

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

Paul Weliczko



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

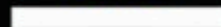
To unlock the computer you are obliged to pay a fine of \$200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]

To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the codes to address fine@fbi.gov.



OK

The image shows a computer screen with a ransomware infection. In the background, a browser window titled "Decrypt service" displays a message: "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 left 103h 37m 58s. Your system: Windows 7 (x64) First connect IP: [redacted]".

In the foreground, a "Cryptolocker 2.0" dialog box is open. It features a shield icon and the text: "Your personal files are encrypted". Below the icon, it says: "Your files will be lost without payment on: 11/24/2013 3:16:34 PM".

The dialog box contains an "Info" section with the following text: "Your important files were encrypted on this computer: photos, videos, documents, etc. You can verify this by click on see files and try to open them. Encryption was produced using unique public key RSA-4096 generated 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 files, is located on a secret server on the Internet, the server will destroy the key within 72 hours after encryption completed. After that, nobody and never will be able to restore files. To retrieve the private key, you need to pay 0.5 bitcoins. 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." At the bottom of the dialog are buttons for "See files", "<< Back", and "Proceed to payment >>".

Below the dialog box, a Notepad window titled "HELP_DECRYPT.TXT - Notepad" is open. It contains the following text: "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 found here: [redacted] what does this mean ? This means that the structure and data within your files have been changed. It is the same thing as losing them forever, but with our help, you can get them back. How did this happen ? Especially for you, on our server was generated the secret key pair. All your files were encrypted with the public key, which has been destroyed. Decrypting of your files is only possible with the help of the private key. what do I do ? Alas, if you do not take the necessary measures for the specified time, your files will be lost forever. If you really value your data, then we suggest you do not waste time. For more specific instructions, please visit your personal home page, there are a few different addresses: 1. http://paytoc4gtpn5czl2.torconnectpaycom/[redacted] 2. http://paytoc4gtpn5czl2.torwalltipaycom/[redacted] 3. http://paytoc4gtpn5czl2.walterwhitepaycom/[redacted] 4. http://paytoc4gtpn5czl2.rossulbrichtpaycom/[redacted] If for some reasons the addresses are not available, follow these steps: [redacted]".

2SPYWAR

<https://www.2-spyware.com/remove-cryptowall-virus.html>

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



CryptoWall

Table 1

Estimation of earnings based on C&C server data

	Compromised computers	Paid up	Percentage	Ransom	Total
Day	5,700	168	2.90%	200	33,600
Month (estimated)	68,000	1972	2.90%	200	394,400

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