清除磁盘引导区病毒和修复磁盘的方法

同济大学 邓长根
上海工业大学 曾康康

摘要：本文介绍了作者近年来应用工具软件 *NU* 清除磁盘引导区和硬盘主引导区病毒、修复引导区损坏磁盘的经验，经实践检验，简便有效。

一、工具软件 NU 简介

工具软件 NU(Norton Utilities, 适用于 DOS 操作系统，具有很强的磁盘管理和维护功能，可以恢复被删除文件，可以以引导区、文件分配表、目录区、文件、族号范围、扇区范围、绝对扇区范围为单元进编辑、显示、读写、查找操作。在以下几方面，NU 的功能优于 PCTOOLS

1.所选单元不同，NU 自动选择最方便的编辑／显示方式，还可根据用户需要在五种方式之间切换：十六进制方式(HEX)、文本方式(TEXT)、目录方式(DIR)，文件分配表方式(FAT)、硬盘分区表方式(PARTITION)。用 FAT 方式编辑／显示 FAT，十进制族号一目了然；用目录方式编辑／显示目录，修改文件或子目录名称和读写、隐含等属性十分方便。

2.可将选定的族号范围、扇区范围或绝对扇区范围内数据存入文件，也可以族号方式、扇区方式或绝对扇区方式定位写到同一磁盘或其它磁盘上。

3.可编辑、显示、读写绝对扇区：0 头、0 柱的各扇区。

4.具有维护功能，可对损坏的磁盘进行读写操作。

利用 NU 的上述优越性能，可以清除磁盘引导区和硬盘主引导区病毒、修复引导区损坏的磁盘。

二、清除磁盘引导区病毒

被引导区病毒感染的磁盘，不管是哪种病毒，实质都是改写了磁盘的引导程序。应用 NU 的按扇区定位或绝对扇区定位读写／编辑功能，就可清除种磁盘引导区和硬盘主引导区病毒。

(一)清除软盘引导区病毒

挑选一张经过格式化、未被病毒感染的洁净软盘(与病毒软盘属同一类，例如两者都是双面双密度、容量 360KB。以下同)，启动 NU 后，选择洁净软盘的 0 扇区，将其定位写到病毒软盘 0 扇区，则原病毒程序被洁净程序覆盖，病毒被清除。

(二)清除硬盘引导区病毒

1.用以下两种方法之一制作硬盘洁净 0 扇区的备份文件：

(1)在硬盘未被引导区病毒感染之前，预先将硬盘 0 扇区信息存入备份文件；

(2)发现硬盘已被引导区病毒感染而没有洁净 0 扇区的备份文件时，可将其它同型号计算机硬盘洁净 0 扇区信息存入备份文件。

2.发现硬盘被引导区病毒感染后，应由洁净软盘启动计算机，运行 NU，将备份文件按扇区定位拷贝到硬盘 0 扇区，病毒程序就被覆盖清除。

(三)清除硬盘主引导区病毒

作者曾遇一例很顽固的打印机病毒(Destory Print)，从硬盘启动计算机后，用清病毒程序 ANTIDOTE4.64 诊治，发现内存中有打印机病毒；然而查遍整个硬盘后，ANTIDOTE 却报告未发现病毒。用 CHKDSK 命令检查硬盘，显示信息指出可能不是 DOS 盘；并且发现不少文件族号交叉(cross linked)，丢失文件内容。用 PCTOOLS 或 NU 查看硬盘 0 扇区，未发现病毒。用 NU 选择硬盘主引导区(绝对扇区：0 头、0 柱、1 扇)，显示出打印机，其后紧接着大麻病毒(Stoned／Marijuana)残部，原来病毒已潜入存放硬盘主引导程序和硬盘分区表的主引导区！选择 NU 的 PARTITION 编辑／显示方式，确定硬盘分区表正确，仅仅是主引导程序被病毒程序覆盖。

清除硬盘主引导区病毒，可采用以下两种方法之

一。作者选择第一种方法，清除了上例的打印机病毒。

1.编辑修改方法

①加参数／P运行NU，屏幕只显示可打印字符，选洁净硬盘主引导区，用HEX方式显示，按屏幕拷贝键，打印出主引导程序(最好在硬盘感染病毒之前预备好主引导程序；也可借用其它计算机硬盘主引导程序)。

