
A cluster of small squares in the top right corner, including cyan, pink, and orange colors, some with solid fills and others as outlines.

Malware Analysis

Anti-Virtual Machine Techniques

GVHD: Trương Tuấn Anh
Học viên: Đinh Thanh Phong

A small cluster of squares in the bottom left corner, including cyan and orange colors, some with solid fills and others as outlines.

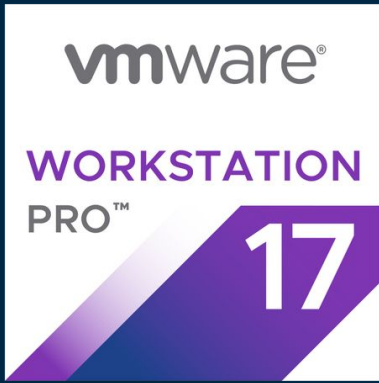
Virtual Machine

- Dynamic analysis is efficient and will show you exactly what the malware does
- Dynamic Analysis: Need to run malware while monitoring the results
- Dynamic Analysis: Requires a safe environment
- Tester must prevent malware from spreading to production machines



Virtual Machine

- The most common method
- Virtual Machine protects the host machine from the malware
- Except for a few very rare cases of malware that escape the virtual machine and infect the host
- Malware may detect that it is in a VM and run differently
- VMware has bugs: malware may crash or exploit it
- Malware may spread or affect the host - don't use a sensitive host machine



Virtual Machine

VMWare Fusion(MAC)/ Workstation(Windows/Linux):
VMWare has some great, comprehensive guides to install both Fusion and Workstation.

- VMWare does offer trial licenses for those interested in trying out the full feature set VMWare Pro line(Fusion Pro and Workstation Pro). VMware also has its Player line, which is free for personal use. Only downside is that the Player version doesn't allow network customization that you should use for your lab. Additionally, only Fusion Player has the ability to take snapshots. Which is the major difference between Workstation Player and Fusion Player.

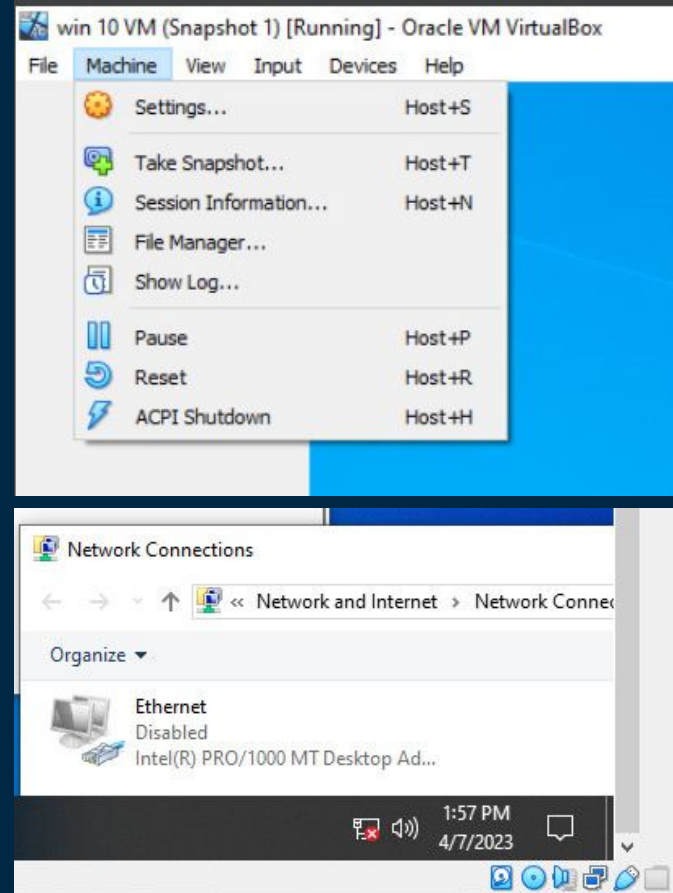


VirtualBox

- VirtualBox: Is the free alternative to VMware and some of the other virtualization software out there. It also has all the feature you need in a VM solution starting out.
- Support for taking snapshot
- Some other such as: Hyper-V, Parallels, or Xen

Virtual Machine

- First thing we should do is set up our isolated custom network we will be using for our lab. Being able to control how the network interacts with a malware sample is extremely important for analysis.
- You also don't want the malware sample to have access to the Internet(at least at first) until you have a decent understanding of what the malware is trying to do.



