(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 102663288 B
(45)授权公告日 2015.04.01

(21)申请号 201210078454.1

(22)申请日 2012.03.22

(73)专利权人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)
专利权人 奇智软件(北京)有限公司

(72)发明人 邵坚磊 马贞辉 谭合力 姚彤

(74)专利代理机构 北京润泽恒知识产权代理有限公司 11319
代理人 苏培华

(51)Int.Cl.
G06F 21/56(2013.01)

(56)对比文件
CN 101650768 A,2010.02.17, 全文.
US 2009/0320134 A1,2009.12.24, 全文.
CN 101350049 A,2009.01.21, 全文.

审查员 谢永坚

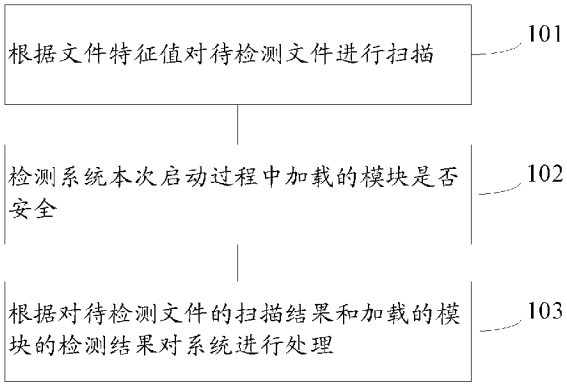
权利要求书2页 说明书7页 附图3页

(54)发明名称

病毒查杀方法及装置

(57)摘要

本申请提供了一种病毒查杀方法,包括以下步骤:根据文件特征值对待检测文件进行扫描;检测系统本次启动过程中加载的模块是否安全;根据对待检测文件的扫描结果和加载的模块的检测结果对系统进行处理。本申请还公开了一种实现前述方法的病毒查杀系统。本申请的病毒查杀方法及装置,能够实现有效的查杀病毒。



CN 102663288 B

1. 一种病毒查杀方法，其特征在于，包括以下步骤：

确定系统本次启动过程中加载的模块的安全级别信息；

根据待检测文件的文件特征值对所述待检测文件进行扫描；

根据安全级别信息检测系统本次启动过程中加载的模块是否安全，其中，所述加载的模块包括驱动程序、应用程序和动态链接库；

根据对待检测文件的扫描结果和加载的模块的检测结果对系统进行处理；

其中，所述确定系统本次启动过程中加载的模块的安全级别信息包括：监控系统本次启动中所有加载的模块，建立模块加载表，在所述模块加载表中记录下所有加载的模块文件特征值；将所述模块加载表中所有被记录的模块的文件特征值发送给服务器端，以供服务器端根据文件特征值进行安全级别信息的确定；接收并记录服务器端返回的安全级别信息。

2. 如权利要求 1 所述的病毒查杀方法，其特征在于，所述检测系统本次启动过程中加载的模块是否安全包括：

在扫描待检测文件的同时，结合检测系统本次启动过程中加载的模块中，与该待检测文件相关联的模块是否安全；

检测系统本次启动过程中加载的模块中是否有与所有待检测文件都不关联的模块，若有，判断其是否安全。

3. 如权利要求 1 所述的病毒查杀方法，其特征在于，所述根据安全级别信息检测系统本次启动过程中加载的模块是否安全包括：

获取系统本次启动过程中加载的模块的安全级别信息；

根据安全级别信息确定模块是否安全。

4. 如权利要求 1 所述的病毒查杀方法，其特征在于，所述确定系统本次启动过程中加载的模块的安全级别信息还包括：

在所述模块加载表中记录下所有加载的模块的路径，以便于根据所述路径查找加载的模块。

5. 如权利要求 1 至 4 任一项所述的病毒查杀方法，其特征在于，所述根据对待检测文件的扫描结果和加载的模块的检测结果对系统进行处理包括对异常系统进行处理，所述处理包括至少包括以下一种或几种：

