第12卷 第3期 华侨大学学报自然科学版 Vol.12 No.3
JOURNAL OF HUAQIAO UNIVERSITY
1991年7月 (NATURAL SCIENCE) Jul. 1991

计算机病毒及诊治

陈 建 生

[计算机科学(电脑)系]

摘要 本文研讨了计算机病毒、病毒传染、病毒预防措施，并介绍了PC上一组查毒、消毒软件的实现方法.

关键词 引导扇区，硬盘分区表，硬盘DOS分区

0 引言

计算机病毒是一种能在计算机系统间秘密传播的程序，它们或轻微地破坏用户的显示环境、显示嘲讽性语句，或严重至毁坏计算机硬盘中的全部数据、使整个计算机网络瘫痪。计算机病毒第一次在美国出现时严重地影响了商用个人计算机的软件产品，目前在港台地区相继出现计算机病毒恐慌风[1]，在我国大陆也发现多种PC病毒。研究并控制计算机病毒已迫在眉睫。本文通过对病毒的深入分析，说明计算机病毒是可以得到有效控制的，并介绍了华侨大学电脑系自行开发成功的PC病毒防治软件的实现方法。

1 计算机病毒分析

1987年Fred Cohen将“计算机病毒”定义为：一种能够“传染”(将自身复制到其它程序中成为其有机的一部分)的程序[2]。计算机病毒不仅能自我繁殖，而且具有对系统的某种攻击性，危及计算机的工作[3]。病毒的危害是双重的：一方面病毒可侵入到整个系统使其受感染，并在一定时机发病，去破坏用户的数据；另一方面，受传染的程序(或磁盘)又以同样的方式去传染其它的程序(或磁盘)，这样病毒由一个程序传到另一个程序，由一个磁盘传到另一个磁盘，通过软盘的跨系统使用又把病毒传到另一个系统等等。

1.1 病毒源

第一个带毒程序(或磁盘)易心术不正者人为地制造的，通过执行带毒程序(或用带毒磁盘启动系统)使病毒代码获得控制权，随后将不断地将病毒透明地传染给其它的程序(或磁盘)，受传染者又可成为新的病毒源去传染其它。

1.2 病毒的传染

本文1989—12—9收到.

计算病毒是何时进入系统的运行空间呢？有两种情况：（1）病毒代码隐藏在磁盘引导扇区或操作系统的代码中、在系统冷、热启动时被ROM中的装入模块读入执行；（2）病毒代码隐藏在可执行程序中，在用户运行该可执行程序时由操作系统读入执行。

病毒代码第一次获得控制权时就使系统进入带毒状态，即由病毒代码控制系统中部分关键性操作，尤其是磁盘读写操作（和网络传输操作）。病毒代码若控制磁盘操作则在用户进行正常的磁盘操作时将病毒代码写入（即传染）所用磁盘而使用户毫无察觉。与此类似，病毒控制的网络传输操作透明地传染网内其它系统。

前述的由带毒的引导扇区引入的病毒对磁盘的传染结果是使之具有相同的带毒引导扇区（称引导扇区型病毒）；由带毒的操作系统引入的病毒对磁盘的传染结果是使之具有相同的带毒操作系统（称操作系统型病毒）；由带毒的可执行程序引入的病毒对磁盘的传染传果是使其上的可执行程序具有相同的带毒形式（称外壳型病毒）。

1.3 病毒的发作和危害

多数病毒具有休眠期：某程序或磁盘被传染后即可使系统处于带毒状态，但不马上发病（虽然它已可作为新的病毒源不停地传染其它程序或磁盘），要在某种条件下受触发而激活去体现其破坏性。如，由机内的运行时间／日期触发（称为定时炸弹，time bomb），或由某特定事务处理的输入触发（称为逻辑炸弹，logic bomb）。

