(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
2013 年 12 月 12 日 (12.12.2013)

WIPO | PCT

(10) 国际公布号
WO 2013/181982 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2013/075472

(22) 国际申请日: 2013 年 5 月 10 日 (10.05.2013)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201210189695.3 2012 年 6 月 8 日 (08.06.2012) 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 14 号兆维大厦 4 层东侧单元, Beijing 100016 (CN)。

(72) 发明人: **刘海粟 (LIU, Haisu)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 **张聪 (ZHANG, Cong)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 **熊昱之 (XIONG, Yuzhi)**; 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: **北京市隆安律师事务所 (BEIJING LONGAN LAW FIRM)**; 中国北京市朝阳区建国门外大街 21 号北京国际俱乐部 188 室, Beijing 100020 (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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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,

[见续页]

(54) **Title**: METHOD, DEVICE AND SYSTEM FOR IDENTIFYING ABNORMALITY OF NETWORK BEHAVIOR OF PROGRAM

(54) **发明名称**: 一种识别程序的网络行为是否异常的方法、装置及系统

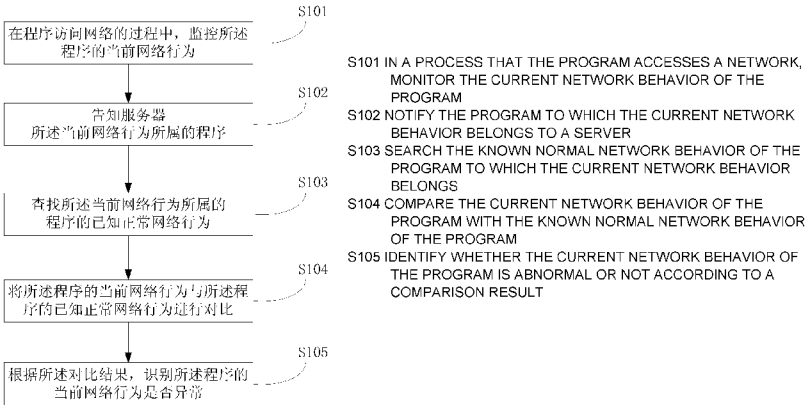


图 1 / FIG. 1

(57) **Abstract**: Disclosed are a method, a device and a system for identifying the abnormality of the network behavior of a program. The method comprises: in a process that the program accesses a network, monitoring the current network behavior of the program; notifying the program to which the current network behavior belongs to a server; searching the known normal network behavior of the program to which the current network behavior belongs; comparing the current network behavior of the program with the known normal network behavior of the program; and identifying whether the current network behavior of the program is abnormal or not according to a comparison result. By means of the present invention, the problem that a virus appearing newly or varying newly cannot be searched and killed in time can be solved.

(57) **摘要**: 本发明公开了一种识别程序的网络行为是否异常的方法、装置及系统，其中所述方法包括：在程序访问网络的过程中，监控所述程序的当前网络行为；告知服务器所述当前网络行为所属的程序；查找所述当前网络行为所属的程序的已知正常网络行为；将所述程序的当前网络行为与所述程序的已知正常网络行为进行对比；根据所述对比结果，识别所述程序的当前网络行为是否异常。通过本发明，可以避免对于新出现或新变种的病毒不能及时进行查杀的问题。

WO 2013/181982 A1

RW, SD, SL, 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, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

一种识别程序的网络行为是否异常的方法、装置及系统

技术领域

本发明涉及计算机技术领域，尤其涉及一种识别网络行为是否异常的方法、装置及系统。

背景技术

随着当前互联网技术的飞速发展与上网成本的普遍降低，互联网已经成为了大多数普通民众日常生活中不可或缺的一个重要组成部分。但是一些天才的程序员为了表现自己和证明自己的能力或者其他方面（如政治，军事，宗教，民族，专利等）的需求，往往会编写出一些影响电脑正常运行的病毒程序，从而使得客户并不能实现自己上网的目的，甚至会使得整个系统出现瘫痪。因而，网络安全就成为了现今关注的焦点。

现有技术中，云安全成为了目前各安全厂商解决个人计算机网络安全问题的首选方案。云安全是通过网状的大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息，推送到服务端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。也就是说安全规则全部由安全厂商来在服务器中来处理完成。这样做虽然会减轻用户端的配置难度和运行负担，但是云安全这一新生事物在带来的诸多便捷与实惠的同时，也存在以下缺陷：

云安全查杀是采用传统的查杀方式，因此对于没保存在数据库中的网络行为只能是一律作为正常网络行为放行，而这些放行的网络行为中，很有可能是新出现或新变种的病毒，但由于数据库的更新都需要一定的时间，所以云安全查杀不能及时将这些不安全网络行为拦截，进而会对系统造成威胁。也就是说，采用传统的云安全查杀方式，对于新出现或新变种的病毒不能及时进行查杀。

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或者减缓上述问题的识别程序的网络行为是否异常的方

法、装置及系统。

根据本发明的一个方面，提供了一种识别程序的网络行为是否异常的方法，包括：在程序访问网络的过程中，监控所述程序的当前网络行为；告知服务器所述当前网络行为所属的程序；查找所述当前网络行为所属的程序的已知正常网络行为；将所述程序的当前网络行为与所述程序的已知正常网络行为进行对比；根据所述对比结果，识别所述程序的当前网络行为是否异常。

根据本发明的另一个方面，提供了一种识别网络行为是否异常的装置，包括：监控单元，用于在程序访问网络的过程中，监控所述程序的当前网络行为；告知单元，用于告知服务器所述当前网络行为所属的程序；查找单元，用于查找所述当前网络行为所属的程序的已知正常网络行为；对比单元，用于将所述程序的当前网络行为与所述程序的已知正常网络行为进行对比；识别单元，用于根据所述对比结果，识别所述程序的当前网络行为是否异常。

依据本发明的再一个方面，提供了识别网络行为是否异常的系统，包括：客户端，用于在程序访问网络的过程中，监控所述程序的当前网络行为；告知服务器所述当前网络行为所属的程序；服务器， 用于查找所述当前网络行为所属的程序的已知正常网络行为；将所述程序的当前网络行为与所述程序的正常网络行为进行对比；识别所述程序的当前网络行为是否异常。

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服务器上运行时，导致所述服务器执行根据权利要求 1-11 中的任一个所述的识别程序的网络行为是否异常的方法。

根据本发明的再一个方面，提供了一种计算机可读介质，其中存储了如权利要求 24 所述的计算机程序。

本发明的有益效果为：

在程序访问网络的过程中，监控程序的当前网络行为，告知服务器所述当前网络行为所属的程序，也就是说，本发明实施例，通过告知服务器当前的网络行为是属于哪个程序的，进而可以查找到与该程序对应的已知正常网络行为。将监控到的程序的当前网络行为与查找到的该程序的正常网络行为进行对比，进而根据对比的结果，识别出当前程序的网络行为是

否异常。由此可见，由于得知了当前的网络行为是属于哪个程序的，所以只要将该程序当前的网络行为与该程序的正常网络行为进行对比就可以将该程序的异常网络行为都识别出来，因此，即便是针对程序的新病毒或变种病毒（以前不知道的病毒），由于其与正常网络行为肯定是不同的，所以也能通过本发明实施例及时识别出来，进而在一定程度上解决了对新出现或新变种的病毒不能及时查杀的问题。

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 示意性地示出了依据本发明一个实施例的识别程序的网络行为是否异常的方法的流程图；

图 2 示意性地示出了依据本发明一个实施例的识别程序的网络行为是否异常的方法的流程图；

图 3 示意性地示出了依据本发明一个实施例的识别程序的网络行为是否异常的装置的示意图；

图 4 示意性地示出了依据本发明一个实施例的识别程序的网络行为是否异常的系统的示意图；

图 5 示意性地示出了用于执行根据本发明的方法的服务器的框图；以及

图 6 示意性地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。

具体实施例

下面结合附图和具体的实施方式对本发明作进一步的描述。

本发明人经过大量的研究和分析发现，现有技术的安全防御系统通常

包含本地防御或网络防御两种独立的方式，但客户端和服务器的互动比较少，也即本地侧和网络侧的互动比较少。例如，如果一个程序的本地行为没有恶意，则客户端不会进行拦截，此时，客户端也不会提供给网络一侧任何信息。因此服务器只能根据现有数据库的数据来进行判断，比如，当前程序的网络行为是要访问某个URL，服务器根据数据库记录能够查找到该URL是合法的，那么就放行；或者根据数据库能够查找到该URL是不合法的，那么就拦截；对于既不能判断是合法的，也不能判断是不合法的，就只能将其放行。

但是，在实践中很多链接并不能被及时收集到数据库，而且病毒更新很频繁，新病毒层出不穷，因此很多恶意URL很有可能还未被及时收集到服务器的数据库中，进而对于这些恶意链接，服务器也只能将其放行。这样，就带来了以下问题：对于新出现的或变种的病毒仍然采用所说的传统查杀方式，就会由于病毒库更新不及时而不能得到及时查杀，甚至病毒作者只要变换IP地址或域名等信息就可以逃脱查杀，进而威胁整个系统。