若待检测文件中包含不安全文件，则删除所述文件；

若加载的模块中包含不安全模块，且系统中有所述不安全模块的启动项，则删除所述启动项；

若加载的模块中包含不安全模块，且系统中没有所述不安全模块的启动项，则强制系统重新启动或禁止系统在关机时写入启动项。

6. 一种病毒查杀装置，其特征在于，包括：

安全级别信息确定模块，用于确定系统本次启动过程中加载的模块的安全级别信息；

静态扫描模块，用于根据待检测文件的文件特征值对所述待检测文件进行扫描；

动态扫描模块，用于根据安全级别信息检测系统本次启动过程中加载的模块是否安全，其中，所述加载的模块包括驱动程序、应用程序和动态链接库；

处理模块，用于根据对待检测文件的扫描结果和加载的模块的检测结果对系统进行处

理；

所述安全级别信息确定模块包括：记录单元，用于监控系统本次启动中所有加载的模块，建立模块加载表，在所述模块加载表中记录下所有加载的模块和文件特征值；发送单元，用于将所述模块加载表中所有被记录的模块的文件特征值发送给服务器端，以供服务器端根据文件特征值进行安全级别信息的确定判断；和，接收单元，用于接收并记录服务器端返回的安全级别信息。

7. 如权利要求 6 所述的病毒查杀装置，其特征在于，所述动态扫描模块包括：

安全级别信息获取单元，用于获取系统本次启动过程中加载的模块的安全级别信息；

安全确定单元，用于根据安全级别信息确定模块是否安全。

8. 如权利要求 6 所述的病毒查杀装置，其特征在于，所述安全级别信息确定模块还包括：

路径记录单元，用于在所述模块加载表中记录下所有加载的模块的路径，以便于根据所述路径查找加载的模块。

9. 如权利要求 6 至 8 任一项所述的病毒查杀装置，其特征在于，所述处理模块包括：

异常处理单元，用于对异常系统进行处理，所述处理至少包括以下一种或几种：

若待检测文件中包含不安全文件，则删除所述文件；

若加载的模块中包含不安全模块，且系统中有所述不安全模块的启动项，则删除所述启动项；

若加载的模块中包含不安全模块，且系统中没有所述不安全模块的启动项，则强制系统重新启动或禁止系统在关机时写入启动项。

病毒查杀方法及装置

技术领域

[0001] 本申请涉及计算机安全技术领域，特别是涉及一种病毒查杀方法及装置。

背景技术

[0002] 为了保证电脑或者手机等电子产品的安全，通常需要安装杀毒软件。常见的杀毒软件都是通过用户连网之后，到杀毒软件厂商的网站上，下载新的病毒库，然后依靠自己的电脑或者手机进行查杀。虽然，随着技术的发展，这一系列的操作已经能够完全由杀毒软件自动完成。但是随着病毒库中病毒种类和数量的日益增多，用户的电脑或者手机上所需要存储的病毒库也会越来越大，这无疑会占用大量的系统资源，从而导致系统越来越慢。

[0003] 由此可见，这种传统的杀毒方法已经无法满足日益发展的病毒查杀需求。云查杀的出现，很好的解决了这个问题。即，各个杀毒软件厂商将查杀的病毒库转移到了服务器端（云端），在查杀时通过与服务器端的连网来实时获取最新的病毒库信息。当有一个客户端发现未知恶意文件时，服务端也就是云端，迅速的把文件特征值入库并迅速下发到其他客户端，这样就以最快的速度扼杀了病毒木马的传播。做到了强大的云查杀，云查杀比较传统的查杀方式做到了更加的及时性和更强大的对未知病毒的探测性，可以把安全领域带入了一个崭新的更高的“云端”

