A Large-Scale, Automated Approach to Detecting Ransomware

Amin Kharraz, Sajjad Arshad, Collin Mulliner, William Robertson, Engin Kirda
A bitcoin ransomware attack on a New Jersey school district has grown into an investigation involving multiple US government agencies.

The Swedesboro-Woolwich School District, which encompasses four elementary schools in Gloucester County, New Jersey, was forced to delay a statewide standardized test earlier this week after the ransomware was discovered over the weekend.
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
Attacks on Hospitals
“Between April 2014 and June 2015, the IC3 received 992 CryptoWall-related complaints, with victims reporting losses totaling over $18 million.”

What is a ransomware attack?

1. Infecting the machine

- Attachments
- Drive-by Downloads
- Malicious binaries
A Typical Ransom Note

Your computer has been locked due to suspicion of illegal content downloading and distribution.

The illegal content (414 Mb of photo and video files) was automatically classified as child pornographic materials.

The downloading and distribution of illegal content, in whole or in part, violate the following U.S. Federal Laws:

18 U.S.C. § 2251 Sexual exploitation of children (Production of child pornography)
18 U.S.C. § 2252C Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)
18 U.S.C. § 2252A Certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 6 months to 10 years and shall be fined up to $250,000.

Your case can be classified as occasional/unmotivated, according to 17 (U.S. Code) §512

Thus it may be closed without prosecution.
Your computer will be unlocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of $300

Exchange your cash for a MoneyPak voucher and use your voucher code in the form below:

Code: 1 2 3 4 5 6 7 8 9 0

Status: Waiting for payment
Permanent lock on 09/26/2013 8:46 p.m. EST

Where can I buy MoneyPak

NEU SECLAB
What is a ransomware attack?

② Paying the ransom fee
What is a ransomware attack?

③ Receiving the decryption key
What is a ransomware attack?

4 Unlocking the machine
How to defend against ransomware attacks?

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

- 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

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

• Ransomware *has to inform* victim that attack has taken place
  – Behavior inherent in its nature
• Ransomware has certain behaviors that are predictable
  – e.g., entropy changes, modal dialogs and background activity, accessing “honey” files
• A good sandbox that looks for some of these signs helps here…
UNVEIL: An Early Warning Dynamic Detection System for Ransomware
Approach

• Detecting ransomware based on two techniques:
  – 1) Crypto-style Ransomware
    • Generating a fake (and attractive) user environment
    • Finding a reliable method for monitoring filesystem activity
  – 2) Desktop Locker
    • Going after the ransom note and using heuristics to detect such a message to the user
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
UNVEIL’s Architecture
$R_{fs} = \langle \text{Time}, \text{Name}, \text{Pid}, \text{PPid}, \text{IRPFlag}, \text{Arg}, \text{Result}, \text{BufEntropy} \rangle$
1 Reading user’s file content

PATH = D:\submission.doc

read(D:\submission.doc)
2. Writing encrypted data on the file

PATH=D:\submission.doc

write(D:\submission.doc)

I/O MANAGER

USER

KERNEL

UNVEIL

NEU SECLAB
1. Reading user’s file content

PATH = D:\submission.doc

user

I/O MANAGER

read(D:\submission.doc)

KERNEL

USER

UNVEIL
2 Creating a new file, and writing encrypted data to it

PATH=D:\submission.doc

PATH=D:\submission.doc.locked

write(D:\submission.doc.locked) USER

write(D:\submission.doc.locked) I/O MANAGER

write I/O MANAGER

write UNVEIL

KERNEL

NEU SECLAB
3 Deleting the original file

PATH = D:\submission.doc

PATH = D:\submission.doc.locked

delete(D:\submission.doc)

USER

I/O MANAGER

KERNEL

UNVEIL

NEU SECLAB
3. Or, overwriting the original file

```plaintext
write(D:\submission.doc)
PATH=D:\submission.doc
```

Or, overwriting the original file

```plaintext
write(D:\submission.doc.locked)
PATH=D:\submission.doc.locked
```

