

Forum:[Hack Forums](#)

Thread: [Offering a UAC Bypass and Personal Training](#)

SIM-5063966 - November 11, 2022, 9:51 am

I am willing to sell a UAC Bypass and teach someone how to use it properly for 250\$ (PM me, if you really are interested / curious about the topic, I may drop the price a little)!

Why is the price so high for a UAC bypass?

Because:

- this isn't made for someone that's already a malware developer / advanced red teamer / experienced in the malware scene, this is made entirely for beginners and intermediates (programmers and non-programmers) that want to learn more about the techniques used by the new threat actors, red teaming and exploit development
- the code is really well documented and commented
- I will help you understand all the topics that we will go through and give you enough information (through personal teaching. courses and books) so you can make your own exploits from now on

Details

- The bypass is written entirely in C++17 and it doesn't require any dependency
- It works from windows 7+ (including windows 10 and 11 newest versions) for both x32 and x64
- The current example is a windows executable (uses WinMain as an entry point), but I can also show you how to implement it in a DLL
- It bypasses UAC and allows you to elevate the process' integrity level silently, without any user interaction
- It's not detected by windows defender (bypasses both static and runtime at the time of writing this thread, but even if the code will get detected after the purchase, the source is pretty easy to reFUD, even without a crypter!)
- The bypass can be converted easily into other languages, I may help you implement it in C# as well
- The bypass can be implemented pretty easily in crypters / packers

Showcase Video

Link: <https://streamable.com/e8ks1d>

Examples shown in the video: Getting administrator CMD / PowerShell

Elevating the process' integrity level

Technique: UAC Bypass

Platform: Windows 10 x64

Antivirus: Windows Defender - 11 November 2022

! All of this was done without running the executables as an administrator

! Really sorry for the shitty quality and the semi-broken VM

So, what will you get in this price?

The C++ files containing the bypass and 4 use cases, for example:

- How to open administrator CMD / PowerShell
- How to run administrator commands in the background
- How to elevate the process' integrity level silently and disable windows defender / add paths or

extensions to exclusions

- How to give it loader capabilities (elevate + add exclusions + download + execute)

Instructions on how to build

- You can build it with Visual Studio (2017 or newer) or g++

Support

- I will help you compile all the examples by yourself
- The source code is pretty clean and has a lots of comments explaining almost everything, so it's pretty easy to understand what's going on after you buy the source, but I can as well show you how some things work

My [Malware Development Pack](#)

- If you aren't experienced enough in C++, don't worry, you will get my EBook + all the resources that come with my [censored] pack, this will help you with compiling and understanding my code and will also create a pretty solid foundation in object oriented programming and exploit development! All you need is some free time and

Are there any vouch copies available?

- I will offer 1 vouch copy to trusted member, he won't get access to the source code, only a custom executable (that will contain his username) to test the UAC bypass

How does it work?

- Buy the source and check it out

Will the exploit get patched in the following windows updates?

- You know as well as I do that I can't guarantee this, but I use this exploit since 2021 and I am pretty sure it's not a widely known method (tho the exploit was made public)

Can I get a refund?

Yes, you can, but only in 2 special cases:

- You decided you don't want the bypass anymore, and I haven't sent you the files yet
- The bypass stopped working in less than 14 days after the purchase

[contract=tid]Start Contract[/contract]

TOS

Payment

- I currently accept only Monero (XMR), Bitcoin (BTC) and Litecoin (LTC)

If you received a Vouch Copy

- I won't be held responsible for the misuse of the executables that I will send, because I can't monitor your activity!
- If you received a vouch copy, you aren't allowed to scan the executable with services that distribute (for example: VirusTotal or AntiScan.me) or share it with anybody else!

If you bought the Source Code

- I won't be held responsible for the misuse of the executables / the source files that I will send, because I can't monitor your activity!
- I will delete / close this thread and I will not sell this anymore
- You aren't allowed to use this in any illegal activity, this is for learning purposes only, that's why I am offering a teaching service for free along with the source!
- You are allowed to share it with your friends / the community / whatever!

- You are allowed to scan the executable with services that distribute!
 - You are allowed to resell it!
- ! You are allowed to do whatever you want tbh, just be reasonable and keep it legal!

If you have any questions / issues

- Don't hesitate to PM me, I will edit my thread accordingly

Rikimaer2 - December 11, 2022, 1:31 pm

Please check your PM

Thanks

SIM-5063966 - December 12, 2022, 7:21 am

(Dec 11, 2022 02:31 PM)Rikimaer2 Wrote: [\[CITE\]](#) Please check your PM

Thanks

Sent you a demo with your name included in your DMs!

ubas - January 11, 2023, 9:07 am

not too familiar with anything besides python and im looking to learn, i will shoot you a dm in a sec :)
looks pretty nifty

Friendz - January 27, 2023, 4:34 pm

This looks a lot like something i'd be interested in.

Just knowledge sitting out there...