Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Arkanix Stealer's Fast-Evolving Design Driving Widespread Compromise

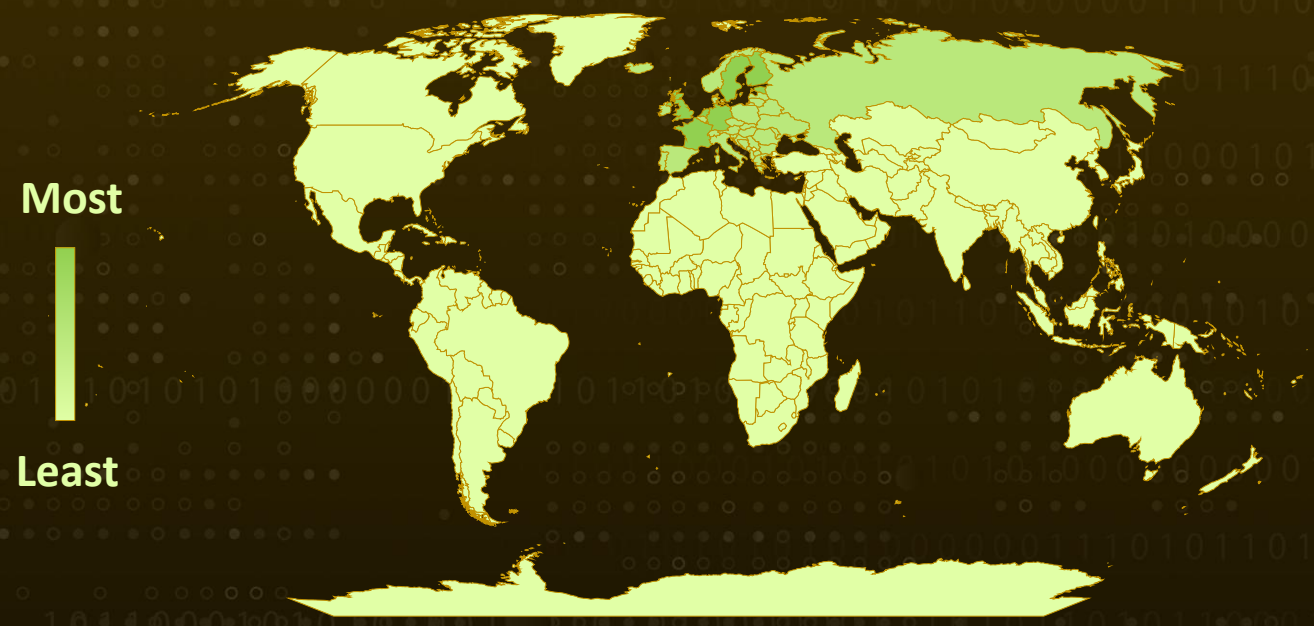
Date of Publication	Admiralty Code	TA Number
December 5, 2025	A1	TA2025369

Summary

First Seen: 2025
Malware: Arkanix Stealer
Targeted Regions: Worldwide

Attack: Arkanix Stealer is a rapidly advancing commodity infostealer circulated through Discord and underground forums, where it is disguised as legitimate software to drive user execution. The stealer targets a wide range of Chromium-based browsers and cryptocurrency extensions, while also harvesting wallet data from standalone clients such as Electrum and Ethereum applications.

Attack Regions



Attack Details

#1 Arkanix Stealer functions as a commodity infostealer designed for rapid monetization. It circulates through Discord channels and online forums, packaged as legitimate tools to prompt users into running it. The operators released an initial Python version, then replaced it within about a month with a more advanced C++ build.

#2 The Python variant relies on Nuitka to produce a standalone executable. Once launched, it unpacks its embedded Python environment, executes the malicious payload from memory, and pulls further code from the command-and-control server. This establishes the baseline workflow used across later versions.

#3 The C++ edition appears as the "Premium" option on the web panel. It expands the feature set with modules for stealing VPN accounts and Steam credentials. It also deploys a post-exploitation tool called "Chrome Elevator," which injects code into the Chrome process to bypass the App-Bound Encryption added in Chrome 127. This enables direct access to cookies and stored credentials by operating inside Chrome's authorized environment.

#4 The web panel manages customer accounts, coordinates configuration updates, and stores stolen data. Arkanix supports data extraction from a wide range of Chromium-based browsers, including Chrome, Edge, Opera, Vivaldi, Tor, and Yandex. It further targets browser extensions tied to cryptocurrency wallets such as MetaMask, Binance, and Exodus. The stealer also pulls wallet information from standalone applications, including Electrum and Ethereum clients.

Recommendations

Monitor Memory-Resident Payloads: Deploy tooling that detects runtime unpacking, interpreter spawning, and anomalous Chrome activity. Prioritize behavioral and memory-based analytics over file-dependent signatures.

Bind Access to Strong Authentication: Protect VPN profiles, Steam accounts, and other auxiliary credentials with MFA and device-bound tokens. Compromised data should yield minimal operational value for attackers.

