(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
2017 年 4 月 6 日 (06.04.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/054716 A1

(51) 国际专利分类号:
G06F 21/55 (2013.01)

(21) 国际申请号: PCT/CN2016/100426

(22) 国际申请日: 2016 年 9 月 27 日 (27.09.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510639832.2 2015 年 9 月 30 日 (30.09.2015) CN
201510639835.6 2015 年 9 月 30 日 (30.09.2015) CN
201510640171.5 2015 年 9 月 30 日 (30.09.2015) CN

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

(72) 发明人: **高庆光 (GAO, Qingguang)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 **贾正强 (JIA, Zhengqiang)**; 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)**; 中国北京市海淀区花园路 13 号 5 幢 320 房间, Beijing 100088 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

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

本国际公布:
— 包括国际检索报告(条约第 21 条(3))。

(54) **Title**: METHOD FOR RECOGNIZING HIJACKED BROWSER AND BROWSER

(54) **发明名称** : 识别被劫持浏览器的方法及浏览器

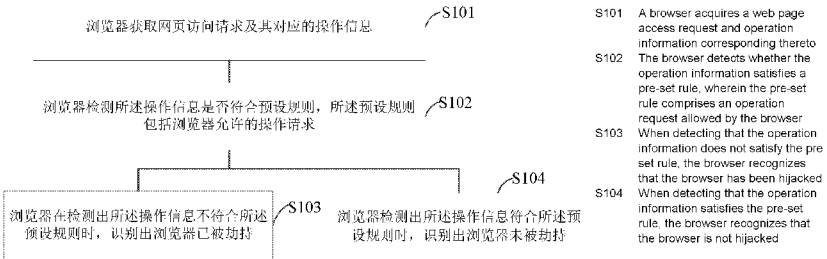

图 1

(57) **Abstract**: A method for recognizing a hijacked browser and a browser. A browser acquires a web page access request and operation information corresponding thereto (S101); the browser detects whether the operation information satisfies a pre-set rule, wherein the pre-set rule comprises an operation request allowed by the browser (S102); when detecting that the operation information does not satisfy the pre-set rule, the browser recognizes that the browser has been hijacked (S103); and when detecting that the operation information satisfies the pre-set rule, the browser recognizes that the browser is not hijacked (S104). By means of the method for recognizing a hijacked browser and the browser, the technical problem of low accuracy of the method for determining whether a browser is hijacked in the prior art is solved, and the technical effect of improving the accuracy of determining whether a browser is hijacked is realized.

(57) **摘要**: 一种识别被劫持浏览器的方法及浏览器，浏览器获取网页访问请求及其对应的操作信息（S101）；所述浏览器检测所述操作信息是否符合预设规则，所述预设规则包括所述浏览器允许的操作请求（S102）；所述浏览器在检测出所述操作信息不符合所述预设规则时，识别出所述浏览器已被劫持（S103）；所述浏览器检测出所述操作信息符合所述预设规则时，识别出所述浏览器未被劫持（S104）。所述识别被劫持浏览器的方法及浏览器，解决了现有技术中判断浏览器是否被劫持的方法存在准确性低的技术问题，实现了提高了判断浏览器是否被劫持的准确性的技术效果。

WO 2017/054716 A1

识别被劫持浏览器的方法及浏览器

技术领域

本发明涉及计算机网技术领域，具体涉及一种识别被劫持浏览器的方法及浏览器。

背景技术

随着互联网的迅速发展，浏览器提供了丰富多样的功能，供用户在网上能够快速查找资料及个人所需要的各种信息。但是，现实中浏览器会通过浏览器插件、浏览器辅助对象（Browser Helper Object，简称 BHO）、WinsockLSP 等形式对浏览器进行篡改，从而使得浏览器被劫持，而在浏览器被劫持时，浏览器的主页及互联网搜索页会变为不知名的网站、访问正常网站时被转向到恶意网页、当输入错误的网址时被转到劫持软件指定的网站和输入字符时浏览器速度严重减慢等。由于这些被劫持的浏览器给用户的日常浏览造成了不良影响，因此网络安全工具一个很重要的工作就是，需要将网络中存在的被劫持的浏览器识别出来。

现有技术中，在判断浏览器被劫持时，通常采用以下方式：其一、用户查看浏览器的主页或其他设置是否已被更改；其二、用户判断是否出现级联弹出窗口，即屏幕上出现看似无穷无尽的连环广告弹出窗口；其三、用户判断是否安装了新的工具栏或收藏夹，并提供指向您不需要的网页的图标和链接；上述判断方式均是用户自行判断浏览器是否被劫持，且用户通常是通过自己的经验来判断浏览器是否被劫持，如此，而用户的经验的多少会直接影响判断的准确性，经验较少的用户必然会出现判断错误的情况，从而导致现有技术中判断浏览器是否被劫持的方法存在准确性较低的问题。

发明内容

本申请实施例通过提供一种识别被劫持浏览器的方法及浏览器，解决了现有技术中判断浏览器是否被劫持的方法存在准确性低的技术问题，实现了提高了判断浏览器是否被劫持的准确性的技术效果。

一方面，本申请通过本申请的一实施例提供如下技术方案：

本申请公开了一种识别被劫持浏览器的方法，包括：

浏览器获取网页访问请求及其对应的操作信息；

所述浏览器检测所述操作信息是否符合预设规则，所述预设规则包括所述浏览器允许的操作请求；

所述浏览器在检测出所述操作信息不符合所述预设规则时，识别出所述浏览器已被劫持；

所述浏览器检测出所述操作信息符合所述预设规则时，识别出所述浏览器未被劫持。

可选的，所述浏览器获取网页访问请求及其对应的操作信息，具体包括：浏览器获取导航页的网页访问请求，以及获取与所述网页访问请求对应的目标域名；

所述浏览器检测所述操作信息是否符合预设规则，具体包括：所述浏览器判断所述目标域名是否与所述导航页的原始域名相一致；

所述浏览器检测出所述操作信息符合所述预设规则时，识别出所述浏览器未被劫持，具体包括：所述浏览器在判断出所述目标域名与所述原始域名一致时，则识别出所述浏览器未被劫持；

所述浏览器在检测出所述操作信息不符合所述预设规则时，识别出所述浏览器已被劫持，具体包括：所述浏览器在判断出所述目标域名与所述原始域名不一致时，则识别出所述浏览器已被劫持。

可选的，所述浏览器获取网页访问请求及其对应的操作信息，具体包括：获取浏览器的快捷方式的命令行的参数设置信息；

所述浏览器检测所述操作信息是否符合预设规则，具体包括：判断所述参数设置信息对应的设置方式是否与预设方式相一致；

所述浏览器在检测出所述操作信息不符合所述预设规则时，识别出所述浏览器已被劫持，具体包括：在判断出所述设置方式与所述预设方式不一致时，识别出所述浏览器已被劫持；

所述浏览器检测出所述操作信息符合所述预设规则时，识别出所述浏览器未被劫持，具体包括：在判断出所述设置方式与所述预设方式一致时，识别出所述浏览器未被劫持。

另一方面，本申请通过本申请的一实施例提供如下技术方案：

本申请公开了一种识别被劫持浏览器的方法，包括：

浏览器获取网页访问请求及其对应的操作信息；

所述浏览器检测所述操作信息是否符合预设规则，所述预设规则包括所述浏览器允许的操作请求；

所述浏览器在检测出所述操作信息不符合所述预设规则时，获取与所述网页访问请求对应的搜索页面的页面地址；

所述浏览器判断所述页面地址是否位于黑名单中，获得判断结果，其中，所述黑名单中存储有劫持所述浏览器的网址信息；

所述浏览器在检测到所述判断结果表征所述页面地址位于所述黑名单中时，则识别出所述浏览器已被劫持；

所述浏览器在检测到所述判断结果表征所述页面地址未位于所述黑名单中时，则识别出所述浏览器未被劫持。

第三方面，本申请通过本申请的一实施例提供如下技术方案：

本申请公开了一种浏览器，所述浏览器包括：

访问请求获取单元，用于获取网页访问请求；

操作信息获取单元，用于获取与所述网页访问请求对应的操作信息；

检测单元，用于检测所述操作信息是否符合预设规则，所述预设规则包括所述浏览器允许的操作请求；

识别单元，用于在检测出所述操作信息不符合所述预设规则时，识别出所述浏览器已被劫持；以及在检测出所述操作信息符合所述预设规则时，识别出所述浏览器未被劫持。

可选的，所述浏览器还包括：

所述访问请求获取单元，具体用于获取浏览器的导航页的网页访问请求；

目标域名获取单元，用于获取与所述网页访问请求对应的目标域名；

判断单元，用于判断所述目标域名是否与所述导航页的原始域名相一致；

所述识别单元，具体用于在判断出所述目标域名与所述原始域名一致时，则识别出所述浏览器未被劫持；以及在判断出所述目标域名与所述原始域名不一致时，则识别出所述浏览器已被劫持。

可选的，所述浏览器还包括：

命令行参数获取单元，用于获取浏览器的快捷方式的命令行的参数设置信息；

判断单元，用于判断所述参数设置信息对应的设置方式是否与预设方式相一致；

所述识别单元，具体用于在判断出所述设置方式与所述预设方式不一致时，识别出所述浏览器已被劫持；以及在判断出所述设置方式与所述预设方式一致时，识别出所述浏览器未被劫持。

第四方面，本申请通过本申请的一实施例提供如下技术方案：

本申请公开了一种浏览器，所述浏览器包括：

访问请求获取单元，用于获取网页访问请求；

操作信息获取单元，用于获取与所述网页访问请求对应的操作信息；

检测单元，用于检测所述操作信息是否符合预设规则，所述预设规则包括所述浏览器允许的操作请求；

页面地址获取单元，用于在检测出所述操作信息不符合所述预设规则时，获取与所述网页访问请求对应的搜索页面的页面地址；

判断单元，用于判断所述页面地址是否位于黑名单中，获得判断结果，其中，所述黑名单中存储有劫持所述浏览器的网址信息；

识别单元，用于在检测到所述判断结果表征所述页面地址位于所述黑名单中时，则识别出所述浏览器已被劫持；以及在检测到所述判断结果表征所述页面地址未位于所述黑名单中时，则识别出所述浏览器未被劫持。

依据本发明的又一方面，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计算设备上运行时，导致所述计算设备执行根据上文所述的识别被劫持浏览器的方法。

依据本发明的再一方面，提供了一种计算机可读介质，其中存储了上述的计算机程序。

本申请实施例中提供的一个或多个技术方案，至少具有如下技术效果或优点：

根据本发明的一种识别被劫持浏览器的方法及浏览器，通过本发明，浏览器获取网页访问请求及其对应的操作信息，再检测所述操作信息是否符合预设规则，在符合所述预设规则时，识别出所述浏览器已被劫持，否则，则识别所述浏览器未被劫持，由于所述预设规则包括所述浏览器允许的操作请求，通过检测所述操作请求是否符合所述预设规则就能够更准确的识别出所述浏览器是否被劫持，如此，使得所述浏览器在根据所述判断结果识别出所述浏览器是否被劫持的准确性得以提高，而且所述浏览器是自行判断是否被劫持，与现有技术中的人工判断相比，其判断的工作效率也能够得到较大的提高。

进一步地，根据本发明的一种通过域名识别被劫持浏览器的方法，通过本发明，浏览器获取网页访问请求及其对应的目标域名，再判断所述目标域名是否与所述导航页的原始域名相一致，在判断出所述目标域名与所述原始域名一致时，则识别出所述浏览器未被劫持；以及在判断出所述目标域名与所述原始域名不一致时，则识别出所述浏览器已被劫持；如此，能通过判断出所述目标域名是否与所述原始域名一致，以此来识别出所述浏览器是否被劫持，其识别的准确性也随之提高，而且是浏览器自行判断自己是否被劫持，与现有技术中的人工判断相比，其判断的工作效率也能够得到较大的提高。

进一步地，通过本发明，获取浏览器的快捷方式的命令行的参数设置信息；判断所述参数设置信息对应的设置方式是否与预设方式相一致；在判断出所述设置方式与所述预设方式不一致时，识别出所述浏览器已被劫持；在判断出所述设置方式与所述预设方式一致时，识别出所述浏览器未被劫持；如此，使得可以通过判断所述设置方式是否与所述预设方式相一致来判断出所述设置方式是否已被修改，而在浏览器未被劫持时，所述设置方式与所述预设方式是一致的，而在浏览器被劫持的情况下，所述设置方式可能会与所述预设方式不一致，从而使得通过判断所述设置方式是否与所述预设方式相一致就能够准确识别出所述浏览器是否被劫持，提高了识别的准确性，而且是通过机器判断方式来判断浏览器是否被劫持的，与现有技术中的人工判断相比，其判断的工作效率也能够得到较大的提高。

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 为本发明实施例提供的识别被劫持浏览器的方法的第一种流程图；

图 2 为本发明实施例提供的识别被劫持浏览器的方法的第二种流程图；

图 3 为本发明实施例提供的浏览器的第一种模块图；

图 4 为本发明实施例提供的浏览器的第二种模块图；

图 5 为本发明实施例提供的通过域名识别被劫持浏览器的方法的流程图；

图 6 为本发明实施例提供的浏览器的模块图；

图 7 为本发明实施例提供的识别被劫持浏览器的方法的第三种流程图；

图 8 为本发明实施例提供的识别被劫持浏览器的方法的第四种流程图；

图 9 为本发明实施例提供的识别被劫持浏览器的设备的模块图；

图 10 示意性地示出了用于执行根据本发明的识别被劫持浏览器的方法的计算设备的框图；以及

图 11 示意性地示出了用于保持或者携带实现根据本发明的识别被劫持浏览器的方法的程序代码的存储单元。

具体实施方式

为了更好的理解上述技术方案，下面将结合说明书附图以及具体的实施方式对上述技术方案进行详细的说明。

参见图 1，本发明实施例提供的识别被劫持浏览器的方法包括以下步骤：

步骤 S101：浏览器获取网页访问请求及其对应的操作信息；

步骤 S102：浏览器检测所述操作信息是否符合预设规则，所述预设规则包括浏览器允许的操作请求；

步骤 S103：浏览器在检测出所述操作信息不符合所述预设规则时，识别出浏览器已被劫持；

步骤 S104：浏览器检测出所述操作信息符合所述预设规则时，识别出浏览器未被劫持。

其中，在步骤 S101 中，浏览器启动之后，会接收到用户的操作信息，基于所述操作信息，浏览器会自动生成并获取到与所述操作信息对应的网页访问请求，如此，使得浏览器能够获取到所述网页访问请求及其对应的操作信息，其中，所述操作信息例如可以是用户点击浏览器的导航页上的超链接的信息，还可以是在浏览器的搜索栏中输入搜索信息的信息。

