HZ BOOKS 华章IT
Mc Graw Hill Education

· 网络空间安全技术丛书 ·

HACKING EXPOSED
MALWARE & ROOTKITS
Security Secrets and Solutions, Second Edition

黑客大曝光

恶意软件和 Rootkit 安全

（原书第 2 版）

[美] 克里斯托弗 C. 埃里森 迈克尔·戴维斯 肖恩·伯德莫 阿伦·勒马斯特斯 著 姚军 译
（Christopher C. Elisan） （Michael Davis） （Sean Bodmer） （Aaron LeMasters）

武装自己，对抗日益升级的恶意软件和 Rootkit

机械工业出版社
China Machine Press

· 网络空间安全技术丛书 ·

黑客大曝光

恶意软件和 Rootkit 安全

（原书第 2 版）

HACKING EXPOSED
MALWARE & ROOTKITS

Security Secrets and Solutions, Second Edition

[美] 克里斯托弗 C. 埃里森 迈克尔 · 戴维斯 肖恩 · 伯德莫 阿伦 · 勒马斯特斯 著 姚军 译
（Christopher C. Elisan） （Michael Davis） （Sean Bodmer） （Aaron LeMasters）

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

黑客大曝光：恶意软件和 Rootkit 安全（原书第 2 版）/（美）克里斯托弗 C. 埃里森等著；姚军译 . —北京：机械工业出版社，2017.9
（网络空间安全技术丛书）
书名原文：Hacking Exposed Malware & Rootkits: Security Secrets and Solutions, Second Edition

ISBN 978-7-111-58054-6

I. 黑… II. ①克… ②姚… III. 计算机病毒 - 防治 IV. TP309.5

中国版本图书馆 CIP 数据核字（2017）第 229017 号

本书版权登记号：图字 01-2017-5490

黑客大曝光：恶意软件和 Rootkit 安全（原书第 2 版）

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码：100037）
责任编辑：陈佳媛　　责任校对：李秋荣
印　　刷：中国电影出版社印刷厂　　版　　次：2017 年 10 月第 1 版第 1 次印刷
开　　本：186mm × 240mm　1/16　　印　　张：18
书　　号：ISBN 978-7-111-58054-6　　定　　价：79.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzit@hzbook.com

对本书第 1 版的赞誉

“本书是《黑客曝光》系列的最新成员，它不是傻瓜书但易于理解，是该系列丛书成为畅销安全书籍的极好诠释。系统管理员和普通的计算机用户都可能需要面对成熟而隐秘的现代恶意软件，本书客观而清晰地揭示了这些威胁。”

——Brian Krebs，《华盛顿邮报》记者和《Security Fix》博客作者

“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 Kaminsky，IOActive 公司渗透测试负责人

“作者用常见的术语和相关的实例说明了恶意软件这一计算机安全中深奥而具有多样性的问题。恶意软件是一种极端危险的黑客工具。作者坦率地描述恶意软件，以简单明了的技术洞察力说明其能力。本书内容很容易理解，即使博学的读者也能从中受益。”

——Christopher Jordan，McAfee Threat Intelligence 副总裁，DHS Botnet Research 主任

“记得期末复习的时候吗？指导老师重温整个学期所学到的所有重要问题，使你能够理解所有关键点，而又为你自己的钻研留下足够的参考。本书采用了和老师类似的做法！本书对新手和安全专家来说都是优秀的参考书，它不仅对所介绍的主题进行了详细解释，而且不会因为提供过多的信息而使安全新手畏缩不前。”

——Ron Dodge，美军中校

“本书提供了对恶意软件和 Rootkit 背景技术的独特视角，如果你负责计算机的安全，马上阅读本书吧！”

——Matt Conover，Symantec Research Labs 高级主任软件工程师

推 荐 序

在今天的互联网上，恶意软件的出现似乎永无止境，其复杂度每分钟都在增加。威胁研究社区和安全行业在先进恶意软件防御的苛刻要求下苦苦挣扎，这是因为这一特殊专业上的人才十分短缺。多年以来，我们见证了防病毒解决方案一直很保守，直到不久前，我们才发现了一些转变，真正重视先发制人地对抗威胁。解决这个问题的尝试之一是承认可伸缩知识转移是至关重要的，这也是本书的由来……

几年来，我有幸和 Christopher Elisan 在一个威胁研究团队中共事，多年来我们一直保持着联系。他对网络威胁来源开发的开创性武器有着渊博的知识，在此基础上表现出了超强的逆向工程和恶意软件分析才能。从第 1 章起，本书直奔主题，然后以快速、稳定的节奏，引领读者阅读精心编写的教程。Christopher 以尊重、信任读者聪明才智和能力的方式，表达了他对于这一主题的信心。对于本书第 2 版的出版，我倍感激动，因为这本书的内容成功地融合了大量深入的主题，同时介绍了多种深思熟虑的扩展应用，帮助读者建立针对某些最先进的技术威胁的主动对策。

