(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2015 年 6 月 11 日 (11.06.2015)

WIPO | PCT

(10) 国际公布号
WO 2015/081900 A1

(51) 国际专利分类号:
G06F 21/56 (2013.01)

(21) 国际申请号: PCT/CN2014/093286

(22) 国际申请日: 2014 年 12 月 8 日 (08.12.2014)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201310656591.3 2013 年 12 月 6 日 (06.12.2013) CN

(71) 申请人: **北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED)** [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室（德胜园区）, Beijing 100088 (CN)。 **奇智软件（北京）有限公司 (QIZHI SOFTWARE (BEIJING) COMPANY LIMITED)** [CN/CN]; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼 B 座 2 层、3 层 301-306 室, Beijing 100015 (CN)。

(72) 发明人: **赵龙 (ZHAO, Long)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 **邹贵强 (ZOU, Guiqiang)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。

(74) 代理人: **北京润泽恒知识产权代理有限公司 (BEIJING RISEHIGH INTELLECTUAL PROPERTY LAW FIRM)**; 中国北京市海淀区中关村南大街 31 号神舟大厦 702, Beijing 100081 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) **Title**: METHOD, DEVICE, AND SYSTEM FOR CLOUD-SECURITY-BASED BLOCKING OF ADVERTISEMENT PROGRAMS

(54) **发明名称**: 基于云安全拦截广告程序的方法、装置和系统

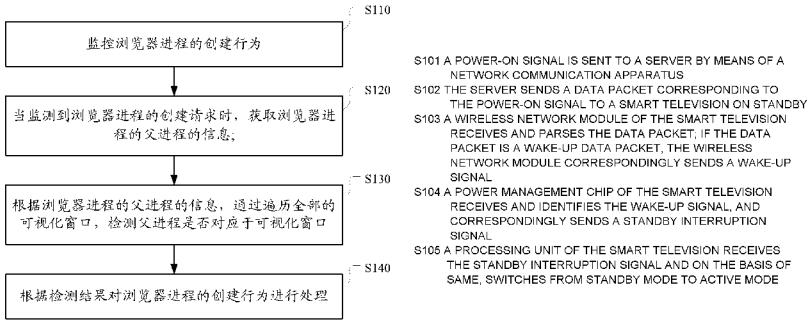

图 1 / Fig. 1

(57) **Abstract**: A method, device, and system for cloud-security-based blocking of advertisement programs. The method comprises: monitoring a browser-process creation activity; upon detecting a creation request for a browser process, obtaining parent process information of said browser process; on the basis of the parent process information of said browser process, testing whether a parent process corresponds to a visible window by analyzing all visible windows; on the basis of testing results, processing the browser-process creation activity. The technical solution provided by the present invention may effectively block browser pages such as pop-up advertisements and phishing sites resulting from hidden-window background processes not authorized by the user. This allows the user to avoid being disturbed by advertisements and other such useless information or being deceived by phony information on malicious websites, thereby improving online security for the user.

(57) **摘要**: 本发明公开了一种基于云安全拦截广告程序的方法、装置和系统，其中，所述方法包括：监控浏览器进程的创建行为；当监测到浏览器进程的创建请求时，获取浏览器进程的父进程的信息；根据浏览器进程的父进程的信息，通过遍历全部的可视化窗口，检测父进程是否对应于可视化窗口；根据检测结果对浏览器进程的创建行为进行处理。根据本发明提供的方案，可以有效拦截隐藏窗口的后台进程未经用户同意而弹出广告、钓鱼网站等浏览器页面，使用户在操作中避免受到广告等无效信息的干扰和各种恶意网站上虚假信息的欺骗，提高了用户网络操作的安全性。

WO 2015/081900 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

基于云安全拦截广告程序的方法、装置和系统

技术领域

本发明涉及计算机安全领域，具体涉及一种基于云安全拦截广告程序的方法、装置和系统。

背景技术

随着互联网的发展，基于浏览器的应用日益普及，比如，人们通过浏览器可以查询银行账户、网上购物、电子商务、查询信息、获取知识、进行娱乐等，基于浏览器的应用为人们提供了方便和快捷的交互方式。然而，人们在上网冲浪浏览网页的同时，经常会遇到未经点击而自动弹出的浏览器页面，例如广告、游戏、购物网页，这些网页的内容通常对用户来说毫无意义，只会对用户的浏览行为造成干扰，更严重的问题是，部分弹出页面还可能来自恶意网站，如钓鱼网站，或者欺诈、假冒网站等，这些页面上通常显示有虚假信息并且页面代码内嵌入有恶意的脚本程序，用于非法获取用户输入的账号、密码等个人信息，对用户利益造成损害。

其中，部分未经许可而打开的浏览器页面是由在后台运行的恶意程序的进程开启的，这些恶意进程通常不具有窗口，或隐藏自身窗口以达到不被用户发现的目的。对于这类恶意程序，现有技术中仍然采用通用的方法，例如基于特征库来分析、匹配程序的特征码，这种方式通常具有滞后性，无法应对新的情况，运营成本也较大。因此，对于这类恶意程序，现有技术中缺乏一种具有针对性的检测和拦截方法。

发明内容

鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的基于云安全拦截广告程序的方法、装置和系统。

根据本发明的一个方面，提供了一种基于云安全拦截广告程序的方法，

包括：监控浏览器进程的创建行为；当监测到浏览器进程的创建请求时，获取浏览器进程的父进程的信息;根据浏览器进程的父进程的信息，通过遍历全部的可视化窗口，检测父进程是否对应于可视化窗口；根据检测结果对浏览器进程的创建行为进行处理。

根据本发明的另一方面，提供了一种基于云安全拦截广告程序的装置，包括：监控模块，适于监控浏览器进程的创建行为；获取模块，适于当监控模块监测到浏览器进程的创建请求时，获取浏览器进程的父进程的信息；检测模块，适于根据浏览器进程的父进程的信息，通过遍历全部的可视化窗口，检测父进程是否对应于可视化窗口；处理模块，适于根据检测结果对浏览器进程的创建行为进行处理。

根据本发明的另一方面，提供了一种基于云安全拦截广告程序的系统，包括上述基于云安全拦截广告程序的装置，还包括向该装置提供云查询服务的服务器。

根据本发明的又一个方面，提供了一种计算机程序，其包括计算机可读代码，当所述计算机可读代码在电子设备上运行时，导致所述电子设备执行根据上述的基于云安全拦截广告程序的方法。

根据本发明的再一个方面，提供了一种计算机可读介质，其中存储了如上所述的计算机程序。

根据本发明的基于云安全拦截广告程序的方案，监控到浏览器进程的创建请求时，获取要创建该浏览器进程的父进程的信息，检测该父进程是否与当前界面中的至少一个可视化窗口对应，从而判断出父进程的安全性，根据检测结果对其创建浏览器进程的行为进行相应的处理。根据该方案，可以有效拦截隐藏窗口的后台进程未经用户同意而弹出广告、钓鱼网站等浏览器页面，使用户在操作中避免受到广告等无效信息的干扰和各种恶意网站上虚假信息的欺骗，提高了用户网络操作的安全性。

上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图 1 示出了根据本发明一个实施例的基于云安全拦截广告程序的方法的流程图；

图 2 示出了根据本发明另一实施例的基于云安全拦截广告程序的方法的流程图；

图 3 示出了根据本发明另一实施例的基于云安全拦截广告程序的方法的流程图；

图 4 示出了根据本发明另一实施例的基于云安全拦截广告程序的方法的流程图；

图 5 示出了根据本发明另一个实施例的基于云安全拦截广告程序的装置的结构框图；

图 6 示出了根据本发明另一个实施例的基于云安全拦截广告程序的装置的结构框图；

图 7 示出了根据本发明另一实施例的基于云安全拦截广告程序的系统的结构框图；

图 8 示出了用于执行根据本发明的方法的电子设备的框图；以及

图 9 示出了用于保持或者携带实现根据本发明的方法的程序代码的存储单元。

具体实施方式

下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地

理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

图 1 示出了根据本发明一个实施例的基于云安全拦截广告程序的方法的流程图，如图 1 所示，该方法包括如下步骤:

步骤 S110，监控浏览器进程的创建行为。

在常见的计算机系统，如 Windows 系统，对浏览器进程的监控通常是基于操作系统提供的 API 接口函数或系统调用来实现的。

该步骤中所说的浏览器包括但不限于运行在各类计算机系统中的 IE、Firefox、Chrome、Safari 等独立内核浏览器，以及常见的基于 IE 内核的，或基于多内核的浏览器，如 360 浏览器，搜狗浏览器等，还包括运行于各种移动终端操作系统中常见的浏览器。一种常见的情况是，系统中安装有一种以上的浏览器，例如，Windows 系统中除了自带的 IE 浏览器，用户出于丰富功能、更高的安全性和个人喜好，可能安装并默认使用上述其他浏览器。这时，对浏览器进程的监控就应该包括对 IE 进程，及其他全部浏览器进程的监控。

步骤 S120，当监测到浏览器进程的创建请求时，获取浏览器进程的父进程的信息。

浏览器进程的父进程就是请求创建该浏览器进程的进程。以 Windows 操作系统为例，各种应用层应用程序都是通过调用各种 API 函数来实现的，父进程创建浏览器进程需要调用相应的 API 函数，检测浏览器进程的创建请求也就是监控创建进程的 API 函数的调用请求，通过捕获该 API 函数，可以从该 API 函数携带的参数中解析出指向的应用程序，判断出创建的是否为浏览器进程。请求调用该函数的进程就是浏览器进程的父进程，父进程的进程信息可以包括但不限于进程名称，进程标识，进程文件的路径信息以及相关的动态链接库文件等。

步骤 S130，根据浏览器进程的父进程的信息，通过遍历全部的可视化窗口，检测父进程是否对应于可视化窗口。

对大多数的应用程序，用户一般通过该程序提供的可视化窗口与系统进行交互。本发明通过检测父进程是否对应于可视化窗口来判断浏览器进程的创建行为是否为用户触发。遍历全部的可视化窗口，如果存在至少一个可视

化窗口与浏览器进程的父进程相对应，认为浏览器进程的创建行为是该可视化窗口对应的应用程序响应于用户在该窗口中的点击、输入等触发行为而发起的，例如，用户点击 QQ 界面上的空间图片，弹出了空间页面，这属于用户允许的安全行为，而如果浏览器进程的父进程不对应于可视化窗口，认为该次创建行为是后台进程未经用户允许而请求的，是可疑的恶意行为。

步骤 S140，根据检测结果对所述浏览器进程的创建行为进行处理。

对于对应于可视化窗口的父进程，允许其创建浏览器进程；对于不对应可视化窗口的父进程，进行拦截，给出提示信息或进一步确认其安全性。

根据本发明上述实施例提供的方法，对浏览器进程的创建行为进行实时的监控，并找到发起该创建请求的进程，作为浏览器进程的父进程，获取该父进程的信息，遍历全部的可视化窗口，检测父进程是否对应于可视化窗口，以此来判断浏览器进程的创建行为是否为用户的主动选择，根据检测的结果对创建行为做相应的处理。根据该方案可以有效拦截隐藏窗口的后台进程未经用户同意而弹出广告、游戏、购物、钓鱼网站等浏览器页面的干扰或威胁，提高了用户网络操作的安全性。

图 2 示出了本发明另一个实施例的基于云安全拦截广告程序的方法的流程图，如图 2 所示，该方法包括如下步骤:

步骤 S210，监控浏览器进程的创建行为。

如同在步骤 S120 中所述的，Windows 系统中，监控浏览器进程的创建行为实际上是监控对相应的 API 函数的调用请求。具体地，应用程序要创建一个 Win32 进程，可能需要调用的 API 函数有 CreateProcess、CreateProcessAsUser 等，创建的新进程运行指定的可执行文件，可执行文件的路径、文件名由 API 函数的参数指定，例如，参数 lpApplicationName 指定了可执行模块的路径，捕获该函数，从其参数中获得可执行文件的路径，文件名等信息，即可判断出本次 API 调用创建的进程是否为浏览器进程。

步骤 S220，获取浏览器进程的父进程信息。

获取请求调用 CreateProcess 等 API 函数的应用程序，从而获取父进程信息。父进程的进程信息可以包括但不限于进程名称，进程标识，进程文件的

路径信息以及相关的动态链接库文件等。

在获取父进程信息时，一种可能的情况是，一些恶意程序为了更好地隐藏自己，可能会通过其进程 A 调用进程 B，然后进程 B 请求调用 API 函数创建浏览器进程，甚至经过更多级的调用。这时，在后续步骤中，仅根据进程 B 的信息并不能做出准确的判断。因此，还要获取进程 B 所在的进程链的多个进程的信息。这可以通过 NtQueryInformationProcess 函数实现，利用该函数逐级查找，获取全部相关进程。

具体地，获取进程名称、进程标识等信息也可以通过调用 API 函数实现，例如，通过 Process Status（进程状态）API 函数下的多个函数获取进程名称；通过 GetCurrentProcessId 获取进程 ID 等。当然，也可以选择其他的 API 函数或者通过高级语言实现。

步骤 S230，遍历全部的可视化窗口并获取每个可视化窗口对应进程的进程标识。

进程被创建时会被分配一个进程标识，直到进程中止这个标识都是有效的，并且不会改变，在进程有效的时间内，每个进程的进程标识都是唯一的，因此，它可以被用来唯一标识这个进程。具体地，该步骤中可以用 EnumWindows 函数遍历窗口，获取窗口的句柄，然后用 GetWindowThreadProcessId 函数获得每个窗口句柄对应的进程标识。

步骤 S240，在全部的可视化窗口的进程标识中查询浏览器进程的父进程标识，如果能查询到父进程标识，则确定父进程对应于可视化窗口，执行步骤 S250，否则，执行步骤 S260。

在同一时刻，进程标识唯一，因此，如果存在至少一个可视化窗口，其进程标识与浏览器进程的父进程的进程标识一致，则认为该父进程对应于该可视化窗口，即可以认为浏览器进程的创建行为是该可视化窗口对应的应用程序响应于用户在该窗口中的点击、输入等触发行为而发起的。

步骤 S250，允许执行父进程创建浏览器进程的行为，结束本次流程。

由下文中步骤 S260 描述可知，一种拦截进程的方法是，在创建进程的任意一个步骤通过钩子函数的方法拦截其所必须调用的 API 函数实现的。因此，

对于允许所监控到的创建行为请求的情形，在本发明实施例的钩子函数执行完毕后，跳转到该文件行为请求对应 API 的原始入口地址去执行相应的指令即可。

步骤 S260，给出风险提示信息，并按照用户根据风险提示信息的选择对所述浏览器进程的创建行为进行拦截。

如果在全部的可视化窗口的进程标识中未查询到父进程标识，认为该父进程创建浏览器进程的行为是后台进程未经用户允许而发起的，是可疑的恶意行为，如广告程序行为，可能需要对该行为进行拦截。

这时，向用户提供风险提示信息，具体地，可以在桌面指定区域弹出消息窗口，将步骤 S220 中获取的父进程信息，如进程名称，进程路径，相应的可执行文件名称等展示给用户，供用户分析以做出决定，还可以根据现有的统计结果，给出进程及相应的应用程序的危险等级、安全评分等信息并向用户提供相应的建议。

在一些情况下，虽然父进程不对应可视化窗口，但该父进程创建浏览器进程的行为并不属于恶意行为，例如，安装、卸载软件时，在安装、卸载程序结束后，经常弹出一些用于信息反馈的浏览器页面，并不具有危害性，如果用户需要，可以选择不对该浏览器进程的创建行为进行拦截。还可以在本地设置一个安全名单，将用户选择不拦截的进程加入该名单中，下次不再提示。

对进程创建行为的拦截可以按如下方式实现。通常，一个进程的创建过程如下：打开要被执行的文件映像，创建执行进程对象，创建初始线程及堆栈及上下文，通知 Windows 子系统有关进程的信息，开始初始线程的执行，执行新进程上下文中的进程初始化。可以在其中任意一个步骤通过钩子函数的方法拦截其所必须调用的 API 函数，达到拦截进程创建的目的。例如，通过在开始初始线程的步骤执行之前，通过对系统服务调度表中的 Native API 函数 ZwCreateProcess 的拦截来实现，即在系统调用 ZwCreateProcess 时，转到钩子程序中进行处理。或者通过拦截其他步骤中调用的 API 函数实现，如 NtCreateSection 函数，该函数用于打开要被执行的文件映像。

图 3 示出了本发明另一个实施例的基于云安全拦截广告程序的方法的流

程图，如图 3 所示，该方法包括如下步骤:

步骤 S310，监控浏览器进程的创建行为;

步骤 S320，获取浏览器进程的父进程信息;

步骤 S330，遍历全部的可视化窗口并获取每个可视化窗口对应进程的进程标识;

其中，步骤 S310-S330 与上一实施例中的步骤 S210-S230 相同，此处不再赘述。

步骤 S340，在全部的可视化窗口的进程标识中查询浏览器进程的父进程标识，如果能查询到父进程标识，则确定父进程对应于可视化窗口，执行步骤 S350，否则，执行步骤 S360。

步骤 S350，允许执行父进程创建浏览器进程的行为，结束本次流程。

步骤 S360，在预置的本地进程白名单中查询不对应于可视化窗口的父进程的进程信息，如果查询成功，执行步骤 S350，否则，执行步骤 S370。

如同在上一实施例中步骤 S260 里所述的，不对应于可视化窗口的父进程的创建行为可能是安全的。然而，用户的判断未必准确。在本实施例中，通过用户判断与黑白名单的方式结合进行更准确的判断。

首先在本地预置的进程白名单中查询父进程信息，本地白名单保存有常见的安全进程，例如，常用软件的安装、卸载相关的进程。与步骤 S260 类似地，在桌面指定区域弹出消息窗口。提示信息窗口还可以接收用户反馈，用于本地进程白名单的维护和更新。例如，用户对某一不在白名单中的进程有特殊需求，可以选择允许其创建浏览器进程，记录用户对该进程的选择，将进程加入到本地进程白名单中，下次不再提示。

步骤 S370，将父进程的进程信息上传至服务器，以供服务器通过云查询获知父进程是否属于服务器保存的进程黑名单，并从服务器接收查询结果。如果查询结果指示该父进程属于服务器保存的进程黑名单，执行步骤 S380。

与本地名单相比，服务器端的黑名单数据库保存有更完整的信息，能够进行更严格准确的判断。具体地，客户端将检测到的可疑进程的进程信息上传至服务器，服务器根据进程信息对相应的可执行文件或应用程序进行杀毒

分析，可以采用传统的特征码匹配方式，或者采用主动防御的方法分析应用程序包含的行为特点。找出特征码与病毒库，或恶意程序相匹配的应用程序，或行为动作触发预设安全规则的应用程序，将相应的进程信息加入到进程黑名单中。

