(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 May 2014 (08.05.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/067424 A1

(51) International Patent Classification:
G06F 11/36 (2006.01)

(21) International Application Number:
PCT/CN2013/085930

(22) International Filing Date:
25 October 2013 (25.10.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201210436204.0 5 November 2012 (05.11.2012) CN

(71) Applicant: **TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED** [CN/CN]; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518044 (CN).

(72) Inventor: **YU, Wenfeng**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen city, Guangdong 518044 (CN).

(74) Agent: **DEQI INTELLECTUAL PROPERTY LAW CORPORATION**; 7/F, Xueyuan International Tower, No. 1 Zhichun Road, Haidian District, Beijing 100083 (CN).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: METHOD AND DEVICE FOR IDENTIFYING ABNORMAL APPLICATION

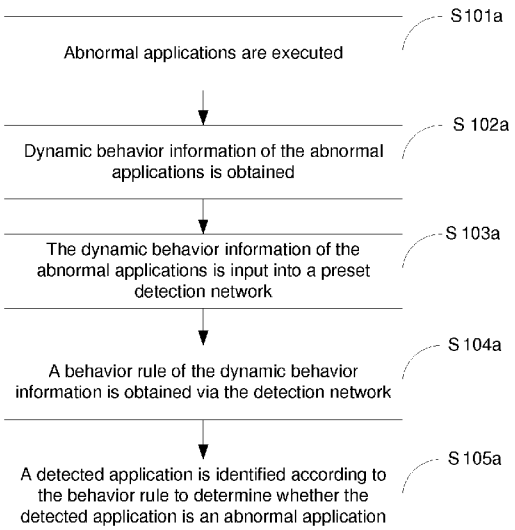

Fig. 1a

(57) Abstract: A method and device for identifying an abnormal application are provided. The method includes: executing abnormal applications; obtaining dynamic behavior information of the abnormal applications; inputting the dynamic behavior information of the abnormal applications into a preset detection network; obtaining a behavior rule of the dynamic behavior information via the detection network; and identifying a detected application according to the behavior rule to determine whether the detected application is an abnormal application. The present disclosure may identify new abnormal applications, such as viruses or Trojans in time and enhance the scanning and killing efficiency of the viruses.

WO 2014/067424 A1

METHOD AND DEVICE FOR IDENTIFYING ABNORMAL APPLICATION

This application claims the benefit of priority from Chinese Patent Application, No. 201210436204.0, entitled "Method and device for identifying and abnormal application" and filed on November 05, 2012, the entire content of which is hereby incorporated by reference.

FIELD OF THE INVENTION

[0001] The present disclosure relates to an Internet field, and more particularly, to a method and device for identifying an abnormal application.

BACKGROUND

[0002] With the growing popularity of the Internet, a high requirement is put forward for a network security performance.

[0003] After a user logs on the Internet using a computer, the computer may be infected by a virus or Trojan for a variety of reasons. In the prior art, there are two methods for identifying the virus or Trojan.

[0004] The first method is a feature scanning method. With this method, if the user finds a new virus, the virus is analyzed, a virus feature is extracted according to characteristics of the virus and the extracted virus feature is added to a virus feature database. In the subsequent virus scanning process, if a suspicious file is found, the suspicious file is compared with virus features in the virus feature database to determine whether the suspicious file is infected by a virus. The weak point of the method is that this method cannot identify an unknown virus. With the increase of types of viruses, especially with the development of polymorphic viruses and hidden viruses, the virus feature database is becoming larger. Apparently, this method cannot satisfy the requirement for rapidly scanning and killing the virus.

[0005] The second method is a human rule behavior heuristic scanning method. With this method, a virus sample is manually analyzed, behavior rules of the virus

sample are summarized and the summarized behavior rules are saved in a database. When the suspicious file is found, runtime behavior of the suspicious file is compared with behavior rules which are stored in advance one by one. If a behavior rule matching with the runtime behavior of the suspicious file is found, suspicious file is determined as the virus. The method may identify some unknown viruses. With the continuing development of the viruses, new viruses appear continuously and virus behavior also changes. The method for manually analyzing and summarizing the virus behavior is inefficient and cannot satisfy the requirement for scanning and killing the viruses.

[0006] In summary, one of technical problems needed to be solved is identifying new viruses in time, enhancing scanning and killing efficiency of the viruses.