本发明实施例对程序的当前网络行为进行监控，并告知当前网络行为所属的程序具体是哪个程序，进而根据之前收集到的信息，可以查找到该程序的正常网络行为，将该程序的当前网络行为与查找到的该程序的正常网络行为进行对比，根据对比结果识别出该程序的当前网络行为是否异常。因此，即便是针对程序的新病毒或变种病毒（以前不知道的病毒），由于其与正常网络行为肯定是不同的，所以也能通过本发明实施例的技术方案及时识别出来，进而在一定程度上可以避免对于新出现或新变种的病毒不能及时进行查杀的问题，提高了查杀率。

参见图1，其为本发明提供的一种识别网络行为是否异常的方法实施例流程图，本发明实施例的具体实施方式如下：

S101：在程序访问网络的过程中，监控所述程序的当前网络行为；

需要说明的是，程序是一个普通的文件，是一个机器代码指令和数据的集合，是一个静态的概念。进程是程序在计算机上的一次执行过程，是一个动态的概念。同一个程序可以同时运行于若干个数据集合上，也就是说同一程序可以对应多个进程。网络行为是由运行中的程序（也即进程）所发起的。程序的当前网络行为，也即是由属于该程序的进程所发起的网络行为。

为了便于理解此步骤，首先简单介绍一下网络行为。网络行为可以理解为需要通过网络进行的各种行为，种类繁多，例如包括 HTTP（hypertext transport protocol，超文本传送协议）访问（常见的有下载文件或上传信息），SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）请求（收发电子邮件），DNS（Domain Name System，域名系统）请求（解析域名对应的 IP 地址等信息）等等。

其次，再介绍一下应用程序访问网络的流程：通常一个程序如果需要连接网络，需要通过操作系统（如 Windows）提供的 API（Application Program Interface，应用程序接口）接口发送连接网络的请求，操作系统接收到应用程序的这种网络请求后，会接收应用程序要发送的数据，并对接收到的数据进行封装，之后将封装的数据发送给物理设备（如网卡等），最后由硬件设备将数据传出。

基于以上应用程序访问网络的流程，在该流程的任何一环节对网络行为的信息进行截获都可以实现监控程序的当前网络行为的目的。具体监控的实施方式可以但不限于以下几种方式：通过在客户端注册协议驱动、创建与操作系统相似的过滤驱动、利用操作系统提供的应用程序编程接口函数（hook 函数）截获当前网络行为的信息、接管程序调用网络编程接口函数（Winsock）的请求或者是利用注册防火墙回调等方式，截获程序的当前网络行为的信息。下面进行具体的说明：

在应用程序访问网络的过程中，操作系统在处理相关数据的时候，会使用一些协议驱动和过滤驱动来获取网络行为的数据，所以可以注册协议驱动或创建与操作系统使用的过滤驱动相似的过滤驱动，进而获取到网络行为的数据。具体实施方式可以是：向 NDIS(Network Driver Interface Specification，网络驱动程序接口规范)注册协议驱动，也可以在 Afd.sys (Ancillary Function Driver for winsock， winsock 的辅助功能驱动) 驱动设备栈、Tdi.sys(Transport Dispatch Interface，传输分配接口)驱动设备栈或 Tcpip.sys （Transmission Control Protocol / Internet Protocol，传输控制/网络通讯协议）驱动设备栈上增加与操作系统相似的过滤驱动。

另外监控还可以通过以下方式来实现：利用 hook 函数将网络行为的数据截获。具体实施方式可以是：用 Hook 函数截获 Windows SSDT（System Services Descriptor Table，系统服务描述符表）中内核提供的与设备通信接口 NtDeviceIoControl 函数，获取所有应用程序与设备通信的数据，过

滤其中对 Afd.sys 发送的请求；还可以是利用 Hook 函数截获 Tcpip.sys 驱动提供的服务函数或者 NDIS.sys 导出的接口等，通过上述方式来监控程序的网络行为。

当然，也可以通过以下方式来对程序的网络行为进行监控：根据 Windows 的 LSP（Layered Service Provider，分层服务提供商），可以将 LSP 机制进行扩展，使用自己的 DLL 文件接管所有应用程序调用 Winsock 的请求后，再转发到 Windows 自身的 mswsock.dll 中去，或者也可以是向 Windows 系统 IP 设备驱动发送 IOCTL_IP_SET_FIREWALL_HOOK 注册防火墙回调等等。

在实践中，监控程序的网络行为数据时，可以根据实际情况选择以上不同的方式，当然监控网络行为数据也不限于以上所列举的方式。

S102：告知服务器所述当前网络行为所属的程序；

在传统的查杀方式中，服务器并不知道当前网络行为是由哪个程序发起的。而本发明实施例告知了服务器当前的网络行为具体属于哪个程序，因此，对于当前的网络行为服务器可以得知其是由哪个程序发起的，进而可以对当前网络行为进行后续处理，也即本发明实施例中的将当前网络行为与正常网络行为进行对比，并识别其是否异常。

具体告知服务器当前网络行为所属的程序的方式可以是：客户端向服务器发送当前网络行为的信息以及当前网络行为所属程序的标识。在实施过程中，发送的方式可以有多种，本发明实施例提供的方式可以是，为程序的当前网络行为的信息添加网络防御标签，该网络防御标签包括当前网络行为所属的程序的标识，之后向服务器发送带有网络防御标签的当前网络行为的信息。需要说明的是，网络防御标签是为属于当前程序的进程所附加的，只要是属于同一程序的进程所附加的网络防御标签是一样的，也就是说为同一程序的网络行为的信息所添加的网络防御标签是一样的。当进程发起网络行为的时候，就可以将当前的网络行为的数据信息和添加的网络防御标签一同发送给服务器。

该网络防御标签一方面包括了当前网络行为所属程序的标识，程序的标识用来确定当前程序的身份，也即用来告知服务器当前网络行为是由哪个程序发起的；另一方面，该网络防御标签也用来告知服务器凡是添加有该标签的网络行为是需要经过特殊处理的，也就说需要通过本发明实施例的方式来识别其是否为异常的网络行为。在接收到带有网络防御标签的当

前网络行为的信息后，服务器对获得的数据信息进行解析，进而可以获知程序的当前网络行为以及其所属程序的标识。因此服务器根据当前网络行为所属程序的标识就可以知道当前网络行为是哪个程序所发出的。具体实施的过程中，可以根据标识的具体内容区分出不同程序的当前网络行为。例如标识的内容可以是“game1”、“jishitongxun1”或者“jishitongxun2”等，而“game1”表示当前的程序为游戏 1，“jishitongxun1”表示当前的程序为即时通讯 1，“jishitongxun2”表示当前的程序为即时通讯 2，进而服务器可以区分出当前的网络行为哪些是游戏 1 程序发出的、哪些是即时通讯 1 程序发出的，以及哪些是即时通讯 2 程序发出的等等。

在具体实施过程中，根据实际需要可以选择将所有当前网络行为所属的程序标识都予以告知，也可以选择只将部分当前网络行为所属的程序标识予以告知。具体如何选择，则可以有多种选择依据。比如根据病毒的流行趋势，来选择某些容易受病毒攻击的程序来进行上述处理，进而可以对这些程序进行有针对性的查杀。

具体而言，根据病毒的流行趋势，判定哪些程序是容易受到病毒攻击的程序或容易被病毒利用的程序，对这些易受病毒攻击的程序或容易被病毒利用的程序进行分类。将这些类别的程序作为特定类别的程序，如果确定当前程序是某一特定类别程序，则告知服务器当前网络行为所属程序的标识。例如，经过一段时间的分析，发现现阶段针对即时通讯软件的病毒不断增多，因此即时通讯 1 或即时通讯 2 等即时通讯类软件程序可能就是目前易受病毒攻击的程序。根据实际情况，可以对这些程序进行细致或粗略的划分。如果划分的比较细致，那么每个程序自身就可以是一类，例如即时通讯 1、即时通讯 2、浏览器 1、浏览器 2、等等，都可以作为划分的类别。而如果划分比较粗略的话，那么可以将程序划分为游戏类、即时通讯类、浏览器类等等，比如，游戏 1 就属于游戏类，即时通讯 1、即时通讯 2 就属于即时通讯类，浏览器 1、浏览器 2 就属于浏览器类等等，之后根据这些预先分好的类别来确定哪些当前网络行为所属的程序信息需要告知，具体方式如下：

当本地计算机（即客户端）启动一个程序后，首先会将该程序的数字签名、文件名、文件路径、原始名等多方面的属性信息发送给服务器，服务器接收客户端发送的该程序的属性信息，然后提取这些属性信息的特征，经过分析这些属性信息的特征来确定该程序是否属于上述预先划分的

特定类别的程序，如果是，则发送指令给客户端，指示客户端将监控到的该程序的当前网络行为的信息以及当前网络行为所属程序的标识告知给服务器。例如，计算机在本地启动了即时通讯 1 程序，并将其数字签名、文件名等信息发送给服务器，服务器对这些信息的特征进行分析后，确定该程序属于特定类别（也即前述根据病毒的流行趋势划分的程序类别）中的即时通讯 1 程序，那么发送指令给客户端，指示客户端将即时通讯 1 程序的当前网络行为的信息以及当前网络行为所属程序的标识（如“jishitongxun1”）发送给服务器，进而服务器就可以得知当前的网络行为是由即时通讯 1 程序发起的，即告知服务器当前网络行为所属的程序。同样，如果本地计算机启动了即时通讯 2 程序，利用同样的方法服务器可以得知当前的网络行为是由 MSN 程序发起的。

