

(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 3 月 20 日 (20.03.2014)



(10) 国际公布号
WO 2014/040571 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2013/083629
- (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:
201210345506.7 2012 年 9 月 17 日 (17.09.2012) 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: 江爱军 (Jiang, Aijun); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。谭合力 (Tan, Heli); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。张波 (Zhang, Bo); 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, 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,

[见续页]

(54) Title: INSPECTION METHOD, DEVICE, AND SYSTEM FOR CONTROLLING NETWORK ACCESS OF CLIENT

(54) 发明名称: 控制客户端访问网络的检测方法、装置和系统

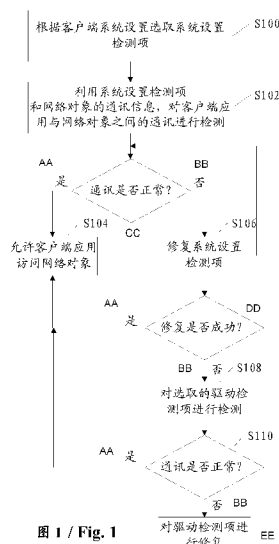


图 1 / Fig. 1

S100 Selection of the system setting inspection item on the basis of client system settings
S102 Inspection of the communication between the client application and the network object by utilizing the system setting inspection item and the communication information of the network object
S104 Permission for client application to access the network object
S106 Repairing of the system setting inspection item
S108 Inspection of the selected driver inspection item
S110 Is the communication normal?
AA Yes
BB No
CC Is the communication normal? (S110)
DD Is the repair successful?
EE Repairing of the driver inspection item

(57) Abstract: The present invention relates to the field of communications. Disclosed are an inspection method, device, and system for controlling network access of a client, allowing, from multiple dimensions such as system kernel and system settings, for inspection and repair of damages made by malicious programs to the network access of client applications. Provided in embodiments of the present invention, the inspection method for controlling the network access of the client comprises: selecting a system setting inspection item on the basis of the system setting of the client; by utilizing the system setting inspection item and communication information of a network object that a client application needs to access, inspecting the communication between the client application and the network object; when the inspection result indicates that the communication is abnormal, repairing the system setting inspection item, and when the inspection result indicates that the communication is normal, allowing the client application to access the network object; when the repair of the system setting inspection item fails, inspecting a driver inspection item, when the inspection result indicates that the communication is abnormal, repairing the driver inspection item, and when the inspection result indicates that the communication is normal, allowing the client application to access the network object.

(57) 摘要: 本发明公开了一种控制客户端访问网络的检测方法、装置和系统, 涉及通信技术领域, 能够从系统内核及系统设置等多个维度检测和修复恶意程序对客户端应用访问网络的破坏。本发明实施例提供的一种控制客户端访问网络的检测方法包括: 根据客户端系统设置选取系统设置检测项; 利用系统设置检测项和客户端应用需要访问的网络对象的通讯信息, 对客户端应用与网络对象之间的通讯进行检测; 当检测结果指示通讯异常时, 修复系统设置检测项, 当检测结果指示通讯正常时, 允许客户端应用访问网络对象; 当修复系统设置检测项失败时, 对驱动检测项进行检测, 当检测结果指示通讯异常时, 修复驱动检测项, 当检测结果指示通讯正常时, 允许客户端应用访问网络对象。

WO 2014/040571 A1



SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ,
VC, VN, ZA, ZM, ZW。

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)。

- (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,

本国际公布:

- 包括国际检索报告(条约第 21 条(3))。

控制客户端访问网络的检测方法、装置和系统

技术领域

本发明涉及通信技术领域，特别涉及一种控制客户端访问网络的检测方法、装置和系统。

发明背景

当前安全防护软件为了快速地识别和查杀新木马，同时为了减轻客户端的资源消耗，会借助于网络服务器提高木马查杀功能。例如，在云安全技术下，客户端安全软件访问云安全中心的服务器，将可疑文件的特征传给云安全中心的服务器，由云安全中心对其安全做出判定，然后客户端安全软件根据云安全中心传回的信息对木马进行报告和处理。

然而，木马病毒以及一些其他的恶意程序为了躲避安全软件的检测，会想方设法破坏客户端安全软件与网络服务器之间的网络通讯，阻止客户端安全软件访问网络服务器，导致客户端无法升级网络服务器端的病毒库，无法识别和清除新木马，削弱了客户端安全软件的安全防护性能。针对这种问题，一些客户端安全软件对主机（Host）文件或 DNS（Domain Name System，域名系统）进行检测和修复，这种仅针对某个点进行检测的方案木马查杀效果较差，现有对如何保证客户端安全软件与网络服务器之间的正常通讯还没有提出有效的解决方案。

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一种控制客户端访问网络的检测方法、装置和系统。

依据本发明的一个方面，提供了一种控制客户端访问网络的检测方法，包括：

根据客户端系统设置选取系统设置检测项；

利用所述系统设置检测项和客户端应用需要访问的网络对象的通讯信息，对客户端应用与所述网络对象之间的通讯进行检测；

当对系统设置检测项的检测结果显示通讯异常时，修复所述系统设置检测项，当检测结果指示通讯正常时，允许客户端应用访问所述网络对象；

当修复所述系统设置检测项失败时，对选取的驱动检测项进行检测，当对

驱动检测项的检测结果指示通讯异常时，修复所述驱动检测项，当对驱动检测项的检测结果指示通讯正常时，允许客户端应用访问所述网络对象。

上述通讯信息包括网络对象的域名和 IP 地址，上述系统设置检测项包括客户端系统的网络协议安全性设置、系统防火墙设置、本地 IP 地址、路由项、域名系统 DNS 设置和/或主机文件，上述利用系统设置检测项和客户端应用需要访问的网络对象的通讯信息，对客户端应用与网络对象之间的通讯进行检测包括：

检测客户端系统的网络协议安全性设置的阻止列表中是否存在网络对象的通讯信息，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常；

和/或，

检测客户端系统的系统防火墙设置的阻止列表的规则条目中是否存在网络对象的 IP 地址和客户端应用的名称，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常；和/或，

检测客户端系统是否存在与网络对象的 IP 地址在同一网段的本地 IP 地址，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常；和/或，

检测客户端系统的路由项中是否存在与网络对象的 IP 地址在同一网段的 IP 地址，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常；

和/或，

检测客户端系统的 DNS 设置中的 IP 地址是否在禁止 DNS 列表中，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常；和/或，

检测客户端系统的主机文件的各条目中是否包括网络对象的域名，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常。

当检测结果指示通讯异常时，修复系统设置检测项包括：

当检测到客户端系统的网络协议安全性设置的阻止列表中存在网络对象的通讯信息时，将网络对象的通讯信息从网络协议安全性设置的阻止列表中清除；和/或，

当检测到客户端系统的系统防火墙设置的阻止列表的规则条目中存在网络对象的 IP 地址和客户端应用的名称时，将包含了网络对象的 IP 地址或客户端应用名称的该规则条目从系统防火墙设置的阻止列表中清除；和/或，

当检测到客户端系统存在与网络对象的 IP 地址在同一网段的本地 IP 地址时，将客户端系统中与网络对象的 IP 地址在同一网段的本地 IP 地址清除；

和/或，

当检测到客户端系统的路由项中存在与网络对象的 IP 地址在同一网段的 IP 地址时,将客户端系统中存在与网络对象的 IP 地址在同一网段的 IP 地址的路由项清除;和/或,

当检测到客户端系统的 DNS 设置中的 IP 地址在禁止 DNS 列表中时,将 DNS 设置中的 IP 地址修改为可信赖的 DNS 服务器地址;和/或,

当检测到客户端系统的主机文件的各条目中包括网络对象的域名时,将客户端系统中包括网络对象的域名的主机文件的条目清除。

上述选取的驱动检测项为网络过滤驱动,本方法对选取的驱动检测项进行检测包括:

检测网络过滤驱动是否存在于黑名单中,若是,检测结果指示通讯异常;若否,检测结果指示通讯正常;

当检测结果指示通讯异常时,修复网络过滤驱动使检测结果指示通讯正常,当检测结果指示通讯正常时,允许客户端应用访问网络对象。

上述修复网络过滤驱动包括:将黑名单中的网络过滤驱动备份后,将该网络过滤驱动清除,检测结果指示通讯正常,允许客户端应用访问网络对象。

在将黑名单中的网络过滤驱动备份后,将该网络过滤驱动从黑名单中清除,检测结果指示通讯正常,允许客户端应用访问网络对象之后,本方法还包括:

当客户端应用访问网络对象失败时,若客户端应用不能成功访问信赖的第三方网络对象,确认客户端应用无法访问网络,若客户端应用能够成功访问信赖的第三方网络对象,判断客户端应用是否具有不存在于黑名单和白名单中的网络过滤驱动,若不具有,确认客户端应用无法访问网络,若具有,将该网络过滤驱动备份后清除,允许客户端应用访问网络对象。

根据本发明的另一方面,提供了一种控制客户端访问网络的检测装置,该装置包括:

检测项选取单元,适于根据客户端系统设置选取系统设置检测项;

检测单元,适于利用所述系统设置检测项和客户端应用需要访问的网络对象的通讯信息,对客户端应用与所述网络对象之间的通讯进行检测;

访问控制单元,适于当对系统设置检测项的检测结果显示异常时,修复所述系统设置检测项,当检测结果指示通讯正常时,允许客户端应用访问所述网络对象;

所述检测项选取单元,还适于选取驱动检测项进行检测;所述检测单元,

还适于当修复所述系统设置检测项失败时，对选取的驱动检测项进行检测；

所述访问控制单元，还适于当对驱动检测项的检测结果显示异常时，修复所述驱动检测项，当对驱动检测项的检测结果显示正常时，允许客户端应用访问所述网络对象。

上述通讯信息包括网络对象的域名和 IP 地址，上述系统设置检测项包括客户端系统的网络协议安全性设置、系统防火墙设置、本地 IP 地址、路由项、域名系统 DNS 设置和/或主机文件，检测单元，具体适于检测客户端系统的网络协议安全性设置的阻止列表中是否存在网络对象的通讯信息，若是，检测结果显示异常，若否，检测结果显示正常；和/或，

检测客户端系统的系统防火墙设置的阻止列表的规则条目中是否存在网络对象的 IP 地址和客户端应用的名称，若是，检测结果显示异常，若否，检测结果显示正常；和/或，

检测客户端系统是否存在与网络对象的 IP 地址在同一网段的本地 IP 地址，若是，检测结果显示异常，若否，检测结果显示正常；和/或，

检测客户端系统的路由项中是否存在与网络对象的 IP 地址在同一网段的 IP 地址，若是，检测结果显示异常，若否，检测结果显示正常；

和/或，

检测客户端系统的 DNS 设置中的 IP 地址是否在禁止 DNS 列表中，若是，检测结果显示异常，若否，检测结果显示正常；和/或，

检测客户端系统的主机文件的各条目中是否包括网络对象的域名，若是，检测结果显示异常，若否，检测结果显示正常。

上述访问控制单元，适于当检测结果显示异常时，通过下述方式修复系统设置检测项：

当检测到客户端系统的网络协议安全性设置的阻止列表中存在网络对象的通讯信息时，将网络对象的通讯信息从网络协议安全性设置的阻止列表中清除；和/或，

当检测到客户端系统的系统防火墙设置的阻止列表的规则条目中存在网络对象的 IP 地址和客户端应用的名称时，将包含了网络对象的 IP 地址和客户端应用名称的该规则条目从系统防火墙设置的阻止列表中清除；和/或，

当检测到客户端系统存在与网络对象的 IP 地址在同一网段的本地 IP 地址时，将客户端系统中与网络对象的 IP 地址在同一网段的本地 IP 地址清除；

当检测到客户端系统的路由项中存在与网络对象的 IP 地址在同一网段的 IP 地址时,将客户端系统中存在与网络对象的 IP 地址相同的 IP 地址的路由项清除;和/或,

当检测到客户端系统的 DNS 设置中的 IP 地址在禁止 DNS 列表中时,将 DNS 设置中的 IP 地址修改为可信赖的 DNS 服务器地址;和/或,

当检测到客户端系统的主机文件的各条目中包括网络对象的域名时,将客户端系统中包括网络对象的域名的主机文件的条目清除。

上述检测项选取单元,还适于选取客户端系统的网络过滤驱动作为系统设置检测项;

检测单元,还适于在访问控制单元允许客户端应用访问网络对象之后,当客户端应用访问网络对象失败时,检测网络过滤驱动是否存在于黑名单中,若是,检测结果指示通讯异常;若否,检测结果指示通讯正常;

访问控制单元,还适于当检测结果指示通讯异常时,修复网络过滤驱动使检测结果指示通讯正常,当检测结果指示通讯正常时,允许客户端应用访问网络对象。

上述访问控制单元,适于通过下述方式修复网络过滤驱动:

将黑名单中的网络过滤驱动备份后,将该网络过滤驱动清除,检测结果指示通讯正常,允许客户端应用访问网络对象。

上述访问控制单元,还适于在将黑名单中的网络过滤驱动备份后,将该网络过滤驱动从黑名单中清除,检测结果指示通讯正常,允许客户端应用访问网络对象之后,当客户端应用访问网络对象失败时,若客户端应用不能成功访问信赖的第三方网络对象,确认客户端应用无法访问网络,若客户端应用能够成功访问信赖的第三方网络对象,判断客户端应用是否具有不存在于黑名单和白名单中的网络过滤驱动,若不具有,确认客户端应用无法访问网络,若具有,将该网络过滤驱动备份后清除,允许客户端应用访问网络对象。

本发明实施例提供的一种通信系统包括客户端设备,所述客户端设备包括上述的控制客户端访问网络的检测装置,

客户端设备上运行的客户端应用需要访问的网络对象为云安全中心服务器;

控制客户端访问网络的检测装置允许客户端应用访问云安全中心服务器时,该客户端应用,适于将可疑文件的信息发送至云安全中心服务器,并接收

云安全中心服务器下发的对可疑文件的信息的分析结果。

根据本发明的又一个方面，提供了一种计算机程序，包括计算机可读代码，当所述计算机可读代码在客户端上运行时，导致所述客户端执行上述任一项所述的控制客户端访问网络的检测方法。

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。

由上所述，本发明实施例通过选取系统设置检测项和驱动检测项，利用系统设置检测项、驱动检测项与网络对象的通讯信息进行访问控制的技术手段，能够从系统内核到系统设置等多个维度检测恶意程序对客户端应用访问系统网络的破坏，有效地修复恶意程序对客户端应用与网络对象之间通讯造成的破坏，保证了客户端应用对网络对象的正常访问。

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。

附图简要说明

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一种控制客户端访问网络的检测流程图；

图 2 示出了根据本发明又一个实施例的基于网络过滤驱动的修复恶意程序对客户端应用访问网络对象的破坏的方法流程图；以及

图 3 示出了根据本发明一个实施例的一种控制客户端访问网络的检测装置结构示意图；

图 4 示出了本发明实施例提供的一种通信系统的结构示意图。

实施本发明的方式

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。

本申请可以应用于计算机系统/服务器，其可与众多其它通用或专用计算机系统环境或配置一起操作。适于与计算机系统/服务器一起使用的众所周知的计算机系统、环境和/或配置的例子包括但不限于：个人计算机系统、服务器计算机系统、瘦客户机、厚客户机、手持或膝上设备、基于微处理器的系统、机顶盒、可编程消费电子产品、网络个人电脑、小型计算机系统、大型计算机系统和包括上述任何系统的分布式云计算技术环境，等等。

