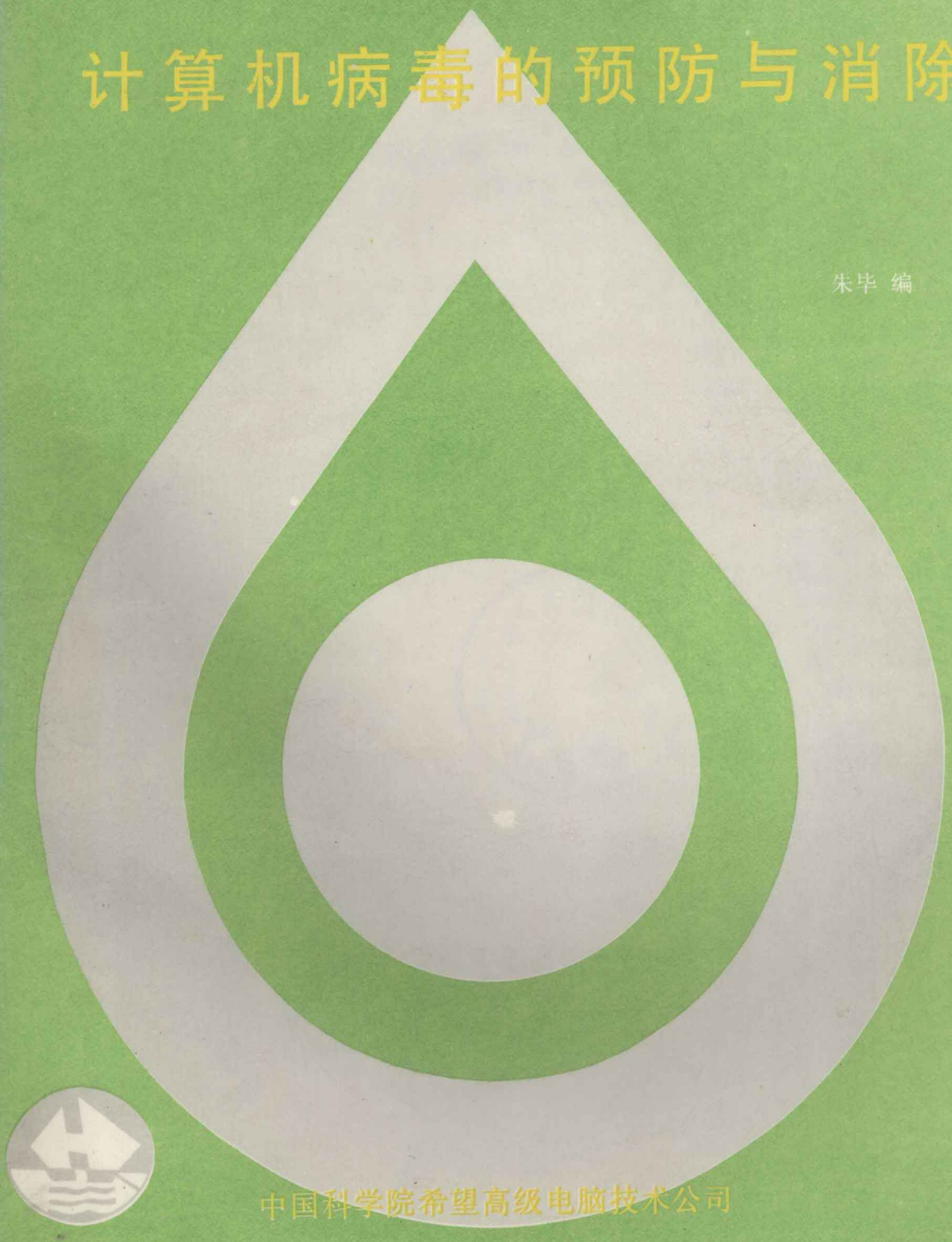
HOPE

IBMPC实用技术高级专题

计算机病毒的预防与消除

朱毕 编



中国科学院希望高级电脑技术公司

IBM PC 实用技术高级专题

计算机病毒的预防与消除

朱 毕 编

中国科学院希望高级电脑公司
一九九二年一月

序　言

病毒是极其影响工作效率的一种程序，病毒的产生，使得人心惶惶。人们为了消除病毒，编制了一些反病毒的程序。但监视和跟踪病毒的努力既浪费时间，反病毒程序也降低了计算机的执行效率。因此跟踪病毒的软件如WATCHDOG、WATCHMEN也不得以成为反病毒的“病毒”。

