Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

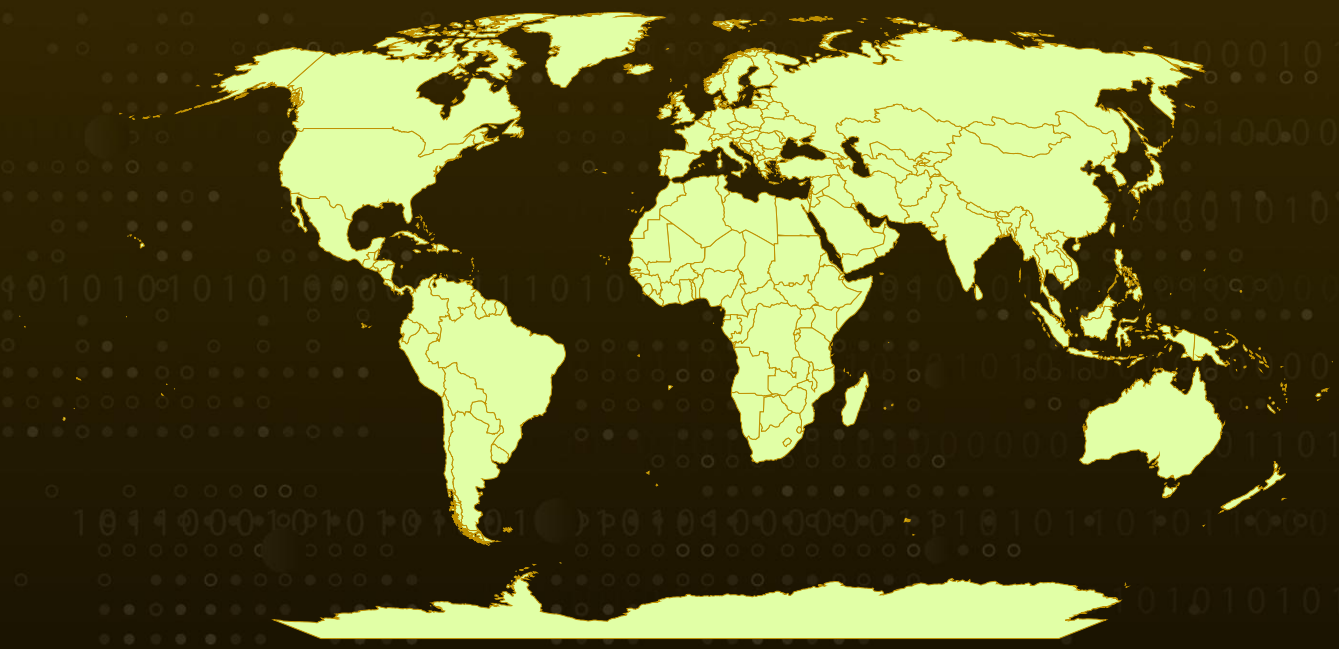
Myth Stealer Strikes Through Game Lures

Date of Publication	Admiralty Code	TA Number
June 11, 2025	A1	TA2025182

Summary

Attack Discovered: Late December 2024
Targeted Countries: Worldwide
Targeted Industry: Gaming
Affected Platform: Windows
Malware: Myth Stealer
Attack: Myth Stealer is a sneaky piece of malware dressed up as game cheats or cracked software, luring gamers into downloading it from fake websites. Once installed, it puts on a convincing show with a fake pop-up window while secretly stealing passwords, browser cookies, saved credit cards, and even screenshots sending everything back to the attacker. Built using Rust and packed with tricks to avoid antivirus tools, this malware keeps evolving with new features like clipboard hijacking to steal crypto. It's being sold on Telegram, complete with glowing reviews and subscription plans, showing just how organized and commercialized cybercrime has become.

Attack Regions



Attack Details

#1 Myth Stealer is a deceptive and evolving infostealer malware that spreads through fraudulent gaming websites, often posing as cheat tools or cracked software. Once installed, it creates a fake window to trick users into believing a legitimate program is running, while silently executing malicious code in the background. It primarily targets browsers built on Chromium and Gecko, such as Chrome and Firefox, aiming to steal sensitive information like saved passwords, cookies, credit card details, and autofill data.

#2 The malware has been built and marketed by an organized team, originally promoting it through a Telegram channel. Even after their initial channel was taken down, the group quickly resurfaced with a new one, continuing to advertise Myth Stealer's features and near-zero detection on VirusTotal. Subscriptions are sold on a weekly or monthly basis, and transactions are handled through cryptocurrency and platforms like Razer Gold. A separate Telegram group allows users to share testimonials and sell stolen data, such as compromised gaming accounts.