服务器上的黑名单也可以通过人工运营的方式产生，服务器端定期对来自客户端的病毒或恶意程序数据进行统计，对使用数量排名靠前或者增长速度靠前或者危险性排名靠前的进程，通过分析其弹出网页的内容等方式判断其安全性，放入黑名单中。

步骤 S380，给出风险提示信息，并按照用户根据风险提示信息的选择对浏览器进程的创建行为进行拦截。

实际中，也可以选择直接拦截创建行为。但考虑用户可能对某些进程存在特殊需求，通常先给出风险提示信息，接收用户反馈。该步骤与 S260 相似，在步骤 S260 的基础上，还可以进一步给出服务器的分析结果。

对于属于白名单的进程，可以允许其创建浏览器的行为。

图 4 示出了本发明另一个实施例的基于云安全拦截广告程序的方法的流程图。如图 4 所示，该方法包括如下步骤:

步骤 S410，监控浏览器进程的创建行为;

步骤 S420，获取浏览器进程的父进程信息;

步骤 S430，遍历全部的可视化窗口并获取每个可视化窗口对应进程的进程标识;

其中，步骤 S410-S430 与前述实施例中的步骤 S210-S230 相同，此处不再赘述

步骤 S440，在全部的可视化窗口的进程标识中查询浏览器进程的父进程标识，如果能查询到父进程标识，则确定父进程对应于可视化窗口，执行步骤 S450，否则，执行步骤 S460。

步骤 S450，允许执行父进程创建浏览器进程的行为，结束本次流程。

步骤 S460，获取父进程创建的浏览器进程所要访问的页面 URL。

一种可能方式是通过浏览器中提供的插件机制，例如，在IE浏览器中，通过响应“BeforeNavigate2”事件可以获取IE当前加载的URL。在火狐（Firefox）浏览器中使用火狐扩展机制提供的指定响应事件接口，获取火狐浏览器当前加载的URL。在谷歌（chrome）浏览器中使用网景插件应用程序编程接口（Netscape Plugin Application Programming Interface，简称：NPAPI）插件机制，获取谷歌浏览器当前加载的URL。

步骤S470，将该页面URL打包成密文后上传至服务器，以供服务器通过云查询获知该页面URL是否属于服务器保存的URL黑名单或白名单，并从服务器接收查询结果。如果查询结果指示该页面URL属于URL黑名单，执行步骤S480；如果查询结果指示该页面URL属于URL白名单，执行步骤S450。

服务器收集常见的广告、游戏等页面的URL，加入黑名单中；对用户允许放行的浏览器创建行为，收集该行为创建的浏览器页面所打开的URL，分析该URL页面的内容，或者统计大量用户对该URL页面的拦截情况，判断该页面是否为正常页面，将判断出的正常页面加入白名单中。

页面URL上传至服务器时，先将页面URL加密成密文，然后发送给服务器。这里，可以采用可逆加密方法对页面URL进行加密，也可以采用不可逆加密方法对页面URL进行加密。举例来说，计算页面URL的特征值作为密文。可选地，特征值可以为根据MD5（Message Digest Algorithm，消息摘要算法第五版）计算得到的哈希值，或SHA1（Secure Hash Algorithm，安全哈希算法）码，或CRC（Cyclic Redundancy Check，循环冗余校验）码等可唯一标识原信息的特征码。需要说明的是，在上传页面URL的密文到服务器的时候，需要首先屏蔽可能带有用户密码的网址字符串，不上传此类信息，以便保证用户信息的安全。

步骤S480，给出风险提示信息，并按照用户根据风险提示信息的选择对浏览器进程的创建行为进行拦截。

出于与步骤S370相同的理由，优选地，先给出风险提示信息。

对于属于白名单的URL对应的父进程，可以允许其创建浏览器的行为。

根据本发明上述实施例提供的方法，通过捕获创建进程所必须的 API 函数实现对浏览器进程创建行为的监控，找到发起该创建请求的父进程，获取该父进程的进程标识，遍历全部的可视化窗口并获取每个可视化窗口对应进程的进程标识，在全部的可视化窗口的进程标识中查询浏览器进程的父进程标识，以此来判断浏览器进程的创建行为是否为用户的主动选择，对于非用户主动选择的可疑进程，给出风险提示信息，或者进一步通过云端的进程黑白名单或 URL 黑白名单确认。根据该方案可以有效拦截隐藏窗口的后台进程未经用户同意而弹出广告、游戏、购物、钓鱼网站等浏览器页面的干扰或威胁，并且，通过云查询的方式，降低了对恶意程序行为和安全行为误判的概率，进一步提高系统的安全性和用户的操作体验。

图 5 示出了本发明另一个实施例的基于云安全拦截广告程序的装置的框图。如图 5 所示，该装置包括:

监控模块 500，适于监控浏览器进程的创建行为；获取模块 502，适于当监控模块 500 监测到浏览器进程的创建请求时，获取所述浏览器进程的父进程的信息；检测模块 504，适于根据所述浏览器进程的父进程的信息，通过遍历全部的可视化窗口，检测所述父进程是否对应于可视化窗口；处理模块 506，适于根据检测结果对所述浏览器进程的创建行为进行处理。

根据本发明上述实施例提供的基于云安全拦截广告程序的装置，对浏览器进程的创建行为进行实时的监控，并找到发起该创建请求的进程，作为浏览器进程的父进程，获取该父进程的信息，遍历全部的可视化窗口，检测父进程是否对应于可视化窗口，以此来判断浏览器进程的创建行为是否为用户的主动选择，根据检测的结果对创建行为做相应的处理。根据该方案可以有效拦截隐藏窗口的后台进程未经用户同意而弹出广告、游戏、购物、钓鱼网站等浏览器页面的干扰或威胁，提高了用户网络操作的安全性。

图 6 示出了本发明另一个实施例的基于云安全拦截广告程序的装置的框图。本实施例的基于云安全拦截广告程序的装置对图 5 所示的装置进行了进一步的优化，优化后的基于云安全拦截广告程序的装置如图 6 所示，该装置包括:

监控模块 510，适于监控浏览器进程的创建行为。

可选地，监控模块 510 通过监控创建进程的 API 函数的调用请求实现对创建行为的监控。具体地，应用程序要创建一个 Win32 进程，可能需要调用的 API 函数有 CreateProcess、CreateProcessAsUser 等，创建的新进程运行指定的可执行文件，可执行文件的路径、文件名由 API 函数的参数指定，例如，参数 lpApplicationName 指定了可执行模块的路径，监控模块 540 捕获该函数，从其参数中获得可执行文件的路径及文件名，即可判断出本次 API 调用创建的进程是否为浏览器进程。

获取模块 520，适于当监控模块 510 监测到浏览器进程的创建请求时，获取浏览器进程的父进程的信息。

例如，获取模块 520 获取请求调用 CreateProcess 等 API 函数的应用程序，从而获取父进程信息。获取模块 520 获取父进程的进程信息可以包括但不限于获取进程名称，进程标识，进程文件的路径信息以及相关的动态链接库文件等。

可选地，获取模块 520 适于当监控模块 510 监测到浏览器进程的创建请求时，获取浏览器进程的父进程标识。获取模块 520 获取进程名称、进程标识等信息也可以通过调用 API 函数实现，例如，通过 Process Status（进程状态）API 函数下的多个函数获取进程名称；通过 GetCurrentProcessId 获取进程 ID 等。

检测模块 530，适于根据浏览器进程的父进程的信息，通过遍历全部的可视化窗口，检测父进程是否对应于可视化窗口。

进程被创建时会被分配一个进程标识。直到进程中止这个标识都是有效的，并且不会改变，在进程有效的时间内，每个进程的进程标识都是唯一的，因此，检测模块 530 可以通过进程标识检测父进程是否对应于可视化窗口。

可选地，检测模块 530 包括：遍历模块 5302 和查询模块 5304。

其中：

遍历模块 5302，适于遍历全部的可视化窗口并获取每个可视化窗口对应进程的进程标识；遍历模块 5302 可以用 EnumWindows 函数遍历窗口，获取窗口的句柄，然后用 GetWindowThreadProcessId 函数获得每个窗口句柄对应

的进程标识。

查询模块 5304，适于在全部的可视化窗口的进程标识中查询浏览器进程的父进程标识，如果查询到浏览器进程的父进程标识，则确定所述父进程对应于可视化窗口；如果没有查询到浏览器进程的父进程标识，则确定所述父进程不对应于可视化窗口。

本实施例的基于云安全拦截广告程序的装置还包括：处理模块 540，适于根据检测结果对浏览器进程的创建行为进行处理。

可选地，处理模块 540 可以包括：第一拦截模块 5402，适于对于不对应于可视化窗口的父进程创建浏览器进程的行为，给出风险提示信息，并按照用户根据风险提示信息的选择对所述浏览器进程的创建行为进行拦截。

处理模块 540 对进程创建行为的拦截可以按如下方式实现。通常，一个进程的创建过程如下：打开要被执行的文件映像，创建执行进程对象，创建初始线程及堆栈及上下文，通知 Windows 子系统有关进程的信息，开始初始线程的执行，执行新进程上下文中的进程初始化。因此，处理模块 540 可以在其中任意一个步骤拦截其所必须调用的 API 函数，达到拦截进程创建的目的。例如，处理模块 540 在开始初始线程的步骤执行之前，对系统服务调度表中的 Native API 函数 ZwCreateProcess 的拦截。