具体来讲，以 a 浏览器为例，在 a 浏览器启动之后，接收到用户在 a 浏览器的搜索栏中输入了 www.axxx.com 的操作信息，a 浏览器基于该操作信息生成访问 www.axxx.com 的网页访问请求例如包含有 String url = " http:// www.axxx.com/"；如此，使得 a 浏览器能够接收到访问 www.axxx.com 的网页访问请求及其对应的操作信息，所述操作信息为在 a 浏览器的搜索栏中输入 www.axxx.com 的信息。

接下来执行步骤 S102，在该步骤中，浏览器检测所述操作信息是否符合预设规则，所述预设规则包括浏览器允许的操作请求。

在具体实施过程中，浏览器通过步骤 S101 获取到所述操作信息之后，检测所述操作信息是否符合所述预设规则，由于所述预设规则包括浏览器允许的操作请求，如此，通过判断所述操作信息是否符合所述预设规则，即可以判断出所述操作信息是否合法。

具体来讲，浏览器允许的操作请求包括在浏览器的搜索栏中输入搜索信息的第一种操作请求和对浏览器的导航页上的超链接进行点击而生成的第二种操作请求，然后检测所述操作信息是否与所述第一种操作请求和所述第二种操作请求中的一种请求相匹配，在所述操作信息与所述第一种操作请求和所述第二种操作请求均不匹配时，则确定所述操作信息不符合所述预设规则；在所述操作信息与所述第一种操作请求和所述第二种操作请求中的任一种请求相匹配时，则确定所述操作信息符合所述预设规则，当然，所述预设规则还包括在浏览器中加载搜索引擎时，在该搜索引擎中输入信息的第三种操作请求，下面具体以所述预设规则为第一、第二种操作请求为例。

例如，以 a 浏览器为例，在 a 浏览器启动之后，接收到用户在 a 浏览器的搜索栏中输入了 www.axxx.com 的搜索信息，a 浏览器基于该操作信息生成访问 www.axxx.com 的网页访问请求例如包含有 String url = " http:// www.axxx.com/"；如此，使得 a 浏览器能够接收到访问 www.axxx.com 的网页访问请求及其对应的操作信息，所述操作信息为在 a 浏览器的搜索栏中输入 www.axxx.com 的搜索信息的请求，由于 a 浏览器的预设规则为在浏览器的搜索栏中输入搜索信息的第一种操作请求和对浏览器的导航页上的超链接进行点击而生成的第二种操作请求，由于所述操作信息与所述第一种操作请求相匹配，则确定所述操作信息符合所述预设规则。

具体的，所述预设规则还可以是判断所述操作信息与所述网页访问请求相匹配，例如所述操作信息为在浏览器的搜索栏中输入的 www.axxx.com 的搜索信息，所述网页访问请求为对 www.bxxx.com 的访问请求，如此，可以判断出所述操作信息与所述网页访问请求不匹配，则确定浏览器被劫持；而在浏览器未被劫持时，所述操作信息与所述网页访问请求是相匹配的。

浏览器在检测出所述操作信息不符合所述预设规则时，执行步骤 S103，识别出浏览器已被劫持；浏览器检测出所述操作信息符合所述预设规则时，执行步骤 S104，识别出浏览器未被劫持。

在具体实施过程中，浏览器通过步骤 S102 检测出所述操作信息不符合所述预设规则时，则确认浏览器已被劫持；若检测出所述操作信息符合所述预设规则时，则确认浏览器未被劫持。

例如，以 a 浏览器为例，在 a 浏览器启动之后，接收到用户在 a 浏览器的搜索栏中输入了 www.axxx.com 的搜索信息，a 浏览器基于该操作信息生成访问 www.axxx.com 的网页访问请求例如包含有 String url = " http:// www.axxx.com/"；如此，使得 a 浏览器能够接收到访问 www.axxx.com 的网页访问请求及其对应的操作信息，所述操作信息为在 a 浏览器的搜索栏中输入 www.axxx.com 的信息，由于 a 浏览器的预设规则为在浏览器的搜索栏中输入搜索信息的第一种操作请求和对浏览器的导航页上的超链接进行点击而生成的第二种操作请求，由于所述操作

信息与所述第一种操作请求相匹配，则确定所述操作信息符合所述预设规则，即使得 a 浏览器可以判断出 a 浏览器未被劫持，如此，使得所述浏览器在根据所述判断结果识别出所述浏览器是否被劫持的准确性得以提高，而且所述浏览器是自行判断是否被劫持，与现有技术中的人工判断相比，其判断的工作效率也能够得到较大的提高。

在另一实施例中，本申请还提供了一种识别被劫持浏览器的方法，参见图 2，所述方法包括以下步骤：

步骤 S201：浏览器获取网页访问请求及其对应的操作信息；

步骤 S202：浏览器检测所述操作信息是否符合预设规则，所述预设规则包括浏览器允许的操作请求；

步骤 S203：浏览器在检测出所述操作信息不符合所述预设规则时，获取与所述网页访问请求对应的搜索页面的页面地址；

步骤 S204：浏览器判断所述页面地址是否位于黑名单中，获得判断结果，其中，所述黑名单中存储有劫持浏览器的网址信息；

步骤 S205：浏览器在检测到所述判断结果表征所述页面地址位于所述黑名单中时，则识别出浏览器已被劫持；

步骤 S206：浏览器在检测到所述判断结果表征所述页面地址未位于所述黑名单中时，则识别出浏览器未被劫持。

其中，在步骤 S201 中，浏览器启动之后，会接收到用户的操作信息，基于所述操作信息，浏览器会自动生成并获取到与所述操作信息对应的网页访问请求，如此，使得浏览器能够获取到所述网页访问请求及其对应的操作信息，其中，所述操作信息例如可以是用户点击浏览器的导航页上的超链接的信息，还可以是在浏览器的搜索栏中输入搜索信息的信息。

接下来执行步骤 S202，在该步骤中，浏览器检测所述操作信息是否符合预设规则，所述预设规则包括浏览器允许的操作请求。

在具体实施过程中，浏览器通过步骤 S101 获取到所述操作信息之后，检测所述操作信息是否符合所述预设规则，由于所述预设规则包括浏览器允许的操作请求，如此，通过判断所述操作信息是否符合所述预设规则，即可以判断出所述操作信息是否合法。

浏览器在检测出所述操作信息不符合所述预设规则时，执行步骤 S203，获取与所述网页访问请求对应的搜索页面的页面地址；

在具体实施过程中，浏览器通过步骤 S202 检测出所述操作信息不符合所述预设规则时，获取与所述网页访问请求对应的搜索页面的页面地址，所述搜索页面可以是浏览器的主页，也可以是浏览器的导航页，还可以是浏览器中加载的搜素引擎页，还可以是在浏览器中加载的其它浏览器的导航页，当然通常浏览器的主页和浏览器的导航页可能是同一个页面。

具体来讲，以 a 浏览器为例，在 a 浏览器启动之后，接收到用户在 a 浏览器的搜索栏中输入了 www.axxx.com 的搜索信息，a 浏览器基于该操作信息生成的网页访问请求中包含 String url = " http:// www.bxxx.com/"，由于所述操作信息表征是输入的 www.axxx.com 的搜索信息，而所述网页访问请求是访问 www.bxxx.com 的请求，由于 www.bxxx.com 与 www.axxx.com 不同，则确定所述操作信息不符合所述预设规则，由于所述网页搜素请求是在 a 浏览器的搜索栏中输入了 www.axxx.com 的搜索信息而生成的，由此，确定所述搜素页面为 a 浏览器的主页，然后获取 a 浏览器的主页的页面地址例如为 http:// hao.axxx.com/。

又例如，以 a 浏览器为例，在 a 浏览器启动之后，a 浏览器上加载了一个 a 导航页，其中，a 导航页为 a 浏览器中的预设导航页，a 浏览器接收到用户在 a 导航页中输入了 www.cxxx.com 的搜索信息，a 浏览器基于该操作信息生成访问 www.cxxx.com 的网页访问请求例如包含有 String url = " http:// www.cxxx.com/"；如此，使得 a 浏览器能够接收到访问 www.axxx.com 的网页访问请求及其对应的操作信息，所述操作信息为在 a 导航页中输入 www.axxx.com 的信息，若所述 a 浏览器的预设规则为在 a 浏览器的搜索栏中输入搜索信息的第一种操作请求和对 a 浏览器的导航页上的超链接进行点击而生成的第二种操作请求时，由于所述操作信息与所述第一种操作请求和第二种操作请求均不匹配，则确定所述操作信息不符合所述预设规则，然后获取与所述网页访问请求对应的搜索页面为 a 导航页，然后获取 a 导航页的页面地址，所述页面地址例如为 http:// hao.axxx.com/。

接下来执行步骤 S204，在该步骤中，浏览器判断所述页面地址是否位于黑名单中，获得

判断结果，其中，所述黑名单中存储有劫持浏览器的网址信息。

在具体实施过程中，在浏览器判断所述页面地址是否位于黑名单中之前，浏览器根据该浏览器被劫持的历史数据，获取并存储所述黑名单，其中，浏览器在获取所述历史数据时，可以通过接收用户的反馈信息来获取所述历史数据，也可以通过数据采集和监控的方式来获取所述历史数据，再通过所述历史数据来获取所述黑名单之后，浏览器还可以不断收集浏览器被劫持的其它数据，以此来不断更新所述黑名单，使得所述黑名单中能够存储更多的劫持浏览器的网址信息，使得通过所述黑名单来判断所述页面地址是否位于所述黑名单而获得所述判断结果能够更准确。

例如，以 a 浏览器为例，a 浏览器收集到 a 浏览器被劫持的历史数据中显示有 A 网址、B 网址和 C 网址均劫持过 a 浏览器，然后建立所述黑名单，使得所述黑名单中存储有 A 网址、B 网址和 C 网址。

又例如，以 a 浏览器为例，a 浏览器根据当前收集到的历史数据生成了所述黑名单，所述黑名单中存储有 A 网址、B 网址、C 网址，在生成所述黑名单之后，a 浏览器持续收集 a 浏览器被劫持的其它数据，在收集到的其它数据中包含有 D 网址也劫持过 a 浏览器的数据时，则将 D 网址添加到所述黑名单中，使得更新后的黑名单中存储有 D 网址，由于更新后的所述黑名单中存储有 D 网址，如此，使得所述黑名单中能够存储更多的劫持浏览器的网址信息，通过更新后的所述黑名单就能够判断出所述页面地址是否位于所述黑名单中时，能够使得所述判断结果能够更准确。

具体的，浏览器通过步骤 S203 获取到所述页面地址之后，判断所述页面地址是否位于所述黑名单中，获取所述判断结果，其中，在所述页面地址位于所述黑名单中时，所述判断结果表征所述页面地址位于所述黑名单中；在所述页面地址未位于所述黑名单中时，所述判断结果表征所述页面地址未位于所述黑名单中。

例如，以 a 浏览器为例，在 a 浏览器启动之后，a 浏览器上加载了一个 b 导航页，其中，b 导航页并不是 a 浏览器中的预设导航页，a 浏览器接收到用户在 b 导航页中输入了 www.cxxx.com 的搜索信息，a 浏览器基于该操作信息生成访问 www.cxxx.com 的网页访问请求例如包含有 String url = " http:// www.cxxx.com/"；如此，使得 a 浏览器能够接收到访问 www.cxxx.com 的网页访问请求及其对应的操作信息，所述操作信息为在 b 导航页中输入 www.cxxx.com 的信息与 a 浏览器的预设规则中的所述第一种操作请求和所述第二种操作请求均不匹配，则确定所述操作信息不符合所述预设规则，然后从所述网页访问请求中提取所述页面地址，所述页面地址为 http:// www.axxx.com/，然后判断 http:// www.axxx.com/是否位于 a 浏览器中存储的黑名单中，若 http:// www.axxx.com/位于所述黑名单中，则所述判断结果表征所述页面地址位于所述黑名单中；若 http:// www.axxx.com/未位于所述黑名单中，则所述判断结果表征所述页面地址未位于所述黑名单中。

浏览器在检测到所述判断结果表征所述页面地址位于所述黑名单中时， 执行步骤 S205，则识别出浏览器已被劫持；以及浏览器在检测到所述判断结果表征所述页面地址未位于所述黑名单中时，执行步骤 S206，则识别出浏览器未被劫持。

在具体实施过程中，通过步骤 S204 获得的所述判断结果能够准确的确定所述页面地址是否位于所述黑名单，浏览器基于所述判断结果，以识别出浏览器是否被劫持。

具体来讲，以 a 浏览器为例，在 a 浏览器启动之后，a 浏览器上加载了一个 b 导航页，其中 b 导航页并不是 a 浏览器中的预设导航页，a 浏览器接收到用户在 b 导航页中输入了 www.axxx.com 的搜索信息，a 浏览器基于该操作信息生成访问 www.axxx.com 的网页访问请求例如包含有 String url = " http:// www.axxx.com/"；如此，使得 a 浏览器能够接收到访问 www.axxx.com 的网页访问请求及其对应的操作信息，所述操作信息为在 b 导航页中输入 www.axxx.com 的信息与 a 浏览器的预设规则中的所述第一种操作请求和所述第二种操作请求均不匹配，则确定所述操作信息不符合所述预设规则，然后获取与所述网页访问请求对应的搜索页面为 b 导航页，然后获取 a 导航页的页面地址，所述页面地址例如为 http:// hao.bxxx.com/，然后判断 http:// www.bxxx.com/是否位于 a 浏览器中存储的黑名单中，若 http:// www.bxxx.com/位于所述黑名单中，则所述判断结果表征所述页面地址位于所述黑名单中，如此，可以识别出 a 浏览器已被劫持；若 http:// www.bxxx.com/未位于所述黑名单中，则所述判断结果表征所述页面地址未位于所述黑名单中，如此，可以识别出 a 浏览器未被劫持；如此，在所述操作信息不符

