个人电脑安全应用36计丛书

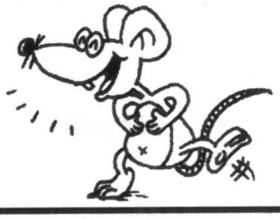
个人电脑攻击防护

李勇 张小苗 编著

国防工业出版社
http://www.ndip.cn

36计

个人电脑安全应用36计丛书



个人电脑

攻击防护36计

李 勇 张小苗 编著

国防工业出版社

·北京·

图书在版编目(CIP)数据

个人电脑攻击防护36计/李勇,张小苗编著.
—北京:国防工业出版社,2004.5
(个人电脑安全应用36计丛书)
ISBN 7-118-03421-5

Ⅰ.个... Ⅱ.①李...②张... Ⅲ.计算机病毒-防治 Ⅳ.TP309.5

中国版本图书馆CIP数据核字(2004)第010021号

责　　编　宋序一

出版发行　国防工业出版社出版发行
地　　址　北京市海淀区紫竹院南路23号
邮　　编　100044
网　　址　http://www.ndip.cn
经　　售　新华书店
印　　刷　北京奥隆印刷厂印刷
开　　本　787×960 1/16
印　　张　20¼
字　　数　431千字
印　　数　1—4000册
版　　次　2004年5月第1版
印　　次　2004年5月北京第1版印刷
定　　价　28.00元

(本书如有印装错误,我社负责调换)

内容简介

本书详细地介绍了常见的网络攻击方式和防护措施,包含了各种典型的攻击性病毒的分析,以及有效的杀毒软件或杀毒方法,如"冲击波"病毒的攻击分析与防治方法。全书具体分为6篇进行讲解:第1篇驱动器,介绍硬盘驱动器、软盘驱动器和光盘驱动器常见的攻击和防护方法;第2篇电脑部件,介绍个人电脑部件(如网卡、键盘和鼠标等)可能遭受到的攻击和防护方法;第3篇整机防护,主要介绍PC、掌上电脑、笔记本、手机等的攻击方法与防护措施;第4篇操作系统,介绍Windows XP、Windows 2000、Linux、UNIX等操作系统常见的攻击及防护方法;第5篇个人应用,主要介绍个人电脑中与个人设置有关的文件夹、网络浏览器、E-mail、注册表以及办公软件、系统软件常见的攻击以及相应的防护手段;第6篇应用软件,介绍国内外流行的攻击与防护软件及一些著名的反黄软件。

附录中提供了国内外著名的安全网站以及一些常用攻防软件的相关资料。

本书适合广大初中级电脑用户及爱好者阅读参考。

丛书序言

本套丛书针对国内书籍市场上个人电脑安全应用方面的需求，经过精心编排，将个人电脑的安全应用与中国传统兵法 36 计相结合，选择了 36 个具有代表性的计谋来讲述个人电脑的安全实用技术，篇篇有谋、计计有谋，使读者能从谋略的角度掌握个人电脑的安全操作。

本丛书一改传统的以安全技术理论为主的写作思路和风格，以大量的实例进行讲解，并配以“猫鼠斗智”的卡通插图，通俗易懂、简单明了。

本丛书所指的安全主要有两个方面的含义：一方面是指隐私安全，即自己的隐私不会泄露和被别人偷看；另一方面是指使用安全，即不会由于病毒破坏而影响自己的使用。因此，本丛书也主要致力于解决这两个方面的安全问题，既保证自己的电脑能够正常地使用，又使自己的隐私不被窃取，资源不被盗用。

本丛书共有 4 个分册，几乎囊括了与个人电脑安全相关的所有技术，每本书侧重一个安全方向，且每本书的附录中都有相关的专业网站资料和工具列表，便于读者查询使用。

《个人电脑加密解密 36 计》

主要讲述个人电脑加密解密的实用技巧和相关软件。

《个人电脑攻击防护 36 计》

主要分析个人电脑各个组成部件常见的攻击以及相应的防护手段。此处要“防护”的不仅仅是黑客和病毒的攻击，对于青少年来说，还包括诸如黄色和暴力等信息的屏蔽。

《个人电脑安全管理 36 计》

主要侧重于介绍与个人电脑安全相关的管理工具的功能和使用方法。

《个人电脑安装维护 36 计》

主要介绍个人电脑各个部件及各种组件的安装维护技术。

由于编著者水平有限，加上时间仓促，书中难免有不妥之处，敬请读者批评指正。

前　言

随着计算机技术的飞速发展及硬件价格的不断下降，个人电脑已经成为我们日常学习生活中必不可少的工具。Internet、USB 等等与电脑相关的新名词迅速、频繁地出现在媒体和生活中，手机、掌上电脑等的普及也大大扩展了电脑的应用，一场信息革命的风暴已经迫在眉睫。这对于许多以前很少有机会接触电脑，但现在又不得不和电脑打交道的人来说，实在是有些措手不及。尤其是目前互联网上越来越猖獗的计算机病毒和黑客攻击，往往让人们防不胜防。

