ASSURED

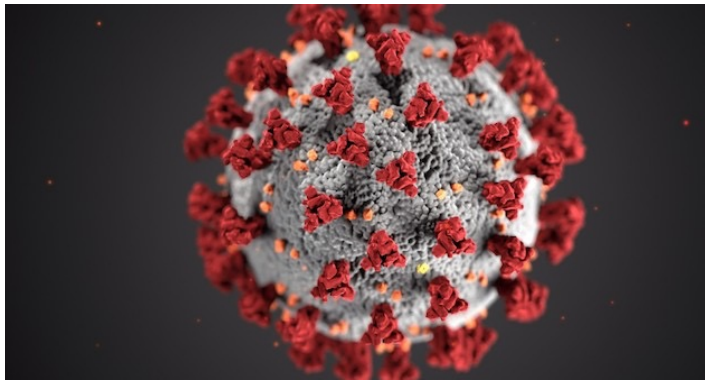
Non-intrusive Code Coverage: How to Use ASSURED for Trace-based Debugging and Runtime Analysis

Dr Ahmad Atamli

TOWARDS SUSTAINABLE SECURITY IN SYSTEMS-OF-SYSTEMS - ASSURED Webinar

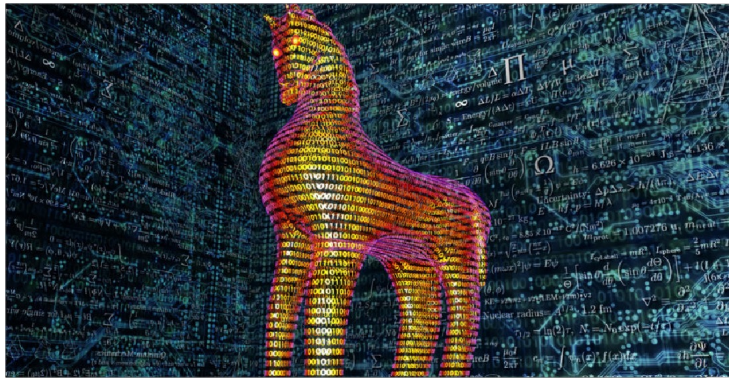
June 2023

Malicious Entities



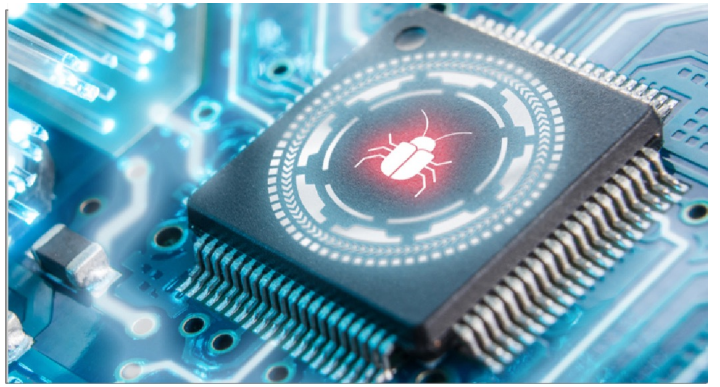
Viruses
Infect and replicate existing files on the target system

Worms
Spread to other systems using computer network



Trojans
Misrepresents themselves to appear useful

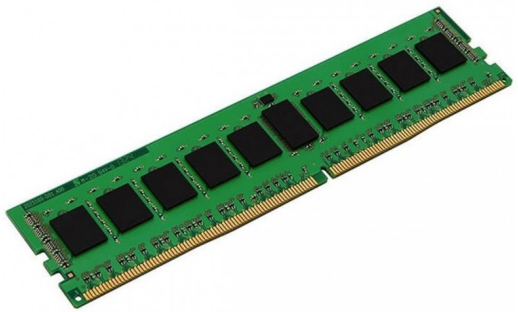
Keyloggers
Record every keystroke



Rootkits
Remotely execute commands/files and change system configurations

WHERE TO LOOK?

