(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 107103238 A
(43)申请公布日 2017.08.29

(21)申请号 201710150404.2

(22)申请日 2012.02.29

(62)分案原申请数据
201210050079.X 2012.02.29

(71)申请人 卡巴斯基实验室封闭式股份公司
地址 俄罗斯联邦莫斯科

(72)发明人 米哈伊尔·A·帕夫柳席奇卡
弗拉季斯拉夫·V·马蒂嫩科
尤里·G·斯洛博迪亚努克

(74)专利代理机构 北京市磐华律师事务所 11336
代理人 高伟 赵楠

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

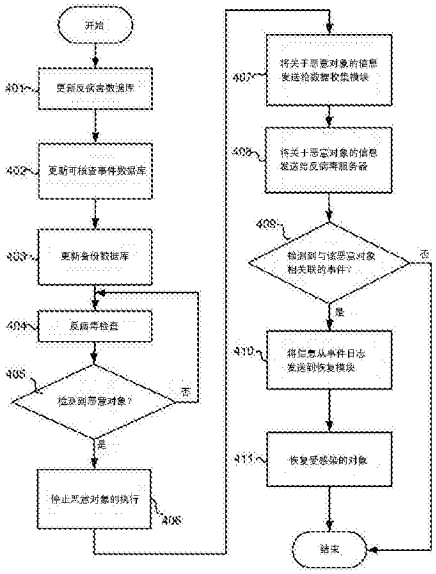
权利要求书4页 说明书9页 附图8页

(54)发明名称

用于保护计算机系统免遭恶意对象活动侵害的系统和方法

(57)摘要

本发明公开了用于保护计算机免遭恶意对象活动侵害的系统、方法和计算机程序产品。该方法包括:对计算机上一个或多个进程的执行事件进行监控;识别被监控事件之中的可核查事件,包括文件的创建、更改或者删除事件,系统注册表的更改事件,以及由在计算机上所执行的进程进行的网络访问事件;在单独的文件、注册表以及网络事件日志中记录识别出的可核查事件;对计算机上的一个或多个软件对象执行恶意软件检查;如果确定了对象是恶意的,那么从文件、注册表和网络事件日志中识别与所述恶意对象相关联的事件;对与所述恶意对象相关联的文件事件执行回退操作;对与所述恶意对象相关联的注册表事件执行回退操作;终止与所述恶意对象相关联的网络连接。



CN 107103238 A

1.一种用于计算机恶意软件防护的方法,所述方法包括:

识别存储在定期更新可核查事件数据库中的可核查事件列表,所述可核查事件列表识别在应当被监控的计算机上的一个或多个软件对象的执行活动,所述执行活动至少包括由所述一个或多个软件对象进行的文件的创建、更改或者删除事件,系统注册表的参数和值的创建、更改或者删除事件,以及网络连接事件;

对所述计算机上的所述一个或多个软件对象的执行事件进行监控;

基于所述可核查事件数据库中的所述可核查事件列表,在单独的文件中,识别并记录被监控的所述一个或多个软件对象的事件日志、注册表事件日志以及网络事件日志,包括识别由所述被监控的一个或多个软件对象所创建的任何文件;

识别父和子进程与由所述被监控的软件对象所生成的执行线程之间的关系;

对所述计算机上的所述被监控的一个或多个软件对象执行恶意软件检查,包括在执行所述被监控的一个或多个软件对象期间所生成的所有进程和线程;

如果基于检测到在执行所述对象期间生成的恶意进程或线程从而由所述恶意软件检查确定了对象是恶意的,那么从存储在所述可核查事件数据中的所述文件事件日志、注册表事件日志和网络事件日志中识别一个或多个与所述恶意对象相关联的文件事件、注册表事件以及网络连接事件,并且进一步识别一个或多个被由所述恶意对象所生成的识别的父和子进程以及执行线程所建立的网络连接以及由每个父和子进程以及执行线程所创建的每个文件;

通过删除由所述恶意对象所创建的所有被识别的文件以及由每个父和子进程以及执行线程所创建的每个文件,对与所述恶意对象相关联的一个或多个文件事件执行回退操作;

对与所述恶意对象相关联的一个或多个注册表事件执行回退操作;

终止与所述恶意对象相关联的一个或多个网络连接,并且进一步终止由所述恶意对象所生成的父和子进程以及执行线程所建立的一个或多个被识别的网络连接。

2.根据权利要求1的方法,其中执行文件事件的回退操作包括:

基于所述识别出的与所述恶意对象相关联的文件事件,识别由所述恶意对象所更改或者删除的一个或多个文件;以及从可信的备份中恢复至少部分的所述被更改和删除的文件。

3.根据权利要求1的方法,其中执行注册表事件的回退操作包括:

基于所述识别出的与所述恶意对象相关联的注册表事件,识别由所述恶意对象所创建、更改或者删除的一个或多个注册表参数和值;

删除由所述恶意对象所创建的新的注册表参数和值;以及

从可信的备份中恢复被更改或者删除的注册表参数和值。

4.根据权利要求1的方法,其中更进一步地包括:从所述文件事件日志、注册表事件日志中识别与一个或多个相关的父和子进程以及由所述恶意对象所生成的执行线程相关联的一个或多个文件事件和注册表事件。

5.根据权利要求4的方法,更进一步的包括:

识别一个或多个被所述父和子进程以及由所述恶意对象所生成的执行线程所创建、更改或者删除的系统和非系统文件;

从可信的备份中恢复至少部分的所述被更改的系统和非系统文件或者被删除的系统和非系统文件；

删除所有识别出的被所述父和子进程以及由所述恶意对象所生成的执行线程所创建的新的非系统文件。

6.根据权利要求4的方法，更进一步的包括：

识别一个或多个被所述父和子进程以及由所述恶意对象所生成的执行线程所创建、更改或者删除的注册表参数和值；

删除一个或多个识别出的被所述父和子进程以及由所述恶意对象所生成的执行线程所创建的新的注册表参数和值；以及

从可信的备份中恢复被更改或者删除的注册表参数和值。

7.根据权利要求1的方法，更进一步的包括：

识别至少一个由所述恶意对象所生成的线程或进程，所述恶意对象执行在所述计算机的安全对象或进程中并创建网络连接；

8.根据权利要求7的方法，其中，如果所述安全对象或进程是所述计算机的系统文件，则终止所述网络连接，并且利用从备份数据库中所获得的文件的备份副本来恢复所述系统。

9.一种用于计算机恶意软件防护的系统，其中所述计算机具有处理器和存储器，所述系统至少包括以下被加载到所述计算机的所述存储器中并可由所述计算机的所述处理器执行的软件模块：

反病毒数据库，其包含与已知恶意对象有关的信息；

定期更新可核查事件数据库，其包含可核查事件的列表，所述可核查事件的列表识别在应当被监控的计算机上的一个或多个软件对象的执行活动，所述活动至少包括由所述计算机上的所述一个或多个软件对象进行的文件的创建、更改或者删除事件，系统注册表的参数和值的创建、更改或者删除事件，以及网络连接事件；

数据收集模块，其经配置以：

对所述计算机上所述一个或多个进程的执行事件进行监控；

基于所述可核查事件数据库中的所述可核查事件列表，在单独的文件中，识别并记录所述被监控的一个或多个软件对象的事件日志、注册表事件日志以及网络事件日志，包括识别由所述被监控的一个或多个软件对象所创建的任何文件；

识别父和子进程与由所述被监控的软件对象所生成的执行线程之间的关系；

识别一个或多个被由所述恶意对象所生成的父和子进程以及执行线程所建立的网络连接；

反病毒模块，其经配置以：

使用包含在所述反病毒数据库中的所述与已知恶意对象有关的信息，对所述计算机上的被监控的一个或多个软件对象执行恶意软件检查，所述反病毒数据库包括在执行所述被监控的一个或多个软件对象期间所生成的所有进程和线程；

如果基于检测到在执行所述对象期间生成的恶意进程或线程从而由所述恶意软件检查确定了对象是恶意的，那么终止由所述恶意对象所建立的一个或多个网络连接，并且进一步终止识别出的所述一个或多个网络连接以及由每个父和子进程以及执行线程所创建

的每个文件，所述识别出的所述一个或多个网络连接被由所述恶意对象所生成的所述父和子进程以及执行线程所建立；

恢复模块，其经配置以：

如果由所述恶意软件检查确定了所述对象是恶意的，

那么通过删除由所述恶意对象所创建的所有被识别的文件以及由每个父和子进程以及执行线程所创建的每个文件，对与所述恶意对象相关联的一个或多个文件事件执行回退操作；以及

对与所述恶意对象相关联的一个或多个注册表事件执行回退操作。

10.根据权利要求9的系统，其中对于对文件事件执行回退操作，所述恢复模块更进一步地经配置以：

基于所述识别出的与所述恶意对象相关联的文件事件，识别由所述恶意对象所更改或者删除的一个或多个文件；以及

从可信的备份中恢复至少部分的所述被更改和删除的文件。

11.根据权利要求9的系统，其中对于对注册表事件执行回退操作，所述恢复模块更进一步地经配置以：

基于所述识别出的与所述恶意对象相关联的注册表事件，识别由所述恶意对象所创建、更改或者删除的一个或多个注册表参数和值；

删除由所述恶意对象所创建的新的注册表参数和值；以及

从可信的备份中恢复被更改或者删除的注册表参数和值。

12.根据权利要求9的系统，其中所述数据收集模块更进一步地经配置以：从所述文件事件日志和注册表事件日志中识别与一个或多个相关的父和子进程以及由所述恶意对象所生成的执行线程相关联的一个或多个文件事件和注册表事件。

