[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/22 (2006.01)
H04L 29/06 (2006.01)

[12] 发明专利说明书

专利号 ZL 200710029168.5

[45] 授权公告日 2010 年 3 月 24 日

[11] 授权公告号 CN 100595778C

[22] 申请日 2007.7.16
[21] 申请号 200710029168.5
[73] 专利权人 珠海金山软件股份有限公司
地址 519015 广东省珠海市吉大景山路莲山巷 8 号金山电脑大厦
[72] 发明人 姚 辉 赵 闽 李 敏 肖 凯 李伟健
[56] 参考文献
CN1314638A 2001.9.26
CN1794258A 2006.6.28
CN1801033A 2006.7.12
US20050132206A1 2005.6.16
US20060198313A1 2006.9.7
US20050132184A1 2005.6.16
CN1859199A 2006.11.8

审查员 杨 洁
[74] 专利代理机构 广州华进联合专利商标代理有限公司
代理人 李双皓

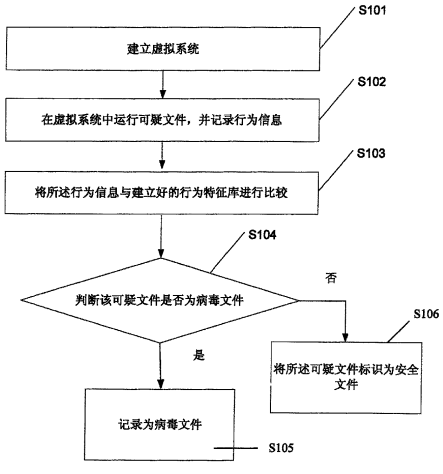
权利要求书 2 页 说明书 8 页 附图 2 页

[54] 发明名称

鉴定病毒文件的方法、装置

[57] 摘要

本发明提供的鉴定病毒文件的方法，建立虚拟系统后在该系统运行可疑文件，记录可疑文件的行为信息；将行为信息与行为特征库的行为特征进行匹配，获取行为特征的权值，检测行为特征的权值之和是否大于设定值，如果是，将可疑文件标识为病毒文件；否则，将可疑文件标识为安全文件。本发明还提供了鉴定病毒文件的装置，包括建立模拟系统的虚拟系统模块，将可疑文件的行为定向至虚拟系统，运行可疑文件；记录可疑文件的行为信息的行为信息收集模块；行为特征分析模块，用于将行为信息与行为特征库的行为特征进行匹配，获取行为特征的权值，检测行为特征的权值之和是否大于设定值，如果是，将可疑文件标识为病毒文件；否则将可疑文件标识为安全文件。



1、一种鉴定病毒文件的方法，其特征在于，包括步骤:

建立虚拟系统，在该虚拟系统中运行可疑文件，记录所述可疑文件的行为信息;

将所述行为信息与行为特征库的行为特征进行匹配，获取所述行为特征的权值，检测所述行为特征的权值之和是否大于设定值，如果是，则将所述可疑文件标识为病毒文件；否则，将所述可疑文件标识为安全文件。

2、根据权利要求 1 所述的鉴定病毒文件的方法，其特征在于，在该虚拟系统中运行可疑文件的过程包括:

所述可疑文件发出行为请求消息，所述虚拟系统根据所述可疑文件的行为请求消息，向所述可疑文件返回行为成功消息，所述可疑文件运行下一行为。

3、根据权利要求 2 所述的鉴定病毒文件的方法，其特征在于，

建立虚拟系统时，还进一步包括：设定所述可疑文件的运行时间;

记录所述可疑文件的行为信息具体包括：在所述运行时间内记录可疑文件的行为信息。

4、根据权利要求 2 所述的鉴定病毒文件的方法，其特征在于，还包括步骤:

当判断所述可疑文件为病毒文件时，将所述病毒文件在所述虚拟系统的行为内容清空。

5、一种鉴定病毒文件的装置，其特征在于，该装置包括:

虚拟系统模块，用于建立虚拟系统，将可疑文件的行为定向至该虚拟系统，运行所述可疑文件;

行为信息收集模块，用于记录所述可疑文件的行为信息;

行为特征分析模块，用于将所述行为信息与行为特征库的行为特征进行匹配，获取所述行为特征的权值，检测所述行为特征的权值之和是否大于设定值，如果是，则将所述可疑文件标识为病毒文件；否则，将所述可疑文件标识为安全文件。

