INFORMATICS INSTITUTE OF TECHNOLOGY

In collaboration with

UNIVERSITY OF WESTMINSTER

A Conceptual Framework to Detect Scheduled Malware Attacks by Analyzing Payload using Reverse Engineering

A dissertation by

B.K.P. Buddhima

Supervised by

Mr. Geethapriya Liyanage

Submitted in partial fulfilment of the requirements for the MSc in Cyber Security and degree at the University of Westminster.

Abstract

Malware attacks can be identified as common threat in cybersecurity which execute actions on a system or on a network without the permission of the user. Most of the existing malware detecting techniques have been relied on the behavior of the malware or on the signature of the malware. The scheduled malware attacks are difficult to be detected since the user is getting to know about the attack after it get executed. Occurring at a specific time, not showing any behavioral changes to be noticed are some other reasons, why it is challenging to detect scheduled malware attacks.

To address the above-mentioned problem, this research is bringing out a conceptual framework as a solution which use reverse engineering to analyze the payload and detect scheduled malware attacks. First the payload data will be retrieved and then it will be analyzed by using reverse engineering technique - disassembling to get the disassembled code. Malware signature will be extracted and it will get compared with the already known malware signatures to be get identified. Characteristics and behavior of the malware will be noticed to identify the malware. Here the reverse engineering technique – monitoring will be used. Then the scheduling mechanism will be detected by analyzing the time-based triggers. Registry keys, and startup entries also will be considered. This research has several benefits than the existing solution, such as identifying scheduled attacks by analyzing the payload directly is giving more accuracy on detecting attacks which may be missed by the other techniques. Therefore, this conceptual framework for detecting scheduled malware attacks by analyzing payload using reverse engineering is representing as a promising approach to addressed problem and can be used to improve the computer system security and network security.

Keywords: Malware, Scheduled Malware Attacks, Payload Analysis, Reverse Engineering

Subject Descriptors: Reverse Engineering, Malware Detection, Scheduled Malware Attacks