

电脑危险代码与防范

华师傅资讯 ◆ 编著

完全曝光

网页恶意代码一网打尽

火眼金睛

恶意代码无所遁形

铜墙铁壁

脚本病毒终极防范之道

身临其境

恶作剧代码运行效果演示

严防死守

IE保护助你冲浪万无一失

源码展现

代码技术深度剖析

精彩光盘

实用反黑工具完全收录

金山病毒专杀工具超值赠送

电脑中毒现象精彩视频演示



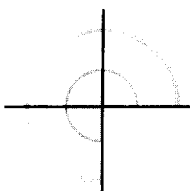
四喜大仙姑

电脑危险代码与防范

编 著 华师傅资讯



山东电子音像出版社出版



内容提要

本手册针对当前越来越严重的网络安全形势，用激烈的语言、清晰的思路和对危险代码的深入剖析，激发读者的安全防范意识，帮助你积极应对来自网络的安全威胁。如果你曾经受到过恶意代码、脚本病毒、木马偷袭、QQ病毒等形形色色的危险代码的威胁，就请拿起我们为你铸造的“电脑危险代码与防范”之剑，勇敢地接受挑战，坚决顽强地与危险代码战斗到底！

光盘内容：

1. 实用反黑工具完全收录
2. 金山病毒专杀工具超值赠送
3. 电脑中毒现象精彩视频演示

书 名：电脑危险代码与防范
编 著：华师傅资讯
责 任 编 辑：李 萍
执 行 编 辑：范晓霞 邢政义
封 面 设 计：邓玉萍
组 版 编 辑：李品娟
监 制：时均建
出 版 单 位：山东电子音像出版社
地 址：济南市胜利大街39号
邮 政 编 码：250001
电 话：(0531)2060055-7616
发 行：山东电子音像出版社
经 销：各地新华书店、报刊亭
C D 生 产：北京中联光碟有限公司
文 本 印 刷：重庆科情印务有限公司
开 本 规 格：787mm × 1092mm 1/16 15.5 印张 400 千字
版 本 号：ISBN 7-89491-074-0
版 次：2005年2月第1版 2005年2月第1次印刷
定 价：19.80元(1CD+手册)

声明

本手册及光盘中所列代码仅供分析、学习之用，请勿用做他用。

本手册及光盘涉及到的互联网站在刊登前经编辑测试，不含非法内容。今后读者若发现非法内容，请及时向当地公安机关举报。

特此声明。

目录

CONTENTS

第1章 恶意代码综述 1

1.1 恶意代码真相 2

1.1.1 恶意代码看过来 2

1.1.2 各种各样的恶意代码 2

1. 网页病毒类恶意代码 2

2. 脚本类恶意代码 3

3. 漏洞攻击类代码行 4

1.1.3 恶意代码的危害 4

1.2 恶意代码的执行环境 5

1.2.1 恶意代码的社会环境 5

1.2.2 恶意代码的系统环境 6

1. WSH 脚本解释机制 6

2. ActiveX 技术集 6

3. 各类软件漏洞 7

4. 即时通讯平台 8

5. 个人安全“三不”意识 8

第2章 网页恶意代码全录 9

2.1 恶意代码之痛 10

2.1.1 另眼相看恶意代码 10

2.1.2 与恶意网站的几次较量 10

1. 恶意网站修改 IE 主页的攻防 11

2. 恶意网站自动跳出 IE 窗口的攻防 11

3. 恶意网站加密脚本的攻防 12

2.2 恶意代码中招典型症状与防治 13

2.2.1 破坏系统的恶意代码防治 13

1. 格式化硬盘的防治 14
2. 自动运行木马的预防 14
3. 小心暗藏“万花谷”病毒的网站 20
4. 非法读取或盗取用户文件的解决办法 22

2.2.2 篡改系统设置的恶意代码防治 23

1. 开机时自动弹出的网页 23
2. 系统启动时弹出对话框 24
3. 注册表被锁定 25
4. 隐藏桌面图标 26
5. 隐藏驱动器 26
6. 隐藏开始菜单关机命令 27
7. 隐藏开始菜单运行命令 27
8. 隐藏开始菜单注销命令 27
9. 不能进入 DOS 模式 / 窗口 28
10. 更改“我的电脑”下的一系列文件夹名称 28
11. 修改登录窗口 30

