(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103971052 B
(45)授权公告日 2017.06.30

(21)申请号 201310031901.2

(22)申请日 2013.01.28

(65)同一申请的已公布的文献号
申请公布号 CN 103971052 A

(43)申请公布日 2014.08.06

(73)专利权人 腾讯科技(深圳)有限公司
地址 518044 广东省深圳市福田区振兴路赛格科技园2栋东403室

(72)发明人 谭文

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 吴贵明 张永明

(51)Int.Cl.
G06F 21/56(2013.01)
G06F 9/445(2006.01)

(56)对比文件
CN 102339371 A,2012.02.01,
CN 101959193 A,2011.01.26,
US 7093239 B1,2006.08.15,
RU 2472215 C1,2013.01.10,

审查员 王春圆

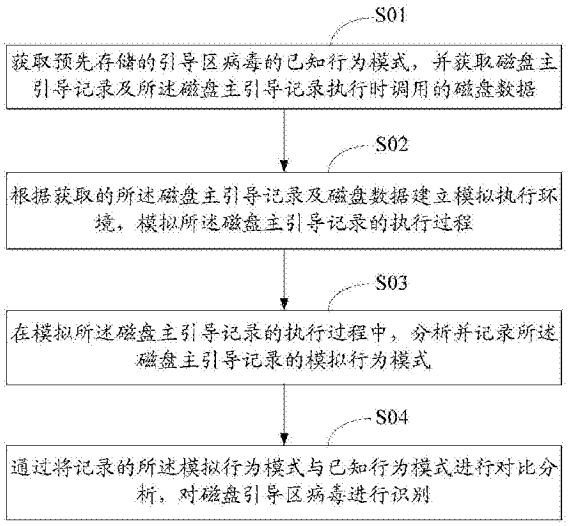
权利要求书2页 说明书8页 附图7页

(54)发明名称

磁盘引导区病毒识别方法及装置

(57)摘要

本发明公开了一种磁盘引导区病毒识别方法及装置，该方法包括以下步骤：获取预先存储的引导区病毒的已知行为模式，并获取磁盘主引导记录及所述磁盘主引导记录执行时调用的磁盘数据；根据获取的所述磁盘主引导记录及磁盘数据建立模拟执行环境，模拟所述磁盘主引导记录的执行过程；在模拟所述磁盘主引导记录的执行过程中，分析并记录所述磁盘主引导记录的模拟行为模式；通过将记录的所述模拟行为模式与已知行为模式进行对比分析，对磁盘引导区病毒进行识别；具有及时、准确地识别新的引导区病毒的有益效果，并能够对识别到的引导区病毒进行及时的响应处理，提高引导区病毒的处理速度。



CN 103971052 B

1.一种磁盘引导区病毒识别方法，所述方法应用于服务端，其特征在于，包括以下步骤：

获取预先存储的引导区病毒的已知行为模式，并获取磁盘主引导记录及所述磁盘主引导记录执行时调用的磁盘数据，其中，所述磁盘主引导记录及所述磁盘数据是所述服务端从磁盘样本开始读取的磁盘样本文件，所述磁盘样本文件为所述服务端从客户端收集的磁盘数据样本；

根据获取的所述磁盘主引导记录及磁盘数据建立模拟执行环境，模拟所述磁盘主引导记录的执行过程；

在模拟所述磁盘主引导记录的执行过程中，服务端通过文件读写接口从磁盘样本开始从所述磁盘样本文件中读取磁盘数据，对所述磁盘样本文件进行读操作，分析并记录所述磁盘样本文件的写操作，并将写入的内容作为所述磁盘主引导记录的模拟行为模式；

通过所述服务端的模拟器与磁盘样本黑白样本判定程序的交互操作将记录的所述模拟行为模式与已知行为模式进行对比分析，对磁盘引导区病毒进行识别；

其中，在通过将记录的所述模拟行为模式与已知行为模式进行对比分析，对磁盘引导区病毒进行识别之后，所述方法还包括：将所述磁盘主引导记录及磁盘数据标记为需进行人工分析的磁盘数据样本。

2.如权利要求1所述的方法，其特征在于，所述通过将记录的所述模拟行为模式与已知行为模式进行对比分析，对磁盘引导区病毒进行识别的步骤包括：

在记录的所述模拟行为模式与已知行为模式匹配成功时，识别所述模拟行为模式所对应的磁盘引导区已被病毒感染，标记所述磁盘主引导记录执行时调用的磁盘数据为黑样本。

3.一种磁盘引导区病毒识别装置，所述装置应用于服务端，其特征在于，包括：

数据获取模块，用于获取预先存储的引导区病毒的已知行为模式，并获取磁盘主引导记录及所述磁盘主引导记录执行时调用的磁盘数据，其中，所述磁盘主引导记录及所述磁盘数据是所述服务端从磁盘样本开始读取的磁盘样本文件，所述磁盘样本文件为所述服务端从客户端收集的磁盘数据样本；

模拟执行模块，用于根据获取的所述磁盘主引导记录及磁盘数据建立模拟执行环境，模拟所述磁盘主引导记录的执行过程；在模拟所述磁盘主引导记录的执行过程中，服务端通过文件读写接口从磁盘样本开始从所述磁盘样本文件中读取磁盘数据，对所述磁盘样本文件进行读操作，分析并记录所述磁盘样本文件的写操作，并将写入的内容作为所述磁盘主引导记录的模拟行为模式；

病毒识别模块，用于通过所述服务端的模拟器与磁盘样本黑白样本判定程序的交互操作将记录的所述模拟行为模式与已知行为模式进行对比分析，对磁盘引导区病毒进行识别；

其中，所述装置还包括：样本标记模块，用于将所述磁盘主引导记录及磁盘数据标记为需进行人工分析的磁盘数据样本。

4.如权利要求3所述的装置，其特征在于，所述病毒识别模块还用于：

在记录的所述模拟行为模式与已知行为模式匹配成功时，识别所述模拟行为模式所对应的磁盘引导区已被病毒感染，标记所述磁盘主引导记录执行时调用的磁盘数据为黑样

本。

磁盘引导区病毒识别方法及装置

技术领域

[0001] 本发明涉及计算机技术领域，尤其涉及一种磁盘引导区病毒识别方法及装置。

背景技术

[0002] 磁盘引导区病毒通常指的是通过感染MBR(Master Boot Record，磁盘主引导记录)的方式，实现比Windows操作系统更早启动、绕过安全软件检查的病毒，比如bootkit病毒。