处理模块 540 向用户提供风险提示信息可以为：在桌面指定区域弹出消息窗口，将获取模块 520 获取的父进程信息，如进程名称，进程路径，相应的可执行文件名称等展示给用户，供用户分析以做出决定，处理模块 540 还可以根据现有的统计结果，给出进程及相应的应用程序的危险等级、安全评分等信息并向用户提供相应的建议。

可选地，处理模块 540 也可以包括：第一云查询接口模块 5404，适于在预置的本地进程白名单中查询不对应于可视化窗口的父进程的进程信息；第一执行模块 5406，适于如果第一云查询接口模块 5404 的查询结果为查询成功，则允许所述父进程创建浏览器进程的行为；否则，将所述父进程的进程信息上传至服务器，以供服务器通过云查询获知父进程是否属于服务器保存的进程黑名单，并从服务器接收查询结果；以及，第二拦截模块 5408，适于如果查询结果指示所述父进程属于所述进程黑名单，给出风险提示信息，并

按照用户根据风险提示信息的选择对所述浏览器进程的创建行为进行拦截。。

例如，第一云查询接口模块 5404 将检测模块 530 检测到的可疑进程的进程信息上传至服务器，服务器根据进程信息对相应的可执行文件或应用程序进行杀毒分析，例如传统的特征码匹配方式，或者采用主动防御的方法，分析应用程序包含的行为特点。找出特征码与病毒库，或恶意程序相匹配的应用程序，或行为动作触发预设安全规则的应用程序，将相应的进程信息加入到进程黑名单中。

服务器上的黑名单也可以通过人工运营的方式产生，服务器端定期对来自客户端的病毒或恶意程序数据进行统计，对使用数量排名靠前或者增长速度靠前或者危险性排名靠前的进程，通过分析其弹出网页的内容等方式判断其安全性，放入黑名单中。

可选地，本实施例的处理模块 540 也可以包括: 页面 URL 提取模块 5410、第二云查询接口模块 5412 和第三拦截模块 5414。

其中:

页面 URL 提取模块 5410，适于对于不对应于可视化窗口的父进程，获取父进程创建的浏览器进程所要访问的页面 URL。

页面 URL 提取模块 570 获取 URL 的一种可能方式是通过浏览器中提供的插件机制，例如，在 IE 浏览器中，页面 URL 提取模块 5410 通过响应“BeforeNavigate2”事件获取 IE 当前加载的 URL，在火狐（Firefox）浏览器中页面 URL 提取模块 5410 使用火狐扩展机制提供的指定响应事件接口，获取火狐浏览器当前加载的 URL。在谷歌（chrome）浏览器中使用网景插件应用程序编程接口（Netscape Plugin Application Programming Interface，简称: NPAPI）插件机制，获取谷歌浏览器当前加载的 URL。

第二云查询接口模块 5412 适于将页面 URL 提取模块 570 所获取的页面 URL 打包成密文后上传至服务器，以供服务器通过云查询获知页面 URL 是否属于服务器保存的 URL 黑名单或白名单，并从服务器接收查询结果。

第三拦截模块 5414 适于如果查询结果指示所述页面 URL 属于所述 URL

黑名单，给出风险提示信息，并按照用户根据风险提示信息的选择对所述浏览器进程的创建行为进行拦截。

需要说明的是，上述多种处理模块的功能实现可以合并设置，也可以单独设置或者选择其中部分设置。同样，上述处理模块中的多个拦截模块可以单独设置实现各自的拦截功能，也可以合并设置实现多种对应的拦截功能。此外，上述处理模块中的第一云查询接口模块和第二云查询接口模块可以单独设置也可以合并设置，以实现相应的功能。

本实施例的基于云安全拦截广告程序的装置用于实现前述多个方法实施例中相应的基于云安全拦截广告程序的方法，并具有相应的方法实施例的有益效果，在此不再赘述。

图 7 示出了本发明另一实施例提供的基于云安全拦截广告程序的系统，如图 7 所示，该系统包括上一实施例中的基于云安全拦截广告程序的装置，还包括：向该装置提供云查询服务的服务器。

根据本发明上述实施例提供的装置和系统，监控模块通过捕获创建进程所必须的 API 函数实现对浏览器进程创建行为的监控，找到发起该创建请求的父进程，获取模块获取该父进程的进程信息，其中包括进程标识，遍历模块遍历全部的可视化窗口并获取每个可视化窗口对应进程的进程标识，查询模块在全部的可视化窗口的进程标识中查询浏览器进程的父进程标识，以此来判断浏览器进程的创建行为是否为用户的主动选择，对于非用户主动选择的可疑进程，处理模块通过相应的拦截模块给出风险提示信息，或者进一步地，通过相应的云查询接口模块将进程信息和/或待访问页面的 URL 发送至服务器，通过云端的进程黑白名单和/或 URL 黑白名单确认。根据该方案，可以有效拦截隐藏窗口的后台进程未经用户同意而弹出广告、游戏、购物、钓鱼网站等浏览器页面的干扰或威胁，并且，通过云查询的方式，降低了对恶意程序行为和安全行为误判的概率，进一步提高系统的安全性和用户的操作体验。

在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，

构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

在此处所提供的说明书中，说明了大量具体细节。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。

类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的程序模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本

发明实施例的基于云安全拦截广告程序的装置和系统中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

例如，图 8 示出了可以实现根据本发明的基于云安全拦截广告程序的方法的电子设备，例如客户端设备。该客户端设备传统上包括处理器 610 和以存储器 620 形式的计算机程序产品或者计算机可读介质。存储器 620 可以是诸如闪存、EEPROM（电可擦除可编程只读存储器）、EPROM、硬盘或者 ROM 之类的电子存储器。存储器 620 具有用于执行上述方法中的任何方法步骤的程序代码 631 的存储空间 630。例如，用于程序代码的存储空间 630 可以包括分别用于实现上面的方法中的各种步骤的各个程序代码 631。这些程序代码可以从一个或者多个计算机程序产品中读出或者写入到这一个或者多个计算机程序产品中。这些计算机程序产品包括诸如硬盘，紧致盘（CD）、存储卡或者软盘之类的程序代码载体。这样的计算机程序产品通常为如参考图 9 所述的便携式或者固定存储单元。该存储单元可以具有与图 8 的电子设备中的存储器 620 类似布置的存储段、存储空间等。程序代码可以例如以适当形式进行压缩。通常，存储单元包括计算机可读代码 631'，即可以由例如诸如 610 之类的处理器读取的代码，这些代码当由电子设备运行时，导致该电子设备执行上面所描述的方法中的各个步骤。

本文中所称的“一个实施例”、“实施例”或者“一个或者多个实施例”意味着，结合实施例描述的特定特征、结构或者特性包括在本发明的至少一个实施例中。此外，请注意，这里“在一个实施例中”的词语例子不一定全指同一个实施例。

在此处所提供的说明书中，说明了大量具体细节。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被实践。在一些实例中，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。

应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施

例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

此外，还应当注意，本说明书中使用的语言主要是为了可读性和教导的目的而选择的，而不是为了解释或者限定本发明的主题而选择的。因此，在不偏离所附权利要求书的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。对于本发明的范围，对本发明所做的公开是说明性的，而非限制性的，本发明的范围由所附权利要求书限定。

权 利 要 求 书

1、一种基于云安全拦截广告程序的方法，包括:

监控浏览器进程的创建行为;

当监测到浏览器进程的创建请求时，获取所述浏览器进程的父进程的信息;

根据所述浏览器进程的父进程的信息，通过遍历全部的可视化窗口，检测所述父进程是否对应于可视化窗口;

根据检测结果对所述浏览器进程的创建行为进行处理。

2、根据权利要求 1 所述的方法，其中，所述获取浏览器进程的父进程的信息的步骤包括：获取浏览器进程的父进程标识;

所述通过遍历全部的可视化窗口，检测父进程是否对应于可视化窗口的步骤包括:

遍历全部的可视化窗口并获取每个可视化窗口对应进程的进程标识;

在全部的可视化窗口的进程标识中查询所述浏览器进程的父进程标识，如果查询到所述浏览器进程的父进程标识，则确定所述父进程对应于可视化窗口；如果没有查询到所述浏览器进程的父进程标识，则确定所述父进程不对应于可视化窗口。

3、根据权利要求 1 或 2 所述的方法，其中，所述根据检测结果对浏览器进程的创建行为进行处理的步骤包括:

对于不对应于可视化窗口的父进程创建浏览器进程的行为，给出风险提示信息，并按照用户根据所述风险提示信息的选择对所述浏览器进程的创建行为进行拦截。

4、根据权利要求 1 或 2 所述的方法，其中，所述根据检测结果对浏览器进程的创建行为进行处理的步骤包括:

在预置的本地进程白名单中查询所述不对应于可视化窗口的父进程的进程信息，如果查询成功，允许所述父进程创建浏览器进程的行为;

否则，将所述父进程的进程信息上传至服务器，以供所述服务器通过云查询获知所述父进程是否属于服务器保存的进程黑名单，并从服务器接收查询结果；

如果查询结果指示所述父进程属于所述进程黑名单，给出风险提示信息，并按照用户根据所述风险提示信息的选择对所述浏览器进程的创建行为进行拦截。

5、根据权利要求 1 或 2 所述的方法，其中，所述根据检测结果对浏览器进程的创建行为进行处理的步骤包括：

对于不对应于可视化窗口的父进程，获取所述父进程创建的浏览器进程所要访问的页面 URL，将该页面 URL 打包成密文后上传至服务器，以供服务器通过云查询获知所述页面 URL 是否属于服务器保存的 URL 黑名单或白名单，并从服务器接收查询结果；