计算机系统/服务器可以在由计算机系统执行的计算机系统可执行指令（诸如程序模块）的一般语境下描述。通常，程序模块可以包括例程、程序、目标程序、组件、逻辑、数据结构等等，它们执行特定的任务或者实现特定的抽象数据类型。计算机系统/服务器可以在分布式云计算环境中实施，分布式云计算环境中，任务是由通过通信网络链接的远程处理设备执行的。在分布式云计算环境中，程序模块可以位于包括存储设备的本地或远程计算系统存储介质上。

计算机系统/服务器也可以与一个或多个外部设备——诸如键盘、指向设备、显示器等等——通信，与一个或者多个使用户能与计算机系统/服务器交互的设备通信，和/或与使计算机系统/服务器能与一个或多个其它计算设备通信的任何设备（例如网卡，调制解调器等等）通信。这种通信可以通过输入/输出（I/O）接口进行。并且，计算机系统/服务器还可以通过网络适配器与一个或者多个网络——诸如局域网（LAN），广域网（WAN）和/或公共网络（例如因特网）——通信。如图所示，网络适配器通过总线与计算机系统/服务器的其它模块通信。应当明白，其它硬件和/或软件模块可以与计算机系统/服务器一起使用。例子包括但不限于：微代码、设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID系统、磁带驱动器以及数据备份存储系统，等等。

本发明一个实施例提供一种控制客户端访问网络的检测方法，参见图 1，所述方法包括：

S100：根据客户端系统选取系统设置检测项，所述系统设置检测项包括客户端系统的网络协议安全性（Internet Protocol Security, IPSec）设置、系统防火墙设置、本地 IP 地址、路由项、DNS 设置和主机文件中的一项或多项。

S102：利用所述系统设置检测项和客户端应用需要访问的网络对象的通讯信息，对客户端应用与所述网络对象之间的通讯进行检测。

本实施例中，通常将上述步骤 S100 中选取的系统设置检测项作为基础的检测项，并在本步骤中对上述所有的系统设置检测项进行检测，可以理解，在本步骤中也可以仅对上述的部分通讯检测项进行检测。通过对系统设置检测项的检测，本方案能够从系统设置的维度对客户端应用访问系统网络进行检测和修复。

上述网络对象为客户端应用要访问的网络设备或系统，如网络对象可以为 Windows 系统下的云安全中心服务器等。

S104: 当对系统设置检测项的检测结果显示通讯正常时，允许客户端应用访问所述网络对象。

S106: 当对系统设置检测项的检测结果显示通讯异常时，修复所述系统设置检测项使检测结果指示通讯正常，当通讯正常时允许客户端应用访问所述网络对象。

S108: 当修复所述系统设置检测项失败时，对选取的驱动检测项进行检测，进入步骤 S110，当修复所述系统设置检测项成功时，表明通讯正常，允许客户端应用访问所述网络对象。通过对驱动检测项的检测，本方案能够从系统内核的维度对客户端应用访问系统网络进行检测和修复。

S110: 当对驱动检测项的检测结果显示通讯异常时，修复所述驱动检测项，当对驱动检测项的检测结果显示通讯正常时，允许客户端应用访问所述网络对象。

由上所述，本发明实施例通过选取系统设置检测项和驱动检测项，利用系统设置检测项、驱动检测项与网络对象的通讯信息进行访问控制的技术手段，能够从系统内核到系统设置等多个维度检测恶意程序对客户端应用访问系统网络的破坏，有效地修复恶意程序对客户端应用与网络对象之间通讯造成的破坏，保证了客户端应用对网络对象的正常访问。

本发明又一个实施例以客户端应用为用于保证客户端网络安全的客户端安全应用、客户端应用需要访问的网络对象为云安全中心服务器的场景为例进行说明。

云计算环境包括云计算消费者使用的本地计算设备可以与其相通信的一个或者多个云计算节点，本地计算设备诸如个人数字辅助设备（PDA）或者是移动电话，台式电脑，笔记本电脑，和/或汽车计算机系统。节点之间可以相互通信。可以在一个或者多个网络——诸如如上所述的私有云、共同体云、公共

云或混合云或者它们的组合——中，将节点进行物理或者虚拟分组（图中未示出）。这允许云计算环境提供云消费者无需在本地计算设备上维护资源就能请求的基础架构即服务、平台即服务和/或软件即服务。应当明白，计算节点以及云计算环境可以与任何类型的网络上的和/或网络可寻址的连接上的任何类型的计算设备（例如使用网络浏览器）通信。

云安全架构基于云计算环境实现，是将所有云安全客户端与云安全服务器实时连接，客户端不断采集上报更新，在服务器端组成一庞大的恶意程序数据库，并将主动防御的分析比对操作放在服务器端完成，从而使整个云安全网络成为一主动防御工具；针对具有威胁的程序行为进行收集并保存在服务器的数据库中，在服务器端进行恶意软件分析时支持直接使用程序行为进行恶意程序判定；

另外，本发明实施例通过客户端收集程序行为并关联到程序特征，从而在数据库中记录程序特征及其对应的程序行为，根据收集到的程序行为和程序特征的关联关系，可以在数据库中对样本进行分析归纳，从而有助于对软件或程序进行黑白的分类判别，还可以针对黑名单中的恶意软件制定相应的清除或恢复措施。

然而，木马病毒以及一些其他的恶意程序为了躲避安全软件的检测，会想方设法破坏客户端安全软件与网络服务器，例如，云安全服务器之间的网络通讯，阻止客户端安全软件访问网络服务器，导致客户端无法升级网络服务器端的病毒库，无法识别和清除新木马。

网络对象的通讯信息包括网络对象的域名和 IP 地址，如云安全中心服务器的多个域名构成的域名列表和多个 IP 地址构成的 IP 地址列表，该域名列表可以表示为 CloudSecCentre (Domain)={D1,D2,...,Dn}，该 IP 地址列表可以表示为 CloudSecCentre (IP)={IP1,IP2,...,IPn}。

则利用系统设置检测项和客户端应用需要访问的网络对象的通讯信息，对客户端应用与所述网络对象之间的通讯进行的检测可以包括如下：

（1）IPSec 设置

考虑到恶意程序（如木马）会将安全厂商的云安全中心服务器 IP 地址或域名加入到 IPSec 设置的阻止列表中来破坏网络通讯，本实施例中检测客户端系统的网络协议安全性设置的阻止列表中是否存在网络对象的通讯信息，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常。

例如,读取客户端系统的IPSec设置,检查设置项的阻止列表中是否存在云安全中心的域名 CloudSecCentre (Domain)和 IP 地址 CloudSecCentre (IP)的项目,如果存在则予以清除,如果不存在,不对 IPSec 设置进行修改。可选的,本实施例中也可以直接对 IPSec 设置中的所有信息进行检测,判断网络对象的通讯信息是否在 IPSec 设置中,若在将网络对象的通讯信息从 IPSec 设置中清除,若不在,保持 IPSec 设置不变。

(2) 系统防火墙设置

考虑到木马会修改 Vista 及以上平台的系统防火墙的出入站规则,把包含云安全中心服务器 IP 地址或客户端安全应用名称的规则条目加入阻止列表中来破坏网络通讯,本实施例中检测客户端系统的系统防火墙设置的阻止列表的规则条目中是否存在网络对象的 IP 地址或客户端应用的名称,若是,检测结果指示通讯异常,若否,检测结果指示通讯正常。

例如,读取客户端系统的系统防火墙设置,逐一检查系统防火墙的阻止列表中的规则条目是否存在云安全中心 IP 地址 CloudSecCentre(IP)或客户端安全应用的名称,若存在则予以清除,即将网络对象的 IP 地址或客户端应用名称的规则条目从系统防火墙设置的阻止列表中清除,若不存在,保持原系统防火墙的设置。

(3) 本地 IP 地址

考虑到木马会通过客户端添加与云安全中心服务器在同一网段的 IP 地址及无效网关地址,使得客户端应用无法访问云安全中心服务器 IP 来破坏通讯,本实施例检测客户端系统是否存在与网络对象的 IP 地址在同一网段的本地 IP 地址,若是,检测结果指示通讯异常,若否,检测结果指示通讯正常。