本书以实例为主线介绍了电脑中存在的安全隐患和一些常见的黑客攻击手段，以及相应的防护措施。其中包括对硬盘、显示器、键盘、鼠标、光驱、网卡、USB 端口等的防护，以及对台式机、笔记本电脑、掌上电脑和手机等的整机防护；并且针对不同操作系统的防护分别做了详细的介绍。

本书选取了 36 个具有代表性的计谋进行讲解，每个计谋分为计谋目标、知识背景、具体实现、疑难解惑和高手点评等 5 个部分进行介绍。其中“计谋目标”主要介绍本计谋的主要内容；“知识背景”介绍本计谋涉及到的基本概念和核心知识；“具体实现”以图解的形式介绍具体的操作过程和方法；“疑难解惑”根据操作中常见的问题，有针对性地进行解答；“高手解答”则是我们邀请了国内知名的专家和学者对该部分的技术进行讲解和指导。

本书面向初中级电脑用户，侧重于实用性和可操作性，语言通俗易懂，同时配以大量的实例和图解。即使读者对相关的技术不是很了解，通过书中介绍的方法和步骤也可以顺利地完成工作，达到预期的目的。

本书由李勇主编，参与本书编写的还有张小苗、尹峻松。同时在本书的编写过程中，还得到了张朝众等的大力支持，在此一并向他们表示衷心的感谢。

目 录

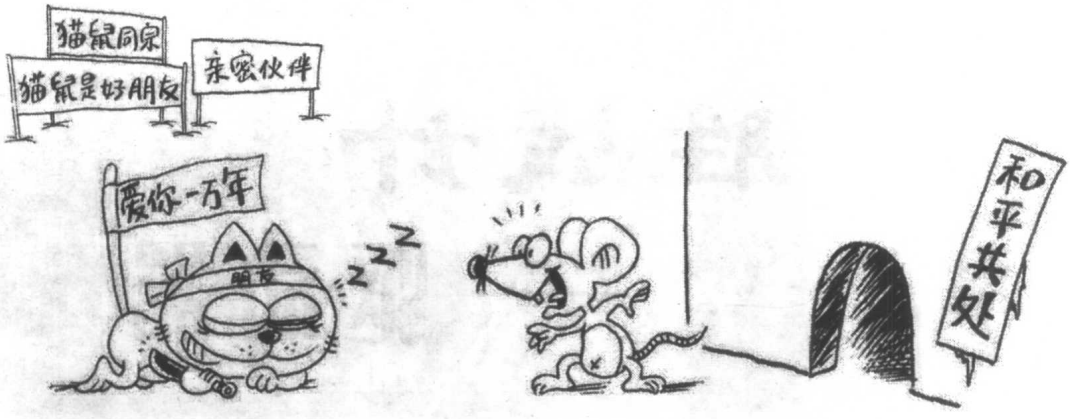
第 1 篇　胜战计——驱动器 1
第 1 计　瞒天过海——硬盘常见的攻击 2
第 2 计　围魏救赵——硬盘的防护手段 14
第 3 计　借刀杀人——来自木马的攻击 23
第 4 计　以逸待劳——反击木马 34
第 5 计　趁火打劫——软驱的攻防 45
第 6 计　声东击西——光驱的攻防 54
第 2 篇　敌战计——电脑部件 63
第 7 计　无中生有——BIOS 的攻防 64
第 8 计　暗度陈仓——键盘的攻防 71
第 9 计　隔岸观火——鼠标的攻防 76
第 10 计　笑里藏刀——网卡的攻防 81
第 11 计　李代桃僵——USB 设备的攻防 89
第 12 计　顺手牵羊——显示器的攻防 94
第 3 篇　攻战计——整机攻防 103
第 13 计　打草惊蛇——台式机的攻防之一 104
第 14 计　借尸还魂——台式机的攻防之二 112
第 15 计　调虎离山——笔记本的攻防之一 120
第 16 计　欲擒故纵——笔记本的攻防之二 128
第 17 计　抛砖引玉——掌上电脑的攻防 136
第 18 计　擒贼擒王——手机的攻防 143
第 4 篇　混战计——操作系统 151
第 19 计　釜底抽薪——Windows XP 的攻防之一 152
第 20 计　混水摸鱼——Windows XP 的攻防之二 158
第 21 计　金蝉脱壳——Windows 2000 的攻防 165
第 22 计　关门捉贼——Windows 98 的攻防 175
第 23 计　远交近攻——Linux 的攻防 184
第 24 计　假途灭虢——UNIX 的攻防 195

