

ABSTRACT

A computer-implementable method comprising receiving an outbound infrastructure traffic, detecting at least one suspicious external IP address in the traffic, scanning a suspicious device located on the detected suspicious IP address, obtaining a list of services running on the suspicious device, sending the detected suspicious IP address and the list to an external computing device, comparing the list with data on known malicious services. In response to a coincidence of a service from the list with the data, considering the suspicious device to be malicious and generating a report on detection of malicious activity in the infrastructure. In response to absence of the coincidence, computing an interval of ownership of a suspicious IP address, and in response to the computed duration of the interval being less than a threshold value, considering the suspicious device to be malicious and generating a report on detection of malicious activity in the infrastructure.

FIG. 1