PROCEDURE TO COMBINE A MALICIOUS BINARY WITH A FILE

BY PHIL NAULT

WHAT THIS IS… AND WHAT IT'S NOT

- USB drops
- E-mail
- Malicious binary

BAIT FILE

- Choose wisely
- Reconnaissance required
- Could be any file whatsoever, but be consistent

STEP 1 – CHOOSE BAIT FILE

- Can be anything. I make an excel spreadsheet called Proposed Salary Increase 2025

STEP 2 – CREATE MALICIOUS BINARY

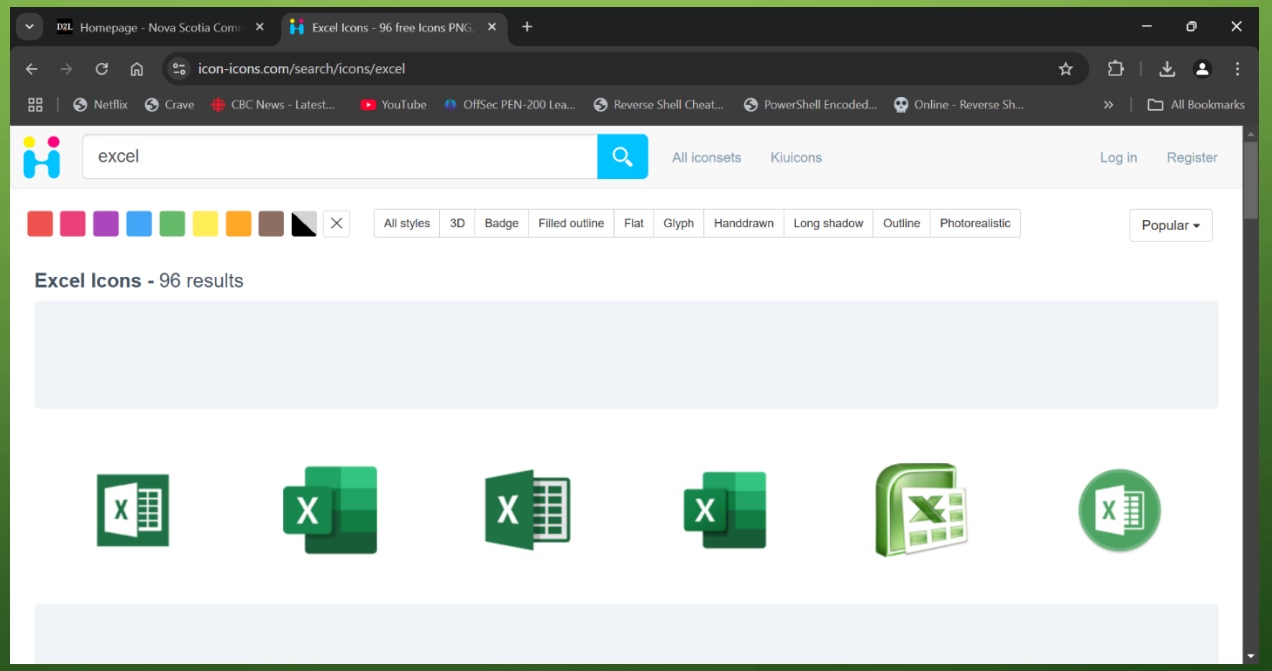
- I called mine config.exe
- The name is not important, the target will not see it
- Simpler is better

STEP 3 – INSTALL WINRAR

- Not sure this can be done on Linux
- Easiest is to use a Windows VM

STEP 4 – FIND THE .ICO IMAGE

- The .ico image needs to be the icon that appears in the OS your target uses
- Can do a google search or find tools that extract .ico from a file

