

Forum:[Hack Forums](#)

Thread: [any RAT that can defeat/bypass/evade windows defender](#)

electro25 - August 4, 2024, 9:10 pm

hi guys i am trying to exploit my 2nd system using different kind of payloads/backdoor which can give me remote code execution i have just been trying with msfvenom but windows defender catches it and deletes it when i tried to download the payload using powershell script and injecting it in ram it resulted in muli/handler to stop after sending stager message . so can someone please nudge me in the right direction how to achieve that goal .

globalroot - August 5, 2024, 3:25 am

There is no malware which comes undetected by default.
You can use AMSI bypass techniques to evade defender.

DramaKing - August 5, 2024, 4:08 pm

(Aug 5, 2024 03:25 AM)globalroot Wrote: [\[CITE\]](#) There is no malware which comes undetected by default.

You can use AMSI bypass techniques to evade defender.
You know of any AMSI bypass techniques that bypass Defender?

globalroot - August 5, 2024, 5:21 pm

(Aug 5, 2024 04:08 PM)DramaKing Wrote: [\[CITE\]](#) You know of any AMSI bypass techniques that bypass Defender?

Yeah, the patching AmsiScanBuffer works

Byte Wizard - August 5, 2024, 5:45 pm

(Aug 4, 2024 09:10 PM)electro25 Wrote: [\[CITE\]](#) hi guys i am trying to exploit my 2nd system using different kind of payloads/backdoor which can give me remote code execution i have just been trying with msfvenom but windows defender catches it and deletes it when i tried to download the payload using powershell script and injecting it in ram it resulted in muli/handler to stop after sending stager message . so can someone please nudge me in the right direction how to achieve that goal .
Metasploit is too old and widely used to bypass antivirus
You would have to heavily obfuscate/crypt the payload or write your own which I would recommend
But since it is your system just turn of Defender and enjoy your remote access