(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105556481 B
(45)授权公告日 2018.05.29

(21)申请号 201480037332.5

(22)申请日 2014.06.23

(65)同一申请的已公布的文献号
申请公布号 CN 105556481 A

(43)申请公布日 2016.05.04

(30)优先权数据
13/929,681 2013.06.27 US

(85)PCT国际申请进入国家阶段日
2015.12.29

(86)PCT国际申请的申请数据
PCT/US2014/043673 2014.06.23

(87)PCT国际申请的公布数据
WO2014/209889 EN 2014.12.31

(73)专利权人 联传科技公司
地址 美国宾州西雀斯特瓦载尔道1235
专利权人 倪朝兴

(72)发明人 倪朝兴

(74)专利代理机构 长沙正奇专利事务所有限责任公司 43113
代理人 何为 袁颖华

(51)Int.Cl.
G06F 11/30(2006.01)

(56)对比文件
US 8230510 B1,2012.07.24,说明书第3栏第22-第8栏第6行、图7.
US 8230510 B1,2012.07.24,说明书第3栏第22-第8栏第6行、图7.
CN 101542451 A,2009.09.23,说明书第9页第27行-第10页第14行.
CN 102664884 A,2012.09.12,说明书第[0021]-[0025]段.
US 2012/0272321 A1,2012.10.25,全文.
CN 101719208 A,2010.06.02,全文.
US 2002/0199116 A1,2002.11.26,全文.
US 2004/0193918 A1,2004.09.30,全文.
US 2010/0083381 A1,2010.04.01,全文.
US 7854006 B1,2010.10.14,全文.

审查员 袁茹芳

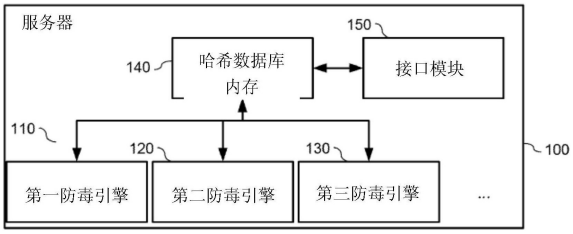
权利要求书2页 说明书4页 附图3页

(54)发明名称

防毒保护系统及方法

(57)摘要

本发明关于防毒保护,且更详而言之是关于云端服务器的防毒保护。本发明保护用户机器不受计算机病毒影响。藉由本发明,使用者不需在使用者机器上运行多重防毒选项即可同时利用此等防毒选项。



CN 105556481 B

1.一种于一服务器上的防毒保护方法,其包含:

使用一防毒选项能够自动化且周期性地反复扫描二进元,该防毒选项具有经持续更新的引擎及计算机病毒定义,其中该扫描二进元的动作系发生于远离使用者机器之处;

识别一计算机病毒;

识别一已受该计算机病毒影响的用户机器;

对该用户建议一用以消灭该计算机病毒的处理方式;以及

于该服务器上更新该使用者机器状态,该服务器储存每一用户计算机上载有的全部应用程序或程序,该些程序以二进元储存并被用于侦测该用户计算机的病毒,让该防毒选项不需要占用该用户计算机的运算资源。

2.如权利要求1所述的方法,其中该识别一已受该计算机病毒影响的用户机器的步骤是使用用户机器上一哈希数据库、应用程序、独特用户机器识别符以及定期更新的应用程序哈希数据库来达成。

3.如权利要求1所述的方法,更包含使用一轻量防病毒软件侦测该使用者机器上的一新安装的程序并发送其哈希或二进元以供承索的远程扫描。

4.如权利要求1所述的方法,其中该扫描是依据来自该服务器的信息识别该用户机器上的所有无病毒程序,且一轻量防病毒软件仅扫描新安装的程序。

5.如权利要求1所述的方法,其中该扫描该二进元的步骤是使用数个防毒选项达成。

6.如权利要求1所述的方法,其中该使用者机器是一智能型手机。

7.如权利要求1所述的方法,其中该使用者机器是一平板计算机。

8.如权利要求1所述的方法,其中该用户机器是一网络安全装置。

9.如权利要求1所述的方法,其中该防毒保护方法用于一企业网络环境。

10.一种远程防毒保护系统,其包含:

