[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 1/00

[12] 发明专利申请公开说明书

[21] 申请号 02806751.7

[43] 公开日 2004 年 5 月 19 日

[11] 公开号 CN 1498363A

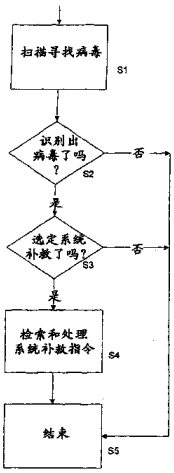
[22] 申请日 2002.3.26 [21] 申请号 02806751.7
[30] 优先权
[32] 2001. 3.30 [33] US [31] 09/823,673
[86] 国际申请 PCT/US2002/009414 2002.3.26
[87] 国际公布 WO02/079956 英 2002.10.10
[85] 进入国家阶段日期 2003.9.17
[71] 申请人 计算机联合思想公司
地址 美国纽约
[72] 发明人 塔拉斯·马利万处克 莫什·达兹奥弗·罗兹奇尔德
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 郭思宇

权利要求书 3 页 说明书 9 页 附图 3 页

[54] 发明名称 恢复受恶性计算机程序破坏的计算机系统的系统和方法

[57] 摘要

恢复被恶性代码修改的计算机系统的方法。该方法扫描计算机系统以发现恶性代码，识别该恶性代码并从数据文件中检索与该恶性代码有关的信息，其中包括至少一个命令用于使计算机系统恢复到受该恶性代码修改之前存在的状态。 这至少一个命令被执行，以把计算机系统恢复到基本上为受该恶性代码修改之前存在的状态。



ISSN1008-4274

1.恢复由恶性代码修改的计算机系统的方法，包含:

扫描计算机系统以发现恶性代码;

识别该恶性代码;

从数据文件中检索与该恶性代码有关的信息，包括至少一个命令用于把该计算机系统恢复为被恶性代码修改之前存在的状态；以及

执行这至少一个命令把该计算机系统恢复到基本上为被恶性代码修改之前存在的状态。

2.根据权利要求1的方法，其中执行至少一个命令的步骤包括读、写和删除数据三个命令之一。

3.根据权利要求1的方法，其中执行至少一个命令的步骤包括重命名和删除文件二个命令中的至少一个。

4.根据权利要求1的方法，其中该恶性代码修改至少一个文件，所述方法包含:

从修改过的文件中读出第二个文件的文件名；以及

修改该第二个文件。

5.根据权利要求1的方法，其中该数据文件包含多个数据文件，所提供的每个数据文件用于特定类型的恶性代码，每个数据文件包括至少一个命令，它能用于把计算机系统恢复为受此特定类型恶性代码修改之前存在的状态。

6.一种存储介质，其中包括计算机可执行代码用于恢复由恶性代码修改的计算机系统，该存储介质包含:

用于扫描计算机系统以发现恶性代码的代码;

用于识别该恶性代码的代码;

用于从数据文件中检索与该恶性代码有关的信息的代码，该信息包括至少一个命令用于把计算机系统恢复到被该恶性代码修改之前存在的状态；以及

用于执行该至少一个命令的代码，以将该计算机系统恢复到基本上

为被恶性代码修改之前存在的状态。

7.根据权利要求6的存储介质，其中用于执行至少一个命令的代码包括能实现读、写和删除数据中至少一个的代码。

8.根据权利要求6的存储介质，其中用于执行至少一个命令的代码包括能实现重命名和删除文件中至少一个的代码。

9.根据权利要求6的存储介质，其中该恶性代码修改至少一个文件，所述存储介质进一步包含:

用于从修改过的文件中读出第二个文件的文件名的代码；以及

用于修改这第二个文件的代码。

10.根据权利要求6的存储介质，其中该数据文件包含多个数据文件，提供每个数据文件用于特定类型的恶性代码，每个数据文件包括至少一个命令，它能用于把计算机系统恢复为受此特定类型恶性代码修改之前存在的状态。

11.在传输介质中实现的计算机数据信号，其中包括计算机可执行指令用于恢复被恶性代码修改的计算机系统，该计算机数据信号包含:

用于扫描计算机系统以发现恶性代码的数据信号部分;

用于识别该恶性代码的数据信号部分;

用于从数据文件中检索与该恶性代码有关的信息的数据信号部分，该信息中包括至少一个命令用于使计算机系统恢复为被该恶性代码修改之前存在的状态；以及

用于执行该至少一个命令的数据信号部分，以将计算机系统恢复到基本上为被恶性代码修改之前存在的状态。

12.根据权利要求11的计算机数据信号，其中用于执行至少一个命令的数据信号部分执行读、写和删除数据中的至少一个。

13.根据权利要求11的计算机数据信号，其中用于执行至少一个命令的数据信号部分实现重命名和删除文件中的至少一个。

14.根据权利要求11的计算机数据信号，其中该恶性代码修改至少一个文件，所述计算机数据信号进一步包含:

用于从修改过的文件中读出第二个文件的文件名的数据信号部分;

以及

用于修改这第二个文件的数据信号部分。

15.根据权利要求11的计算机数据信号，其中该数据文件包含多个数据文件，提供每个数据文件用于特定类型的恶性代码，每个数据文件包括至少一个命令，它能用于把计算机系统恢复为被此特定类型恶性代码修改之前存在的状态。

16.一个被编程的计算机系统，其中包括用于恢复被恶性代码修改的计算机系统的程序，所述被编程的计算机系统包含:

用于扫描计算机系统以发现恶性代码的装置;

用于识别该恶性代码的装置;

用于从数据文件中检索与该恶性代码有关的信息的装置，该信息包括至少一个命令用于把计算机系统恢复到被该恶性代码修改之前存在的状态; 以及

用于执行这至少一个命令的装置，以将计算机系统恢复基本上为被恶生代码修改之前存在的状态。

17.根据权利要求16被编程的计算机系统，其中用于执行至少一个命令的装置包括实现读、写和删除数据中至少一个的装置。

18.根据权利要求16被编程的计算机系统，其中用于执行至少一个命令的装置包括实现重命名和删除文件中至少一个的装置。

19.根据权利要求16被编程的计算机系统，其中该恶性代码修改至少一个文件，所述系统进一步包含:

用于从修改过的文件中读出第二个文件的文件名的装置; 以及

用于修改这第二个文件的装置。

20.根据权利要求16被编程的计算机系统，其中该数据文件包含多个数据文件，提供每个数据文件用于特定类型的恶性代码，每个数据文件包括至少一个命令，它能用于把计算机系统恢复为被此特定类型恶性代码修改之前存在的状态。

恢复受恶性计算机程序破坏的计算机系统的系统和方法

技术领域

本公开内容涉及检测和去掉计算机程序，更具体地说，本公开内容涉及恢复受恶意计算机程序破坏的计算机系统。

背景技术

计算机病毒是现今计算中的主要问题。一般地说，计算机病毒是一个程序（或某一代码单元，例如计算机响应的指令，如代码块、代码元素或代码段），它可以附着在其他程序和/或对象上，可以复制它本身，和/或可以在计算机系统上采取未经请求的或恶性的行动。尽管这里的描述涉及计算机病毒，但本公开内容可以适用于能修改计算机资源的一个或多个部分的任何类型恶性代码。从计算机病毒中恢复的一种措施可以包括去掉该计算机病毒。这可以包括禁止受感染对象中的病毒，该对象可以是例如文件、存储区、或存储介质中的引导扇区。然而，人们还已经看到新近出现的计算机病毒除了原有的受感染对象外，还通过删除或重命名文件、管理系统注册和初始化和/或创建不希望的服务和过程等装置来管理对象。

已经看到，计算机病毒可以对计算机系统上现已存在的文件重新命名和/或以一个不同的文件代替它，造成计算机以不希望的方式操作。此外，病毒可以修改现有的系统配置文件，同时把它自己嵌入计算机系统。能做这两种事情的计算机病毒的一个实例是“Happy 99.Worm（快乐 99.蠕虫）”病毒。这一特定类型的病毒作为一个电子邮件消息的附件传播，并使受感染的计算机把该病毒的副本附加在向外发出的电子邮件消息上。这类病毒还可以在计算机硬驱动器上放置一个或多个隐藏文件和/或改变 Windows 的注册文件。例如，“快乐 99.蠕虫”病毒把文件

