Basic Dynamic Analysis
VMs and Sandboxes

The Need for Dynamic Analysis

- Static analysis has many limits, especially on packed malware
  - Packing obscures metadata, strings, executable code
- Running malware exposes its behavior
  - How it interacts with filesystem, network, registry, etc

A Safe Analysis Environment

- It is very important to prepare an environment for safe dynamic analysis
- Need to set up VMs to run the malware on safely without infecting our host or allowing it contact with the outside world
- Some analysts run on “bare metal” machines that are air-gapped and can be reverted easily
  - Why would this be advantageous?

Safe Malware Analysis Inside a VM

- In order to analyze malware safely, VirtualBox's network settings need to be configured properly

Networking Mode	Host -> VM	VM -> Internet	VM -> Other VMs
Not Attached	X	X	X
NAT	X	✔	X
Bridged Adapter	✔	✔	✔
Internal Network	X	X	✔
Host-Only Adapter	✔	X	✔

Snapshots

- Can save the state of a VM, and revert to it later
- Take one before you run malware on your VM
- Revert once you are done with your analysis

Sandboxes

- Safe, isolated environment that replicates an operating system

- Automatically runs malware and reports on its behavior
  - Filesystem
  - Network connections
  - Registry / system configuration changes
  - Mutexes

Filesystem

- What files did the malware:
  - Read?
  - Create?
  - Modify?
  - Delete?

- Common malware behavior:
  - Copy itself to another location (especially to set up persistence)
  - Delete itself after running

Network

- Network traffic generated by malware may be communications with a command and control (C&C) server
- Malware often beacons to C&C at regular time intervals
- Sandbox saves traffic in a packet capture (pcap) for analysis
  - It is important to consider false positives, because some activity (such as NTP) may look like C&C

Registry

- The Windows Registry is used to store much of the information and settings for software programs, hardware devices, user preferences, operating system configurations, and much more

- Malware often interacts with the registry in the following ways:
  - Query registry keys
  - Create registry keys
  - Modify registry keys
  - Delete registry keys

Persistence

- Persistence – the ability to survive reboots

- Common registry keys used for persistence:
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\
  - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\

- Large list at https://www.andreafortuna.org/dfir/malware-persistence-techniques/

Mutexes

- Global variable that provides locking for shared memory
- Although used for legitimate purposes, frequently used to prevent re-infecting a victim
  - Malware queries for a specific mutex
  - If it does not exist, infects system and creates that mutex
- Can be unique indicators of compromise

Anti Sandbox techniques

- Detecting virtualization
- Stalling malicious activity until sandbox times out
- Detecting hooks (user level or kernel level)
- Prompting for user input / waiting for C&C response
- Sleep

Sandbox Demo!