病毒或属良性，或属恶性，对系统的危害多种多样，参见表1。

表1 常见PC病毒特征表

类型	病毒名称	传染对象	传染区域	发病时刻	发病症状	占用内存	性质
引导扇区型	*Ball*	软盘 硬盘*DOS*引导	引导扇区 1空闲簇	从0点起 每30分钟	上下反复弹动的小球	2*K* 显式	良性
	Stoned	*A*:中软盘 硬盘总引导扇区	引导扇区 根目录	*DOS*启动时随机	*Your PC is now Stoned*	2*K* 显式	良性
	Brain	软盘	引导扇区 3空闲簇	使用系统盘若干次	(卷名被改) 内道磨损	7*K* 显式	恶性
	Crazycat	软盘 硬盘*DOS*引导	引导扇区 根目录	从0点起 每15分钟	更改程序运行中间结果	2*K* 隐式	恶性

操作系统型	病毒名称	传染对象	发病时刻及症状	性质
	Amiga	磁盘上的*COMMAND.COM*	四次传染后清除磁盘上的数据	恶性

外壳型	病毒名称	传染对象	发病时刻及症状	性质
	Jerusalem	可执行程序*.COM*和*EXE*	每逢13日且为星期五清除数据	恶性

由以上对病毒传染、发病过程的分析可以看出：只要系统中的关键性程序不被病毒控制，系统就不遭病毒的危害；只要能及时发现系统中的关键性程序被非法代码所占，就能在出现破坏性事故前发现并消除病毒。

1.4 常见PC病毒

表1为PC系列机中出现最多的病毒的技术特征。

1.5 病毒的防御

为防止病毒侵入，在系统使用中应格外小心，如软盘使用写保护标贴，将所有可执行程序的文件属性改为只读的，系统中仅使用一个引导盘，等等。这样可一定程度上防止病毒侵入、传播，但病毒往往在人们不留心时（如玩游戏或安装程序时）潜入，或通过网络悄然进入。

系统虽有染毒的可能性，但可在系统中装入专门的软件，一有病毒出现能立即报告（若是引导扇区型的病毒能立即清除），从而在病毒传染、发病前及时地加以控制。这种软件分为两类。病毒预防和病毒检查[4]。病毒预防程序（如下述的VL，Virus lookout）驻留于内存中，随时监视运行中的代码是否具有病毒侵入的特征，并阻止对关键性程序（如引导扇区、磁盘操作系统程序、可执行程序）的修改。病毒检查程序（如下述的VD，*Virus detection*）用于系统冷、热启动时例行地执行，检查本次启动时引导扇区、操作系统运行后是否引入病毒，若发现病毒立即发出报警并显示病毒类型。若是引导扇区型病毒还可彻底地加以清除（用下述的RV，*remove Viruses*）。

2　各类PC病毒的检查——VD的实现

为检测运行中的系统是否有毒，可从PCTOOLS等工具了解DOS报告的RAM大小与实际值的差异（对显式更改40H段的0013H、0014H单元——RAM的kb数单元——的*Ball*、*Stoned*、*Brain*等病毒适用）；或用DEBUG读取启动盘的引导扇区与标准的引导扇区的外观格式作比较，辅助判断是否染上病毒。但象Crazy Cat之类的病毒既不显式更改RAM的kb数单元，引导扇区外观又与标准的极为相似，用这两种简单方法无法判断。

考虑到病毒的最大特点在于其（透明）传染性，必更改（启动时立即更改，或延迟一段时间后更改）INT 13H（磁盘IO基层程序）或／和INT 26H（DOS的按扇区写磁盘程序）或／和INT 21H（DOS系统调用）的程序入口，使这些关键性程序由病毒代码控制以使透明地传播病毒。因此病毒检查程序VD从中断向量表入手，根据中断向量的更改情况判断病毒的存在并报告病毒类型。

