

(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
2014 年 6 月 26 日 (26.06.2014)



(10) 国际公布号
WO 2014/094470 A1

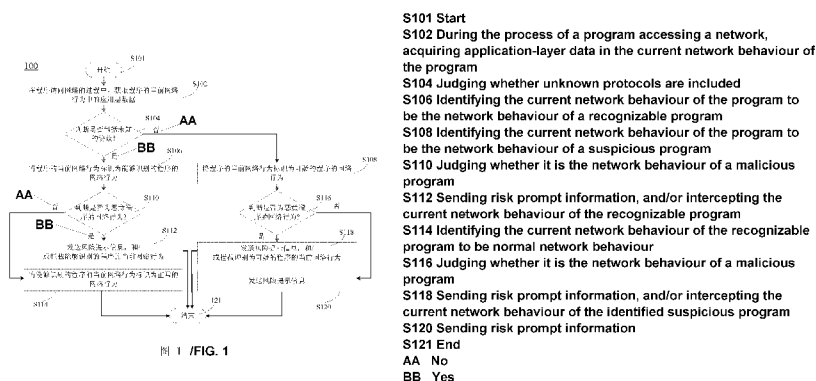
- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2013/083667
- (22) 国际申请日: 2013 年 9 月 17 日 (17.09.2013)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201210551543.3 2012 年 12 月 18 日 (18.12.2012) CN
- (71) 申请人: 北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED) [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 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: 刘海栗 (LIU, Haili); 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: 北京智汇东方知识产权代理事务所 (普通合伙) (WISEAST INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区成府路 28 号优盛大厦 D-1111 室, Beijing 100083 (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, 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, 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, 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)。

[续页]

(54) Title: METHOD, DEVICE AND SYSTEM FOR RECOGNIZING NETWORK BEHAVIOUR OF PROGRAM

(54) 发明名称: 识别程序的网络行为的方法、装置及系统



(57) Abstract: Disclosed are a method, device and system for recognizing network behaviour of a program. The method comprises: during the process of a program accessing a network, acquiring application-layer data in the current network behaviour of the program; judging whether the application-layer data includes unknown protocols; if the protocols in the application-layer data are all known protocols, identifying the current network behaviour of the program to be the network behaviour of a recognizable program; and if the application-layer data includes unknown protocols, identifying the current network behaviour of the program to be the network behaviour of a suspicious program. Thus the accurate recognition of network behaviour of a program is realized, the network prompt information can be sent to a user, and the final selection is performed by the user, thereby solving the problem that a conventional solution for recognizing the network behaviour of a program cannot accurately recognize the network behaviour of a newly-emerged or newly-varied program.

(57) 摘要:

[续页]

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

本发明公开了一种识别程序的网络行为的方法、装置及系统，其中方法包括：在程序访问网络的过程中，获取程序的当前网络行为中的应用层数据；判断应用层数据中是否包括未知的协议；若应用层数据中的协议都是已知的协议，则将程序的当前网络行为标识为能够识别的程序的程序的网络行为；若应用层数据中包括未知的协议，则将程序的当前网络行为标识为可疑的程序的程序的网络行为。由此实现对程序的程序的网络行为的准确识别，将包括未知的协议的程序的程序的网络行为标识为可疑的程序的程序的网络行为，并可向用户发送风险提示信息，由用户进行最终的选择，由此解决了传统的识别程序的程序的网络行为的方案对于新出现或新变种的程序的程序的网络行为不能准确识别的问题。

识别程序的网络行为的方法、装置及系统

技术领域

本发明属于计算机技术领域，尤其涉及一种识别程序的网络行为的方法、装置及系统。

背景技术

众所周知，当今互联网环境中，应用最为广泛的网络结构满足 DoD 模型（又称 TCP/IP 协议族）。该 DoD 模型包括：链路层、互联网层、传输层和应用层。一个程序若要发送或接收互联网数据，就需要让自己的数据符合 TCP/IP 协议标准，才能让数据在互联网中准确且有效的传输。而这四层协议中：链路层、互联网层、传输层的数据结构均有一套相对严格的标准，编程者不能擅自更改其结构，所以很容易被安全软件或安全设备监控到关键数据且难于伪装。唯独应用层的数据结构，具有很高的可定制特性。允许编程人员根据自己的需求和想法任意定义其中的内容与结构。

现有的对应用层的数据结构的检测方案，主要是依靠特征码进行检测——即：研究人员发现了某一种已经出现的网络威胁（远控、木马、蠕虫等），通过对拿到的样本进行研究和分析，抓取其传输的网络数据包，然后提取其固定特征（如某一特定偏移量处出现某一特定字符），作为程序自动检测的依据。而入这样的传统解决方案最大的缺点在于存在滞后性，必须找到新型威胁的样本加以分析，才能做出有效拦截。

由此可知，传统的识别程序的网络行为的方式对于新出现或新变种的程序的网络行为不能准确识别。

发明内容

鉴于上述技术问题，提出了本发明以便提供一种克服上述技术问题或者至少部分地解决上述技术问题的识别程序的网络行为的方法、装置及系统。

依据本发明实施例的一个方面，提供了一种识别程序的网络行为的方法，方法包括：在程序访问网络的过程中，获取程序的当前网络行为中的应用层数据；判断应用层数据中是否包括未知的协议；若应用层数据中的协议都是已知的协议，则将程序的当前网络行为标识为能够识别的程序的当前网络行为；若应用层数据中包括未知的协议，则将程序的当前网络行为标识为可疑的程序的当前网络行为。

根据本发明实施例的另一方面，提供了一种识别程序的网络行为的装置，装置包括：获取模块，用于在程序访问网络的过程中，获取所述程序的当前网络行为中的应用层数据；第一判断模块，用于判断应用层数据中是否包括未知的协议；识别

模块，用于在应用层数据中的协议都是已知的协议时，将程序的当前网络行为标识为能够识别的程序的网络行为；以及当应用层数据中包括未知的协议时，将程序的当前网络行为标识为可疑的程序的网络行为。

根据本发明实施例的又一方面，提供了一种识别程序的网络行为的系统，该系统包括：客户端和云端服务器，其中客户端用于在程序访问网络的过程中，获取程序的当前网络行为中的应用层数据；判断应用层数据中是否包括未知的协议；如果应用层数据中的协议都是已知的协议，则将程序的当前网络行为标识为能够识别的程序的网络行为；如果应用层数据中包括未知的协议，则将程序的当前网络行为标识为可疑的程序的网络行为，然后将能够识别的程序的网络行为或者可疑的程序的
5 网络行为的特征信息发送至云端服务器；云端服务器用于根据特征信息判断能够识别的程序的网络行为、或可疑的程序的网络行为是否为恶意程序的网络行为，并向客户端返回判断结果。

根据本发明实施例的又一方面，提供了一种识别程序的网络行为的系统，包括：客户端和云端服务器，其中客户端，用于在程序访问网络的过程中，获取程序的当前网络行为中的数据包，数据包包括：应用层数据，以及接收云端服务器返回的识别结果；云端服务端，用于接收客户端获取的程序的当前网络行为中数据包，判断应用层数据中是否包括未知的协议；若应用层数据中的协议都是已知的协议，则将程序的当前网络行为标识为能够识别的程序的网络行为；若应用层数据中包括未知的协议，则将程序的当前网络行为标识为可疑的程序的网络行为，向客户端发送识别结果。
15 20

根据本发明实施例的识别程序的网络行为的方法、装置及系统，当程序的当前网络行为中的应用层数据都是已知的协议时，将程序的当前网络行为标识为能够识别的程序的网络行为；当程序的当前网络行为中的应用层数据中包括未知的协议时，将程序的当前网络行为标识为可疑的程序的网络行为，由此实现对程序的网络行为的准确识别，将包括未知的协议的程序的网络行为标识为可疑的程序的网络行为，并可向用户发送风险提示信息，由用户进行最终的选择，由此解决了传统的识别程序的
25 网络行为的方案对于新出现或新变种的程序的网络行为不能准确识别的问题，进一步解决了传统的识别程序的网络行为的方案中不对未知的网络协议进行拦截的问题，提高用户的网络安全性。