“Wsock32.dll”重命名为“Wsock32.ska”并将原“Wsock32.dll”文件替换为它的新版本。“快乐 99.蠕虫”病毒还在计算机系统上创建若干其他文件，包括“Ska.exe”，并在 Windows 注册文件中添加一行，指示该计算机在启动时运行“Ska.exe”文件。

只是简单地禁止或去掉病毒代码而不去恢复或正确地重命名文件等和/或去掉不希望的服务或过程，将不能有效地恢复该计算系统。就是说，恢复已被病毒附着的对象可能并不总是足够的，特别是如果已由计算机病毒创建或修改了若干其他对象的话。

因为每个病毒可能影响一个计算机系统的不同部分，特定的处理是需要的，而且可能需要对任何数量的对象进行若干个与操作系统有关的操作。所以，需要一种对受感染计算机系统的完全补救，以恢复所有受影响的对象。

发明内容

本公开内容涉及一种恢复被恶性代码修改的计算机系统的方法，包含扫描计算机系统以发现恶性代码，识别该恶性代码，从数据文件中检索与该恶性代码有关的信息，其中包括至少一个命令用于使计算机系统恢复到受该恶性代码修改之前存在的状态，以及执行这至少一个命令以把计算机系统恢复到基本上为受该恶性代码修改之前存在的状态。执行这至少一个命令的步骤可以包括读、写和删除数据三种之一。执行这至少一个命令的步骤还可以包括重命名和删除对象二者中的至少一个。

本公开内容还涉及存储介质，其中包括计算可执行代码用于恢复被恶性代码修改的计算机系统，该存储介质中包含扫描计算机系统以发现恶性代码的代码，识别该恶性代码的代码，从数据文件中检索与该恶性代码有关的信息的代码，该信息中包括至少一个用于使计算机系统恢复为受该恶性代码修改之前状态的命令，以及执行这至少一个命令以把计算机系统恢复到基本上是受该恶性代码修改之前存在的状态的代码。

本公开内容还涉及在传输介质中实现的计算机数据信号，其中包括计算机可执行指令用恢复被恶性代码修改的计算机系统，该计算机数据

信号包含扫描计算机系统以发现恶性代码的数据信号部分，识别该恶性代码的数据信号部分，从数据文件中检索与该恶性代码有关的信息的数据信号部分，该信息中包括至少一个用于使计算机系统恢复为受该恶性代码修改之前状态的命令，以及执行这至少一个命令以把计算机系统恢复到基本是受该恶性代码修改之前存在的状态的数据信号部分。

附图说明

通过参考下文中的详细描述并结合附图加以考虑，本公开内容将得到更好的理解，因此人们将更容易得到对本公开内容以及它的许多伴随的优点的更完全的理解，这些附图是:

图 1 显示一个示例计算机系统，对它可以应用根据本公开内容的一个实施例的系统和方法以恢复受恶性代码破坏的计算机系统。

图 2 显示一个过程流程图，该过程用于根据本公开内容的一个实施例恢复受恶性代码破坏的计算机系统。

图 3A 显示一个数据库，其中包括针对病毒的恢复命令数据文件；以及

图 3B 显示根据本公开内容的一个实施例来自恢复命令数据文件之一的命令。

具体实施方式

在描述图中所示本公开内容优选实施例时，为了清楚而使用特定的术语。然而，本公开内容不限于如此选择的特定术语。应该理解，每个特定术语包括以类似方式操作的所有的技术等效物。

图 1 是一个计算机系统 102 的实例方框图，本公开内容的恢复系统和方法可以应用于该系统。计算机系统 102 可以是能运行检测计算机病毒的软件的标准 PC、膝上计算机、主机等。计算机系统 102 还能运行根据本公开内容的软件以把计算机系统 102 恢复到在该系统中放入病毒之前存在的状态。如图所示，计算机系统 102 可以包括中央处理单元(CPU) 2、存储器 4、时钟电路 6、打印机接口 8、显示单元 10、LAN 数据传输

