CS 5472 - Advanced Topics in Computer Security

Topic 7: Ransomware (1)

Spring 2021 Semester
Instructor: Bo Chen
bchen@mtu.edu
https://cs.mtu.edu/~bchen
https://snp.cs.mtu.edu
Malware

• Malware (a portmanteau for malicious software): any software intentionally designed to cause damage to a computer, server, client, or computer network
  • By contrast, software that causes unintentional harm due to some deficiency is typically described as a software bug.

• A wide variety of malware types exist
  • Computer viruses
  • Worms
  • Trojan horses
  • Ransomware
  • Spyware
  • Adware
  • Rootkit
  • Backdoor
  • Etc.
The Growth of Malware Recently

Total malware

AV-TEST

Last update: March 14, 2021

Copyright © AV-TEST GmbH, www.av-test.org
Ransomware

• Ransomware is a special type of malware:
  • infects a computer and restricts access to the computer and/or its files
  • asks for a ransom to be paid in order for the restriction to be removed

• Starting from around 2012, the use of ransomware scams has grown internationally.
  • There were 181.5 million ransomware attacks in the first six months of 2018. This record marks a 229% increase over this same time frame in 2017.
Ransomware Attacks in 2020

Ransomware Attacks by Industry

<table>
<thead>
<tr>
<th>Industry</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturing</td>
<td>40</td>
</tr>
<tr>
<td>Government</td>
<td>40</td>
</tr>
<tr>
<td>Education</td>
<td>32</td>
</tr>
<tr>
<td>Services</td>
<td>31</td>
</tr>
<tr>
<td>Healthcare</td>
<td>30</td>
</tr>
<tr>
<td>Utilities</td>
<td>15</td>
</tr>
<tr>
<td>Technology</td>
<td>18</td>
</tr>
<tr>
<td>Logistics</td>
<td>16</td>
</tr>
<tr>
<td>Retail</td>
<td>8</td>
</tr>
<tr>
<td>Other</td>
<td>16</td>
</tr>
</tbody>
</table>
Ransomware Attacks in 2020

Ransomware Attacks by Country

- USA
- UK
- Australia
- Canada
- Germany
- India
- Japan
- France
- Taiwan
- ROW
Ransomware Propagation
Cast Study: WannaCry

Propagated through EternalBlue, an exploit developed by the US National Security Agency (NSA) for older Windows systems

• Vulnerabilities in Windows Server Message Block (SMB) protocol
• NSA discovered the vulnerability, but used it to create an exploit for its own offensive work, rather than report it to Microsoft

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
Locker Ransomware

• Lock the victim system

• Easy to be combat, since only the system is locked, but data remain intact
How to Combat 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
Crypto Ransomware

• The victim data are encrypted, and cannot be recovered if not able to obtain the key for decryption

• How does it work
  • Symmetric encryption: the encryption and decryption are using the same key
    • Good for ransomware: fast encryption
    • Bad for ransomware: the encryption key in plaintext needs to be distributed during encryption process, and can be easily leaked

  • Asymmetric encryption: use public key to encrypt, but private key to decrypt
    • Good for ransomware: only need to distribute the public key during encryption process
    • Bad for ransomware: the asymmetric encryption is expensive, and can be easily detected
How to Combat Ransomware

• Detection: detect the ransomware once it starts to work (focus of today)
  • Detection needs to be fast enough so that ransomware can be blocked before it causes damages to the victim
  • Rationale: ransomware has some sort of working patterns (e.g., the crypto-ransomware always needs to encrypt the victim’s data, and delete/overwrite the original data)

• Recovery: if all the data encrypted by ransomware can guarantee to be recovered, ransomware would not be a problem (focus of Thursday)
  • Obtaining the key: pay the ransom; extract the key in the victim system
  • Backup
    • Off-device backup: e.g., iCloud
    • In-device backup: e.g., utilizing the out-of-place update property of flash memory, such that old data can be temporarily preserved
  • Detection + recovery
A Little More on Ransomware Detection

• 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
Paper Presentation

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

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

Professor: Dr. Bo Chen
Student: Soheil Sepahyar
Class: CS 5472 (Advanced Topic In Computer Security)
OUTLINE