SUMMARY

[0007] The present disclosure provides a method for identifying an abnormal program to identify new viruses in time and enhance scanning and killing efficiency of the viruses.

[0008] In order to achieve the above technical effect, the present disclosure provides a method for identifying an abnormal application, including:

executing abnormal applications;

obtaining dynamic behavior information of the abnormal applications;

inputting the dynamic behavior information of the abnormal applications into a preset detection network;

obtaining a behavior rule of the dynamic behavior information via the detection network; and

identifying a detected application according to the behavior rule to determine whether the detected application is an abnormal application.

[0009] In an example of the present disclosure, before executing the abnormal applications, the method further includes:

presetting the detection network.

[0010] In an example of the present disclosure, the method for inputting the dynamic behavior information of the abnormal applications into the preset detection network includes:

converting the dynamic behavior information of the abnormal applications into a behavior vector; and

inputting the behavior vector into the detection network.

[0011] In an example of the present disclosure, before executing the abnormal applications, the method further includes:

establishing a dynamic behavior information monitoring point; and

obtaining the dynamic behavior information of the abnormal applications via the dynamic behavior information monitoring point.

[0012] In an example of the present disclosure, the detection network is a back propagation network.

[0013] The present disclosure provides a device for identifying an abnormal program to identify new viruses in time and enhance scanning and killing efficiency of the viruses.

[0014] In order to achieve the above technical effect, the present disclosure provides a device for identifying an abnormal application. The device includes:

a dynamic behavior information obtaining module, to execute abnormal applications and obtain dynamic behavior information of the abnormal applications;

a dynamic behavior information transmission module, to input the dynamic behavior information of the abnormal applications into a preset detection network;

a behavior rule obtaining module, to obtain a behavior rule of the dynamic behavior information via the detection network; and

an identification module, to identify a detected application according to the behavior rule to determine whether the detected application is an abnormal application.

[0015] In an example of the present disclosure, the device further includes: a detection network generation module, to preset the detection network.

[0016] In an example of the present disclosure, the device further includes: a behavior vector conversion module, to convert the dynamic behavior information of the abnormal applications into a behavior vector. The dynamic behavior information transmission module is further to input the behavior vector into the detection network.

[0017] In an example of the present disclosure, the device further includes a monitoring point establishment module, to establish a dynamic behavior information monitoring point. The dynamic behavior information obtaining module is further to obtain the dynamic behavior information of the abnormal applications via the dynamic behavior information monitoring point.

[0018] In an example of the present disclosure, the detection network is a back

propagation network.

[0019] The present disclosure further provides a non-transitory computer-readable medium storing instructions which, when executed by one or more processors, cause a device to perform a method for identifying an abnormal application. The method includes:

executing abnormal applications;

obtaining dynamic behavior information of the abnormal applications;

inputting the dynamic behavior information of the abnormal applications into a preset detection network;

obtaining a behavior rule of the dynamic behavior information via the detection network;

identifying a detected application according to the behavior rule to determine whether the detected application is an abnormal application.

[0020] Compared with the conventional method, in the present disclosure, a detection network is established in advance, stored abnormal applications are executed, the dynamic behavior information of the abnormal applications is obtained, the obtained dynamic behavior information is input into the detection network, the behavior rule for obtaining the abnormal applications is summarized by the detection network and other abnormal applications are identified according to the behavior rule. Apparently, the present disclosure may identify the new viruses in time and enhance the scanning and killing efficiency of the viruses.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] Figure 1a is a flow chart illustrating a method for identifying an abnormal application in accordance with example of the present disclosure;

[0022] Figure 1 is a flow chart illustrating another method for identifying an abnormal application in accordance with an example of the present disclosure;

[0023] Figure 2 is a schematic diagram illustrating a model of a detection network in accordance with an example of the present disclosure; and

[0024] Figure 3 is a schematic diagram illustrating a device for identifying an abnormal application in accordance with an example of the present disclosure.

DETAILED DESCRIPTION

[0025] For simplicity and illustrative purposes, the present disclosure is described by referring to examples. In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present disclosure. It will be readily apparent however, that the present disclosure may be practiced without limitation to these specific details. In other instances, some methods and structures have not been described in detail so as not to unnecessarily obscure the present disclosure. As used throughout the present disclosure, the term “includes” means includes but not limited to, the term “including” means including but not limited to. The term “based on” means based at least in part on. In addition, the terms “a” and “an” are intended to denote at least one of a particular element.