第 5 篇　并战计——个人应用 203
第 25 计　偷梁换柱——文件夹的攻防 204
第 26 计　指桑骂槐——文件的攻防 213
第 27 计　假痴不癫——网络浏览器的攻防 222
第 28 计　上楼去梯——QQ 的攻防 231
第 29 计　树上开花——电子邮件的攻防 238
第 30 计　反客为主——注册表的攻防 245
第 6 篇　败战计——应用软件 255
第 31 计　美人计——BlackICE PC 的使用 256
第 32 计　空城计——LockDown 的使用 266
第 33 计　反间计——“木马克星”的使用 275
第 34 计　苦肉计——“美萍反黄专家”的使用 282
第 35 计　连环计——“护花使者”的使用 291
第 36 计　走为上——国内外流行的防护产品 300
附录 A　安全网站精选 310
附录 B　攻防软件介绍 313

第1篇

胜战计
——驱动器

攻击防护36计



第 1 计　瞒天过海

——硬盘常见的攻击

硬盘，作为信息的主要存储介质，是电脑的核心组成部分。硬盘里保存着电脑用户大量的数据和资料，还保存着计算机赖以生存的操作系统，可以说，计算机如果没有硬盘就什么也干不了。正因为如此，硬盘才成为了入侵者们攻击的主要目标。如果硬盘遭到攻击，不仅大量有用的数据和资料难以恢复，更严重的是整个硬盘都将报废。

知己知彼，百战不殆。要防御对硬盘的攻击，必须首先了解硬盘攻击的方法。我们可以想像，如果对方的电脑中被我们植入病毒而又等待一定的时间或条件再发作的话，就可以达到毁坏硬盘数据的目的，而自己也可以全身而退。

计谋目标

通过直接或远程的方法，利用对方对自己的信任，在对方的计算机中植入自己编写或设置好的病毒。

知识背景

作为存储介质，硬盘用于存储数据。破坏硬盘最简单直接的方法就是破坏硬盘上的有用数据。我们可以通过欺骗性文件将病毒传给对方，或者用大量数据塞满对方硬盘，或者直接以程序的形式欺骗操作系统对硬盘进行破坏。总之，利用对方的疏于防范来达到破坏硬盘数据的目的。

下面通过对几种硬盘病毒的详细介绍来说明硬盘攻击的基本方式。

具体实现

1. CIH 病毒分析

1) CIH 病毒简介

CIH 病毒，又称为切尔诺贝利病毒，是一种相当危险的病毒，由当时的台湾大学学生陈盈豪编制。它使用面向 Windows 的 VxD 技术编制，是继 DOS 病毒、Windows 病毒和宏病毒之后的第四类新型病毒。目前有 V1.0、V1.1、V1.2、V1.3 和 V1.4 五个版本。其中 1.0 版和 1.1 版没有什么破坏力；而 1.2 版加入了破坏硬盘和 BIOS 的程序，在每年的 4 月 26 日发作；1.3 版在每年的 6 月 26 日发作；1.4 版则会在每个月的 26 日发作。随后，又出现了很多 CIH 病毒的变种。

CIH 病毒的破坏力相当的惊人。它的感染速度相当快，计算机里所有的*.exe 文件都会被感染，上面所述的五个版本都只能感染 Windows 95/98 系统，但是，CIH 的一些变种，如圣诞 CIH 病毒，还可以感染其他系统。CIH 病毒一旦在本机上发作，计算机的 Flash BIOS 芯片中的系统程序将遭到破坏，从而导致主板损坏。而且，它会对硬盘进行格式化操作，硬盘驱动器将会不停地旋转，所有数据将会损坏。只有重新进行 FDISK 操作后才有可能挽救硬盘，但此时硬盘中的数据已经全部丢失。

