SAND2008-0857P

Sandia Malware/Botnet Analysis Environment

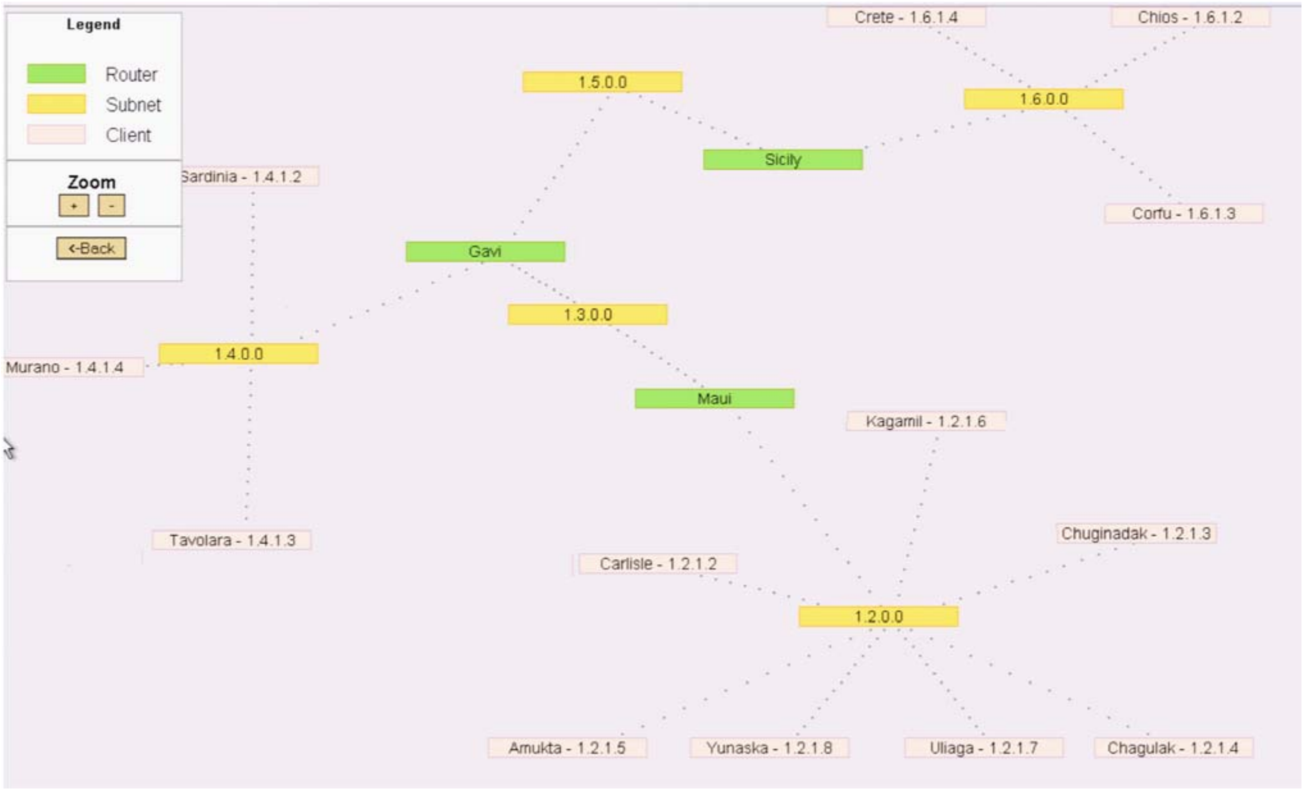
February 4, 2008

ISLAND (Isolated Security Laboratory for Attacks and Network Defense)

ISLAND is an unclassified, reconfigurable test bed for botnet and malware analysis. Approximately thirty machines are connected in a configuration that can be attached to external networks or isolated as a separate LAN. Each of the thirty hosts runs their OS in native mode, not as a virtual machine (VM). Avoiding VMs enables researchers to gain a more accurate view of the malware being studied since much of the current malware is "VM-aware." The test bed can run multiple, simultaneous experiments with varying network topologies and OS selection.

ISLAND Architecture:

- Image Server
  - Stores images and snapshots
  - Host frontend GUI
  - Configures network hardware
- Client Machines
  - Variety of x86 systems
  - Network boot for experiment setup
  - OS Image deployed to local hard disk



FARM (Forensic Analysis Repository for Malware)

FARM (Forensic Analysis Repository for Malware) is an automated system for analyzing malicious code. The system takes as input malicious files and automatically performs multiple analyses (e.g. header parsing, behavioral analysis, packer detection, unpacking, anti-virus scanning, etc.) on the file. The output of the analyses and various characteristics of the malware are stored in a database for reference to aid the analyst in cross correlation of related malware and reverse engineering.