如果查询结果指示所述页面 URL 属于所述 URL 黑名单，给出风险提示信息，并按照用户根据所述风险提示信息的选择对所述浏览器进程的创建行为进行拦截。

6、一种基于云安全拦截广告程序的装置，包括：

监控模块，适于监控浏览器进程的创建行为；

获取模块，适于当所述监控模块监测到浏览器进程的创建请求时，获取所述浏览器进程的父进程的信息；

检测模块，适于根据所述浏览器进程的父进程的信息，通过遍历全部的可视化窗口，检测所述父进程是否对应于可视化窗口；

处理模块，适于根据检测结果对所述浏览器进程的创建行为进行处理。

7、根据权利要求 6 所述的装置，其中，所述获取模块，适于当所述监控模块监测到浏览器进程的创建请求时，获取浏览器进程的父进程标识；

所述检测模块包括：

遍历模块，适于遍历全部的可视化窗口并获取每个可视化窗口对应进程的进程标识；

查询模块，适于在全部的可视化窗口的进程标识中查询所述浏览器进程的父进程标识，如果查询到所述浏览器进程的父进程标识，则确定所述父进程对应于可视化窗口；如果没有查询到所述浏览器进程的父进程标识，则确定所述父进程不对应于可视化窗口。

8、根据权利要求 6 或 7 所述的装置，其中，所述处理模块包括：第一拦截模块，适于对于不对应于可视化窗口的父进程创建浏览器进程的行为，给出风险提示信息，并按照用户根据所述风险提示信息的选择对所述浏览器进程的创建行为进行拦截。

9、根据权利要求 6 或 7 所述的装置，其中，所述处理模块包括：

第一云查询接口模块，适于在预置的本地进程白名单中查询不对应于可视化窗口的父进程的进程信息；

第一执行模块，适于如果所述第一云查询接口模块的查询结果为查询成功，则允许所述父进程创建浏览器进程的行为；否则，将所述父进程的进程信息上传至服务器，以供所述服务器通过云查询获知所述父进程是否属于服务器保存的进程黑名单，并从服务器接收查询结果；

第二拦截模块，适于如果查询结果指示所述父进程属于所述进程黑名单，给出风险提示信息，并按照用户根据所述风险提示信息的选择对所述浏览器进程的创建行为进行拦截。

10、根据权利要求 6 或 7 所述的装置，其中，所述处理模块包括：

页面 URL 提取模块，适于对于不对应于可视化窗口的父进程，获取所述父进程创建的浏览器进程所要访问的页面 URL；

第二云查询接口模块，适于将所述页面 URL 提取模块所获取的页面 URL 打包成密文后上传至服务器，以供服务器通过云查询获知所述页面 URL 是否属于服务器保存的 URL 黑名单或白名单，并从服务器接收查询结果；

第三拦截模块，适于如果查询结果指示所述页面 URL 属于所述 URL 黑名单，给出风险提示信息，并按照用户根据所述风险提示信息的选择对所述浏览器进程的创建行为进行拦截。

11、一种基于云安全拦截广告程序的系统，包括权利要求 6-10 任一项所

述的基于云安全拦截广告程序的装置，还包括：向所述装置提供云查询服务的服务器。

12、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在电子设备上运行时，导致所述电子设备执行根据权利要求 1-5 中的任一个所述的基于云安全拦截广告程序的方法。

13、一种计算机可读介质，其中存储了如权利要求 12 所述的计算机程序。

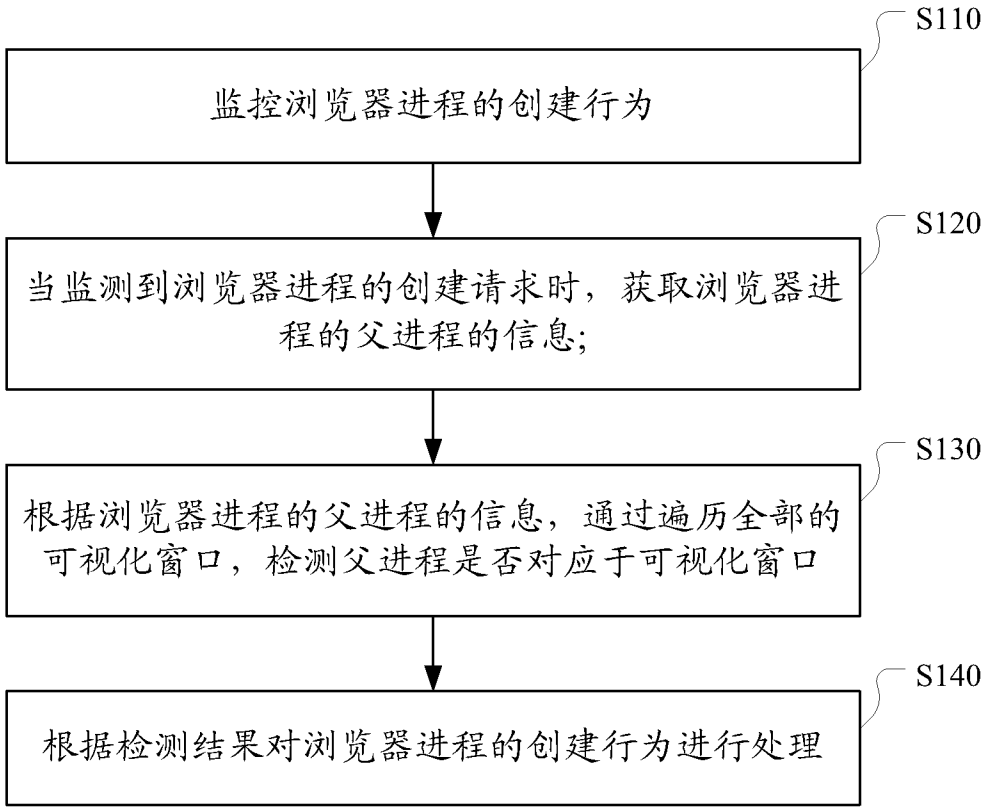
S110
监控浏览器进程的创建行为
S120
当监测到浏览器进程的创建请求时，获取浏览器进程的父进程的信息;
S130
根据浏览器进程的父进程的信息，通过遍历全部的可视化窗口，检测父进程是否对应于可视化窗口
S140
根据检测结果对浏览器进程的创建行为进行处理

图 1

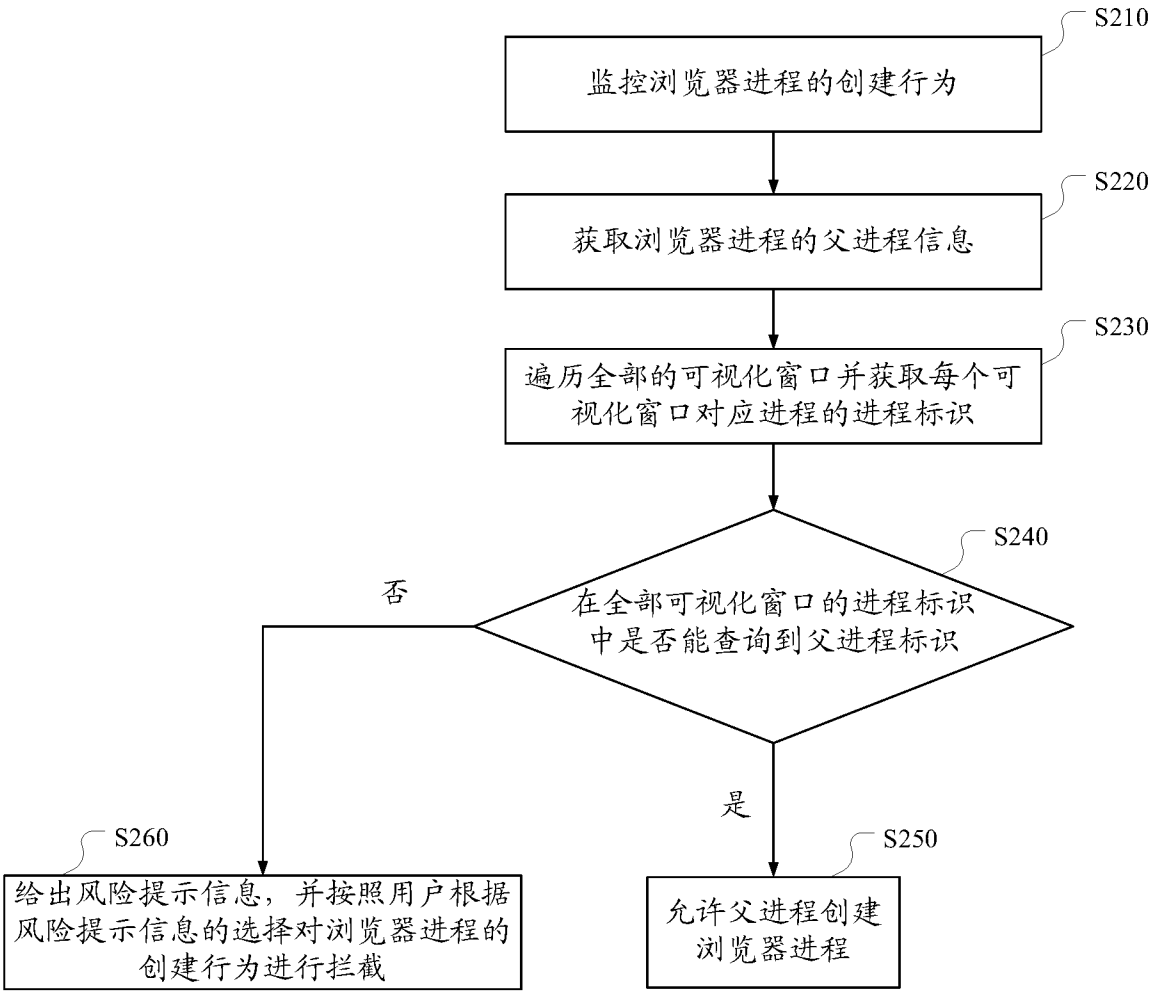
S210
监控浏览器进程的创建行为
S220
获取浏览器进程的父进程信息
S230
遍历全部的可视化窗口并获取每个可视化窗口对应进程的进程标识
S240
在全部可视化窗口的进程标识中是否能查询到父进程标识
否
是
S260
给出风险提示信息，并按照用户根据风险提示信息的选择对浏览器进程的创建行为进行拦截
S250
允许父进程创建浏览器进程

