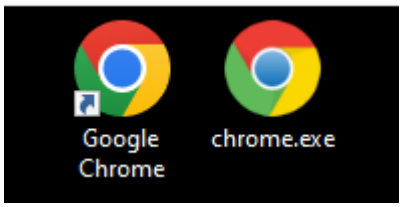
THIS IS FOR EDUCATION PURPOSE ONLY

Step by step: Embedding a Malware Executable into a Legitimate PDF or EXE



HAZWAN JAAFAR
28-10-2024

Disclaimer:

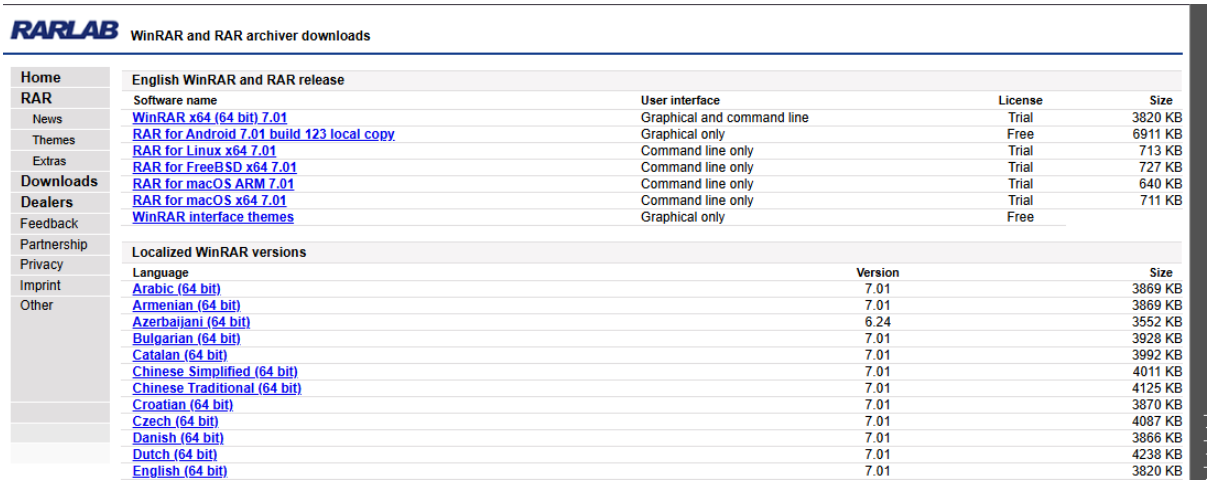
Unauthorized use of these tools and methods on systems or networks without explicit permission is illegal and may result in severe legal consequences. It is your responsibility to ensure you have proper authorization before conducting any testing. Any misuse of these tools is solely at your own risk.

Purpose: The example malware executable can be used for demonstrations or simulations in a controlled environment to showcase cyber-attack scenarios.

Caution: Perform this strictly within your virtual machine environment.

