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

Please cite this article as: L.J. García Villalba, A.L. Sandoval Orozco, J.M. Vidal, Advanced Payload Analyzer Preprocessor, *Future Generation Computer Systems* (2016), http://dx.doi.org/10.1016/j.future.2016.10.032

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%).