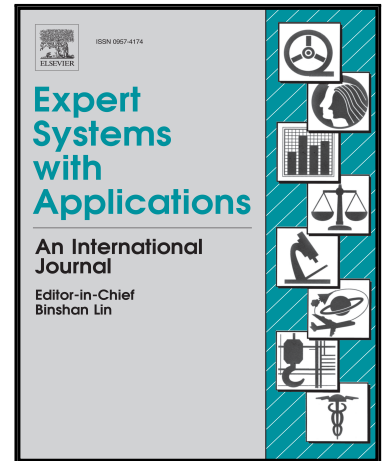


## Accepted Manuscript

Trusted Detection of Ransomware in a Private Cloud Using Machine Learning Methods Leveraging Meta-Features from Volatile Memory

Aviad Cohen , Nir Nissim

PII: S0957-4174(18)30128-3  
DOI: [10.1016/j.eswa.2018.02.039](https://doi.org/10.1016/j.eswa.2018.02.039)  
Reference: ESWA 11843



To appear in: *Expert Systems With Applications*

Received date: 24 October 2017  
Revised date: 26 February 2018  
Accepted date: 27 February 2018

Please cite this article as: Aviad Cohen , Nir Nissim , Trusted Detection of Ransomware in a Private Cloud Using Machine Learning Methods Leveraging Meta-Features from Volatile Memory , *Expert Systems With Applications* (2018), doi: [10.1016/j.eswa.2018.02.039](https://doi.org/10.1016/j.eswa.2018.02.039)

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:**

- A solution for trusted detection of unknown ransomware in VMs is proposed.
- Valuable data is extracted from the VM's memory dump using the *Volatility framework*.
- General descriptive features are proposed and successfully leveraged by ML algorithms.
- The solution was rigorously evaluated using notorious and professional ransomwares.
- The *Random Forest* classifier successfully detected known and unknown ransomware.

ACCEPTED MANUSCRIPT

Download English Version:

<https://daneshyari.com/en/article/6855066>

Download Persian Version:

<https://daneshyari.com/article/6855066>

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