Arkanix Stealer Jumps from Discord to Browser Sessions and Corporate Logins

cybersecsentinel.com/arkanix-stealer-jumps-from-discord-to-browser-sessions-and-corporate-logins

Cybersec Sentinel December 2, 2025

Threat Group – Financially motivated cyber crime cluster operating within a malware as a service ecosystem and using Discord communities, gaming groups and social platforms for distribution
Threat Type – Cross platform information stealer family with native C plus plus and legacy Python variants that focus on credential, cookie and wallet theft
Exploited Vulnerabilities – Abuse of user trust through ClickFix themed social engineering, process injection into Chromium based browsers to bypass App Bound Encryption and theft of locally stored credentials and wireless keys, with no confirmed zero day vulnerabilities
Malware Used – Arkanix Stealer Python loader and C plus plus core stealer, Chrome Elevator post exploitation module and VMProtect wrapped binaries
Threat Score – 6.4 🟠 Elevated due to its advanced decryption bypass, rapid development cycles and ability to harvest corporate identities from consumer devices while still lacking persistence and requiring user execution
Last Threat Observation – 2 December 2025

Overview

The digital threat landscape of late 2025 has been characterised by the widespread adoption of sophisticated evasion techniques across low cost crimeware. Arkanix Stealer is a significant example of this shift. First discovered as a basic Python script circulating inside Discord servers, gaming communities and file sharing groups, it has rapidly evolved into a native C plus plus information stealer with advanced capabilities.

This transformation is not cosmetic. It reflects a move from amateur experimentation to professional malware engineering focussed on harvesting sensitive data at speed and scale. The operators have demonstrated a willingness to update the codebase in response to browser security improvements, detection signatures and affiliate feedback.

A major concern is the integration of the Chrome Elevator module. This post exploitation component bypasses Google Chrome App Bound Encryption. App Bound Encryption was introduced to prevent unauthorised decryption of cookies and passwords by restricting access to recognised browser identities. Chrome Elevator avoids this control through process injection. This restores the ability to harvest high value credential and session data from up to date browsers.

The threat actors target broad demographics including gamers, students, remote workers and users seeking game modifications or cracked tools. This indiscriminate distribution strategy creates a large pool of harvested identities and credentials, which often includes corporate accounts, virtual private network secrets and wireless authentication keys.

Verification of Threat Intelligence

Intelligence Component	Status	Analysis
Malware Family	Confirmed	Arkanix is a distinct stealer family with rapid evolution from Python to C plus plus.
Exploitation Technique	Validated	Chrome Elevator bypasses App Bound Encryption through process injection.
Distribution Vectors	Expanded	Discord, ClickFix themed deception and gaming tool impersonation are confirmed.
Targeting Scope	Refined	Strong focus on virtual private network clients and wireless profiles via netsh commands.
Infrastructure	Confirmed	Command activity anchored on arkanix[.]pw and related subdomains.

Risk Scoring and Justification

The 6.4 Elevated score reflects the significant impact Arkanix can achieve once executed. The threat arises not from its delivery method but from its capability after launch. By bypassing App Bound Encryption, Arkanix regains access that many older stealers have lost. The modular nature of the codebase and the rapid turnaround between updates adds to the risk.

If future versions add persistence, privilege escalation or lateral movement features, a reassessment may be required.

Threat Actor Profile and Operational Timeline

Attribution and Motive

Arkanix operators fit the profile of short term profit cyber criminals. They do not maintain persistent footholds or conduct espionage. They sell stolen logs, cryptocurrency credentials and corporate access on underground markets.

Their development rhythm resembles a startup rather than an advanced intrusion group. They iterate rapidly, incorporate user feedback and adjust to detection quickly. Affiliates distribute the malware through Discord groups and gaming communities while the core team maintains the codebase.

Evolutionary Timeline

Python origins early Q4 2025

Initial versions were Python based and packaged with tools such as PyInstaller. These early samples were large, easy to analyse and focussed on virality. They included a Discord worming feature that sent malicious links to friends and channels automatically.

These variants were noisy and quickly detected by basic antivirus products.

C plus plus pivot late Q4 2025

The operators rewrote Arkanix in C plus plus to improve stealth and performance.

This pivot involved

- Removing the self spreading Discord module
- Introducing Chrome Elevator to retrieve browser credentials protected by App Bound Encryption
- Integrating VMProtect to hinder reverse engineering
- Using native Windows application programming interfaces for faster execution

The rapid evolution demonstrates skill and ongoing maintenance, indicating a committed development crew.

Technical Analysis Arkanix Architecture

Delivery Mechanisms and Infection Vectors

Arkanix relies on social engineering. There is no evidence of exploit kits or drive by compromise.