控制器 12、LAN 接口 14、网络控制器 16、内部总线 18 以及一个或多个输入设备 20，如键盘和鼠标器。当然，计算机系统 102 可以不包括所述每个部件和/或可以包括未示出的附加部件。

CPU2 控制系统 102 的操作，并能运行存储在存储器 4 中的应用。存储器 4 可以包括例如 RAM、ROM、可卸 CDROM、DVD 等。存储器 4 还可以存储为执行应用所必须的各类数据。以及为 CPU 使用而保留的工作区。时钟电路 6 可以包括一个电路以产生指示当前时间的信息，而且可以被编程为能递减计数预先确定的或设置的时间量。

LAN 接口 14 允许网络（未画出）（它可以是 LAN）和 LAN 数据传输控制器 12 之间的通信。LAN 数据传输控制器 12 使用预先确定的协议组与该网络上的其他设备交换信息和数据。计算机系统 102 还可以能够经由路由器（未画出）与其他网络通信。计算机系统 102 还可以能够使用网络控制器 16 经由公共交换电话网（PSTN）与其他设备通信。计算机系统 102 还可以访问 WAN（广域网）和例如因特网。内部总线 18 可能实际上由多个总线构成，它允许与其相连的每个部件之间的通信。

计算机系统 102 能利用为认识和识别计算机病毒而设计的一种或多种扫描程序来扫描存储器 4 的一个或多个部分以发现计算机病毒。例如，扫描程序可以检测病毒的已知签名，或可以使用启发式的逻辑来检测病毒。

本公开内容的系统和方法可以作为计算机可执行代码来实现，该代码本身被存储在存储器 4 或存储在其他地方并可由计算机系统 102 访问。该计算机可执行代码可以被存储在与计算机系统 102 通信的远程站点并在那里执行，以远程修理/恢复计算机系统 102。这里描述的方法和系统能够恢复受计算机病毒破坏的计算机系统。根据一个实施例，多个针对病毒的恢复命令数据文件（见图 3A）可由计算机系统 102 访问。如图 3B 中所示，每个恢复命令数据文件包含命令或系统补救指令，用于恢复受特定病毒破坏的被感染计算机系统。因为一些病毒可能以不同的方式影响不同的操作系统，这些命令可以根据不同操作系统的要求进行分类。这些命令用于恢复文件名、系统注册设置和/或其他操作系统特性，它们

已知被特定的计算机病毒改变或破坏。

可以存储在恢复命令数据文化中并由系统使用的命令实例包括如下命令：复制、删除和重命名文件；读、写、创建和删除 Windows 注册关键字；管理 INI 文件；识别和终止系统存储器中的有效过程；启动外部程序；管理串类型变量，管理数值类型变量；控制补救指令流（取决于运行时间输入参数）；以及控制补救指令流（取决于目标操作系统）。当然，需要时可以提供其他命令，这取决于特定病毒对系统造成的改变。使用上面列出的一个或多个命令，有可能恢复受病毒破坏的计算机系统。

参考图 2，计算机系统 102 使用一个或多个扫描程序扫描至少是一部分存储器 4（步骤 S1）以发现病毒。然后确定是否发现了病毒（步骤 S2）。如果不存在病毒（否，步骤 S2）则过程退出（步骤 S5）。如果存在病毒且已被识别出（是，步骤 S2）则确定是否已选系统补救选项（步骤 S3）。例如，这能是图形用户界面（GUI）形式，它在开始扫描过程之前提示用户选择如果检测到病毒的话是否要应用本公开内容的系统补救特性。如果未曾选定系统补救选项（否，步骤 S3）则过程退出（步骤 S5）。如果已选定系统补救选项（是，步骤 S3），则检索与识别出的病毒对应的恢复命令数据文件。恢复命令数据文件包含系统补救命令，同时把系统恢复到受那个病毒感染之前存在的状态。然后，在恢复命令数据文件中的命令或系统补救指令被检索出来并被处理（步骤 S4）。恢复命令数据文件可以包含特定病毒影响的文件的名称以及为恢复该计算机系统所必须的指令。在命令或系统补救指令已完成之后，完成了的过程退出（步骤 S5）。