2.2.3 改 IE 的恶意代码防治 30

1. IE 标题栏被修改 30
2. 修改 IE 浏览器缺省主页，并且锁定设置项 33
3. IE 默认连接首页被修改 33
4. 篡改 IE 的默认页 34
5. 地址下拉菜单被添加文字信息 34
6. IE 工具 Internet 选项不可用 35
7. IE 右键菜单被修改 36
8. 禁用查看“源文件”菜单 36
9. IE 中鼠标右键失效 37
10. 修改 IE 默认搜索引擎 38
11. 隐藏 IE 浏览器的工具栏 39
12. 在 IE 工具栏非法添加按钮 39
13. IE 收藏夹被强行添加非法网站的地址链接 39
14. 禁止使用 IE 下载 40
15. 时间前面加广告 41

16. IE 窗口定时弹出	41
---------------------	----

第 3 章 火眼金睛看透恶意代码 43

3.1 恶意代码的脚本 44

3.1.1 细说恶意代码脚本 44

3.1.2 WSH与恶意代码脚本 45

1. WSH 再解析 45
2. WSH 的用途 46
3. WSH 的工作流程 46
4. 阅读、编写 WSH 脚本源文件 47
5. WSH 与恶意代码脚本 48

3.1.3 恶意代码运行机制解析 48

1. 预防 JS+WSH 结合的恶意网页 48
2. 剖析被利用的漏洞 49

3.2 恶意 JavaScript 脚本的编写 51

3.2.1 JavaScript恶意脚本要点 51

1. JavaScript 脚本语法标记 52
2. 在Html 文档中嵌入 JavaScript 52
3. JavaScript 脚本操作注册表 53

3.2.2 剖析JavaScript脚本篡改注册表 54

1. 修改 IE 标题栏 54
2. 在右键加进网页链接 55
3. IE 设置项变灰（不可用） 56
4. 把主页加入 Windows 启动 56
5. 恶意代码的综合应用 57

3.2.3 网页恶作剧JavaScript脚本大曝光 60

1. 结束不掉的任务 60
2. 无聊的对话框 61
3. 吓人的女鬼 62
4. 屏幕闪烁 63
5. 全屏死机 64

3.2.4 网页木马全解密	65
1. 网页木马执行的途径	65
2. 让 IE6.0 执行 EXE 文件的网页	67
3.3 注册表脚本应用	70
3.3.1 如何编写注册表脚本	70
3.3.2 注册表脚本应用实例	71
1. 在登录 Windows 时显示消息文字	71
2. 修改 Windows 的常用设置选项	72
3. 修复被恶意代码篡改的项目	73

第4章 危险的VB脚本..... 75

4.1 VB 脚本的编写	76
4.1.1 HTML 页面中的VB脚本	76
1. 什么是 VB 脚本	76
2. 在 HTML 页面中添加 VBScript 代码	76
3. VBScript 页面的简单样例	78
4.1.2 VB脚本访问注册表	79
1. VB 脚本访问注册表基本知识	79
2. VB 脚本访问注册表实例剖析	84
4.1.3 强大的VB脚本	87
1. 获取驱动器信息	88
2. 访问文本文件	90
3. 创建各种快捷方式	95
4.2 VB 脚本病毒	97
4.2.1 VBS脚本病毒原理分析与防范	97
1. VBS 脚本病毒的特点及发展现状	97
2. VBS 脚本病毒原理分析	98
3. VBS 脚本病毒的防范	103
4.2.2 VB脚本病毒代码实例分析	104

1. “欢乐时光”病毒剖析	104
2. “新欢乐时光”病毒剖析	105

第 5 章 危险脚本与黑客攻击 107

5.1 宏病毒剖析与防治	108
5.1.1 宏技术的使用	108
5.1.2 宏病毒的分类及特性	109
5.1.3 宏病毒的作用机制	110
5.1.4 宏病毒的预防与清除	111
1. 宏病毒预防	111
2. 宏病毒清除	113
3. 防治 Access 宏病毒	116
5.1.5 消灭恶意宏魔	117
1. W97M_THUS 的清除	117
2. W97M/Pacol.a 的清除	117
3. W97M_MSKONG.A 的清除	118
4. W97M.Tenda.A 的清除	119
5. W97M.Fool.J.Gen 的清除	121
5.2 ASP 脚本攻击	121
5.2.1 ASP程序数据库密码验证漏洞的防范	122
5.2.2 防止用""&request漏洞猜解用户名和密码	127
5.2.3 用户名与口令被破解怎么办	131
5.2.4 验证被绕过的处理	131
5.2.5 inc文件泄露问题解决办法	132
5.2.6 防止bak文件泄漏asp源代码	132
5.2.7 防止特殊字符攻击	133
5.2.8 防范数据库下载漏洞	133
5.3 PHP 脚本漏洞逐个数	134

5.3.1 PHP脚本是什么	134
5.3.2 PHP开发中的潜在漏洞	136
1. 在PHP中执行系统调用	136
2. 预防系统调用攻击	138
5.3.3 防止PHP远程文件包含漏洞被利用	138
5.3.4 PHP注入实例解析	140
5.3.5 bBlog脚本处理输入URI远程SQL注入漏洞防范	142
5.3.6 PHPShop远程PHP脚本执行漏洞防范	142
5.3.7 JAWS ControlPanel.php脚本处理SQL注入漏洞防范	142
5.3.8 functions.php脚本文件泄露漏洞防范	142
5.3.9 Phorum follow.php脚本远程SQL注入的漏洞防范	143
5.4 Shell 病毒解析	143
5.4.1 Shell脚本的工作方式	143
5.4.2 Shell病毒解析	146
5.5 CGI 脚本攻击与防范	148
5.5.1 CGI脚本和程序	148
5.5.2 防范CGI脚本的攻击	149
1. 两种导致问题的方式	149
2. 不要相信表单数据	150
3. 不合理数据的来源	150
4. 拒绝不合要求的表单数据	151
5. 不要相信路径数据	152
6. 处理外部进程	153
5.5.3 使用他人CGI脚本时的注意事项	154
1. 追根求源	154
2. 注意礼貌	155
5.6 Net 病毒解析	155
5.6.1 微软 .Net 架构	155

1. 通用语言运行库	155
2. 统一编程类	156
3. ASP+ 控件集	156
5.6.2 针对 .Net 的病毒剖析	156
1. Win32. Donut 病毒的剖析	156
2. Win32. Sharpei 病毒的剖析	157

第6章 即时聊天：恶意代码的舞台 159

6.1 即时通讯安全解读	160
6.1.1 即时通讯的安全隐患	160
1. 恶意代码的传播平台	160
2. 惊人的传播速度	162
6.1.2 即时通信安全漏洞管理	162
1. 安全漏洞的管理与对策	162
2. 个人用户自我防范的七步棋	164
3. 企业用户安全管理	164
6.2 QQ 恶意代码剖析	165
6.2.1 QQ 恶意代码攻防	166
1. “QQ 尾巴”病毒攻防	166
2. “QQ 缘”病毒攻防	167
3. “QQ 狩猎者”病毒攻防	168
4. “武汉男生”病毒攻防	169
5. “爱情森林”病毒攻防	171
6. “QQ 女友”病毒攻防	174
7. 超级密码杀手攻防	176
6.2.2 QQ 炸弹攻防	180
1. QQ 炸弹代码攻防	180
2. QQ 炸弹工具攻防	181
6.2.3 QQ 安全工具点击	183
1. 爱情后门专杀工具	183
2. QQ 狩猎者病毒专杀工具	183

3. QQ 自动发消息专杀工具	184
4. QQ 病毒专杀工具 XP	185
6.3 非 QQ 类即时通信工具安全防范	186
6.3.1 ICQ 恶意代码攻防	186
1. ICQ 恶意代码剖析	186
2. ICQ 恶意代码防范	188
6.3.2 雅虎通漏洞防范	189
1. yauto.dll 漏洞防范	189
2. “文件长度”漏洞防范	190
6.3.3 网易泡泡安全漏洞防范	190
6.3.4 MSN 病毒防范	191
1. MSN 病毒简析	191
2. MSN 病毒防范措施	193
6.4 手机病毒剖析与防范	193
1. 手机病毒的实现原理	193
2. 手机漏洞分析	194
3. 手机病毒的主要类型	195
4. 手机病毒的攻击方式	196
5. 手机病毒趋势	197
6. 防范手机病毒	198
6.5 即时通讯安全工具——IMsecure Pro	199

第 7 章 恶意代码免疫法.....205

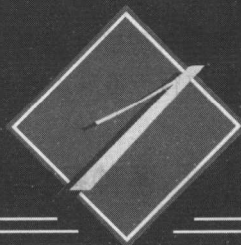
7.1 病毒及恶意代码免疫原理	206
7.1.1 恶意代码免疫原理	206
7.1.2 免疫的方法和缺点	206
1. 针对某一种病毒进行的计算机病毒免疫	206
2. 基于自我完整性检查的计算机病毒的免疫方法	207

