

Forum:[Hack Forums](#)

Thread: [LF UAC bypass written in batch/vbs that works on all versions for upcoming AHK RAT](#)

johnsmith57365420 - February 16, 2023, 7:04 am

Hi, I'm creating an FUD RAT coded in AutoHotkey which includes an anti-virus killer (boots into safe mode, changes IMFO keys, deletes key dependencies, uninstalls using macros and/or social engineering) and will gain admin privileges using a UAC bypass in order to execute the anti-virus killer, it's effectively a short and simple downloader that can run any code written/changed within a GitHub repository, it doesn't contain any seemingly malicious code so it will hopefully stay FUD as long as certain requirements are met.

This has always been a dream of mine so I decided to start coding one all by myself - but I'm running into issues, I can't seem to find a UAC bypass that works on all Windows versions that with my limited coding knowledge would be able to integrate into an AutoHotkey script.

I was hoping to find a registry key manipulation exploit, a simple add/change shell registry key such as one I have found by creating an mscfile shell command key which is called by eventvwr.exe when mmc.exe loads, you can read about this on [enigma0x3 \(2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/\)](#)

I'm currently writing this on a Windows Server 2012 x64 VPS and the above method doesn't appear to work, I believe it would be had I tested it on a normal Windows 7/8/8.1/10/11 machine (can someone clarify this?)

So what I'm looking for is a UAC bypass that works on all Windows versions and is something that could be written in AHK (such as a batch or vbs script).

I found a program called UACMe on GitHub which includes up to 78 UAC bypass methods, however the only ones which are listed (under Keys) as unfixed and working from Windows 7 are ones which I don't believe can be coded in AutoHotkey or at least not with my limited coding skills, such as:

Spoiler ([Click to View](#)) 77. Author: Arush Agarampur

Type: DLL Hijack

Method: IFileOperation

Target(s): \system32\mmc.exe

Component(s): atl.dll

Implementation: ucmAtlHijackMethod

Works from: Windows 7 RTM (7600)

Fixed in: unfixed :see_no_evil:

How: -

* Code status: added in v3.6.4

If anyone could help it would be greatly appreciated.

moom825 - February 16, 2023, 10:00 am

take a look at the cmstp uacbypass, its worked on most version of windows 10+ (i havent tested on win 7).

blyat1337 - February 16, 2023, 9:51 pm

CMSTP UAC bypass is most commonly used in new malware.

However, it can also get easily detect if an antivirus hooks CoGetObject.

My tip is to go lower, CoGetObject is merely a wrapper, check out reactos.

Also, not sure if you are aware but : You can kill most antiviruses if you have admin rights by abusing installers and patching some of them on the fly so there is no real reason to go safe-mode if you are targeting such. (AV's such as malware bytes, avira, eset etc.)

mukku - February 16, 2023, 10:45 pm

sir how to cctv camera hacked please tell me

jmark7 - February 18, 2023, 1:28 pm

(Feb 16, 2023 10:51 PM)blyat1337 Wrote: [\[CITE\]](#) CMSTP UAC bypass is most commonly used in new malware.

However, it can also get easily detect if an antivirus hooks CoGetObject.

My tip is to go lower, CoGetObject is merely a wrapper, check out reactos.

Also, not sure if you are aware but : You can kill most antiviruses if you have admin rights by abusing installers and patching some of them on the fly so there is no real reason to go safe-mode if you are targeting such. (AV's such as malware bytes, avira, eset etc.)

am not an experienced developer but from what I need in new AV you can even uninstall them from uninstaller.

there is a separate app available on there site to uninstall it.