- Introduction To Ransomware Attacks and Background
- How to defend against ransomware attacks?
- Threat Model
- UNVEIL Design (Early Warning Dynamic Detection for Ransomware)
  - Detecting the File Locker
  - Detecting Screen Locker
- UNVEIL Analysis Environment Preparation
- Evaluation
  - Experimental Setup
  - First Experiment and Ground Truth (Labeled Dataset)
  - Second Experiment and Detecting Zero-Day Ransomware
  - New Case Study type of Ransomware (Automated Detection Of a New Ransomware Family)
OUTLINE

- Discussion and Limitations
- Conclusion and My Final Thoughts
- Q & A
- References
1. **Introduction To Ransomware Attacks and Background**

What is Ransomware attacks?

**Ransomware** is malicious software that infects your computer and displays messages demanding a fee to be paid in order for your system to work again.
1. Introduction To Ransomware Attacks and Background

What are the recent and the Most Important Ransomware attacks in 2020 and other years?

1) Communications & Power Industries (CPI) Ransomware Attack

2) University of California San Francisco (UCSF) Ransomware Attack

3) WannaCry Outbreak and ...

On 12 May 2017, an updated version of WCry/WannaCry ransomware called “WanaCrypt0r 2.0” struck hospitals belonging to the United Kingdom’s National Health Service (NHS), internet service provider Telefonica and other high-profile targets around the world. Researchers ultimately determined that WannaCry had made its rounds by exploiting EternalBlue, a vulnerability which Microsoft patched in a security bulletin in March 2017. In total, WannaCry demanded $300 in bitcoin from more than 300,000 organizations worldwide through that attack.
1. Introduction To Ransomware Attacks and Background

A post-mortem on the impact of WannaCry found the outbreak cost U.K. hospitals almost $100 million pounds and caused significant disruption to patient care, such as the cancellation of some 19,000 appointments — including operations — and the disruption of IT systems for at least a third of all U.K. National Health Service (NHS) hospitals and eight percent of general practitioners. In several cases, hospitals in the U.K. were forced to divert emergency room visitors to other hospitals.

WannaCry is an example of crypto ransomware, a type of malicious software (malware) used by cybercriminals to extort money.
How to defend against ransomware attacks?

1) Backup Everything, Every day
2) Screen Your Emails and Don’t Click Suspicious Links or Ads
3) Install an Antivirus Firewall
4) Invest in Security Awareness Training

1) Developing detection tools to assist defenders ⇒ Providing insight from internal behavior

2) Developing protection tools (sitting on the End User Machine and Kill Them) ⇒ Stopping the attack, and keeping the data consistent and Monitor the Virus.
Thread Model

Ransomware can use any techniques to attack the users such as:

1) Inject code into benign processes
2) Perform encrypted communication with the C&C server
3) Leverage arbitrary cryptosystems

It can happen in two different methods?

1) File Encryption
2) Screen Locking
Thread Model

Base Part of Ransomware:

- Ransomware informs the victim that attack has taken place
- Ransomware has certain behaviors that can be predictable (such as entropy changes, iteration of files due to the good amount of access to the data for encryption, Background Activity, accessing user files, Or it might lock your screen!)

Now These hints can be very helpful to detect Ransomwares!!
UNVEIL Architecture

Figure 1: Overview of the design of I/O access monitor in UNVEIL. The module monitors system-wide filesystem accesses of user-mode processes. This allows UNVEIL to have full visibility into interactions with user files.
UNVEIL Design (Early Warning Dynamic Detection for Ransomware)

Detecting The File Locker:

(How UNVEIL uses the output of the filesystem monitor to detect ransomware?)

Detecting Cryptographic Ransomware:

1) Generating a fake (and attractive) user environment
2) Finding a reliable method for monitoring filesystem activity
UNVEIL Design (Early Warning Dynamic Detection for Ransomware)

Why the fake user environment was generated?

1) Making the analysis environment more realistic.