2) 常见的攻击方式

CIH 病毒是一个可执行文件，需要用户执行该程序才可以发作并感染受害计算机，不然只能一直潜伏在计算机中而不会发作，所以，它需要以各种方式来诱骗用户执行该病毒文件。

(1) 电子邮件。随着互联网的迅速普及，网络已经成了病毒的主要传播途径之一。有时，我们会收到一些来历不明的电子邮件，在其附件中往往包含了*.exe 的文件，很有可能就是病毒伪装成贺卡或者其他文件诱骗用户执行。

即使有一些看似正常的可执行文件或者软件程序，也可能有病毒程序依附其中，甚至还发生过恶意攻击者冒充反病毒公司向客户发送最新病毒警报和相应的杀毒工具的情况，而所谓的杀毒工具实际上就是伪装的病毒程序；也有冒充微软公司发布安全公告，在邮件附件中携带自称为安全补丁的病毒，来对用户进行攻击的事例。

(2) 存储介质。常见的存储介质有软盘、光盘、USB 存储器等，这些常常被用作为病毒的载体。如一些盗版的游戏光盘，由于粗制滥造，里面的程序文件中就可能含有 CIH 病毒。有一些则利用 CD-ROM 的自运行特性，将 CIH 混入自动运行的程序中，你只要往光驱中一放，就会发现电脑中的硬盘狂转，然后就蓝屏死机了。而那些在公共机房里使用的软盘和 USB 存储器，由于来源复杂，再加上在多台计算机中相互流通使用，也成为了病毒很好的传播载体。

(3) 网络下载。在网上下载的一些软件可能就是伪装的病毒或者依附了病毒程序，利用人们的好奇心和对某些事物的兴趣来欺骗用户执行病毒程序。例如，CIH 就曾经伪装在一种当时流行的“小龙女”屏幕保护程序中，很多不明真相的用户下载安装以后才发现上了当。

(4) 恶意攻击。主要是指恶意的破坏者将病毒程序通过各种方式拷贝到想要攻击的计算机中，然后在计算机中运行病毒程序，使病毒在目标计算机上发作，达到破坏的目的。这种方式不如上面几种普遍，不过这种方式比诱骗的方式更为直接，攻击成功率很高。

3) 分析

通过对 CIH 病毒常见攻击方式的简要分析，可以看出此类病毒的攻击方式一般都是把自己伪装成一些看似安全的可执行程序或者依附在一些常用的软件中，以各种方式使计算机用户对其放松警惕而运行该病毒程序。它的攻击方式除了上面讲的那种恶意攻击外，基本上算是被动式的，是通过文件来进行传播的。事实上，因为它出现的时间较早，还只能算是一种传统的计算机病毒，传播远不如我们后面将要介绍的病毒快捷迅速，但是它仍然代表了采用这种攻击方式的一大类的病毒软件。

有很多类似于 CIH 的病毒软件，笔者也曾经在网上下载到很多这样的软件，其中大部分的软件都不具有 CIH 这样破坏硬件的能力，但是它们几乎都会对硬盘强制性地进行格式化，删除用户计算机里所有的文件。这样的病毒软件想要传播，几乎都会采用和 CIH 一样的传播方式，都需要用户执行病毒程序才能发作。用户一旦识破，它们的阴谋也就被戳穿了。所以，随着计算机用户防毒意识的加强，现在这种传统的病毒已经出现得较少了。病

毒设计者们也不再关注通过传统介质来传播计算机病毒，而是转向了网络。他们不再满足于欺骗用户执行病毒程序，而是要病毒主动出击，去感染目标计算机。

2. “硬盘杀手”病毒分析

1) “硬盘杀手”病毒简介

2002 年的 12 月 27 日，国内的近百位计算机用户发现他们的计算机遭到了病毒的袭击，硬盘上的数据全部丢失。当时所有的反病毒公司都无法恢复被攻击的硬盘。经瑞星全球反病毒监测网截获，证实为“硬盘杀手”病毒（Worm. Opasoft）。这是一种蠕虫病毒，破坏力极强，可以破坏受害计算机上所有的硬盘数据，数据的破坏速度达到了每分钟 10G 左右。而且遭到攻击后，数据很难恢复。随后的几个月中，“硬盘杀手”的几个早期版本以及新版本不断被发现。较老的版本，如 Worm. Opasoft. c，不会破坏用户计算机，但是会不停地对局域网的 137 端口（NetBIOS）进行试探性询问，由于其不断进行重复的 IP 发送，耗用了大量的网络资源，造成网络堵塞。而新的变种，如 Worm. Opasoft. e，据专家介绍，破坏力直逼 CIH 病毒，而且破坏范围更广，传播更为迅速。

