<<黑客大曝光>>

图书基本信息

书名：<<黑客大曝光>>

13位ISBN编号：9787111340348

10位ISBN编号：7111340345

出版时间：2011-6-10

出版时间：机械工业出版社华章公司

作者：Michael A.Davis,Sean M. Bodmer,Aaron LeMasters

页数：277

译者：姚军

前言

推荐序在我从事信息安全工作的将近15年中，恶意软件（malware）已经成为网络攻击者武器库中最有力的工具。
从窥探财务记录和窃取击键到对等（peer-to-peer）网络和自动更新功能，恶意软件几乎成为所有成功攻击的关键部件。
情况并非从来如此，我记得1998年刚开始从事信息安全工作时，我部署了自己的第一只蜜罐。
这使我能够看到攻击者进入并且接管真实的计算机，由此我学到了关于他们的工具和技术的第一手资料。
在那时候，攻击者通过人工扫描整个网络的各个部分来攻击，他们的目标是建立一个在互联网上能够访问到的IP地址列表。
在花费数天的时间建立这个数据库之后，攻击者将会回来，在他们找到的每台电脑上刺探常用的端口，查找已知的漏洞，例如脆弱的FTP服务器或者开放的Windows文件共享。
一旦发现这些漏洞，攻击者将利用该系统。
刺探和利用的整个过程可能花费几个小时到几周，在每个阶段需要不同的工具。
利用成功之后，攻击者将会上传更多的工具，每个工具都有各自的作用，并且通常人工运行。
例如，一个工具能够清除日志；另一个工具则保护系统；别的工具则检索密码或者扫描其他脆弱的系统。
你往往可以通过攻击者运行不同工具或者执行系统命令时犯错的数量来判断其水平。
观察和学习攻击者，并且识别其身份和动机是令人愉快和感兴趣的，这时候你的感觉就像和闯入你的电脑的人有了私人关系一样。
现在，网络防御的形势已经有了根本的变化。
过去，要攻击和危害一台计算机，每一步几乎都包含着人工交互。
现在，几乎所有的攻击都是高度自动化的，使用最先进的工具和技术。
过去，你可以看到威胁并从中学习，记录攻击者采取的每个步骤。
现在，整个过程都是有预谋的，发生在几秒钟之内，没有任何可观察和学习的东西。
从开始的刺探到泄密再到数据收集，攻击的每个步骤都预先封装到我们所看到的最先进的技术—恶意软件之中。
病毒刚刚问世时，只不过是修改系统上的几个文件以及窃取一些文档，或者试图破解系统密码的简单工具。
现在，恶意软件已经变得极其成熟，它们能够读取受害者的存储器，并且感染启动扇区、BIOS，此外还有基于内核的Rootkit。
更有趣的是，恶意软件利用僵尸网络（botnet）建立和维护对泄密系统的整个网络的控制能力。
这些僵尸网络是网络犯罪分子控制下的有高度组织性的网络。
网络犯罪分子使用这些网络来获取数据并且发送垃圾邮件，攻击其他网络或者部署仿冒站点。
现代的恶意软件使这些僵尸网络成为可能。
更糟糕的是，网络攻击者从全世界获得恶意软件，并且不断地创建和改进恶意软件。
在我写这篇序的时候，全世界正在从一个有史以来最高级的恶意软件Conficker的攻击中恢复。
数百万台电脑受到一群有组织的犯罪分子的侵害和控制。
这次攻击非常成功，以至于整个政府组织（包括美国国防部）都禁止移动媒体的使用，以减缓攻击的蔓延。
Conficker还引入了我们所见过的最高级的恶意软件功能，使用最新的加密技术来进行随机域名生成和自治点对点通信。
不幸的是，这一威胁越来越严重。
防病毒公司每天差不多要对付数千种新的恶意软件变种，这个数字还会不断增长。
我们所看到的恶意软件的最大改变不只是技术，还有这些技术背后的攻击者，以及他们开发恶意软件的动机。

