

(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
2014 年 1 月 3 日 (03.01.2014)



(10) 国际公布号
WO 2014/000616 A1

- (51) 国际专利分类号:
G06F 21/00 (2013.01)
- (21) 国际申请号: PCT/CN2013/077799
- (22) 国际申请日: 2013 年 6 月 24 日 (24.06.2013)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201210213332.9 2012 年 6 月 26 日 (26.06.2012) CN
- (71) 申请人: 腾讯科技(深圳)有限公司 (TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED) [CN/CN]; 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 403 室, Guangdong 518000 (CN)。
- (72) 发明人: 宋爱元 (SONG, Aiyuan); 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 403 室, Guangdong 518000 (CN)。 郭凌 (GUO, Ling); 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 403 室, Guangdong 518000 (CN)。
- (74) 代理人: 北京三高永信知识产权代理有限公司 (BEIJING SAN GAO YONG XIN INTELLECTUAL PROPERTY AGENCY CO., LTD.); 中国北京市

海淀区学院路蓟门里和景园 A-1-102, Beijing 100088 (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, 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, 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, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, 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, KM, 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: SCANNING METHOD AND DEVICE, AND CLIENT APPARATUS

(54) 发明名称: 扫描方法、装置和客户端设备

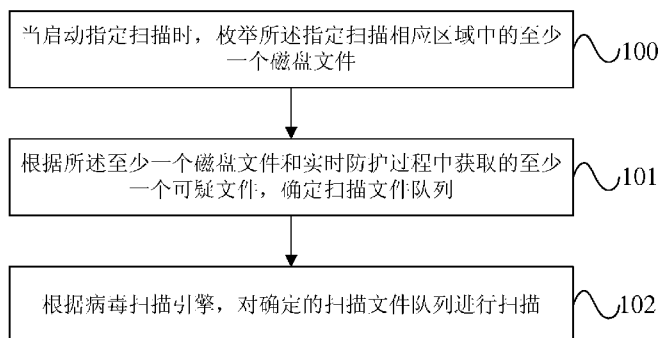


图 1 / FIG.1

- 100 When starting specified scanning, enumerate at least one disk file in an area corresponding to the specified scanning
- 101 Determine, according to the at least one disk file and at least one suspicious file obtained from a real-time protection process, a file scanning queue
- 102 Scan the determined file scanning queue according to a virus scan engine

(57) Abstract: The present invention relates to the field of computer security. Disclosed are a scanning method and device, and a client apparatus. The method comprises: when starting specified scanning, enumerating at least one disk file in an area corresponding to the specified scanning; determining, according to the at least one disk file and at least one suspicious file obtained from a real-time protection process, a file scanning queue; and scanning the determined file scanning queue according to a virus scan engine. The present invention re-determines a scanning queue according to a suspicious file pre-obtained from a real-time protection process, so as to perform full scanning of possible threats and realize thorough scanning and virus removal of files. Compared with the prior art, files can be thoroughly scanned, the capability of threat removal is improved, and the virus scanning and removal efficiency is enhanced.

(57) 摘要: 本发明公开了一种扫描方法、装置和客户端设备, 属于计算机安全领域。所述方法包括: 当启动指定扫描时, 枚举所述指定扫描相应区域中的至少一个磁盘文件; 根据所述至少一个磁盘文件和实时防护过程中获取的至少一个可疑文件, 确定扫描文件队列; 根据病毒扫描引擎, 对确定的扫描文件队列进行扫描。

本发明根据预先获取的实时防护过程中的可疑文件; 重新确定扫描队列, 以便对可能产生的威胁进行全面扫描, 实现对文件的彻底查杀, 与现有技术相比, 能够彻底扫描文件, 提高了清理威胁的能力, 提高病毒查找和清理过程的效率。

WO 2014/000616 A1

说明书

扫描方法、装置和客户端设备

本申请要求于 2012 年 06 月 26 日提交中国专利局、申请号为 201210213332.9、发明名称为“扫描方法和装置”的中国专利申请的优先权，
5 其全部内容通过引用结合在本申请中。

技术领域

本发明涉及计算机安全领域，特别涉及一种扫描方法、装置和客户端设备。

10 背景技术

计算机病毒（Computer Virus）是指：编制者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

15 随着计算机应用的普及以及互联网的快速发展，计算机病毒正在以惊人的速度蔓延。为了保护计算机的资源不受计算机病毒侵害，现有技术提供了安全软件，安全软件是一种可以对病毒、木马等一切已知的对计算机有危害的程序代码进行清除的程序工具。

安全软件的主要任务是实时防护和扫描文件。

20 实时防护，一般是指利用安全软件对系统运行的过程进行同步的监控，比如：杀毒软件对计算机内存监控并调用系统文件的一种操作模式。也即，安全软件在实时防护时，为了发现可能存在的病毒，安全软件中的应用程序将在对象被访问之前对它进行扫描，如果发现病毒，该应用程序会将染毒对象移除或阻止访问。

25 文件扫描，一般是指利用安全软件对计算机系统中磁盘和内存中的文件进行检查，以安全软件的判断为基础，来鉴别磁盘和内存中的文件是否符合安全软件的安全标准。

在实现本发明的过程中，发明人发现现有技术至少存在以下问题：

30 安全软件所提供的实时防护和文件扫描是相互独立工作的，即实时防护所负责的安全任务和文件扫描所负责的安全任务没有交流，这种工作模式便于安全软件的管理和应用，但是却让一些病毒钻了空子。比如现有存在一种母体行

病毒，这种病毒本身具备或者不具备破坏能力，但是它能释放出一个子程序或者子文件放到一个看似与之无关或者随机的文件目录下，而它释放出的这个子程序或者子文件具有破坏计算机或者盗取用户信息等有害的行为。目前的安全软件对于这样的病毒很难做到彻底清理，即只能清理掉该病毒释放出的子程序或子文件，对于这个藏在计算机某处的母体文件不能检查到并有效处理。以
5 至于用户在使用安全软件时会遇到这样几种情况：（1）实时防护功能发现了一个威胁并处理后，还能再次发现这个威胁；（2）文件扫描发现了一个威胁并处理后，还能再次发现这个威胁；（3）文件扫描发现并处理了一个威胁，还能再次发现一个类似的威胁；（4）实时防护拦截到一个威胁并处理后，文件扫描仍能扫描出这个威胁。现有的文件扫描，导致计算机系统内的病毒不能彻底清除，
10 严重影响了清理威胁的能力，使得病毒查找和清理过程效率低。

发明内容

为了彻底清除病毒，提高病毒查找和清理的效率，本发明实施例提供了一种扫描方法、装置和客户端设备。所述技术方案如下：
15

一种扫描方法，所述方法包括：

当启动指定扫描时，枚举所述指定扫描相应区域中的至少一个磁盘文件；

根据所述至少一个磁盘文件和实时防护过程中获取的至少一个可疑文件，确定扫描文件队列；

20 根据病毒扫描引擎，对确定的扫描文件队列进行扫描。

根据所述至少一个磁盘文件和实时防护过程中获取的至少一个可疑文件，确定扫描文件队列，包括：

根据所述至少一个可疑文件的文件信息，判断所述至少一个可疑文件的文件信息中是否包含所述至少一个磁盘文件中任一磁盘文件的文件名；

25 如果是，将文件信息包含所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件和所述至少一个磁盘文件加载至所述扫描文件队列；

如果否，将所述至少一个磁盘文件加载至所述扫描文件队列。

将文件信息包含所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件和所述至少一个磁盘文件加载至所述扫描文件队列，包括：

