<<黑客新型攻击防范>>

图书基本信息

书名：<<黑客新型攻击防范>>

13位ISBN编号：9787115210074

10位ISBN编号：7115210071

出版时间：2009-8

出版时间：人民邮电出版社

作者：Markus Jakobsson,Zulfikar Ramzan

页数：393

字数：632000

译者：石华耀

前言

过去，人们认为恶意软件是一种纯粹的技术威胁，它主要依靠技术漏洞实现感染。
创作者开发它们往往是出于好奇心理，有时则是为了与其他恶意软件创作者比试高低。
本书提请读者注意：这种情况已经成为历史。
今天，攻击者利用社交背景，采用欺骗手段，甚至使用数据挖掘技术向目标受害者实施攻击。
他们的目标是获得经济利润或政治权力。
恶意软件已经变成犯罪软件（crbneware）。
也就是说，如今，恶意软件已经从地下室和大学寝室走出来，成为有组织犯罪集团、恐怖组织和侵略性政府手中的有力工具。
在发生这种转变的同时，我们的社会也在日益依赖因特网以保持其结构完整与稳定，这就引发了一个令人担忧的问题：将来会发生什么情况？
本书通过详细介绍犯罪软件及其运作方式和发展趋势，来尝试回答这个问题。
本书适用于各种背景的读者。
大部分章节首先使用简单易懂的语言概括介绍相关主题，读者不需要高深的技术知识即可理解这些内容。
然后，再深入分析更多细节，最终得出可能只有安全研究人员才会感兴趣的技术细节。
读者可以自己判定何时对某个主题已有了足够理解，而随时转入下一章。
如今，每个专业人员都面对很大的时间压力，所以我们在撰写本书时特意使每章内容相对独立。
读者不必按顺序从头至尾阅读每一章，完全可以精读感兴趣的任何章节，并可自由来回跳读。
本书每一章都由不同的作者撰写，他们各自以独特的视角表达了对于犯罪软件问题的见解.本书适合任何对犯罪软件、计算机安全以及因特网的未来感兴趣的读者。
它并非专门为技术人员撰写，对于法律与政策制订者、用户界面设计者，以及关心用户培训的公司也是适合的。
本书并不是一份系统安全指南，它旨在说明犯罪软件问题的实际情况及发展趋势。
虽然书中经常使用最新的攻击实例强调说明主题，但本书的重点仍在基本的趋势、原理和技术上。
当新一轮攻击来临——无疑，它们会利用新的技术漏洞和人们对网络的日益依赖，这些相同的原理仍然适用。
因此，我们希望，本书在今后几年这个不断变化的领域内，仍然能够为读者提供参考。
可以自豪地说，我们已经实现了这个看似有些矛盾的平衡，希望读者也同意这个观点。

<<黑客新型攻击防范>>

内容概要

本书详细介绍了犯罪软件的概念、运作方式及发展趋势。
书中每一章都由来自学术机构或高科技公司的作者撰写，大部分章节先以简单易懂的语言概括了相关主题，之后对细节进行深入分析，最终得出了安全研究人员感兴趣的技术结论。
本书以犯罪软件的基本原理和技术为中心，使用最新的攻击实例说明相关问题，对于针对新的技术漏洞和日益增强的网络依赖性开展的新型攻击，这些原理和技术仍然适用，可以为读者提供参考。
本书适用于对研究网络安全和对安全问题感兴趣的读者。