13.根据权利要求10的系统，其中所述恢复模块更进一步地经配置以：

识别一个或多个被所述父和子进程以及由所述恶意对象所生成的执行线程所创建、更改或者删除的系统和非系统文件；

从可信的备份中恢复至少部分的所述被更改的系统和非系统文件或者被删除的系统和非系统文件；

删除所有识别出的被所述父和子进程以及由所述恶意对象所生成的执行线程所创建的新的非系统文件。

14.根据权利要求10的系统，其中所述恢复模块更进一步地经配置以：

识别一个或多个被所述父和子进程以及由所述恶意对象所生成的执行线程所创建、更改或者删除的注册表参数和值；

删除一个或多个识别出的被所述父和子进程以及由所述恶意对象所生成的执行线程所创建的新的注册表参数和值；以及

从可信的备份中恢复被更改或者删除的注册表参数和值。

15.根据权利要求9的系统，其中所述数据收集模块更进一步地经配置以识别至少一个或多个由所述恶意对象所生成的线程或进程，所述恶意对象执行在所述计算机的安全对象或进程中并创建网络连接

16.根据权利要求15的系统，其中，如果所述安全对象是所述计算机的系统文件，则所

述反病毒模块更进一步地经配置以终止所述网络连接，并且利用从备份数据库中所获得的文件的备份副本来恢复所述系统。

用于保护计算机系统免遭恶意对象活动侵害的系统和方法

[0001] 本申请是分案申请，其原申请的中国国家申请号为201210050079.X，发明名称为“用于保护计算机系统免遭恶意对象活动侵害的系统和方法”。

技术领域

[0002] 本发明所公开的内容总体上涉及计算机安全领域，并且，具体地说，涉及用于保护计算机系统免遭恶意对象的文件、注册表、系统和网络活动侵害的系统、方法和计算机程序产品。

背景技术

[0003] 当前计算机技术的发展已经达到了很高的水平。随着计算机技术的发展，数字数据的数量以更快节奏的速率在增长。与此同时，数字数据是易损的并且需要防范恶意对象比如病毒、特洛伊木马、蠕虫、间谍软件及其他类型的恶意软件的侵害。

[0004] 使用反病毒系统来保护信息免受恶意软件的侵害，该反病毒系统的基本任务是阻止恶意对象的危险活动。但情况是：反病毒系统不能以及时的方式来阻止恶意的活动。这种情况出现在，例如，新型的恶意软件出现的时候，反病毒系统的可用方法无法将其检测出来，因为这些系统对新的恶意软件一无所知。另一种情况也可能是：恶意软件利用操作系统的弱点或者反病毒系统自身的不足之处来绕过反病毒系统。

[0005] 已经侵入到计算机系统中的恶意软件可以展现出不同类型的恶意活动：文件活动、注册表活动、系统活动以及网络活动。在恶意的文件活动期间，恶意对象可对文件执行不同的操作，比如移除、更改、或者新文件的创建。恶意注册表活动典型地包括注册表参数和值的创建、修改或者移除。关于注册表活动的许多情况都是已知的，例如，恶意对象更改了注册表的参数以便加载操作系统时引起恶意软件的自动启动(auto-launch)。当恶意软件在计算机系统中开始或者停止进程的时候，或者当它在系统或者程序进程中启动新的执行线程的时候，可能发生恶意的系统活动。恶意的网络活动典型地包括由恶意对象来创建新的网络连接。

[0006] 利用这些恶意的活动，恶意软件可以侵入到计算机系统中，并且可以获取其上所存储的数据。因此，需要检测出恶意的活动，并且对恶意活动所损坏、修改或者移动的数据进行恢复。

发明内容

[0007] 本文公开了用于保护计算机免遭恶意对象的文件、注册表、系统和网络活动侵害的系统、方法和计算机程序产品。在一个示例性实施例中，所述系统包括反病毒数据库，以及可核查事件数据库，其中反病毒数据库包含与已知恶意对象有关的信息，可核查事件数据库包含可核查事件的列表，该可核查事件至少包括文件的创建、更改或者删除事件，系统注册表的创建、更改或者删除事件，以及由在计算机上所执行的进程进行的网络访问事件。所述系统还包括数据收集模块，其可操作地用于监控计算机上一个或多个进程的执行事

件;基于包含在可核查事件数据存储器中的可核查事件的列表,识别被监控事件中的可核查事件;并且在存储器所包含的单独的文件、注册表以及网络事件日志中记录所识别出的可核查事件。

[0008] 所述系统还包括反病毒模块,其经配置以:使用包含在反病毒数据库中的关于已知恶意对象的信息,对计算机上的一个或多个软件对象执行恶意软件检查。如果确定了对象是恶意的,那么反病毒模块从网络事件日志中识别一个或多个与所述恶意对象相关联的网络事件,并且终止由所述恶意对象所建立的一个或多个网络连接。所述系统还包括恢复模块,其经配置以:如果确定了对象是恶意的,那么从文件和注册表事件日志中识别一个或多个与所述恶意对象相关联的文件和注册表事件,并且对与所述恶意对象相关联的文件事件以及注册表事件执行回退操作(rollback)。

[0009] 在一个示例性实施例中,用于保护计算机免遭恶意软件侵害的方法包括:对计算机上一个或多个进程的执行事件进行监控;识别被监控事件之中的可核查事件,其中可核查事件包括文件的创建、更改或者删除事件,系统注册表的创建、更改或者删除事件,以及由在计算机上所执行的进程进行的网络访问事件;在单独的文件、注册表以及网络事件日志中记录所识别出的可核查事件;对计算机上的一个或多个软件对象执行恶意软件检查;如果确定了对象是恶意的,那么从文件、注册表和网络事件日志中识别与所述恶意对象相关联的事件;对与所述恶意对象相关联的文件事件执行回退操作;对与所述恶意对象相关联的注册表事件执行回退操作;终止与所述恶意对象相关联的网络连接。

[0010] 上述示例性实施例的简要概括用于提供对于本发明的基本理解。这个概括并非对本发明所有关注方向的广泛概述,并且其既非意图确定所有实施例的关键或者决定因素,也非意图划定任何一个实施例或者所有实施例的范围界限。其唯一的目的是,在下面更加详细地对本发明进行描述之前,以简化的形式来提出一个或多个实施例。为了完成前述事项,所述一个或多个实施例包括了权利要求中所描述并且具体指出的特征。

附图说明

[0011] 并入此说明书并构成此说明书的一部分的附图图示了本发明的一个或多个示例性实施例,并且,与详细说明一起用来解释这些实施例的原理和实现过程。

[0012] 在附图中:

[0013] 图1示出了根据一个示例性实施例的恶意软件保护系统的示意图;

[0014] 图2示出了根据另一个示例性实施例的恶意软件保护系统的操作示意图;

[0015] 图3示出了根据另一个示例性实施例的恶意软件保护系统的操作示意图;

[0016] 图4A-4E示出了根据多个示例性实施例的恶意软件保护系统的操作算法;

[0017] 图5示出了根据一个示例性实施例的计算机系统的示意图。

具体实施方式

[0018] 在此围绕用于保护计算机免遭恶意软件侵害的系统、方法和计算机程序产品来描述本发明的示例性实施例。那些本领域的普通技术人员将意识到以下描述仅仅是说明性的而并非意图以任何方式进行限定。受益于此公开内容,本领域技术人员可以容易地想到其它实施例。现在进行详细地介绍以实现附图中所图示的本发明的示例性实施例。所有的附

图以及随后的描述中都尽可能使用相同的附图标记来表示相同的或者相似的项目。

[0019] 图1示出了根据一个示例性实施例的恶意软件保护系统100的示意图。系统100可由在个人计算机或者网络服务器上所配置的软件应用程序来实现，在下面的图5中对其进行了更为详细地描述。在一个示例性实施例中，系统100包括了反病毒模块120，其执行软件对象110的反病毒检查，所述软件对象110包括对象111，112和113，例如系统和程序文件、脚本及其它在部署有系统100的个人计算机或者服务器上运行的可执行程序代码。软件对象110中的对象112是恶意的。在一个示例性实施例中，反病毒模块120可以是程序模块，其使用驱动器来与其上部署有系统100的计算机的操作系统的核心进行交互。反病毒模块120可以使用不同的恶意软件检测技术，例如签名检查(signal check)，或者试探和行为分析(heuristic and behavioral analysis)，或者其它用于对象110分析的方法。

[0020] 签名检查是以被分析对象110的字节代码与存储在恶意软件签名中的不同的恶意对象代码之间的比较为基础的。在搜索恶意对象时，试探分析使用了分析引擎，该分析引擎灵活地运用了设定模式(set pattern)，例如利用模糊逻辑来描述的模式。在特定情况中，行为分析是以对系统事件的观察为基础的。对于恶意对象的确定是以其在系统中的行为在对恶意软件行为所设定规则的框架内为基础的。

[0021] 在对于对象110进行反病毒检查期间，反病毒模块120也可以检查在这些对象的执行期间所启动的进程和线程。在对象110和相关进程以及线程的分析期间，反病毒模块120可以使用包含在反病毒数据库121中的恶意软件签名和行为签名。恶意软件对象的签名是字节序列，其与正在被检查的对象的程序代码进行比较。在一个示例中，可以将签名视为以校验和(checksum)的形式存在的，其为每个恶意对象加以创建并且存储在反病毒数据库121中。在这种情况下，反病毒模块120可以将正在被分析的对象的校验和与已知的恶意对象的签名进行比较。如果二者之间存在匹配，则表示正在被分析的对象是恶意的。