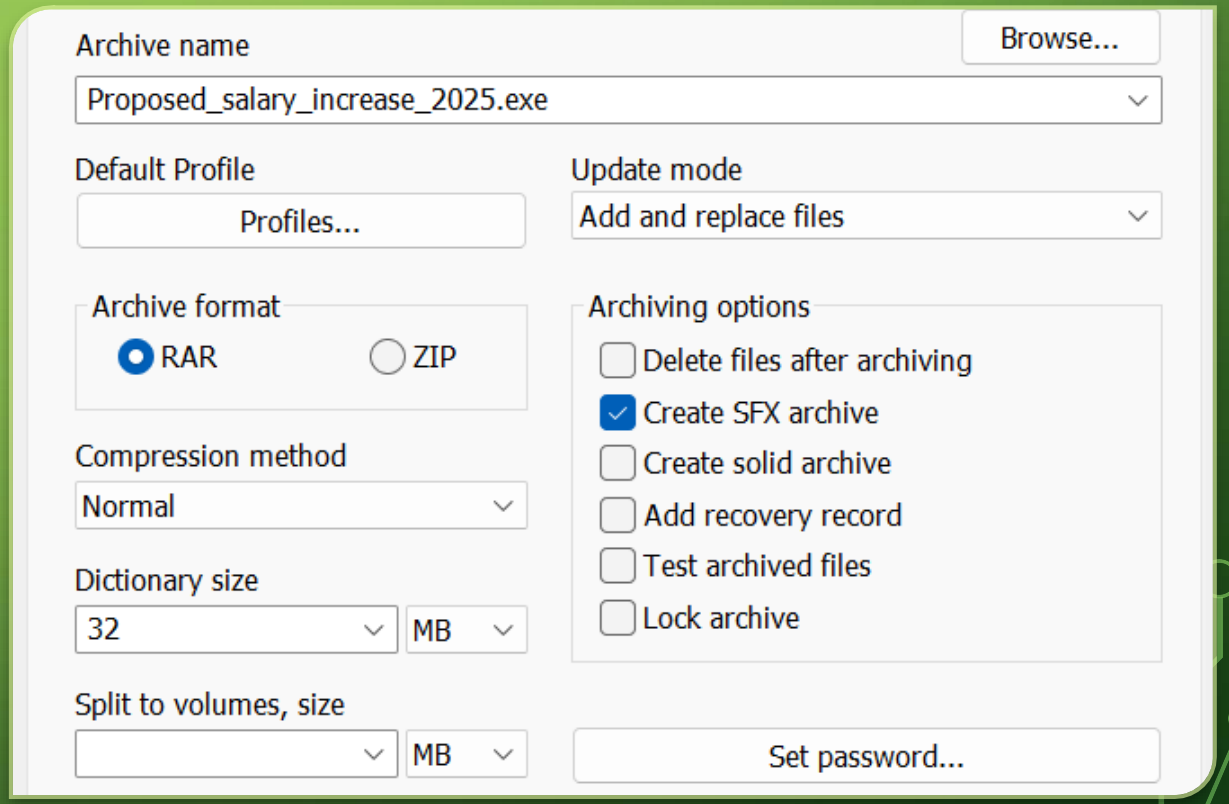


STEP 5 – CREATE THE ARCHIVE

- Select both files
- Right-click and select WinRAR / add to archive

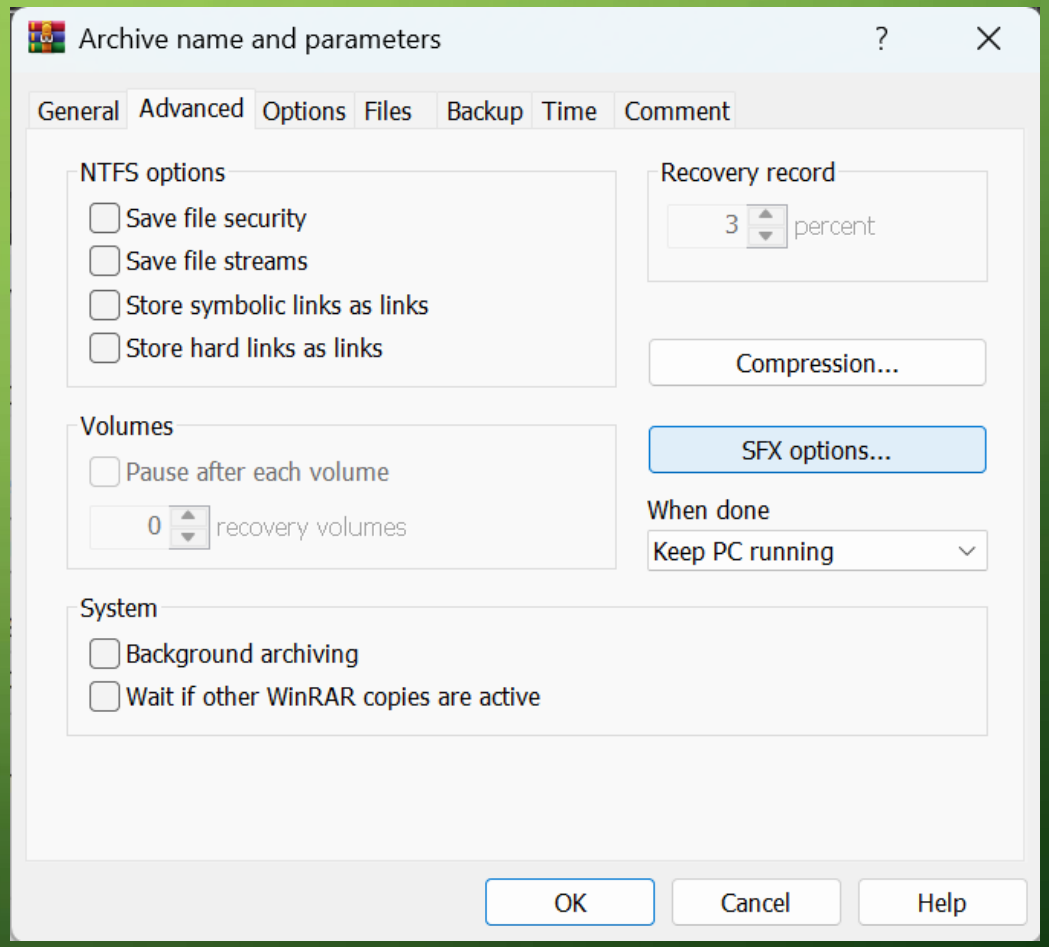
STEP 6 – NAME ARCHIVE

- In the first menu, set the name the same as your bait file, and click create SFX archive. The name will have a .exe added to the end, this is normal



