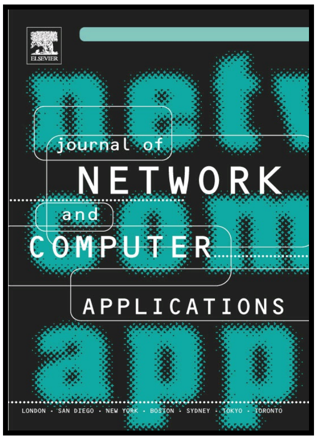
Alert Correlation Framework for Malware Detection by Anomaly-based Packet Payload Analysis

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


journal of
NETWORK
and
COMPUTER
APPLICATIONS
LONDON • SAN DIEGO • NEW YORK • BOSTON • SYDNEY • TOKYO • TORONTO

www.elsevier.com/locate/jnca

PII: S1084-8045(17)30274-6
DOI: http://dx.doi.org/10.1016/j.jnca.2017.08.010
Reference: YJNCA1956

To appear in: *Journal of Network and Computer Applications*

Received date: 14 January 2016
Revised date: 21 February 2017
Accepted date: 22 August 2017

Alert Correlation Framework for Malware Detection by Anomaly-based Packet Payload Analysis

Jorge Maestre Vidal[a,*], Ana Lucila Sandoval Orozco[a], Luis Javier García Villalba[a]

[a] *Group of Analysis, Security and Systems (GASS), Department of Software Engineering and Artificial Intelligence (DISIA), School of Computer Science, Office 431, Universidad Complutense de Madrid (UCM), Calle Profesor José García Santesmases s/n, Ciudad Universitaria, 28040 Madrid, Spain*

Abstract

Intrusion detection based on identifying anomalies typically emits a large amount of reports about the malicious activities monitored; hence information gathered is difficult to manage. In this paper, an alert correlation system capable of dealing with this problem is introduced. The work carried out has focused on the study of a particular family of sensors, namely those which analyze the payload of network traffic looking for malware. Unlike conventional approaches, the information provided by the network packet headers is not taken into account. Instead, the proposed strategy considers the payload of the monitored traffic and the characteristics of the models built during the training of such detectors, in this way supporting the general-purpose incident management tools. It aims to analyze, classify and prioritize alerts issued, based on two criteria: the risk of threats being genuine and their nature. Incidences are studied both in a one-to-one and in a group context. This implies the consideration of two different processing layers: The first one allows fast reactions and resilience against certain adversarial attacks, and on the other hand, the deeper layer facilitates the reconstruction of attack scenarios and provides an overview of potential threats. Experiments conducted by analyzing real traffic demonstrated the effectiveness of the proposal.

Keywords: Alert correlation, anomalies, Intrusion Detection System,

[*] Tel. +34 91 394 76 38, Fax: +34 91 394 75 47

Email addresses: jmaestre@ucm.es (Jorge Maestre Vidal), asandoval@fdi.ucm.es (Ana Lucila Sandoval Orozco), javiergv@fdi.ucm.es (Luis Javier García Villalba)