(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 12 月 31 日 (31.12.2014)

WIPO | PCT

(10) 国际公布号
WO 2014/206183 A1

(51) 国际专利分类号:
G06F 21/56 (2013.01)

(21) 国际申请号: PCT/CN2014/079169

(22) 国际申请日: 2014 年 6 月 4 日 (04.06.2014)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201310268314.5 2013 年 6 月 28 日 (28.06.2013) CN

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

(72) 发明人: 刘娇 (LIU, Jiao); 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: 北京华沛德权律师事务所 (BEIJING BRIGHT & RIGHT LAW FIRM); 中国北京市朝阳区朝外大街乙 12 号昆泰国际大厦 1008 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, IR, 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)。

根据细则 4.17 的声明:
— 关于申请人有权申请并被授予专利(细则 4.17(ii))

[见续页]

(54) Title: MACRO VIRUS SCANNING METHOD AND SYSTEM

(54) 发明名称 : 宏病毒查杀方法及系统

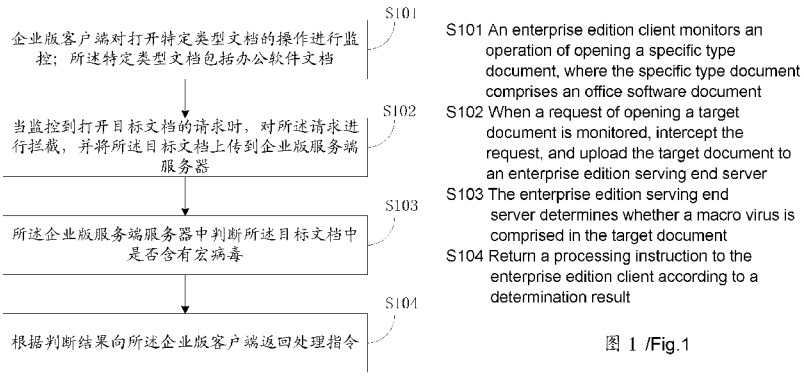

图 1 /Fig.1

(57) Abstract: Disclosed are a macro virus scanning method and system that are applied in an enterprise edition virus scanning application program. The method comprises: an enterprise edition client monitoring an operation of opening a specific type document, where the specific type document comprises an office software document; when a request of opening a target document is monitored, intercepting the request, and uploading the target document to an enterprise edition serving end; the enterprise edition serving end determining whether a macro virus is comprised in the target document; and returning a processing instruction to the enterprise edition client according to a determination result. By means of the foregoing method and system, the spread of macro viruses inside an enterprise network may be prevented more effectively.

(57) 摘要: 公开了宏病毒查杀方法及系统，应用于企业版病毒查杀应用程序中，所述方法包括：所述企业版客户端对打开特定类型文档的操作进行监控；所述特定类型文档包括办公软件文档；当监控到打开目标文档的请求时，对所述请求进行拦截，并将所述目标文档上传到企业版服务端；所述企业版服务端判断所述目标文档中是否含有宏病毒；根据判断结果向所述企业版客户端返回处理指令。通过上述方法和系统，能够更有效地抵御宏病毒在企业网内部的传播。

WO 2014/206183 A1

— 发明人资格(细则 4.17(iv))

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

宏病毒查杀方法及系统

技术领域

本发明涉及计算机安全技术领域，具体涉及宏病毒查杀方法及系统。

背景技术

宏病毒是病毒制造者利用Microsoft Office的开放性，即Office中提供的BASIC编程接口，专门开发的一个或多个具有病毒特点的宏集合。这种病毒宏的集合会影响到计算机使用，并能通过DOC文档及DOT模板进行自我复制及传播。一旦打开感染宏病毒的文档，其宏就会被执行，宏病毒就会被激活，进一步转移到计算机上，并驻留在Normal模板上。从此以后，所有自动保存的文档都会“感染”上这种宏病毒，而且如果其他用户打开了感染病毒的文档，宏病毒又会转移到他的计算机上。

随着微软对Office 97以上版本的修正，使大部分基于以前Word版本的宏病毒无法复制，宏病毒的泛滥得以遏制，但是宏病毒变种却开始感染用户的电脑，同时，宏病毒的感染范围由个人用户逐渐向企业用户过渡，宏病毒对企业的危害开始凸显。宏病毒对于个人用户的危害已经不言而喻，它隐蔽性高、传播快、易变种，使用户无法正常使用办公文档，极易产生文档无法编写、打印机不能使用、文件无法储存等危害。然而，相对于个人用户，企业内网中的宏病毒无疑是更巨大的灾难。其危害性通常表现为以下几点:

第一、宏病毒在内网中极易造成传播，防护难度大。办公文件的流转是办公数据传送的最通常方式之一，无数的办公文件以金字塔般的形式，从上级传播到基层，基层与基层之间又不停地进行互动，这种办公文件的流动忠实地传播和复制宏病毒，让IT管理员束手无策。

第二、宏病毒能够破坏内网中的关键数据，造成内网中数据遭受严重破坏并大规模丢失，要进行恢复，难度大，耗费时间长。

第三、宏病毒变种成本低，对系统威胁严重。大多数文档用宏语言Word Basic编写宏指令，而宏病毒同样用Word Basic编写。Word Basic语言提供了多种系统级底层调用，如Dos、调用Windows API、DLL等，这些操作均可能对系统构成直接威胁。而Word、Excel文档在指令安全性以及完整性上的检测功能很弱，因此，破坏系统的指令就很容易被执行，而对于新变种产生的宏病毒，企业必须对全网的防护软件进行统一的升级才能及时的防护，但这对于企业中的管理员来讲并不是一件简单的事情。

除此之外，内网中如果感染了宏病毒还会造成单位的打印机无法正常使

用、内网设备跨平台交叉感染等危害，因此，防治企业内网中的宏病毒在整个企业的防病毒策略中至关重要。

现行的解决企业内部宏病毒的方法是通过在内网的客户端上部署查杀工具进行查杀，但是，由于宏病毒的变种极快，要想跟随宏病毒的变种速度，需要以相当过程更快的速度更新宏病毒库，这就使得终端保存的宏病毒库不断变得庞大臃肿，影响查杀效率，甚至影响终端系统的正常运行。另外，如果内网的终端不能够连接互联网，那么只能连接管理端进行更新宏病毒库，查杀效率更低，无法快速抵御变种的宏病毒。总之，需要更有效的方式来抵御宏病毒在企业网内部的传播。

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宏病毒查杀方法及系统，能够更有效地抵御宏病毒在企业网内部的传播。

依据本发明的一个方面，提供了一种宏病毒查杀方法，应用于企业版病毒查杀应用程序中，其中，所述企业版病毒查杀应用程序包括安装在企业用户管理控制中心计算设备上的企业版服务端，以及安装在企业用户终端设备上的企业版客户端，通过企业版服务端实现对各个企业版客户端所在用户终端设备的统一管理，所述方法包括：

所述企业版客户端对打开特定类型文档的操作进行监控；所述特定类型文档包括办公软件文档；

当监控到打开目标文档的请求时，对所述请求进行拦截，并将所述目标文档上传到企业版服务端；

所述企业版服务端判断所述目标文档中是否含有宏病毒；

根据判断结果向所述企业版客户端返回处理指令。

根据本发明的另一方面，提供了一种宏病毒查杀系统，应用于企业版病毒查杀应用程序中，其中，所述企业版病毒查杀应用程序包括安装在企业用户管理控制中心计算设备上的企业版服务端，以及安装在企业用户终端设备上的企业版客户端，通过企业版服务端实现对各个企业版客户端所在用户终端设备的统一管理，所述系统包括：

监控单元，位于企业版客户端，用于对打开特定类型文档的操作进行监控；所述特定类型文档包括办公软件文档；

上传单元，位于企业版客户端，用于当监控到打开目标文档的请求时，对所述请求进行拦截，并将所述目标文档上传到企业版服务端；

判断单元，位于企业版服务端，用于判断所述目标文档中是否含有宏病毒；

指令返回单元，位于企业版服务端，用于根据判断结果向所述企业版客户端返回处理指令。

根据本发明的宏病毒查杀方法及系统，在需要打开一个文档时，企业版客户端可以将该文档上传至企业版服务端进行宏病毒的查杀，这样，就不必在企业版客户端保存宏病毒特征库，不会出现病毒库过于庞大臃肿而导致查杀效率下降的问题，并且，企业版服务端保存的宏病毒特征库可以及时的更新，这样可以更及时的应对新的宏病毒变种，达到更全面的宏病毒查杀效果。并且，由于单个用户在操作文件时可以及时发现文件中是否存在宏病毒，因此，可以避免从一个用户到企业网内其他用户的宏病毒传播，提高企业网内部抵御宏病毒的能力。