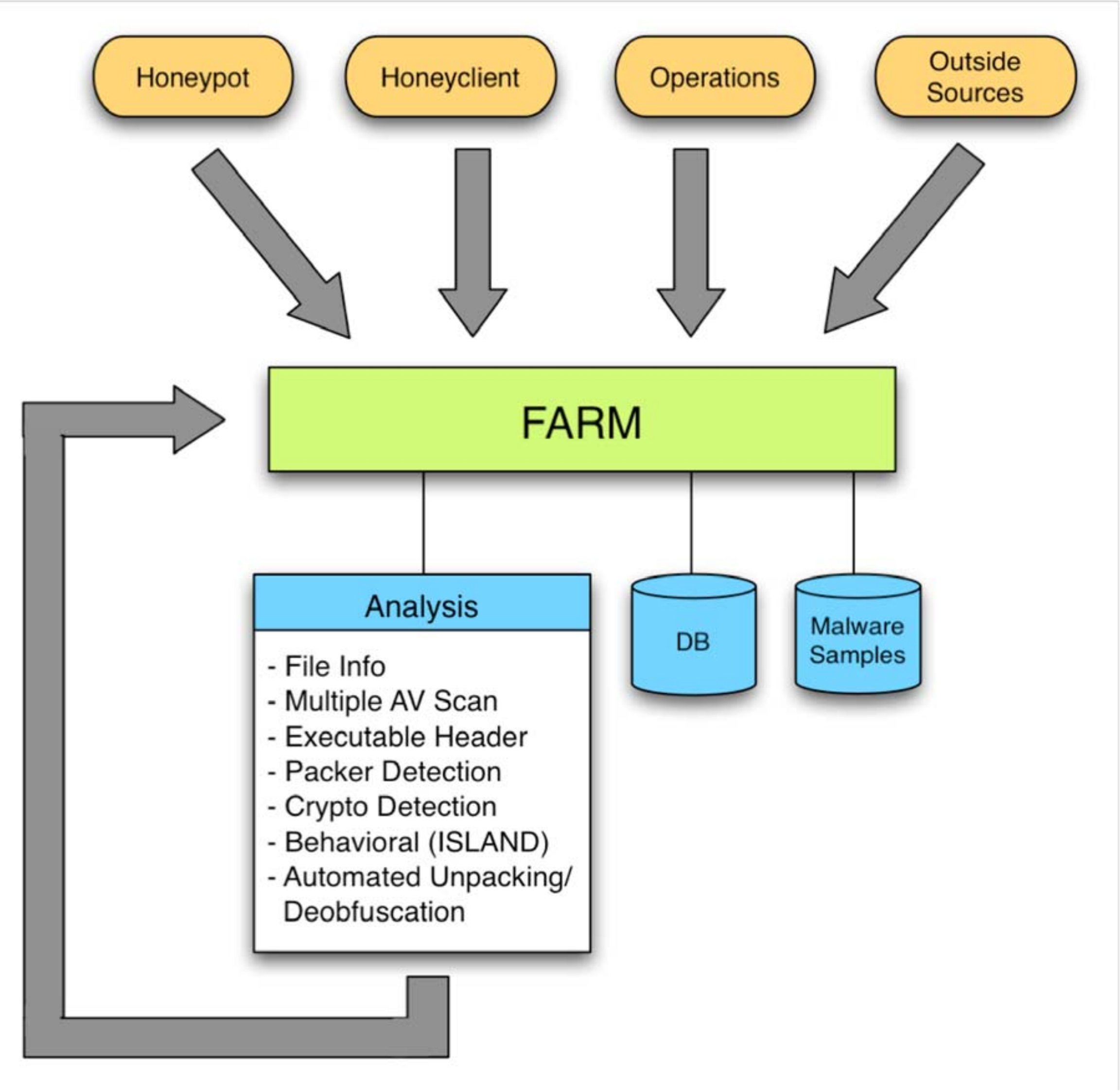
FARM is currently in the prototype stage. It supports the following automated analysis modules:

1. PE header parsing
2. Behavioral Analysis (utilizes ISLAND):
   a. Registry key activities
   b. File activities
   c. DNS queries
   d. IP and port information
3. Saffron automated unpacking (results are resubmitted back to FARM for analysis of the unpacked code/binary)
4. Packer detection using PEiD 0.94
5. Encryption Algorithm detection using PEiD 0.94 Kanal plugin
6. Multiple Anti-virus engine scans:
   a. Avast
   b. F-prot
   c. McAfee
   d. ClamAV

FARM is architected to be modular. As the anti-malware community develops new analysis tools, they can be easily added to FARM.

Future work on FARM will include:

1. More AV scanners: Symantec and others
2. More automated unpackers: Polyunpack, upx, etc.
3. Enhance behavioral analysis:
   a. Include processes created
   b. Add more detailed protocol information
   c. Add ability to execute multi-file malware as well as load kernel level rootkits
4. Add capability to submit manual reverse engineering information
   a. Support IDA Pro databases
   b. HTML Form fields
5. Classification/Grouping of malware using supervised machine-learning techniques
6. Support other executable formats besides PE


Honeypot
Honeyclient
Operations
Outside Sources
FARM
Analysis
- File Info
- Multiple AV Scan
- Executable Header
- Packer Detection
- Crypto Detection
- Behavioral (ISLAND)
- Automated Unpacking/ Deobfuscation
DB
Malware Samples