

Forum:[Hack Forums](#)

Thread: [uac bypass in powershell is working Why ?](#)

arav - August 19, 2024, 3:25 pm

I found a somewhat peculiar powershell script today, the purpose of the script is to obtain administrator privileges and disable Windows antivirus, task manager and cmd by exploiting these privileges. In the git hub repostery the creator recommended converting the ps1 script to .exe and running it as such, surprisingly the executable worked even though my Windows Defender was active, I retested it several times, first trying to run the UAC bypass manually and then reusing the program, strangely the antivirus blocks my attempts but the magic program from github defeats the antivirus even though it doesn't seem like there's anything special to me. The thing that leaves me baffled is that the method used is simply the fudhelper that real-time protection normally blocks without problems. Is there anyone who knows about powershell or UAC bypass who can explain to me how this works? If anyone wants to help me learn more I can send them the github link privately but they have to write to me because I don't have an updated account.

SovietBastard - August 19, 2024, 3:29 pm

(Aug 19, 2024 03:25 PM)arav Wrote: [\[CITE\]](#) I found a somewhat peculiar powershell script today, the purpose of the script is to obtain administrator privileges and disable Windows antivirus, task manager and cmd by exploiting these privileges. In the git hub repostery the creator recommended converting the ps1 script to .exe and running it as such, surprisingly the executable worked even though my Windows Defender was active, I retested it several times, first trying to run the UAC bypass manually and then reusing the program, strangely the antivirus blocks my attempts but the magic program from github defeats the antivirus even though it doesn't seem like there's anything special to me. The thing that leaves me baffled is that the method used is simply the fudhelper that real-time protection normally blocks without problems. Is there anyone who knows about powershell or UAC bypass who can explain to me how this works? If anyone wants to help me learn more I can send them the github link privately but they have to write to me because I don't have an updated account.

if i were to use windows i would have helped you, but im not :)

DramaKing - August 19, 2024, 3:34 pm

[Centsicles](#) should be interested in this.

arav - August 19, 2024, 3:34 pm

(Aug 19, 2024 03:29 PM)SovietBastard Wrote: [\[CITE\]](#) if i were to use windows i would have helped you, but im not :)

yes i can understand, in a hacking forum it's normal that many people use linux xd. maybe i should have posted in the rat section where people know windows targets and privilege escalation methods well.

(Aug 19, 2024 03:34 PM)DramaKing Wrote: [\[CITE\]](#) [Centsicles](#) should be interested in this. I don't know how you manage to reply to every single thread on the forum, I would like this supertre too

SovietBastard - August 19, 2024, 3:41 pm

(Aug 19, 2024 03:34 PM)arav Wrote: [\[CITE\]](#) yes i can understand, in a hacking forum it's normal that many people use linux xd. maybe i should have posted in the rat section where people know windows targets and privilege escalation methods well.

I don't know how you manage to reply to every single thread on the forum, I would like this superptere too
no im not a hacker, im just a drunk programmer

DramaKing - August 19, 2024, 6:25 pm

(Aug 19, 2024 03:34 PM)arav Wrote: [\[CITE\]](#) I don't know how you manage to reply to every single thread on the forum, I would like this superptere too
Too much time on my hands. Not enough motivation to do other stuff.

ttbr0 - August 19, 2024, 8:22 pm

(Aug 19, 2024 03:25 PM)arav Wrote: [\[CITE\]](#) I found a somewhat peculiar powershell script today, the purpose of the script is to obtain administrator privileges and disable Windows antivirus, task manager and cmd by exploiting these privileges. In the git hub repostery the creator recommended converting the ps1 script to .exe and running it as such, surprisingly the executable worked even though my Windows Defender was active, I retested it several times, first trying to run the UAC bypass manually and then reusing the program, strangely the antivirus blocks my attempts but the magic program from github defeats the antivirus even though it doesn't seem like there's anything special to me. The thing that leaves me baffled is that the method used is simply the fudhelper that real-time protection normally blocks without problems. Is there anyone who knows about powershell or UAC bypass who can explain to me how this works? If anyone wants to help me learn more I can send them the github link privately but they have to write to me because I don't have an updated account.

you got the link? i need some more context before coming to a conclusion.

arav - August 20, 2024, 3:40 am

(Aug 19, 2024 08:22 PM)ttbr0 Wrote: [\[CITE\]](#) you got the link? i need some more context before coming to a conclusion.

[this is the link](#) I still don't understand how it works

etizolamvendor - August 20, 2024, 4:43 am

amazing ! thank you brother!

ttbr0 - August 20, 2024, 5:51 am

(Aug 20, 2024 03:40 AM)arav Wrote: [\[CITE\]](#) [this is the link](#) I still don't understand how it works looks like new code. its not surprising nor uncommon that newly rewritten code can bypass av because signatures are fragile like that.

ScrubspooF - August 20, 2024, 5:56 am

Fodhelper method.. this is what ScrubCrypt used as well. Fodhelper runs with escalated (admin) privs and then is manipulated with registry keys, bypassing UAC.

arav - August 20, 2024, 6:42 am

(Aug 20, 2024 05:56 AM)ScrubspooF Wrote: [\[CITE\]](#) Fodhelper method.. this is what ScrubCrypt used as well. Fodhelper runs with escalated (admin) privs and then is manipulated with registry keys, bypassing UAC.

Normally windows real time protection prevents you from launching fodhelper.exe from powershell, I don't know if converting it to executable is normal for the script to bypass windows defender but I don't think so

(Aug 20, 2024 05:51 AM)ttbr0 Wrote: [\[CITE\]](#) looks like new code. its not surprising nor uncommon that newly rewritten code can bypass av because signatures are fragile like that.

yes but in itself it is a very normal code, in short the ps1 in the bypassing section has the same 5 scripts that were used 4 years ago, I would like to understand what is special and why

Centsicles - September 21, 2024, 2:15 am

(Aug 19, 2024 03:34 PM)DramaKing Wrote: [\[CITE\]](#) [Centsicles](#) should be interested in this.

Hello :>,i have fortunately managed to stumble upon this.I've downloaded it,Is it ok if i execute it in my pc now?

DramaKing - September 21, 2024, 5:35 am

(Sep 21, 2024 02:15 AM)Centsicles Wrote: [\[CITE\]](#) Hello :>,i have fortunately managed to stumble upon this.I've downloaded it,Is it ok if i execute it in my pc now?

This is what I've slowly been obfuscating. Whether it currently bypasses Norton, I don't know. I'm also commenting out some lines because it changes a long list of registry keys. Be careful.

Centsicles - September 21, 2024, 9:38 am

(Sep 21, 2024 05:35 AM)DramaKing Wrote: [\[CITE\]](#) This is what I've slowly been obfuscating.

Whether it currently bypasses Norton, I don't know. I'm also commenting out some lines because it changes a long list of registry keys. Be careful.

didn't really wait for you reponse tbh (sorry),i tried it but .ps1 file got blocked and came up with the message something about "this files is dangerous" thats definitely not norton,and the registry file didnt let me execute because i didnt have admin

woo097878781 - October 28, 2024, 3:54 pm

This code has been patched and will report viruses