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

附图说明

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

图1示出了根据本发明一个实施例的方法的流程图；以及，

图2示出了根据本发明一个实施例的系统的示意图；

图3示出了用于执行根据本发明的方法的智能电子设备的框图；以及

图4示出了用于保持或者携带实现根据本发明的方法的程序代码的存储单元示意图。

具体实施方式

下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

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。

参见图1，本发明实施例提供了一种宏病毒查杀方法，该方法可以应用于企业版病毒查杀应用程序中，其中，所述企业版病毒查杀应用程序包括安装在企业用户管理控制中心计算设备上的企业版服务端，以及安装在企业用户终端设备上的企业版客户端，通过企业版服务端实现对各个企业版客户端所在用户终端设备的统一管理。也就是说，这种企业版病毒查杀应用程序相当于在企业网内部形成了一种“私有云”，企业版的服务端，就相当于该私有云的服务器，相对于公有云而言，私有云仅为企业内网的用户服务，企业网客户端与企业网服务端之间可以通过局域网的方式进行通信，因此，即使在企业网客户端没有连接到互联网的情况下，也能利用企业网服务端获取到所需的应用或者服务。在上述部署了私有云的前提下，该方法可以包括以下步骤：

S101：所述企业版客户端对打开特定类型文档的操作进行监控；所述特定类型文档包括办公软件文档；

其中，所谓的特定类型文档就可以包括word、excel等办公软件文档。在本发明实施例中，并不是进行全盘扫描式的宏病毒查杀，而是在用户想要打开某文档时，针对该文档进行宏病毒的查杀。为此，可以预先在系统中注册钩子函数，对文件编辑类的API（Application Programming Interface，应用程序编程接口）函数进行钩挂（HOOK），这样，当通过调用对应的API函数打开某文档时，就会将调用的地址转向本发明实施例提供的宏病毒查杀模块。

S102：当监控到打开目标文档的请求时，对所述请求进行拦截，并将所述目标文档上传到企业版服务端；

监控到打开某文档的请求之后，就可以将该请求进行拦截，也即暂时不会将该请求发送到API函数所在的地址处，而是先进行安全相关的处理。在本发明实施例中，当企业版客户端拦截到打开文档的请求之后，并不是直接在企业版客户端本地对文档进行分析，而是直接将文档上传至企业版服务端，以便在企业版服务端进行具体的分析工作。其中，在部署企业版安全产品时，就可以在各个企业版客户端中保存企业版服务端的地址，因此，在拦截到打开文档的请求之后，就可以根据请求中携带的文档路径等信息找到对应的文档，并按照企业版服务端的地址，将其上传至企业版服务端。

需要说明的是，在对一个打开文档的请求进行拦截之后，由于后续的安全性分析工作需要一段时间，因此，在这段期间内，企业版客户端可以加载显示一个预置的界面，用以显示正在进行宏病毒检测。

S103：所述企业版服务端判断所述目标文档中是否含有宏病毒；

企业版服务端在接收到企业版客户端上传的文档之后，就可以判断文档中是否含有宏病毒。其中，具体在判断一个文档中是否含有宏病毒时，可以根据宏病毒所共有的一些特征进行判断，例如，大多数宏病毒中都含有AutoOpen，AutoClose，AutoNew和AutoExit等自动宏，因为只有这样，宏病毒才能获得文档（模板）操作控制权。有些宏病毒还通过FileNew，FileOpen，FileSave，FileSaveAs，FileExit等宏控制文件的操作。另外，病毒宏中必然含有对文档读写操作的宏指令，宏病毒在.DOC文档、.DOT模板中以BFF(BinaryFileFormat)格式存放，等等。

另外，在本发明实施例中，还可以从文档中进行特征提取，然后将提取到的特征与预先设置的特征库中包括的特征进行比对，进而根据比对的结果判断一个文档中是否包含有宏病毒。其中，根据宏病毒自身的特征，在从待判断的文档中提取宏病毒时，可以首先判断目标文档是否存在脚本文件，如果不存在，则证明该目标文档中不存在宏病毒；如果存在脚本文件，则从脚本中提取特征，例如包含的字符串信息等等，然后再与特征库中的特征进行比对。

其中，特征库里保存的特征可以是已知的宏病毒所具有的特征，也即，该特征库可以是个黑名单，这样，在进行比对时，如果目标文档中提取出的特征出现在该特征库中，则可以证明目标文档中带有宏病毒；如果提取出的特征未出现在该特征库中，则可以认为目标文档中不存在宏病毒，或者也可以作为未知信息提示企业版服务端的技术人员进行进一步的分析判断等等。或者，特征库中保存的特征也可以是一个白名单，这可以看作是一个宏知识库，它记录系统预定义的所有宏，同时还允许用户手工地增加自定义的宏，这样，将目标文档中提取出的特征与特征库中的特征进行匹配时，如果匹配成功，则证明目标文档中不存在宏病毒，否则，如果匹配不成功，则可以认为目标文档中存在宏病毒，或者可能存在宏病毒，提示技术人员进行进一步分析判断，等等。