30 获取文件信息包含所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件在进行文件活动时涉及的文件，并将所述文件信息包含所述至少一个磁

盘文件中任一磁盘文件的文件名的可疑文件、进行文件活动时涉及的文件和所述至少一个磁盘文件加载至所述扫描文件队列。

根据所述至少一个磁盘文件和实时防护过程中获取的至少一个可疑文件，确定扫描文件队列，之前包括：

- 5 在实时防护过程中，获取可疑文件，将所述可疑文件的文件信息保存至指定区域，所述文件信息至少包括所述可疑文件的文件活动。

在实时防护过程中，获取可疑文件，将所述可疑文件的文件信息保存至指定区域，所述文件信息至少包括所述可疑文件的文件活动，之后包括：

- 10 将所述可疑文件的文件信息上传至服务器，使得所述服务器根据所述可疑文件的文件信息进行分析。

将所述可疑文件的文件信息上传至服务器，之后包括：

当确定所述可疑文件的文件信息上传成功时，从所述指定区域删除所述可疑文件的文件信息。

将所述可疑文件的文件信息上传至服务器，之后包括：

- 15 当确定所述可疑文件的文件信息上传失败时，压缩所述可疑文件的文件信息。

一种扫描装置，所述装置包括：

- 20 枚举模块，用于当启动指定扫描时，枚举所述指定扫描相应区域中的至少一个磁盘文件；

队列确定模块，用于根据所述至少一个磁盘文件和实时防护过程中获取的至少一个可疑文件，确定扫描文件队列；

扫描模块，用于根据病毒扫描引擎，对确定的扫描文件队列进行扫描。

所述队列确定模块包括：

- 25 判断单元，用于根据所述至少一个可疑文件的文件信息，判断所述至少一个可疑文件的文件信息中是否包含所述至少一个磁盘文件中任一磁盘文件的文件名；

- 30 加载单元，用于当所述至少一个可疑文件的文件信息中包含所述至少一个磁盘文件中任一磁盘文件的文件名，将文件信息包含所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件和所述至少一个磁盘文件加载至所述扫描文件队列；

所述加载单元,还用于当所述至少一个可疑文件的文件信息中不包含所述至少一个磁盘文件中任一磁盘文件的文件名,将所述至少一个磁盘文件加载至所述扫描文件队列。

5 所述加载单元还用于获取文件信息包含所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件在进行文件活动时涉及的文件,并将所述文件信息包含所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件、进行文件活动时涉及的文件和所述至少一个磁盘文件加载至所述扫描文件队列。

所述装置还包括:

10 获取模块,用于在实时防护过程中,获取可疑文件,将所述可疑文件的文件信息保存至指定区域,所述文件信息至少包括所述可疑文件的文件活动。

所述装置还包括:

上传模块,用于将所述可疑文件的文件信息上传至服务器,使得所述服务器根据所述可疑文件的文件信息进行分析。

所述装置还包括:

15 第一处理模块,用于当确定所述可疑文件的文件信息上传成功时,从所述指定区域删除所述可疑文件的文件信息。

所述装置还包括:

第二处理模块,用于当确定所述可疑文件的文件信息上传失败时,压缩所述可疑文件的文件信息。

20

一种客户端设备,所述客户端设备包括:

一个或多个处理器;和

存储器;

25 所述存储器存储有一个或多个程序,所述一个或多个程序被配置成由所述一个或多个处理器执行,所述一个或多个程序包含用于进行以下操作的指令:

当启动指定扫描时,枚举所述指定扫描相应区域中的至少一个磁盘文件;

根据所述至少一个磁盘文件和实时防护过程中获取的至少一个可疑文件,确定扫描文件队列;

根据病毒扫描引擎,对确定的扫描文件队列进行扫描。

30 优选地,还包含用于进行以下操作的指令;

根据所述至少一个可疑文件的文件信息,判断所述至少一个可疑文件的文

件信息中是否包含所述至少一个磁盘文件中任一磁盘文件的文件名；

如果是，将文件信息中包含有所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件和所述至少一个磁盘文件加载至所述扫描文件队列；

如果否，将所述至少一个磁盘文件加载至所述扫描文件队列。

5 优选地，还包含用于进行以下操作的指令：

获取文件信息中包含有所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件在进行文件活动时涉及的文件，并将所述文件信息中包含有所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件、进行文件活动时涉及的文件和所述至少一个磁盘文件加载至所述扫描文件队列。

10 优选地，还包含用于进行以下操作的指令：

在实时防护过程中，获取可疑文件，将所述可疑文件的文件信息保存至指定区域，所述文件信息至少包括所述可疑文件的文件活动。

优选地，还包含用于进行以下操作的指令：

15 将所述可疑文件的文件信息上传至服务器，使得所述服务器根据所述可疑文件的文件信息进行分析。

优选地，还包含用于进行以下操作的指令：

当确定所述可疑文件的文件信息上传成功时，从所述指定区域删除所述可疑文件的文件信息。

优选地，还包含用于进行以下操作的指令：

20 当确定所述可疑文件的文件信息上传失败时，压缩所述可疑文件的文件信息。

本发明实施例提供的技术方案带来的有益效果是：

25 通过当启动指定扫描时，枚举所述指定扫描相应区域中的至少一个磁盘文件；根据所述至少一个磁盘文件和实时防护过程中获取的至少一个可疑文件，确定扫描文件队列；根据病毒扫描引擎，对确定的扫描文件队列进行扫描。本发明实施例通过采用上述技术方案，能够将实时防护过程和文件扫描过程结合起来，避免了实时防护过程中获取的可疑文件由于指定扫描而被忽略，从而有效地避免了由于指定扫描的限制造成的病毒未被彻底清除的现象。而且采用本发明实施例中，根据预先获取的实时防护过程中的可疑文件；重新确定扫描队
30 列，以便对可能产生的威胁进行全面扫描，实现对文件的彻底查杀，与现有技术相比，能够彻底扫描文件，提高了清理威胁的能力，提高病毒查找和清理过

程的效率。

附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所
5 需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明
的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，
还可以根据这些附图获得其他的附图。

图 1 为本发明实施例提供的扫描方法的流程图；

图 2 为本发明实施例提供的扫描方法的流程图；

10 图 3 为本发明实施例提供的扫描装置的结构示意图；

图 4 为本发明实施例提供的扫描装置的结构示意图；

图 5 为本发明实施例提供的扫描装置的结构示意图；

图 6 为本发明实施例提供的客户端设备的结构示意图。

15 具体实施方式

为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明
实施方式作进一步地详细描述。

图 1 为本发明实施例提供的扫描方法的流程图。如图 1 所示，本实施例的
扫描方法的执行主体为客户端设备，该客户端设备可以是计算机。本实施例的
20 扫描方法，具体可以包括如下步骤：

100、当启动指定扫描时，枚举所述指定扫描相应区域中的至少一个磁盘
文件；

在本实施例中指定扫描泛指对设备进行的部分扫描，而不是全面扫描，指
定扫描可以为安全任务扫描或文件扫描。

25 安全任务扫描是指对内存和/或关键磁盘的扫描，其相应扫描区域是内存和
/或关键磁盘，其扫描对象是内存和/或关键磁盘的磁盘文件，例如关键磁盘为
C 盘，则安全任务扫描的相应扫描区域为内存和 C 盘，其扫描对象为内存的磁
盘文件和 C 盘中的磁盘文件。

