

Inside “SalatStealer” — Reverse Engineering a YouTube Bitcoin Brute Tool Malware

 cyberarmor.tech/blog/inside-salatstealer-youtube-bitcoin-brute-malware-reverse-engineering

Nguyen Nguyen

May 2, 2026

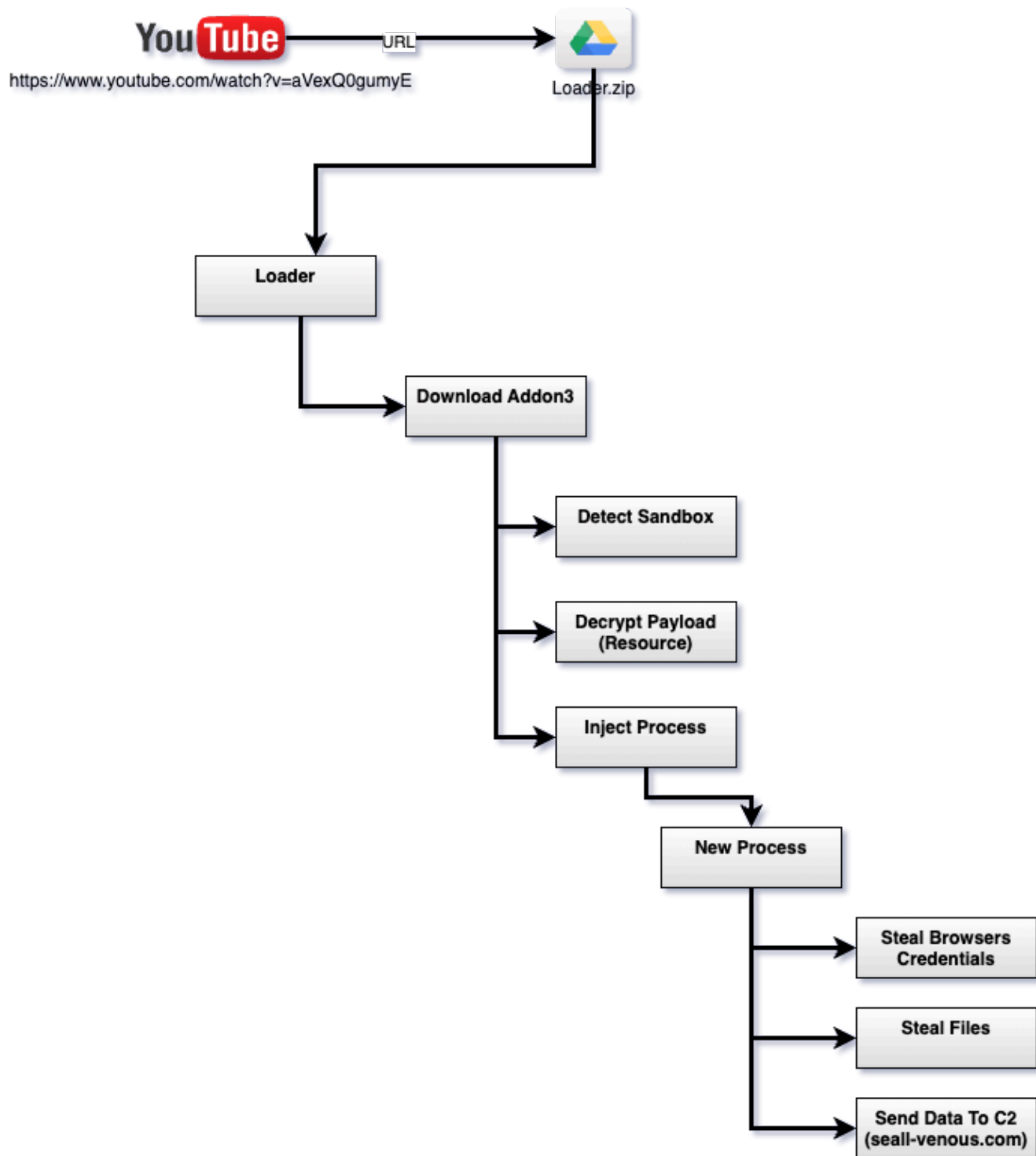


Overview

We recently identified a malware sample distributed through a YouTube video advertising a tool to “brute-force” or recover lost Bitcoin wallets. The lure is effective: it targets users who believe they can recover cryptocurrency, prompting them to execute an unknown binary.

