Ransomware Testing Framework

Project Code Base Structure

Configurations

All configurations are in `config.py` file.

`config.py` files are in 2 parts.

- Paths to different files (using absolute paths)
- Functions to get configurations.

Calling Trace

- `run.py` wrapper
- `utils/toplevel.py` initiate testing
- kernel level tracing
- `utils/core/*.cpp` Use a rb tree to record # clean blocks
- `utils/preproecess.py` initiate ransomware and do `blktrace` and `blkparse`
- `utils/cryptosoft/ransomware.py` run ransomware
- `utils/core/*cpp` Update rb tree to calcuate final result (# clean blocks remaining)
- `utils/toplevel.py` initiate another test

Overview of Ransomware Pattern

Report

center

Testing Framework Structure

For banks, hospitals, private PC, etc. they store files in their system (our target system).

Ransomware reads files in our target system, encrypt it, then overwrite them(in-place or delte then create new copies).

The testing framework detects how susceptible the target system is to ransomware.

It collects data in **target system** (preprocessing), **FS filter** (VFS in Linux) layer as well as **BIO layer**. It also optionally collects data with **standardized ransomware** to illustrate the pattern of attack and verify the sanity of other satistics.

center rans01

Standardized Ransomware (encryption and deletion)

center rans02

Target System (fingerprinting)

center rans04

Statistics

center rans03

Data Structure

center rans05

Basic Implementation

Clone target system, and backup to a safe place

Migrate / Prepare Target System & Preprocess `tar_sys_info`

Add magic numbers to files in target file system

center rans06

MAGIC number should be 8 bytes (to avoid collision) to help BIO layer gather more information more easily.

Launch standardized ransomware, with `rans_info` prepared

When running ransomware

- In standardized ransomware, fill in `stat_fs_filt`
- In BIO, fill in `stat_BIO`.

BIO tracing in Linux

Currently implemented

- Tracing and Logging for EXT(2,3,4), XFS, F2FS, NTFS, BtrFS (without RAID) in BIO layers utilizing different existing tools.
- Automation for different injected pattern and target systems.
- A preliminary version of configurable and standardized ransomware.

TO DO

- Complete different features within ransomwares.