

ABSTRACT

A technique relates to the field of information security. A computer-implementable method of detecting compromised network devices based on DNS tunneling, the method comprising receiving a traffic of a protected network infrastructure; extracting at least one DNS query from the traffic; filtering a list of DNS queries extracted and excluding from the list the queries to a predefined domain name types; feeding one-by-one each of a plurality of domain names remaining in the list as an input to a pre-trained decision rule; if at least one domain name obtains a negative assessment of the decision rule, increasing a penalty for at least one network device which sent at least one DNS query, containing this domain name; if the amount of penalties of at least one network device exceeds a preset threshold, this at least one network device is considered to be compromised, and a corresponding notification is displayed.

Fig. 1