Virtual Machine

- All-in-one software for basic dynamic analysis
- Virtualized environment that simulates network services
- They are expensive but easy to use



Virtual Machine

FLARE VM



REMnux



Virtual Machine

- REMnux® is a Linux toolkit for reverse-engineering and analyzing malicious software.
- REMnux provides a curated collection of free tools created by the community. Analysts can use it to investigate malware without having to find, install, and configure the tools.
- REMnux is a free and open-source reverse engineering and malware analysis-oriented.
- It's a crowd favorite among professional malware analysts due to being modular and feature-rich.



Virtual Machine

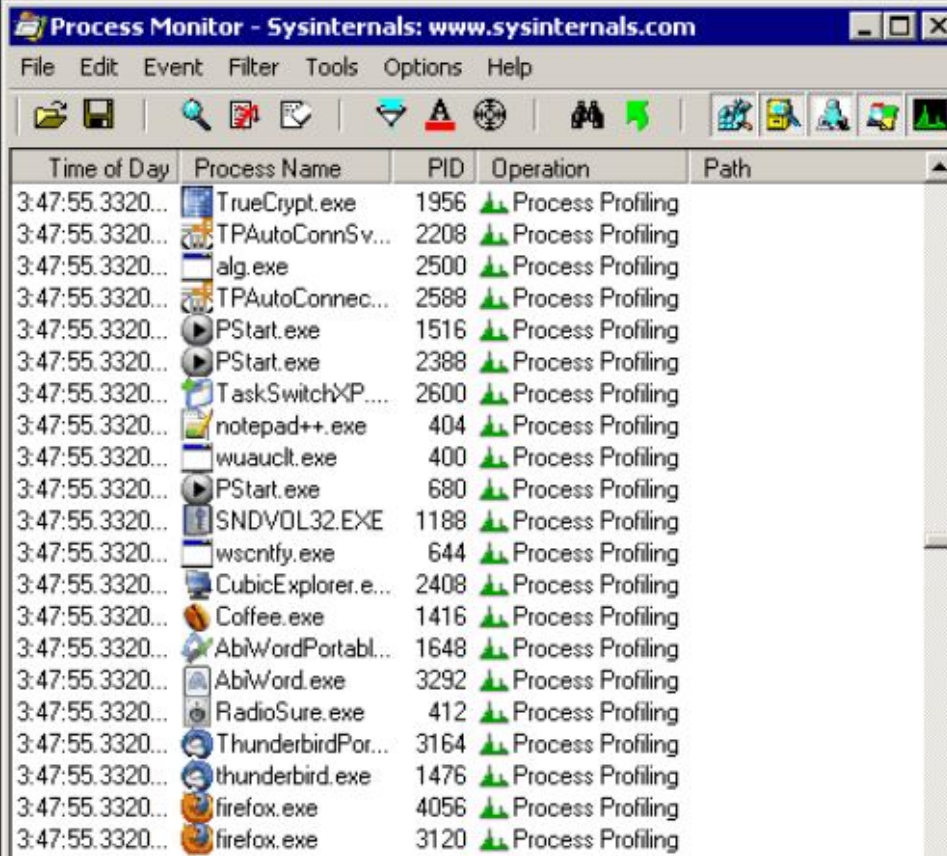
FLARE VM is a freely available and open sourced Windows-based security distribution designed for reverse engineers, malware analysts, incident responders, testers.

- Inspired by open-source Linux-based security distributions like Kali Linux, REMnux and others.
- FLARE VM delivers a fully configured platform with a comprehensive collection of Windows security tools such as debuggers, disassemblers, decompilers, static and dynamic analysis utilities, network analysis and manipulation, web assessment, exploitation, vulnerability assessment applications, and many others.



