Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Stealerium Changing the Rules of Cyber Espionage

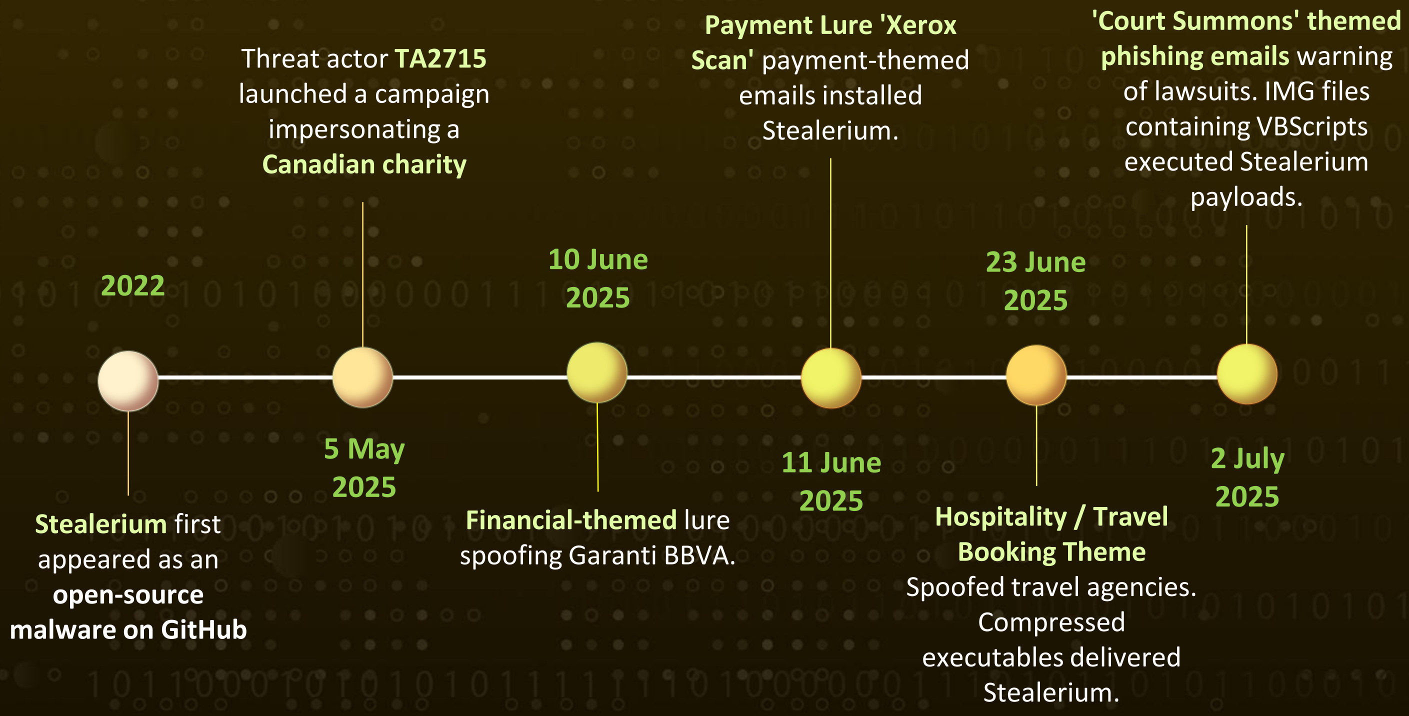
Date of Publication	Admiralty Code	TA Number
September 10, 2025	A1	TA2025275

Summary

First Seen: 2022
Malware: Stealerium, Warp Stealer, Phantom Stealer
Phantom Stealer Pricing Model: 70$ - 700$
Targeted Region: Worldwide
Targeted Industries: Non-Profit, Hospitality, Travel, Education, Finance, Legal, Banking

Attack: Stealerium, an open-source .NET-based information stealer first released in 2022, has quickly evolved into a versatile tool exploited by cybercriminals. Its recent resurgence in 2025 through fear-driven and financial-themed campaigns demonstrates how attackers manipulate emotions to spread malware. With advanced persistence techniques, extensive data theft capabilities, and multiple exfiltration channels, Stealerium's adaptability and accessibility make it a growing threat that's reshaping how malware is deployed and weaponized today.

