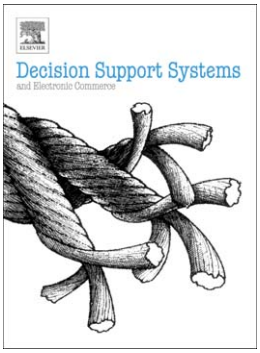

Detection of Online Phishing Email using Dynamic Evolving Neural Network Based on Reinforcement Learning

Sami Smadi, Nauman Aslam, Li Zhang

PII: S0167-9236(18)30001-0
DOI: doi:10.1016/j.dss.2018.01.001
Reference: DECSUP 12916

To appear in: *Decision Support Systems*

Received date: 12 April 2017
Revised date: 18 October 2017
Accepted date: 5 January 2018

Please cite this article as: Sami Smadi, Nauman Aslam, Li Zhang, Detection of Online Phishing Email using Dynamic Evolving Neural Network Based on Reinforcement Learning, *Decision Support Systems* (2018), doi:10.1016/j.dss.2018.01.001

Detection of Online Phishing Email using Dynamic Evolving Neural Network Based on Reinforcement Learning

Sami Smadi, Nauman Aslam and Li Zhang[1]

Department of Computer and Information Science, Northumbria University, UK
{sami.smadi, nauman.aslam, li.zhang}@northumbria.ac.uk

Abstract

Despite state-of-the-art solutions to detect phishing attacks, there is still a lack of accuracy for the detection systems in the online mode which leading to loopholes in web-based transactions. In this research, a novel framework is proposed which combines a neural network with reinforcement learning to detect phishing attacks in the online mode for the first time. The proposed model has the ability to adapt itself to produce a new phishing email detection system that reflects changes in newly explored behaviours, which is accomplished by adopting the idea of reinforcement learning to enhance the system dynamically over time. The proposed model solve the problem of limited dataset by automatically add more emails to the offline dataset in the online mode. A novel algorithm is proposed to explore any new phishing behaviours in the new dataset. Through rigorous testing using the well-known data sets, we demonstrate that the proposed technique can handle zero-day phishing attacks with high performance levels achieving high accuracy, TPR, and TNR at 98.63%, 99.07%, and 98.19% respectively. In addition, it shows low FPR and FNR, at 1.81% and 0.93% respectively. Comparison with other similar techniques on the same dataset shows that the proposed model outperforms the existing methods.

Keywords: `Online Phishing Email Detection, Reinforcement Learning, Neural Network`

1. Introduction

Stealing a person's identity is one of the most popular cybercrime activities. According to the Federal Trade Commission in 2015 (Commission et al., 2016), identity theft was ranked second with 16% of all customer complaints. The most common way to steal an online consumer's personal identity is called phishing, which can be defined as a fraudulent attempt, usually made through