大麻病毒的危害性及染毒磁盘的修复

陕西省工商很行计算中心 贺 江 刘三军 姜 涛

摘要：本文从分析大麻病毒的危害性入手，介绍了如何做好遭到不同程度破坏的染毒磁盘的解毒和修复工作。

目前，大麻病毒与圆点病毒一样，是在我国流行较为猖狂的计算机病毒。但因大麻病毒可造成磁盘数据的破坏，所以其危害性远远超过了圆点病毒。

对于大麻病毒的危害性，迄今还未引起有些同志的足够重视，有的同志虽然认识到了其危害性，但对磁盘解毒特别是修复的措施还不够有力。在解毒后，仍存在一些问题没有解决。如文件被破坏、硬盘不能启动，甚至用软盘启动后不承认硬盘存在等，本文试图从分析大麻病毒的危害性入手，着重介绍如何修复遭到不同程度破坏的各种磁盘。

一、大麻病毒对磁盘的破坏

大麻病毒对磁盘染毒时，在将病毒程序置入磁盘的同时，对于用 DOSV3 · X 和 DOSV2 · X 的 FDISK 命令建立分区的硬盘，还分别将其主引导记录移至了硬盘隐藏扇区和文件分配表区；对于软盘则将其引导记录移至了根目录区。并且对移入的主引导记录或 DOS 引导记录以及移入处原盘扇区的数据均未加以保护。这样，它就直接或间接地对硬盘和软盘造成了各种不同的破坏后果。

先看大麻病毒对于硬盘的破坏。

由大麻病毒的传染机理和 DOS 技术资料可知，病毒对于使用 DOSV3 · X 的 FDISK 命令建立分区的硬盘无破坏作用。因为在这种情况下硬盘主引导记录被移至硬盘的隐藏扇区中，它不会对 DOS 的任何区域造成破坏，系统工作时也不会破坏隐藏扇区中的主引导记录。

对于含有 XENIX 系统的硬盘，由于硬盘隐藏扇区数均不小于 17，一般也无严重危害。但若硬盘同时具有 DOS 分区和 XENIX 分区且 XENIX 分区是活跃的分区，则因系统启动过程中需要两次调用主引导记录，而且第二次要直接在 0 头道 1 扇区调用主引导，这样造成硬盘不能启动的现象。

大麻病毒对于磁盘的破坏作用。主要表现在用 DOSV2 · X 的 FDISK 命令建立分区的硬盘上。因为在这种情况下硬盘只有一个隐藏扇区，被病毒搬家的硬盘主引导记录将落在文件分配表(FAT)的区域内，这时硬盘将可能遭到以下三种情况的破坏：

1.病毒对 FAT 的破坏

对已遭受大麻病毒入侵的硬盘，可以用 DOS 的 CHKDSK 命令检查到硬盘有 100 多个链簇丢失、一些文件簇链被破坏。

病毒对 FAT 的破坏情况，首先与磁盘空间的分配情况有关。

当硬盘整个空间都分配给 DOS 时，对于 10MB 或 20MB 的硬盘来说，其扇区分配情况如表所示。

表 *10MB 或 20MB* 硬盘空间分配情况

	主引导区	DOS 引导区	FAT1	FAT2	根目录区	数据区
占用扇区数	1	1	8	8	32 或 64	其余

大麻病毒侵入该磁盘后，将把主引导区的主引导程序和分区表信息搬移至 FAT1 某一扇区，若该扇区已有文件链簇号在此，则这些簇号将被复盖，文件遭到破坏。若此后再经过一次对涉及该扇区链簇号的文件的写操作，则 FAT2 的相应扇区亦将变得与 FAT1 相同，这时被破坏的文件将可能再也无法恢复。

2.病毒对主引导程序的破坏

由于大麻病毒在将硬盘主引导程序搬移至 FAT1 后，并未对该区域加以保护，因而 DOS 仍将把该区域看

作是文件分配表的一部分，把其中的00字节看作是空闲簇，而把其中的非00字节看作是文件的簇号。当FAT的前几信扇区被文件链簇号占满后，DOS在写入新的文件时将占用主引导记录所在扇区的空闲簇。或者当DOS要删除一个文件链簇号已被破坏的文件时，将可能把该扇区的非00字节清除为00。无论是这两种情况的任何一种发生，都将使完整的主引导程序遭到破坏，硬盘从此不能自行引导启动。

注意，在这种情况下，仅仅用将FAT中主引导记录所在扇区数据直接写回原主引导区的方法来进行解毒，仍不能使硬盘自行引导。

3.病毒对硬盘分区表的破坏

在硬盘主引导区的最后66个字节，即从IBEH到IFFH的这一区域，是硬盘最重要的分区表信息。如果这一部分信息被破坏，轻者使硬盘不能启动，重者将使DOS不承认硬盘的存在。

大麻病毒侵入硬盘后，随着新文件的不断写入，先是在FAT区的主引导程序遭到破坏，接着就威胁到位于其后的分区表信息，一旦分区表信息被破坏，若再用一般的简单方法对硬盘解毒，则将会造成上述的严重后果。