例如,读取客户端系统的所有 IP 地址设置,逐一检查是否存在有 IP 地址与云安全中心服务器 IP 地址 CloudSecCentre(IP)中的某一 IP 在同一网段内,如果存在则清除客户端的此 IP 地址项,即将客户端系统中与网络对象的 IP 地址在同一网段的本地 IP 地址清除,如果不存在,保持客户端系统的 IP 地址设置。

(4) 路由项

考虑到木马会设置错误的路由项导致客户端应用无法访问云安全中心服务器 IP 地址来破坏通讯,本实施例检测客户端系统的路由项中是否存在与网络对象的 IP 地址在同一网段的 IP 地址,若是,检测结果指示通讯异常,若否,检测结果指示通讯正常。

例如，读取客户端系统的所有路由项，逐一检查路由项的网络地址是否与云安全中心服务器 IP 地址 CloudSecCentre(IP)中的网络地址相同，如果相同则清除此路由项，即将客户端系统中存在与网络对象的 IP 地址在同一网段的 IP 地址的路由项清除，如果不同，保持原路由项。

(5) DNS 设置

考虑到木马会修改客户端系统的 DNS 设置，将客户端指向木马作者控制的黑 DNS 服务器，导致无法解析云安全中心域名，从而无法正常通讯，本实施例当检测到客户端系统的 DNS 设置中的 IP 地址在禁止 DNS 列表中时，将 DNS 设置中的 IP 地址修改为可信赖的 DNS 服务器地址。该禁止 DNS 列表由已获知的非法 IP 地址或者禁止客户端应用访问的 IP 地址构成，也可以称之为黑 DNS 列表。

例如，读取客户端系统的网络 DNS 设置，检查 DNS 的 IP 地址是否在禁止 DNS 列表中，如果在，则将 DNS 设置中的 IP 地址修改为可信赖的 DNS 服务器地址，如将 DNS 修正为预置的 DNS 服务器地址：8.8.8.8 和 8.8.4.4，如果不在，保持客户端系统的网络 DNS 设置不变。

(6) 主机文件 (Hosts)

考虑到木马会在客户端系统的主机文件中添加云安全中心服务器域名并使其指向错误的 IP 地址来破坏通讯，本实施例当检测到客户端系统的主机文件的各条目中包括网络对象的域名时，将客户端系统中包括网络对象的域名的主机文件的条目清除。主机文件通常由多行的信息构成，每行信息可视为一个条目，条目中设置有域名信息等。

例如，主机文件通常位于客户端系统的 c:\windows\system32\drivers\etc 目录下，读取客户端系统的主机文件，逐一检查其中的每一条目中的域名是否包含云安全中心的域名 CloudSecCentre (Domain)，如果包含，则将客户端系统中包括网络对象的域名的主机文件的条目清除，如果不包含，则保持主机文件的条目不变。

由上可见，本实施例中采用的修复的方式包括下述的至少一种或其组合：

当检测到客户端系统的 IPsec 设置的阻止列表中存在网络对象的通讯信息时，将网络对象的通讯信息从 IPsec 设置的阻止列表中清除；

当检测到客户端系统的系统防火墙设置的阻止列表的规则条目中存在网络对象的 IP 地址或客户端应用的名称时，将网络对象的 IP 地址或客户端应用名称

的规则条目从系统防火墙设置的阻止列表中清除；

当检测到客户端系统存在与网络对象的 IP 地址在同一网段的本地 IP 地址时，将客户端系统中与网络对象的 IP 地址在同一网段的本地 IP 地址清除；

当检测到客户端系统的路由项中存在与网络对象的 IP 地址在同一网段的 IP 地址时，将客户端系统中存在与网络对象的 IP 地址在同一网段的 IP 地址的路由项清除；

当检测到客户端系统的 DNS 设置中的 IP 地址在禁止 DNS 列表中时，将 DNS 设置中的 IP 地址修改为可信赖的 DNS 服务器地址；

当检测到客户端系统的主机文件的各条目中包括网络对象的域名时，将客户端系统中包括网络对象的域名的主机文件的条目清除。

本实施例中上述系统设置检测项的选取，以及检测和修复的具体方式等是在与木马（如典型的“飓风木马”）对抗实践过程中总结出来的，能有效地修复木马对云安全中心网络通讯造成的破坏，以保证客户端安全软件与云安全中心的正常通讯，为后面的木马查杀提供可靠的网络环境，使得安全软件发挥最好的木马查杀效果。

由于多数情况下，在执行完上述六个关键点的操作后，已经能够检测出并修复完恶意程序对客户端应用访问 Windows 系统网络的破坏，则此时允许客户端安全应用访问云安全中心服务器，从而能够保证客户端及时快速地将可疑文件上报云安全中心服务器。

若在执行完上述六个关键点的木马检测和修复后，客户端安全应用还无法访问云安全中心服务器，则本实施例还包括选取客户端系统的网络过滤驱动作为驱动检测项，基于 NDIS（Network Driver Interface Specification，网络驱动接口规范）网络过滤驱动进行木马查杀。

（7）网络过滤驱动

网络过滤驱动通常包括网络过滤驱动文件和注册表信息，本实施例检测网络过滤驱动是否存在于黑名单中，若是，检测结果指示通讯异常；若否，检测结果指示通讯正常；

当检测结果指示通讯异常时，修复所述网络过滤驱动使检测结果指示通讯正常，当检测结果指示通讯正常时，允许客户端应用访问所述网络对象。参见图 2，示出了基于网络过滤驱动的修复恶意程序对客户端应用访问网络对象的破坏的方法流程图，具体处理如下：

S200: 判断客户端应用能否访问网络对象。

若在执行完上述六个关键点的检测和修复后，客户端应用能访问网络对象，通讯正常，则检测结束。

若在执行完上述六个关键点的检测和修复后，客户端应用还不能访问网络对象，执行步骤 S202。

S202: 获取客户端系统中的所有网络过滤驱动标识信息。

网络过滤驱动标识信息包括网络过滤驱动的签名信息和/或版本信息。通过枚举注册表 HLM\SYSTEM\CurrentControlSet\Control\Network 和 INetCfg 网络配置接口读取系统中所有网络过滤驱动。

S204: 检查网络过滤驱动是否在黑名单和白名单中。

白名单中记录了允许的网络过滤驱动标识信息，黑名单中记录了禁止的网络过滤驱动标识信息。

将位于黑名单中的网络过滤驱动的状态设置为黑，其中，黑代表不可信，将位于白名单中的网络过滤驱动的状态设置为白，白代表可信，将既不位于黑名单中也不位于白名单中的网络过滤驱动的状态设置为灰，灰代表未知。

若客户端系统中的所有网络过滤驱动都位于白名单中，则不在进行后续处理，检测结束，否则，执行步骤 S206。

S206: 若客户端系统中存在黑的网络过滤驱动，则将黑名单中的网络过滤驱动备份后，将黑名单中的网络过滤驱动清除，此时的检测结果指示通讯正常，允许客户端应用访问所述网络对象，执行步骤 S208。

S208: 判断此时的客户端应用能否访问网络对象，若是，通讯正常，结束操作，若否，执行步骤 S210。

S210: 判断客户端在当前的用户环境下是否能够访问信赖的第三方网络对象，若能够，执行步骤 S212，若不能，说明客户端本身的访问出现问题，客户端无法访问网络，结束操作。通过上述在用户环境下检测客户端应用对网络对象的访问，本方案还从用户态的维度对客户端应用访问系统网络进行了检测和修复。

由上可知，本方案能够从系统内核到用户态以及系统设置等多个维度全面检测恶意程序对客户端应用访问系统网络的破坏，保证在进行恶意程序的查杀之前有一个可靠的网络通讯环境。