[0003] 目前安全厂商一般都采取检查本机MBR的方式来发现引导区病毒，通常先收集各种已知引导区感染后的MBR数据的黑样本，以及各种未感染引导区病毒的MBR数据的白样本，将收集的黑样本和白样本保存到后台服务器。杀毒软件在本地检查MBR时，首先读取MBR获取其特征值(比如md5值)并上传至服务器，与服务器上已经保存过的MBR特征值进行比对。一旦发现与已知黑样本数据一致，则认为感染病毒；发现与白样本数据一致，则不加处理；若发现既不是白样本，也不是黑样本，则上传为新样本，由人工分析来决定该新样本是黑样本还是白样本。

[0004] 上述处理方式不能在用户端对未知的引导区病毒进行主动判定，必须上传至服务器分析并确认该病毒的存在之后才能进行处理，从而导致对引导区病毒的处理过于滞后，也不能对其进行及早拦截；由于部分病毒能够快速演化且MBR也不断衍生各种版本，而上述处理方式对每一种演化版本都只能当做未知病毒对待，且需要重新分析，进一步拖慢了对病毒的拦截速度；且MBR样本数量极多，逐一进行人工分析耗时巨大，也容易漏判。

发明内容

[0005] 本发明的主要目的是提供一种硬盘引导区病毒的识别方法及装置，旨在解决不能及时、准确地识别新的引导区病毒的问题。

[0006] 本发明实施例公开了一种磁盘引导区病毒识别方法，包括以下步骤：

[0007] 获取预先存储的引导区病毒的已知行为模式，并获取磁盘主引导记录及所述磁盘主引导记录执行时调用的磁盘数据；

[0008] 根据获取的所述磁盘主引导记录及磁盘数据建立模拟执行环境，模拟所述磁盘主引导记录的执行过程；

[0009] 在模拟所述磁盘主引导记录的执行过程中，分析并记录所述磁盘主引导记录的模拟行为模式；

[0010] 通过将记录的所述模拟行为模式与已知行为模式进行对比分析，对磁盘引导区病毒进行识别。

[0011] 本发明实施例还公开了一种磁盘引导区病毒识别装置，包括：

[0012] 数据获取模块，用于获取预先存储的引导区病毒的已知行为模式，并获取磁盘主引导记录及所述磁盘主引导记录执行时调用的磁盘数据；

[0013] 模拟执行模块，用于根据获取的所述磁盘主引导记录及磁盘数据建立模拟执行环

境，模拟所述磁盘主引导记录的执行过程；在模拟所述磁盘主引导记录的执行过程中，分析并记录所述磁盘主引导记录的模拟行为模式；

[0014] 病毒识别模块，用于通过将记录的所述模拟行为模式与已知行为模式进行对比分析，对磁盘引导区病毒进行识别。

[0015] 本发明通过获取预先存储的引导区病毒的已知行为模式，并获取磁盘主引导记录及所述磁盘主引导记录执行时调用的磁盘数据；根据获取的所述磁盘主引导记录及磁盘数据建立模拟执行环境，模拟所述磁盘主引导记录的执行过程；在模拟所述磁盘主引导记录的执行过程中，分析并记录所述磁盘主引导记录的模拟行为模式；通过将记录的所述模拟行为模式与已知行为模式进行对比分析，对磁盘引导区病毒进行识别的方法，具有及时、准确地识别新的引导区病毒的有益效果，并能够对识别到的引导区病毒进行及时的响应处理，提高引导区病毒的处理速度。

附图说明

[0016] 图1是本发明磁盘引导区病毒识别方法一实施例流程示意图；

[0017] 图2是本发明磁盘引导区病毒识别方法应用于服务端时服务端的功能模块示意图；

[0018] 图3是本发明磁盘引导区病毒识别方法应用于服务端时又一实施例流程示意图；

[0019] 图4是本发明磁盘引导区病毒识别方法应用于客户端时客户端的功能模块示意图；

[0020] 图5是本发明磁盘引导区病毒识别方法应用于客户端时再一实施例流程示意图；

[0021] 图6是本发明磁盘引导区病毒识别装置一实施例功能模块示意图；

[0022] 图7是本发明磁盘引导区病毒识别装置应用于服务端时又一实施例功能模块示意图；

[0023] 图8是本发明磁盘引导区病毒识别装置应用于客户端时再一实施例功能模块示意图。

[0024] 本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

[0025] 以下结合说明书附图及具体实施例进一步说明本发明的技术方案。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0026] 本发明磁盘引导区病毒识别方法及装置，在不影响真实计算机系统的前提下，对采用MBR执行时调用的磁盘数据作为虚拟磁盘进行模拟引导，分析并记录模拟系统引导时的所有行为，从而对MBR中的磁盘数据是否有可疑行为作出判定。上述模拟执行过程可以在服务端执行，也可以在客户端执行。在服务端执行时，可以对大量的MBR数据进行批量处理，自动分离出具有病毒行为的MBR数据和明显无任何可疑的MBR数据，并留下少数自动分析无法确认的样本，并将上述自动分析无法确认的样本标记为需进行人工分析的样本，提醒后台的开发分析人员进行人工分析；在客户端执行时，当发现MBR被未知的病毒如bootkit感染时，即可及时进行拦截和修复，并将被病毒感染的MBR数据标记为黑样本上传到服务端；当传统的黑白样本比对不能得出结论时，与常用的磁盘引导区病毒识别方法相比，本发明

磁盘引导区病毒识别方法及装置能够提高MBR数据的分析效率并提前发现磁盘引导区的新病毒。

[0027] 请参照图1,图1是本发明磁盘引导区病毒识别方法一实施例流程示意图;如图1所示,本发明磁盘引导区病毒识别方法包括以下步骤:

[0028] 步骤S01、获取预先存储的引导区病毒的已知行为模式,并获取磁盘主引导记录及所述磁盘主引导记录执行时调用的磁盘数据;

[0029] 由于服务端预先已收集了各种已知引导区感染后的MBR数据的黑样本,以及各种未感染引导区病毒的MBR数据的白样本,且收集的上述黑样本和白样本均保存在服务端,则在进行磁盘引导区病毒识别时,根据上述已保存的黑样本和白样本,获取上述预先存储的引导区病毒的已知行为模式,所述引导区病毒的已知行为模式包括在进行人工分析引导区病毒如bootkit时,总结的一些引导区病毒的引导过程所具有的特殊的行为模式;本领域的技术人员可以理解,所述一些引导区病毒的引导过程所具有的特殊的行为模式包括但不限于:更改系统内存数量以便为自己留出可用的内存空间、挂钩int 13中断等。同时,获取MBR及该MBR执行时调用的磁盘数据,为后续建立模拟执行环境做准备。在一优选的实施例中,对于少数自动分析无法确认的样本,可以进行人工分析并将得到的新的病毒行为模式存储至服务端,从而使磁盘引导区病毒识别方法的分析精度不断提高。

[0030] 步骤S02、根据获取的所述磁盘主引导记录及磁盘数据建立模拟执行环境,模拟所述磁盘主引导记录的执行过程;

