

HW2 Taosha Gao

Step2. original import table

Header info : [PE-Import.exe] - Size of Code : 001C00h - decimal : 7 KB

The screenshot displays the Exeinfo Pe tool interface. The main window shows the 'Directory Info' section with fields for Export, Import, Resource, Exception, Security, and Base Reloc. The 'Import' field is highlighted, showing '00006000' and '00000718'. The 'From header' section on the right provides details about the PE header, including the size of headers, optional header, number of directories, base of code, image base, and magic optional header. A 'not Signed' button is visible in the 'Security' section.

Below the main window, an 'Imports' dialog box is open, displaying a table of imported DLLs and functions. The table has columns for 'DllName', 'OriginalFirstThunk', 'TimeDateStamp', 'ForwarderChain', 'Name', and 'FirstThunk'. The data rows are:

| DllName | OriginalFirstThunk | TimeDateStamp | ForwarderChain | Name | FirstThunk |
|--------------|--------------------|---------------|----------------|----------|------------|
| KERNEL32.dll | 00006050 | 00000000 | 00000000 | 00006644 | 00006154 |
| msvcrt.dll | 000060A0 | 00000000 | 00000000 | 000066D8 | 000061A4 |
| USER32.dll | 00006128 | 00000000 | 00000000 | 0000670C | 0000622C |

Below the table, there is a section for 'Thunk RVA', 'Thunk Offset', 'Thunk Value', 'Hint/Ordinal', and 'API Name'. The 'API Name' column is currently empty. The dialog box has a 'Clip' button and a 'Close' button with a red X icon.

Step 3.2. packed import table

Header info : [packedPE-Import.exe] - Size of Code : 041000h - decimal : 260 KB

Directory Info :

| | RVA | SIZE | | |
|------------------|----------|----------|------------|---------------------|
| Export : | 00000000 | 00000000 | >> | Not used |
| Import : | 000F9000 | 000000E8 | >> | (03) UPX2 |
| Resource : | 00000000 | 00000000 | 0 % of exe | Nr of ID : 0 |
| Exception : | 00000000 | 00000000 | | 1970-01-01 |
| Security : | 00000000 | 00000000 | not Signed | |
| Base Reloc : | 00000000 | 00000000 | | |
| Debug : | 00000000 | 00000000 | PB | |
| Architecture : | 00000000 | 00000000 | | 1970-01-01 |
| Global PTR : | 00000000 | 00000000 | | |
| TLS Table : | 000F8D28 | 00000018 | >> | (02) UPX1 |
| Load Config : | 00000000 | 00000000 | >> | |
| Bound Import : | 00000000 | 00000000 | | Not used |
| Imp.Table IAT : | 00000000 | 00000000 | | Not used |
| Delay Import : | 00000000 | 00000000 | | |
| Com Descriptor : | 00000000 | 00000000 | >> | .NET Meta Directory |
| reserved : | 00000000 | 00000000 | | |

From header :

| | | | |
|------------------------------------|--------------------------------------|--------------|-------------|
| Size of headers : | 00001000 | Very often : | 400 or 1000 |
| Size of optional header : | 00E0 | | 00E0 |
| Number of Dirs : | 0010 | | 0010h |
| Base of Code : | 000B8000 | | 00001000 |
| Image Base : | 00400000 | | 00400000 |
| Magic optional header : | 010B | | 010B 32bit |
| Debugger Info - size : | No | | |
| File offset to PE : | 0080 | | click me |
| Checksum CRC : | 00000000 | | 00000000 |
| Machine type : | 0x14C Intel I386 (same ID used for 4 | | |
| OS version : | 4.0 4.0 Win NT 4.0 | | |
| From file | | | 4.0 |
| Image version : | 1.00 | | |
| File / sec-n alignment : | 0200 / 1000 | | File icon : |
| Entry Point to End of File bytes : | 1184 = 1.16 KB | | |

