

Forum:[Hack Forums](#)

Thread: [Batch UAC Bypass - Video Demo \(elevate to admin privileges without asking user\)](#)

gogglebot - March 21, 2017, 1:01 pm

Hello HF!

Please note that this has since been patched in at least Windows 10 by an alteration to eventvwr.exe and other similar signed executables, rendering this script/method dead on up to date Win10, I have no idea about other versions of Windows however. Outdated PCs may still be vulnerable however

I recently found out about a method of bypassing the User Account Control (UAC) prompt ([this thing](#)) and decided to implement it into a batch script, thus allowing the script to drop a file/program (be it another .bat, .vbs, or an .exe, etc.) and give it administrator permissions, silently, without telling the user that it is running, and at least in the case of a .bat, runs invisible so there is no cmd prompt window but the batch still runs in the background.

Further the script makes it so your dropped file is run every time the user logs in to their computer, again silently with no window popping up (notice in the video below that no cmd prompt window appears when I log in, it's hidden.)

This could be used as a non-disruptive installer for your piece of software, if you want a file to run hidden at login time, etc.

[Click here for a demo video of it in action!](#)

The code used in the demo video, with annotations, is below in this pastebin:

<http://pastebin.com/bxt4S1MF>

If you would like an in-depth explanation of this script and the mechanisms it uses, ask and I shall update this post (or make a new one later)

SIM-3489054 - March 21, 2017, 3:12 pm

Crazy batch bro thank's for sharing :D

gogglebot - March 21, 2017, 7:18 pm

(Mar 21, 2017 03:12 PM)Biboo Wrote: [\[CITE\]](#) Crazy batch bro thank's for sharing :D
Thanks friend ^.^

WOLGA - March 21, 2017, 7:35 pm

hello,
use 'start /wait' instead of 'timeout'.
-wolga

b00st3d - March 22, 2017, 4:01 am

This works. I'm impressed. I have wanted a good UAC bypass method for a while but never really dug into how to do it. I will use this a starting point to make it run a little cleaner for use in scripts that need elevation.

Cumbax - March 22, 2017, 7:46 am

Yesterday i read a thread posted yesterday about someone asking for a solution.

Keep it up, this is an amazing piece of code, thanks for sharing!

ahebah - March 22, 2017, 8:33 am

Thank's for posting OP, thing's like this come in handy !

ImDeepWithWindows - March 22, 2017, 10:01 am

i havent tested it yet cuz im on a mac but it looks good, if it works props 2 this is a HQ worth knowing manipulation

btw on your pastebin i think u have a typo on line 23 that u might wanna fix, theres only one ">" in your echo command not two (">>"), idk maybe that still works and theres something i dont know that u do, anyway good stuff HQ

TheTurboEngineers - March 22, 2017, 10:07 am

Thanks for the Method.
This will come in handy!

Hoodie+ - March 22, 2017, 10:14 am

(Mar 22, 2017 10:01 AM)ImDeepWithWindows Wrote: [\[CITE\]](#) i havent tested it yet cuz im on a mac but it looks good, if it works props 2 this is a HQ worth knowing manipulation

btw on your pastebin i think u have a typo on line 23 that u might wanna fix, theres only one ">" in your echo command not two (">>"), idk maybe that still works and theres something i dont know that u do, anyway good stuff HQ
One writes to the file, two deletes all content and than writes to the file.

JoshuTee - March 22, 2017, 10:38 am

Sadly Microsoft has recently patched this, so it will only work on computers that have not been updated yet

gogglebot - March 22, 2017, 1:34 pm

(Mar 22, 2017 10:14 AM)Hoodie+ Wrote: [\[CITE\]](#) One writes to the file, two deletes all content and than writes to the file.Nearly, One overwrites, two amends. In your words: one deletes and writes, two writes

(Mar 22, 2017 10:38 AM)JoshuTee Wrote: [\[CITE\]](#) Sadly Microsoft has recently patched this, so it will only work on computers that have not been updated yet

Yeah I found that out earlier today, annoying, took 6 years for them to patch it and they do it just as I make this thing, haha ?

Hoodie+ - March 22, 2017, 1:58 pm

Isn't this method Windows 10 only?

Is it the same as this: <https://enigma0x3.net/2017/03/17/fileless-uac-bypass-using-sdclt-exe/>

b00st3d - March 22, 2017, 3:41 pm

(Mar 22, 2017 01:58 PM)Hoodie+ Wrote: [\[CITE\]](#) Isn't this method Windows 10 only?

