(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106295339 A
(43)申请公布日 2017.01.04

(21)申请号 201610605194.7

(22)申请日 2016.07.28

(71)申请人 韦春
地址 545600 广西壮族自治区柳州市鹿寨县鹿寨镇鹿化第三生活区三段8栋4单元2楼2室

(72)发明人 韦春

(74)专利代理机构 广州三环专利代理有限公司 44202
代理人 温旭 贾允

(51)Int.Cl.
G06F 21/56(2013.01)

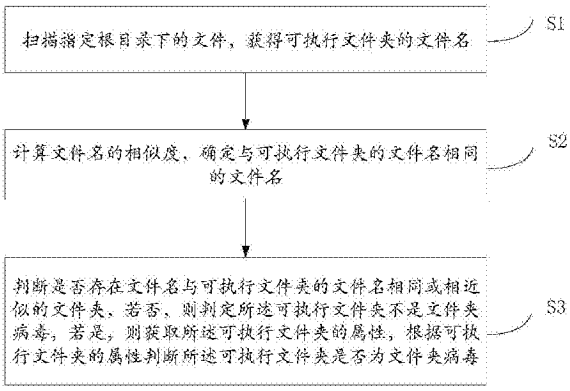
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种识别文件夹病毒的方法

(57)摘要

本发明涉及计算机技术，特别是一种识别文件夹病毒的方法，所述方法包括：扫描指定根目录下的文件，获得可执行文件夹的文件名；计算文件名的相似度，确定与可执行文件夹的文件名相同的文件名；判断是否存在文件名与可执行文件夹的文件名相同的文件夹，若否，则判定所述可执行文件夹不是文件夹病毒，若是，则获取所述可执行文件夹的属性，根据可执行文件夹的属性判断所述可执行文件夹是否为文件夹病毒。本发明可以提高识别文件夹病毒的效率和可靠性。



CN 106295339 A

1.一种识别文件夹病毒的方法，其特征在于，包括：

扫描指定根目录下的文件，获得可执行文件夹的文件名；

计算文件名的相似度，确定与可执行文件夹的文件名相同的文件名；

判断是否存在文件名与可执行文件夹的文件名相同的文件夹，若否，则判定所述可执行文件夹不是文件夹病毒，若是，则获取所述可执行文件夹的属性，根据可执行文件夹的属性判断所述可执行文件夹是否为文件夹病毒。

2.根据权利要求1所述的方法，其特征在于，所述获取所述可执行文件夹的属性，根据可执行文件夹的属性判断所述可执行文件夹是否为文件夹病毒，包括：

对文件夹执行取属性操作；

判断返回值是否包含FILE_ATTRIBUTE_DIRECTORY位，如果返回值不包含FILE_ATTRIBUTE_DIRECTORY位，则判定所述可执行文件不是文件夹病毒，如果返回值包含FILE_ATTRIBUTE_DIRECTORY位，则进一步判断返回值是否包含FILE_ATTRIBUTE_HIDDEN位和FILE_ATTRIBUTE_SYSTEM位中任一个，如果返回值不包含FILE_ATTRIBUTE_HIDDEN位和

FILE_ATTRIBUTE_SYSTEM位种任一个，则判定所述可执行文件不是文件夹病毒，如果返回值包含FILE_ATTRIBUTE_HIDDEN位和

FILE_ATTRIBUTE_SYSTEM位中任一个，则识别所述可执行文件为文件夹病毒。

3.根据权利要求2所述的方法，其特征在于，若不能获取到所述可执行文件夹的属性，则判定所述可执行文件夹为文件夹病毒。

4.根据权利要求2所述的方法，其特征在于，所述方法还包括：

在识别出所述可执行文件夹为文件夹病毒后，删除所识别出的为文件夹病毒的可执行文件夹。

一种识别文件夹病毒的方法

技术领域

[0001] 本发明涉及计算机技术，特别是一种识别文件夹病毒的方法。

背景技术

[0002] 文件夹病毒，是一种利用文件夹图标迷惑用户，双击打开进行复制的病毒。文件夹病毒会遍历移动存储设备的根目录下的文件夹，复制自身到移动存储设备的根目录下，更名为检测到的文件夹的文件名，修改该文件夹的属性为不可见，使用户在使用移动存储设备打开其文件夹时运行病毒，以达到复制的目的。现有技术中，利用病毒数据库，对扫描的文件进行特征匹配，若所述匹配成功，识别所述文件为文件夹病毒。原始的病毒数据库需要由操作人员逐一获取每个文件夹病毒，对每个文件夹病毒文件进行人工识别和特征提取，以建立病毒数据库。

[0003] 然而，现有建立病毒数据库的操作复杂，且容易出错，从而导致了病毒识别的效率和可靠性的降低。

发明内容

[0004] 为了克服现有技术的缺陷，本发明提供一种识别文件夹病毒的方法。可以提高识别文件夹病毒的效率和可靠性。

[0005] 本发明提供一种识别文件夹病毒的方法，包括：

[0006] 扫描指定根目录下的文件，获得可执行文件夹的文件名；

[0007] 计算文件名的相似度，确定与可执行文件夹的文件名相同的文件名；

[0008] 判断是否存在文件名与可执行文件夹的文件名相同的文件夹，若否，则判定所述可执行文件夹不是文件夹病毒，若是，则获取所述可执行文件夹的属性，根据可执行文件夹的属性判断所述可执行文件夹是否为文件夹病毒。

[0009] 进一步地，所述获取所述可执行文件夹的属性，根据可执行文件夹的属性判断所述可执行文件夹是否为文件夹病毒，包括：

[0010] 对文件夹执行取属性操作；

[0011] 判断返回值是否包含FILE_ATTRIBUTE_DIRECTORY位，如果返回值不包含FILE_ATTRIBUTE_DIRECTORY位，则判定所述可执行文件不是文件夹病毒，如果返回值包含FILE_ATTRIBUTE_DIRECTORY位，则进一步判断返回值是否包含FILE_ATTRIBUTE_HIDDEN位和FILE_ATTRIBUTE_SYSTEM位中任一个，如果返回值不包含FILE_ATTRIBUTE_HIDDEN位和FILE_ATTRIBUTE_SYSTEM位种任一个，则判定所述可执行文件不是文件夹病毒，如果返回值包含FILE_ATTRIBUTE_HIDDEN位和FILE_ATTRIBUTE_SYSTEM位中任一个，则识别所述可执行文件为文件夹病毒。

[0012] 进一步地，若不能获取到所述可执行文件夹的属性，则判定所述可执行文件夹为文件夹病毒。

[0013] 进一步地，所述方法还包括：

[0014] 在识别出所述可执行文件夹为文件夹病毒后，删除所识别出的为文件夹病毒的可执行文件夹。

[0015] 本发明的有益效果是：

[0016] 本发明能够对被感染的文件夹病毒进行主动识别，有效提高病毒识别的效率，以及有效提高系统的安全性能。

附图说明

[0017] 为了更清楚地说明本发明的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅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的前提下，还可以根据这些附图获得其它附图。

[0018] 图1是本发明的一种识别文件夹病毒的方法的流程示意图。

具体实施方式

[0019] 下面结合附图和实施例对本申请作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释相关发明，而非对该发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与有关发明相关的部分。

[0020] 需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

[0021] 参见图1，本发明提供一种识别文件夹病毒的方法，包括：

[0022] S1、扫描指定根目录下的文件，获得可执行文件夹的文件名；

[0023] 具体地，可执行文件(executable file)，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.exe、.sys和.scr等。

[0024] S2、计算文件名的相似度，确定与可执行文件夹的文件名相同的文件名；

[0025] S3、判断是否存在文件名与可执行文件夹的文件名相同的文件夹，若否，则判定所述可执行文件夹不是文件夹病毒，若是，则获取所述可执行文件夹的属性，根据可执行文件夹的属性判断所述可执行文件夹是否为文件夹病毒。

