Hybrid Malware Analysis Lab

Emily Eubanks (@droidmlwr)

> whoami

Emily Eubanks

> 2 Years Exp. Security Analyst Intern at MSP

> BSc Info Assurance & Cyber Defense

> AAS Computer Programming

> MiCCDC [2nd Place 2018], [1st Place 2019]

> Competed ISTS17 & ISTS18, Participated on ISTS20 Red Team

Follow along at github.com/droidmlwr/Presentations

Overview

- Architecture
- Malware Sample Run
  - Static Analysis
  - Dynamic Analysis
  - Findings
- Mistakes and Reflections
- Warnings
- Q & A

Physical & Cloud Architecture

Physical Architecture

Physical (Host) Machine: Xubuntu Linux

Analysis Machine(s): Win10 VM [192.168.1.x] [192.168.1.100 GW, DNS]

Monitoring Machine: Ubuntu Linux [192.168.1.100]

Physical Architecture

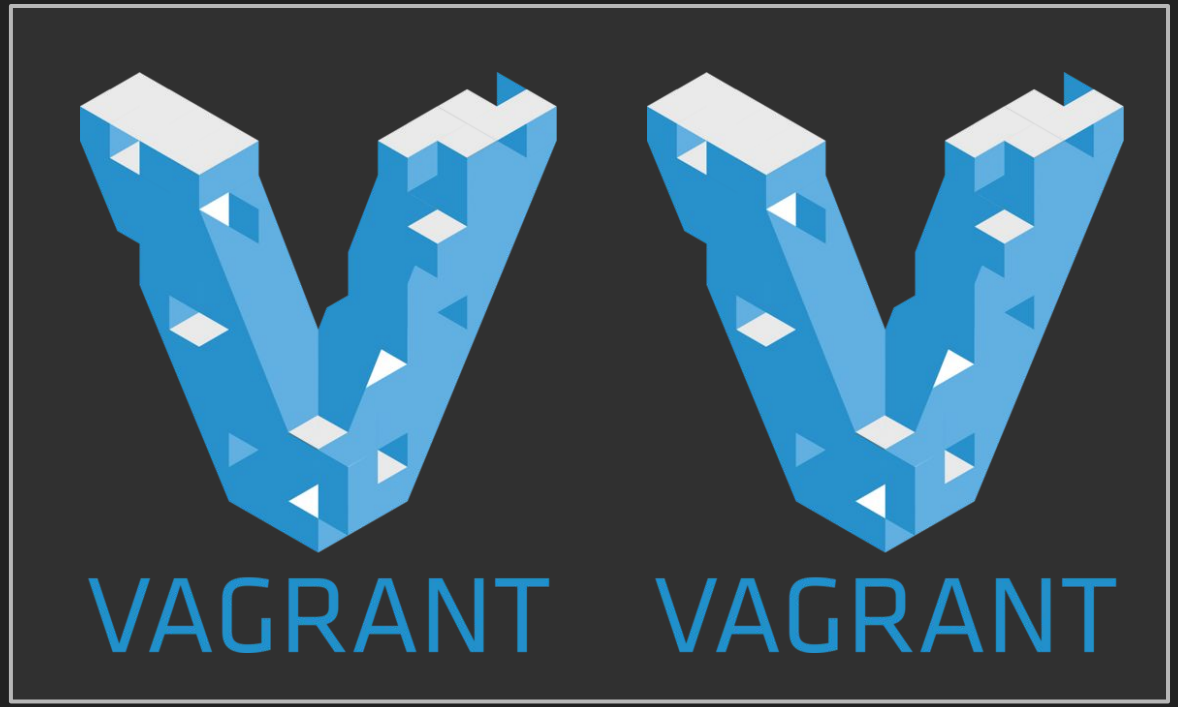
VirtualBox
16 GB RAM
4 CPU (8-Core)
i5-6300U 2.40 Ghz
HOST 10.0.0.x

Physical Architecture

VirtualBox
16 GB RAM
4 CPU (8-Core)
i5-6300U 2.40 Ghz
HOST 10.0.0.x

Physical Architecture

VirtualBox
16 GB RAM
4 CPU (8-Core)
i5-6300U 2.40 Ghz
HOST 10.0.0.x



Physical Architecture

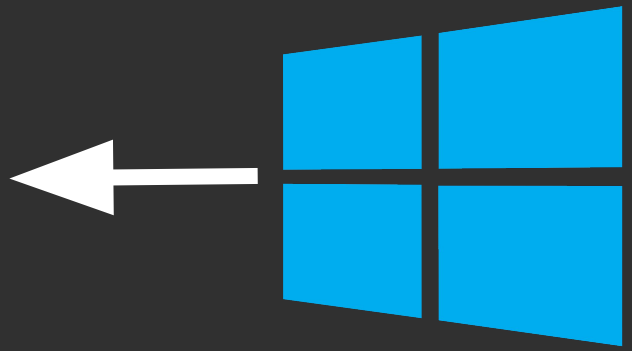
VirtualBox
16 GB RAM
4 CPU (8-Core)
i5-6300U 2.40 Ghz
HOST 10.0.0.x

Simulated DNS
Simulated Internet
Ubuntu 19.10

GW 192.168.0.254

Static & Dynamic
Analysis Machine
Windows 10 Dev

VM 192.168.0.1



Malware Sample Run

Static Analysis

Static Analysis

Filename

File creation date

File compile date

File size

File signatures

File hash signature

Dynamic Analysis

Findings

Mistakes & Things to Learn From

Warnings

Safe Local Lab Environments

Keep virtualization software up-to-date.

