2708 病毒及主引导型病毒的防治

湖南省双峰工商银行　罗　辉

摘要：本文详细地分析了 2708 病毒的特性，得出了它的处理流程，对它的源码程序进行了详尽的注释，给出了简易清除方法，并提出了“以其人之道还治其人之身”的防治引导型病毒的两重诊断和两重保护方法。

2708 病毒又称打印机病毒，它是引导型病毒，感染硬盘主引导扇区和软盘 DOS 引导扇区，由于它的表现部分修改打印机并行口 LPT1 和适配器串行口 COM1 区的内容，足可以使你的系统资源破坏，造成数据丢失，因此它是一种恶性病毒。

病毒编制者都将受到道德的诅咒和法律的惩罚。但是，凡事都应一分为二。我们从纯程序编制技术角度来看，2708 病毒程序却也有些巧妙之处，值得参考。笔者对 2708 病毒进行分析，并提出了一种防治引导型病毒的通用方法，希望它能为大家防治和借鉴病毒提供帮助。

一、2708 病毒的特殊之处

(1)它不只是修改打印机并行口 LPT1 的端地址，同时修改 RS 232 适配器串行口 COM1 的端地址。只不过平时一般没有利用串行口 COM1 外接辅助设备 AUX，因而没有感觉到。

(2)它传染硬盘时，是取代硬盘主引导区，而不是和大麻病毒一样，先将原主引导扇区内容移到其他扇区保存起来，通过病毒体调用原自主引导程序完成系统的引导。它直接完成病毒的安装和系统的启动。

(3)发作部分只是简单的一次，即每次启动系统前安装病毒时就修改打印口 LPT1 和适配器 COM1 的端地址。之后，就只是传染，不再发作。而且硬盘的感染也是在安装病毒体时完成，修改后的 INT13H 只感染软盘，不感染硬盘。

(4)伪装更巧妙。2708 病毒保留了引导扇区的一些典型信息。它空出了偏移 03H－0 AH 的 8 个单元用以存储该软盘的引导区相应位置的信息，如当感染软盘时，它保留的是 DOS 的版本号信息“IBM ＊・＊”。同时在它不利用的 26DH－1 FF 共 144 个字节里全部填入被感染盘的原引导相应位置的内容。比如是感染硬盘，则被感染的主引导区中分区信息表位置仍旧由原分区信息表代替。这样一方面达到了迷惑的目的：你一不细心就不能发现已被感染；另一方面，病毒体就可以根据分区信息表判断是硬盘启动还是软盘启动，同时硬盘启动病毒体就可以根据分区信息表判断是硬盘启动还是软盘启动，同时硬盘启动时由它本身进行系统的装载，而无须保存硬盘主引导程序。不造成硬盘额外的空间开销和破坏，因而被发现的可能性更小。

(5)具有动态的特性，增加阅读的难度。该病毒有两处指令中的操作数内容被其他指令修改(程序中用下划线标出)。修改后的中断 INT 13H 服务子程序中单元 9 F80：006 BH 的 JMP 指令中的转向地址显现在你的眼前的是 9 F80：

0015H，其实这是一个假象，在病毒体执行后它就由单元 0：7 CAOH 的指令填写为正常的 INT 13H 的服务子程序的入口地址。而在它的发作部分中的偏移 156 H 斜打印口 LPT1 的设置端地址指令中的被置数由偏移 167 H 占的指令重新填制。笔者猜测，这样做，是该病毒编制者有意的在他的机器硬盘里的病毒源码中偏移 156 H 中的置数为正常的打印口端地址。这样他的机器启动时打印机端口地址实际没有变，因而病毒对自己不构成影响。但是，由于发作后该置数地址就被偏移 167 H 中指令设为 0，以后传染时是按修改后的病毒体传染，因此传染出来的病毒就可以将打印机端口设置为错误的地址，达到破坏的目的。