[0022] 而行为签名包含了有关潜在恶意对象可能的行为的信息，例如启动系统函数、引用注册表数据等等。反病毒模块120可以监控对象110的行为以及相关的进程和线程；如果所述对象的行为与来自反病毒数据库121的已知的恶意对象的行为签名相似，则将被监控对象112认定为是恶意的。

[0023] 在一个示例性实施例中，如果反病毒模块120检测到了恶意对象112，则其将关于该恶意对象的识别信息传送给数据收集模块150。该识别信息可以包含到恶意对象112的路径、该对象的名称或者，例如，恶意软件的校验和。此外，反病毒模块120可以请求数据收集模块150向反病毒模块120提供与某些系统活动有关的信息，所述系统活动与所识别的恶意对象112的执行相关联，以便检测出任何与该恶意对象相关联的有关恶意进程和线程。

[0024] 在另一个示例性实施例中，反病毒模块120也可以将与所检测出的恶意软件有关的信息经由因特网180发送给远程的中央反病毒服务器(未图示)。而该反病毒服务器可以将与所检测出的恶意对象有关的信息分发给其它的有权访问所述反病毒服务器的恶意软件保护系统。通过中央反病毒服务器，恶意软件信息在部署于网络中的不同计算机上的恶意软件保护系统100之间进行交换，由此可以阻止新型的恶意软件的传播。

[0025] 当反病毒模块120检测到危险的系统活动时，例如由该对象112所启动的危险进程或者由该对象112在另一个进程中所执行的危险线程的启动，则反病毒模块120被配置为终止该危险活动。特别地，反病毒模块120终止了危险进程或者执行线程的执行，并且将识别

信息传送给数据收集模块150，所述识别信息与启动这一进程或者执行线程的恶意对象112有关。

[0026] 在一个示例性实施例中，数据收集模块150经配置以对不同对象110所执行的活动进行监控，并且将对象活动的历史收集到文件或注册表或者其它事件152-154的日志中。例如，在对象110，诸如对象111，112和113的执行的过程中，这些对象可以启动实现文件修改(文件活动)、注册表的更改(注册表活动)、和/或网络连接的创建(网络活动)的进程。该数据收集模块150经配置以记录此活动的历史。在一个示例性实施例中，该数据收集模块150可以参考可核查(auditable)事件数据库151以获得应受监控的事件的列表。该可核查事件列表151包括但是不局限于，文件创建、修改和删除事件，注册表更改事件，进程或者线程生成事件，网络连接创建事件，以及其它可能具有恶意活动特征的事件。此外，为了收集事件数据，数据收集模块150也可以通过跟踪是由哪个进程在何时安装了哪些文件，以及是由哪个进程在何时生成了哪个进程(即，父子关系)，来识别不同对象之间的父子关系。

[0027] 在这些实施例之一中，数据收集模块150可以监控所有在可核查事件数据库151中识别出来的系统事件和/或与特定对象相关联的事件。最后，数据收集模块150可以包含被恶意软件保护系统100所监控的软件对象110的指标列表，例如系统地址。对于所监控的对象，数据收集模块150可以将文件创建、移除或者改变的事件，还有注册表值的创建、移除或者更改的事件，以及其它在可核查事件数据库151中被指示的事件记录到事件的日志152-154。例如，如果该计算机系统中的某个对象在操作系统的系统文件夹中创建了文件，其中反病毒模块120并未确定该对象的恶意性，那么数据收集模块150可以记录这一事件，并且是由什么对象创建了什么文件将会为人所知。随后，当反病毒检查时，如果发现这一文件是由恶意对象所创建的，那么可由恢复模块160将这一文件移除，以下将更为详细地对其进行描述。

[0028] 在一个示例性实施例中，数据收集模块150也可为不同类型的可核查事件维护单独的日志，例如文件事件的日志152以及注册表事件的日志153，其用于存储与被监控对象的文件以及注册表活动有关的信息。在其它的实施例中，系统100还可以保存其它事件的日志154，例如用户活动事件、数据输入-输出事件、网络活动事件等等。以这种方式，系统100可以收集不同对象的系统、文件、注册表以及网络活动的历史。

[0029] 在一个示例性实施例中，该文件事件日志152可包含执行文件活动的对象的标识符(例如，文件名，进程或者线程标识符)、文件活动的类型(例如，新文件的创建，文件的更改，文件的移除)以及对其执行操作的文件的标识符。所述文件标识符可实现为，例如，文件路径、文件校验和、或者文件-路径(file-path)校验和。

[0030] 在一个示例性实施例中，该注册表事件日志153可包含执行注册表活动的对象的标识符、注册表活动的类型(例如，新的注册表参数的创建，注册表参数值的改变，注册表参数或者值的移除)以及对其执行操作的注册表参数的名称。

[0031] 在一个示例性实施例中，网络事件日志154可包含执行网络活动的对象的标识符(例如，文件名，进程或者线程标识符)、网络活动的类型(例如，新的网络连接的创建，网络连接的端口数或者类型，例如TCP，UDP或者FTP等等)以及经由已建立的连接所传送/接收的数据的类型(例如，所接收/传送的文件的标识符)。所述文件标识符可实现为，例如，文件路径、文件校验和、或者文件-路径校验和。

[0032] 在一个示例性实施例中，可以定期更新可核查事件数据库151以及反病毒数据库121。可以伴随着新型威胁的出现来定期地更新该反病毒数据库121，以使该反病毒模块120以及时的方式来可靠执行对恶意对象及其他威胁的检测。也应当对存储在数据库151中的可核查事件的列表进行定期地更新，以确保新型的恶意活动可被该恶意软件保护系统所监控。可以通过更新模块170来更新数据库121以及151，所述更新模块170使用到因特网180的连接，可以从该中央反病毒服务器下载反病毒定义以及可核查事件的最新版本。该更新模块170可以实现为基于提供网络连接的网络适配器的软件模块。

[0033] 在一个示例性实施例中，在常规恶意软件检查期间，当该反病毒模块120检测到恶意对象112时，模块120将与该恶意对象112有关的信息传达给数据收集模块150。模块150从文件事件日志152、注册表事件日志153以及网络事件日志154中提取关于该恶意对象112的文件、注册表、以及网络活动的信息。此外，模块150识别与对象112所生成的所有父进程和子进程以及执行线程相关联的所有文件、注册表以及网络活动。然后，模块150将这一信息发送给恢复模块160。根据所接收到的信息，如果曾创建了新的文件或者注册表参数，则恢复模块160确定哪些文件或者注册表参数需要被移除；以及如果这些文件或者注册表参数已经被更改或者移除，则恢复模块160确定哪些文件或者注册表参数需要被修复。

[0034] 在一个示例性实施例中，已经利用数据收集模块150接收了数据的恢复模块160对与恶意对象相关联的文件和注册表事件执行回退操作。例如，恢复模块160可以删除所有由该恶意对象112创建的新的非系统文件和注册表参数。如果已经更改了任意一些文件或者注册表值，或者已经移除了任意一些文件、注册表值或者参数，那么执行原始文件、注册表值以及参数的恢复。对于原始文件以及注册表数据，恢复模块160可以参考文件备份数据库161以及注册表备份数据库162。在其它的实施例中，系统100也可以包括其它数据备份数据库163，用于诸如用户数据的其它类型数据。

[0035] 在一个示例性实施例中，该文件备份数据库161可包含对于其上部署有系统100的计算机系统的操作来说具有特殊意义的文件130的副本。此类文件可包括系统文件，例如ntoskrnl.exe、ntdetect.com、hal.dll、boot.ini及其它在Microsoft® Windows® NT家族的操作系统中的文件。此外，文件备份数据库161还可以存储其他文件，这些文件的完整性对于该计算机系统或者系统用户来说是非常重要的。该注册表备份数据库162可包含影响操作系统性能的注册表数据140的副本。

[0036] 为了恢复计算机系统的文件130以及注册表数据140，恢复模块160对从数据收集模块150所接收到的数据进行处理，并且接收关于被更改或移除的文件或者注册表参数的信息。此后，恢复模块160在备份数据库161和162中检索对应的文件以及注册表参数。如果找到了这样的文件以及注册表数据，那么恢复模块160修复被所述恶意对象更改或者移除的文件以及注册表数据。

[0037] 在特定的实施例中，恢复模块160可以只对被更改文件的修改部分进行修复而并非对整个文件进行修复。在这种情况下，备份文件数据库161也将包含文件的最有可能遭受到恶意行为侵害的部分。

[0038] 在一个示例性实施例中，可由用户或者经由更新模块170从远程的中央反病毒数据库来对所述备份数据库161-163进行文件以及注册表信息的填写。在后一种情况下，更新模块170使用新的文件以及注册表值来启动对备份数据库161-163的填写，其中所述新的文

件以及注册表值的列表是由更新模块170通过因特网180从中央反病毒服务器或者其它可靠数据源接收而来的。此后，更新模块170可以开始更新进程，并且恢复模块160将文件、注册表及其他数据的备份副本分别填写到备份数据库161-163中。

