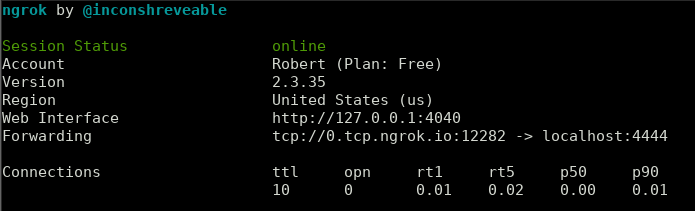
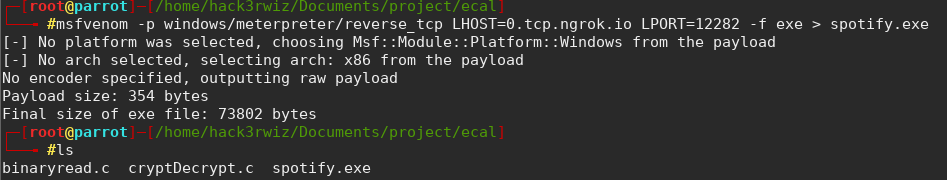
Crypter Implementation Document

**Step 1:** Set up NGROK port forwarding to receive connection directly from the internet to your local machine.

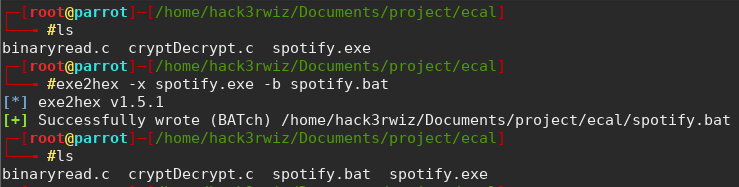




**Step 2:** Create a payload using msfvenom. (in this case: spotify.exe).



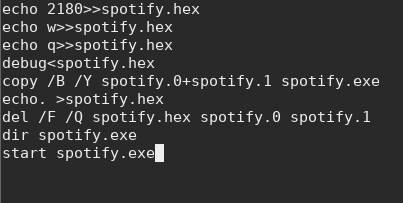
**Step 3: Convert .exe file to .bat file** (converting spotify.exe to spotify.bat)



**Step 4: Edit bat file.**  (in this case spotify.bat)



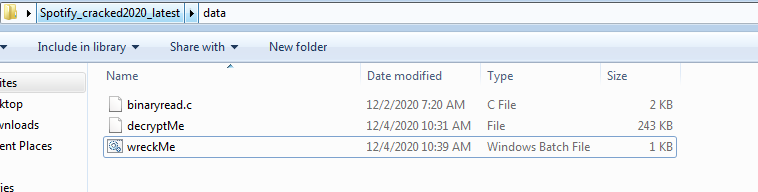
**Step 5: Adding** a statement “**start spotify.exe**” towards the end.



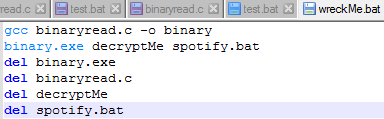
**Step 6: Encrypted “.bat file” and obtaining obfuscated “decryptMe” file.**   
(In this case: spotify.bat -------> decryptMe)



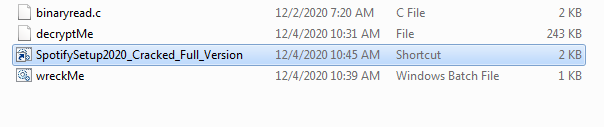
**Step 7) Transfer decryptMe along with binaryread.c** (the crypter) **to victim’s machine.**



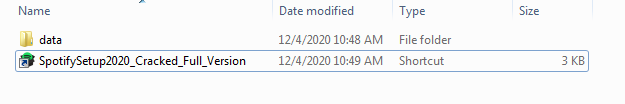
**Step 8: Create** **wreckMe.bat file to automate the infecting process.**



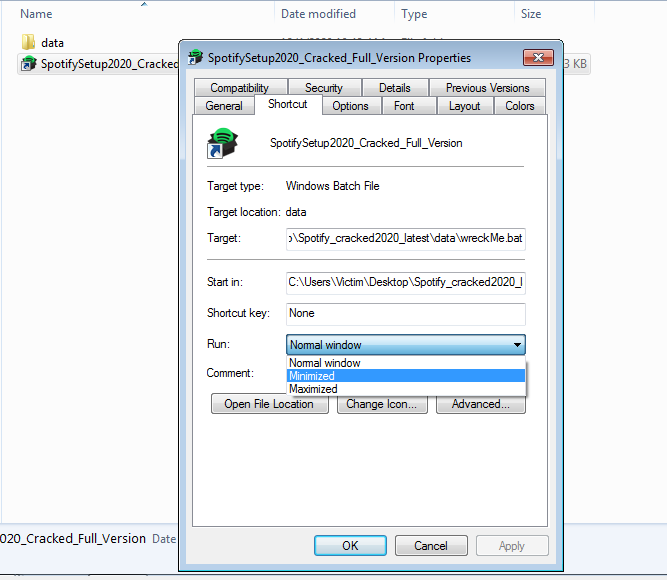
**Step 9: Create a shortcut for wreckMe.bat script.** (In this case SpotifySetup2020\_Cracked\_Full\_Version)



**Step 10: Change the icon of the shortcut file. This is part of social engineering. (All other files are kept hidden in the “data” directory.)**



**Step 11: Change the properties of shortcut file. By changing the “Run” to Minimized, when the victim opens it, the execution will start in minimized mode, making it stealthier.**



**Step 12) When victim runs the shortcut file, the attacker obtains a meterpreter session on his machine that is listening for connections. NGROK forwards the reverse tcp connection over the internet to the attacker’s machine.**

