[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 1/00 (2006.01)
H04L 29/06 (2006.01)

[12] 发明专利说明书

专利号 ZL 02807940.X

[45] 授权公告日 2006 年 5 月 17 日

[11] 授权公告号 CN 1256634C

[22] 申请日 2002.4.9 [21] 申请号 02807940.X
[30] 优先权
[32] 2001.4.10 [33] US [31] 09/829,761
[86] 国际申请 PCT/US2002/011239 2002.4.9
[87] 国际公布 WO2002/084459 英 2002.10.24
[85] 进入国家阶段日期 2003.10.9
[71] 专利权人 国际商业机器公司
地址 美国纽约
[72] 发明人 T·蔡佛莱斯 S·马斯特里安尼
A·莫海因德拉
审查员 袁文婷

[74] 专利代理机构 北京市中咨律师事务所
代理人 于 静 李 峥

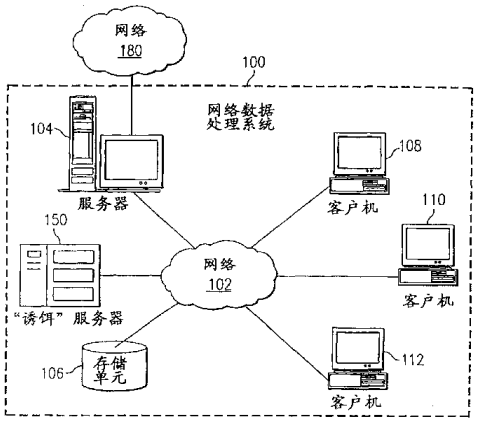
权利要求书 2 页 说明书 12 页 附图 3 页

[54] 发明名称

使用诱饵服务器检测网络上的计算机病毒的方法及装置

[57] 摘要

本发明提供一种方法以及网络数据处理系统，用来识别、定位、以及删除病毒。在一实施例中，网络数据处理系统包含有本地服务器、多个客户端数据处理系统、以及诱饵服务器。诱饵服务器的地址并不向客户端公布。因此，任何访问诱饵服务器的试图都会指出正在尝试访问的客户端上存在有病毒。诱饵服务器会监控本身，并响应来自客户端访问诱饵服务器的尝试，对网络中的所有设备广播有病毒正在进行攻击的指示。诱饵服务器接着会忽略病毒传播的客户端所有进一步的访问请求，直到其接收到该病毒传播客户端已杀毒完成的指示为止，并指示本地服务器从网络中断开该病毒传播客户端。诱饵服务器也会通知本地服务器与/或网络管理者问题所在，以及该病毒传播客户端的标识，允许启动适当的动作以对该病毒传播的客户端进行杀毒。



1. 一种用于识别、定位与删除病毒的网络数据处理系统，其包含有：

一本地服务器；

多个客户端数据处理系统；以及

一具有未公布的网络地址的诱饵服务器，其中

该诱饵服务器会监控自身，并响应该网络数据处理系统中来自一病毒传播系统对该诱饵服务器的试图访问，该诱饵服务器广播有一病毒攻击正在进行的指示至该网络数据处理系统中的所有设备，该诱饵服务器忽略该病毒传播系统所有进一步的访问请求，直到接收到该病毒传播系统已被杀毒的指示为止，并指示该本地服务器从该网络数据处理系统断开与该病毒传播系统的连接。

