(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 105631312 B
(45)授权公告日 2018.09.07

(21)申请号 201510993785.1

(22)申请日 2015.12.25

(65)同一申请的已公布的文献号
申请公布号 CN 105631312 A

(43)申请公布日 2016.06.01

(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 董清 马贞辉

(74)专利代理机构 北京市立方律师事务所 11330
代理人 王增鑫

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

(56)对比文件
CN 104123490 A,2014.10.29,
US 8239947 B1,2012.08.07,
CN 103646209 A,2014.03.19,
CN 104123496 A,2014.10.29,

审查员 陈玲

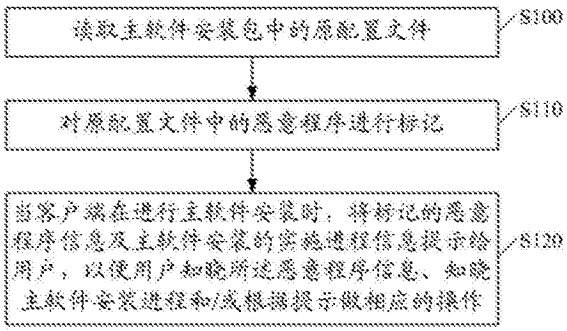
权利要求书4页 说明书18页 附图7页

(54)发明名称

恶意程序的处理方法及系统

(57)摘要

本发明涉及计算机技术领域，尤其涉及一种恶意程序的处理方法及系统。所述的方法包括：读取主软件安装包中的原配置文件；对原配置文件中的恶意程序进行标记；当客户端在进行主软件安装时，将标记的恶意程序信息及主软件安装的实施进程信息提示给用户，以便用户知晓所述恶意程序信息、知晓主软件安装进程和/或根据提示做相应的操作。本方案不仅可实时维护用户所使用终端设备的安全性，并可便于用户实时了解主软件安装进程及恶意程序的拦截进程，且还可便于用户对安装及恶意程序拦截的进程实时干预，以提高用户的参与度，使用户的感觉性更强；同时，用户可根自主求选择主软件安装控制模式，以提高用户软件安装的便捷性及安装控制方式的多样性。



CN 105631312 B

1.一种恶意程序的处理方法，主要用于移动终端，其特征在于，包括以下步骤：

读取主软件安装包中的原配置文件；

对原配置文件中的恶意程序进行标记；

当客户端在进行主软件安装时，将标记的恶意程序信息及主软件安装的实施进程信息提示给用户，以便用户知晓所述恶意程序信息、知晓主软件安装进程和/或根据提示做相应的操作；

在所述当客户端在进行主软件安装时，将标记的恶意程序信息及主软件安装的实施进程信息提示给用户的过程中，包括：

实时检测客户端中进行主软件安装的当前进程；

提示用户选择主软件安装的控制模式；

对用户所选择的主软件安装的控制模式进行识别；

根据用户选择的控制模式，进行相应的安装信息提示及安装进程控制，其中，包括：

当识别到用户选择半自动模式时，将所述标记的恶意程序进行选定，并将该选定信息提示给用户，以便用户对选定信息进行确认和/或调整；

控制禁用下一操作指令的指令按钮，并启动所述指令按钮解禁的倒计时，以便用户在所述指令按钮禁用期间，手动取消选定和/或选定所述标记的恶意程序。

2.如权利要求1所述的方法，其特征在于，在所述对原配置文件中的恶意程序进行标记的步骤之前，还包括：

对原配置文件进行检测，以识别出原配置文件中的恶意程序。

3.如权利要求2所述的方法，其特征在于，所述对原配置文件进行检测，以识别出原配置文件中的恶意程序的步骤中，包括：

将原配置文件的相关信息与预先设置的云端鉴别条件进行匹配，若匹配成功则从原配置文件中将恶意程序的相关信息抓取出来。

4.如权利要求3所述的方法，其特征在于，所述云端鉴别条件中包括多个特定程序匹配条件和满足该特定程序匹配条件后需要检查的特定ELF文件信息。

5.如权利要求4所述的方法，其特征在于，所述将原配置文件的相关信息与预先设置的云端鉴别条件进行匹配的过程中，包括：

将原配置文件的相关信息与所述特定程序匹配条件进行匹配；

获取相匹配的特定程序匹配条件后需要检查的特定ELF文件信息；

将所述特定ELF文件信息作为所述原配置文件的相关信息的ELF文件信息。

6.如权利要求5所述的方法，其特征在于，所述特定程序匹配条件包括以下信息中的至少一种：

文件名称信息、文件大小信息、文件特征值信息、文件图标信息、产品名称信息、内部名称信息、原始文件名信息，以及进程的命令行信息、进程路径信息和父进程路径信息；

所述原配置文件的相关信息包括以下信息中的至少一种：

待执行程序的文件名称信息、文件大小信息、文件特征值信息、文件图标信息、产品名称信息、内部名称信息、原始文件名信息，以及待执行程序创建的进程的命令行信息、进程路径信息和父进程路径信息。

7.如权利要求1所述的方法，其特征在于，还包括：

对所述原配置文件中的恶意程序进行处理。

8.如权利要求7所述的方法，其特征在于，所述对所述原配置文件中的恶意程序进行处理的步骤中，包括：

获取所述恶意程序的数据，从中解析出所述恶意程序待写入的目标路径；

将所述目标路径加入文件防御规则，使用所述文件防御规则在所述恶意程序生成文件时进行文件防御。

9.如权利要求8所述的方法，其特征在于，使用所述文件防御规则在所述恶意程序生成文件时进行文件防御的过程中，包括：

主动防御系统在所述恶意程序生成文件时，获取生成的文件的文件路径；

判断所述生成的文件的文件路径与所述文件防御规则中的目标路径是否匹配；

若匹配，则获取所述生成的文件的文件特征值，对所述生成的文件的文件特征值进行安全性判定；

根据返回结果对所述恶意程序进行相应的文件防御处理。

10.如权利要求1所述方法，其特征在于，所述主软件安装的控制模式包括全自动模式、半自动模式及提示模式。

11.如权利要求1所述的方法，其特征在于，所述根据用户选择的控制模式，进行相应的安装信息提示及安装进程控制的步骤中，包括：

当识别到用户选择全自动模式时，将所述标记的恶意程序进行拦截；

将主软件安装的实时操控指令和/或当前进程信息提示给用户。

12.如权利要求11所述的方法，其特征在于，所述根据用户选择的控制模式，进行相应的安装信息提示及安装进程控制的步骤中，还包括：

根据预设的软件安装方式，实时控制所述主软件的安装进程按照所述预设的软件安装方式进行。

13.如权利要求1所述的方法，其特征在于，所述根据用户选择的控制模式，进行相应的安装信息提示及安装进程控制的步骤中，还包括：

实时识别所述标记的恶意程序的选定情况，以得出最终选定的恶意程序当所述指令按钮解禁后，执行下一操作指令时，将所述最终选定的恶意程序进行拦截。

14.如权利要求1所述的方法，其特征在于，所述根据用户选择的控制模式，进行相应的安装信息提示及安装进程控制的步骤中，包括：

当识别到用户选择提示模式时，实时将标记的恶意程序信息及主软件安装的实施进程信息提示给用户，以便用户选定要拦截的已标记恶意程序和/或选择相应的进程控制的操作指令；

根据用户选定的内容或选择的操作指令，执行对应的操作。

15.如权利要求11～14任一项所述的方法，其特征在于，还包括：

接收用于对用户进行相关提示的文本信息的脚本，并准予所述脚本配置至所述原配置文件中。

16.如权利要求15所述的方法，其特征在于，所述根据用户选择的控制模式，进行相应的安装信息提示及安装进程控制的步骤中，还包括：

根据所述主软件安装的进程，实时调用所述脚本。

17.一种恶意程序的处理系统，主要用于移动终端，其特征在于，包括：

读取模块，用于读取主软件安装包中的原配置文件；

标记模块，用于对原配置文件中的恶意程序进行标记；

提示模块，用于当客户端在进行主软件安装时，将标记的恶意程序信息及主软件安装的实施进程信息提示给用户，以便用户知晓所述恶意程序信息、知晓主软件安装进程和/或根据提示做相应的操作；

所述提示模块包括：

检测子模块，用于实时检测客户端中进行主软件安装的当前进程；

选择提示子模块，用于提示用户选择主软件安装的控制模式；

识别子模块，用于对用户所选择的主软件安装的控制模式进行识别；

操作执行子模块，用于根据用户选择的控制模式，进行相应的安装信息提示及安装进程控制；

所述操作执行子模块包括：

选定提示单元，用于当识别到用户选择半自动模式时，将所述标记的恶意程序进行选定，并将该选定信息提示给用户，以便用户对选定信息进行确认和/或调整；

禁用控制单元，用于控制禁用下一操作指令的指令按钮，并启动所述指令按钮解禁的倒计时，以便用户在所述指令按钮禁用期间，手动取消选定和/或选定所述标记的恶意程序。

18.如权利要求17所述的系统，其特征在于，还包括：

检测模块，用于对原配置文件进行检测，以识别出原配置文件中的恶意程序。

19.如权利要求18所述的系统，其特征在于，所述检测模块包括：

匹配子模块，用于将原配置文件的相关信息与预先设置的云端鉴别条件进行匹配，若匹配成功则从原配置文件中将恶意程序的相关信息抓取出来。

20.如权利要求19所述的系统，其特征在于，所述云端鉴别条件中包括多个特定程序匹配条件和满足该特定程序匹配条件后需要检查的特定ELF文件信息。

21.如权利要求20所述的系统，其特征在于，所述匹配子模块包括：

匹配单元，用于将原配置文件的相关信息与所述特定程序匹配条件进行匹配；

获取单元，用于获取相匹配的特定程序匹配条件后需要检查的特定ELF文件信息；

作为单元，用于将所述特定ELF文件信息作为所述原配置文件的相关信息的ELF文件信息。

22.如权利要求21所述的系统，其特征在于，所述特定程序匹配条件包括以下信息中的至少一种：

文件名称信息、文件大小信息、文件特征值信息、文件图标信息、产品名称信息、内部名称信息、原始文件名信息，以及进程的命令行信息、进程路径信息和父进程路径信息；

所述原配置文件的相关信息包括以下信息中的至少一种：

待执行程序的文件名称信息、文件大小信息、文件特征值信息、文件图标信息、产品名称信息、内部名称信息、原始文件名信息，以及待执行程序创建的进程的命令行信息、进程路径信息和父进程路径信息。

