A Large-Scale, Automated Approach to Detecting Ransomware

Amin Kharraz, Sajjad Arshad, Collin Mulliner, William Robertson, Engin Kirda
What is a ransomware attack?

1. Paying the ransom fee
2. Receiving the decryption key
A Typical Ransom Note

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press ‘View’ to view the list of files that have been encrypted.

Press ‘Next’ for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL loose YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.
Attacks on Hospitals

Privacy & Security

Ransomware attackers collect ransom from Kansas hospital, don't unlock all the data, then demand more money

Kansas Heart Hospital declined to pay the second ransom, saying that would not be wise. Security experts, meanwhile, are warning that ransomware attacks will only get worse.

By Bill Siwicki | May 23, 2016 | 02:58 PM

Kansas Heart Hospital in Wichita paid the initial ransom but decided against paying the second request even though some of its data appears to still be locked.

Kansas Heart Hospital was the victim of a ransomware attack and after it paid the first one, attackers boldly demanded a second ransom to decrypt data.

Kansas Heart Hospital president Greg Duick, MD told local media that patient
University Pays $16,000 to Stop Ransomware Attack

by Jeff John Roberts  @jeffjohnroberts  JUNE 8, 2016, 1:29 PM EDT
Police pay ransom after cyberterror attack on network

By Jayne W. Miller News Editor
Jayne@YourTownCrier.com | 1 comment

Chief: “Paying ransom was the last resort”

TEWKSBURY – Last December Tewksbury Police confronted a new, and growing, frontier in cyberterrorism when the CryptoLocker ransomware virus infected the department’s network, encrypting essential department files until the town paid a $500 bitcoin ransom. In total, police systems were down between four and five days as the department worked with the FBI, Homeland Security, Massachusetts State Police, as well as private firms in an effort to restore their data without paying the ransom.

Thomas Murphy, Daniel Sawicki and Lt. Scott Keddie
New estimates from the FBI show that the costs from so-called ransomware have reached an all-time high.

“Cyber-criminals collected $209 million in the first three months of 2016 by extorting businesses and institutions to unlock computer servers.”

– CNN Interview with FBI, April 2016
How to defend against ransomware attacks?

- Educating end-users
  - Have a reliable backup policy
  - Avoid risky online behavior
- Developing detection tools to assist defenders
  - Providing insight from internal behavior
- Developing protection tools to enhance AV capabilities
  - Stopping the attack, and keeping the data consistent
How to defend against ransomware attacks?

- Educating end-users
  - Have a reliable *backup* policy
  - Avoid risky online behavior

- Developing *detection* tools to assist defenders
  - Providing insight from *internal* behavior

- Developing *protection* tools to enhance AV capabilities
  - Stopping the attack, and keeping the data consistent
Threat Model

- Ransomware can employ any techniques to attack
  - Inject code into benign processes
  - Perform encrypted communication
  - Leverage arbitrary cryptosystems
- We assume that OS kernel, and underlying software and hardware stack are free of malicious code.
- Unveil detects ransomware during dynamic analysis phase, and not at end-user machines.
  - Complements current dynamic analysis systems
  - A cloud-based malware analysis service, sample sharing

But, how can we detect a ransomware sample?
Achilles’ Heel of Ransomware

- Ransomware has to inform victim that attack has taken place

- Ransomware has certain behaviors that are predictable
  - e.g., entropy changes, modal dialogs and background activity, accessing user files

- A good sandbox that looks for some of these signs helps here…
UNVEIL: An Early Warning Dynamic Detection System for Ransomware
UNVEIL’s Architecture

Process 1  Process 2  Process 3  Process N

read  write  write  delete

I/O Scheduler

I/O Requests

UNVEIL

FileSystem Driver

Physical Device

User Mode
Kernel Mode

file’s data Buffer

Identify File OP
I/O Type
Calculate Entropy

Identify Process
I/O Monitor ENTER
I/O Monitor EXIT

Record I/O Request

I/O Access Monitor
Approach

• Detecting Cryptographic Ransomware:
  • Generating a fake (and attractive) user environment
  • Finding a reliable method for monitoring filesystem activity

Why do we generate fake user environments?

• Making the analysis environment more realistic
• Protecting the analysis system from some user environment fingerprinting
  - A static user environment can be easily detected by a malware
Approach

- **Detecting** Cryptographic Ransomware:
  - Generating a fake (and attractive) user environment
  - Finding a reliable method for monitoring filesystem activity

Why do we generate fake user environments?

