WINDOWS MALWARE

STATIC CODE ANALYSIS

Created by Matthias


Hurry!
WARNING: A bomb has been detected in your computer! Click to defuse!
Timer: 2
Defuse

TOPICS

- Motivation
- Malware Structure
- Windows Background
- Come to wisdom
- Demo

MOTIVATION

MOTIVATION

MOTIVATION

Sun Tzu

“If you know the enemy and know yourself you need not fear the results of a hundred battles.”

MOTIVATION

MOTIVATION

Napoleon

“War is ninety percent information.”

MOTIVATION

- Understand Behavior vs AV Signatures
- Normal Attack Noise vs Frequency
- Build Emergency Plan
- Be better prepared

MALWARE STRUCTURE - TYPES

MALWARE STRUCTURE - TYPES

MALWARE STRUCTURE - TYPES

MALWARE STRUCTURE - TYPES

MALWARE STRUCTURE - TYPES

MALWARE STRUCTURE - TYPES

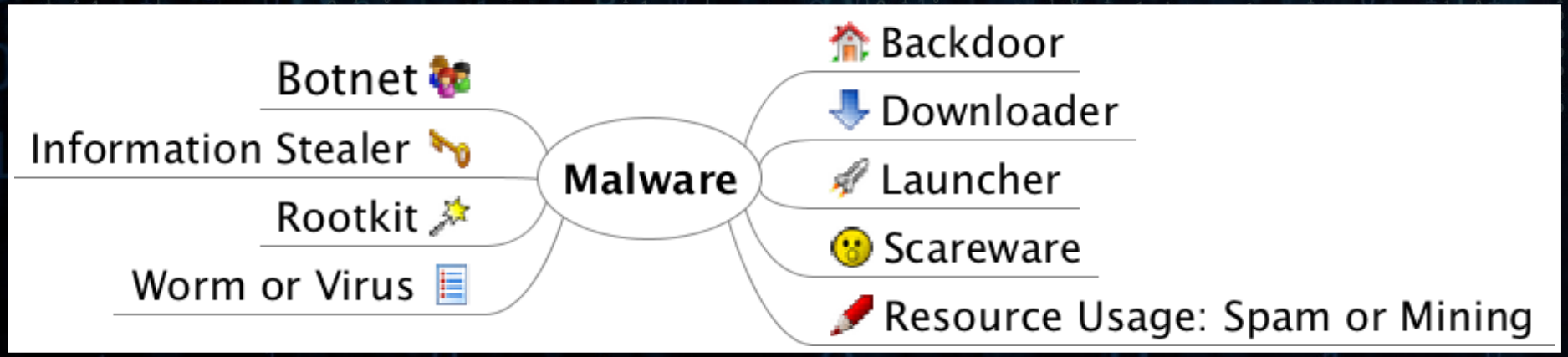
MALWARE STRUCTURE - TYPES

MALWARE STRUCTURE - TYPES

MALWARE STRUCTURE - TYPES

MALWARE STRUCTURE - TYPES

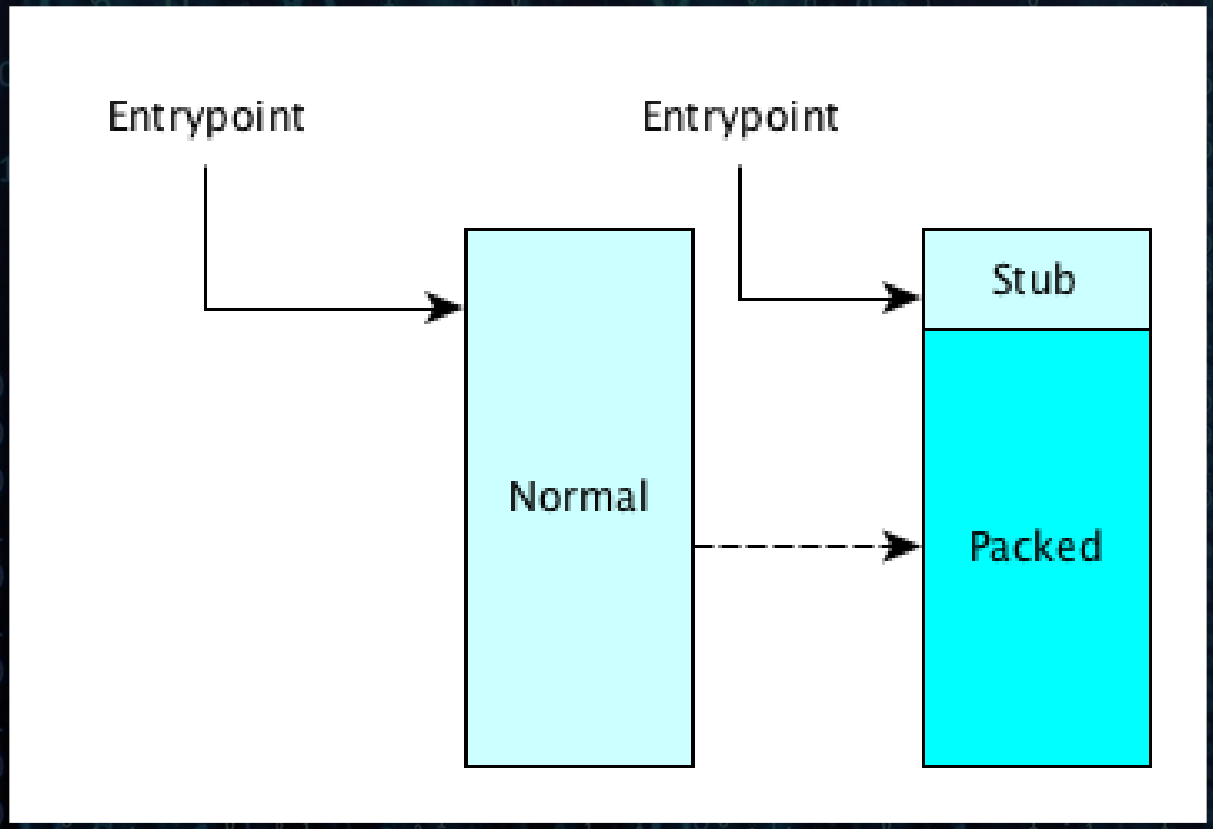
MALWARE STRUCTURE - TYPES



MALWARE STRUCTURE - OBFUSCATION

- Packer
- Cryptor

MALWARE STRUCTURE - OBFUSCATION



MALWARE STRUCTURE - OBFUSCATION

- UPX

```
upx -d file.exe -o out.exe
```

WINDOWS BACKGROUND - DLL

- Dynamic Link Libraries

WINDOWS BACKGROUND - DLL

- Kernel32.dll
- Advapi32.dll
- User32.dll
- Gdi32.dll
- Ws2_32.dll
- Wininet.dll

