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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 March 2014 (13.03.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/036888 A1

(51) International Patent Classification:
G06F 21/56 (2013.01) *G06F 17/30* (2006.01)

(21) International Application Number:
PCT/CN2013/081901

(22) International Filing Date:
20 August 2013 (20.08.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201210330224.X 7 September 2012 (07.09.2012) 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) Inventors: **YAO, Tingguang**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518044 (CN). **LU, Zhaohua**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518044 (CN). **ZHENG, Huijuan**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518044 (CN).

(74) Agent: **ADVANCE CHINA I.P.LAW OFFICE**; Suite 918-920, Dongshan Plaza, No.69 Xianlie Central Road, Guangzhou, Guangdong 510095 (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, 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, DEVICE, AND SYSTEM FOR PROCESSING VIRUS-INFECTED APPLICATIONS

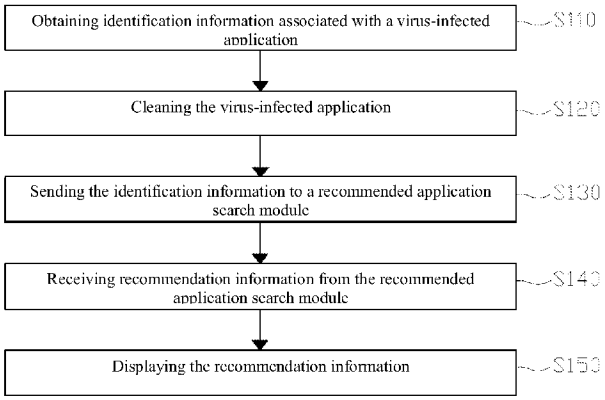

FIG. 1

(57) Abstract: The present disclosure relates to a virus-infected application processing method. The method comprises: obtaining identification information associated with a virus-infected application; cleaning the virus-infected application; sending the identification information to a recommended application search module; receiving recommendation information from the recommended application search module, the recommendation information comprising introduction to one or more applications relevant to the virus-infected application; and displaying the recommendation information. According to the virus-infected application processing method, relevant applications are recommended to a user at the same time as the virus-infected application is cleaned, thereby allowing the user to easily install a same but virus-free application or a similar substitute application. The entire operational process is simple and convenient, and can effectively make up for the functional loss due to the cleaning of the virus-infected application. In addition, the present disclosure provides a virus-infected application processing device.

WO 2014/036888 A1

METHOD, DEVICE, AND SYSTEM FOR PROCESSING VIRUS-INFECTED APPLICATIONS

Description

Cross Reference to Related Application

[0001] This application claims the priority benefit of Chinese Patent Application No. 201210330224.X, filed September 7, 2012, the contents of which are incorporated by reference herein in their entirety for all purposes.

Technical Field

[0002] The present disclosure relates generally to the antivirus technological field, and more particularly, to a method, device, and system for processing virus-infected applications.

Background

[0003] In most virus-infected mobile phone applications, the application program itself and the virus program are packaged together. As a result, in order to clean the virus, the virus-infected application needs to be uninstalled as well. This causes certain loss to user functionalities, and the user needs to download a same or similar substitute application. Not only is the operation cumbersome, it is also possible that the user may download a virus-infected application again when downloading the application.

Summary of the Disclosure

[0004] There is a need for a method, device, and system for processing virus-infected applications. The method, device, and system disclosed herein can recommend to a user one or more relevant applications when cleaning a virus-infected application, thereby allowing the user to easily install a same but virus-free application or a similar substitute application.

[0005] A virus-infected application processing method comprises: obtaining identification information associated with a virus-infected application; cleaning the virus-infected application; sending the identification information to a recommended application search module; receiving recommendation information from the recommended application search module, wherein the

recommendation information comprises introduction to one or more applications relevant to the virus-infected application; and displaying the recommendation information.

[0006] A virus-infected application processing device comprises: an identification information obtaining module that obtains identification information associated with a virus-infected application; an infected application cleaning module that cleans the virus-infected application; an identification information sending module that sends the identification information to a recommended application search module; a recommendation information receiving module that receives recommendation information from the recommended application search module, wherein the recommendation information comprises introduction to one or more applications relevant to the virus-infected application; and a recommendation information display module that displays the recommendation information.

[0007] A virus-infected application processing system comprises a processing device and an application recommending server, wherein the processing device comprises: an identification information obtaining module that obtains identification information associated with a virus-infected application; an infected application cleaning module that cleans the virus-infected application; an identification information sending module that sends the identification information to the application recommending server, the application recommending server comprises: a recommended application search module that receives the identification information from the processing device, searches relevant applications based on the received identification information, generates corresponding recommendation information and sends the generated recommendation information to the processing device, wherein the recommendation information comprises introduction to one or more applications relevant to the virus-infected application, and the processing device further comprises: a recommendation information receiving module that receives the recommendation information from the recommended application search module; and a recommendation information display module that displays the recommendation information.