2. 如权利要求 1 所述的网络数据处理系统，其中该诱饵服务器的地址不向该多个客户端数据处理系统公布。

3. 如权利要求 1 所述的网络数据处理系统，其中该病毒传播系统包含有一个以上数据处理系统。

4. 如权利要求 1 所述的网络数据处理系统，其中该病毒传播系统包含有该本地服务器。

5. 如权利要求 1 所述的网络数据处理系统，其中该病毒传播系统包含有客户端数据处理系统。

6. 如权利要求 1 所述的网络数据处理系统，其中来自该病毒传播系统访问该诱饵服务器的试图包含有对该诱饵服务器进行写入的试图。

7. 如权利要求 1 所述的网络数据处理系统，其中该病毒是蠕虫程序。

8. 如权利要求 1 所述的网络数据处理系统，其中该病毒是特洛伊木马。

9. 如权利要求 1 所述的网络数据处理系统，其中该网络数据处理系统被配置为一旦该病毒传播系统已被杀毒，则允许该病毒传播系统重新连接至该网络数据处理系统。

10. 一种用于检测计算机病毒的存在的方法，该方法包含有：

在一诱饵服务器上接收在该诱饵服务器上执行一功能的请求，其中该诱饵服务器具有未公布的网络地址并且禁止用户对该诱饵服务器的访问；

识别从其发出请求的病毒传播系统；

警告本地服务器，有病毒攻击正在进行，并报出该病毒传播系统的标识；以及

指示该本地服务器从网络断开该病毒传播系统。

11. 如权利要求 10 所述的方法，进一步包含有：

在与该病毒传播系统断开之前，通知该病毒传播系统其已感染了病毒。

12. 如权利要求 10 所述的方法，还包含有：

接收来自病毒传播系统的重新连接请求；

验证该病毒传播系统已被杀毒，并可重新连接至该网络；以及

重新连接该病毒传播系统至该网络。

13. 一种在诱饵服务器中用来识别计算机病毒的存在的方法，其中该诱饵服务器具有未公布的网络地址并且禁止客户机对该诱饵服务器的访问，该方法包含有：

监控该诱饵服务器中的文件；以及

响应该诱饵服务器中一个或多个文件的变化，通知本地服务器有病毒攻击正在进行中。

14. 如权利要求 13 所述的方法，其中该一个或多个文件的变化包含有一个或多个文件的字节大小的变化。

15. 如权利要求 13 所述的方法，其中该一个或多个文件的变化包含有丢失或被删除文件的其中之一。

16. 一种在诱饵服务器中用来识别计算机病毒的存在的方法，其中该诱饵服务器具有未公布的网络地址并且禁止网络用户对该诱饵服务器的访问，该方法包含有：

监控来自网络的试图在该诱饵服务器上执行一功能的请求；

响应检测到一功能请求，通知本地服务器有病毒攻击正在进行中。

使用诱饵服务器检测网络上的计算机病毒的方法及装置

相关申请的交叉参考

本申请涉及 2001 年 2 月 20 日提交的共同未决的美国专利申请 No. 09/789,867 (IBM 文档号 No. YOR920010016US1)，标题为“用来为检测、通知与消除计算机病毒提供商业服务的方法与装置”。上述共同转让及共同未决的美国专利申请的内容在此引入作为参考。

技术领域

本发明涉及一种利用杂收系统提供商业服务以识别网络上计算机病毒的来源的方法与装置。

背景技术

计算机病毒的检测是一种为本领域技术人员所熟知的技术。有几家大型公司从事病毒检测与消除的行业，包括有赛门铁克(Symantec)、McAffee、Shiva 以及英特尔(Intel)。其中有些产品，尤其是赛门铁克，提供软件的企业版，用来在企业内部网上进行管理和使用。在此配置中，病毒检测客户端软件被安装在各客户端计算机上，且病毒检测器会以特定时间间隔执行，以检查客户端机器上的病毒。如果检测到病毒，客户端程序会通知用户已检测到病毒，并采取自动措施，或提示用户根据管理设定来处理。

当检测到病毒时，一般会指示用户隔离感染的文件，从目前使用的系统上将其移除。一旦文件被隔离，用户便可以再次开始使用该系统。接着会指示用户与系统管理者或 IT 部门联系，以警告其病毒的存在。

此策略的问题是对系统的重大损害可能在检测到该病毒之前就已经发

生了。某些称为蠕虫程序(worm)〔Syman 1〕的病毒能够在被检测到之前摧毁几百个甚至几千个文件。更糟的是，到客户端机器检测到病毒时，病毒可能已经在该网络的另一台机器上或在网络共享资源上进行了自我繁殖。病毒可以从网络共享资源开始删除文件，并自我繁殖到其它用户系统上。找到病毒的来源并将其在网络上的踪迹移除，通常需要将网络服务器关闭，网络共享资源移除，且各客户端机器要在与网络断开时完成杀毒。

为了确保病毒已完全清除，需要了解病毒从哪里产生，如此才能对特定机器进行彻底地杀毒。然而，这是很难决定的，尤其是在大型企业网络中，用户可能没有安装防病毒软件，或是其拨号进入网络，无意识地将病毒传入网络，然后便注销了。如果网络已完成杀毒，则病毒传播者重新连接时会再次感染网络。识别病毒传播系统，以避免重新感染的发生是很重要的。

在大部分的情况中，病毒传播者在无意识的情况下传播病毒。有一类称为“蠕虫程序”的病毒会删除文件或将文件长度设定为零，使其完全没用。蠕虫程序通常无法被防火墙软件或过滤器识别出，并会如同一般可执行图像或脚本文件一样到达用户机器。当用户点击此文件时，其会立刻自我繁殖，并寻找网络上的新系统作为蠕虫程序的自愿主机。当其找到自愿主机时，其会自我安装并再次执行，寻找另一自愿主机。这些蠕虫程序需要自愿且杂收的主机，提供其特权需求以达成其恶意的行为。它们会在网络上寻找对计算机或共享资源具有写入访问权的系统，然后使用该能力移除其它系统上的文件。

在大部分的网络中，系统访问作为共享介质的某些类型的共享存储器，也许是另一台计算机的硬盘是很平常的。这称为共享或网络共享，其允许用户很容易共享位于单一位置中的信息、程序、文件与文档。需要访问共享资源的各个系统具有系统管理者或网络服务器的策略许可的访问权。没有共享资源的访问权的系统无法读、写共享资源。读写访问权可以分别授与有权访问共享资源的各系统。

就能够复制到其它系统的病毒来说，很可能病毒在检测到之前便已复

制。在此情况中，对当前的系统进行杀毒已于事无补，由于病毒很快会自身复制回当前系统。为了有效地对邻近的机器进行杀毒，各机器必须从网络断开、杀毒、然后只在各网络客户端均已检查完成且杀毒完成后才连回网络上。必须找到并消除蠕虫程序的来源，否则再次感染的危险性相当高。

这可能是很长的过程，且对于初学用户或管理者来说是很难实现的。虽然大部分具有大型网络的公司具有防止下载潜在有害内容的策略，但对于其员工经验不足的小型公司，更可能会下载潜在的有害内容。