23.如权利要求17所述的系统，其特征在于，还包括：

处理模块，用于对所述原配置文件中的恶意程序进行处理。

24.如权利要求23所述的系统，其特征在于，所述处理模块包括：

解析子模块，用于获取所述恶意程序的数据，从中解析出所述恶意程序待写入的目标路径；

防御子模块，用于将所述目标路径加入文件防御规则，使用所述文件防御规则在所述恶意程序生成文件时进行文件防御。

25.如权利要求24所述的系统，其特征在于，所述防御子模块包括：

生成获取单元，用于主动防御系统在所述恶意程序生成文件时，获取生成的文件的文件路径；

匹配判断单元，用于判断所述生成的文件的文件路径与所述文件防御规则中的目标路径是否匹配；

若匹配，则获取所述生成的文件的文件特征值，对所述生成的文件的文件特征值进行安全性判定；

防御处理单元，用于根据返回结果对所述恶意程序进行相应的文件防御处理。

26.如权利要求17所述系统，其特征在于，所述主软件安装的控制模式包括全自动模式、半自动模式及提示模式。

27.如权利要求17所述的系统，其特征在于，所述操作执行子模块包括：

第一拦截单元，用于当识别到用户选择全自动模式时，将所述标记的恶意程序进行拦截；

第一提示单元，用于将主软件安装的实时操控指令和/或当前进程信息提示给用户。

28.如权利要求27所述的系统，其特征在于，所述操作执行子模块还包括：

控制单元，用于根据预设的软件安装方式，实时控制所述主软件的安装进程按照所述预设的软件安装方式进行。

29.如权利要求17所述的系统，其特征在于，所述操作执行子模块还包括：

选定识别单元，用于实时识别所述标记的恶意程序的选定情况，以得出最终选定的恶意程序

第二拦截单元，用于当所述指令按钮解禁后，执行下一操作指令时，将所述最终选定的恶意程序进行拦截。

30.如权利要求17所述的系统，其特征在于，所述操作执行子模块包括：

第二提示单元，用于当识别到用户选择提示模式时，实时将标记的恶意程序信息及主软件安装的实施进程信息提示给用户，以便用户选定要拦截的已标记恶意程序和/或选择相应的进程控制的操作指令；

指令执行单元，用于根据用户选定的内容或选择的操作指令，执行对应的操作。

31.如权利要求26～30任一项所述的系统，其特征在于，还包括：

接收模块，用于接收用于对用户进行相关提示的文本信息的脚本，并准予所述脚本配置至所述原配置文件中。

32.如权利要求31所述的系统，其特征在于，所述操作执行子模块还包括：

调用单元，用于根据所述主软件安装的进程，实时调用所述脚本。

恶意程序的处理方法及系统

【技术领域】

[0001] 本发明涉及计算机技术领域，尤其涉及一种恶意程序的处理方法及系统。

【背景技术】

[0002] 恶意程序是一个概括性的术语，指任何故意创建用来执行未经授权并通常是有害行为的软件程序。计算机病毒、后门程序、键盘记录器、密码盗取者、Word和Excel宏病毒、引导区病毒、脚本病毒、木马、犯罪软件、间谍软件和广告软件等等，都可以称之为恶意程序。

[0003] 现今，以捆绑方式推广恶意程序已成为一种潮流，所捆绑的软件几乎涉及了电脑日常使用的方方面面。对于广大的普通用户来说，在安装过程中通常并不会去仔细阅读理解被勾选选项的内容，用户通过默认直接点击安装软件的情况下，被恶意程序在用户不知情的情况下即安装在了其电脑上；这样，待用户软件安装完成后，除了该款需要的软件外，还多了一些其他的捆绑安装的软件，这些捆绑的软件是用户并不需要、不想安装的。

[0004] 对于此类恶意程序，当用户试图进行卸载时，势必会浪费用户的时间和精力；而若用户置之不管时，用户的计算机由于安装了不必要的恶意程序，日积月累，恶意程序的数量越来越多，会占用大量的资源，进而影响用户电脑系统的性能，开机、运行等效率降低，甚至影响用户的正常使用；更严重的，有些恶意程序可能会导致用户在不知情的情况下误安装一些恶意软件，或者是广告骚扰程序等，进而不仅仅影响用户电脑的系统性能，影响用户上网及使用软件时的体验，还可能威胁到用户的电脑安全。

[0005] 目前，也有一些针对恶意程序的一些拦截方法，但现有的方法是启动拦截后，是拦截程序自身在运行，用户无法知晓其中的拦截进程，更无法进行拦截干预，用户的参与感及感觉性较弱。

【发明内容】

[0006] 本发明的目的旨在解决上述至少一个问题，提供了一种恶意程序的处理方法及系统。

[0007] 为实现该目的，本发明采用如下技术方案：

[0008] 本发明提供了一种恶意程序的处理方法，主要用于移动终端，其包括以下步骤：

[0009] 读取主软件安装包中的原配置文件；

[0010] 对原配置文件中的恶意程序进行标记；

[0011] 当客户端在进行主软件安装时，将标记的恶意程序信息及主软件安装的实施进程信息提示给用户，以便用户知晓所述恶意程序信息、知晓主软件安装进程和/或根据提示做相应的操作。

[0012] 进一步的，本发明所述的方法，还包括：

[0013] 对原配置文件进行检测，以识别出原配置文件中的恶意程序。

[0014] 具体的，所述对原配置文件进行检测，以识别出原配置文件中的恶意程序的步骤中，包括：

[0015] 将原配置文件的相关信息与预先设置的云端鉴别条件进行匹配，若匹配成功则从原配置文件中将恶意程序的相关信息抓取出来。

[0016] 具体的，所述云端鉴别条件中包括多个特定程序匹配条件和满足该特定程序匹配条件后需要检查的特定ELF(Executable and Linkable Format;可执行连接格式)文件信息。

[0017] 具体的，所述将原配置文件的相关信息与预先设置的云端鉴别条件进行匹配的过程中，包括：

[0018] 将原配置文件的相关信息与所述特定程序匹配条件进行匹配；

[0019] 获取相匹配的特定程序匹配条件后需要检查的特定ELF文件信息；

[0020] 将所述特定ELF文件信息作为所述原配置文件的相关信息的ELF文件信息。

[0021] 具体的，所述特定程序匹配条件包括以下信息中的至少一种：

[0022] 文件名称信息、文件大小信息、文件特征值信息、文件图标信息、产品名称信息、内部名称信息、原始文件名信息，以及进程的命令行信息、进程路径信息和父进程路径信息；

[0023] 所述原配置文件的相关信息包括以下信息中的至少一种：

[0024] 待执行程序的文件名称信息、文件大小信息、文件特征值信息、文件图标信息、产品名称信息、内部名称信息、原始文件名信息，以及待执行程序创建的进程的命令行信息、进程路径信息和父进程路径信息。

[0025] 进一步的，本发明所述的方法，还包括：

[0026] 对所述原配置文件中的恶意程序进行处理。

[0027] 具体的，所述对所述原配置文件中的恶意程序进行处理的步骤中，包括：

[0028] 获取所述恶意程序的数据，从中解析出所述恶意程序待写入的目标路径；

[0029] 将所述目标路径加入文件防御规则，使用所述文件防御规则在所述恶意程序生成文件时进行文件防御。

[0030] 具体的，使用所述文件防御规则在所述恶意程序生成文件时进行文件防御的过程中，包括：

[0031] 主动防御系统在所述恶意程序生成文件时，获取生成的文件的文件路径；

[0032] 判断所述生成的文件的文件路径与所述文件防御规则中的目标路径是否匹配；

[0033] 若匹配，则获取所述生成的文件的文件特征值，对所述生成的文件的文件特征值进行安全性判定；

[0034] 根据返回结果对所述恶意程序进行相应的文件防御处理。

[0035] 具体的，在所述当客户端在进行主软件安装时，将标记的恶意程序信息及主软件安装的实施进程信息提示给用户的过程中，包括：

[0036] 实时检测客户端中进行主软件安装的当前进程。

[0037] 具体的，在所述当客户端在进行主软件安装时，将标记的恶意程序信息及主软件安装的实施进程信息提示给用户的过程中，还包括：

[0038] 提示用户选择主软件安装的控制模式；

[0039] 根据用户选择的控制模式，进行相应的安装信息提示及安装进程控制。

[0040] 具体的，所述主软件安装的控制模式包括全自动模式、半自动模式及提示模式。

[0041] 进一步的，在所述提示用户选择主软件安装的控制模式的步骤之后，还包括：

[0042] 对用户所选择的主软件安装的控制模式进行识别。

[0043] 依据本发明的一个实施例所揭示，所述根据用户选择的控制模式，进行相应的安装信息提示及安装进程控制的步骤中，包括：

[0044] 当识别到用户选择全自动模式时，将所述标记的恶意程序进行拦截；

[0045] 将主软件安装的实时操控指令和/或当前进程信息提示给用户。

[0046] 进一步的，所述根据用户选择的控制模式，进行相应的安装信息提示及安装进程控制的步骤中，还包括：

[0047] 根据预设的软件安装方式，实时控制所述主软件的安装进程按照所述预设的软件安装方式进行。

[0048] 依据本发明的又一个实施例所揭示，所述根据用户选择的控制模式，进行相应的安装信息提示及安装进程控制的步骤中，包括：

[0049] 当识别到用户选择半自动模式时，将所述标记的恶意程序进行选定，并将该选定信息提示给用户，以便用户对选定信息进行确认和/或调整；

[0050] 控制禁用下一操作指令的指令按钮，并启动所述指令按钮解禁的倒计时，以便用户在所述指令按钮禁用期间，手动取消选定和/或选定所述标记的恶意程序。

[0051] 进一步的，所述根据用户选择的控制模式，进行相应的安装信息提示及安装进程控制的步骤中，还包括：

[0052] 实时识别所述标记的恶意程序的选定情况，以得出最终选定的恶意程序

[0053] 当所述指令按钮解禁后，执行下一操作指令时，将所述最终选定的恶意程序进行拦截。

[0054] 依据本发明的又一个实施例所揭示，所述根据用户选择的控制模式，进行相应的安装信息提示及安装进程控制的步骤中，包括：

[0055] 当识别到用户选择提示模式时，实时将标记的恶意程序信息及主软件安装的实施进程信息提示给用户，以便用户选定要拦截的已标记恶意程序和/或选择相应的进程控制的操作指令；

[0056] 根据用户选定的内容或选择的操作指令，执行对应的操作。

[0057] 进一步的，本发明所述的方法，还包括：

[0058] 接收用于对用户进行相关提示的文本信息的脚本，并准予所述脚本配置至所述原配置文件中。

[0059] 进一步的，所述根据用户选择的控制模式，进行相应的安装信息提示及安装进程控制的步骤中，还包括：

[0060] 根据所述主软件安装的进程，实时调用所述脚本。

[0061] 相应的，本发明还提供了一种恶意程序的处理系统，主要用于移动终端，其包括：

[0062] 读取模块，用于读取主软件安装包中的原配置文件；

[0063] 标记模块，用于对原配置文件中的恶意程序进行标记；

[0064] 提示模块，用于当客户端在进行主软件安装时，将标记的恶意程序信息及主软件安装的实施进程信息提示给用户，以便用户知晓所述恶意程序信息、知晓主软件安装进程和/或根据提示做相应的操作。

[0065] 进一步的，本发明所述的系统，还包括：

[0066] 检测模块，用于对原配置文件进行检测，以识别出原配置文件中的恶意程序。

[0067] 具体的，所述检测模块包括：

[0068] 匹配子模块，用于将原配置文件的相关信息与预先设置的云端鉴别条件进行匹配，若匹配成功则从原配置文件中将恶意程序的相关信息抓取出来。

[0069] 具体的，所述云端鉴别条件中包括多个特定程序匹配条件和满足该特定程序匹配条件后需要检查的特定ELF文件信息。

[0070] 具体的，所述匹配子模块包括：

[0071] 匹配单元，用于将原配置文件的相关信息与所述特定程序匹配条件进行匹配；

[0072] 获取单元，用于获取相匹配的特定程序匹配条件后需要检查的特定ELF文件信息；

[0073] 作为单元，用于将所述特定ELF文件信息作为所述原配置文件的相关信息的ELF文件信息。

[0074] 具体的，所述特定程序匹配条件包括以下信息中的至少一种：

[0075] 文件名称信息、文件大小信息、文件特征值信息、文件图标信息、产品名称信息、内部名称信息、原始文件名信息，以及进程的命令行信息、进程路径信息和父进程路径信息；

