

Method and computing device for detection of target malicious web resource

FIELD

[0001] This technical solution relates to a computer field, namely, to the field of information security, specifically, to a computer-implementable method and system of a target malicious web resource detection.

BACKGROUND

[0002] Presently, more than half of malicious actions is perpetrated on the Internet (e.g., malicious SW distribution, phishing etc.) Typically, when doing so the attackers compel their victims to go to malicious web resources (websites, webpages).

[0003] The existing systems of the malicious webpage identification are divided into two categories. The first category uses static analysis methods for analyzing the webpages and their codes (e.g., HTML, CSS, JavaScript or Flash); in the process, a search is being performed for the malicious activity templates.

[0004] Such approach is realized in the technology described in the US9,356,947B2 patent document (Opsec Online LTD). For instance, to identify a malicious website, a data set is used that is divided into several components that include data collected from a plurality of data sources: IP, domain, headers, text fields, that are assigned points based on the comparison with known templates.

[0005] On the other hand, such an approach has been reflected in the RU2668710C1 document (Group-IB TDS, LTD) where a web resource is analyzed based on the established suspiciousness attributes to detect malicious domain names.

[0006] The second category includes the dynamic types of analysis based on circumvention of the suspicious web resources using special instruments (e.g., ACOOC or client honeypot) that are used to monitor the web resources for signs of activity.

[0007] Thus, e.g., in the KR101190261B1 document (for studying of which a machine translation has been used) an approach is described wherein the web search engines load up the webpages with a suspicious content and analyze the negative website behavior and the loaded malicious SW state in the sandbox afterwards.

[0008] All the described approaches help protect the users from malicious web resources; however, they are characterized by a number of limitations to which at least the following can be ascribed: the malefactors bypass them by masking their target websites which is achieved by creating

the web resource chains successively readdressing the user; in some of them, the target resource can be reached only after passing through the whole chain.

[0009] On the other hand, the mentioned methods allow detecting only the malicious pages using the conventional, well known technical vulnerabilities, but do not protect users from the methods of social engineering.

[0010] Additionally, most of the dynamic methods of the malicious web resources detection involve using great volumes of resources.

[0011] The present technical solution provides for using the redirecting chain interceptors, to identify the templates therein that are commonly encountered when interacting with the malefactor pages.

[0012] It is worth noting that by using the redirections to several resources, the fraudsters are capable of separating the use of the known brands webpages and of the actual fraudulent page. This complicates the blocking processes since if the endpoint fraudulent resource contains fewer violations, fewer policies and rules can be applied to it that grant the responsible organization rights to block the resource. Also, the use of several web resources allows the malefactors to limit the organizations reacting to such attacks in their ability to visit the endpoint web resource, while giving the attackers the technical possibility to flexibly change any intermediate link within the chain without all the entry points renewal.

[0013] From the above prior art analysis, the need for developing methods for the exact target malicious web resources detection becomes obvious. Indeed, in the described scenario, when the redirect chains are used, it is the detection and blocking of the target malicious web resource that deprives the attackers the opportunity to practice the actual fraud; additionally, there is no need to spend time and efforts for blocking all (as a rule, quite numerous) intermediate web resources.

[0014] Consequently, the present technical solution has been created to overcome at least one of the above shortcomings related to the methods of the known target malicious web resources detection.

SUMMARY

[0015] The technical problem, for solving of which the claimed solution is intended, is the creation of a method and a system for the target malicious web resources detection.

[0016] The technical result consists in the increasing of the target malicious web resource detection accuracy.

[0017] The claimed result is achieved through the implementation of the target malicious web resource detection method comprising:

a preparatory step, at which:

a reference is obtained to at least one known malicious input web resource;

at least one redirect chain is constructed for each of the obtained malicious input web resources, wherein to construct at least one redirect chain, the pre-formed user behavior vectors (imitating the user behavior) and user parameters (imitating the user environment) are used;

the constructed redirect chains are combined into at least one redirect graph;

the redirect graph is analyzed, and the user redirect rules directing users to the target malicious web resources are identified.

the working stage, at which:

a reference to at least one suspicious input web resource and the user device parameters are obtained from a user device;

at least one redirect chain is constructed for each of the obtained suspicious input web resources;

at least one redirect chain that has been constructed is checked for correspondence with at least one rule of user redirection to the target malicious web resources;

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, the target malicious web resource is identified in at least one constructed chain and blocked; the respective notification is sent to the user device.

[0018] In a particular embodiment of the described method, the reference can comprise at least the following: the domain name, the IP address, the URL address.

[0019] In a particular embodiment of the described method, the user behavior vectors comprise the instructions for applications, wherein the instructions constitute the series and sequence of activities comprising at least the following activities: following the link, data entry, choosing some of the suggested options.

[0020] In a particular embodiment of the described method, the user parameters comprise at least the following: the user device IP address, the user geolocation data, the redirection time, the user device information, the used operating system, operating system interface language, provider, browser, browser version, browser interface language, the cookie files, the system time and the actual time in the user device system, the url-referrer.

[0021] In a particular embodiment of the described method, information is additionally collected on each of the web resources that are part of the detected redirect chains, wherein such information constitutes at least the following:

- The URL link referencing the particular web resource,
- The ID and the other parameters within the URL link body;
- Detection time and date;

- The web resource geolocation data;
- Information on the provider connected to the web resource;
- The ID / company/brand name used by this web resource.

[0022] In a particular embodiment of the described method, to construct the redirect graph, all the redirect chains are taken into account, wherein each of chains contains the following information: on the user behavior vector and on the user parameters used in the said chain construction, on each of the web resources that are part of the said redirect chain and on the sequence of the said web resources.

[0023] In a particular embodiment of the described method, the redirect graph constitutes a combination of nodes each of which corresponds to the detected web resource, and of arcs each of which corresponds to the redirection from one web resource to another.

[0024] In a particular embodiment of the described method, 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 the web resources' URL address constituent parts (i.e., the domain, the page name and the parameter names) match one another;
- the length of the domain name, the length of the top-level domain name, the length of the page names and the parameter names match one another;
- the IP addresses of the web resources match one another.

[0025] In a particular embodiment of the described method, when combining the plurality of the obtained redirect chains into at least one redirect graph, the affiliated web resources are considered to constitute one vertex.

[0026] In a particular embodiment of the described method, when combining the plurality of the obtained redirect chains into at least one redirect graph in a multithreading mode, each of the vertices of each of the detected redirect chains 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, it is added to the graph as a new vertex; plus if no arc exists in the graph connecting this new vertex with the previous one, such an arc is added.

[0027] In a particular embodiment of the described method, the target resource is identified by carrying out additional checks of the web resource for malicious activities.

[0028] In a particular embodiment of the described method, the target web resource is identified by analyzing the HTTP response codes obtained by the browser.

[0029] In a particular embodiment of the described method, the redirect chain is rejected at the working stage if it contains less than the pre-determined number of redirections.

[0030] In a particular embodiment of the described method, 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.

[0031] In a particular embodiment of the described method, the pre-formed user behavior vectors (using which at least one redirect chain has been constructed at the preliminary stage) are used at the working stage to construct at least one redirect chain.

[0032] In a particular embodiment of the described method, such user behavior vectors are used at the working stage that were used at the preliminary 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.

[0033] In a particular embodiment of the described method, to construct at least one redirect chain, all the pre-formed user behavior vectors are used at the working stage.

[0034] In a particular embodiment of the described method, the user redirect rules directing the users to the target malicious web resources for each of the web resources, excluding the target web resource, comprise the following:

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

[0035] The claimed result may also be achieved through the implementation of 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.

[0036] The stated result is also achieved due to the implementation of the computing device for the target malicious resource identification, the said computing device being configured to implement the method of the target malicious resource detection according to any of the above options.

BRIEF DESCRIPTION OF DRAWINGS

[0037] Implementation of the technique will be further described in accordance with the attached drawings, which are presented to clarify the technique chief matter and by no means limit the field of the technique. The following drawings are attached to the application:

[0038] Fig. 1 illustrates a simplified variant of the malicious web resources combination at the detection of the target malicious web resources in which the described solution aims.