ClickFix and deceptive installer patterns

Victims are lured through fake troubleshooting prompts such as

- Browser update required
- DirectX error detected

- Copy this PowerShell fix

In gaming communities these lures appear as

- Frames per second unlockers
- Skin changers
- Cracks for popular titles

Python versions self propagate through Discord messages. C plus plus versions rely on affiliates who distribute pre built installers.

Loading and evasion

Arkanix profiles the host to avoid sandbox analysis. It checks CPU count, memory and screen resolution. Low specifications lead to early exit.

VMProtect virtualises code to break traditional disassembly. Some campaigns use in memory payloads to reduce on disk footprints.

Chrome Elevator bypass of App Bound Encryption

Chrome Elevator bypasses App Bound Encryption by injecting into live browser processes. Instead of decrypting protected files externally, it makes requests from inside the browser itself.

The module

1. Writes an embedded payload to a temporary directory
2. Identifies a browser such as Chrome, Edge or Brave
3. Opens the browser process
4. Allocates memory and writes its payload
5. Executes code inside the browser through remote thread creation

This method is more discreet to users than remote debugging approaches and is highly effective at regaining access to encrypted browser data.

Data Harvesting Inventory

Category	Target Applications or Data	Mechanism or Details
Browsers	Chrome, Edge, Brave, Opera, Vivaldi, Yandex, Tor	Extracts login data, cookies, autofill and history. Chrome Elevator retrieves protected data.
Wallets	MetaMask, Binance, Phantom, TronLink, Exodus, Electrum, Atomic	Looks for wallet files, seeds and extension data.
Virtual private networks	NordVPN, ProtonVPN, Mullvad, ExpressVPN	Extracts stored credentials and configuration files.

Category	Target Applications or Data	Mechanism or Details
Network	Wireless profiles	Executes netsh wlan show profiles key equals clear to recover passwords.
System	OS, CPU, GPU, RAM, screen layout, time zone	Creates a fingerprint for victim valuation.
Files	Desktop, Documents, Downloads	Scans for sensitive keywords and document types.
Gaming	Steam, Roblox, Battle net	Steals session tokens and Steam ssfn files.
Remote access	Remote Desktop configurations	Collects rdp files for reuse.

Infrastructure and Exfiltration

Arkanix command and control is centralised and uses encrypted channels.

- Primary domain is arkanix[.]pw
- Python delivery endpoint is hxxps://arkanix[.]pw/delivery
- C plus plus upload endpoint is hxxps://arkanix[.]pw/api/upload/direct
- User agent string ArkanixStealer/2.0 observed in some samples

Data is sent asynchronously, ensuring partial logs are delivered even if execution is interrupted.

Impact Analysis Organisational Risk

Session hijacking and software as a service compromise

Stolen session cookies enable attackers to bypass multi factor authentication and access cloud services directly. This includes Microsoft 365, Slack and Salesforce. Session revocation is critical during incident response.

Network perimeter breach

Arkanix extraction of virtual private network profiles and wireless keys can lead to direct network access or proximity based attacks. Compromised consumer devices can become entry points to corporate environments.

Data extortion and resale

Arkanix logs are sold to initial access brokers who use them to conduct ransomware operations, business email compromise and further malware deployment. This secondary impact often occurs days or weeks after the initial infection.

Indicators of Compromise

File Hashes

Algorithm	Hash	Context
MD5	2a1f858d330c7555d407c9bb1e8a50b4	Arkanix loader user supplied
MD5	9bf2dd417fa21e4c12249ef800c3c40c	Arkanix payload user supplied
MD5	0af0d77d5ac04db4e2d8b25276abb09d	Arkanix variant user supplied
SHA256	08c9e700f5f0b357868ab209e4533bb67d0539b20e639357b6e9854ed8d56415	Confirmed public sample
SHA256	0222a80c806a1f5746c17090f1379779245dd7d86b70b1c5dc5d0e75a13e5a3f	Confirmed user sample
SHA256	b23a4d87b25c5a80931b4b7c3eed7585a0393c53f73d0ed66d971f663b4f2877	Confirmed user sample
SHA256	6960d27fea1f5b28565cd240977b531cc8a195188fc81fa24c924da4f59a1389	Newly added confirmed Arkanix sample
SHA256	6ea644285d7d24e09689ef46a9e131483b6763bc14f336060afaeffe37e4beb5	Newly added confirmed Arkanix sample

Network Indicators

Type	Indicator	Context
Domain	arkanix[.]pw	Core command and control domain
Domain	panel[.]arkanix[.]pw	Affiliate and operator control panel

Type	Indicator	Context
Domain	storage[.]arkanix[.]pw	Payload or log storage
URL pattern	hxxps://arkanix[.]pw/*	Base request pattern
URL pattern	/api/upload/direct	C plus plus upload endpoint
URL pattern	/delivery	Python delivery endpoint
User agent	ArkanixStealer/2.0	Network signature