[0076] 所述原配置文件的相关信息包括以下信息中的至少一种：

[0077] 待执行程序的文件名称信息、文件大小信息、文件特征值信息、文件图标信息、产品名称信息、内部名称信息、原始文件名信息，以及待执行程序创建的进程的命令行信息、进程路径信息和父进程路径信息。

[0078] 进一步的，本发明所述的系统，还包括：

[0079] 处理模块，用于对所述原配置文件中的恶意程序进行处理。

[0080] 具体的，所述处理模块包括：

[0081] 解析子模块，用于获取所述恶意程序的数据，从中解析出所述恶意程序待写入的目标路径；

[0082] 防御子模块，用于将所述目标路径加入文件防御规则，使用所述文件防御规则在所述恶意程序生成文件时进行文件防御。

[0083] 具体的，所述防御子模块包括：

[0084] 生成获取单元，用于主动防御系统在所述恶意程序生成文件时，获取生成的文件的文件路径；

[0085] 匹配判断单元，用于判断所述生成的文件的文件路径与所述文件防御规则中的目标路径是否匹配；

[0086] 若匹配，则获取所述生成的文件的文件特征值，对所述生成的文件的文件特征值进行安全性判定；

[0087] 防御处理单元，用于根据返回结果对所述恶意程序进行相应的文件防御处理。

[0088] 具体的，所述提示模块包括：

[0089] 检测子模块，用于实时检测客户端中进行主软件安装的当前进程。

[0090] 具体的，所述提示模块还包括：

[0091] 选择提示子模块，用于提示用户选择主软件安装的控制模式；

[0092] 操作执行子模块，用于根据用户选择的控制模式，进行相应的安装信息提示及安装进程控制。

[0093] 具体的，所述主软件安装的控制模式包括全自动模式、半自动模式及提示模式。

[0094] 进一步的，所述提示模块还包括：

[0095] 识别子模块，用于对用户所选择的主软件安装的控制模式进行识别。

[0096] 依据本发明的一个实施例所揭示，所述操作执行子模块包括：

[0097] 第一拦截单元，用于当识别到用户选择全自动模式时，将所述标记的恶意程序进行拦截；

[0098] 第一提示单元，用于将主软件安装的实时操控指令和/或当前进程信息提示给用户。

[0099] 进一步的，所述操作执行子模块还包括：

[0100] 控制单元，用于根据预设的软件安装方式，实时控制所述主软件的安装进程按照所述预设的软件安装方式进行。

[0101] 依据本发明的又一个实施例所揭示，所述操作执行子模块包括：

[0102] 选定提示单元，用于当识别到用户选择半自动模式时，将所述标记的恶意程序进行选定，并将该选定信息提示给用户，以便用户对选定信息进行确认和/或调整；

[0103] 禁用控制单元，用于控制禁用下一操作指令的指令按钮，并启动所述指令按钮解禁的倒计时，以便用户在所述指令按钮禁用期间，手动取消选定和/或选定所述标记的恶意程序。

[0104] 进一步的，所述操作执行子模块还包括：

[0105] 选定识别单元，用于实时识别所述标记的恶意程序的选定情况，以得出最终选定的恶意程序

[0106] 第二拦截单元，用于当所述指令按钮解禁后，执行下一操作指令时，将所述最终选定的恶意程序进行拦截。

[0107] 依据本发明的又一个实施例所揭示，所述操作执行子模块包括：

[0108] 第二提示单元，用于当识别到用户选择提示模式时，实时将标记的恶意程序信息及主软件安装的实施进程信息提示给用户，以便用户选定要拦截的已标记恶意程序和/或选择相应的进程控制的操作指令；

[0109] 指令执行单元，用于根据用户选定的内容或选择的操作指令，执行对应的操作。

[0110] 进一步的，本发明所述的方法，还包括：

[0111] 接收模块，用于接收用于对用户进行相关提示的文本信息的脚本，并准予所述脚本配置至所述原配置文件中。

[0112] 进一步的，所述操作执行子模块还包括：

[0113] 调用单元，用于根据所述主软件安装的进程，实时调用所述脚本。

[0114] 与现有技术相比，本发明具备如下优点：

[0115] 本发明不仅可通过上述方案检测出原配置文件中的恶意程序，并对所述恶意程序进行防御处理，以维护用户所使用的终端设备的安全性，且本发明可对原配置文件中的恶意程序进行标记，然后当客户端在进行主软件安装时，将标记的恶意程序信息及主软件安装的实施进程信息提示给用户，以便用户知晓所述恶意程序信息、知晓主软件安装进程和/或根据提示做相应的操作，该过程可使用户实时知晓主软件的安装进程及拦截进程，且用户还可根据需要参与拦截进程中，以提高用户的参与感，使用户的感觉性更强。

[0116] 另外，用户可根据需求选择全自动模式、半自动模式或提示模式的所述主软件安装控制模式，无论用户选择前述何种控制模式，皆可使用户实时了解主软件安装进程及恶意程序的拦截进程。其中，当识别到用户选择全自动模式时，服务器会将所述标记的恶意程序进行拦截，并将主软件安装的实时操纵指令和/或当前进程信息提示给用户，以便用户实时了解主软件安装进程及恶意程序的拦截进程；当识别到用户选择半自动模式时，服务器将所述标记的恶意程序进行选定，并将该选定信息提示给用户，以便用户对选定信息进行确认和/或调整，同时控制禁用下一操作指令的指令按钮，并启动所述指令按钮解禁的倒计时，以便用户在所述指令按钮禁用期间，手动取消选定和/或选定所述标记的恶意程序，该过程不仅可提高用户对恶意程序的注意度，使用户实时了解主软件安装进程及恶意程序的拦截进程，还可便于用户对安装进程及恶意程序的拦截进程实时干预，提高用户的参与度，使用户的感觉性更强。

[0117] 因此，本发明不仅可实时维护用户所使用终端设备的安全性，且还可便于用户实时了解主软件安装进程及恶意程序的拦截进程，并可便于用户对安装进程及恶意程序的拦截进程实时干预，以提高用户的参与度，使用户的感觉性更强；同时，用户可根据自身需求选择主软件安装控制模式，其无论用户选择前述何种控制模式，皆可使用户实时了解主软件安装进程及恶意程序的拦截进程，在确保拦截用户无需安装的恶意程序的同时，还可提高用户软件安装的便捷性及安装控制方式的多样性。

【附图说明】

[0118] 图1为本发明中恶意程序的处理方法的一个实施例的程序流程图；

[0119] 图2为本发明中恶意程序的处理方法的一个实施例的程序流程图；

[0120] 图3为本发明中恶意程序的处理方法的一个实施例的程序流程图；

[0121] 图4为本发明中恶意程序的处理方法的一个实施例的程序流程图；

[0122] 图5为本发明中恶意程序的处理方法的一个实施例的程序流程图；

[0123] 图6为本发明中恶意程序的处理方法的一个实施例的程序流程图；

[0124] 图7为本发明中所述云端鉴别条件的示意图；

[0125] 图8为本发明中恶意程序的处理系统的一个实施例的结构框图；

[0126] 图9为本发明中恶意程序的处理系统中提示模块的一个实施例的结构框图；

[0127] 图10为本发明中恶意程序的处理系统中操作执行子模块的一个实施例的结构框图；

[0128] 图11为本发明中恶意程序的处理系统中操作执行子模块的一个实施例的结构框图；

[0129] 图12为本发明中恶意程序的处理系统的一个实施例的结构框图；

[0130] 图13为本发明中恶意程序的处理系统的一个实施例的结构框图。

【具体实施方式】

[0131] 下面结合附图和示例性实施例对本发明作进一步地描述，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，仅用于解释本发明，而不能解释为对

本发明的限制。此外，如果已知技术的详细描述对于示出本发明的特征是不必要的，则将其省略。

[0132] 本技术领域技术人员可以理解，除非特意声明，这里使用的单数形式“一”、“一个”、“所述”和“该”也可包括复数形式。应该进一步理解的是，本发明的说明书中使用的措辞“包括”是指存在所述特征、整数、步骤、操作、元件和/或组件，但是并不排除存在或添加一个或多个其他特征、整数、步骤、操作、元件、组件和/或它们的组。应该理解，当我们称元件被“连接”或“耦接”到另一元件时，它可以直接连接或耦接到其他元件，或者也可以存在中间元件。此外，这里使用的“连接”或“耦接”可以包括无线连接或无线耦接。这里使用的措辞“和/或”包括一个或更多个相关联的列出项的全部或任一单元和全部组合。

[0133] 本技术领域技术人员可以理解，除非另外定义，这里使用的所有术语(包括技术术语和科学术语)，具有与本发明所属领域中的普通技术人员的一般理解相同的意义。还应该理解的是，诸如通用字典中定义的那些术语，应该被理解为具有与现有技术的上下文中的意义一致的意义，并且除非像这里一样被特定定义，否则不会用理想化或过于正式的含义来解释。

[0134] 本技术领域技术人员可以理解，这里所使用的“终端”、“终端设备”既包括无线信号接收器的设备，其仅具备无发射能力的无线信号接收器的设备，又包括接收和发射硬件的设备，其具有能够在双向通信链路上，执行双向通信的接收和发射硬件的设备。这种设备可以包括：蜂窝或其他通信设备，其具有单线路显示器或多线路显示器或没有多线路显示器的蜂窝或其他通信设备；PCS(Personal Communications Service，个人通信系统)，其可以组合语音、数据处理、传真和/或数据通信能力；PDA(Personal Digital Assistant，个人数字助理)，其可以包括射频接收器、寻呼机、互联网/内联网访问、网络浏览器、记事本、日历和/或GPS(Global Positioning System，全球定位系统)接收器；常规膝上型和/或掌上型计算机或其他设备，其具有和/或包括射频接收器的常规膝上型和/或掌上型计算机或其他设备。这里所使用的“终端”、“终端设备”可以是便携式、可运输、安装在交通工具(航空、海运和/或陆地)中的，或者适合于和/或配置为在本地运行，和/或以分布形式，运行在地球和/或空间的任何其他位置运行。这里所使用的“终端”、“终端设备”还可以是通信终端、上网终端、音乐/视频播放终端，例如可以是PDA、MID(Mobile Internet Device，移动互联网设备)和/或具有音乐/视频播放功能的移动电话，也可以是智能电视、机顶盒等设备。

[0135] 本技术领域技术人员可以理解，这里所使用的服务器、云端、远端网络设备等概念，具有等同效果，其包括但不限于计算机、网络主机、单个网络服务器、多个网络服务器集或多个服务器构成的云。在此，云由基于云计算(Cloud Computing)的大量计算机或网络服务器构成，其中，云计算是分布式计算的一种，由一群松散耦合的计算机集组成的一个超级虚拟计算机。本发明的实施例中，远端网络设备、终端设备与WNS服务器之间可通过任何通信方式实现通信，包括但不限于，基于3GPP、LTE、WIMAX的移动通信、基于TCP/IP、UDP协议的计算机网络通信以及基于蓝牙、红外传输标准的近距无线传输方式。

[0136] 有必要先对本发明的应用场景及其原理进行如下的先导性说明。

[0137] 互联网中，一般包括用户端(用户移动终端)、网络和服务器(如网站的Web服务器等)。其中用户端可以是用户的互联网移动终端，如台式机(PC)、膝上型计算机(Laptop)，带有网页浏览功能的智能型设备，如个人数字助理(Personal Digital Assisstant，PDA)，以