S212: 判断客户端应用是否具有不存在于黑名单和白名单中的网络过滤驱

动，即是否存在灰的网络过滤驱动，若不具有灰的网络过滤驱动，确认客户端应用无法访问网络，若具有，执行步骤 S214。

S214: 将该灰的网络过滤驱动备份后清除，允许客户端应用访问所述网络对象。

可以理解，对网络过滤驱动的检测也可以和上述六个关键点同时执行。

由上所述，本发明实施例通过选取系统设置检测项和驱动检测项，利用系统设置检测项、驱动检测项与网络对象的通讯信息进行访问控制的技术手段，能够从系统内核到系统设置等多个维度检测恶意程序对客户端应用访问系统网络的破坏，有效地修复恶意程序对客户端应用与网络对象之间通讯造成的破坏，保证了客户端应用对网络对象的正常访问。

本发明一个实施例还提供了一种控制客户端访问网络的检测装置，参见图 3，该装置包括：

检测项选取单元 300，适于根据客户端系统选取系统设置检测项，其中该系统设置检测项包括客户端系统的网络协议安全性设置、系统防火墙设置、本地 IP 地址、路由项、域名系统 DNS 设置和/或主机文件；

检测单元 302，适于利用系统设置检测项和客户端应用需要访问的网络对象的通讯信息，对客户端应用与网络对象之间的通讯进行检测；

访问控制单元 304，适于当对系统设置检测项的检测结果显示通讯异常时，修复所述系统设置检测项，当检测结果指示通讯正常时，允许客户端应用访问所述网络对象；

检测项选取单元 300，还适于选取驱动检测项进行检测；检测单元 302，还适于当修复所述系统设置检测项失败时，对选取的驱动检测项进行检测；

访问控制单元 304，还适于当对驱动检测项的检测结果显示通讯异常时，修复所述驱动检测项，当对驱动检测项的检测结果显示通讯正常时，允许客户端应用访问所述网络对象。

其中，上述通讯信息包括网络对象的域名和 IP 地址，检测单元 302，具体适于检测客户端系统的网络协议安全性设置的阻止列表中是否存在网络对象的通讯信息，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常；和/或，

检测客户端系统的系统防火墙设置的阻止列表的规则条目中是否存在网络对象的 IP 地址或客户端应用的名称，若是，检测结果指示通讯异常，若否，检

测结果指示通讯正常；和/或，

检测客户端系统是否存在与网络对象的 IP 地址在同一网段的本地 IP 地址，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常；和/或，

检测客户端系统的路由项中是否存在与网络对象的 IP 地址在同一网段的 IP 地址，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常；

和/或，

检测客户端系统的 DNS 设置中的 IP 地址是否在禁止 DNS 列表中，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常；和/或，

检测客户端系统的主机文件的各条目中是否包括网络对象的域名，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常。

其中，访问控制单元 304，适于当检测结果指示通讯异常时，通过下述方式修复系统设置检测项：

当检测到客户端系统的网络协议安全性设置的阻止列表中存在网络对象的通讯信息时，将网络对象的通讯信息从网络协议安全性设置的阻止列表中清除；和/或，

当检测到客户端系统的系统防火墙设置的阻止列表的规则条目中存在网络对象的 IP 地址或客户端应用的名称时，将包含网络对象的 IP 地址或客户端应用名称的规则条目从系统防火墙设置的阻止列表中清除；和/或，

当检测到客户端系统存在与网络对象的 IP 地址在同一网段的本地 IP 地址时，将客户端系统中与网络对象的 IP 地址在同一网段的本地 IP 地址清除；

和/或，

当检测到客户端系统的路由项中存在与网络对象的 IP 地址在同一网段的 IP 地址时，将客户端系统中存在与网络对象的 IP 地址相同的 IP 地址的路由项清除；和/或，

当检测到客户端系统的 DNS 设置中的 IP 地址在禁止 DNS 列表中时，将 DNS 设置中的 IP 地址修改为可信赖的 DNS 服务器地址；和/或，

当检测到客户端系统的主机文件的各条目中包括网络对象的域名时，将客户端系统中包括网络对象的域名的主机文件的条目清除。

可选的，检测项选取单元 300，具体适于选取网络过滤驱动作为所述驱动检测项；

检测单元 302，还适于检测网络过滤驱动是否存在于黑名单中，若是，检测

结果指示通讯异常；若否，检测结果指示通讯正常；

访问控制单元 304，还适于当检测结果指示通讯异常时，修复网络过滤驱动使检测结果指示通讯正常，当检测结果指示通讯正常时，允许客户端应用访问网络对象。

其中，上述检测单元 302，具体适于通过下列方式，检测网络过滤驱动是否存在于黑名单中：从客户端系统的注册表和网络配置接口中获取网络过滤驱动的签名信息和版本信息；当网络过滤驱动的签名信息和版本信息位于黑名单中时，确认该网络过滤驱动存在于黑名单中，当网络过滤驱动的签名信息和版本信息不位于黑名单中时，确认该网络过滤驱动不存在于黑名单中。

其中，访问控制单元 304，适于通过下述方式修复网络过滤驱动：将黑名单中的网络过滤驱动备份后，将该网络过滤驱动清除，检测结果指示通讯正常，允许客户端应用访问网络对象。

进一步的，访问控制单元 304，还适于在将黑名单中的网络过滤驱动备份后，将该网络过滤驱动从黑名单中清除，检测结果指示通讯正常，允许客户端应用访问网络对象之后，当客户端应用访问网络对象失败时，若客户端应用不能成功访问信赖的第三方网络对象，确认客户端应用无法访问网络，若客户端应用能够成功访问信赖的第三方网络对象，从客户端系统的注册表和网络配置接口中获取网络过滤驱动的签名信息和/或版本信息，根据网络过滤驱动的签名信息和/或版本信息判断客户端应用是否具有不存在于黑名单和白名单中的网络过滤驱动，若不具有，确认客户端应用无法访问网络，若具有，将该网络过滤驱动备份后清除，允许客户端应用访问网络对象。

检测单元 302，具体适于通过下列方式，检测网络过滤驱动是否存在于黑名单中：从客户端系统的注册表和网络配置接口中获取网络过滤驱动的签名信息和/或版本信息；当网络过滤驱动的签名信息和/或版本信息位于黑名单中时，确认该网络过滤驱动存在于黑名单中，当网络过滤驱动的签名信息和/或版本信息不位于黑名单中时，确认该网络过滤驱动不存在于黑名单中；

检测单元 302，具体适于通过下列方式，判断客户端应用是否具有不存在于黑名单和白名单中的网络过滤驱动：

当网络过滤驱动的签名信息和/或版本信息不存在于黑名单和白名单中时，确认客户端应用具有不存在于黑名单和白名单中的网络过滤驱动，否则，确认客户端应用不具有不存在于黑名单和白名单中的网络过滤驱动。

本发明装置实施例中各单元的具体工作方式可以参见本发明的方法实施例，在此不再赘述。

由上所述，本发明实施例通过选取网络协议安全性设置、系统防火墙设置、本地 IP 地址、路由项、DNS 设置和主机文件作为系统设置检测项，利用系统设置检测项与网络对象的通讯信息进行访问控制的技术手段，能够从系统内核到用户态以及系统设置等多个维度检测恶意程序对客户端应用访问 Windows 系统网络的破坏，有效地修复恶意程序对客户端应用与网络对象之间通讯造成的破坏，保证了客户端应用对网络对象的正常访问。

本发明实施例还提供了一种通信系统，参见图 4，该通信系统包括客户端设备 400，客户端设备 400 包括如上述实施例提供的至少一种的控制客户端访问网络的检测装置 402，

客户端设备 400 上运行的客户端应用 406 需要访问的网络对象为云安全中心服务器 404；

控制客户端访问网络的检测装置 402 允许客户端应用访问云安全中心服务器 404 时，客户端应用 406，适于将可疑文件的信息发送至云安全中心服务器 404，并接收云安全中心服务器 404 下发的对该可疑文件的信息的分析结果。