[0039] 图2示出了根据一个示例性实施例的恶意软件保护系统的操作示意图。恶意对象的文件活动可以并非仅包括文件的创建和移除，而在仅包括文件的创建和移除的情况下将由恢复模块160对文件进行相应地移除或者修复。恶意对象的其它行为也是可能的，例如更改文件。在图2中，恶意对象212更改了对象213，该对象213在该更改行为之前是无害的。该更改行为可以包括例如将恶意代码引入到原始文件213中。在对象213中发生这些改变之后，对象212停止执行任何活动。在另一方面，对象213开始执行例如与文件130或者注册表值140的移除相关联的活动。与此同时，与对象213的活动相关联的行为可能会被数据收集模块150所记录。

[0040] 如果，在反病毒检查的过程中，反病毒模块120确定对象213具有威胁性，亦即，其是恶意的；模块120可以阻断对象213的活动并且将有关这一对象的信息传送给数据收集模块150和反病毒服务器(未图示)。数据收集模块150将有关活动历史记录的信息传送给恢复模块160，其中恢复模块160利用备份数据库161-163来修复已被更改的数据。与此同时，如果对象213的副本在文件备份数据库161中，那么恢复模块160也对对象213进行修复。

[0041] 此外，反病毒模块120可以请求数据收集模块150提供有关与对象213相关联的活动的信息。作为响应，数据收集模块150可以向反病毒模块120提供对象213已经被对象212所更改的信息。然后反病毒模块120可以进行针对对象212的反病毒检查，确定其是恶意的并且对其进行阻断，由此来阻止此对象进一步的恶意行为。

[0042] 图3示出了根据另一个示例性实施例的恶意软件保护系统的操作示意图。某些对象310在其执行过程中可以创建新的网络连接，例如，到因特网180的连接。如果网络连接是由恶意对象创建的，那么由于其增加了计算机的易受攻击性，则可能会导致对于计算机的威胁。恶意对象可以从该计算机传送数据或者从因特网下载其它的危险对象到该计算机上。为了防止这样的情况发生，根据一个实例性实施例，可由数据收集模块150监控对象的网络活动并且将其记录到网络事件日志154中。

[0043] 更具体地说，如果反病毒模块120检测到了恶意对象，那么反病毒模块120可以向数据收集模块150请求与恶意对象的网络活动或者任何与所述恶意对象相关的对象、进程或线程有关的信息。在上述的示例中，对象312为具有网络活动的恶意对象，其中由数据收集模块150将所述网络活动记录在网络事件日志154中。在确定了对象312是恶意的并且识别出与对象312相关联的网络事件之后，反病毒模块120可以终止/阻断所有由恶意对象312所建立的网络连接，终止恶意对象312的执行，并且如果对于这一对象或者任何相关的对象已经观察到了恶意的文件或者注册表活动，则将有关对象312的信息传送给数据收集模块150以便随后对文件和注册表数据进行修复。

[0044] 情况也可能是：恶意对象312在计算机的安全对象或者进程311中生成了进程或者执行线程，然后所述进程或者执行线程又创建了记录在网络事件日志154中的网络连接。随着这种情况的出现，可以区分出两种情形：当恶意对象312将其自身引入到安全对象311或者安全进程中而没有影响系统性能的时候，或者当恶意对象312将其自身引入到表示系统文件或者系统进程的对象313中的时候。

[0045] 在第一种情形下，当被感染的对象或者进程并非系统进程的时候，反病毒模块120会随后记录感染以及后续网络活动的实际情况，并且阻断被修改的对象311。在阻断该对象的过程中，停止其以下活动：

[0046] • 文件活动：该对象不能执行文件操作；

[0047] • 注册表活动：阻断访问系统注册表的可能性；

[0048] • 系统活动：终止所有由该对象启动的进程和流程；

[0049] • 网络活动：阻断创建网络连接的可能性。

[0050] 如果反病毒模块120检测到执行线程是由恶意对象312生成在进程311中的，那么将由反病毒模块120终止所述线程，以及还可由反病毒模块120自动地终止所有与进程311相关联的网络连接。

[0051] 在系统文件或者进程313被修改的情况下，反病毒模块120通常不能阻断系统对象313，因为这样会导致操作系统的故障。然而，一旦检测到了所述被修改的系统文件313的网络活动，反病毒模块120可以停止该网络活动，并且终止仅由所引入的那部分代码所启动的网络连接，同时对象313保持操作。然后可以利用系统对象313在文件备份数据库161中的备份副本来对其进行修复。

[0052] 如果恶意执行线程是由对象312生成在系统对象313中的，那么该恶意线程执行可以被终止而并不影响对象313。

[0053] 图4A示出了根据一个示例性实施例的恶意软件保护系统的操作算法。在步骤401-403，可利用更新模块170来更新反病毒数据库121、可核查事件数据库151以及备份数据库161-163。紧接着，在步骤404，反病毒模块120在计算机系统中执行针对对象110的反病毒检查。如果在步骤405中，发现正在检查的对象或者由这些对象所启动的进程都不是恶意的，那么可以在随后的时段重复步骤405的过程。然而，如果对象110或者相应进程中的任何一个是恶意的，那么则在步骤406中停止该恶意对象的执行。此外，在步骤407，将识别这一对象的信息传送给数据收集模块150，并且在步骤408传送给反病毒服务器。此外，也可以从反病毒服务器接收关于所检测的对象在其它用户的计算机中活动的信息。还可以由反病毒模块120来使用这一信息。在下一个步骤409中，对于是否存在这一对象的活动执行检查。具体地，针对所述恶意对象或者任何相关进程、线程等的活动，在文件事件日志152、注册表事件日志153及其他可用事件日志154中执行数据搜索。如果发现了所述恶意对象的恶意文件或者注册表活动的记录，那么在步骤410将涉及由所述对象所执行的活动的数据传送给恢复模块160。在步骤411，恢复模块160使用这一数据，并利用来自数据库161和162的文件和注册表备份数据，对文件和注册表数据进行修复。

[0054] 图4B示出了恶意软件保护系统响应于恶意网络活动的操作算法的一个示例性实施例。在步骤501，反病毒模块120检查被检测到的恶意对象312或者与其相关联的进程是否已经请求或者打开任何网络连接。可以利用数据收集模块150来获取这一信息。在步骤502，在由反病毒模块120阻断该恶意对象312之后，自动终止由该恶意对象312本身所直接创建的网络连接。如果来自数据收集模块150的信息还指示了这一恶意对象已经对其它的对象311、312做了修改，其中在对象311、312中也已经观察到了网络活动，那么在步骤503，反病毒模块120检查被修改的对象是否为系统对象。如果被修改的对象311不是系统对象，那么在步骤502，反病毒模块120阻断这一对象，并且自动终止该网络连接。如果是系统对象313

发生了更改，那么是不可能阻断所述对象的，因为这样可能会导致操作系统的故障。然而，在步骤504，反病毒模块120可以终止由该被修改的系统对象313中被引入的部分所启动的网络连接。该对象本身仍保持操作。然后，可以利用恢复模块160来修复这一系统对象。在系统进程中加载了恶意线程的情况下，也可以停止这一恶意执行线程。

[0055] 图4C示出了恶意软件保护系统响应于恶意系统活动的操作算法的一个示例性实施例。系统活动包括由恶意对象所启动的进程的出现，以及在其它进程中执行线程的启动。在步骤601，如果反病毒模块120通过例如利用数据收集模块150来请求信息从而识别出恶意对象的系统活动，那么反病毒模块120可在步骤602终止所有与该对象相关联的进程和线程。此外，可将与被终止的进程有关的信息转发给恢复模块160，所述恢复模块160确定是否有任何受感染的文件或者注册表数据需要更新。

[0056] 图4D示出了恶意软件保护系统响应于恶意注册表活动的操作算法的一个示例性实施例。在步骤701，反病毒模块120利用数据收集模块150来确定注册表140是否受到感染，例如通过恶意对象的活动生成了新的注册表入口。如果检测到这种活动，则在步骤702可以指令恢复模块160将新建数据从注册表中移除。如果注册表参数的值已被更改或者移除，或者如果注册表参数已被删除，那么在步骤703恢复模块160检查受感染的注册表值和参数是否在备份注册表数据库162中。如果发现了备份数据，则在步骤705恢复模块160采用备份的副本来修复被更改或者被移除的注册表值或者参数。

[0057] 图4E示出了恶意软件保护系统响应于恶意文件活动的操作算法的一个示例性实施例。在步骤801，反病毒模块120利用数据收集模块150来请求关于所有由恶意对象所创建的新文件的信息。如果创建了新的文件，则在步骤802指令恢复模块160移除此文件。如果没有创建新的文件，但是恶意对象已经更改或者移除了现有的文件，则在步骤803，恢复模块160确定在数据库161中的受感染文件的备份副本是否可用。如果在步骤804发现了所需的文件，则在步骤805恢复模块160修复受感染的文件。

[0058] 图5描绘了其上可部署恶意软件保护系统100的计算机系统5的示例性实施例。计算机系统5可以包括网络服务器、个人计算机、笔记本、平板电脑、智能电话、媒体接收器或者其它类型的数据处理和计算装置。计算机5可以包括一个或多个由系统总线10所连接的处理器15、存储器20、一个或多个硬盘驱动器30、一个或多个光盘驱动器35、一个或多个串行端口40、图形卡45、声卡50和网卡55。系统总线10可以是多种类型总线结构中的任何一种，其中所述总线结构包括了存储器总线或者存储器控制器、外围总线以及使用各种已知的总线架构中的任意一种的局部总线。处理器15可以包括一个或多个Intel® Core 2Quad 2.33GHz处理器或者其它种类的微处理器。

