intel Security

ew

Malware Sandbox Overview, Advantage and Challenge

June 2016

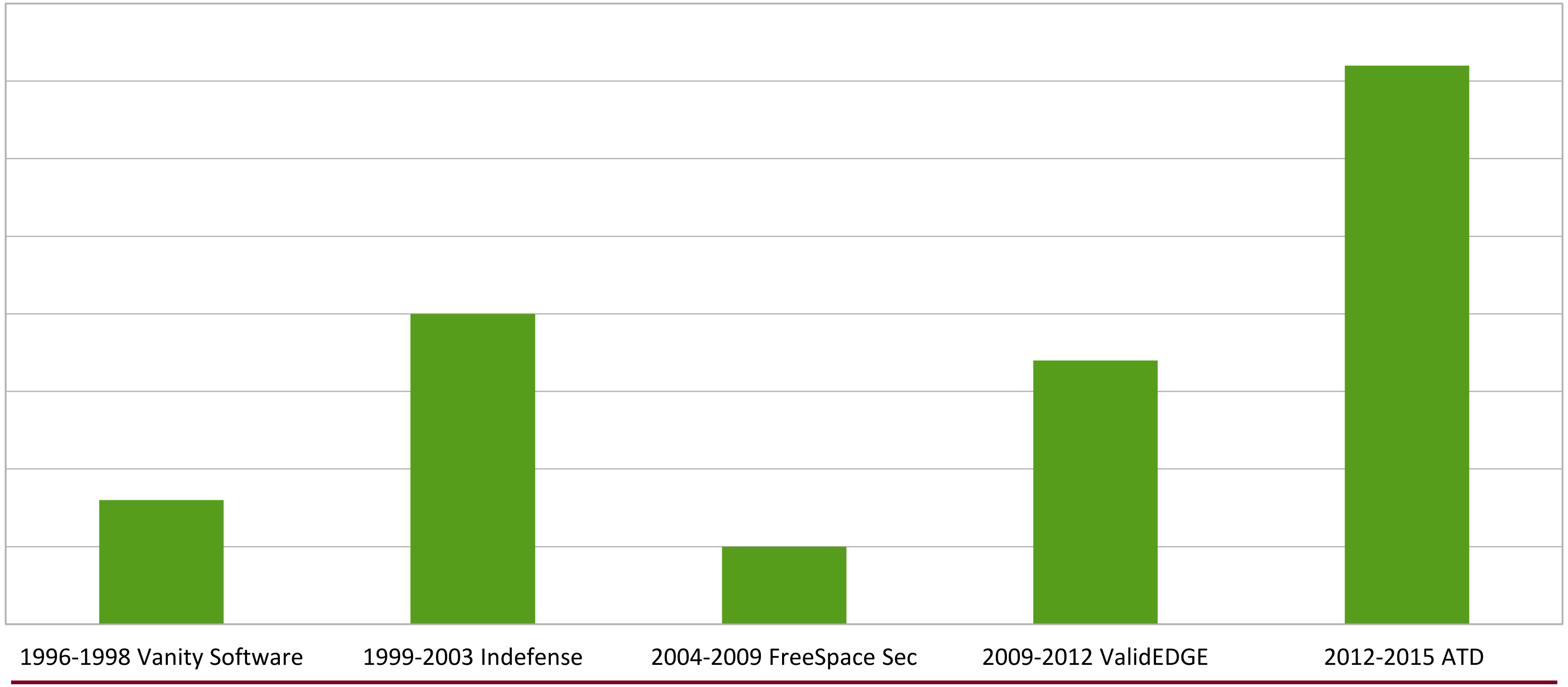
TM

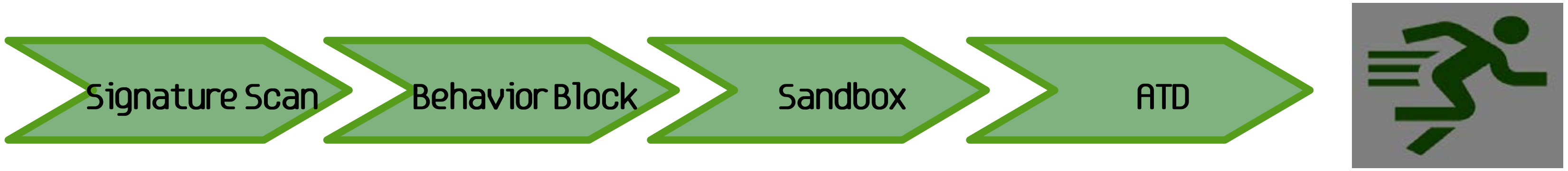
Lixin Lu (Chief Scientist)

