<<木马攻防全攻略>>

图书基本信息

书名：<<木马攻防全攻略>>

13位ISBN编号：9787894761620

10位ISBN编号：7894761621

出版时间：1970-1

出版时间：万立夫 电脑报电子音像出版社 (2009-06出版)

作者：万立夫

页数：344

<<木马攻防全攻略>>

前言

关于计算机病毒、网络盗号的新闻，我相信大家通过各种媒体都有所耳闻吧？
就在2009年的3月15日晚上.中央电视台的3.15晚会全面曝光了个人信息被窃取等一系列安全事件，比如个人信息被运营商暗中频繁交易并从中获利，黑客通过木马病毒盗号窃取用户的银行资金其实作为一个长期关注网络安全的作者，对于“病毒产业链”的勾当也不是现在才知道。
但是当这一切真实地展现在自己眼前时，还是觉得那么不可思议、那么触目惊心。
于是我开始思考.这些可恶的木马病毒是怎么进入计算机系统，并将用户的系统变为传说中的“肉鸡”，从而在系统里面为所欲为的呢？
我突然有了一种想法，就是把自己所了解的，关于黑客从入侵系统到盗号的整个过程，完完整整地展现在各位读者面前，并让整个“病毒产业链”大白于天下。
正巧此时电脑报也在策划一部防范木马入侵的网络安全读物，于是双方很快一拍即合，也就促成了这部《木马攻防全攻略》的最终面市。
由于前期规划比较充分，因此在收集内容、撰写稿件的时候比较轻松，甚至可以说是一气呵成。
首先我以木马程序为切人点，讲解了各种常用木马的使用、测试、免杀、传播，可以说较为全面地展现了“病毒产业链”的每一个环节。
同时还在撰写稿件的时候，全面透切地分析和解读了目前网络中最新的安全事件，让普通读者能够快速了解黑客的最新手法。
如果要说稿件的撰写有没有遇到什么困难，我认为最大的问题就是其中涉及到大量的关于网络安全方面的术语以及PE文件的核心内容。
对于第一次接触到汇编语言的读者，在遇到晦涩难懂的代码时可能更会感到痛苦不堪，于是我尽量使用浅显易懂的语言，再加上大量的小知识和小提示.目的让入门读者能够轻松明白文中的意思。
希望大家阅读之后，能够更好地保护自己在网络中的利益，不要让那些不愉快的被盗事件再次发生在自己的身边。

<<木马攻防全攻略>>

内容概要

如今的网络世界中，木马带来的安全问题已经远超病毒，它们如幽灵般地渗入到计算机中，已成为监控、窃取和破坏我们信息安全的头号杀手。
本手册融合了作者多年的研究成果，真实再现了木马配置、伪装、防杀、植入的全过程，深入浅出地讲解了如“反弹连接”、“线程插入”、“隧道技术”、“键盘记录”、“特征码修改”、“添加花指令”等热点问题，解决困挠大多数木马研究者的疑问！
一直以来，由于公众对木马知之甚少，才使得木马有机可乘，我们坚信只有将木马的伎俩公诸于众，才能更好地提升公众的安全意识，真正捍卫我

<<木马攻防全攻略>>

书籍目录

章节摘录

插图：特洛伊木马（以下简称木马），英文叫做“ Trojan horse ”，其名称取自希腊神话的特洛伊木马记。
古希腊传说，特洛伊王子帕里斯在访问希腊时诱走了王后海伦，希腊人因此远征特洛伊。
围攻9年后到第10年，希腊将领奥德修斯献了一计，就是把一批勇士埋伏在一匹巨大的木马腹内，放在城外后佯作退兵。
特洛伊人以为敌兵已退，就把木马作为战利品搬入城中。
到了夜间，埋伏在木马中的勇士跳出来打开了城门，希腊将士一拥而人攻下了城池。
后来，人们就常用“ 特洛伊木马 ”这一典故，用来比喻在敌方营垒里埋下伏兵里应外合的活动。
特洛伊木马没有复制能力，它的特点是伪装成一个实用工具或一个可爱的游戏，这会诱使用户将其安装在计算机系统或者服务器上。
“ 中了木马 ”就是指安装了木马的服务器程序，例如某电脑被安装了木马服务器程序，那么拥有控制器程序的人就可以完全控制住这台电脑，不论是文件、程序，还是账号、密码都毫无安全可言。
从木马的发展来看，基本上可以分为两个阶段。
当网络还处于以UNIX平台为主的时代木马就产生了，当时的木马程序功能相对简单，往往是将一段程序嵌入到系统文件中，用跳转指令来执行一些远程控制功能，在这个时期木马的设计者和使用者大都是些技术人员，必须具备相当的网络和编程知识。
随着Windows平台的日益普及，一些基于图形操作的木马程序出现了，用户界面的改善“ 普及 ”了木马，让那些不太懂专业知识人都可以熟练地操作木马，因此木马就泛滥了，使用木马入侵的事件也频繁出现。

<<木马攻防全攻略>>

编辑推荐

《木马攻防全攻略》深入剖析木马入侵手法揭秘木马伪装的伎俩，真枪实弹向黑客宣战！
走进木马的世界 初探传统的C/S型木马以无招胜有招适用于任何环境的B/S型木马小到无形的杀手警惕“一句话木马”让防火墙形同虚设“反弹连接”成主流绑架系统进程“线程插人”技术IE浏览器被劫持利用80端口上线的“HTTP隧道技术”马甲花招多重木马加壳实战演示改头换面修改特征码巧过杀毒软件道魔谁更高突破主动防御有新招

<<木马攻防全攻略>>

版权说明