本书致力于病毒的预防和消除。

介绍了病毒预防与消除的功能都很强大的软件包Turbo Anti-Virus。该软件包中的BootSafe程序能备份好的BOOT区，既使感染BOOT区型的计算机病毒之后，只要用无毒启动盘启动，即可恢复原无毒BOOT区。TSafe象人的眼睛一样能时刻提防BOOT区和文件型病毒侵染计算机，发现可疑征状后立即告警，并引发热启动。

Turbo Anti-Virus能查消154种国际流行的病毒，用本书中的程序编译后生成的程序KILL1能消除目前国内所有的BOOT型病毒。

本书编者建议人们不要因编写计算机病毒而成为人们憎恶的“病毒”。

编　者

目　录

第一章　DOS 技术基础

攻击 PC 机的病毒程序通常都巧妙地利用了磁盘操作系统(DOS)的各种强大功能，以实现其传染、隐藏、破坏等目的，有的病毒程序编程水平非常高，因此分析和解消计算机病毒时要求我们对 DOS 系统有足够的了解，本章就六个大的方面对 DOS 系统作了较详细的介绍，这些方面包括了病毒经常使用的各种技术，对于我们搞清楚计算机病毒的原理和机制、消除和免疫是很有帮助的，有兴趣的读者不妨仔细阅读一遍本章的内容，相信你们会有不小的收获。对那些已经比较了解 DOS 系统的读者来说，本章有些内容就显得过于浅显了，因此可以挑选某些节次，比如第二节 DOS 是如何启动的等等加以阅读。

本章包括以下六节内容：

§1. DOS 系统概述
§2. DOS 是如何启动的
§3. DOS 是如何加载文件的
§4. DOS 中断系统
§5. DOS 的文件管理系统
§6. DOS 内存分配

§1.1　DOS 系统概述

§1.1.1　DOS 系统的发展过程

自 1980 年 IBM 公司为其设计的个人计算机系统选定 Microsoft 公司出品的 PC-DOS1.0 作为标准操作系统以来，DOS 的发展历程已经经过了将近十年时间。在这十年中，几乎是连续不断地有 DOS 的新版本推出，这些新版本通常与比其版本号低一些的 DOS 系统完全兼容，并且每一个新版本都增加了一些以前没有的新功能。操作系统的一步步发展是为了适应 PC 机家族逐渐扩充的需要的。自从基本型 PC 机后，IBM 公司又相继推出了 IBM PC/XT，IBM PC/AT(286)，以及 IBM 386 等功能越来越强的新机型，因此 DOS 操作系统也相应地有着与此几乎相同的发展轨迹。

下表描述了 DOS 系统的发展过程

版本号	时间	特　　点
DOS1.0	1981.10	PC机的第一个操作系统，仅支持单面软盘
DOS1.1	1982.10	这是广泛用于PC兼容机的操作系统，可支持双面软盘
DOS2.0	1983.3	PC/XT所用操作系统，支持硬盘
DOS3.0	1984.8	PC/AT(286)所用操作系统，支持1.2MB软盘和大容量硬盘
DOS3.1	1984.11	支持Microsoft网络服务系统

DOS3.2	1986.3	支持3.5英寸软盘，且驱动器中固化了盘格式化程序
DOS3.3	1987	支持虚拟盘，支持硬盘分区且可支持PS/2系统
DOS4.0	1988.6	这是到现在为止最高的DOS版本，支持大于32M的单一分区及许多强大功能

§1.1.2 DOS 常用命令分析

DOS 经启动进驻内存后会出现提示符“>”，此时 DOS 等待用户键入一个 DOS 命令或一个应用程序的命令行。前者是 DOS 提供给用户使用的各种功能，这些功能分为两类，分别称为 DOS 内部命令和 DOS 外部命令。

执行 DOS 命令时必须遵守以下规范

1. 内部命令在 DOS 常驻内存后的任何时刻均可执行。外部命令包含在扩展名为 COM 或 EXE 的文件中，只有这些文件存在于指定驱动器中时才可执行。

2. 各种命令在揭示符“>”后发出，用 RETURN 键确认，若没有出现错误信息则表示该命令执行成功。

3. 有的命令后面可跟一个或多个参数，系统按指定的参数执行相应的 DOS 功能，若未键入参数，则按缺省值处理。多个参数之间通常用空格或逗号、分号等隔开。

4. DOS 提供某些键或键的组合来完成一些特殊功能。

下表列出了所有的 DOS 内部命令(3.0 以上)