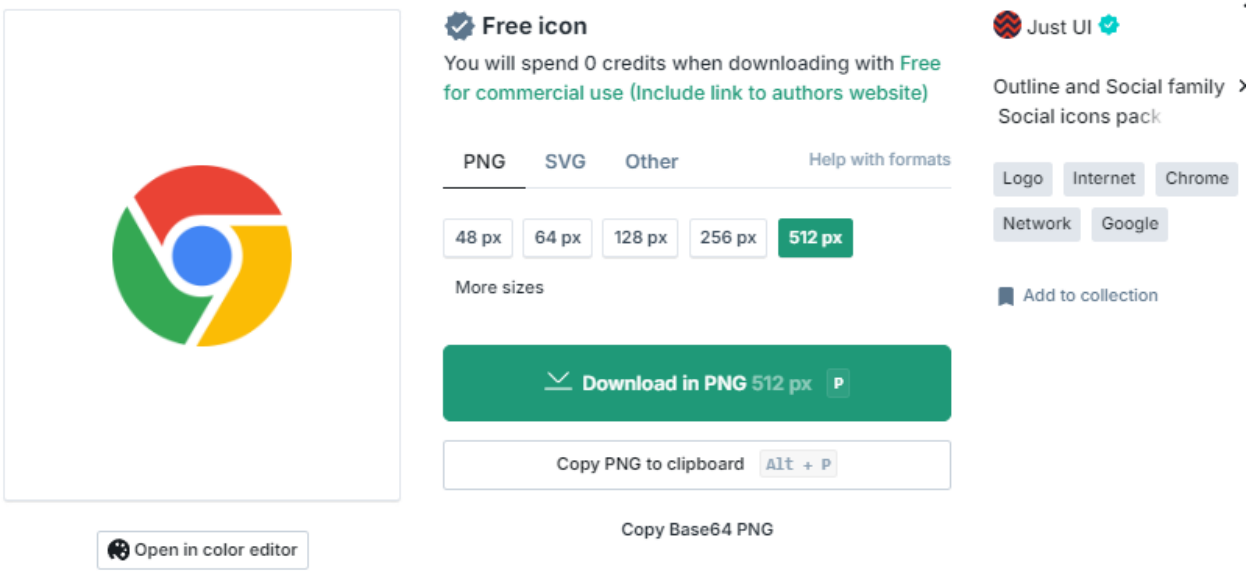
This note will demonstrate how to create a malicious executable that mimics the appearance of a PDF, Word document, or web browser executable. This file will retain the original functionality of the legitimate program while also containing an embedded malicious payload. For this process, we'll use WinRAR, which can be downloaded here:

https://www.rarlab.com

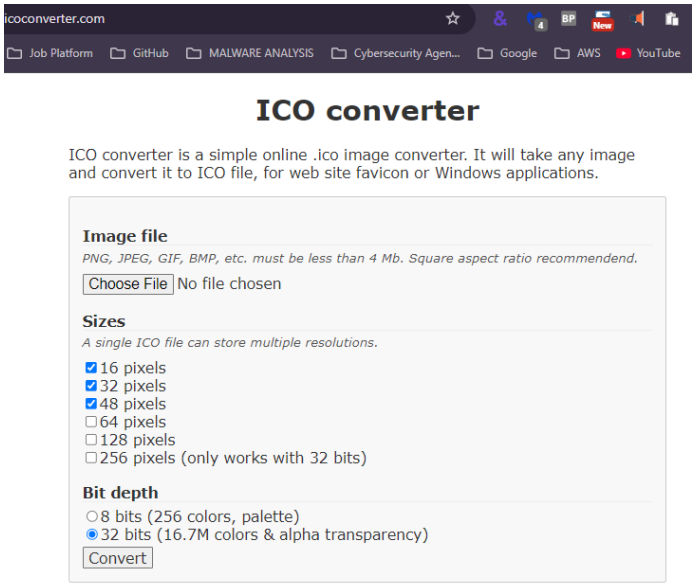


1. First, you need crafted executable that will so domething on the victim host or send us a reverse shell. Example repo: https://github.com/ytisf/theZoo

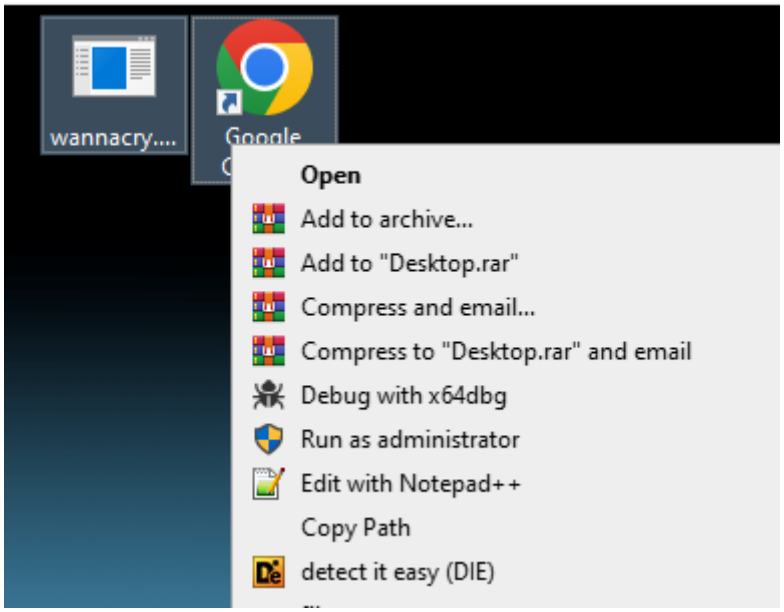
2. Find a PNG icon that matches the appearance you want for your malicious executable on https://iconfinder.com. For this example, use a Chrome icon, but you can search for any file type or logo you prefer. Once you find the desired icon, click 'Download PNG.'



