

Forum:[Hack Forums](#)

Thread: [Is this a good idea? \(FUD Antivirus Disabler\)](#)

Takehito Morokuzu - January 28, 2019, 2:46 pm

[Video: <https://www.youtube.com/watch?v=0kt7ikfXfdY&feature=youtu.be>]

This software I coded can disable any antivirus or antimalware software, while being completely undetected.

The only problem is, the disable process only works in safe mode, so the software needs to reboot the computer in safemode then reboot back to normal mode.

Is this a good idea? I feel like it could be useful for certain targets, but not all.

EDIT: It is currently coded in batch but can be converted to almost any language easily.

Goldmouth - January 28, 2019, 4:37 pm

(Jan 28, 2019 03:46 PM)-yuno gasai- Wrote: [\[CITE\]](#) This software I coded can disable any antivirus or antimalware software, while being completely undetected.

The only problem is, the disable process only works in safe mode, so the software needs to reboot the computer in safemode then reboot back to normal mode.

Is this a good idea? I feel like it could be useful for certain targets, but not all.

EDIT: It is currently coded in batch but can be converted to almost any language easily.

Very nice man. This is diff very useful and even if not successful 100% of the time its still should work. Let me ask you, Does it work with NOD32? ? ?

I.M.P - January 28, 2019, 4:54 pm

I tried making something very similiar specifically for windows defender that used the same values yours does. But we already discussed this :)

M2K - January 29, 2019, 12:38 am

Dude, I can say that that's super amazing really.

Does it work on windows 10 and servers?? if so im willing to pay for that script

CapsLo0ck - January 29, 2019, 12:44 am

(Jan 29, 2019 01:38 AM)M2K. Wrote: [\[CITE\]](#) Dude, I can say that that's super amazing really.

Does it work on windows 10 and servers?? if so im willing to pay for that script

hello

you need crypter or fud ?

Takehito Morokuzu - January 29, 2019, 1:54 am

(Jan 28, 2019 05:37 PM)?HOSTAH? Wrote: [\[CITE\]](#) Very nice man. This is diff very useful and even if not successful 100% of the time its still should work. Let me ask you, Does it work with NOD32? ? ?

Yes it does. I've only added like 10 av and it works on all of them, I just need to add support for more of them.

(Jan 28, 2019 05:54 PM)Atroxcity Wrote: [\[CITE\]](#) I tried making something very similar specifically for windows defender that used the same values yours does. But we already discussed this :)

(Jan 29, 2019 01:38 AM)M2K. Wrote: [\[CITE\]](#) Dude, I can say that that's super amazing really.

Does it work on windows 10 and servers?? if so im willing to pay for that script
It works perfect on windows 10, no idea if it works on servers but I don't see why it wouldn't.

(Jan 29, 2019 01:44 AM)CapsLo0ck Wrote: [\[CITE\]](#) hello
you need crypter or fud ?
FUD at the time of writing

enmafia2 - January 29, 2019, 2:21 am

I won't use this personally but I would be interested in the method just for the knowledge.
Would it be possible to know how you achieved this?

Thanks and good job

Takehito Morokuzu - January 29, 2019, 2:56 am

(Jan 29, 2019 03:21 AM)enmafia2 Wrote: [\[CITE\]](#) I won't use this personally but I would be interested in the method just for the knowledge.

Would it be possible to know how you achieved this?

Thanks and good job

Image File Execution Options ?

It requires safe mode because the AV drivers don't block it in safe mode for some reason ?

But this works on every single av i tested on, the exception being malwarebytes, however all I had to do was disable malwarebytes's safe mode boot, which isn't blocked and that allowed me to add it into IFEO. ?

Jacque Fresco - January 29, 2019, 11:41 am

Hey cool ill approached the same <https://hackforums.net/showthread.php?tid=5878369>
it also worked by starting up into safemode, displaying a SE message and reboot.

However here is a tip, a couple of Antiviruses have a msi installer, just check the registry HKLM\...\Uninstall for their uninstall string and run it Silently (like MsiExec.exe", "/x {FD15FD84-2C5A-4C5F-BE83-79E2459856CA} /passive REBOOT=R) if thats not possible then create a new Account, Log it on and make Mouse clicks trough the uninstaller. Just dont ask me for a script on howto logon a different User (no RunAs doesnt do the job because the Gui will show up on the current user and simple hiding is risky also because some msi uninstaller popup a webpage too ("sadly that you uninstalled 'Antivirus'. State us why")) because i rage quiet google etc. after 2 days of searching for a solution.