Reinforce Recovery and Containment Architecture: Strengthen backup and disaster recovery processes to enable clean system restoration. Segment internal networks to constrain lateral movement pathways during compromise scenarios. Maintain incident response playbooks with security-evasion capabilities.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0010** Exfiltration
TA0011 Command and Control	**T1005** Data from Local System	**T1113** Screen Capture	**T1204.002** Malicious File
T1204 User Execution	**T1059** Command and Scripting Interpreter	**T1059.006** Python	**T1059.001** PowerShell
T1027 Obfuscated Files or Information	**T1027.002** Software Packing	**T1036** Masquerading	**T1036.005** Match Legitimate Resource Name or Location
T1055 Process Injection	**T1555** Credentials from Password Stores	**T1555.003** Credentials from Web Browsers	**T1552** Unsecured Credentials
T1552.001 Credentials In Files	**T1082** System Information Discovery	**T1033** System Owner/User Discovery	**T1016** System Network Configuration Discovery

T1057 Process Discovery	**T1083** File and Directory Discovery	**T1518** Software Discovery	**T1518.001** Security Software Discovery
T1119 Automated Collection	**T1074** Data Staged	**T1056** Input Capture	**T1056.001** Keylogging
T1071 Application Layer Protocol	**T1071.001** Web Protocols	**T1573** Encrypted Channel	**T1573.001** Symmetric Cryptography
T1041 Exfiltration Over C2 Channel	**T1102.002** Bidirectional Communication	**T1102** Web Service	**T1136** Create Account

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	arkanix[.]pw
URLs	hxxps[:]//arkanix[.]pw/stealer[.]py, hxxps[:]//arkanix[.]pw/delivery, hxxps[:]//arkanix[.]pw/api/upload/direct
SHA256	6ea644285d7d24e09689ef46a9e131483b6763bc14f336060afaeffe37e4beb5, 6960d27fea1f5b28565cd240977b531cc8a195188fc81fa24c924da4f59a1389

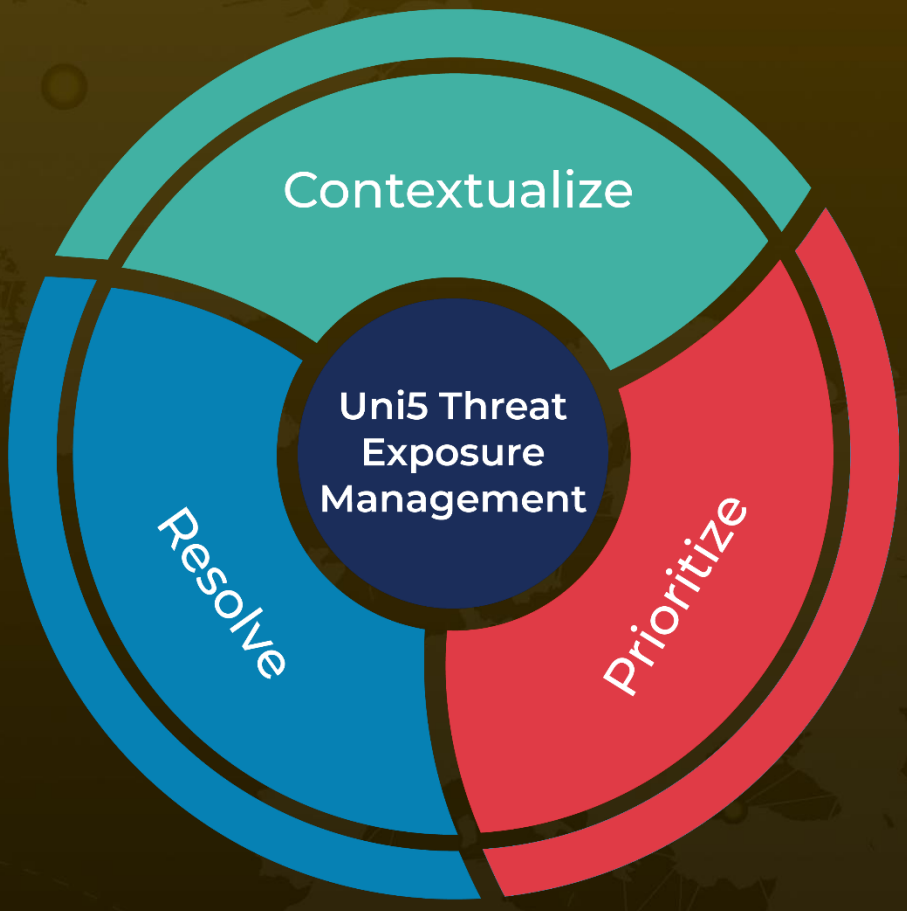
References

https://www.gdatasoftware.com/blog/2025/12/38306-arkanix-stealer

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 5, 2025 • 3:30 AM

More at www.hivepro.com