[0039] Fig. 2 illustrates a simplified variant of the target malicious web resource detection system implementation.

[0040] Fig. 3A, 3B illustrate the flow diagram of the working and preparatory stages for the target web resource detection method implementation.

[0041] Fig. 4A illustrates a simplified example of three redirect chains as part of the malicious web resources combination.

[0042] Fig. 4B illustrates a simplified example of the redirect chain containing similar web resources.

[0043] Fig. 4C illustrates a simplified example of combining several redirect chains into a redirect graph.

[0044] Fig. 5 illustrates a computing device for the described method implementation.

DETAILED DESCRIPTION

[0045] Numerous implementation details intended to ensure clear understanding of this technique are listed in the detailed description of the technique implementation below. However, it is obvious to a person skilled in the art how to use this technique as with the given implementation details as without them. In other cases, the well-known methods, procedures and components have not been described in detail so as not to obscure unnecessarily the present technique.

[0046] Besides, it will be clear from the given explanation that the technique is not limited to the given implementation. Numerous possible modifications, changes, variations and replacements retaining the chief matter and form of this technique will be obvious to persons skilled in the art.

[0047] It should be noted that, within the context of the present description, the «network resource» or «web resource» terms, unless specified otherwise, stand for any element or the combination of the World Wide Web elements that can potentially be accessible through the Internet, i.e., absolutely any element or combination of elements from the whole virtual space volume. Even if an element is stored in an encrypted form and on a closed server, it is potentially accessible; therefore, it also constitutes a network resource. Within the context of this description, the «network resource» or the «web resource» terms imply any data or data set that can be supplied through the network and are

associated with the network resource address. The non-limiting examples of the network resources are HTML pages, documents, images, video recordings, news feeds or the combinations of the above files. The network resources can include content, e.g., words, phrases, images etc. and/or integrated information, e.g., meta data, hyperlinks and/or integrated instructions (e.g., JavaScript scenarios).

[0048] The «redirecting» (or, HTTP redirecting, URL redirecting, URL forwarding) term refers to the method of representing a page, a form or a whole web application with more than one URL address. The redirecting, as a rule, is implemented by sending a certain HTTP response (a code in the form of 301, 302, 303, 304 or 307) to the application (e.g., a browser) with which a user interacts, with a new page following the said response, the user having to get an access to the said page, wherein the URL address of this new page is sent into the HTTP response' location header field. In the process, when the browser obtains the redirection response, it redirects the user to the target page automatically. There are also redirections based on the web page HTML meta tags and the redirections based on JavaScripts or the Flash technology.

[0049] Fig. 1 shows in a simplified manner the plurality 100 of malicious web resources 101...-198 at the detection of the target malicious web resources in which (such as the malicious web resource 194) the described solution is aimed.

[0050] Within the context of this description, the input web resource or the first web page will constitute the webpage to which the user is first redirected when the malefactors compel him/her to use the said plurality 100 of the malicious web resources. For example, in Fig. 1 the input web resources (first webpages) constitute webpages 101, 102, 103, 104, 105, 106, 107 and 108 located on server 110. Note that for the overall simplicity the web resources in the drawings have been grouped on three servers 110, 120 and 190 only. In the actual malicious infrastructure, the web resources can be arranged on hundreds of different servers which are also located in different countries.

[0051] As a result of the first redirection, shown in this example in dashed line, the user is directed to the input web resource 105.

[0052] The first user redirection is usually implemented through ads, phishing emails, messenger postings and social engineering methods. The further user redirections, such as the redirection from the input web resource 105 to the intermediary web resource 122, are controlled by the traffic distribution systems (TDS) that are part of the infrastructure used by the malefactors (e.g., TDS 109 or TDS 129). Such systems automatically determine the next web resource that the user will be directed to, depending on various parameters of the user browser, operating system settings, the data input by the user (e.g., answers for questions) and a plurality of other criteria.

[0053] Within the context of this description, the target web resource constitutes the last webpage in the redirect chain; in Fig. 1, these are webpages 191, 192, 193, 194, 194, 196, 197, 198 located on server 190. It is on such a webpage (located on the target resource) where the malicious actions are taken,

e.g., the deceived user is given an opportunity of purportedly paying for the purchase using a bank card. It is the target web resources that constitute the direct source of the attackers' income; and it is the blocking of the target web resources that destroys the malefactor's structure most effectively.

[0054] The present description also discloses the «redirect chain» term which stands for the sequence of the web resources that the user has been redirected to, from the input resource to the target web resource. In other words, this is the whole set of webpages that the user visited, starting from the input resource and finishing with the target web resource. The simplified example in Fig. 1 shows the redirect chain consisting of webpages 105, 122, 194. The real structures, similar to the one shown in Fig. 1, can contain many more redirections (the webpages visited by the user); accordingly, the length of the redirect chain is considerably longer.

[0055] The additional and/or alternative characteristics, aspects and advantages of the present technical solution embodiments will become obvious from the following description, the accompanying drawings and the appended claims.

[0056] The present technology is aimed at providing a computer-implementable method and system of the malicious web resource detection.

[0057] The claimed computer-implementable method of the malicious web resource detection is realized through the system 200 of a target malicious web resource detection presented in Fig. 2, the same system comprising at least the following: the data transmission network 210; the computing device configured to implement the target malicious web resource 220 detection method; at least one external data repository 230; at least one user device 240, 241, 242.

[0058] The data transmission network 210 can be, e.g., the Internet network or any other computer network.

[0059] In another non-limiting embodiment of the present technique the computing device 220 is configured to obtain information on the input web resources. By way of a non-limiting example, such information can constitute a reference to at least one input network resource (the first webpage). Additionally, the reference can constitute the web resource URL address, the Bitly type links (truncated URLs), the domain name or the IP address.

[0060] In another non-limiting embodiment of the present technique the computing device 220 can comprise a scanning system (a scanner) 221 (not shown in Fig. 2) for searching and obtaining references to the input web resource. The scanner can be fitted with active networking equipment (not shown in Fig. 2) and use it to communicate over the data transmission network 210 with at least one user device (240-242). The active networking equipment can constitute, e.g., routers, connection switches, gateways (not shown in Fig. 2).

[0061] In another non-limiting embodiment of the present technique the computing device 220 can comprise a special framework (a software platform) allowing, e.g., the operator or the computing

device user to send the input web resource references to the system that implements the method, by filling a special form.

[0062] In a non-limiting embodiment of the present technology the computing device 220 is configured to connect to external systems, e.g., to an external data repository 230 and to databases through the data transmission network 210, i.e., through the direct channels and/or one or several networks or other common channels that can include the Internet, intranets and/or other networks and can include wire based and/or wireless communication networks.

[0063] As an example, the computing device 220 can be configured to obtain data both from the external data repositories, such as data repository 230 (containing, e.g., database ranked information on the known fraudulent web resources), and from the internal data repository 225. What is more, the internal database contained in the internal data repository 225 can be periodically replenished by the computing device 220, e.g., through network scanning or through obtaining information from special web resources forms.

[0064] In addition to the above, in one of the non-limiting embodiments of the present technology the analysis instructions set saved in the internal 225 or external data repository 230 can be obtained from the Internet users located in different points of the globe, the same Internet users being involved in the process of collecting the information on the malicious web resources.

[0065] As an example (but without being limited to that example), the computing device 220 is configured to additionally being capable of mirroring the traffic from all the user devices 240-242 connected to it. In the process, the computing device 220 can be additionally configured to analyze the traffic obtained from the user device, to detect references to the input web resource in the said traffic.

[0066] In one of the non-limiting embodiments the internal data repository 225 stores the information related to a plurality of network resources. As is known to a person skilled in the art, the internal data repository 225 can additionally or optionally include one or several databases (not shown in Fig. 2). The mentioned separate databases can be part of one and the same physical database or can be realized as separate physical units.

[0067] The computing device 220, in addition to the above, can include one or several processors, a memory and a communication interface that are connected together by a bus or by another communication channel; although, other network type devices can also be used. The computing device 220 processes (analyses) information received from other devices through the communication network, e.g., in accordance with the HTTP based application' RFC protocol. Various applications can operate on the device 220 and transmit data (e.g., files or web pages) in response to the user devices (240-242) requests.

[0068] It should also be noted that the computing device can also be connected to any other devices, e.g., constituting active network equipment (routers, connection switches, gateways) and client

devices (mobile devices, smartphones, PCs, MFDs) or databases through a data transmission network that can constitute, e.g., the Internet or any other computer network.

[0069] In one of the non-limiting embodiments the computing device 220 is configured to receive the references to the input web resource of the malefactors structure through the data transmission network 210, to model the redirect chain through simulating the users behavior based on the vector data and user images obtained from the internal 225 or external 230 data repository, to construct the redirect graph based on the accumulated redirect chains data, and also to perform analysis to identify the detected redirect chains peculiarities for the purpose of creating rules for the target fraudulent resource identification. The computing device 220 is additionally configured to visualize the created unified redirect graph to give the operators or users the possibility to visually analyze the redirect graph.

[0070] In one of the possible embodiments of the present technology the computing device 220 is configured to receive instructions from at least one user device (e.g., 240), to pre-analyze the redirect chain and to block the target fraudulent web recourse for the user.

[0071] Moreover, the system 200 can include various users of the web-sites and/or applications/services that connect to the system through user devices (such as devices 240-242) which can be stationary devices (e.g., a desktop computer, a workstation or an IoT device) or mobile devices (e.g., a smartphone, a tablet computer, a laptop), to interact with client web applications, such as a browser or an application developed to access a system/service.

[0072] The user devices 240-242 are configured to communicate with the computing device 220 through the data transmission network 210, to provide the computing device 220 with the data for analyzing the references to the input web resource.

[0073] The computing device 220 is configured to establish the connection with the user devices 240-242 through the data transmission network 210; in the process, the computing device 220 can send a specially configured module to the user devices 240-242, the same module being realized in any known programming language and serving for the establishment of a protected channel in the data transmission network 210 and for impelling the user device to re-translate (mirror) to the computing device 220 the references to all the web resources with which the user interacts through the user device 240-242. It should be noted that the frequency of the data acquisition from the user devices 240-242, the data category, the exceptions etc. are set by the user itself. Additionally, the computing device 220 is configured to receive data on the user system environment, to emulate the redirect chain; in doing so, the data that are part of the user's system environment do not contain personal data. As an example, such data can include information on the user region, the used browser version, the type and version of the user device, the used OS etc.

[0074] The user devices 240-242 are configured to connect to the computing device 220 through the data transmission network 210, to supply the former with the data for the analysis.

[0075] The user devices 240-242 are configured to additionally establish a connection with the computing device 220 through the data transmission network 210, to supply the former with the constructed redirect chains.

[0076] The functionality ascribed to the system 200 in this document can be distributed between the components thereof in an alternative manner, e.g., by merging or further separating the functions of one or several components; or, the functionality can be distributed among another components combination. Thus, although only one variant of a specific system component can be illustrated in Fig. 2, it should be understood that other combinations of components that are part of the system can be used too.

[0077] Referring to Fig. 3A, a computer-implementable method of the malicious web resource 300 detection realized through the computing device 220 will be described hereafter.

[0078] The method 300 starts with a preparatory stage including the steps that will be described in detail below.

STEP 310 A REFERENCE IS OBTAINED TO AT LEAST ONE KNOWN MALICIOUS INPUT WEB RESOURCE

[0079] The first step of the method 300 preparatory stage consists in obtaining a reference to at least one known malicious input web resource.

[0080] References to a plurality of web resources can constitute both the web resources themselves (their domain names and/or IP addresses) and, e.g., the links to the web resources, in particular, URLs, available through the data transmission network 210 or another network (not shown) to the computing device 220.

[0081] References to at least one known input malicious network resource can be obtained both from the external 230 and internal data repository 225. As an example, the latter can include the databases of the websites related to the malefactors; also, any other external data repository can be used that is configured to store at least one input web resource reference.

[0082] As has been shown previously, the reference to an input web resource can also be obtained by the computing device 220 from an internal data repository 225. In non-limiting embodiments, the internal data repository 225 can be replenished with the web resource references either by receiving information from the users or by performing a scanning procedure.

[0083] In other embodiments the obtainment of at least one reference directly from the user can be realized, e.g., through a special form created in a user framework described previously, or through entering data into the internal data repository 225 by hand.

[0084] In other embodiments of the present technology the obtainment of at least one reference can be realized through collecting hyperlinks to the known malicious web resources from the messenger messages, social networks, user device mailboxes and during traffic mirroring. In such a case the

computing device 220 can be configured to extract the hyperlinks or other references from the received messages.

[0085] Furthermore, in other embodiments of the present technology the reference to at least one known malicious input web resource can be obtained through the network resources scanning done by the computed device 220.

[0086] For this end, in some of the non-limiting embodiments a web robot or a crawler can be realized on the computing device 220, the same web robot or crawler performing scanning of the network web resources. The computing device 220 can additionally comprise a task scheduler storing the crawler startup timetable and the list of other conditions for network scanning.

[0087] In other non-limiting embodiments, any legal SW capable of network surveillance and identification of the web resources conforming with the set parameters can be used as a scanner to search for the network resources.

[0088] After the computing device 220 obtains the reference to a known input malicious web resource, the method 300 continues with the step 320.

STEP 320 AT LEAST ONE REDIRECT CHAIN IS CONSTRUCTED FOR EACH OF THE OBTAINED MALICIOUS INPUT WEB RESOURCES; WHEREIN TO CONSTRUCT AT LEAST ONE REDIRECT CHAIN, THE PRE-FORMED USER BEHAVIOR VECTORS IMITATING HIS/HER BEHAVIOR AND THE USER PARAMETERS IMITATING HIS/HER ENVIRONMENT ARE USED.

[0089] At this step, at least one redirect chain is constructed for each of the obtained input web resources, wherein to construct at least one redirect chain the pre-formed user behavior vectors imitating his/her behavior and the user parameters imitating his/her environment are used.

[0090] It should be noted that within the context of this description the user environment implies a so-called system environment, i.e., the set of parameters characterizing the settings of the user device itself, of the operating system installed on it, of the user browser etc. Such settings constitute, e.g., the IP address, the operating system interface language etc.

[0091] The performance of this step starts from going to the first network web resource known to be a malicious web resource (namely, constituting the input stage of the multi-step Internet fraudulent scheme) in response to the obtained reference.

[0092] It is worthwhile mentioning that an input malicious web resource, as a rule, is created by the malefactors expressly to collect various user environment information, and usually it is precisely the function that it performs. The collected information can include, at least, the following: information on the IP address, user device type, versions of the programs installed on the device, region, device interface language, operating system language, interface language of the application used to visit the web resource, provider names and cookies stored at the device. These data are used by the malefactor's

system to build a picture of the user and his/her environment. The detected information comes to the malefactors traffic distribution system (TDS) for the selection of the next redirect stage.

[0093] The input web resource may have no content, or the said web resource can constitute a link to the next webpage. At the same time, the input web resource can contain some content which can be. e.g., a graphic banner ad, an invitation text or a user questionnaire form.

[0094] Each of the intermediate web resources of the malefactor's network infrastructure can also gather some information on the user (both «by hand», e.g., by compelling the user to fill in the questionnaire or the survey forms, and automatically, based on the analysis of the user device, its geolocation data, visitation time etc.) Based on the obtained information, at the next stage the traffic distribution system usually redirects the user to the resource containing text in the language that he/she is familiar with, as well as the familiar brand name and other peculiarities providing for higher conversion (i.e., in this case, the user's decision to «enter the promotion», to «pick up a prize for participating in the poll» etc.) In this way the malefactors try to avoid blocking the intermediary network resources (indeed, technically, such intermediary resources don't break any laws in their own right), but, at the same time, to redirect the user to a functional active target resource that will let them one way or another to coax the user out of his/her money. That said, the target web resource is configured in such a way that it is impossible to reach directly, bypassing the whole the redirect chain.

[0095] The present technology implies that to construct the redirect chain, it is necessary to imitate a real user behavior. For the traffic distribution system used by the malefactors to be «sure» that it redirects a real user, the data collected by it at every redirect step should be identical to the data that would come to it if a live Internet user visited the input resource.

[0096] In accordance with the said principle, the method 300 provides for using a plurality of user behavior vectors and user parameters, so that the malefactors traffic distribution system would be able to supply the simulated user with a target content. This would allow constructing at least one redirect chain from the detected input web resources, identifying the regularities based on which the redirection takes place and using these regularities afterwards to detect the analogous fraudulent target web resources and to block them.

[0097] According to the above description, to implement the method 300, controllable runtime environment is used, e.g., virtual machines with a specially installed OS, a sandbox, an emulator or any other applications capable of registering the sequence of user actions and changes that happen in the operating system as a result of them. In particular, as an illustrative example, virtual browsers can be used in a controllable environment, the same browsers being equipped with automation means (such browsers as, e.g., Selenium). During its use, an appropriate extension is installed using the virtual browser setting and the browser cache is cleaned, after which the browser goes to the web resource. In the process, logging is also carried out using the browser features, i.e., the browser automatically saves

to the hard drive all the information on the performed transitions from one resource to another, on the additional parameters inserted into the URL address and corresponding to those transitions, on the user behavior vectors and user profiles used during the said operations; the browser also takes screen shots of every visited web resource. In addition to the browser, any other available SW can be used as a logging instrument, e.g., a script written in any programming language and capable of being interpreted within the controllable environment to obtain the sequence of transitions between the web resources.

[0098] It should be noted that the user behavior on the fraudulent web resource is simulated using the pre-formed user behavior vectors and parameters (profiles) that can be stored both in the internal data repository 225 of the system 200, and in the external trusted data repository 230 available through the data network 210.

[0099] In the non-limiting embodiments of the present technology the user behavior vectors constitute scripts written in advance. They can be written in any programming language allowing to write the instructions for applications in the form of a script (including for the browser, e.g., for Google Chrome). Such instructions usually constitute a set of commands for performing a sequence of actions, such as following a link, data entry, selecting one of the proposed options in the list of options etc. The user behavior vectors can be stored both in the general database 225 of the device 220, and in a specialized user behavior vectors database using any of the commonly known means. Each file containing one specific script or each database record containing a specific script (user behavior vector) can be provided with a unique identifier allowing, firstly, to distinguish this script from other scripts, and secondly, to quickly find it in any databases where it is mentioned. The identifier as such can constitute, e.g., a decimal number or a result of a hash function taking from the given script text.

[0100] The user parameters can be stored, e.g., in a text file format or in the database record format, both in the general database 225 of the device 220, and in a specialized user parameter (profile) database organized through any of the commonly known means. Each such file or database record containing a specific user profile (parameters) can be provided with a unique identifier allowing, firstly, to distinguish this script from other scripts, and secondly, to quickly find it in any databases where it is mentioned. The identifier as such can constitute, e.g., a decimal number or a result of a hash function taking from the content of this file or record.

[0101] Each such file or user parameters record contains a set of the common parameters used by the modern Internet applications and available to any web resources for reading. Using the same parameters, an information on the user and his/her environment is obtained by any legitimate web-sites: the search systems, the online shops etc. These parameters are well known to a person skilled in the art. For example, these parameters can include at least the following: the user IP address, user device geolocation data, redirection time, information on the user device, on the operating system, name of the

used provider, version of the user browser, cookie files, time (system and actual values), URL referrer etc.

[0102] Before going to the input resource, the computing device 220 reads the pre-saved user parameters from the file and places these parameters into a controllable runtime environment as the variable values for this environment. From the «point of view» of any traffic management system, these parameters will be identical to the environment settings of a certain user who entered this web resource from some specific device. After that, the computing device 220, in accordance with the used script describing the preset user behavior vector, goes to the input web resource on the instruction received at stage 310. Thus, the malefactors traffic distribution system is given the opportunity to read the preset user parameters, and they do not fundamentally differ from the similar parameters of the users visiting the same web-site.

[0103] It should be noted that the fraudsters, as a rule, target not the whole population of the planet, but a quite well defined category of users. For example, people living in a certain region or the users with a certain known version of the browser installed that has a vulnerability etc. That is why some of the transitions to the input web resource (those where the system implementing the described method has imitated the parameters or actions of a «wrong» (from the malefactors point of view) user) will not result in constructing of the redirect chain.

[0104] A wide variety of the prearranged user behavior vectors or user parameters can be stored in the internal data repository 225 of the system 200 or in the external data repository 230. From a technical point of view, the storing of such data sets can be implemented, e.g., in the form of a table each of the rows of which (e.g., the «user country» row) can be used for storing a set of various values which can be selected to imitate another visitor (e.g. «Spain, France, Russia») or in a database organized through any of the commonly known means.

[0105] For each of the input web resources, at least two different user behavior vectors and at least two different files containing user parameters are used. In other words, the system implementing the described method goes to every input web resource at least two times; in the process, both parameters and action patterns of two different users are imitated. This allows detecting the redirect chains regularities in the future.

[0106] All the successful (i.e., those that allowed to construct the redirect chain) vectors and user parameters are additionally saved in the system 200 (in the data repository 230 or 225) together with the links, screen shots and content copies of the webpages that were available during the advancement along the redirect chains.

[0107] The item-by-item examination of various user behavior vectors and user parameters is conducted until the target web resource is detected.

[0108] To verify the fact that a certain detected resource is an intermediary one and not a target one, additional checks of every web resource for the presence of malicious actions are performed using any method known from the prior art, e.g., any methods described below with regard to step 380. In one non-limiting example the check can constitute the establishment of the fact that the given web resource contains a suggestion to enter the bank card details. In another non-limiting example the criterion of the web resource belonging to the target web resources can constitute the suggestion to append the scanned image of the passport or the driver's license.

[0109] A variant of the described method implementation is also possible wherein the determination of the redirect chain ending, i.e., the target web resource detection can be implemented based on the analysis of the HTTP response codes received by the browser. For example, when after at least three redirections the system 200 stops receiving HTTP responses containing codes of the 301, 302, 303, 304 or 307 type, it is being recorded that no redirections are effected from the current webpage and, therefore, the current webpage constitutes the target web resource.

[0110] At the intermediate web resources, the HTML code of the web resource page is checked to reveal the questionnaire forms that the malefactors suggest the visitors fill to go to the next node. If such forms have been detected, they can be filled with the data chosen based on each field's format (e.g., the «Telephone» field is filled with seven-digit numerical set, the «Address» field – with a certain address taken from the database related to the same country as the used user profile etc.) The data for filling the fields can be both generated based on the preset templates and retrieved from a prearranged database that can be located both in the internal 225 and external 230 data repository. The field types are determined based on the key words (field headers) or, if this is not possible, through the item-by-item examination of various formats. The main types of formats can be at least the following ones: the address, the telephone number, the email address, the person's full name and the user-defined text field. It should be noted that for every format, both during the filling and during the template based generation, variants can be provided taking into account the regional specifics; e.g., the «ZIP code» can be filled with a six-digit number for the Russian Federation and with a five-digit number for the USA etc.

[0111] If a necessary value format has been figured out for a previously unknown field header, the data can be subsequently used in the system 200 by saving the matching value in the database which can be located both in the internal 225 and external 230 data repository. In the process, the system 200 saves both the identifiers and the value or type of the field (if it can be included with some type). The field identifiers can constitute the following: the field length, name of the field visible on page, field id in the HTML code of the page, field class in the HTML code of the page etc. If the system 200 subsequently encounters an unknown field with one of the previously found identifiers, the identifier search will be conducted in the database, and if the search proves successful, the value format or the value itself will be used that has previously resulted in successful matching.

[0112] Thus, to successfully match the necessary format in the existing fields, the computing device 220 inserts the values of the main types and their combinations by examining them item-by-item until the preset condition is satisfied. In so doing, the successful matching, in accordance with the given condition, is the one that allows avoiding the occurrence of errors and leaving the webpage with a questionnaire or a survey form while advancing further along the redirect chain.

[0113] The data used for filling can be optionally saved together with the information on the webpage where they have been used, for further analysis.

[0114] Further, with reference to Fig. 4A, an example of the redirect chains 400 construction will be described. It is important to note that all the data, including the numbers of the chains, nodes and arcs, are given solely for the purpose of illustration; any other data obtained during the method 300 implementation can be used here, including the fact that the redirect chains can contain other numbers of web resources and transitions between them. For the overall simplicity, the enumeration of the web resources that constitute the redirect chains 400 is taken from Fig. 1.

[0115] In the illustrative example, three redirect chains 410, 420, 430 have been formed. All of them have been constructed based on the reference to the input web resource 105 obtained at the step 310. The redirect chains 410, 420, 430 consist of various web resources; this is due to the fact that, when going to the input web resource 105, the system, as has been described in regard to step 320, used three different pre-formed user behavior vectors and three different pre-formed user profiles (hereinafter, in this and the following paragraphs these data for the sake of simplicity are collectively called «vectors»). As can be seen in Fig. 4A, when going to the input web resource 105 with the user vector 411, a redirection to the web resource 121 has taken place; when going to the web resource 105 with another user vector 421, a redirection to the web resource 127 has taken place; and when going to the input web resource 105 with the third user vector 431, a redirection to the web resource 122 has taken place.

[0116] Therefore, using a successful imitation of the user by vector 411, a redirect chain 410 has been obtained consisting of the web resources 105, 121, 135, 193. Similarly, the use of vector 421 has allowed obtaining the redirect chain 420 consisting of the web resources 105, 127, 138, 194, and the use of vector 431 – obtaining the redirect chain 430 consisting of the web resources 105, 122, 131, 194.

[0117] It is clear that the web resources 193 and 194 in this example are target web resources.

[0118] It should be noted that in the process of transitioning along the redirect chain, information is additionally collected on every web resource that is part of the chain. In the process, at least the following information is recorded:

- The URL link to the detected network resource,
- The ID and other parameters within the body of the URL (link) referencing the web resource;
- Detection time and date;

- The web resource geolocation data;
- Information on the provider associated with the web resource;
- The ID / company or brand name used on the web resource.

[0119] Part of the named data can be obtained, e.g., by using the open web services, such as, e.g., WHOIS allowing obtaining the register's name, localization, language, registration date, website administrator contact information, methods of contacting the administrator and addresses of the DNS servers.

[0120] The information on the companies or brands used on this web resource can be obtained by any commonly known method, e.g., by parsing the text available on the webpage and checking every word found on the page against the pre-arranged brands and companies lists stored in the data repository 225.

[0121] After constructing the redirect chain, the chain itself and all the listed information on each of its web resources, as well as the data on the sequence of transitions between the web resources is saved in the internal data repository 225.

[0122] Next, the method 300 (speaking again of Fig. 3A) begins fulfilling step 330.

STEP 330 THE CONSTRUCTED REDIRECT CHAINS ARE COMBINED INTO AT LEAST ONE REDIRECT GRAPH

[0123] At the next stage, the constructed redirect chains are combined into at least one redirect graph.

[0124] Within the context of this description, the redirect graph is a graph comprising all the detected redirect chains starting from at least one input web resource the reference to which has been obtained at stage 310. The redirect graph is a totality of vertices each of which constitutes a detected web resource, and of arcs that reflect the sequence of transitions from one web resource to another between the input web resource and the target web resource.

[0125] However, it should be noted that although in a simplest case each of the graph vertices constitutes one web resource with one URL address, in several embodiments of the described method each of the graph vertices can constitute a plurality of the grouped (affiliated) webpages having different URL addresses. These pages can be grouped and represented as one vertex due to the fact that all of them have common characteristics (e.g., all of them contain references to the same brand or the same makeup dummy is used on all of these pages etc.)

[0126] In various embodiments of the present technology to determine the web resources that have common features and are related to one another, any method known from the prior art can be used. For example, the method using the web resources screen shots saved in the database 225 – to detect the

web resources templates affiliation; or, the computer vision methods – to detect visually similar resource groups. In addition to that, the methods based on the web resource HTML code analysis can be used.

[0127] That said, it should be noted that prior to constructing the graph, the association of each of the detected affiliated web resources with the main one is established. For example, it can be done in the way shown in Fig. 4B, for the web resources constituting the redirect chain 420 described above in regard to Fig. 4A.

[0128] For example, in the process of the database 225 search it has been established that the resources 114 and 117 contained in the database 225 are visually similar to the input web resource 105, but differ in the known brand logos used in the page design; the web resource 144 contains text completely analogous to the text of the web resource 127, and the web resources 134 and 139 are located at the same IP address that the web resource 138.

[0129] As an example (but not being limited to that example), let us note that in case of the fraudulent pages one and the same brand name can always be used, but, that said, the malicious pages' domain names will be different for different URL addresses; however, other parts of these URL addresses will be the same.

[0130] For example, in the URL address

[http://www.\[some.domain\]/adidas/great-sale-90-discount/register.html?parameter1¶meter2](http://www.[some.domain]/adidas/great-sale-90-discount/register.html?parameter1¶meter2)

various domain names (e.g., freeserver.com, HyperHost.ua, Ucoz.ru etc.) can be used instead of [some.domain].

That said, the rest of the link looks identical for all the pages used by the malefactors.

[0131] In the non-limiting embodiments of the present technology the web resources that are part of the redirect chain can be represented by a plurality of lookalike grouped web resources. Additionally, the web resources can be deemed similar if the following elements match:

- all the parts of the URL address (i.e., the domain, the page name and the parameter names,
- all the parts of the address, except for the top-level domain,
- the top-level domain names;
- the lengths of the domain name, of the top-level domain name, of the page names and of the parameter names;
- IP addresses.

[0132] Thus, with regard to Fig. 4B, the web resources 114, 105, 117 can be grouped into one vertex 450 of the redirect graph, the web resources 127 and 144 – into another vertex 460, and the web resources 134, 138 and 139 – into yet another vertex 470.

[0133] Hereinafter, the process of the redirect graph construction from a plurality of redirect chains will be described in detail. To construct a redirect graph, all the redirect chains saved in the

internal data repository 225 are taken into account, and for every redirect chain at least the following data is stored: information on the input web resource, on the target web resource, on the groups of the detected affiliated web resources, the references (e.g., hyperlinks) to each of the web resources and the information on the user behavior vectors and user parameters used to detect every redirect chain.

[0134] At the initial stage, all the data based on which the redirect graph is constructed have been cleared out. As demonstrated in Fig. 4C, the redirect chains (in this example – chains 410, 420 and 430) are actually combined into the redirect graph 440. For this end, each vertex (web resource) of each of the detected redirect chains is compared with the vertices (web resources) of other detected redirect chains in a multithreading mode. If completely matching vertices (as, e.g., the vertex 450 which is present in all three chains 410, 420 and 430) are found, these matching vertices are considered to be one graph vertex. Therefore, the vertex 450 becomes the input graph vertex common to all three chains 410, 420 and 430.

[0135] If a new vertex is found the value (the web resource associated with this vertex) of which is different from all other vertices, it is added to the graph as a new vertex; plus, if no arc yet exists in the graph connecting this new vertex with the previous one, such an arc is added. Thus, since the vertex 450 in the chain 410 is connected to the vertex 121, the vertex 450 in the chain 420 is connected to the vertex 460 (not coinciding with the vertex 121) and the vertex 450 in the chain 430 is connected to the vertex 122 (not coinciding with the vertices 121 and 460), three new vertices 121, 460 and 122 will be added to the graph, all of those vertices being connected to the vertex 450.

[0136] During the further combining of the chains 410, 420 and 430 based on the above rules, we'll obtain the unified redirect graph 440 shown in Fig. 4C. It's not hard to see that there is only one vertex 194 corresponding to the target web resource and present both in the chain 420 and in the chain 430; that said, other vertices, such as vertex 193, corresponding to the target web resource can be present in the graph.

[0137] The existence of such unified redirect graph, essentially, means that the user having visited the web resource 105 or the similar resources 114, 117 can be redirected to one of the web resources 121, 122, 127, 144 from where he/she will be redirected to one of the web resources 135, 134, 138, 139, 131 from which, in their turn, the user will get at one of the two target web resources 193 or 194. Please, note that Fig. 4C shows a simplified illustrative example of the redirect graph 440. In a real life graph constructed by the system 200 during automated examination of the malefactors web resources structure, the number of vertices and arcs can be almost anything, including much greater that shown in Fig. 4C.

[0138] All the data obtained at this step, including the user behavior vectors and the user parameters 411, 421, 431 used for the detection of each of the redirect chains (not shown in Fig. 4C) are

saved in the database 225, and the method proceeds to step 340 described hereinafter with reference to Fig. 3A.

STEP 340 THE REDIRECT GRAPH IS ANALYZED, AND THE USERS REDIRECT RULES DIRECTING THEM TO THE TARGET MALICIOUS WEB RESOURCES ARE IDENTIFIED.

[0139] At the last step of the preparatory stage, the constructed redirect graph is analyzed, and the rules used by the malefactors traffic management systems in redirecting the users from the input web resource to the target malicious web resources are identified.

[0140] When analyzing the user behavior vectors and the user parameters, the values, parameters or actions that resulted in the redirection of various users to a specific web resource are identified. The redirecting rules identified at this step, essentially, are the traffic management system settings used by the malefactors in the studied infrastructure, that have been reconstructed analytically. As has been mentioned before, the malefactors normally target a specific group of users, and the found regularities will, in fact, describe the user group that the malefactors target with their infrastructure under examination.

[0141] The analysis data constitute the similarities and differences in the user behavior vectors and user parameters that have been used while identifying every redirect chain at the stage 320. By analyzing the user parameters, i.e., their geographical location, the versions of the devices, operating systems and browsers, the OS and the application language settings, the regularities between the fact of various users being redirected to this web resource and the presence (or, on the contrary, absence) of one and the same value pertaining to a certain parameter in all of those users are detected.

[0142] The regularity being detected can be in the form of, e.g., «only the users located in the USA are to be redirected to this web resource» or, on the contrary, «only the users NOT located in the USA are to be redirected to this web resource».

[0143] In another example explained with reference to Fig. 4A, the fact can be established that the users that have gone to the input web resource 105 from a device with the French operating system language installed, have been redirected to the web resource 121; those with the Spanish OS interface language have been redirected to the web resource 122, and the users with the Russian OS interface language have been redirected to the web resource 127. All the other users have not been redirected, i.e., no redirect chains could be constructed for them.

[0144] In yet another example the fact can be established that the users entering the web resource 105 through browser A of v.1.0.1 have been redirected to the web resource 121, whereas the users entering the web resource 105 using browser A of v.1.0.2 or higher have been redirected to the web resource 122, and still those who entered the web resource 105 using any other browser have been redirected to the web resource 127.

[0145] The process of the similarities or non-similarities detection per se is not peculiar in any respect and can be implemented using any of the commonly known means, e.g., by statistical analysis techniques.

[0146] Analyzing the user behavior vectors, similarly to the user parameter sets, the regularities between the fact of various users being redirected to this web resource and the actions performed on the previous web resource webpage or the selection variants (sex: «M» or «F»), or the numerical values (age, ZIP code etc.) specified when filling the forms are detected.

[0147] In the example explained with reference to Fig. 4 B, as a result of analysis, e.g., it can be established that the users who have specified the number belonging to mobile operator B in the «Telephone» field while filling the form on the web resource 127, have been redirected to the web resource 138, and those who specified the number belonging to the mobile operator M, have been redirected to the web-resource 139.

[0148] In another example the fact could have been established that the users who specified male gender while filling the form on the web resource 127 have been redirected to the web resource 138, and those who have specified female gender have been redirected to the web resource 139.

[0149] In every such case the identified regularity can be described in formal lexical terms «IF – THEN» and saved in the database intended for this web resource, e.g., for the web resource 105. Any known actual data entry format can be used; e.g., regular expressions can be used.

[0150] It should be noted that for the subsequent target malicious web resource identification only some of the identified regularities can be used, and not all of them. The regularities for the subsequent usage can be selected based on the preset incidence threshold exceedance condition. For example, the regularity is used to form the final redirect rule only if this regularity has been found in at least 85% of the redirect chains present in this graph. Any other incidence calculation method can be used, without limitations.

[0151] When the analysis of all the web resources that are part of the examined redirect graph is completed, the identified regularities (all or the most frequent of them) are combined, thus obtaining the redirect rule for this graph. This rule can also be described in formal lexical terms, e.g.:

(IF the OS language is Russian, THEN redirect to web resource 127) AND (IF «Regional code \ TEF code» EQUALS _903_ THEN redirect to web resource 138)... etc.

[0152] The obtained redirect rule is saved in the database 225. Any known actual data entry format can be used; e.g., regular expressions can be used.

[0153] In one of the possible alternative implementations of the described method the redirect regularities can be saved not in the form of a unified redirect rule, but separately, – each regularity in its own specific database field. For example, in the «OS language» field, the «Russian» or RU value will be saved; in the «Regional code \ TEF code» field, the 903 value will be saved etc.

[0154] The analysis results are saved in the database 225.

[0155] It should be noted that the detected redirect rules can comprise three types of conditions the fulfillment of which compels the traffic management system to redirect user from a certain web resource to the next web resource in the chain:

- the conditions depending on the user parameters (e.g., as has been shown above, the English language of the operating system interface);
- the conditions depending on the user behavior vector (e.g., as has been shown above, choosing a certain gender in the poll);
- the conditions that depend both on the user parameters and the user behavior vector – e.g., as has been shown above, if the redirection to a certain web resource occurs when the conditions of both types are fulfilled.

[0156] Also, it should be noted that the steps 310-340 are described in the form of a linear sequence of actions for the sake of simplicity. The system implementing the described method can repeat these steps cyclically, including in a multithreading mode, receiving in every cycle a new reference to at least one new input web resource. In this way, a redirect graphs and redirect rules database can be formed containing the information and analysis results for the plurality of the malicious web resources examined as described, the said database being stored, e.g., in the database 225. Also, the system implementing the described method can, with specified periodicity, scan the Internet (including scanning the open websites containing information on the known malicious web resources), find new references to the known malicious resources and process them as described above, replenishing the said database.

[0157] At that, step 340 and the preliminary stage are completed.

[0158] The working stage 350 (described in detail below, with reference to Fig. 3B) starts from step 360.

STEP 360 A REFERENCE IS OBTAINED FROM THE USER DEVICE TO AT LEAST ONE SUSPICIOUS INPUT WEB RESOURCE

[0159] At this step, the computing device 220 obtains a reference to at least one suspicious web resource from one of the user devices 240-242 through the communication network 210.

[0160] In one of the possible embodiments of the present technology the computing device 220 is configured to obtain information on the user environment from a user device such as device 240, 241, 242. The «information on the user environment» term in this case implies at least such data as the user device IP address, the user device geolocation data, the manufacturer, type, model and version of the user device, the operating system, the used provider, the browser version, the language of the operating system and browser interface, the system time, cookie files, the URL referrer (one of the client's request

headers in the HTTP protocol containing the request source URL). All these data can be obtained using any of the commonly known means well known to those skilled in the art.

[0161] For example, the computing device 220 can receive this information from the User Agent that is used to determine the browser version, OS version and some of the installed add-ons versions; in the cases where the User Agent is absent, the browser version can be determined by checking for certain browser functions or features implemented or changed between the releases. In so doing, the computing device 220 can also obtain the list of all the plugins, ActiveX controls and Browser Helper Objects (including their versions) installed in the user device 240-242 system. It should be noted that some of the plugins make their presence known through the HTTP headers.

[0162] Also, the computing device can obtain the information on the installed extensions and other SW associated with the browser from the user device. For example, such SW can constitute the ad blockers introducing certain changes in the pages being browsed; using them, it is possible to determine the extension type and settings. Such peculiarities are characteristic of all web applications – in particular, browsers installed on the device; they cannot be concealed through the privacy settings or any utilities.

