CADS: CRYPTOJACKING ATTACK DETECTION SYSTEM FOR CLOUD INFRASTRUCTURE

R.J.M. KESHANI G. JAYASINGHE

A dissertation submitted in partial fulfilment of the requirement for bachelor of engineering (hons) degree in software engineering

Department of Computing

Informatics Institute of Technology, Sri Lanka in collaboration with University of Westminster, UK

2020

Abstract

Cryptomining is the deed of using an individual's or an organization's computational power in order to mine cryptocurrency. Doing so without the explicit consent of the computer owners is called cryptojacking, and is considered illegitimate. During previous years, attackers' focus was heavily laid on browser-based cryptojacking. However, it was noted that the attackers are now shifting their attention to more robust, more superior targets, such as cloud servers and cloud infrastructure. Poorly configured servers and outdated security groundwork has increased mining activities in the cloud.

Existing systems' detection techniques rely heavily on evasive or exploitable metrics such as the solitary usage of CPU performance or Hardware Performance Counters. A range of evasion techniques are used by attackers to evade such systems: code obfuscation, dead-code injection, proxies and URL randomization, CPU throttling and artificial Hardware Performance Counter manipulation.

The proposed system provides a novel detection classifier which can identify cryptojacking attacks in a cloud environment at runtime with near real-time performance. The system will utilize a range of performance variables, dynamically selected to guarantee the metrics has the highest correlation with the attack status. This will ensure the accurate classification of the attack status even within servers with secure high performing applications, workload spikes and stealthily configured miners with low CPU usage.

Keywords: Security and Privacy, Malware Mitigations, Cryptojacking, Cloud Security, Performance Analysis, Machine Learning, Classification