<<僵尸网络>>

图书基本信息

书名：<<僵尸网络>>

13位ISBN编号：9787030249432

10位ISBN编号：7030249437

出版时间：2009-8

出版时间：科学

作者：(美)席勒|译者:邢健//党开放//刘孜文

页数：294

<<僵尸网络>>

内容概要

网络技术飞速发展．病毒、蠕虫、木马等不断涌现，而僵尸网络则是“网络程序杀手”，其危害远远高于以前的恶意脚本，已经成为网络社会所面临的最大威胁。

本书从一个真实的僵尸网络攻击案例开始，随后结合实例介绍僵尸网络的基础知识，包括僵尸网络的概念、运行方式和环境、生命周期等。

紧接着介绍僵尸网络的检测、跟踪工具和技术，以及0urmon和沙盒工具的使用，最后讲解了如何获取情报资源及如何应对僵尸网络。

本书特色　·第一本专门介绍最新网络威胁——僵尸网络的作品　·介绍了什么是僵尸网络、它们如何传播、利用何种工具来对抗等问题　·全面覆盖Ourmon和其他开放资源工具　·由多位富有丰富实践经验的专家编写

作者简介

Craig A. Schiller（CISSP_ISSMP，ISSAP） 波特兰州立大学首席信息安全官；鹰眼安全培训有限公司总裁；最早的公认系统安全准则（GASSP）的主要作者，与他人合著Handbook of Information Security Management，Data Security Management的特约作者。
Crai9先生也参与编写了Combating Spyware in the Enterprise（Syngress，ISBN：1597490644）和Winternals Defragmentation，Recovery，and AdministrationField Guide（Syngress，ISBN：1597490792）。
他是高级网络安全工程师并负责美国宇航局航空情报服务处信息安全组。
他负责美国俄勒冈州hillisbor0警察局警察储备专家部门。

<<僵尸网络>>

书籍目录

第1章　僵尸网络：呼吁行动 前言 网络程序杀手 问题有多大？
　僵尸网络的概念史　僵尸病毒的新闻案例　业界反响　小结　快速回顾　常见问题第2章　僵尸网络概述 什么是僵尸网络？
　僵尸网络的生命周期　漏洞利用　召集和保护僵尸网络客户端　等候命令并接受payload 僵尸网络究竟做什么？
　吸收新成员　DDoS　广告软件（Adware）和Clicks4Hire的安装　僵尸网络垃圾邮件和网络钓鱼连接存储和分配偷窃或非法（侵犯）知识产权的信息资料　勒索软件（Ransomware）　数据挖掘　汇报结果　销毁证据，放弃（僵尸）客户端 僵尸网络经济　垃圾邮件和网络钓鱼攻击　恶意广告插件和Clicks4Hire阴谋　Ransomware勒索软件　小结　快速回顾　常见问题第3章　僵尸网络C＆C的替换技术 简介：为什么会有C8LC的替换技术？
　追溯C&C的发展历史 DNS和C&C技术　域名技术　多宿（Multihoming）　可替换控制信道 基于Web的C＆C服务器　基于回声的僵尸网络　P2P僵尸网络　即时消息（IM）C&C　远程管理工具　降落区（drop zone）和基于FTP的C&C　基于DNS的高级僵尸网络　小结　快速回顾　常见问题第4章　僵尸网络　简介　SDBot　别名　感染途径　被感染的标志　注册表项　新生成的文件　病毒传播　RBot　别名　感染途径　被感染的标志　Agobot　别名　感染途径　被感染的标志　传播　Spybot　别名　感染途径……第5章　僵尸网络检测：工具和技术第6章　Ourmon：概述和安装　第7章　Ourmon：异常检测工具第8章　IRC和僵尸网络第9章　ourmon高级技术第10章　使用沙盒工具应对僵尸网络　第11章　情报资源　第12章　应对僵尸网络

<<僵尸网络>>

章节摘录

插图：整个2006年，科技安全大会都在讨论最新的“网络程序杀手”。
不幸的是，这种技术主要是为一些不法分子服务的。
新一代高智商而缺乏道德责任感的黑客们，在一些有组织的犯罪集团以及垃圾邮件制造商的资助下，创造了一种致命的摧毁性病毒——僵尸网络。
来自威廉玛丽学院的Norman Elton和Matt Keel在2005年“谁拥有你的网络?”的报告中称，僵尸网络是“人类面对的一个最大的威胁”。
这似乎有些夸张，但是说僵尸网络是网络社会所面临的最大威胁却是有据可依的。
John Canavan在名为“恶意IRC的进化”的白皮书中提到，僵尸网络是“最危险和最广为传播的Win32病毒威胁”。
2006年10月16日e-Week杂志封面称，我们“正在输掉”与僵尸网络的战争。
Ryan Naraine在“与僵尸网络的战争已经失败?”一文中介绍了僵尸网络环境现状：僵尸网络是“组织严谨的全球犯罪链中的关键核心。
它利用僵尸工具盗用带宽，并通过非法网络活动谋取利益”（更多信息参考www．eweek．corn／article2／0，1895，2029720，00．asp）。
而与之形成鲜明对比的是，相应的安全措施刚刚起步，少数安全软件厂商发行了与僵尸网络相关的产品（第一版）。
紧缺急需的情报信息被封锁起来，仅传递给需要它的安全专家，只有信息安全专家清楚地了解安全问题。
有安全专家宣称：“这（指僵尸网络）是不存在的”。
一位供货商告诉我们，他们产品的质量取决于他们情报资源的质量，然而接下来却说，他们不能给我们确保情报资源质量的任何信息。

<<僵尸网络>>

编辑推荐

《僵尸网络：网络程序杀手》：21世纪信息安全大系，科爱传播

版权说明