Imports :

| DllName | OriginalFirstThunk | TimeDateStamp | ForwarderChain | Name | FirstThunk |
|--------------|--------------------|---------------|----------------|----------|------------|
| KERNEL32.DLL | 00000000 | 00000000 | 00000000 | 000F9074 | 000F9050 |
| msvcrt.dll | 00000000 | 00000000 | 00000000 | 000F9081 | 000F9064 |
| USER32.dll | 00000000 | 00000000 | 00000000 | 000F908C | 000F906C |

| Thunk RVA | Thunk Offset | Thunk Value | Hint/Ordinal | API Name |
|-----------|--------------|-------------|--------------|----------|
|-----------|--------------|-------------|--------------|----------|

Clip

Close

Exeinfo Pe

Close

10/10,

10/12,

10/12,

Acti

me: C:\Users\Sand

978.2998046875 Ki

ima: 1 53e

Step 3.3 unpacked import table

Header info : [unpackPE-Import.exe] - Size of Code : 001C00h - decimal : 7 KB

| Directory Info : | RVA | SIZE | |
|------------------|----------|----------|-------------------------|
| Export : | 00000000 | 00000000 | >> Not used |
| Import : | 00006000 | 00000718 | >> (05) .idata |
| Resource : | 00000000 | 00000000 | 0 % of exe Nr of ID : 0 |
| Exception : | 00000000 | 00000000 | 1970-01-01 |
| Security : | 00000000 | 00000000 | not Signed |
| Base Reloc : | 00000000 | 00000000 | |
| Debug : | 00000000 | 00000000 | PB |
| Architecture : | 00000000 | 00000000 | 1970-01-01 |
| Global PTR : | 00000000 | 00000000 | |
| TLS Table : | 00008004 | 00000018 | >> (07) .tls |
| Load Config : | 00000000 | 00000000 | >> |
| Bound Import : | 00000000 | 00000000 | Not used |
| Imp.Table IAT : | 00000000 | 00000000 | Not used |
| Delay Import : | 00000000 | 00000000 | |
| Com Descriptor : | 00000000 | 00000000 | >> .NET Meta Directory |
| reserved : | 00000000 | 00000000 | |

From header : Very often :

| | | |
|---------------------------|----------|-------------|
| Size of headers : | 00001000 | 400 or 1000 |
| Size of optional header : | 00E0 | 00E0 |
| Number of Dirs : | 0010 | 0010h |
| Base of Code : | 00001000 | 00001000 |
| Image Base : | 00400000 | 00400000 |
| Magic optional header : | 010B | 010B 32bit |

Debugger Info - size : No

File offset to PE : 0080 click me

Checksum CRC : 00000000 00000000

Machine type : 0x14C Intel I386 (same ID used for 4

OS version : 4.0 4.0 Win NT 4.0

From file

Image version : 1.00

File / sec-n alignment : 0200 / 1000

Entry Point to End of File bytes : 968000 = 945.31 KB

Exeinfo Pe

Imports :

| DllName | OriginalFirstThunk | TimeDateStamp | ForwarderChain | Name | FirstThunk |
|--------------|--------------------|---------------|----------------|----------|------------|
| KERNEL32.DLL | 00000000 | 00000000 | 00000000 | 00006644 | 00006154 |
| msvrt.dll | 00000000 | 00000000 | 00000000 | 000066D8 | 000061A4 |
| USER32.dll | 00000000 | 00000000 | 00000000 | 0000670C | 0000622C |

| Thunk RVA | Thunk Offset | Thunk Value | Hint/Ordinal | API Name |
|-----------|--------------|-------------|--------------|----------|
|-----------|--------------|-------------|--------------|----------|

Step 4. I altered the code so that it duplicates the file endlessly and then compressed the .exe file with upx, and the modified file is tested malware by 7 detectors.

VIRUSTOTAL

SUMMARY DETECTION DETAILS BEHAVIOR COMMUNITY

SecureAge APEX Malicious ! Malicious

Avira (no cloud) ! HEUR/AGEN.1004702

CrowdStrike Falcon ! Win/malicious_confidence_60% (D)

Cybereason ! Malicious.0f36bf

Cylance ! Unsafe

F-Secure ! Heuristic.HEUR/AGEN.1004702

SentinelOne (Static ML) ! DFI - Suspicious PE

Acronis ✓ Undetected

Ad-Aware ✓ Undetected

AegisLab ✓ Undetected

AhnLab-V3 ✓ Undetected

Alibaba ✓ Undetected