(6)特征码不固定。病毒在传染前判别该磁盘是否已经感染时，不再和其他病毒如小球病毒一样是根据某些固定的特征码来判断的，而只是判别该而不管其为何

值。

(7)高密度软驱，感染该病毒后，会出现在用 DIR 显示目录时，如果你更换软盘，显示的内容还是更换以前的软盘内容的现象。这是由于病毒修改后的中断 INT 13H 在进行正常的软磁盘读、写、或格式化前，病毒要先将病毒体写进软盘，这一磁盘操作将抹掉磁盘介质更换信号。这样正常的 INT 13H 总得不到更换信号而认为是对原盘操作，因而只是简单的将原先在内存的软盘目录再现，而不再读磁盘。为什么对普通 360 K 软盘又没有这一现象呢？原因是普通 360 K 软盘不提供磁盘介质更换信号，DOS 是根据间隔时间的长短来判别的，所以没有这一现象。

二、2708 的磁盘映像

感染硬盘的 2708 病毒一个典型的磁盘映像内容如下：

```
-10000 0 0 1
-d0000 ,01ff
140 E:0000 E9 8B 00 C0 07 E9 99 00-00 1A AF F6 C4 02 74 5B
14CE:0010 F6 C2 30 75 56 50 1 E 31-C0 8 E D8 88 D0 FE C0 84
14CE:0020 06 3F 04 75 44 53 51 52-06 57 56 B8 01 02 0E 07
14CE:0030 BB 00 02 B9 01 00 B6 00-E8 35 00 72 26 0E 1F A1
14CE:0040 89 02 3B 06 89 00 74 1B-B8 01 03 B9 08 27 B6 01
14CE:0050 E8 1D 00 72 0E E8 1F 00-B8 01 03 31 DB 41 B6 00
14CE:0060 E8 9D 00 5E 5F 07 5A 59-5 B 14 58 EA 15 00 80 9F
14CE:0070 9C 2E FF 1E 5C 00 C3 BE-03 02 BF 03 00 B9 08 00
14CE:0080 FC F3 A4 BE 70 08 BF 70-01 B1 90 F3 A4 C3 31 C0
14CE:0090 8E D8 8E D0 BC 00 C3 BE-03 02 BF 03 00 B9 08 00
14CE:00A0 A3 6E 7C A1 13 04 48 A3 -13 04 B1 06 D3 E0 81 C0
14CE:00B0 C7 06 4C 00 0B 00 A3 4E-00 B9 00 02 BE 00 7C 31
14CE:00C0 FF FC F3 A4 50 B8 CA 00-50 CB 31 C0 CD 13 31 C0
14CE:00D0 8E C0 B8 01 02 BB 00 7C-0E 1F B8 3F 00 F6 C1 FF
14CE:00E0 74 08 E8 51 00 EA 00 7 C-00 00 B9 08 27 BA 00 01
14CE:00F0 CD 13 72 F1 0 E 07 B8 01-02 BB 00 02 B9 01 00 BA
14CE:0100 80 00 CD 13 72 DF A1 89-02 39 06 89 00 74 D6 E8
14CE:0110 65 FF B8 01 03 31 DB 41-CD 13 EB C9 BE BE 01 B9
14CE:0120 04 00 80 3C 80 74 07 83-C6 10 E2 F6 EB 07 8B 4C
14CE:0130 02 8B 14 CD 13 C3 F6 06-6F 01 E0 75 15 80 06 6F
14CE:0140 01 01 B8 01 03 0E 07 31-DB B9 01 00 B6 00 CD 13
14CE:0150 EB 0E 31 C0 8E D8 C6 06-08 04 00 C6 06 00 04 00
14CE:0160 0E 1F C6 06 6F 01 00 C6 -06 5A 01 00 C3 00 00 00
14CE:0170 1F 0E 07 BE BE 03 BF BE-01 B9 42 02 F3 A4 B8 01
14CE:0180 03 33 DB FE C1 CD 13 EB-C5 07 00 00 00 00 00 00
14CE:0190 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
14CE:01A0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
14CE:01B0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
14CE:01C0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
14CE:01D0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
14CE:01E0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
14CE:01F0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
```

