Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

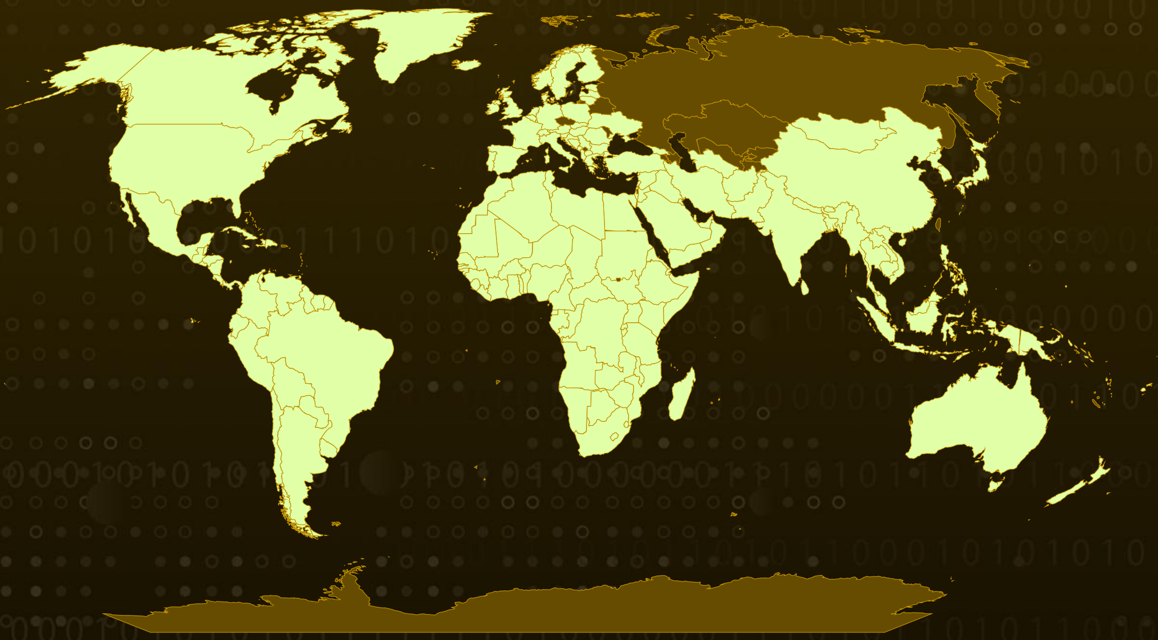
SantaStealer: An Emerging MaaS Infostealer Ahead of Its 2025 Debut

Date of Publication	Admiralty Code	TA Number
December 17, 2025	A1	TA2025380

Summary

Attack Discovered: Early December 2025
Targeted Region: Worldwide (CIS Exclusion)
Affected Platform: Windows
Malware: SantaStealer
Attack: SantaStealer is an emerging Malware-as-a-Service infostealer being actively advertised across Telegram and the Russian-speaking hacker forum, representing a rebranded evolution of the earlier BluelineStealer project. Built with a modular, multi-threaded design, the malware targets sensitive documents, credentials, cryptocurrency wallets, and data from applications such as Telegram, Discord, and Steam, while attempting to operate entirely in memory to evade traditional file-based detection. However, despite aggressive marketing claims of being "fully undetected," current samples analyzed remain largely unobfuscated, exposing symbol names and plaintext strings that make analysis and detection relatively easy. Offered under a subscription model ranging from $175 to $300 per month, SantaStealer clearly reflects commercial ambitions and a potential for broader adoption as it continues to mature.

Attack Regions



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

Attack Details

#1 SantaStealer is a newly emerging malware-as-a-service infostealer surface by late 2025. Previously promoted under the name BluelineStealer, it is being advertised across Telegram and underground forums with bold claims of advanced stealth and “fully undetected” operation. In practice, the malware focuses on stealing credentials, documents, and application data while running largely in memory to limit its on-disk presence. Collected data is sent to command-and-control servers over plain HTTP in compressed chunks, a surprisingly weak design choice that undercuts its marketing narrative.

#2 In December 2025, researchers identified a Windows sample closely resembling commodity infostealers from the Raccoon family. The 64-bit payload was delivered as a DLL with an unusually large export table containing more than 500 clearly named symbols tied to credential theft and anti-analysis logic. Alongside numerous unencrypted strings, this made reverse engineering straightforward and allowed analysts to quickly separate hype from reality.