一非瞬时内存,用以储存一包含至少一哈希的哈希数据库以及对应于一用户机器上至少一程序的程序;

一防毒引擎,连接至该数据库,该防毒引擎使用经持续更新的引擎及计算机病毒定义以能够自动化且周期性地反复扫描一计算机病毒;以及

一接口模块,连接至该哈希数据库,该远程从一远程位置用户机器接收有关一哈希及机器状态的信息,并向一用户机器发送有关一计算机病毒的信息。

11.如权利要求10所述的系统,其中该哈希数据库是于一用户安装一新软件程序时更新。

12.如权利要求11所述的系统,其中该接口模块发送有关该新软件程序状态的信息。

13.如权利要求11所述的系统,其中该新软件程序储存于该用户计算机中。

14.如权利要求10所述的系统,其中该防毒引擎为一可经商业管道取得的防毒选项。

15.如权利要求10所述的系统,其中该防毒引擎为一开放原始码防毒选项。

16.如权利要求10所述的系统,进一步包含一使用者机器,该使用者机器具有一轻量防病毒软件,用以侦测一新安装的程序并将该程序发送以供承索的远程扫描。

17.如权利要求10所述的系统,其中该防毒引擎识别一用户机器上的所有无病毒程序,且一轻量防病毒软件扫描一新安装的程序。

18.如权利要求10所述的系统,其中该防毒引擎使用数个防毒选项。

19.如权利要求10所述的系统,其中该系统用于一企业网络环境。

防毒保护系统及方法

技术领域

[0001] 本发明整体而言是关于防毒保护，且更详而言之是关于经由云端服务器所提供的防毒保护。

背景技术

[0002] 目前市面上虽可见多种防病毒软件选项，但有其不足之处。原因在于现有防毒选项皆是直接于用户计算机上运行，是故具有诸多缺点。

[0003] 例如，使用者于同一时间仅可运行一种防毒选项，因为各种防毒选项无法同时运作。但每种防毒选项所擅长侦测的特定种类计算机病毒可能各有不同，因此最好是能够使用一种以上防毒解决方案。此外，各种防毒选项均分别收取相关授权费用。

[0004] 再者，将计算机病毒加入一防毒选项可拦截的已知计算机病毒列表可能需要很长时间。在某些情况下，将新计算机病毒加入已知计算机病毒列表以供防病毒软件侦测到的程序可能长达90天。

[0005] 现有防毒选项的另一缺点在于必须在用户计算机上运行，因此会占用用户计算机上的运算资源及内存。

[0006] 综言之，吾人实需一防毒解决方案，其应可利用一种以上的防毒选项以快速侦测新计算机病毒，却不会产生多笔授权费用或占用使用者运算资源。

发明内容

[0007] 本发明的实施例是藉由同时于远程使用多种防毒选项保护用户机器不受计算机病毒影响。由于每个防毒选项可能各有其所擅长侦测的计算机病毒，因此使用多种防毒选项有助于提高计算机病毒侦测效果。但通常而言若使用者机器同时运行多种防毒选项，各种防毒选项便可能彼此干扰，无法共同作用。并且，防毒选项所费不赀，其使用往往牵涉极高成本。此外，同时运行多种防毒选项需要大量运算力，因此会于使用者机器上占用过多运算资源。

[0008] 本发明实施例克服上述限制的方案是在云端或远程对用户机器运行防毒选项，而仅于用户机器上运行轻量防病毒软件。在云端运行防毒选项可使各选项在多重机器上运作，从而克服上述限制。

