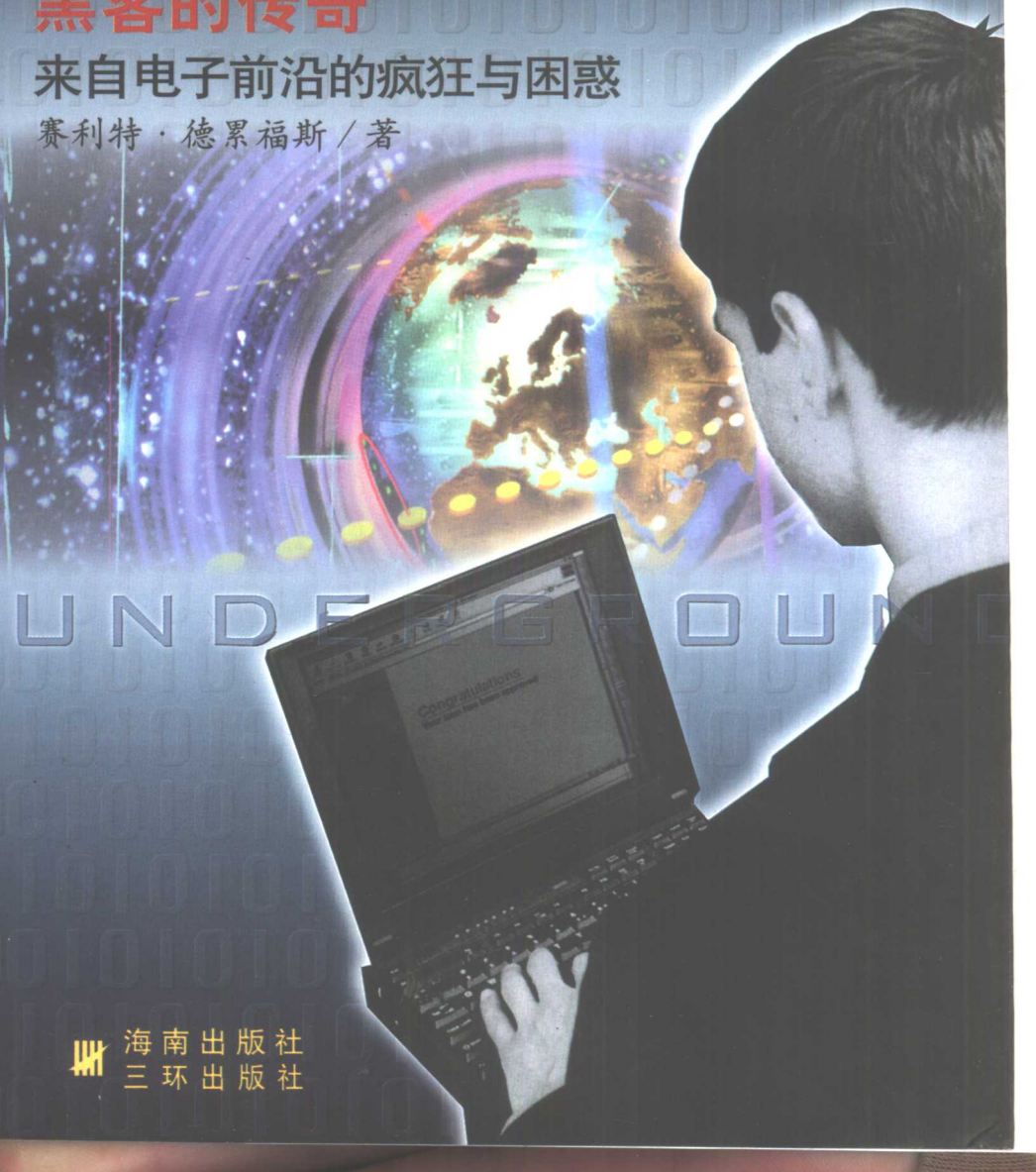
披露黑客社会的第一本畅销小说

地下黑客社会

黑客的传奇

来自电子前沿的疯狂与困惑

赛利特·德累福斯／著



海南出版社
三环出版社

地下黑客社会

UNDERGROUND

黑客的传奇

来自电子前沿的疯狂与困惑

赛利特·德累福斯／著
刘 海 军 等／译

海南出版社

Underground: Tales of Hacking,Madness and Obsession on the Electronic Frontier
by Suelette Dreyfus