②运行NU，选病毒硬盘主引导区，用HEX方式输入主引导程序，覆盖病毒程序。

③如果硬盘分区表已损坏，可用PARTITION方式编辑。如果硬盘分区表参数与原盘相同，就可保全硬盘文件。

2.拷贝覆盖方法

(1)制作洁净硬盘两个备份文件。运行NU，先将硬盘0扇区引导程序存入备份文件BOOT，接着将硬盘绝对扇区：0头、0柱、1至n扇(其中包含1扇主引导区)存入备份文件PARTN，此处n为每柱面扇数。

(2)用这两个备份文件覆盖病毒程序。运行NU，选将备份文件BOOT按扇区定位拷贝到病毒硬盘0扇区，接着将备份文件PARTN按绝对扇区定位拷贝到病毒硬盘0头、0柱、1扇。

应用这一方式，有几点需说明如下：

(1)有些病毒可能侵入硬盘0头、0柱的其它扇区，伺机兴风作浪；有些计算机硬盘0头、0柱的其它扇区可能存放重要信息。基于这两个原因，需将病毒硬盘0头、0柱的n个扇区全部用备份文件覆盖，以彻底清除病毒，完全恢复计算机功能。

(2)这一方法将引导区和主引导区全部换新，故能一次完全清除这两个区中的病毒。

(3)另一关键是制作洁净硬盘两个备份文件。为了防治硬盘引导区病毒、也为了修复硬盘，最好趁早制作这两个备份文件。万一硬盘感染引导区病毒或硬盘引导区损坏，一时又找不到其它同型号计算机硬盘，清除病毒，修复硬盘就很麻烦，有可能丢失硬盘中文件。

三、修复引导区损坏的磁盘

有些磁盘因驱动器故障、或病毒感染、或保管不妥、或使用过久，导致引导区损坏，无法使用。当要显示磁盘文件目录时，屏幕出现“Data error reading drive A”一类的信息，甚至有时使用FORMAT命令对其格式化，出现信息：“Invalid media or track 0 bad-disk unusable”，磁盘无法再用。磁盘引导区损坏，对其进行读的结果，或者读入信息不正确，或者根本就读不进信息。对于硬盘，DOS甚至认为硬盘不存在。通常的软件对这种磁盘无能为力，如果磁盘中存有重要信息，损失就更惨重了。

如果引导区不是物理介质损坏，而是信息出错，则应用NU的维护功能，按特定步骤，可将这类磁盘修复，甚至还能保全磁盘文件。启动NU时，加参数／M，即输入NU／M，则启动NU的维护功能，其特点是对损坏的磁盘也可进行读、写操作。

(一)修复引导区损坏的软盘

(1)启动NU的维护功能。

(2)将(引导区洁净、未损坏的、与损坏软盘同密度的)完好软盘插入软盘驱动器B或A)，在NU中选B盘0扇区。

(3)选NU的写(Write)功能；NU会问写到哪个驱动器，选B；接着会问选用哪种方式，选扇区方式；接着会问从哪一个扇区开始，输入0扇区。在此之前，完好软盘一直留在驱动器B中，这是修复软盘并保全其中文件的关键，避免了NNU读入损坏软盘引导区错误控制信息。

(4)当NU最后问Yes／No时，从驱动器B中取出完好软盘，插入损坏软盘，回答YES，在0扇区写入正确信息，将其修复。因只改写了软盘0扇区，未修改其它扇区，故软盘中文件安全保留。

(二)修复引导区损坏的硬盘

(1)按前述清病毒方法制作硬盘备份文件BOOT和PARTN。

(2)启动NU的维护功能。

(3)将备份文件BOOT按扇区定位拷贝到硬盘0扇区。

(4)将备份文件PARTN按绝对扇区定位拷贝到硬盘0头、0柱、1扇。

(5)退出NU，查看硬盘中文件、子目录是否损坏，若没损坏，则已修复硬盘并保全其中文件，修复结束。

(6)若不能显示硬盘文件目录，指出FAT损坏，可启动NU，查看硬盘第二份FAT是否未损坏，若未损坏，则将第二份FAT所在扇区范围定位拷贝到第一份FAT起始扇区，至此修复硬盘并保全其中文件，修复结束。