Hive Pro

Threat Level

Amber

Hiveforce Labs

# THREAT ADVISORY

## ATTACK REPORT

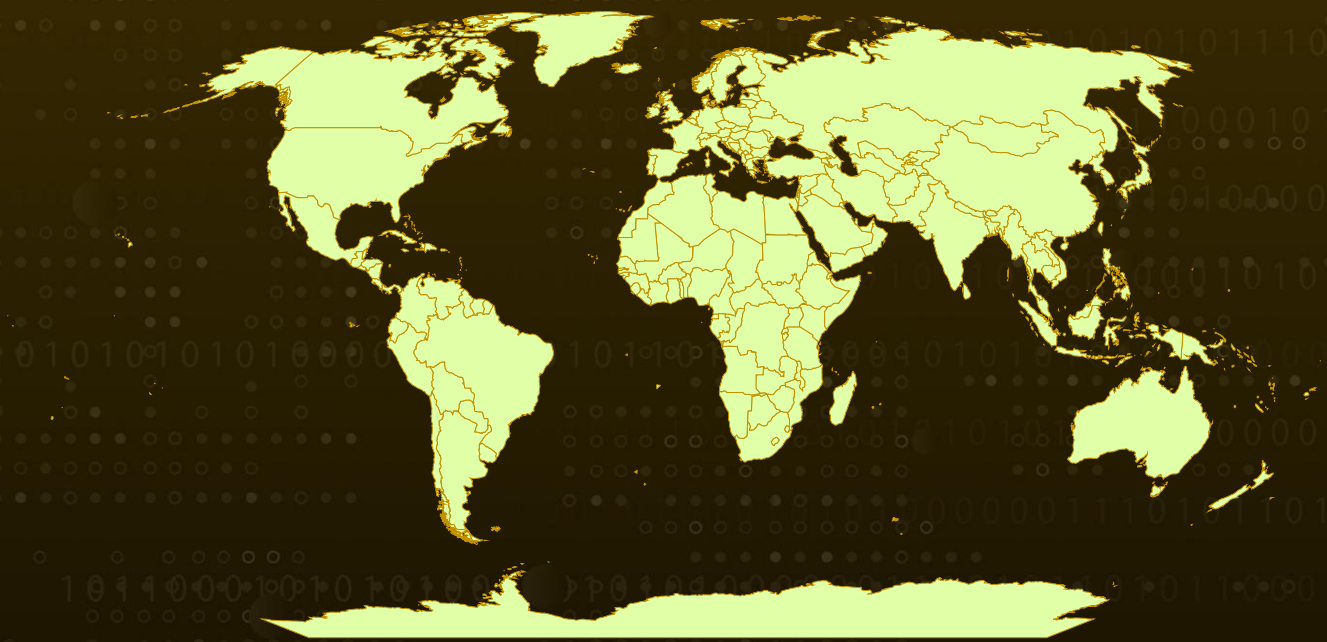
# StealC V2: A Sharpened Blade in the Info-Stealing Arsenal


| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| May 5, 2025 | A1 | TA2025135 |

# Summary

**Attack Discovered:** March 2025
**Targeted Countries:** Worldwide
**Malware:** StealC V2
**Attack:** The notorious StealC malware has leveled up with its March 2025 update, adding powerful features like RC4 encryption, multi-format payload delivery, and advanced evasion tactics. With improved C2 communication, credential brute-forcing, and stealthy data theft mechanisms, StealC V2 poses a serious and growing threat making vigilance and timely patching more critical than ever.

## Attack Regions



# Attack Details

**#1** The **StealC** malware, notorious for its information-stealing and payload delivery abilities, has entered a more dangerous phase with the release of StealC V2 in March 2025. This updated version introduces significant improvements including a revamped command-and-control (C2) protocol, stronger RC4 encryption, expanded payload support (EXE, MSI, and PowerShell), and a redesigned control panel. New features like multi-monitor screenshot capture and server-side brute-forcing for credential theft reveal a clear focus on stealth, efficiency, and adaptability in real-world intrusions.

**#2** StealC V2 continues to employ strong obfuscation techniques such as Themida packing and multi-layered string encryption using RC4, while taking steps to avoid detection like checking system languages and blocking execution in duplicate instances. The malware dynamically gathers configuration details, including C2 endpoints and API functions, and does so with a lightweight footprint by excluding unnecessary third-party components.

**#3** What makes StealC V2 especially dangerous is its high level of operational control. Attackers could define payload execution rules based on stolen data markers for example, if credentials related to Coinbase are found and can communicate via encrypted JSON messages that are uniquely randomized for each victim. The C2 infrastructure incorporates advanced features like fake 404 pages to evade detection, IP and hardware-based access controls, and Telegram bot integration for streamlined management.

**#4** Each new version is distributed as a modular ZIP package, including a version file, a builder executable, and optional patch components making upgrades seamless. From version 2.0.1's encrypted communications using winhttp.dll to the current 2.1.3 release with conditional self-deletion capabilities, StealC V2 showcases a steady trajectory of technical refinement and operational maturity.

**#5** StealC V2 is not just a rehash of an old threat it's a significant evolution that signals the malware is here to stay. With its enhanced encryption, automation, and targeting capabilities, it poses a serious and growing risk to both individuals and enterprises. The active development and operational sophistication behind StealC demand heightened vigilance, proactive defense strategies, and continuous monitoring.

# Recommendations

**Keep Your Devices Updated:** Make sure all your computers, apps, and systems are running the latest updates. Cybercriminals behind threats like StealC often exploit known flaws, so staying patched is one of the simplest and most effective ways to block their attacks.