[0004] 但是，目前常见的是静态的云查杀技术，即通过扫描注册表和系统中所有的文件，将其特征值，比如 MD5 等，传到服务器的云端进行比对，如果发现是有问题的文件，就清除注册表相关项，并删除对应文件。但是因为恶意病毒也随着杀毒技术的发展而发展，新的病毒木马能够针对此种静态的云查杀采用新的对抗和隐藏技术，此种云查杀也无法满足准确查杀病毒的要求。

[0005] 例如，以前的 BYSHELL 木马是一个无进程、无 DLL、无启动项的、集多种 Rootkit 技术特征的独立功能远程控制后门程序 (Backdoor)。其利用线程注射 DLL 到系统进程，解除 DLL 映射并删除自身文件和启动项，关机时恢复。由于木马启动后，删除了自身的文件和注册表启动项，导致在使用云查杀的时候，根本无法查杀，而在关机前，这些木马再回写自身，导致了绕过了云查杀。又如，利用正常文件的木马，比如 a.exe 是个正常程序，会通过 LoadLibrary 加载其可能用到的 b.dll，但云查杀没有对 b.dll 进行验证，导致木马可以替换 b.dll，来达到利用正常文件加载木马的目的，同时也可以在加载后，删除自身，然后关机时回写等，并抹掉自身的 DLL 模块，以内存代码方式存在和执行。因此，可以看出，目前的常规云查杀方法并无法做到有效准确的查杀。

