Accepted Manuscript

CloudIntell: An intelligent malware detection system

Qublai K. Ali Mirza, Irfan Awan, Muhammad Younas

PII: S0167-739X(17)31492-9
DOI: http://dx.doi.org/10.1016/j.future.2017.07.016
Reference: FUTURE 3546

To appear in: *Future Generation Computer Systems*

Received date : 16 January 2017
Revised date : 31 May 2017
Accepted date : 5 July 2017

Please cite this article as: Q.K.A. Mirza, I. Awan, M. Younas, CloudIntell: An intelligent malware detection system, *Future Generation Computer Systems* (2017), http://dx.doi.org/10.1016/j.future.2017.07.016

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

CloudIntell: An Intelligent Malware Detection System

Qublai K. Ali Mirza[1], Irfan Awan

School of Electrical Engineering and Computer Science
University of Bradford, UK

Muhammad Younas

Computing and Communication Technologies
Oxford Brookes University, UK

Abstract

Enterprises and individual users heavily rely on the abilities of antiviruses and other security mechanisms. However, the methodologies used by such software are not enough to detect and prevent most of the malicious activities and also consume a huge amount of resources of the host machine for their regular operations. In this paper, we propose a combination of machine learning techniques applied on a rich set of features extracted from a large dataset of benign and malicious files through a bespoke feature extraction tool. We extracted a rich set of features from each file and applied support vector machine, decision tree, and boosting on decision tree to get the highest possible detection rate. We also introduce a cloud-based scalable architecture hosted on Amazon web services to cater the needs of detection methodology. We tested our methodology against different scenarios and generated high achieving results with lowest energy consumption of the host machine.

Keywords: Malware Analysis, Machine Learning, Cloud, Decision Tree, Boosting, SVM, Security

[1]q.k.alimirza@bradford.ac.uk(Corresponding Author)

Download English Version:

https://daneshyari.com/en/article/6873064

Download Persian Version:

https://daneshyari.com/article/6873064

Daneshyari.com