2) 病毒原理简析

“硬盘杀手”病毒感染的主要对象是装有 Windows 95/98/Me 操作系统的计算机，因为它利用了 Windows 95/98/Me 系统的一个安全漏洞。这些操作系统为共享文件和共享打印设备提供密码保护的功能，但是这个密码并不安全，该漏洞使得恶意的入侵者只要利用一个有效的用户名，即使不知道完整的密码就可以访问共享的文件。“硬盘杀手”利用这个漏洞，只要发送单个字符的密码到网络共享目录就可以得到共享目录的访问权限，然后将自身拷贝到目标计算机上，完成网络感染。由于它是一个蠕虫型病毒，会不断地在网络中复制、传播。只要一台计算机上感染了该病毒，网络中（特别是局域网）中那些没有有效防御措施的计算机很快就会被全部感染，从而造成大面积的破坏。后来出现的“硬盘杀手”病毒的变种，不仅能攻击 Windows 95/98/Me 操作系统，还能攻击 Windows 2000/XP 系统，感染的范围更大。

3) 常见的攻击方式

(1) 传统的攻击方式。该病毒可以利用前面所讲的 CIH 病毒的各种传播方式，特别是利用网络服务，通过各种文件进行传播。主要手段还是诱骗用户执行病毒程序，达到攻击的目的。

(2) 利用网络主动攻击。这一点与 CIH 病毒不同。尽管 CIH 也是利用网络得到了更为广泛的传播，但总的来说，这只是一种被动的攻击方式。而“硬盘杀手”就不同了，它只要在一台计算机上发作，就会不断地对网络中的计算机进行扫描，寻找可加以利用的资源，一旦找到，就将病毒注入其中，完成感染。被感染的计算机又会加入到攻击者中间，去攻击网络内的其他计算机。主动攻击使得病毒不需要诱骗每一个用户执行病毒程序，只要一个人上当，网络内的计算机就会不知不觉地成为受害者。而且，即使部分计算机清除了该病毒，只要有一台计算机还没有完全清除，其他计算机还是会成为该病毒

的攻击对象。

4) 分析

由于广大计算机使用者反病毒意识的提高，通过传统方式进行病毒传播，感染的几率相对来说已经比较小了。那么通过蠕虫病毒的特性，不停地在网络上进行自我复制、主动攻击，可以使很多电脑用户在毫不知情的情况下成为病毒攻击的牺牲品，而且给病毒的清除带来了很大的麻烦。“硬盘杀手”也正代表了这一病毒发展的新趋势。

攻击者可以在位于网络中的任意一台计算机上加载“硬盘杀手”病毒发起攻击。所有被“硬盘杀手”病毒攻击后感染的计算机都将成为新的攻击发起者，这种相互式的感染则会使得整个网络一片混乱。

3. “硬盘炸弹”分析

1) “硬盘炸弹”简介

现在网上流行的“硬盘炸弹”实际上为“江民炸弹”及其变种。所谓的“江民炸弹”实际上是江民公司在KV300 L++中内置的反盗版功能，又称为逻辑锁。如果你不小心运行了这个程序，那么你将会看到你的硬盘被死锁。这时不管你用光驱还是软驱，都无法对系统进行启动了。硬盘几乎和报废了没有什么区别。如果不知道怎么解锁，除了重新买一块硬盘，就再也没有别的方法了。

2) “硬盘炸弹”原理简析

由于计算机在引导DOS系统时会搜索所有逻辑盘的顺序，首先要找的是主引导扇区的分区表信息。分区表信息位于硬盘的零柱面的第一个扇区的OBEH地址开始的地方。如果分区信息开始的地方是80H，则表示这是主引导分区，而其他的为扩展分区。主引导分区会被定义为C盘，扩展分区则依次为D、E、F……盘。而“硬盘炸弹”会修改正常的主引导分区记录而将扩展分区的第一个逻辑盘始终指向自己。这样，在系统启动的时候，查找到第一个逻辑盘后，无论怎么查找下一个逻辑盘总是找到自己，从而形成死循环。无论你用软驱、光驱还是双硬盘，都拿它一点办法没有。

3) 常见的攻击方式

(1) 传统的攻击方式。“硬盘炸弹”可以使用传统的方式进行传播。笔者就曾经有幸在网上下载到这个软件。软件不大，压缩后只有36kB。解压缩以后，发现里面只有三个文件，其中一个名为diskbomb的就是那个万恶的硬盘炸弹了。想不到一个只有1.76kB的可执行文件具有这么大的破坏性。