作为举例，如果“快乐 99.蠕虫”病毒存在并已被识别出来（是，步骤 S2），而且系统补救选项已被选定（是，步骤 S3），则检索出恢复命令数据文件，它对应于“快乐 99.蠕虫”病毒并含有从“快乐 99.蠕虫”病毒中恢复所使用的系统补救指令。然后这些指令被执行（步骤 S4），以使该计算机恢复到正常操作状态。例如，本方法和系统可以执行“删除文件”命令以删除新创建的“Wsock32.dll”和“Ska.exe”文件以及由病毒创建的任何其他文件。它还可以执行“重命名文件”命令以把“Wsock32.ska”文件重命名回到它的原来名称“Wsock32.dll”。最后，

该方法和系统可以使用“ReadRegKey”和“DeleteRegKey”命令去读和删除由该病毒添加到 Windows 注册文件中的任何关键字和值。这些命令或补救指令可以列入恢复命令文件中，例如以编程代码的形式列入。

为了恢复可能已由计算机病毒管理或破坏的文件，恢复命令数据文件可以还包括“删除文件”、“重命名文件”和/或“复制文件”文件系统命令，用于管理位于该计算机系统上的文件。此外，可以提供“外壳”命令，系统外壳命令可以通过该外壳执行。取决于使用情况，这些命令可以使用一个或多个文件名作为输入参数，并在失败时返回一个错误状态。在要被管理的文件当前被系统使用因而不能被访问时，该文件系统命令将不返回错误状态；相反，该命令将告知该计算机系统必须进行计算机重新启动以释放该文件。一旦该文件被释放，则本方法和系统将执行先前尝试过的文件系统命令。

计算机病毒可以启动在计算机系统上运行的不希望的过程和/或服务。因此，恢复命令数据文件也可以包含过程管理命令，用于停止当前在计算机系统上运行的过程或服务。例如，“杀死过程”命令可用于停止当前在计算机系统上运行一个过程，而“杀死服务”命令可用于停止一个服务并把它从 Windows 注册文件中去掉。

计算机病毒还可以窜改操作系统文件，包括 Windows 注册文件和/或初始化文件。Windows 注册是由两个文件构成的数据库，用于存储 Windows 的设置和选项，包含对该计算机所有硬件、软件、用户以及偏好的信息和设置。Windows 注册文件有层次结构，主分支包含子分支，称作“关键字”，它存储的“值”含有该注册文件中存储的实际信息。某些计算机病毒可以窜改 Windows 注册和初始化文件。例如，在安装过程中，“快乐 99.蠕虫”病毒可以向 Windows 注册文件添加一个带有相应值的关键字，这里该值是在系统启动时要被执行的文件的文件名，从而在每次启动计算机时便启动一个不为用户所知的病毒。因此，为了恢复被这样的计算机病毒破坏的计算机系统，恢复命令数据文件也可以包括读、写和删除位于 Windows 文件（如 Windows 注册和/或初始化（INI）文件，如“System.ini”）内的值。使用的 Windows 注册管理命令可以包括

“ReadRegKey”、“WriteRegKey”和“DelRegKey”，而INI文件管理命令可以包括“ReadINIKey”和“WriteINIKey”。这些命令的命令名、输入参数及功能如下：

ReadRegKey（变量，关键字，值）把位于关键字的值字段中的数据读到一个变量中；

WriteRegKey（关键字，值，变量）把来自一个变量的数据写入一个关键字的值字段中。如果不存在该关键字或值，则创建它们；

DleteRegKey（关键字，值）删除指定关键字的值，或者如果该值参数是空的，则删除整个关键字；

ReadINIKey（变量，INI文件名，段，关键字）读位于特定INI文件内的一个关键字的段字段中的数据；以及

WriteINIKey（INI文件名，段，关键字，变量）把来自一个变量的数据写入位于特定INI文件内的一个关键字的段字段中。如果该变量被置为“NULL（空）”，则该关键字被去掉。

