(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102799811 A
(43)申请公布日 2012.11.28

(21)申请号 201210213332.9

(22)申请日 2012.06.26

(71)申请人 腾讯科技(深圳)有限公司
地址 518000 广东省深圳市福田区赛格科技园 2 栋东 403 室

(72)发明人 宋爱元 郭凌

(74)专利代理机构 北京三高永信知识产权代理有限责任公司 11138
代理人 鞠永善

(51)Int.Cl.
G06F 21/00(2006.01)

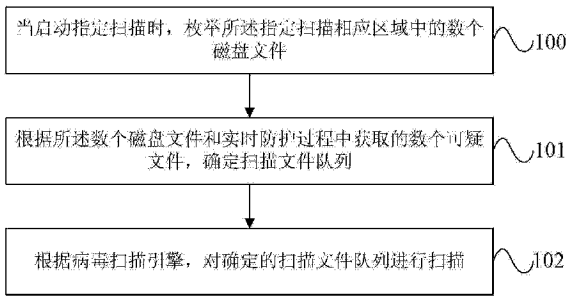
权利要求书 2 页 说明书 9 页 附图 3 页

(54)发明名称

扫描方法和装置

(57)摘要

本发明公开了一种扫描方法和装置，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数个磁盘文件；根据所述数个磁盘文件和实时防护过程中获取的数个可疑文件，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。



CN 102799811 A

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数个磁盘文件；

根据所述数个磁盘文件和实时防护过程中获取的数个可疑文件，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，根据所述数个磁盘文件和实时防护过程中获取的数个可疑文件，确定扫描文件队列，包括：

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

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

如果否，将所述数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数个磁盘文件中任一磁盘文件的文件名的可疑文件和所述数个磁盘文件加载至所述扫描文件队列，包括：

获取文件信息包含所述数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数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数个磁盘文件加载至所述扫描文件队列。

4. 根据权利要求 1-3 任一项所述的方法，其特征在于，根据所述数个磁盘文件和实时防护过程中获取的数个可疑文件，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。

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。

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。

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。

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数个磁盘文件；

队列确定模块，用于根据所述数个磁盘文件和实时防护过程中获取的数个可疑文件，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：

判断单元，用于根据所述数个可疑文件的文件信息，判断所述数个可疑文件的文件信

息中是否包含所述数个磁盘文件中任一磁盘文件的文件名；

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

所述加载单元，还用于当所述数个可疑文件的文件信息中不包含所述数个磁盘文件中任一磁盘文件的文件名，将所述数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数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数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数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。

扫描方法和装置

技术领域

[0001] 本发明涉及计算机安全领域，特别涉及一种扫描方法和装置。

背景技术

[0002] 计算机病毒（Computer Virus）在《中华人民共和国计算机信息系统安全保护条例》中被明确定义，病毒指“编制者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。与医学上的“病毒”不同，计算机病毒不是天然存在的，是某些人利用计算机系统中软件和硬件所固有的脆弱性编制的一组指令集或程序代码。它能通过某种途径潜伏在计算机的存储介质（或程序）里，当达到某种条件时即被激活，通过修改其他程序的方法将自己的精确拷贝或者可能演化的形式放入其他程序中，从而感染其他程序，对计算机资源进行破坏，所谓的病毒就是人为造成的，对其他用户的危害性很大。

[0003] 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。

[0004] 安全软件的主要任务是实时防护和扫描文件。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。由于病毒的存在，程序将在对象访问之前对它进行扫描，如果发现病毒，应用程序会将染毒对象移除或阻止访问。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。

[0005] 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：

[0006] 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，以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后，还能再次发现这个威胁；（2）文件扫描发现了一个威胁后，还能再次发现这个威胁；（3）文件扫描发现了一个威胁，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，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

[0007] 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、和装置。所述技术方案如下：

[0008] 一种扫描方法，所述方法包括：

[0009] 当启动指定扫描时，枚举所述指定扫描相应区域中的数个磁盘文件；

[0010] 根据所述数个磁盘文件和实时防护过程中获取的数个可疑文件，确定扫描文件队列；

[0011] 根据病毒扫描引擎，对确定的扫描文件队列进行扫描。

[0012] 根据所述数个磁盘文件和实时防护过程中获取的数个可疑文件，确定扫描文件队列，包括：

[0013] 根据所述数个可疑文件的文件信息，判断所述数个可疑文件的文件信息中是否包含所述数个磁盘文件中任一磁盘文件的文件名；

[0014] 如果是，将文件信息包含所述数个磁盘文件中任一磁盘文件的文件名的可疑文件和所述数个磁盘文件加载至所述扫描文件队列；

[0015] 如果否，将所述数个磁盘文件加载至所述扫描文件队列。

[0016] 将文件信息包含所述数个磁盘文件中任一磁盘文件的文件名的可疑文件和所述数个磁盘文件加载至所述扫描文件队列，包括：

[0017] 获取文件信息包含所述数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数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数个磁盘文件加载至所述扫描文件队列。