Indications of compromise are not easy to find



System Memory

File System

Network

Virtual Machine Introspection

ASSURE

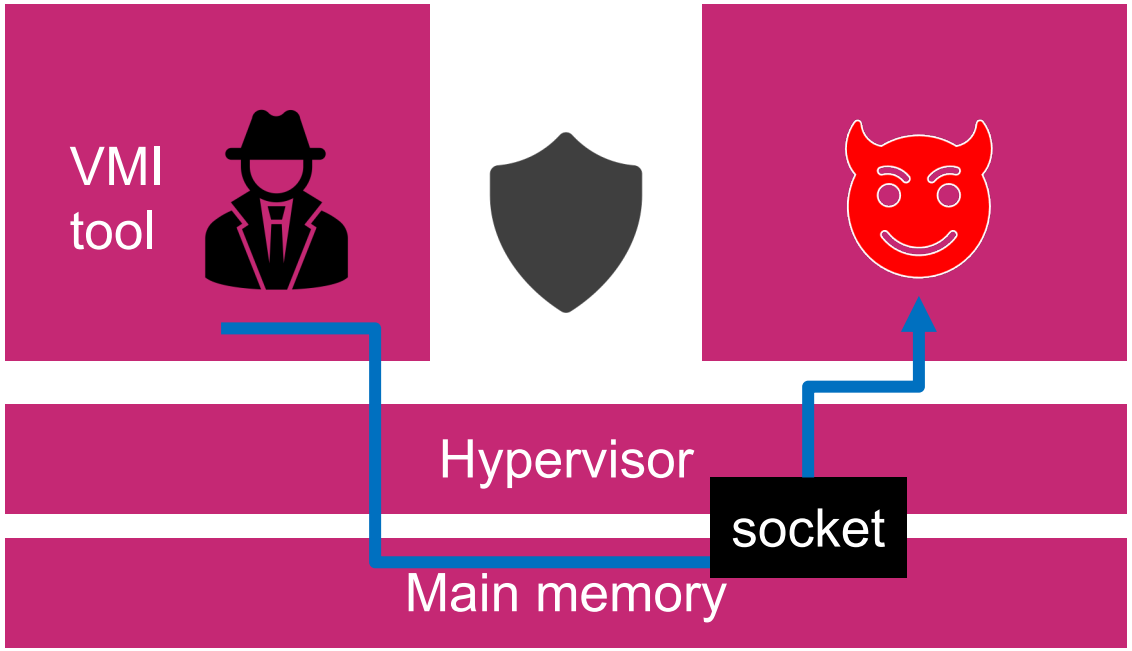
"If the IDS resides on the host, it has an **excellent view** of what is happening in that host's software but is **highly susceptible to attack**. . .if the IDS resides in the network, it is more **resistant to attack**, but has a poor view of what is happening inside the host, making it more **susceptible to evasion**. . .**an architecture that retains the visibility of a host-based IDS**, **but pulls the IDS outside of the host for greater attack resistance**. We achieve this through the use of a virtual machine monitor. Using this approach allows us to isolate the IDS from the monitored host but still retain excellent visibility into the host's state. The VMM also offers us the unique ability to completely mediate interactions between the host software and the underlying hardware."

A Virtual Machine Introspection Based Architecture for Intrusion Detection. Tal Garfinkel, Mendel Rosenblum, 2003

What does non-intrusive means?

Virtual Machine Introspection (Intrusive)

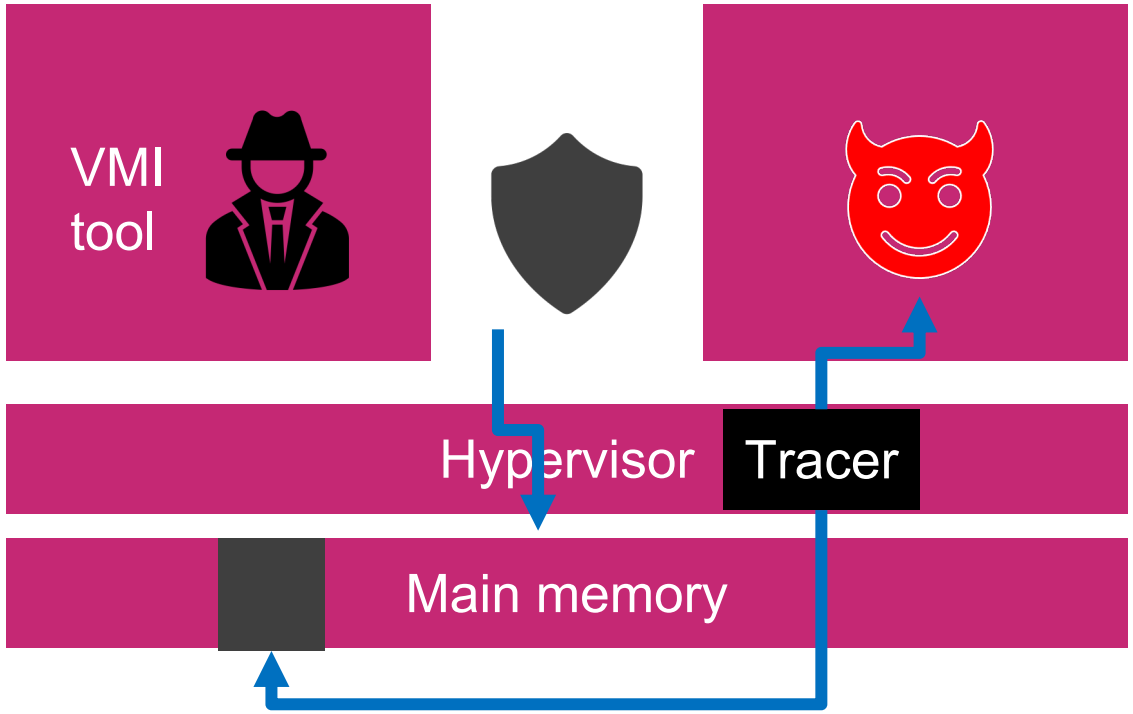
- The VMI tool is synchronized with the inspected VM
  - Hyper calls (Xen)
  - Agents on the VM communicating to Hypervisor (Vmware)



Virtual Machine Introspection (non-intrusive)