[0026] Referring to figure 1a, figure 1a is a flow chart illustrating a method for identifying an abnormal application in accordance with example of the present disclosure. The method includes the following blocks.

[0027] In block 101a, abnormal applications are executed.

[0028] In the present disclosure, in general, the abnormal applications are dangerous applications, such as the viruses and Trojans affecting the normal operation of the computer.

[0029] In block 102a, dynamic behavior information of the abnormal applications is obtained.

[0030] In block 103a, the dynamic behavior information of the abnormal applications is input into a preset detection network.

[0031] In block 104a, a behavior rule of the dynamic behavior information is obtained via the detection network.

[0032] In block 105a, a detected application is identified according to the behavior rule to determine whether the detected application is an abnormal application.

[0033] Referring to figure 1, figure 1 is a flow chart illustrating another method for identifying an abnormal application in accordance with example of the present

disclosure.

[0034] In block S101, a detection network is preset.

[0035] The detection network provided by the present disclosure may be a Back Propagation (BP) neural network. The BP neural network is a multi-layer feed-forward network trained according to an error back propagation algorithm. The BP neural network learns and stores a large number of input/output mode mapping relationships and needs not to real mathematical equations describing the above mapping relationships in advance.

[0036] In block S102, stored abnormal applications are executed and dynamic behavior information of the abnormal applications is obtained.

[0037] For example, the abnormal applications may be a virus or a Trojan program and may be an improper program affecting the usage of the computer or the terminal device. The abnormal applications are not listed here.

[0038] In practice, the stored abnormal applications may be executed on a virtual machine and the dynamic behavior information of the abnormal applications is obtained via a pre-established behavior monitoring point. For example, a danger registry operation monitoring point, a sensitive file operation monitoring point, a network connection monitoring point or Application Programming Interface (API) call monitoring point, etc. may be established on the virtual machine, which is described in detail hereinafter.

[0039] In block S103, the obtained dynamic behavior information is converted into a behavior vector and the behavior vector is input into the preset detection network.

[0040] In practice, a behavior vector mapping rule is established in the present disclosure in advance and the obtained dynamic behavior information is mapped into the behavior vector.

[0041] Whether an operation is performed on a danger registry is determined. If an operation is performed on the danger registry, the result is 1; otherwise, the result is 0.

[0042] Whether an operation is performed on a sensitive file is determined. If an

operation is performed on the sensitive file, the result is 1; otherwise, the result is 0.

[0043] Whether a dangerous operation is performed on network connection is determined. If a dangerous operation is performed on the network connection, the result is 1; otherwise, the result is 0.

[0044] Whether an operation is performed on API (1) is determined. If an operation is performed on API (1), the result is 1; otherwise, the result is 0.

[0045] Whether an operation is performed on API (2) is determined. If an operation is performed on API (2), the result is 1; otherwise, the result is 0.

[0046] A result output vector {0, 1, 0, 1, 1.....} representing the dynamic behavior information is generated.

[0047] The input of the detection network is the behavior vector and the output of the detection network is the result output vector. The result output vector denotes whether the scanned application is in danger, 1 represents that the scanned application is not in danger and 0 represents that the scanned application is in danger.

[0048] An example is given hereinafter taking the detection network as the BP neural network for example. The process for converting the obtained dynamic behavior information into the behavior vector is as follows. Assume that an expression of the BP neural network is y=f(x), x represents the input behavior vector and y represents the result output vector. The result that y equals to 1 represents normal (the result that y equals to 1 or y is closing to 1 is determined as normal). The result that y equals to 0 represents abnormal (The result that y equals to 0 or y is closing to 0 is determined as abnormal). There is a behavior vector, in which x equals to {1, 1, 0, 1, 0, 1, 0, 1...} and the behavior vector belongs to abnormal (yd equals to 0 and yd represents a wished result value). The value x is input into the BP neural network and the output is yc (yc represents an actual output value). A difference square operation ((yd-yc)^2) is performed on yd and yc. Whether the result is less than a threshold value a is determined. If the result is less than a, a weight of each node in the BP neural network needs to be fed back and adjusted. If the result is larger than a, the

weight of each node in the BP neural network needs to be fed back and adjusted, until (yd-yc)^2<a.