[0031] 步骤S03、在模拟所述磁盘主引导记录的执行过程中,分析并记录所述磁盘主引导记录的模拟行为模式;

[0032] 由于客户端的BIOS(Basic Input Output System,基本输入输出系统)进行初始化和上电自检后,启动系统自检程序,检测MBR,并执行MBR中所包含的指令,然后由这些指令去引导windows系统的启动;而磁盘引导区病毒是通过感染MBR的方式、实现比操作系统更早启动且能够绕过客户端安全软件检查的病毒,因此,可以根据获取的MBR及MBR执行时调用的磁盘数据建立一个虚拟的模拟执行环境,模拟MBR的执行过程,分析并记录MBR的模拟行为模式,尽早识别磁盘引导区病毒,并采取相应的措施。

[0033] 本领域的技术人员可以理解,由于MBR比较短小(实际只有512字节),因此即使MBR感染病毒后可能加载更多的指令进行病毒操作,但这个执行过程的时间仍然较短且执行的指令数量不多,很容易分离出一些有明显病毒特征的行为模式,因为这些行为模式是正常的系统引导过程所没有的。因此,模拟执行上述过程所需要的系统资源和时间都相对较少。

[0034] 所述模拟执行是指,在一台计算机上用软件资源来模拟硬件的执行过程,也可以理解为在一台计算机上模拟另一台计算机执行软件的技术。目前,常用的模拟执行方式有多种,比如解释执行方式:对每条指令进行解码,并利用软件资源模拟每一条指令的行为;或者使用VT技术(英特尔公司提供的x86芯片硬件支持的虚拟技术)进行模拟执行,比如开源软件Bochs,本身是一个x86硬件平台的虚拟机,类似于虚拟机VMWare和VirtualBox。由于Bochs也虚拟了所有的硬件,因此运行Bochs并不会对计算机本身真实磁盘中的数据产生实际的影响,且Bochs不会在计算机本机中加载任何驱动程序,仅是一个单纯的应用程序。

[0035] 在一优选的实施例中,本发明磁盘引导区病毒识别方法采用解释执行作为模拟执行的一种较佳的实现方式。利用解释执行的方式进行模拟执行时,不真实执行任何指令,而

是解码每条指令并读取其行为进行虚拟执行，比如：模拟执行“读写寄存器”时，实际执行的是读写虚拟寄存器(比如一些C语言定义的变量)；模拟执行“读写内存”时，实际操作的只是一个数组；模拟执行“IO(Input/Output，输入输出)操作”，实际是和一些虚拟的设备进行交互，而这些虚拟的设备也是一些C语言编写的数据结构以及维持其运作的软件程序；模拟执行“中断”，实际执行的是在指令执行过程中插入一些异步事件。

[0036] 步骤S04、通过将记录的所述模拟行为模式与已知行为模式进行对比分析，对磁盘引导区病毒进行识别。

[0037] 将记录的所述模拟行为模式与已知行为模式进行对比分析，若记录的模拟行为模式与预先存储的MBR白样本一致，则识别对应的磁盘引导区暂时没被引导区病毒感染；若记录的模拟行为模式与预先存储的引导区病毒的已知行为模式匹配成功，或者记录的模拟行为模式与预先存储的MBR黑样本一致，或者，一些明显引导区病毒的行为模式(比如更改系统内存数量以便为自己留出可用的内存空间、挂钩int 13中断、访问磁盘空间的尾部等)，则识别所述模拟行为模式所对应的磁盘引导区已被病毒感染，并标记对应的所述磁盘主引导记录执行时调用的磁盘数据为黑样本。

[0038] 本实施例通过获取预先存储的引导区病毒的已知行为模式、磁盘主引导记录及磁盘主引导记录执行时调用的磁盘数据；根据获取的磁盘主引导记录及磁盘数据建立模拟执行环境，模拟磁盘主引导记录的执行过程，分析并记录磁盘主引导记录的模拟行为模式；通过将记录的模拟行为模式与已知行为模式进行对比分析，对磁盘引导区病毒进行识别的方法，具有及时、准确地识别新的引导区病毒的有益效果。

[0039] 本发明磁盘引导区病毒识别方法应用于服务端时，请参照图2，图2是本发明磁盘引导区病毒识别方法应用于服务端时服务端的功能模块示意图；如图2所示，磁盘引导区病毒识别方法应用于服务端时，磁盘主引导记录及磁盘数据是服务端从磁盘样本MBR开始读取的磁盘样本文件，该磁盘样本文件为服务端从客户端收集的磁盘数据样本。在模拟执行时，服务端通过文件读写接口从MBR开始从上述磁盘样本文件中读取相关磁盘数据，且对上述磁盘样本文件进行读操作，并记录上述磁盘样本文件的写操作及写入的具体内容，作为其行为模式的一部分，通过服务端的模拟器与MBR黑白样本自动判定程序的交互操作，在服务端完成对磁盘引导区病毒的识别过程。

[0040] 结合图1和图2所述的实施例，请参照图3，图3是本发明磁盘引导区病毒识别方法应用于服务端时又一实施例流程示意图；本实施例与图1所述实施例的区别是，仅增加了步骤S11；本实施例仅对步骤S11作具体描述，有关本发明磁盘引导区病毒识别方法所涉及的其他步骤请参照上述相关实施例的具体描述，在此不再赘述。

[0041] 如图3所示，本发明磁盘引导区病毒识别方法在步骤S04、通过将记录的所述模拟行为模式与已知行为模式进行对比分析，对磁盘引导区病毒进行识别的步骤之后还包括步骤：

[0042] 步骤S11、将所述磁盘主引导记录及磁盘数据标记为需进行人工分析的磁盘数据样本。

[0043] 服务端将记录的模拟行为模式与存储的已知行为模式进行比对分析，对于与已知行为模式中的白样本匹配成功的，则识别对应的MBR数据暂时没有安全威胁；对于与已知行为模式中的黑样本匹配成功或者是一些明显的引导区病毒的行为模式的，则识别对应的

MBR数据已感染引导区病毒；而对于既不能与白样本匹配成功，也不能与黑样本匹配成功，且不能识别记录的该模拟行为模式是否为明显的引导区病毒的行为模式，则向客户端发出提示信息，提醒客户端对该模拟行为模式所对应的磁盘主引导记录及磁盘数据进行人工分析，以便及早识别该模拟行为模式所对应的MBR是否已感染病毒，便于及时采取相应措施。

[0044] 本发明磁盘引导区病毒识别方法应用于客户端时，请参照图4，图4是本发明磁盘引导区病毒识别方法应用于客户端时客户端的功能模块示意图；如图4所示，磁盘引导区病毒识别方法应用于客户端时，磁盘主引导记录及磁盘数据是客户端从自身的真实磁盘MBR开始读取的客户端真实磁盘文件。在模拟执行时，客户端通过文件读写接口从MBR开始从上述客户端真实的磁盘中读取磁盘数据，且对上述磁盘文件进行读操作，并记录上述磁盘样本文件的写操作及写入的具体内容，作为其行为模式的一部分，通过客户端的模拟器与MBR黑白样本自动判定程序的交互操作，在客户端完成对磁盘引导区病毒的识别过程。

