<<网页木马攻防实战>>

图书基本信息

书名：<<网页木马攻防实战>>

13位ISBN编号：9787121085567

10位ISBN编号：7121085569

出版时间：2009-5

出版时间：任飞、章炜、 张爱华 电子工业出版社 (2009-05出版)

前言

笔者经常去书店买书，通常在买书之前，都会先把一本书的前言通读一遍，然后再来决定购书的意向。
本书完稿后，很长一段时间里，笔者不知该如何写好这篇前言，写书时的那些灵感刹那间消失了。
网页木马自从诞生那天开始就是大家热衷于讨论的话题，笔者花了半年多时间把平日积累下来的经验转换为文字，希望通过此种方式能与对这些知识感兴趣的人们进行交流。
如果大家能在这本书中学到新的知识和技术，那么这本书就完成了它的使命。
希望这本书不会长时间静静地躺在图书馆或书店的某个角落里，如果您发现了它，请把它带走。
作为一本专门介绍网页木马的书籍，本书的立场是站在防御的角度，深入浅出地剖析网页木马的相关原理和技术，让读者更进一步了解和掌握网页木马的相关知识。
如果您不懂调试和脚本语言，没关系，本书的第3章会帮您解决这个问题；如果您不懂溢出，没关系，本书的第4章会以生动的实例告诉您溢出的详细原理；如果您不懂Shellcode，没关系，相信读完本书的第5章后，您一定能编写出自己的Shellcode。
在您掌握上述相关知识后，通过本书第7章“网页木马实例分析”的学习，可进一步加深理解前几章的内容，以便及时对网页木马采取安全防范措施，减少网页木马给自身带来的损失。
本书的内容安排第1章 网页木马综述本章给读者讲述网页木马的概念，什么是网页木马，网页木马发展的历史，网页木马的种类，可能造成怎样的危害，并通过几个简单的网页木马实例来增加直观性。
第2章 网页木马剖析本章剖析网页木马中使用的几个关键技术，如调试基础、脚本语言、Shellcode编写、网页木马免杀方法等。
第3章 调试器与脚本语言本章介绍调试器和脚本语言的相关知识，使读者对用来调试缓冲区溢出漏洞的这些利器有深入的了解。
第4章 缓冲区溢出本章介绍缓冲区溢出的原理（包括产生原因、种类、危害等），使读者能够对缓冲区溢出有一个整体概念，并通过实例来形象地说明它的危害及其与网页木马之间的关系。
第5章 Shellcode的编写本章介绍如何编写一个Shellcode，并通过几个实例把Shellcode编写中的过程，以及编写过程中可能遇到的问题（例如无效字符、大小、自包含技巧、可移植性等）解释清楚。
第6章 网页木马免杀技术分析本章对网页木马中曾经用过的免杀方法和技术进行了分析，例如网页木马变形技术、网页木马加密技术等。
第7章 网页木马实例分析本章以几个曾经在国内甚至国际非常流行的网页木马为实例来进行具体分析，使读者加深对上述相关章节的理解，以便及时有效地对网页木马采取安全防范措施，减少网页木马给自身带来的损失。
第8章 网页木马防范本章通过给读者一些安全建议，使读者如何尽可能地减少网页木马的危害。
例如：保证系统处于自动更新状态，下载并安装安全补丁；如何安全地设置浏览器；如何设置其他的安全工具辅助（例如防火墙、杀毒软件等）。
随书代码读者可以从博文视点网站http://www.broadview.com/08556下载随书代码和相关资料。
当然您也可以在该站点的相关版面与所有读者共同讨论网页木马的相关技术，撰写精彩的书评，以达到共同进步的目的。
如果您有什么好的建议，同样欢迎您在网站上提出！
致谢在撰写本书的过程中，得到了身边很多朋友的关心和支持，在此表示诚挚的感谢，最重要的是感谢父母多年来对我的培养，真心地感谢你们！

<<网页木马攻防实战>>

内容概要

《网页木马攻防实战》从防御网页木马的角度，深入浅出地分析了网页木马的基本原理及相关核心技术，图文并茂地再现了多种网页木马制作及防御的全过程。
在内容上将针对性、实践性与综合性加以有机的结合，并包含大量有价值代码，以满足广大读者学习代码分析技术的需求。

《网页木马攻防实战》共分为8章，对网页木马进行了全面透彻的解析。
内容包括网页木马综述、网页木马剖析、调试器与脚本语言、缓冲区溢出、Shellcode的编写、网页木马免杀技术分析、网页木马实例分析和网页木马防范。
通过《网页木马攻防实战》的学习，读者能够对网页木马和溢出攻击有更加深入的理解；能够及时有效地对网页木马采取安全防范措施，从而减少网页木马给自身带来的损失。
《网页木马攻防实战》适合于网络技术爱好者、网络系统管理员、软件开发及信息安全技术人员阅读，并可作为大中专院校相关专业学生的学习资料和参考用书。

<<网页木马攻防实战>>

书籍目录

章节摘录

插图：第1章 网页木马综述 1.1 概述 从本质上来说，网页木马就是一个Web页面，可以是一个静态的HTML页面，也可以是ASP、PHP、JSP等动态页面。
从表面上看，它和一个普通的页面并没有太大的区别，但是包含在HTML源代码中的恶意脚本可以使IE浏览器在后台、在用户不知情的情况下下载，并执行恶意的木马。
但是大家也不必“谈马色变”，弄清了它的原理之后，防范其实也是能够做到的。
为什么浏览器会自动下载，并执行木马呢？
现在大部分的网页木马都是针对Windows系统自带的IE浏览器的，针对其他第三方浏览器的网页木马很少；但像Maxthon、腾讯TT等这种基于IE核心的浏览器也和m浏览器一样，会受到网页木马的影响。
那么，使用Firefox等非IE浏览器上网的用户是不是就不会中网页木马了呢？
答案是否定的。
现在有许多应用软件，例如RealPlayer等影音播放软件、RSS阅读器以及迅雷这些程序都是借助于IE核心来显示HTML页的第三方软件的，因此同样存在着中网页木马的风险，也就是说，网页木马是防不胜防的。

<<网页木马攻防实战>>

编辑推荐

《网页木马攻防实战》特点：网页木马综述：讲述网页木马的概念和发展的历史，网页木马的种类，可能造成的危害.并通过几个网页木马的实例来加深理解。
网页木马剖析：介绍剖析网页木马中使用的几项关键技术，如调试器、脚本语言、Shellcode编写、网页木马免杀技术等。
调试器与脚本语言：介绍调试器和脚本语言的相关知识，使读者对用来调试缓冲区溢出漏洞的这些利器有深入的了解。
缓冲区溢出：介绍缓冲区溢出的原理(包括产生原因、种类、危害等)，并通过实例形象地说明它的危害及其与网页木马之间的关系。
shellcode的编写：介绍如何编写一个Shellcode,并通过几个实例把Shellcode编写过程中可能遇到的问题(例如无效字符、大小、自包含技巧、可移植性等)解释清楚。
网页木马免杀技术分析：分析网页木马中使用的免杀技术,例如网页木马变形技术、网页木马加密技术等。
网页木马实例分析：对几个流行的网页木马实例进行具体分析,以便及时对网页木马采取安全防范措施。
网页木马防范：讲述如何减少网页木马的危害.并提出一些安全建议.如：使系统自动下载并安装安全补丁；安全地设置浏览器以及采用其他的安全工具辅助(防火墙、杀毒软件)等。

<<网页木马攻防实战>>

版权说明