
University of Colorado
Boulder

Prognosis Negative: Evaluating Real-Time Behavioral Ransomware Detectors

Abhinav Gupta - **abgu6606@Colorado.edu**
Aditi Prakash
Nolen Scaife
University of Colorado Boulder

Why is ransomware still a problem?

- Ransomware detection still a problem.
  - Lot of research/products from academia and industries.

Reasons:

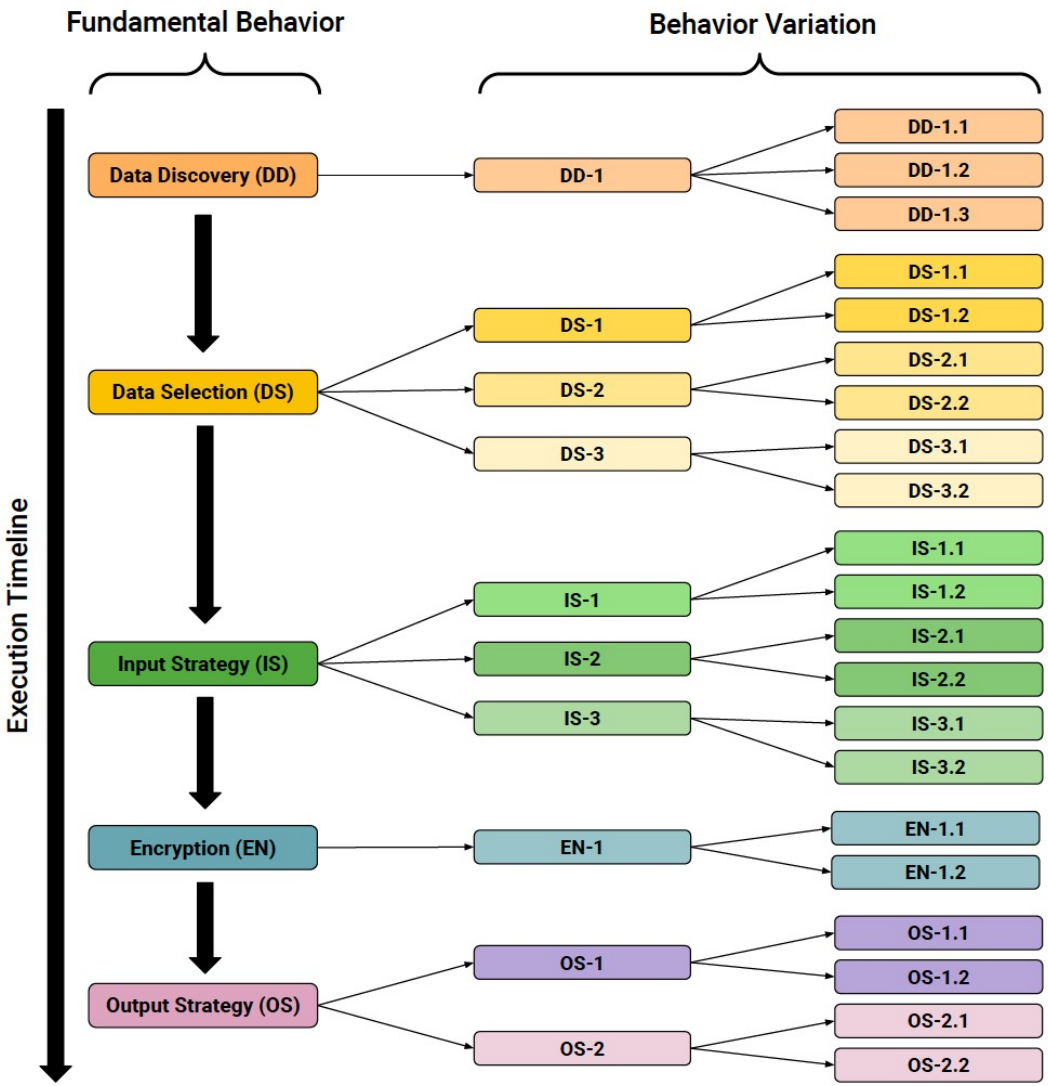
- No access to a wide variety of samples.
- Characterization of ransomware behavior.

Contributions of the paper

- Characterization of Fundamental behavior.
- Identification of Problematic Evaluations.
- Development of reliable open source and extensible testing framework – farfel.

Ransomware life cycle and fundamental behaviors

- Ransomware goal – Survivability and reversibility.
- Why and how we chose them – refer table 2
  - Literature survey
  - Analyzed and filtered behaviors.
- If not, then it will lead to false negatives.
  - Using behaviors that are not fundamental will lead to high false negatives.


