

# WINDOWS MALWARE

## STATIC CODE ANALYSIS

Created by Matthias



Hurry!



WARNING: A bomb has been  
detected in your computer! Click to  
defuse!  
Timer: 1

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

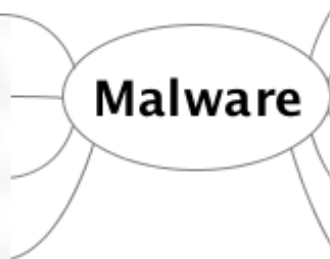




# MALWARE STRUCTURE - TYPES

Botnet 🤖

Malware





# MALWARE STRUCTURE - TYPES

Information Stealer



Malware





# MALWARE STRUCTURE - TYPES

Rootkit 

**Malware**





# MALWARE STRUCTURE - TYPES



Malware

Worm or Virus 



# MALWARE STRUCTURE - TYPES





# MALWARE STRUCTURE - TYPES





# MALWARE STRUCTURE - TYPES





# MALWARE STRUCTURE - TYPES





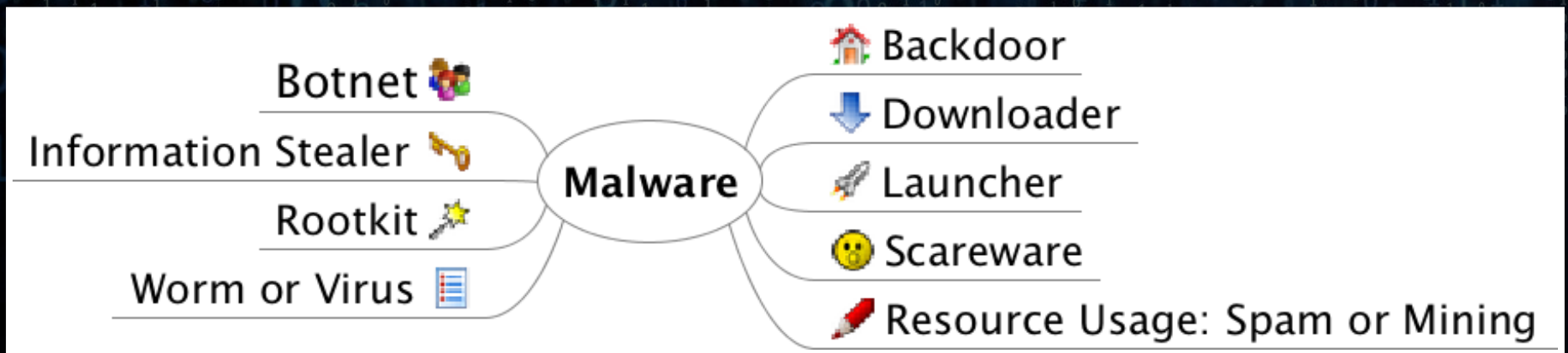
# MALWARE STRUCTURE - TYPES



**Resource Usage: Spam or Mining**



# MALWARE STRUCTURE - TYPES



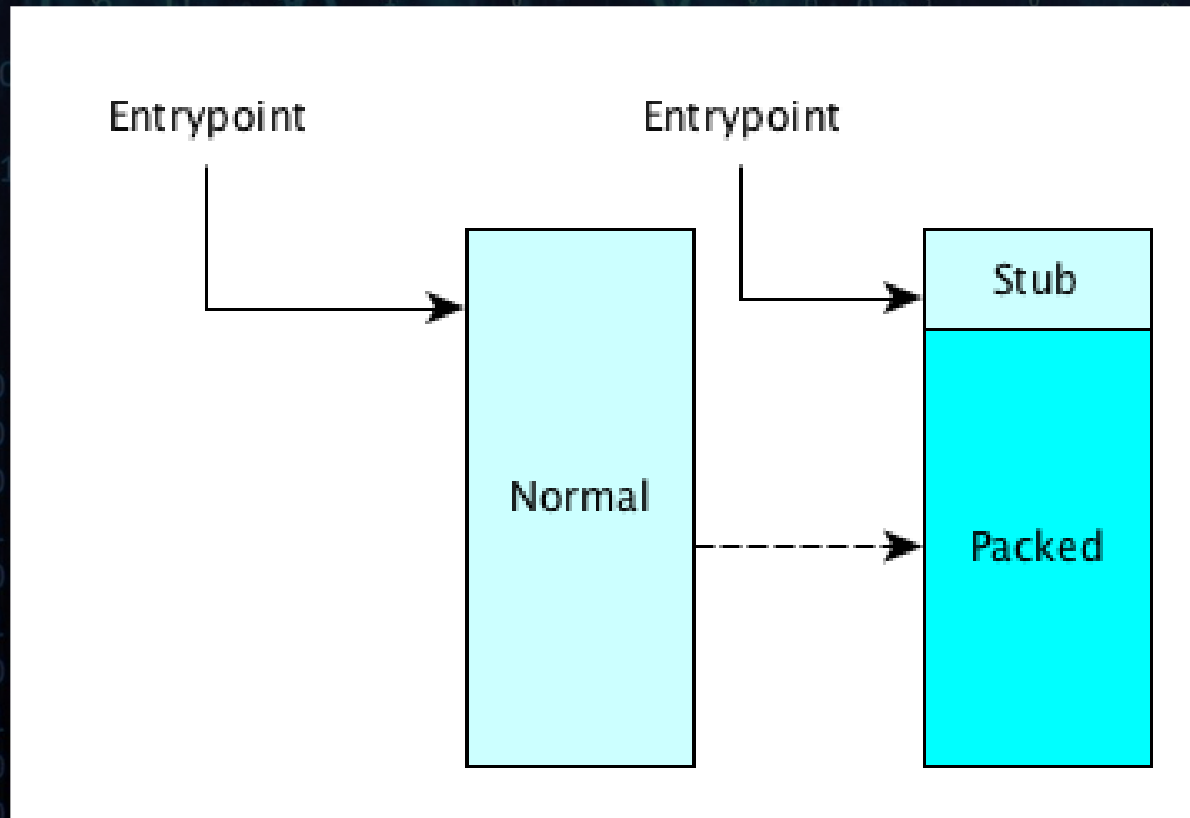


# MALWARE STRUCTURE - OBFUSCATION

- Packer
- Cryptor



# MALWARE STRUCTURE - OBFUSCATION





# MALWARE STRUCTURE - OBFUSCATION

- UPX

