

---

# AI Infostealer: Arkanix Stealer

## A Glimpse into the Future of AI-Generated, Short-Lived Malware

---

# Arkanix Stealer: Two Months, One Stealer, Zero Traces

A new information-stealing malware operation emerged on dark web forums, promising cybercriminals a feature-rich stealer with modular architecture and anti-analysis capabilities. But just two months after its launch, the developer behind Arkanix Stealer abruptly shut down the project without a trace. Researchers now believe this short-lived operation was an experiment, possibly AI-assisted, designed to test how quickly large language models (LLMs) could accelerate malware development and feature delivery.

## Rise & Fall

Arkanix first appeared on hacker forums in October 2025, marketed with two subscription tiers:

- **Basic Level:** A Python-based implementation for entry-level cybercriminals.
- **Premium Level:** A native C++ payload protected with VMProtect, featuring advanced evasion techniques and wallet injection capabilities.
- The operator established a **Discord server** to build community, provide updates, solicit feature feedback, and offer customer support.
- A **referral program** sweetened the deal, referrers received an extra free hour of premium access, while new customers got a full week of the premium version for free.
- Then, without notice, the developer pulled the plug. The **Discord server vanished**. The control panel went dark. The experiment ended.

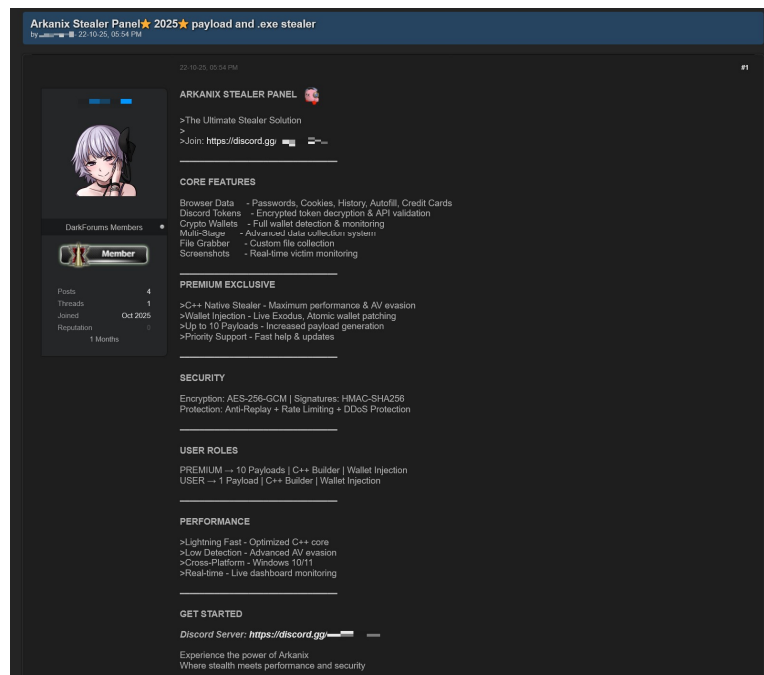


Figure 1 Arkanix Stealer advertisement

## Arkanix Data-theft capabilities

- **Browser Data:** History, autofill information, cookies, and passwords.
- **OAuth2 tokens** from Chromium-based browsers.
- **Cryptocurrency:** Wallet data from 22 different browsers.
- Additional wallet patcher modules for Exodus and Atomic.
- **VPN Credentials:** Targeted Mullvad, NordVPN, ExpressVPN, and ProtonVPN accounts.
- **Apps & Accounts:** Telegram data theft.
- Discord credential stealing and self-propagation via Discord API to victim's friends and channels.
- **System & Files:** System information collection.
- File archiving from local filesystem for **asynchronous exfiltration**.
- Additional modules for FileZilla, Steam, screenshots, and HVNC. The framework demonstrates a startling level of maturity and technical expertise, suggesting its developers possess deep knowledge of systems programming and modern software development.

## Initial infection

The initial infection vector remains unknown. However, based on some of the file names (such as `steam_account_checker_pro_v1.py`, `discord_nitro_checker.py`, and `TikTokAccountBotter.exe`) of the loader scripts we obtained, it can be concluded with high confidence that the initial infection vector involved phishing.

### Native version of stealer

- MD5: a3fc46332dcd0a95e336f6927bae8bb7
- File Name: ArkanixStealer.exe

### Other Payloads

Module name	Endpoint to download	Details
Chrome grabber	<code>/api/chrome-grabber-template/{payload_id}</code>	-
Wallet patcher	<code>/api/wallet-patcher/{payload_id}</code>	Checks whether “Exodus” and “Atomic” cryptocurrency wallets are installed
Extra collector	<code>/api/extra-collector/{payload_id}</code>	Uses a set of options from the config, such as <code>collect_filezilla</code> , <code>collect_vpn_data</code> , <code>collect_steam</code> , and <code>collect_screenshots</code>
HVNC	<code>/hvnc</code>	Is saved to the Startup directory ( <code>%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\hvnc.py</code> ) to execute upon system boot

