UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware

Yashar Dehkan Asl

What is Ransomware?

Ransom:

Money that is paid in order to free someone who has been captured or kidnapped. *-Merriam-Webster*

Ransomware:

A malware designed to block access to a computer system, files, screen, disk or etc. until the requested amount of money is paid.

History

First Ransomware Virus:

AIDS Trojan (1989)

Recent Years

- Locky
- Cerber
- CrypyXXX 3.0
- Dogspectus

Types of Ransomware

Two major types:

- **Locker Ransomware (Computer locker)**

  Denies the access to computer or device

- **Crypto Ransomware (Data locker)**

  Denies the access to files or data

How does Ransomware work?

- Persistent desktop message
- Indiscriminate encryption and deletion of the user’s private files.
- Selective encryption and deletion of the user’s private files based on certain attributes

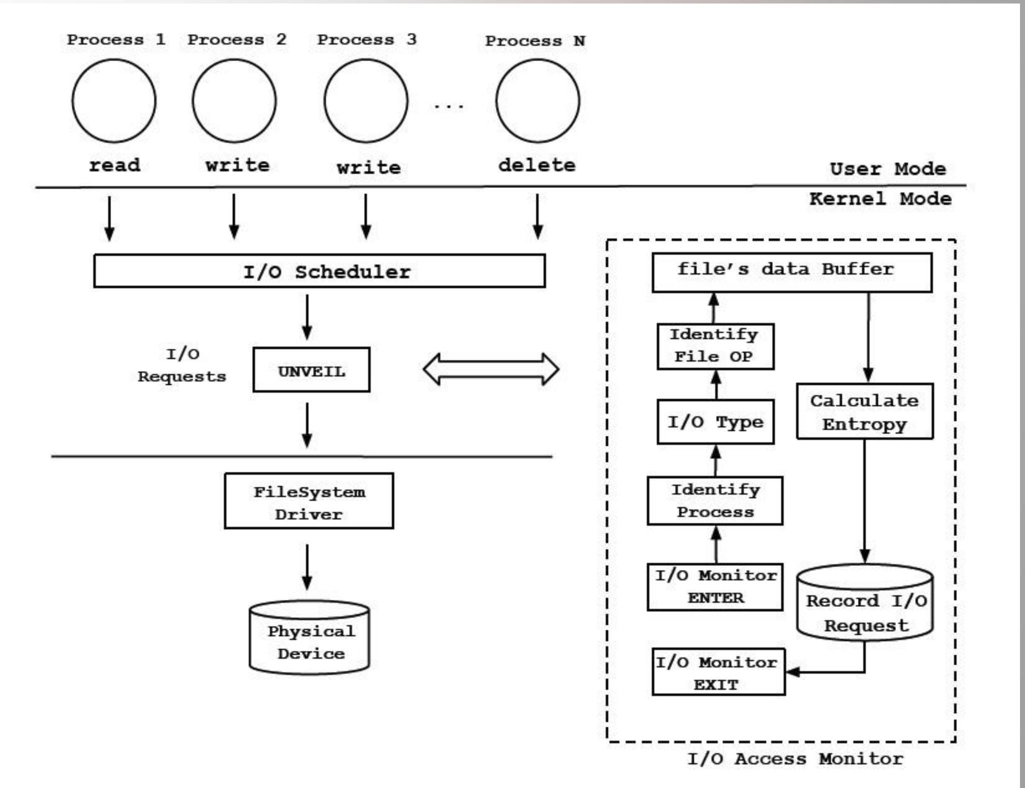
UNVEIL

- **Detecting File Lockers**
- **Detecting Screen Lockers**

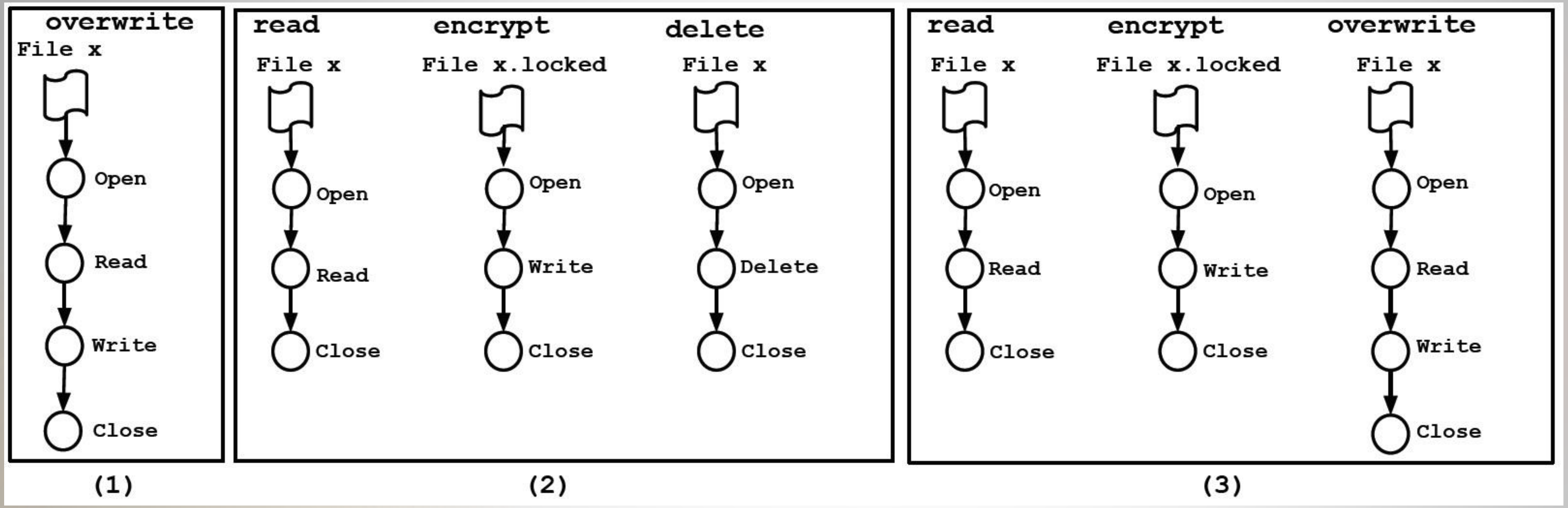
Detecting File Lockers

- **Generating Artificial User Environments**

- **Filesystem Activity Monitor**
  - . I/O Data Buffer Entropy
  - . Constructing Access Patterns



Cont.



Different strategies on ransomware families

Detecting Screen Lockers

- Taking automatic screenshots to detect screen locking ransomware
- Measuring the structural similarity by comparing local petterns of two screenshots
- Closing open windows for screenshots from persistent changes, to avoid false positives