而且，在将程序的当前网络行为标识为能够识别的程序的网络行为之后，或者将程序的当前网络行为标识为可疑的程序的网络行为之后，客户端可以将应用层数据中的特征信息发送至云端服务器，由云端服务器根据黑白名单库中的黑白名单，判断程序的网络行为是否为恶意程序的网络行为，通过将数据量较大、变动比较频繁的一些黑白名单存储在云端服务器上，由云端服务器来识别恶意程序的网络行为，
30 可有效节约客户端本地资源和降低客户端本地机器的性能开销，同时也可加快识别
35

网络行为的响应速度。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。

5 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：

- 10 图 1 示出了根据本发明一个实施例的程序网络行为识别方法 100 的流程图；
图 2 示出了根据本发明另一个实施例的程序网络行为识别装置 200 的结构框图；
图 3 示出了根据本发明又一个实施例的程序网络行为识别系统 300 的结构框图；
图 4 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 5 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
15 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
20 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。

传统的程序网络行为识别方案大多由已知的数据入手，即：试图找到数据中哪些部分是已知的，再从这些已知的数据中找到有用的部分，用于判定该数据是否有威胁。但这种思路的弊病在于一旦网络数据的应用层数据是未知的，那么能拿到的
25 有效已知的数据就会很少，如此就很难对网络行为是否存在威胁作出精确判断，很容易放过未知的具有网络威胁的网络行为。

为此，本发明实施例提出的一种程序网络行为识别方法、装置及系统，其思路是基于 TCP/IP 协议体系中应用层的数据结构具有较高的可定制特性，一旦检测到应用层数据中包括自定义的数据结构，即可认为当前的网络行为存在风险，由此本发
30 明提出的程序网络行为识别方法主要是，通过判断程序的当前网络行为的应用层数据中是否包括未知的协议，若都是已知的协议，则将程序的当前网络行为标识为能够识别的程序的网
络行为；若包括未知的协议，则将程序的当前网络行为标识为可疑的程序的网
络行为。

下面结合图 1 具体说明根据本发明一个实施例的、适于解决上述技术问题的程
35 序网络行为识别方法 100 的流程图。如图 1 所示，本发明实施例的方法 100 始于步

骤 S101。随后，在步骤 S102 中，在程序访问网络的过程中，获取程序的当前网络行为的应用层数据。

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。进程时程序在计算机上的一次执行过程，是一个动态的概念。

- 5 同一个程序可以同时运行于若干个数据集合上，也就是说同一个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
10 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，
15 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，在该流程的任何一个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
20 但不限于以下几种方式：通过在客户端注册协议驱动、创建于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（例如 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
25 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，
30 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，获取程序的当前网络行为中的应用层数据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
35 提供的与设备通信接口 NtDeviceIoControl 函数，获取所有应用程序设备通信的数

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 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)，可以讲 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，当然监控网络行为的方式也不限于以上所列举的方式。

随后，在步骤 S104 中，判断应用层数据中是否包括未知的协议，在一些实施例中，可根据已知的协议的格式，判断应用层数据中是否包括未知的协议。例如：已知的协议至少包括下列中的至少一个：HTTP 协议、DNS 协议、SMTP 协议、FTP 协议 (File Transfer Protocol, 文件传输协议)、SNMP 协议 (Simple Network Management Protocol, 简单网络管理协议) 和 POP3 协议 (邮局协议的第 3 个版本协议)。

可选地，在客户端上预先收集数量足够多的已知的协议，该已知的协议包括：HTTP 协议、DNS 协议、SMTP 协议等三种协议，也可以包括一些加密协议，例如：FTP 协议等。加密协议主要是在数据包中对未知的协议进行统一的加密格式进行封装，数据包里面附加一些可识别的常用协议，这些常用的协议可以包括：SNMP 协议、POP3 协议、eMule/eDonkey 协议，或者 BITTORRENT 协议等。由于不同的协议其本身有一些固定的格式，因此对于已知的协议可检测协议的本身的格式，例如 HTTP 协议包括协议头，但没有协议尾，Host、Refer 等字段均属于协议头中所包含的内容，协议头中常见的格式包括：Host、Refer、User-agent、Url 等字段部分。

如果应用层数据中包括未知的协议，则可认为存在风险。虽然应用层数据可以由软件开发人员随意指定，但为了互联网中数据传输的方便，已经在实际应用过程中形成了一套通用协议 (也可称为已知的协议) 标准。已知的协议如 DNS 协议、HTTP 协议、FTP 协议、SMTP 协议、SSL/TLS 协议、SSH 协议、uTorrent 协议、eMule/eDonkey 协议、BitTorrent 协议等，上述已知的协议占据了网络数据中的绝大部分。只要能有效识别和分析上述已知的协议的数据结构，那么剩下的未知的协议将会是极少数的。由于已知的协议基本可以满足所有数据传输需求，所以有理由认为凡是需要自定义协议 (即未知的协议) 进行数据传输的，都应该是有某种特殊需求而在某一极小范围的特定环境中使用，而不应该在互联网当中广泛传播。故此将包含有未知的协议的应用层数据列为可疑，有必要向用户进行风险提示。

具体到方法 100 的流程中，可预先收集已知的协议的格式，已知的协议包括但不限于 DNS 协议、HTTP 协议、FTP 协议、SMTP 协议、SSL/TLS 协议、SSH 协议、uTorrent 协议、eMule/eDonkey 协议、BitTorrent 协议等，然后在步骤 S104 中，根据预先收

集的已知的协议的格式，对应用层数据中的协议进行识别，如果应用层数据中的协议都能识别，则判断应用层数据中都是已知的协议，如果应用层数据中有至少部分协议不能识别，则判断应用层数据中包括未知的协议。

如果在步骤 S104 中判断出应用层数据中的协议都是已知的协议，则进行步骤 5 S106。在步骤 S106 中，将程序的当前网络行为标识为能够识别的程序的程序的网络行为。

也就是，当网络行为的应用层数据中的协议都是已知的协议时，意味着能够识别该网络行为，此时在步骤 S106 中可将该网络行为标识为能够识别的程序的程序的网络行为。例如通过标识符“1”将网络行为标识为能够识别的程序的程序的网络行为。当然可以理解的是，在本发明的实施例中并不限定标识符的具体形式。

10 在步骤 S106 之后，可进入结束步骤 S121。但是为了进一步判断能够识别的程序的程序的网络行为是否为恶意程序的程序的网络行为，可在步骤 S106 之后进入步骤 S110，在步骤 S110 中，判断能够识别的程序的程序的网络行为是否为恶意程序的程序的网络行为。

恶意程序通常是指带有攻击意图的操作方所编写的一段程序。这些威胁可以分成两个类别：需要宿主程序的威胁和彼此独立的威胁。前者基本上是不能独立于某个实际的应用程序、实用程序或系统程序的程序片段；后者是可以被操作系统调度和运行的自包含程序。恶意程序包括：陷门、逻辑炸弹、特洛伊木马、蠕虫、细菌和病毒等等。

在一些实施例中，可采用以下两种方式判断能够识别的程序的程序的网络行为是否为恶意程序的程序的网络行为，其中，

20 方式一，在客户端上预设一个模块用于存储黑白名单库中的黑白名单，由客户端通过黑白名单以及获取的特征信息可判断网络行为是否为恶意程序的程序的网络行为。

可选地，网络防御相关的黑白名单可以针对不同协议进行不同的检查项。例如：

(1) 通用检查项，包括：检查远端 ip 地址，本地端口、远端端口、传输层协议（通常为 TCP 或 UDP 之一）。(2) 协议类型检查，有些已知协议可能会被木马远控用于 25 传输数据，此类已知协议一旦被发现即可被判断为被恶意程序使用的数据协议包。

