HADES: HIGH-FIDELITY ADAPTIVE DECEPTION & EMULATION SYSTEM

US Pat. No.: 9,742,804
Technology Readiness Level: 7
Demonstration of an actual system prototype in an operational environment

The rise in sophisticated cyberattacks has prompted businesses and organizations to seek out robust security measures with the ability to detect and respond to an adversary's attacks in real-time. Many are using deceptive tools and tactics; however, current deception tools only provide partial solutions to full-spectrum deception. Sandia's High-Fidelity Adaptive Deception & Emulation System (HADES) is a comprehensive cybersecurity platform that utilizes revolutionary advances in deception technologies that allow network defenders to defend and collect information on the adversary in real-time.

HADES

The HADES platform is a deception environment that utilizes Software Defined Networks (SDN), cloud computing, dynamic deception, and agentless Virtual Machine Introspection (VMI). These elements fuse to not only create complex, high-fidelity deception networks, but also provide mechanisms to directly interact with the adversary—something current deception products do not facilitate. At the onset of an attack, adversaries are migrated into an emulated deception environment, where they are able to carry out their attacks without any indication that they have been detected or are being observed. HADES then allows the defender to react to adversarial attacks in a methodical and proactive manner by modifying the environment, host attributes, files, and the network itself in real-time. Through a rich set of data and analytics, cybersecurity practitioners gain valuable information about the tools and techniques used by their adversaries, which can then be fed back to the network defender as threat intelligence.

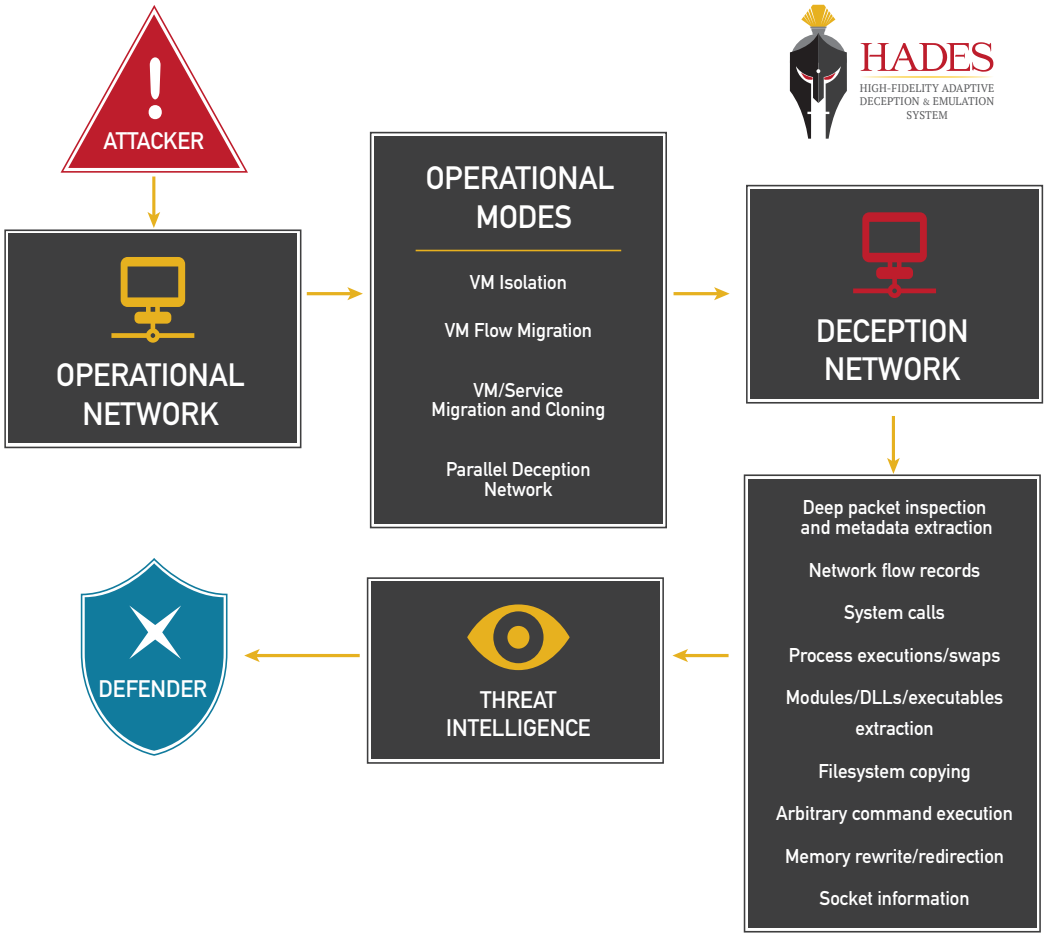
The HADES platform is the only comprehensive solution to deceive, interact with, and analyze adversaries in real-time. The unique insight gathered while using HADES can be used to implement stronger network defenses and prevent future attacks.

TECHNICAL BENEFITS

- Creates high-fidelity deception environments based on real system attributes
- Provides granular insight into attacker's tools and tactics (malware, behavior, workflow)
- Allows interaction with adversaries through host, network, and file modification
- Provides varying operating and deployment modes to facilitate various network models

ip.sandia.gov
ip@sandia.gov

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC.,a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-3364 M



- At the onset, an attacker is detected in the Operational Network by the Network Defender.
- The VM that the attacker has landed on is then migrated into the Deception Network through one or more operational modes. The operational modes increase in level of fidelity, which shares a linear relationship with cost (memory, computation, hardware footprint); the modes are be combined to form varying deception environments:
    - ◊ VM Isolation: Attacker is isolated (quarantined) from the Operational Network
    - ◊ VM Flow Migration: Network flows at the boundary from attacker to VM are shifted to a VM in the Deception Network
    - ◊ VM/Service Migration & Cloning: The VM attacker is on is migrated into a Deception Network; additional VMs from Operational Network are cloned into the Deception Network, maintaining familiarity and memory states
    - ◊ Parallel Deception Network: A parallel Deception Network is created to mimic the Operational Network
- While in the Deception Network, many attributes can be changed allowing for interaction. Through agent-less network and virtual machine introspection, the attacker may be observed. Textual and binary information extracted from the Deception Network may then be recast as threat intelligence (signatures, malwares, workflows) to be fed back to the network defender.

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC.,a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-3364 M