《恶意代码分析实战》

图书基本信息

书名：《恶意代码分析实战》

13位ISBN编号：9787121224682

出版时间：2014-4

作者：Michael Sikorski,Andrew Honig

页数：732

译者：诸葛建伟,姜辉 张光凯

《恶意代码分析实战》

内容概要

本书是一本内容全面的恶意代码分析技术指南，其内容兼顾理论，重在实践，从不同方面为读者讲解恶意代码分析的实用技术方法。
本书分为21章，覆盖恶意代码行为、恶意代码静态分析方法、恶意代码动态分析方法、恶意代码对抗与反对抗方法等，并包含了shellcode 分析，C++恶意代码分析，以及64 位恶意代码分析方法的介绍。
本书多个章节后面都配有实验并配有实验的详细讲解与分析。通过每章的介绍及章后的实验，本书一步一个台阶地帮助初学者从零开始建立起恶意代码分析的基本技能。
本书获得业界的一致好评，IDA Pro 的作者Ilfak Guilfanov 这样评价本书：“ 一本恶意代码分析的实践入门指南，我把这本书推荐给所有希望解剖Windows 恶意代码的读者 ”。

《恶意代码分析实战》

作者简介

本书作者Michael Sikorski, Andrew Honig虽不是安全领域中名声很大的人物，但从背景来看都是工作在一线的安全工程师与培训讲师，相信本书应是一本从事计算机病毒、恶意代码分析的专业人士，以及计算机病毒领域爱好者案头必备的一本实践指南参考书。

《恶意代码分析实战》

书籍目录

《恶意代码分析实战》

精彩短评

1、内容广，适合上手入门。
2、这本书最大的亮点在于实战，每一章都有难度相当的上机实战问题，并指导你如何解决这些问题。
3、值得拥有。放在床头没事了翻翻挺不错，深度和广度都不错

《恶意代码分析实战》

精彩书评

1、随便在哪家网上书城进行搜索可以知道，在计算机安全类，特别是恶意代码分析领域的书籍可谓是凤毛麟角。如果哪位读者对于恶意代码分析有浓厚的兴趣，要么是去一些大型的安全类论坛看他人的分析报告，要么是在众多的安全类书籍中，东找一点西凑一点地进行学习。这也就说明了市面上确实少有专门针对于恶意代码分析的，以实战为主的书籍。而对于我这样的初学者而言，由于我希望成为一名反病毒工程师，因此我特别想能够阅读到在安全领域有着丰富经验的大牛的作品。而现实中的大牛往往很忙，大部分也不愿意将自己的经验记录下来。于是这就出现了学习的瓶颈，不知道如何学，也不知道在哪里能够系统地学。而由Michael Sikorski与Andrew Honig编写的《恶意代码分析实战》这本书，正好填补了这片空白。在本书封底的显著位置，有这样一句话：恶意代码分析人员必须人手一册的经典！推销的噱头见多了，这本书是否真的如此重要呢？在我认真读完后的答案是——确实如此！首先本书的两位作者自身就拥有极其丰富的恶意代码分析经验，而本书正是全面总结了二位作者在实际分析过程中所遇到的恶意程序的各种特性。他们将恶意程序的种种行为总结得非常全面，从某种意义上来说，本书就是一部反恶意程序的百科全书，这是现在市面上任何教程都无法比拟的。书中不单单告诉了读者恶意程序的实现原理，更能教会我们应当如何去应对。由于我在阅读本书之前，也看过不少安全类的教程与书籍，并且在恶意代码分析方面多多少少懂得一些，因此我就很难以“小白”的眼光来看待本书是否真的通俗易懂，只是以我目前的角度来说，其表述还是非常到位的，这就有助于我们快速入门。加上各章节之间并没有绝对的相关性，我们也完全可以挑选自己感兴趣的章节进行学习，而且如果以后遇到困难，也可以将本书作为辞典进行检索，毕竟目前我们能够见到的恶意程序的恶意行为，基本都包含在本书的范围之中了。阅读高手的思想，有助于我们更好地解决自身遇到的实际问题，从而提高我们自身的水平。当然，如果仅仅是“看”书的话，我个人认为，书中虽然涉猎广泛，但是深度略有不足，很多问题可以说就是一笔带过，这样一来，对自身实战水平的培养就略显不足。正所谓师父领进门修行在个人，幸好本书开创性地在每一章节的后面附上了一些练习，要注意，这些可不是普通的练习用的程序，而是实实在在的恶意程序，是需要在虚拟机中进行运行分析的。所以我也希望各位读者切勿眼高手低，一定要踏踏实实地认真分析每一个课后练习，完成后再看书后答案，相信大家会收获颇丰。毕竟在计算机安全领域，空谈理论是没用的，最重要的还是动手实现的过程。由于本书课后的习题只能在作者的网站进行下载，境外的网站我们访问起来可能没那么方便，所以我就将这些习题下载并上传到了我的CSDN资源区中，网址如下：http://download.csdn.net/detail/ioio_jy/8250331希望大家能够按照书中的方法，认真对待每一道题，做完之后再对照答案，从而真正将知识掌握在自己的手中。作为一本译著，尽管译者阵容强大，三位译者在安全领域也有着非常丰富的经验，但是书中的文字依旧摆脱不了绝大部分译著的通病，那就是过于追求原著的语言模式，从而使得很多语句非常生硬，很不符合我们中国人的语言习惯。要知道，英语语法和中文的语法在很多方面是截然不同的，如果硬要依照英文原著中的用词顺序进行翻译，势必会出现很多拗口的语句。而对于英文单词来说，如果我们查英汉辞典，其翻译可能只有几条，但是如果将这个单词运用于实际的句子，之后再翻译成中文，很多时候我们就会发现，如果严格依据辞典中的解释进行翻译，那么结果会很是奇怪。所以我觉得比较妥当的做法是，应当与时俱进，因地制宜地根据我们中文的特色与用词习惯进行翻译，对于某个单词的翻译，可能在辞典中并没有写明，甚至与原始解释多多少少还有些不同，但是放在中文里面却是合适的。我也翻译过书籍文章，因此我对此深有体会。其实我在翻译时，也难以跳出这个怪圈。我所见过的翻译得最为和谐的，是在《0day安全：软件漏洞分析技术（第2版）》中，作者对《Writing Small Shellcode》这篇文章的翻译。个人认为那位译者是彻底消化了那篇英文文章的精髓，并用自己的语言精确地转述出来了。我认为这就是翻译的最高境界，有兴趣的读者可以阅读一下。最后，对于本书，我是强力推荐的，也请大家支持正版书籍。

《恶意代码分析实战》

章节试读

1、《恶意代码分析实战》的笔记-第六章

这里可以结合另一本专门讲C语言代码的汇编结构的书一起看

2、《恶意代码分析实战》的笔记-第690页

700页的书竟然有将近300页是习题答案；翻译水平不太到位；夹带私货，介绍自己开发的产品；总体来看，差评。

《恶意代码分析实战》

版权说明