CLAIMS

1. A method of informing about malicious web resources running on a computing device, the method comprising:

obtaining references to a set of web resources;

identifying malicious web resources in the set of web resources;

establishing web resources that are associated with each of the identified malicious web resources;

identifying additional malicious web resources in the established associated web resources;

determining at least one authorized entity associated with each of the identified malicious web resources and the identified additional malicious web resources;

generating at least one report for at least one of the determined authorized entities based on the data on the identified malicious web resources and the identified additional malicious web resources associated with this authorized entity; and

sending each generated report to the determined authorized entity on the basis of contact details of the authorized entity.

2. The method of claim 1, wherein determining the at least one authorized entity associated with each of the identified malicious web resources and the identified additional malicious web resources comprises determining an owner, administrator, hosting provider and / or domain name registrar associated with the identified malicious web resource and the identified additional malicious web resources.

3. The method of claim 1, further comprising establishing a type of threat from a given set of types of threats for each of the identified malicious web resources and the identified additional malicious web resource; and

generating the at least one report comprises using a template from a specified set of report templates, each template corresponding to one of the given set of types of threats and one of the determined authorized entities.

4. The method of claim 3, wherein a number of reports generated for each authorized entity corresponds to a number of identified types of threats.

5. The method of any of claims 1-4, further comprising adding, to each report, evidence of maliciousness of the each web resource, information about which is comprised in this report.

6. The method of claim 1, wherein identifying the malicious web resources comprises establishing whether each obtained reference at least partially coincides with one of known malicious references.

7. The method of claim 6, wherein identifying the malicious web resources or the additional malicious web resources comprises carrying out at least one of the following operations:

- analyzing domain name of the web resource for harmfulness using at least one method for analyzing domain names;

- obtaining at least one file from a web resource and analyzing the at least one file for maliciousness using at least one method of analyzing files; and

- obtaining html-code of a web resource and analyzing the html-code for maliciousness using at least one method of analyzing html-code.

8. The method of claim 7, wherein analyzing the domain name of the web resource for maliciousness comprises establishing whether this analyzed domain name matches one of known malicious domain names.

9. The method of claim 7, wherein analyzing the at least one file received from the web resource for maliciousness comprises calculating a hash sum of the at least one file and determining whether the calculated hash sum of the analyzed file matches a hash sum of one of known malicious files.

10. The method of claim 7, wherein analyzing the obtained html-code of the web resource comprises conducting a search in the obtained html-code for specific keywords indicating a malicious nature of the web resource.

11. The method of claim 1, wherein establishing the associated web resources comprises determining at least one of the following:

- whether domain names of the web resources have a similar spelling;
- whether domain names are registered to a same person;
- whether same registrant personal data are specified for registered domain names of the web resources;
- whether domain names of the web resources are located at a same IP address; and
- whether references corresponding to the web resources have a same or similar uniform pointer of the web resource “URL”.

12. The method of claim 1, wherein establishing the associated web resources comprises performing at least the following operations:

- creating a mathematical model in the form of a graph, wherein vertices of the graph correspond to at least a first web resource and at least a second web resource, and graph edges are links between at least the first web resource and at least the second web resource at least under one web resource parameter, common for at least the first web resource and at least the second web resource, wherein a number of the links under the one web resource parameter between one first web resource and the second web resources is limited by a predetermined threshold value;

- assigning weights to the links between at least the first web resource and the second web resource by means of a known machine learning algorithm, based on a parameter of the first web resource and the second web resource;

- determining a link coefficient as a ratio of the number of the links under the one parameter of a web resource between one first web resource and the second web resources and the weight of each link for a single web resource parameter between the first web resource and the second web resources; and

- removing the links between at least the first web resource and at least the second web resource in case a value of a certain communication coefficient is less than a predetermined threshold value.

13. The method of claim 1, wherein obtaining the references to the set of web resources comprises performing at least one of the following operations:

- sending a request to at least one source of references to obtain from it at least one reference to a web resource;

- receiving messages from at least one computing device with a provision of their processing to retrieve at least one reference to a web resource;

- receiving messages from at least one mobile device with a provision of their processing to retrieve at least one reference to a web resource; and

- entering search queries in at least one search engine using a specific list of keywords to identify contextual advertising in search results received in response to each request in each of these search engines, ensuring an extraction of at least one reference to a web resource from the identified contextual advertising.

14. A computing device for informing about malicious web resources, comprising a memory for storing machine-readable instructions and at least one computing processor, configured to execute computer-readable instructions while ensuring implementation of the method for informing about malicious web resources according to any one of claims 1-13.