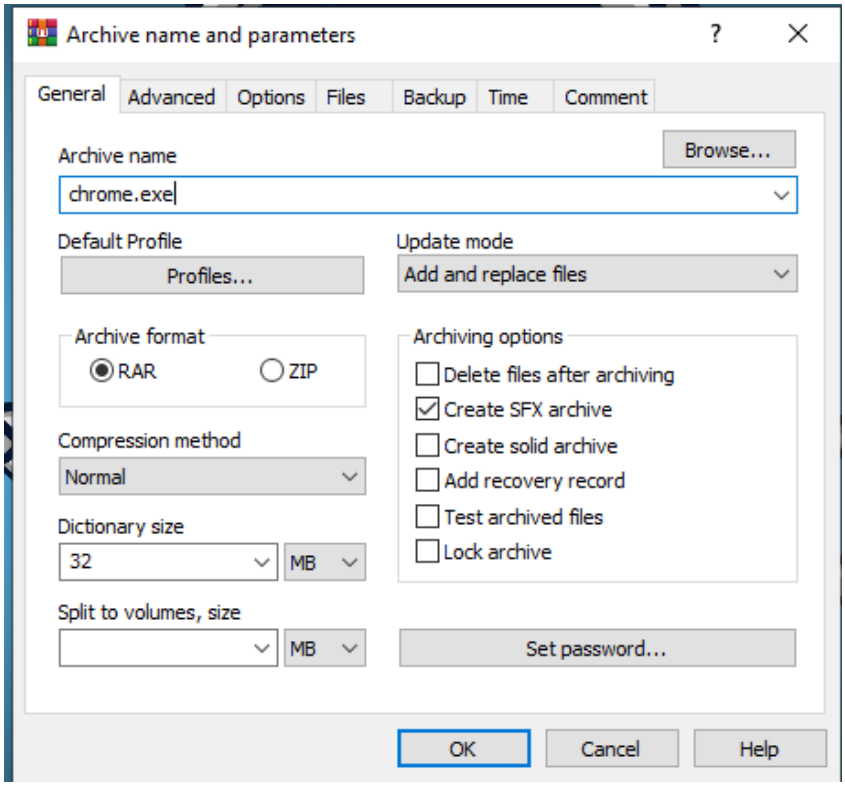
3. Then, covert the icon PNG to a .ico file using https://iconconverter.com. Upload the previous PNG and click ‘Convert’.