我原来所监控的大部分攻击者都可以归类为脚本小孩，即一些没有熟练技能，只能使用从别处拷贝的工具的孩子。
他们为了娱乐或者给朋友们留下印象而进行攻击。
还有一小部分人开发和使用自己的工具，但是动机往往是好奇心，以及对自己的工具或者侵害系统能力的测试，或者是为了出名。
今天我们所面对的威胁与此大不相同，这些威胁正在变得更有组织，更有效率，也更致命。
今天，我们面对着有组织的犯罪分子，他们关注投资回报率（Return On Investment，ROI），拥有研究和开发团队，开发最有利可图的攻击。
和任何具有利益中心的企业一样，这些犯罪分子关注效率和经济性，试图在全球范围获得尽可能多的利益。
此外，这些犯罪分子已经发展了自己的恶意软件黑市。
和其他经济体一样，你能找到一个完整的黑市，犯罪分子在这个黑市中进行交易并且销售最新的恶意软件工具，恶意软件已经成为一种服务。
犯罪分子为客户开发定制的恶意软件或者将恶意软件作为服务进行租赁，服务包括支持、更新，甚至性能的约定。
例如，犯罪分子可以开发定制的恶意软件，并且保证避开大部分防病毒软件，或者设计软件来利用未知的漏洞。
一些国家机构也在开发最新的网络战工具。
这些机构具有几乎无限的预算，并且拥有世界上最先进的技能。
它们所开发的恶意软件用来悄悄地渗透和侵入其他国家，并且尽可能地收集情报，就像我们在最近的美国政府网络攻击案中所看到的那样。
使用恶意软件的国家级攻击还会扰乱其他国家的网络活动，例如，对一些国家的网络分布式拒绝服务攻击就是有组织并由恶意软件发起的。
恶意软件已经成为今天所见的几乎所有攻击的共有因素。
为了保护你的网络，你必须理解和防御恶意软件。
我很高兴看到Michael Davis牵头写作了这本关于Windows恶意软件的书籍：《黑客大曝光：恶意软件和Rootkit安全》。
我无法想到更适合这一任务的人。
从Mike加入Honeynet项目成为Windows的主要研究者开始，我认识他将近10年了。
Mike开发了我们最强有力的数据捕捉工具sebek，这是一个高级的Windows内核工具。
除此之外，Mike在McAfee公司的经历使他拥有了关于恶意软件和防病毒技术的丰富经验，他还有很多帮助提高世界各地客户安全的经验，并理解各种组织所面对的挑战。
他也亲眼目睹了恶意软件成为目前各种组织所面临的最大威胁的过程。
《黑客大曝光:恶意软件和Rootkit安全》为我们提供了令人惊叹的资源，它很及时，关注我们所面临的最大网络威胁和防御。
我强烈推荐阅读本书。
Lance Spitzner, Honeynet项目总裁

<<黑客大曝光>>

内容概要

抵御恶意软件和Rootkit不断掀起的攻击浪潮！
《黑客大曝光：恶意软件和Rootkit安全》用现实世界的案例研究和实例揭示了当前的黑客们是如何使用很容易得到的工具渗透和劫持系统的，逐步深入的对策提供了经过证明的预防技术。
本书介绍了检测和消除恶意嵌入代码、拦截弹出式窗口和网站、预防击键记录以及终止Rootkit的方法，详细地介绍了最新的入侵检测、防火墙、蜜罐、防病毒、防Rootkit以及防间谍软件技术。

《黑客大曝光：恶意软件和Rootkit安全》包括以下内容：
理解恶意软件感染、生存以及在整个企业中传染的方法。

了解黑客使用存档文件、加密程序以及打包程序混淆代码的方法。

实施有效的入侵检测和预防程序。

防御击键记录、重定向、点击欺诈以及身份盗窃威胁。

检测，杀死和删除虚拟模式、用户模式和内核模式Rootkit。

预防恶意网站、仿冒、客户端和嵌入式代码攻击。

使用最新的防病毒、弹出窗口拦截程序和防火墙软件保护主机。

使用HIPS和NIPS识别和终止恶意进程。

作者简介

Michael A. Davis是Savid
Technologies公司的CEO，该公司一家全国性的技术和安全性顾问公司。
他曾经在McAfee公司担任全球威胁高级经理。
他是Honeynet项目成员。

