Basic Dynamic Processes Analysis of Malware in Hypervisors: Type I & II

Ibrahim Waziri Jr, *CERIAS – Purdue University*
Under the direction of: Dr. Sam Liles

Abstract
This study compares, analyze and study the behavior of a malware processes within both Type 1 & Type 2 virtualized environments. In other to achieve this we set up two different virtualized environments and thoroughly analyze each malware processes behavior. The goal is to see if there is a difference between the behaviors of malware within the 2 different architectures. At the end we achieved a result and realized there is no significant difference on how malware processes run and behave on either virtualized environment. However our study is limited to basic analysis using basic tools. An advance analysis with more sophisticated tools could prove otherwise.

Implementation:
In this section, the type I and type II hypervisor environments set up, the malware analysis, the tools used, the resources and hardware used to achieve the goal of this study were introduced. Before carrying out the dynamic analysis, we run a basic static analysis of the malware to give us an idea of what type of malware we are dealing with.

Tools:
Basic Static Analysis: Virustotal.com, PEiD, PEView
Basic Dynamic Analysis: Process Monitor, Process Explorer
The hardware and environmental setup tools used are: VMware ESXi 5.0 hypervisor, VMware vSphere Client, Windows 8.1 64bit OS, VMware Fusion 7 – Hypervisor for OS X.

Type I Environment:
Windows 8.1 operating system with all the tools mentioned used for basic static and dynamic analysis above installed, runs as a virtual machine on a VMware ESXi 5.0 hypervisor installed on a server. A VMware vSphere Client is used to control and monitor the virtual machine. The VMware VSphere is installed inside a Windows 8.1 operating system running on a standalone computer. Figure 1 depicts the Type I Environment infrastructure architecture.

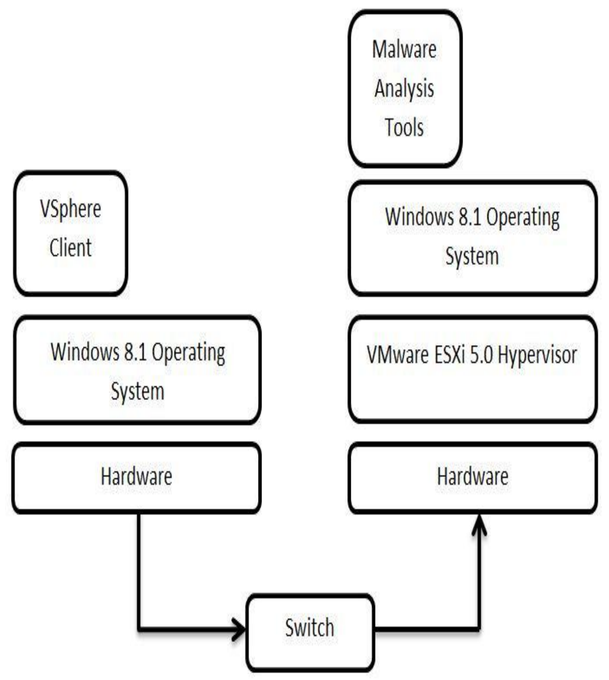

Fig 1: Type I Architecture

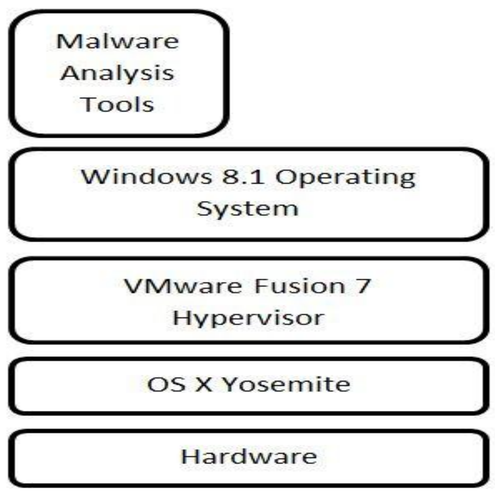

Fig 2: Type II Architecture

Type II Environment:
Another Windows 8.1 operating system with all the malware analysis tools runs as a virtual machine within VMware Fusion 7 hypervisor. The VMware Fusion hypervisor is installed on an OS X Yosemite running on a MacBook Pro laptop. Figure 2 shows the Type II environment architecture.

Results:

	Virus Total		PEiD		PEview	
	Type I	Type II	Type I	Type II	Type I	Type II
Virus Signature	✓	✓				
Compilation Date	✓	✓			✓	✓
Import/Exports	✓	✓			✓	✓
File Size	✓	✓			✓	✓
File Type	✓	✓				
Target OS	✓	✓				
Packed/Unpacked			✓	✓		
Compiler			✓	✓		
Section Numbers					✓	✓
Headers					✓	✓
Time Stamp					✓	✓
Dialog					✓	✓
Accelerators					✓	✓
Version Info					✓	✓

Basic Static Analysis Comparison

	Process Monitor		Process Explorer	
	Type I	Type II	Type I	Type II
Registers			✓	✓
Libraries			✓	✓
Execution Time	✓	✓		
CPU Load	✓	✓		
Average Memory	✓	✓		
Process Name	✓	✓	✓	✓
PID (Process Identifier)			✓	✓
Operation	✓	✓		
Path Address	✓	✓	✓	✓
Category			✓	✓
TID (Thread Identifier)			✓	✓

Basic Dynamic Process Comparison

Conclusion:
This study focused on a comparison of malware processes behavior within a Type I and II hypervisor environments. The analysis was meant to see the difference and similarities between the two architectures. From the analysis result, we see in a tabular form that there is no significant difference between how malware processes run in a Type I environment and that of a Type II. However the analysis we did is just a ground work for malware analysis. To conclude if malware behavior is different or the same within the two types of hypervisors, an advance malware analysis must be carried. This could be the future of this study.