

A decorative graphic on the left side of the slide, consisting of a network of thin, light green lines and small circles, resembling a circuit board or a stylized tree structure, extending from the top to the bottom of the frame.

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

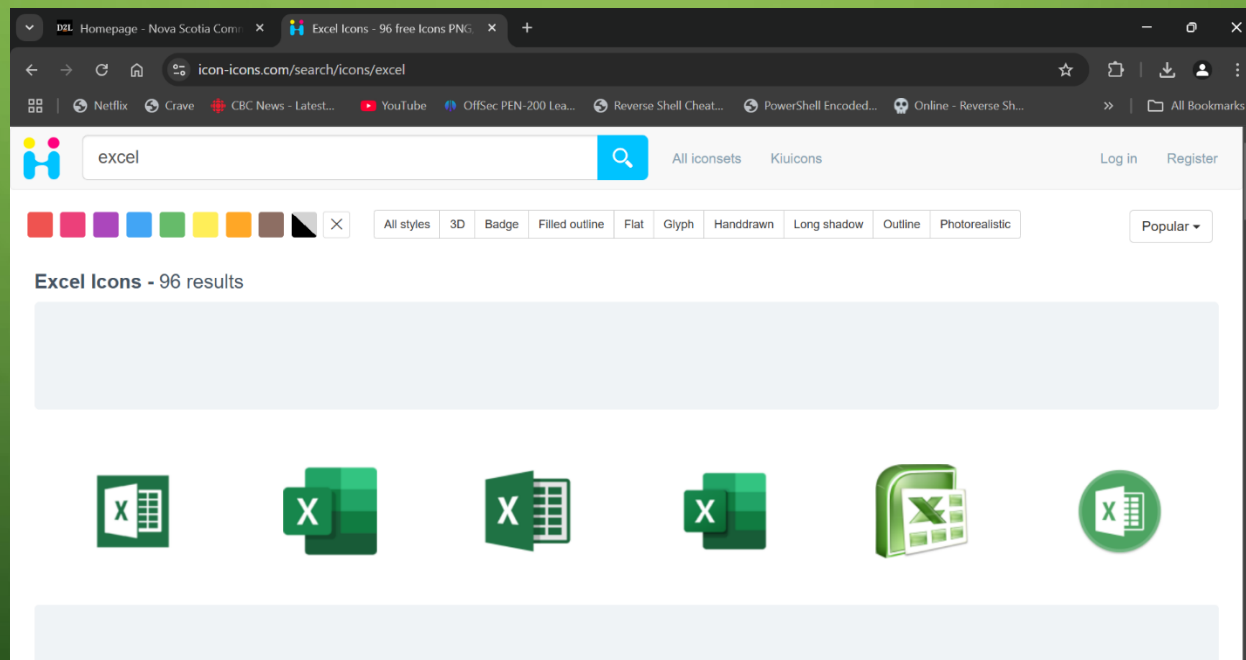
- I called mine config.exe
- The name is not important, the target will not see it
- Simpler is better

