A Context-Aware Trigger Mechanism for Ransomware Forensics

Avinash Singh, Adeyemi Ikuesan and Hein Venter
University of Pretoria, South Africa
asingh@cs.up.ac.za
aikuesan@cs.up.ac.za
hventer@cs.up.ac.za

Abstract: Given the prevailing spate of ransomware-based cyber-attacks, security researchers, particularly digital forensic researchers, are faced with the development of mitigation strategies towards the prevention of ransomware exploits. The generic Anti-virus approach to ransomware detection and prevention utilizes signature-based detection methods as opposed to behaviour-based detection methods. Signature-based detection methods often induce high error rates due to the adaptive techniques employed by exploits as well as the limitations of detecting novel patterns. Similarly, existing methods of recovery without ransom payment involves the identification of loopholes or flaws within the ransomware itself which is ineffective. This inefficiency can be attributed to the inherent weakness to address the time-sensitivity, complexity and the relative dynamic characteristics of mechanisms used in ransomware exploits. As a step towards identifying the emergence of ransomware attacks, and consequently prevent/recover from a ransomware attack, this study developed and evaluated a context-aware ransomware mitigation mechanism. The mechanism integrates diverse ransomware triggers through which ransomware instantiation can be identified. The elicitation method used in the trigger include entropy change, registry analysis, application programming interface activity, and the loading of dynamic link libraries. Using a series of experimental processes, the proposed mechanism was evaluated, and a higher detection rate was obtained. The result supports the underlying theoretical assumption of the study, which further provides a fundamental source for the development of a robust method of ransomware prevention. Furthermore, the result from this study can be integrated into a digital forensic readiness process for ransomware investigation. Such a process can be developed for pre-incident data acquisition and ransomware post-incident recovery.

Keywords: ransomware investigation, ransomware exploit identification, ransomware identification methods, entropy analysis, context-aware

1. Introduction

Malicious software (malware) constitutes one major research challenge to security and digital forensic researchers, as well as practitioners, with diverse variants. With over three decades of existence (Savage et al. 2011) and yearly exponential growth, malware poses a continuous existential nightmare to researchers and practitioners alike. (Abraham & Chengalur-Smith 2010). A variant of malware, known as ransomware, can spread rapidly over a network thus rendering the system inaccessible and the end-user helpless. Ransomware uses strong encryption to encrypt files on a system whilst withholding the decryption keys of these files for a ransom. Such ransom is usually demanded in untraceable currency, cryptocurrency being the most prevalent, for example, Bitcoin. The occurrence of ransomware is commonly found in the Windows Operating System (OS) due to the exploitation of unpatched vulnerabilities and a large user base (Vaughan-Nichols 2017). From the recently reported events (Cabaj et al. 2016), this trend is gradually seeing a drift towards Android devices, particularly mobile cellular phones. This drift is further elicited by the ubiquitous nature, sensitive contents and the attached-importance of Mobile devices which compels an individual to urgently pay such ransom.

Till date, anti-virus software and malicious detection tools have proven to be ineffective to detect new variants of ransomware (Jung & Won 2018). This has been attributed to the limitation of signature-based detection as well as the mitigation techniques employed by sophisticated ransomware (Tailor & Patel 2017). The need for a better detection mechanism thus forms the basis of this study, which attempts to use a context-aware approach whilst utilizing the underlying commonalities of ransomware to improve the detection rate. This mechanism integrates system event triggers such as entropy change, to evaluate the probability of ransomware (Cabaj et al. 2016). Entropy change is a standard feature used by encryption that uses the randomness generated by the OS before to perform encryption (Wojnowicz et al. 2017). This method detects the change and depending on the algorithm employed there is a level of certainty that can accurately identify when a file has been encrypted. This mechanism can, therefore, be applied to actively detect ransomware and provide the necessary information and data repository for further ransomware investigation. The next section discusses the background to the traditional anti-virus and malware detection approaches.