# Embed A Malicious Executable in a Normal PDF or EXE

medium.com/@sam.rothlisberger/embed-a-malicious-executable-in-a-normal-pdf-or-exe-81ee5339707e

Sam Rothlisberger 20 января 2024 г.

## DISCLAIMER: Using these tools and methods against hosts that you do not have explicit permission to test is illegal. You are responsible for any trouble you may cause by using these tools and methods.

Sam Rothlisberger

Today we're going to show how to create a malicious executable that looks like a PDF, word doc, or web browser executable with the functionality of the normal file/program, but also our embedded malicious executable. To do this, we are going to use WinRaR which can be downloaded here:

## WinRAR archiver, a powerful tool to process RAR and ZIP files

### WinRAR is a Windows data compression tool that focuses on the RAR and ZIP data compression formats for all Windows…

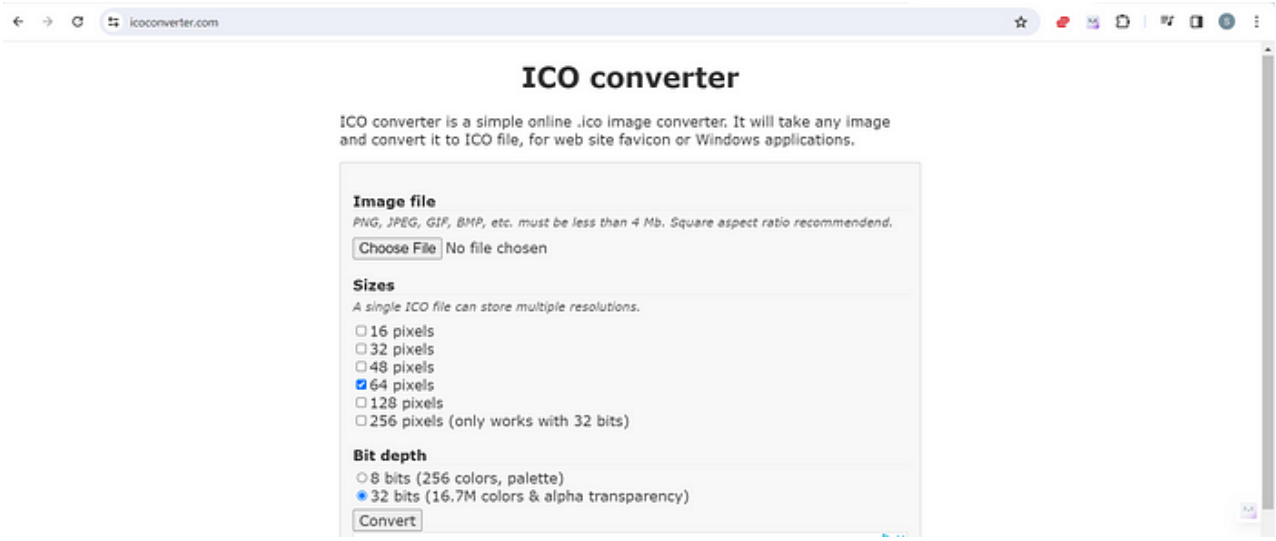
www.rarlab.com

We're going to assume we already crafted our malicious executable that will do something on the victim host or send us a reverse shell. The following are the steps for creating our file that looks legit:

1. Find an icon PNG for what you want your malicious executable to look like using In this example we are using chrome, but you can search any file type logo. Click 'Download PNG'.