而文件扫描是指对指定磁盘上的文件和/或指定磁盘位置的扫描，其相应扫
30 描区域是指定磁盘和/或指定磁盘位置，其扫描对象是指定磁盘和/或指定磁盘
位置的磁盘文件，例如指定磁盘为 D 盘，则文件扫描的相应扫描区域为 D 盘，

其扫描对象为 D 盘中的磁盘文件。

实际应用中，安全任务扫描的相应扫描区域可由技术人员设置，并由用户在使用中进行调整，文件扫描的相应扫描区域也可同理设置，本发明实施例不做具体限定。

5 需要说明的是，本实施例所述的“至少一个”是指一个或一个以上。

101、根据所述至少一个磁盘文件和实时防护过程中获取的至少一个可疑文件，确定扫描文件队列；

由于启动指定扫描时，其扫描的相应区域局限在该指定扫描的相应区域中，而实时防护过程中所获取的可疑文件可能不位于指定扫描的相应区域，则有可能忽略了该可疑文件，而产生安全隐患。因此，需要在枚举的至少一个磁盘文件的基础上，结合至少一个实时防护过程中获取的可疑文件，以便重新确定扫描文件队列，保障扫描的效率。

102、根据病毒扫描引擎，对确定的扫描文件队列进行扫描。

在本实施例中病毒扫描引擎可以为本地引擎，还可以为云端病毒扫描引擎，以供扫描时对扫描文件队列中的文件一一进行比对，以查杀与病毒扫描引擎中病毒特征相符的文件。

综上所述，本实施例提供的扫描方法，通过当启动指定扫描时，枚举所述指定扫描相应区域中的至少一个磁盘文件；根据所述至少一个磁盘文件和实时防护过程中获取的至少一个可疑文件，确定扫描文件队列；根据病毒扫描引擎，对确定的扫描文件队列进行扫描。本发明实施例通过采用上述技术方案，能够将实时防护过程和文件扫描过程结合起来，避免了实时防护过程中获取的可疑文件由于指定扫描的扫描范围的局限性而被忽略扫描的问题，从而有效地避免了由于指定扫描的限制造成的病毒未被彻底清除的现象。而且采用本发明实施例中，根据预先获取的实时防护过程中的可疑文件；重新确定扫描队列，以便对可能产生的威胁进行全面扫描，实现对文件的彻底查杀，与现有技术相比，能够彻底扫描文件，提高了清理威胁的能力，提高病毒查找和清理过程的效率。

可选地，在上述图 1 所示实施例的技术方案的基础上，其中步骤 101 “根据所述至少一个磁盘文件和实时防护过程中获取的至少一个可疑文件，确定扫描文件队列”具体可以包括：

30 (1) 根据所述至少一个可疑文件的文件信息，判断所述至少一个可疑文件的文件信息中是否包含所述至少一个磁盘文件中任一磁盘文件的文件名；

在本实施例中的可疑文件的文件信息至少包括该可疑文件的文件活动，该文件活动是指该可疑文件的运行、加载、生成或修改等。一旦可疑文件的文件信息包含磁盘文件的文件名，则说明该磁盘文件与可疑文件的文件活动相关。优选地，可疑文件和磁盘文件之间具有母文件与子文件的关系，则可疑文件的文件活动中的母体信息或子文件信息为磁盘文件的文件名。例如可疑文件 B 的文件信息中包含加载文件 B-plus 的文件名，则说明在可疑文件 B 的文件活动时，会加载至少一个磁盘文件中的磁盘文件 B-plus，则可获知，该可疑文件 B 与磁盘文件 B-plus 相关联。又如可疑文件为 C-plus，该可疑文件 C-plus 的文件信息中该可疑文件的来源信息为磁盘文件 C，也即是磁盘文件 C 活动时，会加载该可疑文件 C-plus，则可获知，该可疑文件 C-plus 与磁盘文件 C 相关联。再如可疑文件为 A，该可疑文件 A 的文件信息中的子文件信息为磁盘文件 A-1，则该可疑文件 A 为 A-1 的母文件，该可疑文件 A 与至少一个磁盘文件中的磁盘文件 A-1 相关联。

需要说明的是，该可疑文件的文件信息可在实时防护过程中获得并保存至指定区域，以供后续扫描过程中读取。

(2) 当所述至少一个可疑文件的文件信息中包含所述至少一个磁盘文件中任一磁盘文件的文件名时，将文件信息中包含有所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件和所述至少一个磁盘文件加载至所述扫描文件队列；

当确定了所述至少一个可疑文件的文件信息中包含所述至少一个磁盘文件中任一磁盘文件的文件名时，即确定了至少一个可疑文件中包括与所述至少一个磁盘文件中任一磁盘文件相关联的可疑文件。为了保障查杀效率，将该文件信息中包含有所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件和至少一个磁盘文件加载至扫描文件队列。

该文件信息中包含有所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件可以是一个或多个，本发明实施例不做具体限定。

(3) 当所述至少一个可疑文件的文件信息中不包含所述至少一个磁盘文件中任一磁盘文件的文件名时，将所述至少一个磁盘文件加载至所述扫描文件队列。

需要说明的是，本发明实施例中将文件加载至扫描文件队列的方法，详细可以参考现有技术，在此不再赘述。

可选地，在上述图 1 所示实施例的技术方案的基础上，步骤 101 中的步骤（2）“将文件信息中包含有所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件和所述至少一个磁盘文件加载至所述扫描文件队列”具体可以包括：获取文件信息中包含有所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件在进行文件活动时涉及的文件，并将所述文件信息中包含有所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件、进行文件活动时涉及的文件和所述至少一个磁盘文件加载至所述扫描文件队列。

在本实施例中，对于文件信息中包含有所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件来说，其文件活动还可能涉及到其他文件。因此，为了彻底清除威胁，需将与该可疑文件的文件活动相关的文件也加载至扫描文件队列。例如文件信息中包含有所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件为 B，在该可疑文件 B 的文件活动时，会加载至少一个磁盘文件中的磁盘文件 B-plus，还会加载位于 E 盘的磁盘文件 B-1 和 B-2，则在进行加载时，将可疑文件 B、磁盘文件 B-1 和 B-2 和至少一个磁盘文件加载至扫描文件队列。

需要说明的是，该文件信息中包含有所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件的文件信息可在实时防护过程中获得并保存至指定区域，以供后续扫描过程中读取。

另外，可疑文件的文件信息还可以包括可疑文件的文件来源、子文件名称和母体文件信息名称等。因此，通过步骤 101 中（1）的判断，还可以获知至少一个可疑文件中是否包含所述磁盘文件中任一磁盘文件的子文件或母文件。具体地，当可疑文件的文件信息中的文件来源、子文件名称和母体文件信息为所述至少一个磁盘文件中任一磁盘文件的文件名时，则该可疑文件的文件来源为磁盘文件，或该可疑文件的母体文件为磁盘文件，或可疑文件为磁盘文件的文件来源，或可疑文件为磁盘文件的母体文件等，则确定至少一个可疑文件中包含所述至少一个磁盘文件中任一磁盘文件的子文件或母文件。

需要说明的是，该可疑文件的文件信息可由服务器下发，并保存在指定区域。可选地，在上述实施例的技术方案的基础上，其中步骤 102 “根据所述至少一个磁盘文件和实时防护过程中获取的至少一个可疑文件，确定扫描文件队列”，之前还可以包括：

