



- (51) International Patent Classification:
G06F 21/56 (2013.01)
- (21) International Application Number:
PCT/CN2013/085353
- (22) International Filing Date:
17 October 2013 (17.10.2013)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
201210395070.2 17 October 2012 (17.10.2012) 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: **LIU, Zhao**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518044 (CN). **MENG, Qiyuan**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, 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 USER DEVICE FOR PROCESSING VIRUS FILES

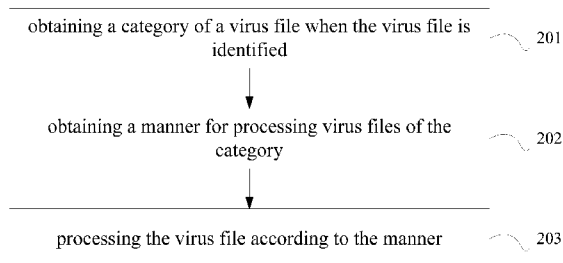


FIG. 2

(57) Abstract: The present disclosure provides a method and a user device for processing virus files. First information of at least one category of virus file and second information of a manner for processing each of the at least one category of virus file are provided. A category of a virus file when the virus file is identified. A manner of processing viruses of the category from the first information and the second information is obtained and the virus file is processed by using the manner without information about the virus file being presented to a user.



METHOD AND USER DEVICE FOR PROCESSING VIRUS FILES

Related documents

[0001] The present disclosure claims priority of Chinese patent application No.
5 201210395070.2 titled “method and user device for processing virus files” and filed on
October 17, 2012 with the Patent Office of the People’s Republic of China, the disclosure
of which is incorporated by reference in its entirety.

Technical Field

[0002] The present disclosure relates to computer security techniques, and particularly
10 to a method and a user device for processing virus files.

Background

[0003] Anti-virus software generally displays information of a virus to a user soon after
the virus is detected to implement a real-time virus report mechanism. When there is a
virus outbreak in a user device, anti-virus software may display too many virus alerts that
15 the user barely has time to process one by one. The alerts distract attention of the user
continuously and disturb the user using the computer.

[0004] Some anti-virus software may display in a dialog the information of all viruses
detected during the period the dialog is being displayed to avoid popping up too many
dialogs and disturbing the user.

Summary

[0005] Various examples of the present disclosure provide a method and a user device
for processing virus files. The technical schemes are as follows.

[0006] A method for processing virus files may include:

providing first information of at least one category of virus file and second
25 information of a manner for processing each of the at least one category of virus file;

obtaining a category of a virus file when the virus file is identified;

obtaining a manner for processing virus files of the category from the first information and the second information and processing the virus file by using the manner without presenting information about the virus file to a user.

[0007] A user device may include:

5 a category obtaining module, configured to obtain a category of a virus file when the virus file is identified without presenting information about the virus file to a user;

a manner obtaining module, configured to obtain a manner for processing virus files of the category by using pre-defined first information of at least one category of virus file and second information of a manner for processing each of the at least one category of virus file without presenting information about the virus file to a user; and
10

a processing module, configured to process the virus file according to the manner without presenting the information about the virus file to the user.

[0008] The technical scheme of the present disclosure classifies virus files detected and processes the virus files according to respective categories of the virus files. The process
15 is implemented at the background silently, thus avoids prompting the user each time when a virus file is detected. The problem of virus alerts disturbing the user is solved, and at the same time, prompt information provided to a user is informative and user-friendly.

Brief Description of the Drawings

[0009] Features of the present disclosure are illustrated by way of example and not
20 limited in the following figures, in which like numerals indicate like elements, in which:

[0010] FIG.1 is a flowchart illustrating a method for processing virus files according to an example of the present disclosure.

[0011] FIG.2 is a flowchart illustrating a method for processing virus files according to an example of the present disclosure;

25 [0012] FIG.3 is a flowchart illustrating a method for processing virus files according to an example of the present disclosure;

[0013] FIG.4 is a schematic diagram illustrating a structure of a user device according to an example of the present disclosure.

Detailed Descriptions

[0014] For simplicity and illustrative purposes, the present disclosure is described by referring mainly to an example thereof. 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
5 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 herein, 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. Due to characteristics of the Chinese language, quantities of an element, unless
10 specifically mentioned, may be one or a plurality of, or at least one.

[0015] In an example, a computer may execute methods and software systems of the present application. FIG.1 is a schematic diagram illustrating an example of a computer. As shown in FIG.1, computer 100 may be a computing device capable of executing a method and apparatus of present disclosure. The computer 100 may, for example, be a
15 device such as a personal desktop computer or a portable device, such as a laptop computer, a tablet computer, a cellular telephone, or a smart phone. The computer 100 may also be a server that connects to the above devices locally or via a network.

