(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 1 月 26 日 (26.01.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/012241 A1

(51) 国际专利分类号:
G06F 21/56 (2013.01)

(21) 国际申请号: PCT/CN2015/096561

(22) 国际申请日: 2015 年 12 月 7 日 (07.12.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510431210.0 2015 年 7 月 21 日 (21.07.2015) CN

(71) 申请人: 安一恒通（北京）科技有限公司 (IYUNTIAN CO., LTD.) [CN/CN]; 中国北京市海淀区东北旺西路 8 号 4 号楼软件广场 C 座 1-01、1-03、1-04 室, Beijing 100091 (CN)。

(72) 发明人: 邹荣新 (ZOU, Rongxin); 中国北京市海淀区东北旺西路 8 号 4 号楼软件广场 C 座 1-01、1-03、1-04 室, Beijing 100091 (CN)。

(74) 代理人: 北京鸿德海业知识产权代理事务所（普通合伙） (BEIJING WISPRO INTELLECTUAL PROPERTY LLP.); 中国北京市海淀区知春路 6 号锦秋国际大厦 A508, 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, 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, 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: FILE INSPECTION METHOD, DEVICE, APPARATUS AND NON-VOLATILE COMPUTER STORAGE MEDIUM

(54) 发明名称 : 文件的检测方法、装置、设备及非易失性计算机存储介质

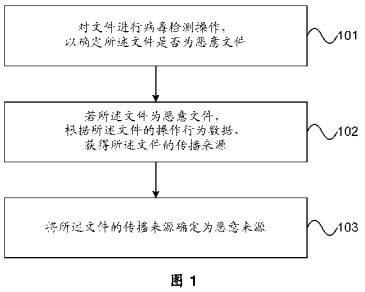

图 1

101 Perform virus inspection operation on a file to determine whether the file is a malicious file
102 If the file is a malicious file, acquire, according to operation action data of the file, a transmission source of the file
103 Determine the transmission source of the file as a malicious source

(57) Abstract: A file inspection method and device. The method comprises: performing virus inspection operation on a file to determine whether the file is a malicious file (101); if so, acquiring, according to operation action data of the file, a transmission source of the file (102); and thereby, determining the transmission source of the file as a malicious source (103). A transmission source of a malicious file is tracked and determined as a malicious source, and therefore, the determined malicious source can be utilized to perform virus inspection operation in advance before acquisition of a file. In this way, a malicious source can be detected in a timely manner to avoid security threats caused by acquisition of a malicious file, thereby improving system security performance.

(57) 摘要: 一种文件的检测方法及装置。通过对文件进行病毒检测操作，以确定所述文件是否为恶意文件(101)，若所述文件为恶意文件，根据所述文件的操作行为数据，获得所述文件的传播来源(102)，使得能够将所述文件的传播来源确定为恶意来源(103)，由于追踪到了恶意文件的传播来源，并将其确定为恶意来源，使得能够在获取一个文件之前，预先利用所确定的恶意来源，执行病毒检测操作，这样，能够及时检测到恶意来源，以避免获取到恶意文件对系统所造成的安全威胁，从而提高了系统的安全性能。

WO 2017/012241 A1

文件的检测方法、装置、设备及非易失性计算机存储介质

本申请要求了申请日为 2015 年 07 月 21 日，申请号为 201510431210.0 发明名称为“文件的检测方法及装置”的中国专利申请的优先权。

技术领域

本发明涉及计算机技术，尤其涉及一种文件的检测方法、装置、设备及非易失性计算机存储介质。

背景技术

病毒是编制或者在应用程序中插入的破坏系统功能的数据，其会影响应用程序的正常使用，并且还能够自我复制，通常以一组指令或者程序代码的形式呈现。病毒，又称为计算机病毒，可以包括但不限于木马、后门、局域网蠕虫、邮件蠕虫、间谍软件、感染型病毒或Rootkits/Bootkits，它们具有破坏性，复制性和传染性的特点。

然而，在一些情况下，例如，杀毒软件的监控能力有限，或者再例如，病毒种类繁多，且增长速度特别快等，因此，运行后的病毒所导致的恶意进程行为难以被及时检测到。

发明内容

本发明的多个方面提供一种文件的检测方法、装置、设备及非易失性计算机存储介质，用以提高系统的安全性能。

本发明的一方面，提供一种文件的检测方法，包括：

对文件进行病毒检测操作，以确定所述文件是否为恶意文件；

若所述文件为恶意文件，根据所述文件的操作行为数据，获得所述文件的传播来源；

将所述文件的传播来源确定为恶意来源。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述文件的传播来源包括：

文件的访问标识；或者

文件的来源文件。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述若所述文件为恶意文件，根据所述文件的操作行为数据，获得所述文件的传播来源之前，还包括：

记录所述文件的操作行为数据，并与所述文件进行关联，以获得所述文件与所述文件的操作行为数据的关联关系，以供根据所述关联关系，获得所述文件的操作行为数据。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述对文件进行病毒检测操作，以确定所述文件是否为恶意文件，包括：

