2022

High-Fidelity Virtual Machine Artifact Mitigation

Singh, Gurminder

Monterey, California: Naval Postgraduate School

HIGH-FIDELITY VIRTUAL MACHINE ARTIFACT MITIGATION

Naval Postgraduate School

Goals

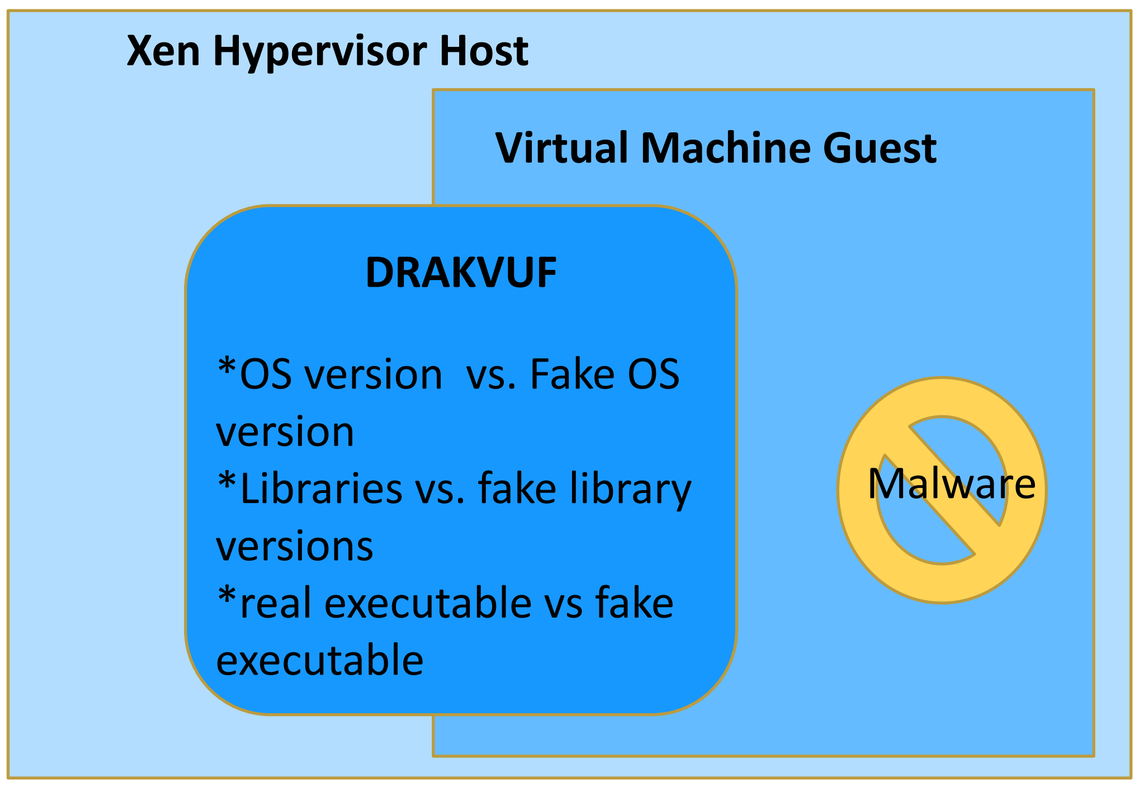
- Protection of Cloud infrastructure
- Resilience of Cloud infrastructure
- Protection from external attackers and internal attackers
- Expose attacker
- Analyze attacker methods

Malware Trends

- Intelligent, analyzes surroundings
- Based on findings, attacks using a series of vectors dependent on surroundings
- If it detects that it is being analyzed, it hides and continues to spread
- Partially automated
- Becoming more important

Methods

- Protection through obfuscation
- Protection by virtual machine introspection
- Protection at the system call kernel level

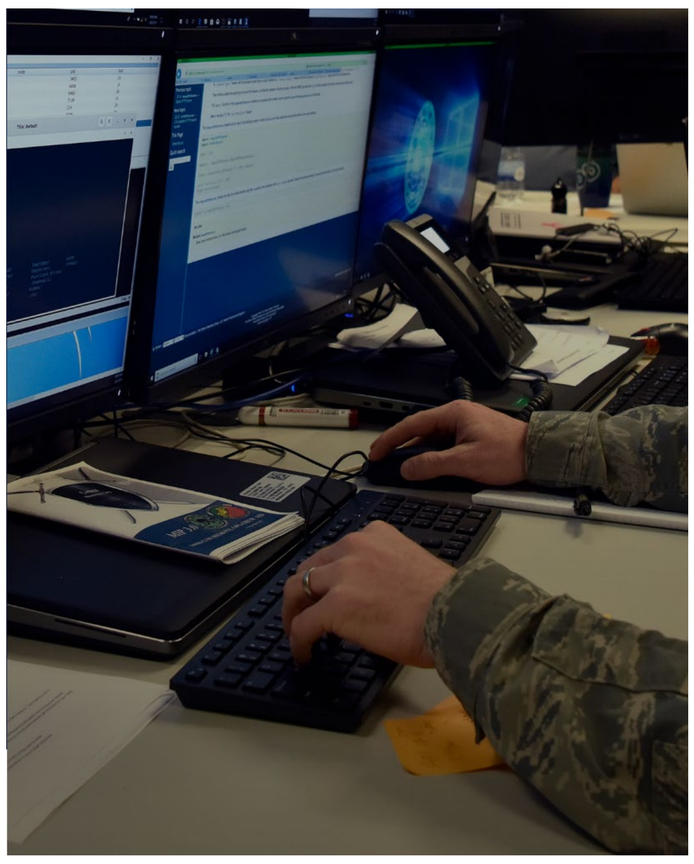


Malware is confused into exposing itself

Persistent Cyber Training Environment (PCTE)

Helps with PCTE

- Training of Malware detection and analysis
- Help with offense cyber operation munitions
- Training of low-level detection of malware
- Creation of better decision trees
- Creation of better Techniques, Tactics, and Practices



Researchers: Dr. Gurminder Singh, Computer Science Dept., Dr. Allan Shaffer, Information Science Dept., and Charles Prince, Computer Science Dept.

Topic Sponsor: Marine Corps Forces Cyberspace Command (MARFORCYBER)

NRP Project ID: NPS-21-M006-A

This research is supported by funding from the Naval Postgraduate School, Naval Research Program (PE 0605853N/2098). Approved for public release; distribution is unlimited.