Fundamental Behavior
Behavior Variation
Execution Timeline
Data Discovery (DD)
Data Selection (DS)
Input Strategy (IS)
Encryption (EN)
Output Strategy (OS)
DD-1
DS-1
DS-2
DS-3
IS-1
IS-2
IS-3
EN-1
OS-1
OS-2
DD-1.1
DD-1.2
DD-1.3
DS-1.1
DS-1.2
DS-2.1
DS-2.2
DS-3.1
DS-3.2
IS-1.1
IS-1.2
IS-2.1
IS-2.2
IS-3.1
IS-3.2
EN-1.1
EN-1.2
OS-1.1
OS-1.2
OS-2.1
OS-2.2

Some commonly-references general behaviors

- Ransom Message
- Execution from a file
- Network Communication
- File extension change

Note: Our framework had some general behavior to show that their presence does not affect the detection much.

Anti-ransomware strategies

- Preventing execution
- Behavioral analysis
  - File content changes
  - Filesystem modification
  - I/O operations
  - Canary files
  - Cryptography usage
  - Network analysis

Ransomware samples collection

- Ways to collect ransomware samples.
  - virustotal.com
  - virusshare.com
  - malwr.com
  - Online forums
  - GitHub Repositories
- Not enough diversity in the samples collected.
- Also cleaning of samples is time consuming.
  - Failure rate of collected samples range from 12% to 67%

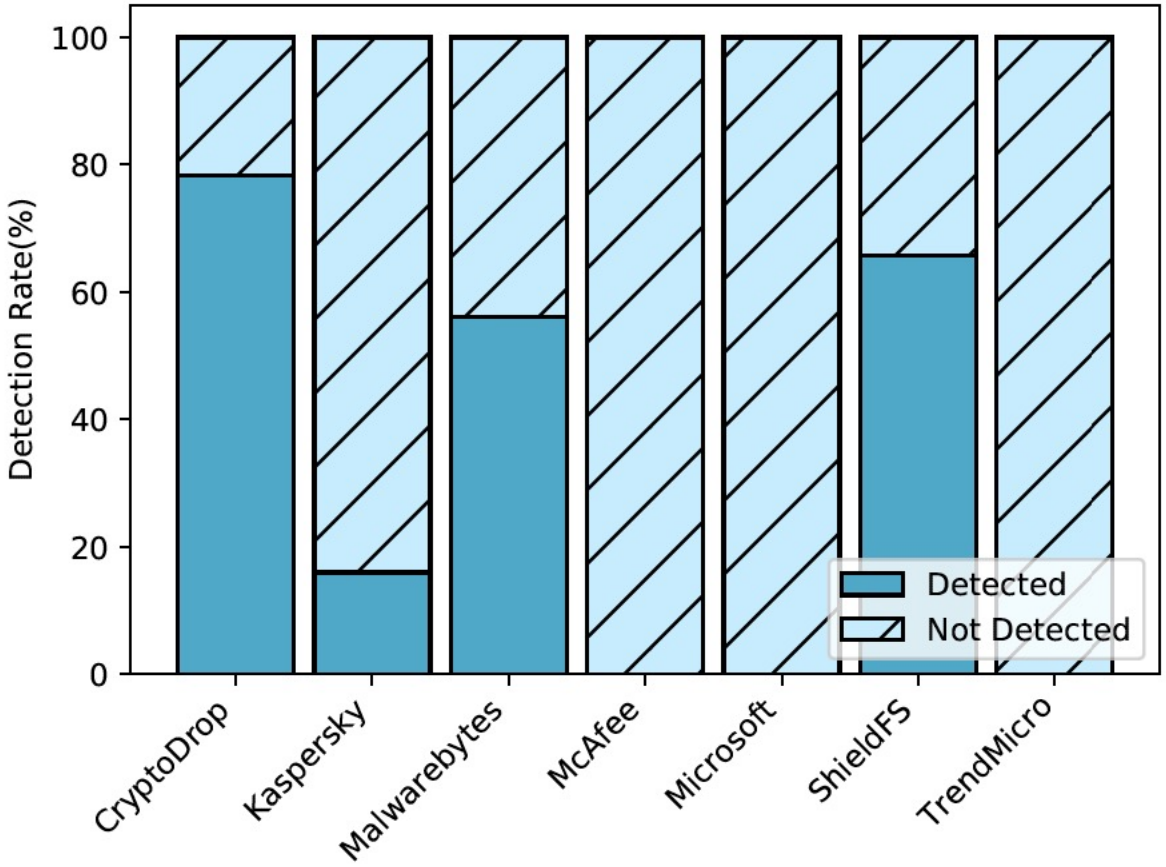
Development of reliable testing framework - farfel