获得所述文件的特征数据；

根据所述文件的特征数据，对所述文件进行检测，以确定所述文件

是否为恶意文件。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述对文件进行病毒检测操作，以确定所述文件是否为恶意文件，包括：

监控所述文件的文件进程的进程行为，以获得目标进程行为的行为信息；

根据所述目标进程行为的行为信息，对所述目标进程行为进行检测，以确定所述目标进程行为是否为恶意进程行为；

根据所述目标进程行为是否为恶意进程行为，确定所述文件是否为恶意文件。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述目标进程行为的行为信息包括下列信息中的至少一项：

目标进程行为的发起者信息；

目标进程行为的目标对象信息；

目标进程行为的附加信息；以及

目标进程行为的标识信息。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述文件包括可执行文件。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述将所述文件的传播来源确定为恶意来源之后，还包括：

利用所述恶意来源，执行病毒检测操作。

本发明的另一方面，提供一种文件的检测装置，包括：

检测单元，用于对文件进行病毒检测操作，以确定所述文件是否为恶意文件；

追踪单元，用于若所述文件为恶意文件，根据所述文件的操作行为数据，获得所述文件的传播来源；

确定单元，用于将所述文件的传播来源确定为恶意来源。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述文件的传播来源包括：

文件的访问标识；或者

文件的来源文件。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述追踪单元，还用于

记录所述文件的操作行为数据，并与所述文件进行关联，以获得所述文件与所述文件的操作行为数据的关联关系，以供根据所述关联关系，获得所述文件的操作行为数据。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述检测单元，具体用于

获得所述文件的特征数据；以及

根据所述文件的特征数据，对所述文件进行检测，以确定所述文件是否为恶意文件。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述检测单元，具体用于

监控所述文件的文件进程的进程行为，以获得目标进程行为的行为信息；

根据所述目标进程行为的行为信息，对所述目标进程行为进行检测，以确定所述目标进程行为是否为恶意进程行为；以及

根据所述目标进程行为是否为恶意进程行为，确定所述文件是否为恶意文件。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述目标进程行为的行为信息包括下列信息中的至少一项：

目标进程行为的发起者信息；

目标进程行为的目标对象信息；

目标进程行为的附加信息；以及

目标进程行为的标识信息。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，所述文件包括可执行文件。

如上所述的方面和任一可能的实现方式，进一步提供一种实现方式，

所述检测单元，还用于

利用所述恶意来源，执行病毒检测操作。

本发明的另一方面，提供一种设备，包括：

一个或者多个处理器；

存储器；

一个或者多个程序，所述一个或者多个程序存储在所述存储器中，当被所述一个或者多个处理器执行时：

对文件进行病毒检测操作，以确定所述文件是否为恶意文件；

若所述文件为恶意文件，根据所述文件的操作行为数据，获得所述文件的传播来源；

将所述文件的传播来源确定为恶意来源。

本发明的另一方面，提供一种非易失性计算机存储介质，所述非易失性计算机存储介质存储有一个或者多个程序，当所述一个或者多个程序被一个设备执行时，使得所述设备：

对文件进行病毒检测操作，以确定所述文件是否为恶意文件；

若所述文件为恶意文件，根据所述文件的操作行为数据，获得所述文件的传播来源；

将所述文件的传播来源确定为恶意来源。

由上述技术方案可知，本发明实施例通过对文件进行病毒检测操作，以确定所述文件是否为恶意文件，若所述文件为恶意文件，根据所述文

件的操作行为数据，获得所述文件的传播来源，使得能够将所述文件的传播来源确定为恶意来源，由于追踪到了恶意文件的传播来源，并将其确定为恶意来源，使得能够在获取一个文件之前，预先利用所确定的恶意来源，执行病毒检测操作，这样，能够及时检测到恶意来源，以避免获取到恶意文件对系统所造成的安全威胁，从而提高了系统的安全性能。

另外，采用本发明所提供的技术方案，通过监控文件的文件进程的进程行为，以获得目标进程行为的行为信息，进而根据所述目标进程行为的行为信息，对所述目标进程行为进行检测，以确定所述目标进程行为是否为恶意进程行为，使得能够根据所述目标进程行为是否为恶意进程行为，确定所述文件是否为恶意文件，由于不再依赖于对目标进程行为进行单个样本的指定特征分析，而是根据所述目标进程行为的行为信息，对所述目标进程行为进行综合检测，能够及时检测到恶意进程行为，从而提高了系统的安全性能。

附图说明

了更清楚地说明本发明实施例中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 为本发明一实施例提供的文件的检测方法的流程示意图；

图 2 为本发明另一实施例提供的文件的检测装置的结构示意图。

具体实施方式

为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

需要说明的是，本发明实施例中所涉及的终端可以包括但不限于手机、个人数字助理（Personal Digital Assistant，PDA）、无线手持设备、平板电脑（Tablet Computer）、个人电脑（Personal Computer，PC）、MP3 播放器、MP4 播放器、可穿戴设备（例如，智能眼镜、智能手表、智能手环等）等。

另外，本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

图 1 为本发明一实施例提供的文件的检测方法的流程示意图，如图 1 所示。

101、对文件进行病毒检测操作，以确定所述文件是否为恶意文件。

102、若所述文件为恶意文件，根据所述文件的操作行为数据，获得所述文件的传播来源。

103、将所述文件的传播来源确定为恶意来源。

其中，病毒，又称为计算机病毒，可以包括但不限于木马、后门、局域网蠕虫、邮件蠕虫、间谍软件、感染型病毒或 Rootkits/Bootkits。

需要说明的是，101~103 的执行主体的部分或全部可以为位于本地终端的应用，或者还可以为设置在位于本地终端的应用中的插件或软件开发工具包（Software Development Kit，SDK）等功能单元，或者还可以为位于网络侧服务器中的处理引擎，或者还可以为位于网络侧的分布式系统，本实施例对此不进行特别限定。

可以理解的是，所述应用可以是安装在终端上的本地程序（nativeApp），或者还可以是终端上的浏览器的一个网页程序（webApp），本实施例对此不进行特别限定。

这样，通过对文件进行病毒检测操作，以确定所述文件是否为恶意文件，若所述文件为恶意文件，根据所述文件的操作行为数据，获得所述文件的传播来源，使得能够将所述文件的传播来源确定为恶意来源，由于追踪到了恶意文件的传播来源，并将其确定为恶意来源，使得能够在获取一个文件之前，预先利用所确定的恶意来源，执行病毒检测操作，这样，能够及时检测到恶意来源，以避免获取到恶意文件对系统所造成的安全威胁，从而提高了系统的安全性能。

可选地，在本实施例的一个可能的实现方式中，在 101 中，所进行的病毒检测操作的对象，可以是可执行文件，或者还可以是其他类型文件的非可执行文件，本实施例对此不进行特别限定。

具体地，可执行文件，是可移植可执行（PE）文件格式的文件，它可以加载到内存中，并由操作系统加载程序执行。可执行文件的扩展名可以包括但不限于.dll、.exe、.ocx、.bat、.js、.zip、.rar、.7z、.msi、.tar、.sys 和.scr，等。

在一个具体的实现过程中，具体可以预先将所进行的病毒检测操作

的对象信息进行配置，以生成配置文件。这样，可以根据该配置文件中所包含的对象信息，确定进行的病毒检测操作的对象。由于采用了配置文件的方式配置进行的病毒检测操作的对象信息，能够有效提高信息配置的灵活性和可靠性。

在执行本发明所提供的技术方案的过程中，还可以进一步修改所生成的配置文件，以更新对象信息。

可选地，在本实施例的一个可能的实现方式中，所述文件的传播来源可以包括但不限于如下内容:

文件的访问标识；或者

文件的来源文件。

所述文件的访问标识，是指用于获取文件的标识信息，可以包括但不限于所述文件的下载地址、所述文件所属页面的统一资源定位符（Uniform Resource Locator，URL）或统一资源名称（Uniform Resource Name，URN），或者还可以包括其他能够访问所述文件的其他标识信息，本实施例对此不进行特别限定。

可以理解的是，本发明所涉及的页面，也可以称为 Web 页面，可以是基于超文本标记语言（HyperText Markup Language，HTML）编写的网页（Web Page），即 HTML 页面，或者还可以是基于 HTML 和 Java 语言编写的网页，即 Java 服务器页面（Java Server Page，JSP），或者还可以为其他语言编写的网页，本实施例对此不进行特别限定。Web 页面可以包括由一个或者多个页面标签例如，超文本标记语言（HyperText Markup Language，HTML）标签、JSP 标签等，定义的一个显示区块，称为页面元素，例如，文字、图片、超链接、按钮、输

入框、下拉框等。

所述文件的来源文件，是指用于产生文件的其他文件，例如，安装文件或压缩文件等。

可选地，在本实施例的一个可能的实现方式中，在 102 之前，还可以进一步记录所述文件的操作行为数据，并与所述文件进行关联，以获得所述文件与所述文件的操作行为数据的关联关系，以供根据所述关联关系，获得所述文件的操作行为数据。

其中，所述文件的操作行为数据可以包括但不限于如下数据中的至少一种：

域名系统（Domain Name System，DNS）访问行为数据；

进程创建行为操作；

下载行为数据；

传输行为数据；

运行行为数据；

安装行为数据；以及

解压缩行为数据。

在获得所述文件与所述文件的操作行为数据的关联关系之后，还可以进一步对所述关联关系进行存储处理。具体地，具体可以将所述关联关系存储在终端的存储设备中。

在一个具体的实现过程中，所述终端的存储设备可以为慢速存储设备，具体可以为计算机系统的硬盘，或者还可以为手机的非运行内存即物理内存，例如，只读存储器（Read-Only Memory，ROM）和内存卡等，本实施例对此不进行特别限定。