Behavioural Indicators

- netsh.exe executed with wlan show profiles key=clear
- High speed read access to Chrome Login Data and Local State
- Processes under %TEMP% or %APPDATA% attempting injection into Chrome, Edge or Brave
- Outbound encrypted traffic to arkanix[.]pw from non browser processes

Detection and Mitigation Strategies

Detection Engineering

WiFi credential dumping

Condition: netsh dot exe with wlan, show profiles and key equals clear
Context: Rare for normal administrative use and strongly associated with stealers

Arkanix command activity

Condition: Requests to dot pw domains with upload or delivery paths
Context: Matches known command infrastructure

Chrome Elevator injection

Condition: Remote thread creation and memory writes targeted at browser processes
Context: Signature behaviour of App Bound Encryption bypass

Mitigation Checklist

Phase one prevention

- Block Arkanix domains and optionally block entire dot pw top level domain
- Enforce application allow listing to block execution from temporary and application data directories
- Disable browser password saving and enforce enterprise password manager usage
- Train users on ClickFix themed social engineering

Phase two containment

- Isolate the affected endpoint
- Revoke active sessions for all cloud services
- Reset credentials after session revocation
- Rotate wireless and virtual private network secrets if present on the device
- Preserve artefacts for forensic analysis
- Reimage the device to ensure integrity

Conclusion and Future Outlook

Arkanix Stealer demonstrates how quickly commodity crimeware can adapt to modern defences. The C plus plus rewrite and Chrome Elevator integration show that browser security controls are not absolute barriers.

Future developments may include deeper stealth, broader token theft or integration into ransomware distribution pipelines. Organisations must treat browsers as primary identity boundaries and place greater scrutiny on unmanaged devices.

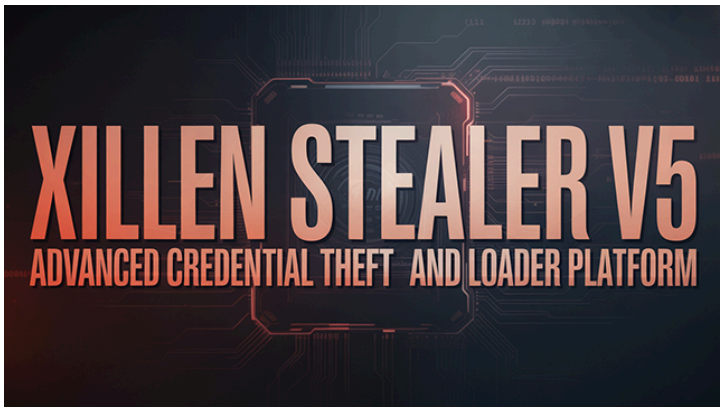
Cybersec Sentinel assesses Arkanix as an Elevated threat with a strong likelihood of continued evolution. Environments with remote workforces or reliance on browser stored credentials should apply this advisory with urgency.

Sources

GData Software – Arkanix Stealer newly discovered short term profit malware – https://www.gdatasoftware.com/blog/2025/12/38306-arkanix-stealer
ESecurity Planet – Rapidly evolving Arkanix Stealer hits credentials and wallets – https://www.esecurityplanet.com/threats/rapidly-evolving-arkanix-stealer-hits-credentials-and-wallets
Cyber Press – New Arkanix Stealer campaign aims to hijack VPN accounts and Wi-Fi credentials – https://cyberpress.org/arkanix-stealer/
Cyber Security News – New Arkanix Stealer attacking users to steal VPN accounts, screenshots and Wi-Fi credentials – https://cybersecuritynews.com/new-arkanix-stealer-attacking-users/

Threat Group – Crimeware cluster similar to UNC5142 access brokers and web compromise crews using Matrix Push C2 Threat Type – Browser based C2 platform, phishing delivery system and malware loader sold as a MaaS service Exploited Vulnerabilities – Abuse of W3C Push API, Service Workers,

notification prompts, clipboard and Run dialog through



Threat Group – Xillen Killers Threat Type – Information stealer and loader operating under a Malware as a Service model Exploited Vulnerabilities – Social engineering and opportunistic scanning for unpatched versions of Cisco AnyConnect, OpenVPN, FortiClient and Pulse Secure in order to access cached credentials Malware Used – Xillen Stealer version five using a

Threat Group – UNC2565 (also tracked as Storm-0494) Threat Type – Malware Loader and Initial Access Platform Exploited Vulnerabilities – No specific CVE confirmed. Campaign relies on SEO poisoning, compromised WordPress sites, archive format inconsistencies, Windows Script Host execution, and legacy filename behaviour. Malware Used – GootLoader, GootBot, secondary payloads such as Cobalt Strike

Cybersec Sentinel © 2025