当然如果预先划分的类别比较粗略的话，例如，划分为游戏类、即时通讯类和浏览器等几大类，经过分析确定本地启动的即时通讯 1 程序是属于预置类别中的即时通讯类，那么服务器会发送指令给客户端，指示客户端告知当前网络行为所属的程序，进而客户端根据指令将即时通讯 1 程序的当前网络行为的信息以及当前网络行为所属程序的标识（如“jishitongxun1”）发送给服务器。

在选择将哪些当前网络行为所属程序的标识需要告知时，除了上述方式，还可以是以下方式：在预先划分的类别里再选择几种当前最容易受病毒攻击的类别或容易被病毒利用的类别，作为特定类别，如果经过分析程序是属于这几种特定类别里的某一种，那么指示客户端告知当前网络行为所属的该程序的标识。例如，现有的预置分类有 10 种类别，而其中的游戏类、浏览器类及即时通讯类是最容易受攻击的，那么将这三中类别的程序作为特定类别，当确定当前程序属于游戏类、浏览器类或即时通讯类中的某一类时，指示客户端告知当前网络行为所属的程序的标识，如果经过分析发现当前的程序虽然属于预先分类里的类别，但是并不属于上述三类特定类别里的任何一类，那么就不发送指令，进而客户端也不会告知当前网络行为所属的程序的标识。此时只要对当前的程序进行传统的查杀即可。如，本地启动了即时通讯 1 程序，经过分析，发现即时通讯 1 是属于预先分好的类别里的程序，同时是属于特定类别的即时通讯类，那么就指示客户端告知当前网络行为所属程序的标识（如 jishitongxun1”）。而如果客户端启动了 game1 程序，game1 是属于预先分类里的类别，但是其并

不属于上述三类特定类别中的任何一类，那么就不必指示客户端告知当前网络行为所属的程序的标识。当然，哪些当前网络行为所属程序的标识需要告知，选择的依据还有其它很多种，本发明不做限制。

而对于另外一些不属于特定类别的程序（通过检测其数字签名、文件名、文件路径等信息，判断出该程序不具有特定类别的程序所具有的特征，也即，这些程序不能被归到特定类别里），可以不采用本发明实施例的方式进行处理，而对其采用传统方式进行查杀，具体方式为：

针对当前程序的本地行为，在客户端检测其是否是已知的恶意文件，是否释放出了其他文件，是否修改了敏感位置注册表值，是否修改了重要系统文件等等，也即判断其行为是否为恶意，如果是恶意行为，则在客户端将其拦截。针对当前程序的网络行为，主要通过程序所访问的网页的标识信息如：URL（Uniform Resource Locator，统一资源定位符）地址、域名，host（主机），端口或IP（Internet Protocol，网络协议）地址等信息，判断其是否存在危险。

当前，除了上述传统查杀方式外，对于这些不属于特定类别（即认为不需要通过程序的已知正常网络行为进行对比来判断当前网络行为是否异常）的程序，还可以采用其他的各种已知查杀方式，甚至不需要也可以不查杀，本发明对此并没有限制。

S103：查找所述当前网络行为所属的程序的已知正常网络行为；

在本发明实施例中，查找当前网络行为所属的程序的已知正常网络行为可以采用以下方式：预先收集多种程序的正常网络行为，并建立程序的标识及其正常网络行为之间的对应关系；根据当前网络行为所属程序的标识，查找该程序的标识对应的正常网络行为，将查找到的正常网络行为作为所述程序的已知正常网络行为。

程序的正常网络行为可以通过各种方式予以收集。比如，可以监控已有程序的网络行为，通过大量的分析总结归纳出某些程序的正常网络行为是什么；也可以通过服务商或者网站所属公司获知某些程序的正常网络行为等等；还可以人工收集一些程序的网络行为数据得到这些程序的正常网络行为，等等，本发明对预先收集程序的已知正常网络行为的方式并没有限制。例如一种常见的收集方式是，一个程序正常的网络行为并不多，比如访问某一公司的官方网站或固定IP地址。由于IP和域名在某个公司购买并使用后，一般情况下，公司都会对其IP和域名进行维护和管理。那

么程序连接该公司的官方地址或其相关的地址（比如程序中存在的图片、广告或合作公司的域名或 IP 地址）的时候，出于对正常程序开发公司的信任，也同时可以信任这些地址。这些地址可以通过在测试正常程序时，同时运行 Wireshark 等专业网络监控工具来获取到。获取到这些地址后，服务器就可以将程序访问这些可信任地址的网络行为作为正常网络行为而保存。

由于在 S102 步骤中，已经将当前网络行为所属的程序是哪个程序，通过程序标识告知了服务器，而该标识与程序的正常网络行为是对应的，因此通过该标识可以查找到当前程序所对应的正常网络行为。例如，服务器通过告知的程序标识得知当前的网络行为是由即时通讯 1 程序发起的，那么相应的就可以从预知的所有正常网络行为中查找到即时通讯 1 程序所对应的正常网络行为。

当然，在具体实施的过程中，可以预先收集能获知的所有程序对应的正常网络行为，也可以根据当前的实际情况只收集当前比较容易受到病毒攻击的一些程序对应的的正常网络行为。例如，当前一段时间，即时通讯 1、即时通讯 2 等程序比较容易受病毒攻击，那么就预先收集即时通讯 1、即时通讯 2 等程序所对应的所有正常网络行为。也就是说，只有一些容易受病毒攻击的程序所对应的正常网络行为会被收集而对于那些不易受病毒攻击的程序则采用传统方式查杀，不必预先收集其正常网络行为，这样也减少了对系统资源的过多占用。

S104: 将所述程序的当前网络行为与所述程序的已知正常网络行为进行对比。

由于在步骤 S101 中已经监控到了程序的当前网络行为，在步骤 S103 中又通过该程序的标识查找到了该程序对应的所有正常网络行为，因此可以将监控到的该程序的当前网络行为与查找到的该程序对应的正常网络行为进行对比。

前文已经说明，服务器可能只是预知容易受病毒攻击的某些类程序的正常网络行为，而且类别在预先划分时可能比较细致，也可能比较粗略。因此，服务器预存的正常网络行为也可能会根据分类的细致与粗略而不同。如果分类比较细致，每一个程序可能就会划分为一类，例如，即时通讯 1 被划分为单独的一类，此时服务器预知的正常网络行为也会比较具体（如为即时通讯 1 程序的正常网络行为）。如果客

户端启动了即时通讯 1 程序，服务器通过分析其数字签名、文件名等信息，确定该程序为上述特定类别里的程序，那么此时就可以指示客户端告知即时通讯 1 程序的当前网络行为的信息以及即时通讯 1 程序的标识属于哪个程序，进而，客户端将当前即时通讯 1 程序的网络行为的数据以及即时通讯 1 程序的标识（如“即时通讯 1”）一并发送给服务器，服务器根据该标识就知道上传的当前网络行为是属于即时通讯 1 程序的（即即时通讯 1 程序发起的），于是就可以查找到预知的即时通讯 1 程序对应的正常网络行为，并将即时通讯 1 程序的当前网络行为与预知的即时通讯 1 程序对应的正常网络行为进行对比。

而如果类别划分比较粗略，可能只是笼统的划分为游戏类、或即时通讯类、浏览器等几大类等，这时，同样通过上述的分析判断出即时通讯 1 程序是对应于即时通讯类，那么就可以利用同样的方法将即时通讯 1 程序的当前网络行为与预知的即时通讯类的正常网络行为进行对比。

当然，也可以是选择预先分好的类别里的其中最容易受攻击的几类作为特定类别。例如：在预先分好的多种类别里当前只有游戏类、即时通讯类、浏览器类是最容易受攻击的三个特定类别，那么经过判断只有当前程序属于这三类中的任何一类时，才将程序的当前网络行为与预知的正常网络行为做对比，而属于这三类之外的其它类别时，则无需进行对比。

S105：根据所述对比结果，识别所述程序的当前网络行为是否异常。

根据上述的对比结果，最终识别出网络行为是否异常。如果对比的结果不一致，那么认为该程序的网络行为为异常网络行为；如果对比结果一致，则认为该程序的网络行为为正常网络行为。

对于识别出为异常的网络行为，在具体实现的过程中可以根据不同的情况进行不同的处理。其中一种情况可以是，通过现有的查杀病毒的方式对当前的异常网络行为进行进一步判断，如果可以确定当前网络行为是非恶意的，那么可以先暂停其网络连接，并向用户发送提示信息，告知用户该程序为异常，由用户做出最终选择，如果用户选择拦截，那么该网络行为将会被彻底阻止。当然，为了系统的安全，并且在用户预先的指示下（比如用户在客户端预先设定某一类型的异常网络行为可以直接拦截），则直接将某种类型的该异常网络行为进