Agenda

- **Introduction**
- **What is malware sandbox ?**
- **Malware Sandbox Architecture**
- **Sandbox Advantage**
- **Sandbox Challenge**
- **Sandbox Future**
- **Q&A**

Security and Entrepreneur Experiences





What is Malware Sandbox?

In computer security, a **sandbox** is a security mechanism for separating running programs. It is often used to execute untested code, or untrusted programs from unverified third parties, suppliers, untrusted users and untrusted websites.

--Wikipedia

In general, a **sandbox** is an isolated computing environment in which a program or file can be executed without affecting the application in which it runs.

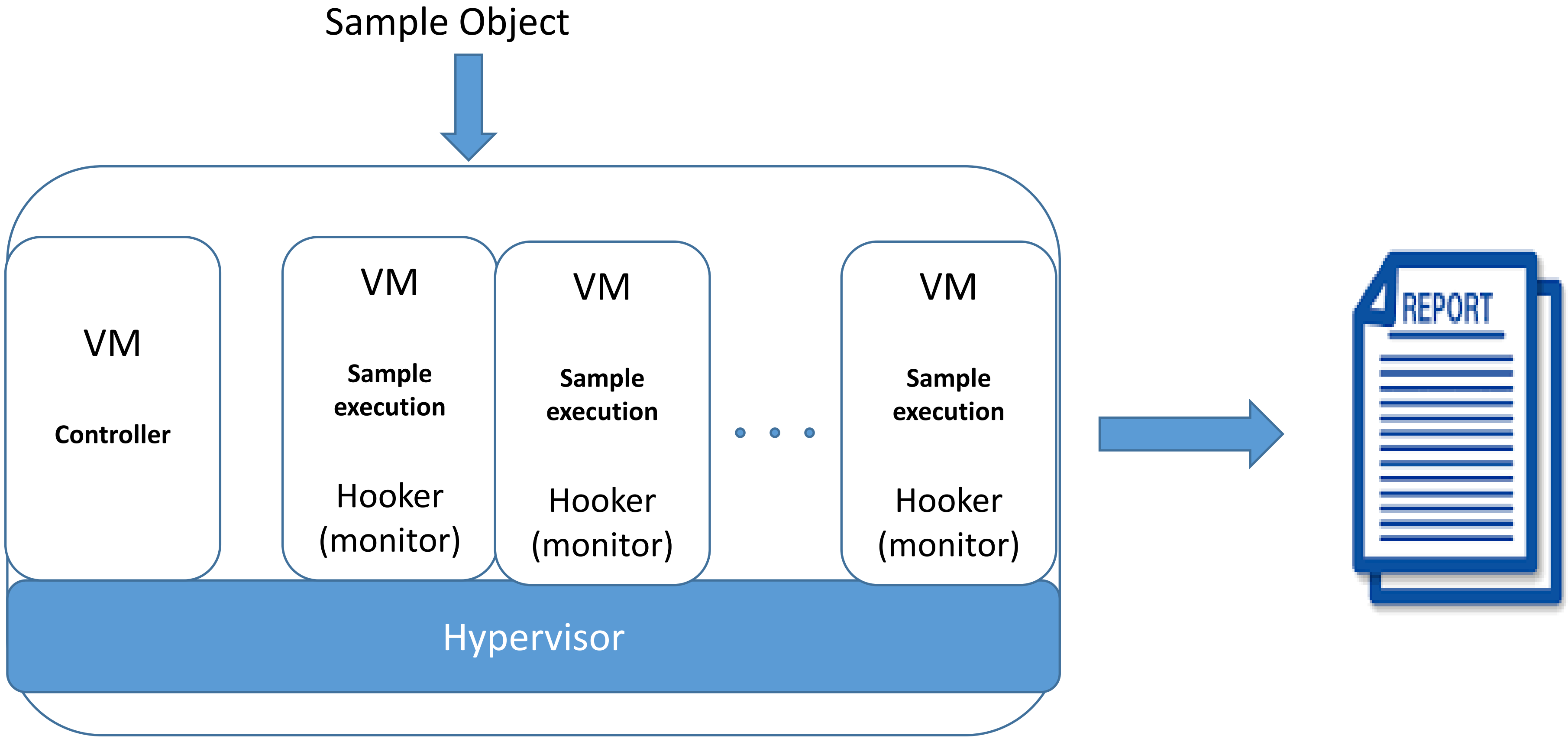
--TechTarget

Sandbox = Isolated Computing Environment + Security

Malware Sandbox = Isolated Malware Execution Environment + Security + Monitor

Malware Sandbox Purpose → Obtain Malware Behavior → Detect Malware

Malware Sandbox Architecture



- File structure
- Behavior IOC
- Disassembly list
- Convict merit points
- API call log
- Other artifacts

Sample object input → VM Guest OS → Monitor → Behavior Analysis → Reports

Malware Sandbox Advantage

Signature scanner detects malware if and only if its signature is available, while sandbox can detect new malware without signature;

Heuristic scanner can detect some new malware without exact signature, but often produce many false negatives, while sandbox collects more evidence, greatly increase detection rate;

Behavior blocking can detect new malware without signature, but it often produces many false positives, while sandbox can wait till a program to complete its entire execution, greatly reduces false positives;