(3) 协议详情检查，其他已知协议，根据协议特有的结构获取其中有参考价值并且不会涉及检测的对象本身，以此为依据作为黑白判断的标准，该协议详情会根据协议的不同而具体项目也会不同，如：在客户端上检测 HTTP 协议中的 URL、Host、Referer、User-Agent 等加密后的字段；检测 DNS 协议中的 Queries 信息中的 Name 30 和 Type 等加密后的字段。

具体地，客户端获取能够识别的程序的程序的网络行为的应用层数据中的特征信息，该特征信息可以是应用层数据中的部分代码、应用层数据中的数据包、或者应用层数据中的数据包中的一段数据；根据客户端上的黑白名单，以及获取的特征信息，判断能够识别的程序的程序的网络行为是否为恶意程序的程序的网络行为。

35 以网络行为是 HTTP 访问行为进行介绍，具体到上述步骤中，在步骤 S102 中获

取 HTTP 访问行为的应用层数据。在步骤 S104 中，根据已知的 HTTP 协议的格式判断出该 HTTP 访问行为包括的协议都是已知的协议。然后在步骤 S106 中，将 HTTP 访问行为标识为能够识别的程序的网络行为。接着在步骤 S110 中，获取 HTTP 访问行为的应用层数据中的特征信息，例如 Host 字段、Url 字段、IP 地址字段等，并根据黑白名单库中的黑白名单判断上述特征信息是否属于恶意程序的网络行为中的特征信息，如果属于，则该网络行为属于恶意程序的网络行为，进入到步骤 S112 中，如果不属于，则该网络行为属于正常的网络行为，进入到步骤 S114 中。

需要说明的是，针对不同的协议，在方式一中的检测的项目不同，例如对于 DNS 协议，主要是针对请求包的域名解析，判断解析的域名的字符串，以及 DNS 返回来的 IP 地址等是否异常。对于 SMTP 协议主要是判断 name 字段部分是否异常，例如检测邮件发送人、接收人、发送人的名称和域名，以及接收人的名称和域名等是否异常。对于 FTP 协议和 HTTP 协议，主要是判断域名和 Url 字段是否异常。如果上述字段与云端服务器或客户端中的黑名单相符合，则认为该协议有风险，有必要向用户进行风险提示。对于 SMTP 协议中取得的一切数据均可以 MD5 等哈希值进行处理后再上传云端服务器，黑白名单在云端服务器中仅检测 SMTP 协议中的数据的 MD5 值，不涉及邮件内容本身。

方式二，在云端服务器上预设一个数据库，该数据库用于存储黑白名单库中的黑白名单，客户端将获取的特征信息发送到云端服务器，由云端服务器根据黑白名单以及接收到的特征信息判断网络行为是否为恶意程序的网络行为。

具体地，首先客户端获取能够识别的程序的网络行为中的应用层数据中的特征信息，该特征信息可以是应用层数据中的部分代码（例如 Host 字段或者 Url 字段）、应用层数据中的数据包、或者应用层数据中的数据包中的一段数据。通常情况下，应用层数据中除了包括用于传输的字段之外，也会有一些自定义的数据。例如用户用 HTTP 或 FTP 向网站或服务器上传文件时，除了由 URL 和 Host 等字段指定用户上传的一些必要识别信息之外，用户上传的文件本身就会被作为一个数据包，附加在 HTTP 或 FTP 协议中向指定服务器进行传输。此时，用户上传的文件内容就属于上述的应用层协议中的数据包（当然，文件大的话有可能会被拆分成多个数据包进行传输）。这仅为一个比较常见的例子，对于不同协议和不同的应用情景，这种数据包会以不同形式出现。当然，某些情形下也可能不存在这种数据包或数据包为空。

然后，客户端将特征信息发送至云端服务器，由云端服务器根据黑白名单库中的黑白名单判断上述特征信息是否属于恶意程序的网络行为中的特征信息，并向客户端返回判断结果，如果属于，则该网络行为属于恶意程序的网络行为，进入到步骤 S112 中，如果不属于，则该网络行为属于正常的网络行为，进入到步骤 S114 中。由于云端服务器的存储空间要远远大于客户端，因此云端服务器上可以尽可能多的预先存储黑白名单库，进而可以提高网络行为识别的准确性。同时，在云端服务器

上对于最新收集到的黑白名单库之后可以及时进行更新处理。

回到上述方法 100 的流程中，如果在步骤 S110 中判断是恶意程序的网络行为，则进入到步骤 S112，在步骤 S112 中，发送风险提示信息和/或拦截能够识别的程序的当前网络行为，然后进入结束步骤 S121。例如，如果可以确定程序的当前网络行为是恶意程序的网络行为，可以先暂停该程序的网络连接，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。相反，如果在步骤 S110 中判断不是恶意程序的网络行为，则进入到步骤 S114 中，将能够识别的程序的当前网络行为标识为正常的网络行为，然后进入结束步骤 S121。正常的网络行为不具有风险或具有极低的风险，允许该正常的网络行为访问网络。

相反，如果在步骤 S104 中判断出应用层数据中包括未知的协议，则进行步骤 S108。在步骤 S108 中，将程序的当前网络行为标识为可疑的程序的程序的网络行为。也就是，将程序的网络行为的应用层数据的协议与通用的协议进行比较，当程序的网络行为的应用层数据中包括未知的协议时，则可认为该程序的网络行为暂时无法准确识别，可认为该网络行为存在风险，此时可将该程序的网络行为标识为可疑的程序的程序的网络行为。例如通过标识符“0”将网络行为标识为可疑的程序的程序的网络行为。当然可以理解的是，在本发明的实施例中并不限定标识符的具体形式。

在步骤 S108 之后，可进入结束步骤 S121。但是为了进一步判断可疑的程序的程序的网络行为是否为恶意程序的网络行为，可在步骤 S108 之后进入步骤 S116。在步骤 S116 中，判断可疑的程序的程序的网络行为是否为恶意程序的网络行为。

恶意程序通常是指带有攻击意图所编写的一段程序，这些威胁可以分成两个类别：需要宿主程序的威胁和彼此独立的威胁。前者基本上是不能独立于某个实际的应用程序、实用程序或系统程序的程序片段；后者是可以被操作系统调度和运行的自包含程序，恶意程序包括：陷门、逻辑炸弹、特洛伊木马、蠕虫、细菌和病毒等等。

在一些实施例中，可采用以下两种方式判断可疑的程序的程序的网络行为是否为恶意程序的网络行为，其中

方式一，在客户端上预设一个模块用于存储黑白名单库中的黑白名单，由客户端通过黑白名单以及获取的特征信息判断网络行为是否为恶意程序的网络行为。

具体地，客户端获取可疑的程序的程序的网络行为的应用层数据中的特征信息，该特征信息可以是应用层数据中的部分代码、应用层数据中的数据包、或者应用层数据中的数据包中的一段数据；根据客户端上的黑白名单，以及获取的特征信息，判断可疑的程序的程序的网络行为是否为恶意程序的网络行为，如果属于，则该网络行为属于恶意程序的网络行为，进入到步骤 S118 中，如果不属于，则该网络行为属于有风险的程序的网络行为，进入到步骤 S120 中。

需要说明的是，针对不同的协议，检测的项目不同，例如对于 DNS 协议，主要是针对请求包的域名解析，判断解析的域名的字符串，以及 DNS 返回来的 IP 地址等是否异常。对于 SMTP 协议主要是判断 name 字段部分，包括：邮件发送人、接收人、发送人的名称和域名，以及接收人的名称和域名等是否异常。对于 HTTP 协议，主要判断 Host、URL、User-Agent、Referer 和 Method 等字段是否异常。对于是否异常

5 的判断，主要是两个大类：（1）精准匹配：比如发现了一个木马，发现该木马连接了某个 IP 地址或 URL，而且该 IP 地址或 URL 没有发现有其他正当用途，那么再发现有程序去连接该 IP 地址或 URL 时，就认为该程序有异常（还可以有更复杂一些的判断标准，比如连接某个特定 IP 的特定端口，才认为有异常）；（2）模糊匹配，经过服务器端的应用程序的长期监控和分析，发现大量木马都是指向同一个 IP 段或同一个顶级域名，而且这个 IP 段或顶级域名上极少出现或根本没出现过正常的网站。那么可以认为连接到这一个 IP 段或顶级域名下的程序就都是有异常的。此种情形可有更复杂的判断标准，例如利用 game456 进行木马传播的例子：game456 的官方域名是 game456.com 和 game456.net，而很多木马所连接的域名都很接近官方域名，比如