及移动互联网设备(Mobile Internet Device,MID)和智能手机(Phone)等。这些移动终端都可以在互联网环境中,典型的如英特网环境中,请求由另一进程(如服务器提供的进程)提供某项服务。

[0138] 服务器通常是可通过互联网等通信媒介,典型的如英特网访问的远程计算机系统。而且,服务器通常可以为来自互联网的多个用户端提供服务。提供服务过程包括接收用户端发来的请求,收集用户端情报和反馈信息等。实质上,服务器充当计算机网络的信息提供者这一角色。服务器通常位于提供服务的一方,或由服务提供方配置以服务内容,这样的服务提供方可以如互联网服务公司的网站等。

[0139] 本发明的有关方法和终端的应用场景,是以适合于信息、数据查找、进程监控、数据处理及数据存储的服务器为下文中的拦截程序服务器,例如杀毒软件、拦截软件等。需要说明的是,该描述仅是示例性的,本发明的范围并不限于此。

[0140] 以下将详细说明为了运用上述的原理实现上述的场景而提出的本发明的若干技术方案的具体实施方式。需要说明的是,本发明提供了一种恶意程序的处理方法,即从移动终端的视角来描述该方法,可以通过编程将恶意程序的处理方法实现为计算机程序在远端网络设备上实现,其包括但不限于计算机、智能手机、智能移动终端、网络主机、单个网络服务器、多个网络服务器集或多个服务器构成的云。

[0141] 请参见附图1,本发明一种恶意程序的处理方法的一个典型实施例,其包括以下步骤:

[0142] S100,读取主软件安装包中的原配置文件。

[0143] 具体的,当主软件安装包下载完成,准备安装时,拦截程序服务器即会对该主软件安装包中的原配置文件进行读取检测。

[0144] 需要说明的是,以Android为例,所述读取的特征信息包括:

[0145] 1)Android安装包包名:packageName;

[0146] 2)Android安装包版本号:versionCode;

[0147] 3)Android安装包的数字签名的MD5(Message-Digest Algorithm 5,信息-摘要算法):signature[0];

[0148] 4)Android组件receiver;

[0149] 5)classes.dex中的指令;

[0150] 6)ELF文件中的字符串;

[0151] 7)assets,res,lib等目录下各文件的MD5;

[0152] 8)Android组件service,activity等。

[0153] S110,对原配置文件中的恶意程序进行标记。

[0154] 具体的,首先根据云端鉴别条件库,对原配置文件中的恶意程序进行精确匹配抓取,其精确匹配抓取方式包括如下过程:将原配置文件中的安装进程的描述信息与云端鉴别条件库中保存的黑名单进行匹配比对,若匹配成功,则对该安装进程文件标记为恶意程序。所述描述信息,包括以下一种或多种的组合:版本号、安装文件的发布公司名称、产品名称、内部名称、签名者、签名日期、安装文件大小、安装范围、安装文件的时间戳、安装命令行信息。

[0155] 其中,所述云端鉴别条件库保存的对应执行拦截策略的行为的描述信息,包括以

下一种或多种的组合：由默认拦截的进程执行的与所述默认拦截的进程无关的文件创建操作的描述信息、由默认拦截的进程执行的与所述默认拦截的进程无关的文件写入操作的描述信息、由默认拦截的进程执行的与所述默认的进程无关的安装操作的描述信息。

[0156] 所述云端鉴别条件库中保存的对应执行拦截策略的安装进程的描述信息，包括以下一种或者多种的组合：由默认拦截的进程启动且与所述默认拦截的进程无关的安装进程的描述信息、已执行拦截的安装进程的描述信息、预先收集的默认拦截的安装进程的描述信息、预先收集的默认拦截的下载进程访问的网络地址。

[0157] S120，当客户端在进行主软件安装时，将标记的恶意程序信息及主软件安装的实施进程信息提示给用户，以便用户知晓所述恶意程序信息、知晓主软件安装进程和/或根据提示做相应的操作。

[0158] 需要说明的是，由于对于一些恶意程序，其还具有修改配置文件，将自身置为自启动程序的行为，因此，本发明还可以通过注入和java hook等手段，实时监听各个软件的启动行为，并能够分析出导致该软件被唤醒的组件。在判定是否为软件的自启行为时，会遵循以下规则：(1)可视化组件(activity组件)引发的启动行为不能被拦截，因为这种行为多由用户触发，并非软件自启；(2)针对broadcast组件，则分两种情况处理。如果包含该broadcast组件的软件已经处于运行状态，则认为当前的启动行为并非自启，不需要被拦截，这种情况一般发生在多进程Android软件中。反之，则认为是自启；(3)针对service组件的判别方式与broadcast组件类似，但是service组件的重要性一般要高于broadcast组件，不恰当的拦截极有可能导致某些软件运行异常，为了避免这种情况，当service组件引发的自启行为被拦截时，我们会给予提示，引导用户完成预期的操作；(4)对于provider组件引发的启动行为，一般不拦截。通过对这些规则的应用，可以较准确的判定软件的自启行为，同时又不对用户的正常使用造成困扰。

[0159] 具体的，请参见附图2，在所述当客户端在进行主软件安装时，将标记的恶意程序信息及主软件安装的实施进程信息提示给用户的过程中，包括：

[0160] S200，实时检测客户端中进行主软件安装的当前进程。

[0161] 具体地，提取文件的特征值可采用多种方法，例如匹配ELF(Executable and Linking Format，可执行链接文件)文件中可执行代码的机器指令，具体在提取文件的特征值时，可以只提取文件中一段指定长度的数据(可执行代码的指令或者是其中一部分)。

[0162] 例如，可以采用如下方式提取文件的特征值：

[0163] 以Android操作系统为例，大部分Android应用都主要是由Java语言编写，编译之后生成了Dalvik虚拟机的字节码(byte code)，打包成了classes.dex文件。解析classes.dex文件，反编译其字节码，就可以得到应用程序所要执行的指令。

[0164] 可以挑选指令中能代表恶意软件特征的指令作为特征码，当发现classes.dex文件中包含这样的特征码时，就作为一个特征。例如，Android.Geinimi木马为了隐藏自己，将一些关键数据(如木马服务器信息)加密之后写入代码中，这些被加密的数据反而成为了检测识别它的特征。用dexdump工具分析classes.dex文件可看到输出中包含以下片段：

[0165] 00d00c:0003 0100 1000 0000 5535 0234 8664...|02d4:array-data(12 units)

[0166] 00d024:0003 0100 1000 0000 1bea c301 eadf...|02e0:array-data(12

units)

[0167] 上述片段就可以提取作为检测识别的特征。

[0168] 当然，dexdump工具只是显示这些特征数据的手段之一，也可以通过其他方式自行实现解析、反编译和识别classes.dex文件的功能。

[0169] 综上所述，样本一不包含ELF文件，所以没有提取到ELF特征。

[0170] 从样本一中提取了上述特征之后，假设安全识别库中存在以下特征记录：

[0171] 特征一：packageName＝com.wbs

[0172] 特征二：无

[0173] 特征三：MD5(signature[0])＝294f08ae04307a649322524713318543

[0174] 特征一+特征三：安全级别为“木马”

[0175] 当检测流程走到“找到包含特征一、特征三的木马”时，找到记录，返回结果为“木马”。

[0176] S210，提示用户选择主软件安装的控制模式。

[0177] 具体的，所述主软件安装的控制模式包括全自动模式、半自动模式及提示模式。

[0178] S220，对用户所选择的主软件安装的控制模式进行识别。

[0179] 具体的，根据用户触发相应的标识指令按钮来识别，并将识别结果反馈至下一级进程控制端，以便下一级进程控制端根据标识指令按钮预设的执行。

[0180] S230，根据用户选择的控制模式，进行相应的安装信息提示及安装进程控制。

[0181] 具体的，所述安装信息提示包括安装进程信息提示及恶意程序的拦截信息提示；所述安装进程控制包括主软件安装进程控制及恶意程序的拦截进程控制。

[0182] 请参见附图3，在本发明的一个实施例中，当识别到用户选择全自动模式时，所述根据用户选择的控制模式，进行相应的安装信息提示及安装进程控制的过程中，包括：

[0183] S300，将所述标记的恶意程序进行拦截。

[0184] 具体的，该过程是拦截程序服务器直接将标记的恶意程序进行选定执行拦截的。

[0185] 需要说明的是，所述将所述标记的恶意程序进行拦截的过程是通过免疫的方式对恶意程序进行查杀，其中，包括：向移动终端发送用于注入到移动终端的指定程序中的查杀代码；同时，指定程序为具有比恶意程序更高的启动优先级；查杀代码用于在指定程序启动时被加载，并关闭恶意程序的进程。

[0186] S310，根据预设的软件安装方式，实时控制所述主软件的安装进程按照所述预设的软件安装方式进行。

[0187] S320，将主软件安装的实时操控指令和/或当前进程信息提示给用户。

[0188] 具体的，所述主软件安装的实时操控指令和/或当前进程信息都是按预设的软件安装方式执行的；所述进程信息提示是随主软件安装的实时进程而实时触发提示给用户的，在进程信息提示的过程中，需根据所述主软件安装的进程，实时调用预设的用于进程信息提示的脚本。例如，所述当前进程信息可为“正在选定恶意程序”、“正在拦截恶意程序”等。其中，该步骤过程是模拟用户手机点击按钮的操作，以Android(安卓)为例，具体的实现方式是Android提供一个名为“辅助功能”的设置，开启之后，可以获得移动终端的屏幕上所有界面的一些基本信息，比如哪个App(应用)切换到桌面、用户触摸屏幕的坐标等等，并且运行程序模拟用户的一些操作，这里模拟的是用户点击某个按钮的操作，模拟用户点击和

用户真实点击的效果是一致的。由于本发明实施例可以在急救箱产品中实现，因而做这些操作的只是急救箱里的一个服务，只要用户开启，这个服务就会在后台一致运行，接收到移动终端界面变化的一些基本信息，如果出现指定的界面变化，比如出现卸载恶意程序的对话框，则找到对话框中的卸载按钮，模拟一次用户点击事件；又如出现禁用恶意程序的设置界面，则找到设置界面中的禁用按钮，模拟一次用户点击。

[0189] 此外，在本发明的另一实施例中，由于在Android系统中，一个App是没法监听到其他App的激活设备管理器事件的，因而当前急救箱的机制是急救箱的进程遍历Android系统中所有安装的App(随后用杀毒引擎进行扫描，如果发现某个App是病毒或恶意程序，就对该App调用系统的一个隐藏接口，即DevicePolicyManager的packageHasActiveAdmins方法来判断这个App是否激活了设备管理器，如果激活了，就取消激活，然后卸载或禁用该App。

[0190] 需要说明的是，所述步骤S300、步骤S310及步骤S320是同步执行。

[0191] 请参见附图4，在本发明的又一个实施例中，当识别到用户选择半自动模式时，所述根据用户选择的控制模式，进行相应的安装信息提示及安装进程控制的过程中，包括：

[0192] S400，将所述标记的恶意程序进行选定，并将该选定信息提示给用户，以便用户对选定信息进行确认和/或调整。

[0193] 具体的，所述选定信息提示是随主软件安装的实时进程而实时触发提示给用户的，在选定信息提示的过程中，需根据所述主软件安装的进程，实时调用预设的用于选定信息提示的脚本。其中，例如，所述选定信息可为“正在选定恶意程序”、“恶意程序已全选定”等。