由上所述，本发明实施例通过选取网络协议安全性设置、系统防火墙设置、本地 IP 地址、路由项、DNS 设置和主机文件作为系统设置检测项，利用系统设置检测项与网络对象的通讯信息进行访问控制的技术手段，能够从系统内核到用户态以及系统设置等多个维度检测恶意程序对客户端应用访问 Windows 系统网络的破坏，有效地修复恶意程序对客户端应用与网络对象之间通讯造成的破坏，保证了客户端应用对网络对象的正常访问。

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控制客户端访问网络的检测装置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。

当本发明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计算机程序时，该计算机程序包括计算机可读代码，当该计算机可读代码在客

户端上运行时，导致客户端执行这里所述的控制客户端访问网络的检测方法。

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。

权利要求书

1、一种控制客户端访问网络的检测方法，所述方法包括：

根据客户端系统设置选取系统设置检测项；

利用所述系统设置检测项和客户端应用需要访问的网络对象的通讯信息，对客户端应用与所述网络对象之间的通讯进行检测；

当对系统设置检测项的检测结果显示通讯异常时，修复所述系统设置检测项，当检测结果指示通讯正常时，允许客户端应用访问所述网络对象；

当修复所述系统设置检测项失败时，对选取的驱动检测项进行检测，当对驱动检测项的检测结果显示通讯异常时，修复所述驱动检测项，当对驱动检测项的检测结果显示通讯正常时，允许客户端应用访问所述网络对象。

2、根据权利要求1所述的方法，其中，所述系统设置检测项包括客户端系统的网络协议安全性设置、系统防火墙设置、本地IP地址、路由项、域名系统DNS设置和/或主机文件。

3、根据权利要求2所述的方法，其中，所述通讯信息包括网络对象的域名和IP地址，所述利用所述系统设置检测项和客户端应用需要访问的网络对象的通讯信息，对客户端应用与所述网络对象之间的通讯进行检测包括：

检测客户端系统的网络协议安全性设置的阻止列表中是否存在网络对象的通讯信息，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常；

和/或，

检测客户端系统的系统防火墙设置的阻止列表的规则条目中是否存在网络对象的IP地址或客户端应用的名称，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常；和/或，

检测客户端系统是否存在与网络对象的IP地址在同一网段的本地IP地址，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常；和/或，

检测客户端系统的路由项中是否存在与网络对象的IP地址在同一网段的IP地址，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常；

和/或，

检测客户端系统的DNS设置中的IP地址是否在禁止DNS列表中，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常；和/或，

检测客户端系统的主机文件的各条目中是否包括网络对象的域名，若是，

检测结果指示通讯异常，若否，检测结果指示通讯正常。

4、根据权利要求3所述的方法，其中，所述当检测结果指示通讯异常时，修复所述系统设置检测项包括：

当检测到客户端系统的网络协议安全性设置的阻止列表中存在网络对象的通讯信息时，将网络对象的通讯信息从网络协议安全性设置的阻止列表中清除；和/或，

当检测到客户端系统的系统防火墙设置的阻止列表的规则条目中存在网络对象的IP地址或客户端应用的名称时，将该规则条目从系统防火墙设置的阻止列表中清除；和/或，

当检测到客户端系统存在与网络对象的IP地址在同一网段的本地IP地址时，将客户端系统中与网络对象的IP地址在同一网段的本地IP地址清除；

和/或，

当检测到客户端系统的路由项中存在与网络对象的IP地址在同一网段的IP地址时，将客户端系统中存在与网络对象的IP地址在同一网段的IP地址的路由项清除；和/或，

当检测到客户端系统的DNS设置中的IP地址在禁止DNS列表中时，将DNS设置中的IP地址修改为可信赖的DNS服务器地址；和/或，

当检测到客户端系统的主机文件的各条目中包括网络对象的域名时，将客户端系统中包括网络对象的域名的主机文件的条目清除。

5、根据权利要求1所述的方法，其中，选取的驱动检测项为网络过滤驱动，所述对选取的驱动检测项进行检测包括：

检测网络过滤驱动是否存在于黑名单中，若是，对网络过滤驱动的检测结果显示通讯异常；若否，对网络过滤驱动的检测结果显示通讯正常。

6、根据权利要求5所述的方法，其中，所述修复所述网络过滤驱动包括：

将黑名单中的网络过滤驱动备份后，将该网络过滤驱动清除，检测结果指示通讯正常时，允许客户端应用访问所述网络对象。

7、根据权利要求6所述的方法，其中，在所述将黑名单中的网络过滤驱动备份后，将该网络过滤驱动从黑名单中清除，检测结果指示通讯正常，允许客户端应用访问所述网络对象之后，所述方法还包括：

当客户端应用访问网络对象失败时，若客户端应用不能成功访问信赖的第三方网络对象，确认客户端应用无法访问网络，若客户端应用能够成功访问信

赖的第三方网络对象，判断客户端应用是否具有不存在于黑名单和白名单中的网络过滤驱动，若不具有，确认客户端应用无法访问网络，若具有，将该网络过滤驱动备份后清除，允许客户端应用访问所述网络对象。

8、根据权利要求 7 所述的方法，其特征在于，

所述检测网络过滤驱动是否存在于黑名单中包括：

从客户端系统的注册表和网络配置接口中获取网络过滤驱动的签名信息和/或版本信息；

当网络过滤驱动的签名信息和/或版本信息位于黑名单中时，确认该网络过滤驱动存在于黑名单中，当网络过滤驱动的签名信息和/或版本信息不位于黑名单中时，确认该网络过滤驱动不存在于黑名单中；

所述判断客户端应用是否具有不存在于黑名单和白名单中的网络过滤驱动包括：

当网络过滤驱动的签名信息和/或版本信息不存在于黑名单和白名单中时，确认客户端应用具有不存在于黑名单和白名单中的网络过滤驱动，否则，确认客户端应用不具有不存在于黑名单和白名单中的网络过滤驱动。

9、一种控制客户端访问网络的检测装置，所述装置包括：

检测项选取单元，适于根据客户端系统设置选取系统设置检测项；

检测单元，适于利用所述系统设置检测项和客户端应用需要访问的网络对象的通讯信息，对客户端应用与所述网络对象之间的通讯进行检测；

访问控制单元，适于当对系统设置检测项的检测结果显示通讯异常时，修复所述系统设置检测项，当检测结果指示通讯正常时，允许客户端应用访问所述网络对象；

所述检测项选取单元，还适于选取驱动检测项进行检测；所述检测单元，还适于当修复所述系统设置检测项失败时，对选取的驱动检测项进行检测；

所述访问控制单元，还适于当对驱动检测项的检测结果显示通讯异常时，修复所述驱动检测项，当对驱动检测项的检测结果显示通讯正常时，允许客户端应用访问所述网络对象。

10、根据权利要求 9 所述的装置，其中，所述系统设置检测项包括客户端系统的网络协议安全性设置、系统防火墙设置、本地 IP 地址、路由项、域名系统 DNS 设置和/或主机文件，所述通讯信息包括网络对象的域名和 IP 地址，

所述检测单元，具体适于检测客户端系统的网络协议安全性设置的阻止列

表中是否存在网络对象的通讯信息，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常；和/或，

检测客户端系统的系统防火墙设置的阻止列表中的规则条目中是否存在网络对象的 IP 地址或客户端应用的名称，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常；和/或，

检测客户端系统是否存在与网络对象的 IP 地址在同一网段的本地 IP 地址，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常；和/或，

检测客户端系统的路由项中是否存在与网络对象的 IP 地址在同一网段的 IP 地址，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常；

和/或，

检测客户端系统的 DNS 设置中的 IP 地址是否在禁止 DNS 列表中，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常；和/或，

