**Unpacking UPX Packed Malware**

Hash: fd6c69c345f1e32924f0a5bb7393e191b393a78d58e2c6413b03ced7482f2320

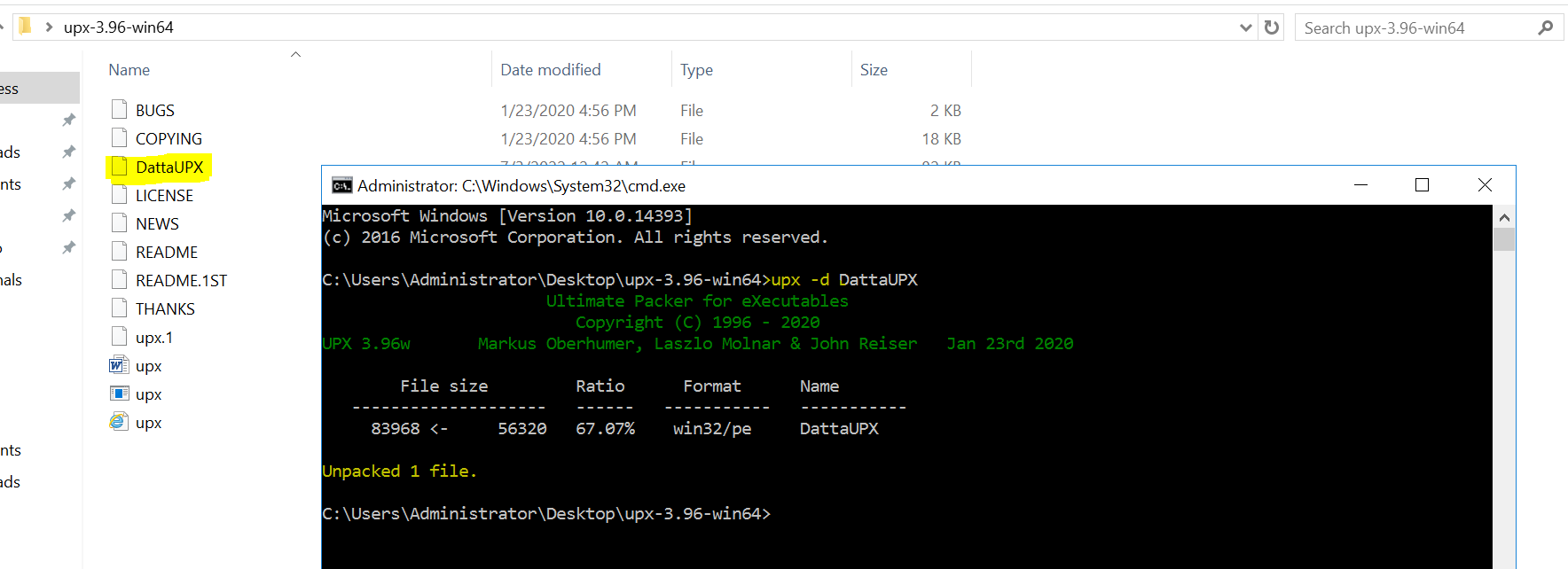
**Graphical user interface, text, application, email

Description automatically generated**

Unpacking this with CMD

Use command **“upx -d YourFileName”** to unpack.

And similarly if you want to Pack (Compress) any unpack file with UPX, use command just “upx YourFileName” to pack.

****

You will notice in the folder your Packed file is now replaced with unpacked file and if you compare this with previous one, the size, entrypoint, entropy, section all is changed. Graphical user interface, application

Description automatically generatedGraphical user interface, text, application

Description automatically generated

So Entrypoint and First Bytes of our Unpacked file is

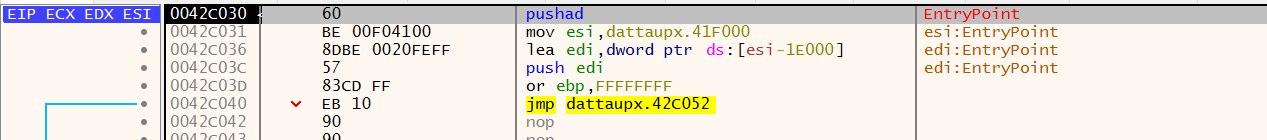
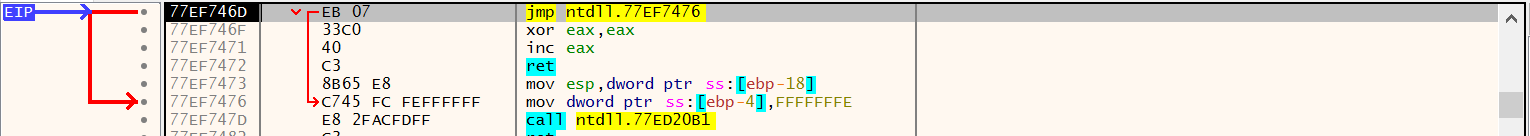
Entrypoint: 1CFE

First Bytes: 52,6A,36,68

Checking this manually with x32dbg

1. Push Pop Method

Load sample in x32dbg and Run the Malware (F9). You’ll be at Entrypoint of your Binary (60 pushad)



Search for 61 popad and put the breakpoint on very next JMP instruction.A picture containing text

Description automatically generated

Hit Enter to JMP. It will take you a place Hit F9 again. Run the sample until you get JMP breakpoint.

