CS 5472 - Advanced Topics in Computer Security

Topic 8: Ransomware (1)

Spring 2018 Semester
Instructor: Bo Chen
bchen@mtu.edu
http://cs.mtu.edu/~bchen
Final Project Presentation

• April 17, April 19, potentially part of April 24. Arranged according to the alphabetical order of students’ last names
  • Sandeep Battula
  • Manu Nandan Chemudupati
  • Sophia Farquhar
  • Ali Jalooli
  • Rahul Javadekar
  • Krishna Kakula
  • Shashank Munnooru
  • Ryan Olson
  • Abheek Srivastava

• Each student has 25 minutes (presentation + Q&A)
  • Problem/motivation (what is the problem? Why doing it?)
  • Related work (What have been done?)
  • Solution (what is your solution?)
  • Evaluation (How can you convince us that your solution is good?)
Final Project Presentation (cont.)

• Survey: Do you want to reduce one more summary so that you can have more time to finish your project? (I observed the quality of summary is improved)
Ransomware Attacks Keep Growing...

- A piece of special malware that infects a computer and restricts access to the computer and/or its files
- Ask for a ransom to be paid in order for the restriction to be removed

*Source: Proofpoint Q1 2017 Quarterly Threat Report*
Ransomware Propagation
WannaCry

Within a day the code was reported to have infected more than 230,000 computers in over 150 countries.
Types of Ransomware

- Locker ransomware
- Crypto ransomware
How to Defend against Locker Ransomware?

• Observation: only the system is locked by the ransomware, but the data are stored intact

• Unplug the storage medium(e.g., hard drives, SSD drives, SD cards), plug the storage medium to a new computing device, and copy out the data

• Plug the storage device back to the device which has been locked, and re-install/initialize the system, then copy the data back
How to Defend against Crypto Ransomware?

• Option 1: detect crypto ransomware *before it causes significant damage to data*
  • Crypto ransomware may be detected since it behaves differently from normal software and other types of malware
  • Crypto ransomware usually *encrypts a large amount of data in a short time, and over-writes the old data*
    • A large number of read access
    • Expensive computation is required for a large amount of encryptions
    • A large number of writes/over-writes in a short time

The most challenging issue is how to detect the crypto ransomware fastly, since the detection is time-sensitive
How to Defend against Crypto Ransomware (cont.)?

• Option 2: make sure the data encrypted by crypto ransomware are **always recoverable**
  - Create backups, but where to store the backups
    - Cloud? Extra cost for purchasing resources and maintaining the backups
    - Local? How to make sure that the crypto ransomware cannot have access to the backups and then corrupt the backups?
How to Defend against Crypto Ransomware (cont.)?

• Option 3: detection + recovery
Paper Presentation

• ShieldFS: A Self-healing, Ransomware-aware Filesystem

• Presented by Ryan Olson