电脑报 总策划

黑客通缉令

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

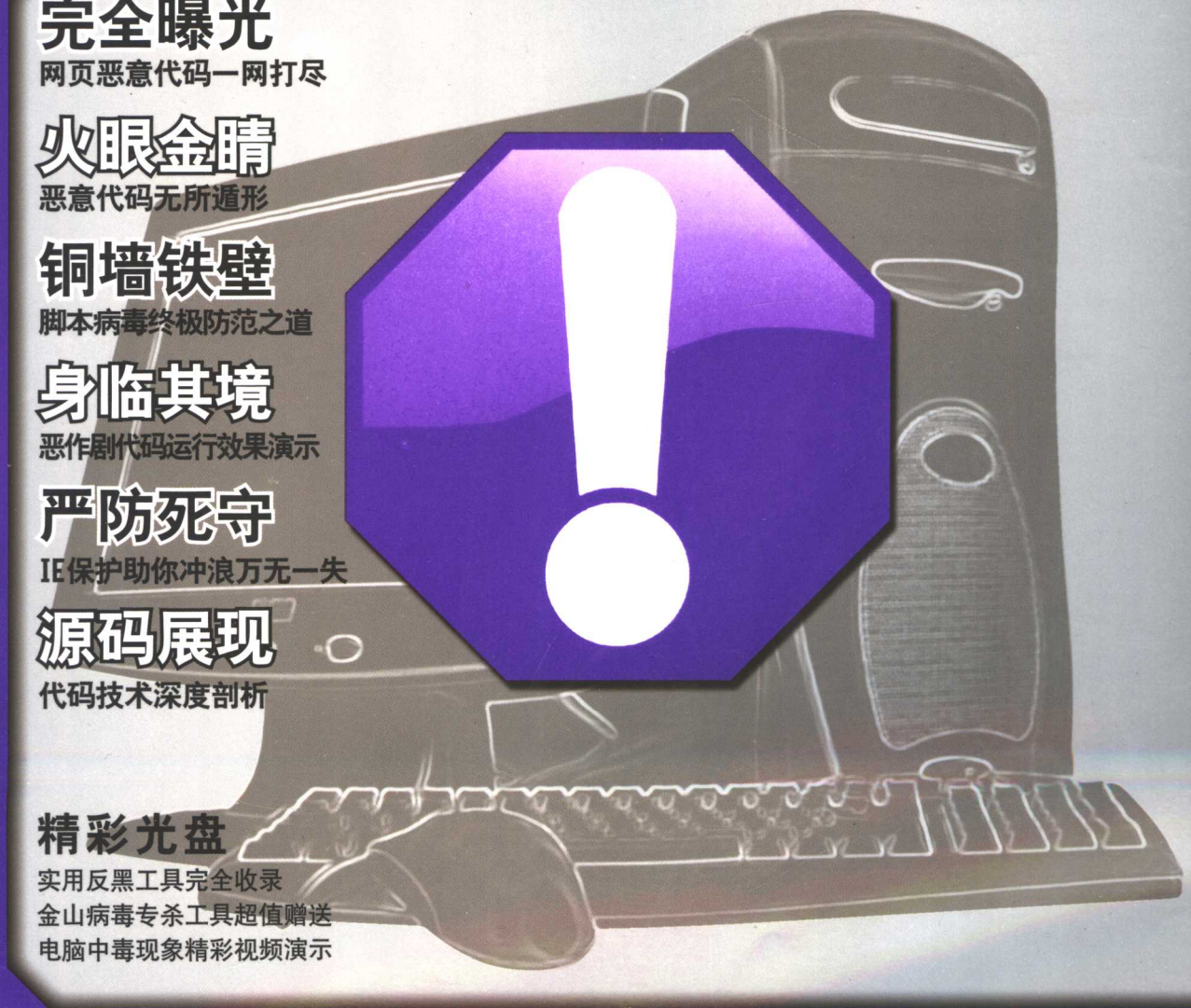
铜墙铁壁
脚本病毒终极防范之道

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

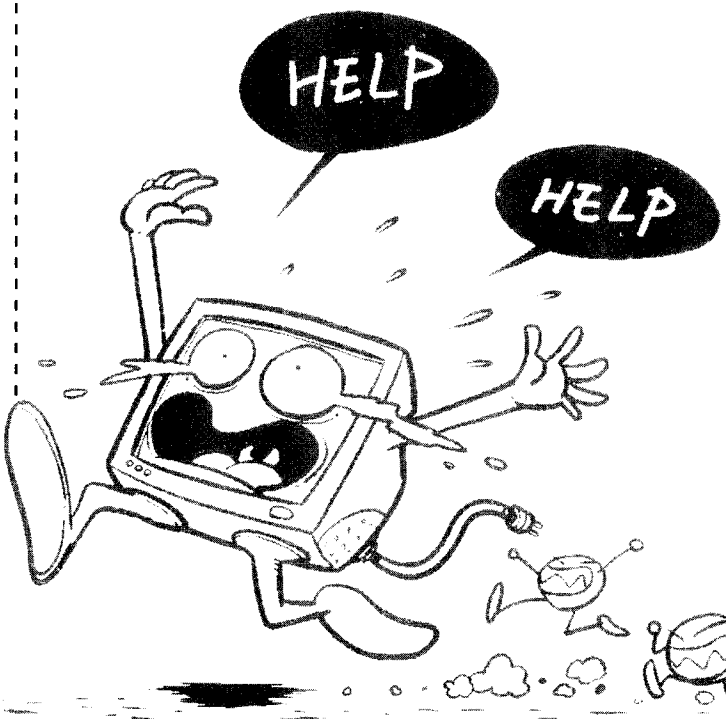


山东电子音像出版社出版

黑客大地城

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)

目录 CONTENTS

第1章

恶意代码综述

1.1 恶意代码真相

1.1.1 恶意代码看过来

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种类：

(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：

```
{\urtf1\ansi\ansicpg936\deff0\deflang1033\deflangfe2052{\fonttbl{1f0\fnil\fcharset2
webdings;}{\fl\fnil\fcharset134\'cb\'ce\'cc\'e5;}} {\colortbl_;\red330\green22\blue0;}
\viewkind4\ucl\pard\cf1\lang2052\f0\fs1638g\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