因此，必须要有一种可以检测、定位、并消除病毒的方法、系统、与计算机程序产品，而不需要管理者有很高技术。

发明内容

本发明提供一种方法、计算机程序产品、以及网络数据处理系统，用来识别、定位、以及删除病毒。在一实施例中，网络数据处理系统包含有本地服务器、多个客户端数据处理系统、以及诱饵服务器。诱饵服务器的地址并不向客户端公布。因此，任何访问诱饵服务器的尝试会指出正在尝试访问的客户端上存在有病毒。诱饵服务器会对自身进行监控，并响应来自客户端访问诱饵服务器的尝试，向网络中的所有设备广播有病毒正在进行攻击的指示。诱饵服务器接着会忽略该传播病毒的客户端的所有进一步的访问请求，直到其接收到该传播病毒的客户端已完成杀毒的指示为止，并引导本地服务器从网络中断开该传播病毒的客户端。诱饵服务器也会通知本地服务器与/或网络管理者问题所在，以及该传播病毒的客户端的标识，允许启动适当的动作以对传播病毒的客户端进行杀毒。

根据本发明的一个方面，提供了一种用于识别、定位与删除病毒的网络数据处理系统，其包含有：一本地服务器；多个客户端数据处理系统；以及一具有未公布的网络地址的诱饵服务器，其中该诱饵服务器会监控自身，并响应该网络数据处理系统中来自一病毒传播系统对该诱饵服务器的试图访问，该诱饵服务器广播有一病毒攻击正在进行的指示至该网络数据处理系统中的所有设备，该诱饵服务器忽略该病毒传播系统所有进一步的

访问请求，直到接收到该病毒传播系统已被杀毒的指示为止，并指示该本地服务器从该网络数据处理系统断开与该病毒传播系统的连接。

根据本发明的再一个方面，提供了一种用于检测计算机病毒的存在的方法，该方法包含有：

在一诱饵服务器上接收在该诱饵服务器上执行一功能的请求，其中该诱饵服务器具有未公布的网络地址并且禁止用户对该诱饵服务器的访问；

识别从其发出请求的病毒传播系统；

警告本地服务器，有病毒攻击正在进行，并报出该病毒传播系统的标识；以及

指示该本地服务器从网络断开该病毒传播系统。

根据本发明的又一个方面，提供了一种在诱饵服务器中用来识别计算机病毒的存在的方法，其中该诱饵服务器具有未公布的网络地址并且禁止客户机对该诱饵服务器的访问，该方法包含有：

监控该诱饵服务器中的文件；以及

响应该诱饵服务器中一个或多个文件的变化，通知本地服务器有病毒攻击正在进行中。

根据本发明的另一个方面，提供了一种在诱饵服务器中用来识别计算机病毒的存在的方法，其中该诱饵服务器具有未公布的网络地址并且禁止网络用户对该诱饵服务器的访问，该方法包含有：

监控来自网络的试图在该诱饵服务器上执行一功能的请求；

响应检测到一功能请求，通知本地服务器有病毒攻击正在进行中。

附图说明

本发明的新颖性陈述于所附权利要求中。然而，通过参考下面结合附图的对示例范性的实施例的详细说明，将会对使用模式、其他的目的与其优点有更好的理解，其中：

图 1 是描述可实施本发明的数据处理系统的网络的图示表示；

图 2 是描述根据本发明以服务器方式实施的数据处理系统的方块图；

图 3 是描述根据本发明以客户端方式实施的数据处理系统的方块图；

图 4 是描述根据本发明用来在诱饵服务器上执行以检测、定位与消除计算机病毒的程序流程与程序功能；以及

图 5 是描述根据本发明可在客户端实现的用来检测病毒存在的程序流程与程序功能。

具体实施方式

现在参照附图，图 1 描述了可实施本发明的数据处理系统的网络。网络数据处理系统 100 为计算机网络，在其中可实施本发明。网络数据处理系统 100 含有网络 102，其是用来为网络数据处理系统 100 中互相连接的各种设备和计算机提供通信链路的媒体。网络 102 可包含如有线、无线通信链路、或光纤电缆等连接。

在该描述的范例中，服务器 104 与储存单元 106 连接到网络 102。除此之外，客户机 108、110 与 112 也连接到网络 102，还有诱饵服务器 150 也连接到网络 102。举例来说，这些客户机 108、110 与 112 可为个人计算机或网络计算机。在描述的范例中，服务器 104 为客户机 108-112 提供数据，如启动文件、操作系统映像、以及应用程序。客户机 108、110 与 112 为服务器 104 的客户机。网络数据处理系统 100 可包含其它的服务器、客户机以及其它未显示的设备。在该描述的范例中，网络数据处理系统 100 为企业内部网络(intranet)、局域网络(LAN)或其它类型的专用网络，如可由公司或学校利用的网络。网络 102 代表使用一组通信协议，如 TCP/IP 协议族以与另一网络或网关通信的网络和网关的集合。服务器 104 还提供网络数据处理系统 100 与外部网络 180 之间的连接，外部网络 180 例如可为因特网 (Internet)。

如果以因特网实施，外部网络 180 代表使用 TCP/IP 协议族以与另一网络或网关通信的世界范围内的网络与网关的集合。因特网的核心为主节点或宿主计算机之间的高速数据通信线路的主干，包含有数千个传送数据

与信息的商业、政府、教育与其它计算机系统。

称为“诱饵服务器”150 的特殊服务器安装于网络 102 上，做为网络蠕虫程序病毒的杂收主机。如这里所使用的，病毒这个名词包含有病毒、蠕虫程序、特洛伊木马、以及任何其它类型的设计来干扰数据处理系统或网络的正常操作的有害程序。诱饵服务器 150 被配置成利用安全监控软件来监控所有网络与登录到其本身的通信业务。诱饵服务器的机器名称或 IP 地址并不公布，且没有用户被允许登录到服务器 150 上。当网络登录请求被发送到诱饵服务器 150 时，由于该请求并非预期的，且来自网络 102 中，所以诱饵服务器 150 可断定该请求来自蠕虫程序病毒，真正试图从被感染的机器自我复制到该诱饵服务器 150。