其中，对于各种形式的特征库，可以是在安装企业版服务端时，就下载最新版本的特征库到企业版服务端所在的计算机本地；而在公有云服务器端，在通过对新的宏病毒变种的分析获得新的宏病毒特征之后，可以及时地对特征库进行更新，而企业版服务端的宏病毒查杀引擎可以定时或者不定时的连接公有云服务器，对特征库进行升级更新。其中，具体在对特征库进行升级时，可以采用覆盖式或者增量式的更新方法。也就是说，由于特征库本身一般是一个文件，因此，当企业版服务端需要更新特征库时，可以从公有云服务器下载完整的最新版本的特征库文件，用新下载到的特征库文件覆盖之前的特征库文件。或者，也可以将当前版本上传到公有云服务器，公有云服务器仅将最新版本中相对于当前版本存在更新的内容返回给企业版服务端，企业版服务端再根据公

有云服务器返回的数据，对之前的特征库文件进行更新，包括增加新的特征、修改原有特征、删除原有特征，等等。

需要说明的是，在本发明实施例中，由于病毒库只保存在企业版服务端所在的计算机上，因此，只要企业版服务端所在的计算机能够连接到互联网，即可及时对特征库进行升级更新，而不需要各个企业版客户端分别进行下载及更新，因此，有利于节省企业网的带宽资源。

S104：根据判断结果向所述企业版客户端返回处理指令。

在判断出目标文档中是否存在宏病毒之后，就可以向企业版客户端返回指令。例如，如果判断出目标文档中不存在宏病毒，则证明目标文档是安全的，因此可以直接返回一个将当前截获到的请求放行的指令，这样，打开文档的请求会顺利到达原调用地址，进行文档的打开及后续的编辑操作。

而如果判断出目标文档中存在宏病毒，则证明目标文档是不安全的，则可以将目标文档中存在的宏病毒清除，得到一个安全文档，并下发给企业版客户端。然后，在返回给企业版客户端的指令中可以包括以下几方面的信息：首先，将当前截获到的请求丢弃，也即确保请求打开原目标文档的请求不会再被执行，同时指示企业版客户端将原目标文档删除，替换为清除了宏病毒之后的安全文档，并将安全文档打开。这样，企业版客户端执行的结果是：向用户打开了一个文档，使得用户能够查看到文档中的内容，并且避免触发原来存在于该文档中的宏病毒，保证系统的安全性。

需要说明的是，具体如何判断一个文档中是否包含宏病毒，以及如何清除文档中的宏病毒，属于已有技术中的方法，这里不再详述。

总之，在本发明实施例中，在需要打开一个文档时，企业版客户端可以将该文档上传至企业版服务端进行宏病毒的查杀，这样，就不必在企业版客户端保存宏病毒特征库，不会出现病毒库过于庞大臃肿而导致查杀效率下降的问题，并且，企业版服务端保存的宏病毒特征库可以及时的更新，这样可以更及时的应对新的宏病毒变种，达到更全面的宏病毒查杀效果。并且，由于单个用户在操作文件时可以及时发现文件中是否存在宏病毒，因此，可以避免从一个用户到企业网内其他用户的宏病毒传播，提高企业网内部抵御宏病毒的能力。

与本发明实施例提供的宏病毒查杀方法相对应，本发明实施例还提供了一种宏病毒查杀系统，该系统应用于企业版病毒查杀应用程序中，其中，所述企业版病毒查杀应用程序包括安装在企业用户管理控制中心计算设备上的企业版服务端，以及安装在企业用户终端设备上的企业版客户端，通过企业版服务端实现对各个企业版客户端所在用户终端设备的统一管理，参见图2，所述系统可以包括以下单元：

