computer
communications

A hybrid layered architecture for detection and analysis of network based Zero-day attack

Saurabh Singh , Pradip Kumar Sharma , Seo Yeon Moon ,
Jong Hyuk Park

PII: S0140-3664(16)30549-7
DOI: 10.1016/j.comcom.2017.01.019
Reference: COMCOM 5456

To appear in: *Computer Communications*

Received date: 13 November 2016
Accepted date: 21 January 2017

Highlights

- The main objectives of a Zero-day attack are for hackers or attackers to be able steal sensitive information, legal documents, enterprises data, and other information. We have analyzed the lifecycle of Zero-day vulnerabilities and different detection methodologies.

- In this paper, we propose a novel hybrid layered architecture framework for Zero-day attack detection and analysis in real-time, which is based on statistics, signatures, and behavior techniques. To enhance our architecture, we used an SVM approach in order to provide unsupervised learning and minimize false alarm detection capabilities.

- In this research, we focus on integrating the anomaly detection and signature generation based methods. In a layered approach, layers are supposed to execute dedicated functionality in parallel. Parallel work of each layer improves the performance of our proposed approach. In this paper, we also present the different experimental comparisons we made between our approach and various standard parameters and our result shows a high detection rate of Zero-day attacks