[0049] An appropriate range of weight adjustment learning rate of the BP neural network is 0.3 to 5.0. An appropriate range of momentum learning rate is 1.0 to 1.5. An appropriate range of error limit is less than or equal to 0.0001. The error calculated using an average value of the difference square is (yd-yc)^2)/m, (yd-yc)^2)/m< 0.0001, yd represents the wished output value, yc represents the actual output value, m represents number of output layer neurons and m equals to 1.

[0050] In block S104, the behavior rule of the behavior vector is obtained via the detection network.

[0051] In block S105, the detected abnormal application is identified with the behavior rule obtained via the detection network.

[0052] In practice, the present disclosure adopts two kinds of application samples. One kind includes completely abnormal applications and the other kind includes completely normal applications. The completely abnormal applications include different types of abnormal applications. The different types of abnormal applications are executed one by one. The dynamic behavior information of the abnormal applications is obtained via an established monitoring point, the obtained dynamic behavior information is converted into the corresponding behavior vector and the converted behavior vector is input into the pre-set detection network to perform the feedback training.

[0053] Then, the completely normal applications are selected and the completely normal applications are executed one by one. The dynamic behavior information of the normal applications are obtained via the established monitoring point, the obtained dynamic behavior information is converted into the corresponding behavior vector and the converted behavior vector is input into the preset detection network to perform the feedback training. In the present disclosure, the completely normal applications are executed, other applications are detected according to the execution result, by which misidentification may be avoided.

[0054] Follow on to the description in block S102, behavior monitoring points in

the present disclosure are classified into four types.

[0055] The first one is danger registry operation monitoring point. That is, a danger registry is established in a database file in advance and registries in which danger may probably exist are defined as the danger registries. Then, the detected application is executed by a virtual machine, an operation registry of the detected application is obtained, the operation registry is matched with the danger registries in the database file and whether there is a danger registry matching with the operation registry of the detected application is determined. If there is a danger registry matching with the operation registry, the result output vector is 1; otherwise, the result output vector is 0.

[0056] The second one is a sensitive file operation monitoring point. That is, a sensitive file table is established in the database file in advance, filenames of sensitive files in which danger may exist and paths of the sensitive files are stored in the sensitive file table. The detected application is executed via the virtual machine, an operation file entry of the detected application is obtained, the operation file entry is matched with the sensitive file table in the database file and whether there is a filename or path of the sensitive file matching with the operation file entry of the detected application is determined. If there is a filename or path of the sensitive file matching with the operation file entry, the result output vector is 1; otherwise, the result output vector is 0.

[0057] The third one is network connection monitoring point. That is, a danger Uniform Resource Location (URL) and IP table is established in the database file. (URL)s and (IP)s, in which danger may exist are stored in the danger URL and IP table. Then, the detected application is executed by the virtual machine, the network connection information of the detected application is obtained and whether there is network connection information in the URL and IP table is determined. If there is network connection information in the URL and IP table, the result output vector is 1; otherwise, the result output vector is 0.

[0058] The fourth one is system API call monitoring point. That is, a system API call table is stored in the database file in advance. Then, the detected application is executed by the virtual machine and the situation of called system (API)s of the detected application is obtained. As shown in the following table, an entry

corresponding to a called system API is configured as 1 and an entry corresponding to the system API which is not called is configured as 0.

API 1 (FindWindow)	1
API 2 (CreateProcess)	0
API 3 (WriteProcessMemory)	1
.....	....

[0059] The detection network provided by the present disclosure, such as the BP neural network, includes an input layer, an intermediate layer and an output layer. The number of neurons of the input layer is 1003. Each of the danger registry operation monitoring point, the sensitive file operation monitoring point and the network connection monitoring point occupies 3 neurons. The system API call monitoring point occupies 1000 input neurons. The intermediate layer includes a first intermediate layer and a second intermediate layer. The number of neurons of the first intermediate layer is 60000 and the number of the neurons of the second intermediate layer is 60000. When the output value of the output layer is closing to 1 or equals to 1, the detected application is normal. When the output value of the output layer is closing to 0 or equals to 0, the detected application is abnormal.

[0060] Referring to figure 2, figure 2 is a schematic diagram illustrating a model of a detection network in accordance with an example of the present disclosure. In practice, in the detection network, formulas (1) and (2) are taken as activation functions (called activation functions) of the model of the detection network.

