Accepted Manuscript

Advanced Payload Analyzer Preprocessor

Luis Javier García Villalba, Ana Lucila Sandoval Orozco, Jorge Maestre Vidal

PII: S0167-739X(16)30478-2

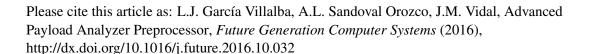
DOI: http://dx.doi.org/10.1016/j.future.2016.10.032

Reference: FUTURE 3204

To appear in: Future Generation Computer Systems

Received date: 18 July 2015

Revised date: 26 November 2015 Accepted date: 27 October 2016



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.



ACCEPTED MANUSCRIPT

Highlights

- A novel network-based intrusion detection system for recognition of unknown threats (zero-day attacks) is proposed.
- Detailed statistical analysis of the binary contents of payloads is applied.
- The information processing involves the use of n-gram and Bloom filter structures.
- Results obtained by analyzing real HTTP traffic prove high hit rate (approx. 95%) and low false positive rate (approx. 0.1%).

Download English Version:

https://daneshyari.com/en/article/4950337

Download Persian Version:

https://daneshyari.com/article/4950337

<u>Daneshyari.com</u>