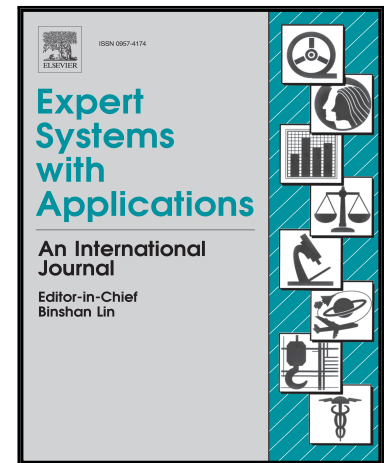


Accepted Manuscript

Quantifying the Resilience of Machine Learning Classifiers Used for Cyber Security

Ziv Katzir , Yuval Elovici

PII: S0957-4174(17)30659-0
DOI: [10.1016/j.eswa.2017.09.053](https://doi.org/10.1016/j.eswa.2017.09.053)
Reference: ESWA 11574



To appear in: *Expert Systems With Applications*

Received date: 24 June 2017
Revised date: 23 September 2017
Accepted date: 24 September 2017

Please cite this article as: Ziv Katzir , Yuval Elovici , Quantifying the Resilience of Machine Learning Classifiers Used for Cyber Security, *Expert Systems With Applications* (2017), doi: [10.1016/j.eswa.2017.09.053](https://doi.org/10.1016/j.eswa.2017.09.053)

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.

Highlights

- Quantifying machine learning classifiers' resilience to adversarial manipulations.
- Formal model for evaluating attacker's budget and the feature manipulation cost.
- Present two adversary aware feature selection using budget and manipulation cost.
- Demonstrate our approach using real life malware and benign executable analysis.

Download English Version:

<https://daneshyari.com/en/article/4943024>

Download Persian Version:

<https://daneshyari.com/article/4943024>

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