[0061] The activation function: $y=1/(1+\exp(-x))$ （1）

[0062] A function obtained by taking a derivative of the activation function: $y=1.0/(\exp(x)*\text{pow}((1.0/\exp(x)+1),2.0))$（2）.

[0063] Referring to the following table

Engine	Scanning number	Detection number	Detection rate

Feature scanning method	5000	1247	24.9%
human rule behavior heuristic scanning method	5000	1375	27.5%
BP neural network engine	5000	1487	29.7%

[0064] According to an example of the present disclosure, 5000 mixed samples are randomly extracted from an application sample database and comparison test scanning is performed on the 5000 mixed samples. Apparently, the detection rate on the basis of the detection network (BP neural network) is higher than any of the detection rates on the basis of the feature scanning method and the human rule behavior heuristic scanning method in the conventional method.

[0065] Referring to figure 3, figure 3 is a schematic diagram illustrating another device for identifying an abnormal application in accordance with an example of the present disclosure. The device for identifying an abnormal application includes a detection network generation module 31, a monitoring point establishment module 32, a dynamic behavior information obtaining module 33, a behavior vector conversion module 34, a dynamic behavior information transmission module 35, a behavior rule obtaining module 36 and an identification module 37.

[0066] The detection network generation module 31 is to generate a detection network in advance. The detection network is a back propagation network. The monitoring point establishment module 32 is to establish a dynamic behavior information monitoring point. For example, a danger registry operation monitoring point, a sensitive file operation monitoring point, a network connection monitoring point or an API call monitoring point, etc. may be established on the virtual machine.

[0067] The dynamic behavior information obtaining module 33 is to execute stored abnormal applications and obtain the dynamic behavior information of the abnormal applications via the dynamic behavior information monitoring point.

[0068] The behavior vector conversion module 34 is to convert the dynamic behavior information of the abnormal applications into a behavior vector. The dynamic behavior information transmission module 35 is to input the behavior vector into the detection network, i.e. input the obtained dynamic behavior information of the obtained abnormal applications into the preset detection network.

[0069] The behavior rule obtaining module 35 is to obtain the behavior rule of the dynamic behavior information via the detection network. The identification module 36 is to identify a detected application according to the obtained behavior rule to determine whether the detected application is an abnormal application.

[0070] The working process of the device for identifying the abnormal application may be obtained by referring to the detailed description of the method for identifying the abnormal application, which is not repeated here.

[0071] In the present disclosure, a detection network is established in advance, stored abnormal applications are executed, the dynamic behavior information of the abnormal applications is obtained, the obtained dynamic behavior information is input into the detection network, the detection network summarizes the behavior rule for obtaining the abnormal applications and other abnormal applications are identified according to the behavior rule. Apparently, the present disclosure may identify the new viruses in time and enhance the scanning and killing efficiency of the viruses.

[0072] The foregoing only describes preferred embodiments of the present invention. The protection scope of the present invention, however, is not limited to the above description. Any change or substitution, easily occurring to those skilled in the art, should be covered by the protection scope of the present invention.

WHAT IS CLAIMED IS:

1. A method for identifying an abnormal application, comprising:

executing abnormal applications;

obtaining dynamic behavior information of the abnormal applications;

inputting the dynamic behavior information of the abnormal applications into a preset detection network;

obtaining a behavior rule of the dynamic behavior information via the detection network; and

identifying a detected application according to the behavior rule to determine whether the detected application is an abnormal application.

2. The method for identifying an abnormal application according to claim 1, wherein before executing the abnormal applications, the method further comprises:

presetting the detection network.

3. The method for identifying an abnormal application according to claim 1, wherein inputting the dynamic behavior information of the abnormal applications into the preset detection network comprises:

converting the dynamic behavior information of the abnormal applications into a behavior vector; and

inputting the behavior vector into the detection network.

4. The method for identifying an abnormal application according to claim 1, wherein before executing the abnormal applications, the method further comprises:

establishing a dynamic behavior information monitoring point; and

obtaining the dynamic behavior information of the abnormal applications via the dynamic behavior information monitoring point.

5. The method for identifying an abnormal application according to claim 1,

wherein the detection network is a back propagation network.

