(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2012 年 2 月 23 日 (23.02.2012)

PCT

(10) 国际公布号
WO 2012/022211 A1

(51) 国际专利分类号:
G06F 21/00 (2006.01)

(21) 国际申请号: PCT/CN2011/077366

(22) 国际申请日: 2011 年 7 月 20 日 (20.07.2011)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201010256960.6 2010 年 8 月 18 日 (18.08.2010) CN

(71) 申请人 (对除美国外的所有指定国): **北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED)** [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室（德胜园区）, Beijing 100088 (CN)。 **奇智软件（北京）有限公司 (QIZHI SOFTWARE (BEIJING) COMPANY LIMITED)** [CN/CN]; 中国北京市朝阳区酒仙桥路 14 号兆维大厦 4 层东侧单元, Beijing 100016 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): **周鸿祎 (ZHOU, Hongyi)** [CN/CN]; 中国北京市朝阳区建国路 71 号惠通时代广场 D 座, Beijing 100025 (CN)。 **徐贵斌 (XU, Guibin)** [CN/CN]; 中国北京市朝阳区建国路 71 号惠通时代广场 D 座, Beijing 100025 (CN)。

(74) 代理人: **北京国昊天诚知识产权代理有限公司 (CO-HORIZON INTELLECTUAL PROPERTY INC.)**; 中国北京市朝阳区酒仙桥路甲 4 号宏源大厦 9 层 910, Beijing 100015 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, 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, KM, 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, PE, PG, PH, PL, PT, RO, RS, RU, 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。

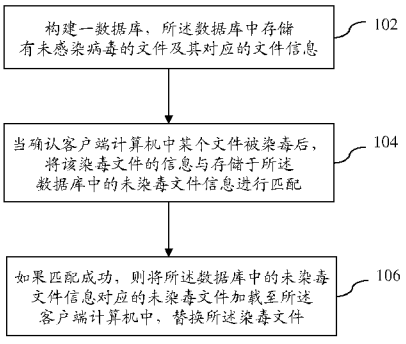
(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

(54) Title: A METHOD AND A DEVICE FOR REMOVING MALICIOUS PROGRAMS

(54) 发明名称 : 一种清除恶意程序的方法和装置



102 CONSTRUCTING A DATABASE WHERE UN-INFECTED FILES AND THEIR CORRESPONDING FILE INFORMATION ARE STORED
104 MATCHING THE INFORMATION OF THE INFECTED FILE WITH THE UN-INFECTED FILE INFORMATION STORED IN THE DATABASE WHEN A CERTAIN FILE IN THE CLIENT'S COMPUTER IS INFECTED WITH THE VIRUS
106 LOADING THE UN-INFECTED FILE CORRESPONDING TO THE UN-INFECTED FILE INFORMATION IN THE DATABASE INTO THE CLIENT'S COMPUTER TO REPLACE THE INFECTED FILE IF THE MATCHING IS SUCCESSFUL

图 1 / Fig. 1

(57) Abstract: A method and a device for removing malicious programs are provided, and the method comprises the following steps: firstly constructing a database where un-infected files and their corresponding file information are stored (102); matching the information of the infected file with the un-infected file information stored in the database when a certain file in the client's computer is infected with a virus (104); loading the un-infected file corresponding to the un-infected file information in the database into the client's computer to replace the infected file if the matching is successful(106). The utilization of the scheme can effectively avoid damaging the file or solve the problem that the file cannot be implemented after removing the computer virus or Trojan and other malicious programs, facilitate the treatment of the infected file for computer users and provide a scheme of removing virus that is safer and more effective.

[见续页]

WO 2012/022211 A1

(57) 摘要:

提供一种清除恶意程序的方法和装置，该方法包括首先构建一数据库，该所述数据库中存储有未染毒的文件及其对应的文件信息（102）；当确认客户端计算机中某个文件被染毒后，将该染毒文件的信息与存储于该数据库中的未染毒文件信息进行匹配（104）；如果匹配成功，则将所述数据库中的未染毒文件信息对应的未染毒文件加载至所述客户端计算机中，替换该染毒文件（106）。利用该方案，可有效避免在清除计算机病毒或木马等恶意程序后导致文件受损，或无法执行的问题，方便了计算机用户对染毒文件的处理，提供了更加安全有效的病毒清除方案。

一种清除恶意程序的方法和装置

技术领域

本发明涉及信息安全技术领域，尤其涉及一种清除恶意程序的方法和装置。

背景技术

随着计算机技术在社会生活中各个领域的广泛运用，恶意程序（Malwar，malicious software）也如同其附属品一样接踵而来。由于这些恶意程序所具有的感染性、复制性及破坏性，其已成为困扰计算机使用的一个重大问题。

恶意程序是一个概括性的术语，指任何故意创建用来执行未经授权并通常是有害行为的软件程序。计算机病毒、后门程序、键盘记录器、密码盗取者、Word 和 Excel 宏病毒、引导区病毒、脚本病毒（batch, windows shell, java 等）、木马、犯罪软件、间谍软件和广告软件等等，都是一些可以称之为恶意程序的例子。

为叙述方便，本发明将未被恶意程序感染或破坏或控制的文件或网页等对象，统称为未染毒文件；将已经被恶意程序感染或破坏或控制的文件或网页等对象，统称为染毒文件。

恶意程序一旦进入计算机并得以执行，其表现是多种多样的，下面主要以病毒作为例子进行说明。例如，正常的计算机程序一般是不会将自身的代码强行连接到其他程序之上的，而病毒却能使自身的代码强行传染到一切符合其传染条件的未受到传染的程序之上。

计算机病毒一旦进入计算机并得以执行，它就会搜寻其他符合其传染条件的程序或存储介质，确定目标后再将自身代码插入其中，达到自我繁殖的目的。只要一台计算机染毒，如不及时处理，那么病毒就会在这台计算机上迅速扩散，其中的大量文件（一般是可执行文件）会被感染。而被感染的文件又成了新的传染源，再与其他机器进行数据交换或通过网络接触，病毒会继续进行传染。

正是由于计算机病毒通过修改磁盘扇区信息或文件内容并把自身嵌入到其中的方法达到传播和扩散的目的，因此，现有的杀毒软件执行“清除病毒”的方法是从被感染病毒的文件中分离出并去除病毒代码，以还原出未经损坏的原文件，例如在 01117726.8 号中国专利申请中介绍的技术方案。

然而，现有的这种清除病毒的方法并不总是有效的，原因在于当去除被感染文件中的某些代码后，有可能会造成原程序无法运行，严重时还会造成某些系统文件无法执行，从而无法正常开启和进入用户的计算机系统，因此，用户有时并不敢轻易的执行病毒清除动作。

因此，如何更好的清除恶意程序，还原文件，已经成为一个困扰信息安全行业很久的问题，亟待业界提出更好的解决方案。

发明内容

本发明所要解决的技术问题在于提供一种清除恶意程序的方法和装置，以更加有效、安全的清除计算机病毒或木马等恶意程序，还原文件。

为解决上述技术问题，本发明提供一种清除恶意程序的方法，包括如下步骤:

构建一数据库，所述数据库中存储有未染毒的文件及其对应的文件信息;

当确认客户端计算机中某个文件被染毒后，将该染毒文件的信息与存储于所述数据库中的未染毒文件信息进行匹配;

如果匹配成功，则将所述数据库中的未染毒文件信息对应的未染毒文件加载至所述客户端计算机中，替换所述染毒文件。

其中，所述构建一数据库的步骤可以包括:

由客户端计算机收集文件及其对应的文件信息，并传送至服务器端;

由服务器端对收集到的文件进行认证，通过认证的，将该文件及其对应的文件信息存储入数据库中。

其中，所述由客户端计算机收集文件及其对应的文件信息步骤，可以进一步包括:

在客户端建立一收集文件列表，根据文件信息确认该文件已经收集过的，则不再重复收集。

其中，所述由服务器端对收集到的文件进行认证的步骤，可以进一步包括:

在服务器端建立一认证文件列表，根据文件信息确认该文件已经认证过的，则不再重复认证。

其中，所述将该染毒文件的信息与存储于所述数据库中的未染毒文件信息进行匹配的步骤，可以包括:

根据存储于数据库中的未染毒文件的信息类型，对应收集该染毒文件的信息;

将收集到的该染毒文件的信息与存储于所述数据库中的未染毒文件信息进行对应匹配，根据事先制定的匹配规则确定是否匹配成功。

其中，所述替换所述染毒文件的步骤，可以包括:

确定染毒文件在该客户端计算机中的安装路径;

删除染毒文件，并根据所述安装路径安装所述未染毒文件。

其中，所述文件信息可以包括文件名，文件路径，文件版本，操作系统，操作系统版本，及相关联到的应用程序组件信息中的至少其中之一。

其中，所述文件信息可以进一步包括文件指纹。

其中，所述方法可以进一步包括步骤:

将未染毒文件的文件指纹信息列入白名单，并将染毒文件的文件指纹信息列入黑名单，以辅助对未知程序的黑白判别。

本发明进而还提供一种清除恶意程序的装置，包括:

数据库模块，用于存储有未感染病毒的文件及其对应的文件信息;

匹配模块，用于当确认客户端计算机中某个文件被染毒后，将该染毒文件的信息与存储于所述数据库中的未染毒文件信息进行匹配;

替换模块，用于当匹配成功时，将所述数据库中的未染毒文件信息对应的未染毒文件加载至所述客户端计算机中，替换所述染毒文件。

其中，所述装置可以进一步包括:

客户端收集单元，用于通过客户端计算机收集文件及其对应的文件信息，并传送至服务器端;

服务器端认证单元，用于通过服务器端对收集到的文件进行认证，通过认证的，将该文件及其对应的文件信息存储入数据库中。

其中，所述客户端收集单元，可进一步用于在客户端建立一收集文件列表，根据文件信息确认该文件已经收集过的，则不再重复收集。

其中，所述服务器端认证单元，可进一步包括在服务器端建立一认证文件列表，根据文件信息确认该文件已经认证过的，则不再重复认证。

其中，所述匹配模块，可根据存储于数据库中的未染毒文件的信息类型，对应收集该染毒文件的信息，并将收集到的该染毒文件的信息与存储于所述数据库中的未染毒文件信息进行对应匹配，根据事先制定的匹配规则确定是否匹配成功。

其中，所述替换模块，可根据染毒文件在该客户端计算机中的安装路径，将未染毒文件加载至所述客户端计算机中，替换所述染毒文件。

其中，所述文件信息可以包括文件名，文件路径，文件版本，操作系统，操作系统版本，及相关联到的应用程序组件信息中的至少其中之一。

其中，所述文件信息可进一步包括文件指纹。

其中，所述数据库进一步包括黑/白名单，所述未染毒文件的文件指纹信息列入白名单，所述染毒文件的文件指纹信息列入黑名单，以辅助对未知程序的黑白判别。

利用本发明，可有效避免在清除计算机病毒或木马等恶意程序后导致文件受损，或无法执行的问题，方便了计算机用户对染毒文件的处理，提供了更加安全有效的病毒清除方案。

附图概述

图 1 为根据本发明实施例所述的清除恶意程序的方法流程图。

图 2 为根据本发明实施例所述的构建一数据库的流程示意图。

图 3 为根据本发明实施例所述的文件信息匹配流程示意图。

图 4 为根据本发明实施例所述的替换文件流程示意图。

图 5 为根据本发明实施例所述的清除受感染文件中的计算机病毒的装置示意图。

图 6 为根据本发明实施例所述的数据库文件收集示意图。

本发明的较佳实施方式

下面参照附图对本发明做进一步的说明。

针对现有清除恶意程序的方法的弊端，本发明的核心思想就是不再使用去除病毒代码的方式，而是直接替换染毒文件，为此需要事先构建一个文件数据库，并注意收集好文件的信息，当可以确定被感染文件及其信息时，可以通过文件信息在数据库中查找事先存储的未被感染病毒的好文件，并将好文件下载至被感染病毒的客户端计算机后，替换染毒文件。

请参考图 1，为根据本发明实施例所述的清除恶意程序的方法流程图，首先构建一数据库，所述数据库中存储有未感染病毒的文件及其对应的文件信息（步骤 102）；当确认客户端计算机中某个文件被染毒后，将该染毒文件的信息与存储于所述数据库中的未染毒文件信息进行匹配（步骤 104）；如果匹配成功，则将所述数据库中的未染毒文件信息对应的未染毒文件加载至所述客户端计算机中，替换所述染毒文件（步骤 106）。

本发明所述数据库可以构建在本地客户端，也可以构建在局域网内，优选的，是构建在服务器端（或云端）的数据中心。

所述数据库中存储的未染毒文件，可以是事先经过人工挑选并验证的文件，优选的，也可以是利用客户端计算机本地自动收集后，由服务器端进行验证后存储在数据库中，如图 2 所示，为根据本发明实施例所述的构建一数据库的流程示意图，首先由客户端计算机收集文件及其对应的文件信息，并传送至服务器端（步骤 202）；然后由服务器端对收集到的文件进行认证，通过认证的，将该文件及其对应的文件信息存储入数据库中（步骤 204）。

上述这种文件未染毒的认证，可以是通过白名单验证，或文件指纹与文件名称的对应，或经过虚拟机验证等方式进行，本发明对此不做限制。

进一步优选的，上述步骤 202 中，还可以在客户端计算机本地建立一收集文件列表，根据文件信息确认该文件是否已经被收集过，如果已经收集过的，则不再重复收集。

同理，上述步骤 204 中，还可以在服务器端建立一认证文件列表，根据文件信息确认该文件已经经过认证，已经认证过的，则不再重复认证。

上述文件列表中可以记录有文件的名称及指纹信息，一旦经过收集或认证后，即可在列表中添加一条记录，以供后续文件的比对判断，本发明对该步骤的具体操作方式不做限制。

当利用查毒软件确定客户端计算机中的染毒文件后，即可利用本发明，将该染毒文件的信息与存储于所述数据库中的未染毒文件信息进行匹配，以便查找到与染毒文件对应的未染毒文件。

上述查毒软件对染毒文件的确认，可以通过特征码扫描，行为判断，云查杀等多种方式，本发明对此不做限制，而本发明的匹配步骤所需要的染毒文件信息，即可利用后台杀毒软件对染毒文件的判断时所获取的文件信息作为匹配所需要的信息，从而提高效率。

当上述对染毒文件的判断所需要的信息不足以提供本发明的匹配步骤所需要的信息时，可先执行染毒文件信息收集动作后再进行匹配，请参考图 3，为根据本发明实施例所述的文件信息匹配流程示意图，首先根据存储于数据库中的未染毒文件的信息类型，对应收集该染毒文件的信息（步骤 302）；然后将收集到的该染毒文件的信息与存储于所述数据库中的未染毒文件信息进行对应匹配，根据事先制定的匹配规则确定是否匹配成功（步骤 304）。

本发明所述的文件信息可以包括文件名，文件路径，文件版本，操作系统，操作系统版本，或相关联到的应用程序组件等，也可以是前述信息的任何组合，至少包括其中之一。

如果在数据库中存储的未染毒文件信息包括了文件名、文件路径及文件版本信息，则对应收集染毒文件的文件名、文件路径及文件版本信息进行匹

配；而匹配规则可以根据文件的重要程度而制定不同的匹配要求，例如，对于系统文件，可以要求文件信息全部一致才认为匹配成功；而对于一般应用程序文件，在版本不一致时，如果存储于数据库中的是基本版本或标准版本，则可以认为匹配成功。上述文件信息类型及规则仅为例举，本发明对此不作任何限制。

在匹配成功后，即可通过替换文件达到清除病毒的目的。如图 4 所示，为根据本发明实施例所述的替换文件流程示意图，首先确定染毒文件在该客户端计算机中的安装路径（步骤 402）；然后删除染毒文件，并根据所述安装路径安装所述未染毒文件（步骤 404）。

如果上述收集的染毒文件信息中包含了文件路径信息，则直接可以确定染毒文件的安装路径，如果未包含文件路径信息，则可以再次执行收集动作。

此外，所述收集的文件信息还可以包括文件指纹信息。文件指纹是使用例如 MD5 文件信息摘要算法算出的一个 32 位的特征编码，或使用 SHA1 或 CRC 等算法算出的特征编码，其相当于为每一个文件计算出一个文件指纹，用于标识文件的唯一性。

这样，可以将未染毒文件的文件指纹信息列入白名单，并将染毒文件的文件指纹信息列入黑名单，以辅助对未知程序的黑白判别。

参考图 5，为根据本发明实施例所述的清除受感染文件中的计算机病毒的装置示意图，数据库模块 502，匹配模块 504，及替换模块 506。

其中，数据库模块 502 用于存储未感染病毒的文件及其对应的文件信息；匹配模块 504 用于当确认客户端计算机中某个文件被染毒后，将该染毒文件的信息与存储于所述数据库中的未染毒文件信息进行匹配；替换模块 506 用于当匹配成功时，将所述数据库中的未染毒文件信息对应的未染毒文件加载至所述客户端计算机中，替换所述染毒文件。

同样，数据库中的文件及信息可以经由客户端计算机自动收集，如图 6 所示，为根据本发明实施例所述的数据库文件收集示意图，包括数据库 502，客户端收集单元 602，服务器认证单元 604。

其中，客户端收集单元 602 用于通过客户端计算机收集文件及其对应的

文件信息，并传送至服务器端；服务器端认证单元 604 用于通过服务器端对收集到的文件进行认证，通过认证的，将该文件及其对应的文件信息存储入数据库中。

优选的，所述客户端收集单元 602，进一步用于在客户端建立一收集文件列表，根据文件信息确认该文件已经收集过的，则不再重复收集。

优选的，所述服务器端认证单元 604，进一步包括在服务器端建立一认证文件列表，根据文件信息确认该文件已经认证过的，则不再重复认证。

与上述在本发明的方法中描述的技术方案类似，本发明的所述匹配模块，可以根据存储于数据库中的未染毒文件的信息类型，对应收集该染毒文件的信息，并将收集到的该染毒文件的信息与存储于所述数据库中的未染毒文件信息进行对应匹配，根据事先制定的匹配规则确定是否匹配成功。