6、如权利要求 5 所述的鉴定病毒文件的装置，其特征在于，所述虚拟系统模块包括可疑文件存储模块，用于存储所述可疑文件，以及

映像加载模块，用于将所述可疑文件在该虚拟系统中逐一加载，并在所述虚拟系统中运行所述可疑文件。

7、如权利要求 6 所述的鉴定病毒文件的装置，其特征在于，该装置还包括:

定时单元，用于设定所述可疑文件运行时间;

所述行为信息收集单元，还用于在所述定时单元设定的运行时间内，记录所述可疑文件的行为信息。

8、如权利要求 7 所述的鉴定病毒文件的装置，其特征在于，该装置还包括：数据安全处理模块，用于当判断所述可疑文件为病毒文件时，将所述病毒文件在所述虚拟系统的行为内容清空，并通知所述映像加载模块加载下一个可疑文件。

鉴定病毒文件的方法、装置

技术领域

本发明涉及计算机反病毒技术领域。

背景技术

近年来，互联网上流行的病毒和木马通常不是单个发作，而是一类的大量变种在互联网上活动，且可频繁升级，因此很容易发生大量的病毒或木马爆发的局面。这对反病毒产品升级的周期提出了更高的要求，反病毒产品的升级速度对是否能有效防杀大量的病毒和木马起到重要的作用。

目前反病毒最成熟的技术之一是特征法。特征法一般包括病毒分析、特征提取、病毒库制作和升级等过程，而这些过程中，鉴定可疑文件是否为病毒的病毒分析过程是最耗时的过程之一。

一种分析病毒的方法是动态分析。动态分析的主要过程是，在用户系统中运行可疑文件，利用半自动工具记录所述可疑文件运行时的行为，通过系统运行前和运行后的比较，得出可疑文件运行后对系统的改动结果，然后对所述结果进行对比、分析，最终确认所述可疑文件是否为病毒，如果所述可疑文件为病毒，则需要重启系统，对系统进行恢复，再继续对下一个可疑文件进行分析。

上述病毒分析方法的不足之处在于，在该方法中，可疑文件在计算机系统中运行，如果该可疑文件是病毒，则会对系统造成损害，在病毒分析过程中为了减少病毒的危害性，需要重启系统对系统进行还原修复，而重启动作使得病毒分析的过程大为延长，从而影响反病毒产品的升级周期；另外，如果病毒使系统崩溃，则需要重装系统，这将更为延长反病毒产品的升级周期。

发明内容

本发明提供一种鉴定病毒文件的方法、装置及网络设备，能够缩短鉴定病毒文件的时间，提高了病毒分析的效率。

为达到上述发明目的，本发明提出以下的技术方案：

本发明提供了鉴定病毒文件的方法：首先建立虚拟系统，在该虚拟系统中运行可疑文件，记录所述可疑文件的行为信息；将所述行为信息与行为特征库的行为特征进行匹配，获取所述行为特征的权值，检测所述行为特征的权值之和是否大于设定值，如果是，则将所述可疑文件标识为病毒文件；否则，将所述可疑文件标识为安全文件。

本发明还提供了鉴定病毒文件的装置，该装置包括：

虚拟系统模块，用于建立模拟系统，将可疑文件的行为定向至虚拟系统，运行可疑文件；

行为信息收集模块，用于记录所述可疑文件的行为信息；

行为特征分析模块，用于将所述行为信息与行为特征库的行为特征进行匹配，获取所述行为特征的权值，检测所述行为特征的权值之和是否大于设定值，如果是，则将所述可疑文件标识为病毒文件；否则，将所述可疑文件标识为安全文件。

在本发明中，由于建立了虚拟系统，在病毒分析过程中，使可疑文件在虚拟的系统中运行，对真实的系统没有损害，一个文件鉴定完毕，只需放弃其在虚拟系统的行为结果即可，而无需对系统进行重启修复，因此系统恢复速度快，节约的大量分析时间，提高了鉴定病毒的效率。

附图说明

图 1 为一个实施例中鉴定病毒文件的流程图；

图 2 为一个实施例中鉴定病毒文件的装置的逻辑框图。

具体实施方式

在病毒分析的过程中，鉴定一个可疑文件是否为病毒文件，通常是通过对该文件的运行时的行为进行分析，从而确认是否为病毒文件。请参阅图 1，本发明提供一种鉴定病毒文件的方法，首先在系统中构造虚拟系统（S101），当发现可疑文件时，令可疑文件在该虚拟系统中运行，并记录可疑文件的行为信息（S102）；并将行为信息和行为特征库进行比对（S103），判断所述可疑文件是否为病毒文件（S104），如果是，则将所述可疑文件标识为病毒文件（S105）；否则，将所述可疑文件标识为安全文件（S106）。