当病毒从客户端计算机，如 108-112 开始传播时，其会快速在网络上定位具有对其他远程文件系统或网络共享资源有写入访问权的杂收系统。病毒会试图自我复制到该诱饵服务器 150，但是诱饵服务器 150 中的监控软件套件会检测到感染的系统对诱饵服务器 150 写入，并诱捕数据。诱饵服务器 150 会立即通知服务器 104 与病毒传播系统中断连接，并拒绝病毒传播系统接下来登录或连接到网络 102 的所有试图。服务器 104 接着会以业务事件通知远程管理者，并经由电子邮件与/或寻呼机通知系统管理员。

作为附加的预防措施，诱饵服务器 150 会继续监控诱饵服务器文件的情况，继续验证其大小与有效性。如果诱饵服务器检测到其中一个诱饵服务器 150 文件的大小被改变或不再存在，诱饵服务器通过向本地服务器 104 发送通知其已检测到病毒，本地服务器 104 移除所有连接并为其自身及网络上其它计算机与共享资源启动杀毒程序。虽然诱饵服务器 150 不可能总在某些初始损害造成之前捕获病毒来源，但其会在非常短时间内捕获病毒传播者以将损害降到最低。

因此，本发明对此问题提供自动解决方案，提供一组硬件与软件组件，其执行辨识驻留于网络上的计算机病毒的来源的任务，而不需要网络管理者或技术人员有很高技术。此自动功能除了增加诱饵服务器外，还可以通过安装于网络服务器 102 与客户端计算机 108-112 上的软件提供，或作为

用户可报名参加的商业服务提供。

如果由诱饵服务器 150 或客户端杀毒软件检测到病毒，且病毒为蠕虫程序，则服务器必须找出病毒来源，并确保产生病毒的机器在被许可重新连接至网络 102 或共享资源之前已完成杀毒。

如果本发明作为商业服务来提供，诱饵服务器 150 通过发送“检测到病毒”业务事件，并发送含有检测到的病毒类型、检测到的含有病毒的客户机名称、以及对系统进行杀毒所采取的步骤的信息的电子邮件消息给远程管理者，来立即通知远程管理者。诱饵服务器 150 也可以呼叫技术人员，启动技术支持的呼叫电话。在接收通知之后，管理者事件路由选择系统会接着产生其它的业务事件、调度对客户的现场（on-site）服务呼叫或电话呼叫，呼叫技术人员，或在最糟的情况下，甚至关闭本地服务器与/或局域网络。

为了对病毒传播计算机定位，如上所述，诱饵服务器 150 被安装于网络 150 上，作为蠕虫程序病毒的“诱饵”与吸引物。这类病毒，如熟知的蠕虫程序，通过轮询网络，来寻找对系统共享资源具有写入能力的计算机来容留该病毒。该病毒会使用各种的技巧找出网络服务器，包括 NETBIOS 广播。利用 NETBIOS 通信协议，病毒会找出网络上具有对其他计算机或网络共享资源有写入访问权的服务器的位置。接着其会自我复制到该服务器、自我安装为一个服务，并在每次操作系统启动或用户登录时开始该服务。一旦执行，该病毒会开始删除本地文件、远程文件和网络共享资源上的文件。若没有立即干涉，病毒会每分钟删除或破坏数千个文件。

诱饵服务器 150 用来监控来自网络 102 上机器的登录与网络请求。由于诱饵服务器 150 对于网络 102 的用户来说是未知的，所以曾试图登录诱饵服务器 150 或经由网络 102 向其发送数据的系统只有病毒本身。诱饵服务器 150 具有激活的安全监控功能，并监控所有网络与安全性请求。诱饵服务器 150 尽可能的开放，具有对单独的公共网络共享资源，其实际上为本地磁盘的写入权。

安装于网络共享资源的通常是蠕虫程序病毒的目标的文件，

如.DOC、.PPT、.H、.CPP、.C、.ASM 以及.XLS。一旦登录请求到达诱饵服务器机器 150，诱饵服务器 150 会立刻切断与请求计算机的连接，并产生业务事件给远程管理服务器，以及发送优先电子邮件消息给系统管理者。各消息包含有如时间、日期、IP 地址与该病毒传播机器名称，以及病毒正试图使用的用户 ID 与密码的信息。诱饵服务器 150 接着会在整个网络内广播有病毒正在进行病毒攻击的消息。

如果对共享的资源写入请求到达诱饵服务器 150，会采取相同的措施。同样的，会收集发送机器的 IP 地址、机器名称、病毒类型、以及其它信息，并发送至本地服务器 104 以进行路由选择。允许本发明充分实施的一个条件是病毒“聪明”到足以首先追随最杂收的机器，而较早暴露其自身。

一旦被从网络 102 中移除，该病毒传播机器的登录帐户便会被取消。任何来自产生病毒事件的 IP 地址或机器名称的随后请求都会被忽略，直到认定病毒已从网络移除，且该病毒传播机器已完成杀毒为止。在此时，该病毒传播机器会重新连接至网络 102，且网络的正常操作会继续进行。

