

<<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

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<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入点，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，解决困扰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

Chapter1 快速走进木马世界1.1 木马的前世和今生1.2 病毒与木马1.2.1 病毒的特点1.2.2 木马与后门1.3 木马与远程控制1.3.1 什么是远程控制1.3.2 远程控制的实现1.3.3 木马的特殊性1.4 木马的入侵途径Chapter2 C/S型木马程序2.1 木马王者——冰河2.1.1 “冰河”的介绍2.1.2 “冰河”的操作2.2 不死鸟——灰鸽子2.2.1 了解“反弹连接”木马2.2.2 配置“灰鸽子”服务端2.2.3 配置“灰鸽子”客户端2.2.4 远程控制服务端2.2.5 线程插入技术2.3 突破主动防御——红狼远控2.3.1 配置“红狼”服务端2.3.2 “红狼”服务端操作2.3.3 “红狼”木马的相关技术Chapter3 B/S型木马程序3.1 浏览器木马——网络精灵3.1.1 网络精灵的由来3.1.2 网络精灵传统控制3.1.3 浏览器远程控制3.2 蔚蓝色的海洋——海阳顶端网ASP木马3.2.1 海阳顶端网ASP木马运行环境3.2.2 海阳顶端网ASP木马的功能3.2.3 配置海阳顶端网ASP木马3.3 多项全能远程控制——rmtsvc3.3.1 rmtsvc命令行参数3.3.2 rmtsvc的配置文件3.3.3 rmtsvc的实际操作Chapter4 特殊类型木马揭秘4.1 木马病毒传送带——木马下载者4.1.1 木马下载者的作用4.1.2 木马下载者操作演示4.1.3 木马下载者特殊技术4.2 脚本木马下载者——一句话木马4.2.1 什么是“一句话木马”4.2.2 配置“一句话木马”4.2.3 另类“一句话木马”4.3 在内网中飞翔——端口映射4.3.1 什么是端口映射4.3.2 端口映射如何实现4.4 在网络中隐身——网络跳板4.4.1 什么是跳板4.4.2 跳板的制作4.5 由黑变白的“黑洞”远程控制4.5.1 配置“黑洞”客户端4.5.2 配置“黑洞”服务端4.5.3 控制“黑洞”服务端Chapter5 搭建木马测试环境5.1 优化配置杀毒软件5.1.1 优化设置5.1.2 隔离还原5.1.3 系统防护5.1.4 放行木马5.2 虚拟机的安装配置5.2.1 什么是虚拟机5.2.2 虚拟机的种类5.2.3 虚拟机的配置5.3 安装配置影子系统5.3.1 影子系统的介绍5.3.2 影子系统的操作5.4 安装配置沙盘安全环境5.4.1 Sandboxie的保护方式5.4.2 Sandboxie的使用方法5.4.3 Sandboxie的其他设置5.5 搭建脚本运行环境5.5.1 搭建ASP脚本运行环境5.5.2 快速搭建ASP运行环境5.5.3 搭建PHP脚本运行环境Chapter6 木马防杀技术6.1 杀毒软件基础知识6.1.1 杀毒软件原理基础6.1.2 基于文件扫描的技术6.1.3 认识PE文件结构6.1.4 认识汇编语言6.2 加壳及多重加壳操作6.2.1 什么是“壳”6.2.2 单一壳的操作6.2.3 壳的变异操作6.2.4 多重加壳演示6.2.5 壳中改籽技巧6.3 花指令的添加和修改6.3.1 什么是花指令6.3.2 利用工具加花6.3.3 修改旧花指令6.3.4 编写新花指令6.3.5 添加新花指令6.4 分析查找木马特征码6.4.1 何谓“特征码”6.4.2 分析文件特征码6.4.3 修改文件特征码6.4.4 关键字分析修改6.4.5 分析内存特征码6.4.6 其他分析方式6.5 PE文件头的分析修改6.5.1 PE文件头的介绍6.5.2 PE文件头的修改6.6 输入表内容分析修改6.6.1 什么是输入表6.6.2 重建输入表6.6.3 转移函数名称Chapter7 另类木马防杀技术7.1 附加数据惹的祸7.1.1 附加数据留下线索7.1.2 “PCshare”的修改7.1.3 “灰鸽子”的修改7.2 修改木马关键字字符串7.2.1 “移花接木”调换字符串7.2.2 “借尸还魂”替代字符串7.3 木马突破主动防御的手段7.3.1 什么是主动防御7.3.2 突破卡巴斯基主动防御7.3.3 其他杀毒软件主动防御7.3.4 木马程序自定义设置7.3.5 简单设置突破主动防御7.3.6 捆绑程序巧过主动防御7.4 脚本木马免杀方法7.4.1 脚本木马工具免杀法7.4.2 脚本木马手工免杀法7.4.3 其他脚本木马免杀法Chapter8 木马伪装的多种方式

<<木马攻防全攻略>>

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，希腊将士一拥而入攻下了城池。

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“线程插入”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

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>