版权合同登记号：图字：30-1998-42号

图书在版编目（CIP）数据
地下黑客社会 /(美)德累福斯(Dreyfus,S.) 著;
刘海军 等 译. -海口: 海南出版社, 2000.12
书名原文: Underground
ISBN 7-80564-951-O
Ⅰ地… Ⅱ.①德… ②刘… Ⅲ.计算机网络-安全技术
Ⅳ.TP393.08
中国版本图书馆CIP数据核字（2000)第76449号

地下黑客社会
作者：（美）赛利特·德累福斯
译者：刘海军 等
责任编辑：孙 忠

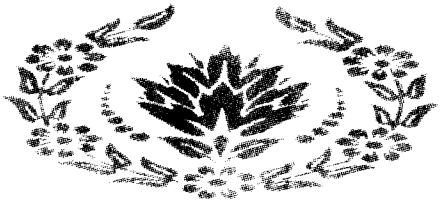
海南出版社 出版发行

地址：海口市金盘开发区建设三横路2号
邮编：570216
电话：0898-6812776
E-mail:hnbook@263.net
经销：全国新华书店经销
印刷：北京博诚印刷厂印刷
出版日期：2000年12月第1版 2000年12月第1次印刷
开本：850×1168毫米 1/32
印张：14.25
字数：250千字
印数：2000册
书号：ISBN 7-80564-951-O/C·14
定价：24.80元

献给彼得和我的家人

S.D.

献给亲爱的J.A.



绪　言

我的姨奶经常进行海底绘画。

1993年路易丝身披沉重的潜水服，手里握着调色板、特制的画笔、画布，慢慢地沉下水面，简直像来自《海底两万里》中的人物。沉入海底后，她支好画架，全身心地沉浸在另一个世界中。红白条纹的鱼群绕着蓝绿色的珊瑚和蓝色条纹的巨蚌穿梭不停。狮子鱼缓慢地滑过，优雅地摆动它们那绚丽而危险的鳍。满身条纹的鳗鱼从礁石缝中向她窥视。

路易丝在世界各地进行潜水绘画——苏禄群岛、墨西哥、澳大利亚大堡礁、夏威夷、婆罗洲。有好几次，她是那些太平洋岛民所见到的第一位白人妇女。她与他们一同生活达数月之久。

小时候，我被大洋底部的未知世界以及她旅途中经历的奇妙美丽的文化所深深吸引。我满怀着对她这种在画布上描绘完全陌生世界本质工作的深深敬畏而长大。

当时，革命性的新技术使她得以完成这项工作。通过空气压缩泵，有时是一个手动气泵连接一根通向水面的软管，人们突然可以长时间地融入一个从前无法到达的世界。新技术让她既得以探入未知疆域，又可以在精致的画布上对其细致描绘。

我步入全新的电子社会，了解其不那么神圣的一面——地下社会，是一件非常偶然的事。它深深地打动了我，使我满怀激动与冲突的情感去探索一个全新的世界。这和半个世纪前姨

奶的探索非常相似。如同她的探索一样，我的艰难跋涉也离不开新技术，我希望能像她一样捕捉这个世界的一个小小角落。

本书讲述电子地下社会的故事，即与执法机构无关，也不是遵照警方的意图而作。在全方位把握有关资料的基础上，我通过许许多多黑客的所见所闻展示一个不同的世界。我希望能为读者提供一个窗口来展示通常难以接近的神秘莫测的世界。

黑客是何方神圣？他们为什么这么做？对此没有简单明了的回答，每名黑客都与众不同。最终，我努力提供一组各自不同而相互联系的黑客群像，他们通过国际性的地下社会而联系在一起，本书所述世界上最聪明的黑客与飞客确有其人其事。不过有些世界级黑客的事迹本书并未提及。我最终决定只对少数黑客进行细致描绘，而不是将所有的黑客罗列成一个浅显的名录。

尽管每位黑客都有不同的故事，在许多故事中，都可见到共同的主旋律：反抗各种权威、家庭不和、聪明的学生被差劲的教师压抑、精神病或残疾、固执与执迷。

我花了很长时间来努力追溯每位主人公的经历：个人黑客冒险、警察突击搜查、法庭审判。有些案例花了数年时间才结案。

黑客们使用网上绰号（handle）。通常有两个目的：掩盖真实身份，在地下社会中的自我评价。“鹰”、“爬行者”、“巨嘴鸟琼斯”、“计算机黑客”、“数据持有人”、“间谍”、“巨人破坏者”、“分数白痴”、“刀锋”，这些都是澳大利亚黑客使用的绰号。

