

Accepted Manuscript

Zero-day Malware Detection using Transferred Generative Adversarial Networks based on Deep Autoencoders

Jin-Young Kim , Seok-Jun Bu , Sung-Bae Cho

PII: S0020-0255(18)30347-5
DOI: [10.1016/j.ins.2018.04.092](https://doi.org/10.1016/j.ins.2018.04.092)
Reference: INS 13659



To appear in: *Information Sciences*

Received date: 22 September 2017
Revised date: 23 March 2018
Accepted date: 29 April 2018

Please cite this article as: Jin-Young Kim , Seok-Jun Bu , Sung-Bae Cho , Zero-day Malware Detection using Transferred Generative Adversarial Networks based on Deep Autoencoders, *Information Sciences* (2018), doi: [10.1016/j.ins.2018.04.092](https://doi.org/10.1016/j.ins.2018.04.092)

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.

Highlight:

- This paper proposes a transferred GAN based on a deep autoencoder for malware detection.
- It can detect zero-day attacks of malware by learning the fake malware generated.
- Experiments show that the proposed method increases the learning stability.
- It outperforms other state-of-the-art data mining techniques in malware detection.

ACCEPTED MANUSCRIPT

Download English Version:

<https://daneshyari.com/en/article/6856252>

Download Persian Version:

<https://daneshyari.com/article/6856252>

[Daneshyari.com](https://daneshyari.com)