#3 The decision to ship SantaStealer as a DLL ultimately worked against its developers. By exporting nearly every function and global variable, the malware exposed its internal architecture, configuration handling, and even statically linked third-party libraries such as cJSON, miniz, and sqlite3. Embedded branding, including a “SANTA STEALER” banner and a Telegram link, led directly to a web-based control panel advertising features and pricing. Despite claims of high-profile targeting, forum activity and infrastructure strongly point to Russian-speaking operators with weak operational security and prematurely leaked builds.

#4 Functionally, SantaStealer uses a modular, multi-threaded design. Its main routine performs basic environment checks, including CIS-related keyboard detection and simple anti-VM techniques. The core stealer targets browser credentials, cookies, and stored passwords, using an auxiliary in-memory component to bypass Chromium protections. This method closely mirrors the publicly available ChromElevator project, suggesting code reuse rather than original development. Additional modules collect screenshots and data from popular applications such as Telegram, Discord, and Steam before bundling everything into a single archive for exfiltration.

#5 Overall, SantaStealer is best described as an evolving but immature infostealer. While its fileless, in-memory approach aligns with current malware trends, its stealth and anti-analysis features remain basic, with detection aided by plaintext configurations and hard-coded C2 details. Despite being marketed as “production-ready,” it remains more notable for its ambition than its execution, making cautious user behavior and basic security hygiene an effective defense.

Recommendations

Stay Alert to Suspicious Messages: Be cautious of unexpected emails, links, or attachments, especially those that push urgency or ask you to run files or commands. Infostealers often rely on simple social tricks, and pausing to verify a message can prevent an infection before it starts.

Avoid Unofficial Software Sources: Cracked software, cheats, and unknown browser extensions are common hiding places for infostealers. Only install applications from trusted vendors and regularly remove tools or plugins you no longer recognize or need.

Lock Down Your Accounts: Use strong, unique passwords and enable multi-factor authentication wherever possible, especially for email and browser-linked accounts. These steps greatly reduce the damage even if credentials are stolen.

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

TA0042 Resource Development	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control
TA0040 Impact	T1087 Account Discovery	T1020 Automated Exfiltration	T1217 Browser Information Discovery
T1560 Archive Collected Data	T1030 Data Transfer Size Limits	T1560.002 Archive via Library	T1119 Automated Collection
T1041 Exfiltration Over C2 Channel	T1115 Clipboard Data	T1622 Debugger Evasion	T1087.003 Email Account

T1083 File and Directory Discovery	**T1552** Unsecured Credentials	**T1552.001** Credentials In Files	**T1555** Credentials from Password Stores
T1005 Data from Local System	**T1555.003** Credentials from Web Browsers	**T1657** Financial Theft	**T1587** Develop Capabilities
T1587.001 Malware	**T1057** Process Discovery	**T1114** Email Collection	**T1114.001** Local Email Collection
T1213 Data from Information Repositories	**T1213.005** Messaging Applications	**T1113** Screen Capture	**T1583** Acquire Infrastructure
T1583.004 Server	**T1518** Software Discovery	**T1497** Virtualization/Sandbox Evasion	**T1497.001** System Checks
T1574 Hijack Execution Flow	**T1574.001** DLL	**T1082** System Information Discovery	**T1614** System Location Discovery
T1614.001 System Language Discovery	**T1497.003** Time Based Checks	**T1140** Deobfuscate/Decode Files or Information	**T1071** Application Layer Protocol
T1071.001 Web Protocols	**T1552.004** Private Keys	**T1027** Obfuscated Files or Information	**T1027.007** Dynamic API Resolution
T1528 Steal Application Access Token	**T1539** Steal Web Session Cookie	**T1027.009** Embedded Payloads	**T1027.013** Encrypted/Encoded File
T1070 Indicator Removal	**T1070.004** File Deletion	**T1055** Process Injection	**T1055.002** Portable Executable Injection
T1055.012 Process Hollowing	**T1620** Reflective Code Loading		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1a277cba1676478bf3d47bec97edaa14f83f50bdd11e2a15d9e0936ed243fd64, abbb76a7000de1df7f95eef806356030b6a8576526e0e938e36f71b238580704, 5db376a328476e670aeefb93af8969206ca6ba8cf0877fd99319fa5d5db175ca, a8daf444c78f17b4a8e42896d6cb085e4faad12d1c1ae7d0e79757e6772bddb9, 5c51de7c7a1ec4126344c66c70b71434f6c6710ce1e6d160a668154d461275ac, 48540f12275f1ed277e768058907eb70cc88e3f98d055d9d73bf30aa15310ef3, 99fd0c8746d5cce65650328219783c6c6e68e212bf1af6ea5975f4a99d885e59, ad8777161d4794281c2cc652ecb805d3e6a9887798877c6aa4babfd0ecb631d2, 73e02706ba90357aeeb4fdcbdb3f1c616801ca1affed0a059728119bd11121a4, e04936b97ed30e4045d67917b331eb56a4b2111534648adcabc4475f98456727, 66fef499efea41ac31ea93265c04f3b87041a6ae3cd14cd502b02da8cc77cca8, 4edc178549442dae3ad95f1379b7433945e5499859fdbfd571820d7e5cf5033c, 926a6a4ba8402c3dd9c33ceff50ac957910775b2969505d36ee1a6db7a9e0c87, 9b017fb1446cdc76f040406803e639b97658b98760197012582696 0e94e9a1a6, F81f710f5968fea399551a1fb7a13fad48b005f3c9ba2ea419d14b597401838c
IPv4:Port	31[.]57[.]38[.]244[:]6767, 80[.]76[.]49[.]114[:]6767