合预设规则时，还需通过所述黑名单进一步判断 a 浏览器是否被劫持，进一步提高了判断的准确性。

在另一实施例中，在所述网页访问请求为浏览器的导航页的网页访问请求时，所述方法还包括：浏览器判断所述导航页的网页访问请求对应的访问地址是否为所述导航页的导航地址；浏览器判断出所述访问地址不为所述导航地址时，则识别出浏览器已被劫持；浏览器判断出所述访问地址为所述导航地址时，则识别出浏览器未被劫持。

具体来讲，浏览器在检测所述网页访问请求为浏览器的导航页的网页访问请求时，浏览器可以通过检测所述网页访问请求是否是在启动时会加载导航页而获取的，如果是，则确定所述网页访问请求为所述导航页的网页访问请求，然后再根据所述网页访问请求，获取所述访问地址，所述访问地址为所述导航页的网址；当然，浏览器在启动之后，浏览器还可以通过检测所述网页访问请求是否是在收到用户启动所述导航页的启动请求时而获取的，如果是，则确定所述网页访问请求为所述导航页的网页访问请求，浏览器根据所述启动请求来加载所述导航页，进而获取到所述导航页的网页访问请求，再根据所述网页访问请求，获取所述访问地址。

具体来讲，浏览器检测到所述网页访问请求为浏览器的导航页的网页访问请求时，判断所述导航页的网页访问请求对应的访问地址是否为所述导航页的导航地址，其中，浏览器的导航页的导航地址可以是预先存储在浏览器中，页可以是预先存储在安装该浏览器的用户终端中，本申请不作具体限制。

例如，以 a 浏览器为例，a 浏览器启动时会自动加载 a 导航页，a 浏览器在加载 a 导航页时，会生成 a 导航页的网页访问请求例如包含有 String url = " http://hao.axxx.cn/"；如此，使得浏览器能够从 a 导航页的网页访问请求中提取访问地址为 http://hao.axxx.cn/；若 a 浏览器启动之后并未自动加载 a 导航页时，接收到用户启动 a 导航页的启动请求时，a 浏览器加载 a 导航页，生成 a 导航页的网页访问请求，然后从 a 导航页的网页访问请求中提取访问地址为 http://hao.axxx.cn/，然后判断 http://hao.axxx.cn/是否与 a 浏览器中导航页的导航地址是否相同。

当然，在 a 浏览器被劫持时，其加载的导航页可能为不是 a 导航页，而是其他网页例如为商业网页、广告网页等。

又例如，以 a 浏览器为例，a 浏览器启动时会自动加载 a 导航页，a 浏览器在加载 a 导航页时，会生成 a 导航页的网页访问请求，若生成的 a 导航页的网页访问请求例如包含有 String url = " http://hao.bxxx.cn/"，浏览器则会从 a 导航页的网页访问请求中提取访问地址为：http://hao.bxxx.cn/，然后判断 http://hao.bxxx.cn/是否与 a 浏览器中导航页的导航地址是否相同，若预先存储的所述导航地址为 http://hao.axxx.cn/，由于 a 导航页的导航地址为 http://hao.axxx.cn/ 与 http://hao.bxxx.cn/ 不同，则 a 浏览器识别出自身已被劫持。

本申请实施例中提供的一个或多个技术方案，至少具有如下技术效果或优点：

根据本发明的一种识别被劫持浏览器的方法及浏览器，通过本发明，浏览器获取网页访问请求及其对应的操作信息，再检测所述操作信息是否符合预设规则，在符合所述预设规则时，识别出所述浏览器已被劫持，否则，则识别所述浏览器未被劫持，由于所述预设规则包括所述浏览器允许的操作请求，通过检测所述操作请求是否符合所述预设规则就能够更准确的识别出所述浏览器是否被劫持，如此，使得所述浏览器在根据所述判断结果识别出所述浏览器是否被劫持的准确性得以提高，而且所述浏览器是自行判断是否被劫持，与现有技术中的人工判断相比，其判断的工作效率也能够得到较大的提高。

进一步的，在所述操作信息不符合所述预设规则时，浏览器还获取网页访问请求对应的访问地址，再判断所述页面地址是否位于黑名单中，根据获得的判断结果，识别出所述浏览器是否被劫持，由于所述黑名单中存储有劫持所述浏览器的网址信息，使得根据所述判断结果能够更准确的识别出所述浏览器是否被劫持，如此，使得所述浏览器在根据所述判断结果识别出所述浏览器是否被劫持的准确性得以提高，而且所述浏览器是自行判断是否被劫持，与现有技术中的人工判断相比，其判断的工作效率也能够得到较大的提高。

根据同一发明构思，本申请另一实施例提供本申请还公开了一种浏览器，参见图 3，所述浏览器包括：

访问请求获取单元 301，用于获取网页访问请求；

操作信息获取单元 302，用于获取与所述网页访问请求对应的操作信息；

检测单元 303，用于检测所述操作信息是否符合预设规则，所述预设规则包括所述浏览器

允许的操作请求；

识别单元 304，用于在检测出所述操作信息不符合所述预设规则时，识别出所述浏览器已被劫持；以及在检测出所述操作信息符合所述预设规则时，识别出所述浏览器未被劫持。

具体的，所述浏览器还包括：

判断单元 305，还用于在所述网页访问请求为所述浏览器的导航页的网页访问请求时，判断所述导航页的网页访问请求对应的访问地址是否为所述导航页的导航地址；

识别单元 304，还用于在判断出所述访问地址不为所述导航地址时，识别出所述浏览器已被劫持；以及判断出所述访问地址为所述导航地址时，识别出所述浏览器未被劫持。

可选的，访问请求获取单元 301，还用于在所述网页访问请求为所述浏览器的导航页的网页访问请求时，启动并加载所述导航页时，获取所述导航页的网页访问请求。

在另一实施例中，本申请另一实施例提供本申请还公开了一种浏览器，参见图 4，所述浏览器包括：

访问请求获取单元 401，用于获取网页访问请求；

操作信息获取单元 402，用于获取与所述网页访问请求对应的操作信息；

检测单元 403，用于检测所述操作信息是否符合预设规则，所述预设规则包括所述浏览器允许的操作请求；

页面地址获取单元 404，用于在检测出所述操作信息不符合所述预设规则时，获取与所述网页访问请求对应的搜索页面的页面地址；

判断单元 405，用于判断所述页面地址是否位于黑名单中，获得判断结果，其中，所述黑名单中存储有劫持所述浏览器的网址信息；

识别单元 406，用于在检测到所述判断结果表征所述页面地址位于所述黑名单中时，则识别出所述浏览器已被劫持；以及在检测到所述判断结果表征所述页面地址未位于所述黑名单中时，则识别出所述浏览器未被劫持。

具体的，所述浏览器还包括：

黑名单获取单元 407，用于在所述浏览器判断所述页面地址是否位于黑名单中之前，根据该浏览器被劫持的历史数据，获取并存储所述黑名单。

上述本申请实施例中的技术方案，至少具有如下的技术效果或优点：

根据本发明的一种识别被劫持浏览器的方法及浏览器，通过本发明，浏览器获取网页访问请求及其对应的操作信息，再检测所述操作信息是否符合预设规则，在符合所述预设规则时，识别出所述浏览器已被劫持，否则，则识别所述浏览器未被劫持，由于所述预设规则包括所述浏览器允许的操作请求，通过检测所述操作请求是否符合所述预设规则就能够更准确的识别出所述浏览器是否被劫持，如此，使得所述浏览器在根据所述判断结果识别出所述浏览器是否被劫持的准确性得以提高，而且所述浏览器是自行判断是否被劫持，与现有技术中的人工判断相比，其判断的工作效率也能够得到较大的提高。

进一步的，在所述操作信息不符合所述预设规则时，浏览器还获取网页访问请求对应的访问地址，再判断所述页面地址是否位于黑名单中，根据获得的判断结果，识别出所述浏览器是否被劫持，由于所述黑名单中存储有劫持所述浏览器的网址信息，使得根据所述判断结果能够更准确的识别出所述浏览器是否被劫持，如此，使得所述浏览器在根据所述判断结果识别出所述浏览器是否被劫持的准确性得以提高，而且所述浏览器是自行判断是否被劫持，与现有技术中的人工判断相比，其判断的工作效率也能够得到较大的提高。

参见图 5，本发明实施例提供的通过域名识别被劫持浏览器的方法包括以下步骤：

S501：浏览器获取导航页的网页访问请求，以及获取与所述网页访问请求对应的目标域名；

S502：浏览器判断所述目标域名是否与所述导航页的原始域名相一致；

S503：浏览器在判断出所述目标域名与所述原始域名一致时，则识别出所述浏览器未被劫持；

S504：浏览器在判断出所述目标域名与所述原始域名不一致时，则识别出所述浏览器已被劫持。

其中，在步骤 S501 中，浏览器在启动时会自动加载导航页，使得浏览器能够获取到所述导航页的网页访问请求，再根据所述网页访问请求，获取所述目标域名；当然，浏览器在启动之后，浏览器接收到用户启动所述导航页的启动请求，浏览器根据所述启动请求来加载所述导

航页，进而获取到所述导航页的网页访问请求，再根据所述网页访问请求，获取所述目标域名。

在具体实施过程中，浏览器在获取所述目标域名时，可以直接从所述网页访问请求中提取所述目标域名，所述网页访问请求具体可以为 http 格式的访问请求。

具体来讲，以 a 浏览器为例，a 浏览器启动时会自动加载 a 导航页，a 浏览器在加载 a 导航页时，会生成 a 导航页的网页访问请求例如包含有 String url = " http://hao.axxx.cn/"；如此，使得浏览器能够从 a 导航页的网页访问请求中提取目标域名为 hao.axxx.cn；若 a 浏览器启动之后，接收到用户启动 a 导航页的启动请求时，a 浏览器加载 a 导航页，生成 a 导航页的网页访问请求，然后从 a 导航页的网页访问请求中提取目标域名为 hao.axxx.cn。

当然，在 a 浏览器被劫持时，其加载的导航页可能为不是 a 导航页，而是其他浏览器的导航页，比如 b 导航页网页例如为商业网页、广告网页等，使得获取的所述目标域名与 a 导航页的原始域名不同；而 a 浏览器未被劫持时，使得获取的所述目标域名与 a 导航页的原始域名相同。

接下来执行步骤 S502，在该步骤中，浏览器判断所述目标域名是否与所述导航页的原始域名相一致。

在具体实施过程中，浏览器判断所述目标域名是否与所述导航页的原始域名相一致之前，浏览器中存储所述导航页的原始域名，如此，在获取所述目标域名之后，浏览器能够将所述目标域名与所述原始域名进行比对，从而判断出所述目标域名是否与所述原始域名相一致，当然，所述原始域名还可以存储在安装该浏览器的用户终端中。

具体来讲，浏览器获取到所述目标域名之后，判断所述目标域名与所述原始域名是否相同，若相同，则判断出所述目标域名与所述原始域名相一致；若不相同，则判断出所述目标域名与所述原始域名不一致。

具体的，在预先存储所述原始域名时，可以直接在浏览器第一次启动并加载所述导航页时，获取所述导航页的网址，然后从所述导航页的网址中提取所述导航页的原始域名，然后将所述原始域名存储在浏览器中；也可以在浏览器未被劫持之前，加载所述导航页时会自动生成所述导航页的网页访问请求，浏览器从所述网页访问请求中提取所述导航页的原始域名，然后在浏览器中存储所述原始域名。

例如，以 a 浏览器为例，a 浏览器启动时会自动加载 a 导航页，a 浏览器在加载 a 导航页时，会生成 a 导航页的网页访问请求例如包含有 String url = " http://hao.bxxx.cn/"；如此，使得浏览器能够从 a 导航页的网页访问请求中提取目标域名为 hao.bxxx.cn，若 a 浏览器中预先存储有 a 导航页的原始域名为 hao.axxx.cn，由于 hao.bxxx.cn 与 hao.axxx.cn 不同，即 a 浏览器判断所述目标域名与所述原始域名不一致；若 a 浏览器中预先存储有 a 导航页的原始域名为 hao.bxxx.cn，由于所述原始域名与所述目标域名相同，即 a 浏览器判断所述目标域名与所述原始域名一致。

浏览器在判断出所述目标域名与所述原始域名一致时，执行步骤 S503，识别出所述浏览器未被劫持；浏览器在判断出所述目标域名与所述原始域名不一致时，执行步骤 S504，识别出所述浏览器已被劫持。

在具体实施过程中，浏览器根据所述步骤 S502，在判断出所述目标域名与所述原始域名一致时，则识别出所述浏览器未被劫持；以及在判断出所述目标域名与所述原始域名不一致时，则识别出所述浏览器已被劫持。

具体来讲，以 a 浏览器为例，a 浏览器启动时会自动加载 a 导航页，a 浏览器在加载 a 导航页时，会生成 a 导航页的网页访问请求例如包含有 String url = " http://hao.bxxx.cn/"；如此，使得浏览器能够从 a 导航页的网页访问请求中提取目标域名为 hao.bxxx.cn，若 a 浏览器中预先存储有 a 导航页的原始域名为 hao.axxx.cn，由于 hao.bxxx.cn 与 hao.axxx.cn 不同，即 a 浏览器判断所述目标域名与所述原始域名不一致，则使得 a 浏览器检测到所述判断结果表征所述目标域名与所述原始域名不一致，从而识别出 a 浏览器已被劫持；若 a 浏览器中预先存储有 a 导航页的原始域名为 hao.bxxx.cn，由于所述原始域名与所述目标域名相同，即 a 浏览器判断所述目标域名与所述原始域名一致，使得 a 浏览器检测到所述判断结果表征所述目标域名与所述原始域名一致，从而识别出 a 浏览器未被劫持；如此，通过判断所述目标域名与所述原始域名是否一致就能够准确判断出 a 浏览器是否被劫持，提高判断的准确性，而且是通过 a 浏览器本身来判断自己是否被劫持，属于机器判断，与人工判断相比，其工作效率得到了较大的提高。

在另一实施例中，在所述识别出浏览器已被劫持时，所述方法还包括：浏览器生成提示信息，并在浏览器加载的页面上生成提示窗口；浏览器将所述提示信息加载在所述提示窗口中进行显示。

在具体实施过程中，浏览器识别出自身被劫持时，浏览器可以生成所述提示信息，所述提示信息具体可以是“浏览器已被劫持”、“浏览器存在安全风险”等文本信息，然后在浏览器加载的页面上生成所述提示窗口，并将所述提示信息加载到所述提示窗口中进行显示，以提醒用户。

具体来讲，所述提示信息还可以包括语音信息，在将所述提示信息加载在所述提示窗口中进行显示时，还可以将所述提示信息进行语音输出。

本申请实施例中提供的一个或多个技术方案，至少具有如下技术效果或优点：

根据本发明的一种通过域名识别被劫持浏览器的方法，通过本发明，浏览器获取网页访问请求及其对应的目标域名，再判断所述目标域名是否与所述导航页的原始域名相一致，在判断出所述目标域名与所述原始域名一致时，则识别出所述浏览器未被劫持；以及在判断出所述目标域名与所述原始域名不一致时，则识别出所述浏览器已被劫持；如此，能通过判断出所述目标域名是否与所述原始域名一致，以此来识别出所述浏览器是否被劫持，其识别的准确性也随之提高，而且是浏览器自行判断自己是否被劫持，与现有技术中的人工判断相比，其判断的工作效率也能够得到较大的提高。

根据同一发明构思，本申请另一实施例提供本申请还公开了一种浏览器，参见图 6，所述浏览器包括：

访问请求获取单元 601，用于获取浏览器的导航页的网页访问请求；

目标域名获取单元 602，用于获取与所述网页访问请求对应的目标域名；

判断单元 603，用于判断所述目标域名是否与所述导航页的原始域名相一致；

识别单元 604，用于在判断出所述目标域名与所述原始域名一致时，则识别出所述浏览器未被劫持；以及在判断出所述目标域名与所述原始域名不一致时，则识别出所述浏览器已被劫持。

具体的，访问请求获取单元 601，具体用于在启动并加载所述导航页时，获取所述导航页的网页访问请求；目标域名获取单元 602，具体用于根据所述网页访问请求，获取所述目标域名，具体可以从所述网页访问请求中提取所述目标域名。

其中，浏览器在启动时会自动加载导航页，访问请求获取单元 601 能够获取到所述导航页的网页访问请求，再根据所述网页访问请求，获取所述目标域名；当然，浏览器在启动之后，访问请求获取单元 601 接收到用户启动所述导航页的启动请求时，根据所述启动请也能够获取到所述导航页的网页访问请求。

具体的，所述浏览器还包括：

域名存储单元 605，用于在判断所述目标域名是否与所述导航页的原始域名相一致之前，存储所述导航页的原始域名。

其中，在判断单元 603 判断所述目标域名是否与所述导航页的原始域名相一致之前，域名存储单元 605 将所述导航页的原始域名存储在浏览器中，如此，在获取所述目标域名之后，判断单元 603 能够将所述目标域名与所述原始域名进行比对，从而判断出所述目标域名是否与所述原始域名相一致，当然，域名存储单元 605 还可以将所述原始域名存储在安装该浏览器的用户终端中。

进一步的，目标域名获取单元 602 获取到所述目标域名之后，判断单元 603 判断所述目标域名与所述原始域名是否相同，若相同，则判断出所述目标域名与所述原始域名相一致；若不相同，则判断出所述目标域名与所述原始域名不一致。

具体的，所述浏览器还包括提示信息和窗口生成单元 606，用于在所述识别出所述浏览器已被劫持时，生成提示信息，并在所述浏览器加载的页面上生成提示窗口；加载单元 607，用于将所述提示信息加载在所述提示窗口中进行显示。

上述本申请实施例中的技术方案，至少具有如下的技术效果或优点：

根据本发明的一种通过域名识别被劫持浏览器的方法，通过本发明，浏览器获取网页访问请求及其对应的目标域名，再判断所述目标域名是否与所述导航页的原始域名相一致，在判断出所述目标域名与所述原始域名一致时，则识别出所述浏览器未被劫持；以及在判断出所述目

标域名与所述原始域名不一致时，则识别出所述浏览器已被劫持；如此，能通过判断出所述目标域名是否与所述原始域名一致，以此来识别出所述浏览器是否被劫持，其识别的准确性也随之提高，而且是浏览器自行判断自己是否被劫持，与现有技术中的人工判断相比，其判断的工作效率也能够得到较大的提高。

参见图 7，本发明实施例还提供了一种识别被劫持浏览器的方法，包括以下步骤：

S701：获取浏览器的快捷方式的命令行的参数设置信息；

S702：判断所述参数设置信息对应的设置方式是否与预设方式相一致；

S703：在判断出所述设置方式与所述预设方式不一致时，识别出所述浏览器已被劫持；

S704：在判断出所述设置方式与所述预设方式一致时，识别出所述浏览器未被劫持。

其中，在步骤 S701 中，本发明的执行主体是设备，所述设备例如可以是平板电脑、笔记本电脑、智能手机、台式电脑等设备，所述设备中安装有浏览器，在获取浏览器的快捷方式的命令行的参数设置信息时，可以通过启动安装在所述设备中的命令行程序，例如在 windows 环境下，命令行程序通常为 cmd.exe，然后所述设备在接收到用户输入的与浏览器的快速方式对应的命令信息时，将所述参数设置信息显示在所述命令行程序中，如此，根据所述显示内容，即可获取所述参数设置信息，其中，所述参数设置信息中包含有所述快捷方式的设置方式信息。当然，还可以通过查看所述浏览器的快捷方式的属性信息来获取所述参数设置信息。

例如，以笔记本电脑 A 为例，在笔记本电脑 A 中安装有 b 浏览器并创建了 b 浏览器的快捷方式，根据接收到的用户在笔记本电脑 A 的开始菜单的搜索栏中输入了 cmd 的信息，则启动 cmd.exe，然后在根据接收到的搜索 b 浏览器的快捷方式对应的命令信息时，将 b 浏览器的快捷方式对应的参数设置信息显示在 cmd.exe 中，如此，使得笔记本电脑 A 获取到所述参数设置信息。

接下来执行步骤 S702，在该步骤中，判断所述参数设置信息对应的设置方式是否与预设方式相一致。

在具体实施过程中，所述预设方式为所述浏览器的快捷方式的默认的设置方式，具体可以是手动设置方式或自动设置方式，下面具体以所述预设方式为手动设置方式为例，在通过步骤 S701 获取到所述参数设置信息之后，从所述参数设置信息中获取所述快捷方式的设置方式信息，基于所述快捷方式的设置方式信息确定所述设置方式，然后判断所述设置方式是否为手动设置方式，在所述设置方式为手动设置方式时，则确定所述设置方式与所述预设方式相一致；若所述设置方式不为手动设置方式时，则确定所述设置方式与所述预设方式不一致，其中，所述预设方式为自动设置方式时其判断方法与上述判断方法相同。

例如，以笔记本电脑 A 为例，在笔记本电脑 A 中安装有 b 浏览器并创建了 b 浏览器的快捷方式，根据接收到的用户在笔记本电脑 A 的开始菜单的搜索栏中输入了 cmd 的信息，则启动 cmd.exe，然后在根据接收到的搜索 b 浏览器的快捷方式对应的命令信息时，将 b 浏览器的快捷方式对应的参数设置信息显示在 cmd.exe 中，如此，使得笔记本电脑 A 获取到所述参数设置信息，若所述参数设置信息中包含的所述快捷方式的设置方式信息显示 b 浏览器的快捷方式对应的设置方式为手动设置方式时，由于手动设置方式与所述预设方式相同，则确定所述设置方式与所述预设方式相一致；若 b 浏览器的快捷方式对应的设置方式为自动设置方式时，由于自动设置方式与所述预设方式不同，则确定所述设置方式与所述预设方式不一致。

在判断出所述设置方式与所述预设方式不一致时，执行步骤 S703，识别出所述浏览器已被劫持；在判断出所述设置方式与所述预设方式一致时，执行步骤 S704，识别出所述浏览器未被劫持。

在具体实施过程中，所述设备在通过步骤 S702 判断出所述设置方式与所述预设方式不一致时，识别出所述浏览器已被劫持，以及在判断出所述设置方式与所述预设方式一致时，识别出所述浏览器未被劫持。

例如，以笔记本电脑 A 为例，在笔记本电脑 A 中安装有 b 浏览器并创建了 b 浏览器的快捷方式，根据接收到的用户在笔记本电脑 A 的开始菜单的搜索栏中输入了 cmd 的信息，则启动 cmd.exe，然后在根据接收到的搜索 b 浏览器的快捷方式对应的命令信息时，将 b 浏览器的快捷方式对应的参数设置信息显示在 cmd.exe 中，如此，使得笔记本电脑 A 获取到所述参数设置信息，若所述参数设置信息中包含的所述快捷方式的设置方式信息显示 b 浏览器的快捷方式对应的设置方式为手动设置方式时，由于手动设置方式与所述预设方式相同，则确定所述设置方式

与所述预设方式相一致，如此，可以确定 b 浏览器未被劫持；若 b 浏览器的快捷方式对应的设置方式为自动设置方式时，由于自动设置方式与所述预设方式不同，则确定所述设置方式与所述预设方式不一致，如此，可以确定 b 浏览器已被劫持。

其中，在 b 浏览器未被劫持时，b 浏览器的快捷方式对应的设置方式必然为所述预设方式，而在 b 浏览器被劫持时，b 浏览器的快捷方式对应的设置方式才会与所述预设方式不同，如此，通过判断 b 浏览器的快捷方式对应的设置方式是否与所述预设方式相一致，即可以准确的判断出 b 浏览器是否被劫持，使得判断的准确性得以提高。

在另一实施例中，本发明实施例还提供了一种识别被劫持浏览器的方法，参见图 8，包括以下步骤：

S801：获取浏览器的快捷方式的命令行的参数设置信息；

S802：判断所述参数设置信息对应的设置方式是否与预设方式相一致；

S803：在判断出所述设置方式与所述预设方式一致时，判断所述参数设置信息对应目的链接是否位于预存的黑名单中，其中，所述黑名单中存储有劫持所述浏览器的网址信息；

S804：在判断出所述目的链接位于所述黑名单中时，则识别出所述浏览器已被劫持；

S805：在判断出所述目的链接未位于所述黑名单中时，则识别出所述浏览器未被劫持。

其中，在步骤 S801 中，本发明的执行主体是设备，所述设备例如可以是平板电脑、笔记本电脑、智能手机、台式电脑等设备，所述设备中安装有浏览器，在获取浏览器的快捷方式的命令行的参数设置信息时，可以通过启动安装在所述设备中的命令行程序，例如在 windows 环境下，命令行程序通常为 cmd.exe，然后所述设备在接收到用户输入的与浏览器的快速方式对应的命令信息时，将所述参数设置信息显示在所述命令行程序中，如此，根据所述显示内容，即可获取所述参数设置信息，其中，所述参数设置信息中包含有所述快捷方式的设置方式信息。当然，还可以通过查看所述浏览器的快捷方式的属性信息来获取所述参数设置信息。

接下来执行步骤 S802，在该步骤中，判断所述参数设置信息对应的设置方式是否与预设方式相一致。

在具体实施过程中，所述预设方式为所述浏览器的快捷方式的默认的设置方式，具体可以是手动设置方式或自动设置方式，下面具体以所述预设方式为手动设置方式为例，在通过步骤 S801 获取到所述参数设置信息之后，从所述参数设置信息中获取所述快捷方式的设置方式信息，基于所述快捷方式的设置方式信息确定所述设置方式，然后判断所述设置方式是否为手动设置方式，在所述设置方式为手动设置方式时，则确定所述设置方式与所述预设方式相一致；若所述设置方式不为手动设置方式时，则确定所述设置方式与所述预设方式不一致，其中，所述预设方式为自动设置方式时其判断方法与上述判断方法相同。

在判断出所述设置方式与所述预设方式一致时，执行步骤 S803，判断所述参数设置信息对应目的链接是否位于预存的黑名单中，其中，所述黑名单中存储有劫持所述浏览器的网址信息。

在具体实施过程中，在所述预设方式为手动设置方式时，若所述设置方式也为手动设置方式，则判断出所述设置方式与所述预设方式一致，此时，再判断所述目的链接是否位于所述黑名单中，即将所述目的链接与所述黑名单中的每一个网址信息进行比对，若所述黑名单中存在与所述目的链接相匹配的网址信息，则确定所述目的链接位于所述黑名单中；若所述黑名单中不存在与所述目的链接相匹配的网址信息，则确定所述目的链接不位于所述黑名单中，其中，所述目的链接可以从所述参数设置信息中提取，例如 b 浏览器的参数设置信息中包括 b 浏览器的快捷方式的设置方式信息、加载的目的链接的网址等信息，如此，根据 b 浏览器的参数设置信息即可以获取所述目标链接。

具体来讲，在将所述参数设置信息对应的目的链接添加到预存的黑名单之前，所述方法还包括：根据所述浏览器被劫持的历史数据，获取并存储所述黑名单，其中，所述设备在获取所述历史数据时，可以通过接收用户的反馈信息来获取所述历史数据，也可以通过数据采集和监控的方式来获取所述历史数据，再通过所述历史数据来获取所述黑名单之后，所述设备还可以不断收集浏览器被劫持的其它数据，以此来不断更新所述黑名单，使得所述黑名单中能够存储更多的劫持浏览器的网址信息，以提高判断的准确性。

例如，以笔记本电脑 A 为例，在笔记本电脑 A 中安装有 b 浏览器，笔记本电脑 A 收集到 b 浏览器被劫持的历史数据中显示有 A 网址、B 网址和 C 网址均劫持过 a 浏览器，然后建立所