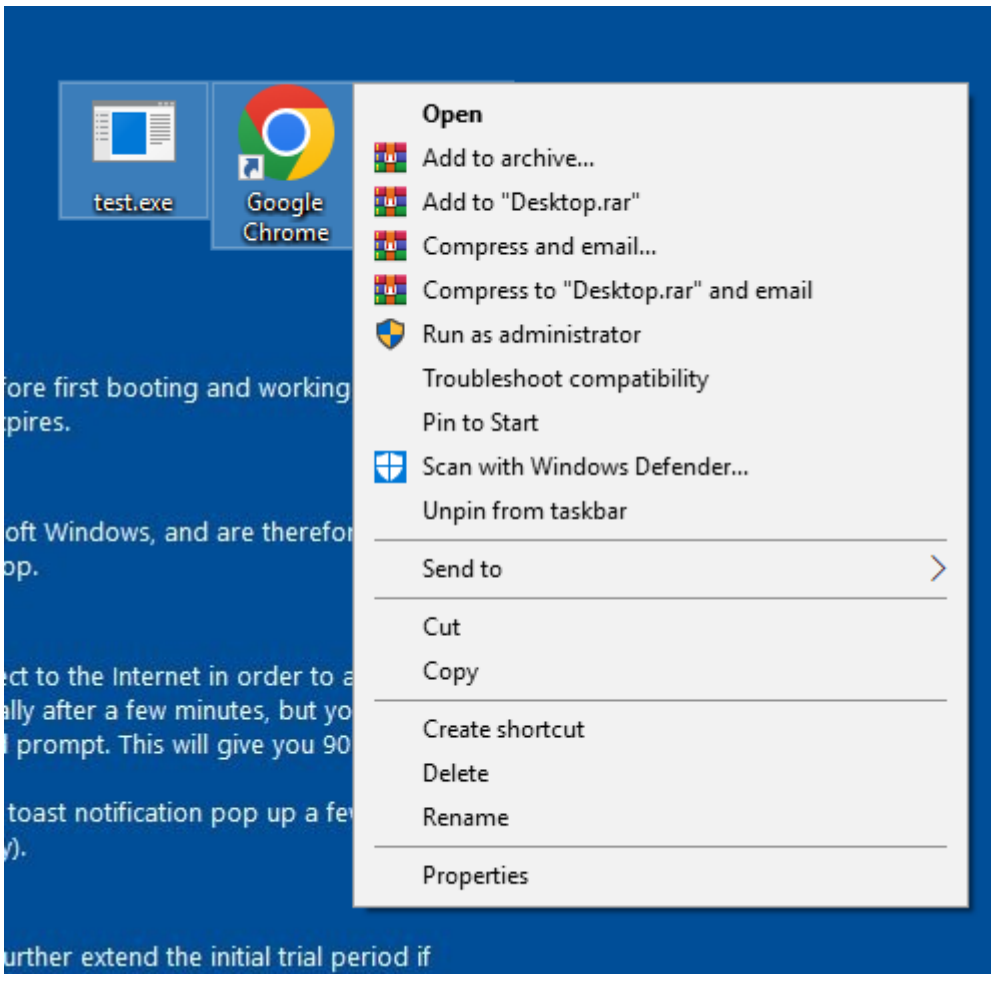
iconfinder.com

2. Covert the icon PNG to a .ico file using https://iconconverter.com. Upload the previous PNG and click 'Convert'.

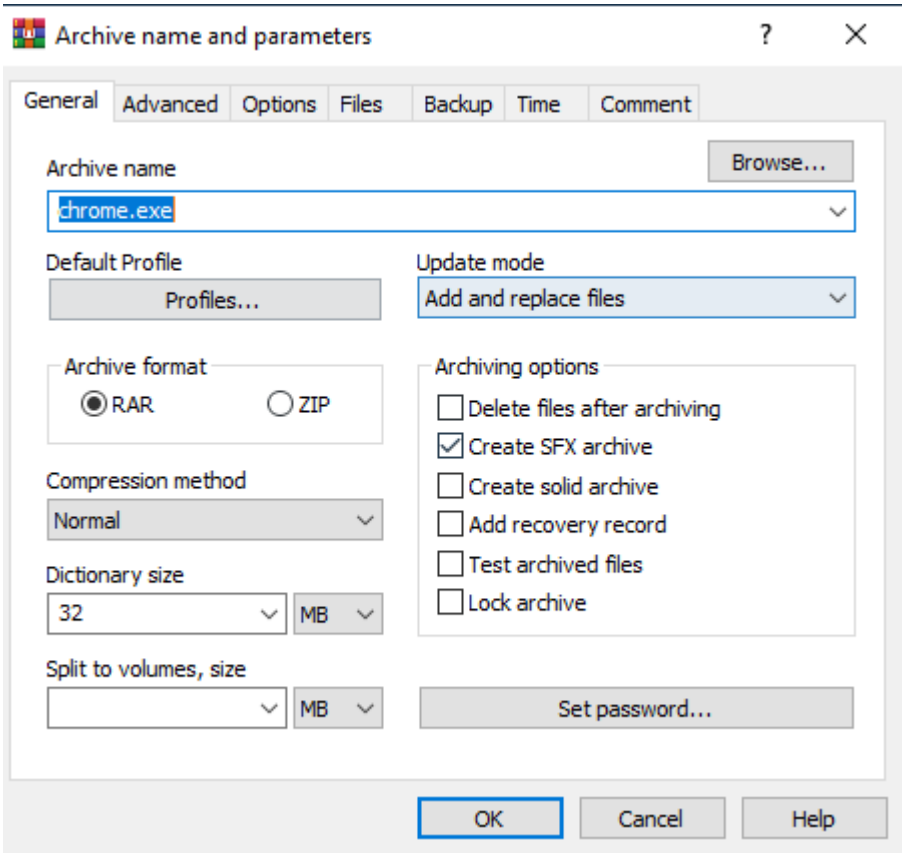



icoconverter.com

3. On your desktop select and right click the real chrome browser exe (in my