2) Protecting the analysis system from some user environment fingerprinting since static environment can be easily tracked.
UNVEIL Design (Early Warning Dynamic Detection for Ransomware)

Generating Fake (Honey) Content:

1) Files with Valid Header
   - Using standard libraries (e.g., python-docx, python-pptx)
   - Meaningful Content
   - Realistic Filename which is not random generated

2) File Path
   - User’s directory structure is generated randomly, but meaningfully

3) File attributes
   - Generate content with different creation, modification, and access times
Extracting I/O Access Sequences

Figure 2: Strategies differ across ransomware families with respect to I/O access patterns. (1) Attacker overwrites the users’ file with an encrypted version; (2) Attacker reads, encrypts and deletes files without wiping them from storage; (3) Attacker reads, creates a new encrypted version, and securely deletes the original files by overwriting the content.
UNVEIL Design (Early Warning Dynamic Detection for Ransomware)

Detecting Screen Locker:

The second core component of UNVEIL is aimed at detecting screen locker ransomware. The key insight behind this component is that the attacker must display a ransom note to the victim in order to receive a payment.
UNVEIL Analysis Environment Preparation

- **UNVEIL is working on top of Cuckoo Sandbox**
  - Support All Windows (Looks Like XP is their experimental OS)
  - This Tool Deployed in the Kernel ⇒ Better Access to the Files
  - Bypassing UNVEIL is not technically easy in user-mode (I think since it has access to the OS layers and resources)

- **Finding Active Malwares**
  - modified some parts of Cuckoo to make it more resilient to environmentally sensitive samples
  - Other anti-evasion measures to look more realistic (such as having Multiple NTFS Drives, IP address changing, etc)
UNVEIL Analysis Environment Preparation

They evaluated UNVEIL using 56 VMs running Windows XP SP3 on a Ganeti cluster based on Ubuntu 14.04 LTS. While Windows XP is not required by UNVEIL, it was chosen because it is well-supported by Cuckoo sandbox.

Each VM had multiple NTFS drives. They took antievasion measures against popular tricks such as changing the IP address range and the MAC addresses of the VMs to prevent the VMs from being fingerprinted by malware authors.
Evaluation

1) Detecting known ransomware samples
   - Collecting ~3500 ransomware from public repo, Anubis, two security companies.
   - 149 benign executables including ransomware-like behavior.
   - 348 malware samples from 36 malware families

<table>
<thead>
<tr>
<th>Family</th>
<th>Type</th>
<th>Samples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptolocker</td>
<td>crypto</td>
<td>33 (1.5%)</td>
</tr>
<tr>
<td>CryptoWall</td>
<td>crypto</td>
<td>42 (2.0%)</td>
</tr>
<tr>
<td>CTB-Locker</td>
<td>crypto</td>
<td>77 (3.6%)</td>
</tr>
<tr>
<td>CrypVault</td>
<td>crypto</td>
<td>21 (1.0%)</td>
</tr>
<tr>
<td>CoinVault</td>
<td>crypto</td>
<td>17 (0.8%)</td>
</tr>
<tr>
<td>Filecoder</td>
<td>crypto</td>
<td>19 (0.9%)</td>
</tr>
<tr>
<td>TeslaCrypt</td>
<td>crypto</td>
<td>39 (1.8%)</td>
</tr>
<tr>
<td>Tox</td>
<td>crypto</td>
<td>71 (3.3%)</td>
</tr>
<tr>
<td>VirLock</td>
<td>locker</td>
<td>67 (3.2%)</td>
</tr>
<tr>
<td>Reveton</td>
<td>locker</td>
<td>501 (23.6%)</td>
</tr>
<tr>
<td>Tobfy</td>
<td>locker</td>
<td>357 (16.8%)</td>
</tr>
<tr>
<td>Uaraya</td>
<td>locker</td>
<td>877 (41.3%)</td>
</tr>
<tr>
<td><strong>Total Samples</strong></td>
<td></td>
<td><strong>2,121</strong></td>
</tr>
</tbody>
</table>

Table 1: The list of ransomware families used in the first experiment.

A Benign Applications Used in Experiment One

<table>
<thead>
<tr>
<th>Application</th>
<th>Main Capability</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>7-zip</td>
<td>Compression</td>
<td>15.06</td>
</tr>
<tr>
<td>Winzip</td>
<td>Compression</td>
<td>19.5</td>
</tr>
<tr>
<td>WinRAR</td>
<td>Compression</td>
<td>5.21</td>
</tr>
<tr>
<td>DiskCryptor</td>
<td>Encryption</td>
<td>1.1.846.118</td>
</tr>
<tr>
<td>AESCrypt</td>
<td>Encryption</td>
<td>—</td>
</tr>
<tr>
<td>Eraser</td>
<td>Shredder</td>
<td>6.2.0.2969</td>
</tr>
<tr>
<td>SDelete</td>
<td>Shredder</td>
<td>1.61</td>
</tr>
</tbody>
</table>

Table 5: The list of benign applications that generate similar I/O access patterns to ransomware.
Evaluation

2) Evaluation UNVEIL with unknown samples

○ The incoming samples were acquired from the daily malware feed provided by Anubis from March 18 to February 12, 2016.