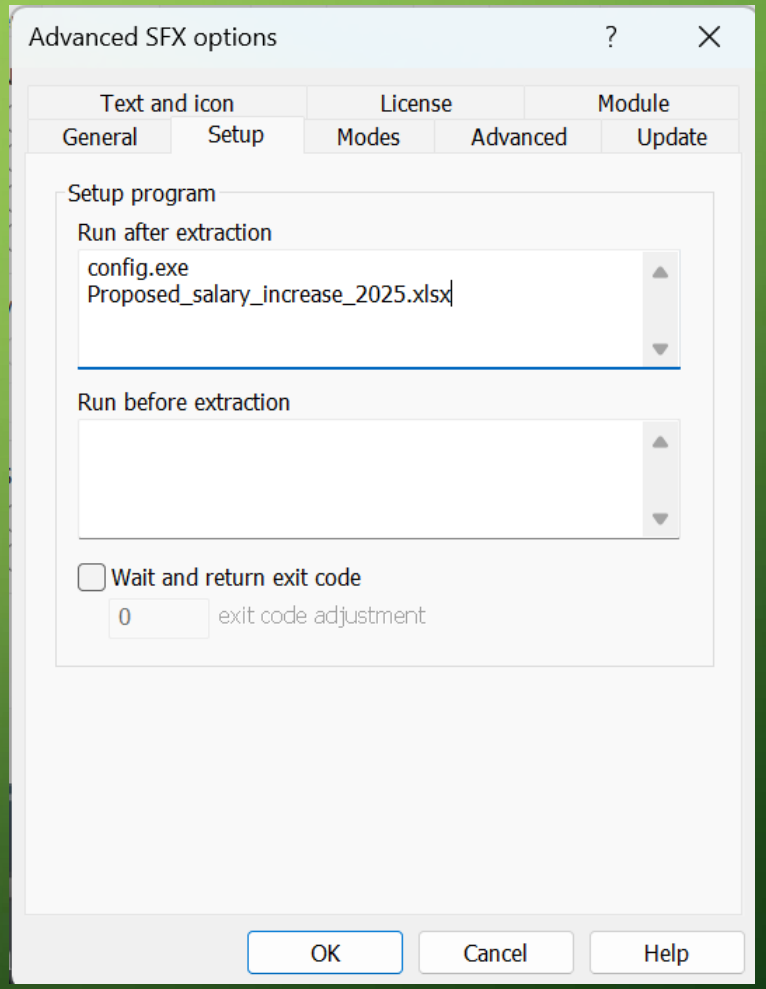
STEP 7 – CREATE ARCHIVE

- Click on the advanced tab and select SFX options



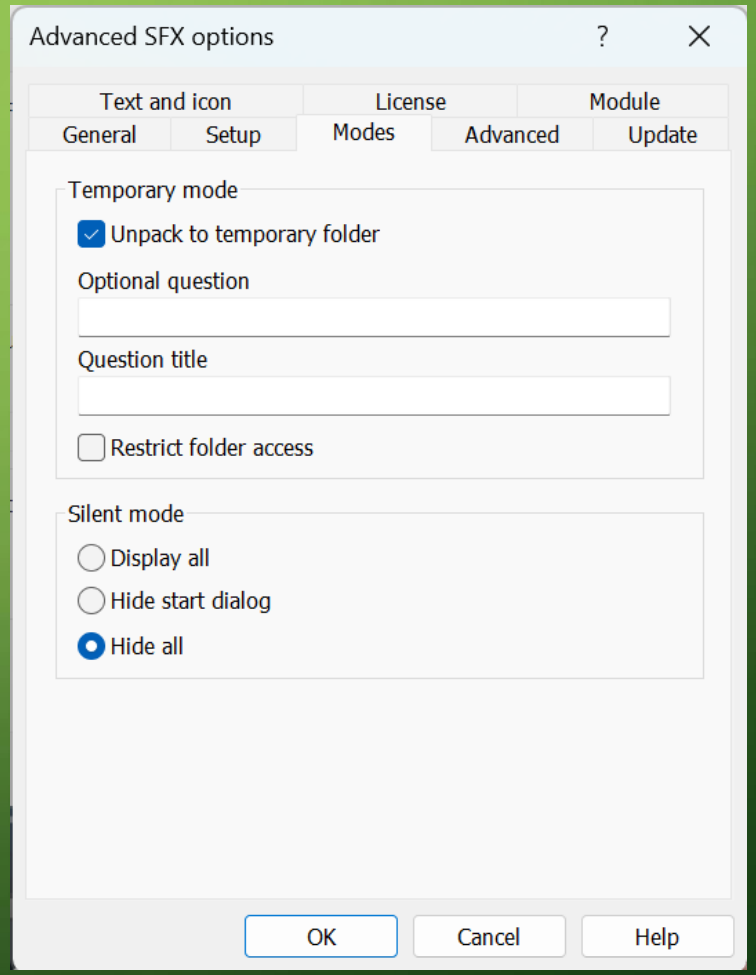
STEP 7 – CREATE ARCHIVE (CONT'D)