- Making the analysis environment more realistic
- Protecting the analysis system from bare-user environment fingerprinting
  - A static user environment can be *easily* detected by a malware

How do we generate fake user environments?
Generating Fake (Honey) Content

• Real files with valid headers
  – Using standard libraries (e.g., python-docx, python-pptx, OpenSSL)
  – Content that appears meaningful
  – File names do not look random, and appear realistic

• File paths
  – User’s directory structure is generated randomly, but meaningfully

• File attributes
  – Generate content with different creation, modification, and access times
\[ R_{fs} = \langle \text{Time}, \text{P}_{\text{name}}, \text{P}_{\text{id}}, \text{PP}_{\text{id}}, \text{IRP}_{\text{flag}}, \text{Arg}, \text{Result}, \text{Buf}_{\text{Entropy}} \rangle \]
Extracting I/O Access Sequences

(1) Overwrites the users’ file with an encrypted version
(2) reads, encrypts and deletes files without wiping them from storage
(3) reads, creates a new encrypted version, and securely deletes the original files
### IO Access Sequences in Multiple Ransomware Families

<table>
<thead>
<tr>
<th>Ransomware Family</th>
<th>IRP Operation</th>
<th>Process</th>
<th>Filename</th>
<th>File Offset</th>
<th>Entropy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CryptoWall</td>
<td>IRP_MJ_CREATE</td>
<td>explorer.exe</td>
<td>honeyfile.doc</td>
<td></td>
<td></td>
<td>Read, write</td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_READ</td>
<td>explorer.exe</td>
<td>honeyfile.doc</td>
<td>[0, 4096)</td>
<td>4.21</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_WRITE</td>
<td>explorer.exe</td>
<td>honeyfile.doc</td>
<td>[0, 4096)</td>
<td>7.11</td>
<td>Read, write</td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_CLEANUP</td>
<td>explorer.exe</td>
<td>honeyfile.doc</td>
<td></td>
<td></td>
<td>Read, write</td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_CLOSE</td>
<td>explorer.exe</td>
<td>honeyfile.doc</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Deleting the Original File</td>
</tr>
<tr>
<td></td>
<td>FileCoder</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_CREATE</td>
<td>svchost.exe</td>
<td>honeyfile.doc</td>
<td>[0, 4096)</td>
<td>4.21</td>
<td>Read</td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_READ</td>
<td>svchost.exe</td>
<td>honeyfile.doc</td>
<td>[0, 4096)</td>
<td>7.02</td>
<td>Read, write</td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_WRITE</td>
<td>svchost.exe</td>
<td>honeyfile.doc</td>
<td>[0, 4096)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_CLEANUP</td>
<td>svchost.exe</td>
<td>honeyfile.doc</td>
<td></td>
<td></td>
<td>Read attributes, delete</td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_CLOSE</td>
<td>svchost.exe</td>
<td>honeyfile.doc</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Deleting the Original File</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Read attributes, delete</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CrypVault</td>
<td>explorer.exe</td>
<td>balance.doc</td>
<td></td>
<td></td>
<td>Read</td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_CREATE</td>
<td>explorer.exe</td>
<td>balance.doc</td>
<td></td>
<td></td>
<td>Read, write</td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_CREATE</td>
<td>explorer.exe</td>
<td>balance.doc.vault</td>
<td>[0, 41014)</td>
<td>4.33</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_READ</td>
<td>explorer.exe</td>
<td>balance.doc</td>
<td>[0, 41014)</td>
<td>7.14</td>
<td>Write</td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_WRITE</td>
<td>explorer.exe</td>
<td>balance.doc.vault</td>
<td>[0, 41014)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_CLEANUP</td>
<td>explorer.exe</td>
<td>balance.doc</td>
<td></td>
<td></td>
<td>Read, write</td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_CLOSE</td>
<td>explorer.exe</td>
<td>balance.doc</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_CREATE</td>
<td>explorer.exe</td>
<td>balance.doc</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_CREATE</td>
<td>explorer.exe</td>
<td>balance.doc</td>
<td>[0, 4096)</td>
<td>4.02</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_WRITE</td>
<td>explorer.exe</td>
<td>balance.doc</td>
<td>[0, 4096)</td>
<td>4.02</td>
<td></td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_CLOSE</td>
<td>explorer.exe</td>
<td>balance.doc.vault</td>
<td>[4096, 8192)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_SET_CREATE</td>
<td>explorer.exe</td>
<td>balance.doc.vault</td>
<td></td>
<td></td>
<td>Read attributes, delete</td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_SET_INFORMATION</td>
<td>explorer.exe</td>
<td>balance.doc.vault</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Iteration over files during a CryptoWall attack