#3 Myth Stealer has grown increasingly sophisticated. It is distributed in various formats including password-protected RAR or ZIP files that hide the malicious executable. One campaign, for instance, distributed a file under the name "ddtrace krx ultimate Crack," complete with a VirusTotal link showing zero detections. The malware, written in Rust, is packaged as a 64-bit loader that decrypts and executes the stealer component in memory. It uses Rust libraries like native-windows-gui and memexec to create fake UI elements and run code stealthily. The stealer component itself is a DLL that employs string obfuscation techniques to hinder analysis and uses sandbox-detection logic to avoid running in virtual environments used by researchers.

#4 Once executed, Myth Stealer attempts to elevate privileges using Windows APIs and steals browser data by tapping into Chrome's debugging features. It also monitors clipboard activity, looking for cryptocurrency wallet addresses to hijack and replace with those of the attacker. Captured data is zipped and exfiltrated to attacker-controlled servers, often alongside a screenshot of the user's desktop. A persistence mechanism is established by copying the malware to the user's AppData folder and registering it to launch at startup.

#5 Myth Stealer's continued evolution with frequent updates, new evasion tactics, and added features like clipboard hijacking and screen capture demonstrates a clear focus on bypassing detection and expanding its reach. The use of Rust makes the malware both efficient and more challenging for traditional antivirus tools to detect. Proactive monitoring, rapid alert response, and continuous threat hunting are essential to minimize exposure and damage from fast-evolving malware like Myth Stealer.

Recommendations

- **Avoid downloading "cheats" or software from unknown websites:** Even if they look legit, these sites often hide malware behind fake game tools or cracks.
- **Stick to trusted platforms for software:** Only download games or related tools from verified sources like official stores or known developer sites.
- **Enable browser and OS protections:** Use features like browser sandboxing and keep your system up to date to reduce exposure to browser-based attacks.
- **Be cautious with what you share online:** Don't trust every forum or Telegram channel promising game hacks they're often scams hiding malware.
- **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

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery	**TA0009** Collection
TA0010 Exfiltration	**TA0011** Command and Control	**T1189** Drive-by Compromise	**T1059** Command and Scripting Interpreter
T1204 User Execution	**T1204.002** Malicious File	**T1113** Screen Capture	**T1115** Clipboard Data
T1140 Deobfuscate/Decode Files or Information	**T1027** Obfuscated Files or Information	**T1614** System Location Discovery	**T1106** Native API

T1574 Hijack Execution Flow	T1574.001 DLL	T1497 Virtualization/Sandbox Evasion	T1057 Process Discovery
T1539 Steal Web Session Cookie	T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers	T1555.004 Windows Credential Manager
T1560 Archive Collected Data	T1082 System Information Discovery	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder
T1547.009 Shortcut Modification	T1037 Boot or Logon Initialization Scripts	T1037.001 Logon Script (Windows)	T1036 Masquerading
T1552 Unsecured Credentials	T1552.001 Credentials In Files	T1068 Exploitation for Privilege Escalation	T1041 Exfiltration Over C2 Channel
T1056 Input Capture	T1056.001 Keylogging	T1056.004 Credential API Hooking	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1847288195fcfc03fc186bf4eead4268048ef5e082dedb963b3450ee07c23883, 65a84024daf30c12fd2e76db661bf6e85f3da30bb3aaa7e774152855d718b0c4, e5d09da6648add4776de8091b0182b935405791bf41476465b0e7dcb066fc0dc, f7cb6626e311181d9ded9536b1fbdf709b8254abd8d0810e04cebefea2fed131, acd66cb5f1447b803245c495400ad0886352920e35defcca6c45519fb7d33693, c7ae9d808e97fe6d6bf97aaf0775b9b6e68449f10bcc933bf07ba9d34d75a379, 6c54e6648a6a33583d7707a9f7c5e83dd08ed481df6354c52e8f81e729d74a82,