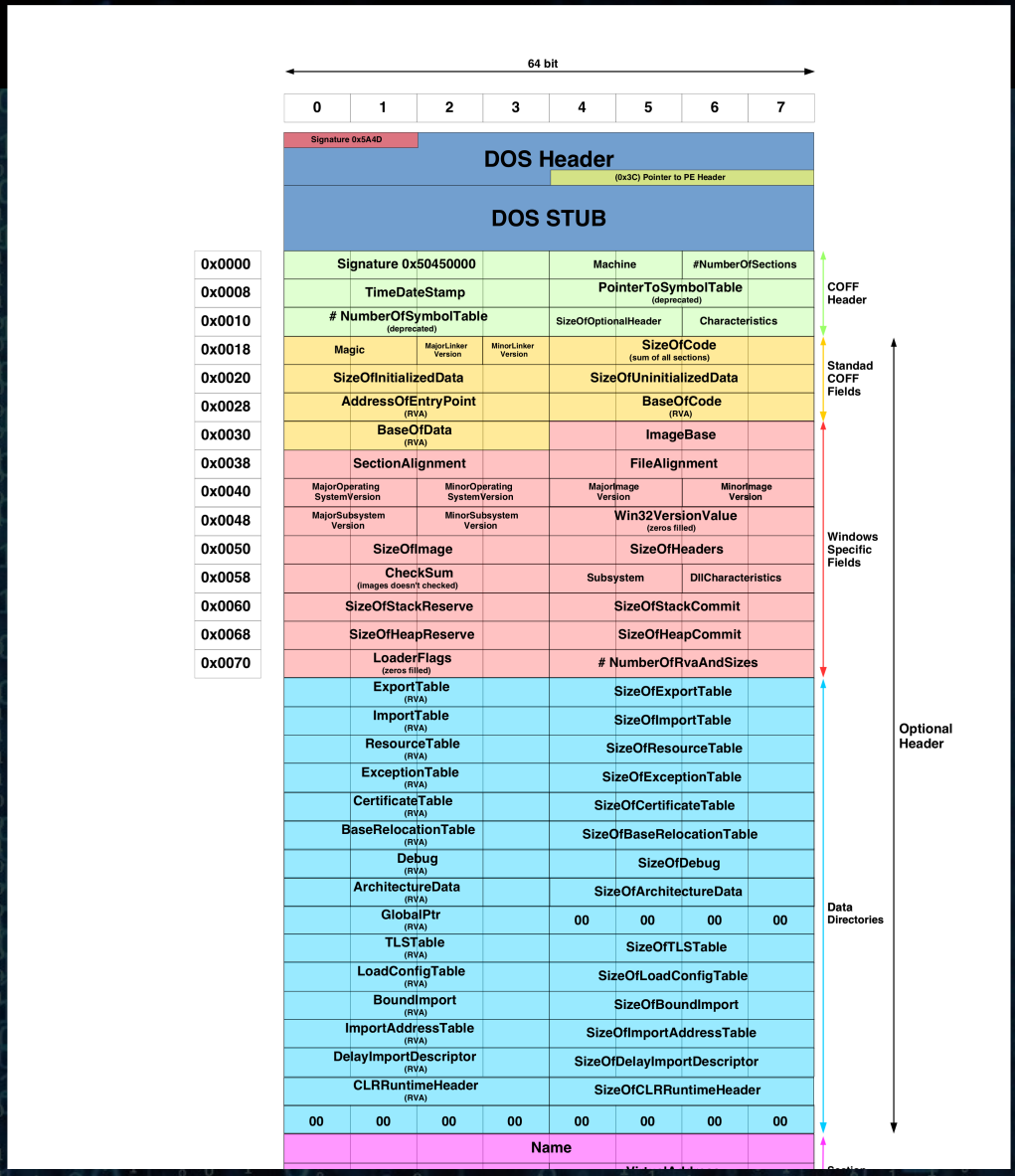
WINDOWS BACKGROUND - DLL

- InfoSec Windows Malware Functions I
- InfoSec Windows Malware Functions II

WINDOWS BACKGROUND - PE

- Portable Executable Format
- Imports
- Exports
- Time Date Stamp
- Sections
- Subsystem
- Resources

MALWARE STRUCTURE - PE



WINDOWS BACKGROUND - SECTIONS PE

- .text
- .data
- .rsrc

WINDOWS BACKGROUND - SECTIONS PE

- .rdata
- .idata
- .edata

COME TO WISDOM

- VirusTotal

COME TO WISDOM

- Hash
- Google it / Use it

```
md5 file
```

```
shasum file
```

COME TO WISDOM

- Strings
- Windows-Pendant

```
strings file