case) and the malicious executable and select ‘Add to Archive…’ to create combined archive.




The Archive file name is just going to be chrome.exe to look legit. Make sure ‘Create SFX archive’ is checked.

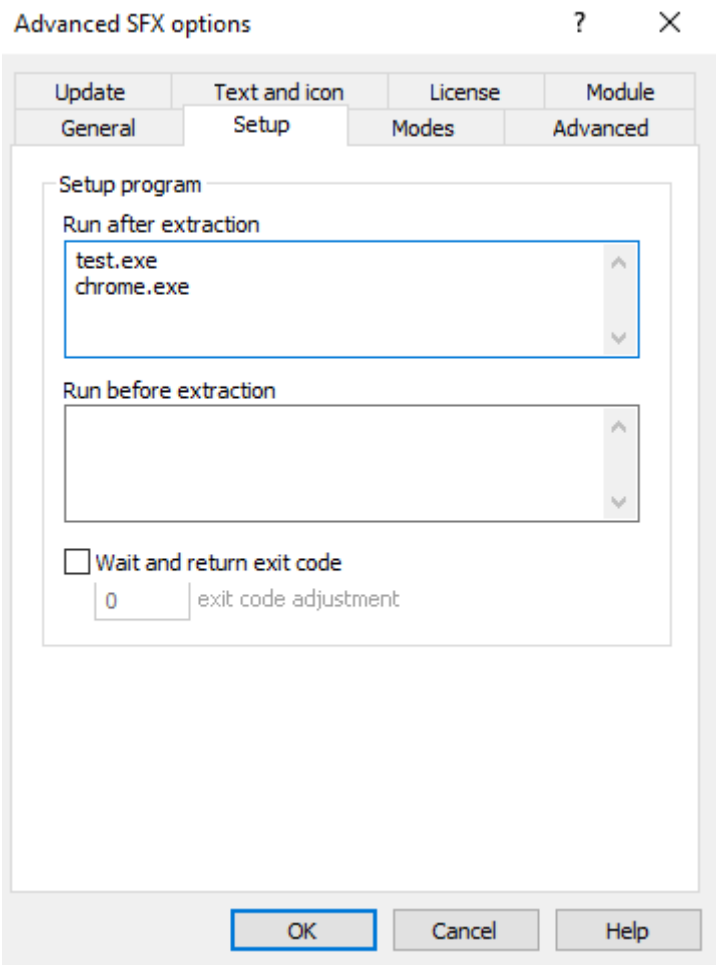



Click Advanced > SFX options > Setup and input the following:

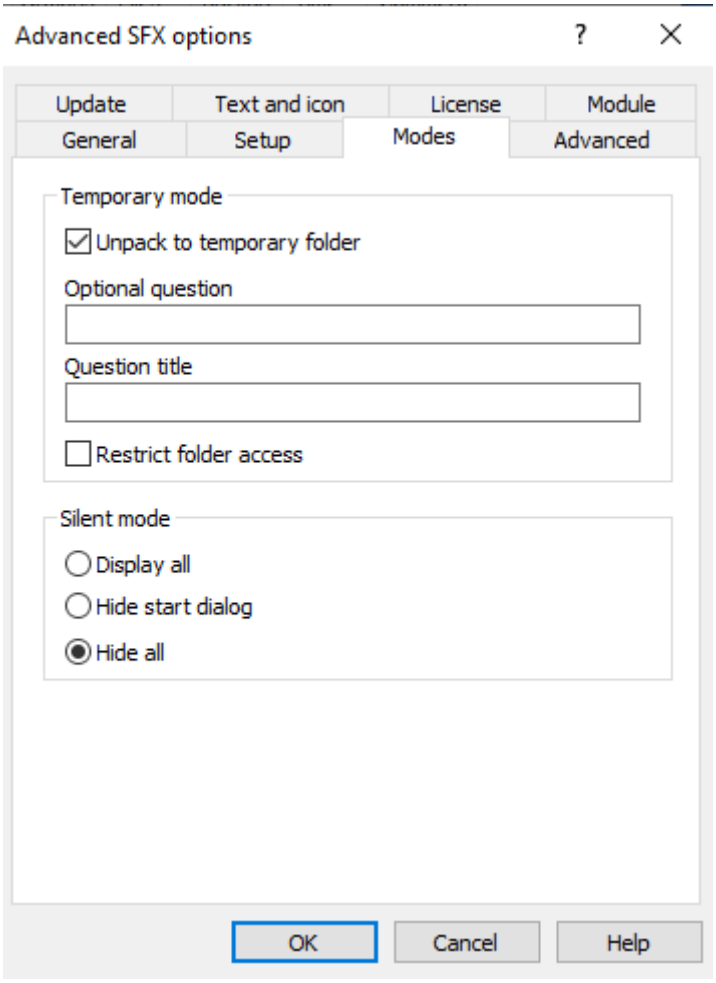
After entering the above parameters, click ‘ok’ and the archive called chrome.exe will pop up on the Desktop with the correct chrome icon. Double clicking on chrome.exe will execute my malicious executable and also open a browser tab like normal. Nothing else is needed to bypass Defender when executing our exe with another non-malicious exe so the job is done.

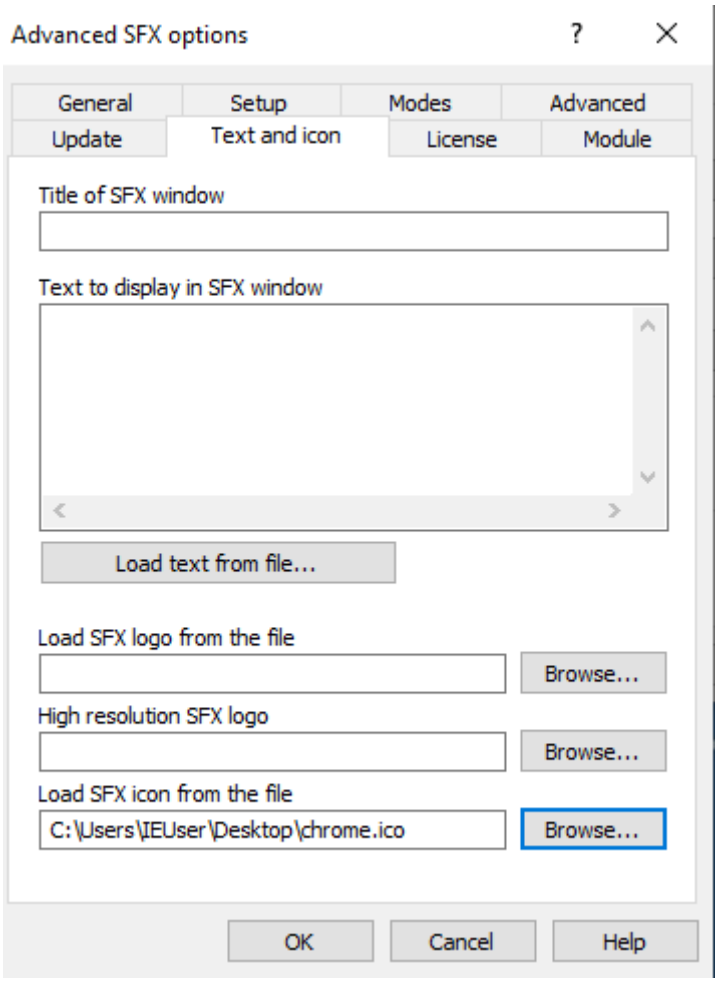
4. (OPTIONAL- **If using another file type other than exe like PDF**) We are going to use Right-To-Left-Override (RTLO) to change the created archive to look like a PDF on the desktop but execute as an EXE. Right-To-Left Override (RTO or RTLO) is a Unicode non-printing character used to write languages read in the right-to-left manner. It takes the input and literally just flips the text the other way round.

Let’s change the file name to something that would look semi-normal flipped around like Reflexe.pdf. We will insert our Unicode so that it looks like Refl[Invisible Unicode stuff]exe.pdf on the victim desktop, but is actually Refl[invisible Unicode stuff]fdp.exe.