[0008] According to the method and in the device and system for processing a virus-infected application, relevant applications are recommended to a user at the same time as the virus-infected application is cleaned, thereby allowing the user to easily install a same but virus-free application or a similar substitute application. The entire operational process is simple and convenient, and can effectively make up for the functional loss due to the cleaning of the virus-infected application.

Brief Description of the Drawings

[0009] FIG. 1 is a schematic diagram illustrating an example of the flow of a virus-infected application processing method according to various embodiments.

[0010] FIG. 2 is a schematic diagram illustrating an example of the flow of a method of searching relevant applications executed by a recommended application search module according to various embodiments.

[0011] FIG. 3 is a schematic diagram illustrating an example of an arrangement of a virus-infected application processing device according to various embodiments.

[0012] FIG. 4 is a schematic diagram illustrating an example of an arrangement of a virus-infected application processing system according to various embodiments.

Detailed Description

[0013] In the following description of embodiments, reference is made to the accompanying drawings which form a part hereof, and in which it is shown by way of illustration specific embodiments of the disclosure that can be practiced. It is to be understood that other embodiments can be used and structural changes can be made without departing from the scope of the disclosed embodiments.

[0014] FIG. 1 is a schematic diagram illustrating an example of the flow of a virus-infected application processing method according to various embodiments. The method can be executed by an electronic device such as a computer, a smartphone, or a tablet PC, etc. According to some embodiments, the method can be executed by a mobile terminal. A mobile terminal can be a mobile phone, a tablet PC, a media player, etc. Examples of mobile terminals that can be used in accordance with various embodiments include, but are not limited to, a tablet PC (including, but not limited to, Apple iPad and other touch-screen devices running Apple iOS, Microsoft Surface and other touch-screen devices running the Windows operating system, and tablet devices running the Android operating system), a mobile phone, a smartphone (including, but not limited to, an Apple iPhone, a Windows Phone and other smartphones running Windows Mobile or Pocket PC operating systems, and smartphones running the Android operating system, the Blackberry operating system, or the Symbian operating system), an e-reader (including, but not limited to, Amazon Kindle and Barnes & Noble Nook), a laptop computer (including, but not limited to, computers running Apple Mac operating system, Windows operating system, Android operating system and/or Google Chrome

operating system), a media player (including, but not limited to, Apple iPod and Microsoft Zoom), or an on-vehicle device running any of the above-mentioned operating systems or any other operating systems, , or any other mobile Internet device ("MID") or intelligent communication terminal, all of which are well known to those skilled in the art. As illustrated in FIG. 1, the virus-infected application processing method can comprise the following steps:

[0015] Step S110: obtaining identification information associated with a virus-infected application. According to some embodiments, the virus-infected application can be identified by antivirus software. According to these embodiments, the identification information associated with the virus-infected application can be obtained after the antivirus software identifies the virus-infected application. Examples of such identification information include, but are not limited to, a name and version of the virus-infected application, a program package name, a certificate, or a feature code, such as a message-digest algorithm 5 ("MD5") feature code.

[0016] Step S120: cleaning the virus-infected application. According to some embodiments, cleaning the virus-infected application comprises completely uninstalling the virus-infected application. This is a common method of cleaning a virus-infected application in the antivirus field, and the method is well known to those skilled in the art.

[0017] Step S130: sending the identification information to a recommended application search module. According to some embodiments, the recommended application search module can be installed locally, e.g., in the same device in which the virus-infected application was installed. For example, the recommended application search module can be a functional module of antivirus software. According to some other embodiments, the recommended application search module can be installed in a remote server. According to some embodiments, the recommended application search module can searches in an application library for applications relevant to the virus-infected application and generate recommendation information based on one or more found applications. According to some embodiments, the application library can be stored in a remote server. Therefore, regardless of whether the recommended application search module is installed locally or remotely, it can search data in an application library stored in a remote server.

[0018] FIG. 2 is a schematic diagram illustrating an example of the flow of a method of searching relevant applications executed by a recommended application search module according to various embodiments. As illustrated in FIG. 2, the method can comprise:

[0019] Step S131: searching one or more applications with same application name, same program package name, and same certificate as the virus-infected application.

[0020] Step S132: searching one or more applications with same application name and same program package name as the virus-infected application if no application with same application name, same program package name, and same certificate as the virus-infected application is found.

[0021] Step S133: searching one or more applications of a same type as the virus-infected application and filtering found applications based on the applications' rating or downloads if no application with same application name and same program package name as the virus-infected application is found.

