GIGARAND: OPEN SOURCE TRIBRID RANSOMWARE DETECTION SYSTEM

Chamupathi Gigara Hettige

A dissertation submitted in partial fulfilment of the requirement for Bachelor of Engineering (Honours) degree in Software Engineering

Department of Computing

Informatics Institute of Technology, Sri Lanka

in collaboration with

University of Westminster, UK

2021

Abstract

Ransomware is one of the most spreading and dangerous kinds of computer malware these days. Attackers are using faster algorithms that have the capability to encrypt files in few seconds. A cryptographic based ransomware attack cannot be decrypted without the encryption key. Attackers are using social engineering techniques to deliver and execute ransomware files on computers. In 2016, 200,000 computers worldwide were got attacked by ransomware called WnnaCry. Large organizations and many numbers of hospitals were lost their data at that time. Operating systems default firewalls and anti-malware tools are not capable of identifying these attacks in real-time.

In this research, the author has proposed an open-source solution to detect ransomware attacks using machine learning. An Artificial Neural Network was built to identify attack by analysing system activities. The system provides a faster detection method to identify attacks. GigaRanD system is working with all the Windows 10 64-bit operating system versions. The system is faster than currently available commercial ransomware detection software also. The GigaRanD system is benchmarked with worlds top rated anti-malware tools such as Kaspersky and ESET. The tool was 4 times faster than the existing systems available. Since the system is an open-source project, future researchers and developers can contribute to the system to improve accuracy and performance.

Keywords—ransomware, cybersecurity, machine learning, Systems security