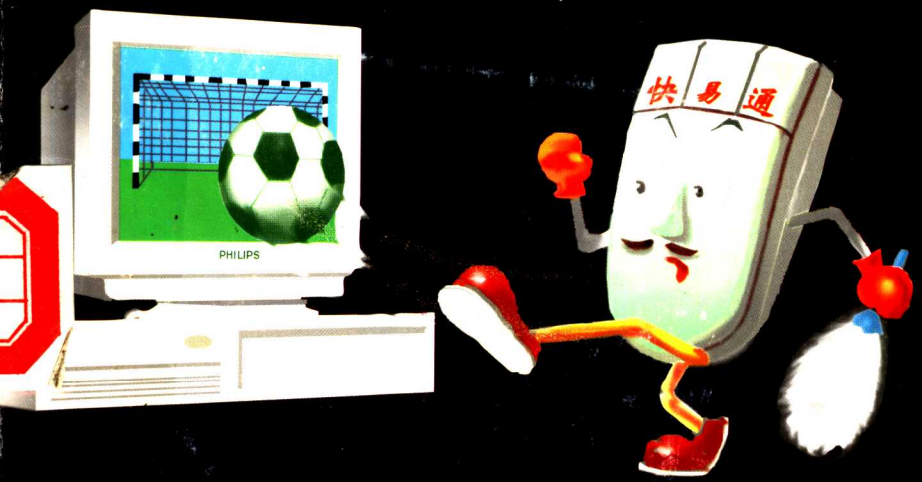
电脑系列丛书

电脑病毒防治快易通

张保田 编

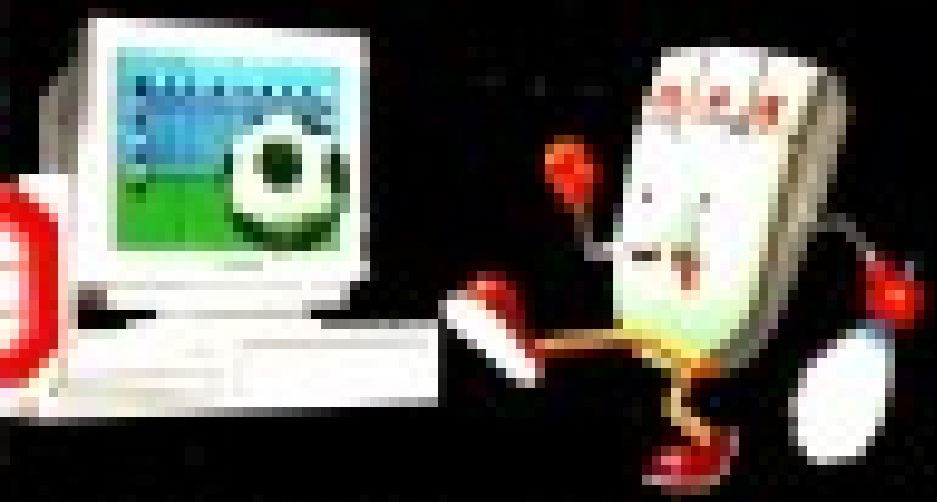


電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

电脑病毒丛书

电脑病毒防治快易通

[illegible]编



电子工业出版社

快易通电脑系列丛书

电脑病毒防治快易通

张保田　编

電子工業出版社

内 容 提 要

本书对于病毒的基本知识、结构、机理、种类以及防反病毒的原理、产品给出了比较详细的描述和分析，对于一些常见的热点问题也给出了详细解答。对于计算机用户更好地保护自己的资源免受病毒侵害提供了很好的帮助。

本书用于计算机用户，病毒防治与研究的技术人员等参考。

快易通电脑系列丛书

电脑病毒防治快易通

张保田 编

责任编辑：吴 源

特约编辑：李海鹏

*

电子工业出版社出版

北京市海淀区万寿路 173 信箱 (100036)

电子工业出版社发行 各地新华书店经销

电子工业出版社计算机排版室排版

北京市顺义县天竺颖华印刷厂印刷

*

开本：850 × 1168 毫米 1/32 印张：4.75 字数：127.6 千字

1996 年 8 月第一版 1996 年 8 月第一次印刷

印数：8000 册 定价：10.00 元

ISBN 7-5053-3455-7/TP . 1362

总　序

微型计算机(又称微电脑)的诞生,使人人用电脑成为现实。"信息高速公路"在全球的迅猛发展,网络对世界的"链接"与"并轨",将个人、家庭、企业与国家连成一体,使我们的世界变成了小小的地球村。一个全民学电脑、用电脑的深层次的普及已在我国兴起,并已成为提高劳动者素质,实现我国经济发展和科技进步的重要保证。

但是如何使用电脑,用好电脑,使电脑真正成为随心所欲的好帮手,则是广大群众所迫切需要了解和掌握的。

本套丛书就是这一背景下,由电子工业出版社、北京软件行业协会、中国电脑教育报、电脑爱好者杂志社,聘请国内计算机专家、教授、科普工作者精心策划编写的一套面向全民的计算机普及读物。丛书选材软硬件兼顾,硬件环境着重于目前的主流微型计算机;软件尽量采用最新版本。快! 易! 通! 体现了本丛书的最大特点。

快:《丛书》选材安排以"少而精"为原则,使读者在最短的时间内学到最基本也是最精华的知识。

易:《丛书》内容介绍上力求生动活泼、图文并茂、幽默风趣。对于专业术语及技术的论述,强调由浅入深,通俗易懂,尽量用生活化、拟人化的语言进行叙述。

通:《丛书》内容选择突出"实用性",即一本书介绍一个实际应用技术,学了就能用,内容重点在于使用与操作步骤。

《丛书》从书面编排、版式设计、标题结构、开本大小上也都突出了创意新颖的特点。

本《丛书》的读者对象是:在校的中小学生及家长;为适应形势而需要学习电脑的各类人员;电脑爱好者、使用者、自学者;各种短训班学员以及各年龄结构、各种职业的人士。

本丛书是打开计算机殿堂的入门钥匙,以其实用、精炼、活泼、耐

读、新颖为宗旨，满足人们快节奏生活和学习电脑的愿望，消除人们对电脑的恐惧感、神秘感，使读者尽快地进入电脑这个神奇而又使人仰目的乐园。

“电脑插上就能用”这一口号已成现实；

“信息垂手即可行”这一目标已在眼前；

“丛书开卷便有益”这一愿望已经出现。

愿本丛书能成为你进入电脑世界最好的伙伴！

本套丛书的编写得到了各方面人士的大力协作，特别是北京市“三金”领导小组办公室（筹）华平澜主任的支持。在丛书的征名中，得到近千人的推荐，最后我们选中了江超和武俊车二位同志举荐的《快、易、通电脑系列丛书》为名，在此一并致谢！

主编　朱继生

1995.9.9

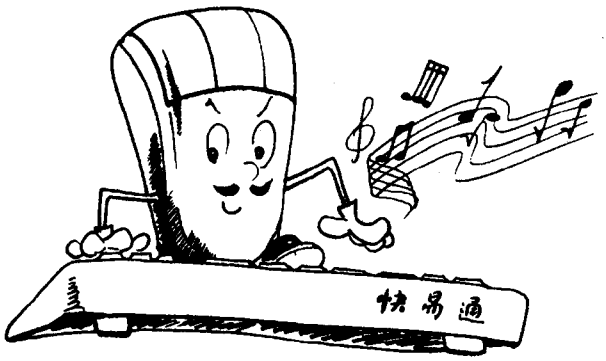
目　录

第一章　计算机病毒的基本知识 …… (1)
1.1　生物病毒与计算机病毒 …… (2)
1.2　计算机病毒的分类 …… (4)
1.3　计算机病毒的结构 …… (6)
1.4　计算机病毒的危害 …… (11)
1.5　深刻认识计算机病毒的传染性 …… (16)
第二章　磁盘结构与引导型病毒 …… (19)
2.1　磁盘结构 …… (20)
2.2　微机引导过程 …… (24)
2.3　引导型病毒 …… (26)
2.4　255 恶性病毒分析 …… (28)
第三章　可执行文件与文件型病毒 …… (33)
3.1　COM 和 EXE 文件 …… (34)
3.2　文件型病毒 …… (37)
3.3　PRG 文件杀手病毒分析 …… (40)
3.4　混合型病毒 …… (46)
第四章　计算机病毒的预防和诊治 …… (47)
4.1　计算机病毒的传染途径与外来软件 …… (48)
4.2　防止计算机病毒侵入微机的预防措施 …… (49)
4.3　计算机病毒的检测 …… (51)
4.4　检测引导型病毒 …… (52)
4.5　消除引导型病毒 …… (56)
4.6　检测文件型病毒 …… (59)
4.7　消除文件型病毒 …… (62)
第五章　反病毒产品的原理与选用 …… (65)
5.1　反病毒产品的分类 …… (67)

5.2 消病毒软件 …… (67)
5.3 防病毒卡 …… (69)
5.4 集成化反病毒卡 …… (72)
5.5 怎样选用反病毒产品 …… (75)
第六章 典型反病毒产品的应用 …… (79)
6.1 KILL 计算机病毒清除工具 …… (80)
6.2 反病毒软件包 CPAV …… (81)
6.3 SCAN 和 CLEAN 软件 …… (90)
6.4 华能 AVC-Ⅱ型反病毒卡 …… (95)
6.5 求真可升级消病毒卡 …… (98)
第七章 病毒与反病毒热点问答 …… (105)
第八章 流行病毒要览 …… (119)
附 录 …… (138)

第一章

计算机病毒的基本知识



在所有计算机软件中，有一类软件最不受欢迎，那就是计算机病毒。幽灵、黑色星期五、磁盘杀手……它们用不着用户去刻意收集，恰恰相反总是千方百计背着用户钻进计算机系统潜伏、传染、激发、破坏。每一位用户都憎恶病毒，却不得不同病毒打交道。

什么是计算机病毒？

怎样防止病毒进入自己的微机系统？

微机万一感染了病毒怎么办？

本书将为用户解答这些问题。

1.1 生物病毒与计算机病毒

病毒一词源于生物学，生物病毒由核酸分子构成，而核酸分子又由四种基本的核苷酸连结而成。核苷酸的排列顺序决定了生物的遗传密码。生物病毒在一定条件下侵入生物细胞，感染了病毒的细胞就成为病毒的“宿主”，病毒在宿主中潜伏、发作、自我复制、再传染……

与生物病毒类似，计算机病毒是一种人为编制的，能够自我复制的计算机程序。病毒的自我复制，也就是通常所说的传染，是在违背用户意愿情况下隐蔽进行的。病毒通过传染可能扩散侵入很多计算机系统，当某种条件被满足时破坏微机的信息资源，给用户造成巨大损失。很多病毒具有明显的破坏作用，但也有些病毒只是单纯地传染。不论是否有明显的破坏行为，只要一个程序在非用户授权情况下进行传染扩散，它就是计算机病毒。

每一个计算机病毒的原始程序都是人为编制的，通常病毒编制者是了解微机原理和操作系统的人，他们设计一段病毒程序，以手工操作的方式把病毒程序“嫁接”到正常磁盘上向外扩散。比方说病毒编制者可以在学校的公用计算机上使用他所炮制的含毒软件，由于病毒具有传染性，会使公用计算机上的很多软件都染上病毒。其他上机者从公用计算机拷贝出带毒软件拿到别的计算机系统使用，病毒会再传染其他系统……这样病毒就以一传十，十传百的树形结构不断传播扩散。

如果人们不能及时发现消除病毒，那么在某种特定条件下，染上病毒的计算机的信息系统会同时被破坏。

计算机病毒的形成有着久远的历史。早在半个世纪以前，伟大的数学家和计算机科学家冯·诺依曼就提出了复杂机械的自动复制理论，也就是计算机程序能够在内存中自我复制。50年代，著名的美国电报电话公司贝尔实验室的一些年轻研究人员热衷于一种他们自己创造的游戏，玩法是每人编制一段小程序去攻击对方的程序，赢家当然是毁灭对方程序者。这种会引起计算机系统瘫痪的危险游戏最终被禁止了。1977年美国著名科普作家雷思在一本科幻小说中构思了一种能够自我复制的计算机程序。这种程序通过信息渠道传播控制了7000多台计算机的操作系统，造成了人类社会巨大的恐慌与动荡。1983年11月3日美国计算机安全专家 Frederick Cohen 在一次计算机安全学术讨论会首次提出计算机病毒的概念，并进行实验演示，证明了计算机病毒可以在短时间内对计算机系统造成严重破坏。历史往往存在着不幸的巧合，恰恰在5年以后的1988年11月3日，美国最大的计算机信息网络 Internet 遭到计算机病毒的攻击。病毒侵入网络中6200台小型机和工作站，造成近亿美元的直接经济损失。而这一事件的始作俑者不过是美国康乃尔大学的一名研究生。

从80年代末起，计算机病毒开始大规模泛滥，目前在全世界已经发现的计算机病毒有数千种之多。病毒不仅每年造成数十亿美元的经济损失，还扰乱人们的社会生活，例如1994年南非实现民族和解后第一次总统选举，就因为计算机系统遭病毒感染而推迟公布选举结果。

在80年代末和90年代初，编制计算机病毒多半是个人行为，一些掌握一定编程技术的人，其中不乏高级技术人员，出于个人目的，比如显示个人技巧、不适当地保护个人知识产权以及进行报复等而编制和扩散计算机病毒。值得注意的是在现代军事领域“软杀伤”的地位越来越突出，所谓软杀伤是指利用电子战等手段干扰破坏敌方的指挥武器系统，达到不战而屈敌之兵的目的。而计算机病毒则被当做是电子战的重要“武器”。据报导有的国家早已开始研究计算机病毒在军事领域

的应用，这无疑将促进“计算机病毒学”的进一步发展。军用病毒在战时将被用来攻击敌方的通讯线路和控制系统，传递有意错报信息，改变对方的通讯卫星软件，通过无线电通信系统侵入敌方的计算机指挥网络等等。毫无疑问在未来的战场上计算机病毒将成为令人生畏的“软”武器，但同时有关专家指出与传统硬武器比较，“军用病毒”技术更容易扩散到民间，对一般计算机用户造成危害。

计算机病毒于 1989 年传入我国，根据较严格的统计，到 1995 年上半年在我国已发现的病毒有 200 余种，其中有一部分出自本土病毒编制者。为了保护国家信息系统的安全，我国政府于 1994 年 2 月 18 日颁布了《中华人民共和国计算机信息系统安全条例》，其中明确规定“故意输入计算机病毒以及其他有害数据危害计算机信息安全”是违法行为。每一位用户都该加强计算机安全意识，保护自己的微机免受计算机病毒侵害，不传播计算机病毒，更不去制造病毒。

1.2 计算机病毒的分类

从 80 年代末至今不到 10 年时间，计算机病毒已经拥有一个很大的家族。让我们从不同角度，观察一下病毒家族中的各类病毒。

一、按破坏性质分类——恶性病毒与良性病毒

计算机病毒的编制者有意在病毒中插入具有破坏性的程序，如删除文件、向硬盘写入垃圾数据、格式化硬盘、封锁计算机的某些功能等等。这些病毒具有明显的破坏意图和行为，被称为恶性病毒。如 DISK KILLER 磁盘杀手、3．6 米凯朗基罗、JERUSALEM 耶路撒冷、PRGKILL PRG 文件杀手、888、DIEHARD 死硬、1091 和 1099 小时、Casper、幽灵等都是著名的恶性病毒。

与恶性病毒相对应，另有些病毒看上去似乎只是传染表现自己，并不主动破坏系统，如 BUPT、基因 GENE 等。BIRTHDAY 病毒表现时甚至还在屏幕上显示一段生日贺语，并无其它明显的破坏作用，称为良性病

毒。良性病毒是计算机病毒产生初期的一种说法，实际上任何病毒都有占用系统资源，干扰运行等不良影响，所以良性病毒的说法现在已经基本不用了。

二、按寄生部位分类——引导型病毒与文件型病毒

磁盘上的病毒不能独立公开地存在，否则用户明知是病毒就绝不会运行使用它。计算机病毒就象寄生虫一样，总是偷偷摸摸地侵占磁盘的某些部位，非法寄生在那里。当然病毒的寄生部位是有选择的，它们总是寻找可能被执行到的地方，就是磁盘的引导扇区或可执行文件，分别称为引导型病毒和文件型病毒，以及两者的组合——混合型病毒。有病毒寄生的磁盘引导区或可执行文件称为病毒的宿主。

病毒占据寄生部位是通过传染实现的，寄生部位和传染对象是一回事。

三、按传染方式分类——覆盖型与非覆盖型病毒

病毒在向寄生部位传染的时候总要占据一定磁盘空间。引导型病毒传染软盘一般多占一个扇区，混合型病毒传染硬盘引导区的同时要占用多个扇区。病毒究竟侵占哪些扇区往往是病毒编制者想当然决定的，所侵占扇区原来的数据全部被覆盖掉。当用反病毒工具处理覆盖型病毒的时候，只能清除病毒，无法恢复被病毒覆盖的数据。

文件型病毒传染的时候利用 DOS 的文件管理机制，能自动在磁盘上搜索尚未使用的部位写入病毒，一般不破坏磁盘数据。

四、按活动形态分类——磁盘静态病毒与内存动态病毒

病毒与其它软件一样是常驻磁盘的，称为磁盘病毒或“静态病毒”。通常所说的杀病毒就是指消除磁盘病毒。磁盘病毒随宿主进入计算机内存，非法参与计算机系统运行，进行传染破坏活动，处于活动状态，称为内存病毒或“动态病毒”，防病毒卡就是通过监视内存中动态病毒的活动而报警的。关掉计算机电源就可以中止内存病毒的当前活动，但

如果不消除磁盘病毒，下次开机病毒还会再次进入内存，所以只有杀除磁盘上的静态病毒才能彻底解除病毒危害。

五、按操作系统分类

已发现的计算机病毒大多是基于 DOS 系统的病毒，所谓 DOS 病毒是指病毒主要利用 DOS 操作系统的功能而且在 DOS 状态下就能传染破坏。DOS 病毒可以在网络上传播从而对网络造成严重的破坏。Windows 3.X 是基于 DOS 的操作系统，DOS 病毒仍会传染在 Windows 环境下运行的 DOS 文件，但不传染 Windows 可执行文件。1995 年 8 月脱离 DOS 的 Windows 95 终于出台，欧美国家立即报导发现攻击 Windows 95 的病毒，尽管这些报道的真实性还有待证实，但可以肯定在冯·诺依曼体系计算机中不管操作系统如何变化，都可能出现新的计算机病毒。

1.3 计算机病毒的结构

现代计算机软件，不论是专业公司的商品化产品，还是用户自行设计的应用程序，都采用模块化结构。计算机病毒作为一种特殊软件也不例外。一般来说，计算机病毒可以按其内部代码的功能划分成解密模块、安装模块、传染模块、破坏模块和表现模块。

一、解密模块

人类对信息进行加密保护已经有很悠久的历史了，在现代计算机中加密技术更是被广泛应用，很多软件都是加密出售的。早期的计算机病毒往往是不加密的明码病毒，容易被发现分析，不利于病毒的隐蔽传染，所以后来很多水平较高的病毒都进行了加密处理。正如密码电报必须经过解密翻译才能看懂一样，磁盘上的密码病毒读入内存后如果不进行解密，CPU 是不能识别执行的，所以加密病毒必然有一个解密模块。病毒随宿主进入内存后首先执行解密模块对病毒的密码部分进行解密，把密码还原成 CPU 能够直接识别的指令数据。解密模块是

病毒进入内存后 CPU 首先执行的程序，它本身当然不能加密，也就是说磁盘上的加密病毒由两部分组成：一部分是经过加密处理的密码部分，另一部分则是未加密的明码。明码部分的作用是对密码部分进行解密，即解密模块。

二、安装模块

磁盘上的计算机病毒随宿主进入微机内存后就立即在内存中安装自己。

1.占据内存

计算机病毒在占据内存的时候要做两件事，一是找一个合适的地方待下来，二是使占据"合法"化。

磁盘上的计算机病毒被读入内存时所占据的内存地址并不一定是病毒可以正常工作的地址。比如引导型病毒按照微机固有的开机流程中被读到内存 0000：7C00 地址，这个地址还将被随后读入的其它软件使用，病毒如果赖在这个地址不走就会被后续软件冲掉，所以引导型病毒将把自己迁移到内存中一个它认为合适的地方安营扎寨，通常是基本内高端。

病毒仅仅占据一块内存并不安全，还必须设法使别的软件不再使用它所占的内存，也就是使占据"合法"化。占据内存高端的引导型病毒通常修改基本内存容量值，该值是在微机开机时检测出来的，存放在内存 0000：0413 字单元，通常是 16 进制数 280，10 进制数为 640，即 640K 基本内存。病毒根据自己的需要减小该单元值。比如 NATAS 病毒把该值减去 6 成为 634，DOS 操作系统就会认为微机只有 634K 内存，从而不再使用病毒占据的高 6K 内存。这样用户白白丢失了 6K 内存，而病毒则有了避风港。

2.修改操作系统

微机的操作系统是开放的，用户可以修改扩充操作系统在微机上实现新的功能。修改操作系统的主要方式之一是扩充中断功能，中断的概念比较复杂，但并不神密。微机中断指令是 INT XX，其中 XX 为中

断号，可以把微机的软中断当作子程序来理解，CPU 执行 INT XX 指令就是调用 XX 号子程序。微机提供很多中断，合理合法地修改中断会给微机增加非常有用的新功能，比如 INT 10 是屏幕显示中断，原只能显示西文，而在各种汉字系统中都可以通过修改 INT 10 使微机能够显示中文。在另一方面，计算机病毒则篡改中断为其达到传染、激发等目的服务，与病毒有关的主要中断有：

INT 08 和 INT 1C 定时中断，每秒调用 18.2 次，有些病毒利用它们计时判断激发条件。

INT 09 键盘输入，病毒用于监视用户击键情况。

INT 10 屏幕输入输出中断，一些病毒用于在屏幕上显示字符图形表现自己。

INT 13 磁盘输入输出中断，引导型病毒用于传染病毒和格式化磁道。

INT 21 DOS 功能调用，包含了 DOS 的大部分功能，已发现的绝大多数文件型病毒修改 INT 21 中断，因此也成为防病毒卡的重点监视部位。

INT 24 DOS 的严重错误处理中断，文件型病毒常进行修改，以防止传染写保护磁盘时被发现。

中断子程序的入口地址存放在微机内存的最低端，病毒窃取和修改中断的入口地址获得中断的控制权，在中断过程插入病毒的“私货”。

3.在安装阶段除占据内存和修改操作系统外，大多数引导型病毒传染硬盘引导区；一些文件型病毒传染重要的 COMMAND.COM 文件；有的恶性病毒判断系统日期等条件，如与病毒预先设定的条件相符就立即激发。

三、传染模块

传染模块通过计算机病毒的安装而进驻内存，伺机搜寻传染目标。引导型病毒多监视 INT 13 的读写软盘过程，并利用 INT 13 的写过程把病毒写到软盘上。文件型病毒多监视 INT 21 的加载文件或列目录过

程，并利用 INT 21 提供的一组文件处理功能传染可执行文件。病毒传染模块的基本机理是：

1.监视微机运行状态，寻找传染对象和时机。病毒传染的对象是磁盘引导区和可执行文件，通常病毒选择用户读写磁盘的时候进行传染，因为这时磁盘驱动器灯要发亮，病毒混水摸鱼，借机把自己写到磁盘上，用户不容易发现。

2.分析将要传染的对象是否有病毒标志，如果有标志说明对象已经染上病毒，不需要再传染。

3.如果要传染的对象没有病毒标志，病毒就非法进行传染。

四、破坏模块

破坏模块是恶性病毒的直接表现，通常由激发条件和破坏程序两部分构成。病毒激发条件的设置是五花八门的。日期是病毒常用的条件，新闻媒体报刊资料中经常介绍某种病毒于某月某日激发，给人们留下深刻的印象。但日期并不是激发条件的唯一选择，有的病毒根据用户击键情况激发，又有的按微机染毒后的开机次数激发等。这些病毒的激发时机很难事先掌握，所以病毒激发是“突然”的，给人以猝不及防的感觉，较之按日期激发的病毒更为危险。

计算机病毒的破坏目标十分广泛：磁盘引导区、文件分配表、文件目录区、COM、EXE、OVL、ASM、PRG、BIN、C 等各种重要文件都成为计算机病毒的篡改删除对象。封锁打印机和键盘、干扰屏幕显示、强行演奏音乐、死机等也是病毒常用的伎俩。

五、表现模块

一些病毒具有强烈的表现欲，病毒表现时的现象比较明显，会给用户造成深刻的印象，所以往往根据表现症状来命名病毒：

毛毛虫病毒，表现为一条毛毛虫在屏幕上自左向右爬行，“吃”掉屏幕上的字符。

红心病毒激发时在屏幕上显示一连串红心，同时格式化硬盘。