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



# WINDOWS BACKGROUND - DLL I

- Dynamic Link Libraries



# WINDOWS BACKGROUND - DLL II

- Kernel32.dll
- Advapi32.dll
- User32.dll
- Gdi32.dll
- Ws2\_32.dll
- Wininet.dll

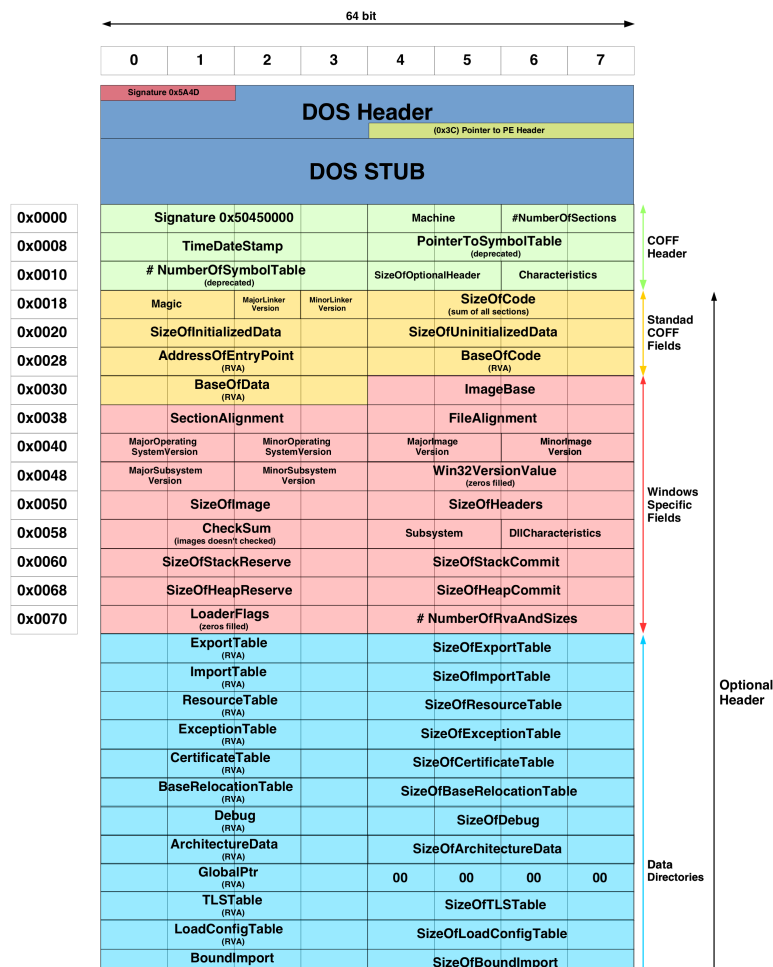


# WINDOWS BACKGROUND - PE

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



# MALWARE STRUCTURE - OBFUSCATION









# WINDOWS BACKGROUND - SECTIONS PE I

- .text
- .data
- .rsrc



# WINDOWS BACKGROUND - SECTIONS PE II

- .rdata
- .idata
- .edata



# COME TO WISDOM

- VirusTotal
- Hash
- Strings
- PEiD / UPX



# COME TO WISDOM - PREVIEW I

- IMAGE\_NT\_HEADERS - IMAGE\_FILE\_HEADER
- Time Date Stamp



# COME TO WISDOM - PVIEW II

- IMAGE\_NT\_HEADERS - IMAGE\_OPTIONAL\_HEADER
- Subsystem CUI vs GUI



# COME TO WISDOM - PEVIEW III

- 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 :-)

