Windows最佳共享程序设计

廖 林 张 斌 编著
东 岳 木 杉 审校

北京希望电脑公司

TP311
0044

Windows 最佳共享程序设计

廖 林 张 斌 编著

东 岳 木 杉 审校

北京希望电脑公司

内容摘要

本书对 Windows 共享程序和开发工具作了全面系统的阐述．全书内容包括：Windows 共享程序、文件与程序管理、图形、文字编辑与搜索、通讯、游戏、公用程序、建立和编辑源程序、资源编译器、建立帮助文件、Windows 调试器：CodeView、80386 调试器、诊断工具、消息监视工具、DDESpy、堆栈浏览器、性能分析工具、压缩和恢复文件．此外在附录部分对 Help 错误信息和资源编译器诊断信息作了描述．

本书内容新颖、论述全面．不失为计算机软件开发人员的一本难得的参考书．

欲购本书的用户可直接与北京 8721 信箱联系，电话 2562329，邮政编码 100080．

Windows 最佳共享程序设计

廖　林　　张　斌　编著

东　岳　　木　杉　审校

京准印字：3314—90314　　内部定价：20.00元

前　言

Windows是一个图形窗口操作环境，它的推出，使得操作计算机的方法和软件开发过程发生了革命性的变化。它提供了一种不同于以往的命令式操作手段，计算机的操作是通过诸如"对话"、"肖像"、"菜单"等图形画面和符号的操作来完成的。

Windows最大成功之一在于拥有一些相当实用的共享程序和开发工具。本书对Windows共享程序和开发工具作了全面系统的阐述。全书内容包括：Windows共享程序、文件与程序管理、图形、文字编辑与搜索、通讯、游戏、公用程序、建立和编辑源程序、资源编译器、建立帮助文件、Windows调试器：CodeView、80386调试器、诊断工具、消息监视工具、DDESpy、堆栈浏览器、性能分析工具、压缩和恢复文件。此外在附录部分对Help错误信息和资源编译器诊断信息作了描述。

本书内容新颖、论述全面。不失为计算机软件开发人员的一本难得的参考书。

本书的出版得到了北京希望电脑公司的大力协助，在此表示衷心的感谢。此外，由于时间仓促，不当之处在所难免，尚望读者提出批评指正。

作者

1993年1月

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

第一章　Windows 共享程序

1.1 如何使用 Windows 共享程序

Windows 最大成功之一在于已有一些相当实用的 Windows 3.x 版程序存在．这些程序称为"共享程序"(shareware)，本书收集了其中一些最佳的程序．

共享程序是一种全新的软件扩展方式，用户可在无须付费的情况下，就可共享到一些功能强大的程序．且在正式付费之前，还可先试用一阵子．试用过后若真的喜欢这些程序，就可正式注册购买，并可获得技术支持，更新的版本，及其它将在本章后面介绍到的产品．

1.2 Viruscan，Clear-Up 及 Vshield

计算机病毒不断地在软盘中秘密复制并寄生到其他程序，经过一段时间后具破坏性的病毒将毁损硬盘上的文件，或执行其他破坏性的动作．

使用 PC 之前，可以将 Windows 3 奥秘#1 软盘插入软盘驱动器中，使用它搜寻硬盘上的病毒．在 DOS 提示下，可以键入下列指令：

A: \SCAN C: D: E:

则 C:、D:、E: 磁盘机都会检查．除非使用其他参数(后面会提到)，否则 SCAN.EXE 将不在硬盘上写入任何信息．如果屏幕上显示"No viruses found"信息，表示的硬盘未受病毒感染；反之，当 SCAN.EXE 发现病毒，请即刻查询本章中如何删除病毒的相关数据．

SCAN.EXE 是以未压缩的文件格式放在软盘#1 的根目录上，让用户随时方便使用．因为本软盘贴有防写标签，在测试任何 PC 时不必担心感染病毒．SCAN.EXE 与 Clean-up，Vshield 及其他 McAfee Associates 程序则放在\VIRUSCAN 目录上，用户可以将它们拷贝出来，以自己惯用的方式使用．

1.3 VIRUSCAN 及 CLEAN-UP

本节告诉用户如何使用 VIRUSCAN 程序侦测病毒，及使用 CLEAR-UP 程序解毒．它们只提供用户相关的信息，要作更详细的了解，请参考程序的文件说明．附加名为 .DOC 的文件，可以使用打印机作每页 60 行的格式打印，而．TXT 文件则无法格式化打印．

VIRUSCAN(SCAN.EXE)

1 拷贝所有的 VIRUSCAN 文件至软盘上.

2 贴上防写标签。

3 将软盘插入 PC 中，并键入:

SCAN C: D: E:

VIRUSCAN 将检查 C:、D:、E: 磁盘，若无 D:、E: 磁盘，可以忽略不写.

4 如果发现病毒感染，可再执行 VIRUSCAN 加 / D 选项如下:

SCAN C: D: E: /D

/ D 选项将受感染的程序删除而不作复元的工作. 如果需要复原程序，请执行 CLEAN-UP 程序.

5 将计算机电源关闭，确定病毒从内存中删除.

CLEAN-UP(CLENA.EXE)

1 拷贝所有的 CLEAN-UP 文件至软盘上.

2 贴上防写标签.

3 关闭染毒系统的电源，重新以未受感染并贴上防写标签的系统程序软盘开机. 请注意: 如果以软盘开机后无法存取到所有的逻辑磁盘机，请检查软盘上的 CONFIG. SYS 文件，是否确定安装有存取硬盘的专用磁盘机驱动程序.

4 将 CLEAN-UP 软盘插入染毒的 PC 中，并键入:

CLEAN C: D: E[病毒标识码]

CLEAN-UP 即清除 C:、D:、E: 磁盘中的病毒，若无 D:、E: 磁盘，则可以省略不写. Jerusalem 病毒的标识码为[JERU]，Stoned 病毒的标识码为[STONED]，其它病毒的标识码可以从 SCAN 程序，或是 RIRLIST. TXT 文件知道，请勿存储方括号"["与"]". 如果想清除感染文件型的病毒，建议增加 / A 选项，以便检查所有文件.

5 关机后重新以硬盘开机.

重要注意事项: 至此已经完成了计算机系统反病毒工作，但是其他的计算机系统与磁盘可能已遭受病毒感染，当前已经拥有未受感染的 PC，藉以扫描及删除它们的病毒.

1.3.1 VIRUSCAN

1.3.1.1 摘要

VIRUSCAN(SCAN.EXE)为 IBM PC 及兼容计算机上侦测并标识病毒的程序，它搜寻内存引导区、分区表及所有文件中的已知病毒，并能侦测未知的病毒.

SCAN 从唯一符合于各种计算机病毒的指令或字符串搜寻病毒，而在发现病毒时予以警告。这是对已知病毒的解决方法，而对未知病毒，VIRUSCAN 产生验证码或是检查 COM 与.EXE 文件的 CRC，如果文件经过修改，则发出可能感染病毒的信息。VIRUSCAN 并能依用户指定的搜寻字符串侦测新的病毒。执行 VIRUSCAN 需有 256KB 以上内存的 PC，及 DOS 2.0 以上的版本。

1.3.1.2 版本验证

VIRUSCAN 执行时有自我测试的功能，如果发现程序受到修改，会发出警告信息，而继续其侦毒的工作。如果 SCAN 报告本身已遭受到修改，建议再从原版软盘拷贝过来。VIRUSCAN 46 版以上的程序与 VALIDATE 程序结合而成 SCAN.EXE，VALIDATE.DOC 文件说明如何使用 VALIDATE 程序。VALIDATE 程序随 VIRUSCAN 程序发表，用以验证 SCAN 的版本。78-B 版的验证结果如下：

FILE NAME: SCAN.EXE
SIZE: 80, 951
DATE: 02-15-1991
FILE AUTHENTICATION
Check Method 1: BD20
Check Method 2: 0D35

如果的 SCAN.EXE 文件与上述不同则可能经过修改，建议再从原版软盘拷贝过来。

1.3.1.3 概论

VIRUSCAN(SCAN.EXE)扫描整个系统以侦测系统感染的病毒，它能标识病毒的种类，并告知受到感染的区域(内存、驱动扇区、或文件)。染毒的文件能以 /D 选项删除，CLEAN-UP 程序则尽可能地修复受感染的系统。

74 版 VIRUSCAN 可以标识 217 种已知的计算机病毒及其变体。许多病毒都有变体存在，综合起来共有 475 种，其中 10 种的出现率高达百分之 95.VIRLIST.TXT 有详细的说明，而每一种病毒的变体数则列在病毒名称后的括号中。

已知的计算机病毒会感染下列的区域：硬盘分区表、硬软盘的 DOS 引导区、系统的可执行文件等。可执行文件包括操作系统文件、COM 文件、.EXE 文件、覆盖文件、及其他可以装入内存执行的文件。可以同时感染多个区域的病毒称为"多重病毒"。

VIRUSCAN 检查受感染的区域或文件，并标识病毒名称与列出用于 CLEAN-UP 解毒程序的标识码。SCAN 能搜寻整个系统、个别软盘、子目录或文件以判断病毒的存在。藉 Add Validation 与 Check Validation 选项，VIRUSCAN 也能搜寻新的未知病毒，作法是：计算一文件的标识码，记录在此文件中，用以作验证此文件之用。如果文件受到修改，则标识码不再相同，暗示此文件可能受到病毒感染。SCAN 以两次独立的 CRC(Cyclic Redundancy Check)检查码放在文件之后，具有自我测试功能的程序将不加以验证，因为如此等于关闭了它自我测试的功能；而具有自我修改功能的程序依修改的状况可能测出有许多病毒。VIRUSCAN 只在.COM 文件及.EXE 文件加标识码，而分区

此为试读，需要完整PDF请访问：www.ertongbook.com

表、引导区及系统文件的标识码则放在该目录的 SCANVAL．VAL 文件中。

VIRUSCAN 可以编辑病毒数据文件以搜寻新的病毒，只要用户输入藉以搜寻病毒的字符串。VIRUSCAN 可以更改或产生显示信息。VURUSCAN 可以在个别或网络 PC 上操作，但不能在文件服务器上使用。当在网络上操作时，需要 NETSCAN 文件服务器扫描程序。

1.3.1.4 操作

特别注意事项：用 VIRUSCAN 程序扫描系统的病毒之前，请为的软盘贴上防写标签。

VIRUSCAN 可以检查每一个指定磁盘机的区域或文件，如果发现病毒，则显示信息告知染毒的文件或系统区域，及感染到的病毒。SCAN 依文件的扩展文件名检查病毒，其预设的扩展文件名有.BIN，.COM，.EXE，.OV?，.PGM，.PIF，.PRG，.SYS 及.XTP。其他的扩展文件名可以自行加入 SCAN 之中，或是检查软盘文件中的所有文件，VIRUSCAN 的指令格式如下：

SCAN d1: …d10: /A/AV/CV/D/E. xxx yyy zzz
/EXT d: filename /FR/MANY/NLZ/NOMEM
/REPORT d: filename /R/X

选项如下

/A 扫描所有的文件的病毒。
/A 加验证码至指定文件。
/CV 检查文件的验证码。
/D 覆盖并删除染毒的文件。
/E .xxx .yyy .zzz 扫描覆盖扩展文件.xxx .yyy .zzz。
/EXT d: filename 依病毒数据文件扫描。
/FR 以法文显示信息。
/M 扫描内存中的病毒。
/MANY 扫描许多软盘，无需重复执行 SCAN。
/NLZ 跳过以 LZEXE 压缩的文件。
/NOMEM 跳过内存检查。
/REPORT d: filename 建立染毒文件的报告文件。
/RV 从指定文件删除验证码。
/X 扫描已绝种及纯属研究的病毒(此版 SCAN 不存在)
(d1…d10: 指定要扫描的磁盘机。

/A 选项指示 SCAN 扫描参考磁盘机的所有文件。这通常使用在已经侦测到文件感染病毒时，否则，/A 选项只用来检查新的程序。/A 选项须以充分的时间扫描。这个选项比/E 选项有较大的优先权。/AV 选项允许用户加验证码于指定的文件，如果

指定整个磁盘机，SCAN 将为分区表、启动扇区及系统文件建验证数据；验证码在文件之后加 10 个字节，而分区表、引导区及系统文件的验证数据存储在被扫描磁盘根目录的隐藏文件中。

• /CV 选项检查通过执行 /AV 选项而产生的验证码。如果发现文件经过修改，SCAN 将显示可能受到感染的信息。使用 /CV 选项会增加约 25%的扫描时间。请注意到一些旧的 HP 及 Zenith PC，当启动系统时会修改引导区与分区表，如果使用 /CV 选项，则 SCAN 依然会警告用户。请查询系统手册看是否有启动时自我修改的特性。

/D 选项告诉 VIRUSCAN 显示染毒的文件并询问用户是否删除?如果用户选择 "Y"，染毒的文件则以十六进位码 C3 覆盖[返回 DOS]，然后加以清除。以 /D 选项清除的文件无法还原。建议使用 CLEAN-UP 而不用 SCAN 清除染毒的文件，因为前者有修复的功能。/D 选项无法清除引导区及分区表，必需以 CLEAN-UP 来执行此项工作。

/E 选项允许用户加入扩展文件名侦测病毒。扩展文件名置于 /E 之后，可以包括 "."，但必须用空白字符分隔 /E 及其他选项。最多可同时使用三个扩展文件名，若需使用更多扩展文件名时，可用 /A 选项。

/EXT 选项使得 VIRUSCAN 通过一用户的文字文件中读取搜寻字符串以侦测病毒，格式如下:

/EXT d: filename

其中 d: 为磁盘机名称，filename 则为用户定义的病毒数据文件。可以参考附录 A 了解如何建立病毒数据文件。注意: /EXT 选项乃是提供给资深用户和计算机反病毒研究者，在暂时或紧急时测知计算机病毒之用。当同时使用 /D 选项时，文件将被清除。所以不可经常使用 /EXT 选项，并且建议谨慎使用。/FR 选项告诉 VIRUSCAN 以法文显示所有信息。/M 选项告诉 VIRUSCAN 检查寄生在内存中的所有已知病毒。SCAN 预设能侦测内存中危险的潜伏性病毒，这些病毒在扫描时能造成致命性的破坏。不管任何状况，SCAN 都会检查下列病毒:

1554	1971	1253	2100
3445-Stealth	4096	512	Anthrax
Brain	Dark Avenger	Disk Killer	Doom-2
EDV	Fish6	Form	Invader
Joshi	Microbes	Mirror	Murphy
Nomenclature	Plastique	Polish-2	P1R(Phoenix)
Taiwan-3	Whale	Zero-Hunt	

如果发现这些病毒，SCAN 将停止执行，并要求用户关闭电源，重新用未染毒的系统软盘开机。或与其它侦/解毒程序同时执行，如果这些程序未由内存中消除搜寻字符

串，SCAN 可能造成误判．使用／M 选项将增加 10-40 秒的扫描时间．

• ／MANY 选项用以扫描同一磁盘机中的多块软盘．如果用户有一片以上的软盘需要检查，则／MANY 选项允许用户不需重复执行 SCAN 而能完成工作．如果系统未受感染，／MANY 与／NOMEN 选择将可增加执行速度．

• ／NLZ 选项要求 VIRUSCAN 无需检查以 LZEXE 程序压缩的文件内部，但依然检查外在病毒．

• ／NOMEM 要求 VIRUSCAN 不检查内存，它适用在已知未染毒的系统．

• ／REPORT 用于产生染毒的程序清单文件．这个清单以 ASCII 文字文件的格式存储．使用／REPORT 的格式如下：

／REPORT d: filename

[请参考后面的范例]

• ／RV 选项用以清除软盘、文件或子目录的验证码．在软盘上使用／RV 将清除分区表，引导区及系统文件的验证码．／RV 选项不能与／AV 选项并用．

／X 选项用以检查"绝种"的病毒，所谓绝种的病毒乃指过去 12 个月来没有感染报告，或是纯为研究用的病毒，它们几乎不流通于一般用户之间．在 VIRLIST．TXT 文件中，绝种病毒以"＊"注明．建议刚开始时使用＼X 选项，以后则无需使用．

注意：绝种病毒并无确切的区别，所以＼X 选项已被删除．

1.3.1.5 范例

下列范例指示如何使用 SCAN:

SCAN C: 扫描 C 磁盘机．

SCAN A: R-HOOPER.EXE 扫描 A 磁盘机的 R-HOOPER.EXE 文件．

SCAN A: ／A 扫描 A 磁盘机的所有文件．

SCAN B: ／D／A 扫描 B 磁盘机的所有文件并指示删除染毒的文件．

SCAN D: E: ／AV／NOMEM 中验证码至 C、D、E 磁盘机的所有文件，但跳过存储体检查．

SCAN C: D: ／M／A／FR 扫描内存，C、D 磁盘机中所有文件的已知及绝种病毒，并以法文显示信息．

SCAN C: D: ／E.WPM.COD 扫描 C、D 磁盘机中以.WPM 与.COD 为扩展文件名的文件．

SCAN A: ／CV 检查 A 磁盘机中已知与未知的病毒(从验证码)．

SCAN C: ／EXT A: SAMPLE．ASC 扫描 C 磁盘机中的已知病毒及定义在外部的病毒数据文件的病毒．

SCAN C: ／M／REPORT A: INFECTN．RPT 扫描内存与 C 磁盘机的所有文件，并于 A 磁盘机建一个 INFECTN．RPT 的文字文件．

1.3.1.6 结束码

当程序结束时，VIRUSCAN 设置 DOS ERROKLEVEL 值如下：

Error Level	说明
0	No Uirases found
1	One or more virases found
2	Abnormal termination (program error)

当用户停止扫描时，SCAN 将视是否发现病毒而设 ERRORLEVEL 为 0 或 1.

1.3.1.7 病毒删除

发现病毒时该怎么办?可以索取解毒公用程序及病毒的详细数据．CLEAN-UP 程序可以解决大多数的计算机病毒，随着新病毒的出现，它亦作不断的更新．

建议处理病毒时要特别谨慎，尤其是能侵入到分区表及引导区的危险性病毒(列于上述／M 选项中)，不当的处理会导致数据的流失或磁盘的损坏．

引导区受感染者:

关闭染毒的系统电源，以未染毒且贴上防写标签的系统软盘重新开机．使用 DOS SYS 命令以重新覆盖启动扇区．可依 VIRUSCAN 视病毒是否可被清除而成: 如果为无法清除的病毒，须先执行文件备份，换句话说，不可以备份启动扇区，然后作低阶的软盘格式化动作．如果软盘受到感染，可将文件以 COPY 指令拷贝至未受感染的磁片，切勿使用 XCOPY 或 DISKCOPY 指令，否则病毒将随之传染．然后重新格式化或丢掉染毒的软盘．

文件感染型病毒:

关闭染毒的系统电源，以未染毒且贴了防为标签的系统软盘重新开关．以／D 及／A 选项执行 VIRUSCAN，扫描软盘中所有文件，并以原版程序置换．

分区表感染型病毒:

关闭染毒的系统电源，以未染毒且贴了防写标签的系统软盘重新开机．执行文件对文件的备份(换句话说，不可备份引导区)，然后作低阶的软盘格式化动作．

解毒公用程序可以用于大多数的计算机病毒．

1.3.1.9 建立病毒字符串文件

可用编辑程序或文字处理程序建扩充病毒数据文件，以 ASCII 文字文件存储且确定每一行以 CR／LF 作为结束．

注意: ／EXT 选项专供紧急或纯研究时使用，它适用于当前 SCAN 无法侦测的新病毒的权宜处理．使用此选项时务必对此病毒有充分的了解．搜寻病毒字符串格式如下:

```
# comment about Virus__1
"aabbccddeeff…" Virus__1__Name
#Comment about Virus__2
"gghhiijjkkll…" Virus__Name

"uuvvwwxxyyzz…" Virus__n__Name
```

其中 aa，bb，cc 等为要扫描字符串的 16 进位字符串．一行表示一种病．每种病毒的名称是强制性的，可以多至 25 个字母．每个 16 进位字前后需有双引号(")．SCAN 即利用此文件搜寻内存，分区表、引导区、系统文件，COM 文件，.EXE 文件及扩展文件名为.BIN，.OV?，.PGM，.PIF，.PRG，.SYS 与.XTP 的覆盖文件．病毒名称可以包括通用符号．

通用符号如下:

固定通用符号: 问号用以表示字符串中固定位置的通用符号．例如，字符串

E9　7C　00　10　?　37　C

可对应"E9　00　10　27　37　CB"，"E9 7C 00 10 9C 37 CB 及类似字符串，无论第五个字符是什么。

广域通用符号: 跟随着前后括号的星号("*")可以表示不同长度的相邻字符串，例如: 字符串

E9　7C　*　(4)　37　C

可以对应"E9 7C 00 37 CB"，"E9 7C 00 11 37 CB"及"E9 7C 00 11 22 37 CB"，而无法对应"E9 7C 00 11 22 33 44 37 CB"，因为，7C 与 37 之间超过 4 个字符，广域通用符号最多允许声明为 99 个字符．

每种病毒字符串至多可用 10 个通用符号．

1.3.1.10 注解

每行前端的井字符("#")代表此行为注解．可以将它用于扩充病毒数据文件，例如:

```
#New .COM virus found in file FRITZ.EXE from
# Schneiderland on 01-22-91
"53 48 45 50" Fritz-1 [F-1]
```

注解可用以描述病毒特性，存在病源的文件，及何时何处受到传染…等．

1.3.2 CLEAN-UP

1.3.2.1 摘要

CLEAN-UP(CLLEAN.EXE)为 IBM PC 及兼容性计算机的解毒程序．它能够搜寻并清除分区表、引导区、文件及用户定义的病毒．一般来说，CLEAN-UP 都能将感染区

域复原．对于 VIRUSCAN(SCAN.EXE)程序能判断的病毒，CLEAN-UP 都能轻易解决 CLEAN-UP 必须有 256KB 以上内存，并需 DOS 2.0 以上版本的 PC 上执行．

1.3.2.2 版本验证

CLENA-UP 执行时能够自行测试，如果发现 CLEAN 被修改，则发出适当警告，而后继续扫毒．如果 CLEAN 报告程序本身已受到损坏，建议以原版未受感染的程序重新拷贝．CLEAN-UP 与 VALIDATE 程序置于一起，以确信 CLEAN.EXE 文件的完整性．VALIDATE.DOC 指示如何使用 VALIDATE 程序．VALIDATE 亦可用于验证 CLEAN 的版本．74B 版的验证结果如下:

FILE NAME: CLEAN.EXE
SIZE: 105, 937
DATE: 02-15-1991
FILE AUTHENTICATION
Check Method 1: 207E
Check Method 2: 04B4

如果 CLEAN.EXE 不同于上列结果，则可能经过修改，最好以原版未受感染的程序重新拷贝．

1.3.2.3 概论

CLEAN-UP 搜寻系统中的病毒并加以删除．当发现受感染的文件，CLEAN-UP 即执行解毒的功能，并尝试修复染毒的部分：如果文件受到较稀有的病毒感染，则 CLEAN-UP 发出警告信息，并提示要用户清除染毒的文件，重新以原版文件拷贝复原。在这种情况清除的文件无法以 CLEAN-UP 复原．

1260	1591	1701	1704
4096	Alabama	Alamed	Ashar
Dark Avenger	DataLock	disk Killer	EDV
Fish	Flip	INvader	Jerusalem A
Uerusalem B	Jerusalem E	Joshi	KeyPress
Liberty	Music Bug	Pakistan Brain	PayDay
Ping Pong B	Plastique	Slow	Stoned
SunDay	Suriv03	Taiwan 3	Taiwan 4
V800	VacSina	Vienna	Violator
Whale	Yankee Doo-	ZeroBug	Bloody
New Jerusale		dle	

此为试读，需要完整PDF请访问：www.ertongbook.com