[0163] Additionally, using any of the commonly known means the computing device 220 can also obtain the client device network protocol settings, e.g., the external IP address, the outbound TCP/IP connections port numbers, the local IP address for the users located behind the NAT or HTTP proxy and information on the proxy servers used by the client that is obtained from the HTTP header.

[0164] After the obtainment of at least one reference and the listed information, step 360 is completed, and the method proceeds to step 370.

STEP 370 AT LEAST ONE REDIRECT CHAIN IS CONSTRUCTED FOR EACH OF THE OBTAINED SUSPICIOUS INPUT WEB RESOURCES

[0165] After receiving the reference to the suspicious input web resource from the user device, the computing device 220 constructs the redirect chain.

[0166] As has been mentioned before, the computing device 220 is configured to obtain information on the user environment from the user device, i.e., such data as the user IP address, user device geolocation data, information on the manufacturer, type, model and version of the user device, its operating system, used provider, browser version, the operating system and the browser interface language, the system time, cookie files, the URL referrer etc.

[0167] At step 370, the computing device 220, in addition to the suspicious web resource reference, receives the specified user environment data from the user device. Based on the obtained data, the inquiry (or inquiries) to the user parameters (profiles) database are built, and the user profiles maximally resembling the environment parameters obtained from the real user device are being found.

[0168] For example, if the information concerning, in particular, the fact that the user device geolocation data corresponds to the USA, its operating system and browser language is English and the browser A version is 1.0.1 has been obtained from the user device, the user profile database inquiry will contain all this information.

[0169] In a particular embodiment of the described method, the computing device 220 uses for further processing all the found user profiles (parameter sets) with at least one matching preset parameter. In another possible embodiment, only the found user profiles with all matching preset parameters (i.e., according to the given example, both interface language, geolocation data and browser version) are used. Any other principles of the user profiles selection (resembling the environment parameters obtained from the real user device) are possible as well, without limitations. For example, the interface language and geolocation data matches could be considered mandatory, and the matching of at least one parameter from among all others could be sufficient.

[0170] Using the identifier of each of the obtained user profiles as the search query, the inquiry or inquiries to the database containing the information on various previously constructed redirect graphs are built, and the user behavior vectors are found each of which has been previously successfully applied together with the given user profile at least once to construct at least one redirect chain.

[0171] After that, the found user behavior vectors are retrieved from the database using their identifiers. From the resulting «user profile – user behavior vector» pairs the controllable runtime environment parameters, e.g., the parameters of the virtual machine imitating the user device are formed, as has been described previously, with regard to stage 320.

[0172] Using the controllable runtime environment set up in this way, the found user description vectors used successfully with the given user profile in the past and the computing device 220, the transition to the suspicious input web resource following the obtained reference is effected.

[0173] An alternative implementation of the described method is also possible, where the user behavior vectors successfully applied in the past are not searched for, but all the user behavior vectors present in the system are used with the suitable user profiles (parameters).

[0174] It should be noted that the computing device 220 is configured to simultaneously launch several configured controllable runtime environments each of which can be fine-tuned using the found user profile parameters. Thus, the transitions to the suspicious input web resource following the obtained reference can be effected simultaneously for various «user profile – user behavior vector» pairs.

[0175] In this way, at least one redirect chain is obtained, analogously to the method described above with respect to stage 320.

[0176] In another possible embodiment of the described method, the reference (e.g., URL) to the suspicious input web resource obtained from the user device is searched for in the redirect graph database.

[0177] Such search can be both clearly defined, when the exact match for the obtained URL is searched for, and fuzzy. In the latter case, the following matches are searched for:

- of all the parts of the URL address, except for the top-level domain,
- of the top-level domain names;
- of the lengths of the domain name, of the top-level domain name, of the page names and of the parameter names;
- of the IP address.

[0178] If the input web resource corresponding to the specified search query is present in the database, at least one user redirect rule associated with the given input web resource is retrieved from the database.

[0179] The previously identified and saved in the database redirect regularities forming the retrieved redirect rule are used for an appropriate configuring of the controllable runtime environment, e.g., a virtual machine simulating a user device. Using the virtual machine configured in this way and the computing device 220, a transition to the suspicious input web resource is effected following the obtained reference, and the redirect chain is constructed analogously to the method described above with respect to step 320.

[0180] The obtained at least one redirect chain is saved in the database. It is also clear that when several different user profiles and/or user behavior vectors are used at this step, considerably more than one redirect chain can be obtained.

[0181] At that, step 370 is completed, and the method proceeds to step 380.

STEP 380 THE CONSTRUCTED AT LEAST ONE REDIRECT CHAIN IS CHECKED FOR COMPLIANCE WITH AT LEAST ONE RULE OF USER REDIRECTION TO THE TARGET MALICIOUS WEB RESOURCES

[0182] At step 380, the constructed (at the previous step) at least one redirect chain is checked for the correspondence of the redirections identified in this chain with at least one rule (identified at the preliminary stage) of user redirection to the target malicious resources.

[0183] Before this, a number of conditions are additionally checked, the correspondence with which allows one to be reasonably assured that the chain is not malicious.

[0184] Specifically, if no redirect chain could be constructed for any of the found user parameter variants, i.e., the input web resource the reference to which has been obtained at stage 360 does not implement a multi-step fraudulent scheme at the given user parameters, this web resource is considered safe for the user the notification of which fact is sent through the computing device 220 to the user device that the reference has been obtained from. With this, the method is completed.

[0185] A variant of this method implementation is also possible, where if at least one redirect chain could not have been constructed, the input web resource is additionally checked for being one of malicious resources using any of the commonly known methods; the notification is sent to the user device only if the web resource is not malicious. With this, the method is completed.

[0186] For every redirect chain detected and saved in the data repository 225, the number of redirects (i.e., the arcs in this chain) is determined and compared with a preset threshold value. In the example given in Fig. 4A-B, this number will be very small (equaling three) since the example of a real fraudulent infrastructure comprising, as a rule, many more web resources, would be hard to grasp. That said, it is believed that if the average chain length exceeds the preset threshold value (e.g., equaling 6 redirects), the examined redirect chains are malicious. The information on this is saved in the internal data repository 225.

[0187] If the number of redirects in the given redirect chain does not exceed the preset threshold value (e.g., equaling 2 or 4), such a chain is rejected and excluded from further examination. This is done so because small number of redirects is not typical for malefactors; more likely, it can signify legal web resource actions, e.g., promotional campaigns.

[0188] If after the counting of the redirects for all the chains that were able to construct during stage 370, not a single chain the number of redirects in which exceeds the given threshold remains, the given input resource is considered safe for the given user, and an appropriate message is sent through the computing device 220 to the user device from which the reference has been obtained. With this, the method is completed.

[0189] Alternatively, if the number of redirects exceeds the preset threshold value for at least one chain, the user redirect rule (or, what is the same, the set of conditions for redirecting from one web resource to another) is being identified for every redirect chain for which the said condition has been fulfilled.

[0190] This is done exactly as has been described for step 340 above.

[0191] A described method implementation variation is also possible where the constructed redirect chains with the length exceeding a preset threshold value are pre-combined into a redirect graph, as has been described for step 330.

[0192] The identified user redirect rule is checked for matching with all the known redirect rules identified at the preliminary stage. For this end, an inquiry is sent to the database containing the identified redirect graphs and redirect rules using any commonly known method; all the known redirect rules are retrieved from the database. After this, each of the redirect rules identified at this stage is compared, either one at a time or in a multithreading mode, with all the redirect rules identified at the preliminary stage. The comparison can also be done using any method known from the prior art, e.g., by the method allowing identification of the complete or partial regular expressions matching.

[0193] If at least one matching of at least one redirect rule identified at this stage with any of the redirect rules identified at the preliminary stage is detected, the suspicious web resource obtained at step 360 is considered to be part of a multi-step fraudulent Internet scheme. At that, step 380 is completed, and the method proceeds to step 390.