Sandbox can defeat most malware packing and encryption mechanism;

Sandbox helps SOC operator during malware reverse engineering research.

Malware Sandbox Challenge

Sandbox is slow in general, it needs to wait for malware completing execution;

Sandbox needs system API hook and monitor, which can be easily detected by malware during execution;

Sandbox environment and limited resources can cause malware's behavior differently from real world environment;

Some malware need live connection and info exchange or user interaction during its runtime, which is usually not available in sandbox and thus missed detection;

Malware can be file-less or memory only, there is nothing to be sent to sandbox for analysis;

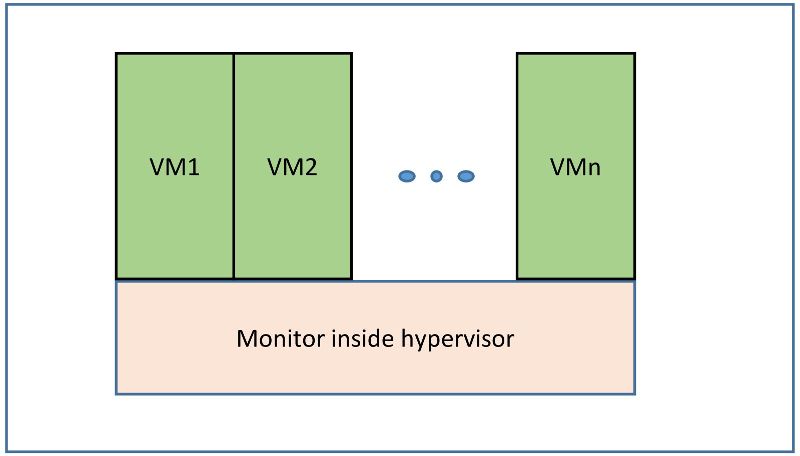
Malware can spread in multiple pieces and/or embedded into video/image files, to avoid sandbox analysis.

Malware Sandbox Future

Sandbox in cloud

- Hybrid VM and physical environments;
- No resource limitation
- Leverage other intelligence;
- Easier to update and more service coverage.

Monitor inside hypervisor



- No change to VM guest OS;
- No hooker to be detected.

- Using sandbox to improve SOC and Lab operation process, to help malware reverse engineering and deep analysis;
- Integrate sandbox with multiple products, such as FW, IPS, and endpoint products, to provide security-connected solution;
- Leverage sandbox on micro level analysis with big data mining and machine learning on macro level, to improve overall security ecosystem.

Q & ***A***