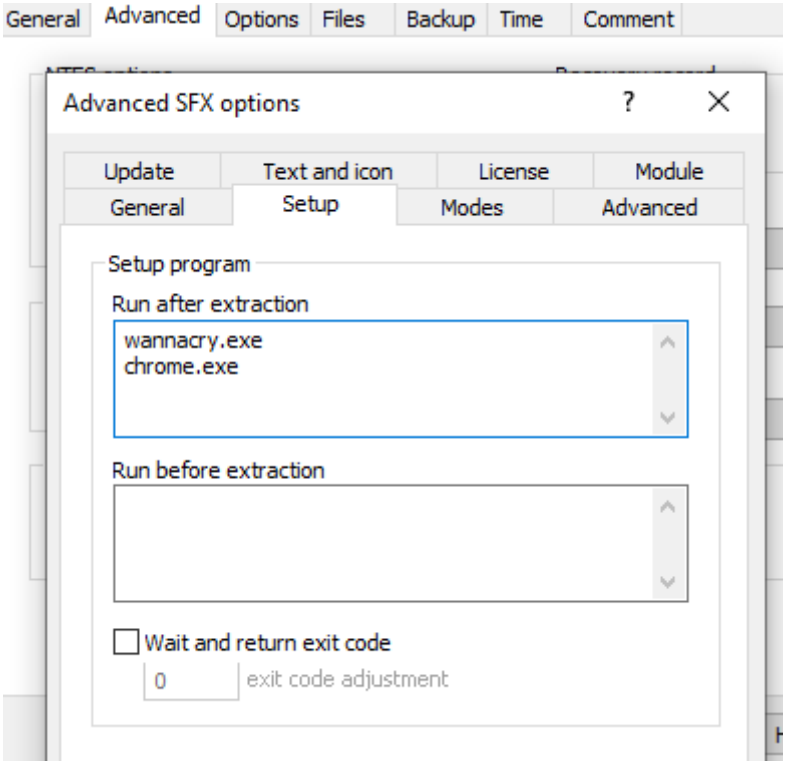
4. Next, select both legit Google Chrome and Wannacry malware, right click them and select ‘Add to Archive to create combined archive.



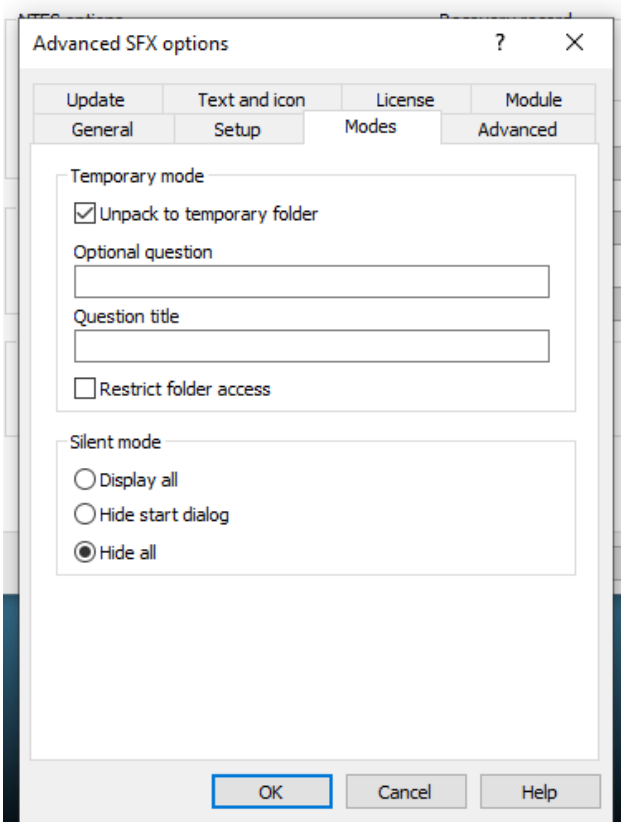
5. The archive name going to be chrome.exe to look legit. Ensure to ‘Create SFX archive ‘ is checked.

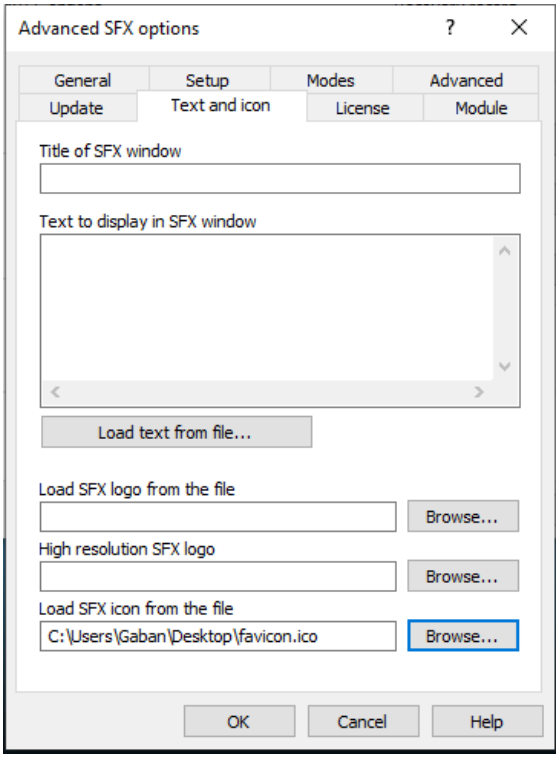


6. Then, click Advanced > SFX options > Setup and input the following:

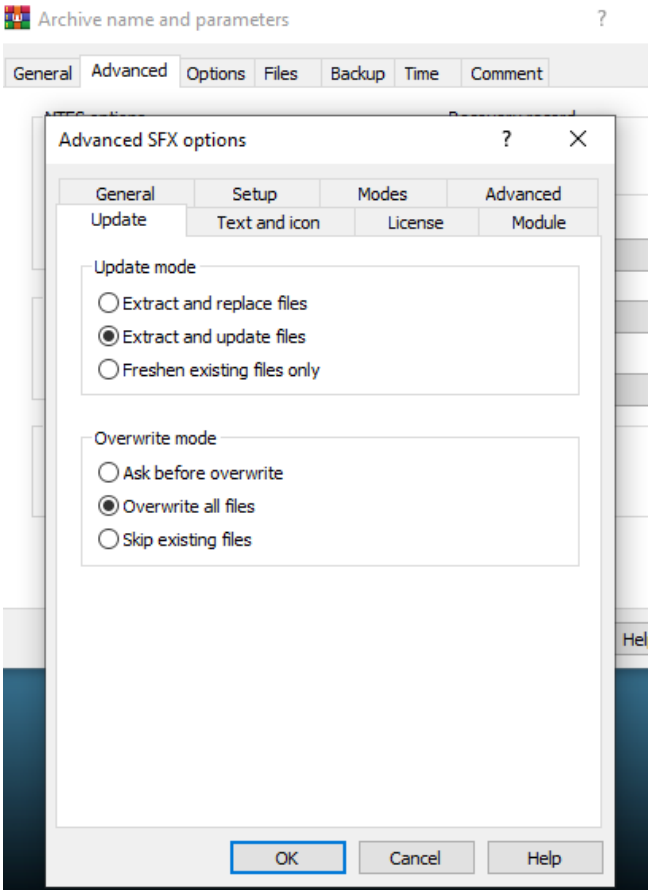


Step by step: Embedding a Malware Executable into a Legitimate PDF or EXE

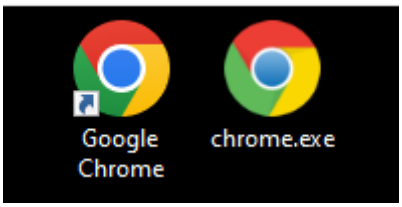




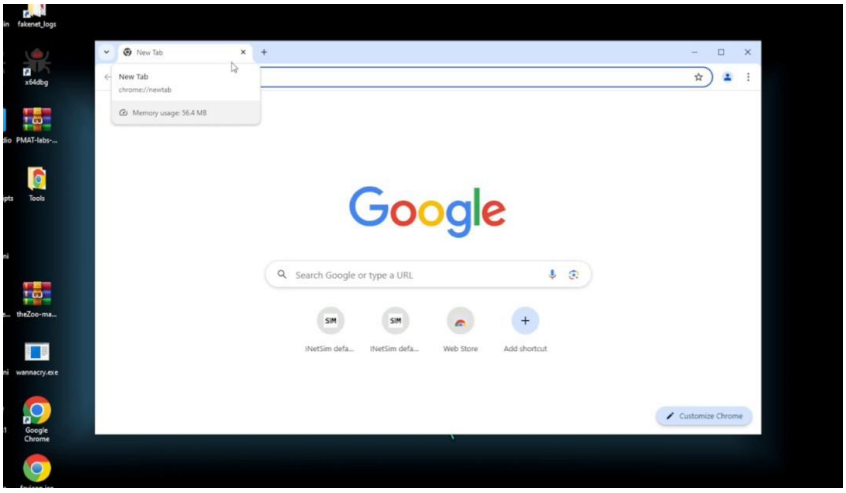
Hazwan Jaafar



7. Once you've entered the parameters, click 'OK.' An archive named **chrome.exe** will appear on the desktop, displaying the correct Chrome icon.