检测客户端系统的主机文件的各条目中是否包括网络对象的域名，若是，检测结果指示通讯异常，若否，检测结果指示通讯正常。

11、根据权利要求 9 所述的装置，其中，所述访问控制单元，适于当检测结果指示通讯异常时，通过下述方式修复所述系统设置检测项：

当检测到客户端系统的网络协议安全性设置的阻止列表中存在网络对象的通讯信息时，将网络对象的通讯信息从网络协议安全性设置的阻止列表中清除；和/或，

当检测到客户端系统的系统防火墙设置的阻止列表中的规则条目中存在网络对象的 IP 地址或客户端应用的名称时，将该规则条目从系统防火墙设置的阻止列表中清除；和/或，

当检测到客户端系统存在与网络对象的 IP 地址在同一网段的本地 IP 地址时，将客户端系统中与网络对象的 IP 地址在同一网段的本地 IP 地址清除；

和/或，

当检测到客户端系统的路由项中存在与网络对象的 IP 地址在同一网段的 IP 地址时，将客户端系统中存在与网络对象的 IP 地址在同一网段的 IP 地址的路由项清除；和/或，

当检测到客户端系统的 DNS 设置中的 IP 地址在禁止 DNS 列表中时，将 DNS 设置中的 IP 地址修改为可信赖的 DNS 服务器地址；和/或，

当检测到客户端系统的主机文件的各条目中包括网络对象的域名时，将客

户端系统中包括网络对象的域名的主机文件的条目清除。

12、根据权利要求 9 所述的装置，其中，

所述检测项选取单元，具体适于选取网络过滤驱动作为所述驱动检测项；

所述检测单元，还适于检测网络过滤驱动是否存在于黑名单中，若是，对网络过滤驱动的检测结果显示通讯异常；若否，对网络过滤驱动的检测结果显示通讯正常。

13、根据权利要求 12 所述的装置，其中，

所述访问控制单元，适于通过下述方式修复所述网络过滤驱动：将黑名单中的网络过滤驱动备份后，将该网络过滤驱动清除，检测结果指示通讯正常，允许客户端应用访问所述网络对象。

14、根据权利要求 13 所述的装置，其中，所述访问控制单元，还适于在所述将黑名单中的网络过滤驱动备份后，将该网络过滤驱动从黑名单中清除，检测结果指示通讯正常，允许客户端应用访问所述网络对象之后，当客户端应用访问网络对象失败时，若客户端应用不能成功访问信赖的第三方网络对象，确认客户端应用无法访问网络，若客户端应用能够成功访问信赖的第三方网络对象，判断客户端应用是否具有不存在于黑名单和白名单中的网络过滤驱动，若不具有，确认客户端应用无法访问网络，若具有，将该网络过滤驱动备份后清除，允许客户端应用访问所述网络对象。

15、根据权利要求 14 所述的装置，其中，

所述检测单元，具体适于通过下列方式，检测网络过滤驱动是否存在于黑名单中：从客户端系统的注册表和网络配置接口中获取网络过滤驱动的签名信息和/或版本信息；当网络过滤驱动的签名信息和/或版本信息位于黑名单中时，确认该网络过滤驱动存在于黑名单中，当网络过滤驱动的签名信息和/或版本信息不位于黑名单中时，确认该网络过滤驱动不存在于黑名单中；

所述检测单元，具体适于通过下列方式，判断客户端应用是否具有不存在于黑名单和白名单中的网络过滤驱动：

当网络过滤驱动的签名信息和/或版本信息不存在于黑名单和白名单中时，确认客户端应用具有不存在于黑名单和白名单中的网络过滤驱动，否则，确认客户端应用不具有不存在于黑名单和白名单中的网络过滤驱动。

16、一种通信系统，所述系统包括客户端设备，所述客户端设备包括如上述权利要求 9 至 15 任一项所述的控制客户端访问网络的检测装置，

所述客户端设备上运行的客户端应用需要访问的网络对象为云安全中心服务器；

所述控制客户端访问网络的检测装置允许客户端应用访问云安全中心服务器时，所述客户端应用，适于将可疑文件的信息发送至云安全中心服务器，并接收云安全中心服务器下发的对所述可疑文件的信息的分析结果。

17、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客户端上运行时，导致所述客户端执行根据权利要求 1-8 中的任一项所述的控制客户端访问网络的检测方法。