(2) 修改IE攻击。很多上网的朋友都遇到过IE被一些恶意的网页修改的事情，要不是主页被修改，就是IE的标题栏被篡改，真是让人头疼不已。只不过，这样的修改，只是让人生厌，好像还没有对我们造成多大的损失。但是如果你这么想，那就大错特错了！

大家都知道，我们在浏览网页的时候，通常会采用直接点击IE工具栏上的程序按钮来执行相应的操作的方式。例如我们要下载文件，就可以直接点击工具栏上的网际快车按钮，如图1-1所示。

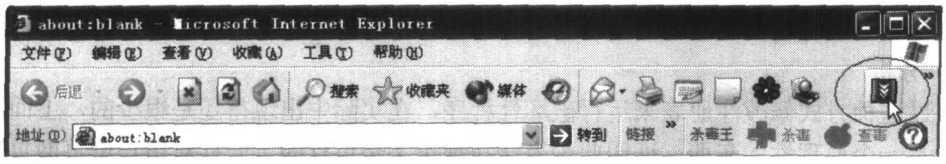


图 1-1　浏览器中的快捷按钮

IE 工具栏上的按钮的内容全部保存在注册表的 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Extension 下面。这个文件夹里有几项由字母和数字组成的键值。单击【开始】|【运行】菜单项，在弹出的对话框中输入 regedit，弹出注册表编辑器窗口，如图 1-2 所示，找到相应的文件夹。

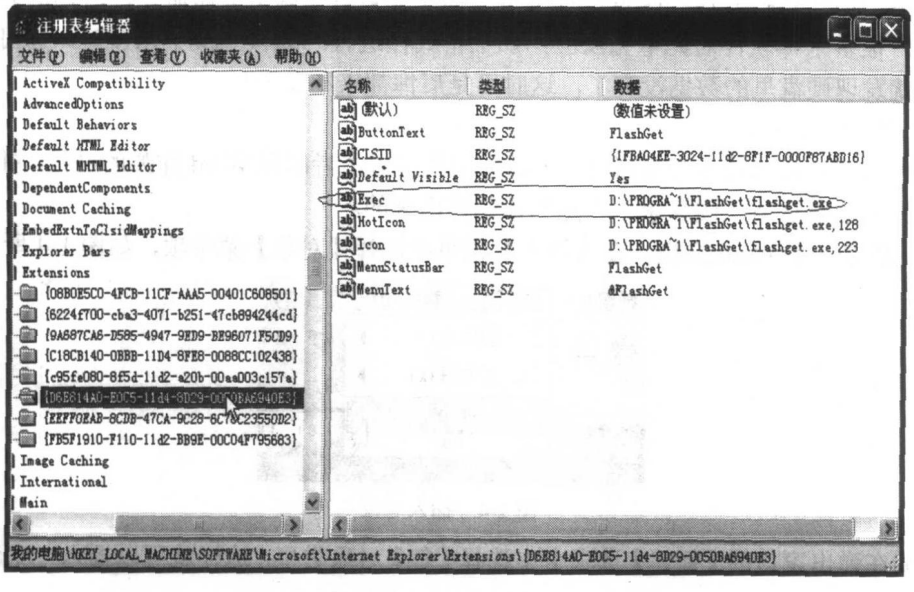


图 1-2　快捷按钮在注册表中对应的位置

这样我们就可以修改相应的键值，将其指向我们所需要运行的程序。

如图 1-3 所示，我们对【数值数据】文本框的内容进行修改，将其中的 flashget.exe 文件修改为“硬盘杀手”或者是其他危险的程序。

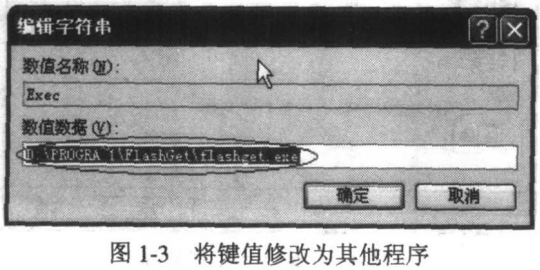


图 1-3　将键值修改为其他程序

这样，一旦你单击 IE 工具栏上的网际快车按钮进行下载，马上就会遭到灭顶之灾。

4) 分析

通过这种方式修改注册表来运行破坏性程序，在实际中出现得还是很少的，上面所写得也仅仅是一个原理性的东西，证明此种方法在理论上是可行的。而针对用户浏览网页来进行硬盘的攻击的方法，已经在网上出现了，下面我们向大家介绍一下“能够格式化硬盘的网页”。