Virtual Machine

- Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity.
- All recorded events are kept, but you can filter the display to make it easier to find items of interest

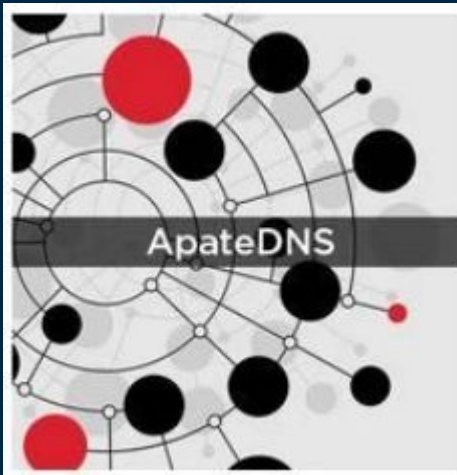


The screenshot shows the Process Monitor application window. The title bar reads "Process Monitor - Sysinternals: www.sysinternals.com". The menu bar includes File, Edit, Event, Filter, Tools, Options, and Help. The toolbar contains icons for file operations, search, and process management. The main display is a table with the following columns: Time of Day, Process Name, PID, Operation, and Path. The table lists various processes and their operations, all of which are "Process Profiling".

Time of Day	Process Name	PID	Operation	Path
3:47:55.3320...	TrueCrypt.exe	1956	Process Profiling	
3:47:55.3320...	TPAutoConnSv...	2208	Process Profiling	
3:47:55.3320...	alg.exe	2500	Process Profiling	
3:47:55.3320...	TPAutoConnec...	2588	Process Profiling	
3:47:55.3320...	PStart.exe	1516	Process Profiling	
3:47:55.3320...	PStart.exe	2388	Process Profiling	
3:47:55.3320...	TaskSwitchXP...	2600	Process Profiling	
3:47:55.3320...	notepad++.exe	404	Process Profiling	
3:47:55.3320...	wuauclt.exe	400	Process Profiling	
3:47:55.3320...	PStart.exe	680	Process Profiling	
3:47:55.3320...	SNDVOL32.EXE	1188	Process Profiling	
3:47:55.3320...	wscntfy.exe	644	Process Profiling	
3:47:55.3320...	CubicExplorer.e...	2408	Process Profiling	
3:47:55.3320...	Coffee.exe	1416	Process Profiling	
3:47:55.3320...	AbiWordPortabl...	1648	Process Profiling	
3:47:55.3320...	AbiWord.exe	3292	Process Profiling	
3:47:55.3320...	RadioSure.exe	412	Process Profiling	
3:47:55.3320...	ThunderbirdPor...	3164	Process Profiling	
3:47:55.3320...	thunderbird.exe	1476	Process Profiling	
3:47:55.3320...	firefox.exe	4056	Process Profiling	
3:47:55.3320...	firefox.exe	3120	Process Profiling	

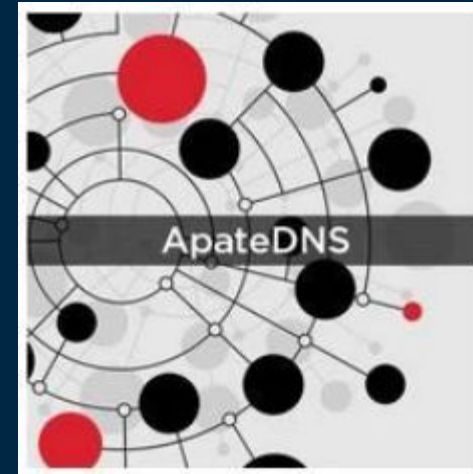
Virtual Machine

Faking a Network



Virtual Machine

- ApateDNS™ is a tool for controlling DNS responses through an easy-to-use GUI. As a phony DNS server, ApateDNS spoofs DNS responses to a user-specified IP address.
- ApateDNS also automatically sets the local DNS to localhost. Upon exiting the tool, it sets back the original local DNS settings.
- It comes in handy especially for network administrators who need to track DNS requests made by malicious software, trick the malware to send its traffic to a host, as well as catch additional domains used by viruses.



Virtual Machine

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection.

1. **Packet Capture:** Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
2. **Filtering:** Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.
3. **Visualization:** Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.



Virtual Machine

InetSim is a software suite for simulating common internet services in a lab environment, e.g. for analyzing the network behaviour of unknown malware samples.

InetSim supports simulation of the following services: HTTP, SMTP, POP3, DNS, FTP, NTP, TFTP, IRC, Ident, Finger, Syslog, 'Small servers' (Daytime, Time, Echo, Chargen, Discard, Quotd)

Additional features:

- Faketime
- Connection redirection
- Detailed logging and reports



Cảm ơn thầy và các bạn.