[0009] 本发明的实施例利用哈希数据库判断用户机器中是否存有一特定档案或应用程序。因此，云端不需要直接存取使用者机器，只需存取用户机器上的哈希数据即可。

[0010] 读者参照以下说明及申请专利范围搭配附图，将可更加知悉本发明的其他目的及功效，并对本发明有更完整的认识。

附图说明

[0011] 以下将参照本发明实施例说明，各实施例的范例系如附图所示。本案附图仅为说明之用，不具限制性。虽然本发明以此等实施方式为例说明，应知本发明并不受限于此等特

定实施例的范围。

[0012] 图1为依据本发明一防毒系统的方块图。

[0013] 图2为依据本发明一防毒系统及其与用户机器互动的方块图。

[0014] 图3为依据本发明一防毒方法的流程图。

[0015] 图4为依据本发明一用户接口的实施例。

具体实施方式

[0016] 以下叙述的目的在于提供解说以利读者了解本案发明。然而，熟悉此技术的人应知本发明在此所述的实施例及其他实施例可运用于不同运算系统及装置。本发明的实施例可为硬件、软件或韧体的型态。图中所示结构仅为本发明实施例的示范，且以避免模糊本发明的焦点为考虑。此外，图中组件间的连接并不限于直接连接，实则组件间的数据可经中间组件修改、重新制作格式或以其他方式改变。

[0017] 本案说明书中所称“一实施例”、“在一实施例中”或“一实施例”等等意欲指称与本发明至少一实施例相关的特定功征、结构、特性或功能包含于该实施例中。说明书中各处所称“在一实施例中”的语未必全部参照相同实施例。

[0018] 图1为本发明防毒系统的方块图。图1显示服务器100。服务器100可使用一或多台计算机实施。服务器100包括内含哈希数据库以及对应应用程序的非瞬时内存140。哈希为防毒选项中所使用的独特指纹。每一程序各有其独特哈希。例如，Microsoft Word即有一特定哈希。稍早版本的Word则具有另一哈希，Microsoft Excel亦有其专属哈希。此外，哈希的储存所占内存空间不多。哈希数据库140为一与应用程序及用户机器相关的哈希列表。

[0019] 图1亦显示接口模块150。接口模块150与用户机器通讯。接口150从用户机器将信息提供至服务器100，如下文将参照图2详述者。接口模块150亦向用户机器提供信息，例如，是否侦测到计算机病毒的状态。接口模块150亦可向用户机器发送建议的处理方式。

[0020] 配合服务器100运作的哈希数据库140包含用户机器上所有应用程序的储存，可供本发明的实施例从远程使用第一防毒引擎110、第二防毒引擎120及第三防毒引擎130等等扫描用户机器上的应用程序。所述远程扫描可为利用经持续更新的引擎及计算机病毒定义所进行的反复扫描。如熟悉此技术的人所应知，反复扫描意指自动再次扫描档案而非手动扫描或用户所要求的程序。如熟悉此技术的人所应知，经持续更新的引擎及定义意指，因应新计算机病毒遭辨识而成为已知，周期性更新防毒引擎。持续更新并不需要任何特定更新间隔。

[0021] 防毒引擎110-130可为任何可经商业管道取得的防毒选项或开放原始码防毒选项。熟悉此技术的人应知所有防毒选项110-130皆可彼此搭配运作，使服务器可运用任何或所有可用防毒选项进行扫描。或者，亦可单独使用一个防毒引擎。因此，可将一或多个防毒引擎的任何组合实施于一或多台机器。

[0022] 远程位置可为所谓“云端”，经由因特网连接至使用者机器的服务器上。所述远程位置亦可经由企业内部网络连接至用户机器。例如，本发明的实施例可实施于企业环境中，由服务器100扫描员工使用的所有应用程序，并利用哈希数据库140判定哪一或哪些员工受到计算机病毒感染。

[0023] 图2为本发明中防毒系统及其与用户机器互动的方块图。图2中显示图1的部分组

件，例如防毒引擎110-130，并显示第n防毒引擎210，表示防毒引擎数目不限。图2中亦显示哈希数据库140、服务器220及样本机器230。样本机器230表示可能有多台机器用为服务器上程序的主机。样本机器用于上传通用应用程序二进元，而不需从使用者机器收集，可免于造成网络带宽过载。