[0018] 根据所述数个磁盘文件和实时防护过程中获取的数个可疑文件，确定扫描文件队列，之前包括：

[0019] 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。

[0020] 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：

[0021] 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。

[0022] 将所述可疑文件的文件信息上传至服务器，之后包括：

[0023] 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。

[0024] 将所述可疑文件的文件信息上传至服务器，之后包括：

[0025] 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。

[0026] 一种扫描装置，所述装置包括：

[0027] 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数个磁盘文件；

[0028] 队列确定模块，用于根据所述数个磁盘文件和实时防护过程中获取的数个可疑文件，确定扫描文件队列；

[0029] 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。

[0030] 所述队列确定模块包括：

[0031] 判断单元，用于根据所述数个可疑文件的文件信息，判断所述数个可疑文件的文件信息中是否包含所述数个磁盘文件中任一磁盘文件的文件名；

[0032] 加载单元，用于当所述数个可疑文件的文件信息中包含所述数个磁盘文件中任一

磁盘文件的文件名，将文件信息包含所述数个磁盘文件中任一磁盘文件的文件名的可疑文件和所述数个磁盘文件加载至所述扫描文件队列；

[0033] 所述加载单元，还用于当所述数个可疑文件的文件信息中不包含所述数个磁盘文件中任一磁盘文件的文件名，将所述数个磁盘文件加载至所述扫描文件队列。

[0034] 所述加载单元还用于获取文件信息包含所述数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数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数个磁盘文件加载至所述扫描文件队列。

[0035] 所述装置还包括：

[0036] 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。

[0037] 所述装置还包括：

[0038] 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。

[0039] 所述装置还包括：

[0040] 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。

[0041] 所述装置还包括：

[0042] 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。

[0043] 本发明实施例提供的技术方案带来的有益效果是：

[0044] 通过当启动指定扫描时，枚举所述指定扫描相应区域中的数个磁盘文件；根据所述数个磁盘文件和实时防护过程中获取的数个可疑文件，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

[0045] 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。

[0046] 图 1 为本发明实施例提供的扫描方法的流程图；

[0047] 图 2 为本发明实施例提供的扫描方法的流程图；

[0048] 图 3 为本发明实施例提供的扫描装置的结构示意图；

[0049] 图 4 为本发明实施例提供的扫描装置的结构示意图；

[0050] 图 5 为本发明实施例提供的扫描装置的结构示意图。

具体实施方式

[0051] 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。

[0052] 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如计算机。本实施例的扫描方法，具体可以包括如下步骤：

[0053] 100、当启动指定扫描时，枚举所述指定扫描相应区域中的数个磁盘文件；

[0054] 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，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。

[0055] 需要说明的是，本实施例所述的“数个”是指一个或一个以上。

[0056] 101、根据所述数个磁盘文件和实时防护过程中获取的数个可疑文件，确定扫描文件队列；

[0057] 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，需要在枚举的数个磁盘文件的基础上，结合数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。

[0058] 102、根据病毒扫描引擎，对确定的扫描文件队列进行扫描。

[0059] 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。

[0060] 通过当启动指定扫描时，枚举所述指定扫描相应区域中的数个磁盘文件；根据所述数个磁盘文件和实时防护过程中获取的数个可疑文件，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。

[0061] 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“根据所述数个磁盘文件和实时防护过程中获取的数个可疑文件，确定扫描文件队列”具体可以包括：

[0062] （1）根据所述数个可疑文件的文件信息，判断所述数个可疑文件的文件信息中是

否包含所述数个磁盘文件中任一磁盘文件的文件名；

[0063] 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，会加载数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 与数个磁盘文件中的磁盘文件 A-1 相关联。

[0064] 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。

[0065] （2）当所述数个可疑文件的文件信息中包含所述数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数个磁盘文件中任一磁盘文件的文件名的可疑文件和所述数个磁盘文件加载至所述扫描文件队列；

[0066] 当确定了所述数个可疑文件的文件信息中包含所述数个磁盘文件中任一磁盘文件的文件名时，即确定了数个可疑文件中包括与所述数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，将该文件信息包含所述数个磁盘文件中任一磁盘文件的文件名的可疑文件和数个磁盘文件加载至扫描文件队列。