行拦截。例如：本地启动一个程序，该程序的当前网络行为是从网络资源中下载某一文件，该网络行为通过本发明实施例的方式已经识别出是一个异常网络行为。而且通过现有的病毒查杀方法判断出了该下载的文件本身并不是病毒，也就是说，当前的异常网络行为并非是恶意的。假设该文件表明自身只是一个视频播放软件程序，对于客户来说，下载该文件的目的仅仅是想获取一个视频播放器，而且通过文件名等信息也相信该文件只是一个视频播放软件程序，但是当用户去运行该软件程序的时候，发现该程序不仅仅安装了视频播放器，同时也安装了一个浏览器，和其它一些用户并不需要的软件，也就是说在用户不知情的情况下，该程序文件欺骗用户额外安装了其它的软件，而该文件里的其它用户所不需要的软件，也只是程序的发明者为了达到推广的目的而添加的，本身也并非是恶意的。本发明实施例对这种非恶意的异常网络行为所采用的方式是，只将当前的异常网络行为暂停或拦截。当然，当前网络行为并非是恶意的情况有很多中，上述只是通过举例介绍其中的一种。

对于识别出当前网络行为是异常网络行为之后，本发明实施例还提供了另外一种处理方式，具体为：如果程序的当前网络行为是恶意的，并且不确定程序是否为恶意程序，则暂停或拦截程序的全部网络行为。也就是说，识别出当前网络行为为异常，并且通过现有的查杀病毒的方式判断出该异常网络行为是恶意的，例如，该异常网络行为通过连接网络之后会下载病毒程序，但是通过该异常网络行为并不能确定发起该网络行为的程序是否是恶意程序，也就是说该异常网络行为是相对独立的，根据该异常网络行为不能确定其本地行为是否是恶意，那么为了系统整体安全，就将当前恶意网络行为所对应程序的全部网络行为都暂停或拦截。在实际实施的过程中，用户也可以通过手动操作选择只拦截当前的恶意网络行为，而将程序其他的网络行为放行，当然也可以选择将程序的全部网络行为都拦截，甚至有必要的话，也可以选择拦截该程序的全部网络行为和全部本地行为。

当然，识别出当前网络行为是异常网络行为之后，还可以通过以下方式进行处理，具体为：如果所述程序的当前网络行为是恶意的，并且确定所述程序为恶意程序，则暂停或拦截所述程序的全部行为。也就是说，识别出当前网络行为为异常，并且通过现有的查杀病毒的方式判断出该异常

网络行为是恶意的，同时，根据该恶意网络行为可以确定发起该恶意网络行为的程序本身就为病毒程序，那么就将当前恶意网络行为所对应程序的本地行为和网络行为全部暂停或者拦截。例如，当前的恶意网络行为是与病毒服务器进行连接，并且连接之后会上传用户的隐私信息给病毒服务器，而如果要上传用户隐私数据，程序的本地行为首先得获取用户的隐私数据，之后网络行为再将这些数据上传，本地的这种获取用户隐私数据的行为本身就是一种恶意行为，也就是说，通过异常网络行为可以判断出发出该异常网络行为的程序所执行的本地行为也是恶意的，所以可以判断该程序本身就是恶意程序，那么，就将该程序的全部行为，也即本地行为和网络行为全部暂停或拦截。

在具体实施的过程中，到底采用上述哪种方式对异常网络行为进行处理，要根据客户端上传的数据（当前网络行为数据）在命中不同的拦截规则后，根据不同的规则，进行相应的处理。

需要说明的是，本发明实施例可以通过以下方式实现：在客户端预设一个模块用来预存少量程序的已知正常网络行为，当客户端的监控模块监控到程序的当前网络行为时，告知客户端的正常网络行为预存模块该程序是什么程序，进而可以在正常网络行为预存模块对应查找到该程序的正常网络行为，将该程序的当前网络行为与查找到的正常网络行为在客户端进行对比，最终根据对比结果，识别该程序的当前网络行为是否异常。

当然本发明实施例也不限于上述的实现方式，优选的，也可以是由客户端监控程序的当前网络行为，并告知服务器当前网络行为所属的程序，在服务器查找当前网络行为所属的程序的已知正常网络行为，并将程序的当前网络行为与该程序的正常网络行为进行对比，最后根据对比结果，识别出该程序的当前网络行为是否异常。也就是说，以上优选方案中，程序的正常网络行为都预存在服务器，因为经过长期的运营之后，搜集到的程序的正常网络行为会非常多，数据也越来越庞大，而大型服务器的存储空间要远远大于客户端，因此，在服务器侧可以尽可能多的预存程序的正常网络行为，进而可以提高查杀的全面性。同时，对于最新搜集到的正常网络行为，服务器可以及时进行更新，对最新出现的异常网络行为或者病毒在进行对比之后可以及时进行处理。而如果将程序的正常网络行为预存在客户端，查找到程序的正常网络行为之后，将程序的当前网络行为与该程序的正常网络行为在客户端进行对比，不仅由于大量硬盘空间的占用使得

用户机器速度慢，而且，对于更新的正常网络行为，还需要客户端通过联网升级的方式进行更新，因此也就不能及时找出新出现的异常网络行为或者病毒，进而也就不能对新出现的异常网络行为或病毒进行及时处理。

下面再通过一具体实施方式来说明本发明实施例的具体实现方案，请参见图 2，其为本发明提供的一种识别网络行为是否异常的方法具体实施方式流程图。

本地客户端启动某一程序（程序执行），并将该程序的属性信息发送给服务器，其中属性信息包括该程序的数字签名、文件名、文件路径和/或原始名等信息，服务器对数字签名、文件名等属性信息的特征进行检测，经过检测后判断该程序是否具有某类特定类别（如根据当前病毒流行趋势判定是当前一定时间段内容易受到病毒攻击的程序类别和/或容易被病毒利用的程序类别）程序的特征，即是否属于特定类别。如果经过分析判断出该程序不具有特定类别程序的特征，则对该程序进行其他检测（比如采用其它现有的方式查杀）。如果具有某类特定类别程序的特征，则指示客户端监控当前网络行为，并给当前网络行为所对应的进程打上 NDCAT(Network Defender Category，网络防御标签)标签，之后将该标签（即该程序所属类别对应的 NDCAT 标签）及当前网络行为的信息一同发送给服务器。

当接收到带有标签的网络行为的数据时，服务器便可知道当前的网络行为是需要进行特殊处理的，也即需要通过本发明实施例的方式来识别其是否异常，同时服务器根据该标签内包括的当前程序的标识也可以得知当前的网络行为是由哪个程序所发起的。由于服务器预存有带有 NDCAT 标签的进程所属程序的正常网络行为，因此，根据接收到的标签，便可以查找到该标签所对应程序的正常网络行为，并将监控获得的该程序的当前网络行为与查找到的该程序对应的已知正常网络行为进行对比，如果当前网络行为与预存的已知正常网络行为不一致，即认为该网络行为为异常网络行为，可能存在危险，此时可以暂停该程序的网络行为（比如暂停该程序的网络连接），并以某种形式（如弹窗报警）提示给用户，等待用户处理，由用户选择是否将程序的部分或全部网络行为拦截；如果判断与已知网络行为一致，则继续监控其他网络行为。

下面通过一个具体应用程序的例子说明一下本发明实施例具体如

何识别出程序的异常网络行为。

456游戏大厅是一款广受欢迎的在线游戏平台软件，同时由于其虚拟货币与现实货币存在兑换关系，让该游戏平台也成为了许多病毒木马作者下手的对象。病毒木马作者通常是首先搭建一个与456游戏大厅官网非常相似的钓鱼网站，诱骗用户下载其提供的虚假客户端程序。而这个虚假的客户端程序中，病毒木马作者只是修改了正常客户端程序中的一个名为system.ini的配置文件，其余所有可执行文件均为正常。而当游戏客户端程序启动的时候，会读取system.ini配置文件中的信息，并按照对应的网址（下载地址）去检查并下载更新。此时，被修改过的system.ini就将升级程序按照对应的下载地址指向了病毒木马作者自己的服务器。

此种情况下，如果采用传统的云安全查杀方式，由于游戏客户端程序在启动时，只是读取 system.ini 配置文件中的信息，并按照对应的网址去检查并下载更新，其本身一开始并没有恶意的本地行为，所以本地防御不会拦截。而客户端与服务器在传统的查杀过程中，互动比较少。因此，客户端也不会提供给服务器任何信息，所以服务器只会检测被修改过的 system.ini 所指向的网址，由于服务器并不知道这个联网下载的行为是由 456 游戏大厅发起的，所以也肯定不能采用非白即黑的拦截方式，只能采用传统的非黑即白的拦截方式。即，除非下载地址是已知的危险地址，才会拦截，否则便会一律放行。而对于上述升级程序所指向的网址很可能由于病毒库没有及时更新，而没有对其进行收集，这样，就会将上述指向病毒作者自己服务器的联网下载行为放过。