8. Left is legit Google Chrome and right is Chrome that has been embedded with Wannacry malware. This will be the attachment inside the phishing email for example. When launched the Google Chrome will be launching as normal, and the malware is running at the background.



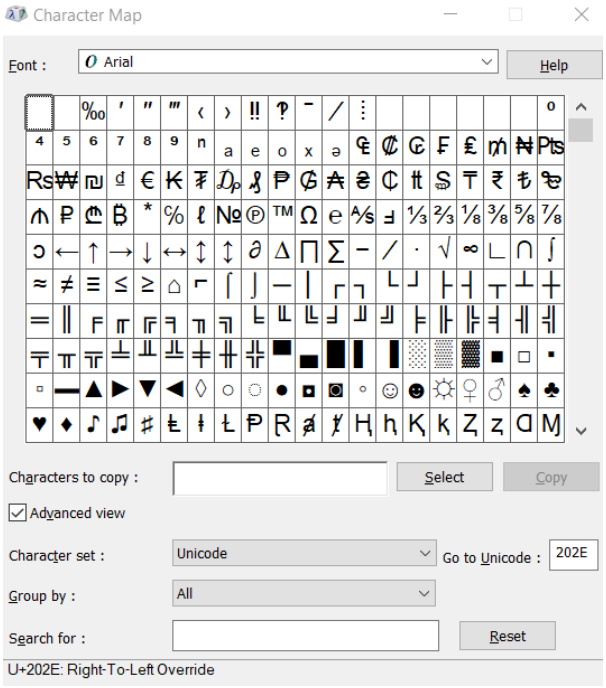
The aftermath of malware ransomware by Wannacry

Hazwan Jaafar

(Optional - If Using a File Type Other Than EXE, Like PDF):
We will apply the **Right-To-Left Override (RTLO)** technique to make the created archive appear as a PDF on the desktop, while still executing as an EXE. RTLO is a Unicode non-printing character commonly used for languages that are read from right to left. This trick reverses the text order, making the filename appear as a different file type to deceive the user.

1. 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.

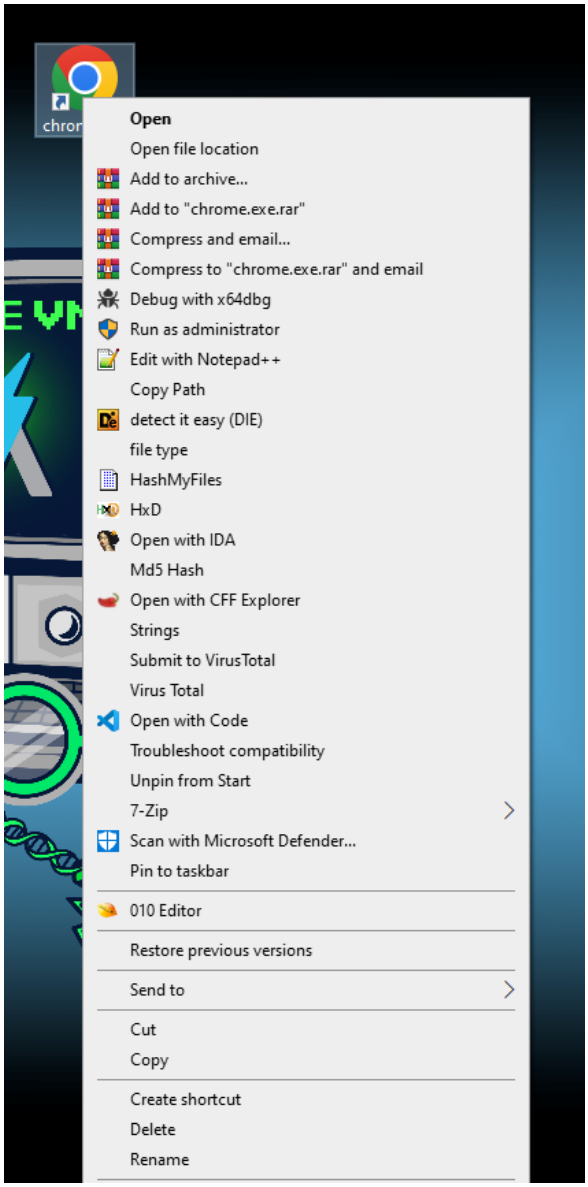
2. Open the Character Map app on Windows and check the 'Advanced View' box. In the 'Go to Unicode' option, type in 202E.
   Here's How to open Character Map:
   Open **Run** (Win+R), type **charmap** into Run, and click/tap on **OK** to open Character Map.