作者简介

Markus Jakobsson 博士，帕洛阿尔托研究中心首席科学家和印第安纳大学助手副教授，与人合作发表了100多篇论文，联合发明了50多个专利。

<<黑客新型攻击防范>>

书籍目录

章节摘录

插图：Web浏览器是非常复杂的应用程序，因此它们不可避免地包含许多安全漏洞。
犯罪软件常常利用这些漏洞进行传播。
如果用户访问一个恶意的Web站点，Web浏览器中的漏洞就可能被该站点上的代码利用。
这些漏洞可能与代码编写、解析、处理及显示内容有关，或者与任何其他能够令浏览器执行恶意代码的组件有关。
有时候，在浏览器供应商发现某个漏洞前，攻击者已经利用这个漏洞实施了攻击。
这种攻击叫做零天攻击（zeroday）。
并非所有对Web浏览器漏洞的利用都是通过恶意Web点来实施的。
通过跨站点脚本（cross－sitescripting）等内容注入攻击，合法的Web站点也可用于传播犯罪软件。
内容注入（contentinjection）是指在合法站点中插入恶意内容的过程。
除进行欺骗活动（如将用户重定向到其他站点）外，恶意内容还可以通过Web浏览器漏洞或社交工程骗局（如要求用户下载并安装实际上包含犯罪软件的虚假防病毒软件）在用户的计算机上安装犯罪软件。
有三类主要的内容注入攻击，每一类都有许多可能的变种。
攻击者可以通过安全漏洞攻破一台服务器，用恶意内容取代合法内容，或将恶意内容插入到合法内容之中。
犯罪软件可以通过跨站点脚本漏洞插入到站点中。
跨站点脚本漏洞是一种编程缺陷，即代码中包含来自外界的内容，如博客、用户在电子商站点查看的一款产品、拍卖、公告牌中的消息、搜索词，或基于Web的电子邮件。
这些外界提供的内容中可能包含一段恶意脚本，或其他站点服务器上安装的软件无法过滤或编码的内容。
随后，如果访问者通过Web浏览器访问该站点，这些内容就会运行。
用户可能认为这些内容是由站点的所有者创建的，因而很可能会信任它们。
利用SQL注入漏洞可对站点实施恶意行为。
利用这种方法可以在远程服务器上执行数据库命令.执行数据库命令可能会导致信息泄露、故意破坏，或注入恶意内容并随后将其传送给受害者。
与跨站点脚本漏洞一样，SQL注入漏洞也是由过滤不完全造成的。

媒体关注与评论

“迄今为止对网络安全威胁最全面的介绍！
它不仅讨论了当今的网络问题，而且还预测了未来几年可能出现的问题，这些都对深入理解目前的犯罪软件有非常重大的意义。
每个相关人士都应该拥有此书，随时可以参考。
”　　——Garth Bruen，KnujOn项目设计者　　“Jakobsson和Ramzan凭借此书为安全设置了一个新标准，内容实用且非常专业……不只是让你认清目前形势，还花了更多篇幅来谈论防御措施。
参编此书的研究人员多达50位，真希望我能向每位合著者表达我的感谢。
此书值得拥有，快去买吧！
”　　——Stephen Northcutt，GIAC（国际信息体系认证）的创立者　　“最近5年里，网络安全最引人关注的动向是恶意分子开始利用安全漏洞从事经济犯罪。
此书非常及时地揭露了犯罪分子目前用到的以及将来可能会用到各种犯罪软件工具。
”　　——Ross Anderson，技术作家、行业顾问、剑桥大学安全工程教授

<<黑客新型攻击防范>>

编辑推荐

《黑客新型攻击防范深入剖析犯罪软件》由人民邮电出版社出版。
有一类高科技罪犯分子使用软件窃取金钱及最高机密信息，他们使用的危险软件工具被称为“犯罪软件”。
随着大批公司和组织加入因特网，我们迫切需要理解和防范这些在线威胁。
Markus Jakobsson 和 Zulfikar Ramzan 领衔的众多安全领域专家凭借本书对犯罪软件做了全面的概述，不仅阐述了业界流行的观点，而且也涉及了目前为止只能在实验室看到的研究成果。
《黑客新型攻击防范深入剖析犯罪软件》将帮助安全技术人员、技术经理、学生和研究人员了解并识别各类犯罪软件，引导读者掌握基本安全原则、技术措施，从容地应对各类威胁。
不管攻击技术和战术如何变化多端，你总是能领先罪犯一步，成为不折不扣的网络安全高手。

版权说明