监控单元201，位于企业版客户端，用于对打开特定类型文档的操作进行监控；所述特定类型文档包括办公软件文档；

上传单元202，位于企业版客户端，用于当监控到打开目标文档的请求时，对所述请求进行拦截，并将所述目标文档上传到企业版服务端；

判断单元203，位于企业版服务端，用于判断所述目标文档中是否含有宏病毒；

指令返回单元204，位于企业版服务端，用于根据判断结果向所述企业版客户端返回处理指令。

具体实现时，根据查杀结果的不同，所述指令返回单元204具体可以包括：

第一指令返回子单元，用于如果判断结果为所述目标文档中不含有宏病毒，则向所述企业版客户端返回将所述请求放行的指令。

或者，所述指令返回单元204也可以包括：

清除子单元，用于如果判断结果为所述目标文档中含有宏病毒，则将所述目标文档中的宏病毒清除，得到安全文档；

第二指令返回子单元，用于向所述企业版客户端返回所述安全文档，以及返回丢弃所述请求、用所述安全文档替换所述目标文档并打开所述安全文档的指令。

在实际应用中，由于宏病毒查杀的过程中可能需要一段时间，因此，在从拦截到请求到接收到企业版服务端返回指令之前，该装置还可以包括：

显示单元，位于企业版客户端，用于所述对所述请求进行拦截之后，加载显示预置的界面，用以显示正在进行宏病毒检测。

具体实现时，所述判断单元203可以包括：

特征提取子单元，用于从所述目标文档包含的脚本中进行特征提取；

特征比对子单元，用于将提取到的特征与预置的宏病毒库中保存的特征进行比对，根据比对结果判断是否存在宏病毒。

另外，该系统还可以包括：

更新单元，位于企业版服务端，用于连接公有云服务器，以便对企业版服务端的宏病毒库进行升级更新。

总之，在本发明实施例中，在需要打开一个文档时，企业版客户端可以将该文档上传至企业版服务端进行宏病毒的查杀，这样，就不必在企业版客户端保存宏病毒特征库，不会出现病毒库过于庞大臃肿而导致查杀效率下降的问题，并且，企业版服务端保存的宏病毒特征库可以及时的更新，这样可以更及时的应对新的宏病毒变种，达到更全面的宏病毒查杀效果。并且，由于单个用户在操作文件时可以及时发现文件中是否存在宏病毒，因此，可以避免从一个

用户到企业网内其他用户的宏病毒传播，提高企业网内部抵御宏病毒的能力。

在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

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

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

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

本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，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宏病毒查杀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3示出了可以实现根据本发明的移动终端处理可视化图形编码的方法的智能电子设备。该智能电子设备传统上包括处理器310和以存储器320形式的计算机程序产品或者计算机可读介质。存储器320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320具有用于执行上述方法中的任何方法步骤的程序代码331的存储空间330。例如，用于程序代码的存储空间330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331。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4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3的智能电子设备中的存储器320类似布置的存储段或者存储空间等。程序代码可以例如以适当形式进行压缩。通常，存储单元包括用于执行根据本发明的方法步骤的程序331'，即可以由例如诸如310之类的处理器读取的代码，这些代码当由智能电子设备运行时，导致该智能电子设备执行上面所描述的方法中的各个步骤。

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。

权 利 要 求

1、一种宏病毒查杀方法，应用于企业版病毒查杀应用程序中，其中，所述企业版病毒查杀应用程序包括安装在企业用户管理控制中心计算设备上的企业版服务端，以及安装在企业用户终端设备上的企业版客户端，通过企业版服务端实现对各个企业版客户端所在用户终端设备的统一管理，所述方法包括:

所述企业版客户端对打开特定类型文档的操作进行监控;所述特定类型文档包括办公软件文档;

当监控到打开目标文档的请求时，对所述请求进行拦截，并将所述目标文档上传到企业版服务端;

所述企业版服务端判断所述目标文档中是否含有宏病毒;

根据判断结果向所述企业版客户端返回处理指令。

2、如权利要求1所述的方法，所述根据判断结果向所述企业版客户端返回处理指令包括:

如果判断结果为所述目标文档中不含有宏病毒，则向所述企业版客户端返回将所述请求放行的指令。

3、如权利要求1所述的方法，所述根据判断结果向所述企业版客户端返回处理指令包括:

如果判断结果为所述目标文档中含有宏病毒，则将所述目标文档中的宏病毒清除，得到安全文档;

向所述企业版客户端返回所述安全文档，以及返回丢弃所述请求、用所述安全文档替换所述目标文档并打开所述安全文档的指令。

4、如权利要求1所述的方法，还包括:

所述企业版客户端对所述请求进行拦截之后，加载显示预置的界面，用以显示正在进行宏病毒检测。

5、如权利要求1至4任一项所述的方法，所述判断所述目标文档中是否含有宏病毒，包括:

从所述目标文档包含的脚本中进行特征提取;

将提取到的特征与预置的宏病毒库中保存的特征进行比对，根据比对结果判断是否存在宏病毒。

6、如权利要求5所述的方法，还包括:

连接公有云服务器，以便对企业版服务端的宏病毒库进行升级更新。

7、一种宏病毒查杀系统，应用于企业版病毒查杀应用程序中，其中，所述企业版病毒查杀应用程序包括安装在企业用户管理控制中心计算设备上的

企业版服务端，以及安装在企业用户终端设备上的企业版客户端，通过企业版服务端实现对各个企业版客户端所在用户终端设备的统一管理，所述系统包括:

监控单元，位于企业版客户端，用于对打开特定类型文档的操作进行监控；所述特定类型文档包括办公软件文档；

上传单元，位于企业版客户端，用于当监控到打开目标文档的请求时，对所述请求进行拦截，并将所述目标文档上传到企业版服务端；

判断单元，位于企业版服务端，用于判断所述目标文档中是否含有宏病毒；

指令返回单元，位于企业版服务端，用于根据判断结果向所述企业版客户端返回处理指令。

8、如权利要求7所述的系统，所述指令返回单元包括:

第一指令返回子单元，用于如果判断结果为所述目标文档中不含有宏病毒，则向所述企业版客户端返回将所述请求放行的指令。

9、如权利要求7所述的系统，所述指令返回单元包括:

清除子单元，用于如果判断结果为所述目标文档中含有宏病毒，则将所述目标文档中的宏病毒清除，得到安全文档；

第二指令返回子单元，用于向所述企业版客户端返回所述安全文档，以及返回丢弃所述请求、用所述安全文档替换所述目标文档并打开所述安全文档的指令。

10、如权利要求7所述的系统，还包括:

显示单元，位于企业版客户端，用于所述对所述请求进行拦截之后，加载显示预置的界面，用以显示正在进行宏病毒检测。

11、如权利要求7至10任一项所述的系统，所述判断单元包括:

特征提取子单元，用于从所述目标文档包含的脚本中进行特征提取；

特征比对子单元，用于将提取到的特征与预置的宏病毒库中保存的特征进行比对，根据比对结果判断是否存在宏病毒。

12、如权利要求11所述的系统，还包括:

更新单元，位于企业版服务端，用于连接公有云服务器，以便对企业版服务端的宏病毒库进行升级更新。

13、一种计算机程序，包括计算机可读代码，当智能电子设备运行所述计算机可读代码运行时，导致权利要求1-6中的任一项权利要求所述的方法被执行。

14、一种计算机可读介质，其中存储了如权利要求13所述的计算机程序。

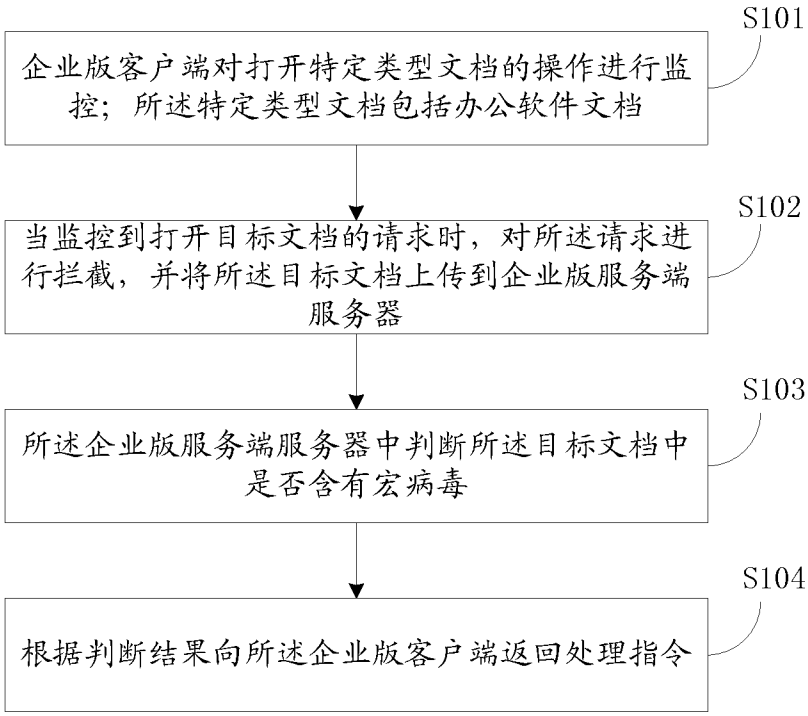
S101
企业版客户端对打开特定类型文档的操作进行监控；所述特定类型文档包括办公软件文档
S102
当监控到打开目标文档的请求时，对所述请求进行拦截，并将所述目标文档上传到企业版服务端服务器
S103
所述企业版服务端服务器中判断所述目标文档中是否含有宏病毒
S104
根据判断结果向所述企业版客户端返回处理指令

