2016 IEEE 36th International Conference on Distributed Computing Systems

CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data

Nolen Scaife
University of Florida
scaife@ufl.edu

Henry Carter
Villanova University
henry.carter@villanova.edu

Patrick Traynor
University of Florida
traynor@cise.ufl.edu

Kevin R.B. Butler
University of Florida
butler@ufl.edu

***Abstract*—Ransomware is a growing threat that encrypts a user's files and holds the decryption key until a ransom is paid by the victim. This type of malware is responsible for tens of millions of dollars in extortion annually. Worse still, developing new variants is trivial, facilitating the evasion of many antivirus and intrusion detection systems. In this work, we present CryptoDrop, an early-warning detection system that alerts a user during suspicious file activity. Using a set of behavior indicators, CryptoDrop can halt a process that appears to be tampering with a large amount of the user's data. Furthermore, by combining a set of indicators common to ransomware, the system can be parameterized for rapid detection with low false positives. Our experimental analysis of CryptoDrop stops ransomware from executing with a median loss of only 10 files (out of nearly 5,100 available files). Our results show that careful analysis of ransomware behavior can produce an effective detection system that significantly mitigates the amount of victim data loss.**

I. Introduction

Encrypting ransomware (a.k.a. crypto ransomware) attempts to extort users by holding their files hostage. Such ransomware differs from other types of malware in that its effects are reversible only via the cryptographic keys held by a remote adversary. Users can only regain access to their files through the use of anonymous payment mechanisms (e.g., Bitcoin), further frustrating efforts to take down these campaigns. While this class of malware has existed for well over a decade, its increasingly widespread use now causes tens of millions of dollars in consumer losses annually [37]. Compounding this problem, an increasing number of law enforcement agencies have also been the victim of ransomware [4], [18], losing valuable case files and forcing these organizations to ignore their own advice and pay the attackers. As such, ransomware represents one of the most visible threats to all users.

Combating ransomware is difficult for a number of reasons. First, this malware is easy to obtain or create [48] and elicits immediate returns, creating lucrative opportunities for attackers. Second, the operations performed by such malware are often difficult to distinguish from those of benign software. Finally, ransomware often intentionally targets unsophisticated users who are unlikely to follow best practices such as regular data backups. Accordingly, a solution to automatically protect such users even in the face of previously unknown samples is critical.

In this paper, we make the following contributions:

- **Develop an early-warning system for ransomware:** CryptoDrop is fundamentally different from existing methods of detecting ransomware, which inspect programs and their activity for malicious characteristics. Our system is the first ransomware detection system that monitors user data for changes that may indicate transformation rather than attempting to identify ransomware by inspecting its execution (e.g., API call monitoring) or contents. This allows CryptoDrop to detect suspicious activity regardless of the delivery mechanism or previous benign activity. Our system does not attempt to prevent all files from loss and is not intended to replace a user's normal anti-malware software; rather, CryptoDrop is designed to be effective *even when the user's anti-malware software has failed to block the malware*. Our system is built on Windows, a platform frequently targeted for ransomware attacks, providing a realistic solution to "in-the-wild" threats. In doing so, we attack the core behavior of ransomware in a novel and practical manner that other anti-malware technologies fundamentally cannot.
- **Identify three primary indicators suited to detect malicious file changes:** These indicators each measure an aspect of a file's transformation, and when all three have manifested, a ransomware file transformation has likely occurred. This union indication assists CryptoDrop in reliably detecting ransomware while incurring few false positives. These indicators have not been previously employed in a ransomware detection system, and our analysis of their effectiveness in isolation and unison provides insight into the ability to detect ransomware.
- **Perform most extensive analysis of encrypting ransomware to date:** Demonstrate a 100% true positive rate over 492 distinct ransomware samples across 14 families after as few as 0 and a median of 10 (0.2%) files lost from our test corpus. Finally, we discuss the observed behavior of our samples and discuss how CryptoDrop remains robust despite the significant behavioral differences between families. Through reduction of the number of files lost, we demonstrate that CryptoDrop reduces the need for the victim to pay the ransom, choking attackers' revenue and rendering the malware ineffective.

The remainder of the paper is structured as follows: In Section II, we perform a literature analysis. In Section III, we define and classify ransomware behaviors, our system's indicators, and demonstrate how these are insufficient for fast detection in isolation. Section IV details CryptoDrop's implementation and its scoring and detection mechanisms. In Section V, we obtain live ransomware samples, demonstrate CryptoDrop's effectiveness against real-world attacks, and analyze the behavior of the samples. We conclude in Section VI.

1063-6927/16 $31.00 © 2016 IEEE
DOI 10.1109/ICDCS.2016.46