述黑名单，使得所述黑名单中存储有 A 网址、B 网址和 C 网址。

又例如，以笔记本电脑 A 为例，在笔记本电脑 A 中安装有 b 浏览器，笔记本电脑 A 根据当前收集到的历史数据生成了所述黑名单，所述黑名单中存储有 A 网址、B 网址、C 网址，在生成所述黑名单之后，笔记本电脑 A 持续收集 b 浏览器被劫持的其它数据，在收集到的其它数据中包含有 D 网址也劫持过 b 浏览器的数据时，则将 D 网址添加到所述黑名单中，使得更新后的黑名单中存储有 D 网址，由于更新后的所述黑名单中存储有 D 网址，如此，使得所述黑名单中能够存储更多的劫持浏览器的网址信息，通过更新后的所述黑名单就能够判断出所述访问地址是否位于所述黑名单中时，使得判断的准确性得以提高。

具体的，所述设备还可以在判断出所述设置方式与所述预设方式不一致时，识别出所述浏览器已被劫持时，将所述参数设置信息对应的目的链接添加到预存的黑名单中，其中，所述黑名单中存储有劫持所述浏览器的网址信息。

例如，以笔记本电脑 A 为例，在笔记本电脑 A 中安装有 b 浏览器并创建了 b 浏览器的快捷方式，根据接收到的用户在笔记本电脑 A 的开始菜单的搜索栏中输入了 cmd 的信息，则启动 cmd.exe，然后在根据接收到的搜索 b 浏览器的快捷方式对应的命令信息时，将 b 浏览器的快捷方式对应的参数设置信息显示在 cmd.exe 中，如此，使得笔记本电脑 A 获取到所述参数设置信息，若根据所述参数设置信息，获取到的 b 浏览器的快捷方式对应的设置方式为自动设置方式时，由于自动设置方式与所述预设方式不同，则确定所述设置方式与所述预设方式不一致，如此，可以确定 b 浏览器已被劫持，这时，可以从所述参数设置信息中提取所述目的链接例如为 E 网址，则将 E 网址则添加到所述黑名单中，如此，使得所述黑名单中能够存储更多的劫持浏览器的网址信息。

在判断出所述目的链接位于所述黑名单中时，执行步骤 S804，识别出所述浏览器已被劫持；在判断出所述目的链接未位于所述黑名单中时，执行步骤 S805，识别出所述浏览器未被劫持。

在具体实施过程中，所述设备在通过步骤 S803 判断出所述目的链接位于所述黑名单中时，则确认所述浏览器已被劫持；以及判断出所述目的链接未位于所述黑名单中时，则确认所述浏览器未被劫持。

例如，以笔记本电脑 A 为例，在笔记本电脑 A 中安装有 b 浏览器并创建了 b 浏览器的快捷方式，根据接收到的用户在笔记本电脑 A 的开始菜单的搜索栏中输入了 cmd 的信息，则启动 cmd.exe，然后在根据接收到的搜索 b 浏览器的快捷方式对应的命令信息时，将 b 浏览器的快捷方式对应的参数设置信息显示在 cmd.exe 中，如此，使得笔记本电脑 A 获取到所述参数设置信息，若根据所述参数设置信息，获取到的 b 浏览器的快捷方式对应的设置方式为手动设置方式时，由于手动设置方式与所述预设方式不同，则确定所述设置方式与所述预设方式一致，如此，可以确定 b 浏览器未被劫持，这时，可以从所述参数设置信息中提取所述目的链接例如为 A 网址，若所述黑名单中存储有 A 网址、B 网址和 C 网址，可知所述目的链接位于所述黑名单中，则确认 b 浏览器已被劫持；若所述目的链接例如为 D 网址，而所述黑名单中未存储有 D 网址，则可以确定 b 浏览器未被劫持；如此，再判断出所述设置方式与所述预设方式一致时，通过所述目的链接是否位于所述黑名单来进一步判断 b 浏览器是否被劫持，以进一步提高判断所述浏览器是否被劫持的准确性。

在另一实施例中，在所述识别出浏览器已被劫持时，所述方法还包括：生成提示信息，并在浏览器加载的页面上生成提示窗口；将所述提示信息加载在所述提示窗口中进行显示。

在具体实施过程中，所述设备识别出浏览器被劫持时，自动生成所述提示信息，所述提示信息具体可以是“浏览器已被劫持”、“浏览器存在安全风险”等文本信息，并在所述浏览器加载的页面上生成所述提示窗口，将所述提示信息加载到所述提示窗口中进行显示，以提醒用户。

具体来讲，所述提示信息还可以包括语音信息，在将所述提示信息加载在所述提示窗口中进行显示时，还可以将所述提示信息进行语音输出。

本申请实施例中提供的一个或多个技术方案，至少具有如下技术效果或优点：

根据本发明的一种识别被劫持浏览器的方法及设备，通过本发明，获取浏览器的快捷方式的命令行的参数设置信息；判断所述参数设置信息对应的设置方式是否与预设方式相一致；在判断出所述设置方式与所述预设方式不一致时，识别出所述浏览器已被劫持；在判断出所述设

置方式与所述预设方式一致时，识别出所述浏览器未被劫持；如此，使得可以通过判断所述设置方式是否与所述预设方式相一致来判断出所述设置方式是否已被修改，而在浏览器未被劫持时，所述设置方式与所述预设方式是一致的，而在浏览器被劫持的情况下，所述设置方式可能会与所述预设方式不一致，从而使得通过判断所述设置方式是否与所述预设方式相一致就能够准确识别出所述浏览器是否被劫持，提高了识别的准确性，而且是通过机器判断方式来判断浏览器是否被劫持的，与现有技术中的人工判断相比，其判断的工作效率也能够得到较大的提高。

进一步的，通过本发明，在判断出所述设置方式与所述预设方式一致时，还可以判断所述参数设置信息对应的目的链接是否位于预存的黑名单中，以此来判断所述浏览器是否被劫持，由于所述黑名单中存储有劫持所述浏览器的网址信息，使得根据所述判断结果能够更准确的识别出所述浏览器是否被劫持，如此，使得所述浏览器在根据所述判断结果识别出所述浏览器是否被劫持的准确性得以进一步提高。

根据同一发明构思，本申请另一实施例提供本申请还公开了一种识别被劫持浏览器的设备，参见图 9，所述设备包括：

命令行参数获取单元 901，用于获取浏览器的快捷方式的命令行的参数设置信息；

判断单元 902，用于判断所述参数设置信息对应的设置方式是否与预设方式相一致；

识别单元 903，用于在判断出所述设置方式与所述预设方式不一致时，识别出所述浏览器已被劫持；以及在判断出所述设置方式与所述预设方式一致时，识别出所述浏览器未被劫持。

其中，所述预设方式为所述浏览器的快捷方式的默认的设置方式，具体可以是手动设置方式或自动设置方式

具体的，判断单元 902，具体用于在所述预设方式为手动设置方式时，判断所述设置方式是否为手动设置方式。

具体的，所述设备还包括添加单元 904，用于在所述识别出所述浏览器被劫持之后，将所述参数设置信息对应的目的链接添加到预存的黑名单中，其中，所述黑名单中存储有劫持所述浏览器的网址信息。

具体的，判断单元 902，还用于在判断出在所述设置方式为手动设置方式时，判断所述参数设置信息对应目的链接是否位于预存的黑名单中，其中，所述黑名单中存储有劫持所述浏览器的网址信息；

识别单元 903，还用于在判断出所述目的链接位于所述黑名单中时，识别出所述浏览器已被劫持；在判断出所述目的链接未位于所述黑名单中时，则识别出所述浏览器未被劫持。

具体的，所述设备还包括黑名单存储单元 905，用于在将所述参数设置信息对应的目的链接添加到预存的黑名单之前，根据所述浏览器被劫持的历史数据，获取并存储所述黑名单。

具体的，所述设备还包括：

提示信息和窗口生成单元 906，用于在所述识别出所述浏览器已被劫持时，生成提示信息，并在所述浏览器加载的页面上生成提示窗口；

加载单元 907，用于将所述提示信息加载在所述提示窗口中进行显示。

上述本申请实施例中的技术方案，至少具有如下的技术效果或优点：

根据本发明的一种识别被劫持浏览器的方法及设备，通过本发明，获取浏览器的快捷方式的命令行的参数设置信息；判断所述参数设置信息对应的设置方式是否与预设方式相一致；在判断出所述设置方式与所述预设方式不一致时，识别出所述浏览器已被劫持；在判断出所述设置方式与所述预设方式一致时，识别出所述浏览器未被劫持；如此，使得可以通过判断所述设置方式是否与所述预设方式相一致来判断出所述设置方式是否已被修改，而在浏览器未被劫持时，所述设置方式与所述预设方式是一致的，而在浏览器被劫持的情况下，所述设置方式可能会与所述预设方式不一致，从而使得通过判断所述设置方式是否与所述预设方式相一致就能够准确识别出所述浏览器是否被劫持，提高了识别的准确性，而且是通过机器判断方式来判断浏览器是否被劫持的，与现有技术中的人工判断相比，其判断的工作效率也能够得到较大的提高。

进一步的，通过本发明，在判断出所述设置方式与所述预设方式一致时，还可以判断所述参数设置信息对应的目的链接是否位于预存的黑名单中，以此来判断所述浏览器是否被劫持，由于所述黑名单中存储有劫持所述浏览器的网址信息，使得根据所述判断结果能够更准确的识别出所述浏览器是否被劫持，如此，使得所述浏览器在根据所述判断结果识别出所述浏览器是否被劫持的准确性得以进一步提高。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以

在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

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

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

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

本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，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浏览器、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 10 示出了可以实现识别被劫持浏览器的方法的计算设备。该计算设备传统上包括处理器 1010 和以存储器 1020 形式的计算机程序产品或者计算机可读介质。存储器 1020 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 1020 具有用于执行上述方法中的任何方法步骤的程序代码 1031 的存储空间 1030。例如，用于程序代码的存储空间 1030 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 1031。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 11 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 10 的计算设备中的存储器 1020 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 1031’，即可以由例如诸如 1010 之类的处理器读取的代码，这些代码当由计算设备运行时，导致该计算设备执行上面所描述的方法中的各个步骤。

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

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、一种识别被劫持浏览器的方法，包括：

浏览器获取网页访问请求及其对应的操作信息；

所述浏览器检测所述操作信息是否符合预设规则，所述预设规则包括所述浏览器允许的操作请求；

所述浏览器在检测出所述操作信息不符合所述预设规则时，识别出所述浏览器已被劫持；

所述浏览器检测出所述操作信息符合所述预设规则时，识别出所述浏览器未被劫持。

2、如权利要求 1 所述的方法，其中，在所述网页访问请求为所述浏览器的导航页的网页访问请求时，所述方法还包括：

所述浏览器判断所述导航页的网页访问请求对应的访问地址是否为所述导航页的导航地址；

所述浏览器判断出所述访问地址不为所述导航地址时，则识别出所述浏览器已被劫持；

所述浏览器判断出所述访问地址为所述导航地址时，则识别出所述浏览器未被劫持。

3、如权利要求 2 所述的方法，其中，在所述网页访问请求为所述浏览器的导航页的网页访问请求时，所述浏览器获取导航页的网页访问请求，具体包括：

所述浏览器启动并加载所述导航页时，获取所述导航页的网页访问请求。

4、如权利要求 1 所述的方法，其中，

所述浏览器获取网页访问请求及其对应的操作信息，具体包括：浏览器获取导航页的网页访问请求，以及获取与所述网页访问请求对应的目标域名；

所述浏览器检测所述操作信息是否符合预设规则，具体包括：所述浏览器判断所述目标域名是否与所述导航页的原始域名相一致；

所述浏览器检测出所述操作信息符合所述预设规则时，识别出所述浏览器未被劫持，具体包括：所述浏览器在判断出所述目标域名与所述原始域名一致时，则识别出所述浏览器未被劫持；

所述浏览器在检测出所述操作信息不符合所述预设规则时，识别出所述浏览器已被劫持，具体包括：所述浏览器在判断出所述目标域名与所述原始域名不一致时，则识别出所述浏览器已被劫持。