[0022] The inclusion of a process of certificate verification in Step S131 ensures that any found application and the virus-infected application are published by the same person or organization. Therefore, the searching criteria pursuant to Step S131 are the strictest. Compared to Step S131, Step S132 does not include the process of certificate verification, but because it includes a process of verifying application name and program package name, it can find most repackaged applications. Step S133 can provide a user with even more choices because it can find some most popular applications (e.g., those with the highest ratings or the most downloads) based on the type of the virus-infected application and filtering of applications of the same type as the virus-infected application based on the applications' rating or downloads.

[0023] According to some embodiments, Steps S131-S133 can proceed as illustrated in FIG. 2, and different numbers of recommended applications can be provided for a user to select based on the user's selection along each step. Those skilled in the art can readily appreciate that a process of searching relevant applications is not limited to the one illustrated in FIG.2. For example, part but not all of Steps S131-S133 can be adopted. According to some embodiments, other identification information such as one or more feature codes can be used for searching and verification.

[0024] After one or more relevant applications are found, the recommended application search module can generate recommendation information based on the one or more found applications and return the recommendation information. Examples of recommendation information include but are not limited to introduction to applications relevant to the virus-infected application and their download links.

[0025] Step S140: receiving recommendation information from the recommended application search module. According to the embodiments where the recommended application search module is installed locally, the recommendation information can be transmitted within a process or between processes. According to the embodiments where the recommended application search module is installed in a remote server, the recommendation information can be transmitted via a network.

[0026] Step S150: displaying the recommendation information. According to some embodiments, the recommendation information can be displayed in the form of a list to introduce the recommended applications. According to some embodiments, relevant applications can be automatically downloaded and installed after a user clicks a relevant link or button.

[0027] According to the above described virus-infected application processing method, relevant applications are recommended to a user at the same time as the virus-infected application is cleaned, thereby allowing the user to easily install a same but virus-free application or a similar substitute application. The entire operational process is simple and convenient, and can effectively make up for the functional loss due to the cleaning of the virus-infected application.

[0028] As illustrated in FIG. 3, a virus-infected application processing device 200 can comprise: an identification information obtaining module 210, an infected application cleaning module 220, an identification information sending module 230, a recommendation information receiving module 240, and a recommendation information display module 250.

[0029] The identification information obtaining module 210 obtains identification information associated with a virus-infected application. According to some embodiments, the virus-infected application can be identified by antivirus software. According to these embodiments, the identification information associated with the virus-infected application can be obtained after the antivirus software identifies the virus-infected application. Examples of such identification information include, but are not limited to, a name and version of the virus-infected application, a program package name, a certificate, or a feature code, such as a MD5 feature code.

[0030] The infected application cleaning module 220 cleans the virus-infected application. According to some embodiments, cleaning the virus-infected application comprises completely uninstalling the virus-infected application. This is a common method of cleaning a virus-infected application in the antivirus field, and the method is well known to those skilled in the art.

[0031] The identification information sending module 230 sends the identification information to a recommended application search module. According to some embodiments, the recommended application search module can be installed locally, e.g., in the same device in which the virus-infected application was installed. For example, the recommended application search module can be a functional module of antivirus software. According to some other embodiments, the recommended application search module can be installed in a remote server. According to some embodiments, the recommended application search module searches in an application library for applications relevant to the virus-infected application and generates recommendation information

based on one or more found applications. According to some embodiments, the application library can be stored in a remote server. Therefore, regardless of whether the recommended application search module is installed locally or remotely, it can search data in an application library stored in a remote server.

[0032] FIG. 2 is a schematic diagram illustrating an example of the flow of a method of searching relevant applications executed by the recommended application search module according to various embodiments. As illustrated in FIG. 2, the method can comprise:

[0033] Step S131: searching one or more applications with same application name, same program package name, and same certificate as the virus-infected application.

[0034] Step S132: searching one or more applications with same application name and same program package name as the virus-infected application if no application with same application name, same program package name, and same certificate as the virus-infected application is found.

[0035] Step S133: searching one or more applications of a same type as the virus-infected application and filtering found applications based on the applications' rating or downloads if no application with same application name and same program package name as the virus-infected application is found.

[0036] The inclusion of a process of certificate verification in Step S131 ensures that any found application and the virus-infected application are published by the same person or organization. Therefore, the searching criteria pursuant to Step S131 are the strictest. Compared to Step S131, Step S132 does not include the process of certificate verification, but because it includes a process of verifying application name and program package name, it can find most repackaged applications. Step S133 can provide a user with even more choices because it can find some most popular applications (e.g., those with the highest ratings or the most downloads) based on the type of the virus-infected application and filtering of applications of the same type as the virus-infected application based on the applications' rating or downloads.

[0037] According to some embodiments, Steps S131-S133 can proceed as illustrated in FIG. 2, and different numbers of recommended applications can be provided for a user to select based on the user's selection along each step. Those skilled in the art can readily appreciate that a process of searching relevant applications is not limited to the one illustrated in FIG.2. For example, part but not all of Steps S131-S133 can be adopted. According to some embodiments, other identification information such as one or more feature codes can be used for searching and verification.

