World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:10, No:04, 2016

Malware Beaconing Detection by Mining Large-scale DNS Logs for Targeted Attack Identification

Authors : Andrii Shalaginov, Katrin Franke, Xiongwei Huang

Abstract : One of the leading problems in Cyber Security today is the emergence of targeted attacks conducted by adversaries with access to sophisticated tools. These attacks usually steal senior level employee system privileges, in order to gain unauthorized access to confidential knowledge and valuable intellectual property. Malware used for initial compromise of the systems are sophisticated and may target zero-day vulnerabilities. In this work we utilize common behaviour of malware called ”beacon”, which implies that infected hosts communicate to Command and Control servers at regular intervals that have relatively small time variations. By analysing such beacon activity through passive network monitoring, it is possible to detect potential malware infections. So, we focus on time gaps as indicators of possible C2 activity in targeted enterprise networks. We represent DNS log files as a graph, whose vertices are destination domains and edges are timestamps. Then by using four periodicity detection algorithms for each pair of internal-external communications, we check timestamp sequences to identify the beacon activities. Finally, based on the graph structure, we infer the existence of other infected hosts and malicious domains enrolled in the attack activities.

Keywords : malware detection, network security, targeted attack, computational intelligence
Conference Title : ICCISIS 2016 : International Conference on Computational Intelligence in Security Information Systems
Conference Location : Paris, France
Conference Dates : April 25-26, 2016