**Control What Runs on Your Systems:** Use application whitelisting to block any unauthorized programs from executing especially PowerShell scripts, MSI files, and unfamiliar EXE files, which StealC V2 often uses to drop malicious payloads. This adds a strong layer of defense against infection.

**Watch for Suspicious Login Activity:** Regularly audit your systems for signs of credential theft look out for unusual login attempts, brute-force activity, or other anomalies that could indicate StealC V2 is trying to steal or abuse account credentials. Prompt detection can stop further damage.

**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<br>Execution | TA0005<br>Defense Evasion | TA0006<br>Credential Access | TA0007<br>Discovery |
| TA0009<br>Collection | TA0010<br>Exfiltration | TA0011<br>Command and Control | T1113<br>Screen Capture |
| T1132<br>Data Encoding | T1132.001<br>Standard Encoding | T1056<br>Input Capture | T1056.001<br>Keylogging |
| T1573<br>Encrypted Channel | T1573.001<br>Symmetric Cryptography | T1082<br>System Information Discovery | T1539<br>Steal Web Session Cookie |

| | | | |
|---|---|---|---|
| **T1005** Data from Local System | **T1140** Deobfuscate/Decode Files or Information | **T1027** Obfuscated Files or Information | **T1083** File and Directory Discovery |
| **T1057** Process Discovery | **T1059** Command and Scripting Interpreter | **T1059.001** PowerShell | **T1071** Application Layer Protocol |
| **T1071.001** Web Protocols | **T1518** Software Discovery | **T1110** Brute Force | **T1614** System Location Discovery |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| SHA256 | 0b921636568ee3e1f8ce71ff9c931da5675089ba796b65a6b212440425d63c8c, e205646761f59f23d5c8a8483f8a03a313d3b435b302d3a37061840b5cc084c3, a1b2aecdd1b37e0c7836f5c254398250363ea74013700d9a812c98269752f385, 27c77167584ce803317eab2eb5db5963e9dfa86450237195f5723185361510dc, 27c77167584ce803317eab2eb5db5963e9dfa86450237195f5723185361510dc, dd36c7d50cb05761391a7f65932193ec847d34f8ba1bb2f2a43ecf4985d911f4, 87618787e1032bbf6a6ca8b3388ea3803be20a49e4afaba1df38a6116085062f |
| URLs | hxxp[:]//45[.]93[.]20[.]64/c090b39aa5004512[.]php, hxxp[:]//45[.]93[.]20[.]28/3d15e67552d448ff[.]php, hxxp[:]//88[.]214[.]48[.]93/ea2cb15d61cc476f[.]php |

## References

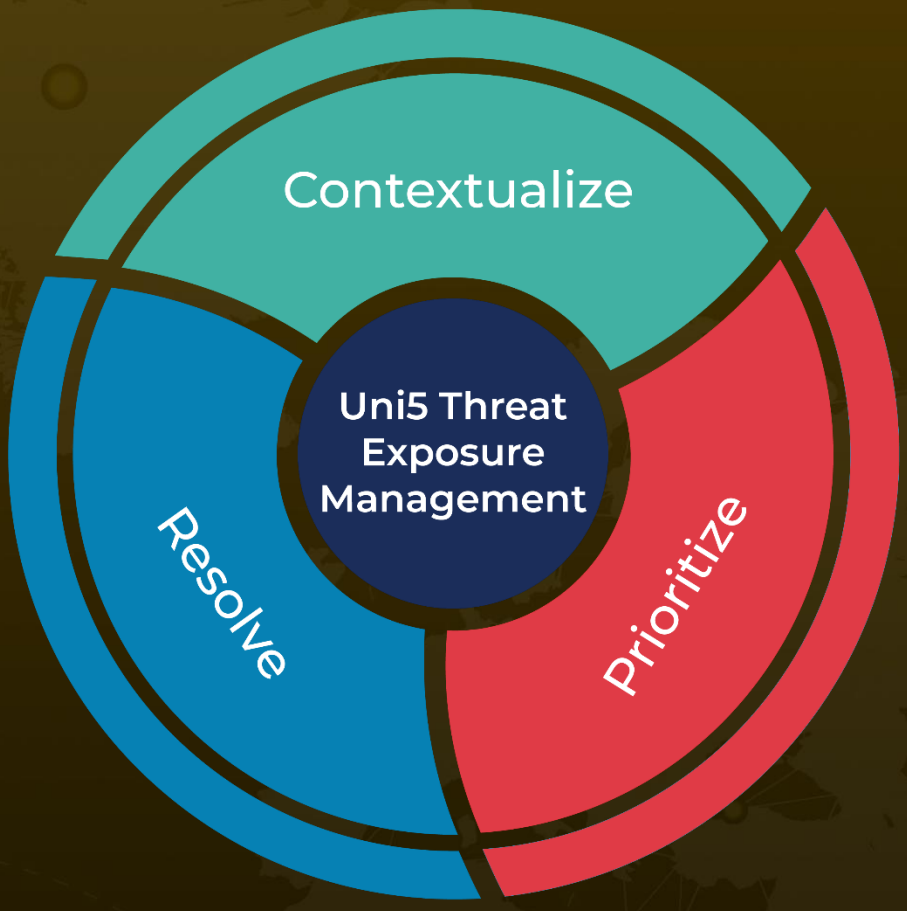

https://www.zscaler.com/blogs/security-research/i-stealc-you-tracking-rapid-changes-stealc

https://hivepro.com/threat-advisory/a-new-info-stealing-malware-named-stealc-targeting-cryptocurrency-wallets/

# 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

**May 5, 2025 • 5:30 AM**



More at www.hivepro.com