



Mockingbird

Secure Malware Analysis for Cuckoo

Background: Cuckoo open source malware sandbox

- Cuckoo users deploy suspected malware in a virtual machine, called the analysis guest
- An agent, running in the analysis guest, collects data from the malware and infected analysis guest
- The agent delivers collected data to an analysis system for review with a collection of bundled tools



Mockingbird

Secure Malware Analysis for Cuckoo

PROBLEM

The Cuckoo agent is vulnerable to malware

Cuckoo collects data from within the infected analysis guest:

- Malware can detect the agent and change behavior to evade analysis
- Malware may subvert analysis guest dependencies or directly attack the Cuckoo agent to corrupt collections
- Memory analysis integrity degraded due to in-guest agent running alongside malware

The Cuckoo agent relies on the infected host network to deliver collected data:

- A lack of network isolation may allow propagation to analysis network
- A disabled network interface card in the analysis guest will thwart delivery of collected data

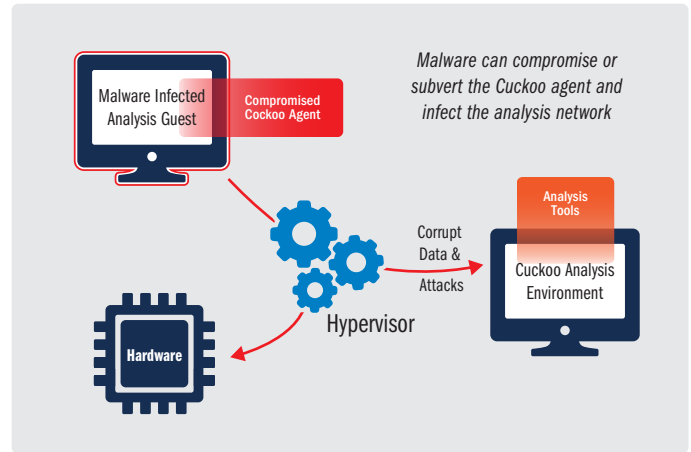


Figure 1: Cuckoo Architecture

Secure malware analysis requires separation of the infected guest from the collection agent and network

APPROACH

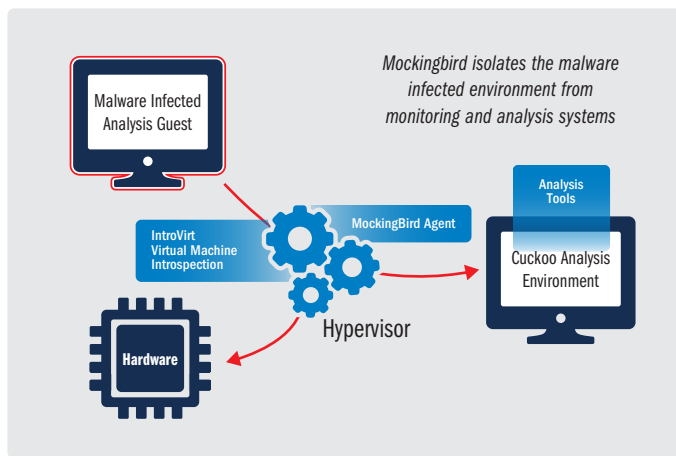


Figure 2: Mockingbird Architecture Segregates Analysis from Monitoring

Mockingbird protects Cuckoo data collection using virtual machine introspection

- Hypervisor agent moves monitoring out of reach of malware
 - Maintains compatibility with existing Cuckoo framework, modules and APIs
- Integrity provided to memory snapshots and analysis due to clean environment
- Monitoring agent uses communications channels isolated from infected guest
- Extend the Cuckoo API to provide customization of the analysis environment
- Powered by the AIS IntroVirt® virtual machine introspection (VMI) technology

USE MOCKINGBIRD TECHNOLOGY NOW!

- XenMachinery part of Cuckoo release 2.0
- A full Mockingbird evaluation and trial access is available from the AIS Mockingbird Team

FOR MORE INFORMATION

bd@ainfosec.com

New York • Colorado • Georgia • Oregon • Massachusetts • Maryland • Virginia