[0024] 图2亦显示服务器100与因特网或局域网络(LAN)240间的界面。因特网或LAN 240系连接至用户计算机250。如图2所示，用户计算机可为桌上型个人计算机或笔记本电脑。此外，用户计算机亦可为智能型手机、平板计算机或网络安全装置。网络安全装置包括侵入防护系统、集中式威胁管理(UTM)或任何其他用以预防计算机病毒攻击网络的网络安全装置。

[0025] 用户于计算机250上备有各种软件应用程序或程序。在本发明一实施例中，使用者亦安装一轻量防病毒软件的应用程序，其可从用户计算机收集哈希。此等哈希经由接口模块150发送至服务器100。在图2的实施例中，哈希系经由因特网或LAN发送至服务器100。若在服务器中找不到程序代码，亦可将实际程序代码发送至服务器100。

[0026] 服务器100储存每一用户计算机上载有的全部应用程序或程序。服务器100可因此利用第一防毒引擎110、第二防毒引擎120、第三防毒引擎130等等直到第n防毒引擎210来扫描计算机病毒。如此一来，使用者可得益于使用诸多不同防毒选项。不同防毒选项可能各有擅长侦测的计算机病毒种类。再者，用户可享有更完整的防毒扫描，却无需让防毒选项占用运算资源。此外，用户不需为多重防毒选项支付费用。

[0027] 在一实施例中，当轻量防病毒软件侦测到用户安装新程序时，用户计算机250可向服务器100的接口模块150发送讯息。之后服务器可使用第一防毒引擎110至第n防毒引擎210扫描新程序，且可经由接口模块150向用户计算机250发送讯息，表明此一新程序是否包含已知计算机病毒。若侦测到计算机病毒，用户可实时决定是否安装此项新程序，且实际上可选择不要安装此新程序。

[0028] 在一实施例中，用户计算机并非连接服务器，而是由轻量防病毒软件接手扫描安装之新程序以厘清有无计算机病毒，同时忽略先前已由服务器100确认为无病毒的所有其他程序。如此一来，不论用户机器是否具有网络连接性，皆能有效进行防毒。

[0029] 在一实施例中，侦测到计算机病毒后，服务器100经由接口模块150向用户计算机250发送讯息，表明已侦测到计算机病毒。服务器100亦可建议一种不致影响用户计算机250操作且能够消灭计算机病毒的处理方式。

[0030] 图3显示本发明防毒方法的流程图。图3显示使用防毒选项310反复扫描二进元。如上所述，反复扫描310是于服务器100中远程执行，且可使用一个或多个或全部已知防毒选项。如上所述，防毒选项可持续更新且包含经持续更新的定义。

[0031] 图3亦显示识别一计算机病毒的步骤320。由一或多个防毒引擎110-130识别计算机病毒320。图3亦显示识别用户机器是否受计算机病毒感染340的步骤。利用哈希数据库140判定用户机器是否已受计算机病毒感染340。哈希数据库140记录哪些哈希与每台用户机器上的程序相关。因此，服务器100可利用哈希数据库140鉴别哪一台用户机器受到计算机病毒340感染。

[0032] 图3亦显示向用户建议用以消灭该计算机病毒350的处理方式。处理方式350建议系利用接口模块150提出。接口模块150可向用户机器250发送讯息，说明建议的处理方式。图3亦显示于服务器更新用户机器状态360的流程。上述更新系藉由在使用者机器250上运

行的轻量防病毒软件实现，以鉴别哈希并将鉴别结果告知服务器100。

[0033] 图4依据本发明的各种态样显示用户接口的一种实施例。图4为用户接口400的一种范例，其可用于使用者机器250上，传达用户机器250中存有计算机病毒的讯息。图4亦显示采取若干用户可用选项之形式所提出的建议处理方式，例如，隔离、移除或允许。图4亦显示针对特定计算机病毒威胁所用之防毒选项及结果。待用户选定项目后，系统会将此项目告知服务器100。