[0059] 系统存储器20可以包括只读存储器(ROM)21以及随机存取存储器(RAM)23。存储器20可实现为DRAM(动态随机存取存储器)、EPROM、EEPROM、闪存或者其它类型的存储器架构。ROM 21存储了包含有基本例行程序的基本输入/输出系统22(BIOS)，所述基本例行程序有助于在计算机系统5的组件之间传送信息，例如在启动期间。RAM 23存储了操作系统24(OS)，例如Windows® XP Professional或者其它类型的操作系统，所述操作系统负责对计算机系统5中的进程进行管理和协调，并且对计算机系统5中的硬件资源进行配置和共享。系统存储器20也存储了应用程序和程序25，例如服务306。系统存储器20也存储了由程序25所使用的各种运行时(runtime)数据26。

[0060] 计算机系统5可更进一步地包括硬盘驱动器30，例如SATA磁性硬盘驱动器(HDD)，以及用于从可移动光盘，例如CD-ROM、DVD-ROM或者其它光媒体进行读取或者写入的光盘驱动器35。驱动器30和35及其相关联的计算机可读媒体提供了计算机可读指令、数据结构、应用程序和程序模块/子程序的非易失性存储，其中上述计算机可读指令、数据结构、应用程序和程序模块/子程序实现了在此公开的算法以及方法。虽然示范性的计算机系统5使用了磁盘以及光盘，但是本领域技术人员应该了解到在所述计算机系统的可替换实施例中也可以使用其他类型的可以储存计算机系统5可访问的数据的计算机可读介质，例如磁带盒、闪存卡、数字视频光盘、随机存取存储器、只读存储器、可擦除可编程只读存储器及其它类型的存储器。

[0061] 计算机系统5更进一步地包括多个串行端口40，例如通用串行总线(USB)，其用于连接数据输入设备75，例如键盘、鼠标、触摸板及其它设备。串行端口40也可用于连接数据输出设备80，例如打印机、扫描仪及其他设备，以及连接其它的外围设备85，例如外部数据存储设备等。系统5也可包括图形卡45，例如nVidia® GeForce® GT 240M或者其它的视频卡，用于与监视器60或者其它的视频再现设备相连接。系统5也可包括声卡50，用于经由内部或者外接扬声器65再现声音。此外，系统5可以包括网卡55，例如以太网、WiFi、GSM、蓝牙或者其它有线、无线或蜂窝网络接口，用于将计算机系统5连接到网络70，例如因特网。

[0062] 在不同的实施例中，在此所描述的算法以及方法都可以通过硬件、软件、固件或者其任何组合方式来实现。如果用软件来实现，那么其功能可以以一个或多个指令或者代码的方式存储在非暂时性计算机可读介质上。计算机可读介质同时包括计算机存储和通信介质，二者有助于将计算机程序从一个地方传送到另一个地方。存储介质可以是可由计算机访问的任何可用介质。举例来说，而并非限定，这种计算机可读介质可以包括RAM、ROM、EEPROM、CD-ROM或其它的光盘存储器、磁盘存储器或其它的磁存储设备、或者任何其它可用于携带或存储所需的以指令或者数据结构的形式存在的程序代码并且可由计算机访问的介质。此外，任何连接都可被称为计算机可读介质。例如，如果利用同轴电缆、光纤电缆、双绞线、数字用户线路(DSL)或者无线技术如红外线、无线电和微波来从网站、服务器或者其它的远程资源传输软件，则其均包括在所述介质的定义中。

[0063] 为了清楚起见，在此并未对实施例的所有常规特征加以示出和描述。应当意识到在任何这类实际的实施方式的开发过程中，必须做出大量特定的实施方式决策以实现开发者的特定目标，同时应当意识到这些特定目标将随实施方式的不同以及开发者的不同而改变。而且，应当意识到这类开发工作可能是复杂且耗费时间的，但是对于受益于本文公开内容的本领域的普通技术人员而言，都将是常规的工程任务。

[0064] 此外，可以理解的是在此使用的措辞或术语是为了描述而非限定的目的，以便本领域的技术人员根据在此提出的教导及指引并结合相关领域技术人员所掌握的知识来解读本说明书中的措辞或术语。而且，除非如此明确的予以阐述，否则本说明书或权利要求中的任何术语均并非意图归结为非常规或者特殊的含义。

[0065] 在此披露的各种实施例包含在此通过示例的方式所提及的已知组件的现在和将来的已知等同物。而且，尽管已经示出及描述了实施例及其应用，但对于受益于本发明的本领域的技术人员而言显而易见的是，在不脱离本申请中所披露的发明构思的情况下，比以上提及的更多的修改是可能的。

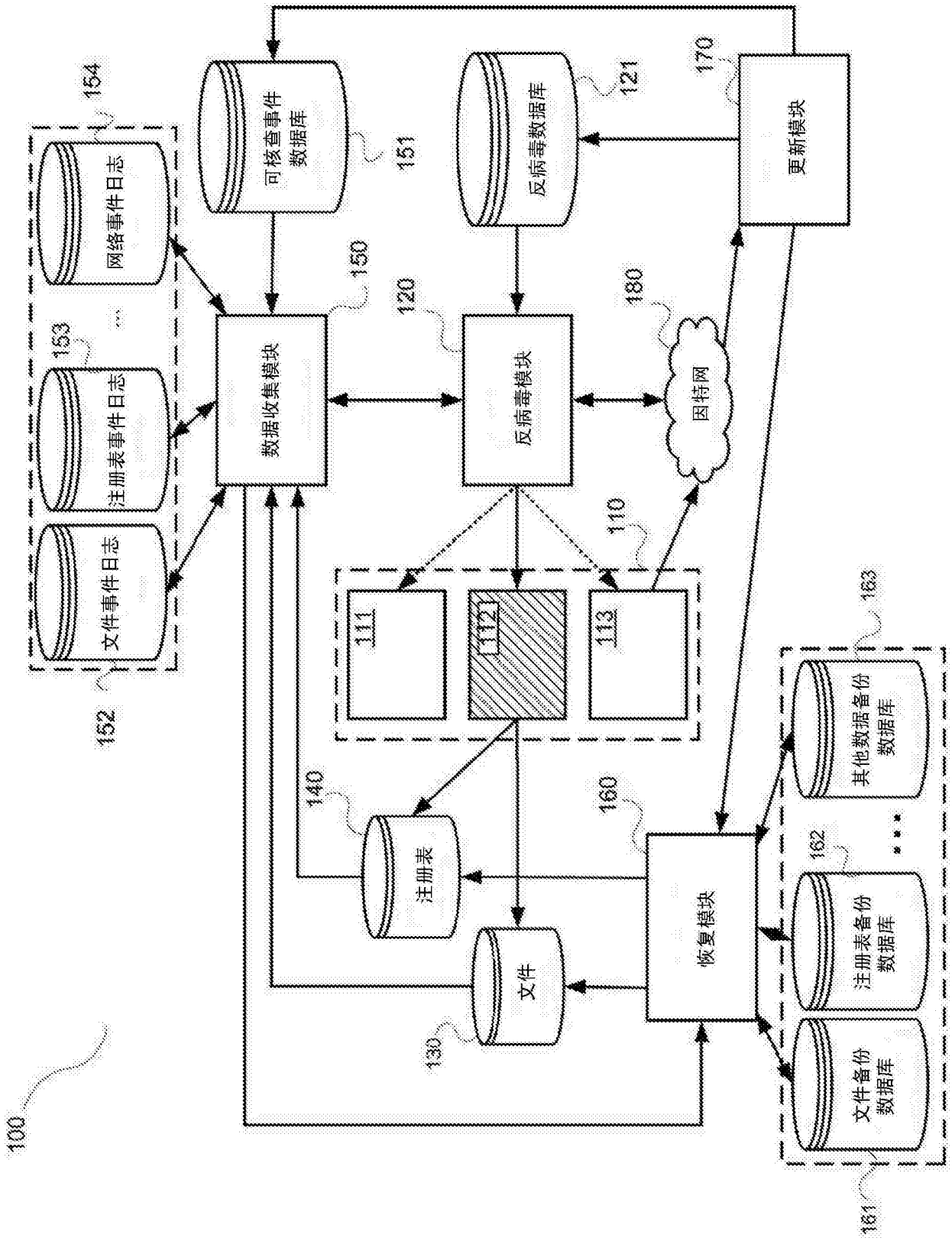

100
可核查事件数据库
151
反病毒数据库
121
更新模块
170
网络事件日志
154
注册表事件日志
153
文件事件日志
152
数据收集模块
150
反病毒模块
120
因特网
180
110
111
112
113
注册表
140
文件
130
恢复模块
160
其他数据备份数据库
163
注册表备份数据库
162
文件备份数据库
161