下面具体介绍采用本发明实施例的方式如何识别出上述应用环境中的异常网络行为。如果本地的客户端启动了 456 游戏大厅程序，客户端将会监控 456 游戏大厅程序当前的网络行为，并将该程序的数字签名、文件名、文件路径等信息发送给服务器，服务器通过综合分析这些发送的信息，可以判断出该程序为预置类别里的 456 游戏大厅程序，进而服务器则指示客户端发送该程序的当前网络行为及其所属程序的标识（如“456game”）。通过该标识服务器可以确定当前网络行为是 456 游戏大厅所发起的，而服务器预存有 456 游戏大厅对应的正常网络行为，所以可以根据该标识对应查找到预存的 456 游戏大厅所对应的正常网络行为。将监控到的 456 游戏大厅程序的当前网络行为与正常的网络行为进行对比，发现访问病毒作者自己的服务器的网络行为，并不在已知的正常网络行为中，也即识别出该

网络行为不属于正常的网络行为。此时可暂停或拦截该网络行为，或者也可以根据实际需要暂停或拦截该程序的全部网络行为，当然，如果发现该程序的本地行为也是不安全的，则可以暂停或拦截该程序的全部行为。

通过另外一个应用程序的具体例子也可以看出本发明的效果。暴风影音是国内知名的视频播放器，用户量很大，并且所有程序组件带有北京暴风科技股份有限公司的合法数字签名。

基于对数字签名体系的信任，传统安全软件在识别带有这种合法数字签名的程序时，是直接放行其全部行为的。而这一点也就给了一些病毒可乘之机。

暴风影音的程序组件中带有暴风影音升级程序“BaofengUpdate.exe”，在运行升级时会自动调用同目录下的“Update.dll”进行升级操作。利用这一点，针对暴风影音出现了大量的病毒木马。这些木马一般会释放出两个文件：一个带有有效数字签名的官方版“BaofengUpdate.exe”程序，另一个是病毒作者自己编写的“Update.dll”木马。释放这两个文件之后，“BaofengUpdate.exe”，会自动加载“Update.dll”，并执行其中的恶意代码——下载病毒到本地运行或上传用户的隐私信息。由于是被加载的，所以真正的木马程序“Update.dll”不会出现在进程列表中，而进程列表中出现的“BaofengUpdate.exe”又会因为带有有效的数字签名而被传统安全软件轻易地放过。

下面说明一下针对以上例子，采用本发明实施例的方式如何将病毒识别出来，进而进行查杀。当本地的客户端启动了 BaofengUpdate.exe 程序，客户端将会监控该程序的当前网络行为，并将该程序的数字签名、文件名、文件路径等信息发送给服务器，服务器通过综合分析这些发送的信息，可以判断出该程序为“BaofengUpdate.exe”程序，此时，服务器将指示客户端发送当前网络行为的信息及其所属程序的标识（如“BaofengUpdate”）。进而，客户端为该程序的当前进程打上标签（代表了该程序的标识信息，）并上传至服务器。然后，服务器根据该标识查找到该程序的正常网络行为。一般情况下，如果该升级程序是正常的，则只会访问暴风自己旗下域名的网站。即,只有发起的 DNS 请求的一级域名部分是 baofeng.com 的网络行为是正常的网络行为。

据此，便可以将监控到的带有“BaofengUpdate”标识的程序的当前网络行为（即发起 DNS 请求）与“BaofengUpdate.exe”程序的正常的网络行为

进行对比，只要DNS请求中的一级域名部分不是“baofeng.com”，也即，与正常的网络行为不一致，则认为该请求的网络行为为异常。

通过上述的例子可以看到，本发明实施例通过告知当前网络行为是哪个程序发起的，进而可以将程序的当前网络行为与程序已知的正常网络行为进行对比，最终将不属于该程序正常网络行为的所有异常网络行为都识别出来，从而对于新出现或新变种的病毒可以进行及时查杀，提高了查杀率。

与本发明实施例提供的一种识别网络行为是否异常的方法相对应，本发明实施例还提供了一种识别网络行为是否异常的系统，参见图3，其为本发明提供的一种识别网络行为是否异常的系统实施例示意图，该系统包括:

监控单元301，用于在程序访问网络的过程中，监控所述程序的当前网络行为;

告知单元302，用于告知服务器所述当前网络行为所属的程序;

查找单元303，用于查找所述当前网络行为所属的程序的已知正常网络行为;

对比单元304，用于将所述程序的当前网络行为与所述程序的已知正常网络行为进行对比;

识别单元305，用于根据所述对比结果，识别所述程序的当前网络行为是否异常。

当然在具体实施过程中，可以是对能搜集到正常网络行为的所有程序都进行本发明实施例所提供的方案的处理，也可以是有选择性的针对某些容易受病毒攻击的程序进行处理。也就是说可以根据病毒的流行趋势，确定几类容易受病毒攻击的特定程序来进行处理，因此，该系统还可以包括:

类别确定单元，用于接收客户端发送的所述程序的属性信息，并根据所述程序的属性信息确定所述程序是否属于特定类别;

指示单元，用于在所述类别确定单元确定所述程序属于特定类别的情况下，则指示客户端告知所述程序的当前网络行为所属的程序。

可选的，程序的属性信息包括:

程序的数字签名、文件名、文件路径和/或原始名。

可选的，特定类别具体是当前一定时间段内容易受到病毒攻击的程序类别和/或容易被病毒利用的程序类别。

其中，告知单元 302 可以包括发送子单元，用于向服务器发送所述当前网络行为的信息以及所述当前网络行为所属程序的标识。

具体的，发送子单元用于为程序的当前网络行为的信息添加网络防御标签，网络防御标签包括当前网络行为所属的程序的标识；

向服务器发送带有网络防御标签的当前网络行为的信息。

其中，查找单元 303 可以包括正常网络行为查找子单元，用于根据所述当前网络行为所属程序的标识，查找所述程序的已知正常网络行为。

在具体实施过程中，正常网络行为查找子单元用于预先收集多种程序的正常网络行为，并建立程序的标识及其正常网络行为之间的对应关系；

根据所述当前网络行为所属程序的标识，查找该程序的标识对应的正常网络行为，将所述查找到的正常网络行为作为程序的已知正常网络行为

在实施的过程中，监控单元 301 可以通过截获程序的当前网络行为的信息得到监控的目的，具体可以包括：

第一截获子单元，用于通过在客户端注册协议驱动，截获所述程序的当前网络行为的信息；

或者，

第二截获子单元，用于通过创建与操作系统相似的过滤驱动，截获所述程序的当前网络行为的信息；

或者，

第三截获子单元，用于利用操作系统提供的应用程序编程接口函数截获所述程序的当前网络行为的信息；

或者，

第四截获子单元，用于接管程序调用网络编程接口函数的请求，截获所述程序的当前网络行为的信息；

或者，

第五截获子单元，用于利用注册防火墙回调，截获所述程序的当前网络行为的信息。

其中，识别单元 305 用于根据所述对比结果，识别所述程序的当前网络行为是否异常。

实施过程中，识别单元具体包括：

第一识别子单元，用于如果对比结果不一致，识别所述程序的当前网络行为为异常网络行为；

第二识别子单元，用于如果对比结果一致，识别所述程序的当前网络行为为正常网络行为。

根据最终的识别结果，还可以根据不同情况针对异常网络行为进行不同的处理，因此第一识别子单元还可以包括：

第一异常处理单元，用于暂停或拦截所述程序的当前异常网络行为；

或者，

第二异常处理单元，用于暂停或拦截所述程序的全部网络行为；

或者，

第三异常处理单元，用于暂停或拦截所述程序的全部行为。

可选的：

所述第一异常处理单元，具体用于检测到所述程序的异常网络行为是非恶意的网络行为，暂停或拦截所述程序的异常网络行为；

或者，

所述第二异常处理单元，具体用于检测到所述程序的异常网络行为是恶意的网络行为，但不确定所述程序是否为恶意程序，暂停或拦截所述程序的全部网络行为；

或者，

第三异常处理单元，具体用于检测到所述程序的异常网络行为是恶意的网络行为，并且所述程序为恶意程序，暂停或拦截所述程序的全部网络行为和全部本地行为。

上述的装置实施例中，其中监控单元 301、告知单元 302，可以是属于本地模块，查找单元 303、对比单元 304、识别单元 305 可以是属于网络模块。

本发明实施例还提供了一种识别网络行为是否异常的系统，参见图 4，其为本发明提供的一种识别网络行为是否异常的系统实施例示意图，该系统包括客户端 401 和服务器 402，客户端 401 用于在程序访问网络的过程中，监控所述程序的当前网络行为；告知服务器所述当前网络行为所属的程序；服务器 401,用于查找所述当前网络行为所属的程序的已知正常网络行为；将所述程序的当前网络行为与所述程序的正常网络行为进行对比；识别所述程序的当前网络行为是否异常。

其中，客户端 401 具体包括：监控模块 4011，用于在程序访问网络的过程中，监控所述程序的当前网络行为；告知模块 4012，用于告知服

务器当前网络行为所属的程序;

其中，服务器 402 包括：查找模块 4021，用于根据客户端告知的当前网络行为所属的程序，来对应查找预知的该程序的正常网络行为；对比模块 4022，用于将该程序的当前网络行为与查找到的该程序的正常网络行为进行对比；识别模块 4023，用于最终识别出该程序的当前网络行为是否异常。