在电子地下社会，绰号就是黑客的名字。加之许多黑客已经开始新生活，我只用绰号称呼他们。如果一名黑客有多个绰号，我选择他喜欢用的那个。

本书每一章都以选自“开夜车”（Midnight Oil）乐队组合的歌曲来表达该章的主题。该乐队由地道的澳洲人组成。他们通过歌声反抗现行制度——特别是军事工业体制。在音乐起着举足轻重作用的地下社会中，歌声通过共鸣而形成主旋律。

选用“开夜车”歌曲的想法产生于对本文第一章的内容进行调查之际。该章揭示了美国宇航局（NASA）发生的 WANK 蠕虫危机。除了 RTM 蠕虫，WANK 也是第一个带有政治色彩的蠕虫。

WANK 事件是对艺术作品的模仿。电脑蠕虫的概念来自约翰·布伦纳的科幻小说《震荡波骑士》（The shakewave rider），该书描绘了一件带政治色彩的蠕虫事件。

据信，WANK 是第一个由澳大利亚人编写的蠕虫。

第一章描述了电脑系统管理员——黑客死敌的情况，最后还写到澳大利亚黑客在世界范围的地下社会中所引发的讨论。

随后的章节揭示和展现了早期地下社会的转变：失去清白、日益狭小的圈子中封闭的等级制度以及不可避免的命运——孤独。起初，电子地下社会比如“角落”俱乐部是个开放友善的场所。可现在，经历短暂与迅速地扩张之后，黑客们很少相聚。最初关于“开放”社会的设想已一去不复返。

随时间推移，电子地下社会发生了一些变化，主要是由于全球范围内新的计算机犯罪法律的实施以及警方的拘捕。本书不仅努力去记述澳大利亚黑客历史中重要的一页，也尽量去展示地下社会中的实质性转变——从本质上展示地下社会如何越陷越深，愈发不见天日。

目　录

第一章 10，9，8，7，6，5，4，3，2，1

有人离去，有人等待，有人试图告诉我什么。
——摘自 Midnight Oil 专辑《10，9，8，7，6，5，4，3，2，1》中的“有人试图告诉我什么”。

1989 年 10 月 16 日星期一
佛罗里达州肯尼迪航天中心

美国宇航局内洋溢着发射前的兴奋，伽俐略号探测器要向木星发射。

这家世界上最著名的航天机构中的管理人员与科学家们已花费了数年时间准备发射无人太空探测器。到 10 月 16 日星期一，如果一切顺利，载有 5 名宇航员的亚特兰蒂斯号航天飞机顶部载着伽俐略号探测器，将从佛罗里达州卡那维拉尔角的肯尼迪航天中心起飞，环绕地球第五圈时，于墨西哥湾上空 295 公里的高度，宇航员将释放这颗 3 吨重的探测器。

一小时后，伽俐略号安全地从航天飞机上脱离，探测器 32500 磅重的推进系统将点火，届时美国宇航局的工作人员将注视着这一人类智慧的结晶开始为期 6 年飞向太阳系最大行星的旅程。伽俐略号必须采取环行路线，绕过金星一次，地球两

次，通过重力加速效应来获得足以到达木星的动量。

美国宇航局科学家一直为如何使探测器穿越太阳系苦思冥想。方案之一是利用太阳能，可是因为由地球到木星路途遥远，而且木星离太阳更远——精确距离是7.783亿公里。在如此远离太阳的地方，伽俐略号需要巨大得不切实际的太阳能电池板才能获得足够能量。最后，美国宇航局的工程师们决定试用一种地球资源——原子能。

原子能非常适合太空航行。没有人类生命迹象的太空完全可以容纳一点点放射性的二氧化钚^{238}。根据所需能量值，将一定量的钚密封起来，并保持很长时间，这看来相当合理。只要把不到24千克的钚封在铅盒中，让其自然衰变，产生的能量足以供伽俐略号上的设备所需，伽俐略号就可以开始飞向木星的行程。