须重点检测的中断类型有：05H、08H、09H、10H、13H、16H、17H（分别为屏幕打印、时钟中断、键盘中断、显示器IO、磁盘IO、键盘IO、打印机IO程序），因为这些BIOS程序被频繁地调用，若更改它们的入口于病毒代码中，病毒代码便在这些BIOS程序执行时掌握控制权。检查上述的中断入口地址，（1）若在ROM中，认为合法；（2）若在DOS的运行段与当前程序（VD）的运行段之间，认为被正常的常驻内存程序（如SK等）所改；(3)除了向量的段值为70H（IBMBIO．COM的工作段）需作进一步判断外，认为该中断已被病毒代码所占。DOS 3.00以后各版在IBMBIO、COM 初始化时将某些中断类型的向量原内容存于70H段的单元中，改新入口于70H段的代码中，新的代码在作一些判断、处理后间接地转入原来的入口。所以为判所该中断向量是否被更改，需且只需对间接转入点作类似的判断（上述（1）、（2）、（3））。

若类型13H（类型21H、26H的处理与此类似）中断被病毒所占，其入口地址可用来报告病毒类型：（1）若INT 13H入口的偏移量为某已知的病毒的设置值且程序首部若干字节与该病毒的INT 13H程序相一致，则显示出该病毒名称（如*Ball*，*Brain*等），进一步从含毒

的INT 13H程序的间接转入点是否在ROM或RAM的合法区域（方法与上同），判断是否还有第二层病毒。若有，报告其类型……如此不断递归可按顺序报告混合病毒的名称；②否则说明此病毒为新发现的，报告*Unknown*（不论是否已知的，只要是引导扇区型病毒均可消除，见下述）。

3 各类PC病毒的预防——VL的实现

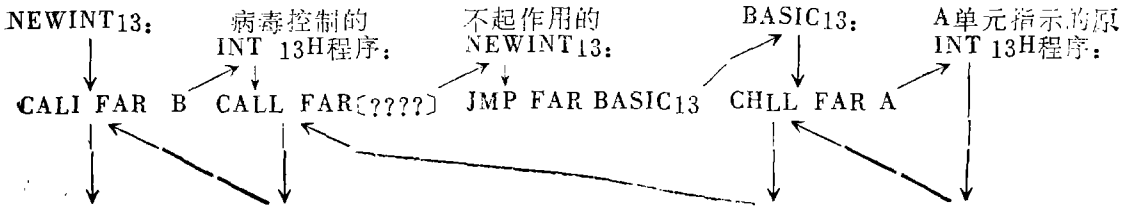
VL与VD作用不同。VD用于DOS启动时检测系统，确保启动后系统运行空间中无病毒代码。但病毒可能在某程序执行后引入，所以需有运行中时刻监视可能有的病毒侵入的机构。VL正是用于此目的，它能发现病毒的侵入特征（但不能象VD探测出病毒的类型及互嵌状态）。

为达到病毒传染的透明性，唯有在用户要求读、写盘时插入复制病毒代码的操作，方法是：取出并保存原磁盘操作程序的入口以备写病毒代码时用；更改其入口到病毒程序中。由病毒控制的磁盘操作程序通过调用原磁盘操作程序完成指定操作，此外调用原磁盘操作程序将内存中的病毒代码写入磁盘。总之，其特征是：在一次用户盘操作期间包含多次对原磁盘操作程序的调用。

可用来写磁盘的程序有：INT 13H程序（可读、写磁盘任意位置上的扇区）、INT 26H程序（可写软盘内和硬盘DOS分区内的任意扇区）、INT 21H程序（可读、写磁盘上任意目录下的文件）。因此VL严密地监视着这三个程序的调用情况。

*VL*的实现方法如下（以INT 13H为例）：（1）保存VL运行时的INT 13H入口地址于A单元（INT 13H程序的最内层的地址），将VL的BASIC13的地址存于B单元。BASIC 13通过调用A单元所指示的程序完成磁盘操作；（2）更改INT 13H程序入口于VL的NEWINT13处，NEWINT13通过调用*B*单元所指示的程序完成磁盘操作；（3）运用时钟中断程序迫使NEWINT13为INT 13H程序的最外层：若INT 13H的入口被改，则将新入口存于B单元，INT 13H入口重新改于NEWINT13并使前一级NEWINT13直接进入BASIC13程序。

假如某带毒的可执行程序运行后用INT 13H准备传染病毒，则内存中INT 13H程序调用流程为



一般地，每次用户要磁盘操作时执行NEWINT13，这期间BASIC13被调用且仅被调用一次。当病毒控制的INT 13H程序试图传染时，因其透明写盘而发生NEWINT13一次执行期间对BASID13进行两次以上的调用，由此VL可发现传染现象并及时报告。若系统运行于DOS 3.00以后版，VL可从D单元中的地址了解病毒代码所占用的内存区间，进而从相应的PSP（程序段前缀）中了解、报告此病毒是运行了何程序后引入的。

4　引导扇区型PC病毒的消除——RV的实现

为消除以引导扇区为传染目标的病毒，运用下面基本思想：模拟DOS启动过程，跟踪读出的扇区系列。先读入A：中软盘的引导扇区（或硬盘总引导扇区）到000：7C00H并执行之，若是含病毒的引导扇区，其执行过程中将读入原来的引导扇区（到0000：7C00H）并转入执行，这样不论是单一病毒或多种病毒互嵌，最后一次读到07C00H的扇区将是无毒的引导扇区，将它写入相应的引导扇区驻盘位置即可消毒（此过程不仅可消毒，而且可了解病毒代码的驻留位置及调入执行的顺序）。

依此设计，实现了消毒程序RV：（1）确定开机后ROM BIOS设置的INT 13H入口（在ROM），以后RV读写磁盘时用此INT 13H程序，以免在有毒的运行状态下的消毒过程所需的写盘动作同时把病毒也写入（因为往往用户发现病毒时其所有磁盘均已染毒，而在带毒的状态下每次磁盘操作均可传播病毒）；（2）将RV自举到RAM高区，为启动DOS作准备；（3）更改INT 13H入口于RV中的相应程序；（4）执行INT 19H重新启动DOS。

RV中的INT 13H程序仅读盘不写盘（从而避免了启动待消毒盘时的病毒传染，RV需写盘时直接用ROM中的程序）；若读入数据块的地址为07C00H，（1）对于软盘消毒：将每次读得的数据写于A：盘0道0面1扇区。（2）对于硬盘消毒：判断本次读入的是否硬盘总引导扇区，若是，写入C：盘0道0磁头1扇区；否则写入C：盘之DOS分区的引导扇区。今后，很有可能造出（国际上目前尚未发现）不保留原引导扇区备份的病毒，对未来的这种病毒RV采用另一工作方式：按照具体磁盘参数生成引导扇区并写入待消毒盘。为生成正确的软盘引导扇区、硬盘DOS分区引导扇区，使用RV自备的引导扇区标准代码，其首部的磁盘参数表根据待消毒盘（在内存中）的BPB（磁盘参数块）设置。同时，为生成正确的硬盘总引导扇区，使用RV自备的引导扇区标准代码，其尾部的硬盘分区表取自待消毒盘的当前分区表。

5　结束语

本文对病毒的分析、防治方法适用于各类计算机。VD、VL、RV运行于PC、XT、AT及其各类兼容机（DOS 2.00以后各版）。RV的突出之处在于它不是只对某一种或特定的某几种病毒作消毒，而是对一切引导扇区型PC病毒消毒，且不论是否同时含有多种病毒均一次性彻底消除。VL在处理公认的比较棘手的“在线监视”问题上也有独到之处，可完全冻结病毒的破坏能力。

参 考 文 献

[1] 电脑病毒专访，微电脑技术，6(1989)，41—43.
[2] Virus, Worms et al, *Software World*, 20, 3 (1989), 12—14.
[2] Martin King, Viruses and related mechanisms. *Sofware world*, 20, 1 (1989), 2—4.
[4] 熊璋，计算机病毒与防治，计算机世界周报，28(1989)，32—33.

Computer Viruses and Methods of Detection and Disinfection

Chen Jiansheng

(*Department of Computer Science*)

Abstract This Paper deals with computer viruses, their detection and Preventive measures, and the implementation of a set of detecting and disinfecting software on a personal computer.

Key words boot sector, fixed disk partition table, fixed disk DOS partition