图 1

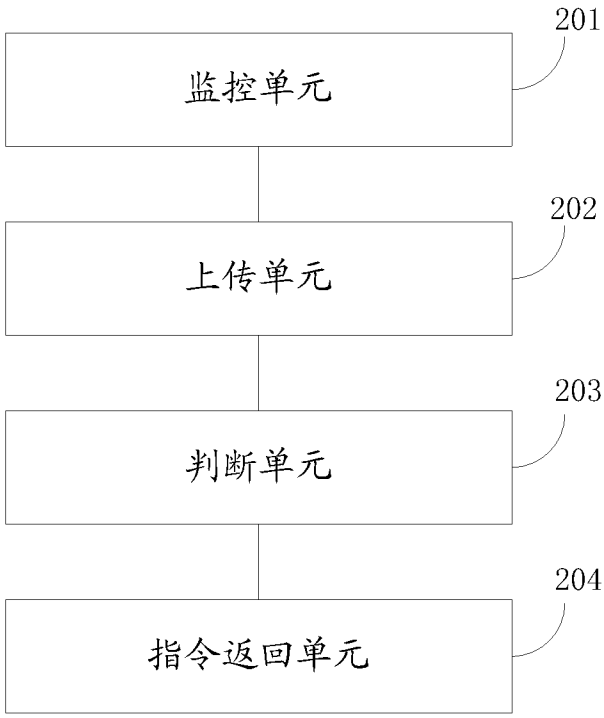
201
监控单元
202
上传单元
203
判断单元
204
指令返回单元

图 2

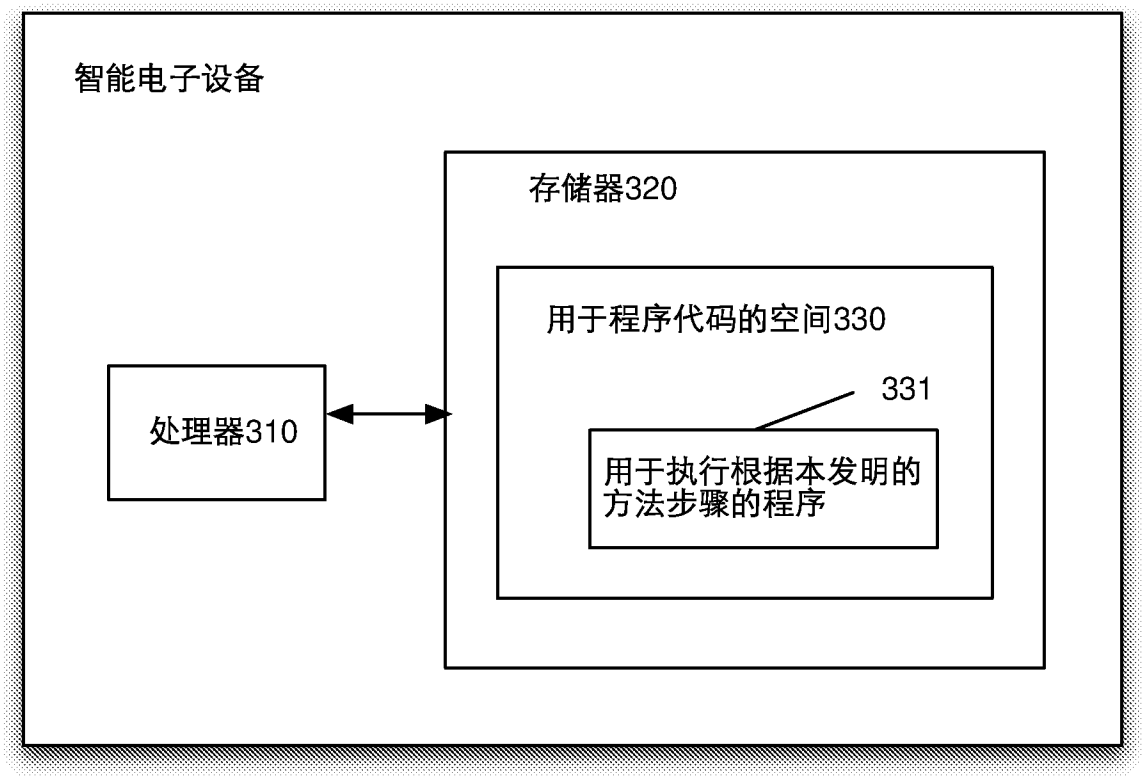
智能电子设备
存储器320
用于程序代码的空间330
331
处理器310
用于执行根据本发明的方法步骤的程序