[0016] The computer 100 may vary in terms of capabilities or features. Claimed subject matter is intended to cover a wide range of potential variations. For example, the
20 computer 100 may include a keypad/keyboard 156. It may also comprise a display 154, such as a liquid crystal display (LCD), or a display with a high degree of functionality, such as a touch-sensitive color 2D or 3D display. In contrast, however, as another example, a web-enabled computer 100 may include one or more physical or virtual keyboards, and mass storage medium 130.

[0017] The computer 100 may also include or may execute a variety of operating systems 141, including an operating system, such as a Windows™ or Linux™, or a mobile operating system, such as iOS™, Android™, or Windows Mobile™. The computer 100 may include or may execute a variety of possible applications 142, such as an anti-virus application 145. An application 142 may enable processing virus files
30 without presenting alerts to the user of the computer 100.

[0018] Further, the computer 100 may include one or more non-transitory processor-readable storage media 130 and one or more processors 122 in communication

with the non-transitory processor-readable storage media 130. For example, the non-transitory processor-readable storage media 130 may be a RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of non-transitory storage medium known in the art. The one or more non-transitory processor-readable storage media 130 may store sets of instructions, or units and/or modules that comprise the sets of instructions, for conducting operations described in the present application. The one or more processors may be configured to execute the sets of instructions and perform the operations in examples of the present application.

[0019] FIG.2 is a flowchart illustrating a method for processing virus files according to an example of the present disclosure. In the example, the method may be implemented by a user device, e.g., a fixed terminal device or a mobile terminal device. The fixed terminal device may be a PC and the like. The mobile terminal device may be a smart phone, a tablet computer, a MP3 player, a PDA and the like. As shown in FIG.2, the method may include the following procedures.

[0020] In block 201, a category of a virus file is obtained when the virus file is identified.

[0021] The user device may identify a virus file by using various methods, e.g., identifying the virus file by using an anti-virus engine installed in the user device or by using an anti-virus engine in a cloud and so on, and this is not limited in the present disclosure.

[0022] In an example, the category of the virus file may be determined by at least one of the directory in which the virus file is located, a process accessing the virus file (i.e., an object being infected), the infection manner and the like.

[0023] A virus file may belong to multiple categories, e.g., the virus file may belong to a category of system directories when the virus file is located in a system directory; the virus file may belong to a category of extraction of a compressed archive when the virus file is a file obtained by extracting a compressed archive. Describing a virus file by using several categories enables viewing the virus file from multiple aspects. The virus file may be processed in different manners corresponding to the different categories.

[0024] In block 202, a manner for processing virus files of the category is obtained.

[0025] The method of obtaining the manner may include: (1) storing a manner for each category in the user device and/or in a server in a cloud in advance, obtaining the manner corresponding to the category when the category is identified; (2) when the category is identified, judging whether there is a manner associated with the category in the user device or in the server in the cloud, and obtaining the manner associated with the category in response to a determination that there is a manner associated with the category in the user device or in the server in the cloud, or obtaining a manner selected by a user in response to a determination that no manner is associated with the category in the user device or in the server in the cloud. Several options may be provided for the user to choose from.

[0026] When the manner for processing virus files of the category is obtained, no alert is prompted to the user, and the virus file is directly processed at the background.

[0027] In block 203, the virus file is processed according to the manner.

[0028] In various examples, the processing of a virus file may include, but not limited to, deleting the virus, deleting the virus file completely, isolating the virus file, and the like.

[0029] In an example, a method for processing virus files obtains the category of a virus file when the virus file is identified, obtains a manner for processing virus files of the category and processes the virus file by using the manner. The technical scheme of the present disclosure classifies virus files detected and processes the virus files according to the categories of the virus files. The process is implemented at the background silently, thus avoids prompting the user each time when a virus file is detected. The mechanism avoids disturbing user by too many virus alerts, and prompt information provided to the user is informative and user-friendly.

[0030] In an example, the method of obtaining the category of the virus file when the virus file is identified in block 201 may include: obtaining the category of the virus file at least by using the directory in which the virus file is located and/or a process accessing the virus file when the virus file is identified.

[0031] In this example, the category of the virus file may be configured by a technician in advance, or may be configured during the process the user uses the device at least according to the directory in which the virus file is located and/or the process accessing the virus file.

[0032] During an outbreak of viruses, a lot of files in one directory may all have got infected. When a user performs an operation on the directory such as copy or cut the directory and so on, the anti-virus software may detect a large amount of viruses. By classifying files in one directory into the same category, the user may decide not to have information of all viruses found in the directory presented. Therefore, information of a virus file is not presented when the virus file is in the same directory.

