GitHub - wgpsec/CreateHiddenAccount: A tool for creating hidden accounts using the registry || 一个使用注册表创建隐藏帐户的工具

By teamssix

Archived: 2026-04-05 17:46:21 UTC

中文 | EN

Tool Introduction

There are two common ways to create a hidden account. One is to add the $ sign directly after the user name to create it, and the other is to use the registry to clone the user to create. .

So I wondered if I could implement the process of cloning accounts using the registry. After searching on the Internet, I couldn't find a convenient tool, so I wrote one myself.

In addition to adding hidden accounts, the tool also adds functions to check hidden accounts and delete hidden accounts, so that both the red team and the blue team can use this tool.

**DISCLAIMER: DO NOT USE THE TOOL FOR ILLEGAL USE, THE DEVELOPER IS NOT RESPONSIBLE OR RESPONSIBLE FOR ANY MISUSE OR DAMAGE. **

Download Link

https://github.com/wgpsec/CreateHiddenAccount/releases

- CreateHiddenAccount.exe BypassAV works better
- CreateHiddenAccount_upx.exe Smaller size

Help Information

Use `CreateHiddenAccount.exe -h` for help

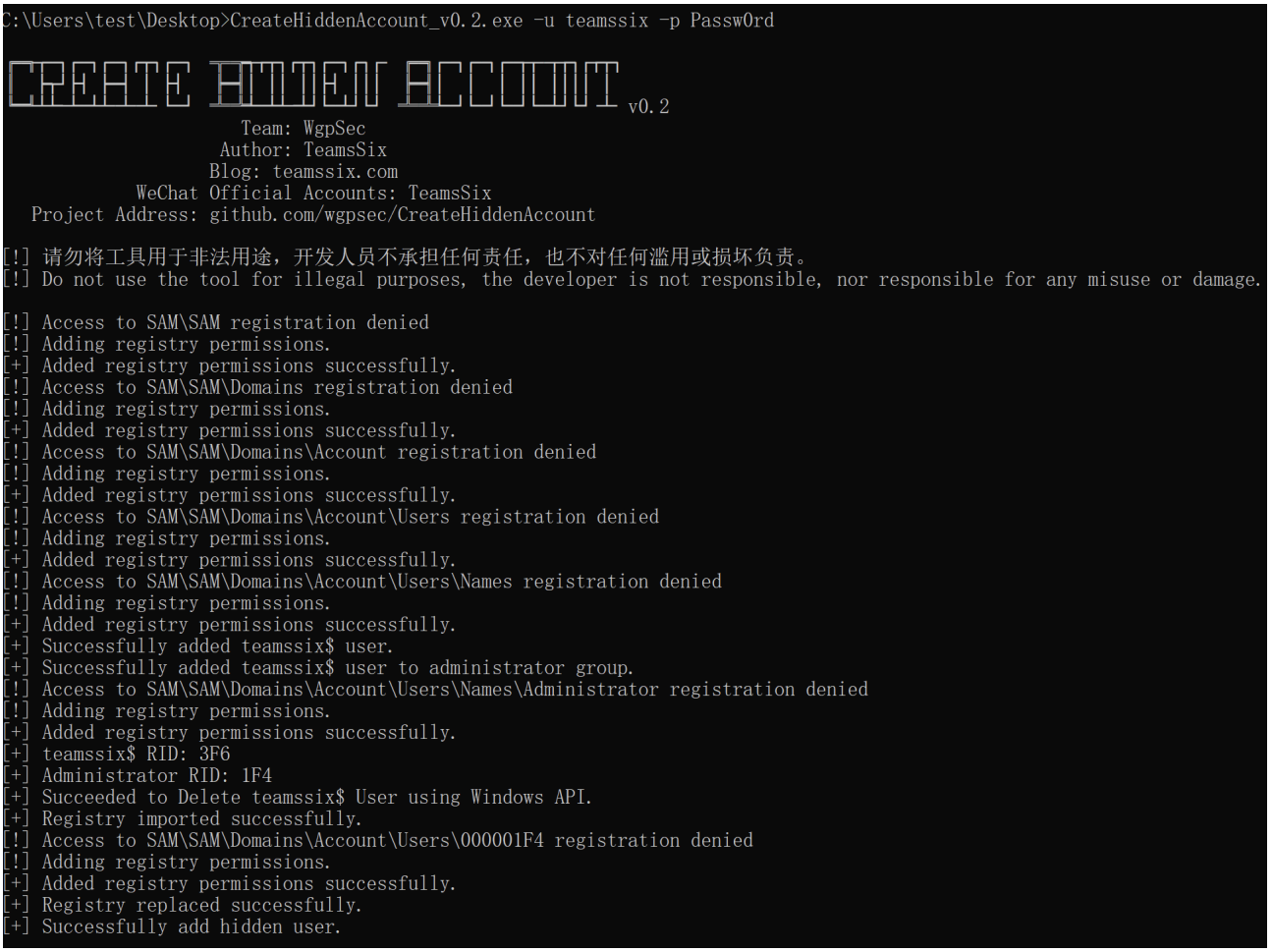
- -c Check the hidden accounts of the current system
- -cu Set clone user (default "Administrator")
- -d Set delete username, If the username does not end with a $ sign, a $ sign will be added automatically
- -oc Only create hidden users, do not clone users by modifying the registry
- -p Set password
- -u Set username, If the username does not end with a $ sign, a $ sign will be added automatically
- -v View version

✨ Example

Add a hidden account with the user name teamssix, the tool will automatically add the $ character after the user name, so the created user name is teamssix$