命　令	解　　释
CD	改变当前目录
CLS	清屏
COPY	拷贝磁盘文件
CTTY	改变主控制台
DATE	修改系统日期
DEL	删除磁盘文件
DIR	列文件清单
ERASR	删除磁盘文件
MKDIR	建立子目录
PATH	建立搜寻目录
PROMPT	定义系统揭示符
REN	修改文件名
RD	删除空目录
SET	设置运行环境

TIME	修改系统时间
TYPE	显示文件内容
VER	显示DOS版本号
VERIFY	验证写盘数据
VOL	显示磁盘卷标
ECHO	显示字符串
FOR	循环执行命令
GOTO	控制跳转命令
IF	条件执行命令
PAUSE	暂停命令
REM	显示注释信息
SHIFT	移位替换参数
BREAK	中断DOS开关
BUFFERS	置DOS缓冲区
COUNTRY	指定国家名称
DEUICE	安装设备驱动程序
FCBS	置打开的FCB数
FILES	置打开文件数
LASTDRIVE	置最后驱动器号
SHELL	定义外壳程序

注: 上表中自 BREAK 以后为系统配置命令。

下表列出了所有的 DOS 外部命令

命 令 字	解 释
ASSIGN	分派驱动器请求
ATTRIB	置文件只读属性
BACKUP	磁盘文件转储
CHKDSK	磁盘状态检验
COMMAND	加载命令处理程序

COMP	磁盘文件比较
DEBUG	DOS调试程序
EISCOPY	复制整张软盘
EDLIN	行编辑程序
EXEIBIN	EXE文件转换成COM文件
FDISK	硬盘分区
FIND	输出指定字符串
FORMAT	磁盘格式化
GRAFTABL	装入附加图符表
GRAPHICS	拷贝屏幕图形
JOIN	将驱动器连接目录
KEYBYY	装入键盘替换程序
LABEL	设置磁盘卷标
LINK	DOS连接程序
MODE	设置设备操作方式
MORE	屏幕显示过滤
PRINT	假脱机打印文件
RECOVER	恢复磁盘文件
RESTORE	磁盘文件复原
SELECT	选择国别代码
SHARE	装入文件共享程序
SORT	文件排序过滤
SUBST	驱动器替换路经
SYS	传送系统隐含文件
TREE	显示树型目录

下表列出了所有的 DOS 专用键

键组合	解释
Ctrl+Alt+Del	系统热启动

Ctrl+Break(或Ctrl+C)	中止命令运行
Shift+Prtsc	当前屏幕打印
Ctrl+P	打印机联机开关
Ctrl+Numlock(或Ctrl+S)	暂停命令执行开关
F1或→	从最后一行起一个个显示字符
F2	显示最后一行中指定字符前所有字符
F3	显示最后一行
F4	跳过最后一行指定字符前的字符
F5	存储当前行
F6	给出文件结束符Ctrl+Z

下面我们介绍一些常用的 DOS 命令：

§ 1.1.2.1 DIR 命令

格式：DIR[d:][Path][filename][/p][/w]

解释：列文件清单命令，被文件型病毒感染的系统中用此命令查看文件长度，可发现某些文件变长了，该文件有可能就是染有病毒的文件。

[d:] 表示驱动器号
[Path] 表示路径名
[filename] 表示文件名
[/P] 表示逐屏显示
[/W] 表示多列显示

举例：

```
A>DIR C:\SAFE\*.*
Volume in drive C has no label
Directory of    C:\SAFE
.              <DIR>      2-05-91     4:05p
..             <DIR>      2-05-91     4:05p
SCAN    EXE    46912    12-17-89    12:52p
KILL    EXE     8256     1-01-80    12:04a
SCAN63  EXE    46535     6-02-90     6:06p
        3 File(s)     3350528 bytes free
```

§ 1.1.2.2 COMP 命令

格式：[d:][Path]COMP [d:][Path][filename]
[d:][Path][filename]

说明：磁盘文件比较命令。这是一个 DOS 外部命令，最前面的[d:][Path]指名了 COMP

文件所在的驱动器号及路径名。之后的两个[d:][Path][filename]分别表示两个待比较的文件，前一个称为主文件，后一个称为次文件，在内存中驻留有某些病毒时，我们用 DIR 命令看不到文件长度的增加(如 4096 病毒)，但如果我们用 COMP 命令比较一个正确的文件和一个被感染过的文件(必须是两个长度一样的文件)时，就有可能发现病毒。

举例：

```
A>COMP A:A1.EXE B:A2.EXE
Compare error at offset 156
File1=MZ
File2=ND
1 Mismatches ending compare
```