Also to counter the suspicion fact, steal the Icon of the Antivirus and implement it into your own application (automatically of course) and let it display. Alot of users just watch for the Icon and think they are safe.

Edge of Nowhere - January 29, 2019, 11:45 am

i personally think that disabling any AV will raise some suspicions.

I.M.P - January 29, 2019, 12:28 pm

(Jan 29, 2019 01:23 PM)JSanti13 Wrote: [\[CITE\]](#) You're a stupid son of a bitch, aren't you?

Disabling AV will only prevent detection, since there's no AV to detect you. It's this think called logig

and maybe you should use it.

yea but notifications to the user "HEY YOUR ANTIVIRUS MIGHT NOT BE WORKING" will cause suspicion I think that's what he means

JSanti13 - January 29, 2019, 12:30 pm

(Jan 29, 2019 01:28 PM)Atroxcity Wrote: [\[CITE\]](#) yea but notifications to the user "HEY YOUR ANTIVIRUS MIGHT NOT BE WORKING" will cause suspicion I think that's what he means

Thanks for the response. We greatly appreciate your feedback and will use it to continue to improve our service. Have a nice day!

I.M.P - January 29, 2019, 12:30 pm

(Jan 29, 2019 01:30 PM)JSanti13 Wrote: [\[CITE\]](#) Thanks for the response. We greatly appreciate your feedback and will use it to continue to improve our service. Have a nice day!
what? ?

Takehito Morokuzu - January 29, 2019, 12:31 pm

(Jan 29, 2019 01:28 PM)Atroxcity Wrote: [\[CITE\]](#) yea but notifications to the user "HEY YOUR ANTIVIRUS MIGHT NOT BE WORKING" will cause suspicion I think that's what he means

I have not gotten that message after disabling it on my end. I can block any exe file I want so I should be able to block that message if it's related to an exe file that is running.

I.M.P - January 29, 2019, 12:32 pm

(Jan 29, 2019 01:31 PM)-yuno gasai- Wrote: [\[CITE\]](#) I have not gotten that message after disabling it on my end. I can block any exe file I want so I should be able to block that message if it's related to an exe file that is running.

oh interesting now that's pretty good ?

Jacque Fresco - January 29, 2019, 12:32 pm

(Jan 29, 2019 01:23 PM)JSanti13 Wrote: [\[CITE\]](#) You're a stupid son of a bitch, aren't you?

Disabling AV will only prevent detection, since there's no AV to detect you. It's this thing called logiG and maybe you should use it.

(Jan 29, 2019 01:28 PM)Atroxcity Wrote: [\[CITE\]](#) yea but notifications to the user "HEY YOUR ANTIVIRUS MIGHT NOT BE WORKING" will cause suspicion I think that's what he means

(Jan 29, 2019 01:30 PM)JSanti13 Wrote: [\[CITE\]](#) Thanks for the response. We greatly appreciate your feedback and will use it to continue to improve our service. Have a nice day!

what a 100 to 0 ... haha this got me laughing very good answer :D

I.M.P - January 29, 2019, 12:33 pm

(Jan 29, 2019 01:32 PM)Jacque Fresco Wrote: [\[CITE\]](#) what a 100 to 0 ... haha this got me laughing very good answer :D

I felt confused as well ? pretty funny though

Takehito Morokuzu - January 29, 2019, 12:33 pm

(Jan 29, 2019 12:41 PM)Jacque Fresco Wrote: [\[CITE\]](#) Hey cool ill approached the same

<https://hackforums.net/showthread.php?tid=5878369>

it also worked by starting up into safemode, displaying a SE message and reboot.

However here is a tip, a couple of Antiviruses have a msi installer, just check the registry HKLM\...\Uninstall for their uninstall string and run it Silently (like MsiExec.exe"/x {FD15FD84-2C5A-4C5F-BE83-79E2459856CA} /passive REBOOT=R) if that's not possible then create a new Account, Log it on and make Mouse clicks through the uninstaller. Just don't ask me for a script on how to logon a different User (no RunAs doesn't do the job because the Gui will show up on the current user and simply hiding is risky also because some msi uninstaller popup a webpage

too ("sadly that you uninstalled 'Antivirus'. State us why")) because i rage quiet google etc. after 2 days of searching for a solution.

Also to counter the suspicion fact, steal the Icon of the Antivirus and implement it into your own application (automatically of course) and let it display. Alot of users just watch for the Icon and think they are safe.

Interesting, I should make it detect what AV is installed and adapt. I think many uses won't even notice the AV is not there, many people use defender and that does not have a tray icon.