**I/O MANAGER**

**USER**

**KERNEL**

**UNVEIL**

**NEU SECLAB**
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></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></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>FileCoder</td>
<td>IRP_MJ_CREATE</td>
<td>svchost.exe</td>
<td>honeyfile.doc</td>
<td></td>
<td></td>
<td>Read</td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_CREATE</td>
<td>svchost.exe</td>
<td>honeyfile.doc.crypt</td>
<td></td>
<td></td>
<td>Read, write</td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_READ</td>
<td>svchost.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>svchost.exe</td>
<td>honeyfile.doc.crypt</td>
<td>[0, 4096)</td>
<td>7.02</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_CLEANUP</td>
<td>svchost.exe</td>
<td>honeyfile.doc</td>
<td></td>
<td></td>
<td></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>IRP_MJ_CREATE</td>
<td>svchost.exe</td>
<td>honeyfile.doc</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_SET_INFORMATION</td>
<td>svchost.exe</td>
<td>honeyfile.doc</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></td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_CLOSE</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.crypt</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_CLOSE</td>
<td>svchost.exe</td>
<td>honeyfile.doc.crypt</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_CLOSE</td>
<td>svchost.exe</td>
<td>honeyfile.doc.crypt</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>CryptVault</td>
<td>IRP_MJ_CREATE</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_READ</td>
<td>explorer.exe</td>
<td>balance.doc</td>
<td>[0, 41014)</td>
<td>4.33</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_WRITE</td>
<td>explorer.exe</td>
<td>balance.doc</td>
<td>[0, 41014)</td>
<td>7.14</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>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_WRITE</td>
<td>explorer.exe</td>
<td>balance.doc</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>IRP_MJ_CLOSE</td>
<td>explorer.exe</td>
<td>balance.doc</td>
<td></td>
<td></td>
<td>Read attributes, delete</td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_SET_CREATE</td>
<td>explorer.exe</td>
<td>balance.doc</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IRP_MJ_SET_INFORMATION</td>
<td>explorer.exe</td>
<td>balance.doc</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Desktop Locker Ransomware

Analysis Environment

- User Data
- Windows XP
- Cuckoo Sandbox
Desktop Locker Ransomware

Malware run

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

2. Malware run
Desktop Locker Ransomware

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

2. Malware run

3. NEU SECLAB
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>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>
<thead>
<tr>
<th>Ransomware Families</th>
</tr>
</thead>
<tbody>
<tr>
<td>Family</td>
</tr>
<tr>
<td>Cryptolocker</td>
</tr>
<tr>
<td>CryptoWall</td>
</tr>
<tr>
<td>CTB-Locker</td>
</tr>
<tr>
<td>CrypVault</td>
</tr>
<tr>
<td>Filecoder</td>
</tr>
<tr>
<td>Reveton</td>
</tr>
<tr>
<td>Tobfy</td>
</tr>
<tr>
<td>Urausy</td>
</tr>
</tbody>
</table>

Total Samples 1,926
Finding the best threshold value
Detecting known ransomware samples

![Graph showing precision and recall vs dissimilarity threshold](image)
Detecting known ransomware samples

![Graph showing precision and recall for dissimilarity threshold](image)

**NEU SECLAB**

33
Detecting known ransomware samples

The threshold value $t = 0.32$ gives the highest recall with 100% precision
Large-Scale Evaluation

~ 1200 malware samples per day

56 UNVEIL-enabled VMs on 8 Servers

Ganeti Cluster
(4 compute nodes)
Large-Scale Evaluation

- 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.
The results are concentrated either towards small or very large detection ratios.

A sample is either detected by a relatively small number, or almost all of the scanners.
## 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

• 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

- **QUERY OP**: Userspace file fingerprinting
- **READ OP**: Periodic file encryption
- **WRITE OP**: Creating a list of files

*NEU SECLAB*
Detection: New Ransomware Family
Conclusion

- Defending against ransomware is not as complex as it is reported.
- Current analysis systems are not still ready to detect evasive ransomware attacks.
- UNVEIL is the introduction of concrete techniques to detect ransomware.
- SilentCrypt shows that AV industry is not still ready to detect evasive samples.
Thank You