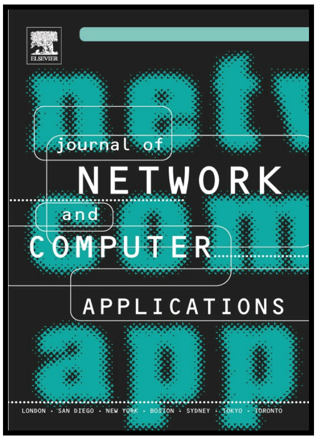
Countering Cyber Threats for Industrial Applications: An Automated Approach for Malware Evasion Detection and Analysis

Muzzamil Noor, Haider Abbas, Waleed Bin Shahid


ELSEVIER
journal of
NETWORK
and
COMPUTER
APPLICATIONS
LONDON • SAN DIEGO • NEW YORK • BOSTON • SYDNEY • TOKYO • TORONTO

www.elsevier.com/locate/jnca

PII: S1084-8045(17)30316-8
DOI: https://doi.org/10.1016/j.jnca.2017.10.004
Reference: YJNCA1984

To appear in: *Journal of Network and Computer Applications*

Received date: 6 February 2017
Revised date: 29 August 2017
Accepted date: 3 October 2017

Cite this article as: Muzzamil Noor, Haider Abbas and Waleed Bin Shahid, Countering Cyber Threats for Industrial Applications: An Automated Approach for Malware Evasion Detection and Analysis, *Journal of Network and Computer Applications,* https://doi.org/10.1016/j.jnca.2017.10.004

Countering Cyber Threats for Industrial Applications: An Automated Approach for Malware Evasion Detection and Analysis

Muzzamil Noor, Haider Abbas, Waleed Bin Shahid
National University of Sciences and Technology (NUST), Islamabad, Pakistan

Muzzamil.is-10@mcs.edu.pk

haiderabbas-mcs@nust.edu.pk

Waleed.shahid@mcs.edu.pk

ABSTRACT

The widespread adoption of IoT in industrial systems has made malware propagation more voluminous and sophisticated. Detection and prevention against these malware threats rely on automated dynamic analysis techniques. Malware writers on the other hand, are resorting towards analysis evasion techniques that pose a great deal of challenge for the malware research community. Various approaches mostly based on virtual machines or emulators have been proposed for the analysis of such envisions. However, the practicality of these approaches is still an open debate. This paper presents a malware analysis system, capable of encountering known evasion methods of malware. A novel technique for detection of malware evasive behavior is presented, which is based on measuring the deviation from normal behavior of a program or malware. Evaluations and analysis shows that this approach is effective against detecting the variations in malware behavior. Moreover, countermeasures implemented by the Analysis Evasion Malware Sandbox (AEMS) are effective for large percentage of malware detection.

Keywords
Malware, Dormant Functionality, Malware Evasion Detection, Analysis Evasion Malware Sandbox, AEMS, Malware Attribute Enumeration

Introduction

The ubiquitous nature of internet has paved the way for cyber security threats. Malwares are malicious software or applications that cause infection in the system with a malicious intent, like stealing confidential information, harming, disrupting or sabotaging harming and disrupting the system without user's consent. Malwares can be classified into rootkits, trojans, viruses, worms, backdoors, spyware and adware. This classification is based on their mode of proliferation, their functionality, and intent and attack pattern. Malwares have seen rapid surge in recent years as thousands of new malware samples are reported from all over the world every day. In 2014, AV-Test reported 390,000 new malware samples per day [1].