[0034] 虽然本发明配合若干具体实施例加以说明，熟悉此技艺人士应可藉由上述说明思及诸多其他替代方案、修改及变化。因此，在此描述的发明意欲包含所有落入本发明精神及所附申请专利范围定义范畴的此等替代方案、修改、应用、组合、置换及变化。

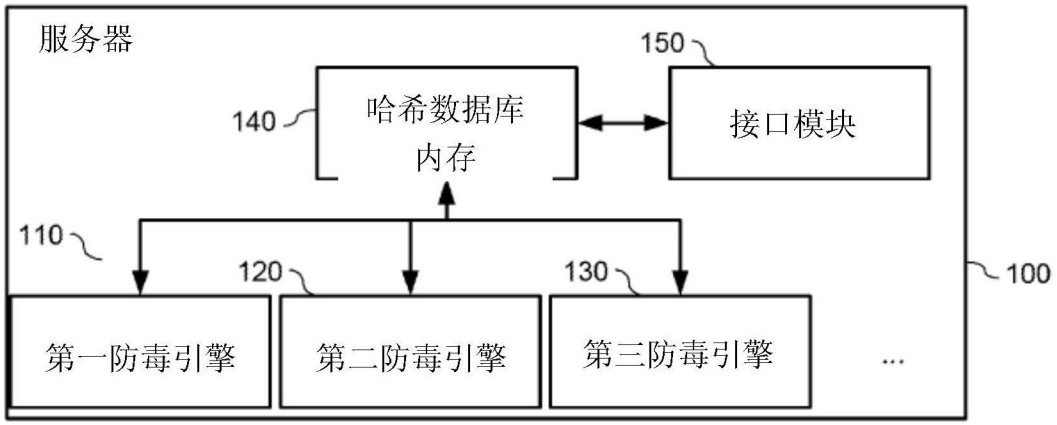

服务器
150
140
哈希数据库
内存
接口模块
110
120
130
100
第一防毒引擎
第二防毒引擎
第三防毒引擎
...