5、如权利要求 4 所述的方法，其特征在于，所述浏览器获取导航页的网页访问请求，以及获取与所述网页访问请求对应的访问地址，具体包括：

所述浏览器启动并加载所述导航页时，获取所述导航页的网页访问请求；

所述浏览器根据所述网页访问请求，获取所述目标域名。

6、如权利要求 4 或 5 所述的方法，其特征在于，所述浏览器判断所述目标域名是否与所述导航页的原始域名相一致之前，所述方法还包括：

所述浏览器中预先存储所述导航页的原始域名。

7、如权利要求 4 或 5 所述的方法，其特征在于，在所述识别出所述浏览器已被劫持时，所述方法还包括：

所述浏览器生成提示信息，并在所述浏览器加载的页面上生成提示窗口；

所述浏览器将所述提示信息加载在所述提示窗口中进行显示。

8、如权利要求 1 所述的方法，其中，

所述浏览器获取网页访问请求及其对应的操作信息，具体包括：获取浏览器的快捷方式的命令行的参数设置信息；

所述浏览器检测所述操作信息是否符合预设规则，具体包括：判断所述参数设置信息对应的设置方式是否与预设方式相一致；

所述浏览器在检测出所述操作信息不符合所述预设规则时，识别出所述浏览器已被劫持，具体包括：在判断出所述设置方式与所述预设方式不一致时，识别出所述浏览器已被劫持；

所述浏览器检测出所述操作信息符合所述预设规则时，识别出所述浏览器未被劫持，具体包括：在判断出所述设置方式与所述预设方式一致时，识别出所述浏览器未被劫持。

9、如权利要求 8 所述的方法，其中，在所述预设方式为手动设置方式时，所述判断所述参数设置信息是否与预设方式相一致，具体包括：

判断所述设置方式是否为手动设置方式。

10、如权利要求 9 所述的方法，其中，所述识别出所述浏览器被劫持之后，所述方法还包括：

将所述参数设置信息对应的目的链接添加到预存的黑名单中，其中，所述黑名单中存储有劫持所述浏览器的网址信息。

11、如权利要求 9 所述的方法，其中，所述在判断出所述设置方式与所述预设方式一致时，所述方法还包括：

在所述设置方式为手动设置方式时，判断与所述参数设置信息对应的目的链接是否位于预存的黑名单中，其中，所述黑名单中存储有劫持所述浏览器的网址信息；

在判断出所述目的链接位于所述黑名单中时，则识别出所述浏览器已被劫持；

在判断出所述目的链接未位于所述黑名单中时，则识别出所述浏览器未被劫持。

12、如权利要求 11 所述的方法，其中，在将所述参数设置信息对应的目的链接添加到预存的黑名单之前，所述方法还包括：

根据所述浏览器被劫持的历史数据，获取并存储所述黑名单。

13、如权利要求 8 或 11 所述的方法，其中，在所述识别出所述浏览器已被劫持时，所述方法还包括：

生成提示信息，并在所述浏览器加载的页面上生成提示窗口；

将所述提示信息加载在所述提示窗口中进行显示。

14、一种识别被劫持浏览器的方法，包括：

浏览器获取网页访问请求及其对应的操作信息；

所述浏览器检测所述操作信息是否符合预设规则，所述预设规则包括所述浏览器允许的操作请求；

所述浏览器在检测出所述操作信息不符合所述预设规则时，获取与所述网页访问请求对应的搜索页面的页面地址；

所述浏览器判断所述页面地址是否位于黑名单中，获得判断结果，其中，所述黑名单中存储有劫持所述浏览器的网址信息；

所述浏览器在检测到所述判断结果表征所述页面地址位于所述黑名单中时，则识别出所述浏览器已被劫持；

所述浏览器在检测到所述判断结果表征所述页面地址未位于所述黑名单中时，则识别出所述浏览器未被劫持。

15、如权利要求 14 所述的方法，其中，在所述浏览器判断所述页面地址是否位于黑名单中之前，所述方法还包括：

所述浏览器根据该浏览器被劫持的历史数据，获取并存储所述黑名单。

16、一种浏览器，包括：

访问请求获取单元，用于获取网页访问请求；

操作信息获取单元，用于获取与所述网页访问请求对应的操作信息；

检测单元，用于检测所述操作信息是否符合预设规则，所述预设规则包括所述浏览器允许的操作请求；

识别单元，用于在检测出所述操作信息不符合所述预设规则时，识别出所述浏览器已被劫持；以及在检测出所述操作信息符合所述预设规则时，识别出所述浏览器未被劫持。

17、如权利要求 16 所述的浏览器，其中，所述浏览器还包括：

判断单元，还用于在所述网页访问请求为所述浏览器的导航页的网页访问请求时，判断所述导航页的网页访问请求对应的访问地址是否为所述导航页的导航地址；

所述识别单元，还用于在判断出所述访问地址不为所述导航地址时，识别出所述浏览器已被劫持；以及判断出所述访问地址为所述导航地址时，识别出所述浏览器未被劫持。

18、如权利要求 17 所述的浏览器，其中，所述访问请求获取单元，还用于在所述网页访问请求为所述浏览器的导航页的网页访问请求时，启动并加载所述导航页时，获取所述导航页的网页访问请求。

19、如权利要求 16 所述的浏览器，其中，所述浏览器还包括：

所述访问请求获取单元，具体用于获取浏览器的导航页的网页访问请求；

目标域名获取单元，用于获取与所述网页访问请求对应的目标域名；

判断单元，用于判断所述目标域名是否与所述导航页的原始域名相一致；

所述识别单元，具体用于在判断出所述目标域名与所述原始域名一致时，则识别出所述浏览器未被劫持；以及在判断出所述目标域名与所述原始域名不一致时，则识别出所述浏览器已被劫持。

20、如权利要求 19 所述的浏览器，其中，所述访问请求获取单元，具体用于在启动并加载所述导航页时，获取所述导航页的网页访问请求；

所述目标域名获取单元，具体用于根据所述网页访问请求，获取所述目标域名。

21、如权利要求 19 或 20 所述的浏览器，其中，所述浏览器还包括：

域名存储单元，用于在判断所述目标域名是否与所述导航页的原始域名相一致之前，存储所述导航页的原始域名。

22、如权利要求 19 或 20 所述的浏览器，其中，所述浏览器还包括：

提示信息和窗口生成单元，用于在所述识别出所述浏览器已被劫持时， 生成提示信息，并在所述浏览器加载的页面上生成提示窗口；

加载单元，用于将所述提示信息加载在所述提示窗口中进行显示。

23、如权利要求 16 所述的浏览器，其中，所述浏览器还包括：

命令行参数获取单元，用于获取浏览器的快捷方式的命令行的参数设置信息；

判断单元，用于判断所述参数设置信息对应的设置方式是否与预设方式相一致；

所述识别单元，具体用于在判断出所述设置方式与所述预设方式不一致时，识别出所述浏览器已被劫持；以及在判断出所述设置方式与所述预设方式一致时，识别出所述浏览器未被劫持。

24、如权利要求 23 所述的浏览器，其中，所述判断单元，具体用于在所述预设方式为手动设置方式时，判断所述设置方式是否为手动设置方式。

25、如权利要求 24 所述的浏览器，其中，所述浏览器还包括：

添加单元，用于在所述识别出所述浏览器被劫持之后，将所述参数设置信息对应的目的链接添加到预存的黑名单中，其中，所述黑名单中存储有劫持所述浏览器的网址信息。

26、如权利要求 24 所述的浏览器，其中，所述判断单元，还用于在判断出在所述设置方式为手动设置方式时，判断所述参数设置信息对应目的链接是否位于预存的黑名单中，其中，所述黑名单中存储有劫持所述浏览器的网址信息；

所述识别单元，还用于在判断出所述目的链接位于所述黑名单中时，识别出所述浏览器已被劫持；在判断出所述目的链接未位于所述黑名单中时，则识别出所述浏览器未被劫持。

27、如权利要求 26 所述的浏览器，其中，所述浏览器还包括：

黑名单存储单元，用于在将所述参数设置信息对应的目的链接添加到预存的黑名单之前，根据所述浏览器被劫持的历史数据，获取并存储所述黑名单。

28、如权利要求 23 或 26 所述的浏览器，其中，所述浏览器还包括：

提示信息和窗口生成单元，用于在所述识别出所述浏览器已被劫持时，生成提示信息，并在所述浏览器加载的页面上生成提示窗口；

加载单元，用于将所述提示信息加载在所述提示窗口中进行显示。

29、一种浏览器，包括：

访问请求获取单元，用于获取网页访问请求；

操作信息获取单元，用于获取与所述网页访问请求对应的操作信息；

检测单元，用于检测所述操作信息是否符合预设规则，所述预设规则包括所述浏览器允许的操作请求；

页面地址获取单元，用于在检测出所述操作信息不符合所述预设规则时，获取与所述网页访问请求对应的搜索页面的页面地址；

判断单元，用于判断所述页面地址是否位于黑名单中，获得判断结果，其中，所述黑名单中存储有劫持所述浏览器的网址信息；

识别单元，用于在检测到所述判断结果表征所述页面地址位于所述黑名单中时，则识别出所述浏览器已被劫持；以及在检测到所述判断结果表征所述页面地址未位于所述黑名单中时，则识别出所述浏览器未被劫持。

30、如权利要求 29 所述的浏览器，其中，所述浏览器还包括：

黑名单获取单元，用于在所述浏览器判断所述页面地址是否位于黑名单中之前，根据该浏

览器被劫持的历史数据，获取并存储所述黑名单。

31、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计算设备上运行时，导致所述计算设备执行根据权利要求 1 至 15 任一项所述的识别被劫持浏览器的方法。

32、一种计算机可读介质，其中存储了如权利要求 31 所述的计算机程序。

5

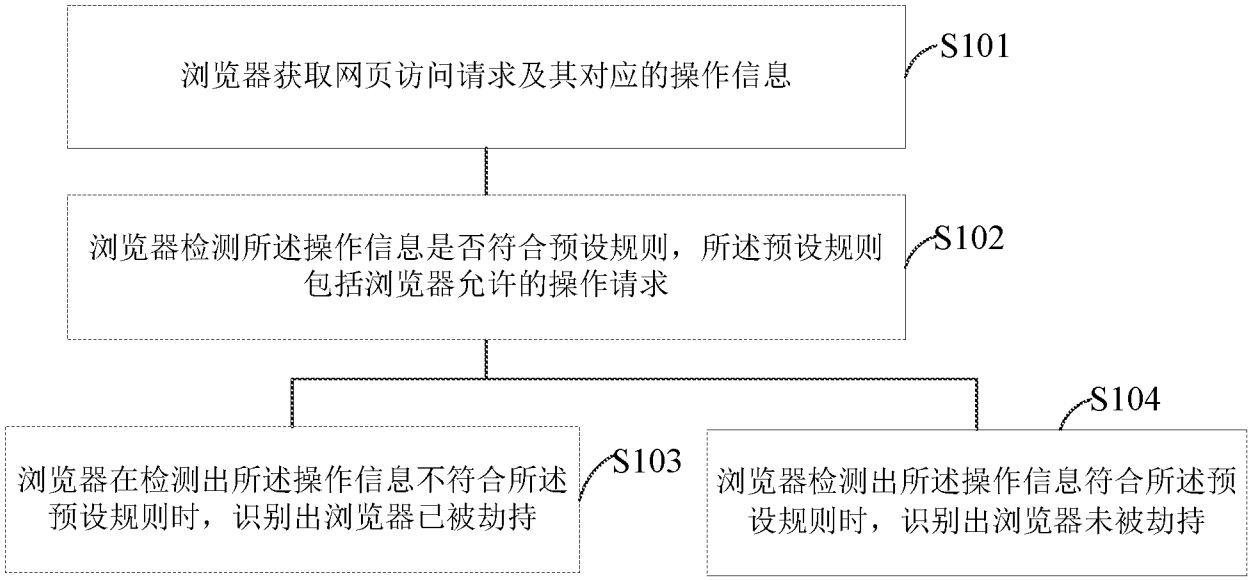
浏览器获取网页访问请求及其对应的操作信息
S101
浏览器检测所述操作信息是否符合预设规则，所述预设规则包括浏览器允许的操作请求
S102
浏览器在检测出所述操作信息不符合所述预设规则时，识别出浏览器已被劫持
S103
S104
浏览器检测出所述操作信息符合所述预设规则时，识别出浏览器未被劫持

图 1

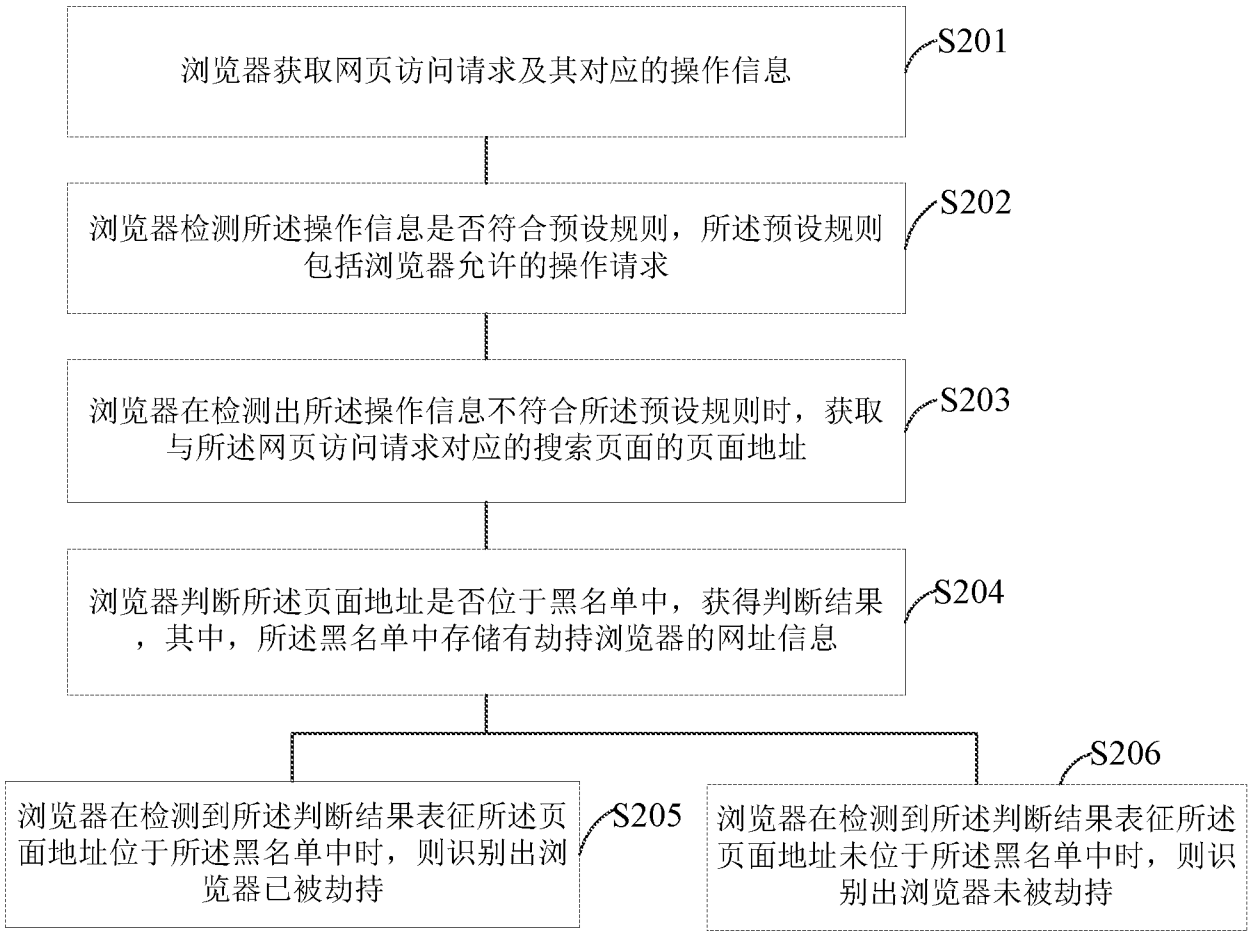
浏览器获取网页访问请求及其对应的操作信息
S201
浏览器检测所述操作信息是否符合预设规则，所述预设规则包括浏览器允许的操作请求
S202
浏览器在检测出所述操作信息不符合所述预设规则时，获取与所述网页访问请求对应的搜索页面的页面地址
S203
浏览器判断所述页面地址是否位于黑名单中，获得判断结果，其中，所述黑名单中存储有劫持浏览器的网址信息
S204
浏览器在检测到所述判断结果表征所述页面地址位于所述黑名单中时，则识别出浏览器已被劫持
S205
S206
浏览器在检测到所述判断结果表征所述页面地址未位于所述黑名单中时，则识别出浏览器未被劫持