图 1 为范例，但并不构成对本发明的结构的限制。

参阅图 2，其描述根据本发明以服务器方式，如图 1 中的“诱饵”服务器 150 或服务器 104，实现的数据处理系统的方块图。数据处理系统 200 可为对称多处理器(SMP)系统，其包含有连接至系统总线 206 的多个处理器 202 与 204。或者，可使用单处理器系统。同样连接至系统总线 206 的有存储器控制器/高速缓存 208，其提供对本地存储器 209 的接口。I/O 总线桥 210 连接至系统总线 206，并提供对 I/O 总线 212 的接口存储器。控制器/高速缓存 208 与 I/O 总线桥 210 可集成在一起，如图所示。

连接至 I/O 总线 212 的外围部件互连(PCI)总线桥 214 提供对 PCI 局部总线 216 的接口。数个调制解调器可连接至 PCI 总线 216。一般的 PCI 总线实施方式会支持四个 PCI 扩展槽或附加连接器。通过附加板连接至 PCI 局部总线 216 的调制解调器 218 和网络适配器 220，可提供到图 1 的网络计算机 108-112 的通信链路。

附加的 PCI 总线桥 222 与 224 为附加的 PCI 总线 226 与 228 提供接口，

从其可支持附加的调制解调器或网络适配器。依此方式，数据处理系统 200 允许连接至多个网络计算机。存储器映射图形适配器 230 与硬盘 232 也可连接至 I/O 总线 212，如图所示，不论是直接或间接。

本领域的普通技术人员将意识到，图 2 中所示的硬件可有不同变化。举例来说，其它的外围设备，如光盘驱动器等，也可用于取代所述硬盘。所描述的范例并不意味着对本发明的系统结构的限定。

例如，图 2 中所述的数据处理系统可为 IBM RISC/System 6000 系统，其为纽约阿蒙市的国际商业机器（IBM）公司的产品，其运行高级交互执行(AIX)操作系统。

现在参阅图 3，其描述根据本发明以客户机方式实现的数据处理系统的方块图。数据处理系统 300 为客户端计算机的范例，举例来说，其可为图 1 中任一客户机 102-110。数据处理系统 300 使用外围部件互连(PCI)局部总线结构。虽然所述的范例使用 PCI 总线，但也可使用其它如图形加速端口(AGP)与工业标准结构(ISA)的总线结构。处理器 302 与主存储器 304 通过 PCI 桥 308 连接于 PCI 局部总线 306。PCI 桥 308 也可以包括用于处理器 302 的集成的存储器控制器与高速缓存。附加的与 PCI 局部总线 306 的连接可通过直接部件互连或通过附加板实现。在所述的范例中，局域网(LAN)适配器 310、SCSI 主机总线适配器 312、以及扩展总线接口 314 藉由直接部件连接被连至 PCI 局部总线 306。相对的，音频适配器 316、图形适配器 318、以及音频/视频适配器 319 藉由插入扩展槽的附加板连接至 PCI 局部总线 306。扩展总线接口 314 为键盘与鼠标适配器 320、调制解调器 322、以及附加存储器 324 提供连接。小型计算机系统接口(SCSI)主机总线适配器 312 为硬盘机 326、磁带机 328、以及光盘驱动器 330 提供连接。典型的 PCI 局部总线实现方式支持三个或四个 PCI 扩展槽或附加连接器。

运行于处理器 302 上的操作系统用来对图 3 的数据处理系统 300 中各种部件进行协调并提供控制。此操作系统可为可购买到的操作系统，如 Windows 2000，其为微软公司发行。面向对象的程序设计系统，如 Java，可与操作系统一起执行，并提供来自在数据处理系统 300 上执行的 Java

程序或应用程序呼叫对操作系统的调用。“Java”为 Sun 微系统公司(Sun Microsystems, Inc.)的注册商标。操作系统、面向对象的程序设计系统以及应用程序或程序的指令位于存储设备上，如硬盘机 326，并可被加载到主存储器 304 中，以由处理器 302 执行。

本领域的普通技术人员会理解图 3 中的硬件可以视具体实现而异。其它的内部硬件或外围设备，如闪速 ROM(或等效的非易失性存储器)或光盘驱动器等类似设备，可附加或代替图 3 中所述的硬件。同样的，本发明的连接可用于多处理器数据处理系统。

作为另一个例子，数据处理系统 300 可为独立系统，不需依赖某类型的网络通信接口便可启动，不论数据处理系统 300 是否包含有某类型的网络通信接口。再作为另一个例子，数据处理系统 300 可为个人数字助理(PDA)设备，其含有 ROM 与/或闪速 ROM，以提供用于存储操作系统文件与/或用户产生的数据的非易失性存储器。

图 3 所述的范例与上述范例并非意味对结构的限制。举例来说，除了采用 PDA 的形式之外，数据处理系统 300 也可为笔记本型计算机或掌上型计算机。数据处理系统 300 也可以是 kiosk 或万维网装置。

现在请参阅图 4，其描述根据本发明用来在诱饵服务器上执行以检测、定位与消除计算机病毒的方法流程与程序功能。举例来说，过程 400 可实现于图 1 中的诱饵服务器 150 上。开始，在 402 开启诱饵服务器，并在 404 开始具有病毒监控功能的正常操作。如果发生断电事件(步骤 406)，过程会结束。然而，除非诱饵服务器关闭，否则诱饵服务器会持续自我监控，以判断是否检测到病毒事件(步骤 408)。