[0194] S410，控制禁用下一操作指令的指令按钮，并启动所述指令按钮解禁的倒计时，以便用户在所述指令按钮禁用期间，手动取消选定和/或选定所述标记的恶意程序。

[0195] 具体的，在指令按钮禁用期间，用户无法点击生效该禁用的指令按钮；启动所述指令按钮解禁的倒计时是与时间戳相配合的，所述倒计时是预设的，例如倒计时可预设为10秒等；用户可在步骤S400中已将标记的恶意程序全都选定的情况下，根据自身需求，手动调整恶意程序的选定；该过程不仅可提高用户对恶意程序的注意度，使用户实时了解主软件安装进程及恶意程序的拦截进程，还可便于用户对安装进程及恶意程序的拦截进程实时干预，提高用户的参与度，使用户的感觉性更强。

[0196] S420，实时识别所述标记的恶意程序的选定情况，以得出最终选定的恶意程序。

[0197] 具体的，可实时识别拦截程序服务器自动选定的恶意程序和用户手动调整的恶意程序选定情况。

[0198] S430，当所述指令按钮解禁后，执行下一操作指令时，将所述最终选定的恶意程序进行拦截。

[0199] 需要说明的是，可预设为当所述指令按钮解禁后，需用户点击生效下一操作指令，拦截程序服务器才会执行下一操作指令程序进程，也可预设为，当所述指令按钮解禁后，拦截程序服务器自动控制执行下一操作指令程序进程。

[0200] 在本发明的又一个实施例中，当识别到用户选择提示模式时，所述根据用户选择的控制模式，进行相应的安装信息提示及安装进程控制的过程中，包括：实时将标记的恶意程序信息及主软件安装的实施进程信息提示给用户，以便用户选定要拦截的已标记恶意程序和/或选择相应的进程控制的操作指令；根据用户选定的内容或选择的操作指令，执行对

应的操作。

[0201] 进一步的，请参见附图5，本发明所述的方法，还包括步骤：

[0202] S130，接收用于对用户进行相关提示的文本信息的脚本，并准予所述脚本配置至所述原配置文件中。

[0203] 具体的，所述相关提示的文本信息的脚本是预先根据帮用户记录拦截程序服务器远程执行的操作方式制作而成的，然后配置至原配置文件中，以便拦截程序服务器根据主软件安装进程的而实时调用。

[0204] 进一步的，请参见附图6，本发明所述的方法，还包括步骤：

[0205] S140，对原配置文件进行检测，以识别出原配置文件中的恶意程序。

[0206] 具体的，所述对原配置文件进行检测，以识别出原配置文件中的恶意程序的过程包括：将原配置文件的相关信息与预先设置的云端鉴别条件进行匹配，若匹配成功则从原配置文件中将恶意程序的相关信息抓取出来。所述云端鉴别条件中包括多个特定程序匹配条件和满足该特定程序匹配条件后需要检查的特定ELF文件信息。其中，所述将原配置文件的相关信息与预先设置的云端鉴别条件进行匹配的过程包括：将原配置文件的相关信息与所述特定程序匹配条件进行匹配；获取相匹配的特定程序匹配条件后需要检查的特定ELF文件信息；将所述特定ELF文件信息作为所述原配置文件的相关信息的ELF文件信息。

[0207] 需要说明的是，所述特定程序匹配条件包括以下信息中的至少一种：

[0208] 文件名称信息、文件大小信息、文件特征值信息、文件图标信息、产品名称信息、内部名称信息、原始文件名信息，以及进程的命令行信息、进程路径信息和父进程路径信息。

[0209] 所述原配置文件的相关信息包括以下信息中的至少一种：

[0210] 待执行程序的文件名称信息、文件大小信息、文件特征值信息、文件图标信息、产品名称信息、内部名称信息、原始文件名信息，以及待执行程序创建的进程的命令行信息、进程路径信息和父进程路径信息。

[0211] 为了便于理解，现对原配置文件的相关信息与云端鉴别条件进行匹配的过程进行举例说明。

[0212] 如图7所示，是所述云端鉴别条件的示意图。

[0213] 从图7中可以看出，在该云端鉴别条件中包括条件和返回值两个部分，其中条件一列中包含了多个表达式，这些表达式即为本发明所述的特定程序匹配条件，返回值一列包含了多个字符串，这些字符串中指定了满足对应的特定程序匹配条件后需要检查的特定ELF文件信息。

[0214] 在条件一列的表达式中可以包括产品名称信息(hi.GEN)、文件大小信息(hi.DSI)、内部名称信息(hi.ITN)、原始文件名信息(hi.ORN)、进程路径信息(hi.DST)、父进程路径信息(hi.SRC)、进程命令行信息(hi.CLE)等信息，这些信息适于与待执行程序的特征信息进行匹配。

[0215] 在返回值一列的字符串中“ELF:”后指定了满足对应的特定程序匹配条件后需要检查的特定ELF文件信息，在本实施例中，所述ELF文件信息可以为ELF文件的名称。另外，在返回值一列的字符串中，可以指定多个需要检查的特定ELF文件信息，每个ELF文件信息之间以逗号相隔。

[0216] 例如，获取到当前待执行程序的特征信息为产品名称信息“金山重装高手”，然后

将该产品名称信息与云端鉴别条件进行匹配，经过判断，特定程序匹配条件中的“(hi.GEN:like,金山重装高手)”是与产品名称信息“金山重装高手”相匹配的条件，因此，可以从该条件对应的返回值“(return_extinfo:<hips>ELF:kdump.elf,irrlicht.elf</hips>)”中获取需要检查的ELF文件名称为“kdump.elf”和“irrlicht.elf”。

[0217] 需要说明的是，本实施例所述的云端鉴别条件还可以包括其他的信息，例如是否生效、条件序号、应用比例等，本领域技术人员根据实际情况进行相应处理即可，本实施例对此并不加以限制。

[0218] 进一步的，请参见附图6，本发明所述的方法，还包括步骤：

[0219] S150，对所述原配置文件中的恶意程序进行处理。

[0220] 具体的，所述对所述原配置文件中的恶意程序进行处理的过程包括：获取所述恶意程序的数据，从中解析出所述恶意程序待写入的目标路径；将所述目标路径加入文件防御规则，使用所述文件防御规则在所述恶意程序生成文件时进行文件防御。其中，使用所述文件防御规则在所述恶意程序生成文件时进行文件防御的过程包括：主动防御系统在所述恶意程序生成文件时，获取生成的文件的文件路径；判断所述生成的文件的文件路径与所述文件防御规则中的目标路径是否匹配；若匹配，则获取所述生成的文件的文件特征值，对所述生成的文件的文件特征值进行安全性判定；根据返回结果对所述恶意程序进行相应的文件防御处理。其中，所述步骤S150与步骤S120无必要的先后顺序之分，可同步执行。

[0221] 其中，服务端存储有相应的文件判定规则，预先通过对文件特征值进行分析将文件等级分类，确定生成的文件为白文件(即安全文件)，则可以放行；若确定生成的文件为黑文件(恶意程序文件)，则进行拦截或提示报警等处理；若不能确定文件的性质，则提示用户，由用户进行相应的处理，如决定放行或禁止等。若生成的文件的文件路径与文件防御规则中的目标路径不匹配，则可以根据设置的其他规则进行处理，如放行、提示、或者使用AD(Application Defend，应用程序防御体系)规则进行防御等。

[0222] 例如，将文件的文件特征值如文件哈希值发送到服务器进行查询，服务器中预先保存有根据文件哈希值划分的文件等级，根据查询结果确定文件的等级。另外，对于有白签名的文件，服务器会按白文件处理。服务器的数据库保存有白名单，该白名单可以包括目标白名单和来源白名单，以便于对生成的文件及其来源进行安全性判定，其中，目标白名单和来源白名单也可以统一为同一个白名单来进行安全性判定，也可以划分为不同的白名单，保存在服务器中数据库的不同的位置。

[0223] 其中，文件哈希值可以是经由MD5运算得出的MD5验证码，或SHA1码，或CRC(Cyclic Redundancy Check，循环冗余校验)码等可唯一标识原程序的特征码。

[0224] 另一种使用文件防御规则在程序生成文件时进行文件防御的方式是：主动防御系统在程序生成文件时，获取生成的文件的文件路径；判断生成的文件的文件路径与文件防御规则中的目标路径是否匹配；若匹配，则获取生成的文件，判断生成的文件是否在目标白名单中；若生成的文件在目标白名单中，且生成的文件的来源在来源白名单中，则将生成的文件放行。

[0225] 其中，当主动防御系统判断生成的文件的文件路径与文件防御规则中的目标路径匹配时，获取生成的文件，先判断生成的文件是否符合预置的临界文件规则，其中，临界文件规则用于指示生成的文件为除白名单文件、黑名单文件和可疑文件之外的文件；若符合，

则判断生成的文件的来源是否在来源白名单中;若是,则将生成的文件放行;若否,则进行报警提示。临界文件规则可以由本领域技术人员根据实际情况适当设置,如根据文件等级判断生成的文件是否为灰名单文件等,其中,灰名单文件可以是危险级别大于白名单文件,但又小于可疑文件的文件。但不限于此,也可以将灰名单文件和可疑文件等均囊括入临界文件中。在FD(File Defend,文件防御体系)规则中放过了白来源(即来源白名单中的文件来源)的文件,可以有效减少误报。如果该文件的来源是白的,则可以直接放过,运行其写注册表等。

[0226] 需要说明的是,本方案中的服务器可以是部署于主动防御系统所在设备之外的后台服务器,如后台云服务器,但不限于此,在硬件条件许可的情况下,该服务器也可以与主动防御系统合并设置,即主动防御系统与服务器设置在一台机器上。

[0227] 优选的,当程序写注册表时,主动防御系统会启动RD(Registry Defend,注册表防御体系)。RD提供了对常见的系统敏感注册表项进行监视,如启动项、服务驱动项、系统策略项、浏览器设置或网络设置(包括NameServer)项的添加修改。当有程序进行修改表项的操作时,目前默认都被RD视为敏感行为而拦截挂起,这种拦截挂起造成了现有主动防御系统的漏报或者误报。当程序写注册表项时,若主动防御系统确定程序写入的注册表目标项不存在,不会进行拦截挂起,而是将待写入的目标路径加入FD规则,等待后续的FD。例如,注册表中不存在程序写入的注册表目标项,如程序写入的目标路径不是系统中当前已经存在的现有路径而是新路径,则主动防御系统不会进行拦截挂起,而是将待写入的目标路径加入FD规则,等待后续的FD。

[0228] 优选的,文件防御体系(FD),用于监视系统敏感目录的文件(如HOSTS)操作,如修改删除系统目录里的任何文件或创建新文件等,也可用来发现被驱动木马隐藏的文件本体。实现文件防御体系的要点同样也是拦截系统底层函数如NtOpenFile等,HIPS默认对系统敏感目录进行监控保护,一旦发现异常读写,则把相关操作挂起,并根据一定的匹配模式决定放行、阻止或则弹框提示用户。如果程序写入的注册表目标项,如写入的目标路径不存在时,主动防御系统不会拦截,因为拦截容易造成误报,但是不拦截又有可能会产生漏报。而根据本发明的安全防御方案,当程序写入的注册表目标项不存在时,主动防御系统不会报警,但会将该目标项中的目标路径加入文件防御规则,在生成文件时进行文件防御。通过本实施例,对RD中取决于目标的规则,如果目标不存在,那么使用FD防护规则,在文件生成的时候拦截,解决了现有的安全防御方法无法对注册表和/或文件的改动进行精确地防御,以致漏报和误报的情况时有发生的问题,达到RD和FD联合防御,减少漏报和误报的效果。