三、2708 病毒的主流程图和修改后的 INT 13H 的处理流程

下面的分析都是按照病毒执令的实际内存地址加以说明的，而且都是基于 640 K 内存分析的。病毒的装载是在系统装载以前由 INT 19H 完成的，系统启动时病毒体已经由 ROM BIO 读到内存 0000:7 C00H 处。

病毒主程序的处理流程如下：

四、2708 病毒的简易清除法和引导型病毒的通用防治方法

(1)2708 病毒的简易清除。软盘上的 2708 病毒的清除只需将被藏在 1 头 27 道 8 扇区的真正的 DOS 引导区内容搬回引导区覆盖病毒体即可，步骤是：

```
A>DEBUG
-L  100 0 0 1 查该盘 DOS 引导区是否感染
-D  100
-A  100 读回真正的引导程序到偏移 0200H 处
CS:0100 MOV AX,0201
CS:0103 MOV DX,0100
CS:0106 MOV CX,2708
CS:0109 MOV BX,0200
CS:010 C INT 13
CS:010 E INT 20
CS:0110
-G=100
```

-A　100 将偏移 0200H 处的引导程序写入 DOS 引导区

CS:0100 MOV AX,0301

CS:0103

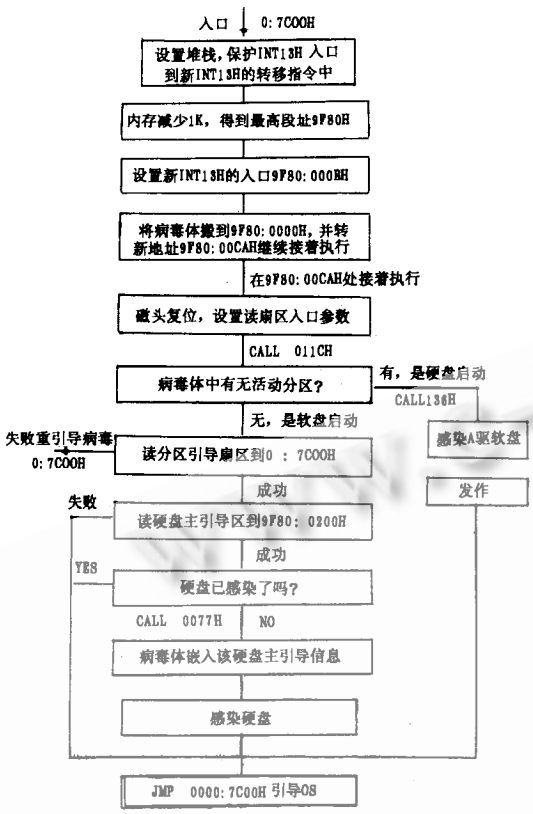

图 1 病毒主程序的处理流程

-G = 100

-Q

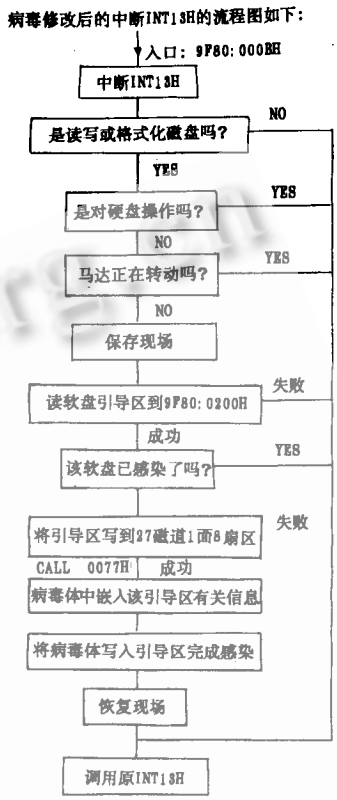

图 2 病毒修改后的中断 INT 13H 上流程序

硬盘上的 2708 病毒清除方法有二:

