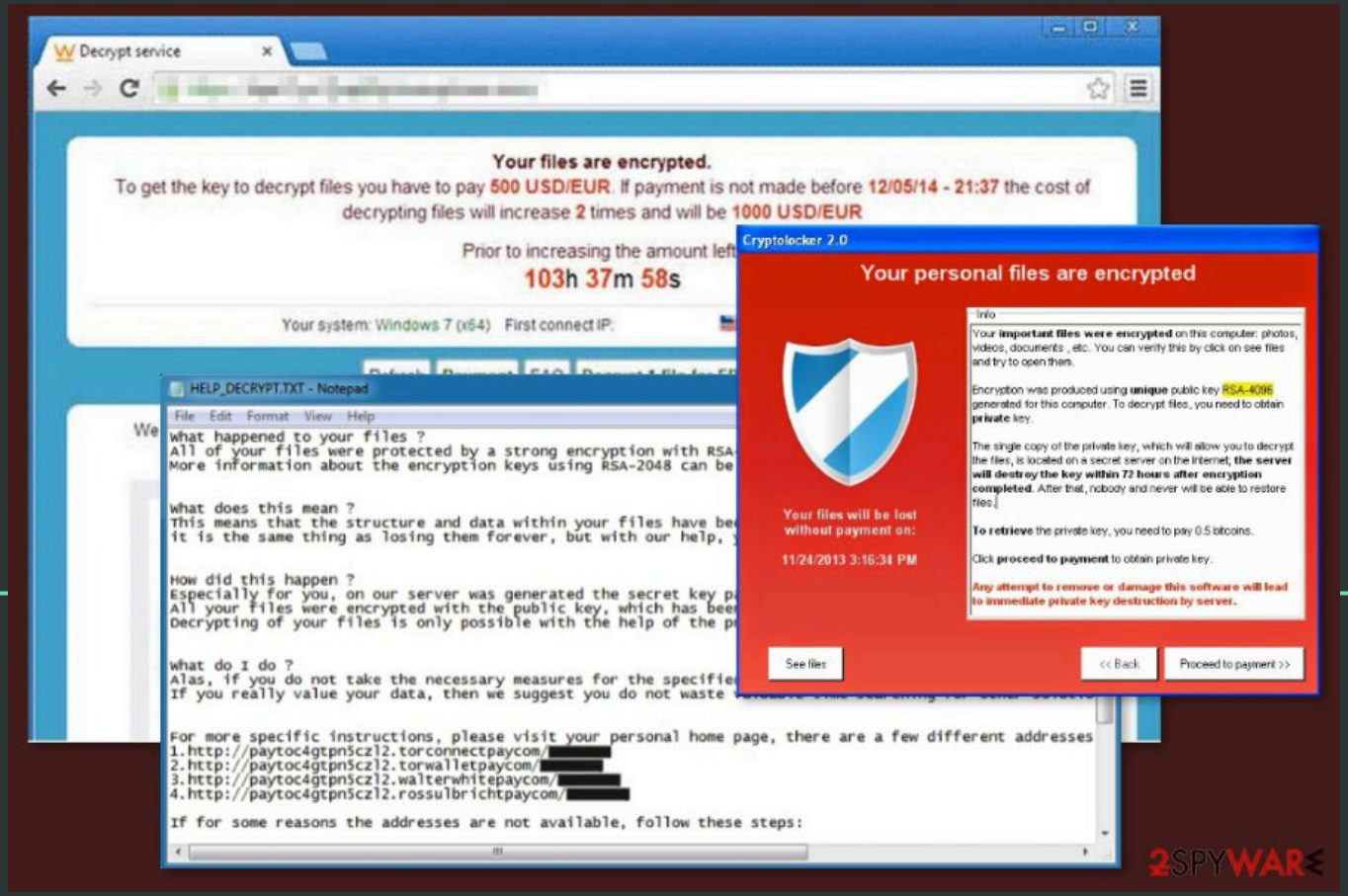
UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware

Paul Weliczko

https://arstechnica.com/information-technology/2012/11/mushrooming-growth-of-ransomware-extorts-5-million-a-year/



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**

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