在另一个具体的实现过程中，所述终端的存储设备还可以为快速存储设备，具体可以为计算机系统的内存，或者还可以为手机的运行内存即系统内存，例如，随机存储器（Random Access Memory，RAM）等，本实施例对此不进行特别限定。

可选地，在本实施例的一个可能的实现方式中，在 101 中，具体可以获得所述文件的特征数据，进而根据所述文件的特征数据，对所述文件进行检测，以确定所述文件是否为恶意文件。

具体地，可以对文件进行基于特征匹配的数值运算，进而，根据数值运算的运算结果，检测文件是否为病毒文件。这个方法同样适用于各种类型文件的检测，只要根据检测需求，合理挖掘匹配的特征即可。

然而，由于数值运算较为复杂，因此，可能需要较多的处理资源，这样，会占用终端的大量处理资源，从而导致终端的处理性能降低。

可选地，在本实施例的一个可能的实现方式中，在 101 中，具体可以监控所述文件的文件进程的进程行为，以获得目标进程行为的行为信息，进而，根据所述目标进程行为的行为信息，对所述目标进程行为进行检测，以确定所述目标进程行为是否为恶意进程行为，根据所述目标进程行为是否为恶意进程行为，确定所述文件是否为恶意文件。由于不再依赖于对目标进程行为进行单个样本的指定特征分析，而是根据所述目标进程行为的行为信息，对所述目标进程行为进行综合检测，能够及时检测到恶意进程行为，从而提高了系统的安全性能。

其中，所述进程行为可以包括但不限于下列操作中的至少一项：

文件操作行为；

进程操作行为；以及

注册表操作行为。

在一个具体的实现过程中，监控所述文件的文件进程的进程行为，这一操作的依据，可以为一预先配置的可疑行为决策库。该可疑行为决策库中存储有已经确定的可疑进程行为的相关信息，例如，可疑目标进程行为的标识信息，可疑目标进程行为的发起者信息等，确定所监控的进程的进程行为是否为可疑进程行为即目标进程行为，进而获得该目标进程行为的行为信息。

可以理解的是，由于监控的目的，只是确定目标进程行为，并不是确定恶意进程行为，因此，所述可疑行为决策库的配置策略，可以适当地将监控范围控制得大一些，能够有效避免漏报的情况发生。

在另一个具体的实现过程中，所获得的所述目标进程行为的行为信息可以包括但不限于下列信息中的至少一项：

目标进程行为的发起者信息；

目标进程行为的目标对象信息；

目标进程行为的附加信息；以及

目标进程行为的标识信息。

其中，

所述目标进程行为的发起者信息，可以为发起进程行为的对象标识，例如，文件标识等。

所述目标进程行为的目标对象信息，可以为进程行为将要施加的对象标识，例如，其他文件的文件标识。

所述目标进程行为的附加信息，可以为进程行为所产生的数据信息，例如，。

所述目标进程行为的标识信息，可以为进程行为的标识（Identifier，ID）。

在另一个具体的实现过程中，具体可以监控系统中全部进程的进程行为，以获得目标进程行为的行为信息。

在另一个具体的实现过程中，具体可以根据预先配置的可疑目标进程行为的标识信息，监控系统中部分进程的进程行为，以获得目标进程行为的行为信息。

这样，在获得所述目标进程行为的检测结果即恶意进程行为或非恶意进程行为之后，则可以根据该检测结果，生成操作指示信息，以使得根据所述操作指示信息，对所述目标进程行为执行操作。

其中，所述操作指示信息可以包括但不限于：

用以指示所述目标进程行为为恶意进程行为的指示信息和用以指示对所述目标进程行为进行拦截操作的提示信息；或者

用以指示所述目标进程行为为非恶意进程行为的指示信息和用以指示对所述目标进程行为进行放行操作的提示信息。

在另一个具体的实现过程中，获得目标进程行为的行为信息之后，具体可以根据所述目标进程行为的行为信息，利用预先配置的恶意行为决策库，该恶意行为决策库中存储有已经确定的恶意进程行为的行为信息进行匹配，对所述目标进程行为进行检测，以确定所述目标进程行为是否为恶意进程行为。

若匹配到与所述目标进程行为的行为信息一致的恶意进程行为，说明该目标进程行为为恶意进程行为，则可以确定所述目标进程行为为恶意进程行为。

若没有匹配到与所述目标进程行为的行为信息一致的恶意进程行为，说明该目标进程行为为未知的进程行为，则可以进一步利用已经确定的至少一个的恶意进程行为或者其他检测装置发送的其他目标进程行为，对该未知的目标进程行为进行检测。

具体地，具体可以根据所述目标进程行为的行为信息和已经确定的至少一个的恶意进程行为的行为信息，对所述目标进程行为进行检测，以确定所述目标进程行为是否为恶意进程行为。

