# NightfallGT/Mercurial-Grabber: Grab Discord tokens, Chrome passwords and cookies, and more

github.com/NightfallGT/Mercurial-Grabber

NightfallGT

# NightfallGT/**Mercurial-Grabber**

Grab Discord tokens, Chrome passwords and cookies, and more

| 👥 1 | ⊙ 73 | ☆ 249 | ⑂ 222 |
|------|------|-------|-------|
| Contributor | Issues | Stars | Forks |

## Builder Preview

## Features

- Grabs Roblox cookies from Roblox Studio
- Grabs Minecraft sessions
- Grabs Google Chrome passwords
- Grabs Google Chrome cookies
- Grabs Discord token
- Grabs victim machine info
- Grabs Windows product key
- Grabs IP address, geolocation
- Grabs screenshot
- Anti Virutal Machine
- Anti Debug

## Customization

- Add a custom icon
- Custom exe name

## Info

Please do not use the program maliciously. This program is intended to be used for educational purposes only. Mercurial is only used to demonstrate what type of information attackers can grab from a user's computer. This is a project was created to make it easier for malware analysts or ordinary users to understand how credential grabbing works and can be used for analysis, research, reverse engineering, or review.

What is malware?

> Malware is a term that is used for malicious software that is designed to do damage or unwanted actions to a computer system.

An explanation of this tool:

Google Chrome always store user data in the same place, so the stealer generated by Mercurial Grabber has no problem in finding it. In theory at least, this data is stored in encrypted form. However, if the malware has already penetrated the system, then its actions are done in your name.

Therefore, the malware simply finds a way to decrypt information stored on your computer (by making it seem like thie user is requesting it) . The stealer gets all your passwords and cookies.

The tool is also able to find Roblox cookies that are stored in the Windows Registry. By running the malicious .exe file, it is able to search for the Roblox cookie. The same goes for Minecraft sessions, Discord tokens, etc since it is stored in the user's computer.

Recommended tools for testing Mercurial: (when running the produced output after building)

- Virtualbox
- VMware
- Process Hacker
- VirusTotal

Tips to check if an exe file is safe:

- Analyze the file with VirusTotal
- Check if the exe file has a publisher
- Check it in a sandbox
- Monitor the file's network activity for strange behavior

## Educational Purposes Only

This tool demonstrates and makes it easy to create your own grabber. This shows what type of information attackers can grab from a victim's computer. Only use this on your own PC and do not use it on other people maliciously.