CMSC 426
Principles of Computer Security

Malware Analysis

Last Class We Covered

- Live demo of malware analysis
- Types of malware
- Well-known malware families
  - Gratuitous examples of malware

Any Questions from Last Time?

Today's Topics

- Malware analysis
  - Basic/advanced
  - Static/dynamic
- Packing
- Sandboxes
- Malware signatures
- Exam review and details

Malware Analysis

	Static	Dynamic
Basic	Looking at details of the malware when it is “at rest” *ex*: virusTotal, strings	Running the malware and observing changes/output *ex*: regShot, DebugView
Advanced	Closely examining the malware’s code in detail *ex*: IDA Pro	Running the malware and using a debugger to control details of its execution *ex*: ollyDbg

Basic Static Analysis

- Examining the malware while it is “at rest”

- Plain-text strings within the code
- Hashes (MD5, SHA-1, imphash, fuzzy)
- Functions used (Windows API, etc.)
- General information (malware type and family)
- Other known instances of the malware

Basic Dynamic Analysis

- Observing the output and/or changes when the malware is run
  - But not interfering or interacting with the malware

- Debug/error messages the malware outputs
- Changes to the registry

Advanced Static Analysis

- Examining the malware's code (assembly) in detail
- Disassemblers organize the code into subroutines, and allow the analyst to more easily trace their way through the code
  - Much, much easier than reading the raw assembly
- This information is normally used to inform what actions the analyst takes in the debugger

Advanced Dynamic Analysis

- Using a debugger to control any and all aspects of the malware as it is being executed
  - Registers, stack, memory, and code

- In the demo, we saw this used to “trick” the malware into accepting any *incorrect* password as correct

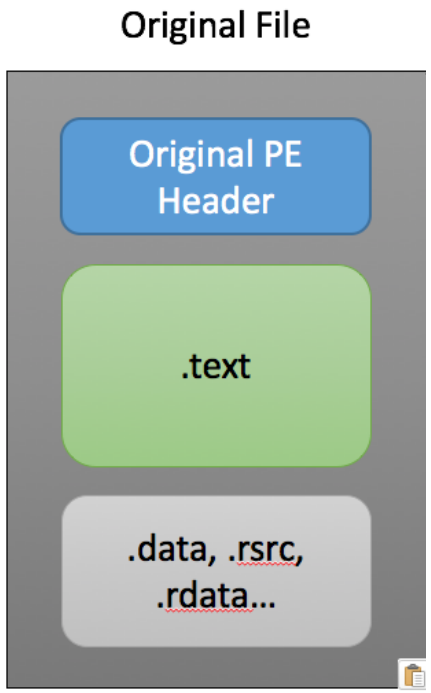
More Malware Analysis Info

Malware Packers

- Goal is to obfuscate information about the malware
  - Code, strings, and sometime imports
  - Makes the malware more difficult to analyze
- Does this by compressing and/or encrypting the malware
  - Simpler for the attackers than directly implementing protection within the code itself
- Decrease chance of detection and increase amount of time/effort required for effective analysis

Information taken from https://securingtomorrow.mcafee.com/business/malware-packers-use-tricks-avoid-analysis-detection/

Malware Packer Example



Information taken from https://securingtomorrow.mcafee.com/business/malware-packers-use-tricks-avoid-analysis-detection/

Sandboxing

- Automated technology for malware detection
  - Sandbox attempts to analyze the malware automatically
- Place malware into a closed, controlled environment
  - Simpler setup; less complex environment
- Reasons for using sandbox
  - Can’t cause any lasting damage
  - Easier to analyze

Information taken from https://www.apriorit.com/dev-blog/545-sandbox-evading-malware

Sandbox Evading

- Malware can attempt to recognize if it's in a sandbox
  - Won't do anything malicious if it realizes this is the case

- Some techniques include:
  - Not running unless certain dll files are available (many of which are not included in the sandbox)
  - Running at a specific date/time
  - Requiring user interaction (sandbox is automated)

Information taken from https://www.apriorit.com/dev-blog/545-sandbox-evading-malware

Malware Signatures vs Behavior

- Two different aspects of malware that can be analyzed

- Signature
  - Aspects of the malware that show up “at rest”
  - Strings and byte sequences
- Behavior
  - Actions the malware takes when run
  - API functions called, etc.

Midterm Info and Review

Exam Rules

- The midterm is closed everything:
  - No books
  - No notes
  - No cheat sheets
  - No laptops
  - No calculators
  - No phones

Exam Rules

- Place your bag under your desk/chair
  - NOT on the seat next to you
- You may have on your desk:
  - Pencils, erasers
    - You **must** use a pencil, not a pen
  - Water bottle
  - **UMBC ID**
    - You **must** bring your UMBC ID with you to the exam! We won't accept your test without it.

Exam Rules

- Your TA or instructor may ask you to move at any time during the test
  - This doesn't mean we think you're cheating

- That being said, **DO NOT CHEAT!!!**
- Cheating will be dealt with severely and immediately
  - There will be no retakes or partial credits

Exam Format

- Multiple Choice
- True/False
- Short answer
  - Similar difficulty to questions on homeworks/labs

Exam Content

- Heavy on stack overflow attacks, medium-light on malware
- Very little you should need to memorize by rote
  - Not going to ask about many specific pieces of malware
  - Very few acronyms will be used
- Exam is designed to test actual knowledge and understanding
  - If you didn't complete Lab 1, talk to someone who did (or come to office hours)

Exam Advice

- When you first get the exam...

- Write down your name
  - Make sure your name is ***legible*** and on the line
- Circle your section number
- Read the Academic Integrity agreement
  - Sign your name underneath

Announcements

- Paper 2 and 3 have been combined into one assignment – coming out next Wednesday, will have two weeks to complete
- Lab 2 coming out later today
- Midterm 1 is happening next class