7.1.3 恶意代码的免疫	207
7.2 IE 恶意代码免疫	208
7.2.1 注册表免疫	208
1. 修改注册表免疫	208
2. 网页免疫	208
7.2.2 免疫工具逐个数	209
1. 黄山 IE 修复专家	209
2. IE 恶性代码杀手终结者 2004	210
3. 3721、CNNIC、百度、新浪免疫程序 (V2.14)	211
4. VBScript 免疫	211
5. 网络免疫大使	212
6. Anti ActiveX nags (V1.02)	212
7. 龙帝免疫王	213
7.3 病毒免疫	214
7.3.1 QQ病毒免疫	214
1. QQ 病毒免疫	214
2. 腾讯 QQ 病毒专杀工具	217
7.3.2 应用程序病毒免疫器	219
1. 病毒免疫器的免疫原理	219
2. 免疫软件的具体使用	219
7.3.3 新蠕虫病毒免疫模块	222
7.3.4 冲击波病毒万能免疫程序	222
7.3.5 CIH终身免疫	223
7.3.6 尼姆达+求职信免疫程序 1.0	224
7.3.7 终极防线	224
7.4 木马免疫	226
7.4.1 木马天敌	226
7.4.2 网页病毒木马免疫疫苗 (V1.0)	227

7.4.3 木马免疫DIY	227
1. 根据木马自启动特征免疫	227
2. 将EXE程序与Explorer.exe绑定	228
7.5 恶意代码的防御.....	229
7.5.1 脚本安全管理	229
1. 卸载WSH	229
2. 禁止脚本运行	230
3. 实时保护IE	231
7.5.2 注册表安全管理	231
1. 禁止使用注册表	231
2. 注册表备份	232
7.5.3 恶意代码防火墙	233
1. GoldTach Pro 防火墙	233
2. 瑞星杀毒软件 2005.....	234

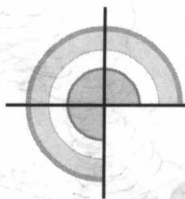


第



章

恶意代码综述



1.1

恶意代码真相



1.1.1 恶意代码看起来

我们时常听到“恶意代码”的说法，但在不同场合，“恶意代码”的含义是不确定的。多数情况下，我们把嵌入一个网页中具有恶意改变 IE 设置、系统设置、甚至格式化硬盘功能，随 IE 浏览该页面而自动在 Windows 特定环境下执行的有害代码叫“恶意代码”。但是经常使用 QQ 的用户对“恶意代码”则有另外一种理解，即被一些恶作剧网友利用软件缓冲区漏洞发送来攻击 QQ，造成 QQ 一系列错误的代码。在一些杀毒软件厂家看来，前者又被叫做网页病毒（职业眼光），而后者则纯粹是由系统漏洞引发的事件。但不论我们怎样定义恶意代码，最重要的一点，就是代码的“恶意”性质及其给用户造成的伤害已经引起普遍的关注，我们有必要对恶意代码进行一番深入剖析，彻底识破恶意代码的种种假面，揭穿代码恶意执行的真相。



1.1.2 各种各样的恶意代码

从上面的定义可以看出，恶意代码有两种基本表现形式，一种是杀毒软件厂商眼中的网页病毒，另一种是 QQ 用户眼中的漏洞攻击代码。

1. 网页病毒类恶意代码

既然被称为“网页病毒”，我们就可以从病毒的角度给恶意代码定义——即利用软件或系统操作平台安全漏洞，通过嵌入在网页 HTML 标记语言内的 Java Applet 应用程序、JavaScript 脚本程序、ActiveX 网络交互支持自动执行，强行修改用户注册表及系统配置，或非法控制系统资源、盗取用户文件，恶意删除文件，甚至格式化硬盘的非法恶意程序。

这种非法恶意程序能够得以被自动执行，在于它完全不受用户的控制。一旦浏览了含毒的网页，即可在不知不觉的情况下中招，给系统带来一般性的、或轻度的、或严重的破坏。根据目前互联网上流行的常见网页病毒的作用对象及表现特征，网页病毒可归纳为以下两大类：

(1) 通过 Java Script、Applet、ActiveX 编辑的脚本程序修改 IE 浏览器，表现为：

- 默认主页被修改；
- 默认首页被修改；
- 默认的微软主页被修改；

- 主页设置被屏蔽锁定，且设置选项无效不可改回；
- 默认的 IE 搜索引擎被修改；
- IE 标题栏被添加非法信息；
- OE 标题栏被添加非法信息；
- 鼠标右键菜单被添加非法网站广告链接；
- 鼠标右键弹出菜单功能被禁用失常；
- IE 收藏夹被强行添加非法网站的地址链接；
- 在 IE 工具栏非法添加按钮；
- 锁定地址下拉菜单及其添加文字信息；
- IE 菜单“查看”下的“源文件”被禁用。