(a) 在实时防护过程中，获取可疑文件，将所述可疑文件的文件信息保存至指定区域，所述文件信息至少包括所述可疑文件的文件活动。

具体地，启动实时防护；检测磁盘文件的文件活动；当根据磁盘文件的文件活动获取到可疑文件时，判断该可疑文件是否已经被记录；如果是，则结束，
5 如果否，则将可疑文件记录为可疑文件，并将可疑文件的文件信息保存至指定区域。其中，判断该可疑文件是否已经被记录的方法在现有技术中可以有多种实现方式，本发明不一一赘述。

在本实施例中指定区域是指在磁盘上划分的用于保存可疑文件的文件信息的区域，该可疑文件的文件信息在实时防护过程中获取并保存，该指定区域的位置和容量均可以由技术人员、使用者设置或调整，本发明实施例不做具体限定。
10 可疑文件的文件活动包括但不限于以下任一文件活动：(i) 释放子文件，相应地，文件信息包括子文件名称、子文件存储路径、子文件修改时间和子文件建立时间中的至少一种。(ii) 加载文件，相应地，文件信息包括加载的文件名称和加载的文件路径中的至少一种。(iii) 可疑文件的建立或修改，相应地，
15 文件信息包括可疑文件的建立时间或修改时间、可疑文件的母体文件信息和母体文件路径中的至少一种。

需要说明的是，在实时防护过程中需要保存的文件信息可由技术人员设置或调整，该设置和调整均可通过软件更新实现，本发明实施例不做具体限定。

20 可选地，在上述实施例的技术方案的基础上，在上述步骤(a)“在实时防护过程中，获取可疑文件，将所述可疑文件的文件信息保存至指定区域，所述文件信息至少包括所述可疑文件的文件活动”，之后包括：(b) 将所述可疑文件的文件信息上传至服务器，使得所述服务器根据所述可疑文件的文件信息进行分析。

25 本实施例中的服务器可以为云端服务器，通过将可疑文件的文件信息上传至云端服务器，可以使得技术人员根据上传的可疑文件的文件信息对可疑文件的文件活动以及其病毒特征等进行分析，以供对病毒扫描引擎进行升级等处理，本实施例不做具体限定。进一步地，在将可疑文件的文件信息上传服务器时，可根据各个可疑文件的文件特征值判断服务器上是否已经保存有该可疑文件的文件信息；
30 如果是，则不上传该可疑文件的文件信息；如果否，则继续上传该可疑文件的文件信息。更进一步地，该上传过程的上传方式可以是周期性

上传，还可以每次实时保护过程结束时上传，还可以在检测到可疑文件的文件信息发生了更新以后上传，本实施例不做具体限定。

可选地，在上述实施例的技术方案的基础上，在上述步骤（b）“将所述可疑文件的文件信息上传至服务器”，之后包括：

（c）当确定所述可疑文件的文件信息上传成功时，从所述指定区域删除所述可疑文件的文件信息。

为了节省磁盘资源，当确定所述可疑文件的文件信息已经成功上传至服务器时，则删除可疑文件的文件信息。需要说明的是，确定文件信息是否上传成功为现有技术，在此不再赘述。

可选地，在上述实施例的技术方案的基础上，在上述步骤（b）“将所述可疑文件的文件信息上传至服务器”，之后包括：当确定所述可疑文件的文件信息上传失败时，压缩所述可疑文件的文件信息。

用户网络异常等原因可能导致步骤（b）的上传失败，则为了在不浪费磁盘资源的情况下保留文件信息，则对该文件信息做压缩处理。进一步地，当用户的网络恢复正常后，将该可疑文件的文件信息上传至服务器，并在本地将该文件信息做删除处理。

需要说明的是，上述所有可选技术方案可以采用互相结合的任何方式组成本发明实施例的可选技术方案，在此不再一一举例。

上述实施例通过采用上述技术方案，能够将实时防护过程和文件扫描过程结合起来，避免了实时防护过程中获取的可疑文件由于指定扫描的扫描范围局限性而被忽略扫描的问题，从而有效地避免了由于子母文件或指定扫描的限制造成的病毒未被彻底清除的现象。而且采用本发明实施例中，根据预先获取的实时防护过程中的可疑文件；重新确定扫描队列，以便对可能产生的威胁进行全面扫描，实现对文件的彻底查杀，与现有技术相比，能够彻底扫描文件，提高了清理威胁的能力，提高病毒查找和清理过程的效率。

图2为本发明实施例提供的扫描方法的流程图。本实施例的扫描以包括上述所有可选技术方案为例，更加详细地介绍本发明的技术方案。如图2所示，本实施例的扫描方法，具体可以包括如下步骤：

200、在实时防护过程中，获取可疑文件，将所述可疑文件的文件信息保存至指定区域，所述文件信息至少包括所述可疑文件的文件活动；执行201；

201、将所述可疑文件的文件信息上传至服务器，使得所述服务器根据所述可疑文件的文件信息进行分析；执行 202；

进一步地，将所述可疑文件的文件信息上传至服务器，之后包括：

当确定所述可疑文件的文件信息上传成功时，从所述指定区域删除所述可疑文件的文件信息。

进一步地，将所述可疑文件的文件信息上传至服务器，之后包括：

当确定所述可疑文件的文件信息上传失败时，压缩所述可疑文件的文件信息。

202、当启动指定扫描时，枚举所述指定扫描相应区域中的至少一个磁盘文件；执行 203；

203、根据所述至少一个可疑文件的文件信息，判断所述至少一个可疑文件的文件信息中是否包含所述至少一个磁盘文件中任一磁盘文件的文件名；如果是，执行 204；如果否，执行 205；

204、将文件信息中包含有所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件和所述至少一个磁盘文件加载至所述扫描文件队列，执行 206；

205、将所述至少一个磁盘文件加载至所述扫描文件队列，执行 206；

206、根据病毒扫描引擎，对确定的扫描文件队列进行扫描。

本发明实施例通过采用上述技术方案，能够将实时防护过程和文件扫描过程结合起来，避免了实时防护过程中获取的可疑文件由于指定扫描的扫描范围的局限性而被忽略扫描的问题，从而有效地避免了由于子母文件或指定扫描的限制造成的病毒未被彻底清除的现象。而且采用本发明实施例中，根据预先获取的实时防护过程中的可疑文件；重新确定扫描队列，以便对可能产生的威胁进行全面扫描，实现对文件的彻底查杀，与现有技术相比，能够彻底扫描文件，提高了清理威胁的能力，提高病毒查找和清理过程的效率。

图 3 为本发明实施例提供的扫描装置的结构示意图。如图 3 所示，所述扫描装置，具体可以包括：枚举模块 10、队列确定模块 11 和扫描模块 12。

枚举模块 10，用于当启动指定扫描时，枚举所述指定扫描相应区域中的至少一个磁盘文件；枚举模块 10 和队列确定模块 11 连接，队列确定模块 11，用于根据所述至少一个磁盘文件和实时防护过程中获取的至少一个可疑文件，确定扫描文件队列；队列确定模块 11 和扫描模块 12 连接，扫描模块 12，用于根

据病毒扫描引擎，对队列确定模块 11 确定的扫描文件队列进行扫描。

本实施例的扫描装置，通过采用上述模块实现文件扫描与上述相关方法实施例的实现机制相同，详细可以参考上述相关方法实施例的记载，在此不再赘述。

- 5 本实施例的扫描装置，能够将实时防护过程和文件扫描过程结合起来，避免了实时防护过程中获取的可疑文件由于指定扫描的扫描范围的局限性而被忽略扫描的问题，从而有效地避免了由于子母文件或指定扫描的限制造成的病毒未被彻底清除的现象。而且采用本发明实施例中，根据预先获取的实时防护过程中的可疑文件；重新确定扫描队列，以便对可能产生的威胁进行全面扫描，
- 10 实现对文件的彻底查杀，与现有技术相比，能够彻底扫描文件，提高了清理威胁的能力，提高病毒查找和清理过程的效率。