○ The dataset contained 148,223 distinct samples.
Evaluation

2) Evaluation UNVEIL with unknown samples

VT == VirusTotal

Figure 4: Evolution of VT scanner reports after six submissions. 72.2% of the samples detected by UNVEIL were not detected by any of AV scanners in the first submission. After a few re-submissions, the detection results do not change significantly. The detection results tend to be concentrated either towards small or very large detection ratios. This means that a sample is either detected by a relatively small number of scanners, or almost all of the scanners.
Evaluation (Final Results)

<table>
<thead>
<tr>
<th>Evaluation</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Samples</td>
<td>148,223</td>
</tr>
<tr>
<td>Detected Ransomware</td>
<td>13,637 (9.2%)</td>
</tr>
<tr>
<td>Detection Rate</td>
<td>96.3%</td>
</tr>
<tr>
<td>False Positives</td>
<td>0.0%</td>
</tr>
<tr>
<td>New Detection</td>
<td>9,872 (72.2%)</td>
</tr>
</tbody>
</table>

Table 4: UNVEIL detection results. 72.2% of the ransomware samples detected by UNVEIL were not detected by any of AV scanners in VirusTotal at the time of the first submission. 7,572 (76.7%) of the newly detected samples were destructive file locker ransomware samples.
Evaluation

New Case Study type of Ransomware (Automated Detection Of a New Ransomware Family)

During the experiments, they discovered a new malware family named “SilentCrypt”:

analysis concluded that the malicious activity is started only if user activity is detected. Unlike other ransomware samples that immediately attack a victim’s files when they are executed.

Figure 5: I/O activities of a previously unknown ransomware family detected by UNVEIL. The sample first performs victim file fingerprinting to ensure that the running environment is not a bare user environment.
Discussion and Limitations

- The evaluation section demonstrates that UNVEIL achieves good, practical, and useful detection results on a large, real-world dataset compare with a lot of other advanced AV scanner.

- Another possibility is that a malware might only encrypt a specific part of a file instead of aggressively encrypting the entire file, or simply shuffle the file content using a specific pattern that makes the files unreadable.

- Clearly, there is always the possibility that an attacker will be able to fingerprint the dynamic analysis environment. For example, stalling code has become increasingly popular to prevent the dynamic analysis of a sample. Such code takes longer to execute in a virtual environment, preventing execution from completing during an analysis.
Static and Dynamic Analyses Explained

1) Static analysis is performed in a non-runtime environment. Static application security testing (SAST) is a testing process that looks at the application from the inside out. This test process is performed without executing the program, but rather by examining the source code, byte code or application binaries for signs of security vulnerabilities.

2) Dynamic application security testing (DAST) looks at the application from the outside in — by examining it in its running state and trying to manipulate it in order to discover security vulnerabilities. The dynamic test simulates attacks against a web application and analyzes the application’s reactions, determining whether it is vulnerable.
Conclusion and My Final Thoughts

- Ransomware is a serious threat.
- UNVEIL introduces concrete models to detect Ransomware.
- Detecting an unknown family shows that the solutions are useful in practice.
- Great Job regarding the importance of this work and ransomware.
- I think Screen Lockers detection can be very much improved with Machine Learning and Deep Learning algorithms rather than mostly pure algorithms. (One example can be transparency issue of the ransomware app on the desktop)
- I also think the author also could put more effort into the changes in the entropy of the file to detect ransomware in addition to checking file system monitoring...
Questions?
References


2. A Large-Scale, Automated Approach to Detecting Ransomware Amin Kharraz, Sajjad Arshad, Collin Mulliner, William Robertson, Engin Kirda


6. https://www.veracode.com/blog/secure-development/static-testing-vs-dynamic-testing