一是类似软盘的消毒,在一个正常机器里采集一个正常的硬盘 BOOT 区数据覆盖该硬盘主引导区即可,方法从上可类推,操作较复杂容易失误,不再介绍。

二是改写病毒体,屏蔽其的发作和传染部分即可正常操作,操作简单,步骤如下:

C>DEBUG

-A　100　　读硬盘主引导区到偏移0200H处

CS:0100　　MOV AX,0201

CS:0103　　MOV DX,0080

CS:0106　　MOV CX,0001

CS:0109　　MOV BX,0200

CS:010 C　　INT 13

CS:010 E　　INT 20

CS:0110

-G = 100

-A 20B　　屏蔽 INT 13H 中的传染部分

CS:020 B JMP 026 B

-A 336　　屏蔽发作部分(即发作时什么也不做)

CS:0336 RET

-A 100　　将偏移 0200H 处修改后的引导程序写入硬盘主引导区

CS:0100 MOV AX,0301

-G = 100

-Q

(2)硬盘主引导型病毒的通用防治法。从上面的分

析可以看出，主引导型病毒的安装都是在启动系统之前完成的，而其在传染之前都要通过特征码比较判别磁盘引导区(或硬盘主引导区)是否已经感染上了该病毒，然后才决定是否感染。俗话说："以其人之道还治其人之身"，我们也可以仿效病毒的这一处理方法，来对抗病毒攻击。笔者编了一个防治主引导型病毒的程序，它包括安装部分和检测部分。安装部分判别启动盘引导区是否有防毒主引导程序，如果没有，它将其引导区内容移于物理地址 0 磁道 0 面 2 扇区(硬、软盘这一扇区都未利用)。然后它将硬盘主引导区的分区表部分或软盘 DOS 引导区相应部分的内容嵌入防毒主引导程序相应地方、构成新的引导程序写入引导区取代原引导程序，同时将该新引导区内容生成 BOOT·DAT 文件保存在该盘的根目录里并置成隐含和只读属性。另一方面，它修改 COMMAND·COM，使 COMMAND·COM 不装 AUTOEXEC·BAT 批处理文件而改为装载 LUOHUI·BAT 批处理文件。在 LUOHUI·BAT 文件里，首先调用防毒检测部分检查内存低地址 0：0195H—0：0198H(INT 65H 的中断向量存储单元，DOS 未利用)内容有否"12345678"标志，有则启动盘引导区感染了病毒，程序将 BOOT·DAT 的新引导区覆盖启动盘引导区，然后调用中断 INT 19H 重新启动系统；否则退出检测，并调用 AUTOEXEC·BAT 批处理文件完成用户的应用程序的装载。

新引导程序所要做的事是：首先判别启动盘的物理地址零磁道零面一扇区内容是否即新引导程序本身，如不是，说明感染了病毒，置内存低地址段 0：0195H～0：0198H 的内容为"12345678"，然后将 0 磁道 0 面 2 扇区的原引导区内容读到内存 0：7 C00H 处，转原引导程序引导系统；否则说明系统未感染病毒，再判别是否硬盘引导，于是就根据分区信息表将分区引导区装入 0"7 C00H，否则将软盘的引导区保存在 0 磁道 0 面 2 扇区的引导信息装载到内存 0：7 C00H 处，然后转 0：7 C00H 处执行原引导程序。

这一防毒系统由于采用了两重诊治方式(引导程序诊治和自动批处理程序 LUOHUI·BAT 中诊治程序诊治)和两重保护方式(利用 0 道 0 面 2 扇区保护原引导区和利用 BOOT·DAT 文件保护新的引导区)，从而使引导型病毒基本上没有窥视的机会，达到防治的目的。经几个单位的使用，效果很好。

▲