SAND2019-8384D

FARM: Forensic Analysis Repository for Malware

Students: Marton Demeter, Evan Laufer, Alex Mullins, James Picker
Mentors: Ken Chiang, Michael Carson, Thanh Nguyen, Chris Harrell

Problem

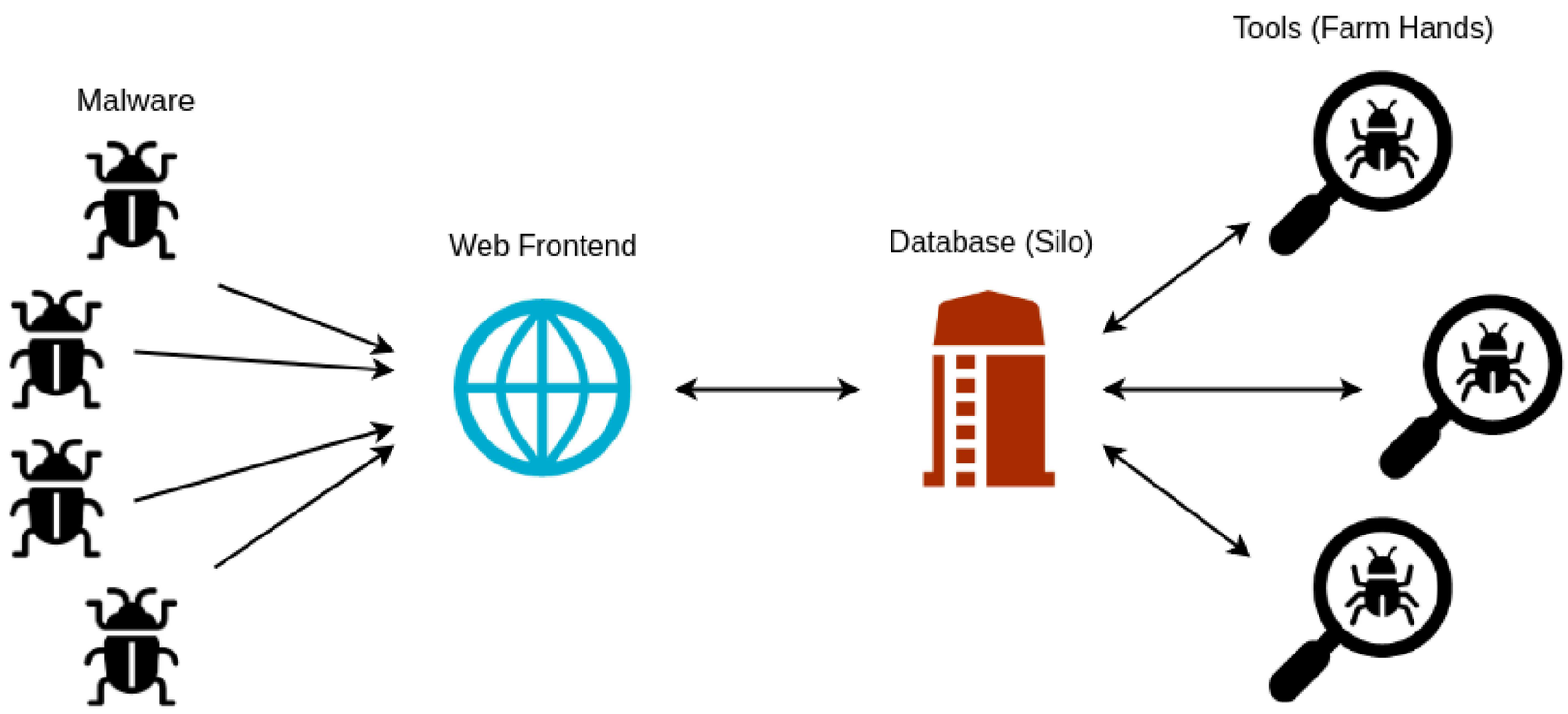
Malware analysis is one of the most important steps in understanding and defending against malicious actors. As more malware is created, it becomes unfeasible to analyze every sample manually. Additionally, manual analysis requires repeating the same steps on different samples, consuming a large amount of researchers' time.

FARM

Forensic Analysis Repository for Malware (FARM) is a system that stores and automatically runs reverse engineering tools on over 100 million malware samples. It acts as a central storage location and knowledge base for all types of malware, and can be accessed remotely over the Internet.

Using FARM

1. Upload the sample to FARM using the web interface.
2. Enter information such as a description, source, and parent sample.
3. Select various tools (Farm Hands) to run. These tools extract useful information for determining the behavior and maliciousness of the sample.
4. Results are made available to authorized FARM users.



Current Work

Kubernetes

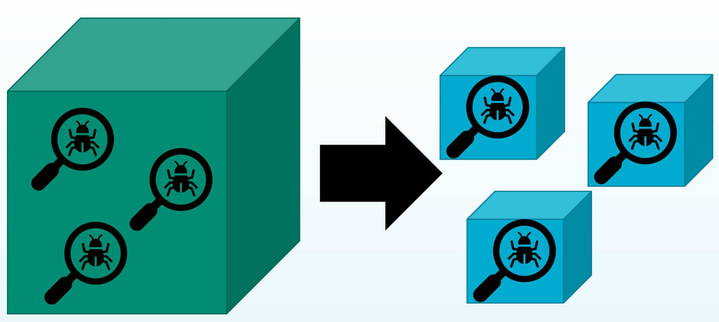
One of the limitations of FARM is its difficulty scaling to meet the demands of the growing userbase. To solve these issues, we are migrating FARM to Kubernetes, allowing individual FARM components to be updated and scaled on-demand.

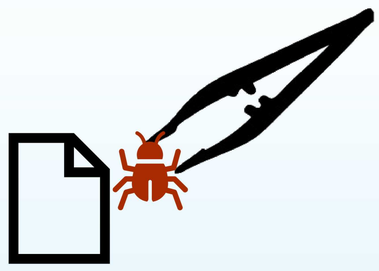
VBA Extraction

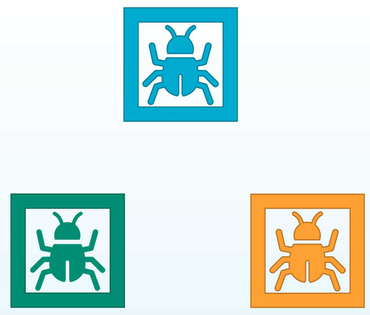
FARM traditionally analyzes x86 executables in Window's PE format. Work is being done to extend FARM's capabilities to Microsoft Word, Excel, and PowerPoint files. Similarity analysis is used on VBA scripts extracted from these documents in order to group malicious files.

Execution Environments

FARM allows malware analysts to run malware in a variety of secure environments. We are updating the number of execution environments available, allowing analysts to continue testing with the most modern malware samples.







Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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.
SAND No. _____