

Forum:[Hack Forums](#)

Thread: [how make meterpreter undetected](#)

nitrogen_oxide - June 28, 2021, 8:14 am

hi,

I have trouble with meterpreter being always detected by windows defender, tried encoding with x86_shikata_ga_nai, but that still gets detected, injecting it into another app using shellter is not reliable and sometimes still gets detected.

anyone know how to make a virus fully undetectable?

Elweth - June 29, 2021, 1:30 am

You can't use the existing tools afaik, AVs have updated to handle them. Try writing your own code to lower detection.

itsonlyparsa - July 16, 2021, 8:30 am

Hello sry i don't know where to contact u, can u check the contract i started ?

linkinpork - July 17, 2021, 5:05 pm

(Jun 28, 2021 08:14 AM)nitrogen_oxide Wrote: [\[CITE\]](#) hi,

I have trouble with meterpreter being always detected by windows defender, tried encoding with x86_shikata_ga_nai, but that still gets detected, injecting it into another app using shellter is not reliable and sometimes still gets detected.

anyone know how to make a virus fully undetectable?

Hi,

Meterpreters are so common and so easy to use that Windows 10 is almost totally immune to it.

As an alternative you can try to use payload/generic/shell_reverse_tcp if it helps, as it has a much smaller footprint. Although there's no guarantee that it's undetectable.

Here's the description of the payload

https://www.rapid7.com/db/modules/payload/generic/shell_reverse_tcp/

Cheers!

ARX134 - July 19, 2021, 11:33 am

Nowadays it is difficult there will be new updates thats make hard to hack other computers

DI?E - July 20, 2021, 5:45 am

(Jul 17, 2021 05:05 PM)linkinpork Wrote: [\[CITE\]](#) Hi,

Meterpreters are so common and so easy to use that Windows 10 is almost totally immune to it.

As an alternative you can try to use payload/generic/shell_reverse_tcp if it helps, as it has a much smaller footprint. Although there's no guarantee that it's undetectable.

Here's the description of the payload

https://www.rapid7.com/db/modules/payload/generic/shell_reverse_tcp/

Cheers!

Yeah even that one is detected at runtime as well. I would say though to the OP there are plenty of good code on GitHub to get you in the right direction. You can go search some of my posts.

johnd9601 - August 6, 2021, 3:00 pm

The best way is only to generate your shellcode with meterpreter and run it through a custom loader with c or csharp

You can find many examples from Github that you can customize on your own

Cyr0x - September 1, 2021, 4:15 pm

Windows 10 is far from being immune to meterpreter. First of all, forget about normal payloads or encryption routines that are already integrated or used by common tools like donut or sgn. AV already know them very well...

Write your own packers with C # /. Net or work with process hollowing. Use files that are relevant for the operating system and are therefore not scanned so intensively by the AV (e.g. svchost). Ideally, you do not write any files to the hard drive and load the payload directly into the memory via reflective loading. For transferring the payload check out LOLBAS.

webdev77 - September 1, 2021, 4:26 pm

(Sep 1, 2021 04:15 PM)Cyr0x Wrote: [\[CITE\]](#) Use files that are relevant for the operating system and are therefore not scanned so intensively by the AV (e.g. svchost). Ideally, you do not write any files to the hard drive and load the payload directly into the memory via reflective loading. For transferring the payload check out LOLBAS.

Attempting to use a system file isn't not a great idea since all of those are in fact verifiable by the OS. Windows Defender of all things will flag any process using the name of a system process if it isn't a legitimate system process.

Trying to load things directly into memory raises all kinds of red flags for AV software. If a typical user program wouldn't do that thing, your malicious code should not do such things either. Anything unusual tends to stand out.

T r a p p y - September 2, 2021, 5:52 pm

Its easy to do fud with meterpreter on kali, very easy