<table>
<thead>
<tr>
<th>File</th>
<th>Operation</th>
<th>Process</th>
<th>Entropy</th>
</tr>
</thead>
<tbody>
<tr>
<td>midterm_paper.docx</td>
<td>IRP_MJ_CREATE</td>
<td>svchost.exe</td>
<td>—</td>
</tr>
<tr>
<td>midterm_paper.docx</td>
<td>IRP_MJ_READ</td>
<td>svchost.exe</td>
<td>4.01</td>
</tr>
<tr>
<td>midterm_paper.docx</td>
<td>IRP_MJ_WRITE</td>
<td>svchost.exe</td>
<td>7.28</td>
</tr>
<tr>
<td>midterm_paper.docx</td>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>midterm_paper.docx</td>
<td>IRP_MJ_CLEANUP</td>
<td>svchost.exe</td>
<td>—</td>
</tr>
<tr>
<td>midterm_paper.docx</td>
<td>IRP_MJ_CLOSE</td>
<td>svchost.exe</td>
<td>—</td>
</tr>
<tr>
<td>myweddingparty.mpeg</td>
<td>IRP_MJ_CREATE</td>
<td>svchost.exe</td>
<td>—</td>
</tr>
<tr>
<td>myweddingparty.mpeg</td>
<td>IRP_MJ_READ</td>
<td>svchost.exe</td>
<td>5.14</td>
</tr>
<tr>
<td>myweddingparty.mpeg</td>
<td>IRP_MJ_WRITE</td>
<td>svchost.exe</td>
<td>7.24</td>
</tr>
<tr>
<td>myweddingparty.mpeg</td>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>myweddingparty.mpeg</td>
<td>IRP_MJ_CLEANUP</td>
<td>svchost.exe</td>
<td>—</td>
</tr>
<tr>
<td>myweddingparty.mpeg</td>
<td>IRP_MJ_CLOSE</td>
<td>svchost.exe</td>
<td>—</td>
</tr>
</tbody>
</table>
Desktop Locker Ransomware

1. Analysis Environment
   - User Data
   - Windows XP
   - Cuckoo Sandbox

2. Malware run

3. NEU SECLAB
Desktop Locker Ransomware

Dissimilarity Score
Preparing the Analysis Environment

- UNVEIL is deployed on top of Cuckoo Sandbox
  - UNVEIL supports all versions of Windows platforms.
  - Our tool is deployed in Kernel.
  - Bypassing UNVEIL is not technically easy in user-mode.

- Finding active malware is not easy
  - We modified some parts of Cuckoo to make it more resilient to environmentally sensitive samples
    - e.g., fake response to some of the environment checks
  - Other anti-evasion measures to look more realistic
    - e.g., defining multiple NTFS drives, changing IP address range and MAC addresses
Evaluation

1) Detecting known ransomware samples

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

<table>
<thead>
<tr>
<th>Benign Applications</th>
<th>Ransomware Families</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application</strong></td>
<td><strong>Main Capability</strong></td>
</tr>
<tr>
<td>7-zip</td>
<td>Compression</td>
</tr>
<tr>
<td>Winzip</td>
<td>Compression</td>
</tr>
<tr>
<td>WinRAR</td>
<td>Compression</td>
</tr>
<tr>
<td>DiskCryptor</td>
<td>Encryption</td>
</tr>
<tr>
<td>AESCrypt</td>
<td>Encryption</td>
</tr>
<tr>
<td>Eraser</td>
<td>Shredder</td>
</tr>
<tr>
<td>SDelete</td>
<td>Shredder</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total Samples</strong></td>
<td></td>
</tr>
</tbody>
</table>
Dissimilarity score is different from family to family
Detecting known ransomware samples

The threshold value $t = 0.32$ gives the highest recall with 100% precision.
Evaluation UNVEIL with unknown samples

~ 1200 malware samples per day

56 UNVEIL-enabled VMs on 8 Servers
Evaluation UNVEIL with unknown samples

- We used the same similarity threshold \((t = 0.32)\) for the large scale experiment.
- 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.
Cross-checking with VirusTotal

- Pollution ratio is defined as the ratio of the number of scanners that identified the sample to the number of scanners in VirusTotal
## Detection 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>
Detection: New Ransomware Family

- Query Operation (QUERY OP)
- Read Operation (READ OP)
- Write Operation (WRITE OP)

Userspace file fingerprinting
Periodic file encryption
Creating a list of files
Detection: New Ransomware Family

• During our experiments, we discovered a new malware family
  – We call it “SilentCrypt”
  – After we reported it, others started detecting it as well
  – We were not able to find any information about this family online
  – The ransomware first checks for private files of a user, contacts the C&C server, and starts the attack based on the answer
Detection: New Ransomware Family
Conclusion

- Ransomware is a serious threat
- UNVEIL introduces concrete models to detect Ransomware
- Detecting an unknown family shows that the solutions are useful in practice
- We continue to improve functionality tuned towards detecting ransomware
Thank You