MALWARE
INVESTIGATOR

Automated Malware Analysis

Federal Bureau of Investigation | Operational Technology Division

FBI Malware Analysis Timeline

1998
- NIPC Created
- Malware Analysis Began
- 100% of Malware Analysis was Manual

2004
- FREE Developed
- First Attempt for Enterprise Malware Repository
- 100% of Malware Analysis was Manual

2010
- FREE deemed Inadequate
- BACSS Initiated
- 100% of Malware Analysis was Manual

2011
- BACSS Deployed
- Vast Majority of Malware Analysis now Automated

2013
- Malware Investigator Development Begins
- Automated Malware Analysis to be provided to IC, ISLT LE, Private Partners

2014

MALWARE
INVESTIGATOR

Malware Investigator

What is Malware Investigator?

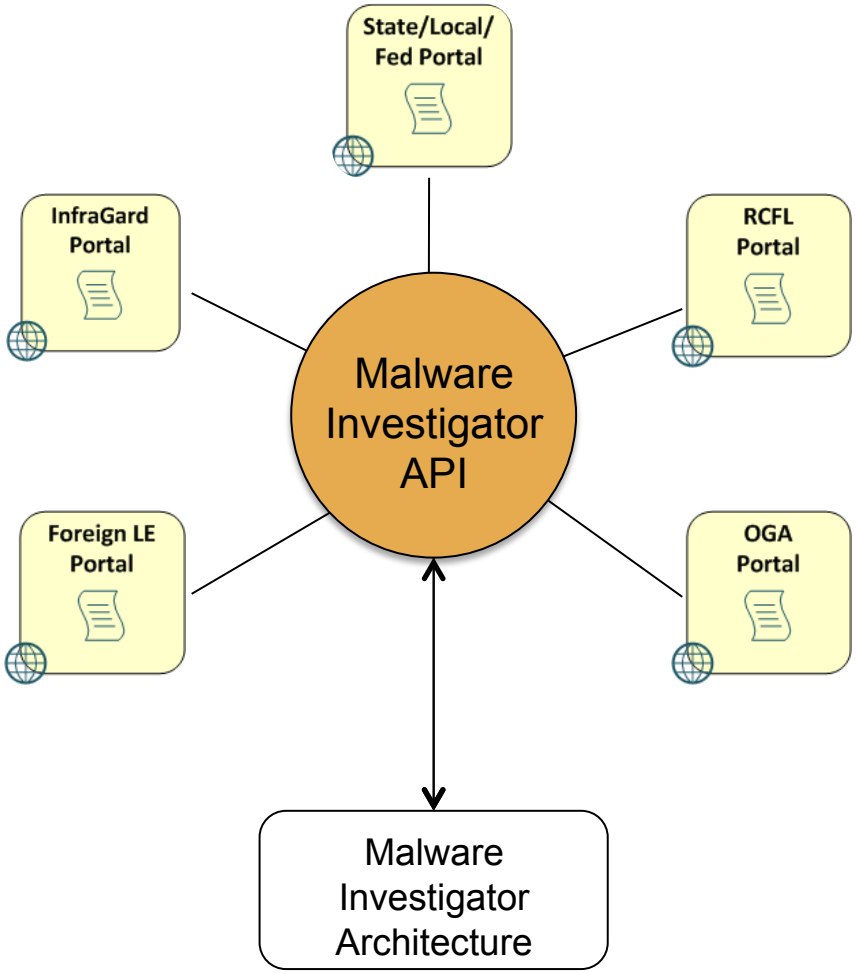
- FBI developed automated analysis and repository system for suspected malware
- 80% solution for malware analysis
- Provides users with information needed to further investigation or respond to incidents vs. waiting for full reverse-engineering
- Correlates malware submitted across the Malware Investigator user community

Malware Investigator Reporting Information

- File Hashes (MD5, SHA-1, SHA-256, SSDEEP)
- Correlation
- Malware Comparison (similarity analysis)
  - Fuzzy Hashing
  - Section Hashing
- Virus Scanning Cluster
- Sandboxing (PE32 exe, PDF, MS Office docs)
  - File System Modification
  - Processes
  - Registry Modification
  - Network Connections Attempted
- Other (file typing, function imports, behavior over time)
- Strings

Access to Malware Investigator

- Available to partners with some form of relationship with the FBI
- Web Service available for law enforcement, non-profits, and private sector (can share as much or as little intelligence, as desired)
- API access for those who wish to integrate the resource into existing systems.



Malware Investigator Key Points

- Malware Investigator provides two main functions
  - Analysis – technical results
  - Collaboration – venue for sharing information with other users
- Available to academia, security researchers, private sector and law enforcement partners
- Your privacy is a top consideration
- You maintain control over your sharing
- We're always looking for new ideas and ways to improve Malware Investigator for its users

Sharing Demonstration

Movie

MALWARE
INVESTIGATOR

Start the Discussion:

#FBIMALWARE, #MALWAREINVESTIGATOR, #MALWAREWATCH

Federal Bureau of Investigation | Operational Technology Division