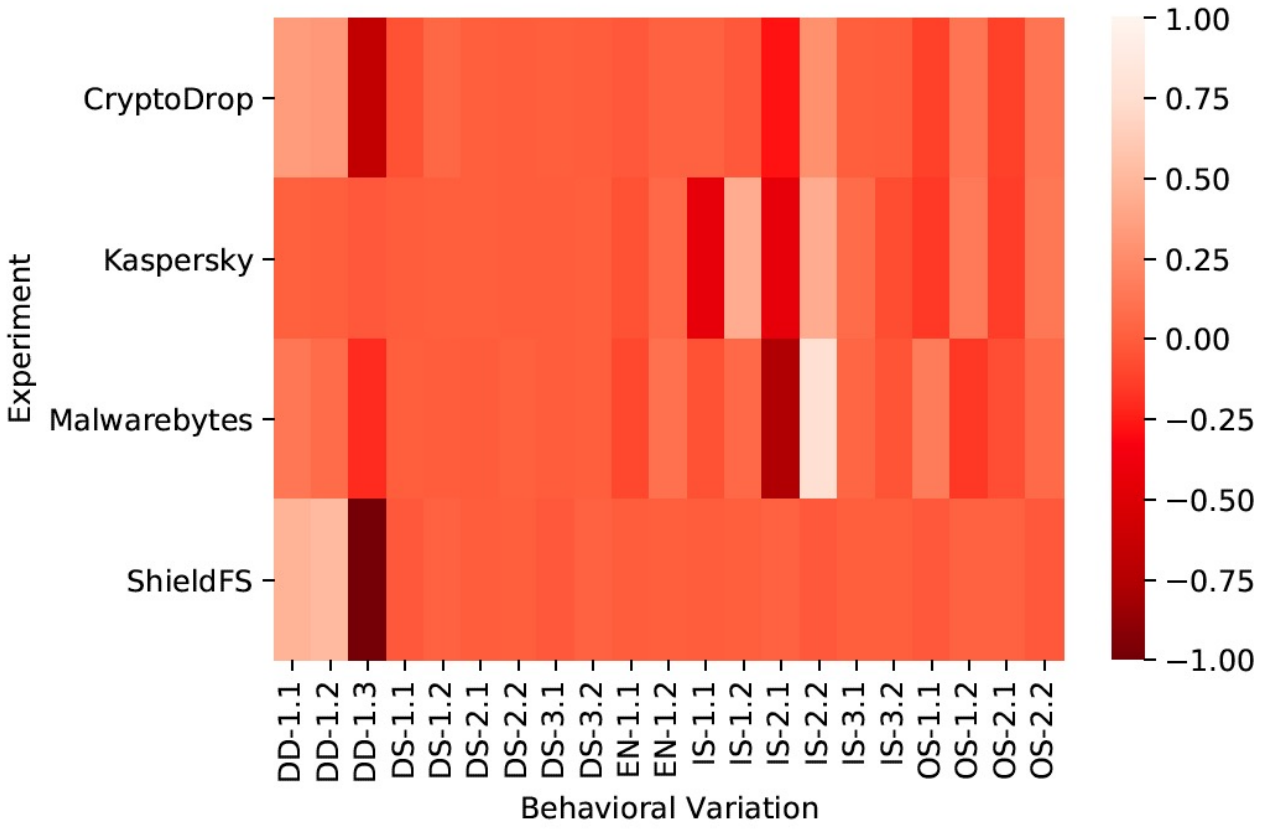
- 1536 unique attacks and 21 unique behavior variations.
- Extensible, customizable and open source.
- Quickly iterate and select the desired ransomware behavior.
- Semantically correct execution.
- Self contained and safe to handle.

Testing

- Commercial anti-ransomware software
  - Kaspersky Anti-virus
  - Malwarebytes
  - McAfee Total Protection
  - Microsoft windows defender
  - Trend Micro Maximum security
- Academic anti-ransomware
  - ShieldFS
  - CryptoDrop Anti-Ransomware

Results


Detection Rate(%)
100
80
60
40
20
0
CryptoDrop
Kaspersky
Malwarebytes
McAfee
Microsoft
ShieldFS
TrendMicro
Detected
Not Detected


CryptoDrop
Kaspersky
Malwarebytes
ShieldFS
Experiment
DD-1.1
DD-1.2
DD-1.3
DS-1.1
DS-1.2
DS-2.1
DS-2.2
DS-3.1
DS-3.2
EN-1.1
EN-1.2
IS-1.1
IS-1.2
IS-2.1
IS-2.2
IS-3.1
IS-3.2
OS-1.1
OS-1.2
OS-2.1
OS-2.2
Behavioral Variation
1.00
0.75
0.50
0.25
0.00
−0.25
−0.50
−0.75
−1.00

Future work

- False positives
- Implementing new behaviors
- Implementing heuristics for intent of a program
- Increase in speed of testing – cloud based.

Summary

- Ransomware attacks increase in both prevalence and severity.
- It’s difficult to make robust anti-ransomware.
- Characterization of ransomware behavior as fundamental and general.
- Designed and implemented an open-source and extensible framework (farfel) for testing anti-ransomware software.
- Evaluation of seven anti-ransomware (5 commercial and 2 academic) products.

Thank You

Abhinav – abgu6606@Colorado.edu