10 game456.me、game456.3322.org、game456.com.abcd.org 等等。那么可认为凡是类似于 game456 官方域名，具有一定欺骗性的这些域名，就都是有异常的。

方式二，在云端服务器上预设一个模块用于存储黑白名单库中的黑白名单，客户端将获取的特征信息发送到云端服务器，由云端服务器根据黑白名单以及接收到的特征信息判断网络行为是否为恶意程序的网络行为。客户端上传到云端服务器的

20 特征信息可以经过加密处理，例如：通过 MD5 算法可以计算全部 URL、主机 URL、域名 URL、分级域名 URL、查询路径 URL 的哈希值，将此 MD5 哈希值发送至云端服务器，云端服务器将密文数据连同 MD5 哈希值返回客户端，密文数据包括 MD5 哈希值。

具体地，客户端获取可疑的程序的程序的网络行为中的应用层数据中的特征信息，该特征信息可以是应用层数据中的部分代码（例如 Host 字段或者 Url 字段）、应用层

25 数据中的数据包、或者应用层数据中的数据包中的一段数据；客户端将特征信息发送至云端服务器，由云端服务器根据黑白名单库中的黑白名单判断上述特征信息是否属于恶意程序的网络行为中的特征信息，并向客户端返回判断结果，如果属于，则该网络行为属于恶意程序的网络行为，进入到步骤 S118 中，如果不属于，则该网络行为属于有风险的网络行为，进入到步骤 S120 中。

30 由于云端服务器的存储空间要远远大于客户端，因此云端服务器上可以尽可能多的预先存储黑白名单库，进而可以提高网络行为识别的准确性。同时，对于最新收集到的黑白名单库之后可以及时进行处理。在一些实施例，为了节约客户端的本地资源和降低客户端的性能开销，同时也为了提高响应速度，可把数据量较大、变动比较频繁的一些黑白名单保存到云端服务器上，而把一些相对比较固定、命中

35 非常精准、数据量很小的一部分黑白名单保存到客户端上。

如果在步骤 S116 中判断是恶意程序的网络行为，则进入到步骤 S118 中。在步骤 S118 中，发送风险提示信息和/或拦截标识为可疑的程序的当前网络行为，然后进入结束步骤 S121。例如，如果可以确定程序的当前网络行为是恶意程序的网络行为，可以先暂停该程序的网络连接，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。

相反，如果在步骤 S116 中判断不是恶意程序的网络行为，则进入到步骤 S120 中。在步骤 S120 中，发送风险提示信息，然后进入结束步骤 S121。也就是，虽然可疑的程序的程序的网络行为不是恶意程序的网络行为，但该可疑的程序的程序的网络行为存在风险，因此通过步骤 S120 向用户发送风险提示信息，由用户做出最终的选择。

需要说明的是，图 1 所示的方法并限定按所示的各步骤的顺序进行，可以根据需要调整各步骤的先后顺序，另外，所述步骤也不限定于上述步骤划分，上述步骤可以进一步拆分成更多步骤也可以合并成更少步骤。

下面结合图 2 说明根据本发明另一个实施例的、适于解决上述问题的一种程序网络行为识别装置 200。

如图 2 所示，该程序网络行为识别装置 200 包括：获取模块 202、第一判断模块 204 和识别模块 206，其中：获取模块 202，用于获取程序的当前网络行为中的应用层数据；第一判断模块 204，用于判断应用层数据中是否包括未知的协议；识别模块 206，用于在应用层数据中的协议都是已知的协议时，将程序的当前网络行为标识为能够识别的程序的程序的网络行为；以及当应用层数据中包括未知的协议时，将程序的当前网络行为标识为可疑的程序的程序的网络行为。

在一些实施例中，第一判断模块 202 进一步用于根据已知的协议的格式，判断应用层数据中是否包括未知的协议。例如，在客户端上预先存储数量足够多的已知的协议，该已知的协议包括：HTTP 协议、DNS 协议、SMTP 协议等三种协议，也可以包括一些加密协议，例如：FTP 协议等。加密协议主要是在数据包中对未知的协议进行统一的加密格式进行封装，数据包里面附加一些可识别的常用协议，这些常用的协议可以包括：SNMP 协议、POP3 协议、EDONKEY 协议，或者 BITTORRENT 协议等。由于不同的协议其本身有一些固定的格式，因此对于已知的协议可检测协议的本身的格式，例如：HTTP 协议检测协议头和协议尾，Host，Refer 等字段部分，HTTP 协议包括协议头，但没有协议尾，Host、Refer 等字段均属于协议头中所包含的内容，协议头中常见的格式包括：Host、Refer、User-agent、Url 等字段部分。而未知的协议则认为是有风险的，如果是未知的协议，不在可识别的协议所包括的范围内，则有可能有自定义的协议在里面。

参见图 2，在本发明的另一个实施例中，装置 200 还包括：第二判断模块 208 和第一处理模块 210，其中第二判断模块 208 用于判断能够识别的程序的程序的网络行为是否为恶意程序的网络行为；第一处理模块 210 用于当第二判断模块 208 判断能够识

别的程序的网络行为为恶意程序的网络行为时，发送风险提示信息，和/或拦截能够识别的程序的当前网络行为；当第二判断模块 208 判断能够识别的程序的当前网络行为不是恶意程序的网络行为，将能够识别的程序的当前网络行为识别正常的网络行为。

在一些实施例中，第二判断模块 208 包括：第一获取单元和第一判断单元，其中
5 中第一获取单元用于获取能够识别的程序的当前网络行为中的应用层数据中的特征信息，特征信息可以是应用层数据中的部分代码、应用层数据中的数据包、或者应用层数据中的数据包中的一段数据；第一判断单元用于根据特征信息，判断能够识别的程序的当前网络行为是否为恶意程序的网络行为。

在一些实施例中，第二判断模块 208 还包括：第二获取单元、第一发送单元和
10 第一接收单元，其中第二获取单元用于获取能够识别的程序的当前网络行为中的应用层数据中的特征信息，特征信息可以是应用层数据中的部分代码、应用层数据中的数据包、或者应用层数据中的数据包中的一段数据；第一发送单元用于将特征信息发送至云端服务器，由云端服务器根据特征信息判断能够识别的程序的当前网络行为是否为恶意程序的网络行为；以及第一接收单元用于接收所述云端服务器返回的判断结果。
15

继续参见图 2，装置 200 还包括：第三判断模块 212 和第二处理模块 214，其中第三判断模块 212 用于判断标识为可疑的程序的当前网络行为是否为恶意程序的网络行为；第二处理模块 214 用于当第三判断模块 212 判断可疑的程序的当前网络行为是恶意程序的网络行为时，发送风险提示信息，和/或拦截标识为可疑的程序的当前网络行为；当第三判断模块 212 判断可疑的程序的当前网络行为不是恶意程序的网络行为，发
20 送风险提示信息。

在一些实施例中，第三判断模块 212 包括：第三获取单元和第二判断单元，其中第三获取单元用于获取能够识别的程序的当前网络行为中的应用层数据中的特征信息，特征信息可以是应用层数据中的部分代码、应用层数据中的数据包、或者应用
25 层数据中的数据包中的一段数据；第二判断单元用于根据特征信息，判断能够识别的程序的当前网络行为是否为恶意程序的网络行为。

在一些实施例中，第三判断模块 212 还包括：第四获取单元、第二发送单元和第二接收单元，其中第四获取单元用于获取标识为可疑的程序的当前网络行为中的应用层数据中的特征信息，特征信息可以是应用层数据中的部分代码、应用层数据中的
30 数据包、或者应用层数据中的数据包中的一段数据；第二发送单元用于将特征信息发送至云端服务器，由云端服务器根据特征信息，判断标识为可疑的程序的当前网络行为是否为恶意程序的网络行为；以及第二接收单元用于接收云端服务器返回的判断结果。