4. 能够格式化硬盘的网页或文件

1) 攻击原理简介

目前不少的网站上都有这个网页甚至是源程序提供下载。经过研究网页源程序发现，此类网页大多数都是在源程序中调用一些诸如 format.com 和 deltree.exe 等 DOS 下的程序来进行破坏。你一旦打开这些网页进行浏览，程序就会自动调用上述命令，对你的硬盘进行格式化。很多杀毒软件对此毫无反应，加上格式化进行时默认为最小化窗口，你可能稀里糊涂地就发现硬盘里的数据没有了，这时可是后悔都来不及了！

2) 攻击实例介绍

这种攻击方式的技术含量极低，下面介绍某些攻击者制作 Word 炸弹的过程，并以此为例，让大家了解这些“硬盘杀手”是如何制作出来的。

(1) 新建一个 Word 文档，在【插入】菜单中选择【对象】菜单项，如图 1-4 所示。

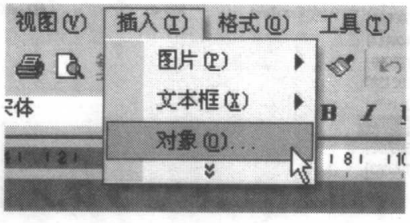


图 1-4　插入对象

(2) 在弹出窗口的【新建】选项卡中选择【包】对象类型，这样就可以插入一个包对象，如图 1-5 所示。

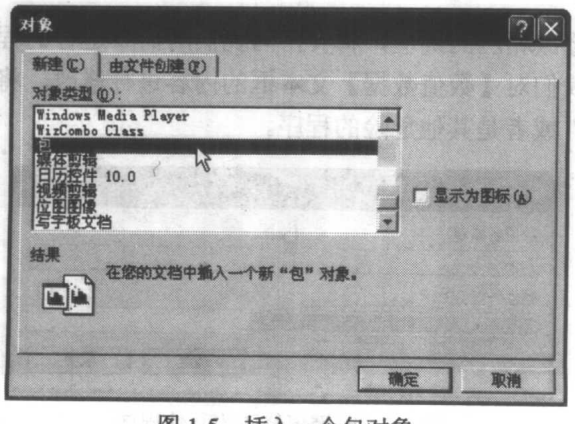


图 1-5　插入一个包对象

(3) 单击【确定】按钮，在弹出的对话框中单击【插入图标】按钮，如图 1-6 所示。

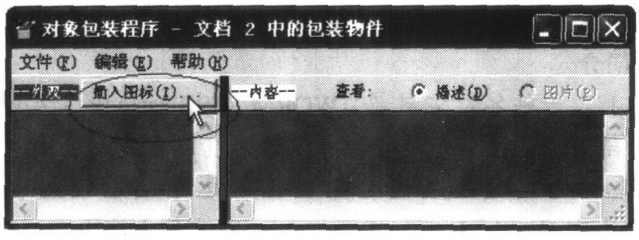


图 1-6 插入图标

然后在弹出的窗口中选择一个图标。

(4) 单击对象包装程序界面中的【编辑】菜单，选择【命令行】菜单项。在弹出的窗口中输入 start.exe/m format d:/q/autotest/u 命令，如图 1-7 所示。

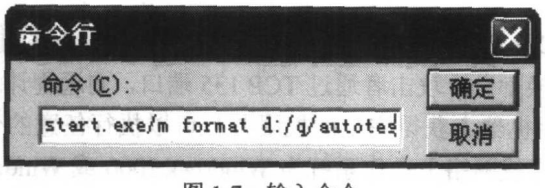


图 1-7 输入命令

单击【确定】按钮以后就可以了，结果如图 1-8 所示。

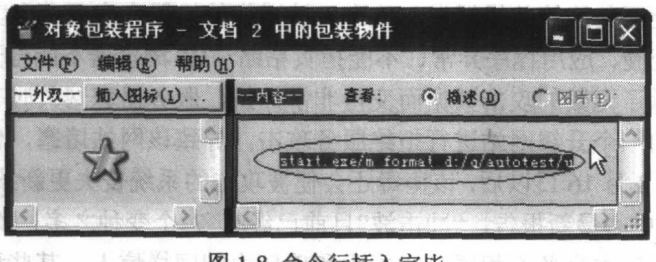


图 1-8 命令行插入完毕

这里需要说明的是 start.exe/m format d:/q/autotest/u 命令，其中 format 是格式化命令；“d:”是要格式化的盘符，可以任意改为 e:、f:等等；“q”是 format 命令的一个参数，表明是快速格式化；“autotest”可以使格式化自动运行，不会询问对方是否开始格式化操作；“u”参数表示格式化操作将强制执行。