[0033] When a user decompresses a compressed archive which includes a large amount of viruses, the anti-virus software may also detect a lot of virus files. Thus, files extracted by the same data compression software may be classified into the same category so that the user may decide not to have virus information detected in files extracted from one de-compression process presented. As such, information of a virus file may not be displayed when the virus file is extracted in the same de-compression process.

[0034] Virus files may be classified according to any classification rule to obtain a category. In an example, a virus file may also be classified by using at least the above two manners to obtain at least two categories, i.e., multi-dimensional classification, to increase the chance of the virus file having a processing manner associated with the category of the virus file, and thus to further reduce the need of displaying prompt information for the virus file.

[0035] In an example, other schemes for classifying and removing duplicated virus alerts may be designed for some typical scenarios by analyzing possible situations where a large amount of viruses may be detected by a technician or a user. When the user has explicitly expressed his/her unwillingness to receive prompt information for a certain category, the amount of alerts displayed can be reduced.

[0036] In an example, the method of obtaining the category of the virus file at least by using the directory in which the virus file is located and/or the process accessing the virus file may at least include any of the following procedures 201a and 201b.

[0037] In procedure 201a, a first category of the virus file is obtained by classifying the directory where the virus file is located by using a directory classifier when the virus file is identified.

[0038] When the classifying method is configured to be classification based on the directory in which the virus file is located, a directory classifier is used to determine the

category of the virus file by using the directory in which the virus file is located. The category of the virus file obtained by using a directory classifier is referred to as the first category of the virus file for simplicity.

5 [0039] In procedure 201b, a second category of the virus file is obtained by classifying the process accessing the virus file using a process classifier when the virus file is identified.

[0040] When the classifying method is configured to be classification based on the process accessing the virus file, a process classifier is used to determine the category of the virus file by using the process accessing the virus file. The category of the virus file
10 obtained by using a process classifier is referred to as the second category of the virus file for simplicity.

[0041] The above examples classify a virus file by using the directory in which the virus file is located and/or the process accessing the virus file. Other examples may also classify the virus file by using other parameters, such as a name suffix of the virus file
15 and the like, and are not elaborated here.

[0042] The above mentioned classifiers are merely an example. Other classifiers may be adopted in other examples to classify the virus file.

[0043] In an example, the classification process may classify a virus file which does not belong to any of pre-configured categories into an unknown category, then present
20 information of the virus file of the unknown category to the user to make the user select a manner for processing the virus file of the unknown category.

[0044] In an example, the method of obtaining a manner for processing virus files of the category in block 202 of FIG.2 may include the following procedures.

[0045] In procedure 202a, it is judged whether there is a manner that is associated with
25 the category of the virus file.

[0046] Categories and associated processing manners may be stored in the user device in advance, and are either configured by a technician or determined and saved by the user during the process of the using the user device.

[0047] When the user decides not to have virus alert for a category of viruses, the user
30 device may store the decision. When a virus of the same category is detected the next

time, the step of presenting information of the virus may be skipped and an operation selected by the user is directly performed so as not to disturb the user.

[0048] In an example, the judging in procedure 202a may be performed by using categories and associated processing manners stored in a server in the cloud, or by using
5 categories and associated processing manners stored in the user device and categories and associated processing manners stored in the server in the cloud.

[0049] When a processing manner associated with the category of the virus category is obtained from pre-stored information, the step of presenting the information of the virus file may be skipped and the operation required by the user is directly performed so as not
10 to disturb the user.

[0050] In procedure 202b, when there is a manner associated with the category of the virus file, the manner associated with the category of the virus file is obtained.

[0051] In response to a determination that there is a processing manner associated with the category of the virus file in the user device and/or in a server in the cloud, the
15 processing manner is obtained. The classification process and the process of obtaining the category involve no virus alert presented to the user, thus reduce virus alerts by using selections of the user stored in the user device and/or experiences stored in the server in the cloud.

[0052] In procedure 202c, in response to a determination that no manner is associated
20 with the category of the virus file, information of the virus file is presented to a user, a manner selected by the user is obtained and associated with the category of the virus file.

[0053] When the user selects a manner for processing the virus file, the user device may associate the manner with the category of the virus file so that the operation selected by the user can be directly performed on a virus of the same category detected the next time
25 and the step of presenting virus information can be skipped to avoid disturbing the user.

[0054] When the user selects to have no virus alert for the category of the virus file, the processing manner selected by the user may be stored. When receiving the decision of the user for not presenting alerts for the category of virus, the user device may store the decision, skip the step of presenting virus information the next time when a virus of the
30 category is detected and directly perform the operation selected by the user so avoid disturbing the user.