图1

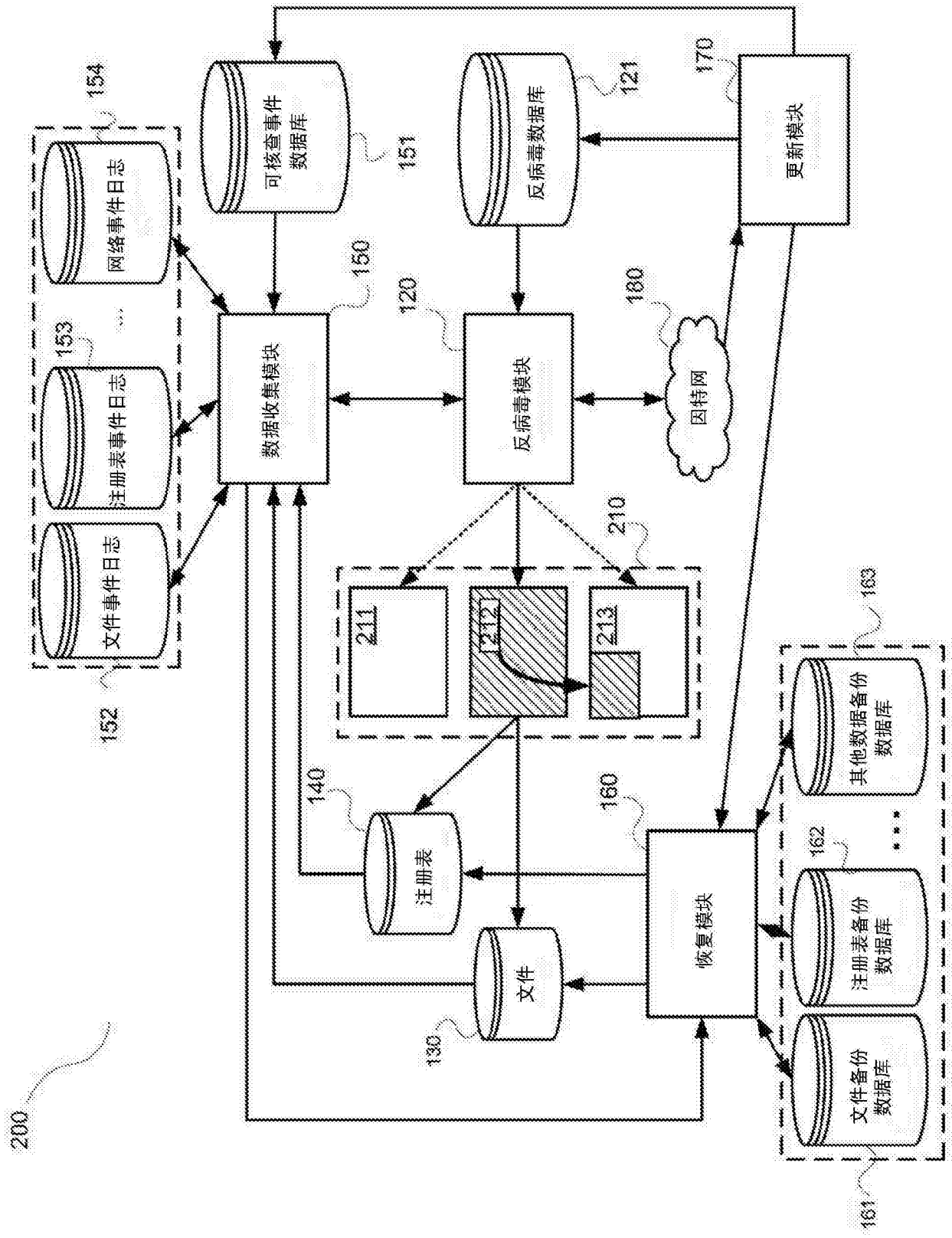

200
152
154
网络事件日志
...
153
注册表事件日志
文件事件日志
可核查事件数据库
151
150
数据收集模块
反病毒数据库
121
120
反病毒模块
170
更新模块
180
因特网
210
211
212
213
140
注册表
130
文件
160
恢复模块
163
其他数据备份数据库
162
注册表备份数据库
文件备份数据库
161

图2

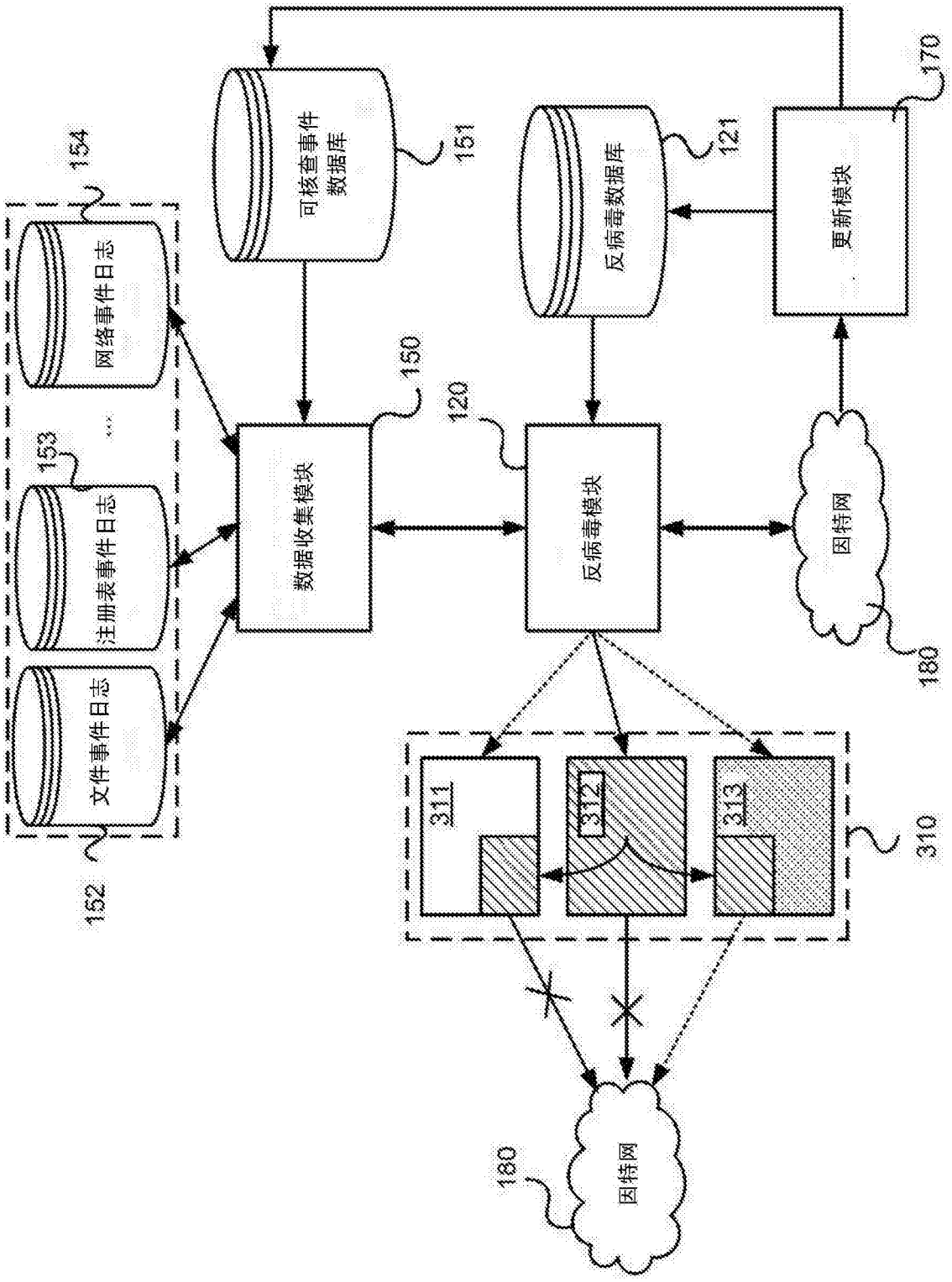

可核查事件数据库
151
反病毒数据库
121
更新模块
170
154
网络事件日志
...
153
注册表事件日志
文件事件日志
152
数据收集模块
150
120
反病毒模块
因特网
180
311
312
313
310
因特网
180

