《恶意软件分析诀窍与工具箱》

图书基本信息

书名：《恶意软件分析诀窍与工具箱》

13位ISBN编号：9787302274407

10位ISBN编号：7302274401

出版时间：2012-1

出版社：清华大学出版社

作者：Michael Hale Ligh,Steven Adair,Blake Hartstein,Matthew Richard

页数：584

译者：胡乔林,钟读航

《恶意软件分析诀窍与工具箱》

内容概要

针对多种常见威胁的强大而循序渐进的解决方案
我们将《恶意软件分析诀窍与工具箱——对抗“流氓”软件的技术与利器》称为工具箱，是因为每个诀窍都给出了解决某个特定问题或研究某个给定威胁的原理和详细的步骤。在配书光盘中提供了补充资
源，您可以找到相关的支持文件和原始程序。您将学习如何使用这些工具分析恶意软件，有些工具是作者
自己开发的，另外数百个工具则是可以公开下载的。如果您的工作涉及紧急事件响应、计算机取证、系统
安全或者反病毒研究，那么本书将会为您提供极大的帮助。

- 学习如何在不暴露身份的前提下进行在线调查
- 使用蜜罐收集由僵尸和蠕虫分布的恶意软件
- 分析JavaScript、PDF文件以及Office文档中的可疑内容
- 使用虚拟或基础硬件建立一个低预算的恶意软件实验室
- 通用编码和加密算法的逆向工程
- 建立恶意软件分析的高级内存取证平台
- 研究主流的威胁，如Zeus、Silent Banker、CoreFlood、Conficker、Virut、Clampi、Bankpatch、BlackEnergy等

《恶意软件分析诀窍与工具箱》

作者简介

Michael Hale Ligh是Verisign iDefense公司的恶意代码分析专家，专门从事开发各种用于检测、解密以及调查恶意软件的工具。在过去数年里，他在里约热内卢、上海、吉隆坡、伦敦、华盛顿特区和纽约等地讲授恶意软件分析课程，已经培训了数百名学生。在进入Verisign iDefense公司之前，Michael在全国最大的医疗保健服务提供商之一中担任漏洞研究员，并提供黑客伦理服务。正是由于担任过该职务，他对逆向工程以及操作系统内部的背景有着深刻理解。在此之前，Michael为新英格兰地区的金融机构提供网络防御以及取证调查方面的服务。他目前是MNIN安全有限公司的特别项目主管。
Steven Adair是Shadowserver Foundation的研究员，同时也是eTouch联邦系统的首席架构师。在Shadowserver组织中，Steven主要分析恶意软件和跟踪僵尸网络，并重点调查与网络间谍组织相关联的各种网络攻击。Steven经常出席该领域相关专题的国际会议，并且合著了论文“ Shadows in the Cloud: Investigating Cyber Espionage 2.0 ”。在日常工作中，他在一个联邦机构中领导网络威胁行动小组以主动检测、降低以及预防网络入侵活动，他有效地集成了最佳安全实践和创新技术，成功地在全网中实现了企业级反恶意软件解决方案。Steven每天的工作都涉及恶意软件研究，无论是为公司客户提供支持或者在Shadowserver组织中贡献自己的业余时间。
Blake Hartstein是Verisign iDefense公司的快速响应工程师，主要负责分析以及报告恶意软件的可疑活动。他是Jsunpack工具的编写者，致力于自动分析以及检测基于Web的漏洞攻击，并分别在Shmoocon 2009和Shmoocon 2010会议中做了关于Jsunpack的报告。Blake同时还为Emerging Threats项目编写和贡献Snort规则。
Matthew Richard是雷神(Raytheon)公司的恶意代码操作部领导，主要负责分析以及报告恶意代码。Matthew之前是iDefense公司快速响应部门主管。在此7年之前，Matthew创建并运营了一家向130多家银行以及信用机构提供安全服务的公司。此外，他还对国内以及全球多家公司提供独立的网络取证咨询服务。Matthew现持有CISSP、GCIA、GCFA和GREM认证。