发明内容

[0006] 本申请提供一种病毒查杀方法及装置，能够解决无法有效查杀病毒的问题。

[0007] 为了解决上述问题，本申请公开了一种病毒查杀方法，包括以下步骤：

[0008] 根据文件特征值对待检测文件进行扫描；

[0009] 检测系统本次启动过程中加载的模块是否安全；

[0010] 根据对待检测文件的扫描结果和加载的模块的检测结果对系统进行处理。

[0011] 进一步地，所述检测系统本次启动过程中加载的模块是否安全包括：

[0012] 在扫描待检测文件的同时，结合检测系统本次启动过程中加载的模块中，与该待检测文件相关联的模块是否安全；

[0013] 检测系统本次启动过程中加载的模块中是否有与所有待检测文件都不关联的模块，若有，判断其是否安全。

[0014] 进一步地，所述检测系统本次启动过程中加载的模块是否安全包括：

[0015] 获取系统本次启动过程中加载的模块的安全级别信息；

[0016] 根据安全级别信息确定模块是否安全。

[0017] 进一步地，所述检测系统本次启动过程中加载的模块是否安全之前还包括：

[0018] 确定系统本次启动过程中加载的模块的安全级别信息。

[0019] 进一步地，所述确定系统本次启动过程中加载的模块的安全级别信息包括：

[0020] 监控系统本次启动中所有加载的模块，建立模块加载表，在所述模块加载表中记录下所有加载的模块文件特征值；

[0021] 将所述模块加载表中所有被记录的模块的文件特征值发送给服务器端，以供服务器端根据文件特征值进行安全级别信息的确定；

[0022] 接收并记录服务器端返回的安全级别信息。

[0023] 进一步地，所述确定系统本次启动过程中加载的模块的安全级别信息还包括：

[0024] 在所述模块加载表中记录下所有加载的模块的路径，以便于根据所述路径查找加载的模块。

[0025] 进一步地，所述根据对待检测文件的扫描结果和加载的模块的检测结果对系统进行处理包括对异常系统进行处理，所述处理包括至少包括以下一种或几种：

[0026] 若待检测文件中包含不安全文件，则删除所述文件；

[0027] 若加载的模块中包含不安全模块，且系统中有所述不安全模块的启动项，则删除所述启动项；

[0028] 若加载的模块中包含不安全模块，且系统中没有所述不安全模块的启动项，则强制系统重新启动或禁止系统在关机时写入启动项。

[0029] 为了解决上述问题，本申请还公开了一种病毒查杀装置，包括：

[0030] 静态扫描模块，用于根据文件特征值对待检测文件进行扫描；

[0031] 动态扫描模块，用于检测系统本次启动过程中加载的模块是否安全；

[0032] 处理模块，用于根据对待检测文件的扫描结果和加载的模块的检测结果对系统进行处理。

[0033] 进一步地，所述动态扫描模块包括：

[0034] 进一步地，所述动态扫描模块包括：

[0035] 安全级别信息获取单元，用于获取系统本次启动过程中加载的模块的安全级别信息；

[0036] 安全确定单元，用于根据安全级别信息确定模块是否安全。

[0037] 进一步地，所述装置还包括：

[0038] 安全级别信息确定模块，用于确定系统本次启动过程中加载的模块的安全级别信

息。

[0039] 进一步地，所述安全级别信息确定模块包括：

[0040] 记录单元，用于监控系统本次启动中所有加载的模块，建立模块加载表，在所述模块加载表中记录下所有加载的模块文件特征值；

[0041] 发送单元，用于将所述模块加载表中所有被记录的模块的文件特征值发送给服务器端，以供服务器端根据文件特征值进行安全级别信息的确定判断；和

[0042] 接收单元，用于接收并记录服务器端返回的安全级别信息。

[0043] 进一步地，安全级别信息确定模块还包括：

[0044] 路径记录单元，用于在所述模块加载表中记录下所有加载的模块的路径，以便于根据所述路径查找加载的模块。

[0045] 进一步地，所述处理模块包括：

[0046] 异常处理单元，用于对异常系统进行处理，所述处理至少包括以下一种或几种：

[0047] 若待检测文件中包含不安全文件，则删除所述文件；

[0048] 若加载的模块中包含不安全模块，且系统中有所述不安全模块的启动项，则删除所述启动项；

[0049] 若加载的模块中包含不安全模块，且系统中没有所述不安全模块的启动项，则强制系统重新启动或禁止系统在关机时写入启动项。

[0050] 与现有技术相比，本申请包括以下优点：

[0051] 本申请的病毒查杀方法通过静态扫描和动态扫描的结合。在系统启动时记录下动态文件信息，即本次启动过程中所加载的模块的信息，并预先通过服务器端对这些加载的模块的安全级别信息进行判断。系统启动早期属于真空期，某些病毒会利用该真空期进行工作。在静态扫描时，加入这些动态文件（本次启动过程中所加载的模块）的安全级别判断，可以识别出真空期加载的病毒文件。例如利用正常文件加载的木马程序以及加载后抹掉启动信息，关机回写的木马程序。从而保证识别出系统中隐藏，无法通过静态扫描查杀的病毒，实现有效的病毒查杀。

[0052] 优选地，在检测出恶意模块的加载，还可以及时提醒用户进行进一步地云查杀，达到木马预警或对其他类型的恶意程序进行预警的功能。

[0053] 当然，实施本申请的任一产品不一定需要同时达到以上所述的所有优点。

附图说明

[0054] 为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例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申请的一些实施例，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。

[0055] 图 1 是本申请的病毒查杀方法实施例一的流程图；

[0056] 图 2 是本申请的病毒查杀方法实施例二的流程图；

[0057] 图 3 是本申请的安全级别信息的确定过程的流程图；

[0058] 图 4 是本申请的病毒查杀装置实施例一的结构示意图；

[0059] 图 5 是本申请的病毒查杀装置实施例二的结构示意图。

具体实施方式

[0060] 下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员所获得的所有其他实施例，都属于本申请保护的范围。

[0061] 参照图 1，示出本申请的一种病毒查杀方法实施例一，包括以下步骤：

[0062] 步骤 101，根据文件特征值对待检测文件进行扫描。

[0063] 当用户手动或系统自动执行选择病毒查杀或者杀毒软件自动开始病毒查杀时，首先进行静态云扫描。文件特征值

[0064] 步骤 102，检测系统本次启动过程中加载的模块是否安全。

[0065] 系统本次启动过程中加载的模块是否安全包括：获取系统本次启动过程中加载的模块的安全级别信息；根据安全级别信息确定模块是否安全。系统启动过程中加载的模块包括驱动程序（.sys）、应用程序（.EXE）和动态链接库（.DLL）等等。