在上述命令中，如果在“读”和“删除”过程中在该计算机系统上不存在关键字或值的输入，以及如果在“写”和“删除”命令中发生写失败事件，则可能产生错误状态。如果一个命令在执行后返回一个错误，如一个错误指出复制一个不存在的文件失败或读一个不存在的Wndows注册关键字，则本方法和系统可以或者忽略该错误或者停止这一补救过程。例如，如果包括一个OnErrorAbort命令，则在发生这第一个错误时将造成该补救过程被放弃，而包括一个OnErrorContinue命令则将在发生一个或多个错误时使补救过程继续下去。本方法和系统默认设置到OnErrorCotinue，从而在发生一个或多个错误时也能继续补救过程。

恢复命令数据文件还可以包括串管理命令用于当串被病毒改变时管理这些串变量。这类命令的实例可以包括StrCpy命令，它把一个源串、宏或常数值复制到一个目的串中。StrCat命令可以把源串、宏或常数值连接到一个目的串上。

恢复命令数据文件可以存储在存储器4中的数据存储区中和/或可由计算机系统102访问的其他存储介质中。例如，恢复命令数据文件可以

存储在通过局域网或因特网连接的单独存储系统上，在那里它们可被直接访问和周期性更新。图 3B 中示出一个恢复命令数据文件的内容举例，该数据文件可用于使计算机系统从“快乐 99.蠕虫”病毒中恢复过来。在“VirusStart”和“RemoveEnd:”之间的代码部分是用于检测病毒和恢复受感染的文件。在恢复命令数据文件中可以提供也可以不提供这部分代码。在“SysCureStart”和“SysCureEnd”之间的代码部分是用于采用这里描述的技术恢复计算机系统。

在计算机系统识别出病毒并访问适当的恢复命令数据文件之后，计算机系统从该数据文件中读出恢复该计算机系统所用命令列表。如图 3B 中所示，SysCureStart 和 SysCureEnd 标记开始和终止数据文件中找到的命令块。根据这一实例，计算机系统首先利用从该数据文件中检索出的关键字和值参数执行 DdlRegKey 命令。该关键字和值参数是针对病毒的，在这一案例中分别是“HK-LOCAL-MACHINE\ Software\ Microsoft\ Windows\Run”和“Virus”。当这个关键字和值被病毒插入到 Windows 注册文件中时，这一关键字和值的组合使该计算机系统在启动时执行文件“Virus（病毒）”。因此，一旦由计算机系统利用本系统的方法从 Windows 注册文件中删除这个值，则计算机系统在启动时将不再试图执行那个文件。

尽管该计算机系统在启动时将不再试图执行该病毒文件，但可执行的病毒文件仍驻留在该系统上，应予以删除。因此，该恢复命令数据文件还包括 ReadRegKey 命令以及目标变量、关键字和值参数，用于把位于特定值字段中的值加载到它被存储的第一个变量中。这个值是“快乐 99.蠕虫”安排成要在系统启动时执行的那个可执行文件的名称，如“Ska.exe”。然后，计算机系统执行 StrCat 命令把这一变量与系统目录的路径名连在一起构成第二个变量，这里的系统目录随系统而变，因此用系统宏“%SysDir%”来符号化，现在这第二个变量含有系统路径后跟可执行病毒文件名。然后计算机系统执行 DelFile，以这第二个变量作为一个参数，从而删除该可执行文件。这一技术允许计算机系统删除该病毒。不依赖于该可执行文件的实际名称。

一个操作系统（OS）变量可用于标识一个操作系统，所列出的命令在其后可能在该系统内执行，该变量可以设置为 Windows95、Windows98、Windows NT、Windows2000 或 All（全部）。如果有一个命令是针对某一操作系统的，则该命令可以被列在由那个操作系统标识的恢复命令数据文件子部分之下。如果一个命令可在全部操作系统上使用，则那个命令可以被列在一个通用部分或一个子部分之下并为所有操作系统执行。在图 3B 中，操作系统变量“Win9x”表明在该代码部分内列出的命令要在运行 Windows95、98、ME 操作系统的计算机系统上执行。本系统和方法可以使用标准系统应用程序接口（API）确定该操作系统。一旦操作系统被确定，这一信息可被存储起来，并在执行恢复命令数据文件中的命令时用于条件分支操作。