6. A device for identifying an abnormal application, comprising:

a dynamic behavior information obtaining module, to execute abnormal applications and obtain dynamic behavior information of the abnormal applications;

a dynamic behavior information transmission module, to input the dynamic behavior information of the abnormal applications into a preset detection network;

a behavior rule obtaining module, to obtain a behavior rule of the dynamic behavior information via the detection network; and

an identification module, to identify a detected application according to the behavior rule to determine whether the detected application is an abnormal application.

7. The device for identifying an abnormal application, further comprising:

a detection network generation module, to preset the detection network.

8. The device for identifying an abnormal application, further comprising:

a behavior vector conversion module, to convert the dynamic behavior information of the abnormal applications into a behavior vector; wherein

the dynamic behavior information transmission module is further to input the behavior vector into the detection network.

9. The device for identifying an abnormal application according to claim 6, further comprising:

a monitoring point establishment module, to establish a dynamic behavior information monitoring point; wherein

the dynamic behavior information obtaining module is further to obtain the dynamic behavior information of the abnormal applications via the dynamic behavior information monitoring point.

10. The device for identifying an abnormal application according to claim 6, wherein the detection network is a back propagation network.

11. A non-transitory computer-readable medium storing instructions which, when executed by one or more processors, cause a device to perform a method for identifying an abnormal application, the method comprising:

executing abnormal applications;

obtaining dynamic behavior information of the abnormal applications;

inputting the dynamic behavior information of the abnormal applications into a preset detection network;

obtaining a behavior rule of the dynamic behavior information via the detection network;

identifying a detected application according to the behavior rule to determine whether the detected application is an abnormal application.

12. The non-transitory computer-readable medium according to claim 11, wherein the non-transitory computer-readable medium further stores instructions which, when executed by one or more processors, cause a device to

preset the detection network before executing the abnormal applications.

13. The non-transitory computer-readable medium according to claim 11, wherein the non-transitory computer-readable medium further stores instructions which, when executed by one or more processors, cause a device to input the dynamic behavior information of the abnormal applications into the preset detection network by:

converting the dynamic behavior information of the abnormal applications into a behavior vector; and

inputting the behavior vector into the detection network.

14. The non-transitory computer-readable medium according to claim 11, wherein the non-transitory computer-readable medium further stores instructions which, when executed by one or more processors, cause a device to

establish a dynamic behavior information monitoring point before executing the abnormal applications; and

obtain the dynamic behavior information of the abnormal applications via the

dynamic behavior information monitoring point.

15. The non-transitory computer-readable medium according to claim 11, wherein the detection network is a back propagation network.

5

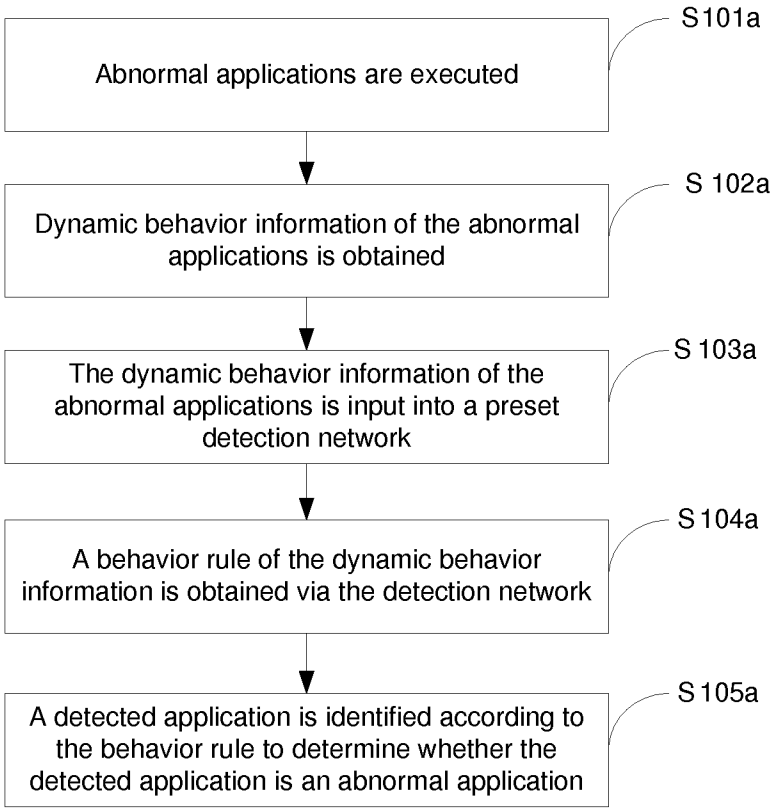
Abnormal applications are executed
S101a
Dynamic behavior information of the abnormal applications is obtained
S 102a
The dynamic behavior information of the abnormal applications is input into a preset detection network
S 103a
A behavior rule of the dynamic behavior information is obtained via the detection network
S 104a
A detected application is identified according to the behavior rule to determine whether the detected application is an abnormal application
S 105a