[0055] When no processing manner is associated with the category of a virus file, it means the user has not explicitly provided a manner for processing viruses of the category, thus information of the virus file is to be presented to the user. When presenting the information, the anti-virus software may not only guide the user to process the current virus file, but also prompt the user to decide whether to adopt the same processing manner for viruses of the same category in the future without presenting virus alerts. For example, a check box presenting “remember my choice, and remind me no more” may be displayed.

[0056] In an example, the step of presenting information of the virus file to the user and obtaining and associating a processing manner selected by the user with the category of the virus file in procedure 202c may include: presenting information of the virus file to the user, obtaining a processing manner selected by the user; associating the processing manner selected by the user with the category of the virus file in response to a determination that the number of times the processing manner is selected by the user for the category of the virus file exceeds a pre-defined threshold.

[0057] In an example, a decision as to whether the selected processing manner is saved may be obtained from the user. In response to a determination that the user selects to save the processing manner, the processing manner is associated with the category of the virus file. In an example, the number of times a processing manner is selected by the user for the category of the virus file may be counted, and the processing manner is associated with the category of the virus file in response to a determination that the number of times the processing manner is selected by the user for the category of the virus file reaches a pre-defined threshold.

[0058] In an example, a method for processing virus files obtains the category of a virus file when the virus file is identified, obtains a manner for processing the category of the virus file and processes the virus file by using the manner. The technical scheme of the present disclosure classifies virus files detected and processes the virus files according to the categories of the virus files. The process is implemented at the background silently, thus avoids prompting the user each time when a virus file is detected. The problem of virus alerts disturbing the user is solved, and at the same time, prompt information provided to a user is informative and user-friendly.

[0059] Any of the above examples may be combined to form a technical scheme, and all the available technical scheme are not listed herein.

[0060] FIG.3 is a flowchart illustrating a method for processing virus files according to an example of the present disclosure. FIG.3 provides a more detailed example of the method with reference to the content as shown in FIG.2. As shown in FIG.3, the method may include the following procedures.

[0061] In block 300, a user device performs virus scan.

[0062] The virus scan may be performed through an anti-virus application or the like, and this is not limited in the present disclosure.

[0063] In block 301, the category of a virus file is obtained by using at least one of a directory where the virus file is located and a process accessing the virus file when the virus file is identified.

[0064] One or multiple categories of the virus file may be obtained.

[0065] In block 302, it is judged whether there is a manner that is associated with the category of the virus file.

[0066] The procedure in block 303 is performed in response to a determination that there is a manner associated with the category of the virus file.

[0067] The procedure in block 304 is performed in response to a determination that no manner is associated with the category of the virus file.

[0068] In block 303, the user device obtains a manner for processing virus files of the category, and the procedure in block 305 is performed.

[0069] In block 304, the user device presents information of the virus file to the user and obtains a manner selected by the user, and the procedure in block 305 is performed.

[0070] In an example, the manner selected by the user is associated with the category of the virus file in response to a determination that the number of times the manner is selected by user for the category of the virus file reaches a pre-defined threshold.

[0071] The example merely provides one method of storing a processing manner. In another example, the processing manner is associated with the category of the virus file as long as the processing manner is selected by the user. When a virus of the same category

is detected the next time, the step of presenting information of the virus is skipped and an operation selected by the user is directly performed so as not to disturb the user.

[0072] In block 305, the virus file is processed by using the manner.

[0073] FIG.4 is a schematic diagram illustrating a structure of a user device according to an example of the present disclosure. As shown in FIG.4, the user device may include the following components.

[0074] A category obtaining module 10 is configured to obtain a category of a virus file when the virus file is identified.

[0075] A manner obtaining module 20 is configured to obtain a manner for processing virus files of the category.

[0076] A processing module 30 is configured to process the virus file according to the manner.

[0077] In an example, the category obtaining module 10 may obtain the category of the virus file by using at least one of a directory where the virus file is located and a process accessing the virus file when the virus file is identified.

[0078] In an example, the category obtaining module 10 may obtain a first category of the virus file by classifying the directory in which the virus file is located by using a directory classifier; and/or obtain a second category of the virus file by classifying the process visiting the virus file by using a process classifier.

[0079] In an example, the manner obtaining module 20 may include:

[0080] a judging unit, configured to judge whether there is a manner that is associated with the category of the virus file;

[0081] an obtaining unit, configured to obtain the manner associated with the category of the virus file in response to a determination that there is a manner associated with the category of the virus file; and to present information of the virus file to a user in response to a determination that no manner is associated with the category of the virus file, obtain a manner selected by the user, and associate the manner selected by the user with the category of the virus file.

[0082] In an example, the obtaining unit may present the information of the virus file to the user, obtain a manner selected by the user; associate the manner with the category of

the virus file in response to a determination that the number of times the manner is selected by the user exceeds a pre-defined threshold.

[0083] The user device including the above components as shown in FIG.3 is merely an example. In various examples, a user device may include any combination of features in
5 the above examples as long as the combined scheme is feasible.

[0084] The user device implements obtaining a category of a virus file and a processing manner for processing the category of the virus file by using the above modules in the same manner of the above method embodiment. Details of the implementation can be found in the above description in connection with the above method, and will not be
10 described further herein.

[0085] It should be understood that in the above processes and structures, not all of the procedures and modules are necessary. Certain procedures or modules may be omitted according to the needs. The order of the procedures is not fixed, and can be adjusted according to the needs. The modules are defined based on function simply for facilitating
15 description. In implementation, a module may be implemented by multiple modules, and functions of multiple modules may be implemented by the same module. The modules may reside in the same device or distribute in different devices. The “first”, “second” in the above descriptions are merely for distinguishing two similar objects, and have no substantial meanings.

[0086] In various embodiments, a hardware module may be implemented mechanically or electronically. For example, a hardware module may comprise dedicated circuitry or logic that is permanently configured (e.g., as a special-purpose processor, such as a field programmable gate array (FPGA) or an application-specific integrated circuit (ASIC)) to perform certain operations. A hardware module may also comprise programmable logic or
25 circuitry (e.g., as encompassed within a general-purpose processor or other programmable processor) that is temporarily configured by software to perform certain operations. It will be appreciated that the decision to implement a hardware module mechanically, in dedicated and permanently configured circuitry, or in temporarily configured circuitry (e.g., configured by software) may be driven by cost and time considerations.

[0087] A machine-readable storage medium is also provided, which is to store instructions to cause a machine to execute a method as described herein. Specifically, a
30

system or apparatus having a storage medium which stores machine-readable program codes for implementing functions of any of the above examples and which may make the system or the apparatus (or CPU or MPU) read and execute the program codes stored in the storage medium. In addition, instructions of the program codes may cause an operating system running in a computer to implement part or all of the operations. In addition, the program codes implemented from a storage medium are written in a storage device in an extension board inserted in the computer or in a storage in an extension unit connected to the computer. In this example, a CPU in the extension board or the extension unit executes at least part of the operations according to the instructions based on the program codes to realize the technical scheme of any of the above examples.

[0088] The storage medium for providing the program codes may include floppy disk, hard drive, magneto-optical disk, compact disk (such as CD-ROM, CD-R, CD-RW, DVD-ROM, DVD-RAM, DVD-RW, DVD+RW), magnetic tape drive, Flash card, ROM and so on. Optionally, the program code may be downloaded from a server computer via a communication network.

[0089] The scope of the claims should not be limited by the embodiments set forth in the examples, but should be given the broadest interpretation consistent with the description as a whole.

Claims

1. A method for processing virus files, comprising:

providing first information of at least one category of virus file and second information of a manner for processing each of the at least one category of virus file;

5 obtaining a category of a virus file when the virus file is identified;

obtaining a manner of processing viruses of the category from the first information and the second information and processing the virus file by using the manner without presenting information about the virus file to a user.

2. The method of claim 1, wherein obtaining the category of the virus file when the
10 virus file is identified comprises:

obtaining the category of the virus file by using at least one of a directory where the virus file is located and a process accessing the virus file when the virus file is identified.

3. The method of claim 2, wherein obtaining the category of the virus file by using at least one of a directory where the virus file is located and a process accessing the virus
15 file comprises:

obtaining a first category of the virus file by classifying the directory where the virus file is located by using a directory classifier.

4. The method of claim 2, wherein obtaining the category of the virus file by using at least one of a directory where the virus file is located and a process accessing the virus
20 file comprises:

obtaining a second category of the virus file by classifying the process accessing the virus file by using a process classifier when the virus file is identified.

5. The method of claim 1, wherein obtaining the manner for processing virus files of the category comprises:

25 judging whether there is a manner that is associated with the category of the virus file,

obtaining the manner associated with the category of the virus file in response to a determination that there is a manner associated with the category of the virus file;

presenting information of the virus file to a user in response to a determination that no manner is associated with the category of the virus file, obtaining a manner selected by the user, and associating the manner selected by the user with the category of the virus file.

- 5 6. The method of claim 5, wherein presenting information of the virus file to a user in response to a determination that no manner is associated with the category of the virus file, obtaining a manner selected by the user, and associating the manner selected by the user with the category of the virus file comprise:

 presenting information of the virus file to the user and obtaining the manner selected
10 by the user;

 associating the manner selected by the user with the category of the virus file in response to a determination that the number of times the manner is selected by user for the category of the virus file has exceeded a pre-defined threshold.

7. The method of claim 1, wherein obtaining a manner of processing viruses of the
15 category from the first information and the second information and processing the virus file by using the manner without presenting information about the virus file to a user comprises:

 performing, by a background process, the obtaining step and the processing step.

8. The method of claim 1, wherein obtaining a manner of processing viruses of the
20 category from the first information and the second information and processing the virus file by using the manner without presenting information about the virus file to a user comprises:

 prohibiting information of the virus file to be presented to the user.

9. A user device for processing virus files, comprising:

- 25 a category obtaining module, configured to obtain a category of a virus file when the virus file is identified;

 a manner obtaining module, configured to obtain a manner for processing virus files of the category by using pre-defined first information of at least one category of virus file and second information of a manner for processing each of the at least one category of
30 virus file without presenting information about the virus file to a user;

a processing module, configured to process the virus file according to the manner without presenting the information about the virus file to the user.

10. The user device of claim 9, wherein the category obtaining module is configured to obtain the category of the virus file by using at least one of a directory where the virus
5 file is located and a process accessing the virus file.

11. The user device of claim 10, wherein the category obtaining module is configured to obtain a first category of the virus file by classifying a directory in which the virus file is located by using a directory classifier.

12. The user device of claim 10, wherein the category obtaining module is
10 configured to obtain a second category of the virus file by classifying a process visiting the virus file by using a process classifier.

13. The user device of claim 9, wherein the manner obtaining module comprises:

a judging unit, configured to judge whether there is a manner that is associated with the category of the virus file;

15 an obtaining unit, configured to obtain the manner associated with the category of the virus file in response to a determination that there is a manner associated with the category of the virus file; and to present information of the virus file to a user in response to a determination that no manner is associated with the category of the virus file, obtain a manner selected by the user, and associat the manner selected by the user with the
20 category of the virus file.

14. The user device of claim 13, wherein the obtaining unit is further configured to present the information of the virus file to the user, obtain a manner selected by the user; associate the manner with the category of the virus file in response to a determination that the number of times the manner is selected by the user exceeds a pre-defined threshold.

25 15. The user device of claim 9, wherein the manner obtaining module and/or the processing module is implemented by using a background process.

16. The user device of claim 9, wherein the manner obtaining module and/or the processing module is configured to prohibit information of the virus file to be presented to the user

17. A non-transitory computer-readable storage medium comprising a set of instructions for processing virus files, the set of instructions to direct at least one processor to perform acts of:

providing first information of at least one category of virus file and second
5 information of a manner for processing each of the at least one category of virus file;

obtaining a category of a virus file when the virus file is identified;

obtaining a manner of processing viruses of the category from the first information and the second information and processing the virus file by using the manner without presenting information about the virus file to a user.

10 18. The non-transitory computer-readable storage medium of claim 17, wherein obtaining the category of the virus file when the virus file is identified comprises:

obtaining the category of the virus file by using at least one of a directory where the virus file is located and a process accessing the virus file when the virus file is identified.

15 19. The non-transitory computer-readable storage medium of claim 18, wherein obtaining the category of the virus file by using at least one of a directory where the virus file is located and a process accessing the virus file comprises:

obtaining a first category of the virus file by classifying the directory where the virus file is located by using a directory classifier; and/or

20 obtaining a second category of the virus file by classifying the process accessing the virus file by using a process classifier when the virus file is identified.

20. The non-transitory computer-readable storage medium of claim 17, wherein obtaining the manner for processing virus files of the category comprises:

judging whether there is a manner that is associated with the category of the virus file,

25 obtaining the manner associated with the category of the virus file in response to a determination that there is a manner associated with the category of the virus file;

presenting information of the virus file to a user in response to a determination that no manner is associated with the category of the virus file, obtaining a manner selected by

the user, and associating the manner selected by the user with the category of the virus file.

1/3

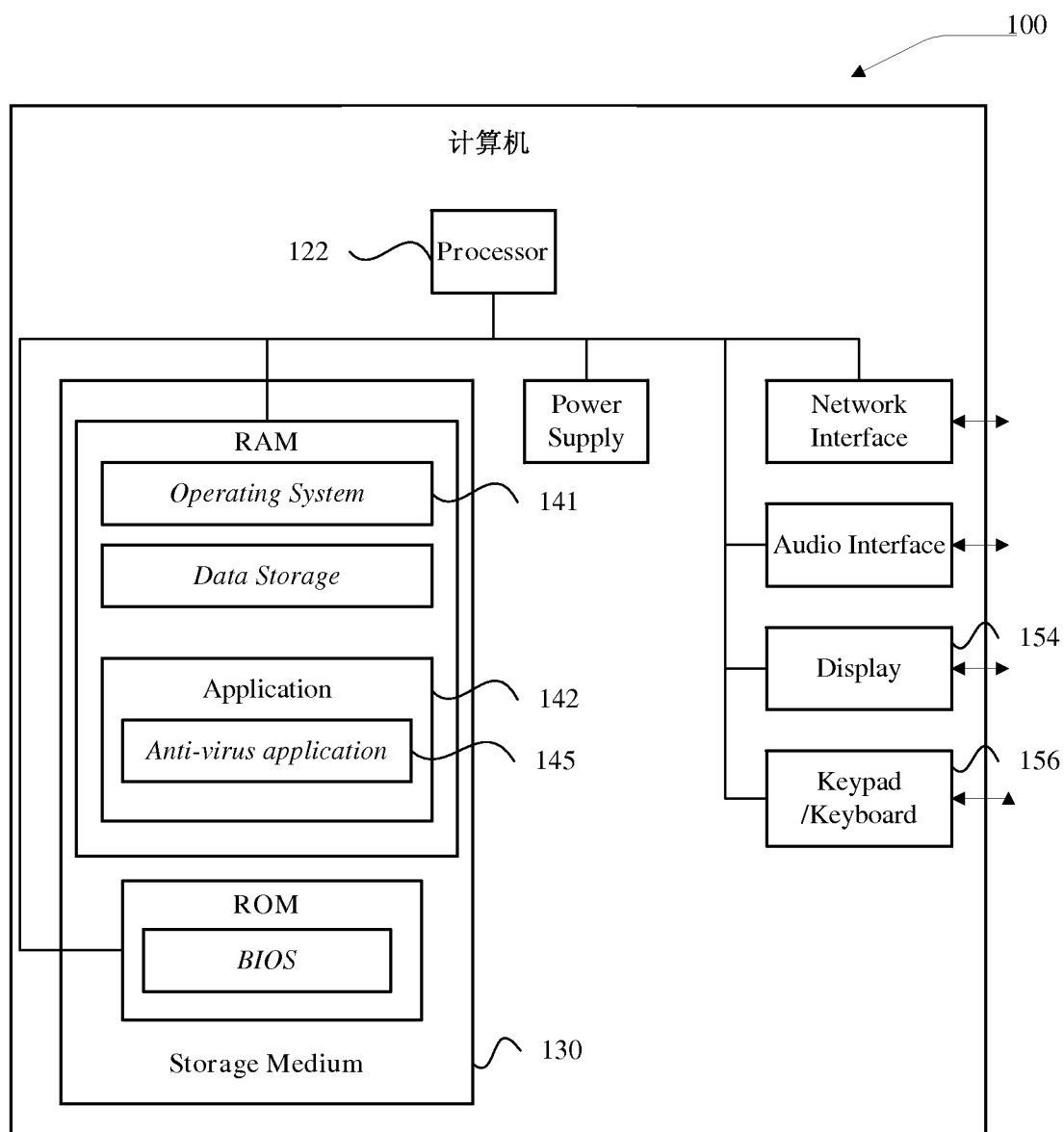


FIG. 1

2/3

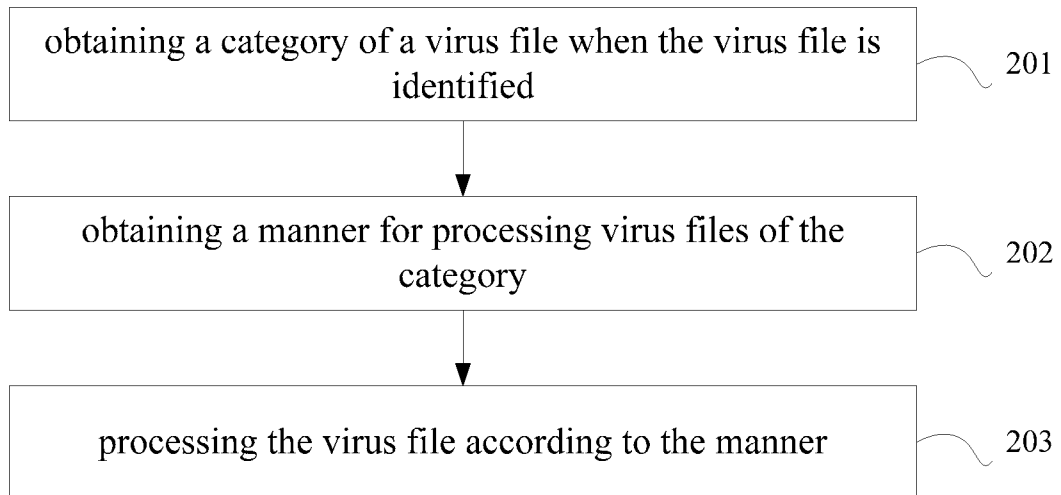


FIG. 2

3/3

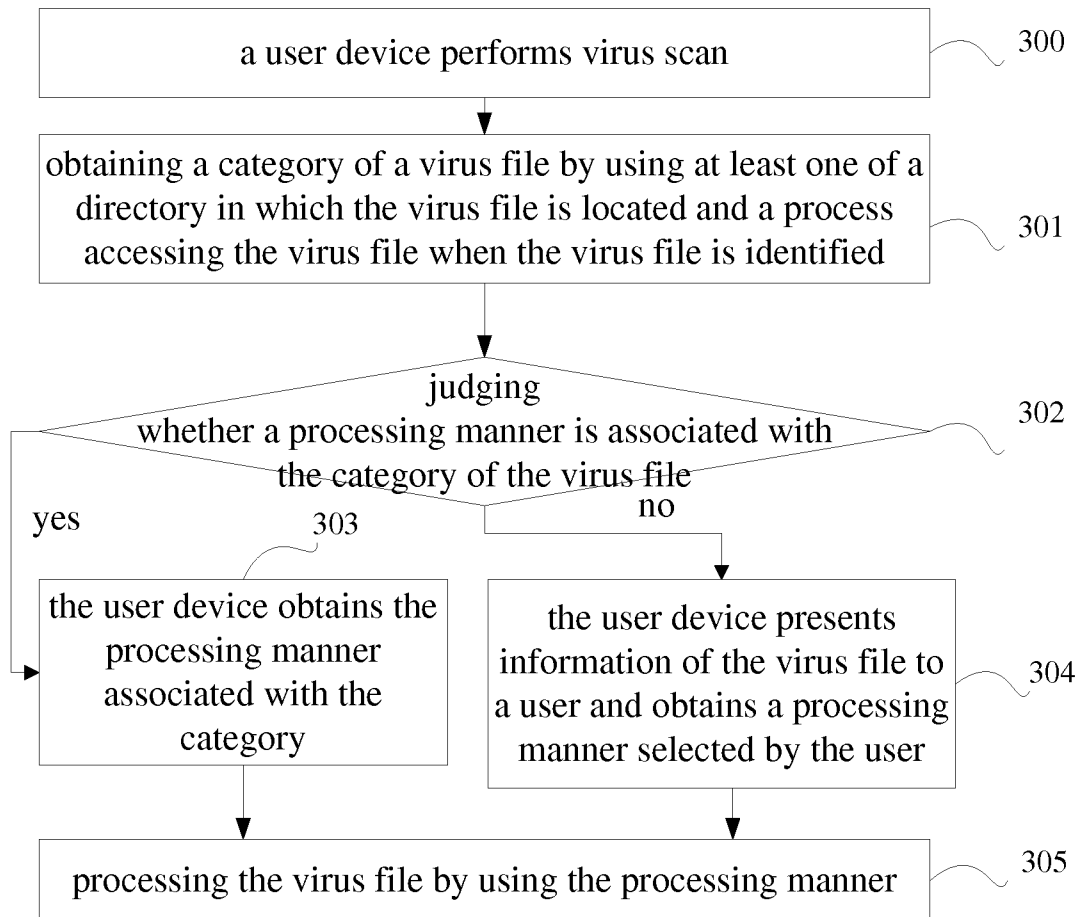


FIG. 3

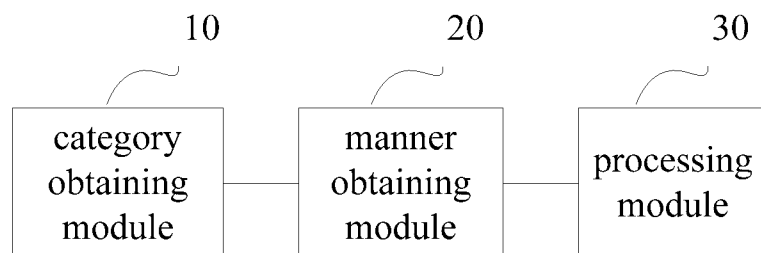


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/085353

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/56 (2013.01) 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)

CNABS, DWPI, SIPOABS, CNKI: virus, file, information, category, process+, manner

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101382984 A (JIANG, Qiyu) 11 March 2009(11.03.2009) description, page 5, line 9 to page 15, line 9	1-20
A	US 2008155691 A1 (FORTINET INC) 26 June 2008(26.06.2008) the whole document	1-20
A	CN 102194072 A (QIZHI SOFTWARE BEIJING CO., LTD.) 21 September 2011(21.09.2011) the whole document	1-20

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

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 02 January 2014 (02.01.2014)	Date of mailing of the international search report 30 Jan. 2014 (30.01.2014)
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 ZHANG Yan Telephone No. (86-10)62411651

International application No.
PCT/CN2013/085353

Form PCT/ISA /210 (patent family annex) (July 2009)