Evasive Malware Detects and Defeats Virtual Machine Analysis

lastline.com/blog/evasive-malware-detects-and-defeats-virtual-machine-analysis/

October 24, 2016

Posted by Lastline ON OCT 24, 2016

Advanced malware solutions ("sandboxes") traditionally use virtual machines (VM) to analyze suspicious objects to find out if they are malicious. However, advanced malware is capable of detecting the presence of the virtual machine technology used by conventional sandboxes and leveraging this weakness to evade detection.

Sandbox technologies typically leverage VM environments like VMware, Xen, Parallels/Odin and VDI. This allows a user or an administrator to run one or more "guest" operating systems on top of another "host"operating system. Each guest operating system executes within an emulated environment and allows managed access to both virtual and actual hardware. In theory, the environment provided by the VM is self-contained, isolated, and indistinguishable from a "real" machine.

VM technology has long been considered an effective approach for analyzing malware because it provides an isolated environment or sandbox where the malware can be triggered and monitored. However, today's advanced malware is more sophisticated and is quite capable of evaluating a VM environment and tailoring its actions to avoid detection.

Advanced Malware Easily Detects VM Environments

Conventional sandbox analysis inserts artifacts into the guest operating system, which allows advanced malware to determine if a system is running in a virtual environment. Here are some of the techniques used by malware to recognize VM environments:

- Examining registry keys for values that are unique to virtual systems. In VMware, there are over 300 references in the registry to “VMware”.
- Looking to see if VM tools are installed. In a VMware Windows Workstation, there are over 50 references in the file system to “VMware” or “vmx”.
- Checking for certain process and services that are specific to VM environments such as VMwareService.exe, VMwareTray.exe, etc.
- Identifying the BIOS serial number or MAC address of the virtual network adapter to reveal the vendor. For example, MAC addresses beginning with 00-05-69, 00-0c-29, 00-1c-14 or 00-50-56 are associated with VMware.
- Analyzing specific structures within system Memory, such as the Store Interrupt Descriptor Table (SIDT), Store Local Descriptor Table (SLDT) and Store Task Register (STR). These tables are located in different areas for VM environments compared with physical machines.
- Examining specific hardware parameters that are unique to either VM or real physical environments. Advanced malware may query various attributes like serial numbers or other values belonging to the motherboard, processor, SCSI controller, etc.

It has become easier for malware to detect its target environment and take evasive action because many of the toolkits designed to perform VM analysis are readily available to those who create malware. Not surprisingly, as malware becomes more sophisticated, enterprise systems become more vulnerable to destructive cyber attacks.

Advanced Malware Alters Its Behavior When a VM is Detected

Once modern malware detects a virtual machine, it can alter its behavior to avoid detection by using some of the following tactics:

- The injection or modification of code within other applications will be suspended until operating outside of the VM.
- Advancements to establish persistence and download additional code will be put on hold.
- Malicious code will remain encrypted or otherwise hidden.
- Attempts to move laterally within the network will be suspended until the malware is operating outside of the sandbox or VM.
- Connections to the malware’s command and control servers (CNC) will be avoided.

By modifying its behavior, malware can avoid detection by traditional or first-generation security solutions running in virtualized environments.

Unlike conventional sandboxing solutions, the next-generation Lastline products possess an entirely different architecture that does not produce artifacts, making it more difficult for malware to determine its location. In fact, the Lastline solution is specifically designed to detect advanced malware, even when it uses sophisticated evasion techniques.

Click here to learn more about the Lastline solution.

- About
- Latest Posts

Lastline

Latest posts by Lastline (see all)

- Lastline Boosts SOC Efficiency by 100%, Effectively Doubling Productivity of SOC Teams - May 21, 2020
- Lastline Named as One of the Best Places to Work - February 20, 2020
- Don’t Hate Your Legacy IDPS – Replace It - February 3, 2020

Tags:

Advanced Malware Detection, Avoid Detection, Cyberattack, Evasive Malware, Sandboxing, VM