

Forum:[Hack Forums](#)

Thread: [Bypass antivirus -- repack/spoof executables?](#)

skillz0r1337 - February 27, 2024, 11:54 pm

Hi guys!

I'm studying pentesting right now (no BS lol). We have many tasks during this education, but a thing I notice is that Windows Defender acts upon some tools that I'm trying to use.

For instance nc.exe (Netcat) and also WinPEAS (Enumeration tool). Is it possible to "repack" or spoof these executables to bypass Windows defender?

Thanks

psickophant - February 28, 2024, 10:40 am

Ahh... Windows Defender. The short answer to your questions is yes. This can be a fairly advanced topic though. First, you should research more about how antivirus/windows defender works. You need to understand the techniques used by WD in order to get around them. There are a variety of different ways commonly found to beat WD. Encryption, obfuscation, patching, in-memory execution, packing, etc. Currently, I think most people use a paid cryptor to encrypt the payloads that are then decrypted prior to execution. There are a ton of free cryptors out there but sadly most are detected now. Paid cryptors are the way to go. I would recommend learning how to code your own cryptor too. You will learn a ton about the topic doing so. Good luck!!

DramaKing - February 28, 2024, 12:01 pm

(Feb 28, 2024 12:54 AM)skillz0r1337 Wrote: [\[CITE\]](#) Hi guys!

I'm studying pentesting right now (no BS lol). We have many tasks during this education, but a thing I notice is that Windows Defender acts upon some tools that I'm trying to use.

For instance nc.exe (Netcat) and also WinPEAS (Enumeration tool). Is it possible to "repack" or spoof these executables to bypass Windows defender?

Thanks

I would say that the simple answer is no. WD and other AVs don't check a file signature against the virus definitions and see if it matches or not. They search for signatures within a file and will trigger if anything within is malicious. Binder applications also get fingerprinted and will get quarantined regardless of what has been bound.

Using ncat should at least get you a shell, and you can try upgrading it to Meterpreter or doing a UAC bypass to be able to run the almighty 'Set-MpPreference' cmdlet. WinPEAS is nice for checking lots of exploits, but Metasploit has some privesc exploits, and there are others you can try like the one below.