Fig. 1a

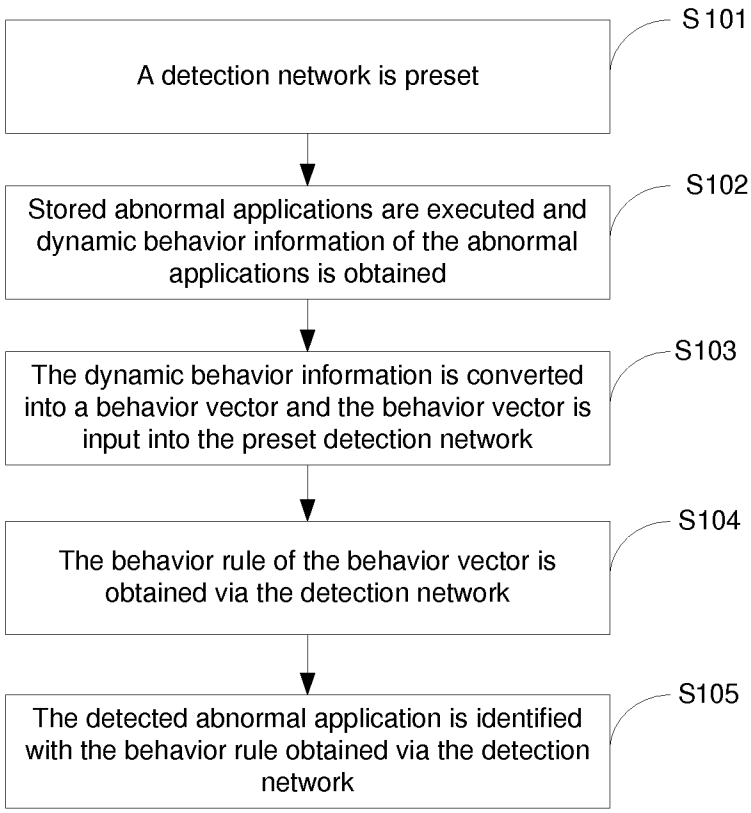
A detection network is preset
S 101
Stored abnormal applications are executed and dynamic behavior information of the abnormal applications is obtained
S102
The dynamic behavior information is converted into a behavior vector and the behavior vector is input into the preset detection network
S103
The behavior rule of the behavior vector is obtained via the detection network
S104
The detected abnormal application is identified with the behavior rule obtained via the detection network
S105