恢复命令数据文件还可包括其他类型的命令。例如，如果必须修复或替换不容易得到的文件或数据，则在恢复命令数据文件中可以提供代码用于提示用户插入含有适当文件或数据的系统盘。可以在恢复命令数据文件中包括代码用于从系统盘中检索这些文件或数据并用于替换计算机系统上的受破坏的或丢失的文件。恢复命令数据文件还可包括代码用于从计算机系统启动因特网浏览器和访问具有恢复该计算机系统所用适当文件或数据的已知网站。在恢复命令数据文件中可包括代码用于提示用户从该网站下载适当的文件和数据，或者用于从该网站自动下载文件或数据，以及用于恢复计算机系统上丢失的或受破坏的文件或数据。

使用根据本说明教导编程的一个或多个传统的通用数字计算机和/或服务器，能方便地实现本公开内容。根据本公开内容的教导，有技术的程序员能容易地准备适当的软件代码。本公开内容还可以通过准备特定于应用的集成电路或通过对传统部件电路进行适当的连网来实现。

考虑上述教导，对本公开内容的大量附加修改和变化是可能的。所以，应该理解，在所附权利要求的范围内，本公开内容可以其他方式实现，而不仅是这里具体描述的那样。

图1

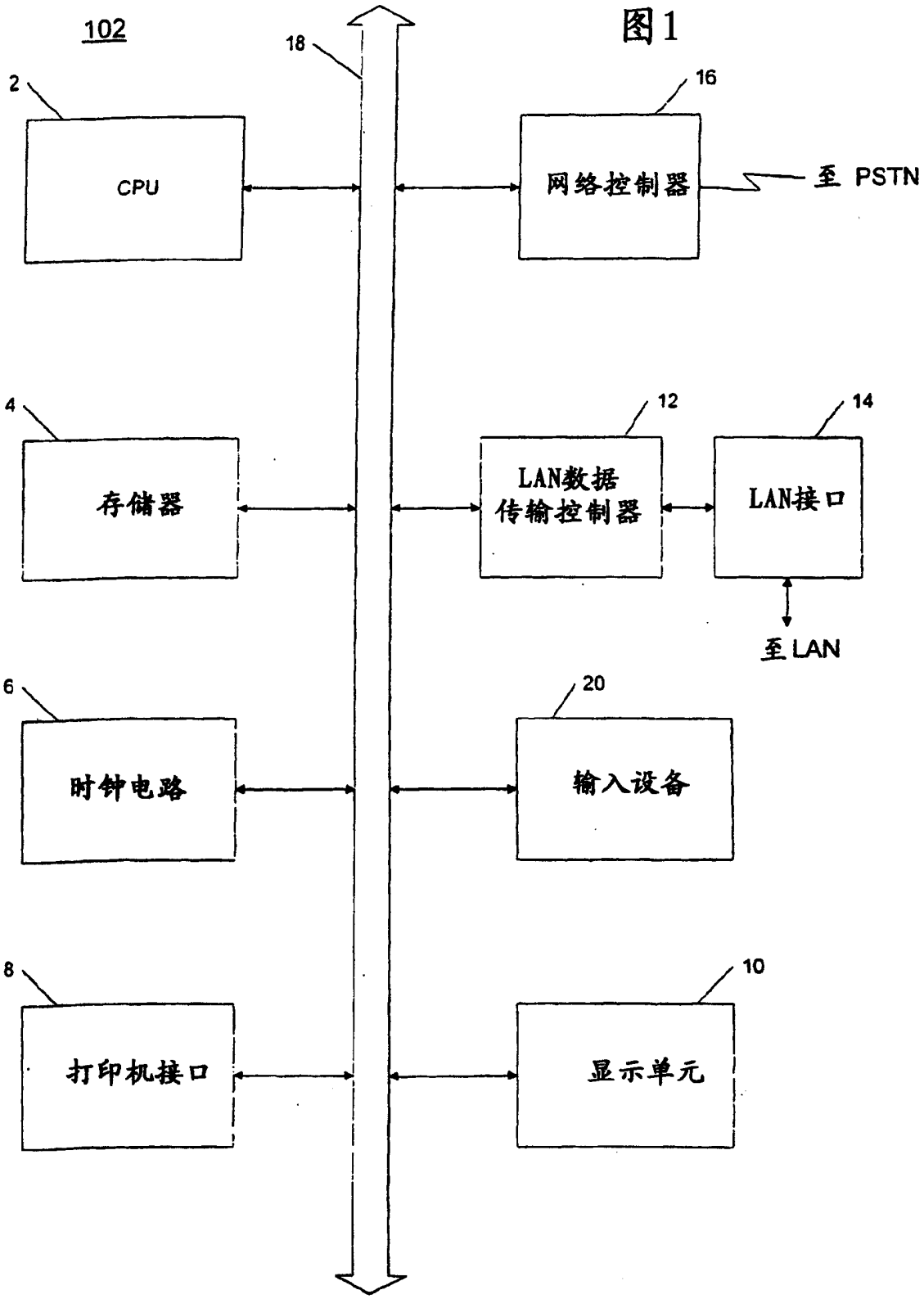

102
18
2
CPU
16
网络控制器
至 PSTN
4
存储器
12
LAN数据
传输控制器
