Lecture 11
Dynamic Analysis

NMSU Reverse Engineering
Joshua Reynolds
Spring 2024

Static vs. Dynamic Analysis

Everything we have done so far in the course has not actually required us to run malware – but sometimes this is helpful.

If you run malware inside a **sandbox** with instrumentation, you can see what it does to that environment

If you run malware with a **debugger**, you can pause at strategic locations, such as right after a cryptor or packer has unpacked the actual code to be run.

If you run malware with a **network simulator**, you can find indicators of compromise, what data is exported, and where the malware looks for **C^2**

FakeNet - Network Simulation tool in FlareVM

Intro: https://www.mandiant.com/resources/blog/fakenet-ng-next-gen

“By default, FakeNet-NG is configured to start several most commonly used services:

- DNS Listener on UDP port 53
- HTTP Listener on TCP port 80
- HTTPS Listener on TCP port 443
- SMTP Listener on TCP port 25
- Raw Binary Listener on both TCP and UDP ports 1337. This service is also used as a default listener to handle all communications. Default listeners are explained below.”

RegShot - Registry Snapshot & Diff Tool in FlareVM

https://bromiley.medium.com/malware-monday-regshot-6826ae22ba29

Steps:

1. Define the snapshot scope by registry hive and directories
2. Take a snapshot before running the malware
3. Run the malware
4. Take another snapshot, and compare to the first

WinDBG – Windows GDB Equivalent

Debugger built by Microsoft (can also be used to debug kernel-mode drivers)

Activity 1 – Tutorial on how to use:

https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/getting-started-with-windbg

The textbook shows another debugger, x64dbg

(BTW, Ghidra and IDA both have built-in debuggers as well)

Sandbox Services

Run instrumented virtual machines, allow you to upload malware to run.

Run for limited time, and provide a report of files changes, registry keys changed, screenshots of pop-ups, etc.

EX:

- any.run
- hybrid-analysis.com
- joesandbox.com