图 2

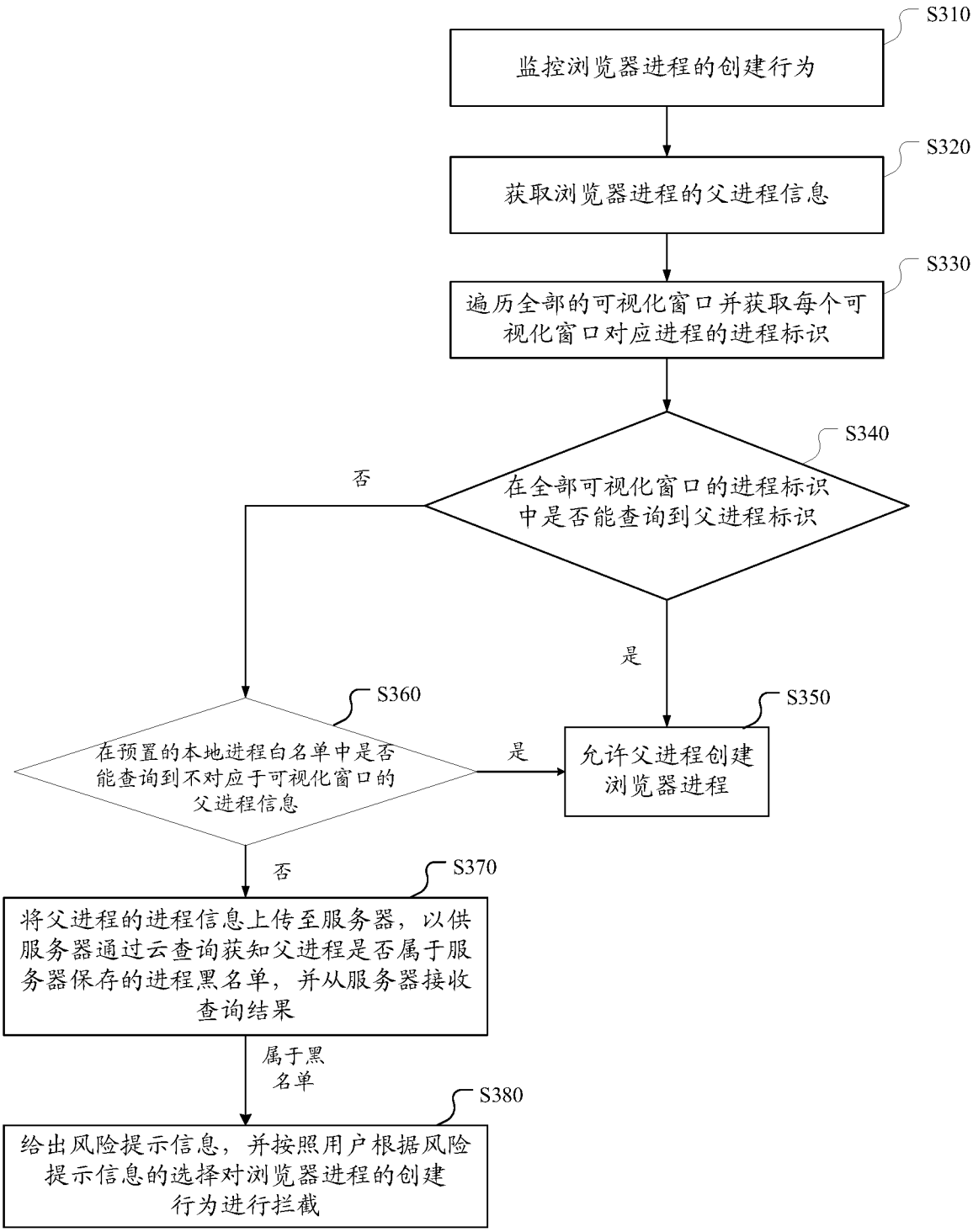
S310
监控浏览器进程的创建行为
S320
获取浏览器进程的父进程信息
S330
遍历全部的可视化窗口并获取每个可视化窗口对应进程的进程标识
S340
在全部可视化窗口的进程标识中是否能查询到父进程标识
否
是
S360
在预置的本地进程白名单中是否能查询到不对应于可视化窗口的父进程信息
是
S350
允许父进程创建浏览器进程
否
S370
将父进程的进程信息上传至服务器，以供服务器通过云查询获知父进程是否属于服务器保存的进程黑名单，并从服务器接收查询结果
属于黑名单
S380
给出风险提示信息，并按照用户根据风险提示信息的选择对浏览器进程的创建行为进行拦截

图 3

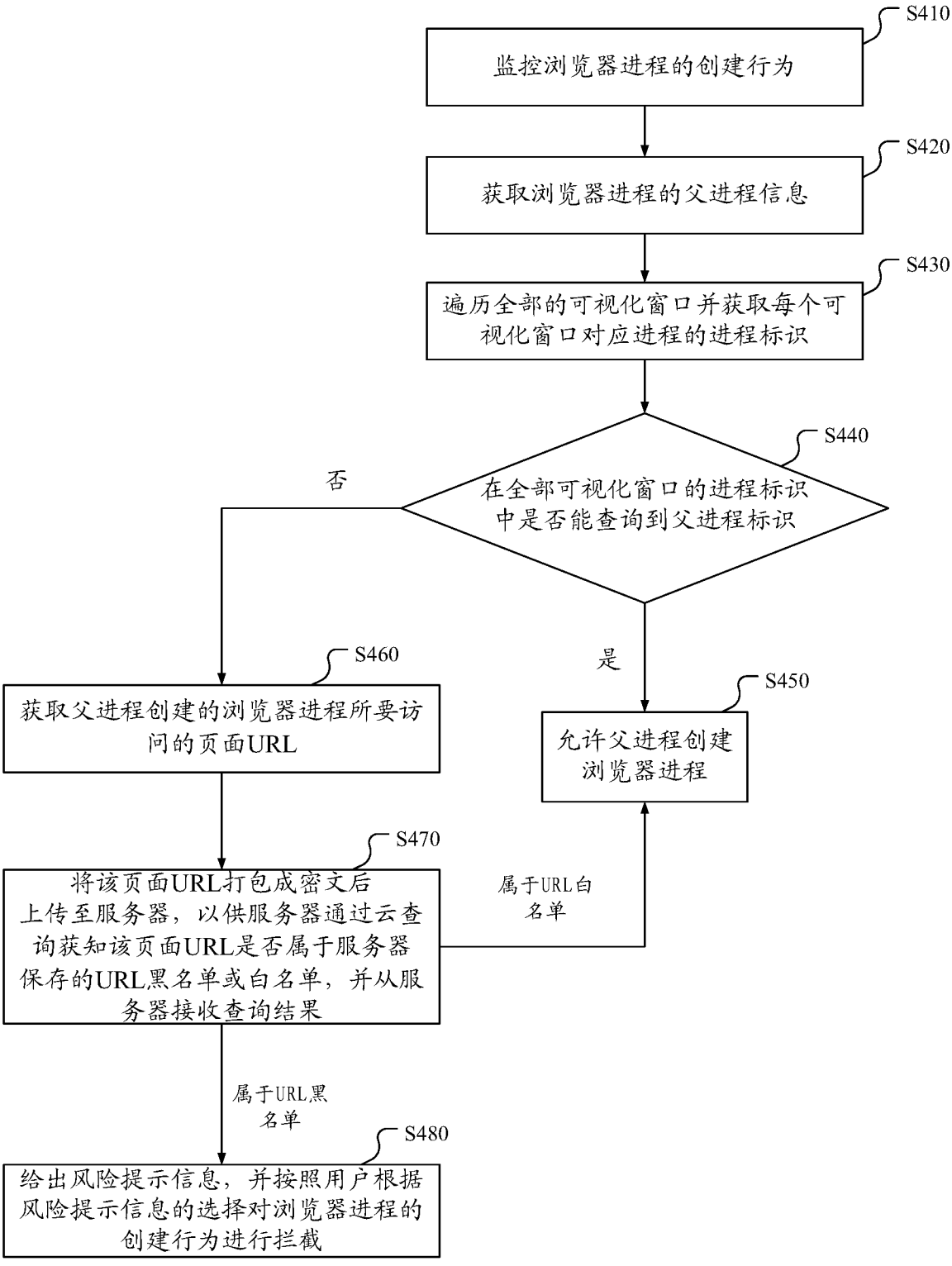
S410
监控浏览器进程的创建行为
S420
获取浏览器进程的父进程信息
S430
遍历全部的可视化窗口并获取每个可视化窗口对应进程的进程标识
S440
在全部可视化窗口的进程标识中是否能查询到父进程标识
否
是
S460
获取父进程创建的浏览器进程所要访问的页面URL
S450
允许父进程创建浏览器进程
S470
将该页面URL打包成密文后上传至服务器，以供服务器通过云查询获知该页面URL是否属于服务器保存的URL黑名单或白名单，并从服务器接收查询结果
属于URL白名单
属于URL黑名单
S480
给出风险提示信息，并按照用户根据风险提示信息的选择对浏览器进程的创建行为进行拦截