[0038] After one or more relevant applications are found, the recommended application search module can generate recommendation information based on one or more found applications and return the recommendation information. Examples of recommendation information include but are not limited to introduction to applications relevant to the virus-infected application and their download links.

[0039] The recommendation information receiving module 240 receives the recommendation information from the recommended application search module, wherein the recommendation information comprises introduction to one or more applications relevant to the virus-infected application. According to the embodiments where the recommended application search module is installed locally, the recommendation information can be transmitted within a process or between processes. According to the embodiments where the recommended application search module is installed in a remote server, the recommendation information can be transmitted via a network.

[0040] The recommendation information display module 250 displays the recommendation information. According to some embodiments, the recommendation information can be displayed in the form of a list to introduce the recommended applications. According to some embodiments, relevant applications can be automatically downloaded and installed after a user clicks a relevant link or button.

[0041] In the above described virus-infected application processing device, relevant applications are recommended to a user at the same time as the virus-infected application is cleaned, thereby allowing the user to easily install a same but virus-free application or a similar substitute application. The entire operational process is simple and convenient, and can effectively make up for the functional loss due to the cleaning of the virus-infected application.

[0042] As illustrated in FIG. 4, a virus-infected application processing system comprises a processing device 200 illustrated in FIG. 3 and an application recommending server 300.

[0043] The processing device 200 has been described in detail hereinabove. The application recommending server 300 can comprise: a recommended application search module 310. The recommended application search module 310 receives identification information associated with the virus-infected application sent from the identification information sending module 230 in the processing device 200, searches relevant applications based on the identification information, generates recommendation information and returns the recommendation information to the processing device 200. According to some embodiments, the recommendation information can comprise introduction to one or more applications relevant to the virus-infected application.

[0044] According to some embodiments, the recommended application search module 310 searches applications relevant to the virus-infected application in an application library and generates recommendation information based on one or more found applications. According to some embodiments, the application library can be stored directly in the application recommending server or in a storage server in a cloud.

[0045] FIG. 2 is a schematic diagram illustrating an example of the flow of a method of searching relevant applications executed by the recommended application search module 310 according to various embodiments. As illustrated in FIG. 2, the method can comprise:

[0046] Step S131: searching one or more applications with same application name, same program package name, and same certificate as the virus-infected application.

[0047] Step S132: searching one or more applications with same application name and same program package name as the virus-infected application if no application with same application name, same program package name, and same certificate as the virus-infected application is found.

[0048] Step S133: searching one or more applications of a same type as the virus-infected application and filtering found applications based on the applications' rating or downloads if no application with same application name and same program package name as the virus-infected application is found.

[0049] The inclusion of a process of certificate verification in Step S131 ensures that any found application and the virus-infected application are published by the same person or organization. Therefore, the searching criteria pursuant to Step S131 are the strictest. Compared to Step S131, Step S132 does not include the process of certificate verification, but because it includes a process of verifying application name and program package name, it can find most repackaged applications. Step S133 can provide a user with even more choices because it can find some most popular applications (e.g., those with the highest ratings or the most downloads) based on the type of the virus-infected application and filtering of applications of the same type as the virus-infected application based on the applications' rating or downloads.

[0050] According to some embodiments, Steps S131-S133 can proceed as illustrated in FIG. 2, and different numbers of recommended applications can be provided for a user to select based on the user's selection along each step. Those skilled in the art can readily appreciate that a process of searching relevant applications is not limited to the one illustrated in FIG.2. For example, part but not all of Steps S131-S133 can be adopted. According to some embodiments, other identification information such as one or more feature codes can be used for searching and verification.

[0051] According to some embodiments, after finding one or more relevant applications, the recommended application search module 310 can generate recommendation information based on the found one or more applications and return the recommendation information to the recommendation information receiving module 240 in the processing device 200.

[0052] In the above described virus-infected application processing system, relevant applications are recommended to a user at the same time as the virus-infected application is cleaned, thereby allowing the user to easily install a same but virus-free application or a similar substitute application. The entire operational process is simple and convenient, and can effectively make up for the functional loss due to the cleaning of the virus-infected application.

[0053] Persons of ordinary skill in the art can readily appreciate that all or part of the steps of the methods described in the embodiments above can be executed by relevant hardware instructed by a program that may be stored in a computer-readable memory medium. The readable memory medium may be, for example, a read-only memory ("ROM"), a random access memory ("RAM"), a magnetic disk or a compact disc.

[0054] Although the disclosed embodiments have been fully described with reference to the accompanying drawings, it is to be noted that various changes and modifications will become apparent to those skilled in the art. Such changes and modifications are to be understood as being included within the scope of the disclosed embodiments as defined by the appended claims.