[0067] 该文件信息包含所述数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。

[0068] （3）当所述数个可疑文件的文件信息中不包含所述数个磁盘文件中任一磁盘文件的文件名，将所述数个磁盘文件加载至所述扫描文件队列。

[0069] 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。

[0070] 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）“将文件信息包含所述数个磁盘文件中任一磁盘文件的文件名的可疑文件和所述数个磁盘文件加载至所述扫描文件队列”具体可以包括：获取文件信息包含所述数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数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数个磁盘文件加载至所述扫描文件队列。

[0071] 在本实施例中对于文件信息包含所述数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。例如文件信息包含所述数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，会加载数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 和数个磁盘文件加载至扫描文件队列。

[0072] 需要说明的是，该文件信息包含所述数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。

[0073] 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，还可以获知数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数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，则确定数个可疑文件中包含所述数个磁盘文件中任一磁盘文件的子文件或母文件。

[0074] 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 “根据所述数个磁盘文件和实时防护过程中获取的数个可疑文件，确定扫描文件队列”，之前还可以包括 ：

[0075] （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。

[0076] 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，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。

[0077] 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。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、子文件修改时间或子文件建立时间。（ⅱ）加载文件，相应地，文件信息包括加载的文件名称、加载的文件路径。（iii）可疑文件的建立或修改，相应地，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、母体文件路径。

[0078] 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。

[0079] 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。

[0080] 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可疑文件的文件信息，如果是，则不上传可疑文件的文件信息，如果否，则继续上传可疑文件的文件信息。更近一步地，该上传可以是周期性上传，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。

[0081] 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：

[0082] （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。

[0083] 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。

[0084] 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。

[0085] 用户网络异常等原因可能导致（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。

[0086] 需要说明的是，上述所有可选技术方案可以采用可以结合的任意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。

[0087] 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而被忽略，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。

[0088] 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：

[0089] 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；

[0090] 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；

[0091] 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：

[0092] 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。

[0093] 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：

[0094] 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。

[0095] 202、当启动指定扫描时，枚举所述指定扫描相应区域中的数个磁盘文件；执行 203；

[0096] 203、根据所述数个可疑文件的文件信息，判断所述数个可疑文件的文件信息中是否包含所述数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；

[0097] 204、将文件信息包含所述数个磁盘文件中任一磁盘文件的文件名的可疑文件和

所述数个磁盘文件加载至所述扫描文件队列，执行 206 ；

[0098] 205、将所述数个磁盘文件加载至所述扫描文件队列，执行 206 ；

[0099] 206、根据病毒扫描引擎，对确定的扫描文件队列进行扫描。

[0100] 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。

[0101] 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。

[0102] 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数个磁盘文件 ；枚举模块 10 和队列确定模块 11 连接，队列确定模块 11，用于根据所述数个磁盘文件和实时防护过程中获取的数个可疑文件，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。

[0103] 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。

[0104] 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而被忽略，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。

[0105] 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，用于根据所述数个可疑文件的文件信息，判断所述数个可疑文件的文件信息中是否包含所述数个磁盘文件中任一磁盘文件的文件名 ；加载单元，用于当所述数个可疑文件的文件信息中包含所述数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数个磁盘文件中任一磁盘文件的文件名的可疑文件和所述数个磁盘文件加载至所述扫描文件队列 ；所述加载单元，还用于当所述数个可疑文件的文件信息中不包含所述数个磁盘文件中任一磁盘文件的文件名，将所述数个磁盘文件加载至所述扫描文件队列。

[0106] 进一步地，所述加载单元还用于获取文件信息包含所述数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数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数个磁盘文件加载至所述扫描文件队列。

[0107] 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。

[0108] 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文件的文件活动。

[0109] 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。

[0110] 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。

[0111] 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。

[0112] 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。

[0113] 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。

[0114] 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而被忽略，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。

