

Forum:[Hack Forums](#)

Thread: [Is it the end of MSFVenom?](#)

sammich777 - March 13, 2020, 2:55 pm

So I got into hacking back when I was still in middle school and backtrack 4 had come out. Back then in the late 2000s it was trivial getting a meterpreter session on anyone and phishing them using either the file format exploits found inside metasploit or just zipping msfvenom exe payloads and sending them over email or myspace links. it was great. but it's not 2008 anymore sadly. With Windows 10 becoming the norm now and windows 7 now almost entirely gone even here in my country where most computers are out of date, we have to fight with defender.

Have to give it to Microsoft, they really stepped up their game when it comes to blocking malware on windows computers. seems unless your write your own unique malware your no longer able to reuse cheap or free malware like we were all able too back then. So that leaves the question... where does that put MSFVenom? I know most here would rather use a traditional windows rat but I really fell in love with the metasploit project after all these years using it as my main method of intrusion. specially the good old reverse tcp meterpreter payload.

Anyone here still use the metasploit payloads at all? if so, how are you dealing with Windows 10? I am able to bypass it for a while, given some functions will get my flagged like screenshot or sharescreen but it still have been very useful over the years and I don't know where I would be without it.

My main method of bypassing Defender has been using x86/shikata_na_gai but it seems like even that is almost always being flagged even when I compile my own exe loader for my shellcode. Are we seeing the end of msfvenom or am I just a total noob still? inb4 "just use a crypter bro" heuristic scanning... so? what do you guys think?