下面结合图 3 说明根据本发明又一个实施例的、适于解决上述问题的一种程序
35 网络行为识别系统 300。

如图 3 所示, 根据本发明实施例的一个方面该程序网络行为识别系统 300, 该系统包括: 客户端 302 和云端服务器 304, 其中

客户端 302, 用于在程序访问网络的过程中, 获取程序的当前网络行为中的应用层数据; 判断应用层数据中是否包括未知的协议; 如果应用层数据中的协议都是已知的协议, 则将程序的当前网络行为标识为能够识别的程序的的网络行为; 如果应用层数据中包括未知的协议, 则将程序的当前网络行为标识为可疑的程序的的网络行为, 然后将能够识别的程序的的网络行为或者可疑的程序的的网络行为的特征信息发送至云端服务器; 可选地, 该客户端可以是移动电话、平板电脑或者个人计算机等;

云端服务器 304 用于根据特征信息判断能够识别的程序的的网络行为、或可疑的程序的的网络行为是否为恶意程序的的网络行为, 并向客户端返回判断结果。

在一些实施例中, 云端服务器 304 中包括一用于存储黑白名单库的数据库, 云端服务器根据黑白名单库中的黑白名单, 判断能够识别的程序的的网络行为、或者可疑的程序的的网络行为是否为恶意程序的的网络行为。

如图 3 所示, 根据本发明实施的另一个方面该程序网络行为识别系统 300, 包括: 客户端 302 和云端服务器 304, 其中

客户端 302, 用于在程序访问网络的过程中, 获取程序的当前网络行为中的数据, 数据包包括: 应用层数据, 以及接收云端服务器 304 返回的识别结果;

云端服务端 304, 用于接收客户端 302 获取的程序的当前网络行为中数据包, 判断应用层数据中是否包括未知的协议; 若应用层数据中的协议都是已知的协议, 则将程序的当前网络行为标识为能够识别的程序的的网络行为; 若应用层数据中包括未知的协议, 则将程序的当前网络行为标识为可疑的程序的的网络行为, 向客户端发送识别结果。

在一些实施例中, 云端服务器 304 还可获取能够识别的程序的的网络行为或者可疑的程序的的网络行为的特征信息, 根据特征信息判断所述能够识别的程序的的网络行为、或所述可疑的程序的的网络行为是否为恶意程序的的网络行为, 并向客户端 304 返回判断结果, 该特征信息包括: 应用层数据中的部分代码、应用层数据中的数据包、或者应用层数据中的数据包中的一段数据。

在一些实施例中, 该客户端 302 还可包括存储器 (其可包括一个或多个计算机可读存储介质), 存储器控制器, 一个或多个处理单元 (CPU), 外设接口, RF 电路, 音频电路, 扬声器, 传声器, 输入/输出 (I/O) 子系统, 其他输入会控制客户端, 以及外部端口。客户端可以包括一个或多个光学传感器, 这些部件可以通过一个或多个通信总线或信号线来通信。

应当理解, 客户端 302 仅仅是便携式多功能设备的一个示例, 并且客户端可以具有比所示出的更多或更少的部件, 可以组合两个或更多个部件, 或者可以具有不同的部件配置或设置。

存储器可以包括高速随机存取存储器，并且还可以包括非易失性存储器，例如一个或多个磁盘存储器件、闪存器件、或其他非易失性存储器。客户端的诸如 CPU 和外设接口的其他部件对存储器的访问可由存储器控制器来控制。

5 外设接口将客户端的输入和输出外设耦接到 CPU 和存储器。一个或多个处理器运行或执行存储在存储器中的各种软件程序和/或指令集，以实现客户端的各种功能并且处理数据。

在一些实施例中，外设接口、CPU 以及存储器控制器可以在诸如芯片的单个芯片上实现。在一些其他实施例中，它们可以在分立的芯片上实现。

10 RF（射频）电路接收并发送 RF 信号。RF 电路将电信号转换为电磁信号/将电磁信号转换为电信号，并且通过该电磁信号与通信网络以及其他通信设备进行通信。RF 电路可以包括用于执行这些功能的已知电路，其包括但不限于天线系统、RF 收发机、一个或多个放大器、调谐器、一个或多个振荡器、数字信号处理器、CODEC 芯片组、用户标识模块（SIM）卡、存储器等等。

15 音频电路、扬声器、以及传声器提供了用户与客户端之间的音频接口。音频电路从外设接口接收音频数据，将该音频数据转换为电信号，并且将该电信号发送给扬声器。扬声器将该电信号转换为人听得到的声波。音频电路还接收传声器从声波转换来的电信号。音频电路将电信号转换为音频数据，并将该音频数据发送到外设接口用以进行处理。可通过外设接口从存储器和/或 RF 电路检索音频数据并且/或者将音频数据发送到存储器和/或 RF 电路。

20 I/O 子系统将客户端上的输入/输出外设耦接到外设接口。I/O 子系统可包括显示控制器和用于其他输入或控制客户端的一个或多个输入控制器。一个或多个输入控制器从/向其他输入或控制客户端接收/发送电信号。其他输入/控制客户端可以包括物理按钮、拨号盘、滑动开关、操纵杆、点击滚轮等等。在一些另选实施例中，输入控制器可以耦接到以下中的任一个：键盘、红外端口、USB 端口、以及诸如鼠标的指示设备。

25 触摸敏感式触摸屏提供了客户端与用户之间的输入接口和输出接口。显示控制器从/向触摸屏接收和/或发送电信号。触摸屏将可视输出显示给用户。可视输出可包括图形、文本、图标、视频以及其任意组合（统称为“图形”）。

30 触摸屏具有用于基于触觉和/或触感接触接受来自用户的输入的触摸敏感表面、传感器或传感器组。触摸屏以及显示控制器检测触摸屏上的接触，并将检测到的接触转换为与显示在触摸屏上的用户界面对象的交互。在一个示例实施例中，触摸屏与用户之间的接触点对应于用户的手指。在其他实施例中也可采用其他显示技术。

对于与其他实施例的识别程序的网络行为的方法类似的步骤，在这里不再详述。

35 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搜索设备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实施例的识别程序的网络行为的方法的服务器，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 540 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 540。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 5 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有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网址访问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。

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的方法，其特征在于，所述方法包括：
在程序访问网络的过程中，获取程序的当前网络行为中的应用层数据；
5 判断所述应用层数据中是否包括未知的协议；

若所述应用层数据中的协议都是已知的协议，则将所述程序的当前网络行为标识为能够识别的程序的网络行为；

若所述应用层数据中包括未知的协议，则将所述程序的当前网络行为标识为可疑的程序的网络行为。

10 2. 根据权利要求 1 所述的方法，其特征在于，所述判断所述应用层数据中是否包括未知的协议的步骤为：

根据已知的协议的格式，判断所述应用层数据中是否包括未知的协议，如果应用层数据中的协议都能识别，则判断应用层数据都是已知的协议，如果应用层数据中有至少部分协议不能识别，则判断应用层数据包括未知的协议。

15 3. 根据权利要求 2 所述的方法，其特征在于，所述已知的协议至少包括下列中的至少一个：超文本传送协议、域名系统协议、简单邮件传输协议、文件传送协议、简单网络管理协议和邮局协议第 3 版协议。

4. 根据权利要求 1 至 3 任一所述的方法，其特征在于，在将所述程序的当前网络行为标识为能够识别的程序的网络行为的步骤之后，所述方法还包括：

20 判断所述能够识别的程序的网络行为是否为恶意程序的网络行为；

若是恶意程序的网络行为，则发送风险提示信息，和/或拦截所述能够识别的程序的当前网络行为；

若不是恶意程序的网络行为，则将所述能够识别的程序的当前网络行为标识为正常的网络行为。

25 5. 根据权利要求 4 所述的方法，其特征在于，所述判断所述能够识别的程序的网络行为是否为恶意程序的网络行为的步骤包括：

获取所述能够识别的程序的网络行为中的应用层数据中的特征信息，所述特征信息包括：应用层数据中的部分代码、应用层数据中的数据包、或者应用层数据中的数据包中的一段数据；