[0115] 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。

[0116] 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。

[0117] 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。

[0118] 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。

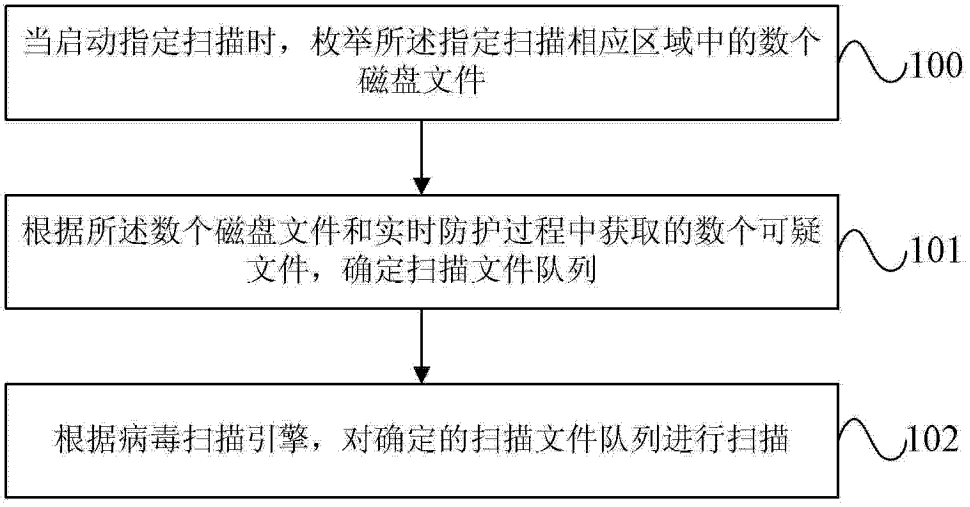

当启动指定扫描时，枚举所述指定扫描相应区域中的数个磁盘文件
100
根据所述数个磁盘文件和实时防护过程中获取的数个可疑文件，确定扫描文件队列
101
根据病毒扫描引擎，对确定的扫描文件队列进行扫描
102

