

DETECTION OF INFECTED NETWORK DEVICES VIA ANALYSIS OF RESPONSELESS OUTGOING NETWORK TRAFFIC

ABSTRACT

The present disclosure describes one or more systems, methods, routines and/or techniques for detection of infected network devices via analysis of responseless outgoing network traffic. A computer implemented method may include executing a routine that receives as input first packet information. The method may include executing a routine that analyzes the first packet information to determine whether the first packet information identifies an outgoing network packet that is associated with the initiation of a network communication. The method may include executing a routine that causes storage and/or tracking, in one or more data stores, of the first packet information if the first packet information is determined to be a potential responseless packet. The method may include executing a routine that causes removal and/or ends tracking of the first packet information if the first packet information is determined to not be a responseless packet based on analysis of second packet information.

Figure 1