图 4

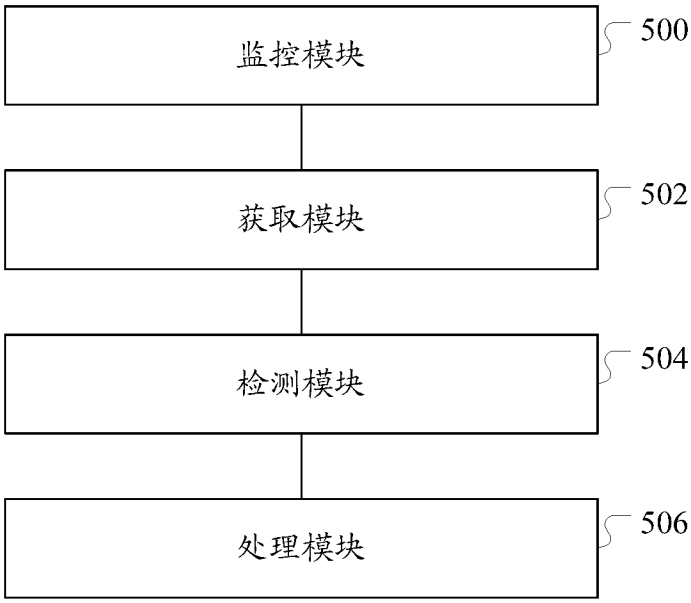

图 5

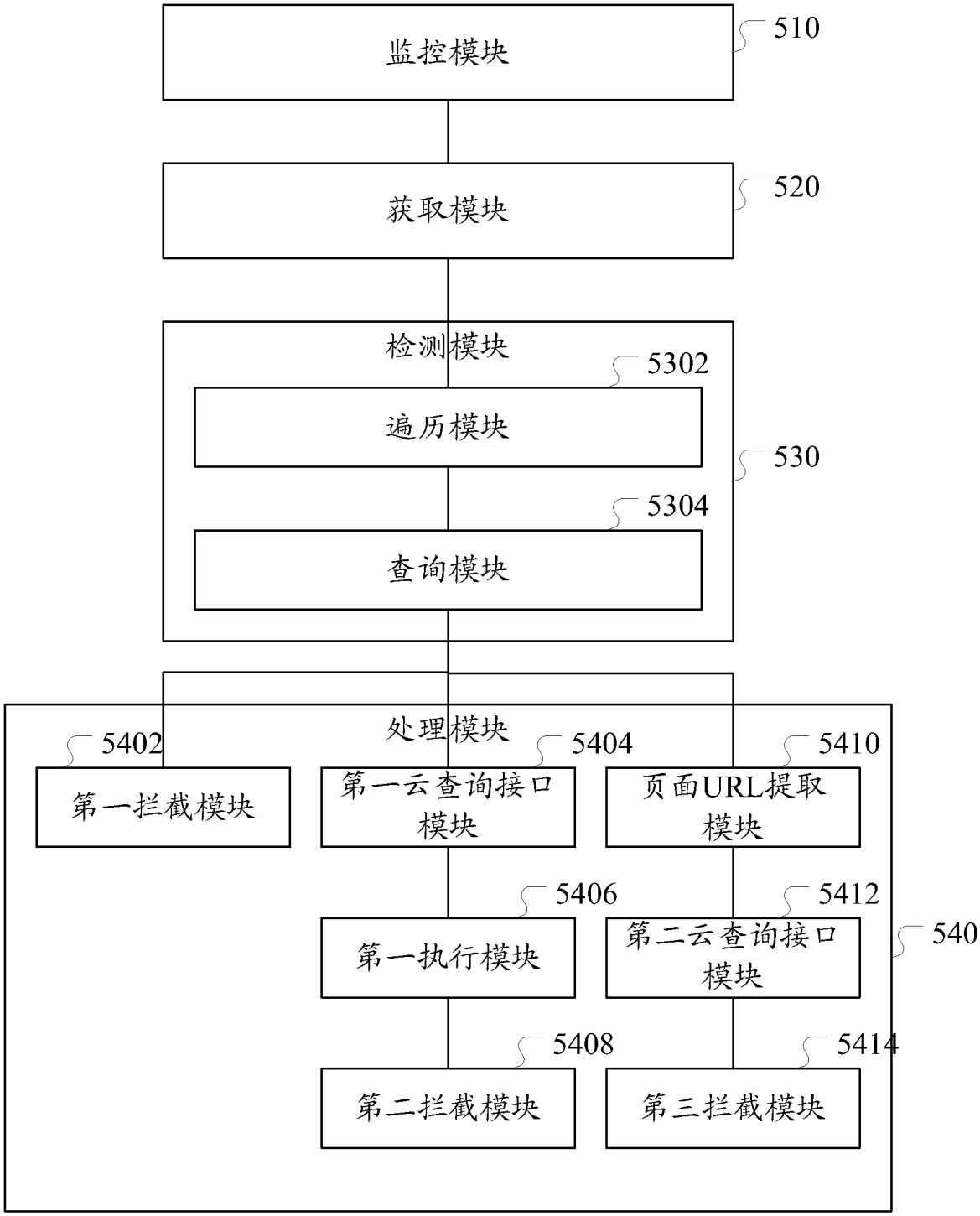
监控模块
510
获取模块
520
检测模块
5302
遍历模块
530
5304
查询模块
处理模块
5402
第一拦截模块
5404
第一云查询接口模块
5410
页面URL提取模块
5406
第一执行模块
5412
第二云查询接口模块
540
5408
第二拦截模块
5414
第三拦截模块

图 6

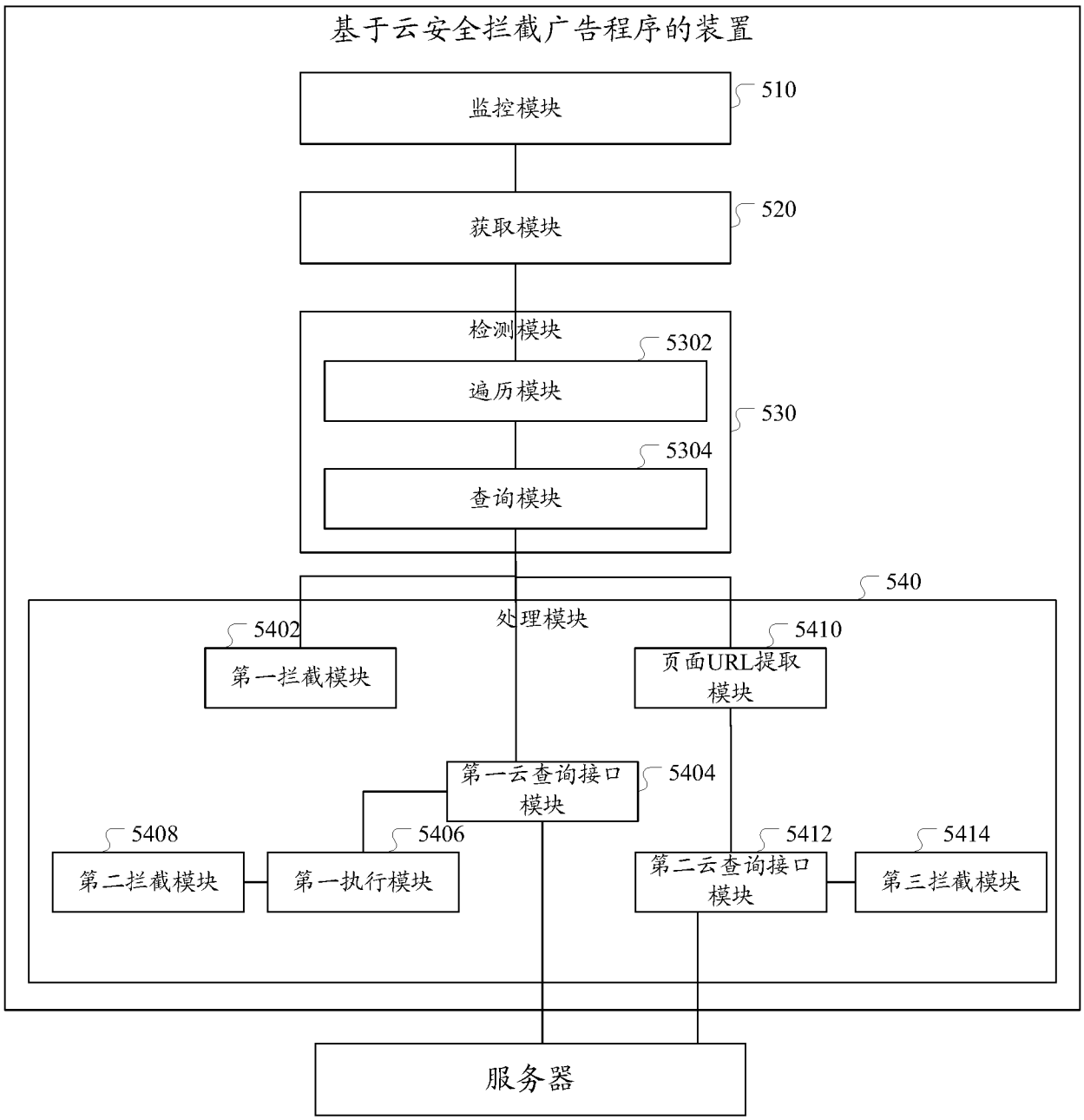
基于云安全拦截广告程序的装置
监控模块
510
获取模块
520
检测模块
5302
遍历模块
530
5304
查询模块
540
处理模块
5402
第一拦截模块
5410
页面URL提取模块
第一云查询接口模块
5404
5408
第二拦截模块
5406
第一执行模块
5412
第二云查询接口模块
5414
第三拦截模块
服务器