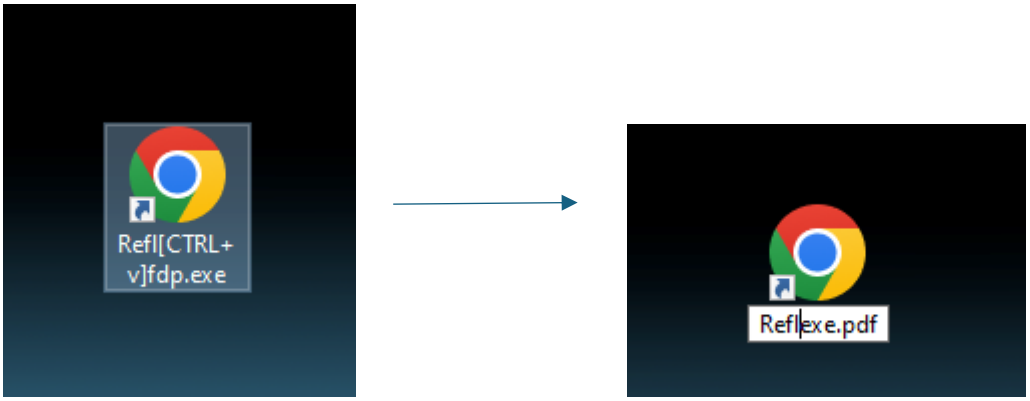
3. Hit the 'Select' and 'Copy' buttons respectively and edit the file name of the WinRaR archive we created. You enter the file name Refl[CTRL+ v]fdp.exe and then go back and paste the Unicode where specified. The file should then change to Reflexe.pdf as soon as you hit paste.