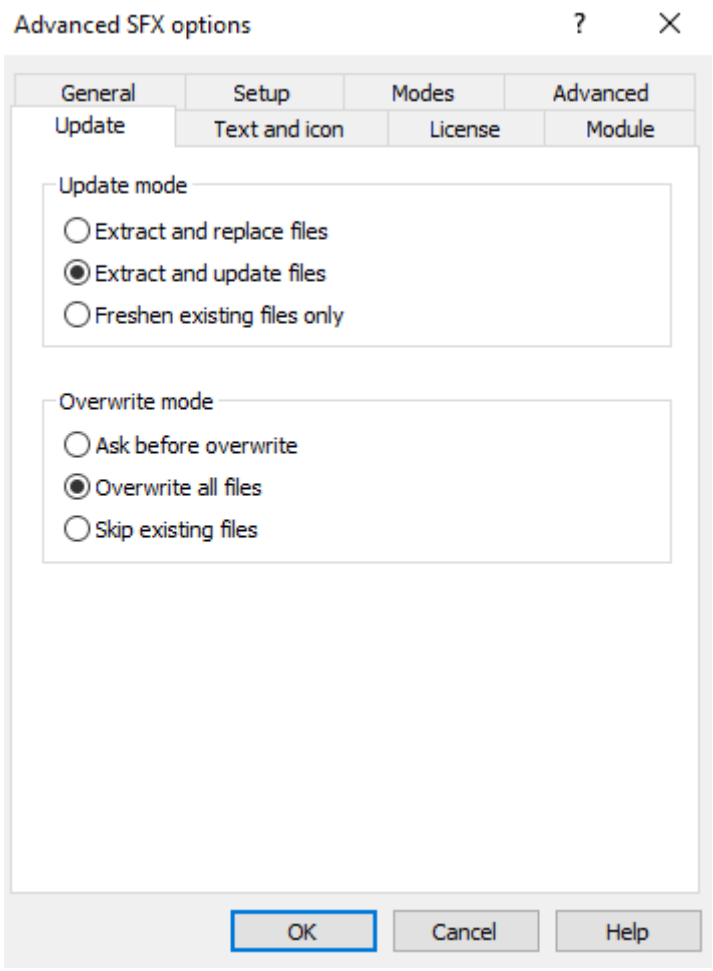


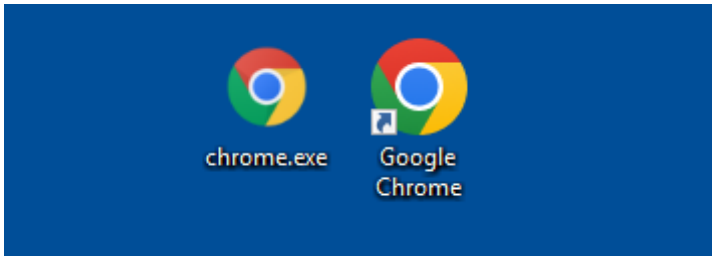

Enter test.exe (your malicious exe) and legitimate chrome.exe (program to open after executing malicious exe)


Advanced SFX options
Update
Text and icon
License
Module
General
Setup
Modes
Advanced
Temporary mode
Unpack to temporary folder
Optional question
Question title
Restrict folder access
Silent mode
Display all
Hide start dialog
Hide all
OK
Cancel
Help




Input file icon

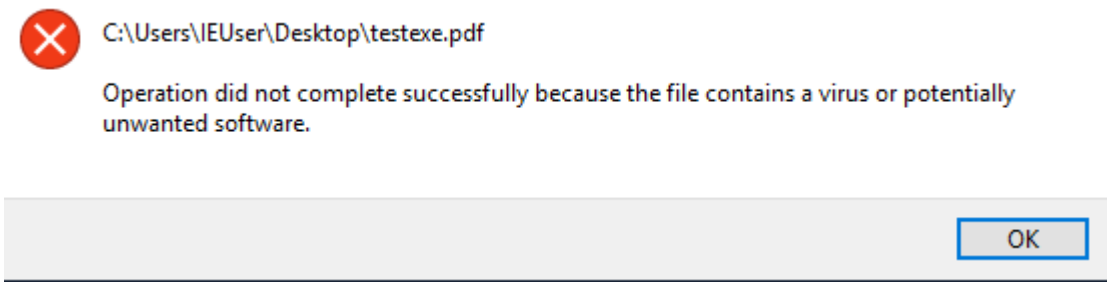



Malicious Chrome next to real Chrome


Open the Character Map app on Windows and check the ‘Advanced View’ box. In the ‘Go to Unicode’ option, type in 202E. Hit the ‘Select’ and ‘Copy’ buttons respectively and edit the file name of the WinRaR archive we created. You enter the file name Refl[CTRL+ v]fdp.exe and then go back and paste the Unicode where specified. The file should then change to Reflexe.pdf as soon as you hit paste.