§1.1.2.3 FDISK 命令

格式: FDISK

解释: 硬盘分区命令。这是一个外部命令，只对硬盘操作。在硬盘物理格式化后用此命令建立分区，然后运行格式化命令，在这几个步骤完成之后，硬盘才真正可以使用。

用法:在 A>号下键入 FDISK

屏幕上会出现 FDISK 的菜单如下:

1. Create DOS Partition
2. Change Active Partition
3. Delete DOS Partition
4. Display partition Data

若系统配置了两个硬盘，则还有

5. Select Next Fixed Disk Dive

这些功能分别是建立 DOS 分区、改变活动分区、删除 DOS 分区、显示分区信息和选则下一个硬盘。

具体用法在一般的 DOS 手册上有详细介绍，此处不再讲述。

§1.1.2.4 FORMAT 命令

格式: [d:][path] FORMAT [d:][/s][/1][/8][/V][/8][/4]

解释：磁盘格式化命令，这是一个外部命令。当发生病毒的交叉感染等情况后磁盘数据变得无法挽回了，我们需要对其重新格式化。

最前面的[d:][path]指明了 FORMAT 文件所在的驱动器及路径。

[/s]参数表示格式化后立即传送三个系统文件，使之成为可以启动的系统盘.

[/1]参数表示将软盘格示化成单面的。

[/8]参数表示软盘采用每道 8 扇区的格式，否则采用每道 9 或 15 扇区的格式(缺省值)。

[/V]参数表示要求用户给出一个卷标。

[/B]参数表示为目标软盘格式化成每道 8 扇区的格式，同时分配空间准备存放 DOS 两个隐含文件。用 SYS 命令可将任何 DOS 版本的系统文件传送到 FORMAT/B 格式化的软盘上。若未用/B，则只有 2.X 版或 3.X 版的 DOS 才能用相应的 SYS 命令传送系统，

该参数不能与/8 和/V 同时使用。

[/4]表示在高密驱动器上对双面双密软盘进行格式化。

§1.1.2.5 系统配置命令

FILES 命令

设置同时打开的文件句柄数。最大值为 20，其中包括 DOS 为标准 I/O 设备预留的 5 个文件句柄:标准输入(0)，标准输出(1)，标准错误(2)，辅助输入输出(3)和标准打印(4)。用于用户程序的文件句柄数为 5-19，所以应用程序一次打开的文件不能超过 15 个。

格式:FILES=X; X 是 8-255 中任一个数,缺省值是 8.

FCBS 命令

设置同时打开的文件控制块数。在网络系统中，当装入文件共享支持软件 SHARE 后，本命令设置允许 DOS 一次同时打开的文件控制块数以及打开的 FCB 中不允许 DOS 自动关闭的文件控制块数。

格式：FCBS=m，n

m 指一次能打开的 FCB 数目，取值 1-255，缺省值为 4。

n 指打开的 FCB 中不能由 DOS 自动关闭的文件数目，取值范围为 0-255，缺省值为 0。

m 必须大于 n。

BUFFERS 命令

分配磁盘缓冲区数量命令。磁盘缓冲区是 DOS 用于存放从磁盘读取或写入磁盘的数据的一块内存。每区容量为 528 个字节。

格式：BUFFERS=X，X 是 1-99 中任一数，缺省值为 2。

DEVICE 命令

安装设备驱动程序命令。在 DOS 启动中，本命令将指定的设备驱动程序装入内存并常驻。

设备驱动程序为.SYS 文件或.BIN 文件，由设备头，策略过程和中断过程三部分组成，包含驱动设备运行的全部代码。

格式：DEVICE=[d:][path][filename]

[d:][pat]分别指明了设备驱动程序所在的驱动器号和路径；

[filename]表示该设备驱动程序的文件名。

所有的系统配置命令均应写在 CONFIG.SYS 文件中，当系统启 动时进行加载。

§1.2 DOS 是如何启动的

§1.2.1 DOS 的构成

DOS 由几个主要部分组成，每一部分对应用程序提供特定支持，这些部分分别称为 DOS Bios 模块，DOS Kernel 模块和 DOS Shell 模块。在 MS-DOS 中，这三个模块分别对

应三个文件，其文件名为 IO.SYS、MSDOS.SYS 和 COMMAND.COM，在 PC-DOS 中则为 IBMBIO.COM、IBMDOS.COM 和 COMMAND.COM。其中前两个文件为系统兼隐含型，用 DIR 命令看不到，但用 PCTOOLS 等软件可以看到。

