“中国一号”病毒剖析及消除

人民银行贵州分行科技处 卢向阳

“中国一号”病毒得名于在其头部有“China I.O”字样。该病毒属文件型病毒，攻击 COM 类可执行文件。有毒文件运行后，病毒驻留于内存高端，之后若运行无毒 COM 类文件，则该文件被感染。此病毒的破坏性是修改定时器中断 INT1C，使之做一些毫无意义的空转，而且逐渐增加空转次数，从而使机器运行速度逐渐降低，一定时间后，病毒内部的空转计数器清零并重新开始累加，机器又重复由快到慢的过程。笔者曾在长城 0520-DH 机上做过实验；用 dir 命令列出盘上 77 个文件，正常情况下只需六秒左右，将病毒激活后三十分钟，重复同样的过程足足用了二分半钟，可谓难以忍受。

为了消除“中国一号”病毒的危害，下面对该病毒的作用机理进行剖析并介绍免疫、解毒的方法。

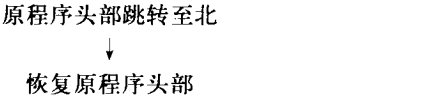
一、病毒重要特征

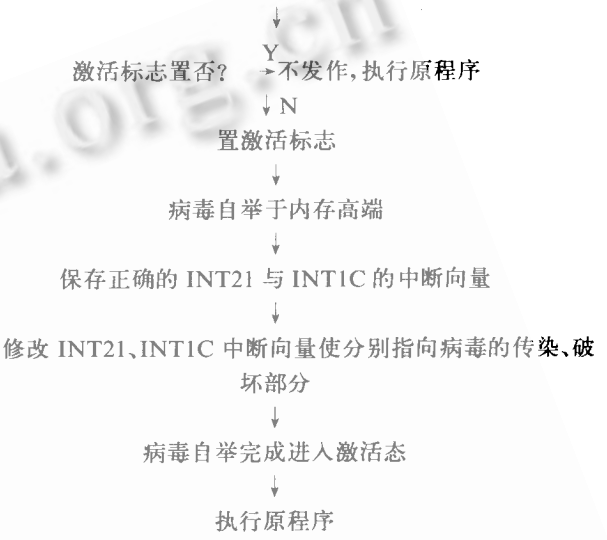
该病毒长 489 字节，有效部分还要少些。如发现某 COM 类文件长度增加了 489 字节，则可能已染上该毒。另外，该病毒头部及尾部分别有“china I.O”和“Hello world!”字样，故用 debug、pctools 等工具检查 com 类文件，如有以上字样出现，则也可能染毒。当然，病毒的重要特征还是发作之后机器速度逐渐变慢。

二、病毒主要流程

1.引导部分

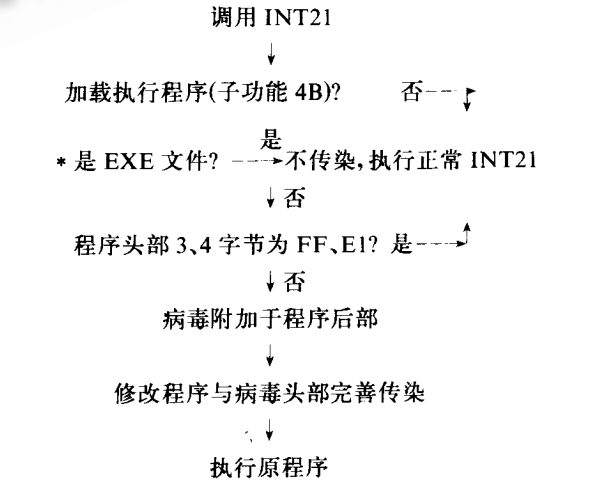
原程序头部被改为跳转向病毒头部的指令，从而进入病毒引导部分。该部分用于完成病毒的引导自举，使之激活并驻留内存，同时修改 INT21 和 INT1C 的中断向量，分别作传染、破坏用。其流程图如下：





2.传染部分

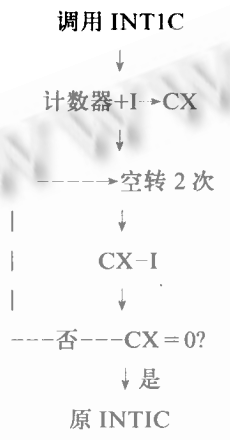
“中国一号”病毒的传染是在加载执行 COM 类文件时进行，这是通过修改 INTZI 的中断向量来完成的。当加载执行程序即调用 DOS 的 EXEC 功能时，首先执行病毒的传染部分，判别特征字，如符合条件就传染，否则执行正常的 INT21。这部分主要流程图如下：



＊判断是否为 EXE 文件是通过程序头部第 0、1 字节是否为 4D、5A 来判断的，4D、5A 是 EXE 文件文件头的 EXE 文件标识。

3.破坏部分

该病毒的破坏作用是通过修改定时器中断 INT1C 的中断向量来完成的，所以其破坏作用是自病毒驻留内存时就发生作用了。在原 INT1C 的中断服务程序中只安排了一条中断返回指令 IRET，被修改后增加了一些无用的空转指令以占用 CPU 运行时间，降低运行速度，达到破坏目的。在病毒偏移 OICO 处一个字用作空转计数器，在其超过 FFFF 之后清零并重新开始累加，故机器的速度是时快时慢。这一部分的主要流程图如下：



三、解毒方法

如染毒文件有无毒备份，则最简单的解毒方法即是删去有毒文件，拷入其无毒备份即可。如手边没有无毒备份，则只有根据病毒作用机理进行手工解毒。下面介绍一种方法。

重新启动机器并保证要使用的 debug 无毒。假设染毒文件为 VIRUS.COM，如下进行消毒即可。其中，CX 为文件长度，减去病毒长 1E9 得 3E19，为原文件长。而病毒是从偏移 3E19+100＝3F19 处开始的（程序段前缀 100H 字节）。病毒开始的六个字节是原文件头部的六个字节，将它们写回，然后修改文件长度后存盘即可。

```
C>DEBUG VIRUS.COM
-R
AX=0000  BX=0000  CX=4002  DX=0000  SP=FFFE  BP=0000  SI=0000  DI=0000
DS=1AD9  ES=1AD9  SS=1AD9  CS=1AD9  IP=0100  NV UP EI PL NZ NA PO NC
1AD9:0100 B9393F MOV CX,3F39
-D3F19 3F1E
1AD9:3F10                    E9 84 3D 43 6F 63 ..=Con
1AD9:0100 B9.E9 39.84 3F.3D FF.43 E1.6F E8.6E
-RCX
CX 4002
:3E19
-W
Writing 3e19 bytes
-Q
```

四、免疫方法

从前面的分析得知，若激活标志已置，则运行染毒文件时病毒并不发作，这个标志在内存 0:0300 处。根据这一特点，笔者在硬盘 DOS 引导记录中剩余空间处加入几条指令，使启动时即置激活标志，即将字[0:0300]置为 IIII 即可。这样，盘上的“中国一号”病毒将永不会发作。如下是在浪潮 0530-H 机上修改 DOS3.3 引导记录的过程。

```
C>debug
-1 0100 201
-a0100
1AC4:0100 jmp 02ec
1AC4:0103
-ao2ec
1AC4:02EC push ax
1AC4:02ED push ds
1AC4:02EE xor ax,ax
1AC4:02FO mov ds,ax
1AC4:02F2 mov word ptr [0300],1111
1AC4:02f8 pop ds
1AC4:02F9 pop ax
1AC4:02FA jmp 0136
1AC4:02FD
-w 0100 201
```