But we have a problem — Because this is a known file type (.pdf) that is initiating an executable, it is flagged by windows defender very quickly.



One way to get around this is using Homoglyph's. At the end of the day, we only want this to look like a PDF to the user, so how likely is that they'll catch that one letter looks alittle different? I used this resource to manually test what Defender would flag:

## Homoglyph Attack Generator

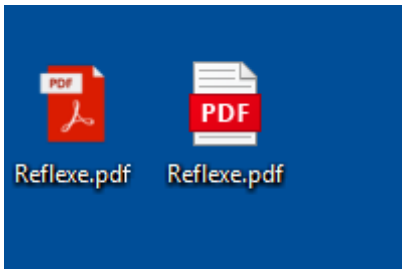
### Irongeek's Information Security site with tutorials, articles and other information.

www.irongeek.com

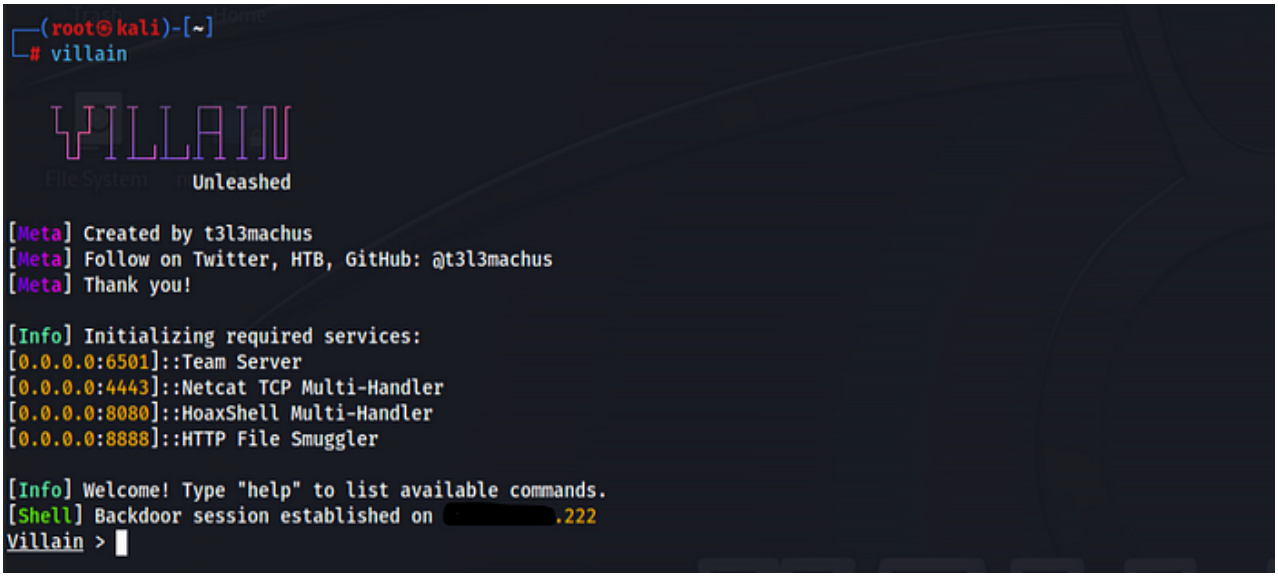
I focused on the letters p, d, and f to see if I could swap any out that wouldn't be noticed and I found this variation of 'f' that looked suitable. I swapped the Homoglyph 'f' with the normal 'f' in the name Refl**f**dp.exe and then inserted the RTLO right before it like before to create Reflexe.pd**f** which should give a different signature to defender:

Sweet, you can't (I cant..) tell the difference by looking at it! With my new .pdf extension, Windows Defender actually started a scan before the pdf opening, let it open, and then quarantined my PDF file acouple seconds later. However, this was after my malicious executable initiated the reverse shell. In my case, I receive a netcat shell through Villain on my attacker machine:)


Homoglyph 'f'




File name with fake 'f' vs File name with real 'f'




Now we just social engineer the victim to download and open this Reflexe.pdf or chrome.exe on their Windows host. I hope you enjoyed this post!