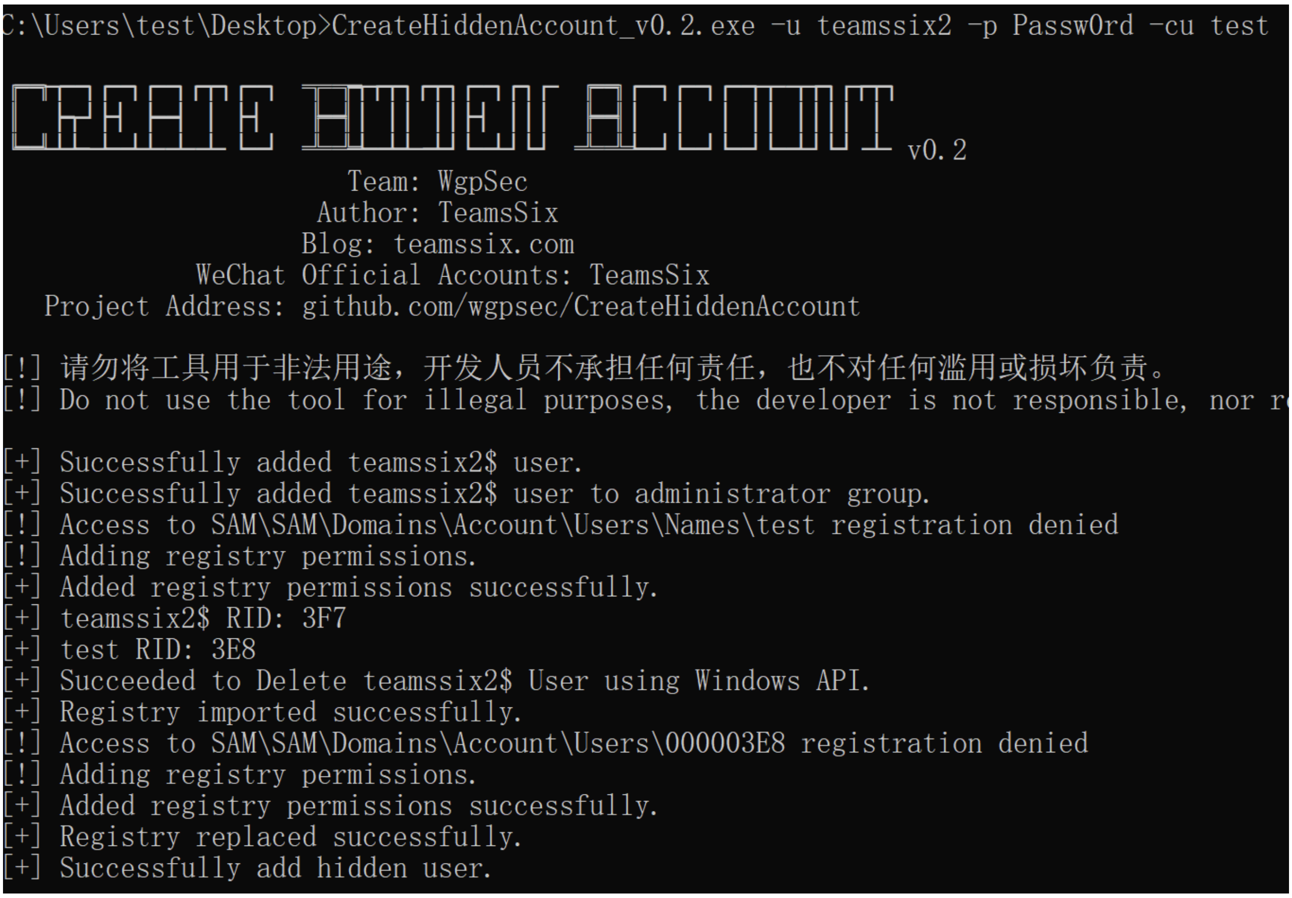
When using, remember to run under administrator privileges, otherwise it will prompt insufficient privileges.

```
CreateHiddenAccount.exe -u teamssix -p Passw0rd
```



Select the username you want to clone

```
CreateHiddenAccount.exe -u teamssix2 -p Passw0rd -cu test
```



Only create hidden users, do not modify the registry

```
CreateHiddenAccount.exe -u teamssix3 -p Passw0rd -oc
```

Check the hidden accounts of the current system.

```
CreateHiddenAccount.exe -c
```

Delete the teamssix hidden account

```
CreateHiddenAccount.exe -d teamssix
```

In the end, if there is any bug to open an issue, the Star will be gone, you know.

⚠️ Notice

- The tool requires administrator privileges to run
- This tool is not guaranteed to work properly on 32-bit systems

- On the domain controller machine, this tool will only add hidden users and will not modify the registry, because on the domain controller machine, user information is not stored in the registry.
- If the control panel shows that there is a hidden user, but both tools and net user show that the user does not exist, then when the computer restarts, the hidden user in the control panel will disappear.
- The tool will automatically add the $ character to the username without the $ character. For example, if -u specifies the user name as teamssix, the actual account added is teamssix$; if -u specifies the user name as teamssix$, then the actual added account is or teamssix$

> The purpose of this is because if the user name does not have the $ character, then hiding the user is meaningless. If you just want to add an account, just use net user directly.

Changelog

v0.2 2021.1.18

- Enhanced the ability to detect hidden accounts
- Added ability to select clone user
- Added the function of only creating hidden users without modifying the registry
- Added tool version display

v0.1 2021.1.17
