<<安全编程修炼之道>>

图书基本信息

书名：<<安全编程修炼之道>>

13位ISBN编号：9787302132165

10位ISBN编号：730213216X

出版时间：2006.08

出版时间：清华大学出版社

作者：James C. Foster

页数：629

字数：930000

译者：邓劲生

<<安全编程修炼之道>>

内容概要

从计算时代的早期开始到现在，安全行业经历了巨大的变化。
早期的病毒、蠕虫和恶意软件在当今看来，简直都成了小儿科。
随着行业的进一步发展，它又面临着一个转折点。
这种日益激烈的矛盾关系(就是这种矛盾关系导致了这个行业的诞生)将会影响到我们的社会、文化和市场吗？
　让我们来看一组数据。
如果研究一下1999年一个漏洞转化成蠕虫病毒所需的时间，再将这个数据与今天相比，就会发现现在出现一个自我繁殖的蠕虫要比1999年快20倍以上：在1999年需要280天，而在2004年仅需4天。
这些蠕虫很容易就被制造出来并且随时可能触发，而完成攻击几乎就不需要什么知识。
这就意味着有更多的黑客在更短的时间内编写出更多的攻击工具。
　我们第一次碰到这种新型的狡猾蠕虫，是在20世纪90年代后期出现的“ sadmind ”等蠕虫。
它从攻击Solaris操作系统本地的RPC服务开始，在完成感染之后，它就从Sun Solaris系统向Windows系统进军，再循环往复。
我们还看到了同时使用多个攻击方向的蠕虫，采用了针对不同服务的多种攻击技术。
还有一些可以自动变种的蠕虫，使得检测和防护它们更加困难。
大量的威胁在黑暗中等待，并且还不仅仅是蠕虫。
明天的蠕虫将会融合所有这些方面(多系统平台、多应用程序和多方向)产生zero-day蠕虫，却没有修复或防止措施。
　这些蠕虫将会造成怎样的破坏呢？
它会影响所有一切。
我们的大部分市场、基础设施和银行都已经计算机化，并且进行了联网。
想想看，如果长达一个月时间，不能够从银行或经纪人那里取出现金；或者不能够横穿铁路或马路，因为飞驰而来的列车或小车也和您一样看到绿灯，那会发生什么情况呢？
这些场景都是小说中编造的吗？
再仔细想想。
　以Banker.J worm为例吧。
这个蠕虫对系统的影响基本上和前面所说的蠕虫类似，但是另外有个重要的问题就是它首次采用了phishing技术。
所谓phishing攻击是指将用户误导到攻击者伪造的Web站点，以期窃取用户的银行用户名和密码的伎俩。
当进入这种伪造的站点之后，它自己再使用这个用户名和密码登录到银行，设置一个在线交易收款人，然后进行支付。
但是蠕虫并不直接将用户重定向到伪造的站点，而是显示受感染系统上的同样Web页面。
　他们到底是谁，他们又为什么要这么做呢？
他们大部分是些不谙世事的年轻人，受到自负心理和优越感的驱使。
另外有些是出于受金钱驱使或者有组织犯罪。
无论这些出发动机如何，或者伪造攻击的理由如何，管理员都必须提高自身素质，并解决问题出现的根源。
每个产品或步骤都存在有漏洞，在被管理并修复之前，攻击者总会去试图利用它们。
没有万全之策可以解决这个问题，也没有某个产品或服务或培训能够给出所有的工具来与这些威胁作斗争。
　正如战场上的战士一样，您需要掌握一切可以掌握的武器。
本书就是您的弹药，是为了保证安全战士们不至于折戟沙场的重要武器。
仔细研读本书的每一页，理解其内容，然后做到为我所用。
不要让这部出色的作品从您手中轻易滑过。

作者简介

James C.Foster是Computer Sciences公司是Global Security Solution Development的负责人，主要负责物理、人事和数据安全解决方案的研究和开发。
在进入Computer Sciences公司之前，Foster是Foundstone公司（后被McAfee收购）的研发部主任，负责产品、咨询和相应R & D建议等各

<<安全编程修炼之道>>

书籍目录

<<安全编程修炼之道>>

版权说明