- 本实施例的扫描装置在上述图 3 所示实施例的基础上，进一步可以包括如下技术方案：所述队列确定模块 11 包括：判断单元和加载单元（图中未示），判断单元与加载单元连接，判断单元，用于根据所述至少一个可疑文件的文件
- 15 信息，判断所述至少一个可疑文件的文件信息中是否包含所述至少一个磁盘文件中任一磁盘文件的文件名；加载单元，用于当所述至少一个可疑文件的文件信息中包含所述至少一个磁盘文件中任一磁盘文件的文件名，将文件信息中包含有所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件和所述至少一个磁盘文件加载至所述扫描文件队列；所述加载单元，还用于当所述至少一个可疑文件的文件信息中不包含所述至少一个磁盘文件中任一磁盘文件的文件名，将所述至少一个磁盘文件加载至所述扫描文件队列。
- 20

- 进一步地，所述加载单元还用于获取文件信息包含所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件在进行文件活动时涉及的文件，并将所述文件信息包含所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件、进行文件活动时涉及的文件和所述至少一个磁盘文件加载至所述扫描文件队列。
- 25

图 4 为本发明实施例提供的扫描装置的结构示意图。如图 4 所示，本实施例的扫描装置在上述图 3 所示实施例的基础上，进一步可以包括如下技术方案。

- 如图 4 所示，本实施例的扫描装置中还包括获取模块 13，获取模块 13 和队列确定模块 11 连接，获取模块 13 用于在实时防护过程中，获取可疑文件，将所述可疑文件的文件信息保存至指定区域，所述文件信息至少包括所述可疑
- 30

文件的文件活动。

图 5 为本发明实施例提供的扫描装置的结构示意图。如图 5 所示，本实施例的扫描装置在上述图 4 所示实施例的基础上，进一步可以包括如下技术方案。

如图 5 所示，本实施例的扫描装置中还包括上传模块 14，上传模块 14 和获取模块 13 连接，上传模块 14 用于将所述可疑文件的文件信息上传至服务器，使得所述服务器根据所述可疑文件的文件信息进行分析。

可选地，本实施例的扫描装置中还包括第一处理模块（图中未示），用于当确定所述可疑文件的文件信息上传成功时，从所述指定区域删除所述可疑文件的文件信息。

可选地，本实施例的扫描装置中还包括第二处理模块（图中未示），用于当确定所述可疑文件的文件信息上传失败时，压缩所述可疑文件的文件信息。

本实施例的扫描装置，通过采用上述模块实现文件扫描与上述相关方法实施例的实现机制相同，详细可以参考上述相关方法实施例的记载，在此不再赘述。

本实施例的扫描装置，能够将实时防护过程和文件扫描过程结合起来，避免了实时防护过程中获取的可疑文件由于指定扫描的扫描范围的局限性而被忽略扫描的问题，从而有效地避免了由于子母文件或指定扫描的限制造成的病毒未被彻底清除的现象。而且采用本发明实施例中，根据预先获取的实时防护过程中的可疑文件；重新确定扫描队列，以便对可能产生的威胁进行全面扫描，实现对文件的彻底查杀，与现有技术相比，能够彻底扫描文件，提高了清理威胁的能力，提高病毒查找和清理过程的效率。

需要说明的是：上述实施例提供的扫描装置在扫描时，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将设备的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。另外，上述实施例提供的扫描的装置与扫描方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

上述扫描装置可以用于包括但不限于个人计算机的具有杀毒功能的任一客户端设备。

图 6 是本发明实施例涉及的客户端设备的结构示意图。所述客户端设备

600 可以为常规的台式计算机或者膝上型笔记本，所述客户端 600 包括中央处理单元（CPU）601、包括随机存取存储器（RAM）602 和只读存储器（ROM）603 的系统存储器 604，以及连接系统存储器 604 和中央处理单元 601 的系统总线 605。所述客户端设备 600 还包括帮助计算机内的各个器件之间传输信息的基本输入/输出系统（I/O 系统）606，和用于存储操作系统 613、应用程序 614 和其他程序模块 615 的大容量存储设备 607。

所述基本输入/输出系统 606 包括有用于显示信息的显示器 608 和用于用户输入信息的诸如鼠标、键盘之类的输入设备 609。其中所述显示器 608 和输入设备 609 都通过连接到系统总线 605 的输入输出控制器 610 连接到中央处理单元 601。所述基本输入/输出系统 606 还可以包括输入输出控制器 610 以用于接收和处理来自键盘、鼠标、或电子触控笔等多个其他设备的输入。类似地，输入输出控制器 610 还提供输出到显示屏、打印机或其他类型的输出设备。

所述大容量存储设备 607 通过连接到系统总线 605 的大容量存储控制器（未示出）连接到中央处理单元 601。所述大容量存储设备 607 及其相关联的计算机可读介质为客户提供非易失性存储。也就是说，所述大容量存储设备 607 可以包括诸如硬盘或者 CD-ROM 驱动器之类的计算机可读介质（未示出）。

不失一般性，所述计算机可读介质可以包括计算机存储介质和通信介质。计算机存储介质包括以用于存储诸如计算机可读指令、数据结构、程序模块或其他数据等信息的任何方法或技术实现的易失性和非易失性、可移动和不可移动介质。计算机存储介质包括 RAM、ROM、EPROM、EEPROM、闪存或其他固态存储其技术，CD-ROM、DVD 或其他光学存储、磁带盒、磁带、磁盘存储或其他磁性存储设备。当然，本领域技术人员可知所述计算机存储介质不局限于上述几种。上述的系统存储器 604 和大容量存储设备 607 可以统称为存储器。

根据本发明的各种实施例，所述客户端设备 600 还可以通过诸如因特网等网络连接到网络上的远程计算机运行。也即客户端设备 600 可以通过连接在所述系统总线 605 上的网络接口单元 611 连接到网络 612，或者说，也可以使用网络接口单元 111 来连接到其他类型的网络或远程计算机系统（未示出）。

所述存储器还包括一个或者一个以上的程序，所述一个或者一个以上程序存储于存储器中，且经配置以由一个或者一个以上中央处理单元 601 执行所述

一个或者一个以上程序包含用于执行图 1 所示实施例所提供的扫描方法和图 2 所示实施例所提供的扫描方法。

本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。所述计算机可读存储介质存储有一个或者一个以上程序，所述一个或者一个以上程序被一个或者一个以上的处理器用来执行图 1 所示实施例所提供的扫描方法和图 2 所示实施例所提供的扫描方法。

以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权 利 要 求 书

1、一种扫描方法，其特征在于，所述方法包括：

当启动指定扫描时，枚举所述指定扫描相应区域中的至少一个磁盘文件；

5 根据所述至少一个磁盘文件和实时防护过程中获取的至少一个可疑文件，
确定扫描文件队列；

根据病毒扫描引擎，对确定的扫描文件队列进行扫描。

2、根据权利要求 1 所述的方法，其特征在于，根据所述至少一个磁盘文件
10 和实时防护过程中获取的至少一个可疑文件，确定扫描文件队列，包括：

根据所述至少一个可疑文件的文件信息，判断所述至少一个可疑文件的文
件信息中是否包含所述至少一个磁盘文件中任一磁盘文件的文件名；

如果是，将文件信息中包含有所述至少一个磁盘文件中任一磁盘文件的文
件名的可疑文件和所述至少一个磁盘文件加载至所述扫描文件队列；

15 如果否，将所述至少一个磁盘文件加载至所述扫描文件队列。

3、根据权利要求 2 所述的方法，其特征在于，将文件信息包含所述至少一个
磁盘文件中任一磁盘文件的文件名的可疑文件和所述至少一个磁盘文件加载
至所述扫描文件队列，包括：