Attack Timeline



2022

Stealerium first appeared as an **open-source malware on GitHub**

5 May 2025

Threat actor **TA2715** launched a campaign impersonating a **Canadian charity**

10 June 2025

Financial-themed lure spoofing Garanti BBVA.

11 June 2025

Payment Lure 'Xerox Scan' payment-themed emails installed Stealerium.

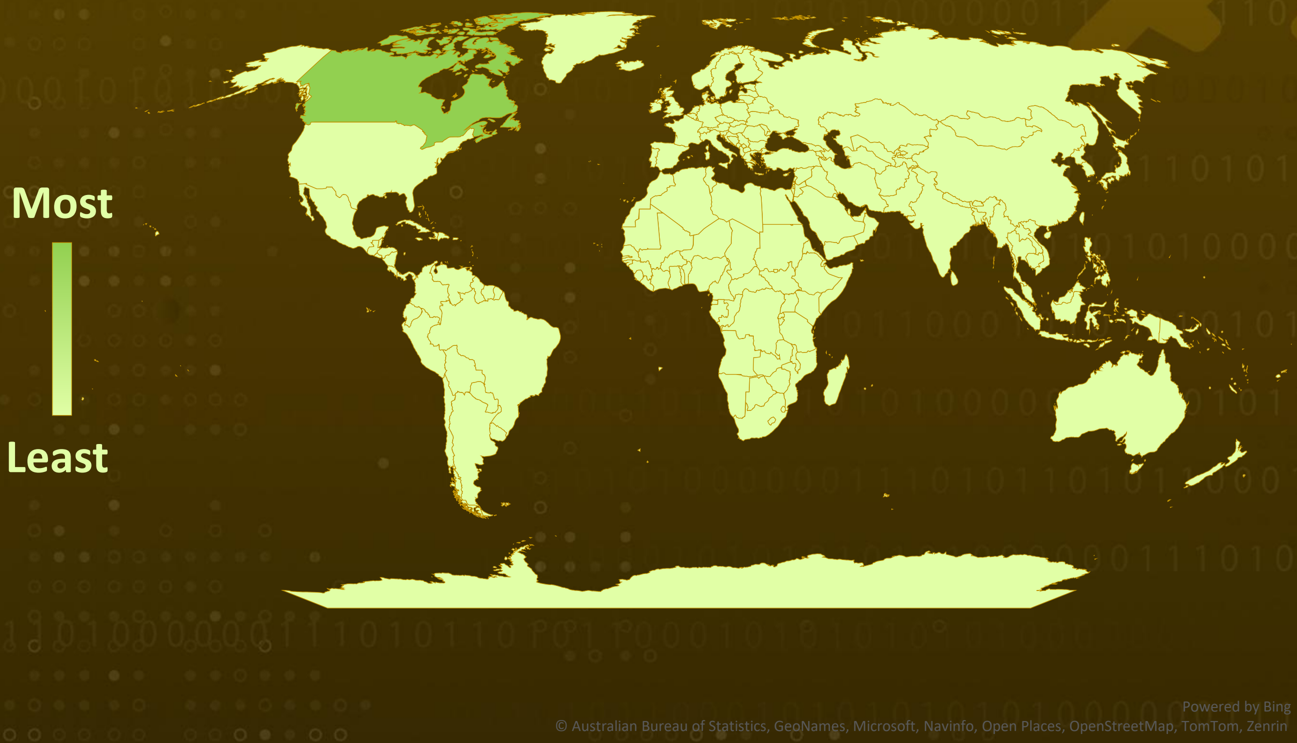
23 June 2025

Hospitality / Travel Booking Theme Spoofed travel agencies. Compressed executables delivered Stealerium.