14
LAN接口
至LAN
6
时钟电路
20
输入设备
8
打印机接口
10
显示单元

图 2

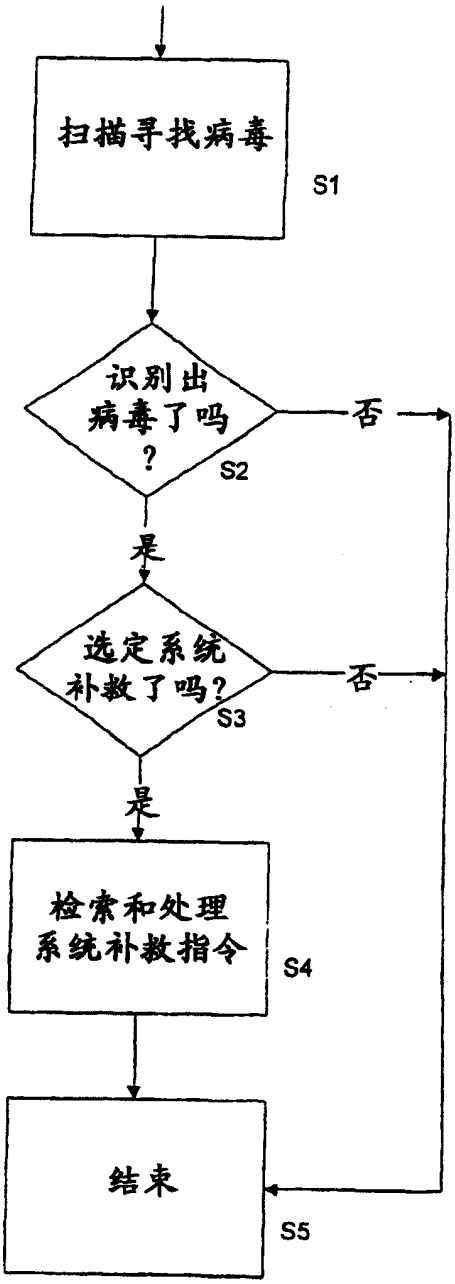


图 3A

恢复命令数据文件

W32/裸的

VBS/SST.Worm

Stages.A

Resume.A

Happy99.Worm

Win32/SouthPark.Worm

•
•
•

VBS/LoveLetter.AWorm

图 3B

```
Virus Start:
    Signature:>xx<xx xx ...
    RemoveEXE:
    .
    .
    .
    RemoveEnd:
    SysCureStart:
        DelRegKey: "HK_LOCAL_MACHINES\Software\Microsoft\Windows\Run","Virus"
    Win9x:
        ReadRegKey:ST0, "HK_LM..", "Filename"
        Strcpy:ST1, %SysDir%
        Strcat:ST1,St0
        DelFile: ST1
    SysCure End:
VirusEnd:
```