Claims

1. A virus-infected application processing method comprising:

obtaining identification information associated with a virus-infected application,

cleaning the virus-infected application,

sending the identification information to a recommended application search module,

receiving recommendation information from the recommended application search module, wherein the recommendation information comprises introduction to one or more applications relevant to the virus-infected application, and

displaying the recommendation information.

2. The method of claim 1, wherein the identification information comprises at least one of a name and version of the virus-infected application, a program package name, a certificate, and a feature code.

3. The method of claim 1, wherein cleaning the virus-infected application comprises uninstalling the virus-infected application.

4. The method of claim 1, wherein the recommended application search module is installed locally.

5. The method of claim 1, wherein the recommended application search module is installed in a remote server.

6. The method of claim 1, wherein displaying the recommendation information comprises displaying the recommendation information in the form of a list.

7. A virus-infected application processing method comprising:

receiving identification information associated with a virus-infected application from a terminal,

searching in an application library for one or more applications relevant to the virus-infected application,

generating recommendation information based one or more found applications, wherein the recommendation information comprises introduction to the one or more found applications, and

sending the recommendation information to the terminal.

8. The method of claim 7, wherein searching in an application library for one or more applications relevant to the virus-infected application comprises searching one or more applications with same application name, same program package name, and same certificate as the virus-infected application.

9. The method of claim 8, wherein searching in an application library for one or more applications relevant to the virus-infected application comprises searching one or more applications with same application name and same program package name as the virus-infected application if no application with same application name, same program package name, and same certificate as the virus-infected application is found.

10. The method of claim 7, wherein searching in an application library for one or more applications relevant to the virus-infected application comprises:

searching one or more applications of a same type as the virus-infected application, and

filtering found applications based on the applications' rating or downloads.

11. A virus-infected application processing device comprising:

an identification information obtaining module that obtains identification information associated with a virus-infection application,

an infected application cleaning module that cleans the virus-infected application,

an identification information sending module that sends the identification information to a recommended application search module,

a recommendation information receiving module that receives recommendation information from the recommended application search module, wherein the recommendation information comprises introduction to one or more applications relevant to the virus-infected application, and

a recommendation information display module that displays the recommendation information.

12. The device of claim 11, wherein the identification information comprises at least one of a name and version of the virus-infected application, a program package name, a certificate, and a feature code.

13. The device of claim 11, wherein the infected application cleaning module uninstalls the virus-infected application.

14. The device of claim 11, wherein the recommended application search module is installed locally in the device.

15. The device of claim 11, wherein the recommended application search module is installed in a remote server.

16. The device of claim 11, wherein the recommendation information display module displays the recommendation information in the form of a list.

17. A virus-infected application processing system comprising:

a processing device and

an application recommending server, wherein

the processing device comprises:

an identification information obtaining module that obtains identification information associated with a virus-infected application,

an infected application cleaning module that cleans the virus-infected application,

an identification information sending module that sends the identification information to the application recommending server,

a recommendation information receiving module that receives recommendation information from the application recommending server, wherein the recommendation information comprises introduction to one or more applications relevant to the virus-infected application,

a recommendation information display module that displays the recommendation information, and

the application recommending server comprises:

a recommended application search module that receives the identification information from the processing device, searches relevant applications based on the identification information, generates the recommendation information and sends the recommendation information to the processing device.

18. The system of claim 17, wherein the identification information comprises at least one of a name and version of the virus-infected application, a program package name, a certificate, and a feature code.

19. The system of claim 17, wherein the infected application cleaning module uninstalls the virus-infected application.

20. The system of claim 17, wherein the recommendation information display module displays the recommendation information in the form of a list.

21. The system of claim 17, wherein the recommended application search module searches in an application library for one or more applications relevant to the virus-infected application and generates the recommendation information based on one or more found applications.

22. The system of claim 21, wherein the application library is stored in the application recommending server.

23. The system of claim 17, wherein the recommended application search module searches one or more applications with same application name, same program package name, and same certificate as the virus-infected application.

24. The system of claim 23, wherein the recommended application search module searches one or more applications with same application name and same program package name as the virus-infected application if no application with same application name, same program package name, and same certificate as the virus-infected application is found.

25. The system of claim 17, wherein the recommended application search module searches one or more applications of a same type as the virus-infected application and filters found applications based on the applications' rating or downloads.