TYPE	VALUE
SHA256	7e2bed39eea850960a0d043e6e671154f413f5fe2cc7cafe6d92c903b3a2e8d1, b180f6f9f7eb0bb1a12a7e7c8216499366419b1083c84c4af5b0ee69b3016186, 0631a62a173833c7c821989e63f77632ecce30ca5a7049db4898ff0505abf32e, 565863cf176e5d094e75e31844eb542ca07c516673ed245a424d7326bd474e0b, 2e2cf06b6c7949b139356fb95c7ac0246c94f769d85dfa85122c004b9a2989e7, 858ec188573e8989c9be47263c8520fe8546a583dfd35e62241dc26f4ba90491, 55a418f8562684607ee0acd745595e297ab7e586d0a5d3f8328643b29c72dfa2, 100a36c2c6934b93f00dc7432bb1c6c4d849586d851fd6358d062435d1e3dae7, 4caa37c208ce1bb54791c0b13af2bd45bf90ea456098aaca37a0a9c53ebdccff, d147b9bde49b53e83b9c0b37d2001ccf7d195371672e782d58a12ef639efa95c
URLs	hxxps[:]//cheatglobal[.]com/konu/ddrace-krx-ultimate-crack[.]72186/page-1, hxxps[:]//gofile[.]io/d/tr1WIK, hxxp[:]//everlight-beta[.]netlify[.]app/, hxxps[:]//yomiragame[.]blogspot[.]com/2025/03/yomiragame[.]html, hxxps[:]//luraka-game[.]github[.]io/luraka/, hxxps[:]//www[.]plaquist-simulator[.]com/, hxxps[:]//185[.]224[.]3[.]219/screen, hxxps[:]//discord[.]com/api/webhooks/1324002441498202153/0KSAK6Fw00eryKz4BpysAJbo4jCxaJY3bRlcZGdmFhx03854FFdFvic1hQZDaZ2fmUIr, hxxp[:]//82[.]153[.]138[.]221[:]7340/post, hxxps[:]//185[.]224[.]3[.]219[:]8080/api/send
Domain	myth[.]cocukporno[.]lol

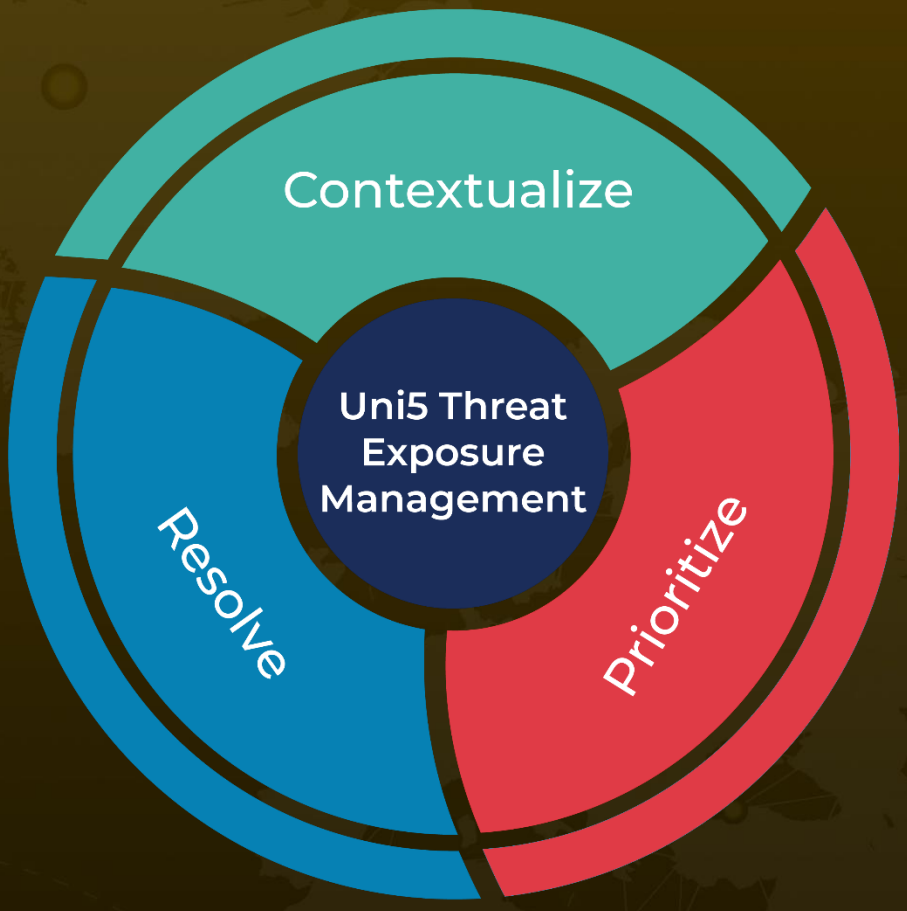
References

https://www.trellix.com/en-in/blogs/research/demystifying-myth-stealer-a-rust-based-infostealer/

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

June 11, 2025 • 5:30 AM

More at www.hivepro.com