Is it the same as this: <https://enigma0x3.net/2017/03/17/fileless-uac-bypass-using-sdclt-exe/>
No this works on 7. I have it running on a VM now.

gogglebot - March 22, 2017, 5:27 pm

(Mar 22, 2017 01:58 PM)Hoodie+ Wrote: [\[CITE\]](#) Isn't this method Windows 10 only?

Is it the same as this: <https://enigma0x3.net/2017/03/17/fileless-uac-bypass-using-sdclt-exe/>
7 8 and 10, not sure about vista and probably not XP
The video is of it working on Windows 7 ^.^

Mr. Kim - March 25, 2017, 6:56 am

Thanks for the share! Very useful :)

PS, you own me a shitty drawn paint.net picture <3
(enjoy the BTC)

gogglebot - March 25, 2017, 9:26 am

(Mar 25, 2017 06:56 AM)M3MORY Wrote: [\[CITE\]](#) Thanks for the share! Very useful :)

PS, you own me a shitty drawn paint.net picture <3
(enjoy the BTC)
Quite alright!
Omg someone actually gave me BTC! What would you like drawn?
I'll make it as shitty as possible <3

Mr. Kim - March 25, 2017, 6:18 pm

(Mar 25, 2017 09:26 AM)gogglebot Wrote: [\[CITE\]](#) Quite alright!
Omg someone actually gave me BTC! What would you like drawn?
I'll make it as shitty as possible <3
Can't PM yet my dude, could I get a shitty drawing of a penguin holding an american flag?

enjoy your ramen <3

gogglebot - March 26, 2017, 8:09 pm

(Mar 25, 2017 06:18 PM)M3MORY Wrote: [\[CITE\]](#) Can't PM yet my dude, could I get a shitty drawing of a penguin holding an american flag?

enjoy your ramen <3
Once my laptop has stopped having a heart attack for long enough to be usable I shall deliver for you!

dzirione1 - March 29, 2017, 9:33 pm

THANKS THANKS THANKS THANKSTHANKS

Monyaks - March 30, 2017, 10:03 pm

Awesome UAC patch. Thanks for the share.

Jar Jar Binks - March 30, 2017, 10:05 pm

Great batch!! Repped asf!

doctor.alpha - March 30, 2017, 10:13 pm

That's pretty nice dude i already knew you can do it with batch.

ImDeepWithWindows - April 4, 2017, 3:12 pm

(Mar 22, 2017 10:14 AM)Hoodie+ Wrote: [\[CITE\]](#) One writes to the file, two deletes all content and than writes to the file.

rly? all with all my laptops its been the other way around and one means overwrite the text files text and two means add to the end of the text file, what ver of windows r u using? i wanna see if thats changed in the new versions

motherfawker666 - April 4, 2017, 5:44 pm

This is gold. Thanks for contributing this...

IGNOR4NCE - April 7, 2017, 12:15 pm

A big thanks! If it work without OS problems it can be very usefull !

-> Add in a .NET app -> silent UAC byps... ?

(I will try it later ?)

gogglebot - April 7, 2017, 3:36 pm

(Apr 4, 2017 03:12 PM)ImDeepWithWindows Wrote: [\[CITE\]](#) rly? all with all my laptops its been the other way around and one means overwrite the text files text and two means add to the end of the text file, what ver of windows r u using? i wanna see if thats changed in the new versions

You are right, IDwW, he just made an honest mistake and got them switched, nothing has changed :)

(Mar 30, 2017 10:05 PM)Jar Jar Binks Wrote: [\[CITE\]](#) Great batch!! Repped asf!

Thank you very much ?

Considering how I could improve, but not sure where to take it

Phlox - May 22, 2018, 9:02 am

Fantastic script mate, keep up the good work!

gogglebot - May 23, 2018, 9:47 am

(May 22, 2018 09:02 AM)Phlox Wrote: [\[CITE\]](#) Fantastic script mate, keep up the good work!

Nice gravedig ;) Wont complain given I was pretty happy with this one

Cheers man, however should note as a few mentioned in replies, this was fixed at least in Win10 by an update shortly after this thread was made :(Unsure if that same update made it to Win8/7, you'd have to confirm for yourself using an up-to-date install.

Phlox - May 23, 2018, 10:38 am

If the script good it should be bumped to let others know this script exist in my view.

Erhan - May 26, 2018, 8:48 pm

I can use this script thank you!