Fig. 1

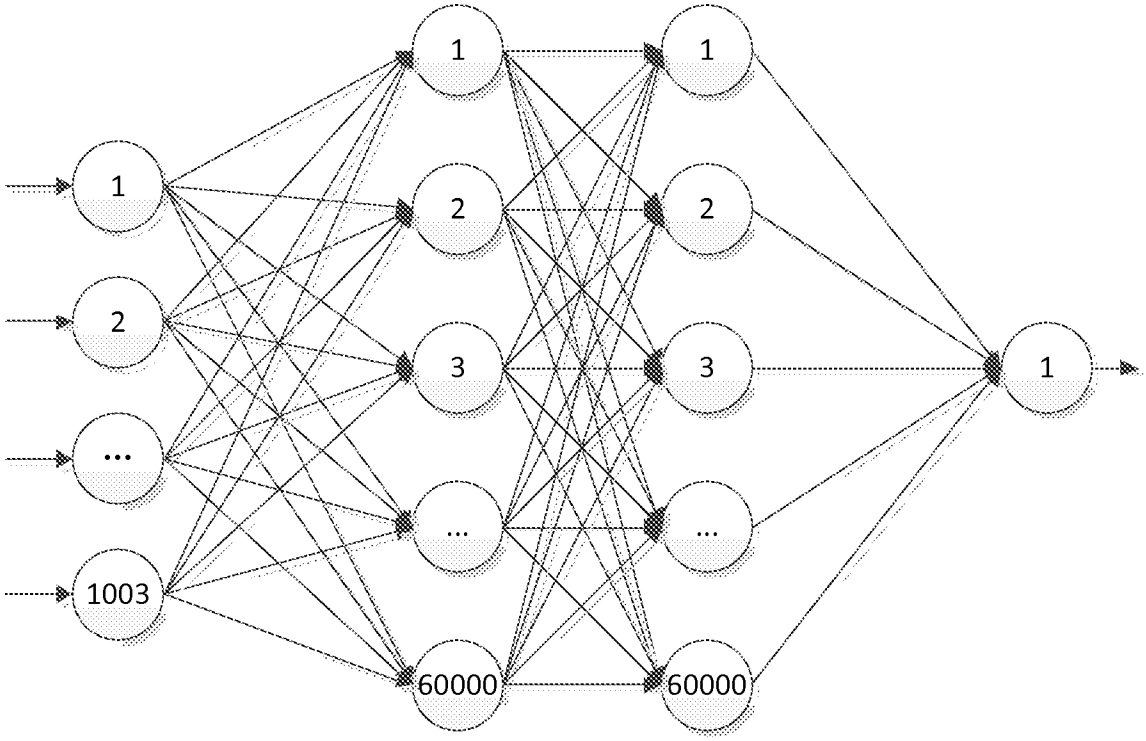
1
2
...
1003
1
2
3
...
60000
1
2
3
...
60000
1

Fig. 2

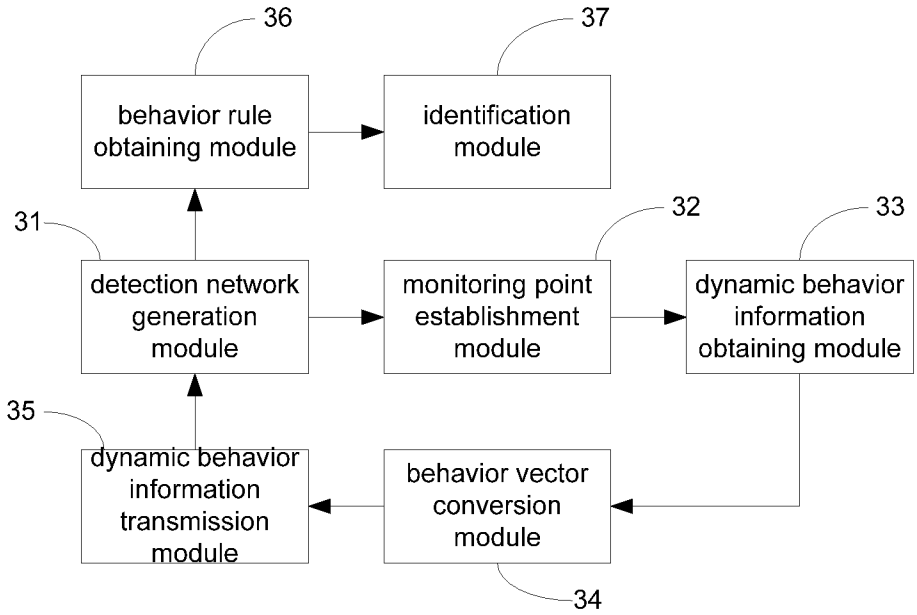
36
37
behavior rule obtaining module
identification module
31
32
33
detection network generation module
monitoring point establishment module
dynamic behavior information obtaining module
35
dynamic behavior information transmission module
behavior vector conversion module
34

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/085930

A. CLASSIFICATION OF SUBJECT MATTER

G06F 11/36 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CPRSABS, CNKI, DWPI, SIPOABS: program, application, software, behavior, action, rule, vector, neural network, BPNN

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102508768 A (QIZHI SOFTWARE BEIJING CO., LTD.) 20 June 2012 (20.06.2012) claims 1-6	1-15
X	CN 102034042 A (UNIV SICHUAN) 27 April 2011(27.04.2011) claim 1	1-15

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 December 2013(25.12.2013)	**23 Jan. 2014 (23.01.2014)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer KANG, Jian Telephone No. (86-10)62411639

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/085930

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102508768 A	20.06.2012	None	
CN 102034042 A	27.04.2011	CN 102034042 B	03.10.2012