例如，具体可以对已经确定的至少一个的恶意进程行为的行为信息进行聚类分析，以获得相似的行为信息，用以确定未知的目标进程行为是否为恶意进程行为。如，根据目标进程行为的目标对象信息、目标进程行为的附加信息和目标进程行为的标识信息，对所述至少一个的恶意进程行为的行为信息进行聚类，获得相似的目标进程行为的发起者信息。

具体地，具体可以根据所述目标进程行为的行为信息和其他检测装置发送的其他目标进程行为的行为信息，对所述目标进程行为进行检测，以确定所述目标进程行为是否为恶意进程行为。

例如，具体可以对所述目标进程行为的行为信息和其他检测装置发送的其他目标进程行为的行为信息进行聚类分析，以获得聚类结果。进而，再进一步分析所述目标进程行为的行为信息所属的聚类结果，以确定未知的目标进程行为是否为恶意进程行为。

这样，由于能够利用已经确定的至少一个的恶意进程行为或者其他检测装置发送的其他目标进程行为，对未知的目标进程行为进行检测，以确定该未知的目标进程行为是否为恶意进程行为，使得能够及时检测到恶意进程行为，能够有效提高检测的可靠性和灵活性，从而进一步提

高了系统的安全性。

可以理解的是，若所确定的未知的目标进程行为为恶意进程行为，还可以进一步将所确定的该目标进程行为的行为信息添加到恶意行为决策库中，以提高恶意行为决策库的决策能力。

可以理解的是，恶意行为决策库中，还可以进一步存储针对每个恶意进程行为的防御查杀方案。那么，在生成操作指示信息的同时，还可以进一步获取防御查杀方案，以便能够根据该防御查杀方案，进行有效的杀毒处理。

可选地，在本实施例的一个可能的实现方式中，在 103 之后，还可以进一步利用所述恶意来源，执行病毒检测操作。如果检测到恶意来源的存在，就可以尽早阻止恶意文件的传播。

在一个具体的实现过程中，在确定恶意来源之后，还可以进一步将所确定的恶意来源的特征数据，进行存储处理，以作为后续执行病毒检测操作的检测依据。

例如，对待检测的对象进行基于特征匹配的数值运算或逻辑运算等运算，进而，根据运算结果，检测对象是否为病毒。其中，基于特征匹配的数值运算较为复杂，因此，可能需要较多的处理资源，这样，会占用终端的大量处理资源，导致终端的处理性能降低。而基于特征匹配的逻辑运算，相比数值运算简单很多，不需要较多的处理资源，因此，不会占用终端的大量处理资源，从而提高了终端的处理性能。

本实施例中，通过对文件进行病毒检测操作，以确定所述文件是否为恶意文件，若所述文件为恶意文件，根据所述文件的操作行为数据，获得所述文件的传播来源，使得能够将所述文件的传播来源确定为恶意

来源，由于追踪到了恶意文件的传播来源，并将其确定为恶意来源，使得能够在获取一个文件之前，预先利用所确定的恶意来源，执行病毒检测操作，这样，能够及时检测到恶意来源，以避免获取到恶意文件对系统所造成的安全威胁，从而提高了系统的安全性能。

另外，采用本发明所提供的技术方案，通过监控文件的文件进程的进程行为，以获得目标进程行为的行为信息，进而根据所述目标进程行为的行为信息，对所述目标进程行为进行检测，以确定所述目标进程行为是否为恶意进程行为，使得能够根据所述目标进程行为是否为恶意进程行为，确定所述文件是否为恶意文件，由于不再依赖于对目标进程行为进行单个样本的指定特征分析，而是根据所述目标进程行为的行为信息，对所述目标进程行为进行综合检测，能够及时检测到恶意进程行为，从而提高了系统的安全性能。

需要说明的是，对于前述的各方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，因为依据本发明，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是本发明所必须的。

在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

图 2 为本发明另一实施例提供的文件的检测装置的结构示意图，如图 2 所示。本实施例的文件的检测装置可以包括检测单元 21、追踪单元 22 和确定单元 23。其中，检测单元 21，用于对文件进行病毒检测操作，

以确定所述文件是否为恶意文件；追踪单元 22，用于若所述文件为恶意文件，根据所述文件的操作行为数据，获得所述文件的传播来源；确定单元 23，用于将所述文件的传播来源确定为恶意来源。

需要说明的是，本实施例所提供的文件的检测装置的部分或全部可以为位于本地终端的应用，或者还可以为设置在位于本地终端的应用中的插件或软件开发工具包（Software Development Kit，SDK）等功能单元，或者还可以为位于网络侧服务器中的处理引擎，或者还可以为位于网络侧的分布式系统，本实施例对此不进行特别限定。