对于步骤 S101，虚拟系统可以通过使用计算机程序监控系统关键 API、以及模拟真实系统某些功能的方式构建一种虚拟框架，可以模拟真实的系统加载程序的过程，以便使可疑文件作用于真实系统的行为能够被重定向与该

虚拟系统中。

对于步骤 S102，当通过模拟系统对可疑文件进行加载后，令其在虚拟系统中运行，当可疑文件需要执行某个行为时，通常需要发出行为请求消息，此时虚拟系统根据可疑文件的行为请求消息，向所述可疑文件返回所述行为成功消息，当可疑文件收到成功消息后认为前述的行为成功，因此继续运行下一行为。例如，假设一个可疑文件的行为是打开一个 IE、链接到一个网站，在收集到可疑文件的该行为请求消息后，虚拟系统向该可疑文件行为发出消息：打开 IE 及网站链接成功，在接收到该成功消息后，这个可疑文件认为这个成功是真实的，从而进行下一步的动作。对于步骤 S102，对可疑文件在虚拟系统中执行的行为信息进行记录，由于真实的操作系统没有执行对应于该可疑文件的行为动作，因此，在可疑文件进行下一步的动作之后，以同样的方式进行记录该行为的行为信息。在一个实施例中，由计算机系统来进行上述记录过程，可以将记录结果存放到数据库里，也可以存放为某种文件格式、日志、分析报告或者当该可疑文件是用户上报上来的时候，可以将记录结果回馈给用户等。

对于步骤 S103，当该可疑文件在虚拟系统中的运行完成后，对所记录的所有的行为信息进行分析，在一个实施例中，通过分析虚拟系统运行前和运行后的变化获得可疑文件运行后对系统的改动结果，行为信息可以是可疑文件对系统的改动结果，可以包括对虚拟系统的注册表、文件、网络或进程等的影响。以对文件的改动为例，可以包括对文件的感染、修改、添加和删除。将行为信息与行为特征库进行比对，如果行为特征库中存在这个可疑文件的行为信息，则将其标识为病毒，进行下一步的处理工作，如果不存在，则认为该可疑文件是正常的行为特征，让它在真实的系统上真实运行。

作为本发明的进一步改进，在一个实施例中，对于行为特征库中存在的

行为特征，可以设定相应的权值，当将行为信息与行为特征库进行比对时，将行为特征库中对应的各权值进行相加，当权值大于某个设定值时，则判定该可疑文件为病毒了。

另外，由于在对可疑文件的行为进行分析时需要考虑到各行为的权值之和，为了进一步加强对可疑文件分析的准确性，一个实施例中对所有的可疑文件依次进行分析，并且对每个可疑文件的行为进行分析时，将该可疑文件的每个行为分别进行分析，以避免多个行为的权值之间相互影响，造成误判。

以下列举一个对行为特征库中的行为特征设定权值的实例，在该实例中设定当可疑文件的各行为的权值大于 3 时，该可疑文件为病毒。

在该实施例中，行为特征库中可以包括以下行为特征:

一、注册表行为特征:

1、在注册表中添加启动项:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

在该实施例中将行为特征库中的该行为特征的权值设置为 2;

2、删除以下注册表键值，破坏系统的安全模式，导致用户不能选择进入安全模式:

HKEY_CURRENT_USER\SYSTEM\CurrentControlSet\Control\SafeBoot

在该实施例中将行为特征库中的该行为特征的权值设置为 4;

二、文件行为

1、将可疑文件自身复制到系统目录，在\Windows\system32\复制一个名为 svch0st.exe 的病毒本体。

在该实施例中将行为特征库中的该行为特征的权值设置为 2;

2、同时枚举 d-z 的分区生成文件 autorun.inf 和病毒体本身(auto.exe)，通过

系统的自动运行来激活病毒或传播病毒。

在该实施例中将行为特征库中的该行为特征的权值设置为 5;