[0066] 其中，检测系统本次启动过程中加载的模块是否安全和根据文件特征值对待检测文件进行扫描可以同时或分步进行。

[0067] 同时进行包括：在扫描待检测文件的同时，结合检测系统本次启动过程中加载的模块中，与该待检测文件相关联的模块是否安全；检测系统本次启动过程中加载的模块中，是否有与所有待检测文件都不关联的模块，若有，判断其是否安全。

[0068] 例如，在每扫描一个注册表对应文件的同时，结合查询该文件对应的本次加载的模块是否安全，并进行标记。比如查询到某个注册表启动项时，先用常规静态云扫描处理后，如果查询该文件为安全文件，再结合系统本次启动过程中加载的模块的相关记录信息，查询与该文件关联的所有模块是否都安全，如果都安全，则确定该文件为安全文件，反之，则确定该文件为异常文件，那么可以确定系统异常。如果待检测文件经过静态扫描没有发现异常，且与其相关的模块也未出现异常，则需要检测系统本次启动过程中加载的模块中，是否有与所有待检测文件都不关联的模块，若有，在再进一步判断其是否安全。如果这些模块不安全，则也可以确定系统异常。如果静态扫描结果和系统本次启动过程中加载的模块都是安全，才可以确定系统正常。

[0069] 分步进行是指，可以先进行静态扫描后再进行系统本次启动过程中加载的模块是否安全的判断，也可以调换顺序。

[0070] 步骤 103，根据对待检测文件的扫描结果和加载的模块的检测结果对系统进行处理。

[0071] 当待检测文件的扫描结合和加载的模块的检测结果都是安全，则确定系统正常，可以不进行处理，反之，则说明系统异常，需要进行相应的处理。

[0072] 系统异常和对应的处理具体包括以下一种或几种情况：

[0073] 若待检测文件中包含不安全文件，则删除所述文件；

[0074] 若加载的模块中包含不安全模块，且系统中有所述不安全模块的启动项，则删除所述启动项；

[0075] 若加载的模块中包含不安全模块，且系统中没有所述不安全模块的启动项，则强

制系统重新启动或禁止系统在关机时写入启动项。

[0076] 可以理解，当发现系统异常时，除了及时对异常情况进行处理，还可以提醒用户，进行进一步地查杀（例如，云查杀等等），实现预警功能，确保查杀的有效性。

[0077] 参照图 2，示出本申请的病毒查杀方法实施例二，在步骤 102 或步骤 101 之前还可以包括以下步骤：

[0078] 步骤 201，确定系统本次启动过程中加载的模块的安全级别信息。

[0079] 参照图 3，安全级别信息的确定过程如下：

[0080] 步骤 2011，监控系统本次启动过程中所有加载的模块，建立模块加载表，在所述模块加载表中记录下所有加载的模块文件特征值。

[0081] 监控系统本次启动过程中所有加载的模块通过修改系统模块的加载顺序的方式实现，即，在系统启动时，将本申请的病毒查杀装置设置为最先加载的模块，然后再根据系统提供的各种函数来获取其他所有加载的模块文件特征值。其中，加载的模块包括驱动程序（.sys）、应用程序（.EXE）和动态链接库（.DLL）。例如，以 windows 操作系统为例，其在注册表（\Registry\Machine\System\CurrentControlSet\Control\ServiceGroupOrder）中定义了各模块加载的顺序。通过将本申请的病毒查杀装置组定义为 System ReserVed，就可以确保本申请的病毒查杀装置在系统启动的最早阶段就被加载，然后监控所有系统其他模块的加载，并记录下所有其他启动过程中所加载的模块文件特征值（例如，MD5 等）。windows 操作系统提供了函数 PsSetLoadImageNotifyRoutine，通过设置一个回调函数，本申请的病毒查杀装置就可以在任何模块被加载前获得通知。

[0082] 优选地，还可以在模块加载表中记录下所有加载的模块的路径，以便于根据所述路径查找加载的模块。以 windows 操作系统为例，其中的 FullImageName 为被加载模块的全路径名，通过该全路径名可以获得加载模块的全路径。

[0083] 因此，本申请的病毒查杀装置可以在系统加载任何一个模块的时候获得该文件的路径和文件特征值信息，并进行记录保存。

[0084] 优选地，除了建立模块加载表来记录所加载的模块的路径和文件特征值，还可以根据所加载的模块的类型对各模块进行标记，用以快速区分各模块类型。例如，模块是驱动程序、应用程序还是动态链接库等等。仍以 windows 操作系统为例，其中，SystemModeImage，用来标记是否是驱动程序、还是应用程序，或者是动态链接库。

[0085] 另外，对于不同类型的模块，可以在加载时记录不同的模块信息。例如，加载应用程序时，可以记录下应用程序文件所在的路径和文件特征值。加载其他模块，比如动态链接库时，则除了记录下动态链接库文件所在的路径和文件特征值，还可以记录下动态链接库所在的应用程序文件的路径和文件特征值（MD5 等）。从而保证记录信息的完整性，以保证后续病毒查杀的准确性。

[0086] 步骤 2012，将所述模块加载表中所有被记录的模块的文件特征值发送给服务器端，以供服务器端根据文件特征值进行安全级别信息的确定。

[0087] 其中，病毒查杀装置通过所在客户端将文件特征值发送给服务器端，可以在系统启动后，网络可用时立即发送，也可以在用户手动选择病毒查杀或者杀毒软件自动进行病毒查杀的时候发送。只要能在病毒查杀完成之前得出结果即可。

[0088] 步骤 2013，接收并记录服务器端返回的安全级别信息。

[0089] 服务器端根据文件特征值进行安全级别信息的确定，得出具体的安全级别信息后回传给客户端的病毒查杀装置。病毒查杀装置对模块的安全级别信息进行记录保存。

[0090] 其中，服务器端确定的安全级别信息可以自定义，例如包括安全、危险、未知等级别，也可以采用一级、二级、三级等方式来进行区分，只要能够体现出各模块是否安全状态即可，具体的确定规则也可以根据实际需要预先设置，本申请对此并不限制。

[0091] 本申请的病毒查杀方法在系统启动时记录下动态文件信息，即本次启动过程中加载的模块的信息，并预先通过服务器端对这些模块的安全级别进行判断。系统启动早期属于真空期，某些病毒会利用该真空期进行工作。在静态扫描时，加入这些动态文件（本次启动过程中所加载的模块）的安全级别信息的判断，可以识别出真空期加载的病毒文件。

[0092] 例如利用正常文件加载的木马程序以及加载后抹掉启动信息，关机回写的木马程序。从而保证识别出系统中隐藏，无法通过静态扫描查杀的病毒，实现有效的病毒查杀。优选地，在检测出恶意模块的加载，还可以及时提醒用户进行云查杀，达到木马预警的功能。

[0093] 例如，以 byshell 为例，当其被系统加载的时候，就被记录下来了，后续进行云查杀的时候，虽然静态扫描无法查询到该木马对应的文件和注册表，但通过查询动态的模块加载表，就可以知道系统存在这种加载，并自动销毁自身的木马，然后通过强制重新启动，让木马在关机重新启动的时候，没机会回写自身，达到重新启动后，清除木马的目的。

[0094] 再如前述的正常文件被利用问题，在扫描到启动项的时候，查询动态生成的模块加载表中对应的应用程序所加载的模块列表中是否存在可疑动态链接库模块，如存在，即使是一个正常文件，也可以将其清除掉，从而解决了原来无法处理的正常文件被利用的问题。

[0095] 参照图 4，示出本申请的病毒查杀装置实施例一，包括静态扫描模块 10、动态扫描模块 20 和处理模块 30。

[0096] 静态扫描模块 10，用于根据文件特征值对待检测文件进行扫描。

[0097] 动态扫描模块 20，用于检测系统本次启动过程中加载的模块是否安全。

[0098] 处理模块 30，用于根据对待检测文件的扫描结果和加载的模块的检测结果对系统进行处理。

[0099] 其中，动态扫描模块 20 和静态扫描模块 10 可以完全独立工作，即二者均可以由系统发出的扫描指令触发，可以同时扫描，也可以分步扫描。可以理解，两者也可以相互关联，即静态扫描模块 10 进行扫描时，扫描到某个文件，则可以触发动态扫描模块 20 扫描与该文件相关的模块，反之，动态扫描模块 20 在扫描时也可以触发静态模块 10 进行扫描，本申请对此并不限制。

[0100] 参照图 5，示出本申请的病毒查杀装置实施例二，优选地，该装置还包括安全级别信息确定模块 50，用于确定系统本次启动过程中加载的模块的安全级别信息。

[0101] 其中，安全级别信息确定模块 50 包括记录单元、发送单元和接收单元。记录单元，用于监控系统本次启动过程中所有加载的模块，建立模块加载表，在所述模块记载表中记录下所有加载的模块文件特征值；

[0102] 发送单元，用于将所述模块记载表中所有被记录的模块的文件特征值发送给服务器端，以供服务器端根据文件特征值进行安全级别信息的确定；

[0103] 接收单元，用于接收并记录服务器端返回的安全级别信息。

[0104] 优选地，安全级别信息确定模块 50 还包括路径记录单元，用于在所述模块加载表中记录下所有加载的模块的路径，以便于根据所述路径查找加载的模块。

[0105] 优选地，动态扫描模块 20 包括安全级别信息获取单元，用于获取系统本次启动过程中加载的模块的安全级别信息；安全确定单元，用于根据根据安全级别信息确定模块是否安全。

[0106] 优选地，处理模块 30 包括异常处理单元，用于对异常系统进行处理，所述处理至少包括以下一种或几种：

[0107] 若待检测文件中包含不安全文件，则删除所述文件；

[0108] 若加载的模块中包含不安全模块，且系统中有所述不安全模块的启动项，则删除所述启动项；

[0109] 若加载的模块中包含不安全模块，且系统中没有所述不安全模块的启动项，则强制系统重新启动或禁止系统在关机时写入启动项。

[0110] 本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。对于装置实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0111] 通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到本申请可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如 ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例或者实施例的某些部分所述的方法。

[0112] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于装置或系统实施例而言，由于其基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。以上所描述的装置及系统实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[0113] 以上对本申请所提供的病毒查杀方法及装置进行了详细介绍，本文中应用了具体个例对本申请的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的一般技术人员，依据本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本申请的限制。


根据文件特征值对待检测文件进行扫描
101
检测系统本次启动过程中加载的模块是否安全
102
根据对待检测文件的扫描结果和加载的模块的检测结果对系统进行处理
103

图 1


确定系统本次启动过程中加载的模块的安全级别信息
201
根据文件特征值对待检测文件进行扫描
101
检测系统本次启动过程中加载的模块是否安全
102
根据对待检测文件的扫描结果和加载的模块的检测结果对系统进行处理
103

图 2

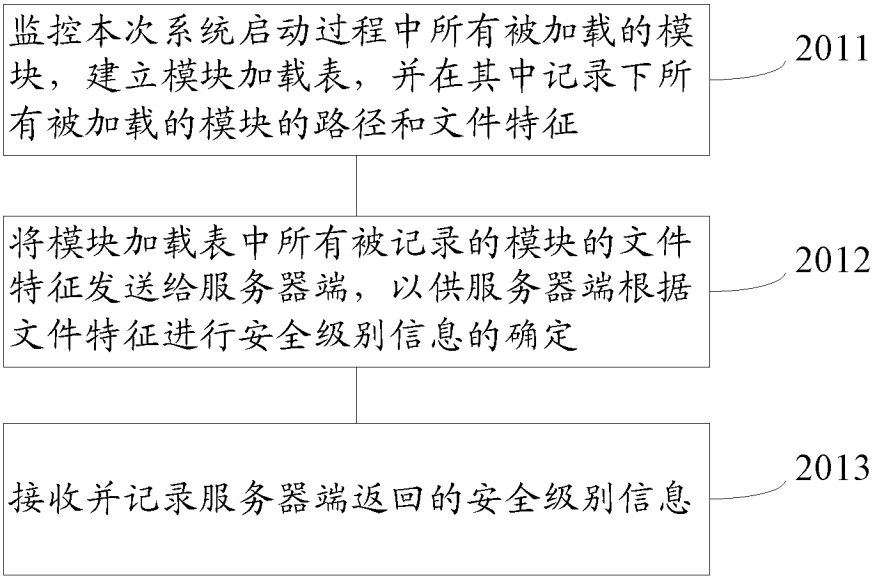

监控本次系统启动过程中所有被加载的模块，建立模块加载表，并在其中记录下所有被加载的模块的路径和文件特征
2011
将模块加载表中所有被记录的模块的文件特征发送给服务器端，以供服务器端根据文件特征进行安全级别信息的确定
2012
接收并记录服务器端返回的安全级别信息
2013

图 3

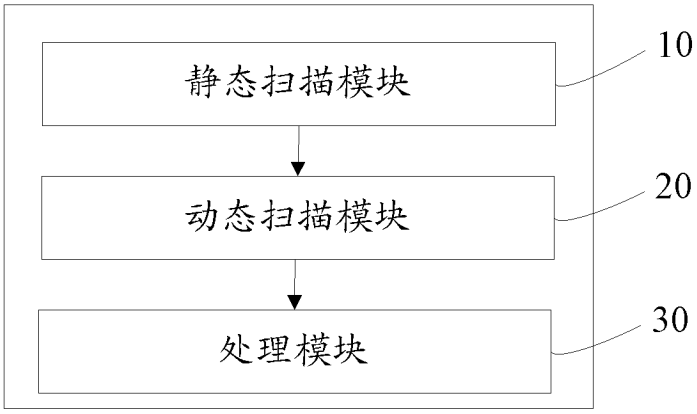

静态扫描模块
10
动态扫描模块
20
处理模块
30

图 4

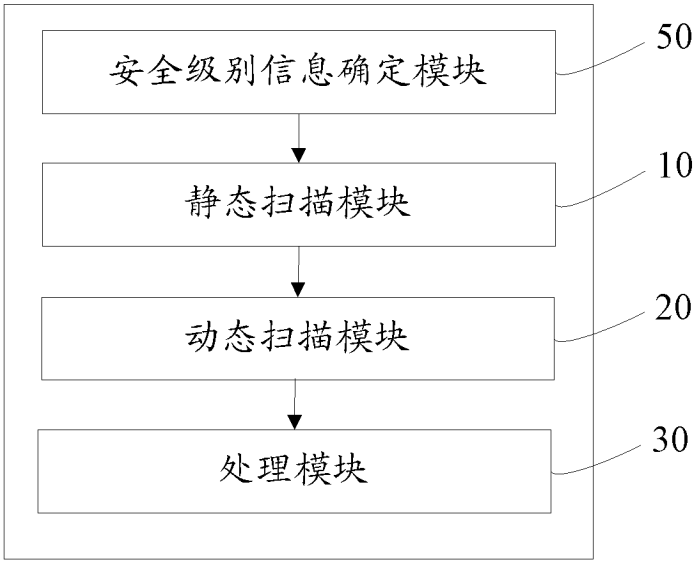


图 5