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

Paul Weliczko
Your files are encrypted.

To get the key to decrypt files you have to pay 500 USD/EUR. If payment is not made before 12/05/14 - 21:37 the cost of decrypting files will increase 2 times and will be 1000 USD/EUR.

Prior to increasing the amount length 103h 37m 58s

HELP_DECRYPT.TXT - Notepad

what happened to your files?

All of your files were protected by a strong encryption with RSA-2048. More information about the encryption keys using RSA-2048 can be obtained here http://www.securityfocus.com.

what does this mean?

This means that the structure and data within your files have been encrypted. It is the same thing as losing them forever, but with our help, you can retrieve them.

How did this happen?

Especially for you, on our server was generated the secret key pair for the encryption. All your files were encrypted with the public key, which is only possible with the help of the private key.

what do I do?

As a first step, do not take the necessary measures for the specific situation. If you really value your data, then we suggest you do not waste time and use our service.

For more specific instructions, please visit your personal home page, there are a few different addresses:

1. http://paytoc4tpn5c2z2.topconnectpay.com
2. http://paytoc4tpn5c2z2.topconnectpay.com

If for some reasons the addresses are not available, follow these steps:

1. Visit your personal home page from the address you received.
2. Enter your service ID and password.
3. Click on the “Proceed to payment” button.

Your files will be lost without payment on:

11/04/2013 3:16:34 PM

Select files

Note:
Your important files were encrypted on this computer. Photos, videos, documents, etc. Can be verified by click on any file and try to open it.

Encryption was produced using unique public key RSA-2048 and private key for this computer. To decrypt files, you need to obtain private key.

The single copy of the private key, which will allow you to decrypt the file, is stored on a secret server on the Internet. The server will destroy the key within 72 hours after encryption completion. After that, nobody and never will be able to restore data.

It is possible to extract the private key, you need to pay 500 USD.

Click proceed to payment to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.
Outline

● Introduction
● Motivation
● Background
● UNVEIL Design
● Implementation
● Evaluation
● Discussion and Limitations
● Questions
Introduction

- Ransomware’s resurgence in popularity
- Use in combination with cryptocurrencies

- Successful attack requires tampering with a user’s files or desktop
- UNVEIL generates an artificial user environment and detects when ransomware interacts with user data
Motivation

- One of the largest security threats on the Internet today
- CryptoWall 3.0 caused $325M in damages
- Sony ransomware attack
- Potential to be highly profitable

Table 1

<table>
<thead>
<tr>
<th></th>
<th>Compromised computers</th>
<th>Paid up</th>
<th>Percentage</th>
<th>Ransom</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day</td>
<td>5,700</td>
<td>168</td>
<td>2.90%</td>
<td>200</td>
<td>33,600</td>
</tr>
<tr>
<td>Month (estimated)</td>
<td>68,000</td>
<td>1972</td>
<td>2.90%</td>
<td>200</td>
<td>394,400</td>
</tr>
</tbody>
</table>

Images from https://www.secureworks.com/research/cryptowall-ransomware
Background

- Dynamics of Ransomware
- Evading detection, propagation, and attacking users (like other malware)
- Attack
  - Multi-infection or process injection
  - Send user info to 3rd party
  - Encrypt files
  - Establish communication with C&C servers
Just Ransomware Things

- Persistent desktop message
  - API functions (ex. CreateDesktop()) or HTML

- Indiscriminate encryption and deletion of the user’s private files
  - aggressive encryption, deletion or overwriting
  - encryption keys generated locally or remotely
  - Windows API functions, secure deletion via Windows Secure Deletion API

- Selective encryption and deletion (by size, date, accessed, extension)
  - To avoid detection, files are encrypted selectively
  - Simple- view access date; More advanced- open app and view recently accessed; Even more advanced- inject mal. code into any Windows app
UNVEIL Design: Detecting File & Screen Lockers

- **Detecting File Lockers**
  - Monitors the filesystem activity

- **Generating Artificial User Environment**
  - Malware can detect artificial environment
  - UNVEIL creates user data that seems real (valid content, files paths, time attributes, etc.)

- **Detecting Screen Lockers**
  - Takes screenshots outside of analysis environment to prevent tampering
  - Uses Tesseract-OCR, open source OCR engine, to extract text from the ransom notes in the images
  - Also compares the screenshots before and after sample execution and compare images
Implementation

- Prototype built on top of Cuckoo Sandbox
- Used 56 VMs running Windows XP SP3
- Anti-evasion measures
  - Changing IP address range and MAC addresses
- Limited access to the Internet
  - Filtering and limiting IRC, DNS, and HTTP traffic so samples could communicate with C&C
- Each sample
  - Executed 20 minutes
  - Filesystem IO traces recorded
  - Pre- and post-execution screenshots taken
Evaluation

- 2 Experiments: Detect known ransomware & unknown ransomware
- FP=0% and TP=96.3%
- Able to distinguish between benign apps (ex. 7-zip, AESCrypt, etc.) and ransomware
Discussions & Limitations

- Automated, practical and useful detection on large, real-world dataset
- Malware authors observe defense and adapt
- Fingerprinting Artificial User Environment
  - Can use heuristics to look for specific behavior from user before locking the desktop
  - Makes detection easier since it requires hooking specific functions in the operating system
  - Delay attack and also give more time to detect the attack
- Shuffling Instead of Encrypting
- Modifying Language in Ransom Note
- Stalling code to prevent analysis
- Kernel level ransomware (currently most is user level)
  - More sophisticated and higher barrier to entry
Questions