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软件模块实现，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识别网络行为是否异常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 5 示出了可以实现根据本发明的识别网络行为是否异常的方法的服务器，例如应用服务器。该服务器传统上包括处理器 510 和以存储器 520 形式的计算机程序产品或者计算机可读介质。存储器 520 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 520 具有用于执行上述方法中的任何方法步骤的程序代码 531 的存储空间 530。例如，用于程序代码的存储空间 530 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 531。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 6 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 5 的服务器中的存储器 520 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 531'，即可以由例如诸如 510 之类的处理器读取的代码，这些代码当由服务器运行时，导致该服务器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

1、一种识别程序的网络行为是否异常的方法，其包括:

在程序访问网络的过程中，监控所述程序的当前网络行为;

告知服务器所述当前网络行为所属的程序;

查找所述当前网络行为所属的程序的已知正常网络行为;

将所述程序的当前网络行为与所述程序的已知正常网络行为进行对比;

根据所述对比结果，识别所述程序的当前网络行为是否异常。

2、根据权利要求 1 所述的方法，其中，还包括:

服务器接收客户端发送的所述程序的属性信息，根据所述程序的属性信息确定所述程序是否属于特定类别;

如果属于特定类别，则指示客户端告知所述程序的当前网络行为所属的程序。

3、根据权利要求 2 所述的方法，其中，所述特定类别具体包括:

当前一定时间段内容易受到病毒攻击的程序类别和/或容易被病毒利用的程序类别。

4、根据权利要求 1 所述的方法，其中，所述告知服务器所述当前网络行为所属的程序包括:

向服务器发送所述当前网络行为的信息以及所述当前网络行为所属程序的标识。

5、根据权利要求 4 所述的方法，其中，所述向服务器发送所述当前网络行为的信息以及所述当前网络行为所属的程序的标识包括:

为所述程序的当前网络行为的信息添加网络防御标签，所述网络防御标签包括所述当前网络行为所属的程序的标识;

向服务器发送带有所述网络防御标签的当前网络行为的信息。

6、根据权利要求 1 至 5 中任一项所述的方法，其中，所述查找所述当前网络行为所属程序的已知正常网络行为包括:

根据所述当前网络行为所属程序的标识，查找所述程序的已知正常网络行为。

7、根据权利要求 6 所述的方法，其中，所述根据所述当前网络行为所属程序的标识，查找所述程序的已知正常网络行为包括:

预先收集多种程序的正常网络行为，并建立程序的标识及其正常网络行为之间的对应关系；

根据所述当前网络行为所属程序的标识，查找该程序的标识对应的正常网络行为，将所述查找到的正常网络行为作为所述程序的已知正常网络行为。

8、根据权利要求 1 至 5 中任一项所述的方法，其中，所述监控所述程序的当前网络行为包括：

通过在客户端注册协议驱动，截获所述程序的当前网络行为的信息；

或者，

通过创建与操作系统相似的过滤驱动，截获所述程序的当前网络行为的信息；

或者，

利用操作系统提供的应用程序编程接口函数截获所述程序的当前网络行为的信息；

或者，

接管程序调用网络编程接口函数的请求，截获所述程序的当前网络行为的信息；

或者，

利用注册防火墙回调，截获所述程序的当前网络行为的信息。

9、根据权利要求 1 至 5 中任一项所述的方法，其中，所述根据所述对比结果，识别所述程序的网络行为是否异常包括：

如果对比结果不一致，识别所述程序的当前网络行为为异常网络行为；

如果对比结果一致，识别所述程序的当前网络行为为正常网络行为。

10、根据权利要求 9 所述的方法，其中，如果识别所述程序的当前网络行为为异常网络行为，还包括：

暂停或拦截所述程序的当前异常网络行为；

或者，

暂停或拦截所述程序的全部网络行为；

或者，

暂停或拦截所述程序的全部网络行为和全部本地行为。

11、根据权利要求 10 所述的方法，其中：

检测到所述程序的异常网络行为是非恶意的网络行为，暂停或拦截所述程序的异常网络行为；

或者，

检测到所述程序的异常网络行为是恶意的网络行为，但不确定所述程序是否为恶意程序，暂停或拦截所述程序的全部网络行为；

或者，

检测到所述程序的异常网络行为是恶意的网络行为，并且所述程序为恶意程序，暂停或拦截所述程序的全部网络行为和全部本地行为。

12、一种识别网络行为是否异常的装置，其包括：

监控单元，用于在程序访问网络的过程中，监控所述程序的当前网络行为；

告知单元，用于告知服务器所述当前网络行为所属的程序；

查找单元，用于查找所述当前网络行为所属的程序的已知正常网络行为；

对比单元，用于将所述程序的当前网络行为与所述程序的已知正常网络行为进行对比；

识别单元，用于根据所述对比结果，识别所述程序的当前网络行为是否异常。

13、根据权利要求 12 所述的装置，其中，还包括：

类别确定单元，用于接收客户端发送的所述程序的属性信息，并根据根据所述程序的属性信息确定所述程序是否属于特定类别；

指示单元，用于在所述类别确定单元确定所述程序属于特定类别的情况下，指示客户端告知所述程序的当前网络行为所属的程序。

14、根据权利要求 13 所述的装置，其中，所述特定类别具体包括：

当前一定时间段内容易受到病毒攻击的程序类别和/或容易被病毒利用的程序类别。

15、根据权利要求 12 所述的装置，其中，所述告知单元包括：

发送子单元，用于向服务器发送所述当前网络行为的信息以及所述当前网络行为所属程序的标识。

16、根据权利要求 15 所述的方法，其中：

所述发送子单元，具体用于为所述程序的当前网络行为的信息添加网

络防御标签，所述网络防御标签包括所述当前网络行为所属的程序的标识；向服务器发送带有所述网络防御标签的当前网络行为的信息。

17、根据权利要求 12 至 16 中任一项所述的装置，其中，所述查找单元包括：

正常网络行为查找子单元，用于根据所述当前网络行为所属程序的标识，查找所述程序的已知正常网络行为。

18、根据权利要求 17 所述的装置，其中：

所述正常网络行为查找子单元，具体用于预先收集多种程序的正常网络行为，并建立程序的标识及其正常网络行为之间的对应关系；根据所述当前网络行为所属程序的标识，查找该程序的标识对应的正常网络行为，将所述查找到的正常网络行为作为所述程序的已知正常网络行为。

19、根据权利要求 12 至 16 中任一项所述的装置，其中，所述监控单元具体包括：

第一截获子单元，用于通过在客户端注册协议驱动，截获所述程序的当前网络行为的信息；

或者，

第二截获子单元，用于通过创建与操作系统相似的过滤驱动，截获所述程序的当前网络行为的信息；

或者，

第三截获子单元，用于利用操作系统提供的应用程序编程接口函数截获所述程序的当前网络行为的信息；

或者，

第四截获子单元，用于接管程序调用网络编程接口函数的请求，截获所述程序的当前网络行为的信息；

或者，

第五截获子单元，用于利用注册防火墙回调，截获所述程序的当前网络行为的信息。

20、根据权利要求 12 至 16 中任一项所述的装置，其中，所述识别单元包括：

第一识别子单元，用于如果对比结果不一致，识别所述程序的当前网络行为为异常网络行为；

第二识别子单元，用于如果对比结果一致，识别所述程序的当前网络

行为为正常网络行为。

21、根据权利要求 20 所述的装置，其中，还包括:

第一异常处理单元，用于暂停或拦截所述程序的当前异常网络行为;

或者，

第二异常处理单元，用于暂停或拦截所述程序的全部网络行为;

或者，

第三异常处理单元，用于暂停或拦截所述程序的全部网络行为和全部本地行为。

22、根据权利要求 21 所述的装置，其中:

所述第一异常处理单元，具体用于检测到所述程序的异常网络行为是非恶意的网络行为，暂停或拦截所述程序的异常网络行为;

或者，

所述第二异常处理单元，具体用于检测到所述程序的异常网络行为是恶意的网络行为，但不确定所述程序是否为恶意程序，暂停或拦截所述程序的全部网络行为;

或者，

第三异常处理单元，具体用于检测到所述程序的异常网络行为是恶意的网络行为，并且所述程序为恶意程序，暂停或拦截所述程序的全部网络行为和全部本地行为。

23、一种识别网络行为是否异常的系统，其包括:

客户端，用于在程序访问网络的过程中，监控所述程序的当前网络行为；告知服务器所述当前网络行为所属的程序;

服务器， 用于查找所述当前网络行为所属的程序的已知正常网络行为；将所述程序的当前网络行为与所述程序的正常网络行为进行对比; 识别所述程序的当前网络行为是否异常。

24、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服务器上运行时，导致所述服务器执行根据权利要求 1-11 中的任一个所述的识别程序的网络行为是否异常的方法。

