CLAIMS

1. A computer-implementable method for detection of a target malicious web resource comprising:

a preparatory stage, comprising:

- obtaining a reference to at least one known malicious input web resource;

- constructing at least one redirect chain for each of the malicious input web resources, using pre-formed user behavior vectors imitating user behavior and user parameters imitating user environment for constructing at least one redirect chain;

- combining the constructed redirect chains into at least one redirect graph; and

- analyzing the redirect graph, and identifying user redirect rules directing users to the target malicious web resources;

a working stage, comprising:

- obtaining a reference to at least one suspicious input web resource and user device parameters from a user device;

- constructing at least one redirect chain for each of the obtained suspicious input web resources;

- checking the constructed at least one redirect chain for compliance with at least one rule of user redirection to the target malicious web resources; and

- in response to the correspondence of at least one constructed redirect chain with at least one rule of user redirection to the target malicious web resources: identifying the target malicious web resource in at least one constructed chain; blocking the said target malicious web resource; and sending a notification to the user device.

2. The Method of claim 1, wherein the reference is at least the following: domain name, IP address, URL address.

3. The Method of claim 1, wherein the user behavior vectors comprise instructions for applications, wherein the instructions constitute the series and sequence of activities comprising at least the following activities: following the link, data entry, selection from suggested options.

4. The Method of claim 1, wherein the user parameters comprise at least the following: the user device IP address, the user geolocation data, redirection time, the user device information, operating system, operating system interface language, provider, browser, browser version, browser interface language, cookie files, system time and actual time in the user device system, url-referrer.

5. The Method of claim 1, further comprising collecting information about each web resource included in the detected redirect chains, wherein such information comprises at least the following:

- URL link referencing the said web resource,
- ID and other parameters within the URL link body;
- Detection time and date;
- The web resource geolocation data;
- Information about the provider associated with the web resource;
- ID / company/brand name used by the said web resource.

6. The Method of claim 1, further comprising considering all redirect chains to construct the redirect graph, wherein each chain comprises the following information: about the user behavior vector and the user parameters used in the said chain construction, about each web resource of contained in the said redirect chain and about the sequence of the said web resources.

7. The Method of claim 1, wherein the redirect graph constitutes a combination of nodes and arcs, wherein each of nodes corresponds to the detected web resource, and each of arcs corresponds to the redirection from one web resource to another.

8. The Method of claim 1, wherein when combining the plurality of the obtained redirect chains into at least one redirect graph, the web resources are considered affiliated if at least one of the following conditions is true:

• all constituent parts of the web resources URL addressees i.e., domain, page name and parameter names, match one another;

• length of domain name, length of top-level domain name, length of page names and parameter names match one another;

• IP addresses of the web resources match one another.

9. The Method of claim 1, wherein when combining the plurality of the obtained redirect chains into at least one redirect graph, affiliated web resources are considered to constitute one vertex.

10. The Method of claim 1, wherein when combining the plurality of the obtained redirect chains into at least one redirect graph in a multithreading mode, each vertex of each detected redirect chain is compared with the vertices of other detected redirect chains, and

- if the matching vertices are found that are present in more than one chain, these matching vertices are considered to constitute one graph vertex.

- if a vertex is found that is different from all other vertices, the said vertex is added to the graph as a new vertex; wherein if no arc exists in the graph connecting this new vertex with the previous one, such an arc is added.

11. The Method of claim 1, wherein the target malicious web resource is identified through additional checks of the web resource for malicious activities.

12. The Method of claim 1, wherein the target malicious web resource is identified by analyzing the HTTP response codes obtained by a browser.

13 The. Method of claim 1, wherein the redirect chain is rejected at the working stage if the redirect chain contains less than the pre-determined number of redirections.

14. The Method of claim 1, wherein the pre-formed user parameters corresponding to the user device parameters obtained from the user device are used at the working stage to construct at least one redirect chain.

15. The Method of claim 1, wherein the pre-formed user behavior vectors are used at the working stage to construct at least one redirect chain, wherein at least one redirect chain is constructed at the preparatory stage using the said pre-formed user behavior vectors.

16. The Method of claim 15, wherein the user behavior vectors are used at the working stage, wherein the said user behavior vectors are used at the preparatory stage for the construction of at least one redirect chain together with the user parameters corresponding to the user device parameters obtained from the user device.

17. The Method of claim 1, wherein all pre-formed user behavior vectors are used at the working stage to construct at least one redirect chain.

18. The Method of claim 1, wherein rules of redirection of the users to the target malicious web resources for each web resource, excluding the target malicious web resource, comprise the following:

- conditions of transition to the next web resource, depending on the user parameters;
- conditions of transition to the next web resource, depending on the user behavior vector;
- conditions of transition to the next web resource, depending both on the user parameters and the user behavior vector.

19. A computer-implementable method for detection of a target malicious web resource comprising:

- obtaining a reference to at least one suspicious input web resource and user device parameters from a user device;

- constructing at least one redirect chain for each of the obtained at least one suspicious input web resource;

- checking the constructed at least one redirect chain for compliance with at least one rule of user redirection to a target malicious web resource;

- in response to the correspondence of the at least one constructed redirect chain with the at least one rule of user redirection to the target malicious web resource, identifying the target malicious web resource in at least one constructed chain; blocking the target malicious web resource; and sending a notification to the user device.

20. A computing device for detection of a target malicious web device, configured to implement the method for detection of the target malicious web resource according to any of the claims 1-18.