举例来说，诱饵服务器会藉由观察对诱饵服务器的试图访问，例如试图写入数据到诱饵服务器中，来检测病毒事件。由于诱饵服务器的地址并没有公布，且不为网络执行其它的功能，所以任何试图访问诱饵服务器都很可疑，且表示网络上存在病毒。作为附加的预防措施，诱饵服务器会持续监控诱饵服务器文件的情况，持续验证其大小与有效性。如果诱饵服务器检测到其中一个诱饵服务器文件的大小改变或不再存在，这可以表示存

在病毒。有病毒试图访问诱饵服务器的病毒传播计算机的位置，会通过记录请求访问诱饵服务器的计算机地址被识别出来。

如果没有检测到病毒事件，诱饵服务器会继续正常操作与病毒监控(步骤 404)。如果检测到病毒事件，诱饵服务器会发送消息给远程管理者(步骤 410)，通知远程管理者检测到病毒，以及网络中产生病毒的计算机标识。诱饵服务器接着会去除对病毒传播计算机的连接与共享(步骤 412)，同时指示病毒传播计算机进行杀毒(步骤 414)。

诱饵服务器接着会等待来自病毒传播计算机的重新连接请求(步骤 416)。如果还没有接收到重新连接请求(步骤 418)，诱饵服务器会继续等待(步骤 416)。然而，即使在诱饵服务器正在识别一个产生病毒的病毒传播计算机、通知管理者、断开病毒传播计算机、并等待重新连接请求期间，诱饵服务器也会继续自我监控其它的病毒事件。当接收到重新连接请求时，诱饵服务器会重新连接病毒传播计算机(步骤 420)，并继续正常操作与病毒监控(步骤 404)。

因此，诱饵服务器一般会以相当快的速度检测到并去除病毒，避免对网络的严重损害或中断。此外，藉由确定病毒第一次获准进入网络的计算机的标识，在病毒有时间感染更多网络中计算机前断开计算机并杀毒。

如果病毒从其进入网络的病毒传播计算机为本地服务器，操作方式基本上与客户端计算机相同。诱饵服务器会发送病毒攻击消息给客户机，使其断开并移除连接。本地服务器确保所有连接都已移除，自我杀毒，然后当客户机可用时重新连接至客户机。

现在参阅图 5，其描述根据本发明可在客户机实现的用来检测病毒存在的方法流程与程序功能。举例来说，过程 500 可执行于图 1 中的任何客户机 108-112。开始，计算机开机并连接至网络(步骤 502)。该计算机接着会进入正常操作(步骤 504)。如果发生断电事件(步骤 506)，该过程显然会结束。除非发生断电事件，否则该计算机会持续正常操作并藉由等待来自网络的通知，来判断诱饵服务器是否检测到病毒(步骤 508)。如果没有接收到指示病毒存在于该计算机中的通知，该计算机会继续正常操作(步骤

504)。

如果接收到指示病毒存在于该计算机中的病毒通知，该计算机会藉由呈现消息于显示器或呼叫其所有者或用户的方法，来发送通知给其所有者(步骤510)。该计算机接着会断开与网络的连接(步骤512)，然后自身杀毒(步骤514)。该计算机会自动执行病毒检测与消除程序来自身杀毒，该程序例如是各式各样的可购买到的产品。或者，杀毒过程会需要重要的用户介入，也许是如网络管理员的专业人员的服务。

一旦该计算机完成杀毒，该计算机会发送重新连接至网络的请求(步骤516)，并等待请求被许可。该计算机接着会判断请求是否被许可(步骤518)，且如果没有，则继续等待。如果请求被许可，该计算机会连接至网络，并继续正常操作(步骤504)。

有一点很重要的是要注意以上是在一种完整功能的数据处理系统的背景下描述了本发明，但本领域的普通技术人员应该了解本发明的过程可以计算机可读介质上的指令的形式以及各式各样的形式来发布，且本发明在应用时与用于承载发布的信号承载介质的特定类型无关。计算机可读介质的范例包含有可记录型介质，如软盘、硬盘机、RAM、以及 CD-ROM，以及传输型介质，如数字与模拟通信链路。

此处所呈现的本发明的说明仅用于举例与说明的目的，并非将本发明限制于所公开的形式。很显然的，本领域的普通技术人员可作出许多修改与变化。所选择与描述的实施例仅为了更好地说明本发明的原理、实际应用、以及让其它本领域的普通技术人员理解本发明的不同实施例，而这些实施例具有不同修改以适合特殊用途。