图1

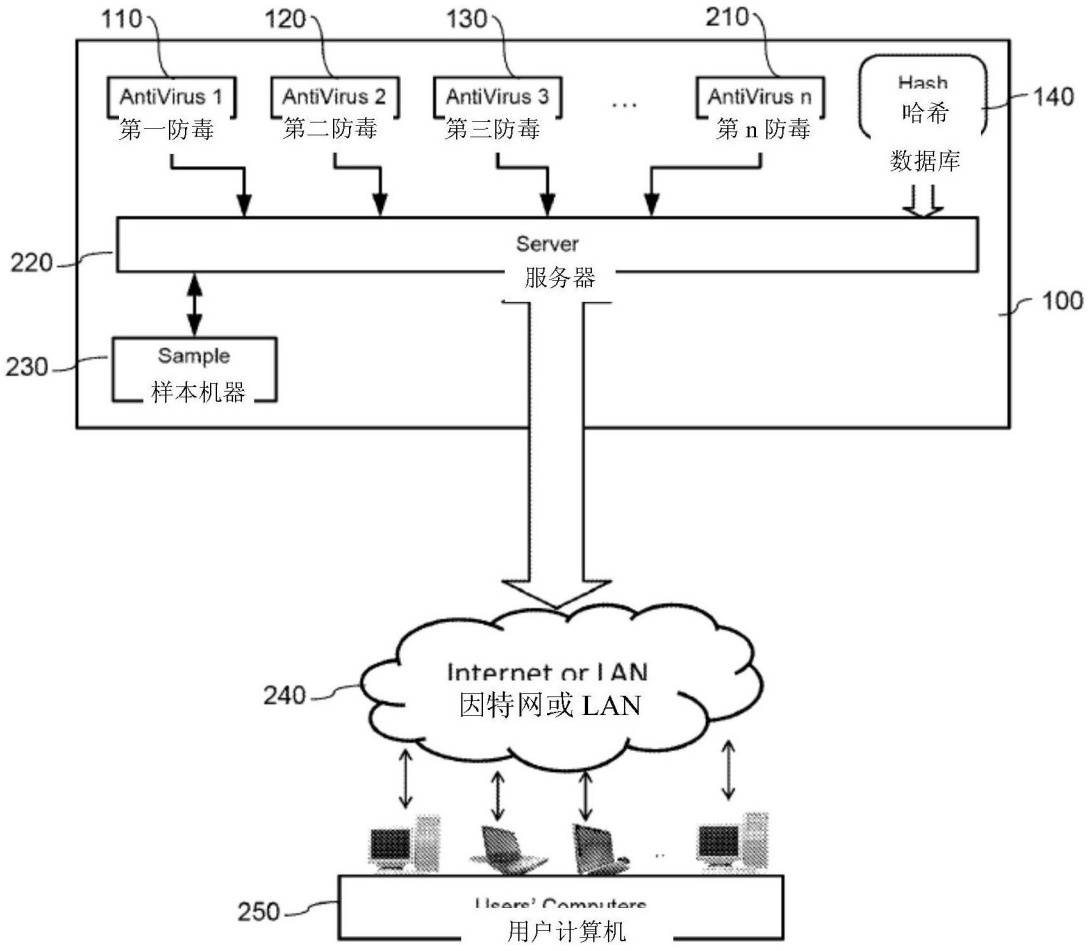

110
120
130
210
AntiVirus 1
第一防毒
AntiVirus 2
第二防毒
AntiVirus 3
第三防毒
...
AntiVirus n
第 n 防毒
Hash
哈希
数据库
140
Server
服务器
220
100
Sample
样本机器
230
Internet or LAN
因特网或 LAN
240
250
用户计算机

图2

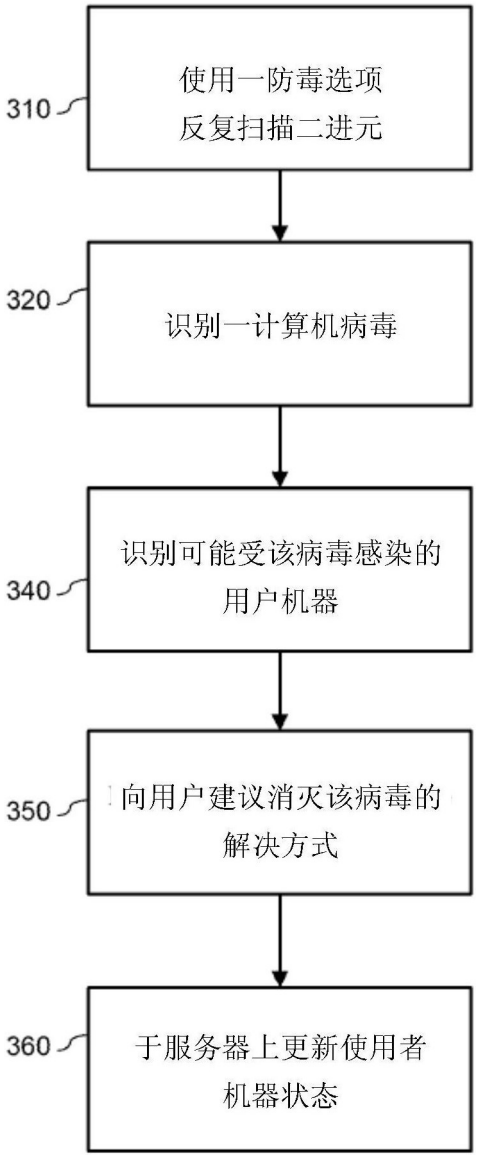

310
使用一防毒选项
反复扫描二进元
320
识别一计算机病毒
340
识别可能受该病毒感染的
用户机器
350
向用户建议消灭该病毒的
解决方式
360
于服务器上更新使用者
机器状态

