

Accepted Manuscript

Multiple Instance Learning for Malware Classification

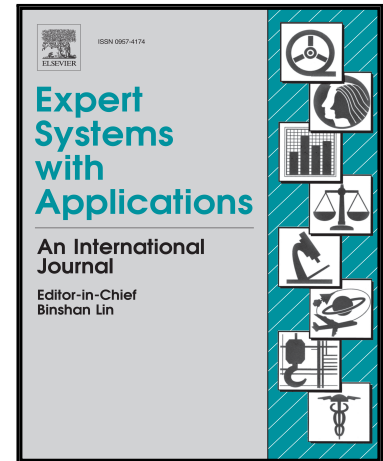
Jan Stiborek, Tomáš Pevný, Martin Rehák

PII: S0957-4174(17)30717-0
DOI: [10.1016/j.eswa.2017.10.036](https://doi.org/10.1016/j.eswa.2017.10.036)
Reference: ESWA 11619

To appear in: *Expert Systems With Applications*

Received date: 15 June 2017
Revised date: 13 October 2017
Accepted date: 14 October 2017

Please cite this article as: Jan Stiborek, Tomáš Pevný, Martin Rehák, Multiple Instance Learning for Malware Classification, *Expert Systems With Applications* (2017), doi: [10.1016/j.eswa.2017.10.036](https://doi.org/10.1016/j.eswa.2017.10.036)



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

- System resources can be used for modeling malware's behavior.
- Novel similarity measure for file paths reflecting directory structure is defined.
- The variability in the number of system resources can be addressed with MIL.

ACCEPTED MANUSCRIPT

Download English Version:

<https://daneshyari.com/en/article/6855402>

Download Persian Version:

<https://daneshyari.com/article/6855402>

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