(2) 通过 Java Script、Applet、ActiveX 编辑的脚本程序修改用户操作系统，表现为：

- 开机出现对话框；
- 系统正常启动后，但 IE 被锁定网址自动调用打开；
- 格式化硬盘；
- 暗藏“万花谷”病毒，全方位侵害封杀系统，最后导致瘫痪崩溃；
- 非法读取或盗取用户文件；
- 锁定禁用注册表；
- 注册表被锁定禁用之后，编辑 *.reg 注册表文件打开方式错乱；
- 时间前面加广告；
- 启动后首页被再次修改；
- 更改“我的电脑”下的一系列文件夹名称。

2. 脚本类恶意代码行

一旦把网页恶意代码归入病毒一类，我们发现对恶意代码理解的思路豁然开朗，既然网页恶意代码可以被称为病毒，而网页恶意代码又都是用 JavaScript 等脚本编写，那么同样是使用简单脚本编写、具有恶意功能的 VB 脚本病毒、宏病毒、PHP 病毒也可称为“恶意代码”了，这样理解其实就接近了本书要探讨的恶意代码的实质——脚本。

脚本，英文为 Script。实际上脚本就是程序，一般都是由应用程序提供的编程语言。应用程序包括浏览器（JavaScript、VBScript）、多媒体创作工具，应用程序的宏和操作系统的批处理语言也可以归入脚本一类。脚本同我们平时使用的 VB、C 语言的区别主要是：

- 脚本语法比较简单，比较容易掌握；
- 脚本与应用程序密切相关，所以包括相对应用程序自身的功能；
- 脚本一般不具备通用性，所能处理的问题范围有限。

脚本在每一种应用程序中所起的作用都是不一样的，比如在网页中可以实现各种动态效果，各种特效处理，实现各种 HTML 不能实现的功能。而在 Office 组件中，我们会经常看到“宏”这个工具，它其实是一系列命令和指令，可以实现任务执行的自动化，用于提供工作效



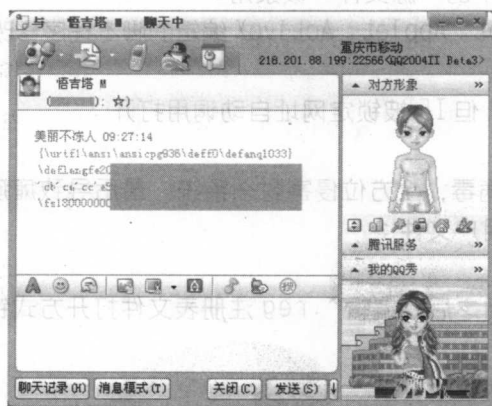
率，或者制造宏病毒。

3. 漏洞攻击类代码

对于 QQ 用户而言，对于作为对漏洞进行攻击的“代码行”这一点，可谓记忆犹新。比如这样一行代码：

```
{\urtfl\ansi\ansicpg936\deff0\deflang1033\deflangfe2052{\fonttbl{\lf0\fnil\charset2webdings;}}{\fl\fnil\charset134\cb\ce\ce\ce5;}} {\colortbl\red330\green22\blue0;}\viewkind4\uc1\pard\cfl\lang2052\fs1638gc\cf0\fl\fs18\par }
```

你只要将它发送到对方的 QQ 上，对方的 QQ 就会立即死掉：



让 QQ 死掉的恶意代码

这类代码，在黑客攻击案例中应用较多。对于这类“代码行”，本书只着重关注其对 QQ 等实时聊天工具的攻击与防范，这也是广大网友最关心的。



1.1.3 恶意代码的危害

从上一节恶意代码的表现，我们就可以知道恶意代码的危害有多大了。对系统而言，可谓“轻者致残，重者丧命”。

一些网站为了强行留住网民对自己网站的访问，让我们的浏览器长期为其做广告，利用网页技术中的恶意脚本程序，将访问者的 IE 不由分说地进行修改。一般改掉你的起始页和默认主页，为了不让你改回去，甚至将 IE 选项中的默认主页按钮变为失效的灰色——这还算是轻一点的了。

还有一类恶意代码，如果你不小心浏览了含有这类恶意代码的网页，其后果是：“关闭系统”、“运行”、“注销”、注册表编辑器、DOS 程序、运行任何程序被禁止，系统无法进入“实