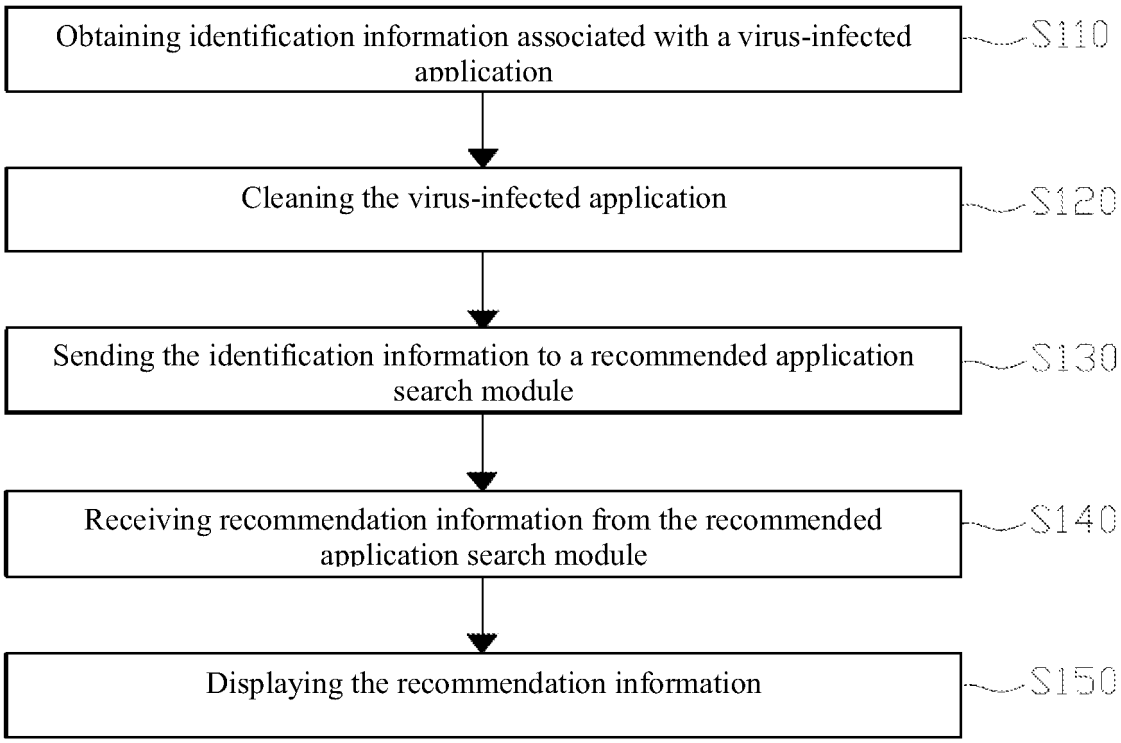
Obtaining identification information associated with a virus-infected application
S110
Cleaning the virus-infected application
S120
Sending the identification information to a recommended application search module
S130
Receiving recommendation information from the recommended application search module
S140
Displaying the recommendation information
S150

FIG. 1

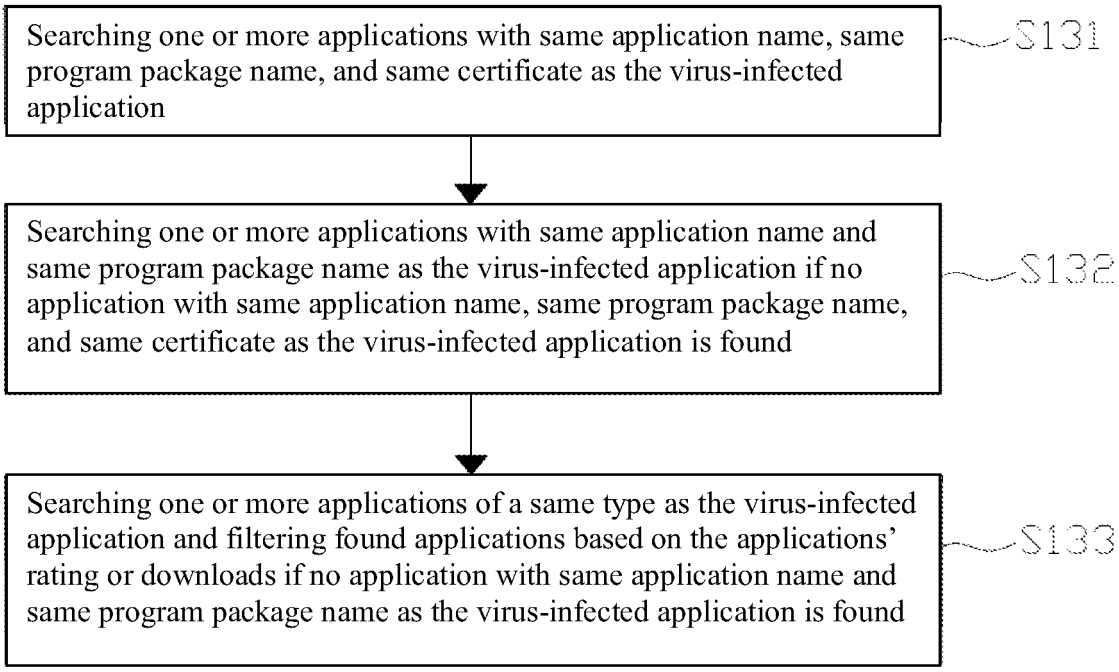
Searching one or more applications with same application name, same program package name, and same certificate as the virus-infected application
S131
Searching one or more applications with same application name and same program package name as the virus-infected application if no application with same application name, same program package name, and same certificate as the virus-infected application is found
S132
Searching one or more applications of a same type as the virus-infected application and filtering found applications based on the applications' rating or downloads if no application with same application name and same program package name as the virus-infected application is found
S133