图 3

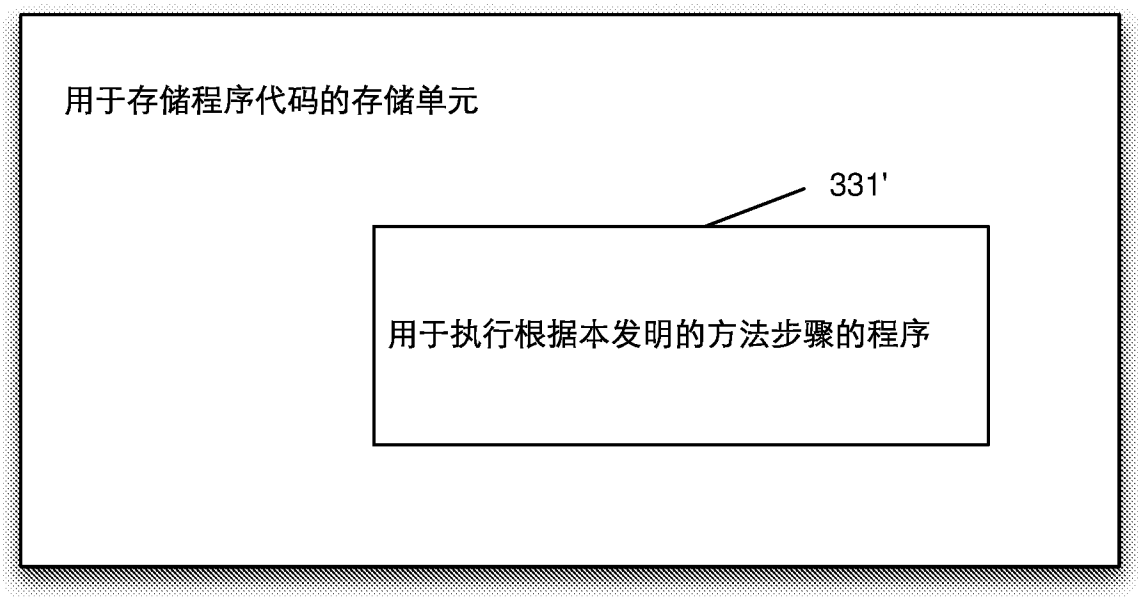
用于存储程序代码的存储单元
331'
用于执行根据本发明的方法步骤的程序

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/079169

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/56 (2013.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

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, EPODOC, WPI: malware, check, monitor, virus, search, client, server, upload, file, operation, watch

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 103294955 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 11 September 2013 (11.09.2013), description, paragraphs [0002]-[0126]	1-14
X	CN 101039177 A (ZHUHAI KINGSOFT SOFTWARE CO., LTD.), 19 September 2007 (19.09.2007), description, page 1, paragraph 2 to page 7, the last paragraph	1-14
X	CN 102664875 A (HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY), 12 September 2012 (12.09.2012), description, paragraphs [0002]-[0054]	1-14
X	CN 103001947 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 27 March 2013 (27.03.2013), description, paragraphs [0002]-[0086]	1-14
X	CN 102982281 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 20 March 2013 (20.03.2013), description, paragraphs [0002]-[0085]	1-14
X	CN 102346828 A (HAINAN YIYUAN HIGH-TECH CO., LTD. et al.), 08 February 2012 (08.02.2012), description, paragraphs [0002]-[0081]	1-14

☐ 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
07 August 2014 (07.08.2014)	**01 September 2014 (01.09.2014)**
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 **MIAO, Wei** Telephone No.: (86-10) **62414039**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2014/079169

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103294955 A	11 September 2013	None	
CN 101039177 A	19 September 2007	JP 2008276774 A	13 November 2008
CN 102664875 A	12 September 2012	None	
CN 103001947 A	27 March 2013	WO 2014071867 A1	15 May 2014
CN 102982281 A	20 March 2013	None	
CN 102346828 A	08 February 2012	None	

国际检索报告

国际申请号 PCT/CN2014/079169

A. 主题的分类

G06F 21/56 (2013.01) i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F

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,EPODOC,WPI:病毒，恶意软件，查杀，客户端，上传，文档，操作，监控，virus，search，client，server，upload，file，operation，watch

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 103294955 A (北京奇虎科技有限公司 等) 2013年 9月 11日 (2013-09-11) 说明书第[0002]-[0126]段	1-14
X	CN 101039177 A (珠海金山软件股份有限公司) 2007年 9月 19日 (2007-09-19) 说明书第1页第2段-第7页最后一段	1-14
X	CN 102664875 A (华中科技大学) 2012年 9月 12日 (2012-09-12) 说明书第[0002]-[0054]段	1-14
X	CN 103001947 A (北京奇虎科技有限公司 等) 2013年 3月 27日 (2013-03-27) 说明书第[0002]-[0086]段	1-14
X	CN 102982281 A (北京奇虎科技有限公司 等) 2013年 3月 20日 (2013-03-20) 说明书第[0002]-[0085]段	1-14
X	CN 102346828 A (海南意源高科技有限公司 等) 2012年 2月 08日 (2012-02-08) 说明书第[0002]-[0081]段	1-14

☐ 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
2014年 8月 07日	2014年 9月 01日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国	苗伟
传真号 (86-10)62019451	电话号码 (86-10)62414039

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2014/079169

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 103294955 A	2013年 9月 11日	无	
CN 101039177 A	2007年 9月 19日	JP 2008276774 A	2008年 11月 13日
CN 102664875 A	2012年 9月 12日	无	
CN 103001947 A	2013年 3月 27日	WO 2014071867 A1	2014年 5月 15日
CN 102982281 A	2013年 3月 20日	无	
CN 102346828 A	2012年 2月 08日	无	