30 根据所述特征信息，判断所述能够识别的程序的网络行为是否为恶意程序的网络行为。

6. 根据权利要求 4 所述的方法，其特征在于，所述判断所述能够识别的程序的网络行为是否为恶意程序的网络行为的步骤包括：

35 获取能够识别的程序的网络行为中的应用层数据中的特征信息，所述特征信息包括：应用层数据中的部分代码、应用层数据中的数据包、或者应用层数据中的数

据包中的一段数据；

将所述特征信息发送至云端服务器，由所述云端服务器根据所述特征信息判断所述能够识别的程序的的网络行为是否为恶意程序的的网络行为，并返回判断结果。

7. 根据权利要求 1 至 4 任一所述的方法，其特征在于，在将所述程序的当前网络行为标识为可疑的程序的的网络行为的步骤之后，所述方法还包括：

判断所述可疑的程序的的网络行为是否为恶意程序的的网络行为；

若是恶意程序的的网络行为，则发送风险提示信息，和/或拦截所述可疑的程序的当前网络行为；

若不是恶意程序的的网络行为，则发送风险提示信息。

8. 根据权利要求 7 所述的方法，其特征在于，所述判断所述可疑的程序的的网络行为是否为恶意程序的的网络行为的步骤包括：

获取所述可疑的程序的的网络行为中的应用层数据中的特征信息，所述特征信息包括：应用层数据中的部分代码、应用层数据中的数据包、或者应用层数据中的数据包中的一段数据；

根据所述特征信息，判断所述可疑的程序的的网络行为是否为恶意程序的的网络行为。

9. 根据权利要求 7 所述的方法，其特征在于，所述判断所述可疑的程序的的网络行为是否为恶意程序的的网络行为的步骤包括：

获取所述可疑的程序的的网络行为中的应用层数据中的特征信息，所述特征信息包括：应用层数据中的部分代码、应用层数据中的数据包、或者应用层数据中的数据包中的一段数据；

将所述特征信息发送至云端服务器，由所述云端服务器根据所述特征信息判断所述可疑的程序的的网络行为是否为恶意程序的的网络行为，并返回判断结果。

10. 一种识别程序的的网络行为的装置，其特征在于，所述装置包括：

获取模块，用于在程序访问网络的过程中，获取所述程序的当前网络行为中的应用层数据；

第一判断模块，用于判断所述应用层数据中是否包括未知的协议；

识别模块，用于在所述应用层数据中的协议都是已知的协议时，将所述程序的当前网络行为标识为能够识别的程序的的网络行为；以及当所述应用层数据中包括未知的协议时，将所述程序的当前网络行为标识为可疑的程序的的网络行为。

11. 根据权利要求 10 所述的装置，其特征在于，所述第一判断模块进一步用于根据已知的协议的格式，判断所述应用层数据中是否包括未知的协议。

12. 根据权利要求 11 所述的装置，其特征在于，所述已知的可以识别的协议至少包括下列中的至少一个：超文本传送协议、域名系统协议、简单邮件传输协议、文件传送协议、简单网络管理协议和邮局协议第 3 版协议。

13. 根据权利要求 10 至 12 任一所述的装置，其特征在于，所述装置还包括：
第二判断模块，用于判断所述能够识别的程序的的网络行为是否为恶意程序的
网络行为；

第一处理模块，用于当所述第二判断模块判断所述能够识别的程序的的网络行为
5 是恶意程序的的网络行为时，发送风险提示信息，和/或拦截所述能够识别的程序的当前网络行为；以及用于当所述第二判断模块判断所述能够识别的程序的的网络行为不是恶意程序的的网络行为，将所述能够识别的程序的当前网络行为识别正常的网络行为。

14. 根据权利要求 13 所述的装置，其特征在于，所述第二判断模块包括：
10 第一获取单元，用于获取能够识别的程序的的网络行为中的应用层数据中的特征信息，所述特征信息包括应用层数据中的部分代码、应用层数据中的数据包、或者应用层数据中的数据包中的一段数据；

第一判断单元，用于根据所述特征信息，判断所述能够识别的程序的的网络行为是否为恶意程序的的网络行为。

15 15. 根据权利要求 13 所述的装置，其特征在于，所述第二判断模块包括：
第二获取单元，用于获取能够识别的程序的的网络行为中的应用层数据中的特征信息，所述特征信息包括：应用层数据中的部分代码、应用层数据中的数据包、或者应用层数据中的数据包中的一段数据；

第一发送单元，用于将所述特征信息发送至云端服务器，由所述云端服务器根
20 据所述特征信息判断所述能够识别的程序的的网络行为是否为恶意程序的的网络行为；
第一接收单元，用于接收所述云端服务器返回的判断结果。

16. 根据权利要求 10 至 13 任一所述的装置，其特征在于，所述装置还包括：
第三判断模块，用于判断所述可疑的程序的的网络行为是否为恶意程序的的网络行为；

25 第二处理模块，用于当所述第三判断模块判断所述可疑的程序的的网络行为是恶意程序的的网络行为时，发送风险提示信息，和/或拦截所述可疑的程序的当前网络行为；以及用于当所述第三判断模块判断所述可疑的程序的的网络行为不是恶意程序的的网络行为时，发送风险提示信息。

17. 根据权利要求 16 所述的装置，其特征在于，所述第三判断模块包括：
30 第三获取单元，用于获取能够识别的程序的的网络行为中的应用层数据中的特征信息，所述特征信息包括：应用层数据中的部分代码、应用层数据中的数据包、或者应用层数据中的数据包中的一段数据；

第二判断单元，用于根据所述特征信息，判断所述能够识别的程序的的网络行为是否为恶意程序的的网络行为。

35 18. 根据权利要求 16 所述的装置，其特征在于，所述第三判断模块包括：

第四获取单元，用于获取所述可疑的程序的网络行为中的应用层数据中的特征信息，所述特征信息包括：应用层数据中的部分代码、应用层数据中的数据包、或者应用层数据中的数据包中的一段数据；

第二发送单元，用于将所述特征信息发送至云端服务器，由所述云端服务器根据所述特征信息，判断所述可疑的程序的网络行为是否为恶意程序的网络行为；

第二接收单元，用于接收所述云端服务器返回的判断结果。

19. 一种识别程序的网络行为的系统，其特征在于，包括：客户端和云端服务器，其中

所述客户端，用于在程序访问网络的过程中，获取程序的当前网络行为中的应用层数据；判断所述应用层数据中是否包括未知的协议；若所述应用层数据中的协议都是已知的协议，则将所述程序的当前网络行为标识为能够识别的程序的网络行为；若所述应用层数据中包括未知的协议，则将所述程序的当前网络行为标识为可疑的程序的网络行为，然后将能够识别的程序的网络行为或者可疑的程序的网络行为的特征信息发送至云端服务器，所述特征信息包括：应用层数据中的部分代码、应用层数据中的数据包、或者应用层数据中的数据包中的一段数据；

所述云端服务器，用于根据所述特征信息判断所述能够识别的程序的网络行为、或所述可疑的程序的网络行为是否为恶意程序的网络行为，并向所述客户端返回判断结果。

20. 一种识别程序的网络行为的系统，其特征在于，包括：客户端和云端服务器，其中

所述客户端，用于在程序访问网络的过程中，获取程序的当前网络行为中的数据包，所述数据包包括：应用层数据，以及接收所述云端服务器返回的识别结果；

所述云端服务端，用于接收所述客户端获取的程序的当前网络行为中数据包，判断所述应用层数据中是否包括未知的协议；若所述应用层数据中的协议都是已知的协议，则将所述程序的当前网络行为标识为能够识别的程序的网络行为；若所述应用层数据中包括未知的协议，则将所述程序的当前网络行为标识为可疑的程序的网络行为，向所述客户端发送识别结果。