In reality, the payload is an **infostealer**, not a recovery tool.

This blog documents the reverse engineering process and initial findings. Figure 1 shows the overview of the campaign.



Delivery Method

- Video claims to recover lost BTC wallets
- Download link provided in description or comments to Google Drive
- Payload presented as a legitimate utility

This approach lowers suspicion and increases execution rates, especially among non-technical users.

Below is the youtube channel.

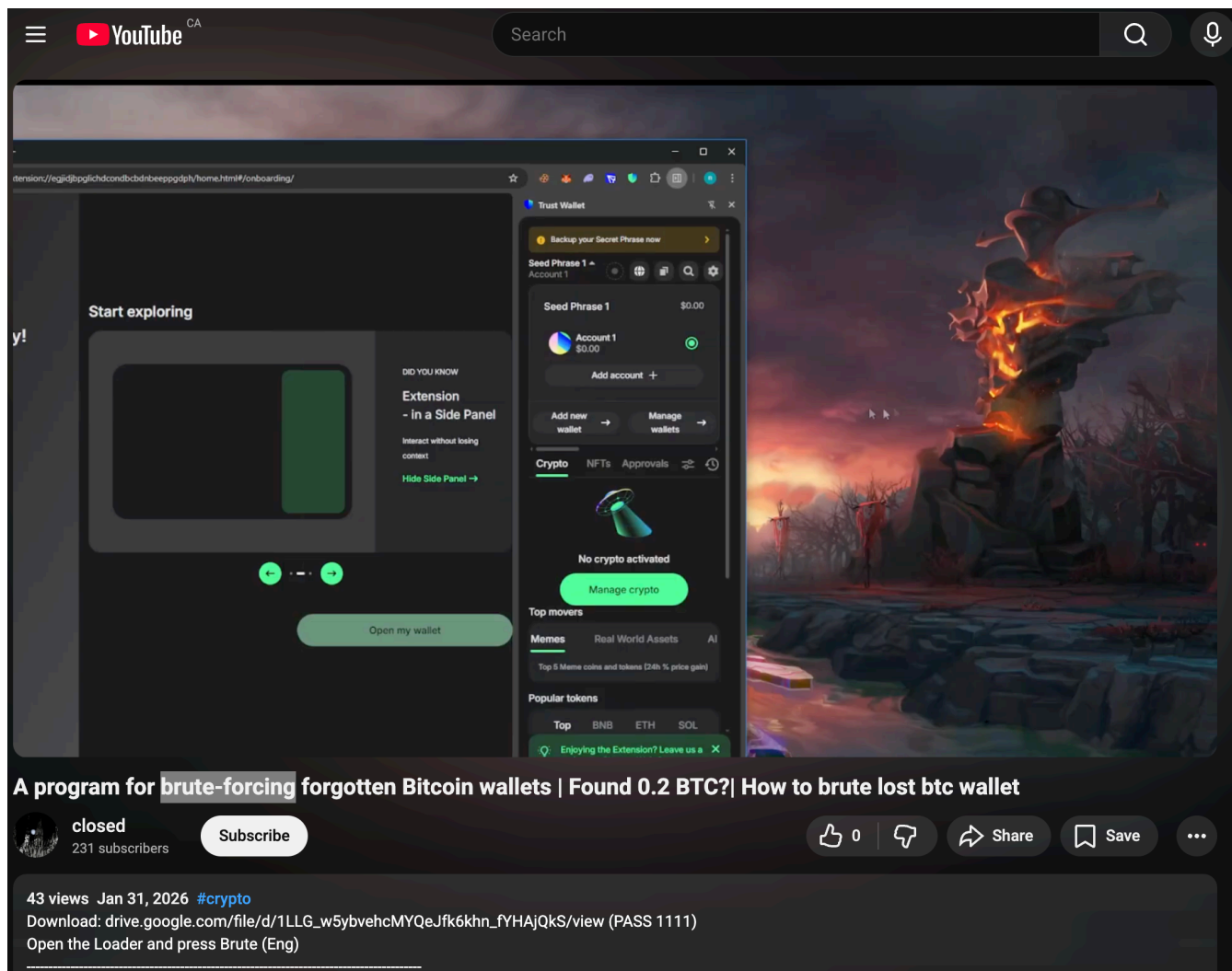


Figure 2: YouTube Channel Delivering the Loader

In the description, the page includes a download link to Google Drive, as shown below. The file is encrypted, which helps it evade Google's detection and removal mechanisms.

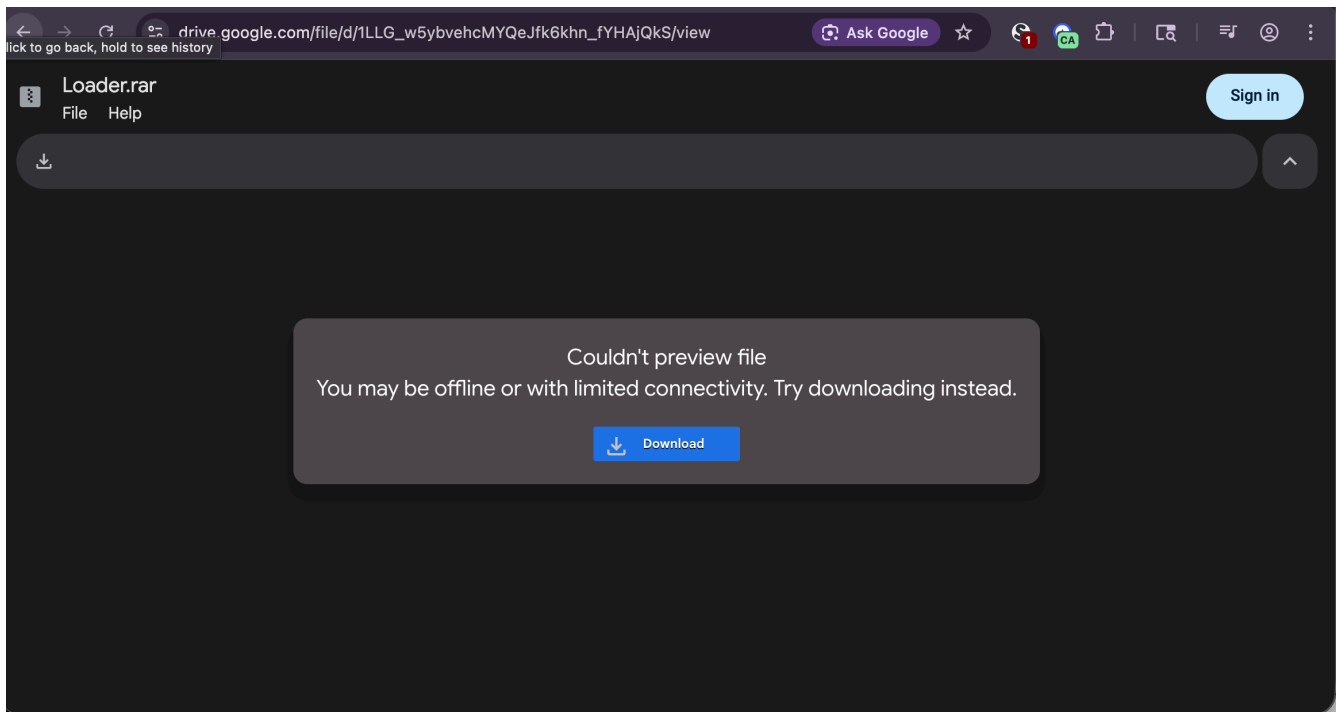


Figure 3: Link to File on Google Drive

Once you download and extract the file using the password “1111,” the extracted file is a SalatStealer loader with the following properties.