Sean M. Bodmer是Savid
Corporation公司的政府项目主管。
他是一位活跃的Honeynet研究人员，精于分析对恶意软件和攻击者的特征、模式和行为。
Sean是Honeynet项目和
Hacker Profiling项目的参与者。

Aaron
LeMasters是一位精通计算机取证、恶意软件分析和漏洞研究的安全性研究人员。
他在保护不设防的国防部网络上投入了5年的时间，现在他是Raytheon
SI的高级软件工程师。

<<黑客大曝光>>

书籍目录

章节摘录

在仿冒和垃圾邮件方面取得的新进展说明，攻击者的方法已经更趋向于心理学方面而非技术方面。
现在，通过电子邮件和IWeb，用户成为了目标，仿冒网站看上去如此可信，使得许多人没办法看出与真实网站的不同，从而交出自己的敏感信息，例如网上银行的用户名和密码。
根据McAfee的网站指南，在他们所做的间谍软件调查问卷（测试中询问受访人一个网站是否安全）中，12万名受访者中的95%错误地认为一个含有恶意软件的网站是安全的。
McAfee的调查问卷是用户所面对的问题的绝好实例，他们必须一眼就能看出某些网络内容是否会对自己的机器带来负面的影响。
考虑到安全意识的缺失，这个重要的决定类似于让一个4岁的孩子确定他的父亲是不是真的能从耳朵里拿出一个25美分的硬币。
一旦攻击者哄骗用户下载了恶意软件，就能够随意地访问网络空间的最新边界——你的工作站，获取机密信息、用户名和密码，还有类似社会保险号码或者银行账户信息等个人身份信息。
你最后一次从当地报纸中了解到严重的病毒爆发是什么时候？
两年前？
病毒已经成为过去。
从2004年Bagle和INetsky病毒爆发以来，蠕虫和病毒对个人用户和公司网络的威胁已经显著减少了。
但是，病毒爆发的停止不是因为病毒编写者决定洗手不干，而是因为他们的主要目标——公众注意力，已经不再让他们感兴趣了。
病毒编写者想要更多，比如金钱、敏感信息，以及对未授权系统的持续访问以利用这些系统资源，因此他们改变了方法、技术和工具，变得更加谨慎和针对特定目标，以适应新的动机，于是恶意软件和IRootkit的时代开始了。
恶意软件制作者的一些改变是由于安全界提升了安全军备竞赛的水平。
未经证明的Microsoft操作系统远程漏洞的减少和边界安全产品的广泛使用迫使攻击者提升自己的水平。
1.1 这种安全设施可能确实有用安全工具和产品一般被看作是降低生产率和浪费资源，或者没有真正的投资回报的东西，但是因为安全是“策略”所以必须实施。
许多安全产品本身没有提供价值，而且生产软件的公司的最新改进已经显著减少了漏洞的数量和类型。
攻击者利用核心操作系统部件缓冲区溢出来获得远程管理权限的时代一去不复返了。
现在的漏洞远比过去复杂，在代码中隐藏得很深，要找到它需要更多的技巧，而且发布的频率也比过去要低得多；发现这些漏洞需要攻击者花费更多的时间。

媒体关注与评论

“本书揭示了恶意软件可能的藏身之地，给出了寻找它们的方法”。
——Dan Kami rlsky，IOActive公司渗透测试负责人“本书为我们提供了令人惊叹的资源，它很及时地关注了我们所面临的最大网络威胁和防御。
”——Lance Spitzrler，HorleynetI页目总裁

编辑推荐

《黑客大曝光:恶意软件和Rootkit安全》是信息安全技术丛书之一。

版权说明