美国反原子能抗议者并不这么认为。他们设想发射失败后可能会出现的问题，对可能发生“钚雨”而非常不安。美国宇航局保证伽俐略号的能量包非常安全，该机构花费了5000万美元证实伽俐略号的动力装置是非常安全的。在发生各种爆炸、故障、意外时，动力装置均能保持严密封闭。美国宇航局向记者透露，由于意外造成的探测器重新进入大气层后钚的泄漏机率只有三百万分之一，由于发射失败造成的放射泄漏只有1/2700。

反原子能人士并不能直接阻止发射。按照美国解决争端的最佳传统，他们迅速向法院提起诉讼。反原子能人士和其他团体联合起来起诉，声称美国宇航局可能发生钚泄漏，并希望华盛顿特区法院裁定终止发射。申请书递交之后，法院决定于10月12日举行听证会，仅在发射前数天，这种情况从未有过先例。

数周来，抗议者全力出击，争取媒体注意力。这件事被炒得火爆。10月7日星期六，反原子能分子戴着防毒面具，挥舞着标语，穿行在卡那维拉尔角周围的街道，表示抗议。10月9日星期一早晨8点，美国宇航局开始为发射倒计时。正当亚特兰蒂斯号上的时钟开始倒计时之际，来自佛罗里达州“和平与正义联盟”的抗议者在中心的游客大厦示威。

这些示威者多多少少分散了人们对美国宇航局勇敢的太空计划本身的注意力，不过这倒不令宇航局担心。真正令人头痛的是佛罗里达州“和平与正义联盟”向媒体声称，他们将组织群众到发射台进行非暴力示威。该联盟的领导人布鲁斯·加尼翁用朴素平实的语言将这种抗议描述成弱小的民众反抗一个邪恶的庞然大物般的政府机构。另一个抗议团体经济趋势基金会的主席杰里米·里夫金也将“普通民众”与“美国宇航局那帮人”区分。他告诉合众国际社记者，宇航局自告奋勇进行发射，而可能成为核污染的牺牲品的世界各国人民并不情愿。

但是，能影响媒体的不仅是抗议者。美国宇航局知道如何利用新闻媒介。他们只是推出了超级明星——宇航员。毕竟这些敢于为全人类的利益而冒险进入阴冷太空的人们才是真正的火线英雄。亚特兰蒂斯号的机长唐纳德·威廉姆斯并未对抗议者直接反击，他只是远远地旁敲侧击。“无论干什么，总有人说三道四，”他告诉记者，“另一方面，限制或禁止什么很容易，真正做事情可不那么简单。”

在航天英雄中，美国宇航局还有一张王牌，亚特兰蒂斯号副驾驶麦克尔·麦卡利说，放射性同位素热电发电机（RTGs）——放在铅盒中的一片片钚，毫无危险。实际上，他决定安排他的亲友在宇航中心观看起飞。

正如抗议者暗示的那样，宇航员也许是固执的冒险家，但

英雄决不会令他的家人身处险境。另外，美国副总统丹·奎尔也计划从肯尼迪航天中心的控制室内观看发射，那里距发射台只有7英里远。

美国宇航局表面不动声色，控制着局势，增加了保安力量。大约有200名保安人员监视着发射现场。美国宇航局并不是在冒险，科学家们为这一时刻期盼已久，伽俐略号的行程决不会被一小伙反原子能分子所干扰。

发射计划已经拖延了7年，1972年国会同意发射伽俐略号探测器。最初预算为4亿美元，预定于1982年发射，然而从一开始，该计划就命运多舛。

1979年美国宇航局因为航天飞机开发计划将该发射计划推迟到1984年。当时计划采用“二次发射法”进行，即将母船和探测器分两次送入太空，到1981年，由于费用激增，美国宇航局对该计划进行了重大改动，停止“二级推进系统”的研究转而采取一种全新的系统，再次将发射计划推迟到1985年。在1981年联邦预算削减之后，为拯救伽俐略号的“推进器计划”，美国宇航局又推迟到1986年。1986年由于挑战者号爆炸，美国宇航局因安全问题再一次推迟发射。该计划一拖再拖。

最好的方案是两阶段，固体燃料的IUS系统，只有一个问题，采用该系统，伽俐略号可以到达金星和火星，但难以到达木星。美国宇航局喷气推进实验室的罗杰·迪尔想出一个好办法。让伽俐略号靠近并环绕附近的数个行星，可以获得重力加速，然后就可以飞向木星，伽俐略号的VEEGA路线，需要多花3年时间，但最终能到达木星。