MD5: dede03baf3db18febbfdab6068dd9df4

SHA1: d50a0c1b413b59e508f4964ce97496a9de75ff9c

SHA256: 2469940f2355e150186c64ebe756df4d56fca02cac8dc1716f4df7cebcfb7b85

Once you running floss on the Loader, it shows a list of URL the malware download.

hxxp://147.45.219[.]144/disable_defender_and_setup.bat

hxxp://147.45.219[.]144/run_silent.vbs

hxxp://147.45.219[.]144/SteamSetup.exe

hxxp://147.45.219[.]144/AirDrop.exe

hxxp://147.45.219[.]144/Addon2.exe

hxxp://147.45.219[.]144/Addon.exe

hxxp://147.45.219[.]144/BruteForce.exe
hxxp://147.45.219[.]144/MetaSkins.exe
hxxp://147.45.219[.]144/Addon3.exe
hxxp://147.45.219[.]144/Overplus.exe
hxxp://147.45.219[.]144/Drift.exe
hxxp://147.45.219[.]144/VMPProtectSDK64.dll

Addon3 - Stealer Dropper

Addon3.exe is the primary file referenced by the loader; it turns out to be the malware dropper. The file has the following properties.

MD5: dee62f6b131ca23940ec51701df7154c

SHA1: 458a87d8af348401cf6335a76c3c1ac999d5ae05

SHA256: b74f067d9363faf3b6528914073908cd304799992d8b1611e213dbade92127fc

Obfuscation and Decryption

During analysis, the malware uses a **simple but effective obfuscation technique**:

- The payload is stored in the resource
- Encoded payload stored within the binary
- Decryption routine applied in memory
- Key-based transformation to reconstruct original data

The payload is encrypted with the following format. Once the key is obtain, the decryption

Addon3 - Encrypted Payload Structure



Below is where you can insert your code snippet:

The decryption code can be download here.

https://raw.githubusercontent.com/cyberarmortech/iocs/refs/heads/main/Addon3_decryptor.py

The final payload is obfuscated using the [rust-obfuscator](#) library. You can decrypt the strings using the following function.

https://github.com/cyberarmortech/iocs/blob/main/Addon3_final_payload_string_decryptor.py

Key Observations

- The malware is **not sophisticated**, but effective due to distribution
- Relies more on **social engineering than technical evasion**
- Targets high-value data such as credentials and wallet information
- Likely part of a broader infostealer ecosystem

Conclusion

“SalatStealer” is a reminder that:

- The delivery vector is often the weakest link
- Even simple malware can be highly effective
- Reverse engineering remains critical to understanding real-world threats

IOCs:

hxxps://www.youtube[.]com/watch?v=aVexQ0gumyE

hxxps://drive.google[.]com/file/d/1LLG_w5ybvehcMYQeJfk6khn_fYHAjQkS/view

hxxps://seall-vernous[.]com:443

hxxps://t[.]me/gerj_threuh

hxxp://147.45.219[.]144/disable_defender_and_setup.bat

hxxp://147.45.219[.]144/run_silent.vbs

hxxp://147.45.219[.]144/SteamSetup.exe

hxxp://147.45.219[.]144/AirDrop.exe

hxxp://147.45.219[.]144/Addon2.exe

hxxp://147.45.219[.]144/Addon.exe

hxxp://147.45.219[.]144/BruteForce.exe

hxxp://147.45.219[.]144/MetaSkins.exe

hxxp://147.45.219[.]144/Addon3.exe

hxxp://147.45.219[.]144/Overplus.exe

hxxp://147.45.219[.]144/Drift.exe

hxxp://147.45.219[.]144/VMProtectSDK64.dll

Want to detect threats 8+ months earlier?

See how DarkArmor's PreBreach intelligence can protect your organization.

[Book a Demo](#)



About the Author

Nguyen Nguyen

Nguyen (Founder & CEO @ CyberArmor) is a seasoned cybersecurity leader with over 15 years of experience in software engineering, malware research, and cyber threat intelligence.

[LinkedIn Profile](#)