FIG. 2

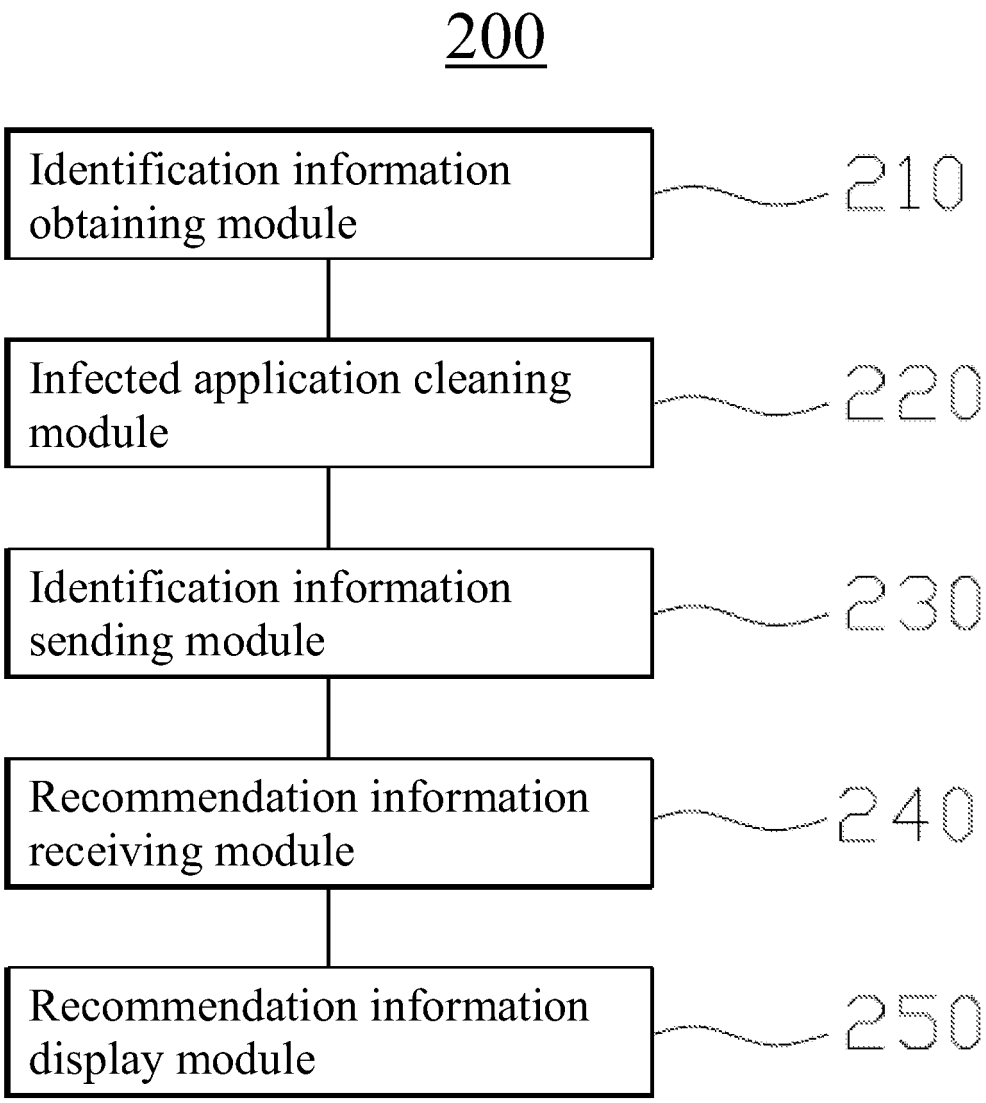
200
Identification information obtaining module
210
Infected application cleaning module
220
Identification information sending module
230
Recommendation information receiving module
240
Recommendation information display module
250