现在再看看大麻病毒对于软盘的破坏。

软盘引导记录被移至根目录区后，移入处扇区原有的文件名就被复盖掉，文件将丢失。对于360 KB的软盘来说，由于该扇区位于根目录区的最后，一般磁盘不常用到，因此危害还不大。但对于1·2 MB的软盘来说，则因该扇区处于根目录区前面经常要使用的位置，因而危害比较严重。此时，不仅该扇区的16个文件遭到破坏，而且位于其后的所有文件都将丢失。

二、磁盘解毒及修复

磁盘感染了大麻病毒后，一般的解毒方法是：将被病毒搬家的磁盘主引导记录或DOS引导记录从现在所在扇区移回主引导区位置，再将移留下的扇区位置填充以全"0"。这种方法在一般情况下是可行的，但它不能恢复被破坏的硬盘主引导记录、FAT及软盘根目录。在个别情况下，这样处理甚至会造成整个硬盘数据的丢失。

我们在仔细剖析了大麻病毒程序、并深入研究了其对磁盘的各种破坏情况之后，采取了一系列具体措施，在对磁盘进行解毒的同时，最大限度地保护并修复了磁盘数据，将大麻病毒的破坏后果，限制到了最低限度。

对于软盘、含有XENIX系统的硬盘以及用DOS V3·X的FDISK命令建立分区的硬盘，其解毒可用上述简单的方法处理，以下主要介绍对于用DOSV2·X的FDISK命令建立分区的硬盘的解毒与修复，以及软盘根目录区的修复。

1.恢复硬盘主引导程序

当硬盘主引导程序被破坏时，可把另一正常硬盘(最好是同类型硬盘)的主引导记录拷贝在一张软盘上，将它与被破坏的硬盘主引导进行比较。若除个别地方外主引导程序基本相同，则可参照正常的主引导程序进行修改，或者干脆用正常主引导程序直接覆盖遭到破坏的主引导程序。注意，先不要修改主引导程序后面的分区表信息(IBEH～IFFH部分)，以免破坏硬盘分区表，造成无法弥补的损失。

如果找不到其他硬盘，可试着自行修改。在主引导程序破坏不太严重的情况下，只要将001 AH字节必为"06"，将001 BH、0089H、008 AH字节改为"00"，即可使硬盘正常启动。

以上恢复硬盘主引导程序的工作最好的对硬盘解毒前进行，即应对有毒硬盘FAT区中主引导记录所在扇区做修改，以便下一步进而恢复硬盘分区表信息。

2.恢复硬盘分区表信息

当大麻病毒侵入造成硬盘不能正常启动时，硬盘分区表也可能被破坏。只是由于大麻病毒在对硬盘进行染毒的同时，还保留了一份分区表的备份，才使其危害未立即表现出来。但若我们使用前面所述一般的简单方法进行解毒后，则会造成分区表的彻底破坏。因此，在发现硬盘不能启动时，则在恢复主引导程序后，还应恢复硬盘分区表信息。其具体做法是，在按第1条做好硬盘主引导程序的修复工作后，再将大麻病毒所保存的正常分区表信息移至主引导记录的相应位置。这样便得到了正常的硬盘主引导程序和分区表信息。这时，再将其写入硬盘主引导区，就完成了硬盘的解毒和主引导程序、分区表信息的恢复工作。

这里需要强调指出的是，目前社会上一些大麻病毒的解毒软件，在对磁盘解毒时大多采用简单的方法进行处理，不但不能恢复遭到破坏的硬盘主引导程序和分区

表，反而可能丢失原有的一些重要信息，造成硬盘的严重损坏，希望广大计算机用户引起注意。如果万一出现这种情况，可按第一条所述先恢复硬盘主引导程序，再用硬盘启动机器。如果不能启动，那便是分区表已被破坏，这时可试按以下步骤恢复分区表信息：

(1)在 DEBUG 下通过一段小程序调入硬盘主引导区。

(2)检查 IBEH～IFFH 的分区表信息，在 IBEH、ICEH、IDEH、IEEH 处寻找活动分区标志“80”，若无“80”，可将“8 X”改为“80”。

(3)若已知该硬盘全部分配给 DOS，则除活动分区外，其余分区应全部清“0”。否则，仅将其余分区标志处修改为“00”。

(4)将活动分区前 5 个字节改为“80 00 02 00 01”，(表示活跃的操作系统分区从硬盘 0 头 0 道 2 扇区开始，其 FAT 每个表项长 1.5 字节)，第 10～12 字节、第 15～16 字节全部改为“00”。

(5)将修改后的分区表信息与主引导程序一起写入硬盘主引导区。经过上述修改，一般硬盘即可正常启动了。如果仍不能启动硬盘，则需找一台同类型并装有同样系统的硬盘，参照其分区表信息进行修改。

3.恢复硬盘 FAT

当硬盘感染了大麻病毒后，其 FAT1 某一扇区就被破坏，如果此后 DOS 对文件的写操作不涉及该扇区簇号的更新，则 FAT2 相应扇区写至 FAT1。这样，被破坏的 FAT 便会完全恢复正常。