图 2

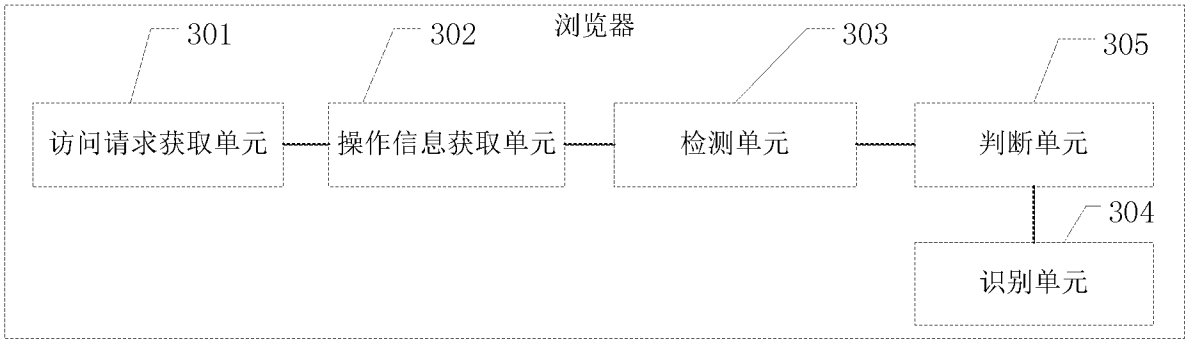
浏览器
301
302
303
305
304
访问请求获取单元
操作信息获取单元
检测单元
判断单元
识别单元

图 3

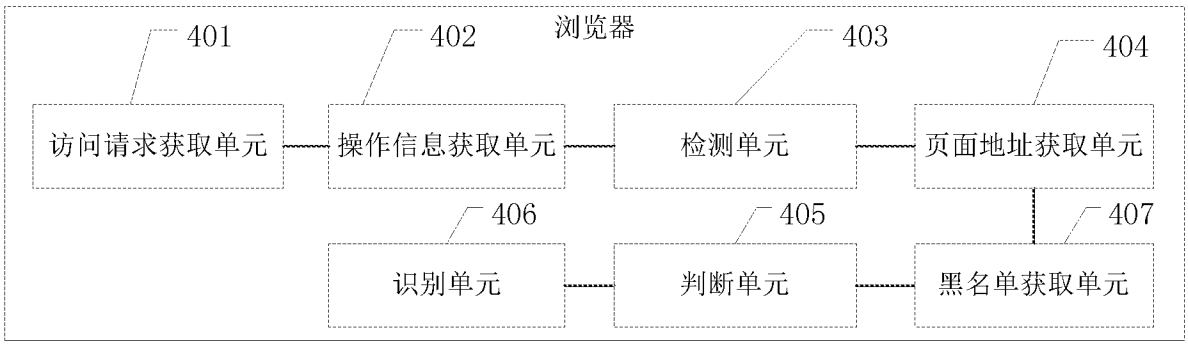
浏览器
401
402
403
404
406
405
407
访问请求获取单元
操作信息获取单元
检测单元
页面地址获取单元
识别单元
判断单元
黑名单获取单元

图 4

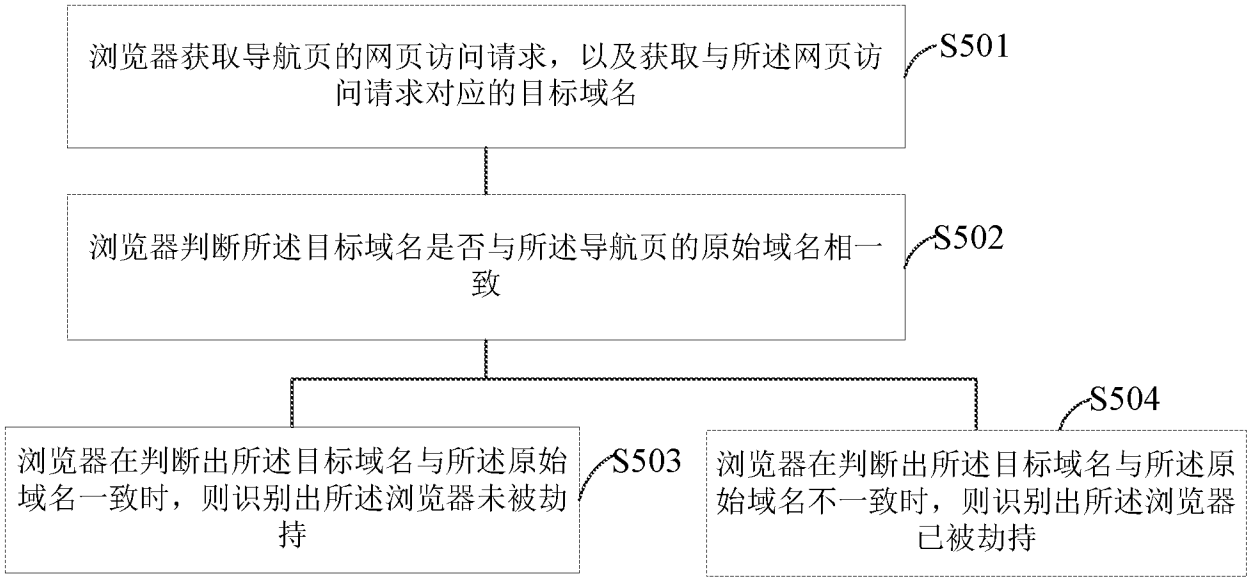
浏览器获取导航页的网页访问请求，以及获取与所述网页访问请求对应的目标域名
S501
浏览器判断所述目标域名是否与所述导航页的原始域名相一致
S502
浏览器在判断出所述目标域名与所述原始域名一致时，则识别出所述浏览器未被劫持
S503
浏览器在判断出所述目标域名与所述原始域名不一致时，则识别出所述浏览器已被劫持
S504

图 5

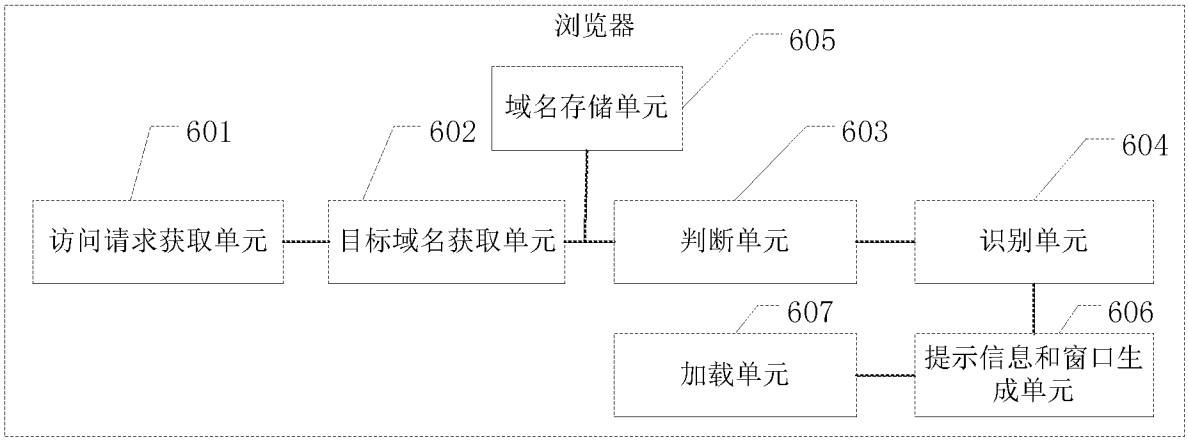
浏览器
605
域名存储单元
601
602
603
604
访问请求获取单元
目标域名获取单元
判断单元
识别单元
607
606
加载单元
提示信息和窗口生成单元

图 6

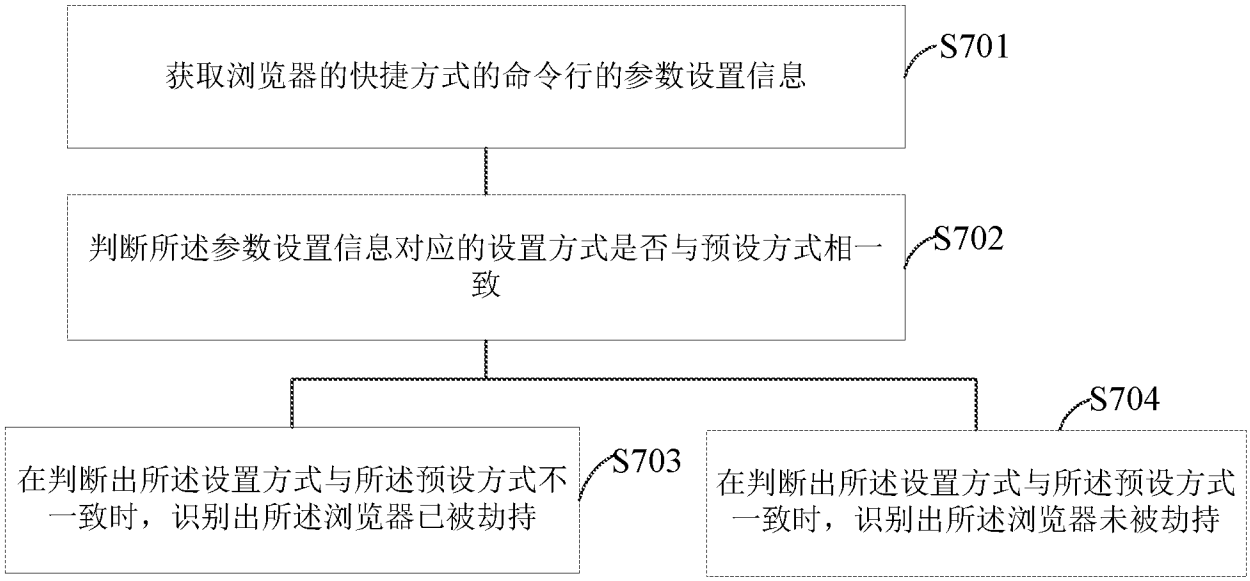
获取浏览器的快捷方式的命令行的参数设置信息
S701
判断所述参数设置信息对应的设置方式是否与预设方式相一致
S702
S704
在判断出所述设置方式与所述预设方式不一致时，识别出所述浏览器已被劫持
S703
在判断出所述设置方式与所述预设方式一致时，识别出所述浏览器未被劫持

图 7

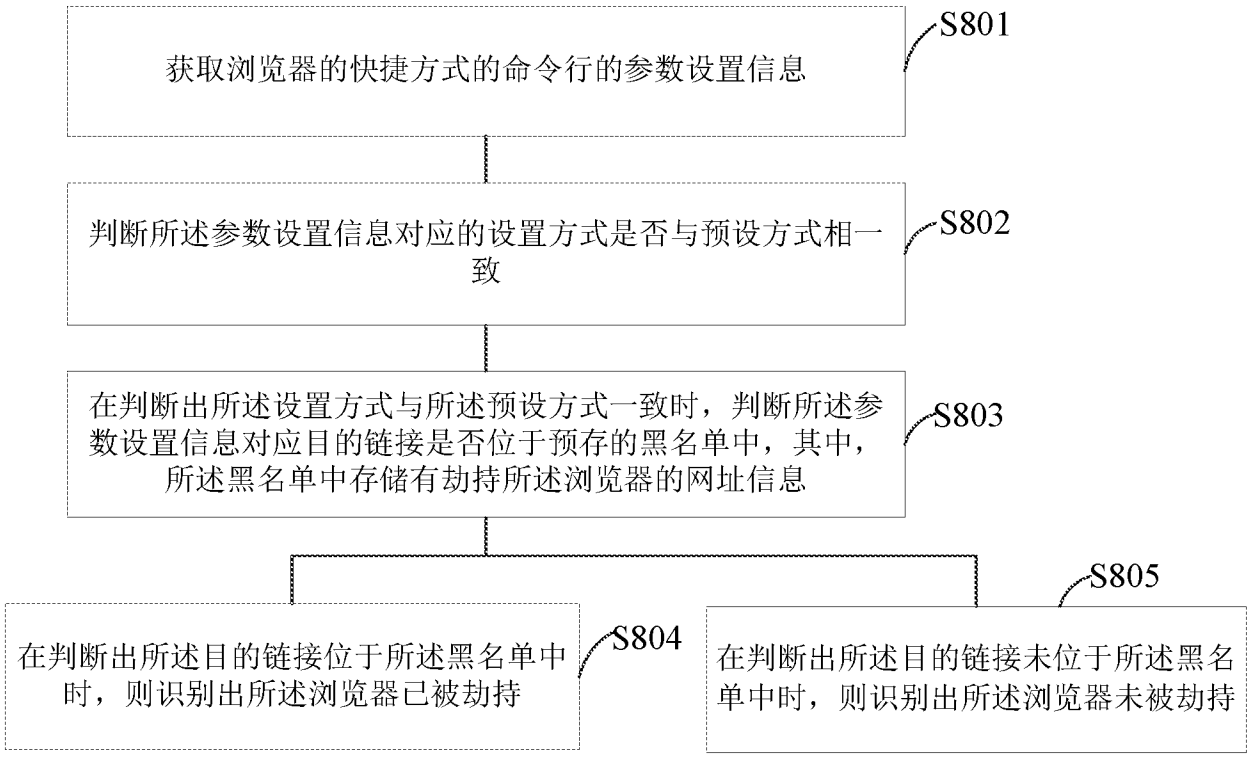
获取浏览器的快捷方式的命令行的参数设置信息
S801
判断所述参数设置信息对应的设置方式是否与预设方式相一致
S802
在判断出所述设置方式与所述预设方式一致时，判断所述参数设置信息对应目的链接是否位于预存的黑名单中，其中，所述黑名单中存储有劫持所述浏览器的网址信息
S803
在判断出所述目的链接位于所述黑名单中时，则识别出所述浏览器已被劫持
S804
S805
在判断出所述目的链接未位于所述黑名单中时，则识别出所述浏览器未被劫持