18、一种计算机可读介质，其中存储了如权利要求 17 所述的计算机程序。

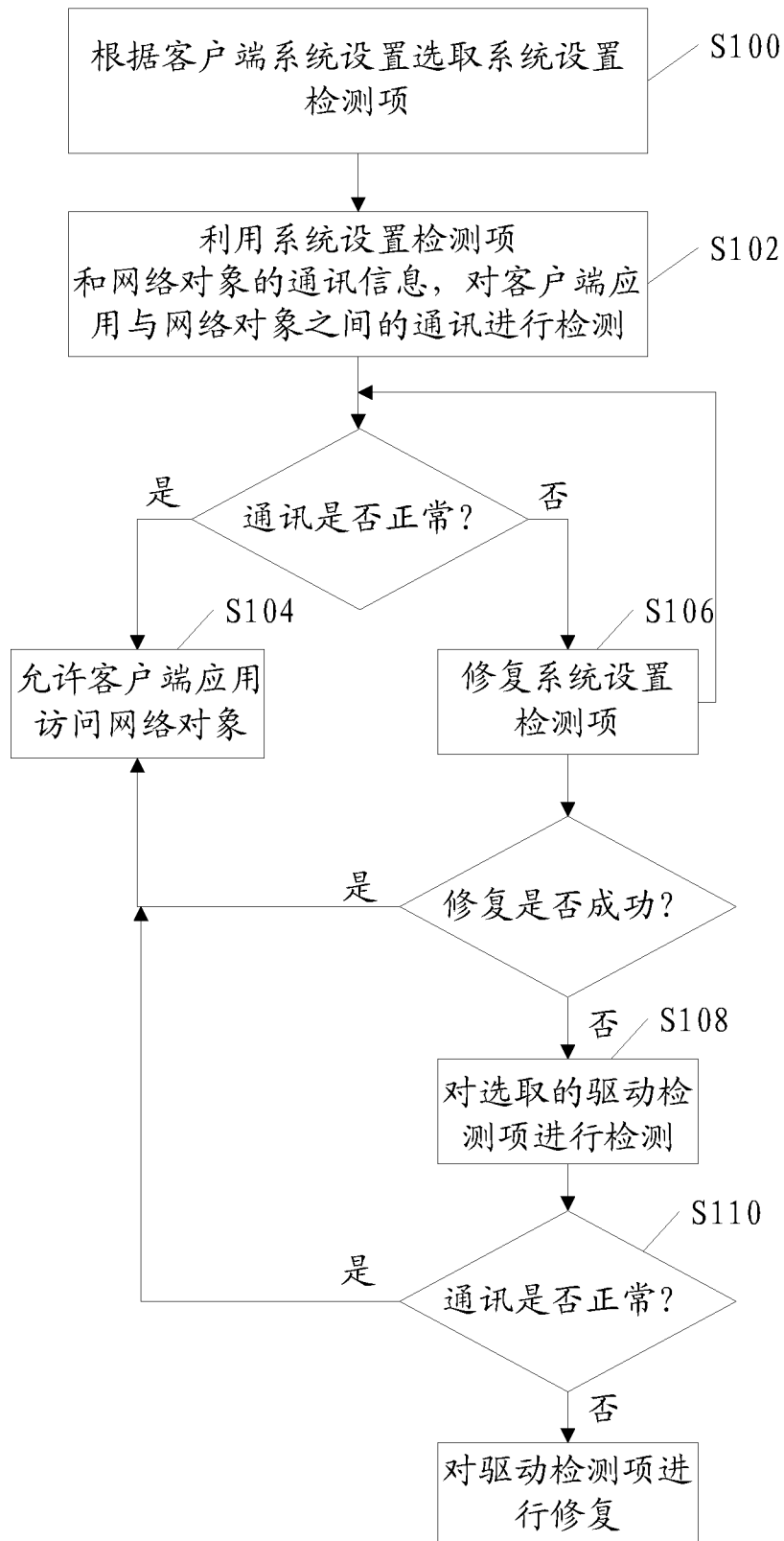


图 1

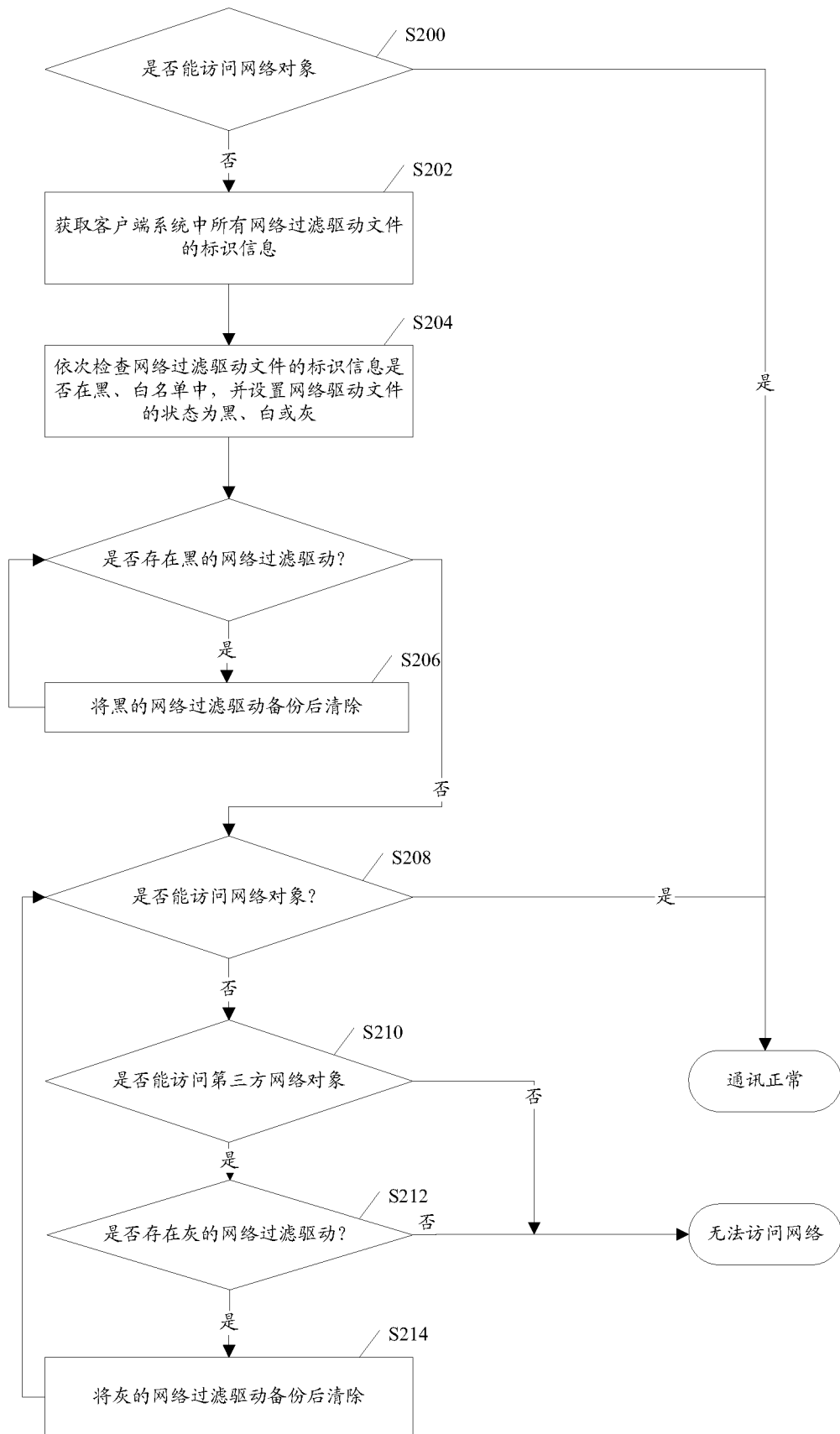


图 2



图 3

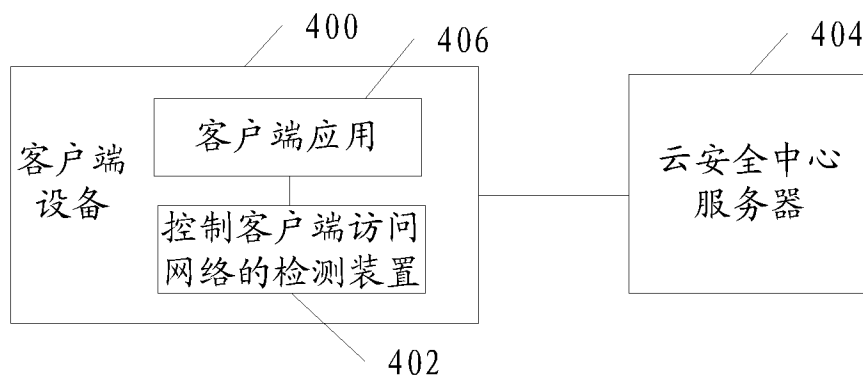


图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/083629

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)

CNKI, CNPAT, WPI, EPODOC: virus, worm, trojan, malicious, juggle, tamper, list, repair, restore, blacklist, filter, driver, access, communicate, upgrade, abnormal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 102868694 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.) 09 January 2013 (09.01.2013) claims 1 to 16, description, paragraph [0179]	1-18
A	CN 101141243 A (FORTINET INFORMATION TECHNOLOGY (BEIJING) CO., LTD.) 12 March 2008 (12.03.2008) description, page 10, lines 3 to 17	1-18
A	CN 102436560 A (GAO, Zhenyu et al.) 02 May 2012 (02.05.2012) the whole document	1-18
A	US 2010/0037321 A1 (YOGGIE SECURITY SYSTEMS LTD.) 11 February 2010 (11.02.2010) the whole document	1-18

☐ 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
21 November 2013 (21.11.2013)

Date of mailing of the international search report
26 December 2013 (26.12.2013)

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
WANG, Zhaoying
Telephone No. (86-10) 82245234

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/CN2013/083629

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102868694 A	09.01.2013	None	
CN 101141243 A	12.03.2008	CN 101141244 A	12.03.2008
		CN 101141447 A	12.03.2008
CN 102436560 A	02.05.2012	None	
US 2010/0037321 A1	11.02.2010	None	

国际检索报告

国际申请号

PCT/CN2013/083629

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))

CNKI, CNPAT, WPI, EPODOC: 病毒, 木马, 蠕虫, 恶意, 不良, 破坏, 阻止, 禁止, 访问, 通信, 通讯, 修改, 升级, 消除, 清除, 修复, 异常, 表, virus, worm, trojan, malicious, juggle, tamper, list, repair, restore, blacklist, filter, driver

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 102868694 A (北京奇虎科技有限公司 等) 09.1 月 2013 (09.01.2013) 权利要求 1-16, 说明书第[0179]段	1-18
A	CN 101141243 A (飞塔信息科技(北京)有限公司) 12.3 月 2008 (12.03.2008) 说明书第 10 页第 3-17 行	1-18
A	CN 102436560 A (高振宇 等) 02.5 月 2012 (02.05.2012) 全文	1-18
A	US 2010/0037321 A1 (YOGGIE SECURITY SYSTEMS LTD.) 11.2 月 2010 (11.02.2010) 全文	1-18



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

21.11 月 2013 (21.11.2013)

国际检索报告邮寄日期

26.12 月 2013 (26.12.2013)

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

王朝英

电话号码: (86-10) **82245234**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2013/083629

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 102868694 A	09.01.2013	无	
CN 101141243 A	12.03.2008	CN 101141244 A	12.03.2008
		CN 101141447 A	12.03.2008
CN 102436560 A	02.05.2012	无	
US 2010/0037321 A1	11.02.2010	无	