

COMPUTING DEVICE AND METHOD FOR DETECTING MALICIOUS DOMAIN NAMES IN A NETWORK TRAFFIC

ABSTRACT

5

A computing device for detecting malicious domain names in network traffic and a method for operating said computing device are proposed. The computing device includes a communication module, configured to receive network traffic from a data network. In addition, the computing device comprises a filtering module that can be connected to the communication
10 module to receive captured network traffic from it and can perform at least the following operations: extracting a set of data packets from the received network traffic and analyzing the specified extracted data packets to ensure the extraction of at least one domain name from them. The computing device also includes an analyzing module, connected to the filtering
15 module to receive the specified domain names from it and to analyze each of the obtained domain names, ensuring that a given numerical value is assigned to each of a given set of features of a domain name suspiciousness corresponding to one of a given set of analysis methods, for each analyzed domain name, depending on the results of its analysis using the specified analysis techniques. In addition, the computing device also includes a processing
20 module, configured to receive the indicated features of suspiciousness with assigned numerical values for each domain name and with the possibility of analyzing them using a specified set of analysis methods ensuring that each domain name is classified as malicious domain names, if the received results of the analysis of features of suspiciousness are characteristic of malicious domain names.

25 Fig. 2