反原子能分子认为，每飞经一次地球，就会增加一份核事故的风险，但美国宇航局认为这是发射过程的必然代价。

最近，伽俐略号因其他原因推迟发射。10 月 9 日星期一，美国宇航局宣布在控制航天飞机的二号主引擎的计算机中出现一个小故障。尽管问题出在亚特兰蒂斯号航天飞机而不是伽俐略号上，在反原子能分子的诉讼活动正在进行的背景下，出现技术问题确实有些棘手，更不用说出在控制引擎的计算机上了。

美国宇航局的工程师们在电话会议上讨论了这个问题。排除故障可能需要几个小时，也可能数天，可伽俐略号发射活动不容耽搁。由于各行星旋转轨道不同，探测器必须在 11 月 21 日前发射进入太空。如果亚特兰蒂斯号不能顺利升空，伽俐略号只好再等 19 个月发射，该计划已比最初预算多花了 10 亿美元。再等一年，需额外花费 1.3 亿美元。计划很可能会被取消。要么现在发射成功，要么永远不再发射。尽管大雨如注，在发射台处降雨达 100mm，邻近的佛罗里达州墨尔本地区达到 150mm，发射倒计时一直正常进行。此刻，美国宇航局决定推迟发射 5 天，直至 10 月 17 日，以排除计算机故障。

对那些一开始就为伽俐略号工作的科学家和工程师而言，当时命运真是和伽俐略号作对，不知什么原因，宇宙中特别是地球上的各种力量竭力不让人类仔细观察木星。只要美国宇航局搬掉一块绊脚石，那只看不见的手就会再扔下一块。

△ △ △

1989 年 10 月 16 日星期一

美国宇航局弋达德航天飞行中心，Greenbelt，马里兰州

美国宇航局帝国分布广泛，从马里兰州到加利福尼亚，从欧洲到日本，所有员工都在互相打招呼，查看收件箱中的邮件，啜饮咖啡，坐进椅子准备登录进入计算机进行一天复杂的物理工作，可是许多计算机的状况出人意料。

职员们一开始登录就清楚地看到计算机被某人或某个程序接管了。他们没有看到确认身份的条框，而是下列信息：

反抗核杀手的蠕虫

WANK

你的系统已被 WANK 接管

你们满口是全人类的和平，却为战争而准备。

WANK？全美计算机系统管理员从未听说过这一名词。到底是谁想侵入美国宇航局的计算机系统？“反抗核杀手的蠕虫”到底是怎么回事？它来自一个古怪的激进政治团体，还是游击战恐怖分子发动的对美国宇航局的攻击？为什么叫“蠕虫”呢？“蠕虫”作为一个吉祥物而言，对于一个革命组织并不太合适。蠕虫处于生物链的底层，恰如俗语所言“像蠕虫一样低等”，谁会选择蠕虫作为象征呢？

至于“核杀手”就更怪异了，至少那句箴言“你们满口是全人类的和平，却为战争而准备”并不适合美国宇航局。该机构并不制造核导弹，只是将人类送上月球。某些研究项目确实得到军方赞助，但与其他美国政府机构如国防部相比，其核武器研究并不占重要地位。所以大家产生一个疑问：为什么美国宇航局成为攻击目标？

而且“WANK”这个词并没有实际含义，一个系统被 WANK 掉意味什么？它意味着美国宇航局已失去对计算机系统

的控制。

一位美国宇航局的科学家在周一上午登录进入计算机，发现下列信息：

删除文件〈文件名 1〉
删除文件〈文件名 2〉
删除文件〈文件名 3〉
删除文件〈文件名 4〉
删除文件〈文件名 5〉
删除文件〈文件名 6〉

同时计算机告诉科学家："我正在删除你的所有文件。"看起来就好像科学家自己键入指令：delete/log＊.＊（删除/目录＊.＊）专删除所有文件。

美国宇航局的这名科学家看到她的文件名在计算机屏幕上逐行滚动，逐行消失一定非常惊慌。肯定出了问题，她可能曾试着同时按"Control"和"C"键来终止上述过程。这个指令本该终止计算机程序，可是控制计算机的不是科学家而是侵入者。侵入者告诉计算机："那个指令无意义，忽略！"