# The AI Connection

Researchers analyzing Arkanix found telltale signs of LLM assistance in its code. The development patterns suggested that AI tools may have drastically reduced the time and cost required to build such a feature-rich stealer.

```
# Left panel - Input
left_panel = Frame(main, bg='#2b2d31')
left_panel.pack(side=LEFT, fill=BOTH, expand=True)

Label(left_panel, text="Nitro Gift Codes (one per line):",
      font=("Segoe UI", 11, "bold"), bg='#2b2d31', fg='#f2f3f5').pack(anchor=W)

# File buttons
file_frame = Frame(left_panel, bg='#2b2d31')
file_frame.pack(fill=X, pady=(0,12))

Button(file_frame, text="Load from File", command=self.load_file,
      bg='#5865f2', fg='white', font=("Segoe UI", 10, "bold"),
      relief=FLAT, padx=18, pady=8, cursor='hand2').pack(side=LEFT, padx=(0,8))

Button(file_frame, text="Clear List", command=self.clear_list,
      bg='#ed4245', fg='white', font=("Segoe UI", 10, "bold"),
      relief=FLAT, padx=18, pady=8, cursor='hand2').pack(side=LEFT, padx=(0,8))

Button(file_frame, text="Paste", command=self.paste_codes,
      bg='#3ba55d', fg='white', font=("Segoe UI", 10, "bold"),
      relief=FLAT, padx=18, pady=8, cursor='hand2').pack(side=LEFT)

sub_14009DBBC(v496, v12, "stealer_debug.txt");
sub_1400A4D3C(&Ptr_);
sub_14009835C(v491);
sub_14009F8FC(v491, v496, 8);
sub_14009DC8C(v491, "=== STEALER STARTED ===\n");
v13 = sub_14009DC8C(v491, "Data Folder: ");
v14 = unknown_Libname_5(v13, v474);
sub_14009DC8C(v14, "\n");
v15 = sub_14009DC8C(v491, "Folder exists: ");
v16 = sub_1400B85A4(v474);
NO = "NO";
if ( v16 )
    NO = "YES";
v18 = sub_14009DC8C(v15, NO);
sub_14009DC8C(v18, "\n\n");
sub_14009DC8C(v491, "[BROWSER] Starting...\n");
sub_14009D810(PathName);
sub_1400AEA4C(PathName);
sub_14009D810(LpPathName);
sub_1400A9E14(LpPathName);
v19 = sub_14009DC8C(v491, "[BROWSER] Found ");

progress_pct = (i+1) / len(codes) * 100
self.progress.config(text=f"Validating Nitro codes... (progress_pct:.1f)%", fg=
self.stats.config(text=f"Valid: {valid}\nInvalid: {invalid}\nClaimed: {claimed}"
self.root.update()

self.progress.config(text=f" Validation completed | Found {valid} valid codes!",
self.start_btn.config(state=NORMAL, text=" Start Validation")

if valid > 0:
    messagebox.showinfo(" Validation Complete",
                        f"Results:\n\n
                        f" Valid (Unclaimed): {valid}\n"
                        f" Valid (Claimed): {claimed}\n"
                        f" Invalid: {invalid}\n"
                        f" Total Checked: {len(codes)}\n\n"
                        f"Success Rate: {valid/len(codes)*100:.2f}%\n\n"
                        f"Valid codes are shown in the results window.")
else:
    messagebox.showinfo("Validation Complete",
                        f"No valid codes found.\n\n"
                        f"Checked: {len(codes)} codes\n"
                        f"Already Claimed: {claimed}")
```

Figure 2 Example of LLM-specific patterns

The experiment's true purpose remains unclear. Were the developers testing AI's limits? Proving a concept? Or simply cashing in quickly before moving on? Whatever the intent, Arkanix demonstrates a future where malware families appear, thrive, and vanish in the blink of an eye, powered by AI generated code.

**THE NEXT ARKANIX MIGHT NOT DISAPPEAR AFTER TWO MONTHS, IT MIGHT EVOLVE, ADAPT, & STAY!**

## Indicators of Compromise (IoCs)

### File hashes

- 752e3eb5a9c295ee285205fb39b67fc4
- c1e4be64f80bc019651f84ef852dfa6c
- a8eeda4ae7db3357ed2ee0d94b963eff
- c0c04df98b7d1ca9e8c08dd1ffbdd16b
- 88487ab7a666081721e1dd1999fb9fb2
- d42ba771541893eb047a0e835bd4f84e

- 5f71b83ca752cb128b67dbb1832205a4
- 208fa7e01f72a50334f3d7607f6b82bf
- e27edcdeb44522a9036f5e4cd23f1f0c
- ea50282fa1269836a7e87eddb10f95f7
- 643696a052ea1963e24cfb0531169477
- f5765930205719c2ac9d2e26c3b03d8d
- 576de7a075637122f47d02d4288e3dd6
- 7888eb4f51413d9382e2b992b667d9f5
- 3283f8c54a3ddf0bc0d4111cc1f950c0

### Domains and IPs

- arkanix[.]pw
- arkanix[.]ru

**Ready to see how AICenturion can secure you against AI risks?**

Request a demo today: [hello@cytex.io](mailto:hello@cytex.io)

Connect with our social media channels