[0194] If no matches have been identified, at this stage the additional checks can be performed for whether one of the web resources that is part of this at least one redirect chain is a known malicious resource.

[0195] This is performed by searching the database containing the list of the known malicious web resources and the redirect graphs' and redirect rules database built at the preliminary stage, as it was described above with respect to Fig. 3A. If any redirect chain contains malicious web resource, such chain is marked as malicious; this information is also saved in the internal data repository 225.

[0196] Those skilled in the art are well aware of other technologies and methods for the detection of the web resources' malicious nature, e.g., by analyzing the URL addresses by the URL masks and the domain names – by key words. The checkups can also be conducted by identifying the fact of the loading by the examined pages of the original websites content, by checking for the presence of the images related to a certain brand (e.g., for names and logos of banks, payment systems, resources, websites, services etc.) or by checking the web resource track record. Such methods and technologies of counteracting phishing, Internet fraudulence and illegal access to the users (webpage visitors or application (including mobile applications) users)' confidential information and, in particular, the methods and technologies for the phishing webpages detection can additionally involve the detection of the domain name registration date (and also of its expiration date). The checkups built on calculation of the hash function values obtained from the webpages and their comparison with the previously calculated values are also known.

[0197] Moreover, at this stage other attributes can be additionally detected too, the same attributes pointing out at the fact that the examined redirect chain is malicious.

[0198] Such attributes are, at least, the following:

- complete or almost complete matching of the examined web resource page text with the text contained in the known malicious web pages; such attributes are identified by performing a search (using any of the commonly known methods) for the examined webpage text in the malicious web pages' text databases prepared beforehand.
- the intermediate web resources properties characteristic of the malicious web resources;
- the length and structure of the URLs used in every redirect chain, including the length and structure of the domain names that are part of the URL.

[0199] For instance, by analyzing the properties of the intermediate web pages (such as web pages 121, 122, 127, 135, 138 etc.), e.g., the geographical location of the servers hosting those pages, it is being determined whether they are the same for different resources. In the process, if it has been determined, e.g., that all the web resources have a substantially different geographical location, e.g., located in different countries and not within one country, the examined redirect chain is suspected to be malicious. The geographical location of a specific server is identified using any commonly known method.

[0200] By analyzing the lengths of the links used for the navigation from one web resource to another and located in one vertex, as well as the lengths of the domain names constituting such links, the cases are identified when the majority of the links have the same or similar length. Such redirect chain is also deemed potentially malicious.

[0201] At that, step 380 is completed, and the method proceeds to step 390.

STEP 390 IN RESPONSE TO THE CORRESPONDENCE WITH AT LEAST ONE KNOWN REDIRECT RULE, AT LEAST ONE TARGET MALICIOUS WEB RESOURCE IS IDENTIFIED WITHIN AT LEAST ONE REDIRECT CHAIN; THE SAID RESOURCE IS BLOCKED AND THE NOTIFICATION IS SENT TO THE USER DEVICE

[0202] If it has been established that the rules implemented by at least one redirect chain conform with at least one known redirect rule, at least one target web resource is identified in it.

[0203] The same actions are performed if no correspondence with the known redirect rules has been detected, but the length of the redirect chain exceeds the preset threshold value, and based on the results of the totality of various checkups described above with regard to step 380 it has been established that at least one web resource in this chain is malicious. This condition corresponds to the case when new, previously unknown multi-stage fraudulent Internet scheme has been detected.

[0204] In one non-limiting example the web checkup for being one of malicious resources can constitute the establishment of the fact that the given web resource contains a suggestion to input the bank card details. In another non-limiting example the criterion of the web resource belonging to the target web resources can constitute the suggestion to append the scanned image of the passport or the driver's license. Such checkups are done using any method known from the prior art, e.g., by analyzing the HTML code of the web resource and by identifying the key words and data input fields in this code that are well known to those skilled in the art.

[0205] A variant of the described method implementation is also possible wherein the determination of the redirect chain ending, i.e., the target web resource detection can be implemented based on the analysis of the HTTP response codes obtained by the browser during the redirect chain construction. For example, when after at least three redirections the system 200 stops receiving HTTP responses containing codes of the 301, 302, 303, 304 or 307 type, it is being recorded that no redirections

are effected from the current webpage and, therefore, the current webpage constitutes the target web resource.

[0206] If at least one target malicious web resource has been identified at step 390, it is blocked and the notification is sent to the user device. These actions are well known to those skilled in the art and can be done using any commonly known method.

[0207] Embodiments of the present technology are known wherein the target malicious web resource blocking measures can be supplemented with at least the following:

- blocking of all the detected intermediary and the target web resources;
- adding all the detected intermediary and the target web resource into the malicious resources databases;
- collecting the body of evidence in support of the web resource fraudulent actions;
- automated investigation of the malicious web resource affiliation;
- effecting a legal impact on the fraudulent web resource, including on its owner, by using the automatically generated claim templates for sending them to the authorized bodies;
- notification of users on the web resource maliciousness through the output warnings and explanatory reports.

[0208] The response measures can differ depending on the target network resource affiliation, its localization, the brand that it's using, the persons whose rights are violated by the fraudulent resource, its subject matter etc.

[0209] All the listed measures have no peculiarities, are well known to those skilled in the art and can be implemented using any commonly known method.

[0210] It should also be noted that upon a target malicious web resource detection a notification or a warning is sent to the user device. This constitutes a message which can also include a report on the analysis and its results.

[0211] With this, the method is completed.

[0212] Fig. 5 shows the general schematic diagram of the computing device 500 providing for the data processing necessary for the implementation of the claimed solution.

[0213] In general, the device 500 comprises such components as: one or more processors 501, at least one memory 502, the data storage means 503, the input/output interfaces 504, the input/output means 505 and the networking means 506.

[0214] The device processor 501 executes main computing operations required for functioning of the device 500 or for providing functionality of one or more of its components. The processor 501 runs the required machine-readable commands contained in the random-access memory 502.

[0215] The memory 502, typically, is in the form of RAM and comprises the necessary program logic ensuring the required functions.

[0216] The data storage means 503 could be in the form of HDD, SSD, RAID, networked storage, flash-memory, optical drives (CD, DVD, MD, Blue-Ray disks), etc. The means 503 provides for a long-term storing of different information, e.g., the above-mentioned files with user data sets, the database comprising records of the time intervals measured for each of the users, the user identifiers, etc.

[0217] Interfaces 504 are the standard means for the connection and operation with the server side, e.g. USB, RS232, RJ45, LPT, COM, HDMI, PS/2, Lightning, FireWire, etc. Selection of interfaces 504 depends on the specific device (600), which could be a personal computer, mainframe, server cluster, thin client, smartphone, laptop, etc.

[0218] Keyboard could be used as data input/output means 505. Besides a keyboard, the input/output means could also include: a joystick, a display (touch-screen display), a projector, a touch pad, a mouse, a trackball, a light pen, loudspeakers, a microphone, etc.

[0219] The networking means 506 are selected from the devices providing the network data reception and transmission, e.g., Ethernet cards, WLAN/Wi-Fi modules, Bluetooth modules, BLE modules, NFC modules, IrDa, GSM modems etc. The means 506 provide for an arrangement of data exchange through the wire based or wireless data communication channel, e.g. WAN, PAN, LAN, Intranet, Internet, WLAN, WMAN or GSM.

[0220] The components of the device 500 are interconnected using the common data bus 510.

[0221] The application materials have presented the preferred embodiment of the claimed technical solution, which shall not be used as limiting the other particular embodiments, which are not beyond the claimed scope of protection and are obvious to persons skilled in the art.

CLAIMS

1. A computer-implementable method for detection of a target malicious web resource, wherein the target web resource is the last webpage in the redirect chain, the webpage configured to accept payments from a visitor, the method 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 behavior of different users and user parameters imitating user environment on different devices 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 different users to the target malicious web resources depending on their user environment and behavior;

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, wherein the target web resource is the last webpage in the redirect chain, the webpage configured to accept payments from a visitor, the method 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 for different users to a target malicious web resource depending on the user environment and behavior;
- 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 1-19.