2 July 2025

'Court Summons' themed phishing emails warning of lawsuits. IMG files containing VBScripts executed Stealerium payloads.

Attack Regions


Most
Least
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 Stealerium first appeared in 2022 as an open-source information stealer written in .NET and hosted on GitHub, explicitly labeled 'for educational purposes.' However, its accessible codebase has been exploited by malicious actors who adapt, modify, and propagate the malware for harmful purposes.

#2 The malware reemerged in May 2025 when the threat actor TA2715 launched a campaign impersonating a Canadian charity. The attack used 'request for quote' emails containing compressed executable files that, once opened, installed Stealerium.

#3 Later that month, another low-skilled actor, TA2536, also deployed Stealerium. This resurgence was significant, as both actors had previously relied on Snake Keylogger, indicating a shift in their malware strategy.

#4

Throughout June 2025, Stealerium was distributed through multiple campaigns targeting different sectors. Stealerium often uses social engineering that leverages fear-based tactics. Once activated, Stealerium executes a wide range of actions. It uses 'netsh wlan' commands to collect stored Wi-Fi profiles and nearby networks, potentially for geolocation or lateral movement.

#5

It also creates PowerShell exclusions and scheduled tasks to maintain persistence and may enable Chrome's remote debugging to bypass browser defenses and steal sensitive data such as cookies and credentials. Stealerium's data theft capabilities are extensive, harvesting browser credentials, banking details, cryptocurrency wallets, email and chat data, gaming tokens, VPN credentials, and confidential files. Notably, it can detect adult content in browser sessions and capture both screenshots and webcam footage, possibly for blackmail.

#6

For data exfiltration, Stealerium employs multiple channels, including SMTP email, Discord webhooks, and Telegram. Less frequently, it uses Gofile uploads and even Zulip chat integration. To evade detection, the malware incorporates anti-analysis techniques like random execution delays, blocklists of usernames, IP addresses, GPUs, and processes, and the ability to self-delete if checks fail.

#7

Stealerium shares considerable code overlap with other malware families such as Phantom Stealer and Warp Stealer. Phantom Stealer, marketed as an 'ethical hacking tool,' reuses much of Stealerium's code, while Warp Stealer integrates Stealerium components into its architecture.

Recommendations

Strengthen Email Security and Filtering: Implement advanced email filtering solutions to detect and block suspicious attachments, especially compressed files, VBScript, and JavaScript payloads commonly used in malware campaigns.

Monitor Network Traffic for Anomalies: Continuously monitor for unusual network commands such as 'netsh wlan' and suspicious access to Wi-Fi profiles or unexpected outbound connections to SMTP servers, Discord, Telegram, or obscure platforms.

Enforce Multi-Factor Authentication and Strong Passwords: Protect sensitive accounts, including browsers, email, and VPN services, by enforcing multi-factor authentication and requiring strong, regularly updated passwords.

Limit Remote Debugging and Unnecessary Features: Disable unnecessary browser features, such as Chrome's remote debugging, to prevent malware from exploiting them to steal cookies and credentials.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection
TA0011 Command and Control	TA0010 Exfiltration	TA0040 Impact	T1566 Phishing
T1566.001 Spearphishing Attachment	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1059.005 Visual Basic
T1059.007 JavaScript	T1204 User Execution	T1053 Scheduled Task/Job	T1562 Impair Defenses
T1562.001 Disable or Modify Tools	T1480 Execution Guardrails	T1070 Indicator Removal	T1555 Credentials from Password Stores

T1555.003 Credentials from Web Browsers	**T1046** Network Service Discovery	**T1056** Input Capture	**T1056.001** Keylogging
T1056.003 Web Portal Capture	**T1115** Clipboard Data	**T1606** Forge Web Credentials	**T1606.001** Web Cookies
T1114 Email Collection	**T1082** System Information Discovery	**T1087** Account Discovery	**T1534** Internal Spearphishing
T1021 Remote Services	**T1005** Data from Local System	**T1213** Data from Information Repositories	**T1113** Screen Capture
T1048 Exfiltration Over Alternative Protocol	**T1567** Exfiltration Over Web Service	**T1102** Web Service	**T1573** Encrypted Channel
T1565 Data Manipulation	**T1490** Inhibit System Recovery	**T1027** Obfuscated Files or Information	**T1497** Virtualization/Sandbox Evasion

