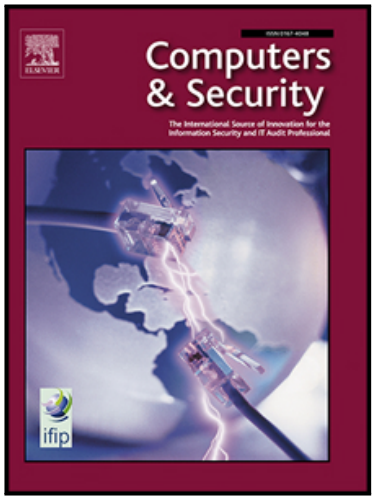
Journal Pre-proof




# A Novel Method for Malware Detection on ML-based Visualization Technique

Xinbo Liu, Yaping Lin, He Li, Jiliang Zhang

PII: S0167-4048(18)31462-7
DOI: https://doi.org/10.1016/j.cose.2019.101682
Reference: COSE 101682

To appear in: *Computers & Security*

Received date: 22 December 2018
Revised date: 11 October 2019
Accepted date: 26 November 2019

Please cite this article as: Xinbo Liu, Yaping Lin, He Li, Jiliang Zhang, A Novel Method for Malware Detection on ML-based Visualization Technique, *Computers & Security* (2019), doi: https://doi.org/10.1016/j.cose.2019.101682

# A Novel Method for Malware Detection on ML-based Visualization Technique

Xinbo Liu[a,b], Yaping Lin[a,b,*], He Li[a], Jiliang Zhang[a]

[a] *The College of Computer Science and Electronic Engineering, Hunan University, Changsha, China*
[b] *Hunan Provincial Key Laboratory of Trusted System and Networks in Hunan University, Changsha, China*

**Abstract**

Malware detection is one of the challenging tasks in network security. With the flourishment of network techniques and mobile devices, the threat from malwares has been of an increasing significance, such as metamorphic malwares, zero-day attack, and code obfuscation, *etc.* Many machine learning (ML)-based malware detection methods are proposed to address this problem. However, considering the attacks from adversarial examples (AEs) and exponential increase in the malware variant thriving nowadays, malware detection is still an active field of research. To overcome the current limitation, we proposed a novel method using data visualization and adversarial training on ML-based detectors to efficiently detect the different types of malwares and their variants. Experimental results on the MS BIG malware database and the Ember database demonstrate that the proposed method is able to prevent the zero-day attack and achieve up to 97.73% accuracy, along with 96.25% in average for all the malwares tested.

*Keywords:* *Malware Detection, Adversarial Training, Adversarial Examples, Image Texture, Data visualization*

*2018 MSC:* 00-01, 99-00

*Corresponding author:
*Email address:* yplin@hnu.edu.cn (Yaping Lin)