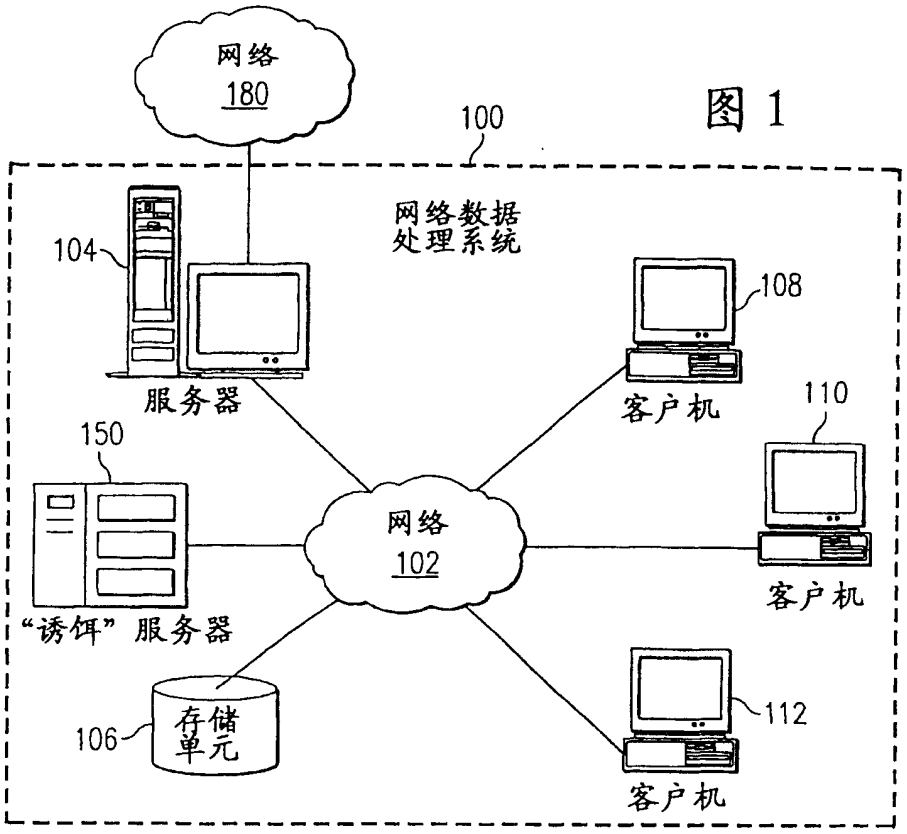

网络
180
100
网络数据
处理系统
104
服务器
108
客户机
110
客户机
150
"诱饵"服务器
网络
102
106
存储
单元
112
客户机

图 1

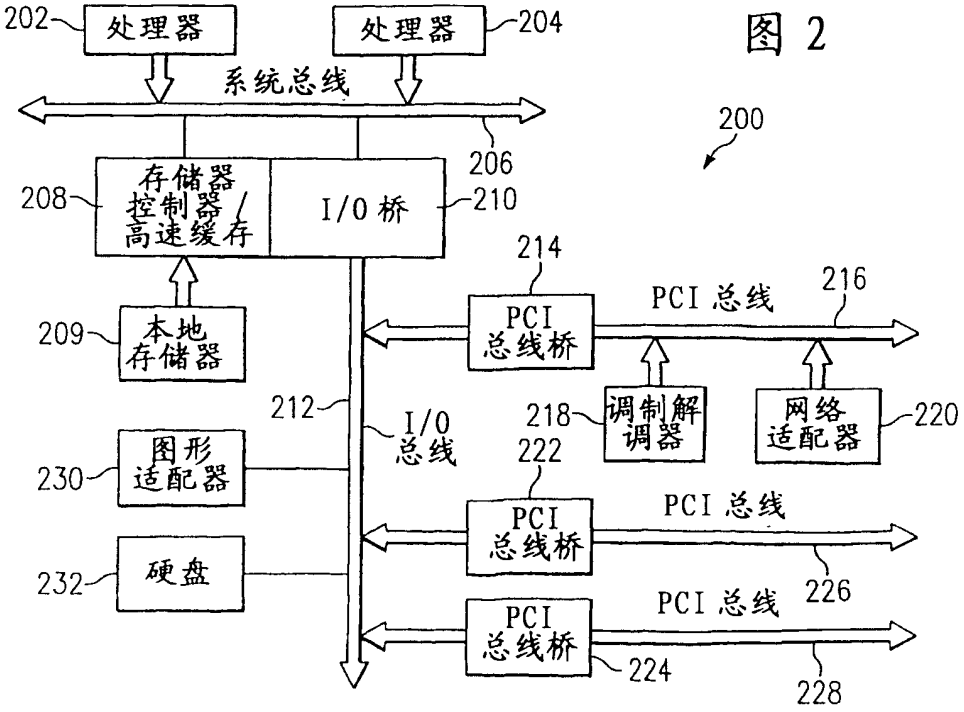

202
处理器
处理器
204
系统总线
206
200
208
存储器
控制器/
高速缓存
I/O 桥
210
214
PCI
总线桥
PCI 总线
216
209
本地
存储器
212
I/O
总线
218
调制解
调器
网络
适配器
220
222
230
图形
适配器
PCI
总线桥
PCI 总线
232
硬盘
226
PCI
总线桥
PCI 总线
224
228