[0045] 结合图1和图4所述的实施例，请参照图5，图5是本发明磁盘引导区病毒识别方法应用于客户端时再一实施例流程示意图；本实施例与图1所述实施例的区别是，仅增加了步骤S12；本实施例仅对步骤S12作具体描述，有关本发明磁盘引导区病毒识别方法所涉及的其他步骤请参照上述相关实施例的具体描述，在此不再赘述。

[0046] 如图5所示，本发明磁盘引导区病毒识别方法在步骤S04、通过将记录的所述模拟行为模式与已知行为模式进行对比分析，对磁盘引导区病毒进行识别的步骤之后还包括步骤：

[0047] 步骤S12、将标记为黑样本的所述磁盘数据上传至服务端，并进行客户端自身的修复操作。

[0048] 客户端将记录的模拟行为模式与存储的已知行为模式进行比对分析，对于与已知行为模式中的白样本匹配成功的，则识别对应的MBR数据暂时没有安全威胁；对于与已知行为模式中的黑样本匹配成功或者是一些明显的引导区病毒的行为模式的，则识别对应的MBR数据已感染引导区病毒；客户端将标记为黑样本的磁盘数据上传至服务端，并进行自身的修复操作。

[0049] 在一优选的实施例中，对于既不能与白样本匹配成功，也不能与黑样本匹配成功的模拟行为模式，则将上述模拟行为模式上传至服务端，由服务端对其进行分析，并与存储的黑白样本进行匹配；若服务端分析后，仍不能对该模拟行为模式进行确认，则由后台分析人员对其进行人工分析，根据分析结果对其进行处理；比如，分析结果为，该模拟行为模式为安全行为，则不对其进行处理；分析结果为，该模拟行为模式会对客户端造成安全威胁，则将该模拟行为模式所对应的磁盘数据进行删除、修复等处理，并将上述分析结果及处理过程均上传至服务端。客户端可以根据分析结果将安全行为所对应的磁盘数据标记为白样本，将对客户端造成安全威胁的磁盘数据标记为黑样本后，将所述白样本及黑样本上传至服务端。

[0050] 本实施例在客户端识别引导区病毒后，进行自身修复操作，具有对识别到的引导区病毒进行及时响应处理的有益效果，提高了客户端引导区病毒的处理速度。

[0051] 参照图6，图6是本发明磁盘引导区病毒识别装置一实施例功能模块示意图；如图6所示，本发明磁盘引导区病毒识别装置包括：数据获取模块01、模拟执行模块02和病毒识别模块03。

[0052] 数据获取模块01，用于获取预先存储的引导区病毒的已知行为模式，并获取磁盘主引导记录及所述磁盘主引导记录执行时调用的磁盘数据。

[0053] 由于服务端预先已收集了各种已知引导区感染后的MBR数据的黑样本，以及各种未感染引导区病毒的MBR数据的白样本，且收集的上述黑样本和白样本均保存在服务端，则在进行磁盘引导区病毒识别时，根据上述已保存的黑样本和白样本，数据获取模块01获取上述预先存储的引导区病毒的已知行为模式，所述引导区病毒的已知行为模式包括在进行人工分析引导区病毒如bootkit时，总结的一些引导区病毒的引导过程所具有的特殊的行为模式；本领域的技术人员可以理解，所述一些引导区病毒的引导过程所具有的特殊的行为模式包括但不限于：更改系统内存数量以便为自己留出可用的内存空间、挂钩int 13中断等。同时，数据获取模块01获取MBR及该MBR执行时调用的磁盘数据，为后续建立模拟执行环境做准备。在一优选的实施例中，对于少数自动分析无法确认的样本，可以进行人工分析并将得到的新的病毒行为模式存储至服务端，从而使磁盘引导区病毒识别装置对引导区病毒的分析精度不断提高。

[0054] 模拟执行模块02，用于根据获取的所述磁盘主引导记录及磁盘数据建立模拟执行环境，模拟所述磁盘主引导记录的执行过程；在模拟所述磁盘主引导记录的执行过程中，分析并记录所述磁盘主引导记录的模拟行为模式。

[0055] 由于客户端的BIOS进行初始化和上电自检后，启动系统自检程序，检测MBR，并执行MBR中所包含的指令，然后由这些指令去引导windows系统的启动；而磁盘引导区病毒是通过感染MBR的方式、实现比操作系统更早启动且能够绕过客户端安全软件检查的病毒，因此，模拟执行模块02可以根据数据获取模块01获取的MBR及MBR执行时调用的磁盘数据建立一个虚拟的模拟执行环境，模拟MBR的执行过程，分析并记录MBR的模拟行为模式，尽早识别磁盘引导区病毒，并采取相应的措施。

[0056] 本领域的技术人员可以理解，由于MBR比较短小(实际只有512字节)，因此即使MBR感染病毒后可能加载更多的指令进行病毒操作，但这个执行过程的时间仍然较短且执行的指令数量不多，很容易分离出一些有明显病毒特征的行为模式，因为这些行为模式是正常的系统引导过程所没有的。因此，模拟执行上述过程所需要的系统资源和时间都相对较少。

[0057] 有关模拟执行的相关描述，请参照上述相关实施例的具体描述，在此不再赘述。

[0058] 在一优选的实施例中，本发明磁盘引导区病毒识别装置采用解释执行作为模拟执行的一种较佳的实现方式。利用解释执行的方式进行模拟执行时，不真实执行任何指令，而是解码每条指令并读取其行为进行虚拟执行，比如：模拟执行“读写寄存器”时，实际执行的是读写虚拟寄存器(比如一些C语言定义的变量)；模拟执行“读写内存”时，实际操作的只是一个数组；模拟执行“IO操作”，实际是和一些虚拟的设备进行交互，而这些虚拟的设备也是一些C语言编写的数据结构以及维持其运作的软件程序；模拟执行“中断”，实际执行的是在指令执行过程中插入一些异步事件。

[0059] 病毒识别模块03，用于通过将记录的所述模拟行为模式与已知行为模式进行对比分析，对磁盘引导区病毒进行识别。

[0060] 病毒识别模块03将模拟执行模块02记录的模拟行为模式与数据获取模块01获取的已知行为模式进行对比分析，若记录的模拟行为模式与预先存储的MBR白样本一致，病毒识别模块03识别对应的磁盘引导区暂时没被引导区病毒感染；若记录的模拟行为模式与预

先存储的引导区病毒的已知行为模式匹配成功，或者记录的模拟行为模式与预先存储的MBR黑样本一致，或者，一些明显引导区病毒的行为模式(比如更改系统内存数量以便为自己留出可用的内存空间、挂钩int 13中断、访问磁盘空间的尾部等)，病毒识别模块03则识别所述模拟行为模式所对应的磁盘引导区已被病毒感染，并标记对应的所述磁盘主引导记录执行时调用的磁盘数据为黑样本。

[0061] 本实施例通过获取预先存储的引导区病毒的已知行为模式、磁盘主引导记录及磁盘主引导记录执行时调用的磁盘数据；根据获取的磁盘主引导记录及磁盘数据建立模拟执行环境，模拟磁盘主引导记录的执行过程，分析并记录磁盘主引导记录的模拟行为模式；通过将记录的模拟行为模式与已知行为模式进行对比分析，对磁盘引导区病毒进行识别，具有及时、准确地识别新的引导区病毒的有益效果。

[0062] 结合图2和图6所述的实施例，请参照7，图7是本发明磁盘引导区病毒识别装置应用于服务端时又一实施例功能模块示意图；本实施例与图6所述实施例的区别是，仅增加了样本标记模块04，本实施例仅对样本标记模块04做具体描述，本发明磁盘引导区病毒识别装置所涉及的其他模块请参照相关实施例的具体描述，在此不再赘述。

[0063] 如图7所示，本发明磁盘引导区病毒识别装置应用于服务端时，还包括：

[0064] 样本标记模块04，用于将所述磁盘主引导记录及磁盘数据标记为需进行人工分析的磁盘数据样本。

[0065] 病毒识别模块03将模拟执行模块02记录的模拟行为模式与数据获取模块01获取的已知行为模式进行对比分析，对于与已知行为模式中的白样本匹配成功的，则识别对应的MBR数据暂时没有安全威胁；对于与已知行为模式中的黑样本匹配成功或者是一些明显的引导区病毒的行为模式的，则识别对应的MBR数据已感染引导区病毒；而对于既不能与白样本匹配成功，也不能与黑样本匹配成功，且不能识别记录的该模拟行为模式是否为明显的引导区病毒的行为模式，样本标记模块04向客户端发出提示信息，提醒客户端对该模拟行为模式所对应的磁盘主引导记录及磁盘数据进行人工分析，以便及早识别该模拟行为模式所对应的MBR是否已感染病毒，便于及时采取相应措施。

[0066] 结合图4和图6所述的实施例，请参照图8，图8是本发明磁盘引导区病毒识别装置应用于客户端时再一实施例功能模块示意图。本实施例与图6所述实施例的区别是，仅增加了数据修复模块05；本实施例仅对数据修复模块05作具体描述，本发明磁盘引导区病毒识别装置所涉及的其他模块请参照相关实施例的具体描述，在此不再赘述。

[0067] 如图8所示，本发明磁盘引导区病毒识别装置应用于客户端时，还包括：

[0068] 数据修复模块05，用于将标记为黑样本的所述磁盘数据上传至服务端，并进行客户端自身的修复操作。

[0069] 病毒识别模块03将模拟执行模块02记录的模拟行为模式与数据获取模块01获取的已知行为模式进行对比分析，对于与已知行为模式中的白样本匹配成功的，则识别对应的MBR数据暂时没有安全威胁；对于与已知行为模式中的黑样本匹配成功或者是一些明显的引导区病毒的行为模式的，则识别对应的MBR数据已感染引导区病毒；客户端的数据修复模块05将标记为黑样本的磁盘数据上传至服务端，并进行自身的修复操作。

[0070] 在一优选的实施例中，对于既不能与白样本匹配成功，也不能与黑样本匹配成功的模拟行为模式，数据修复模块05将上述模拟行为模式上传至服务端，由服务端对其进行

分析，并与存储的黑白样本进行匹配；若服务端分析后，仍不能对该模拟行为模式进行确认，则由后台分析人员对其进行人工分析，根据分析结果对其进行处理；比如，分析结果为，该模拟行为模式为安全行为，则数据修复模块05不对其进行处理；分析结果为，该模拟行为模式会对客户端造成安全威胁，则数据修复模块05将该模拟行为模式所对应的磁盘数据进行删除、修复等处理，并将上述分析结果及处理过程均上传至服务端。数据修复模块05可以根据分析结果将安全行为所对应的磁盘数据标记为白样本，将对客户端造成安全威胁的磁盘数据标记为黑样本后，将所述白样本及黑样本上传至服务端。

[0071] 本实施例在客户端识别引导区病毒后，进行自身修复操作，具有对识别到的引导区病毒进行及时响应处理的有益效果，提高了客户端引导区病毒的处理速度。

[0072] 以上所述仅为本发明的优选实施例，并非因此限制其专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

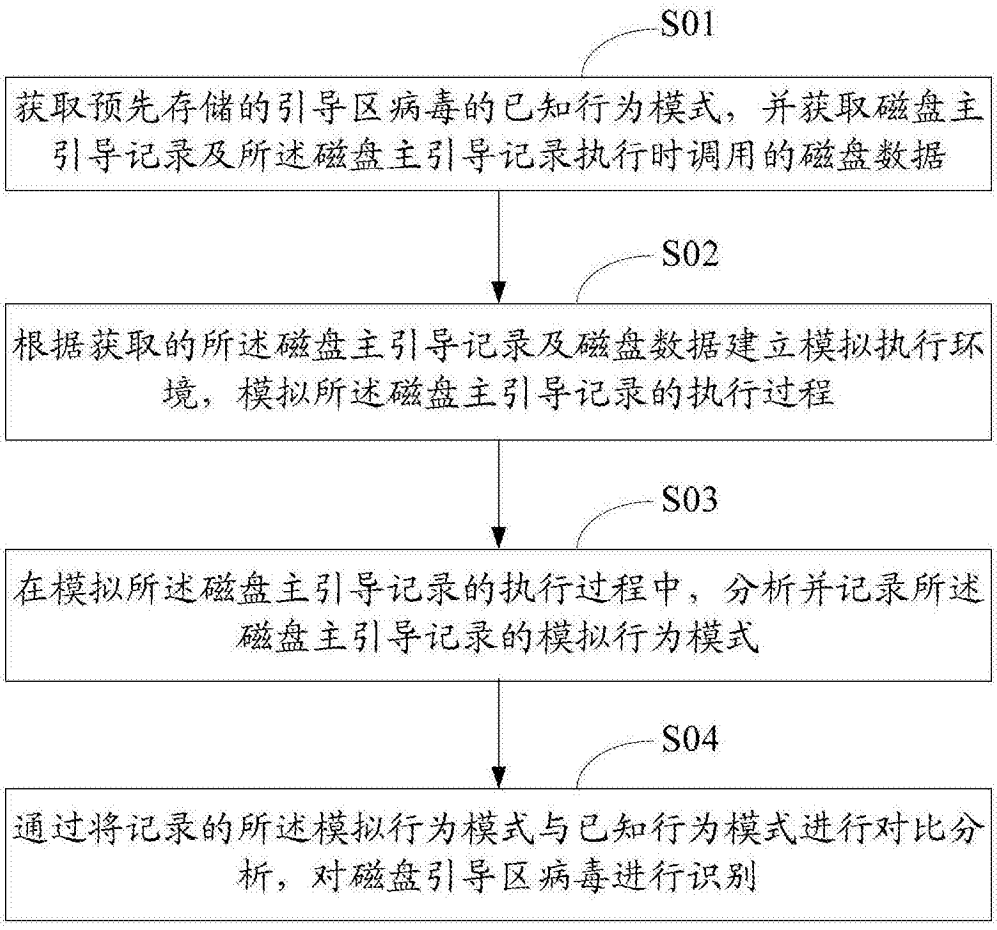

S01
获取预先存储的引导区病毒的已知行为模式，并获取磁盘主引导记录及所述磁盘主引导记录执行时调用的磁盘数据
S02
根据获取的所述磁盘主引导记录及磁盘数据建立模拟执行环境，模拟所述磁盘主引导记录的执行过程
S03
在模拟所述磁盘主引导记录的执行过程中，分析并记录所述磁盘主引导记录的模拟行为模式
S04
通过将记录的所述模拟行为模式与已知行为模式进行对比分析，对磁盘引导区病毒进行识别

图1

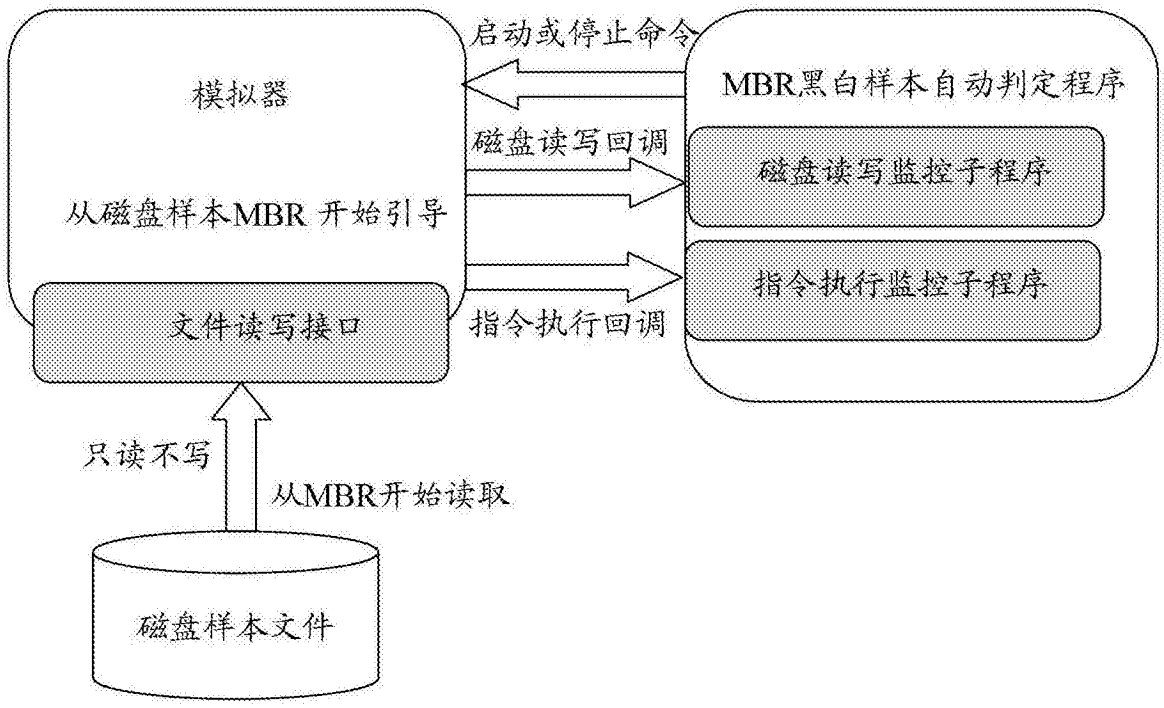

模拟器
从磁盘样本MBR 开始引导
文件读写接口
启动或停止命令
磁盘读写回调
指令执行回调
MBR黑白样本自动判定程序
磁盘读写监控子程序
指令执行监控子程序
只读不写
从MBR开始读取
磁盘样本文件

图2

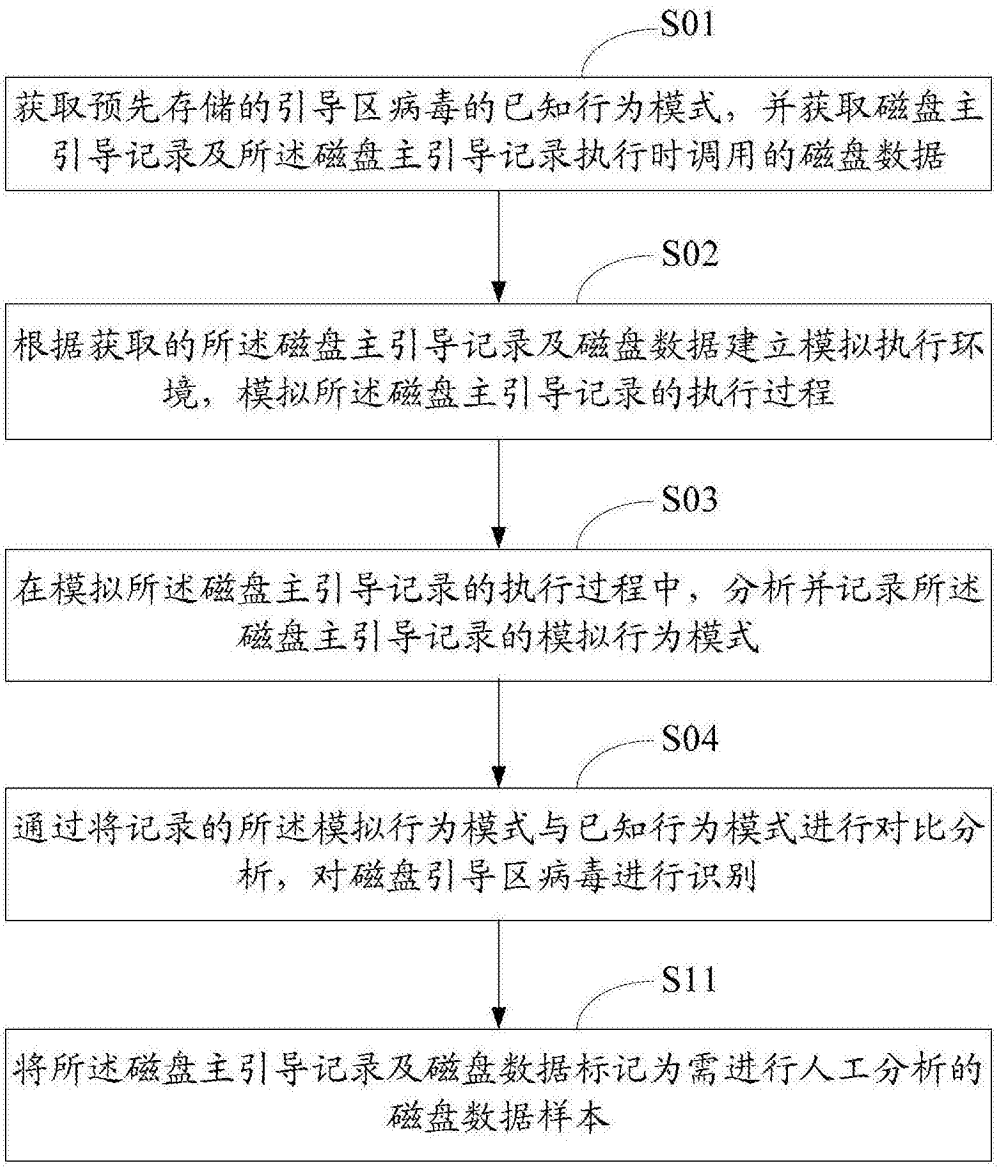

S01
获取预先存储的引导区病毒的已知行为模式，并获取磁盘主引导记录及所述磁盘主引导记录执行时调用的磁盘数据
S02
根据获取的所述磁盘主引导记录及磁盘数据建立模拟执行环境，模拟所述磁盘主引导记录的执行过程
S03
在模拟所述磁盘主引导记录的执行过程中，分析并记录所述磁盘主引导记录的模拟行为模式
S04
通过将记录的所述模拟行为模式与已知行为模式进行对比分析，对磁盘引导区病毒进行识别
S11
将所述磁盘主引导记录及磁盘数据标记为需进行人工分析的磁盘数据样本

图3

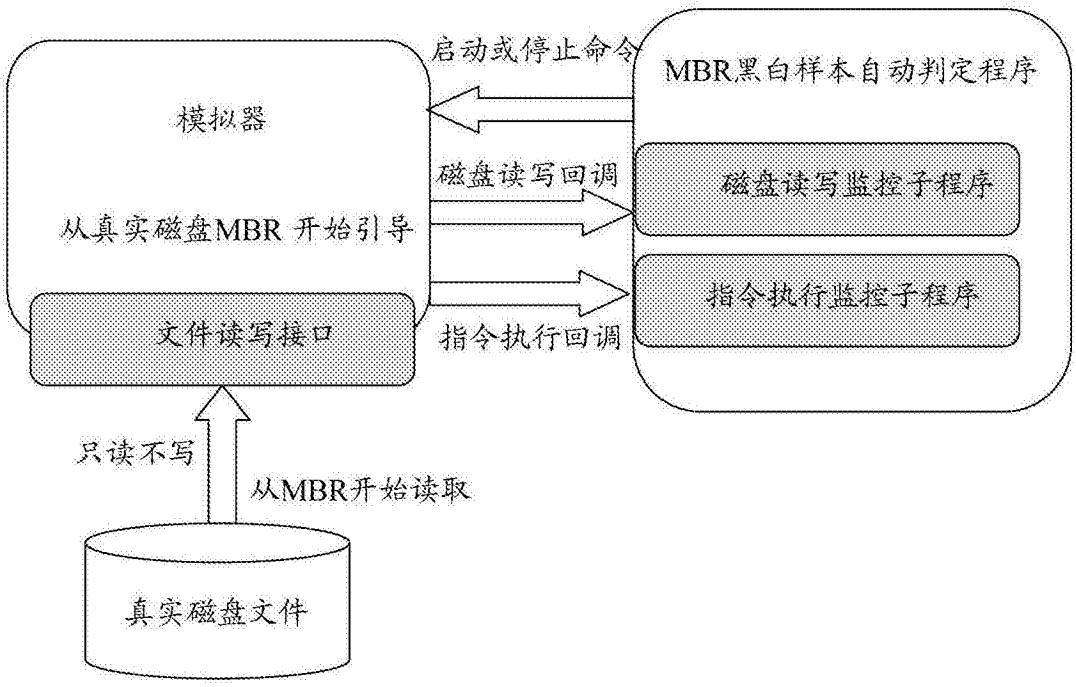

启动或停止命令
MBR黑白样本自动判定程序
模拟器
磁盘读写回调
磁盘读写监控子程序
从真实磁盘MBR 开始引导
指令执行监控子程序
文件读写接口
指令执行回调
只读不写
从MBR开始读取
真实磁盘文件