[0026] 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。

[0027] 进一步地，所述获取所述可执行文件夹的属性，根据可执行文件夹的属性判断所述可执行文件夹是否为文件夹病毒，包括：

[0028] 对文件夹执行取属性操作；

[0029] 判断返回值是否包含FILE_ATTRIBUTE_DIRECTORY位，如果返回值不包含FILE_ATTRIBUTE_DIRECTORY位，则判定所述可执行文件不是文件夹病毒，如果返回值包含FILE_ATTRIBUTE_DIRECTORY位，则进一步判断返回值是否包含FILE_ATTRIBUTE_HIDDEN位和FILE_ATTRIBUTE_SYSTEM位中任一个，如果返回值不包含FILE_ATTRIBUTE_HIDDEN位和FILE_ATTRIBUTE_SYSTEM位种任一个，则判定所述可执行文件不是文件夹病毒，如果返回值包含FILE_ATTRIBUTE_HIDDEN位和FILE_ATTRIBUTE_SYSTEM位中任一个，则识别所述可执行

文件为文件夹病毒。

[0030] 进一步地，若不能获取到所述可执行文件夹的属性，则判定所述可执行文件夹为文件夹病毒。

[0031] 进一步地，所述方法还包括：

[0032] 在识别出所述可执行文件夹为文件夹病毒后，删除所识别出的为文件夹病毒的可执行文件夹。

[0033] 本发明能够对被感染的文件夹病毒进行主动识别，有效提高病毒识别的效率，以及有效提高系统的安全性能。

[0034] 以上描述仅为本申请的较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解，本申请中所涉及的发明范围，并不限于上述技术特征的特定组合而成的技术方案，同时也应涵盖在不脱离所述发明构思的情况下，由上述技术特征或其等同特征进行任意组合而形成的其它技术方案。例如上述特征与本申请中公开的(但不限于)具有类似功能的技术特征进行互相替换而形成的技术方案。

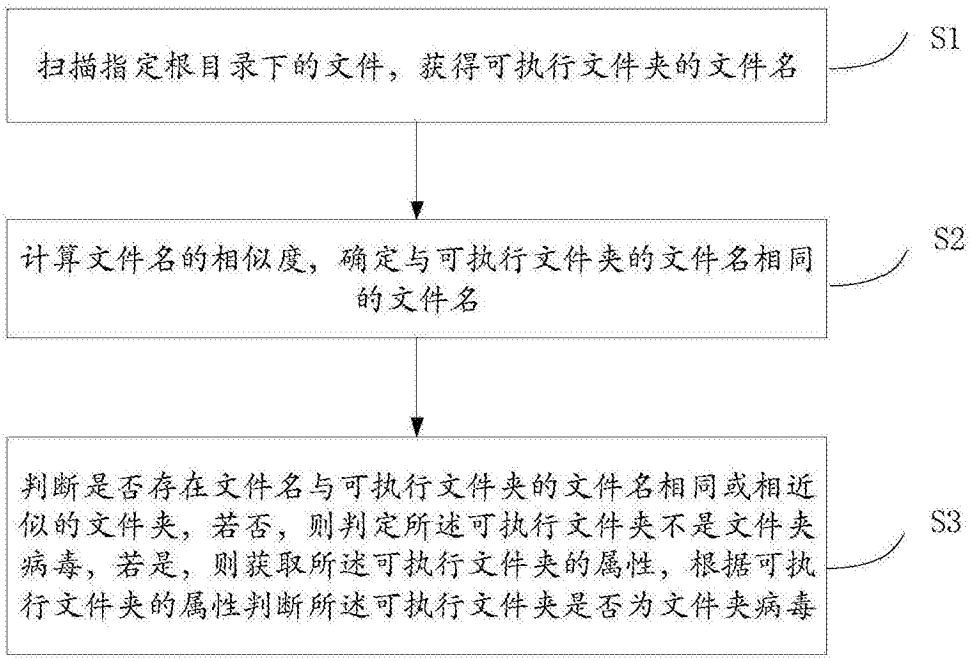

扫描指定根目录下的文件，获得可执行文件夹的文件名
S1
计算文件名的相似度，确定与可执行文件夹的文件名相同的文件名
S2
判断是否存在文件名与可执行文件夹的文件名相同或相近似的文件夹，若否，则判定所述可执行文件夹不是文件夹病毒，若是，则获取所述可执行文件夹的属性，根据可执行文件夹的属性判断所述可执行文件夹是否为文件夹病毒
S3

图1