20 获取文件信息中包含有所述至少一个磁盘文件中任一磁盘文件的文件名的
可疑文件在进行文件活动时涉及的文件，并将所述文件信息中包含有所述至少
一个磁盘文件中任一磁盘文件的文件名的可疑文件、进行文件活动时涉及的文
件和所述至少一个磁盘文件加载至所述扫描文件队列。

25 4、根据权利要求 1-3 任一项所述的方法，其特征在于，根据所述至少一个
磁盘文件和实时防护过程中获取的至少一个可疑文件，确定扫描文件队列，之
前包括：

在实时防护过程中，获取可疑文件，将所述可疑文件的文件信息保存至指
定区域，所述文件信息至少包括所述可疑文件的文件活动。

30 5、根据权利要求 4 所述的方法，其特征在于，在实时防护过程中，获取可

疑文件，将所述可疑文件的文件信息保存至指定区域，所述文件信息至少包括所述可疑文件的文件活动，之后包括：

将所述可疑文件的文件信息上传至服务器，使得所述服务器根据所述可疑文件的文件信息进行分析。

5

6、根据权利要求5所述的方法，其特征在于，将所述可疑文件的文件信息上传至服务器，之后包括：

当确定所述可疑文件的文件信息上传成功时，从所述指定区域删除所述可疑文件的文件信息。

10

7、根据权利要求5所述的方法，其特征在于，将所述可疑文件的文件信息上传至服务器，之后包括：

当确定所述可疑文件的文件信息上传失败时，压缩所述可疑文件的文件信息。

15

8、一种扫描装置，其特征在于，所述装置包括：

枚举模块，用于当启动指定扫描时，枚举所述指定扫描相应区域中的至少一个磁盘文件；

20 队列确定模块，用于根据所述至少一个磁盘文件和实时防护过程中获取的至少一个可疑文件，确定扫描文件队列；

扫描模块，用于根据病毒扫描引擎，对确定的扫描文件队列进行扫描。

9、根据权利要求8所述的装置，其特征在于，所述队列确定模块包括：

25 判断单元，用于根据所述至少一个可疑文件的文件信息，判断所述至少一个可疑文件的文件信息中是否包含所述至少一个磁盘文件中任一磁盘文件的文件名；

30 加载单元，用于当所述至少一个可疑文件的文件信息中包含所述至少一个磁盘文件中任一磁盘文件的文件名，将文件信息包含所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件和所述至少一个磁盘文件加载至所述扫描文件队列；

所述加载单元，还用于当所述至少一个可疑文件的文件信息中不包含所述

至少一个磁盘文件中任一磁盘文件的文件名,将所述至少一个磁盘文件加载至所述扫描文件队列。

10、根据权利要求 9 所述的装置,其特征在于,所述加载单元还用于获取文件信息包含所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件在进行文件活动时涉及的文件,并将所述文件信息包含所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件、进行文件活动时涉及的文件和所述至少一个磁盘文件加载至所述扫描文件队列。

11、根据权利要求 8-10 任一项所述的装置,其特征在于,所述装置还包括:获取模块,用于在实时防护过程中,获取可疑文件,将所述可疑文件的文件信息保存至指定区域,所述文件信息至少包括所述可疑文件的文件活动。

12、根据权利要求 11 所述的装置,其特征在于,所述装置还包括:上传模块,用于将所述可疑文件的文件信息上传至服务器,使得所述服务器根据所述可疑文件的文件信息进行分析。

13、根据权利要求 12 所述的装置,其特征在于,所述装置还包括:第一处理模块,用于当确定所述可疑文件的文件信息上传成功时,从所述指定区域删除所述可疑文件的文件信息。

14、根据权利要求 13 所述的装置,其特征在于,所述装置还包括:第二处理模块,用于当确定所述可疑文件的文件信息上传失败时,压缩所述可疑文件的文件信息。

15、一种客户端设备,其特征在于,所述客户端设备包括:
一个或多个处理器;和
存储器;

所述存储器存储有一个或多个程序,所述一个或多个程序被配置成由所述一个或多个处理器执行,所述一个或多个程序包含用于进行以下操作的指令:
当启动指定扫描时,枚举所述指定扫描相应区域中的至少一个磁盘文件;

根据所述至少一个磁盘文件和实时防护过程中获取的至少一个可疑文件，确定扫描文件队列；

根据病毒扫描引擎，对确定的扫描文件队列进行扫描。

- 5 16、根据权利要求 15 所述的客户端设备，其特征在于，还包含用于进行以下操作的指令；

根据所述至少一个可疑文件的文件信息，判断所述至少一个可疑文件的文件信息中是否包含所述至少一个磁盘文件中任一磁盘文件的文件名；

- 10 如果是，将文件信息中包含有所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件和所述至少一个磁盘文件加载至所述扫描文件队列；

如果否，将所述至少一个磁盘文件加载至所述扫描文件队列。

17、根据权利要求 16 所述的客户端设备，其特征在于，还包含用于进行以下操作的指令：

- 15 获取文件信息中包含有所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件在进行文件活动时涉及的文件，并将所述文件信息中包含有所述至少一个磁盘文件中任一磁盘文件的文件名的可疑文件、进行文件活动时涉及的文件和所述至少一个磁盘文件加载至所述扫描文件队列。