图 1

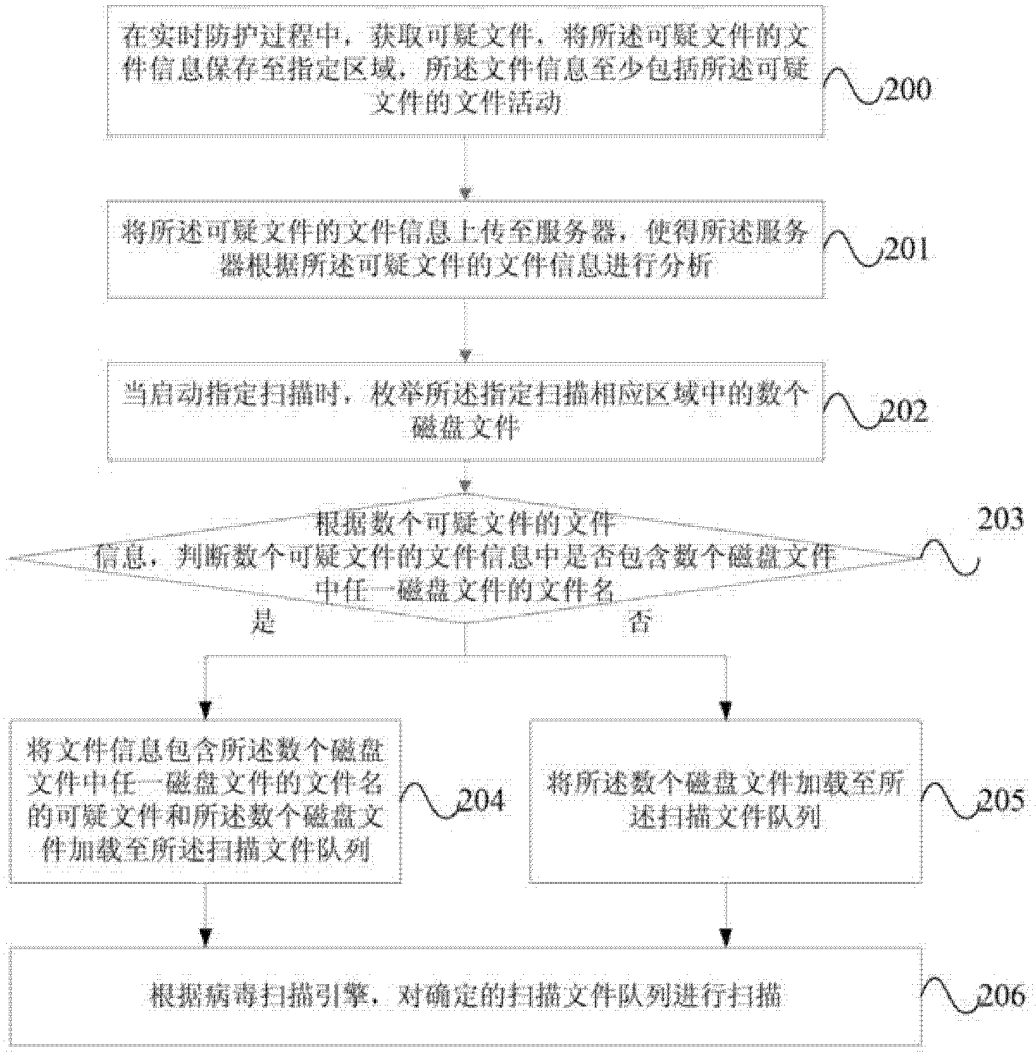

在实时防护过程中，获取可疑文件，将所述可疑文件的文件信息保存至指定区域，所述文件信息至少包括所述可疑文件的文件活动
200
将所述可疑文件的文件信息上传至服务器，使得所述服务器根据所述可疑文件的文件信息进行分析
201
当启动指定扫描时，枚举所述指定扫描相应区域中的数个磁盘文件
202
根据数个可疑文件的文件信息，判断数个可疑文件的文件信息中是否包含数个磁盘文件中任一磁盘文件的文件名
203
是
否
将文件信息包含所述数个磁盘文件中任一磁盘文件的文件名的可疑文件和所述数个磁盘文件加载至所述扫描文件队列
204
将所述数个磁盘文件加载至所述扫描文件队列
205
根据病毒扫描引擎，对确定的扫描文件队列进行扫描
206

图 2


10
11
12
枚举模块
队列确定模块
扫描模块

图 3

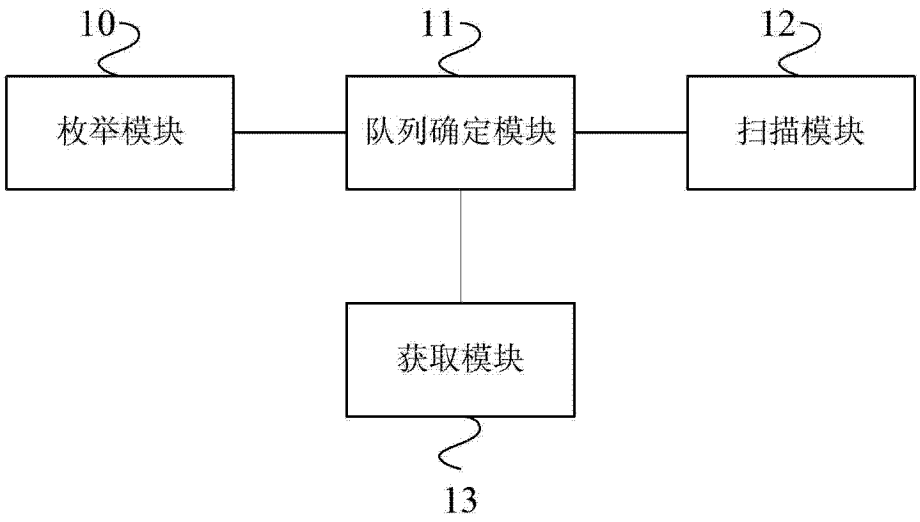

10
11
12
枚举模块
队列确定模块
扫描模块
获取模块
13

图 4

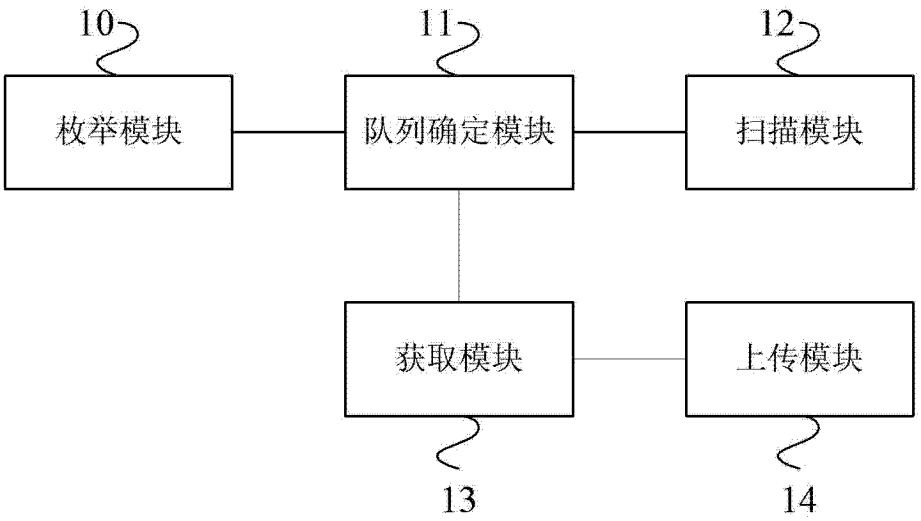

10
11
12
枚举模块
队列确定模块
扫描模块
获取模块
上传模块
13
14

图 5