Introduction to Malware Analysis

What is Malware Analysis and why is it Useful?

- Anti-Virus cannot be relied on
- 50% to 97% of Breaches involve malware
- Breach happens- Now what?
  - Typical:
    - Reimage the machine
  - Advanced: Incident Response
    - Analyze Logs, network traffic, strange processes etc.
    - Is it any where else?
    - How did it get there?
  - Mature: Gather Intelligence
    - What is the Impact?
    - What is the Risk?
    - Finically Motivated? Hacktivism? Opportunistic? Advanced Persistent Threat (APT)?

“70–90% OF MALWARE SAMPLES ARE UNIQUE TO AN ORGANIZATION.”
-Verizon Data Breach Report 2015

Scope

- Beginner’s Intro to:
  - Windows Malware Analysis
  - Basic Forensics / Incident Response / Malware Discovery
  - Basic Reverse Engineering
- Recommended Background:
  - Networking – TCP/IP
  - Operating System Internals
  - Programming (C, C++)
  - Software Vulnerabilities
  - Hacking

What is Malware

- **Mal**icious Soft**ware**
- Executes without permission or Knowledge
- Software Problems like every other product:
  - Compatibility Issues
  - Bugs
  - Customer service
  - Versions/Updating Issues
  - Team Development / Source Code Control

Malware Types/Functionality

General:

Virus	(file infector rare)
Trojan	(common)
Worm	(rare)
Bot	(very common)
Rootkits	(uncommon)
RAT	(Very Common)

More Specialized

- Scareware
- Spyware
- Adware
- Backdoors
- Credential Stealers
- Anti-Analysis
- Defenses
- Stealth
- Loader / Downloader

Other Malicious Software

- Builders
- Exploit Kit
- Packer / Crypter

Types of Analysis

- Dynamic Analysis
  - Executing the Malware. Simple, Fast. Easy to miss things.
- Static Analysis
  - Reverse Engineering. Slow, Deep technical knowledge. With enough time anything can be reversed
- Hybrid Static/ Dynamic
  - Most Analysis is a mixture: You find something in the disassembly then you confirm/investigate while the malware is executing.
  - Memory Forensics. Can be very useful, but is not the end-all-be-all

Basic Tools

- SysInternals - https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx
- MAP Pack - http://sandsprite.com/CodeStuff/map_setup.exe
- 010 - http://www.sweetscape.com/010editor/
- PE viewer: CFF Explorer, PE Exploter, PE View, PE studio
- A disassembler: IDA Pro, x64_dbg, Hopper, etc
- Other (personal preference):
  - Cygwin – md5sum, gcc, xxd, file, strings, python https://cygwin.com/install.html
  - Notepad++ - http://notepad-plus-plus.org/
  - 7zip

Note: keep it to a Minimum

One Minute Triage

- MAP -> MD5 Hash
  - Virus Total
    - Common names
    - Indicators of Compromise (IoC's)
  - Anubis
- Strings
- Hex Editor
- Next: Run it in a Virtual Machine (Next Video)

Get Samples

- Contagio Malware Dump: Free; password required
- KernelMode.info: Free; registration required
- Malshare: Free
- Malware.lu's AVCaesar: Free; registration required
- MalwareBlacklist: Free; registration required
- Malware DB: Free
- Malwr: Free; registration required
- Open Malware: Free
- SecuBox Labs: Free
- VirusShare: Free
- Catch Your own: Honey Pot
- Make your own:
  - Program Based on Description
  - Download a 'Builder': http://www.poisonivy-rat.com/

Note for the Paranoid:

- Some Malware can Execute upon:
  - Being Scanned
  - Viewing the Icon
    - Word
    - PDF
    - System Icon
  - Extracting the file from an Archive
- MD5 vs. SHA256

Recap & List Good Resources:

- What is Malware
- Malware Types and Functionality
- One Minute Triage
- Basic Tools
- Where to get Samples

- Practical Malware Analysis
  - Michael Sikorski, Andrew Honig
- Virus Research and Defense
  - Peter Szor