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



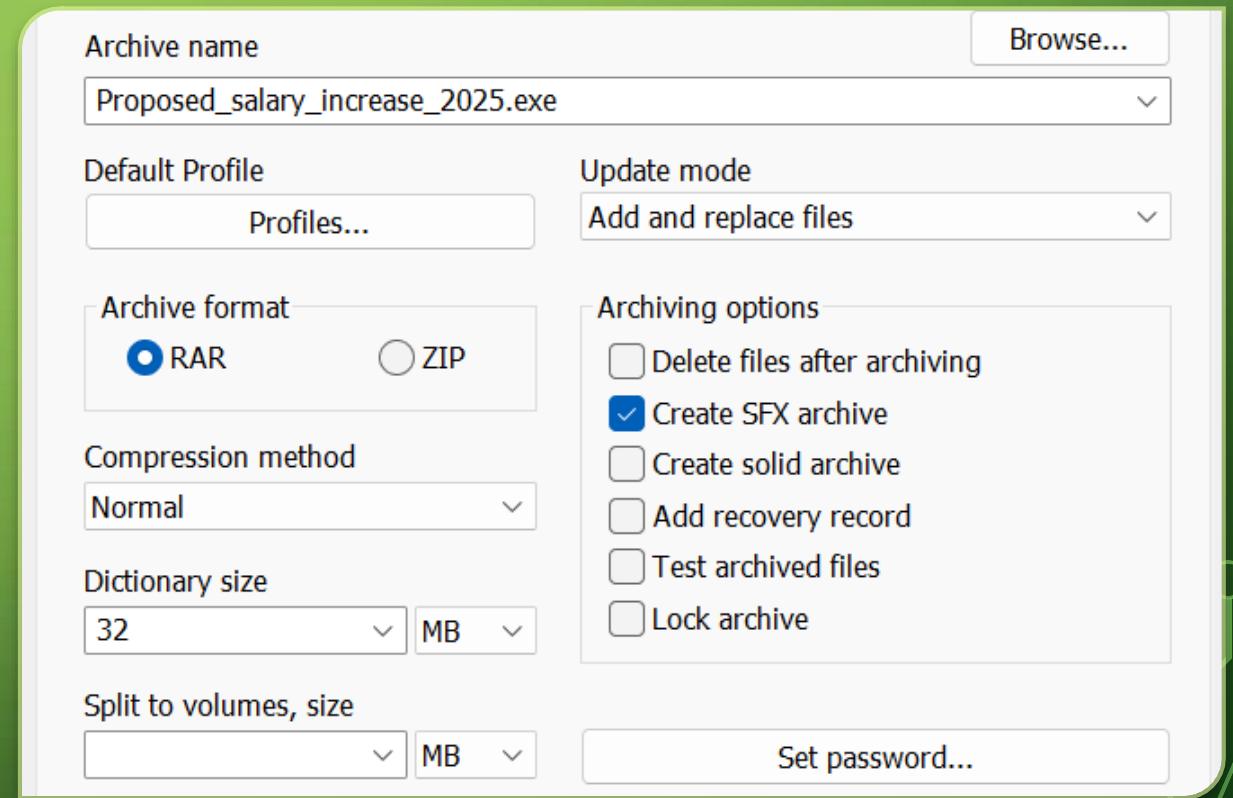
STEP 5 – CREATE THE ARCHIVE

- 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



The screenshot shows the 'Archive name and parameters' dialog box in WinRAR. The 'Archive name' field is set to 'Proposed_salary_increase_2025.exe'. The 'Default Profile' is 'Profiles...'. The 'Update mode' is 'Add and replace files'. The 'Archive format' is 'RAR' (selected) and 'ZIP'. The 'Compression method' is 'Normal'. The 'Dictionary size' is '32 MB'. The 'Split to volumes, size' is set to 'MB'. The 'Archiving options' section includes: 'Delete files after archiving' (unchecked), 'Create SFX archive' (checked), 'Create solid archive' (unchecked), 'Add recovery record' (unchecked), 'Test archived files' (unchecked), and 'Lock archive' (unchecked). A 'Set password...' button is at the bottom right.

Archive name Browse...

Proposed_salary_increase_2025.exe

Default Profile Profiles...