Text

Description automatically generated

Do step over (F7). You can see your entrypoint and first byte of unpacked malware.

(1CFE & 52,6A,36,68)

Text

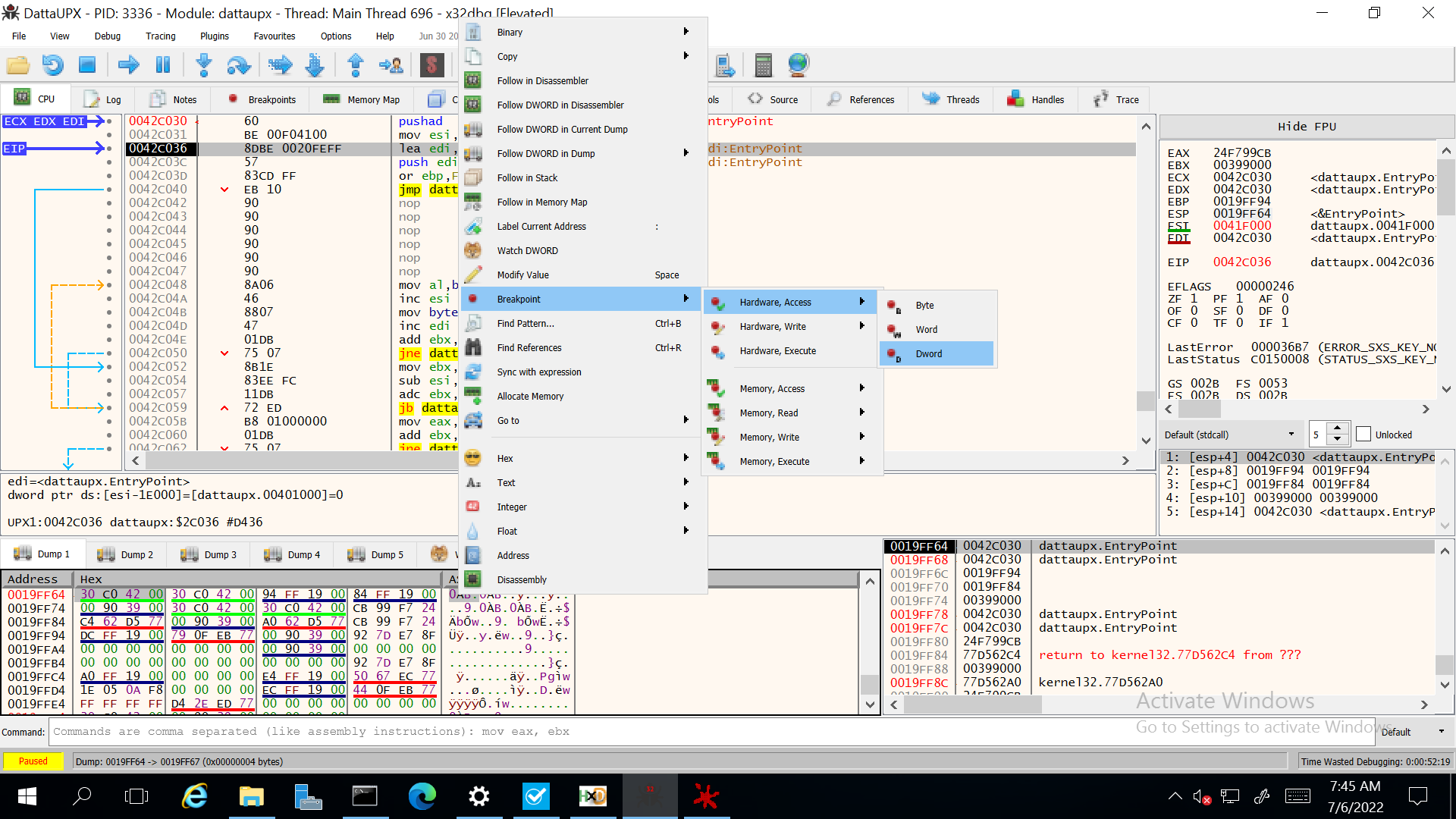
Description automatically generated

1. ESP Method

Run the sample and do step over. You’ll see Entrypoint at ESP in Registers section. Right click to that address and do “follow in dump”



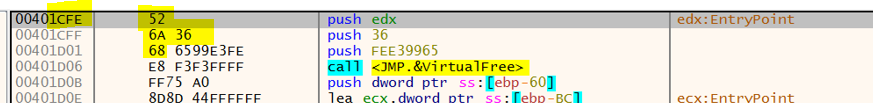
Do BreakPoint>Hardware Access>Dword at the Dword (4Bytes) in Dump.



Then Run the Sample. Hit the very next JMP.



You’ll be at Entrypoint of your unpacked Malware (1CFE & 52,6A,36,68)



Importing Unpacked Malware

Use Scylla plugin in x32dbg for this. Check IAT info, you’ll see your OEP. Click IAT autosearch

Graphical user interface, text, application, chat or text message

Description automatically generated

Then click on Get Imports for imports then Dump and save your unpacked binary.

Graphical user interface, text, application

Description automatically generated