- 20 18、根据权利要求 15-17 任一项所述的客户端设备，其特征在于，还包含用于进行以下操作的指令：

在实时防护过程中，获取可疑文件，将所述可疑文件的文件信息保存至指定区域，所述文件信息至少包括所述可疑文件的文件活动。

- 25 19、根据权利要求 18 所述的客户端设备，其特征在于，还包含用于进行以下操作的指令：

将所述可疑文件的文件信息上传至服务器，使得所述服务器根据所述可疑文件的文件信息进行分析。

- 30 20、根据权利要求 19 所述的客户端设备，其特征在于，还包含用于进行以下操作的指令：

当确定所述可疑文件的文件信息上传成功时，从所述指定区域删除所述可疑文件的文件信息。

21、根据权利要求 19 所述的客户端设备，其特征在于，还包含用于进行以下操作的指令：

当确定所述可疑文件的文件信息上传失败时，压缩所述可疑文件的文件信息。

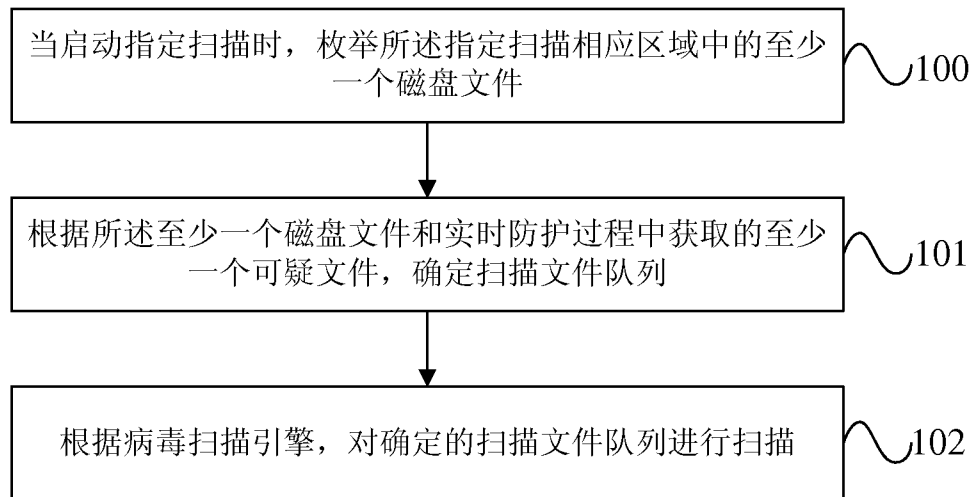


图 1

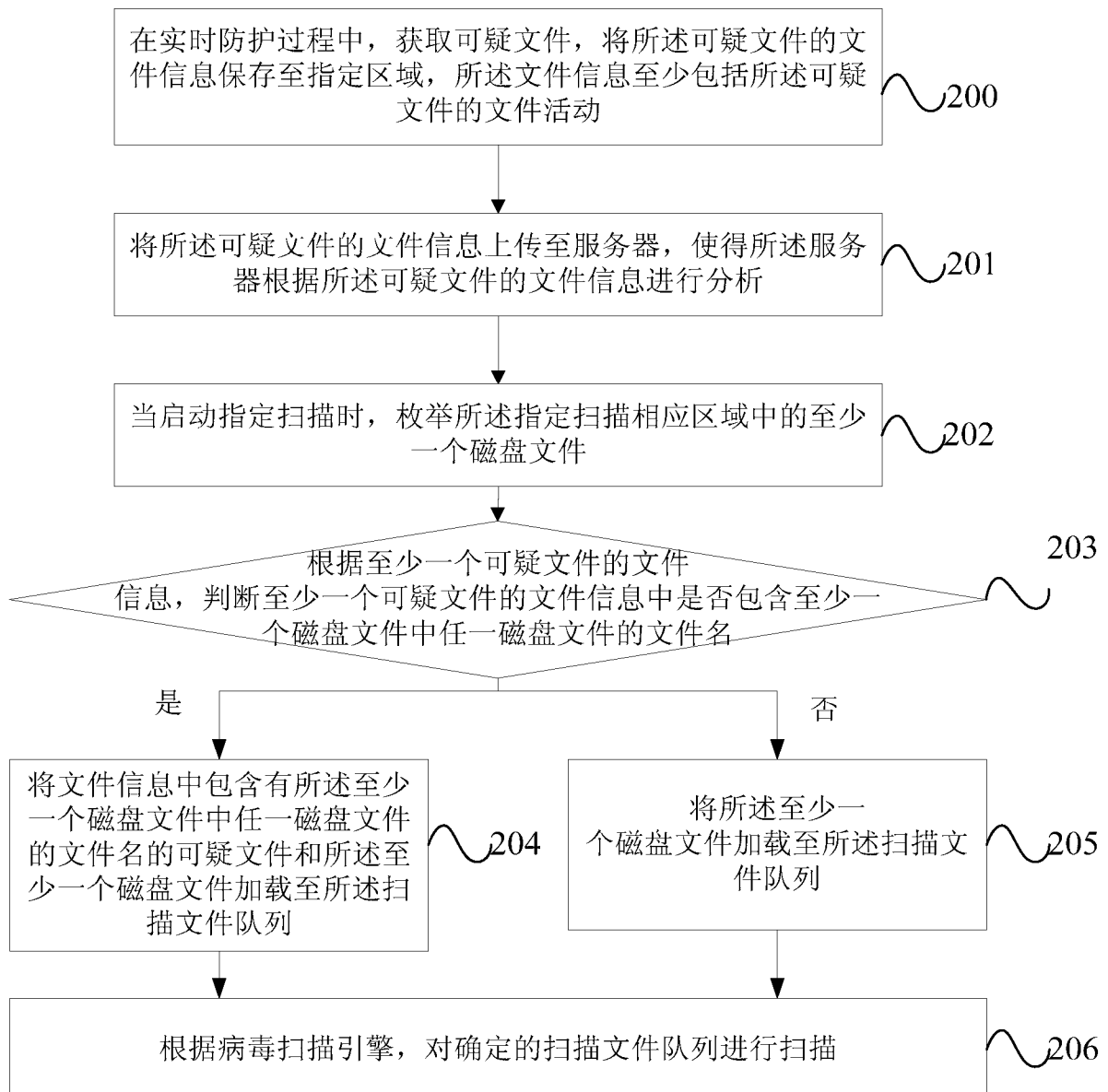


图 2

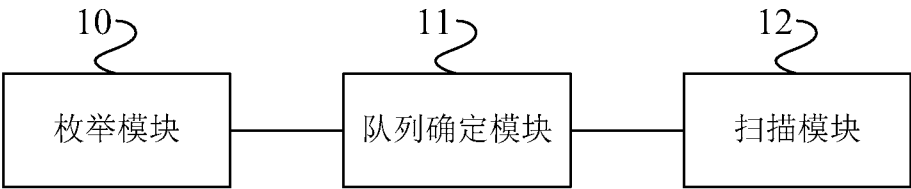


图 3

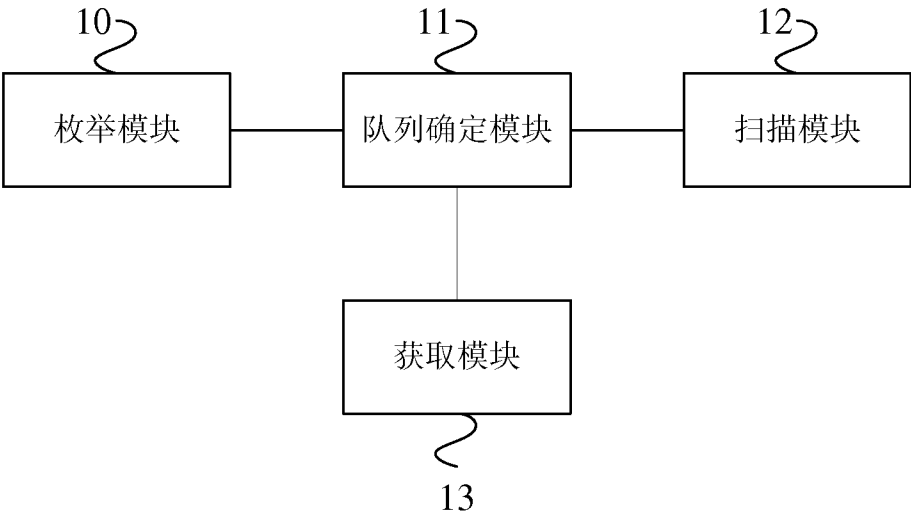


图 4

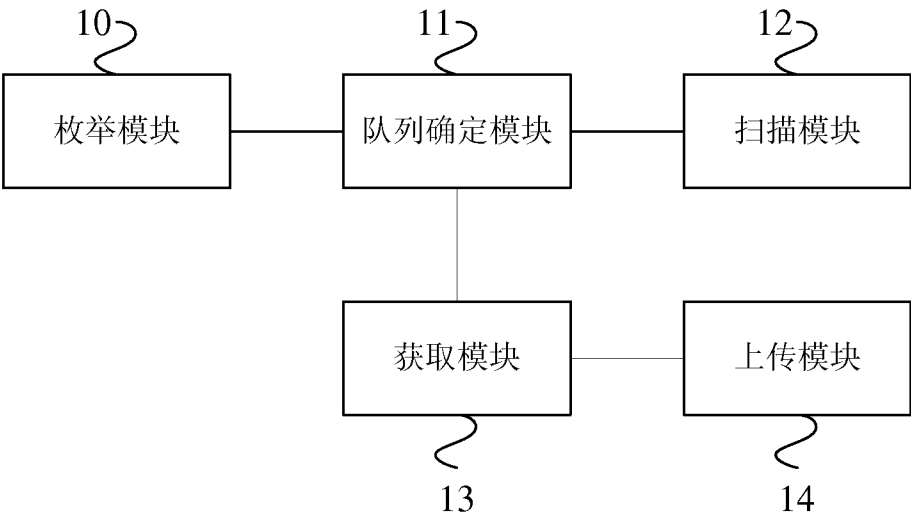


图 5

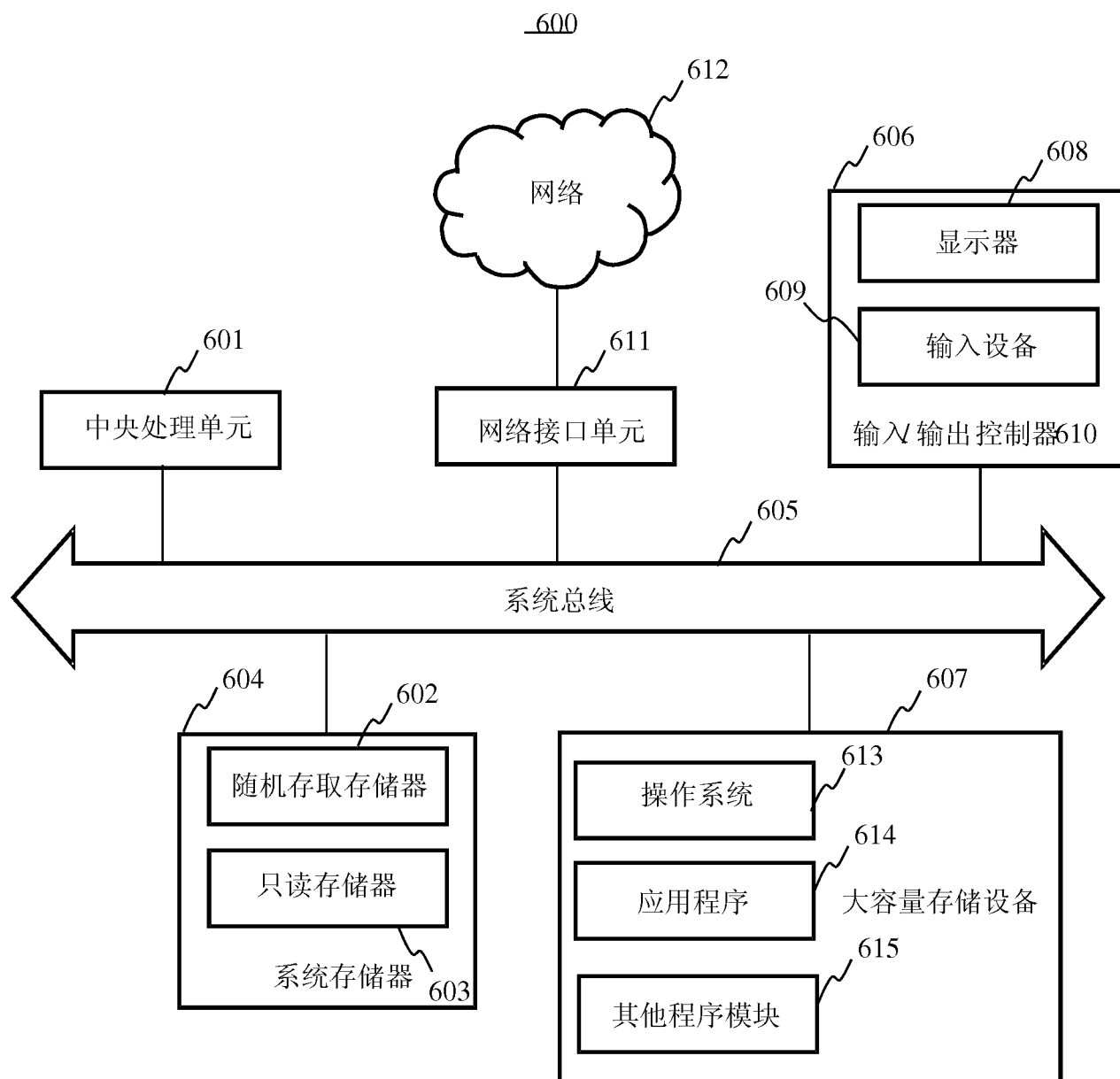


图 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/077799

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/00 (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; 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)

WPI, EPODOC, GOOGLE, CNPAT, CNKI, IEEE: protection, scan, search, kill, real-time, virus, suspicious, safe, enumerate, file, array, queue, engine

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 102799811 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 28 November 2012 (28.11.2012), the whole document	1-21
X	CN 102194073 A (QIZHI SOFTWARE (BEIJING) CO., LTD.), 21 September 2011 (21.09.2011), description, paragraphs [0054]-[0091]	1-21
A	CN 102012992 A (QIZHI SOFTWARE (BEIJING) CO., LTD.), 13 April 2011 (13.04.2011), the whole document	1-21