Update mode Add and replace files

Archive format ☒ RAR ☐ ZIP

Compression method Normal

Dictionary size 32 MB

Split to volumes, size MB

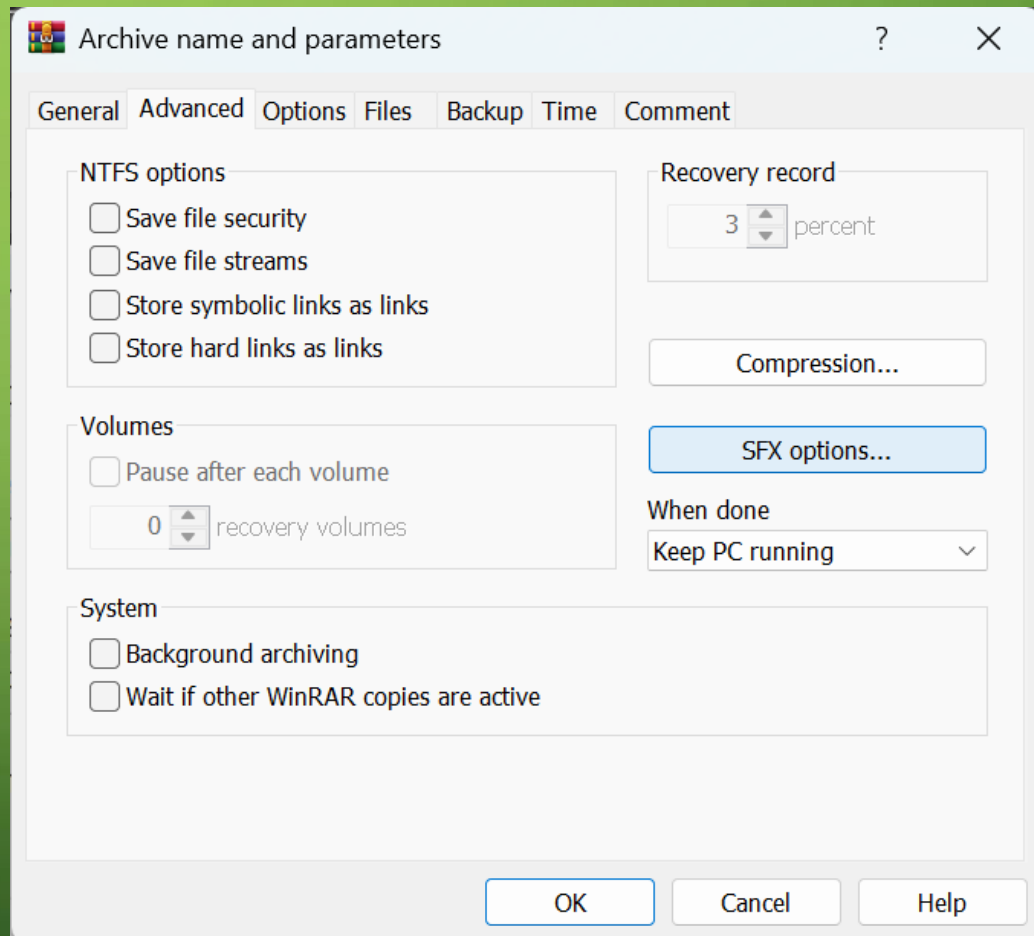
Archiving options

- ☐ Delete files after archiving
- ☒ Create SFX archive
- ☐ Create solid archive
- ☐ Add recovery record
- ☐ Test archived files
- ☐ Lock archive

Set password...

