DOS下内存中计算机病毒的查消

郭 涛 傅奇芳 聂 昱 (武汉大学)

现在的查消病毒的软件只是跟着病毒走,随着病毒的发展不断推出新版本。对病毒的自动查消应是努力的方向。

当内存中存在计算机病毒时,对于存储介质上的病毒的消除是不安全的,因为在我们消除病毒的同时,由于内存病毒的存在,可能使存储介质在消除病毒的同时染上病毒,所以只有确认内存中不存在计算机病毒,才能保证消除过程是安全的。因此判断内存中有没有病毒,存在何种病毒,如何消除,是消除存储介质上病毒的前提。

目前的消毒软件对内存病毒的检查分三种形式:

1.不进行检查。要求用干净的系统盘启动,消毒程序假定内存中不存在病毒。

2.只检查内存中有无已知病毒。

3.只识别特定的DOS环境,若内存中存在驻留程序则可能发生误报。

但是三种检查形式都不完善,因为它们都不能保证消毒程序是在无毒环境下工作,而且当内存中存在病毒又没有确认无毒的系统盘时,目前的商品化消毒软件尚不能消除内存病毒,因此它们无法工作。

针对上述情况,我们提出一种可以有效查找和消除计算机内存病毒的方法——调用程序链法。所谓调用程序链法就是根据内存病毒的特点,通过对存储介质访问过程的跟踪,记录下调用的所有程序,判断这些程序中是否存在病毒而达到自动查消内存计算机病毒的目的。

要了解调用程序链法的原理,我们首先要谈谈内存病毒的特点。

内存中的计算机病毒要得到传播机会就必须得到控制权,即必须有程序调用病毒代码。不能得到控制权的内存病毒代码是不能传播病毒的。消除内存病毒就是要使驻留在内存中的病毒代码得不到控制权。

那么计算机病毒将从哪些方面得到系统控制权呢?我们知道内存病毒的传播是将病毒代码复制到存储介质上,而对存储介质的访问通常会有某些显著的表现,所以如果病毒不想让人轻易的发现,必然要在系统访问存储介质的同时访问存储介质,也就是说,一个不易被发现的病毒是在系统访问存储介质时得到控制权的。在DOS下涉及存储介质操作的有中断INT 13H, INT21H, INT25H, INT26H以及块设备驱动程序等。因此病毒要传播,很可能修改上述中断之一或设备驱动,也可能修改其他。不管病毒修改什么,它要传播而不被轻易发现就必须在系统访问存储介质时得到控制权,在访问存储介质过程中就必须执行病毒程序,因此,如果我们记录下在访问存储介质的过程中执行的所有程序,就一定能够判断内存中是否存在病毒。

记录下来的,在一组操作中所执行的全部程序的调用次序就是调用程序链。根据所有存储介质访问操作的调用程序链,我们可以判断内存中是否存在病毒,据此我们可以消除内存中的病毒。

调用程序链法查找和消除内存病毒的基本算法框架如下:

begin

执行包含所有访问存储介质操作的特定过程,记录下这一执行过程的调用程序链。

分析调用程序链中每个程序所处的内存块,判断可能是病毒的程序。

若是病毒,则改变调用病毒程序的调用地址,使其跳过对病毒程序的调用,达到消除病毒的目的。

end

记录调用程序链有很多方法,一种是仿真执行过程的所有指令,这种方法没有什么特殊的要求,是一定可行的,但是仿真程序的编制是复杂的。另一种方法是通过修改单步向量 INT1,跟踪执行过程,达到记录调用程序链的目的。这种方法程序相对比较简单,但是这种方法对于所跟踪的执行过程有特殊的要求,即要求执行过程不修改 INT1 中断,且整个执行过程允许中断的发生,采用这种方法要求执行过程满足可进行检查假设:执行过程不修改 INT1 中断,且整个执行过程允许中断的发生。

如果记录下所有调用程序指令,那数据量大得让人难以接受。因此有必要引入另一个假设—可查出假设:每一个驻留在内存中的病毒占用一个单独的段址。在这一假设的基础上,能大大减少记录的数据量,我们可以只记录段址发生改变时,调用被调用程序的指令地址和被调用程序的入口指令地址,而不会记录不到病毒程序。

记录下了调用程序链,下一步的任务是从中找出病毒程序段。实际上我们并不能知道哪一段程序是病毒,只能知道一段程序是否是正规的,或者说是正常的。

首先,对于出现在调用程序链中,单独占用一个内存块的程序我们是无法判断它是否病毒,必须由人来判断,当然程序可以提供相当多的信息来辅助判断,如:内存块名、执行的文件等,如果一个不驻留内存的程序在内存中被发现,则显然是病毒。

其次,若是 ROM 中的程序则一定不是病毒。

若程序出现在 DOS 管理的内存之外则一定是病毒。

若程序出现在 DOS 区开始之后,第一个内存块之前,则一定不是病毒。

最复杂的是当被调用程序出现在第一个内存块中,即在 DOS 数据区中,则此程序可能是扩展的设备驱动程序,也可能是 DOS 数据区程序,还可能是病毒,出于安全考虑,应该进行询问。

在实际应用中,可以将人工判断的结果记录在一个文件中,这样当遇到同样的程序时,查毒程序可以根据该文件直接判断此程序是否为病毒。通常只是在新程序第一次遇到时才会向人询问,在一般情况下,程序可以自动判断,而不需要向人询问。

查到了病毒,如何消除呢?我们先讨论一个消除内存病毒的可行性。理论上说,可以进行段间转移的指令序列是很多的,但在实际程序中使用的却只有几种,它们是:

1.jmp dword ptr cs:[xxxx]

2.jmp xxxx:xxxx

3.call dword ptr cs:[xxxx]

4.call xxxx:xxxx

5.int xx

对此,我们提出一种可消除假设:即每一个正规程序对中断的修改是正规的,或者说一个正规的程序调用下一步程序所采用的方式只有上述 5 种。

那么病毒具体是如何消除的呢?举个例子说明:

假设程序 A 通过上述 5 种方式之一调用了程序 B,程序 B 调用程序 C,程序 C 的入口地址是 D,现在发现程序 B 是病毒,那么消除病毒 B 就是让程序 A 不调用病毒 B,而直接调用程序 C,即将程序 C 的入口地址 D 代替原来 A 程序调用中程序 B 的入口地址,如果程序 A 调用程序 B 的方式只有上述 5 种,这一过程是很容易实现的。因此病毒是可以消除的。

1993 年 6 月提出调用程序链法,1993 年 10 月实现,这种方法对于查找和消除内存中的计算机病毒是极其有效的。目前尚未发现用这种方法无法查出的驻留内存的病毒,除 DIR-2 外,不存在这种方法无法消除的病毒。从 DOS5.00 到 DOS6.20,从 286 到 Pentium,这种方法都能正常工作。

如果满足方法的三个假设,这种方法可用于文件型病毒的自动消除,但是已经存在好几种反跟踪的文件病毒,破坏了可进行检查假设,因此这种方法用于文件病毒的查消不是很成功的。