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

Amin Kharraz, Sajjad Arshad, Collin Muliner, William Robertson, Engin Kirda

Northeastern University, Boston, USA

Abstract. Although the concept of ransomware is not new (i.e., such attacks date back at least as far as the 1980s), this type of malware has recently experienced a resurgence in popularity. In fact, in the last few years, a number of high-profile ransomware attacks were reported, such as the large-scale attack against Sony that prompted the company to delay the release of the film The Interview. Ransomware typically operates by locking the desktop of the victim to render the system inaccessible to the user, or by encrypting, overwriting, or deleting the users files. However, while many generic malware detection systems have been proposed, none of these systems have attempted to specifically address the ransomware detection problem. In this paper, we present a novel dynamic analysis system called UNVEIL that is specifically designed to detect ransomware. The key insight of the analysis is that in order to mount a successful attack, ransomware must tamper with a users files or desktop. UNVEIL automatically generates an artificial user environment, and detects when ransomware interacts with user data. In parallel, the approach tracks changes to the systems desktop that indicate ransomware-like behavior. Our evaluation shows that UNVEIL significantly improves the state of the art, and is able to identify previously unknown evasive ransomware that was not detected by the anti-malware industry[1].

Reference

[1] Amin Kharraz, Sajjad Arshad, Collin Mulliner, William Robertson, Engin Kirda, UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware, USENIX 2016. Austin, Texas, August 2016.

RSAConference Security Scholar

A Large-Scale, Automated Approach to Detecting Ransomware

Amin Kharraz
Northeastern University

Problem Statement and Goals

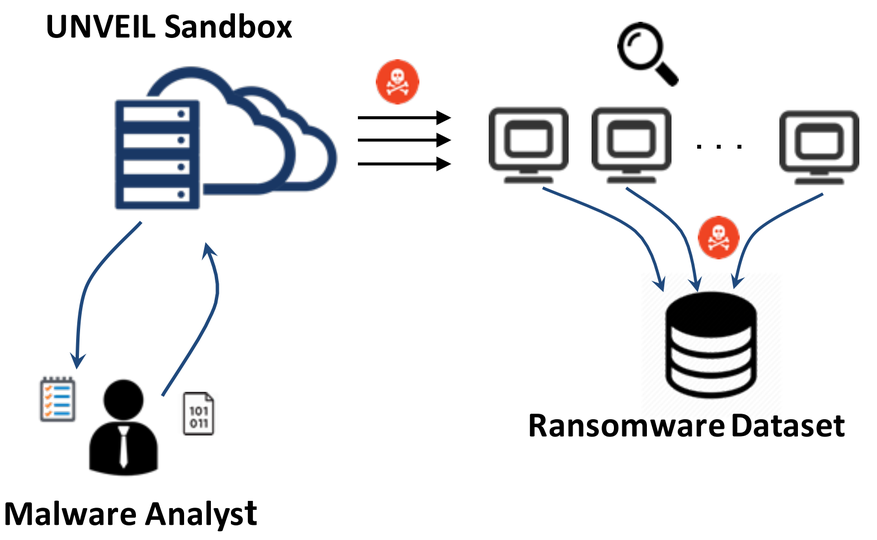

Figure 1. UNVEIL Deployment Scenario

- We designed a dynamic analysis system, called UNVEIL, specifically designed to detect ransomware.
- UNVEIL automatically creates an artificial, realistic execution environment and monitors how ransomware interacts with that environment.
- UNVEIL can detect cryptographic as well as desktop locking ransomware.
- UNVEIL can be easily deployed on any malware analysis system by simply attaching to the filesystem driver in the analysis environment.

Approach

- We implemented UNVEIL on top of Cuckoo Sandbox.
- UNVEIL is implemented through Windows kernel drivers that provide monitoring capabilities for the filesystem.
- UNVEIL monitors how ransomware sample attacks user data by logging the I/O access sequences.
- UNVEIL creates fake environment to make the analysis environment more realistic
- UNVEIL detects desktop locker ransomware by calculating structural dissimilarity before and after each run.

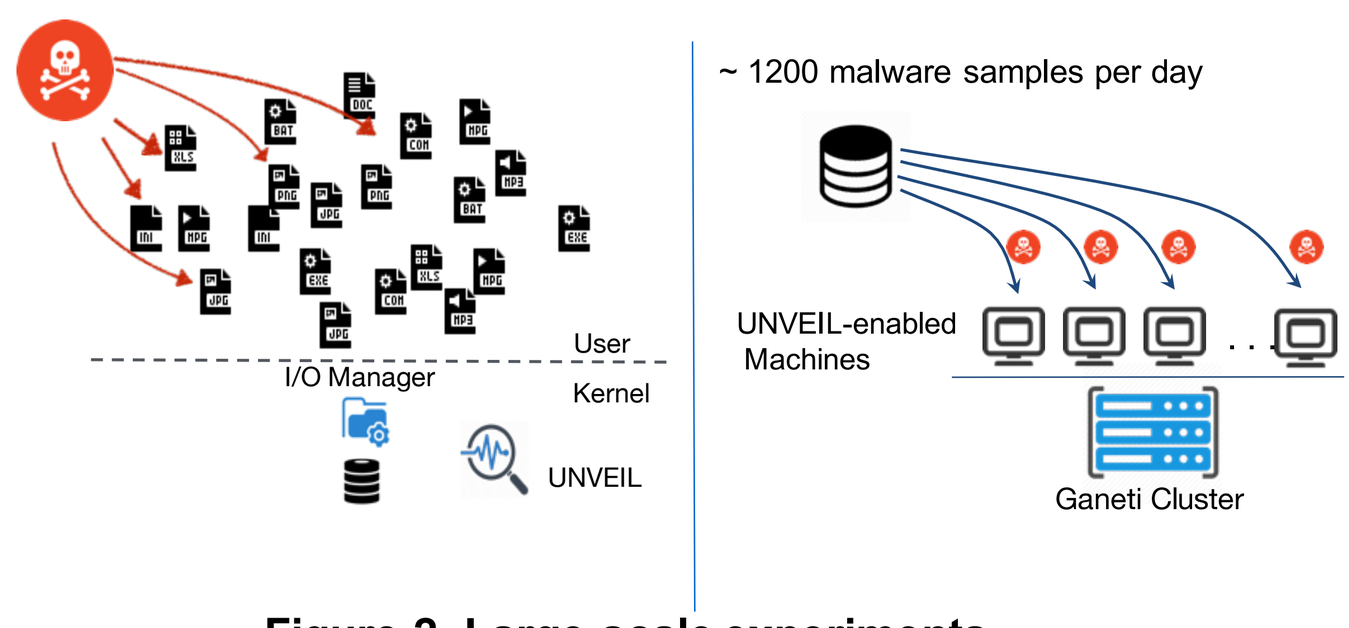

Figure 2. Large-scale experiments

Results

- The dataset contained 148,223 distinct samples.
- Achieving a TP rate 96.3% at zero FPs.
- We submitted each sample to Virus Total 6 times to monitor how the detection results change over time.
- 72% of the ransomware samples were not detected by AV scanners in the first submission.
- We also identified a new ransomware family, called SilentCrypt. An anti-malware company confirmed our finding.
- The evaluation shows that UNVEIL outperformed all existing AV scanners in detecting both superficial and technically sophisticated ransomware families.