Lab Exercise

Instructions for Malware Sample 2

Instructions

- Try this on your own first – before seeing the next videos
- Use the correct tool to check if it is packed
- This sample is packed with upx
- The unpacking command is (open cmd and do):

  upx –d –o newname.exe originalname.exe
- After unpacking, use the unpacked exe for analysis
- This is live malware – so be careful – run in vm and set vm to host only mode (if necessary)

Good Luck