25、一种计算机可读介质，其中存储了如权利要求 24 所述的计算机程序。

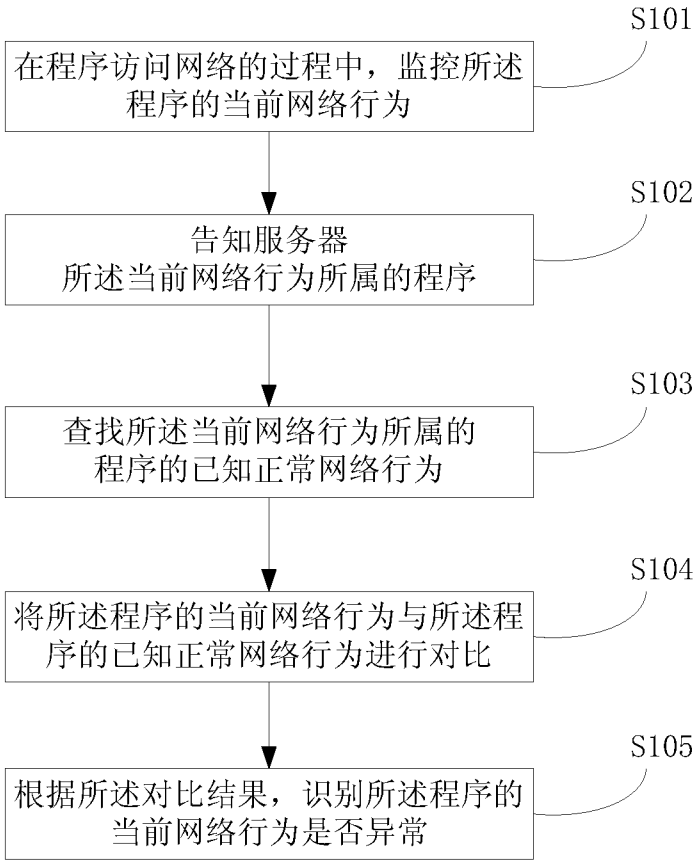

S101
在程序访问网络的过程中，监控所述程序的当前网络行为
S102
告知服务器所述当前网络行为所属的程序
S103
查找所述当前网络行为所属的程序的已知正常网络行为
S104
将所述程序的当前网络行为与所述程序的已知正常网络行为进行对比
S105
根据所述对比结果，识别所述程序的当前网络行为是否异常

图 1

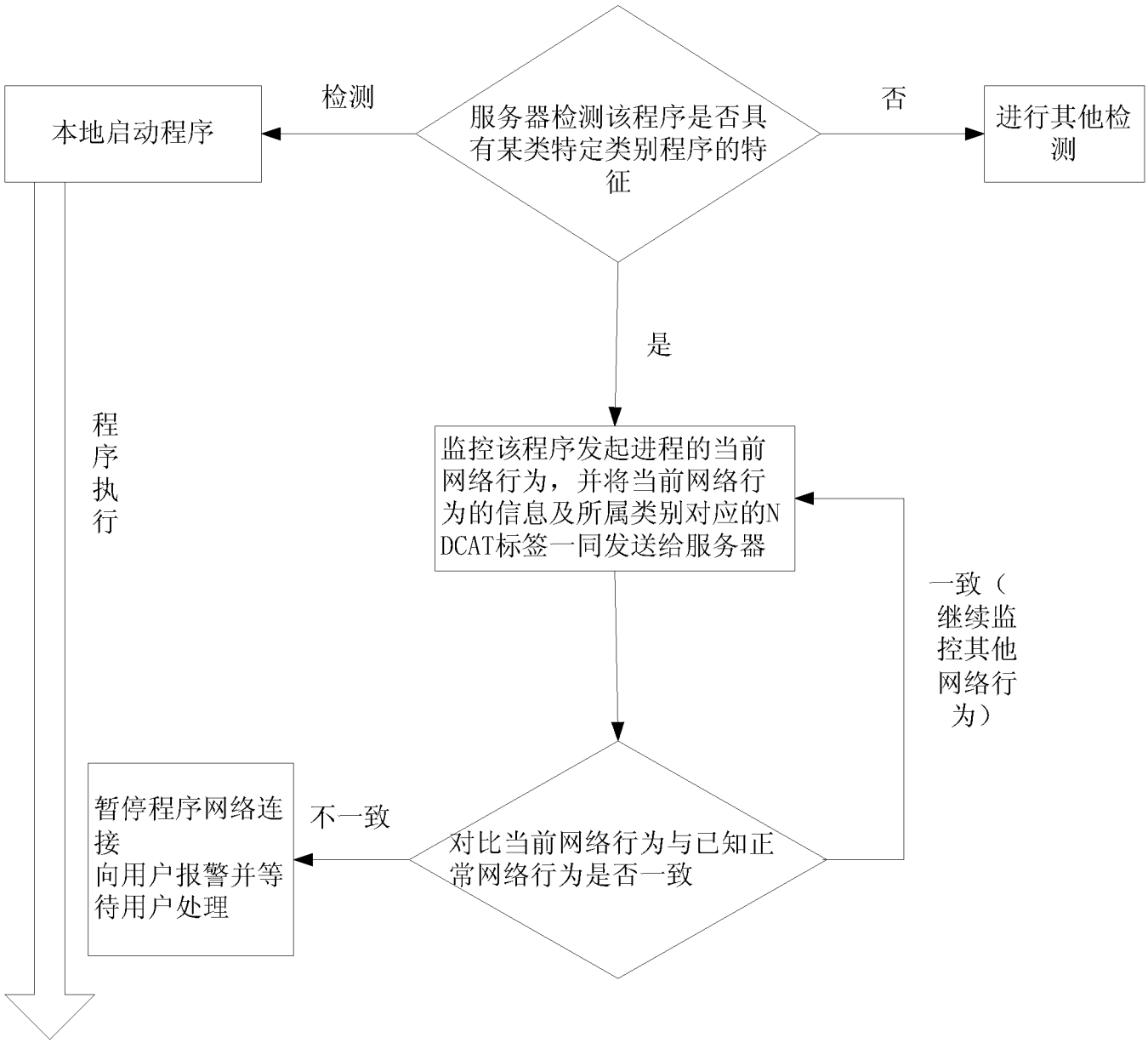

本地启动程序
检测
服务器检测该程序是否具有某类特定类别程序的特征
否
进行其他检测
是
程序执行
监控该程序发起进程的当前网络行为，并将当前网络行为的信息及所属类别对应的NDCAT标签一同发送给服务器
一致（继续监控其他网络行为）
对比当前网络行为与已知正常网络行为是否一致
不一致
暂停程序网络连接
向用户报警并等待用户处理