图 8

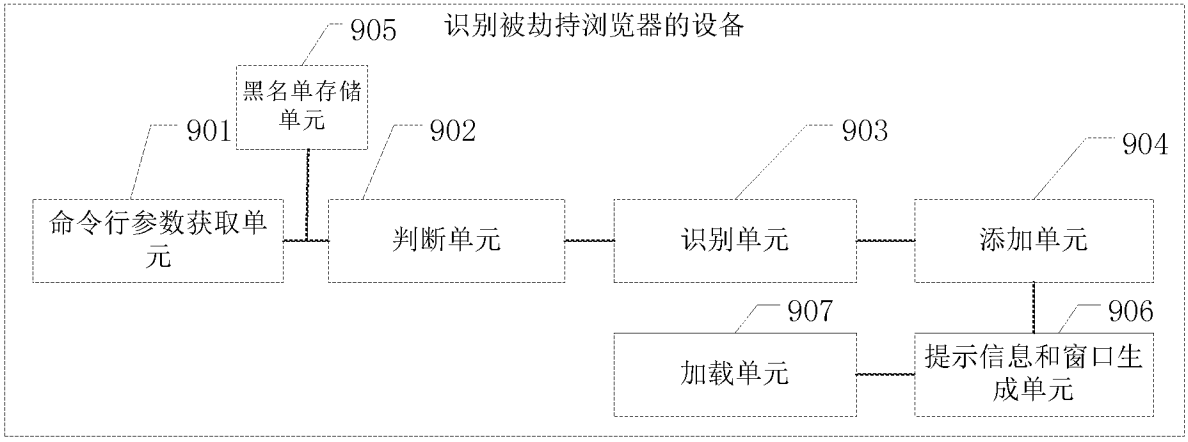
识别被劫持浏览器的设备
905
黑名单存储单元
901
902
903
904
命令行参数获取单元
判断单元
识别单元
添加单元
907
906
加载单元
提示信息和窗口生成单元

图 9

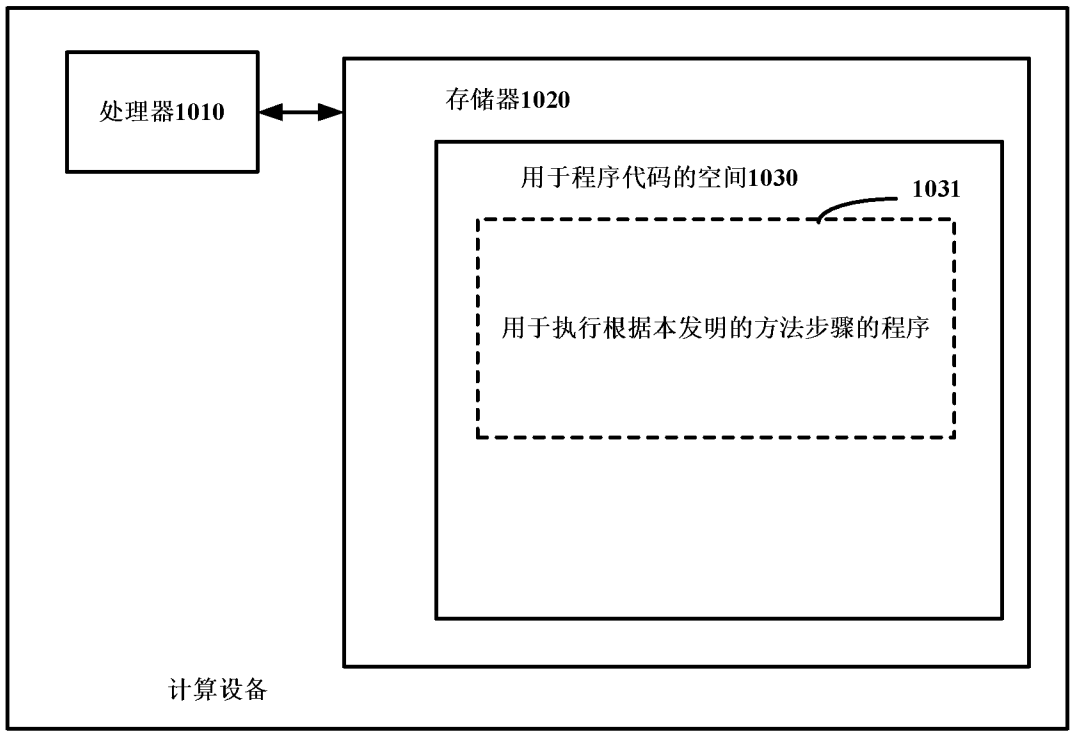
处理器1010
存储器1020
用于程序代码的空间1030
1031
用于执行根据本发明的方法步骤的程序
计算设备

图 10

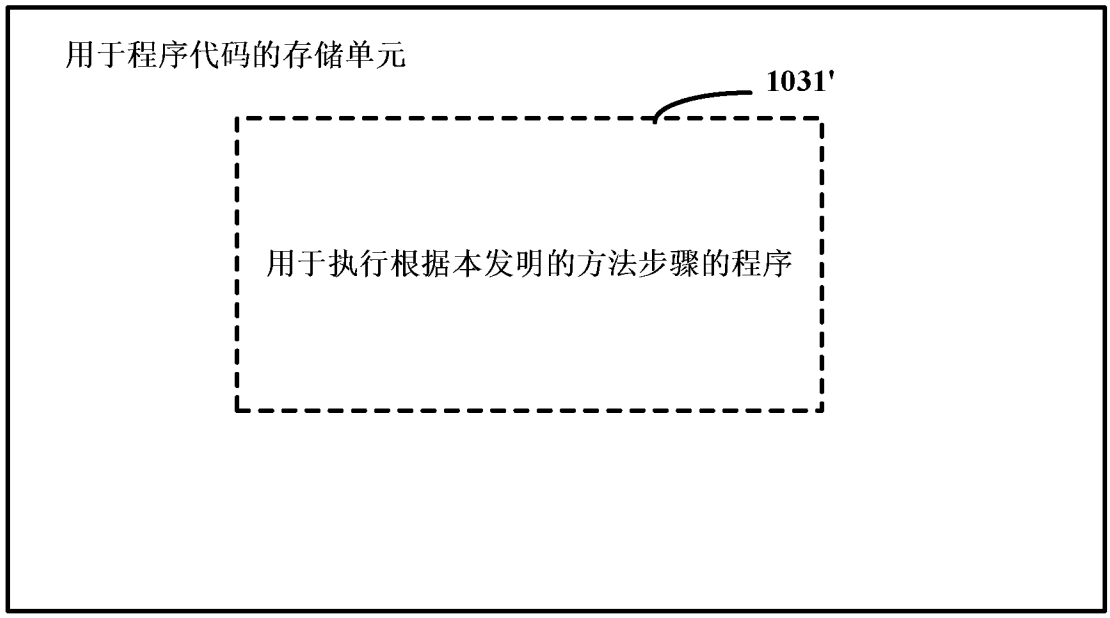
用于程序代码的存储单元
1031'
用于执行根据本发明的方法步骤的程序

图 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/100426

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/55 (2013.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F, H04L

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

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

CNPAT, CNKI, WPI, EPODOC, GOOGLE: web address, uniform resource locator, consistent, conform, browser, hijack, attack, tamper, navigation page, domain name, shortcut, search page, start page, main page, web page, address, URL, same, different, black list

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102780684 A (TONGJI UNIVERSITY), 14 November 2012 (14.11.2012), description, paragraphs 5 and 23-36, and figure 1	1, 14-16, 29-32
PX	CN 105160246 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 16 December 2015 (16.12.2015), claims 1-10, and description, paragraphs 125-128	1-3, 14-18, 29-32
PY	CN 105160246 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 16 December 2015 (16.12.2015), claims 1-10, and description, paragraphs 125-128	4-13, 19-28
PY	CN 105160247 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 16 December 2015 (16.12.2015), claims 1-10	8-13, 23-28
PY	CN 105357265 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 24 February 2016 (24.02.2016), claims 1-8	4-7, 19-22
PX	CN 105354490 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 24 February 2016 (24.02.2016), description, paragraphs 44-59 and 96-99	1, 4-6, 8-9, 16, 19-21, 23-24, 31-32

☒ 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
17 December 2016 (17.12.2016)	**03 January 2017 (03.01.2017)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **DONG, Libo** Telephone No.: (86-10) **61648110**

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/100426

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 105243134 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 13 January 2016 (13.01.2016), description, paragraphs 40-53 and 84-87	1, 4-6, 8-9, 16, 19-21, 23-24, 31-32
PX	CN 105224653 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 06 January 2016 (06.01.2016), description, paragraphs 45-59 and 117-120	1, 4-6, 8-9, 16, 19-21, 23-24, 31-32
PX	CN 105205393 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 30 December 2015 (30.12.2015), description, paragraphs 47-63 and 123-126	1, 4-6, 8-9, 16, 19-21, 23-24, 31-32
A	CN 104486140 A (NORTH CHINA ELECTRIC POWER UNIVERSITY et al.), 01 April 2015 (01.04.2015), the whole document	1-32
A	CN 102375951 A (BEILONG KNET (BEIJING) TECHNOLOGY CO., LTD.), 14 March 2012 (14.03.2012), the whole document	1-32
A	US 7712132 B1 (OGILVIE, J.W.), 04 May 2010 (04.05.2010), the whole document	1-32
A	CN 104601543 A (BAIDU ONLINE NETWORK TECHNOLOGY (BEIJING) CO., LTD.), 06 May 2015 (06.05.2015), the whole document	1-32

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/100426

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102780684 A	14 November 2012	None	
CN 105160246 A	16 December 2015	None	
CN 105160247 A	16 December 2015	None	
CN 105357265 A	24 February 2016	None	
CN 105354490 A	24 February 2016	None	
CN 105243134 A	13 January 2016	None	
CN 105224653 A	06 January 2016	None	
CN 105205393 A	30 December 2015	None	
CN 104486140 A	01 April 2015	None	
CN 102375951 A	14 March 2012	None	
US 7712132 B1	04 May 2010	US 2012110666 A1	03 May 2012
		US 2010269178 A1	21 October 2010
CN 104601543 A	06 May 2015	None	

国际检索报告

国际申请号 PCT/CN2016/100426

A. 主题的分类

G06F 21/55(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F, H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNPAT, CNKI, WPI, EPODOC, GOOGLE: 浏览器, 劫持, 攻击, 篡改, 导航页, 域名, 快捷方式, 搜索页面, 主页, 网址, 统一资源定位符, 相同, 一致, 相符, 不同, 黑名单, browser, hijack, attack, tamper, navigation page, domain name, shortcut, search page, start page, main page, web page, address, URL, same, different, black list

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
X	CN 102780684 A (同济大学) 2012年 11月 14日 (2012-11-14) 说明书第5, 23-36段, 图1	1, 14-16, 29-32
PX	CN 105160246 A (北京奇虎科技有限公司等) 2015年 12月 16日 (2015-12-16) 权利要求1-10, 说明书第125-128段	1-3, 14-18, 29-32
PY	CN 105160246 A (北京奇虎科技有限公司等) 2015年 12月 16日 (2015-12-16) 权利要求1-10, 说明书第125-128段	4-13, 19-28
PY	CN 105160247 A (北京奇虎科技有限公司等) 2015年 12月 16日 (2015-12-16) 权利要求1-10	8-13, 23-28
PY	CN 105357265 A (北京奇虎科技有限公司等) 2016年 2月 24日 (2016-02-24) 权利要求1-8	4-7, 19-22
PX	CN 105354490 A (北京奇虎科技有限公司等) 2016年 2月 24日 (2016-02-24) 说明书第44-59, 96-99段	1, 4-6, 8-9, 16, 19-21, 23-24, 31-32

☑ 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
2016年 12月 17日	2017年 1月 3日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	董立波
传真号 (86-10)62019451	电话号码 (86-10)61648110

国际检索报告

国际申请号
PCT/CN2016/100426

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 105243134 A (北京奇虎科技有限公司等) 2016年 1月 13日 (2016 - 01 - 13) 说明书第40-53, 84-87段	1, 4-6, 8-9, 16, 19-21, 23-24, 31-32
PX	CN 105224653 A (北京奇虎科技有限公司等) 2016年 1月 6日 (2016 - 01 - 06) 说明书第45-59, 117-120段	1, 4-6, 8-9, 16, 19-21, 23-24, 31-32
PX	CN 105205393 A (北京奇虎科技有限公司等) 2015年 12月 30日 (2015 - 12 - 30) 说明书第47-63, 123-126段	1, 4-6, 8-9, 16, 19-21, 23-24, 31-32
A	CN 104486140 A (华北电力大学等) 2015年 4月 1日 (2015 - 04 - 01) 全文	1-32
A	CN 102375951 A (北龙中网北京科技有限责任公司) 2012年 3月 14日 (2012 - 03 - 14) 全文	1-32
A	US 7712132 B1 (OGILVIE, JOHN W.) 2010年 5月 4日 (2010 - 05 - 04) 全文	1-32
A	CN 104601543 A (百度在线网络技术北京有限公司) 2015年 5月 6日 (2015 - 05 - 06) 全文	1-32

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/100426

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	102780684	A	2012年 11月 14日	无			
CN	105160246	A	2015年 12月 16日	无			
CN	105160247	A	2015年 12月 16日	无			
CN	105357265	A	2016年 2月 24日	无			
CN	105354490	A	2016年 2月 24日	无			
CN	105243134	A	2016年 1月 13日	无			
CN	105224653	A	2016年 1月 6日	无			
CN	105205393	A	2015年 12月 30日	无			
CN	104486140	A	2015年 4月 1日	无			
CN	102375951	A	2012年 3月 14日	无			
US	7712132	B1	2010年 5月 4日	US	2012110666	A1	2012年 5月 3日
				US	2010269178	A1	2010年 10月 21日
CN	104601543	A	2015年 5月 6日	无			