Spin up new VM with each investigation.

Do not store sensitive information in the VM.

To prevent malware from reaching the public internet, consider using “Host-Only” network configuration or restrict network traffic within the lab environment using simulated internet services.

Investigate Windows malware on a Linux machine and vice-versa. If malware escapes there is a lower change it will be able to infect the host machine.

Why Malware Analysis?

Determine type/nature/purpose of malware.

Deduce motive of attacker.

Gain understanding of system compromise.

Identify network signatures for prevention and detection controls.

Identify host-based signatures for prevention and detection controls.

Malware Analysis Types

- Code Analysis
  - Static Analysis
  - Dynamic (Behavioral) Analysis
- Memory Analysis (Memory Forensics)

Malware Types

Virus or Worm
Trojan
Backdoor / Remote Access Trojan (RAT)
Adware
Botnet
Information Stealer
Ransomware
Rootkit
Downloader/Dropper

Basic Malware Analysis

Static Analysis

Dynamic Analysis

Third-Party Malware Sandbox Reports

- VirusTotal - https://www.virustotal.com/
- Hybrid Analysis - https://www.hybrid-analysis.com/
- Joe’s Sandbox - https://www.joesandbox.com/

Basic Malware Analysis

Static Analysis

Dynamic Analysis

Third-Party Malware Sandbox Reports

- VirusTotal - https://www.virustotal.com/
- Hybrid Analysis - https://www.hybrid-analysis.com/
- Joe’s Sandbox - https://www.joesandbox.com/

Malware Lab Examples

MalwareTech's 2017 Malware Lab

All Versions of Windows 32 and 64 bit

Windows XP

Windows Vista

Windows 7

Windows 8

Windows 8.1

Windows 10

SudoSev's 2019 Malware Lab

Windows 7 Virtual Machine (home network)

Windows 10 Virtual Machine (home network)

Ubuntu 15.10 Virtual Machine (home network)

Ubuntu 14.04 SSH Honeypot (VPS)

Windows Server 2012 R2 (VPS)

Security Onion on an empty server which I'm still configuring

Various email spam traps for collecting macro malware & other specimens (such as phishing attempts or malware which may be hosted on a link in an email).

Emily’s 2020 Malware Lab

LOCAL

- Windows 10 (Dynamic Analysis)
- Windows 10 (IDA Freeware)
- Ubuntu 19.10 (Radare2)

AZURE

- Windows 10 (IDA Freeware)
- Windows 10 (Dynamic Analysis)

MALWARE ANALYSIS TOOLS

Static

IDA Freeware
PEiD (Plugins Dynamic)
PEExplorer
Dependency Walker
radare2
Binary Ninja
Resource Hacker
PEStudio
UPX

Dynamic

OllyDbg (Static & Dynamic)
Ghidra (Static & Dynamic)
Process Monitor
RegShot / TotalCommander
Process Explorer
Fakenet / ApateDNS
Hexinator
Wireshark / tshark / TCPdump
INetSim

Malware Sample Sources

Hybrid Analysis: https://www.hybrid-analysis.com/
KernelMode.info: http://www.kernelmode.info/forum/viewforum.php?f=16
VirusBay: https://beta.virusbay.io/
Contagio malware dump: http://contagiodump.blogspot.com/
AVCaesar: https://avcaesar.malware.lu/
Malwr: https://malwr.com/
VirusShare: https://virusshare.com/
theZoo: http://thezoo.morirt.com/
ANY.RUN: Registration required
Contagio Malware Dump: Password required
CAPE Sandbox
Das Malwerk
FreeTrojanBotnet: Registration required
Hybrid Analysis: Registration required

SNAPSHOT

Snapshot machine after first bootup.

Snapshot machine after installing software and any local configuration.

Snapshot machine after downloading malware.

Snapshot machine after executing malware.

SNAPSHOT

Snapshot machine after first bootup.

Snapshot machine after installing software and any local configuration.

Snapshot machine after downloading malware.

Snapshot machine after executing malware.

SNAPSHOT

Snapshot machine after first bootup.

Snapshot machine after installing software and any local configuration.

Snapshot machine after downloading malware.

Snapshot machine after executing malware.

Preventing Malware VM Detection

Windows API call “CheckRemoteDebuggerPresent” checks to see if a specific process is being debugged. (? Set to 1 for true or 0 for false.)

Harden VirtualBox to prevent malware from discovering it is operating in a virtual machine.

Hfiref0x - VBoxHardenedLoader - https://github.com/hfiref0x/VBoxHardenedLoader

Learning More

Learning More: Books