21、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 至 9 中的任一所述的识别程序的网络行为的方法。

22、一种计算机可读介质，其中存储了如权利要求 21 所述的计算机程序。

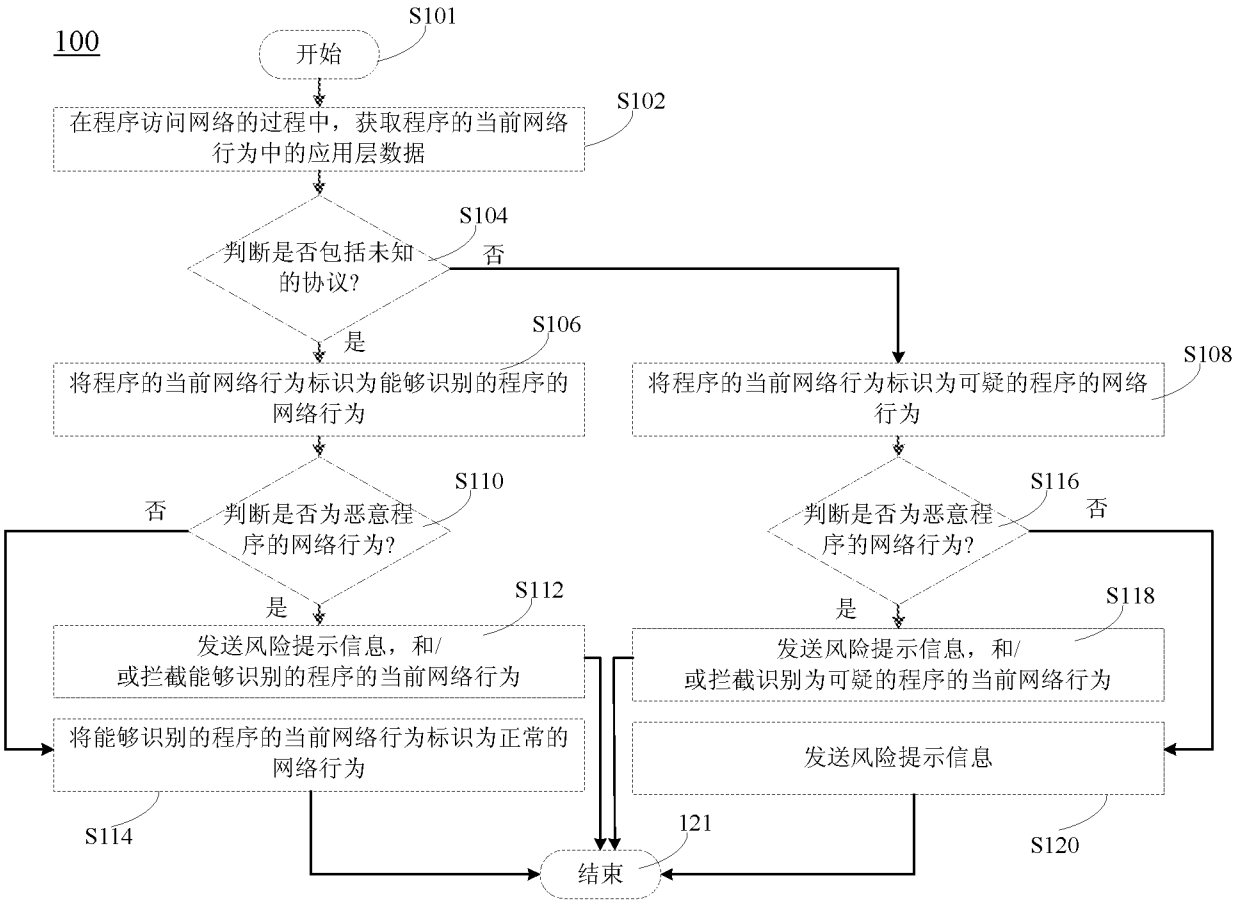


图 1

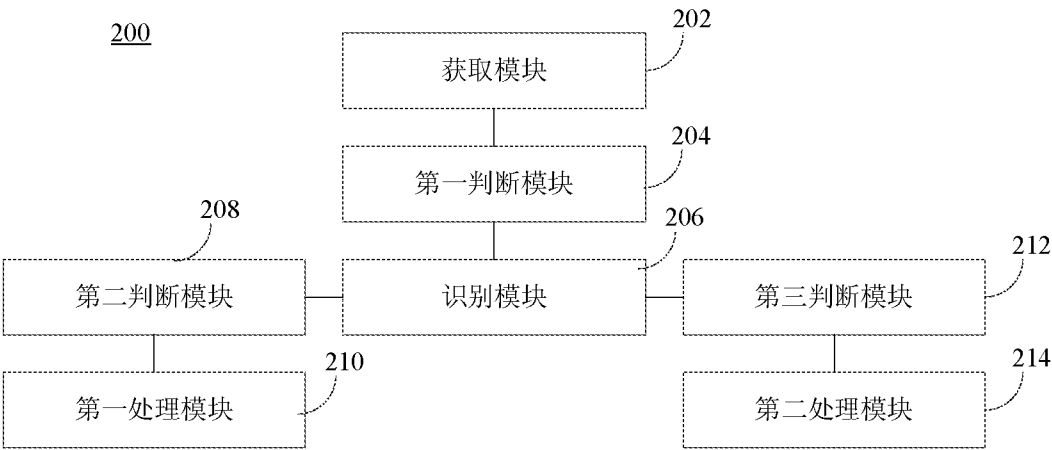


图 2

300

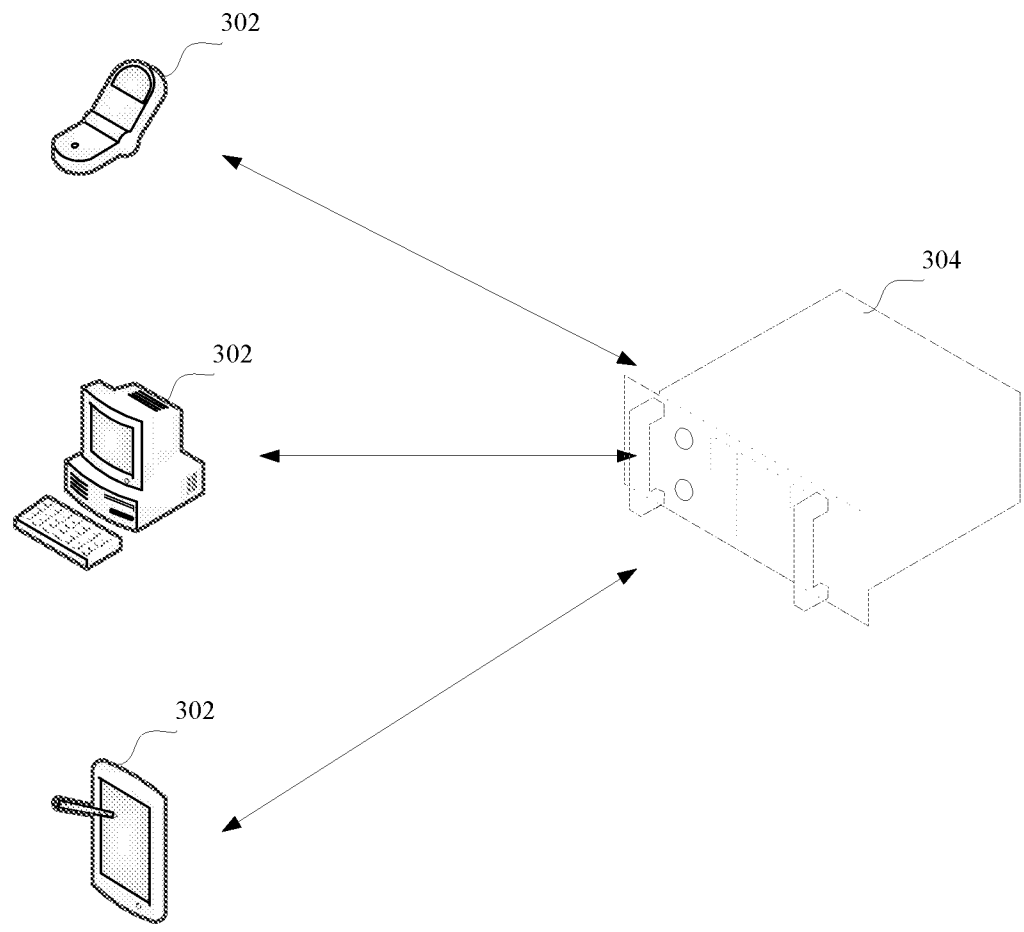


图 3

3/3

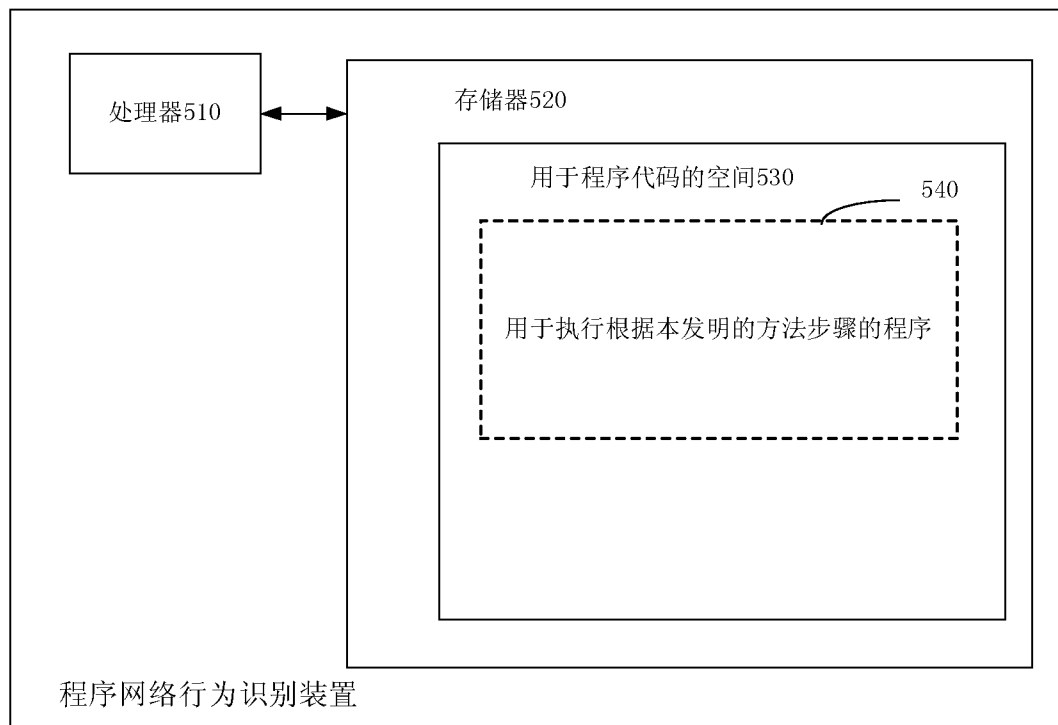


图 4

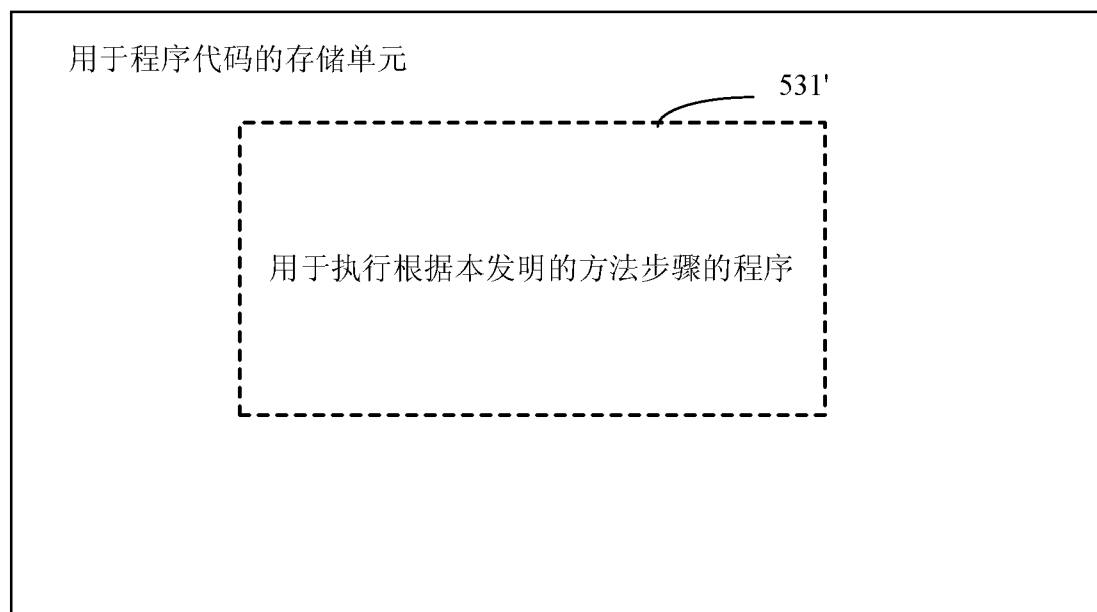


图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/083667

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)

WPI, EPODOC, CNPAT, CNKI: network action, behavior, access, protocol, application layer, menace, trojan virus, worm, shadiness, distrustful, security, unbeknown, unknown, known, distinguish, differentiate, server, client

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 103051617 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.) 17 April 2013 (17.04.2013) description, paragraphs [0005] to [0096]	1-22
PX	CN 103067360 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.) 24 April 2013 (24.04.2013) description, paragraphs [0005] to [0089]	1-22
A	CN 101272380 A (BEIDA FANGZHEN GROUP CO., LTD. et al.) 24 September 2008 (24.09.2008) description, page 2, line 4 to page 18, line 3	1-22
A	US 2010/0191853 A1 (ROJAS, Bud A. et al.) 29 July 2010 (29.07.2010) the whole document	1-22

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search 17 October 2013 (17.10.2013)	Date of mailing of the international search report 12 December 2013 (12.12.2013)