图3

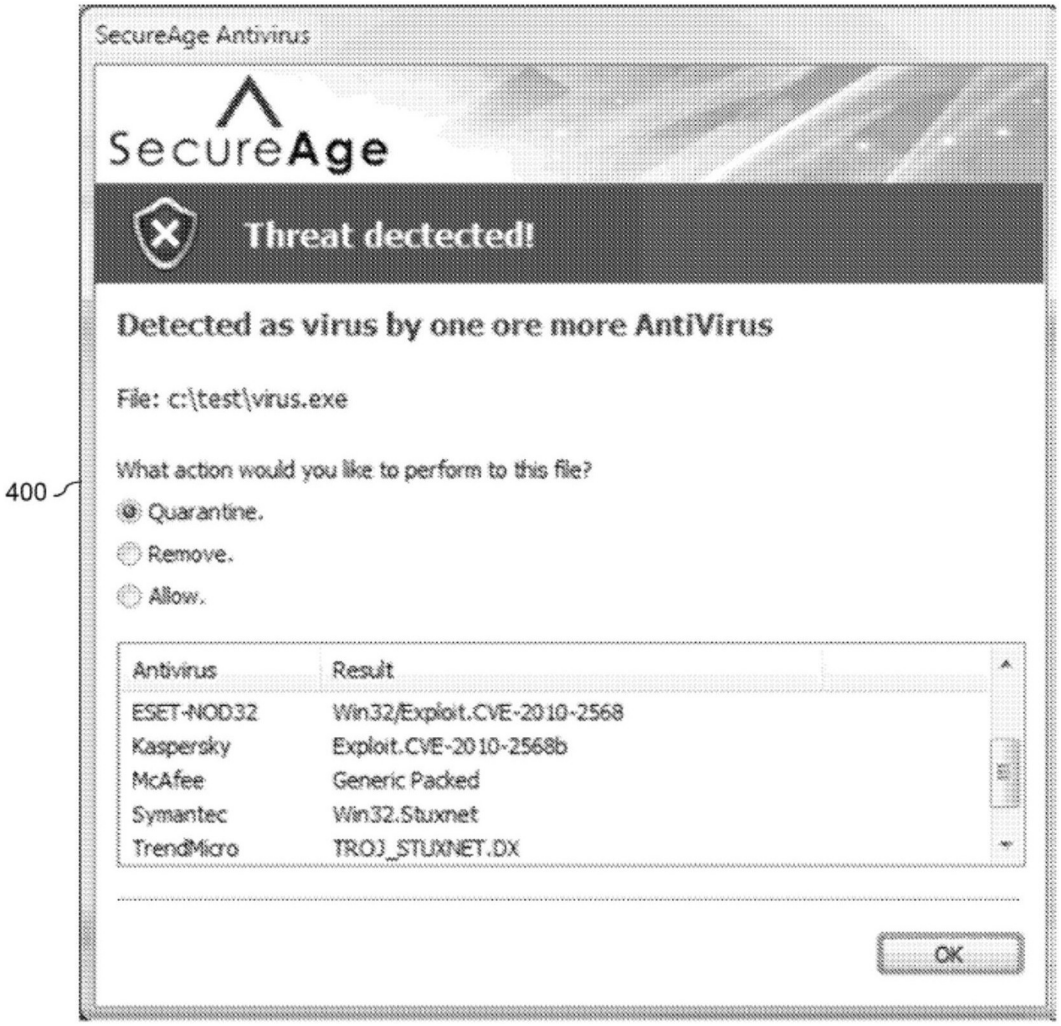

SecureAge Antivirus
SecureAge
Threat dectected!
Detected as virus by one ore more AntiVirus
File: c:\test\virus.exe
What action would you like to perform to this file?
Quarantine.
Remove.
Allow.
Antivirus
Result
ESET-NOD32
Win32/Exploit.CVE-2010-2568
Kaspersky
Exploit.CVE-2010-2568b
McAfee
Generic Packed
Symantec
Win32.Stuxnet
TrendMicro
TROJ_STUXNET.DX
OK
400

图4