图 7

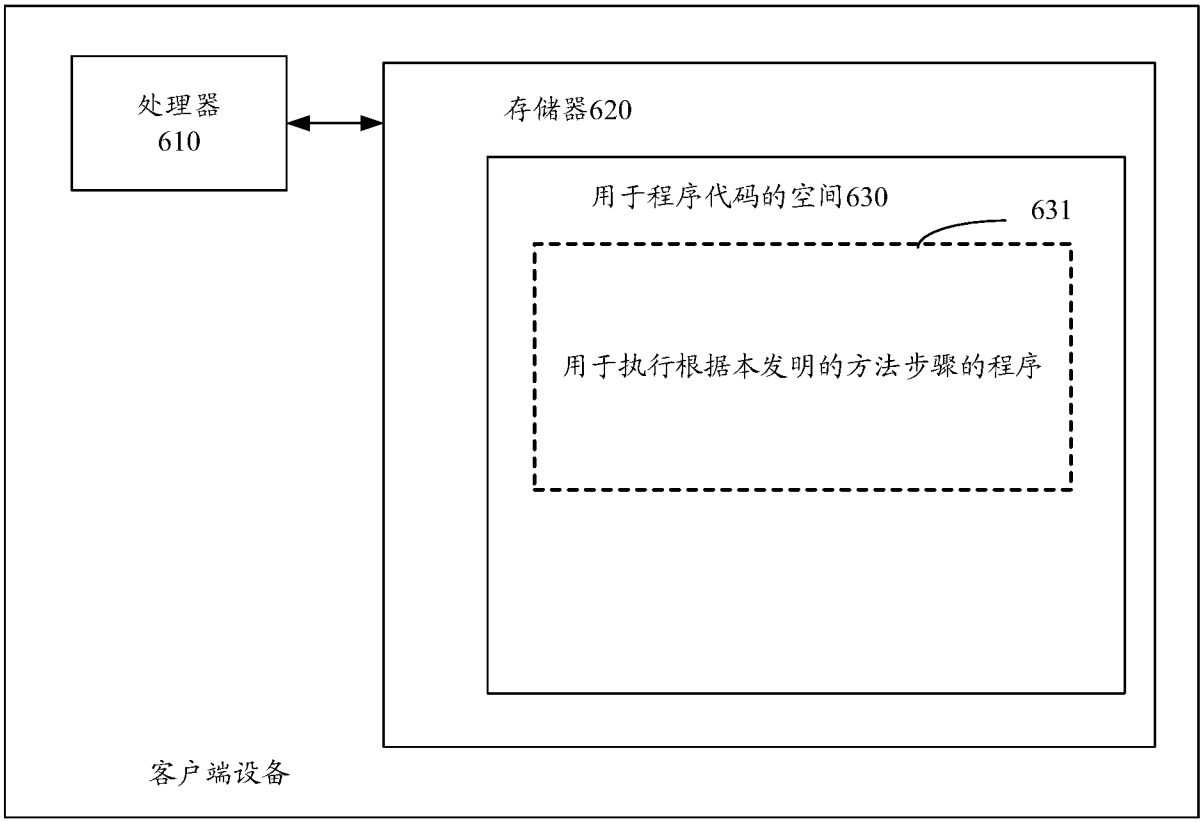
处理器
610
存储器620
用于程序代码的空间630
631
用于执行根据本发明的方法步骤的程序
客户端设备

图 8

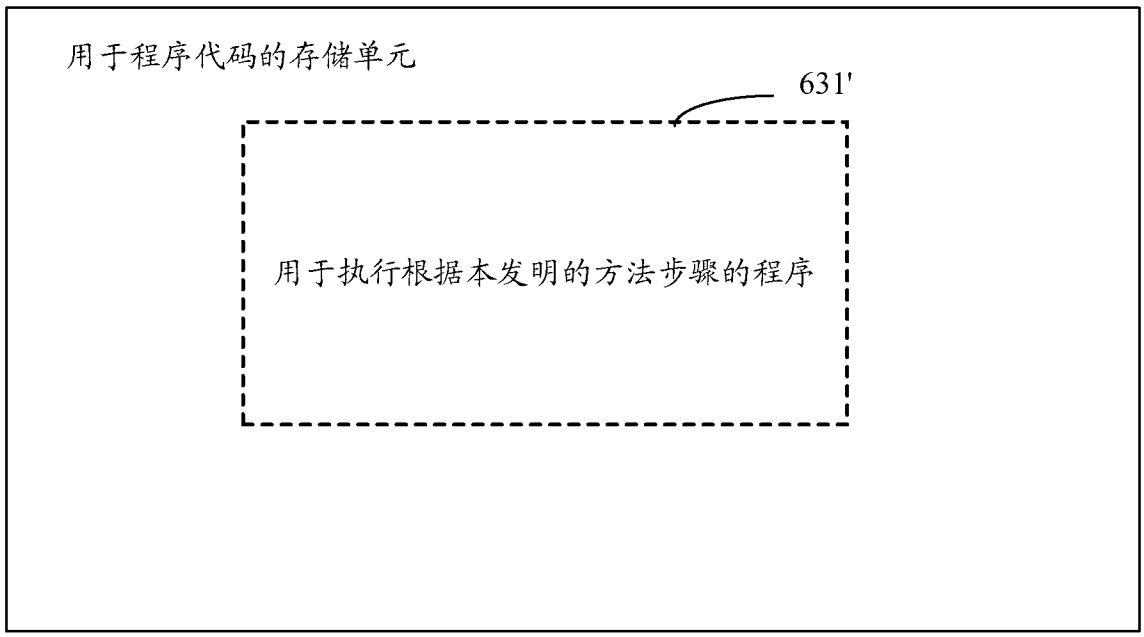
用于程序代码的存储单元
631'
用于执行根据本发明的方法步骤的程序

图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/093286

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/56 (2013.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNTXT; CNABS; VEN; CNKI: parent process, cloud security, intercept, advertisement, start, browser, process, parent, window, creat+, generat+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 103617395 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 05 March 2014 (05.03.2014), the whole document	1-13
A	CN 101350053 A (BEIJING RISING INTERNATIONAL SOFTWARE CO., LTD.), 21 January 2009 (21.01.2009), the whole document	1-13
A	CN 103279707 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 04 September 2013 (04.09.2013), the whole document	1-13
A	CN 103077353 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 01 May 2013 (01.05.2013), the whole document	1-13
A	CN 1925494 A (BEIJING INSTITUTE OF TECHNOLOGY), 07 March 2007 (07.03.2007), the whole document	1-13

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 February 2015 (13.02.2015)	**18 March 2015 (18.03.2015)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **WANG, Yue** Telephone No.: (86-10) **62089109**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2014/093286

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103617395 A	05 March 2014	None	
CN 101350053 A	21 January 2009	JP 2011501280 A	06 January 2011
		WO 2009049556 A1	23 April 2009
		US 2010306851 A1	2 December 2010
CN 103279707 A	04 September 2013	None	
CN 103077353 A	01 May 2013	None	
CN 1925494 A	07 March 2007	CN 100571276 C	16 December 2009

国际检索报告

国际申请号
PCT/CN2014/093286

A. 主题的分类

G06F 21/56 (2013.01) i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F, H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNTXT;CNABS;VEN;CNKI:浏览器，进程，窗，父进程，云安全，拦截，广告，创建，生成，启动，browser, process, parent, window, creat+, generat+

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 103617395 A (北京奇虎科技有限公司 等) 2014年 3月 5日 (2014 - 03 - 05) 全文	1-13
A	CN 101350053 A (北京瑞星国际软件有限公司) 2009年 1月 21日 (2009 - 01 - 21) 全文	1-13
A	CN 103279707 A (北京奇虎科技有限公司 等) 2013年 9月 4日 (2013 - 09 - 04) 全文	1-13
A	CN 103077353 A (北京奇虎科技有限公司 等) 2013年 5月 1日 (2013 - 05 - 01) 全文	1-13
A	CN 1925494 A (北京理工大学) 2007年 3月 7日 (2007 - 03 - 07) 全文	1-13

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2015年 2月 13日	2015年 3月 18日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国 传真号 (86-10)62019451	王越 电话号码 (86-10)62089109

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2014/093286

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	103617395	A	2014年 3月 5日		无		
CN	101350053	A	2009年 1月 21日	JP	2011501280	A	2011年 1月 6日
				WO	2009049556	A1	2009年 4月 23日
				US	2010306851	A1	2010年 12月 2日
CN	103279707	A	2013年 9月 4日		无		
CN	103077353	A	2013年 5月 1日		无		
CN	1925494	A	2007年 3月 7日	CN	100571276	C	2009年 12月 16日