Name and mailing address of the ISA 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 TIAN, Tao Telephone No. (86-10) 62413319

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/083667

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103051617 A	17.04.2013	None	
CN 103067360 A	24.04.2013	None	
CN 101272380 A	24.09.2008	None	
US 2010/0191853 A1	29.07.2010	None	

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))

WPI, EPODOC, CNPAT, CNKI: 网络行为, 访问, 接入, 协议, 应用层, 威胁, 木马, 蠕虫, 病毒, 可疑, 安全, 未知, 陌生, 已知, 识别, 区别, 服务器, 客户端, network action, behavior, access, protocol, application layer, menace, trojan virus, worm, shadiness, distrustful, security, unbeknown, unknown, known, distinguish, differentiate, server, client

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 103051617 A (北京奇虎科技有限公司等) 17.4 月 2013 (17.04.2013) 说明书第[0005]-[0096]段	1-22
PX	CN 103067360 A (北京奇虎科技有限公司等) 24.4 月 2013 (24.04.2013) 说明书第[0005]-[0089]段	1-22
A	CN 101272380 A (北大方正集团有限公司等) 24.9 月 2008 (24.09.2008) 说明书第 2 页第 4 行-第 18 页第 3 行	1-22
A	US 2010/0191853 A1 (ROJAS, Bud A.等) 29.7 月 2010 (29.07.2010) 全文	1-22

☐ 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

17.10 月 2013 (17.10.2013)

国际检索报告邮寄日期

12.12 月 2013 (12.12.2013)

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

田涛

电话号码: (86-10) 62413319

国际检索报告

关于同族专利的信息

国际申请号

PCT/CN2013/083667

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 103051617 A	17.04.2013	无	
CN 103067360 A	24.04.2013	无	
CN 101272380 A	24.09.2008	无	
US 2010/0191853 A1	29.07.2010	无	