如果已经发现两分 FAT 相应扇区均破坏，可借助于 CHKDSK 命令和 PCTOOLS 工具，仍可恢复 FAT 该扇区的大部分及至全部链簇。其具体步骤如下：

(1)键入“CHKDSK C:*.*”(按回车键)，检查硬盘。记下有簇链错误的文件名，同时这些文件中有不相邻块(non-contiguous blocks)的文件。

(2)在 DEBUG 或 PCTOOLS 下进入磁盘根目录区，抄录下第一步所记文件的首簇号(在目录表项第 27、28 字节处)。

(3)检查第一步中记下的具有不相邻块的文件，如该文件能够正常使用，可将其拷贝至软盘或硬盘子目录内。

(4)删除第一步中记下的有链簇错误的文件。

(5)进入 PCTOOLS，用 Undelete 功能去恢复刚才被删去的文件。恢复的顺序是：先恢复长度不超过一簇的文件(10MB 硬盘为 4096 字节，20MB 硬盘为 8192 字节)，再恢复长度超过一簇但无不相邻块的文件，最后恢复长度大于一簇且有不相邻块的文件。恢复有不相邻块的文件时，要先恢复首簇号不在被破坏 FAT 扇区内的文件。恢复文件时应使用 F1 键(自动恢复)。

(6)多数文件经过恢复后均可正常使用，读者可逐一检查，若还有少数文件不正常，可再删去并重新恢复。注意，这些文件都是有不相邻块的文件，再次恢复时应重新调整文件的先后顺序。

(7)若几次调整顺序恢得仍有文件不正常，则该文件簇链无法恢复正常。可删去这些文件，不必再恢复。

(8)将第 3 步拷贝在软盘或硬盘子目录下的文件拷贝回根目录中。

上述工作完成后，硬盘便基本可以正常使用了，只是用 CHKDSK 命令检查硬盘，仍显示有一百多个链簇丢失，这是由于病毒程序占据了空闲的结果。这时，可用 CHKDSK 命令的 F 参数对硬盘进行处理，再删去 F 参数所建立的 FILEnnnn.CHK 文件，即可使硬盘释放掉这些无用的链簇。

上述所有涉及硬盘写操作的工作均需特别小心，为防止误操作，最好在操作前对有关扇区内容作好备份。

4.恢复软盘文件

大麻病毒感染到软盘上后，位于软盘根目录区的部分文件目录将被破坏。在对软磁盘解毒后，还需恢复被破坏的文件。由于这些文件仅仅是目录区遭到破坏，其在 FAT 中的簇链和数据区中的文件内容仍完好无损，因此，可以借助 DOS 的 CHKDSK 命令或 RECOVEER 命令很方便地恢复它们。下面介绍一下使用 CHKDSK 命令恢复文件的步骤：

(1)如果解毒后软盘根目录区被破坏的扇区未予清“0”，可将该扇区清“0”

(2)键入“CHKDSK d:/F”(按回车键)，并回答“Y”去恢复文件。CHKDSK 将把簇链完好的文件恢复成名为 FILEnnnn.CHK 的文件(nnnn 从 0000 开始)，这些文件的长度均为 1 KB 的倍数，大于或等于原文件长度。

(下转第 42 页)

(上接第 45 页)

(3)在 DEBUG 或 PCTOOLS 下打开文件,根据文件内容、特征,找到文件结束处,确定文件原长度,部分或全部确定文件原名称。例如:若是文本文件或 DBF 文件,其内容基本是可阅读的,且其结束标志为"1 A"。若是 EXE 文件则其第 1、2 字节肯定是"4 D 5 A",且可通过其第 3 ~6 字节计算文件原长度。具体方法请参阅有关资料,本文不再赘述。

(4)对于实在不能确定原名称和长度的文件,可以根据文件内容重新起一个合适的名称并保留其现长度,不会影响文件正常使用。

若用 RECOVER 命令做这一工作。应注意将未遭破坏的正常文件(包括遭破坏扇区后面的文件)先采取措施拷贝在其他盘上保护起来,以免也被改名。

经过上述工作,软盘文件便恢复正常,可以投入使用了。

我们所开发的圆点/大麻病毒解毒免疫软件 QDL-2 D·COM 在对磁盘进行解毒的同时,对于被病毒破坏的磁盘数据均尽可能自动地予以恢复,不能自动恢复的也保留了必要的信息,以便手工顺利恢复。QDL-2 D·COM 本自备有 5 种不同的硬盘主引导程序,在对硬盘解毒时可恢复遭到不同程度破坏的主引导程序和分区表,避免一般解毒软件的缺陷。经过一段时间的考验后,该软件已推广至全国工商银行系统使用。本文所述有关磁盘解毒、修复方法同样也适用于被"六·四"病毒破坏的磁盘。

本文所述修复磁盘主引导区、FAT 区及根目录区的方法,原则上也适用于因意外原因遭到非物理损伤的各种硬盘或软盘。

▲