Hazwan Jaafar

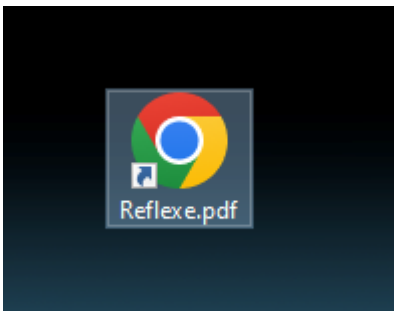
The WinRAR archive



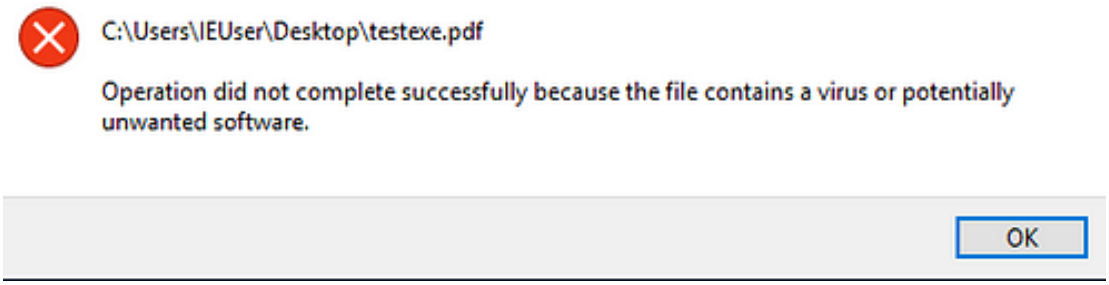
Rename the exe file



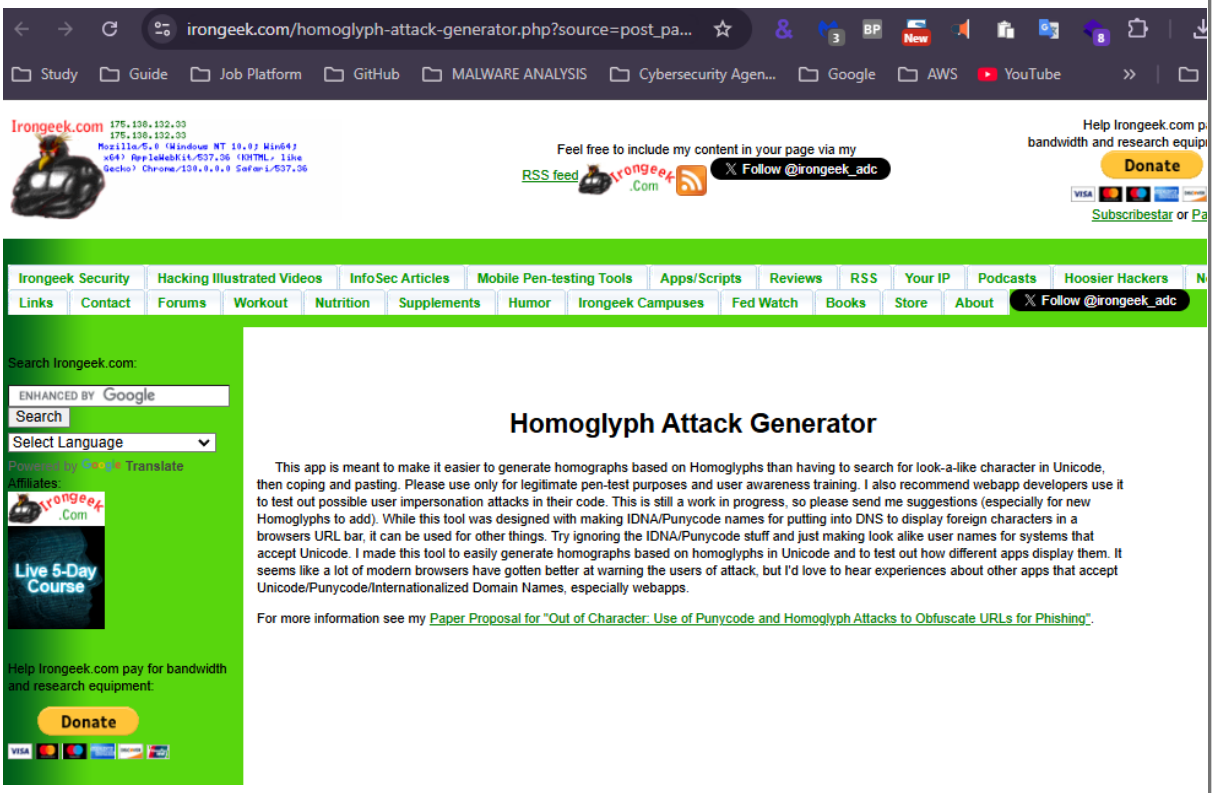
Then it becomes:



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.

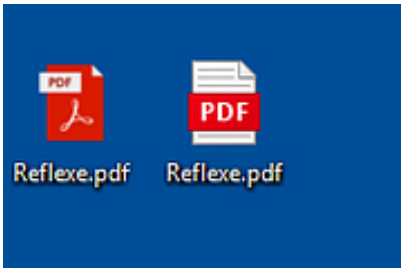


One way to get around this is using Homoglyph's. At the end of the day, we only want this to look like a PDF to the user, so how likely is that they'll catch that one letter looks alittle different? I used this resource to manually test what Defender would flag:



4. 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:

Homoglyph 'f'



5. Can you tell the difference by looking at it!

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

Hazwan Jaafar