CLAIMS

1. A computer-implementable method of detecting compromised network devices based on DNS tunneling, the method comprising:

receiving traffic of a protected network infrastructure;

extracting at least one DNS query from the traffic;

filtering a list of extracted DNS queries by excluding from the list queries to predefined domain name types;

feeding one-by-one each of a plurality of domain names in the filtered 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 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 displaying a corresponding notification;

wherein the predetermined types of domain names include at least:

second level domain names,

low entropy domain names, and

knowingly trusted domain names from well-known reliable sources.

2. A computer-implementable method of detecting compromised network devices based on DNS tunneling, the method comprising:

receiving traffic of a protected network infrastructure;

extracting at least one DNS query from the traffic;

filtering a list of extracted DNS queries by excluding from the list queries to 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 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 displaying a corresponding notification;

searching for the at least one domain name obtained the negative assessment in the history of all inbound and outbound traffic from at least one network device of the protected infrastructure, and

in response to detection entries of the at least one domain name obtained the negative assessment:

either additionally penalizing every network device of the protected infrastructure which communicated with the given domain name,

or penalizing every network device which is not penalized before.

3. The method of claim 1 or 2, wherein receiving the traffic of the protected network infrastructure also comprises receiving an inbound network traffic of the protected network infrastructure.

4. The method of claim 1 or 2, wherein the traffic is received by a traffic mirroring method.

5. The method of claim 1 or 2, wherein for each DNS query extracted from the traffic at least following data are extracted: a domain name; a sender IP address and a recipient IP address.

6. The method of claim 5, further comprises checking whether at least one recipient IP address is in a blacklist and in a whitelist, and

in response to at least one recipient IP address is in the blacklist, increasing the penalty for at least one network device which sent at least one DNS query, containing this at least one recipient IP address;

in response to at least one recipient IP address is in the whitelist, skipping the DNS query.

7. The method of claim 1 or 2, wherein the pre-trained decision rule comprises at least one the following heuristic methods: dividing domains by entropy level, selecting n-grams in domain names.

8. The method of claim 1 or 2, wherein the pre-trained decision rule is a LSTM neural network.

9. The method of claim 8, wherein LSTM neural network is additionally fed with statistics of a network interactions of the network device which sent the DNS query, containing the given domain name, as well as the penalty of this network device,

wherein statistics of network interactions is collected during last T minutes.

10. The method of claim 1 or 2, wherein pre-trained decision rule is a combination of LSTM neural network and at least one of the following heuristic methods: dividing domains by entropy level, selecting n-grams in domain names.

11. The method of claim 1 or 2, further comprising:

blocking the domain name obtained the negative assessment for every network device included into the protected infrastructure,

generating notifications on maliciousness of the blocked domain name,

creating template emails for notifying interested parties about blocked domain name,

adding the blocked domain name to at least one blacklist.

12. A computing device for detecting compromised network devices based on DNS tunneling, the computing device is configured to perform the method of detecting compromised network devices based on DNS tunneling according to any of claims 1-11.