JSanti13 - January 29, 2019, 12:35 pm

(Jan 29, 2019 01:32 PM)Jacque Fresco Wrote: [\[CITE\]](#) what a 100 to 0 ... haha this got me laughing very good answer :D

(Jan 29, 2019 01:33 PM)Atroxcity Wrote: [\[CITE\]](#) I fell confused as well ? pretty funny though I've been banned a few times recently and noticed nobody was posting in the threads I was following. I've also been messing with the HF mods a bit.

I wanted to make sure the HF admins weren't messing with me back and showing static content. It was a leap, but better safe than sorry.

Think of it as a human verification for an entire forum - post polarizing messages and see who responds.

Takehito Morokuzu - January 29, 2019, 12:38 pm

(Jan 29, 2019 01:35 PM)JSanti13 Wrote: [\[CITE\]](#) I've been banned a few times recently and noticed nobody was posting in the threads I was following. I've also been messing with the HF mods a bit.

I wanted to make sure the HF admins weren't messing with me back and showing static content. It was a leap, but better safe than sorry.

Think of it as a human verification for an entire forum - post polarizing messages and see who responds.

Sorry bud I honestly have no idea what you're talking about. You got banned and you thought HF staff were messing with you? They ain't got time for that lol

Jacque Fresco - January 29, 2019, 12:41 pm

(Jan 29, 2019 01:33 PM)-yuno gasai- Wrote: [\[CITE\]](#) Interesting, I should make it detect what AV is installed and adapt. I think many uses won't even notice the AV is not there, many people use defender and that does not have a tray icon.

Yeah adaption is needed, write for every AV a different Module let it then get executed by a controller. Why? Because all the different Antiviruses are blocking different things and have different heuristics. Avira for example blocks editing the registry on some points.. so i uninstalled all the drivers, killed all possible processes and let the program then do the edit.. but it did not work. then i found an article which showed that Avira is running some parts of the Windows os in a virtual machine (dont ask, i cant explain that anymore). So what i mean with different modules is that some code gets more likely detected than another, another which you dont even use for this specific av but it is build in for another av. You get what i mean?

However im not sure what you saw there on the win10 machine, may thats language specific (i wonder if and why) because on my machines with the defender as main AV it clearly shows an tray icon.

Also it depends on the country, atleast in the country i live in i havent seen anyone without a Antivirus.

JSanti13 - January 29, 2019, 12:51 pm

(Jan 29, 2019 01:50 PM)-yuno gasai- Wrote: [\[CITE\]](#) This isn't the thread to argue on. Either take it to PMs or IM.

You realize I'm on my third account today, right? You saw me mention that before? If that's the case, then you already know the rules are irrelevant to me.

In any case,

Thanks for the response. We greatly appreciate your feedback and will use it to continue to improve our service. Have a nice day!

Takehito Morokuzu - January 29, 2019, 12:53 pm

(Jan 29, 2019 01:41 PM)Jacque Fresco Wrote: [\[CITE\]](#) Yeah adaption is needed, write for every AV a different Module let it then get executed by a controller. Why? Because all the different Antiviruses are blocking different things and have different heuristics. Avira for example blocks editing the registry on some points.. so i uninstalled all the drivers, killed all possible processes and let the program then do the edit.. but it did not work. then i found an article which showed that Avira is running some parts of the Windows os in a virtual machine (dont ask, i cant explain that anymore). So what i mean with different modules is that some code gets more likely detected than another, another which you dont even use for this specific av but it is build in for another av. You get what i mean?

However im not sure what you saw there on the win10 machine, may thats language specific (i wonder if and why) because on my machines with the defender as main AV it clearly shows an tray icon.

Also it depends on the country, atleast in the country i live in i havent seen anyone without a Antivirus.

Less tech savvy users likely won't install an antivirus. Anyway I can check my VM again but I think I will still block all the antivirus exes so that the user can't install another. Anyway I will check if possible which avs can be silently uninstalled without several reboots. Thanks for your advice

Jacque Fresco - January 29, 2019, 12:54 pm

However im planning to go into this Project again and finish it. May we could work together and Release it as a Anti Anti Virus tool. Of course only for users who have problems uninstalling their Anti Virus ?

EDIT: may in your country they are less likely todo that. But thats not the point we want to get rid of AV's

Your Welcome ?

Katyuska - January 30, 2019, 12:28 am

My opinion is its a great idea. Definitely would be useful in a few different situations. I like the idea of having this kind of tool for special cases.