《恶意软件分析诀窍与工具箱》

书籍目录

目　录

章节摘录

版权页：插图：日常生活中，我们喜欢拥有某种程度的隐私。窗户上有窗帘，办公室有门，甚至计算机都有特制的屏保以防止窥视。对隐私的需求也延伸到Internet的使用上。我们不希望其他人知道我们在Google中输入的内容、即时通信对话的内容，以及访问的网站。但是，如果有人监视，那么他们往往可以看到您的私密信息。访问Intemet时有许多选择匿名方式的理由。而匿名并不意味着是您在做违法或错误的事情。调查恶意软件和追踪别有用心者时，进行匿名的理由非常直接。您不希望信息显示在日志或其他记录中，因为这可能暴露自己或自己所在公司的信息。例如，假设您在金融公司工作，最近检测到银行特洛伊木马感染了系统中的部分计算机。您收集恶意域名、IP地址和恶意软件相关的其他数据。在调查中，随后采取的步骤是找到罪犯拥有的网站。结果，如果未提前采取措施进行匿名访问，那么您的IP地址会被记录到各种日志中，还会被罪犯看到。

媒体关注与评论

“本书是我今年所阅读过的最有用的安全技术书籍，对于所有希望保护其系统免受恶意软件威胁的人员来说，这是一本必备书籍。” ——Lenny Zeltser,Savvis公司的安全业务主管和SANS机构的高级教师“每个恶意软件分析受好者的终极行动指南。” ——Ryan，Olson VeriSign iDefense公司快速响应部门的主管 “每一页都充满了实用的恶意软件知识、创新的理念、有用的工具，非常值得购买！” ——AAron Walters Terremark公司的Volatility和VP安全研究项目的领导者

《恶意软件分析诀窍与工具箱》

编辑推荐

《恶意软件分析诀窍与工具箱:对抗"流氓"软件的技术与利器》编辑推荐：“ 一本极好的恶意软件书籍 ”August14，2011By Ashraf Aziz “ Ash Aziz ”“ 我乐意向在计算机取证领域工作的任何人甚至是桌面支持人员推荐《恶意软件分析诀窍与工具箱:对抗"流氓"软件的技术与利器》，不要忘记使用配书光盘中的命令和示例，它们也很有帮助。 ”“ 恶意软件分析人员（包括反应人员和CERT）必备书籍 ”January1，2011By Aaed Salah Nemer “ 我已经阅读过很多有关恶意软件从概念到实验分析的安全书籍，但从来没有一本书籍像《恶意软件分析诀窍与工具箱:对抗"流氓"软件的技术与利器》这样给出了大量的技术细节。我进行的大量的安全活动，需要我具有最新的恶意软件的坚实背景，并提升我的事件响应技能和分析技术。 ”“ 一本优秀的书籍 ”December14，2010By ShaWn “ 这是我读过的有关恶意软件分析的最好、最容易的书籍。《恶意软件分析诀窍与工具箱:对抗"流氓"软件的技术与利器》包含了有用的代码、巧妙的方法以及其他实用的信息。这并不是一本随便拼凑编写几个工具的典型的大杂烩书籍。显而易见，作者在内容和组织上花费了大量心思。如果您也认真对待恶意软件分析，那么《恶意软件分析诀窍与工具箱:对抗"流氓"软件的技术与利器》值得您拥有。 ”

《恶意软件分析诀窍与工具箱》

精彩短评

1、内容全面丰富，极具实践性！
2、新的思路，想法，很详细！
3、恶意软件分析入门级的书
4、好书，做病毒分析，买来当参考书
5、对于恶意软件分析技术，有较强的实用性，在中国很少有看到这种实践针对性强的书了
6、有朋友说这本书写的比较浅。但对我来说，已经足够深了！深浅是相对的，但作为一个不想成为病毒专家的逆向票友来说。只有浅薄过，才能深
7、非常不错的恶意软件分析书籍
8、针对多种常见威胁的强大而循序渐进的解决方案
　　我们将《恶意软件分析诀窍与工具箱——对抗“流氓”软件的技术与利器》称为工具箱，是因为每个
诀窍都给出了解决某个特定问题或研究某个给定威胁的原理和详细的步骤。在配书光盘中提供了补充资
源，您可以找到相关的支持文件和原始程序。您将学习如何使用这些工具分析恶意软件，有些工具是作者
自己开发的，另外数百个工具则是可以公开下载的。如果您的工作涉及紧急事件响应、计算机取证、系统
安全或者反病毒研究，那么本书将会为您提供极大的帮助。
9、很多干货嘛
10、比较不错，实用性不强，但是很有意思。

《恶意软件分析诀窍与工具箱》

精彩书评

1、我看过了这本书，内容相当的全面，这本书确实有很多进行恶意软件分析的，平时想问而又不知道到哪里问的知识！尤其是后面的几个章节，详细的步骤和代码，绝对可以帮我们入门。翻译的质量也还是不错的。推荐网络安全的同学，尤其是分析恶意代码的，值得读一下

《恶意软件分析诀窍与工具箱》

版权说明