[0229] 通过上述方式,实现了AD、RD及FD规则的联防;RD规则、FD规则和AD规则,是通过TRAY下发给驱动的,其中TRAY规定了每个规则如何根据不同的行为定义拦截,例如,当木马写入文件到一个文件路径下,替换该路径本身的文件(文件名不变),此时,主动防御系统的服务TRAY还未运行起来,而此时木马却运行起来,则主动防御系统无法进行拦截防护。而通过将开机启动程序的路径加入FD规则中,则很好地解决了这一问题。

[0230] 综上,本发明不仅可通过上述方案检测出原配置文件中的恶意程序,并对所述恶意程序进行防御处理,以维护用户所使用的终端设备的安全性,且本发明可对原配置文件中的恶意程序进行标记,然后当客户端在进行主软件安装时,将标记的恶意程序信息及主软件安装的实施进程信息提示给用户,以便用户知晓所述恶意程序信息、知晓主软件安装

进程和/或根据提示做相应的操作，该过程可使用户实时知晓主软件的安装进程及拦截进程，且用户还可根据需要参与拦截进程中，以提高用户的参与感，使用户的感觉性更强。

[0231] 另外，用户可根据需求选择全自动模式、半自动模式或提示模式的所述主软件安装控制模式，无论用户选择前述何种控制模式，皆可使用户实时了解主软件安装进程及恶意程序的拦截进程。其中，当识别到用户选择全自动模式时，服务器会将所述标记的恶意程序进行拦截，并将主软件安装的实时操纵指令和/或当前进程信息提示给用户，以便用户实时了解主软件安装进程及恶意程序的拦截进程；当识别到用户选择半自动模式时，服务器将所述标记的恶意程序进行选定，并将该选定信息提示给用户，以便用户对选定信息进行确认和/或调整，同时控制禁用下一操作指令的指令按钮，并启动所述指令按钮解禁的倒计时，以便用户在所述指令按钮禁用期间，手动取消选定和/或选定所述标记的恶意程序，该过程不仅可提高用户对恶意程序的注意度，使用户实时了解主软件安装进程及恶意程序的拦截进程，还可便于用户对安装进程及恶意程序的拦截进程实时干预，提高用户的参与度，使用户的感觉性更强。

[0232] 相应的，依据计算机软件的功能模块化思维，本发明还提供了一种恶意程序的处理系统，也即一种恶意程序的处理方法的拦截程序服务器。请参见附图8，以下具体揭示本系统包括的模块及各模块实现的具体功能。该系统包括：

[0233] 读取模块11，用于读取主软件安装包中的原配置文件。

[0234] 具体的，当主软件安装包下载完成，准备安装时，所述读取模块11即会对该主软件安装包中的原配置文件进行读取检测。

[0235] 标记模块12，用于对原配置文件中的恶意程序进行标记。

[0236] 具体的，首先根据云端鉴别条件库，对原配置文件中的恶意程序进行精确匹配抓取，其精确匹配抓取方式包括如下过程：将原配置文件中的安装进程的描述信息与云端鉴别条件库中保存的黑名单进行匹配比对，若匹配成功，则对该安装进程文件标记为恶意程序。所述描述信息，包括以下一种或多种的组合：版本号、安装文件的发布公司名称、产品名称、内部名称、签名者、签名日期、安装文件大小、安装范围、安装文件的时间戳、安装命令行信息。

[0237] 其中，所述云端鉴别条件库保存的对应执行拦截策略的行为的描述信息，包括以下一种或多种的组合：由默认拦截的进程执行的与所述默认拦截的进程无关的文件创建操作的描述信息、由默认拦截的进程执行的与所述默认拦截的进程无关的文件写入操作的描述信息、由默认拦截的进程执行的与所述默认的进程无关的安装操作的描述信息。

[0238] 所述云端鉴别条件库中保存的对应执行拦截策略的安装进程的描述信息，包括以下一种或者多种的组合：由默认拦截的进程启动且与所述默认拦截的进程无关的安装进程的描述信息、已执行拦截的安装进程的描述信息、预先收集的默认拦截的安装进程的描述信息、预先收集的默认拦截的下载进程访问的网络地址。

[0239] 提示模块13，用于当客户端在进行主软件安装时，将标记的恶意程序信息及主软件安装的实施进程信息提示给用户，以便用户知晓所述恶意程序信息、知晓主软件安装进程和/或根据提示做相应的操作。

[0240] 具体的，请参见附图9，所述提示模块13包括：

[0241] 检测子模块131，用于实时检测客户端中进行主软件安装的当前进程。

[0242] 选择提示子模块132，用于提示用户选择主软件安装的控制模式。

[0243] 具体的，所述主软件安装的控制模式包括全自动模式、半自动模式及提示模式。

[0244] 识别子模块133，用于对用户所选择的主软件安装的控制模式进行识别。

[0245] 具体的，根据用户触发相应的标识指令按钮来识别，并将识别结果反馈至下一级进程控制端，以便下一级进程控制端根据标识指令按钮预设的执行。

[0246] 操作执行子模块134，用于根据用户选择的控制模式，进行相应的安装信息提示及安装进程控制。

[0247] 具体的，所述安装信息提示包括安装进程信息提示及恶意程序的拦截信息提示；所述安装进程控制包括主软件安装进程控制及恶意程序的拦截进程控制。

[0248] 请参见附图9及附图10，在本发明的一个实施例中，当所述识别子模块133识别到用户选择全自动模式时，所述操作执行子模块134包括：

[0249] 第一拦截单元103，用于将所述标记的恶意程序进行拦截。

[0250] 具体的，该过程是拦截程序服务器直接将标记的恶意程序进行选定执行拦截的。

[0251] 控制单元101，用于根据预设的软件安装方式，实时控制所述主软件的安装进程按照所述预设的软件安装方式进行。

[0252] 第一提示单元105，用于将主软件安装的实时操控指令和/或当前进程信息提示给用户。

[0253] 具体的，所述主软件安装的实时操控指令和/或当前进程信息都是按预设的软件安装方式执行的；所述进程信息提示是随主软件安装的实时进程而实时触发提示给用户的，在进程信息提示的过程中，需根据所述主软件安装的进程，实时调用预设的用于进程信息提示的脚本。例如，所述当前进程信息可为“正在选定恶意程序”、“正在拦截恶意程序”等。

[0254] 需要说明的是，所述第一拦截单元103、控制单元101及第一提示单元105同步协同工作。

[0255] 请参见附图9及附图11，在本发明的又一个实施例中，当所述识别子模块133识别到用户选择半自动模式时，所述操作执行子模块134包括：

[0256] 选定提示单元102，用于将所述标记的恶意程序进行选定，并将该选定信息提示给用户，以便用户对选定信息进行确认和/或调整。

[0257] 具体的，所述选定信息提示是随主软件安装的实时进程而实时触发提示给用户的，在选定信息提示的过程中，需根据所述主软件安装的进程，实时调用预设的用于选定信息提示的脚本。其中，例如，所述选定信息可为“正在选定恶意程序”、“恶意程序已全选定”等。

[0258] 禁用控制单元104，用于控制禁用下一操作指令的指令按钮，并启动所述指令按钮解禁的倒计时，以便用户在所述指令按钮禁用期间，手动取消选定和/或选定所述标记的恶意程序。

[0259] 具体的，在指令按钮禁用期间，用户无法点击生效该禁用的指令按钮；启动所述指令按钮解禁的倒计时是与时间戳相配合的，所述倒计时是预设的，例如倒计时可预设为10秒等；用户可在被所述选定提示单元102已将标记的恶意程序全都选定的情况下，根据自身需求，手动调整恶意程序的选定；该过程不仅可提高用户对恶意程序的注意度，使用户实时

了解主软件安装进程及恶意程序的拦截进程，还可便于用户对安装进程及恶意程序的拦截进程实时干预，提高用户的参与度，使用户的感觉性更强。

[0260] 选定识别单元106，用于实时识别所述标记的恶意程序的选定情况，以得出最终选定的恶意程序。

[0261] 具体的，可实时识别选定提示单元102自动选定的恶意程序和用户在所述禁用控制单元104工作期间手动调整的恶意程序选定情况。

[0262] 第二拦截单元108，用于当所述指令按钮解禁后，执行下一操作指令时，将所述最终选定的恶意程序进行拦截。

[0263] 需要说明的是，可预设为当所述指令按钮解禁后，需用户点击生效下一操作指令，第二拦截单元108才会执行下一操作指令程序进程；也可预设为，当所述指令按钮解禁后，第二拦截单元108自动控制执行下一操作指令程序进程。

[0264] 在本发明的又一个实施例中，当所述识别子模块133识别到用户选择提示模式时，所述操作执行子模块134包括：

[0265] 第二提示单元，用于实时将标记的恶意程序信息及主软件安装的实施进程信息提示给用户，以便用户选定要拦截的已标记恶意程序和/或选择相应的进程控制的操作指令；指令执行单元，用于根据用户选定的内容或选择的操作指令，执行对应的操作。

[0266] 需要说明的是，在上述三个实施例中，所述操作执行子模块还包括：

[0267] 调用单元，用于根据所述主软件安装的进程，实时调用所述脚本。

[0268] 具体的，在所述第一提示单元105、选定提示单元102或第二提示单元工作时，需通过所述调用单元实时调用预设于原配置文件中的相关提示信息的脚本。

[0269] 进一步的，请参见附图12，本发明所述的系统，还包括：

[0270] 接收模块14，用于接收用于对用户进行相关提示的文本信息的脚本，并准予所述脚本配置至所述原配置文件中。

[0271] 具体的，所述相关提示的文本信息的脚本是预先根据帮用户记录拦截程序服务器远程执行的操作方式制作而成的，然后配置至原配置文件中，以便调用单元根据主软件安装进程的而实时调用。

[0272] 进一步的，请参见附图13，本发明所述的系统，还包括：

[0273] 检测模块15，用于对原配置文件进行检测，以识别出原配置文件中的恶意程序。

[0274] 具体的，所述检测模块15包括：匹配子模块，用于将原配置文件的相关信息与预先设置的云端鉴别条件进行匹配，若匹配成功则从原配置文件中将恶意程序的相关信息抓取出来。所述云端鉴别条件中包括多个特定程序匹配条件和满足该特定程序匹配条件后需要检查的特定ELF文件信息。其中，所述匹配子模块包括：匹配单元，用于将原配置文件的相关信息与所述特定程序匹配条件进行匹配；获取单元，用于获取相匹配的特定程序匹配条件后需要检查的特定ELF文件信息；作为单元，用于将所述特定ELF文件信息作为所述原配置文件的相关信息的ELF文件信息。

[0275] 需要说明的是，所述特定程序匹配条件包括以下信息中的至少一种：

[0276] 文件名称信息、文件大小信息、文件特征值信息、文件图标信息、产品名称信息、内部名称信息、原始文件名信息，以及进程的命令行信息、进程路径信息和父进程路径信息。