这名科学家可能一再按指令键，一次比一次急切。她立刻被计算机的这种非逻辑性本质所困扰，愈发不安。数周至数月揭示宇宙奥秘的工作全部毁于一旦。所有这一切在她亲眼注视下被计算机吞噬，她却无计可施。一切成果迅速在眼前消失，灰飞烟灭。

人们在无法控制他们的计算机时，反应很差劲，明显地暴露出他们的弱点。忧虑者通过写信发出哀诉，敏感者令人心酸地乞求帮助，发号施令者擂着桌子大吼不止。

设想你是一名美国宇航局计算机系统的管理员，在那个周一早晨，跨入办公室时发觉电话响个不停。每个电话都来自忧心忡忡、迷惑不解的宇航局工作人员，每个电话都让你相信他或她的文件或帐户记录或研究计划等一切文件都从计算机系统中消失了——实际上还在计算机中。

该事件由于美国宇航局各中心之间经常为研究项目而竞争，显得益发严峻。当开展一项最新的飞行计划时，两到三个各有数百名雇员的研究中心会参与竞争。如果失去对计算机的控制，所有的数据、计划书和支出帐目全部丢失，竞标肯定失败，并因而失去一大笔经费。

这一天对那些在美国宇航局太空物理分析网（SPAN）计算机网络办公室的工作人员不那么好过，同样对约翰·麦克马洪也是个苦日子。

约翰·麦克马洪是马里兰州美国宇航局弋达德航空中心DECNET协议助理管理员，他通常管理弋达德中心15—20幢建筑物之间的SPAN计算机网络。

麦克马洪工作地点编码是630.4，即弋达德高级数据流通技术办公室，位于第28号楼。弋达德的科学家会给他打电话求教计算机方面的事情。他最常听到的两句话是“这机器好像不能工作了”或“我无法和某处网络联系”。

SPAN是太空物理分析网络的缩写，该网络与全球约100万计算机终端连为一体。它与互联网络（Internet）不同。后者广泛地对公众开放，而SPAN仅连接美国宇航局的科研人员、美国能源部和包括大学在内的科研机构。从技术角度看，二者也有显著差异，操作系统不同。互联网上的多数大型机使用Unix操作系统而SPAN主要由运行VMS操作系统的VAX计算机构成。该网络的工作方式类似于互联网，但所使用的“语

言”不同。互联网用 TCP/IP（传输控制协议/互联网协议）系统，而 SPAN 使用 DECNET。

实际上，SPAN 网被称为“DECNET”互联网。大多数计算机由马萨诸塞州的 DEC（数字设备公司）制造，因而得名 DECNET。DEC 生产功能强大的计算机，SPAN 网上的每一台 DEC 计算机都可以连接 40 个终端，有些甚至更多。一台 DEC 计算机为 400 人服务的情形并非罕见。总共有不少于 25 万的科学家、工程师或其他脑力劳动者使用该网络。

麦克马洪是一名正在接受培训的电子工程师，来自美国宇航局宇宙背景探测计划小组。在该计划中，他负责管理数百名研究人员使用的计算机。弋达德 7 号楼，是他在宇宙背景探测计划小组中的工作地点。这个小组开展一些有趣的研究，试图为宇宙画图。科研人员使用人类肉眼看不见的波长进行探测。美国宇航局计划 1989 年 11 月发射宇宙背景研究小组的卫星，来探测天文学边界内的早期宇宙的红外衍射与微波辐射。在普通观察者看来，该计划像一幅现代风格的艺术作品，可称为“红外宇宙图”。

10 月 16 日，麦克马洪走进办公室坐下来工作，却接到一个来自 SPAN 计划中心的电话，图特·巴特和罗恩·滕卡提是太空科学数据中心的工作人员，负责管理美国宇航局中一半的 SPAN 网络，他们发现一个奇怪的未经授权的东西在网络中蔓延，看来像个蠕虫。

电脑蠕虫有点像电脑病毒，它侵入计算机系统，干扰正常功能。它可以在兼容的计算机网络中游荡，停下来敲打与网络相连的计算机系统的大门。如果该系统在安全方面存在缺陷，它就会爬进去，然后发出指令采取一些行动，从向计算机用户发出一条信息到试图控制整个系统。蠕虫不同于病毒等其他计