ASSURE

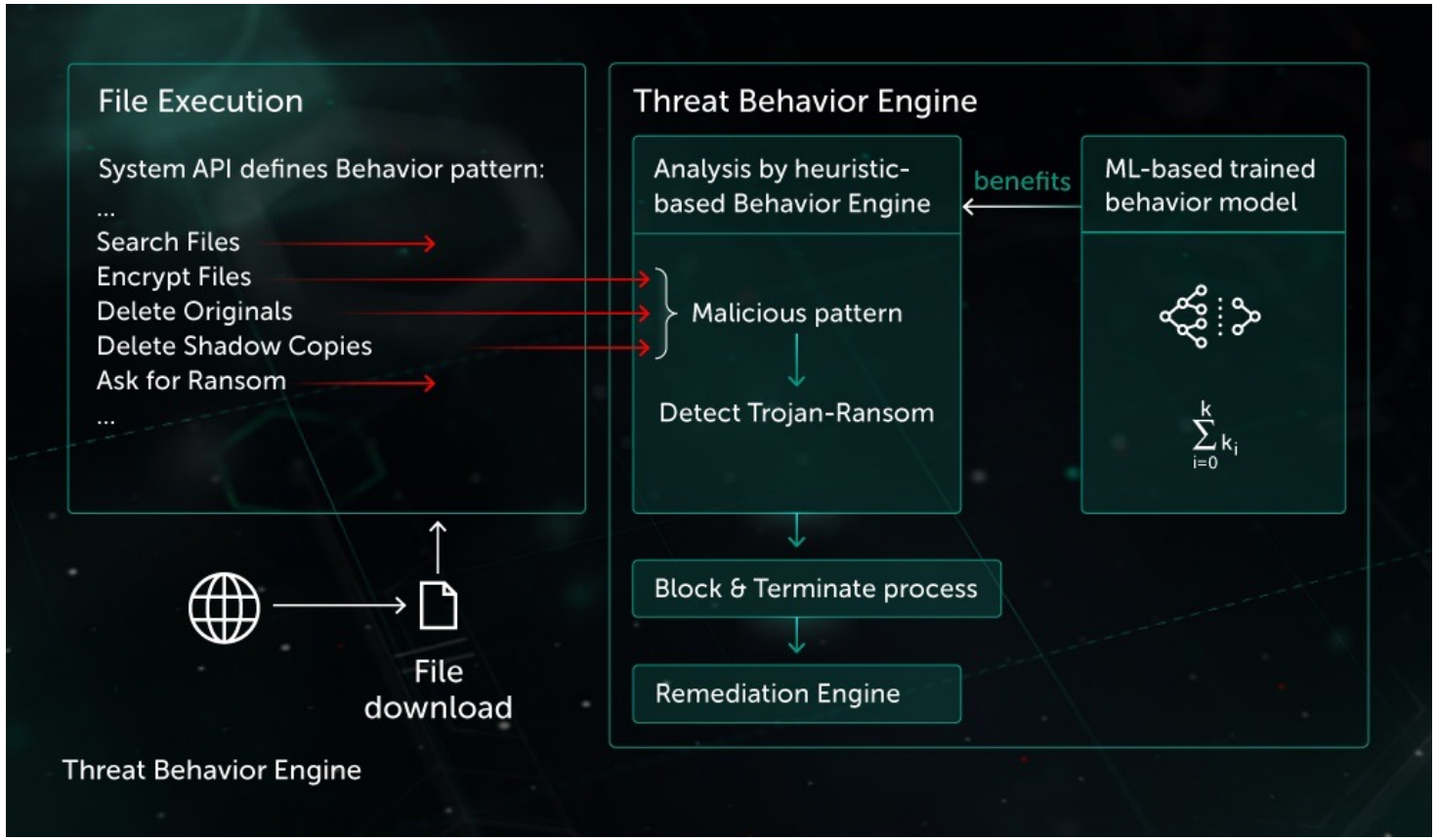
- Based on shared memory and CPU State
- VMI tool is asynchronous to the VM
- Hypervisor/OS does not interrupt or interfere with the VM execution
- Hypervisor sends information to VMI tool over shared buffer
- CPU Hardware Extension involved (ARM Coresight, Intel PT)



Malware detection

Behavior analysis

- Behavioral model
  - Benign execution
  - Malicious execution
- Next-generation protection
  - Fileless malware
  - Ransomware
  - Zero-day malware
- Our focus:
  - **Run-time tracing towards attestation**



What to collect?

- Running Processes
- Loaded Kernel Drivers
- Kernel
- Application Control Flow graph
- CPU State
- Active Network Connections

Motivation and Vision

Synchronous system tracing has disadvantages

- Observer Effect
- System calls implementation in the inspected machine
- Changes to System APIs

Our vision to solve these issues with Asynchronous tracing and Hardware Support

- Least intrusive
- Does not require involvement of the inspected target
- Stealthy
- Visibility to CPU execution

THANKS

PROJECT-ASSURED.EU

@Project_Assured

ASSURED project is funded by the EU's Horizon2020 programme under Grant Agreement number 952697