```

COME TO WISDOM

- PEiD

COME TO WISDOM

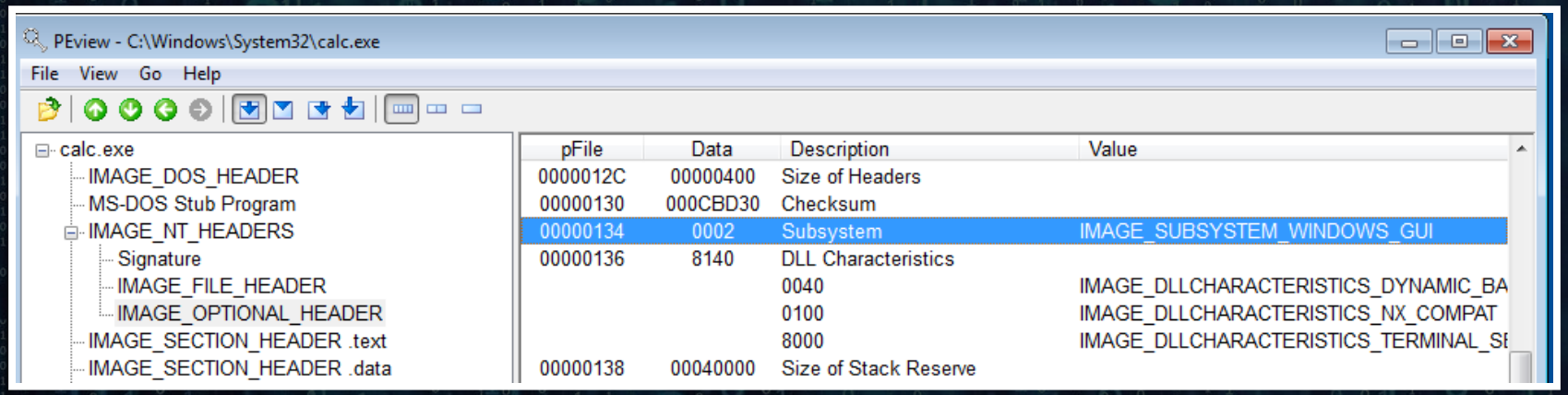
- PEView

COME TO WISDOM - PEVIEW

- IMAGE_NT_HEADERS - IMAGE_FILE_HEADER
- Time Date Stamp

COME TO WISDOM - PEVIEW

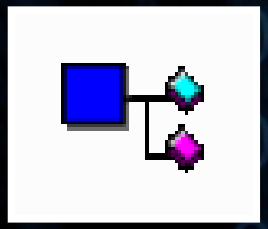
- Subsystem CUI vs GUI



COME TO WISDOM - PEVIEW

- Packer Detection
- Sections
- Virtual Size vs Size of Raw Data
- Odd Section Headers
- Few Imports

COME TO WISDOM - DEPENDENCY WALKER



- Imports
- Ordinals
- DLL Versions

COME TO WISDOM - RESOURCE HACKER

- .rsrc
- Icons, Images, Menus
- Strings
- Binary Data

DEMO

HAPPY REST MEETUP :-)