图4

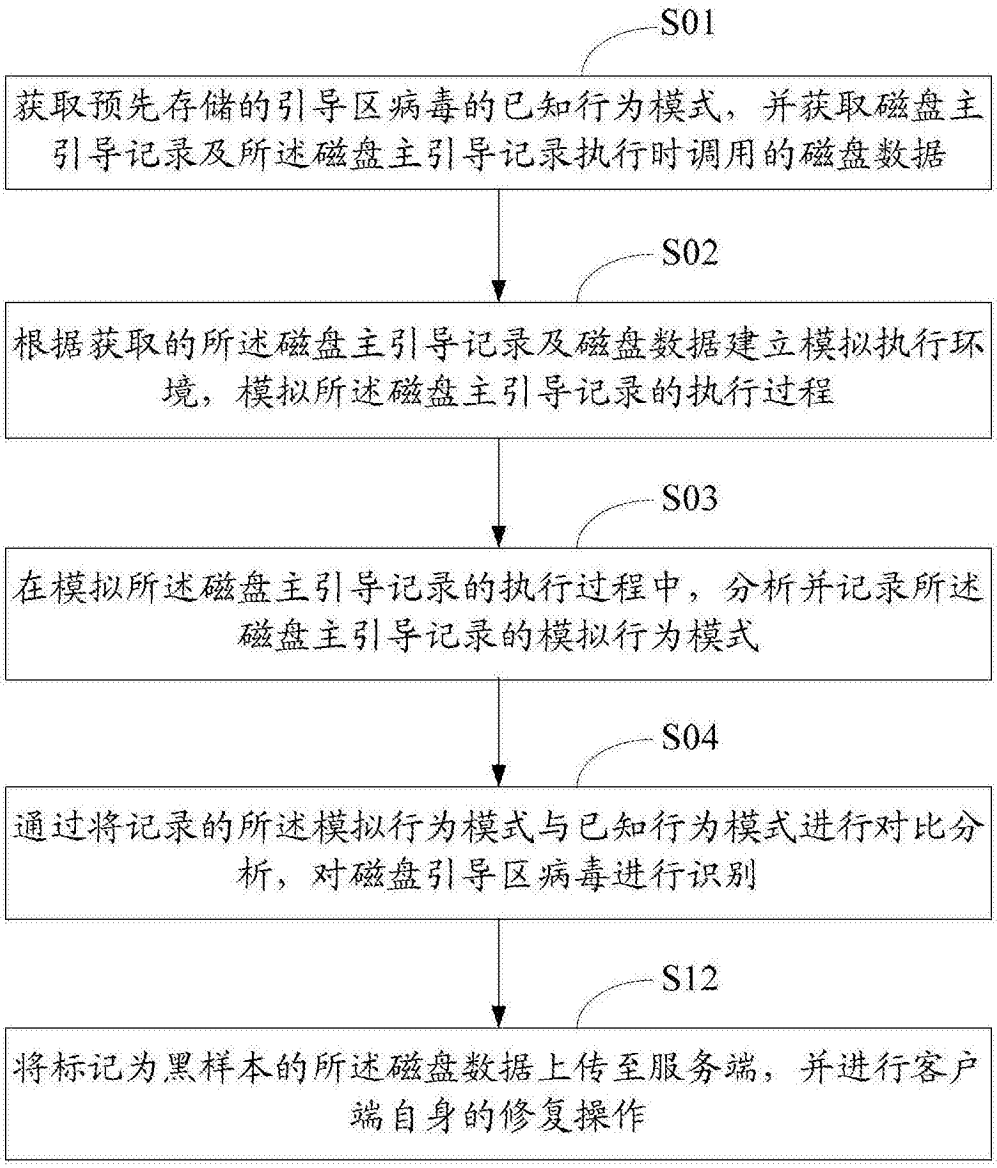

S01
获取预先存储的引导区病毒的已知行为模式，并获取磁盘主引导记录及所述磁盘主引导记录执行时调用的磁盘数据
S02
根据获取的所述磁盘主引导记录及磁盘数据建立模拟执行环境，模拟所述磁盘主引导记录的执行过程
S03
在模拟所述磁盘主引导记录的执行过程中，分析并记录所述磁盘主引导记录的模拟行为模式
S04
通过将记录的所述模拟行为模式与已知行为模式进行对比分析，对磁盘引导区病毒进行识别
S12
将标记为黑样本的所述磁盘数据上传至服务端，并进行客户端自身的修复操作

图5

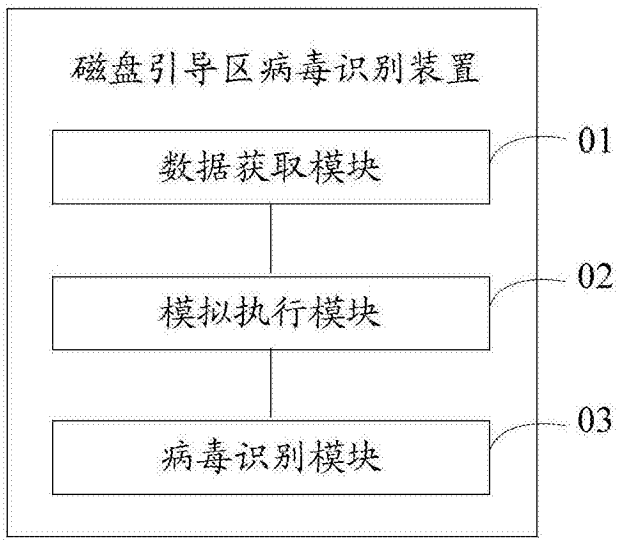

磁盘引导区病毒识别装置
数据获取模块
01
模拟执行模块
02
病毒识别模块
03

图6

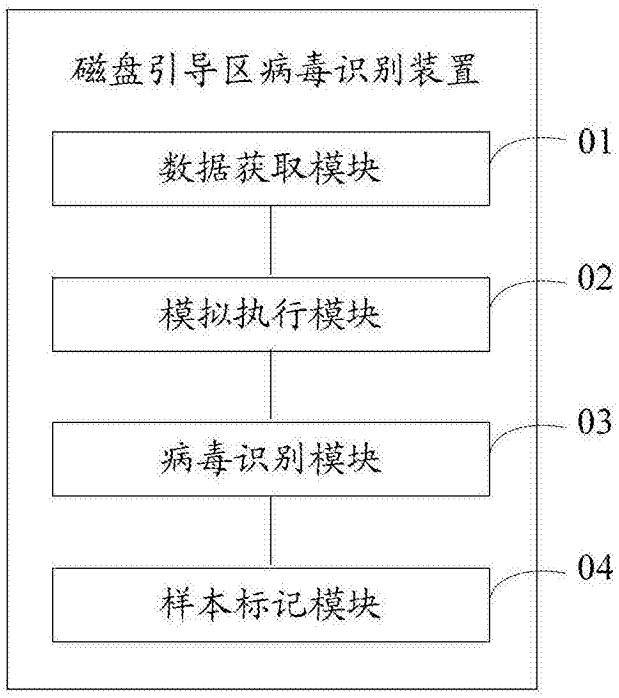

磁盘引导区病毒识别装置
数据获取模块
01
模拟执行模块
02
病毒识别模块
03
样本标记模块
04

图7

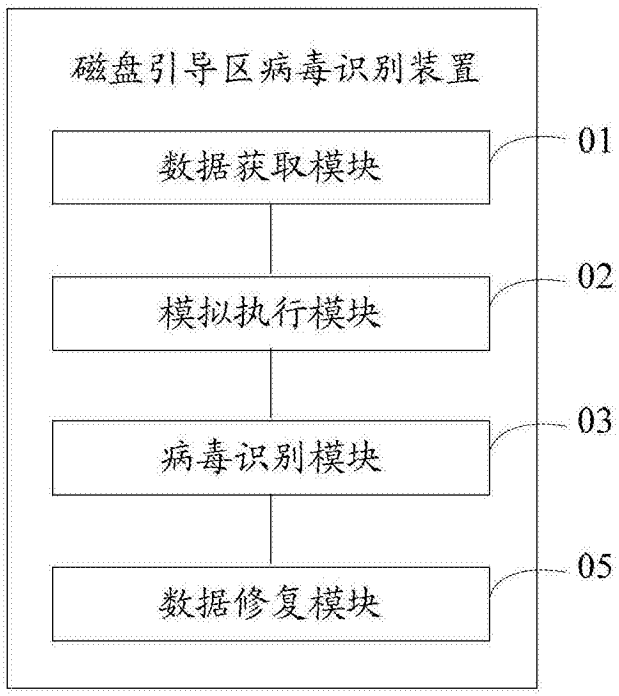


图8