# EECS 444 Homework 2: Mimic You - Malware!

#### Yida Liu

October 12, 2019

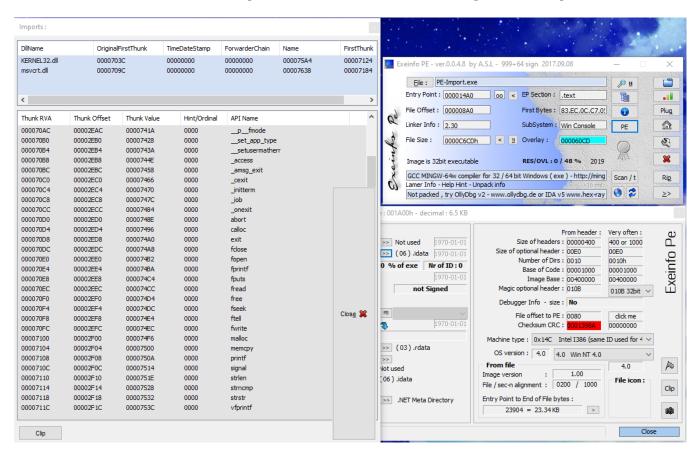
# 1 Write a program using c to implement the function

See ./PE-Import.c for the source of the program.

We used the gcc compiler included in mingw-x86\_64 to compile the program to ./PE-Import.exe.

# 2 Check the Import Table of ./PE-Import.exe

We used Exeinfo PE to check the import table. Here is a screenshot output of the Import Table.



# 3 Original vs. Packed

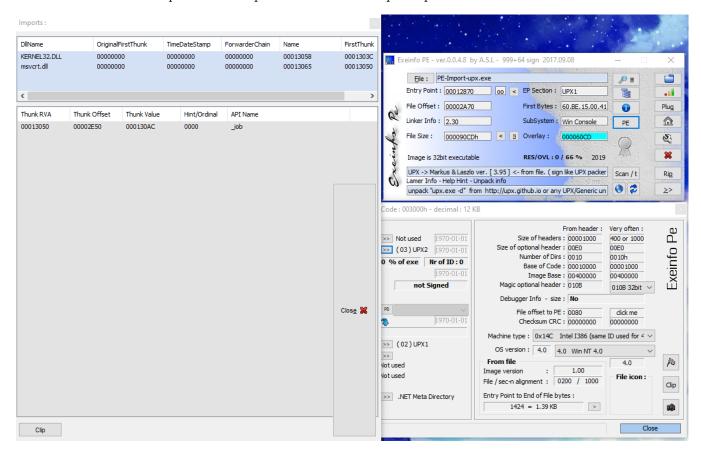
#### 3.1 Use UPX to pack PE file

We used the following command using UPX to pack the compiled program to PE-Import-upx.exe.

```
# Pack using UPX
upx -9 PE-Import.exe -0 PE-Import-upx.exe
```

### 3.2 Check the Import Table of the Packed Executable

Here is a screenshot output of the Import Table of ./PE-Import-upx.exe

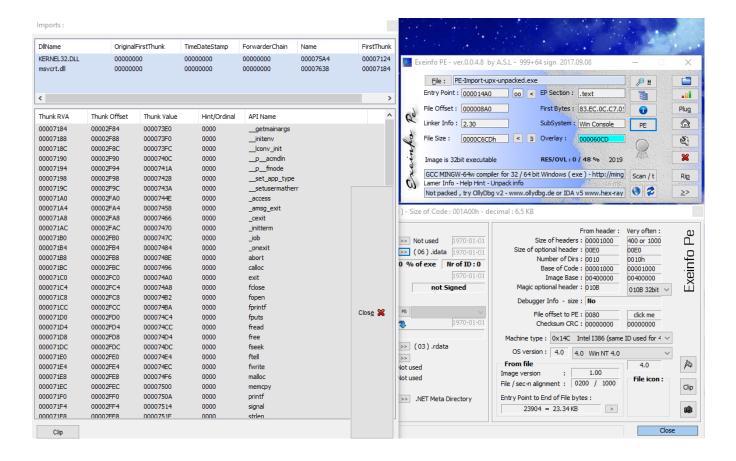


#### 3.3 Use UPX to unpack the Packed Executable

We used the following command to use UPX to unpack the packed executable to PE-Import-upx-unpacked.exe

```
# Unpack using UPX
upx -d PE-Import-upx.exe -o PE-Import-upx-unpacked.exe
```

Here is a screenshot output of the Import Table of ./PE-Import-upx-unpacked.exe



#### 4 Fool Anti-Malware Scanner

First, we used the Virustotal to scan the original PE-Import.exe. Virustotal reports that 1 out of 70 engines reported unsafe of this program.

Our technique is quite simple and straight forward. We use the privious ./PE-Import-upx.exe and use PELock to pack an additional layer of protection in ./PE-Import-upx-pelock.exe . Our justification is that virus / trojan often employes multiple layers of packing to hide the actual code underneath it. This file was detected malicious and dangerous by 28 out of 70 engines in VirusTotal.