图 2

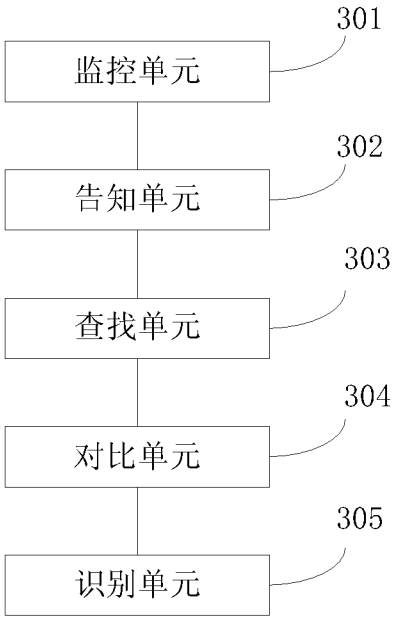

301
监控单元
302
告知单元
303
查找单元
304
对比单元
305
识别单元

图 3

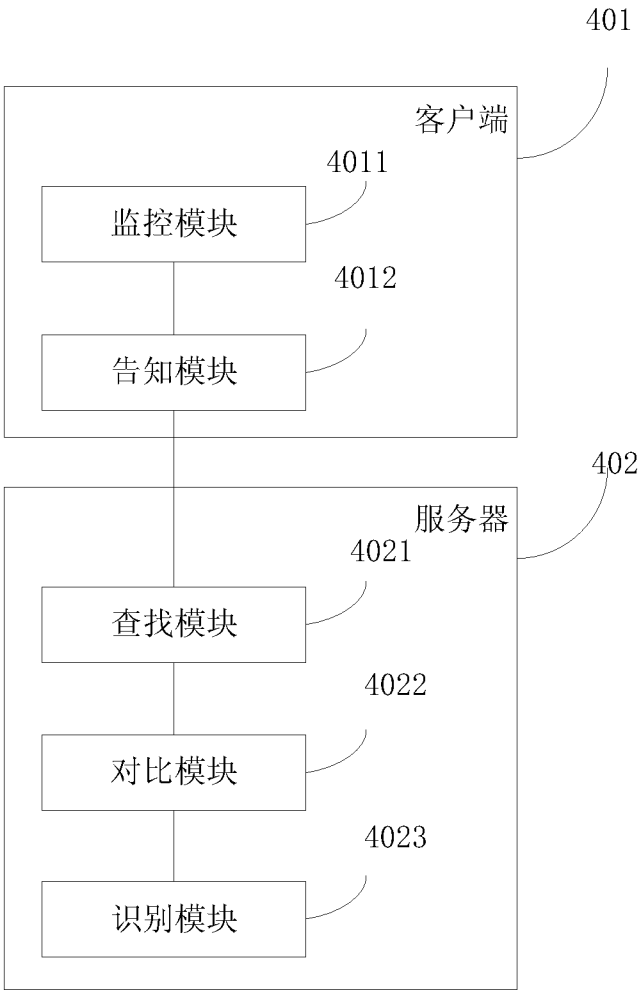

401
客户端
4011
监控模块
4012
告知模块
402
服务器
4021
查找模块
4022
对比模块
4023
识别模块

图 4

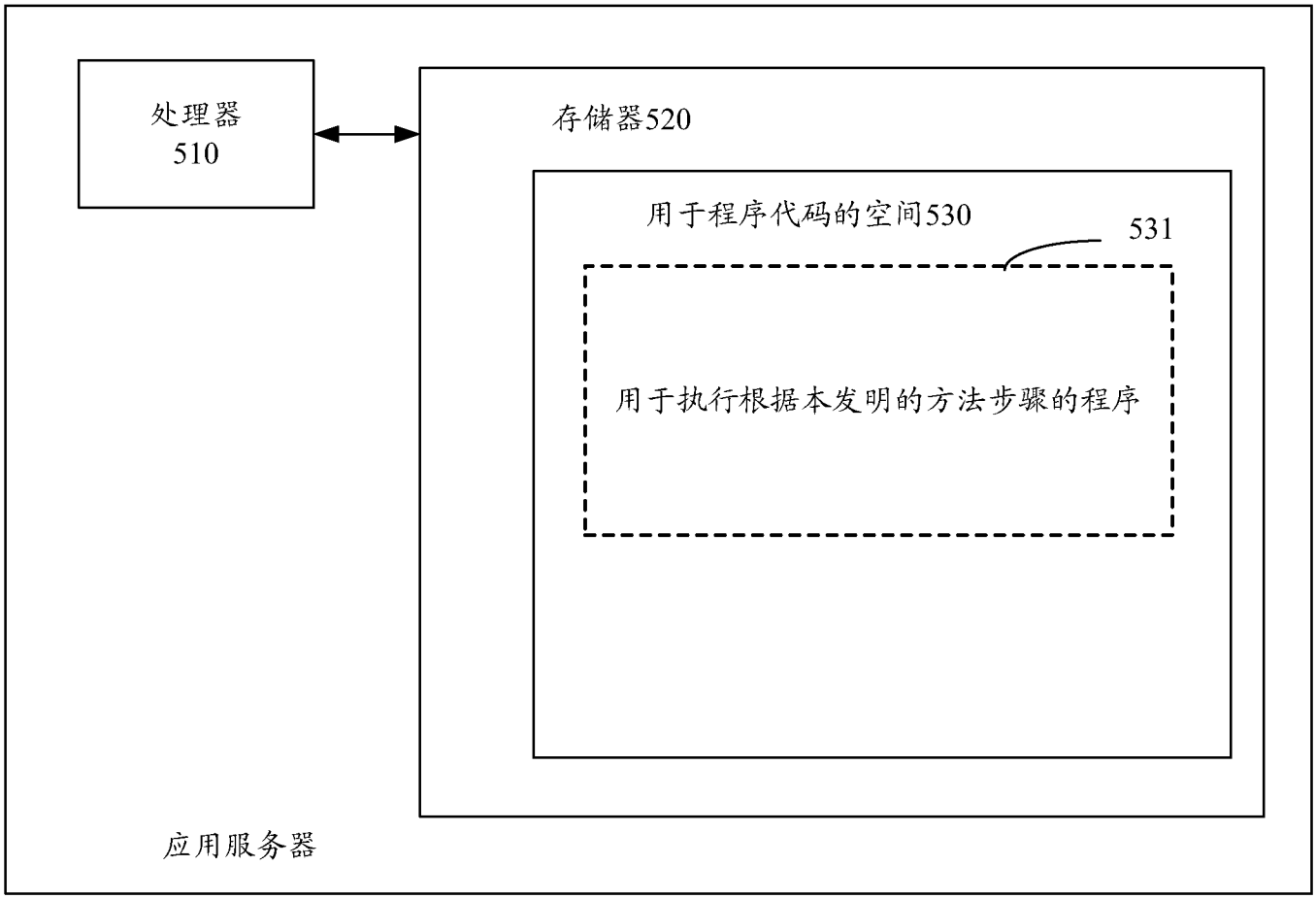

处理器
510
存储器520
用于程序代码的空间530
531
用于执行根据本发明的方法步骤的程序
应用服务器

图 5

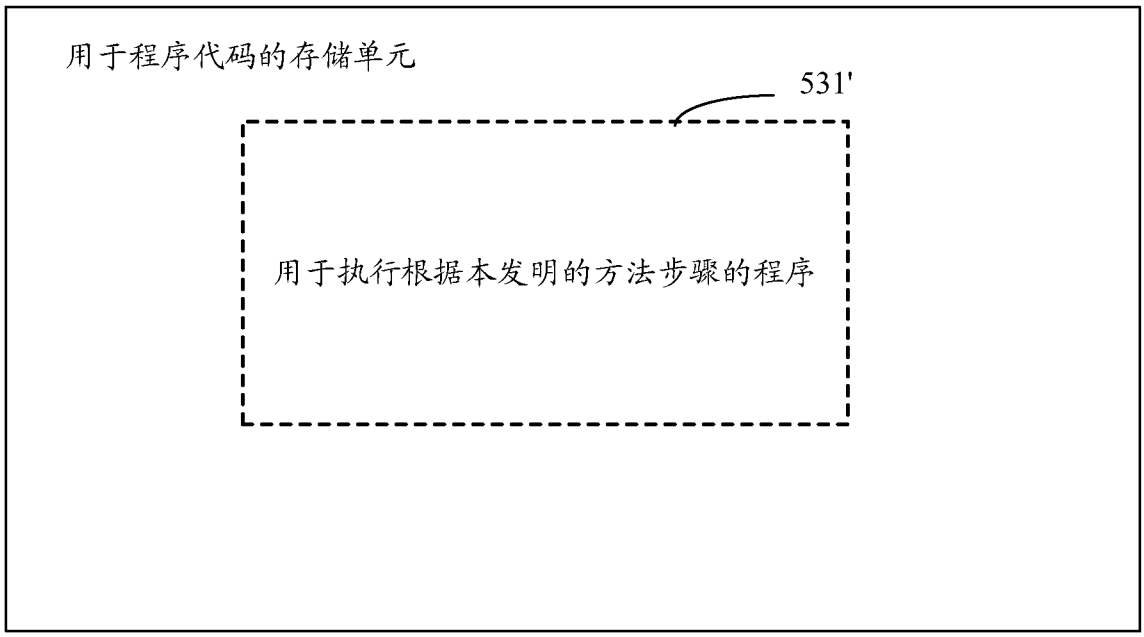

用于程序代码的存储单元
531'
用于执行根据本发明的方法步骤的程序

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/075472

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) 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)

IPC: H04L; G06F

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)

CNPAT, CNKI, WPI, EPODOC: virus, antivirus, timely, variation, client, server, action, activity, behavior, software, process, compar???, match???, new, unknown

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 102694817 A (QIZHI SOFTWARE (BEIJING) CO., LTD.) 26 September 2012 (26.09.2012) claims 1-23 and description, paragraph [0141]	1-25
A	CN 102082802 A (CHEN, Biao) 01 June 2011 (01.06.2011) description, paragraphs [0013]-[0061]	1-25
A	US 2008/0066179 A1 (FUJIAN EASTERN MICROPOINT INFO-TECH CO., LTD.) 13 March 2008 (13.03.2008) the whole document	1-25

☐ 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
27 July 2013 (27.07.2013)	15 August 2013 (15.08.2013)

Name and mailing address of the ISA	Authorized officer
State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	YANG, Kaipeng Telephone No. (86-10) 62413436

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/075472

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102694817 A	26.09.2012	None	
CN 102082802 A	01.06.2011	None	
US 2008/0066179 A1	13.03.2008	US 7870612 B2	11.01.2011

国际检索报告

国际申请号
PCT/CN2013/075472

A. 主题的分类

H04L 29/06 (2006.01) 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)

IPC: H04L; G06F

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）)

CNPAT,CNKI,WPI,EPODOC: 病毒, 查毒, 杀毒, 及时, 变异, 变种, 未知, 程序, 软件, 客户端, 服务器, virus, action, activity, behavior, software, process, compar???, match???, new, unknown

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 102694817 A (奇智软件(北京)有限公司) 26.9 月 2012 (26.09.2012) 权利要求 1-23、说明书第[0141]段	1-25
A	CN 102082802 A (陈彪) 01.6 月 2011 (01.06.2011) 说明书第[0013]-[0061]段	1-25
A	US 2008/0066179 A1 (FUJIAN EASTERN MICROPOINT INFO-TECH CO., LTD.) 13.3 月 2008 (13.03.2008) 全文	1-25

☐ 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
27.7 月 2013 (27.07.2013)	**15.8 月 2013 (15.08.2013)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号：　(86-10)62019451	受权官员 杨凯鹏 电话号码：(86-10) 62413436

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2013/075472

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN 102694817 A	26.09.2012	无	
CN 102082802 A	01.06.2011	无	
US 2008/0066179 A1	13.03.2008	US 7870612 B2	11.01.2011