- Extracting the text within the area

Implementation

Generating User Environments

- Valid Content
- File Path
- Time Attributes

Cont.

Filesystem Activity Monitor

- UNVEIL monitors filesystem I/O activity using the Windows Filesystem Minifilter Driver
- Monitoring and retrieving logs of entire system
- UNVEIL’s monitor sets callback on all I/O request to the filesystem.

Cont.

Desktop Lock Monitor

- Captures screenshots from outside of dynamic analysis environment
- Converts the image to floating point data then calculates parameters

Evaluation

Two experiments:

- **To show the system can detect known ransomware samples**
- **To show that UNVEIL can detect previously unknown ransomware samples**

Cont.

Experimental Setup

- Build up a prototype on top of Cuckoo Sandbox
- Use 56 VMs with Windows XP SP3
- Multiple NTFS drives on each VM
- Take anti-evasion measures against popular tricks
- Permit controlled access to the internet

Cont.

Ground Truth (Labeled) Dataset

- Filesystem Activity of Benign Application with Potential Ransomware-like Behavior

- Similarity Threshold

Cont.

Detecting Zero-Day Ransomware

- **Detecting Results**

  Evaluation of false positive

  Evaluation of false negative

- **Early Warning**

Discussion and Limitations

It’s always possible that attackers find ways to fingerprint the automatically generated user environment and avoid it.

Malware might encrypt part of a file, not all of it, or it might make the file unreadable.

Text extraction can be improved

Ransomware may run at kernel level