图3

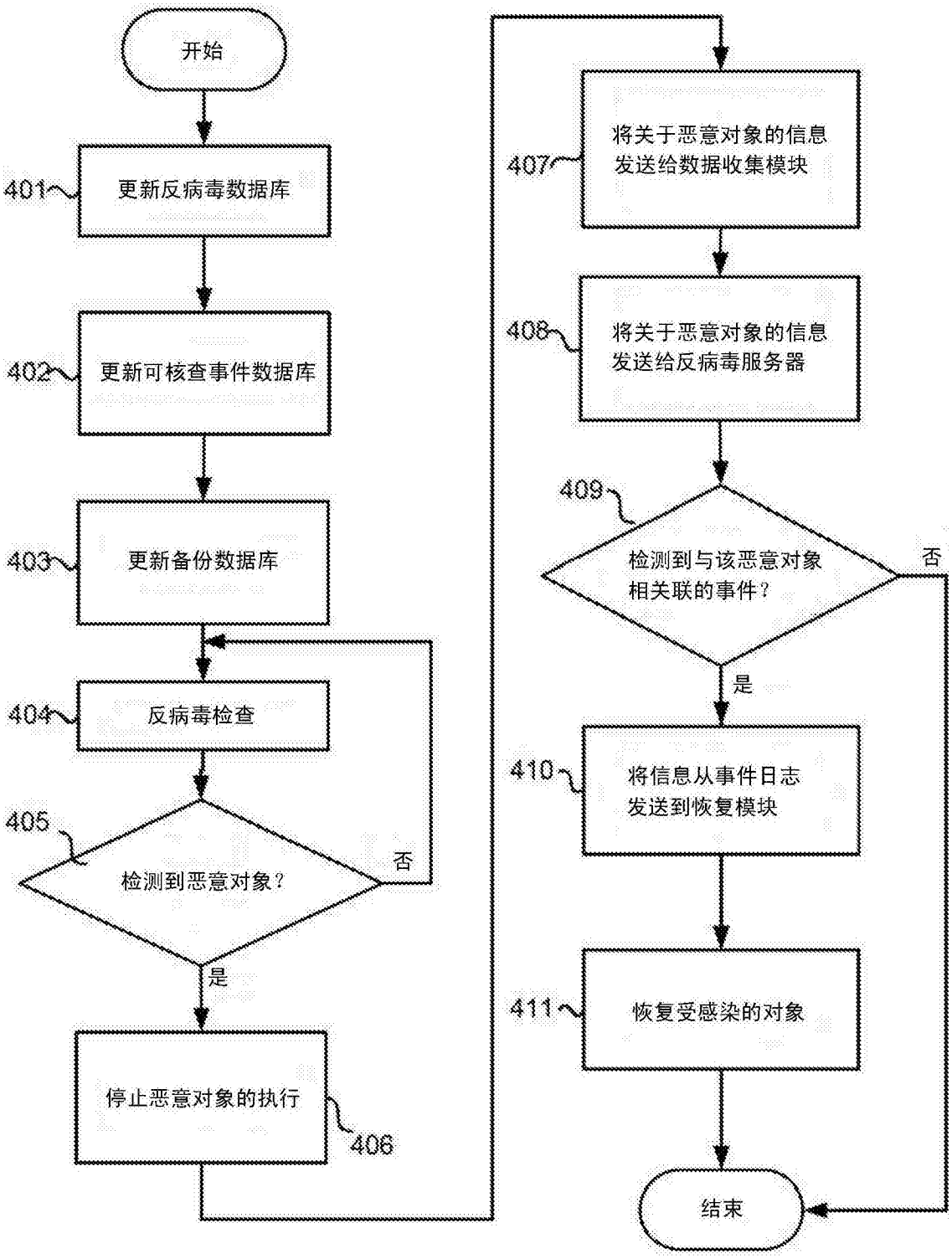

开始
401
更新反病毒数据库
402
更新可核查事件数据库
403
更新备份数据库
404
反病毒检查
405
检测到恶意对象？
否
是
406
停止恶意对象的执行
407
将关于恶意对象的信息发送给数据收集模块
408
将关于恶意对象的信息发送给反病毒服务器
409
检测到与该恶意对象相关联的事件？
否
是
410
将信息从事件日志发送到恢复模块
411
恢复受感染的对象
结束