§ 1.2.1.1 IBMBIO.COM 文件

这个文件完成 DOS 的基本输入输出管理功能。它是 DOS 中最依赖于硬件的部分，不仅提供所有标准设备驱动程序而且支持装载和初始化系统。

该文件由两部分组成，分别是系统初始化程序 SYSINT 和标准设备驱动程序。

SYSINT 程序完成系统启动过程中的初始化工作，其中包括确定内存容量、定位 IBMDOS.COM 解释 CONFIG.SYS 并设置系统运行环境等。

标准设备驱动程序由 11 个驱动程序的设备链组成。这 11 个驱动程序分为 6 类，它们分别是:

(1) 标准输入输出设备驱动程序，支持显示器和键盘，名为 CON。

(2) 标准制表设备驱动程序，支持打印机，名为 PRN，LPT1，LPT2，LPT3。

(3) 辅助输入输出设备驱动程序，支持异步串行通信接口，名为 AUX，COM1，COM2。

(4) 时钟设备驱动程序，支持时间和日期的服务，名为 CLOCK$。

(5) 块设备驱动程序，支持软盘和硬盘的操作，无设备名。

(6) 空设备驱动程序，支持应用程序的模块操作，其名为 NUL。

这些设备驱动程序由 IBMDOS 通过设备请求头调用。设备请求头是一个有定义的数据结构，含有请求操作的命令码。返回的状态字、传送的内存地址及扇区或字节计数器。设备驱动程解释这些请求并将其转化为不同硬件设备控制器相应的控制命令。

固化在 ROM 中的硬件驱动程序是独立的，它不仅可由 IBMBIO.COM 调用，而且也可以由应用程序调用。但由于 ROM—BIOS 依赖于硬件，所以直接调用 ROM-BIOS 功能的程序是无法在其它兼容机上运行的。

总之，IBMBIO.COM 是 DOS 内核与 ROM-BIOS 之间的接口，基于 IBMBIO.COM 的编程可运行于硬件不完全相同的兼容机。

§ 1.2.1.2 IBMDOS.COM 文件

这个文件完成 DOS 的文件管理和系统调用功能，它是 DOS 的核心。它也由两部分组成，它们分别是内核初始化程序和系统功能调用程序。

前者完成 DOS 内部的初始化工作。包括设置 DOS 中断向量入口，检查常驻的设备驱动链，建立磁盘参数表、设置缺省的磁盘扇区缓冲区等。

后者主要由系统功能调用 INT 21H 构成。该程序向用户提供了一套由 0-63H 子程序号组成的系统功能调用。这些调用都脱离于具体硬件，具有很好的兼容性。

这些功能分别是:

(1) 字符设备输入输出功能。

(2) 磁盘控制功能。

(3) 动态存储管理功能。

(4) 目录管理功能。

(5) 文件管理功能。

(6) 其它系统功能。

§ 1.2.1.3 COMMAND.COM 文件

这个文件是 DOS 命令的解释程序，它是操作系统和用户的接口。该文件由三部分组成，它们分别是常驻部分，暂驻部分和 Shell 初始化程序。

常驻部分由 IBMBIO.COM 加载到内存低端位于 DOS 内核和可安装的设备驱动程序之上。它包括中断 22H，27H(控制暂存应用程序的退出或驻留)，23H(Ctrl-C 处理)和 24H(严重错误处理)以及重新装入暂驻部分的加载程序等。

暂驻部分由 IBMBIO.COM 加载到内存高端。它包括命令解程序、内部命令程序、批处理程序等。该部分占据的存贮空间有可能被应用程序覆盖。当应用程序退出时，常驻部分检查暂驻部分是否仍然存在，若不存在则要重新加载暂住部分。

初始化部分在启动后退出内存。

§ 1.2.2 DOS 的软盘启动过程

§ 1.2.2.1 软盘的 DOS 引导记录

引导记录由三部分组成；它们分别是引导记录块、软盘 I/O 参数表、软盘基数表。

(1) 软盘 I/O 参数表

该表占 19 个字节，从偏移 0BH 处开始，具体内容如下表所示：

字节位移	含义	双面软盘	高密软盘
0-1	每扇区字节数	512	512
2	每族扇区数	2	1
3-4	保留扇区数	1	1
5	FAT表数	2	2
6-7	根目录项数	112	224
8-9	总扇区数	2DOH	960H
0AH	磁盘标志	FDH	F9H
0BH-0CH	每个FAT表所占扇区数	2	7
0DH-0EH	每道扇区数	9	15
0FH-10H	磁头数	2	2
11H-12H	隐含扇区数	0	0

(2) 软盘基数表

该表占 11 个字节，从偏移 21H 开始，下表描述了其详细参数: