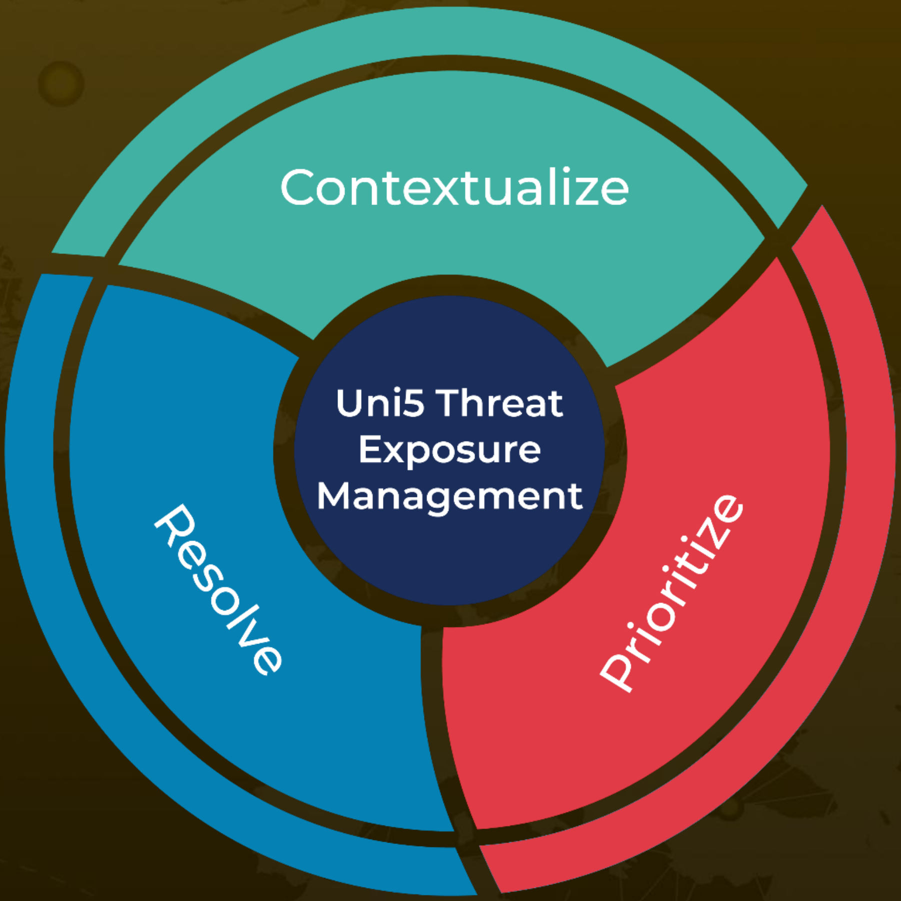
References

https://www.acronis.com/en/tru/posts/vidar-stealer-20-distributed-via-fake-game-cheats-on-github-and-reddit/

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 19, 2026 • 8:30 AM

More at www.hivepro.com