

Forum:[Hack Forums](#)

Thread: [how to bypass antivirus for a metasploit payload?](#)

BrunoB - June 14, 2019, 7:59 am

Hi,
I'm trying to get a meterpreter exe through windows 10 AV.
I tried using shellter witch unfortunately doesn't work. The windows AV gets it.
Any suggestions on how I could get this through?

P.S. I'm new to this so I don't have much experience...

__Digital__ - June 14, 2019, 10:52 am

(Jun 14, 2019 07:59 AM)BrunoB Wrote: [\[CITE\]](#) Hi,
I'm trying to get a meterpreter exe through windows 10 AV.
I tried using shellter witch unfortunately doesn't work. The windows AV gets it.
Any suggestions on how I could get this through?

P.S. I'm new to this so I don't have much experience...

The best way to get your payload to the machine is to use a downloader. The downloader would interact/use the builtin cmdlets for defender to tell defender what to do instead of its default settings. Once you have executed the correct cmdlets your file would be downloaded and executed which would bypass defender if done correctly.

BrunoB - June 14, 2019, 11:21 am

(Jun 14, 2019 10:52 AM)__Digital__ Wrote: [\[CITE\]](#) The best way to get your payload to the machine is to use a downloader. The downloader would interact/use the builtin cmdlets for defender to tell defender what to do instead of its default settings. Once you have executed the correct cmdlets your file would be downloaded and executed which would bypass defender if done correctly. what downloader would you recommend?

Faith Connors - June 14, 2019, 11:25 am

(Jun 14, 2019 11:21 AM)BrunoB Wrote: [\[CITE\]](#) what downloader would you recommend?
the one you write yourself

come on, its literally a single line of powershell code

javinzplayer - June 14, 2019, 12:40 pm

You can use some of the evasion techniques like [Veil Evasion](#) or use any other EXE cryptots like Themida, Enigma, and others.

__Digital__ - June 14, 2019, 1:28 pm

(Jun 14, 2019 11:21 AM)BrunoB Wrote: [\[CITE\]](#) what downloader would you recommend?
As Faith told you before i could the one you make yourself then you know its clean and not dirty.

W32.DisTrack - June 15, 2019, 7:31 am

(Jun 14, 2019 11:25 AM)Faith Connors Wrote: [\[CITE\]](#) the one you write yourself

come on, its literally a single line of powershell code
Yeah, any skid can do that ;)

Faith Connors - *June 15, 2019, 10:58 am*

(Jun 15, 2019 07:31 AM)W32.DisTrack Wrote: [\[CITE\]](#) Yeah, any skid can do that ;)
i mean im a skid and i can do it :P

W32.DisTrack - *June 15, 2019, 11:39 am*

(Jun 15, 2019 10:58 AM)Faith Connors Wrote: [\[CITE\]](#) i mean im a skid and i can do it :P
Exactly my point lol. I'm not sure why the skids haven't hopped on the powershell train.