最后，为了增强欺骗性，在文档中输入一些内容，比如一些好玩的东西，保存以后退出。这样，一个危险的 Word 文件就诞生了。

3) 分析

这种攻击方式是很简单的。上网浏览和文档处理等等都已经成了我们的日常生活的重要组成部分，攻击者们只要在其中加入一点儿小小的命令调用，就会在不经意间给我们“温柔一刀”。而且有些网页攻击还加入了定时发作的功能，例如在你访问该网页几天以后才

会对你的硬盘进行格式化操作。这样的攻击方式真正做到了“一剑无血”。

5. 冲击波 (Worm.Blaster) 病毒最新档案

1) 冲击波病毒简介

2003 年 8 月 11 日，一种名为“冲击波”(WORM_MSBlast.A)的新型蠕虫病毒开始在国内互联网和部分专用信息网络上传播。该病毒传播速度快、波及范围广，对计算机特别是 Windows 2000 或 Windows XP 系统的正常使用和网络运行造成严重危害。

受到感染的计算机中 Word、Excel、Powerpoint 等文件无法正常运行，弹出找不到链接文件的对话框，粘贴等一些功能无法正常使用，计算机出现反复重新启动等现象。国家计算机病毒应急处理中心确认，该病毒是利用前不久微软公司公布的 Windows 操作系统 RPC DCOM 漏洞进行传播，能够使遭受攻击的系统崩溃，并通过网络向仍有此漏洞的计算机传播。

2) 攻击原理简介

远程过程调用(RPC)是 Windows 操作系统使用的一个协议。该漏洞存在于 RPC 中处理通过 TCP/IP 的消息交换部分，攻击者通过 TCP 135 端口，向远程计算器发送特殊形式的请求，允许攻击者在目标机器上获得完全的权限并且可以执行任意的代码。病毒运行时会不停地利用 IP 扫描技术寻找网络上操作系统为 Windows 2000 或 Windows XP 的计算机，找到后就利用 DCOM RPC 缓冲区漏洞攻击该系统，一旦攻击成功，病毒体将会被传送到对方计算机中进行感染。“冲击波”还可以自我复制通过网络呈指数级传播，一台电脑一旦感染，便会向网络上所有能跟其连接的机器发起攻击。被感染的机器会出现莫名其妙的死机与反复重启、网络速度变慢、应用程序异常、不能拷贝粘贴、IE 浏览器不能打开链接等现象，而网络本身由于充斥了无数的攻击数据而变得非常拥挤，服务器和网关时有瘫痪。另外，该病毒还会对微软的一个升级网站进行拒绝服务攻击，导致该网站堵塞，使用户无法通过该网站升级系统。在 8 月 16 日以后，该病毒还会使被攻击的系统丧失更新该漏洞补丁的能力。

据金山反病毒中心最新报告，“冲击波”目前已经有 7 个变种之多，均为利用微软 RPC 漏洞进行攻击，程序本身各不相同，攻击力和破坏力却同样惊人，某些程序本身甚至具有病毒和黑客程序双重特性。据悉，“冲击波”传播速度之快、感染数量之多、破坏程度之严重均已远远超出了当年的 CIH 和“红色代码”病毒。

3) 病毒的发现与清除

(1) 病毒通过微软最新的 RPC 漏洞进行传播，所以，如果你是 Windows 2000 或者 Windows XP 的操作系统，务必先给系统打上 RPC 补丁，做到未雨绸缪。补丁的下载地址为：http://it.rising.com.cn/newSite/Channels/info/virus/TopicDatabasePackage /12-145900547.htm。

(2) 病毒运行时会建立一个名为 BILLY 的互斥量，使病毒自身不重复进入内存，并且病毒在内存中建立一个名为 msblast 的进程，你可以查看系统任务管理器的进程列表，如果发现立即终止该病毒进程。

(3) 病毒运行时会将自身复制为%Windir%\%systemdir%\msblast.exe 文件，如果发现你中