所述替换模块，可以根据染毒文件在该客户端计算机中的安装路径，将未染毒文件加载至所述客户端计算机中，替换所述染毒文件。

此外，所述文件信息除可以包含文件名，文件路径，文件版本，操作系统，操作系统版本，及相关联到的应用程序组件等之任意组合外，还可以包括文件指纹。

相应的，所述数据库中可进一步记录有黑/白名单，并将所述未染毒文件的文件指纹信息列入白名单，将所述染毒文件的文件指纹信息列入黑名单，以辅助对未知程序的黑白判别。

上述对于本发明的方法所作出的有关实施例的细节说明，对于本发明的装置同样适用，在此不再赘述。

工业实用性

本发明提供了更为安全有效的恶意程序清除方案，保障了计算机用户对染毒文件的安全处理，在清除计算机病毒或木马等恶意程序后，不会导致文件受损，或无法执行的问题。

权 利 要 求 书

1、一种清除恶意程序的方法，其特征在于，包括如下步骤:

构建一数据库，所述数据库中存储有未染毒的文件及其对应的文件信息;

当确认客户端计算机中某个文件被染毒后，将该染毒文件的信息与存储于所述数据库中的未染毒文件信息进行匹配;

如果匹配成功，则将所述数据库中的未染毒文件信息对应的未染毒文件加载至所述客户端计算机中，替换所述染毒文件。

2、如权利要求 1 所述的方法，其特征在于，所述构建一数据库的步骤包括:

由客户端计算机收集文件及其对应的文件信息，并传送至服务器端;

由服务器端对收集到的文件进行认证，通过认证的，将该文件及其对应的文件信息存储入数据库中。

3、如权利要求 2 所述的方法，其特征在于，所述由客户端计算机收集文件及其对应的文件信息步骤，进一步包括:

在客户端建立一收集文件列表，根据文件信息确认该文件已经收集过的，则不再重复收集。

4、如权利要求 2 所述的方法，其特征在于，所述由服务器端对收集到的文件进行认证的步骤，进一步包括:

在服务器端建立一认证文件列表，根据文件信息确认该文件已经认证过的，则不再重复认证。

5、如权利要求 1 所述的方法，其特征在于，所述将该染毒文件的信息与存储于所述数据库中的未染毒文件信息进行匹配的步骤，包括:

根据存储于数据库中的未染毒文件的信息类型，对应收集该染毒文件的信息;

将收集到的该染毒文件的信息与存储于所述数据库中的未染毒文件信息进行对应匹配，根据事先制定的匹配规则确定是否匹配成功。

6、如权利要求 1 所述的方法，其特征在于，所述替换所述染毒文件的步骤，包括:

确定染毒文件在该客户端计算机中的安装路径;

删除染毒文件，并根据所述安装路径安装所述未染毒文件。

7、如权利要求 1 所述的方法，其特征在于，所述文件信息包括文件名，文件路径，文件版本，操作系统，操作系统版本，及相关联到的应用程序组件信息中的至少其中之一。

8、如权利要求 7 所述的方法，其特征在于，所述文件信息进一步包括文件指纹。

9、如权利要求 8 所述的方法，其特征在于，进一步包括步骤:

将未染毒文件的文件指纹信息列入白名单，并将染毒文件的文件指纹信息列入黑名单，以辅助对未知程序的黑白判别。

10、一种清除恶意程序的装置，其特征在于，包括:

数据库模块，用于存储有未感染病毒的文件及其对应的文件信息;

匹配模块，用于当确认客户端计算机中某个文件被染毒后，将该染毒文件的信息与存储于所述数据库中的未染毒文件信息进行匹配;

替换模块，用于当匹配成功时，将所述数据库中的未染毒文件信息对应的未染毒文件加载至所述客户端计算机中，替换所述染毒文件。

11、如权利要求 10 所述的装置，其特征在于，进一步包括:

客户端收集单元，用于通过客户端计算机收集文件及其对应的文件信息，并传送至服务器端;

服务器端认证单元，用于通过服务器端对收集到的文件进行认证，通过认证的，将该文件及其对应的文件信息存储入数据库中。

12、如权利要求 11 所述的装置，其特征在于，所述客户端收集单元，进一步用于在客户端建立一收集文件列表，根据文件信息确认该文件已经收集过的，则不再重复收集。

13、如权利要求 11 所述的装置，其特征在于，所述服务器端认证单元，

进一步包括在服务器端建立一认证文件列表，根据文件信息确认该文件已经认证过的，则不再重复认证。

14、如权利要求 10 所述的装置，其特征在于，所述匹配模块，根据存储于数据库中的未染毒文件的信息类型，对应收集该染毒文件的信息，并将收集到的该染毒文件的信息与存储于所述数据库中的未染毒文件信息进行对应匹配，根据事先制定的匹配规则确定是否匹配成功。

15、如权利要求 10 所述的装置，其特征在于，所述替换模块，根据染毒文件在该客户端计算机中的安装路径，将未染毒文件加载至所述客户端计算机中，替换所述染毒文件。

16、如权利要求 10 所述的装置，其特征在于，所述文件信息包括文件名，文件路径，文件版本，操作系统，操作系统版本，及相关联到的应用程序组件信息中的至少其中之一。

17、如权利要求 16 所述的装置，其特征在于，所述文件信息进一步包括文件指纹。

18、如权利要求 17 所述的装置，其特征在于，所述数据库进一步包括黑/白名单，所述未染毒文件的文件指纹信息列入白名单，所述染毒文件的文件指纹信息列入黑名单，以辅助对未知程序的黑白判别。

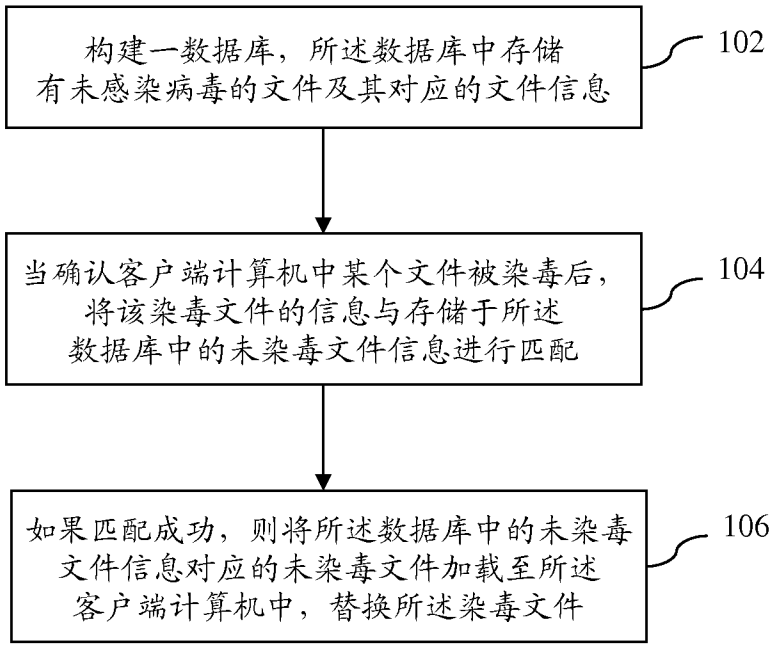

构建一数据库，所述数据库中存储有未感染病毒的文件及其对应的文件信息
102
当确认客户端计算机中某个文件被染毒后，将该染毒文件的信息与存储于所述数据库中的未染毒文件信息进行匹配
104
如果匹配成功，则将所述数据库中的未染毒文件信息对应的未染毒文件加载至所述客户端计算机中，替换所述染毒文件
106

图1

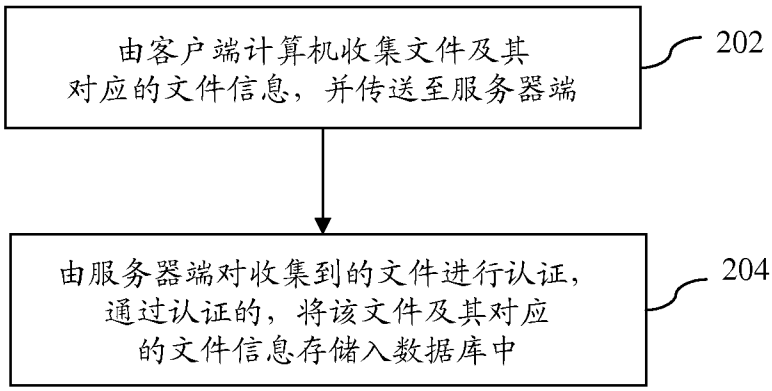

由客户端计算机收集文件及其对应的文件信息，并传送至服务器端
202
由服务器端对收集到的文件进行认证，通过认证的，将该文件及其对应的文件信息存储入数据库中
204

图2

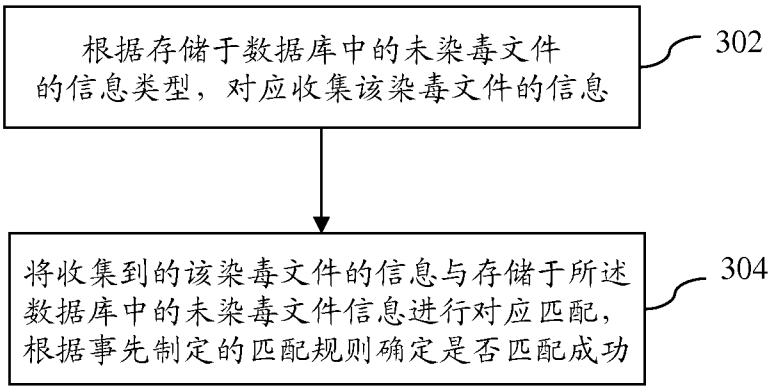

根据存储于数据库中的未染毒文件
的信息类型，对应收集该染毒文件的信息
302
将收集到的该染毒文件的信息与存储于所述
数据库中的未染毒文件信息进行对应匹配，
根据事先制定的匹配规则确定是否匹配成功
304

图 3

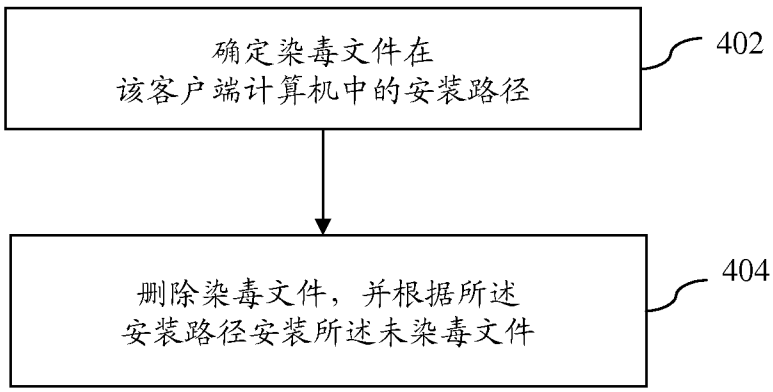

确定染毒文件在
该客户端计算机中的安装路径
402
删除染毒文件，并根据所述
安装路径安装所述未染毒文件
404

图 4

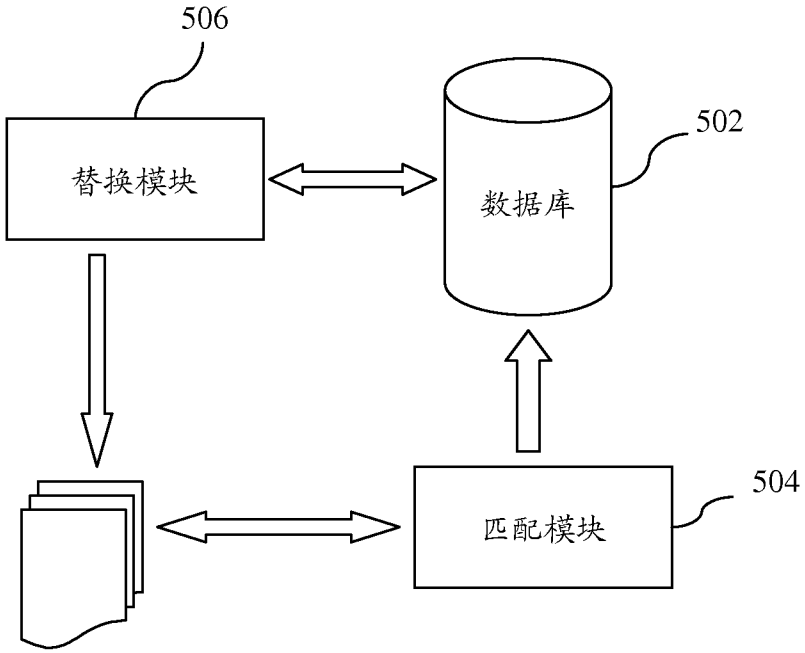


图5

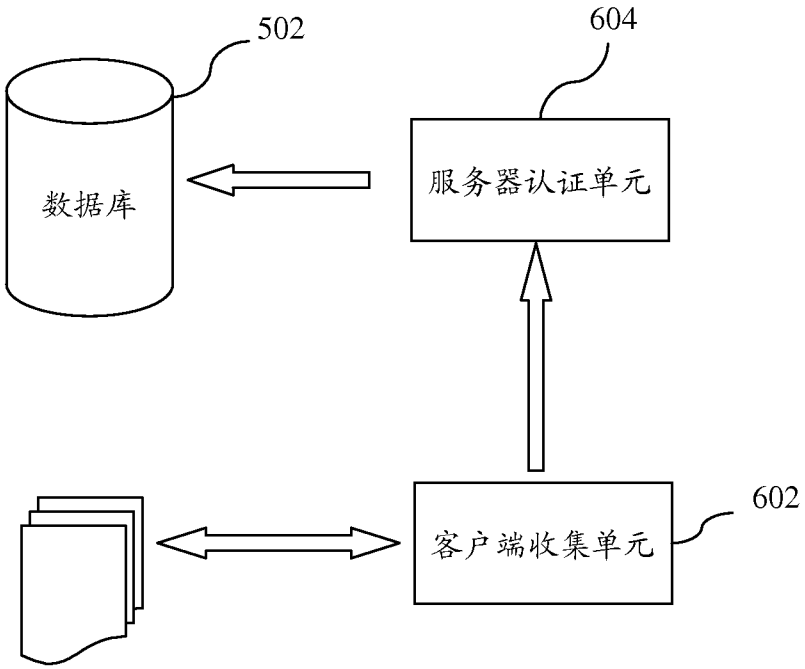


图6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2011/077366

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/00 (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, H04L

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)

CNKI, VEN, CPRSABS: infected by virus, virus, infect+, file, information, match, store, copy, backup, replace, authentication

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 101950336 A (QIZHI SOFTWARE (BEIJING) CO., LTD.), 19 January 2011 (19.01.2011), see claims 1-18	1-18
X	CN 101243400 A (EMC CORPORATION), 13 August 2008 (13.08.2008), see page 3, paragraph 4 to page 6, paragraph 1 of the description, claims 1-15 and figure 2	1, 5-10, 14-18
Y		2-4, 11-13
Y	CN 1595366 A (TIANJIN BRIWAVE SOFTWARE CO., LTD.), 16 March 2005 (16.03.2005), see page 2, paragraphs 1-5 of the description	2-4, 11-13
A	CN 1744607 A (GUANGZHOU RESEARCH INSTITUTE OF CHINA TELECOM CORPORATION LIMITED), 08 March 2006 (08.03.2006), see the whole document	1-18

☐ 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
08 September 2011 (08.09.2011)	**13 October 2011 (13.10.2011)**
Name and mailing address of the ISA/CN State Intellectual Property Office of the P.R.China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer **CHEN, Anan** Telephone No. (86-10) **62411828**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2011/077366