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	d4a33be36cd0905651ce69586542ae9bb5763feddc9d1af98e90ff86a6914c0e, 41700c8fe273e088932cc57d15ee86c281fd8d2e771f4e4bf77b0e2c387b8b23, b640251f82684d3b454a29e962c0762a38d8ac91574ae4866fe2736f9ddd676e, a00fda931ab1a591a73d1a24c1b270aee0f31d6e415dfa9ae2d0f126326df4bb, e590552eea3ad225cfb6a33fd9a71f12f1861c8332a6f3a8e2050fffce93f45e, 50927b350c108e730dc4098bbda4d9d8e7c7833f43ab9704f819e631b1d981e3

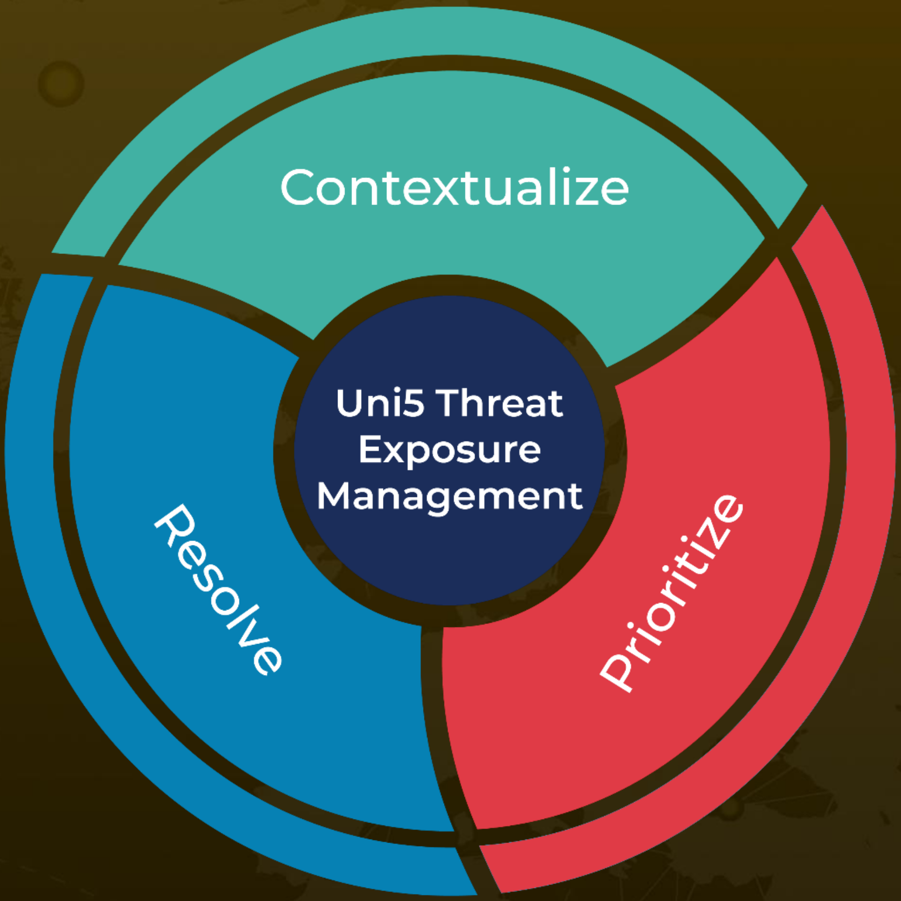
References

https://www.proofpoint.com/us/blog/threat-insight/not-safe-work-tracking-and-investigating-stealerium-and-phantom-infostealers

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

September 10, 2025 • 4:00 AM

More at www.hivepro.com