Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Hannibal Stealer: Rebranded, Resurrected, and Ruthless

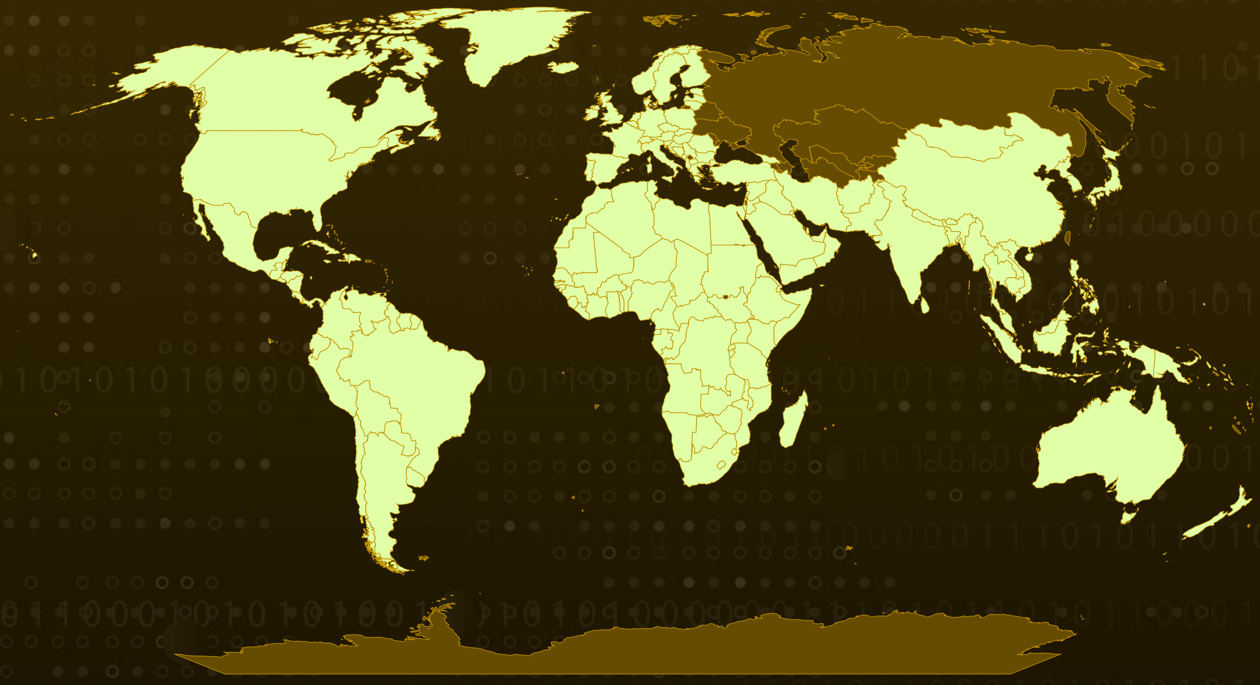
Date of Publication	Admiralty Code	TA Number
April 30, 2025	A1	TA2025132

Summary

First Seen: February 2, 2025
Malware: Hannibal Stealer
Subscription Pricing: $150 for 1 month, $300 for 3 months, and $650 for 7 months
Targeted Regions: Worldwide (excludes Russia, Belarus, Ukraine, Moldova, Kazakhstan, Kyrgyzstan, Uzbekistan, Armenia, Azerbaijan, Tajikistan, Turkmenistan)

Attack: Hannibal Stealer is a newly rebranded, highly capable piece of malware making waves in the cybercrime underworld. Evolving from its predecessors, Sharp and TX Stealer, it targets browsers, cryptocurrency wallets, and communication apps while slipping past modern security protections. Hannibal isn't just another stealer, it's a growing threat that blurs the line between financial cybercrime and hacktivist agendas, signaling a dangerous shift in the digital threat landscape.

Attack Regions



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

Attack Details

#1 The Hannibal Stealer is a sophisticated and malicious strain of malware, recently rebranded yet firmly rooted in the legacy of two earlier info stealers, Sharp and TX Stealer. Written in C# for the .NET Framework, it targets Chromium- and Gecko-based browsers, bypassing Chrome's Cookie V20 protection to extract sensitive data. It also steals credentials from cryptocurrency wallets, FTP clients, VPN configurations, and apps like Telegram and Discord.

#2 The stealer performs thorough system profiling, capturing OS details, hardware information, network settings, and clipboard contents, swapping crypto wallet addresses via clipboard hijacking. It selectively harvests credentials from high-value targets using a hardcoded domain list, optimizing efficiency and reducing detection risk.

#3 A Django-based command-and-control (C2) panel centralizes the management of infections, logs, credentials, and screenshots. The malware includes geofencing features to avoid operating in certain countries, mainly within the former Soviet bloc.

#4 Hannibal is sold on dark web forums like BreachForums and Darkforums, with subscription packages ranging from $150 to $650. A bulk installation service, launched in 2025, expanded its distribution, supported by several Telegram channels for marketing and customer support.

#5 Clear ties link Hannibal's developers to Sharp and TX Stealer through shared handles, forum posts, and promotional patterns. While its technical upgrades are modest, Hannibal remains dangerous due to its broad targeting scope, integrated C2 framework, and dual-use potential combining financial cybercrime with hacktivist activity, reflecting the modern threat landscape’s convergence of crime and ideology.