- Click on the Setup tab and add your malicious .exe name and bait file name to the Run after extraction area



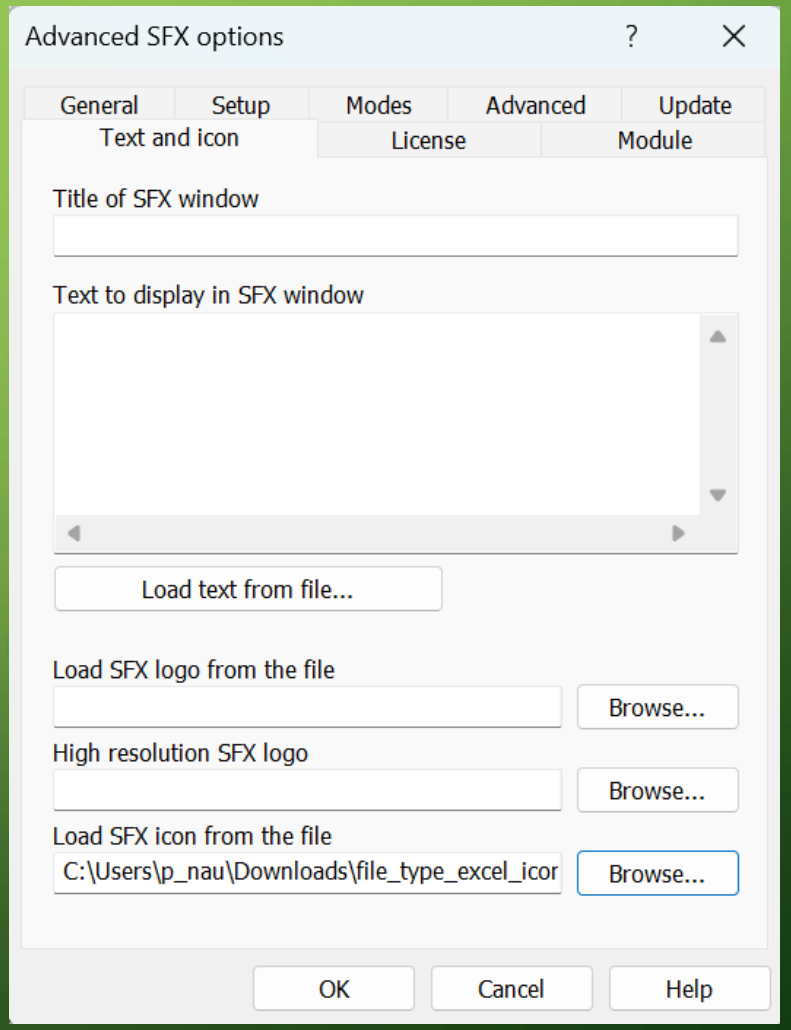
STEP 7 – CREATE ARCHIVE (CONT'D)