三、内存行为

1、可疑文件在系统中查找安全软件的进程并进行中止行为，安全软件的进程可以是以下关键字的进程名:

kvolself.exe

KvReport.kxp

KVScan.kxp

KVSrvXP.exe

KVStub.kxp

kvupload.exe

kvwsc.exe

KvXP.kxp

KvXp_1.kxp

KWatch.exe

KWatch9x.exe

KWatchX.exe

MagicSet.exe

在该实施例中将行为特征库中的该行为特征的权值设置为 5。

在该实施例中，将可疑文件的行为信息与行为特征库的行为特征进行匹配，获取所述行为的权值，当某个可疑文件的行为包含以上至少一项与上述行为特征匹配的行为信息，并且各行为信息的权值的和大于 3 时，则认为该可疑文件为病毒文件，否则，判断所述可疑文件为安全文件。

在本发明的一个实施例中，设定了所述可疑文件在虚拟系统中的运行时间；在规定时间内对可疑文件的行为信息进行追踪，可疑文件可以不必运行完所有的行为，以节约分析可疑文件的时间。

由上所述，本发明提供的鉴定病毒文件的方法是由系统执行的动态分析过程，另外，现有技术中的鉴定病毒文件通常需要对系统进行重启，是由于现有技术中的鉴定病毒文件的方法是对可疑文件在真实的操作系统中的行为进行分析，为了减小病毒文件对系统的损害，在对一个可疑文件进行鉴定分析后，需要将系统进行重启来对系统进行还原，而本发明的鉴定病毒文件的方式是在一个虚拟的环境里进行，可疑文件在虚拟的系统里运行，因此不会对真实的系统产生影响，从而本发明的方案既不影响真实的系统，避免了重启动系统损耗的时间，节省了鉴定病毒文件的时间。

进一步，由于可疑文件作用于虚拟的系统，不作用于真实系统的，因此当对可疑文件分析完成时，通过放弃该可疑文件在虚拟系统中所产生的行为结果，就可以将系统恢复，即将病毒文件在虚拟系统中的行为内容删除。比如：清除病毒在虚拟的系统中创建的文件，也就是说，本发明不需要重新启动系统，可自我恢复系统，从而加快对可疑文件的鉴定效率。

对应于上述鉴定病毒文件的方法，本发明还提供一种鉴定病毒文件的装置，请参阅图 2，该装置包括虚拟系统模块 201，用于建立虚拟系统，将可疑文件的行为定向至虚拟系统，运行可疑文件；行为信息收集模块 202，用于记录所述可疑文件的行为信息；行为特征分析模块 203，用于根据所述行为信息和行为特征库，判断所述可疑文件为病毒时，将所述可疑文件标识为病毒；判断所述可疑文件为安全文件时，将所述可疑文件标识为安全文件。

所述虚拟系统模块 201 可以包括可疑文件存储模块 2011 和映像加载模块 2012。

虚拟系统模块 201 通过监控真实系统的关键 API 以及模拟真实系统的某些功能建立一个虚拟系统，可疑文件存储模块 2011 将所有的可疑文件组成文件

队列，进行存储；映像加载模块2012模拟真实系统的加载程序的过程，从可疑文件存储模块2011获取可疑文件，逐一将可疑文件加载到内存，当收到可疑文件的行为请求信息后，向该可疑文件发送成功消息，令可疑文件在虚拟系统中运行；行为信息收集模块2012从虚拟系统模块201中获取可疑文件的各种行为信息，进行规范记录；行为特征分析模块203将行为信息收集模块202的信息记录与行为特征库进行匹配，获得该行为的权值，并将分析结果发送给数据安全处理模块204，数据安全处理模块204将分析结果是病毒文件的可疑文件对虚拟系统作用的内容进行清空，通知映像加载模块2012加载下一个可疑文件。

上文所述的各实施例中的鉴定病毒文件的方法中各步骤可以通过一条或多条指令实现，上述鉴定病毒文件的装置可以用于反病毒引擎工作过程中进行可疑文件的鉴定，并最终确定可疑文件为病毒文件，所述反病毒引擎利用被鉴定为病毒的文件的特征去标识其它文件为病毒并进行清除；所述指令可以被配置在包含处理器的网络设备中，由该处理器执行，同时，所述指令可以存储在存储介质中。所述网络设备可以是计算机等网络设备。