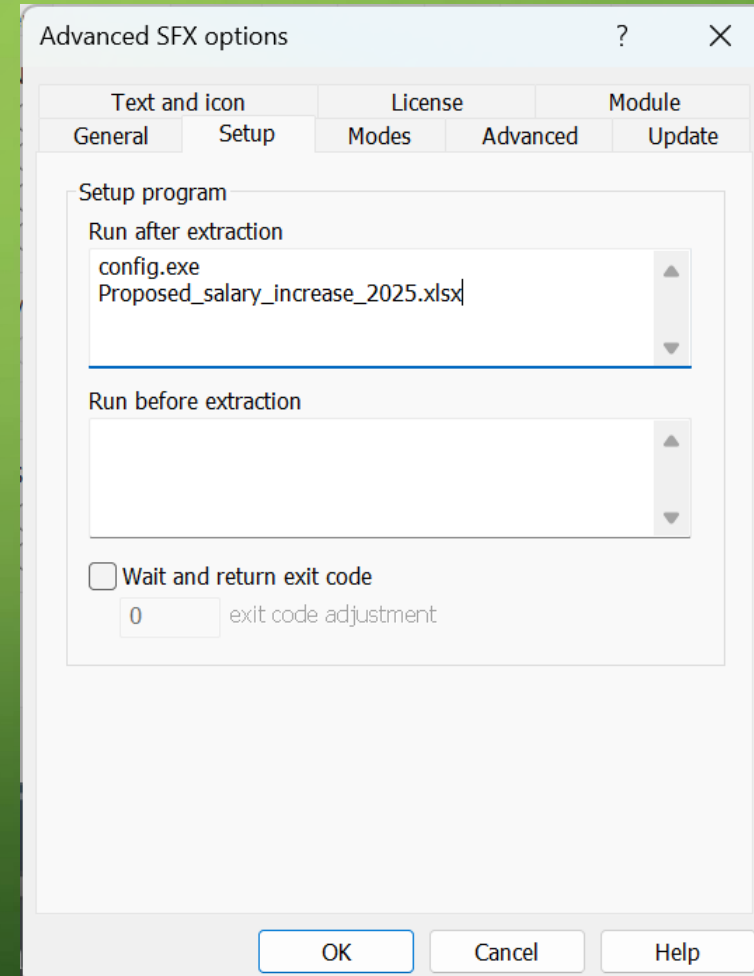
STEP 7 – CREATE ARCHIVE

- Click on the advanced tab and select SFX options



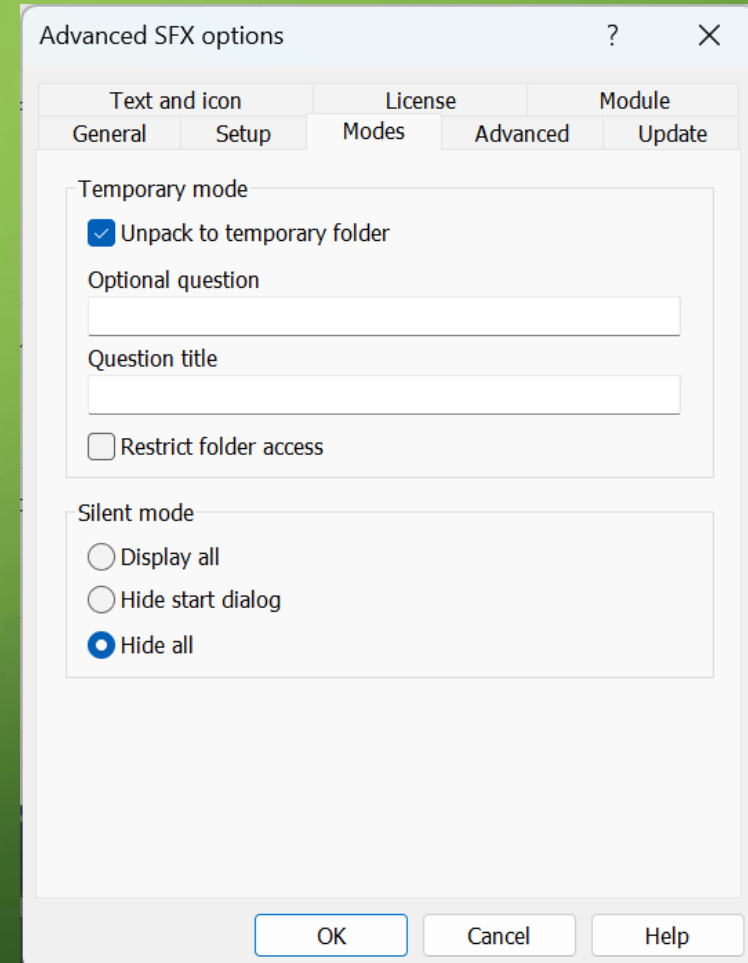
STEP 7 – CREATE ARCHIVE (CONT'D)

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



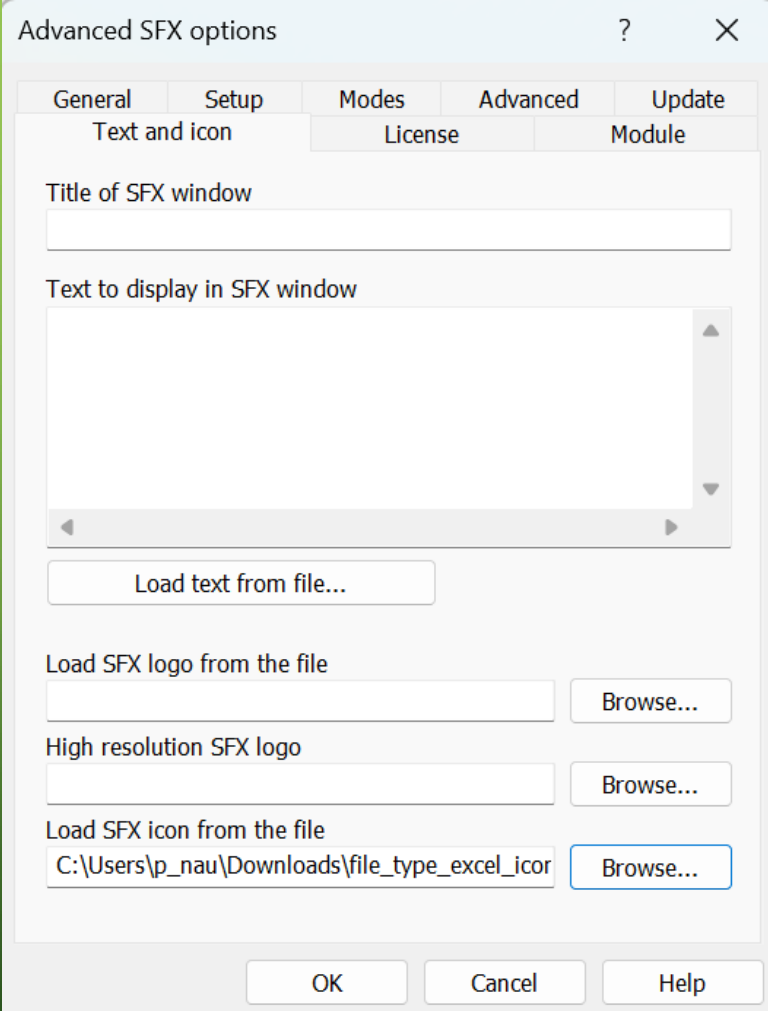
STEP 7 – CREATE ARCHIVE (CONT'D)