A	US 7681237 B1 (SYMANTEC CORPORATION), 16 March 2010 (16.03.2010), the whole document	1-21
A	US 6968461 B1 (NETWORKS ASSOCIATES TECHNOLOGY, INC.), 22 November 2005 (22.11.2005), the whole document	1-21

☐ 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 10 September 2013 (10.09.2013)	Date of mailing of the international search report 26 September 2013 (26.09.2013)
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 WU, Shaohong Telephone No.: (86-10) 62413694

International application No.
PCT/CN2013/077799

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

国际检索报告

国际申请号

PCT/CN2013/077799

A. 主题的分类

G06F 21/00 (2013.01) 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))

WPI, EPODOC, GOOGLE, CNPAT, CNKI, IEEE: 扫描, 查, 杀, 实时, 防护, 毒, 可疑, 安全, 枚举, 文件, 队列, 引擎, scan, search, kill, real-time, virus, suspicious, safe, enumerate, file, array, queue, engine

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	CN 102799811 A (腾讯科技(深圳)有限公司) 28.11 月 2012 (28.11.2012) 全文	1-21
X	CN 102194073 A (奇智软件(北京)有限公司) 21.9 月 2011 (21.09.2011) 说明书 [0054]-[0091]段	1-21
A	CN 102012992 A (奇智软件(北京)有限公司) 13.4 月 2011 (13.04.2011) 全文	1-21
A	US 7681237 B1 (SYMANTEC CORPORATION) 16.3 月 2010 (16.03.2010) 全文	1-21
A	US 6968461 B1 (NETWORKS ASSOCIATES TECHNOLOGY, INC.) 22.11 月 2005 (22.11.2005) 全文	1-21



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

10.9 月 2013 (10.09.2013)

国际检索报告邮寄日期

26.9 月 2013 (26.09.2013)

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

授权官员

吴少鸿

电话号码: (86-10) **62413694**

关于同族专利的信息

PCT/CN2013/077799

无