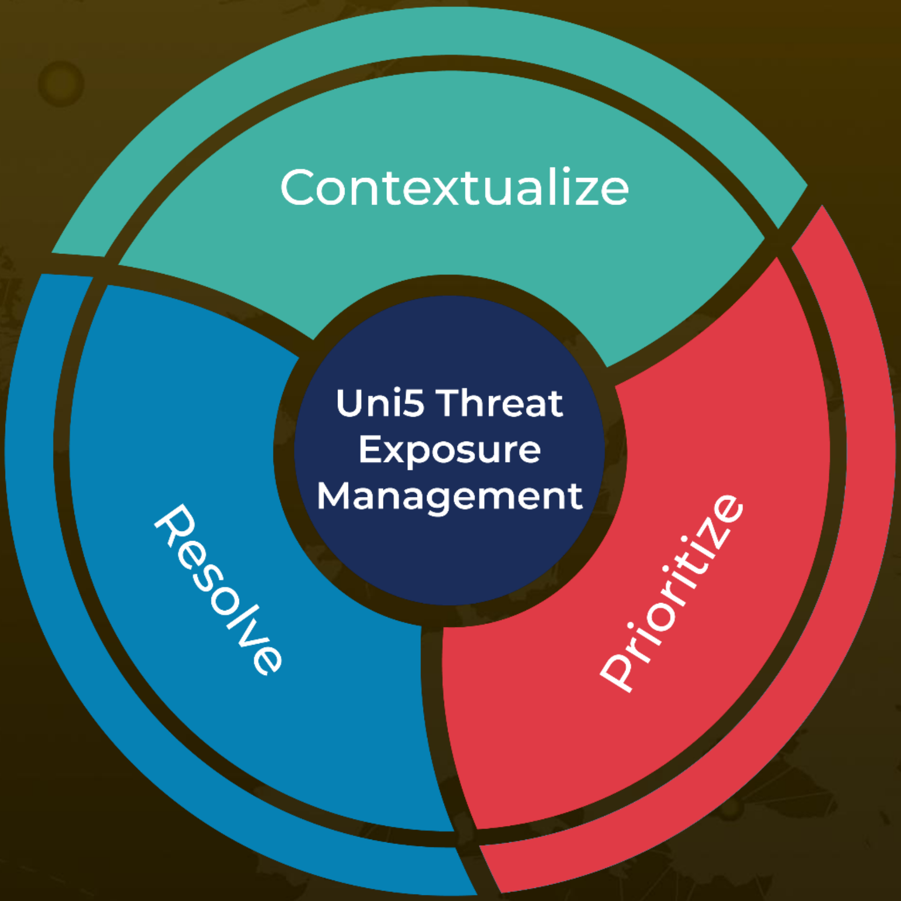
References

https://www.rapid7.com/blog/post/tr-santastealer-is-coming-to-town-a-new-ambitious-infostealer-advertised-on-underground-forums/

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

December 17, 2025 • 7:30 AM

More at www.hivepro.com