- Click on the modes tab and select extract to temporary folder and hide all



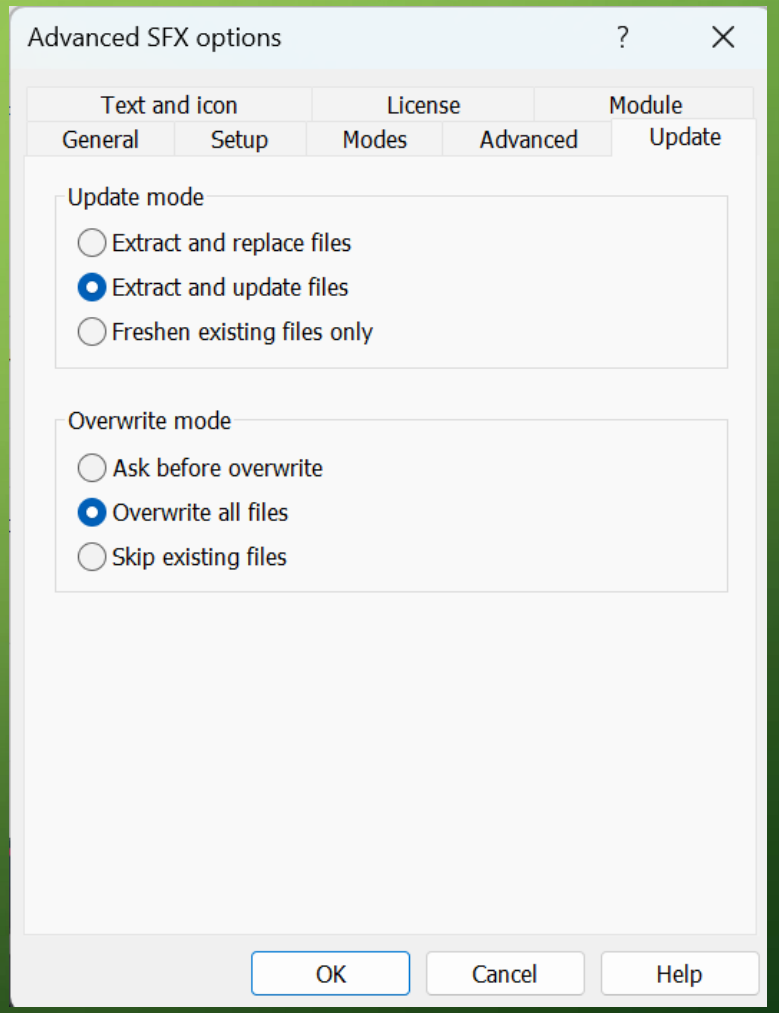
STEP 7 – CREATE ARCHIVE (CONT'D)

- Click on the Text and icon tab, and select the .ico file you selected for the file



STEP 7 – CREATE ARCHIVE (CONT'D)

- Click on the Update tab and select Extract and Update files, and Overwrite all files



STEP 8 – FINALIZE ARCHIVE

- Click Ok twice
- Archive will be a .exe file that will look like a regular file