# “系统消毒”是防治计算机病毒的重要环节

陕西省工商银行计算中心　贺江　刘三军　姜涛

**摘要**：本文针对许多已解毒磁盘(或文件)很快再度染毒的现象，在分析了多种计算机病毒传染和表现的一般规律后，提出了防治病毒的“系统消毒”观点，认为它对于各种计算机病毒的防治均具有普遍的意义。文章介绍了针对“圆点”病毒、“大麻”病毒和“犹太人”病毒的系统消毒具体实现方法，并提出了监测未知病毒入侵的有效手段。

## 一、引言

自 1989 年初以来，我国计算机界普遍发现了各种计算机病毒。这些病毒，严重干扰了计算机的正常工作，影响了计算机事业的正常发展。许多计算机工作者不得不停止手中的其他工作，开始了对计算机病毒防治的研究。目前，各种计算机病毒解毒免疫软件都已相继面世，得到了广大计算机工作者和备受各种病毒困扰的计算机用户的欢迎。这里，我们谈谈在防治计算机病毒工作中的一些体会，愿与广大同仁共同探讨。

## 二、系统消毒的作用

如何有效防止已解毒的磁盘(或文件)很快又被病毒再度感染的问题，并引起了极大的关注。一些同志在有病毒的系统环境下对带病毒的磁盘(或文件)进行操作。结果惊讶地发现：该磁盘(或文件)又被感染上了病毒！

这一现象说明解毒者没有注意处理系统内存中正在活跃的病毒程序，从而使刚刚解毒的磁盘(或文件)重新被病毒感染。

目前许多病毒防治软件都在进行解毒工作的同时，也对磁盘或文件做了免疫处理，从而防止了上述现象的发生。但是应当指出，在有些情况下，不可能对每个已解毒的磁盘或文件都做到免疫。而且在一般情况下，也不便于对全部正常磁盘或文件都进行免疫处理。这样，在有病毒的系统环境下，就始终存在着磁盘或文件被病毒感染的可能性。因而，保证系统环境的清洁仍然是防治病毒的一个重要环节。

怎样实现系统环境的洁净无毒呢？则“系统消毒”就是实现这一目标的唯一途径。

从对多种计算机病毒的分析中，可以看出，大多数计算机病毒只有在其侵入计算机系统而处于动态活跃状态时，才能够广泛传染和进行各种破坏活动。病毒侵入计算机系统的方式一般分为两种。对于操作系统类型(引导型)的病毒，如“圆点”病毒、“大麻“病毒，它们是在用病毒磁盘启动机器时，先于操作系统而自举至内存高端的。它们将自己屏蔽在几 K 字节的内存中，在计算机进入 DOS 状态后，只要一发现有正常磁盘在进行操作，就伺机出击，将病毒传染给正常磁盘。(“大麻“病毒对硬盘的传染是在病毒自举进进行，属于特例)对于非操作系统类型的病毒，如“犹太人”病毒(即耶路撒冷)、“下雨”病毒，它们则是在计算机运行带病毒文件时，先于所运行文件而自举至内存某一区域的。病毒常驻在这一内存区域并隐蔽起来，当系统运行其他正常文件时，便开始对正常文件进行染毒或破坏。

由些可见，系统内存中被病毒程序所占据的区域，乃是计算机病毒藉以栖身并充分发挥其攻击性、广泛传播病毒的基地。如果在病毒防治工作中只注意了磁盘介质或文件本身的解毒，而忽视了系统内存中有省略病毒的消除，则解毒后病毒死灰复燃的情况仍然可能发生。因此，在防治病毒时，必须做到既要重视处理磁盘介质或文件内静止的暂无攻击性的病毒，又须认真对付系统内存中动态的正发挥着其强烈攻击性的病毒。只有这样双管齐下，才能达到彻底干净消除病毒的目的。

所谓“系统消毒”，就是对付系统内存中的病毒。其实质就是要使系统内存不再被计算机病毒用作传播病毒

和破坏计算机工作的基地。要害就是使内存中的病毒丧失活力。

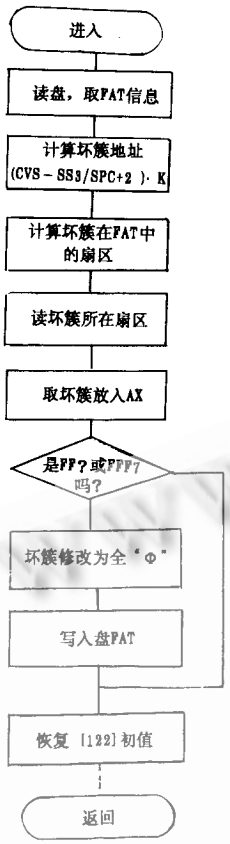


图 1 修改 FAT 流程图

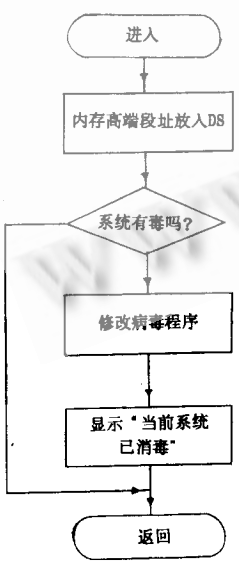


图 2 系统消毒流程图

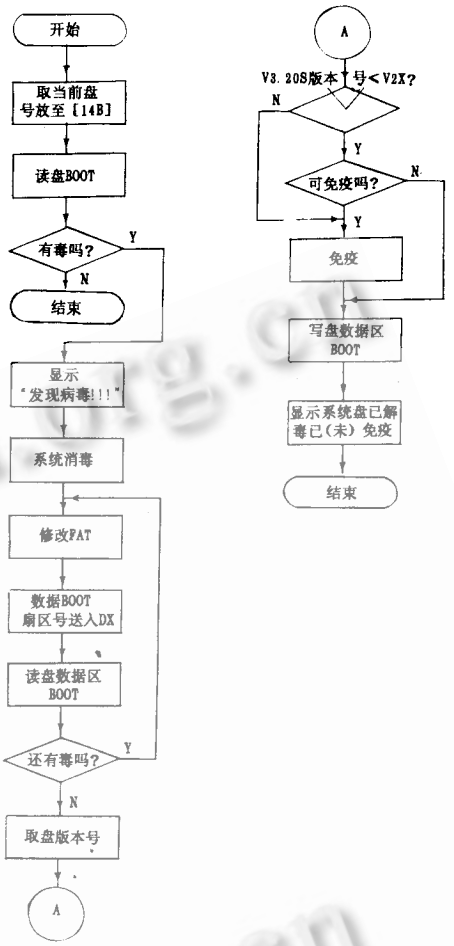


图 3 JD—XG COM 流程图

## 三、如何实现系统消毒

怎样做好系统消毒工作呢？用无毒系统盘重新启动机器，这无疑是最简单实用的方法，但一般人难以马上判定当前系统是否有病毒以及所用系统盘是否有毒，况且这还要中断系统正在进行的工作。这就是需要另辟捷径，寻找一种既不中断计算机的工作又能迅速准确判定当前系统是否有毒并且进行系统消毒的方法。通过对"圆点"、"大麻"、"犹太人"一种病毒程度的深入剖析，经过反复试验，我们终于找到了这种方法，实现了"系统消毒"的设想。

由于病毒侵入计算机后，必然要在系统中留下其入侵的痕迹，通过程序检查这些痕迹的特征，对于非操作系统类型的病毒，则着重在中断向量表内寻找有无病毒修改的特定地址，这里不再详述。下面主要谈谈如何实现

"圆点"、"大麻"和"犹太人"病毒的系统消毒。

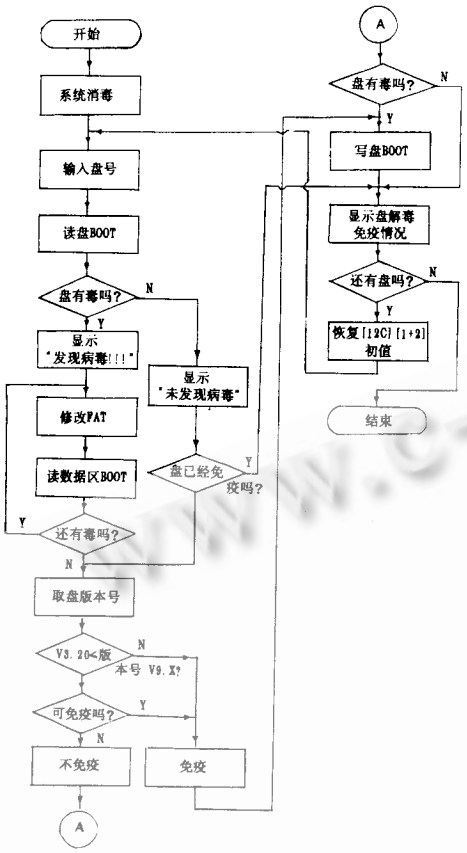


图 4　*JD--XG COM* 流程图

对于"圆点"病毒，我们发现病毒程序在自举至内存高端后，其 01F7 H 字节被初始化为 00H。病毒程序在对正常磁盘染毒时，先要判断该字节第 0 位是否为"0"，是"0"则对该磁盘进行染毒，为"1"则不去染毒。因而我们对"圆点"病毒程序是在进入其传染部分之后才会修改 INT 8 中断向量去影响正常屏幕显示的，因而病毒也就不会有屏幕上显示跳动的光点了。这样，病毒的活力丧失了，也就达到了系统消毒的目的。

在对"大麻"病毒的剖析中，可以看到，该病毒程序修改了 DOS 的 INT 13 中断向量，它把 INT 13 中断引至系统内存中病毒的一些判断。我们便从这里入手，将内存中病毒程序 0015H 处指令修改为"JMP 35"，使其不做磁盘染毒判断，直接去执行正常的 INT 13 中断处理，从而实现了对"大麻"病毒的系统消毒。

同样，对于非操作系统类型的"犹太人"病毒，也是从该病毒所修改的 INT 21 中断向量入手，将内存中病毒程序 0237H 处指令修改为"JMP 278"，跳过了病毒程序的传染部分，消除其对正常文件的染毒功能。与处理"圆点"、"大麻"两种病毒不同之处是：由于"犹太人"病毒影响屏幕正常显示而修改 INT 8 中断向量的工作不包括在其传染部分之内，因而为保证计算机正常工作，还要把被病毒程序修改的 INT 8 中断向量地址再修改回来，或者使病毒程序跳过表现部分而直接执行真正的 INT 8 中断处理。对上述三种病毒进行系统消毒的具体实施方法可有多种，还可以通过修改内存中病毒程序的其他指令来实现，这里就不再赘述了。

总之，对计算机进行系统消毒，就是通过适当修改内存中病毒程序的某些指令或数据，消除其传染病毒与破坏计算机工作的能力，保证计算机正常工作。当再有同类病毒要入侵时，则因内存中已被肢解的病毒形体还在，便误认为系统已有病毒，就不会使系统再次染毒。

实践证明，只要做到了系统消毒，对于磁盘或文件即使不做免疫处理，也能有效防止病毒扩散传染或数据丢失、显示异常的现象发生，甚至对有病毒的磁盘、文件不进行解毒，也可保证计算机正常工作而不遭病毒破坏。我们所开发的计算机系统消毒软件，经许多用户使用，反映甚好。尤其是当该软件用于自动批处理文件中时，每次开机后，无需操作人员举手之劳，便可自动检查并消除系统内存中的病毒，这对于许多基层单位计算机操作人员来说，无疑是除掉病毒骚扰的一剂良药。

需要指出的是，对于非操作系统类型的病毒，由于是在计算机工作期间随机地侵入计算机的，因此在进行系统消毒而未发出该类病毒时，应将这类病毒的免疫疫苗常驻于内存中，这样便能有效防止非操作系统类型的病毒在计算机工作期间侵入系统。对于一些未知的非操作系统型病毒，还可用常驻内存的一段小程序定时检查 INT 13、INT 21 等中断向量，发现异常立即告警，并可用予先保存的正确向量地址将其恢复，以保证系统的正常工作。

▲