以上所述的本发明实施方式，并不构成对本发明保护范围的限定。任何在本发明的精神和原则之内所作的修改、等同替换和改进等，均应包含在本发明的权利要求保护范围之内。

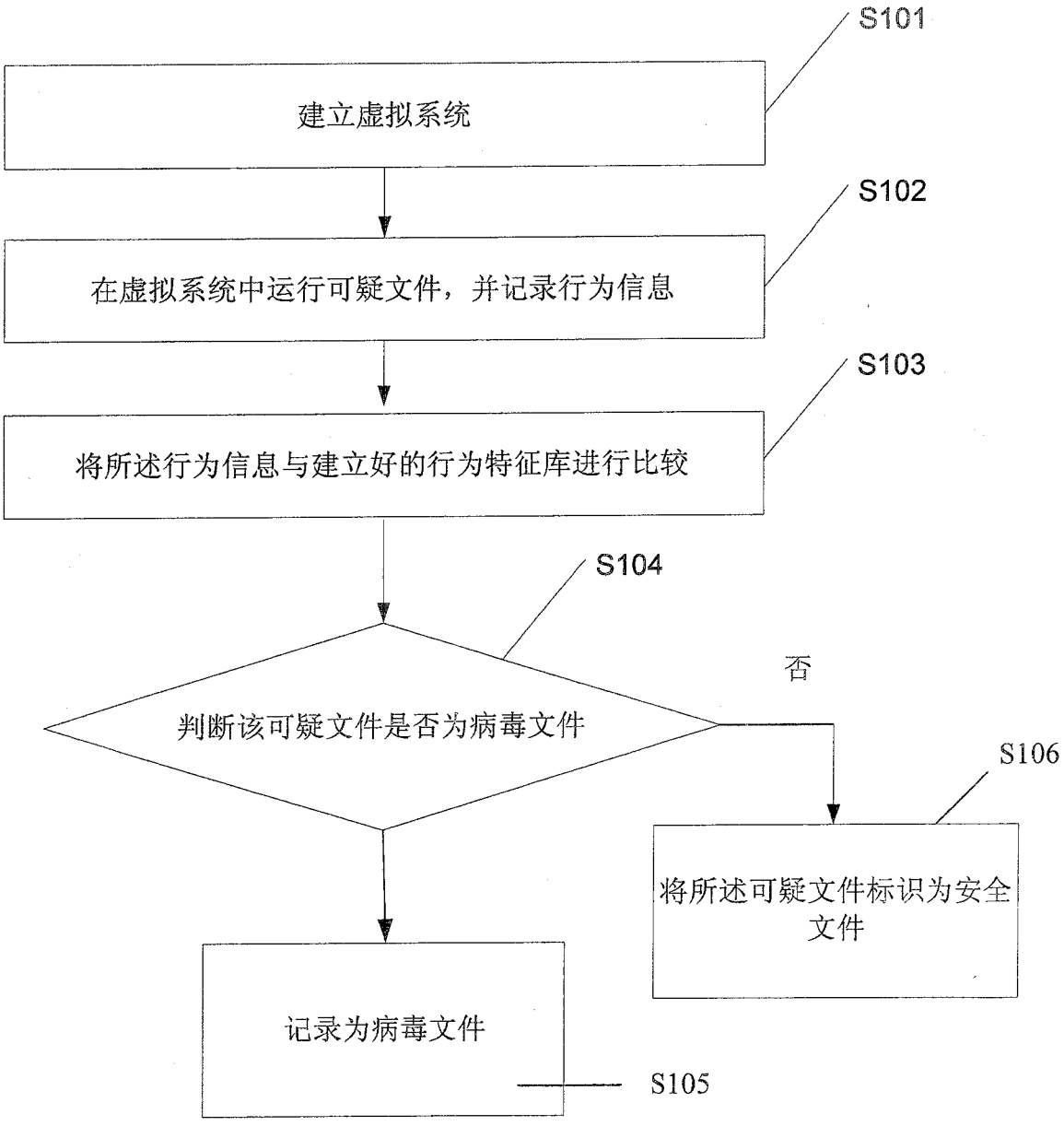

S101
建立虚拟系统
S102
在虚拟系统中运行可疑文件，并记录行为信息
S103
将所述行为信息与建立好的行为特征库进行比较
S104
判断该可疑文件是否为病毒文件
否
S106
将所述可疑文件标识为安全文件
记录为病毒文件
S105

图 1


虚拟系统模块201
可疑文件存储模块2011
映像加载模块2012
行为信息收集模块202
行为特征分析模块203
数据安全处理模块204

图 2