FIG. 3

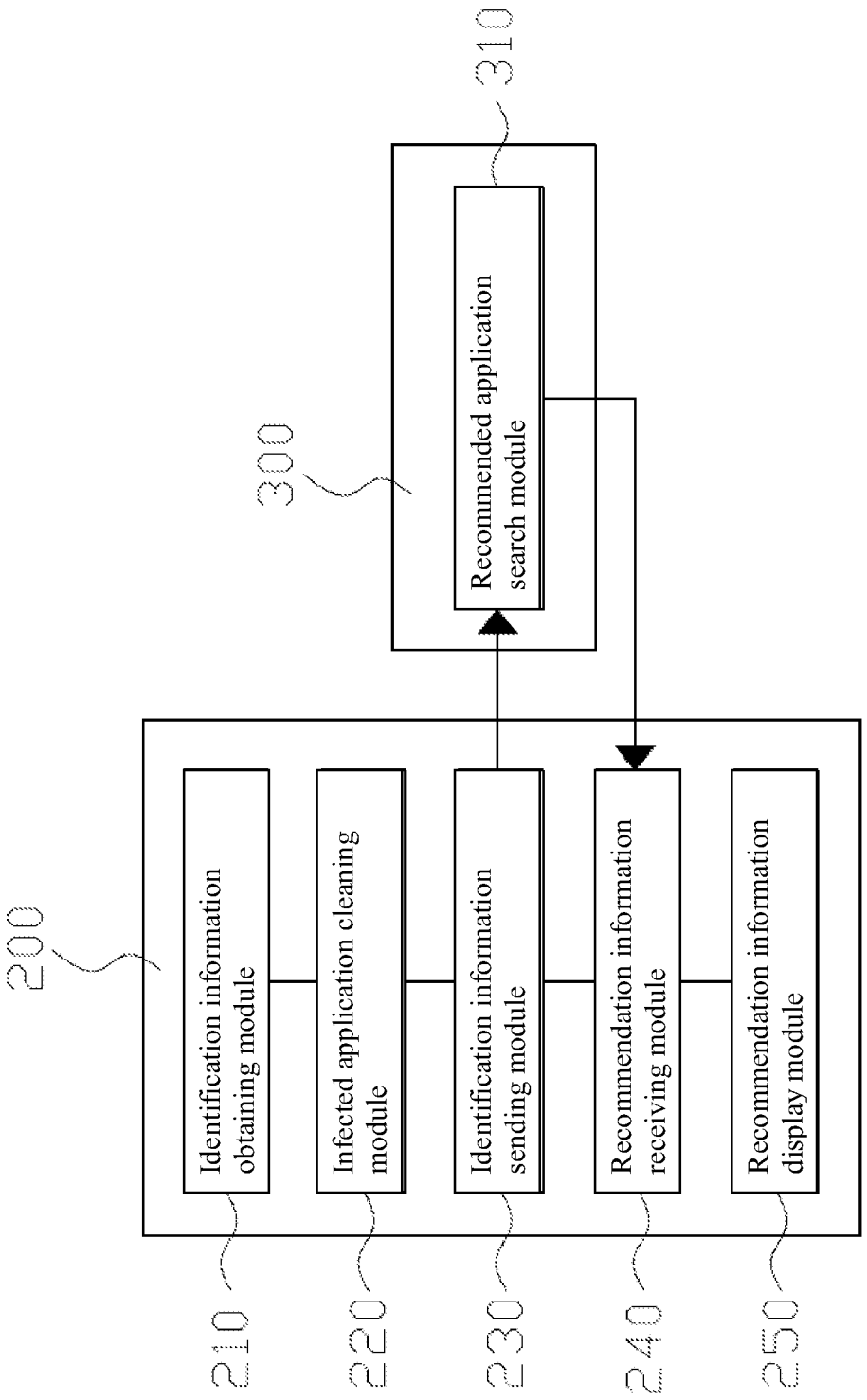
200
Identification information obtaining module
Infected application cleaning module
Identification information sending module
Recommendation information receiving module
Recommendation information display module
210
220
230
240
250
300
Recommended application search module
310

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/081901

A. CLASSIFICATION OF SUBJECT MATTER

See extra sheet

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,CNABS,CNTXT,GOOGLE,SIPOABS,DWPI: virus, Trojan, application, clean, uninstall+, interrelated, relevant, relational, program, download, install+, advice, information, recommendation, infected

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 102867145 A (TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED) 09 January 2013 (09.01.2013) claims 1-14	1-25
X	WO 2012/022211 A1 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED) 23 February 2012 (23.02.2012) abstract and claims 1-13	1-25
A	US 7013330 B1 (NETWORKS ASSOCIATES TECHNOLOGY,INC.) 14 March 2006 (14.03.2006) the whole document	1-25
A	US 6088803 B1 (INTEL CORPORATION) 11 July 2000 (11.07.2000) the whole document	1-25

☐ 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
30 October 2013 (30.10.2013)	**21 Nov. 2013 (21.11.2013)**
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 ZHANG,Tao Telephone No. (86-10)62414427

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/081901

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102867145 A	09.01.2013	None	
WO 2012/022211 A1	23.02.2012	CN 101950336 A	19.01.2011
US 7013330 B1	14.03.2006	None	
US 6088803 B1	11.07.2000	None	

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/081901

CLASSIFICATION OF SUBJECT MATTER:

G06F 21/56 (2013.01) i

G06F 17/30 (2006.01) i