Recommendations

Implement Advanced Endpoint Protection: Deploy behavior-based EDR (Endpoint Detection and Response) solutions capable of detecting unusual clipboard activities, system profiling attempts, and unauthorized credential access.

Inspect Suspicious TLS Traffic: Use SSL/TLS inspection on outbound traffic to detect malicious C2 communications disguised over HTTPS, particularly those connecting to newly registered or obscure domains.

Develop Fast-Track Quarantine Workflows: Automate the isolation of infected or suspicious systems showing malware behaviors like unauthorized clipboard access, registry modifications, or C2 callbacks.

Audit Third-Party Software Use and Supply Chains: Regularly review third-party applications and services integrated into your environment to identify potential infection vectors or exploited vulnerabilities.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
TA0010 Exfiltration	**TA0040** Impact	**T1047** Windows Management Instrumentation	**T1106** Native API
T1129 Shared Modules	**T1055** Process Injection	**T1543** Create or Modify System Process	**T1547** Boot or Logon Autostart Execution
T1574 Hijack Execution Flow	**T1574.002** DLL Side-Loading	**T1027** Obfuscated Files or Information	**T1003** OS Credential Dumping
T1552 Unsecured Credentials	**T1552.001** Credentials In Files	**T1555** Credentials from Password Stores	**T1555.003** Credentials from Web Browsers
T1010 Application Window Discovery	**T1016** System Network Configuration Discovery	**T1018** Remote System Discovery	**T1033** System Owner/User Discovery

T1057 Process Discovery	**T1082** System Information Discovery	**T1083** File and Directory Discovery	**T1087** Account Discovery
T1518 Software Discovery	**T1518.001** Security Software Discovery	**T1614** System Location Discovery	**T1005** Data from Local System
T1113 Screen Capture	**T1115** Clipboard Data	**T1213** Data from Information Repositories	**T1071** Application Layer Protocol
T1102 Web Service	**T1105** Ingress Tool Transfer	**T1573** Encrypted Channel	**T1041** Exfiltration Over C2 Channel
T1485 Data Destruction	**T1496** Resource Hijacking		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	d18961f7777d329e17cfb824926d9e12
SHA256	f69330c83662ef3dd691f730cc05d9c4439666ef363531417901a86e7c4d31c8, 251d313029b900f1060b5aef7914cc258f937b7b4de9aa6c83b1d6c02b36863e
URLs	hxxp[:]//45[.]61[.]151[.]60/login/, hxxp[:]//45[.]61[.]141[.]160[:]8001/login/, www[.]hannibal[.]dev

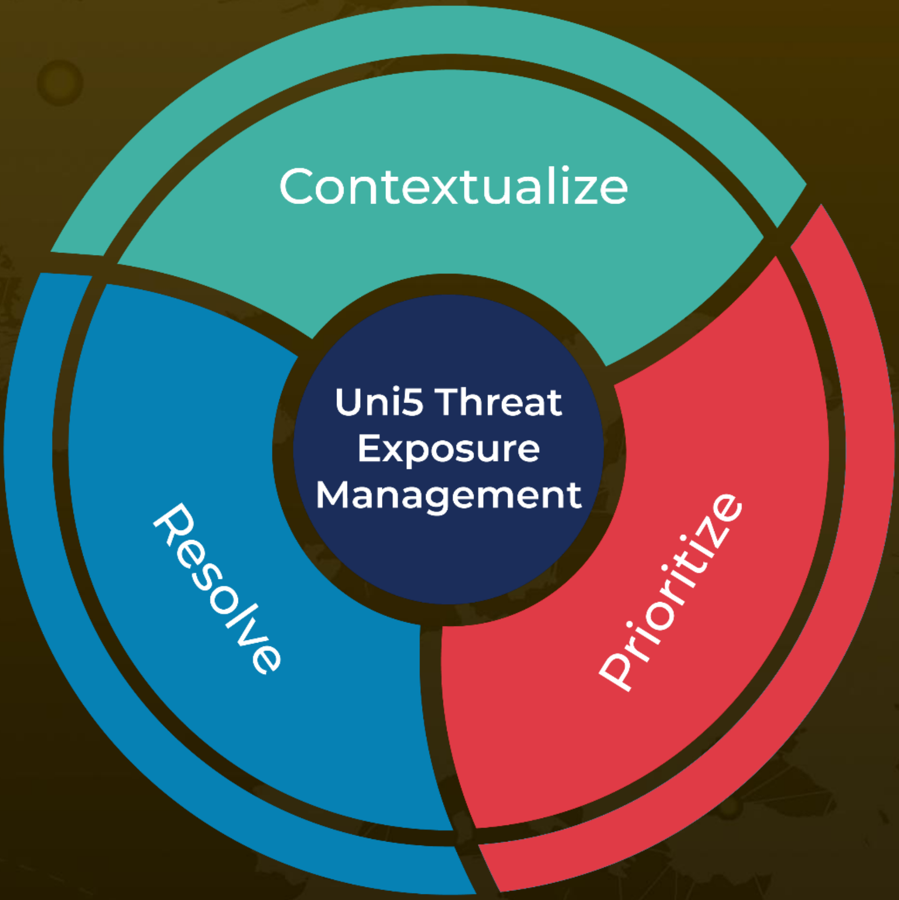
References

https://www.cyfirma.com/research/hannibal-stealer-a-rebranded-threat-born-from-sharp-and-tx-lineage/

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

April 30, 2025 • 4:30 AM

More at www.hivepro.com