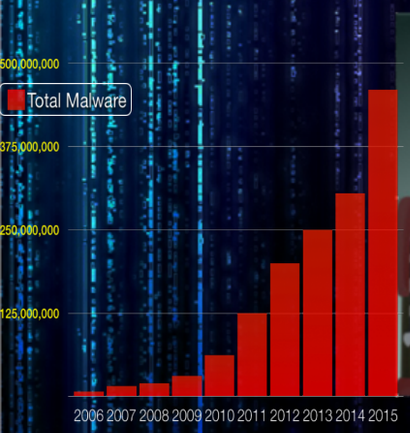
Machine Learning and Malware Classification



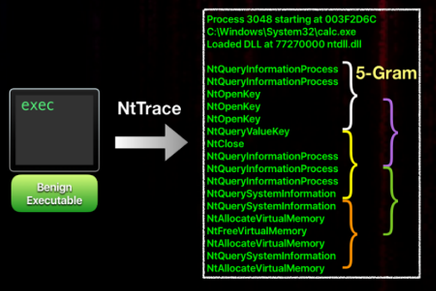
Observations so far…

- Static analysis should be preferred over dynamic analysis when dealing with large volume of malware
- Combinational approaches (blacklisting and whitelisting) should be preferred for effective malware classification
- Sophisticated malware that use encryption are very difficult to classify

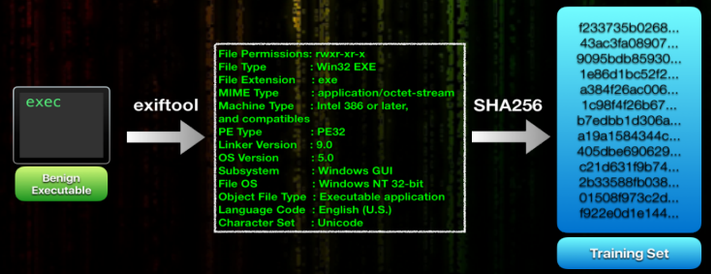
Whitelisting approach

- **Advantages**
  - Highly Secure
  - Can Prevent Zero Day Attack
- **Disadvantages**
  - Need To Frequently Update The Training Set
  - Functional Inflexibility

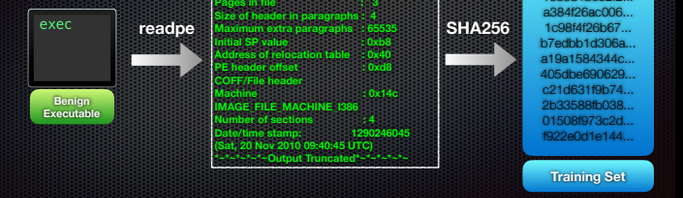
Dynamic Analysis



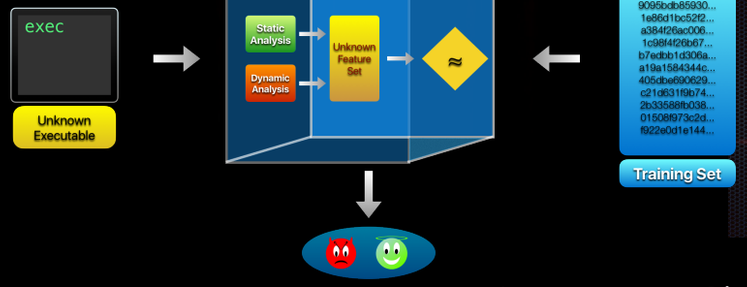
Static Analysis



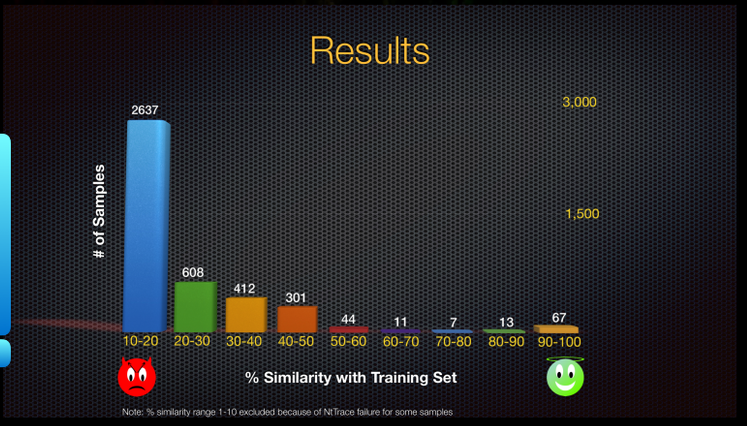
Static Analysis (Cont.)



Classifier



Results



By:Amit Raut raut.am@husky.neu.edu, Pranav Sharma sharma.pran@husky.neu.edu