图4A

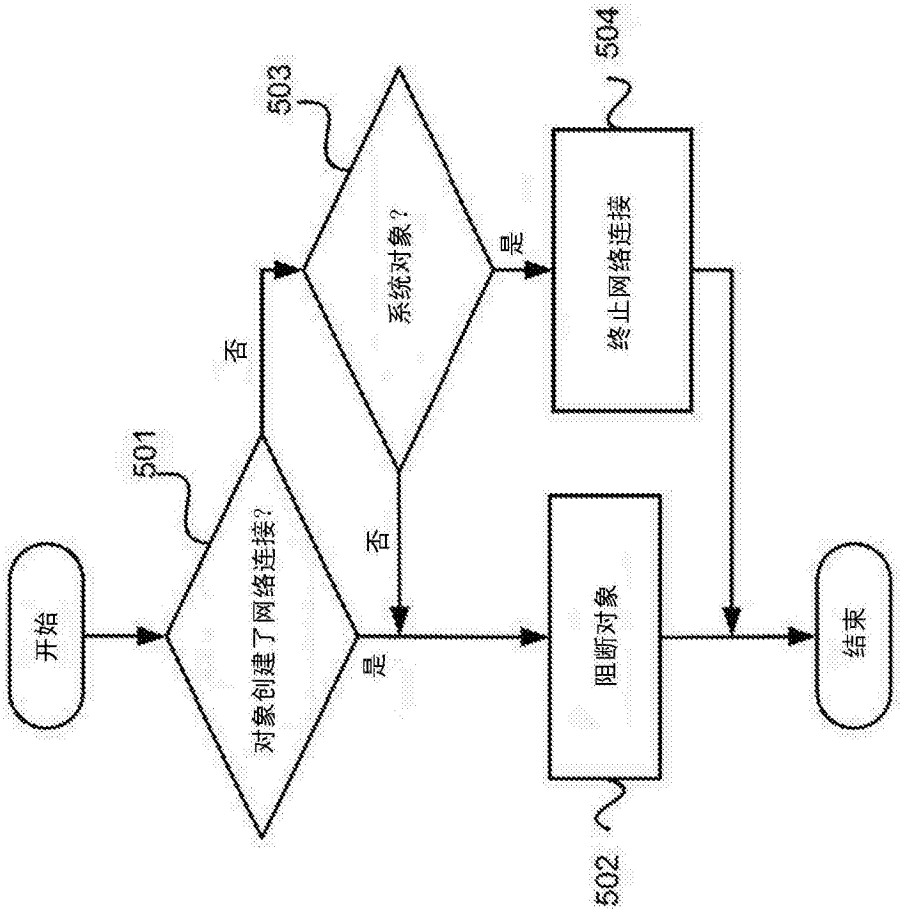

开始
对象创建了网络连接?
501
否
是
系统对象?
503
是
否
终止网络连接
504
阻断对象
502
结束

图4B

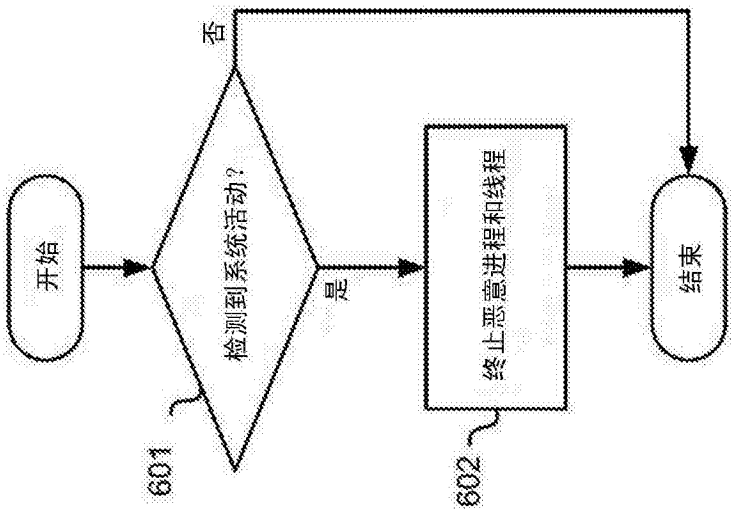

开始
检测到系统活动?
601
否
是
终止恶意进程和线程
602
结束

图4C

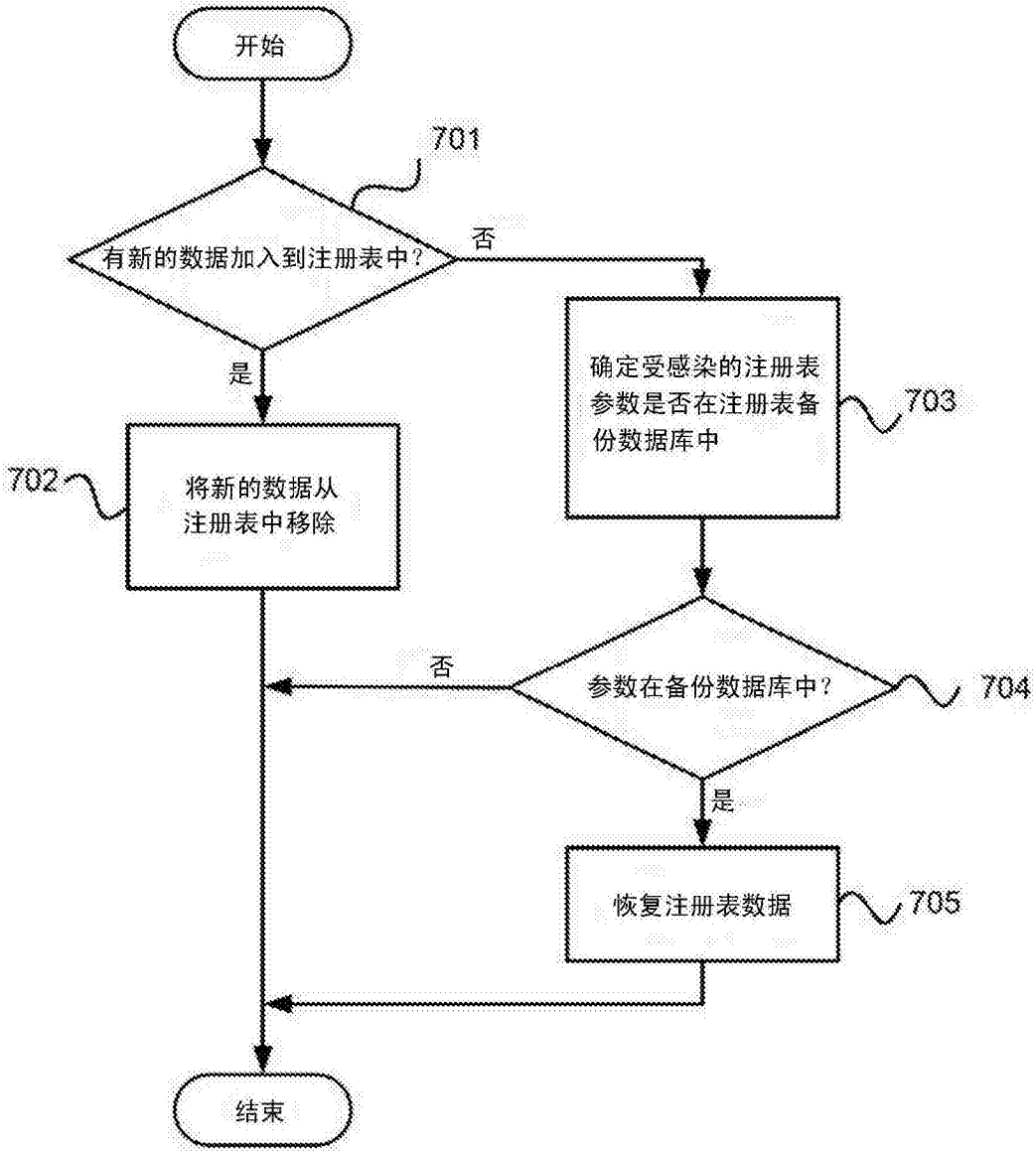

开始
701
有新的数据加入到注册表中？
否
是
确定受感染的注册表参数是否在注册表备份数据库中
703
702
将新的数据从注册表中移除
否
参数在备份数据库中？
704
是
恢复注册表数据
705
结束

图4D

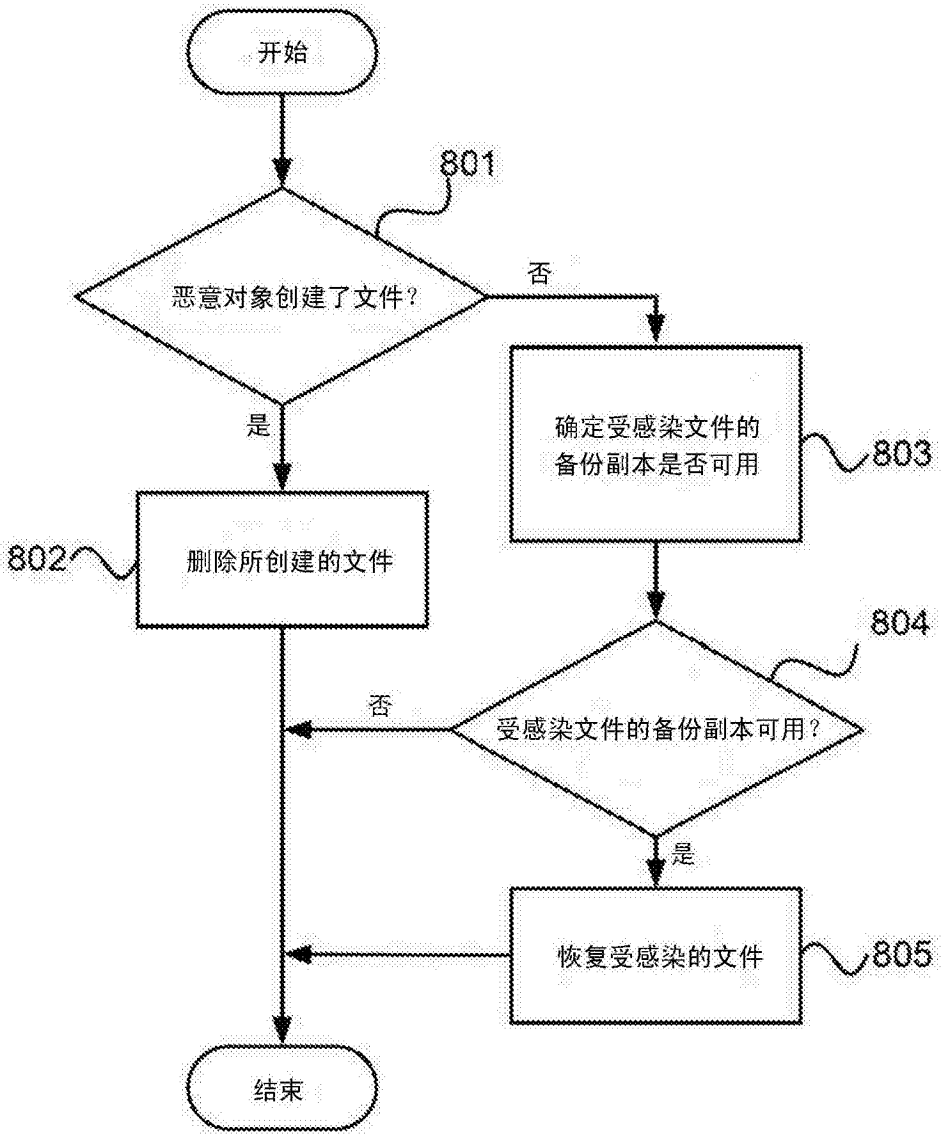

开始
801
恶意对象创建了文件？
否
是
确定受感染文件的
备份副本是否可用
803
802
删除所创建的文件
804
否
受感染文件的备份副本可用？
是
恢复受感染的文件
805
结束

图4E

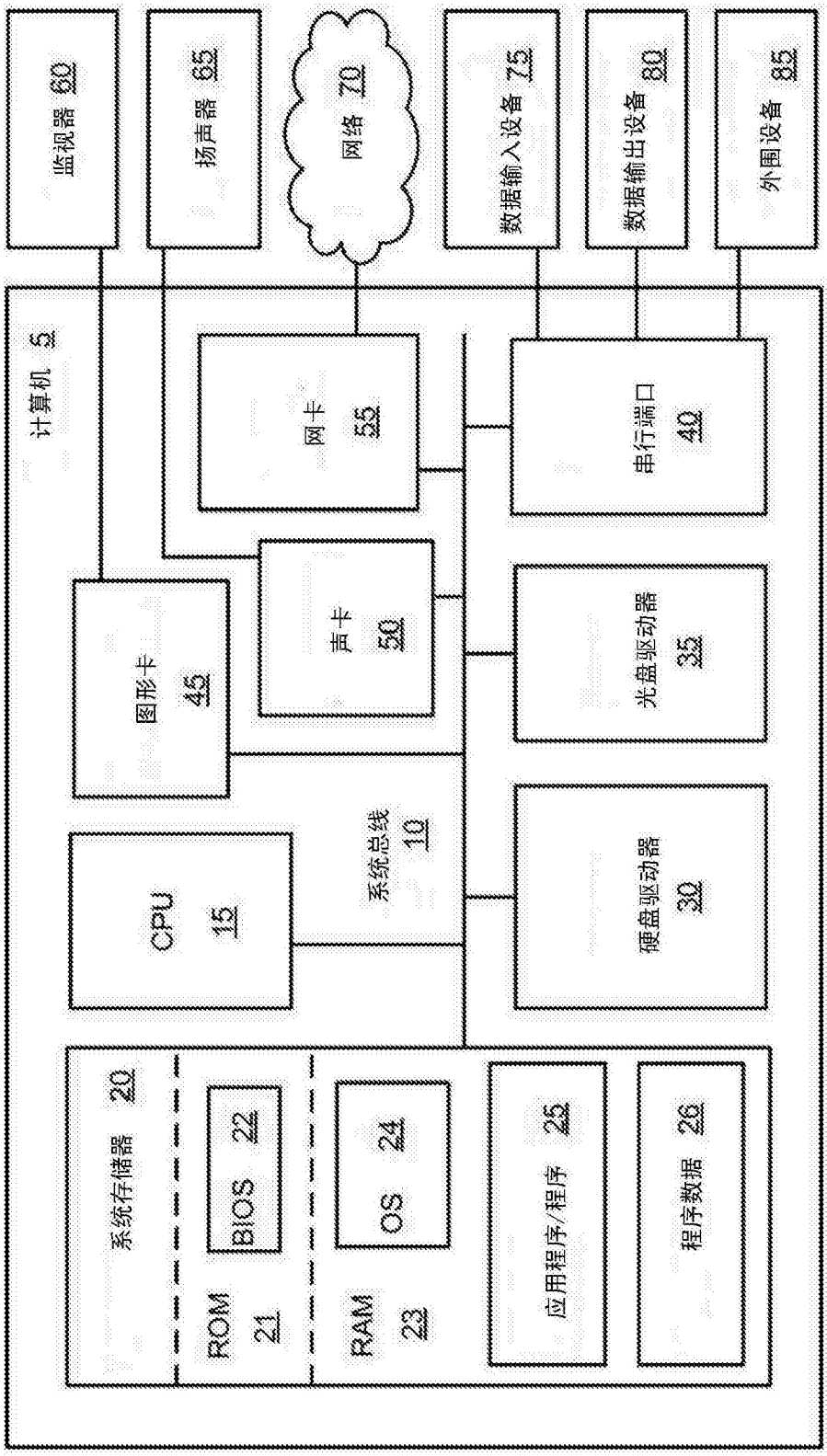

监视器 60
扬声器 65
网络 70
数据输入设备 75
数据输出设备 80
外围设备 85
计算机 5
网卡 55
串行端口 40
图形卡 45
声卡 50
光盘驱动器 35
系统总线 10
CPU 15
硬盘驱动器 30
系统存储器 20
ROM 21
BIOS 22
RAM 23
OS 24
应用程序/程序 25
程序数据 26

图5