[0277] 所述原配置文件的相关信息包括以下信息中的至少一种：

[0278] 待执行程序的文件名称信息、文件大小信息、文件特征值信息、文件图标信息、产品名称信息、内部名称信息、原始文件名信息，以及待执行程序创建的进程的命令行信息、进程路径信息和父进程路径信息。

[0279] 进一步的，本发明所述的系统，还包括：

[0280] 处理模块16，用于对所述原配置文件中的恶意程序进行处理。

[0281] 具体的，所述处理模块16包括：解析子模块，用于获取所述恶意程序的数据，从中解析出所述恶意程序待写入的目标路径；防御子模块，用于将所述目标路径加入文件防御规则，使用所述文件防御规则在所述恶意程序生成文件时进行文件防御。其中，所述防御子模块包括：生成获取单元，用于主动防御系统在所述恶意程序生成文件时，获取生成的文件的文件路径；匹配判断单元，用于判断所述生成的文件的文件路径与所述文件防御规则中的目标路径是否匹配；若匹配，则获取所述生成的文件的文件特征值，对所述生成的文件的文件特征值进行安全性判定；防御处理单元，用于根据返回结果对所述恶意程序进行相应的文件防御处理。

[0282] 综上，本发明不仅可通过上述方案检测出原配置文件中的恶意程序，并对所述恶意程序进行防御处理，以维护用户所使用的终端设备的安全性，且本发明可对原配置文件中的恶意程序进行标记，然后当客户端在进行主软件安装时，将标记的恶意程序信息及主软件安装的实施进程信息提示给用户，以便用户知晓所述恶意程序信息、知晓主软件安装进程和/或根据提示做相应的操作，该过程可使用户实时知晓主软件的安装进程及拦截进程，且用户还可根据需要参与拦截进程中，以提高用户的参与感，使用户的感觉性更强。

[0283] 另外，用户可根据需求选择全自动模式、半自动模式或提示模式的所述主软件安装控制模式，无论用户选择前述何种控制模式，皆可使用户实时了解主软件安装进程及恶意程序的拦截进程。其中，当识别到用户选择全自动模式时，服务器会将所述标记的恶意程序进行拦截，并将主软件安装的实时操纵指令和/或当前进程信息提示给用户，以便用户实时了解主软件安装进程及恶意程序的拦截进程；当识别到用户选择半自动模式时，服务器将所述标记的恶意程序进行选定，并将该选定信息提示给用户，以便用户对选定信息进行确认和/或调整，同时控制禁用下一操作指令的指令按钮，并启动所述指令按钮解禁的倒计时，以便用户在所述指令按钮禁用期间，手动取消选定和/或选定所述标记的恶意程序，该过程不仅可提高用户对恶意程序的注意度，使用户实时了解主软件安装进程及恶意程序的拦截进程，还可便于用户对安装进程及恶意程序的拦截进程实时干预，提高用户的参与度，使用户的感觉性更强。

[0284] 在此处所提供的说明书中，虽然说明了大量的具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实施例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0285] 虽然上面已经示出了本发明的一些示例性实施例，但是本领域的技术人员将理解，在不脱离本发明的原理或精神的情况下，可以对这些示例性实施例做出改变，本发明的范围由权利要求及其等同物限定。

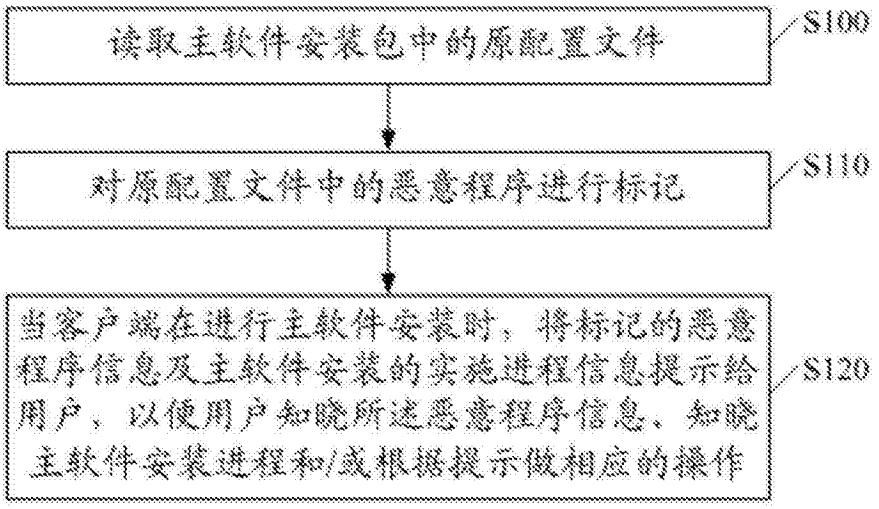

读取主软件安装包中的原配置文件
S100
对原配置文件中的恶意程序进行标记
S110
当客户端在进行主软件安装时，将标记的恶意程序信息及主软件安装的实施进程信息提示给用户，以使用户知晓所述恶意程序信息、知晓主软件安装进程和/或根据提示做相应的操作
S120

图1

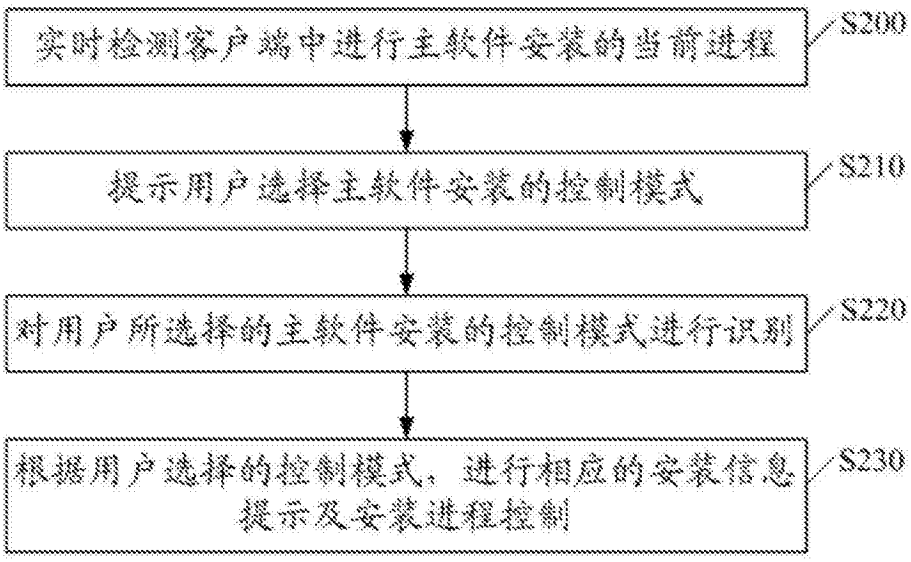

实时检测客户端中进行主软件安装的当前进程
S200
提示用户选择主软件安装的控制模式
S210
对用户所选择的主软件安装的控制模式进行识别
S220
根据用户选择的控制模式，进行相应的安装信息提示及安装进程控制
S230

图2

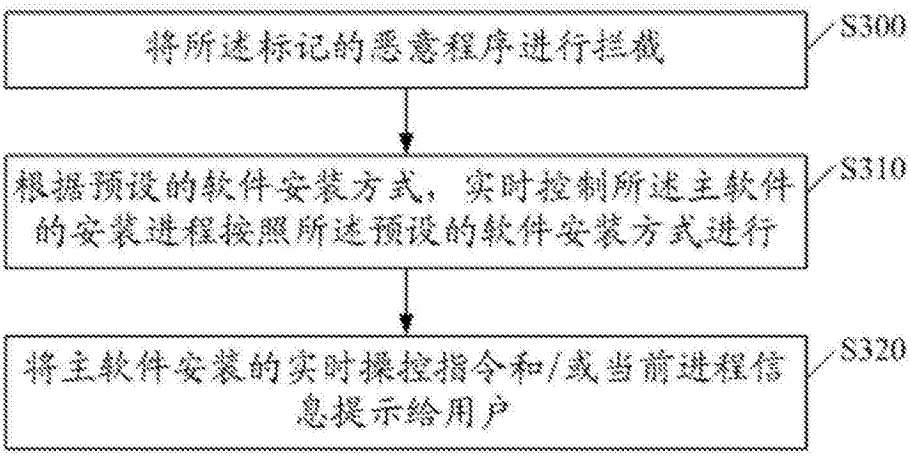

将所述标记的恶意程序进行拦截
S300
根据预设的软件安装方式，实时控制所述主软件的安装进程按照所述预设的软件安装方式进行
S310
将主软件安装的实时操控指令和/或当前进程信息提示给用户
S320

图3

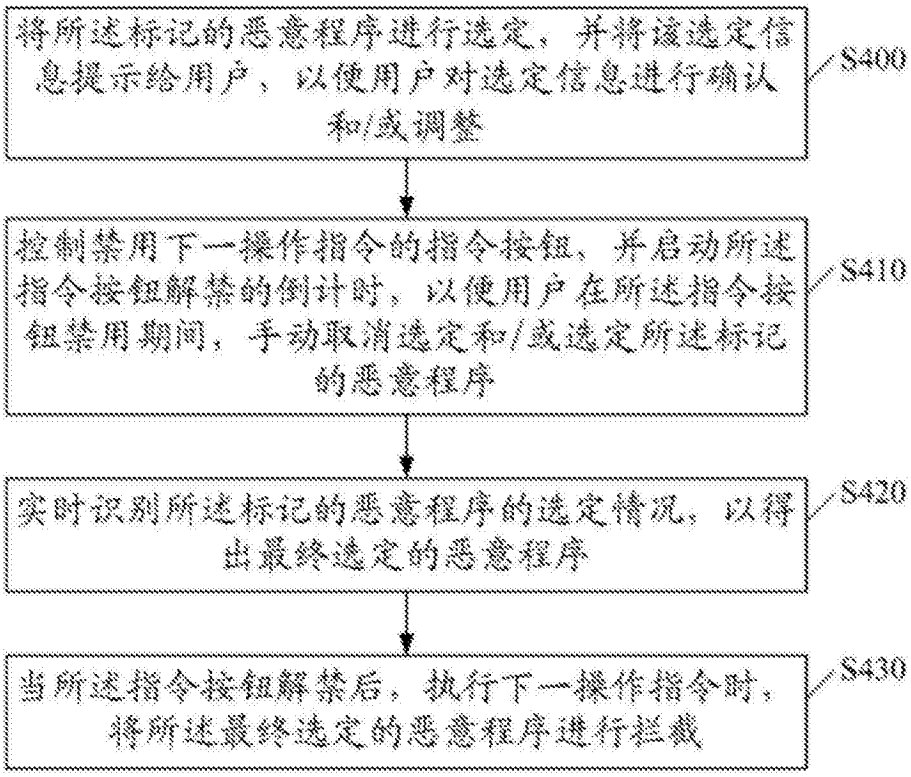

将所述标记的恶意程序进行选定，并将该选定信息提示给用户，以使用户对选定信息进行确认和/或调整
S400
控制禁用下一操作指令的指令按钮，并启动所述指令按钮解禁的倒计时，以使用户在所述指令按钮禁用期间，手动取消选定和/或选定所述标记的恶意程序
S410
实时识别所述标记的恶意程序的选定情况，以得出最终选定的恶意程序
S420
当所述指令按钮解禁后，执行下一操作指令时，将所述最终选定的恶意程序进行拦截
S430