图 2

图 3

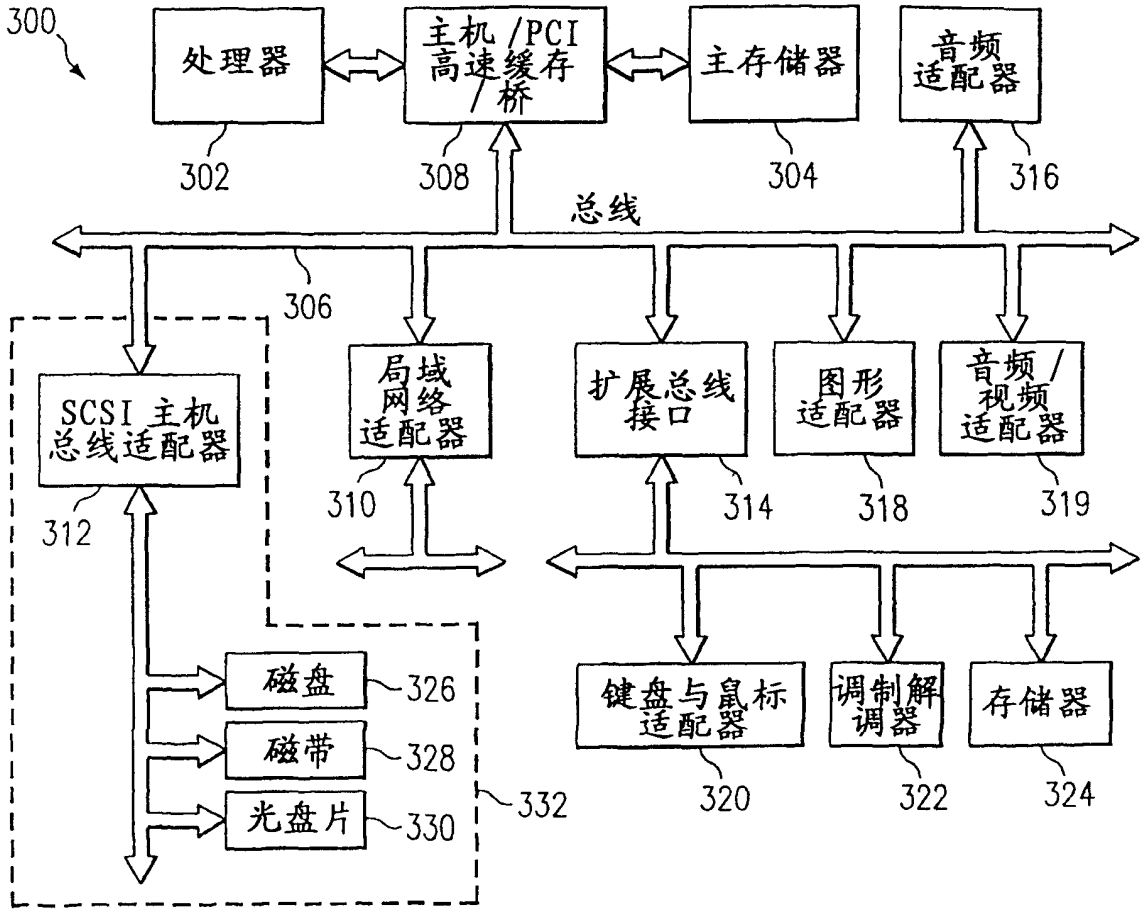
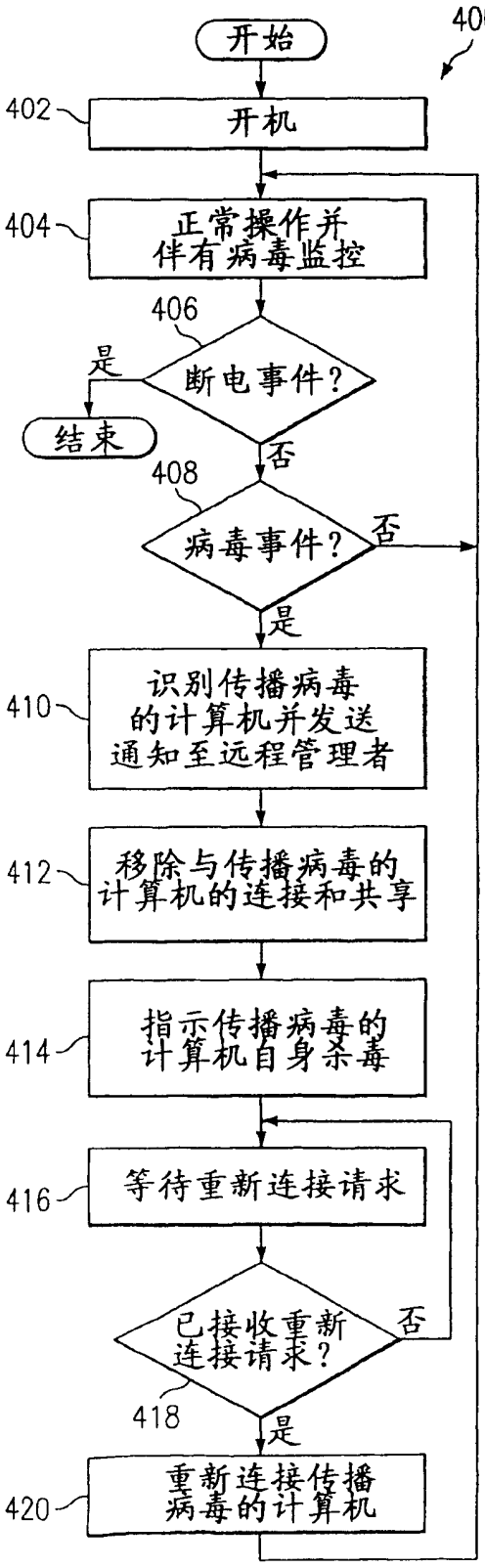

300
处理器
主机/PCI高速缓存/桥
主存储器
音频适配器
302
308
304
316
总线
306
SCSI 主机总线适配器
局域网络适配器
扩展总线接口
图形适配器
音频/视频适配器
312
310
314
318
319
磁盘
326
磁带
328
光盘片
330
332
键盘与鼠标适配器
调制解调器
存储器
320
322
324

图 4 服务器操作



客户端操作 图 5