- 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



The screenshot shows the 'Advanced SFX options' dialog box with the 'Text and icon' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar are five tabs: 'General', 'Setup', 'Modes', 'Advanced', and 'Update'. The 'Text and icon' sub-tab is active. The main area contains a text input field for 'Title of SFX window', a larger text area for 'Text to display in SFX window' with a scrollbar, and a 'Load text from file...' button. Below these are three sections for loading assets: 'Load SFX logo from the file' with a text field and 'Browse...' button; 'High resolution SFX logo' with a text field and 'Browse...' button; and 'Load SFX icon from the file' with a text field containing the path 'C:\Users\p_nau\Downloads\file_type_excel_icor' and a 'Browse...' button. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Advanced SFX options

General Setup Modes Advanced Update
Text and icon License Module

Title of SFX window

Text to display in SFX window

Load text from file...

Load SFX logo from the file

Browse...

High resolution SFX logo

Browse...

Load SFX icon from the file

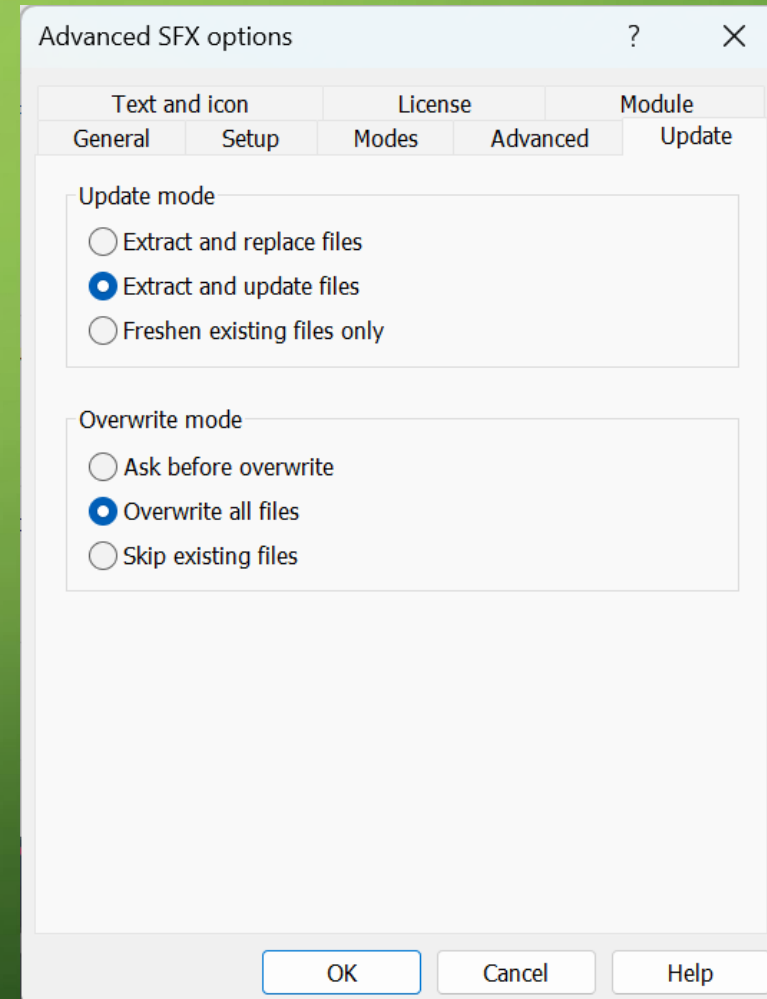
C:\Users\p_nau\Downloads\file_type_excel_icor

Browse...

OK Cancel Help

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