可以理解的是，所述应用可以是安装在终端上的本地程序（nativeApp），或者还可以是终端上的浏览器的一个网页程序（webApp），本实施例对此不进行特别限定。

可选地，在本实施例的一个可能的实现方式中，所述检测单元 21 所进行的病毒检测操作的对象，可以是可执行文件，或者还可以是其他类型文件的非可执行文件，本实施例对此不进行特别限定。

具体地，可执行文件，是可移植可执行（PE）文件格式的文件，它可以加载到内存中，并由操作系统加载程序执行。可执行文件的扩展名可以包括但不限于.dll、.exe、.ocx、.bat、.js、.zip、.rar、.7z、.msi、.tar、.sys 和.scr，等。

可选地，在本实施例的一个可能的实现方式中，所述文件的传播来源可以包括但不限于如下内容：

文件的访问标识；或者

文件的来源文件。

可选地，在本实施例的一个可能的实现方式中，所述追踪单元 22，

还可以进一步用于记录所述文件的操作行为数据，并与所述文件进行关联，以获得所述文件与所述文件的操作行为数据的关联关系，以供根据所述关联关系，获得所述文件的操作行为数据。

可选地，在本实施例的一个可能的实现方式中，所述检测单元 21，具体可以用于获得所述文件的特征数据；以及根据所述文件的特征数据，对所述文件进行检测，以确定所述文件是否为恶意文件。

可选地，在本实施例的一个可能的实现方式中，所述检测单元 21，具体可以用于监控所述文件的文件进程的进程行为，以获得目标进程行为的行为信息；根据所述目标进程行为的行为信息，对所述目标进程行为进行检测，以确定所述目标进程行为是否为恶意进程行为；以及根据所述目标进程行为是否为恶意进程行为，确定所述文件是否为恶意文件。

在一个具体的实现过程中，所获得的所述目标进程行为的行为信息可以包括但不限于下列信息中的至少一项：

目标进程行为的发起者信息；

目标进程行为的目标对象信息；

目标进程行为的附加信息；以及

目标进程行为的标识信息。

可选地，在本实施例的一个可能的实现方式中，所述检测单元 21，还可以进一步用于利用所述恶意来源，执行病毒检测操作。

需要说明的是，图 1 对应的实施例中方法，可以由本实施例提供的文件的检测装置实现。详细描述可以参见图 1 对应的实施例中的相关内容，此处不再赘述。

本实施例中，通过检测单元对文件进行病毒检测操作，以确定所述

文件是否为恶意文件，追踪单元若所述文件为恶意文件，根据所述文件的操作行为数据，获得所述文件的传播来源，使得确定单元能够将所述文件的传播来源确定为恶意来源，由于追踪到了恶意文件的传播来源，并将其确定为恶意来源，使得能够在获取一个文件之前，预先利用所确定的恶意来源，执行病毒检测操作，这样，能够及时检测到恶意来源，以避免获取到恶意文件对系统所造成的安全威胁，从而提高了系统的安全性能。

另外，采用本发明所提供的技术方案，通过监控文件的文件进程的进程行为，以获得目标进程行为的行为信息，进而根据所述目标进程行为的行为信息，对所述目标进程行为进行检测，以确定所述目标进程行为是否为恶意进程行为，使得能够根据所述目标进程行为是否为恶意进程行为，确定所述文件是否为恶意文件，由于不再依赖于对目标进程行为进行单个样本的指定特征分析，而是根据所述目标进程行为的行为信息，对所述目标进程行为进行综合检测，能够及时检测到恶意进程行为，从而提高了系统的安全性能。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统，设备和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本发明所提供的几个实施例中，应该理解到，所揭露的系统，设备和方法，可以通过其它的方式实现。例如，以上所描述的设备实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所

显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，设备或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

上述以软件功能单元的形式实现的集成的单元，可以存储在一个计算机可读取存储介质中。上述软件功能单元存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）或处理器（processor）执行本发明各个实施例所述方法的部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（Read-Only Memory，ROM）、随机存取存储器（Random Access Memory，RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和

范围。

权 利 要 求 书

1、一种文件的检测方法，其特征在于，包括:

对文件进行病毒检测操作，以确定所述文件是否为恶意文件;

若所述文件为恶意文件，根据所述文件的操作行为数据，获得所述文件的传播来源;

将所述文件的传播来源确定为恶意来源。

2、根据权利要求 1 所述的方法，其特征在于，所述文件的传播来源包括:

文件的访问标识; 或者

文件的来源文件。

3、根据权利要求 1 或 2 所述的方法，其特征在于，所述若所述文件为恶意文件，根据所述文件的操作行为数据，获得所述文件的传播来源之前，还包括:

记录所述文件的操作行为数据，并与所述文件进行关联，以获得所述文件与所述文件的操作行为数据的关联关系，以供根据所述关联关系，获得所述文件的操作行为数据。

4、根据权利要求 1~3 任一权利要求所述的方法，其特征在于，所述对文件进行病毒检测操作，以确定所述文件是否为恶意文件，包括:

获得所述文件的特征数据;

根据所述文件的特征数据，对所述文件进行检测，以确定所述文件是否为恶意文件。

5、根据权利要求 1~4 任一权利要求所述的方法，其特征在于，所述对文件进行病毒检测操作，以确定所述文件是否为恶意文件，包括:

监控所述文件的文件进程的进程行为，以获得目标进程行为的行为信息；

根据所述目标进程行为的行为信息，对所述目标进程行为进行检测，以确定所述目标进程行为是否为恶意进程行为；

根据所述目标进程行为是否为恶意进程行为，确定所述文件是否为恶意文件。

6、根据权利要求 5 所述的方法，其特征在于，所述目标进程行为的行为信息包括下列信息中的至少一项：

目标进程行为的发起者信息；

目标进程行为的目标对象信息；

目标进程行为的附加信息；以及

目标进程行为的标识信息。

7、根据权利要求 1~6 任一权利要求所述的方法，其特征在于，所述文件包括可执行文件。

8、根据权利要求 1~7 任一权利要求所述的方法，其特征在于，所述将所述文件的传播来源确定为恶意来源之后，还包括：

利用所述恶意来源，执行病毒检测操作。

9、一种文件的检测装置，其特征在于，包括：

检测单元，用于对文件进行病毒检测操作，以确定所述文件是否为恶意文件；

追踪单元，用于若所述文件为恶意文件，根据所述文件的操作行为数据，获得所述文件的传播来源；

确定单元，用于将所述文件的传播来源确定为恶意来源。

10、根据权利要求 9 所述的装置，其特征在于，所述文件的传播来源包括:

文件的访问标识；或者

文件的来源文件。

11、根据权利要求 9 或 10 所述的装置，其特征在于，所述追踪单元，还用于

记录所述文件的操作行为数据，并与所述文件进行关联，以获得所述文件与所述文件的操作行为数据的关联关系，以供根据所述关联关系，获得所述文件的操作行为数据。

12、根据权利要求 9~11 任一权利要求所述的装置，其特征在于，所述检测单元，具体用于

获得所述文件的特征数据；以及

根据所述文件的特征数据，对所述文件进行检测，以确定所述文件是否为恶意文件。

13、根据权利要求 9~12 任一权利要求所述的装置，其特征在于，所述检测单元，具体用于

监控所述文件的文件进程的进程行为，以获得目标进程行为的行为信息；

根据所述目标进程行为的行为信息，对所述目标进程行为进行检测，以确定所述目标进程行为是否为恶意进程行为；以及

根据所述目标进程行为是否为恶意进程行为，确定所述文件是否为恶意文件。

14、根据权利要求 13 所述的装置，其特征在于，所述目标进程行

为的行为信息包括下列信息中的至少一项：

目标进程行为的发起者信息；

目标进程行为的目标对象信息；

目标进程行为的附加信息；以及

目标进程行为的标识信息。

15、根据权利要求 9~14 任一权利要求所述的装置，其特征在于，所述文件包括可执行文件。

16、根据权利要求 9~15 任一权利要求所述的装置，其特征在于，所述检测单元，还用于

利用所述恶意来源，执行病毒检测操作。

17、一种设备，包括：

一个或者多个处理器；

存储器；

一个或者多个程序，所述一个或者多个程序存储在所述存储器中，当被所述一个或者多个处理器执行时：

对文件进行病毒检测操作，以确定所述文件是否为恶意文件；

若所述文件为恶意文件，根据所述文件的操作行为数据，获得所述文件的传播来源；

将所述文件的传播来源确定为恶意来源。

18、一种非易失性计算机存储介质，所述非易失性计算机存储介质存储有一个或者多个程序，当所述一个或者多个程序被一个设备执行时，使得所述设备：

对文件进行病毒检测操作，以确定所述文件是否为恶意文件；

若所述文件为恶意文件，根据所述文件的操作行为数据，获得所述文件的传播来源；

将所述文件的传播来源确定为恶意来源。

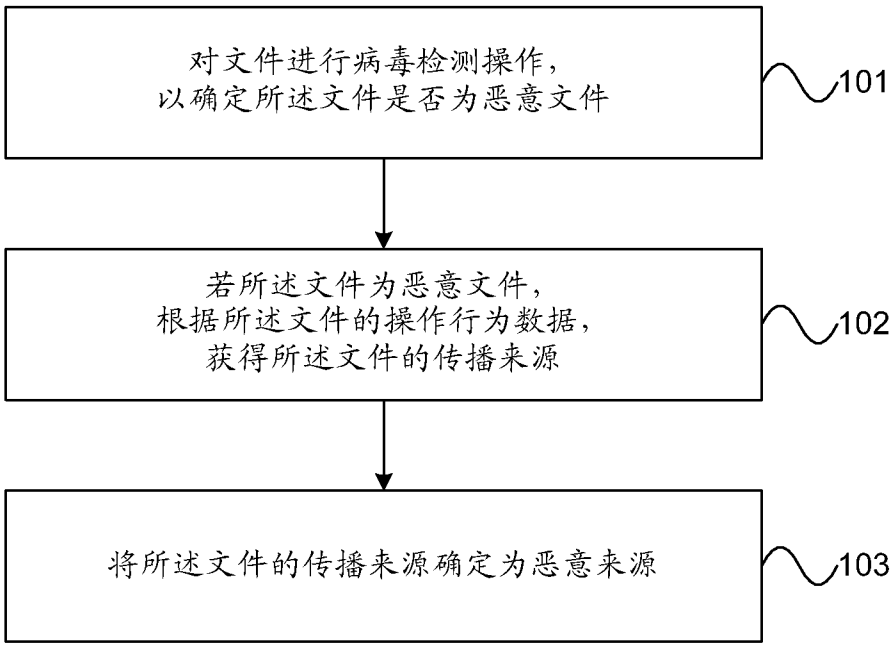
对文件进行病毒检测操作，
以确定所述文件是否为恶意文件
101
若所述文件为恶意文件，
根据所述文件的操作行为数据，
获得所述文件的传播来源
102
将所述文件的传播来源确定为恶意来源
103

图 1

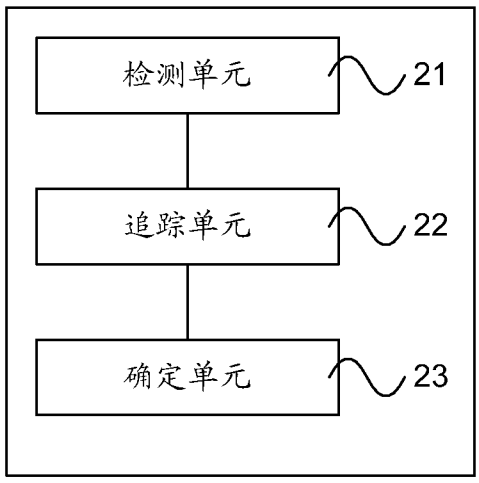
检测单元
21
追踪单元
22
确定单元
23

图 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/096561

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)

WPI, EPODOC, CNPAT, CNKI: malicious, behaviour, file, detect+, source, monitor+, virus, progress, action

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 105095759 A (ANYIHENGTONG (BEIJING) TECHNOLOGY CO., LTD.), 25 November 2015 (25.11.2015), claims 1-16, and description, paragraphs [0128]-[0158]	1-18
X	CN 103955645 A (BAIDU ONLINE NETWORK TECHNOLOGY (BEIJING) CO., LTD.), 30 July 2014 (30.07.2014), description, paragraphs [0055]-[0095]	1-18
X	CN 103559446 A (XIAMEN MEIYA PICO INFORMATION CO., LTD.), 05 February 2014 (05.02.2014), description, paragraphs [0032]-[0045]	1-18
A	US 8990944 B1 (FIREEYE, INC.), 24 March 2015 (24.03.2015), the whole document	1-18

☐ 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
21 March 2016 (21.03.2016)	**21 April 2016 (21.04.2016)**
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 **TIAN, Jing** Telephone No.: (86-10) **62413701**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/096561

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 105095759 A	25 November 2015	None	
CN 103955645 A	30 July 2014	US 2015310211 A1	29 October 2015
		EP 2940957 A1	04 November 2015
		KR 20150124370 A	05 November 2015
CN 103559446 A	05 February 2014	None	
US 8990944 B1	24 March 2015	None	

国际检索报告

国际申请号
PCT/CN2015/096561

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））

WPI, EPODOC, CNPAT, CNKI: 病毒, 检测, 监测, 恶意, 来源, 行为, 进程, file, detect+, source, monitor+, virus, progress, action

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 105095759 A (安一恒通北京科技有限公司) 2015年 11月 25日 (2015-11-25) 权利要求第1-16项, 说明书第[0128]-[0158]段	1-18
X	CN 103955645 A (百度在线网络技术北京有限公司) 2014年 7月 30日 (2014-07-30) 说明书第[0055]-[0095]段	1-18
X	CN 103559446 A (厦门市美亚柏科信息股份有限公司) 2014年 2月 5日 (2014-02-05) 说明书第[0032]-[0045]段	1-18
A	US 8990944 B1 (FIREEYE, INC.) 2015年 3月 24日 (2015-03-24) 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	国际检索报告邮寄日期
2016年 3月 21日	2016年 4月 21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	田晶
传真号 (86-10)62019451	电话号码 (86-10)62413701

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/096561

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	105095759	A	2015年 11月 25日	无			
CN	103955645	A	2014年 7月 30日	US	2015310211	A1	2015年 10月 29日
				EP	2940957	A1	2015年 11月 4日
				KR	20150124370	A	2015年 11月 5日
CN	103559446	A	2014年 2月 5日	无			
US	8990944	B1	2015年 3月 24日	无			