图4

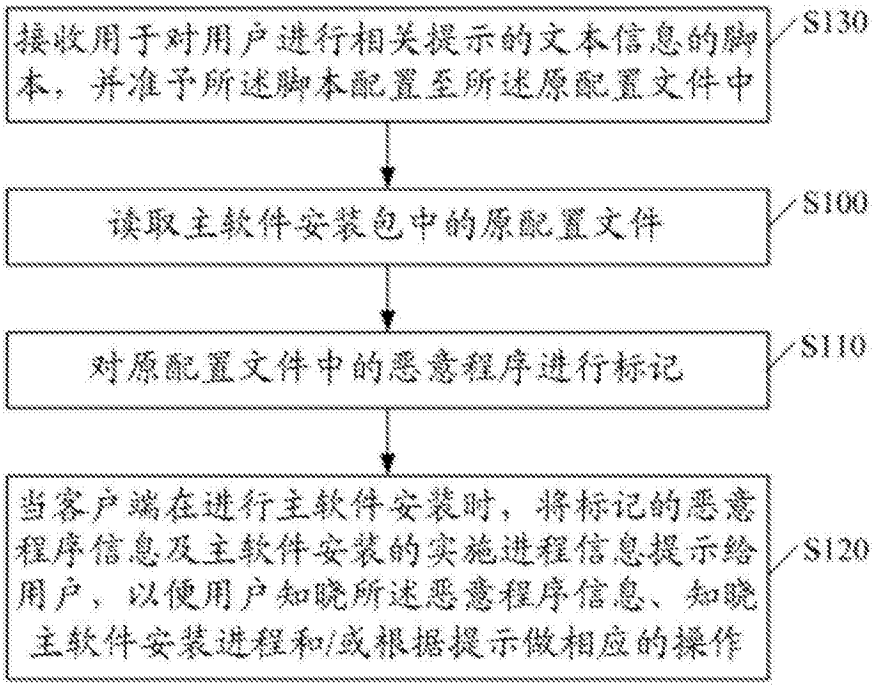

接收用于对用户进行相关提示的文本信息的脚本，并准予所述脚本配置至所述原配置文件中
S130
读取主软件安装包中的原配置文件
S100
对原配置文件中的恶意程序进行标记
S110
当客户端在进行主软件安装时，将标记的恶意程序信息及主软件安装的实施进程信息提示给用户，以使用户知晓所述恶意程序信息、知晓主软件安装进程和/或根据提示做相应的操作
S120

图5

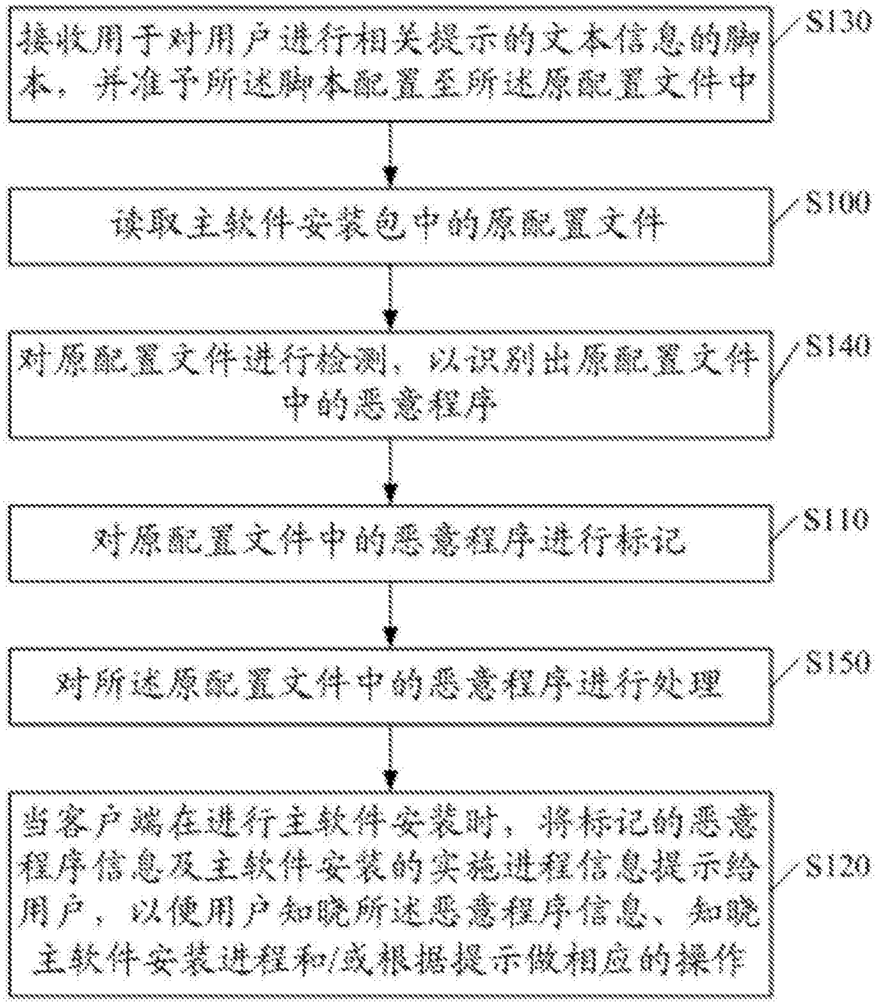


图6

[illegible]	[illegible]
{return_extinfo:<hips>ELF:kdump.ei{inSicht.dll</hips>}	{hi.GEN:like,金山[illegible]}
{return_extinfo:<hips>ELF:kdump.ei{inSicht.dll}</hips>}	{hi.GEN:like,金山[illegible]}
{return_extinfo:<hips>ELF:hwsig.ei</hips>}	{hi.GEN:like,[illegible]}&&{icon_dna:dna,100,96,YeNLJwMFmizLmz4BOyyA/ODFZL1DeV
{return_extinfo:<hips>ELF:hwsig.ei</hips>}	{hi.GEN:like,[illegible]}
{return_extinfo:<hips>ELF:F1DrvLift.ei</hips>}	{hi.DST:like,\\F1DrvLift\.EXE$}&&{file_dna:dna,100,6144,bPTCLNSmBXoCjlq1Oqjcq+8OnC
{return_extinfo:<hips>ELF:sogouexplorer.ei</hips>}	{hi.GEN:like,[illegible]}&&{hi.DST:like,\\(sogou.*[illegible]|[illegible])\\sogouexplorer\.exe$

图7

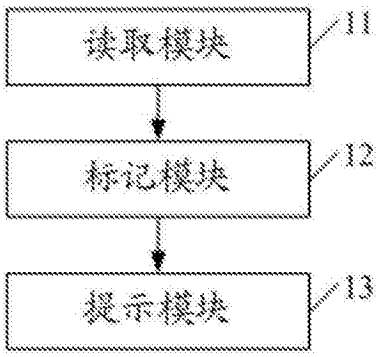

读取模块
11
标记模块
12
提示模块
13

图8

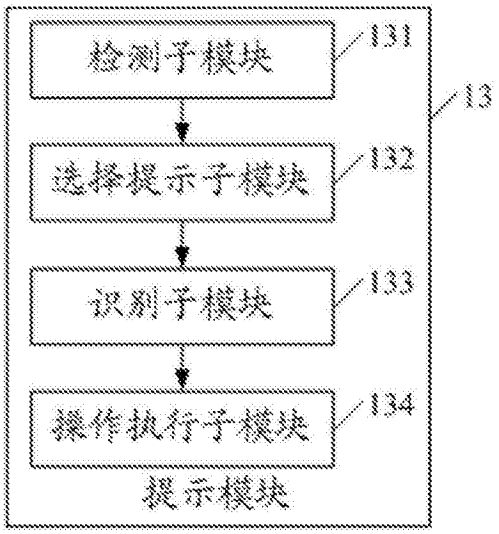

检测子模块
131
13
选择提示子模块
132
识别子模块
133
操作执行子模块
134
提示模块

图9

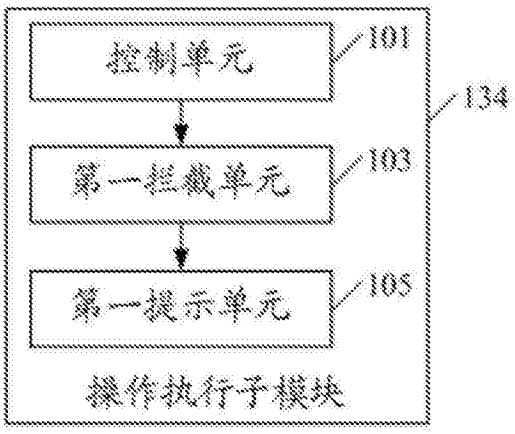

控制单元
101
134
第一拦截单元
103
第一提示单元
105
操作执行子模块

图10

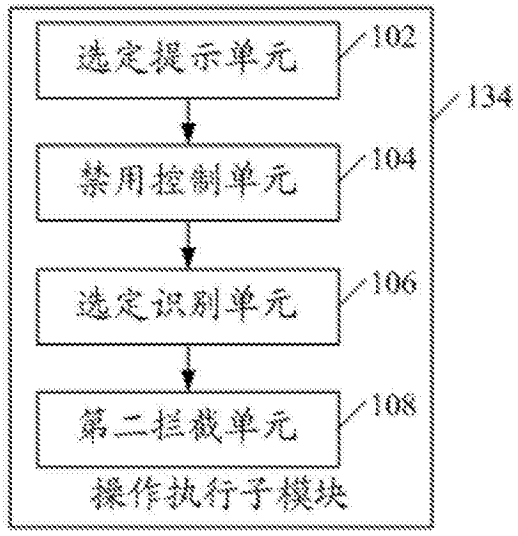

选定提示单元
102
134
禁用控制单元
104
选定识别单元
106
第二拦截单元
108
操作执行子模块

图11

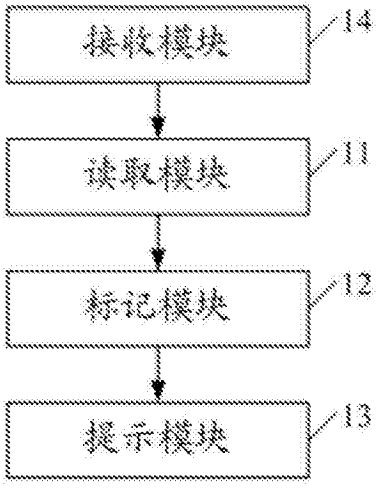

接收模块
14
读取模块
11
标记模块
12
提示模块
13

图12

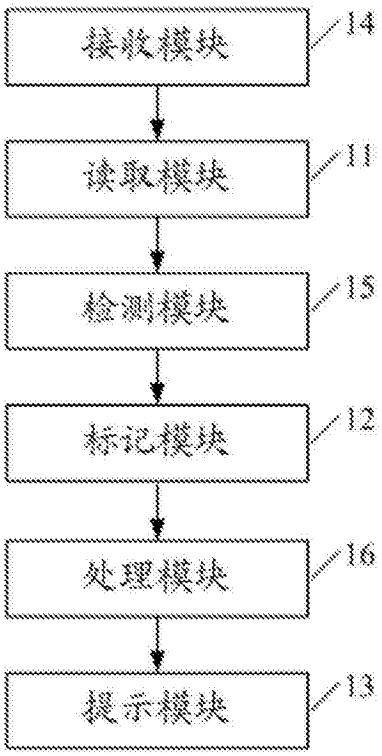


图13