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN101950336A	19.01.2011	None	
CN101243400A	13.08.2008	WO2007022392A2	22.02.2007
		WO2007022392A3	04.10.2007
		US2008016564A1	17.01.2008
		EP1915719A2	30.04.2008
		JP2009505295T	05.02.2009
CN1595366A	16.03.2005	CN1315048C	09.05.2007
CN1744607A	08.03.2006	CN100464548C	25.02.2009

国际检索报告

国际申请号
PCT/CN2011/077366

A. 主题的分类

G06F21/00 (2006.01) i

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: G06F, H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)CNKI,VEN,CPRSABS,:病毒，感染，染毒，文件，信息，匹配，存储，拷贝，备份，替换，认证， virus, infect+, file, information, match, store, copy, backup, replace, authentication

C. 相关文件

类　型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN101950336A（奇智软件（北京）有限公司）19.1 月 2011（19.01.2011）参见权利要求 1-18	1-18
X	CN101243400A（EMC 公司）13.8 月 2008（13.08.2008）参见说明书第 3 页第 4 段-第 6 页第 1 段，权利要求 1-15，图 2	1，5-10，14-18
Y		2-4，11-13
Y	CN1595366A（天津百维软件科技有限公司）16.3 月 2005（16.03.2005）参见说明书第 2 页第 1-5 段	2-4，11-13
A	CN1744607A（广东省电信有限公司研究院）08.3 月 2006（08.03.2006）参见全文	1-18

☐ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
08.9 月 2011（08.09.2011）	**13.10 月 2011 (13.10.2011)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号：　(86-10)62019451	受权官员 **陈安安** 电话号码：(86-10) **62411828**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2011/077366

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN101950336A	19.01.2011	无	
CN101243400A	13.08.2008	WO2007022392A2	22.02.2007
		WO2007022392A3	04.10.2007
		US2008016564A1	17.01.2008
		EP1915719A2	30.04.2008
		JP2009505295T	05.02.2009
CN1595366A	16.03.2005	CN1315048C	09.05.2007
CN1744607A	08.03.2006	CN100464548C	25.02.2009