不管你是刚刚开始着手恶意软件的研究，还是这一领域的老兵，在读完本书之后都会感到满意，因为你可以得到独特而切题的深刻见解，这将大大提高你在这一领域的成就。

我要真诚、自豪地对读者们说，好好享受本书带来的一切吧！

Lance James

Flashpoint 首席科学家

译 者 序

《黑客曝光：恶意软件和 Rootkit 安全》第 1 版出版已经 6 年，在此期间，安全业界和黑客社区之间的“军备竞赛”仍在激烈地进行，如何做好准备，去迎接各种安全威胁的挑战呢？广大读者都期盼着本书的全面更新。

操作系统和安全软件的全面升级确实在一定程度上缓解了传统恶意软件的威胁，Windows 10 的推出使微软操作系统逐渐摆脱了“最不安全系统”的恶名，反观对手，恶意软件和 Rootkit 似乎没有太多的新概念，我们可以高枕无忧了吗？

确实，恶意软件和 Rootkit 这些年来在形式上并没有太多的变化，但是在任何领域都是“道高一尺，魔高一丈”，第 1 版中介绍的各种恶意软件仍然可以“旧瓶装新酒”，演变出新的威胁，因此，本书的新版本不仅保留了第 1 版中丰富的信息，而且介绍了许多安全业界和黑客社区的新发展，帮助读者温故知新，更好地对抗网络中不知名的对手。

很高兴有机会再次翻译本书，希望新的版本能够为奋战在网络安全战线上的读者们带来更多的益处，也希望广大读者多提宝贵意见，在此感谢华章公司的吴怡编辑为翻译工作提供的帮助。

译者

2017 年 6 月

作者简介

Christopher C. Elisan

Christopher C. Elisan 是安全行业的老兵，20 世纪 90 年代从学校毕业时就投身于这一职业。他是经验丰富的逆向工程和恶意软件研究人员。从 DOS 时代到现在，他见证了日益复杂精密的恶意软件开发。他目前是 EMS 安全分布——RSA 的首席恶意软件科学家和恶意软件情报团队高级经理。

Elisan 是 Trend Micro 的 TrendLabs 实验室的先驱之一，在那里他以恶意软件逆向工程人员的身份开始了职业生涯。在 TrendLabs，他曾经担任过多个技术和管理职位。离开 Trend Micro 之后，Elisan 加入 F-Secure，建立了 F-Secure 的亚洲研发中心，并担任多个项目的领军人物，包括漏洞发现、Web 安全和移动安全。之后他加入了 Damballa 公司，担任高级威胁分析师，专门负责恶意软件研究。Elisan 拥有计算机工程学士学位，并通过了如下行业认证：认证道德黑客、微软认证系统工程师、微软认证系统管理员、微软认证专家和认证敏捷专家。

Elisan 是世界级的恶意软件、数字欺诈和网络犯罪主题专家之一。他用自己的专业知识帮助了不同的执法机构，并为领先的行业和主流出版物提供关于恶意软件、僵尸网络和高级持续性威胁的专业意见，包括《今日美国》《旧金山纪事报》《SC 杂志》《信息周刊》《福克斯商业》和《Dark reading》。他还经常在全球的安全会议上发表演讲，包括 RSA 大会、SecTor、HackerHalted、TkaeDownCon、Toorcon、$(ISC)^2$ 安全会议、Rootcon 和 B-Sides。他还是《Malware，Rootkits &Botnets：A Beginner's Guide》（McGraw-Hill 于 2012 年出版）一书的作者。

在不解剖或者讨论恶意软件时，Christopher 将时间花在和孩子们打篮球和游戏上。他和家人还喜欢观看亚特兰大老鹰队击败对手的比赛。如果时间允许，他会在亚特兰大当地的摇滚乐队担任歌手 / 吉他手，继续自己的摇滚明星梦。

你可以通过推荐 @Tophs 关注他。

Michael Davis

Michael Davis 是 Savid Technologies 公司的 CEO，该公司是一家全国性的技术和安全咨

询公司。由于 Michael 将 snort、ngrep、dsniff 和 honeyd 这样的安全工具移植到 Windows 平台，因此他在开源软件安全界声名卓著。作为 Honeynet 项目[⊖]成员，他为基于 Windows 的 honeynet（蜜罐）开发了数据和网络控制机制。Michael 还是 sebek for Windows 的开发者，这是一种基于内核的 honeynet 数据收集和监控工具。Michael 曾经在领先的防病毒保护和漏洞管理企业——McAfee 公司担任全球威胁高级经理，领导一个研究机密审查和尖端安全的团队。在 McAfee 工作之前，Michael 曾在 Foundstone 工作过。

Sean Bodmer，CISSP，CEH

Sean Bodmer 是 Savid Corporation 公司的政府项目主管。Sean 是一位活跃的 honeynet 研究人员，精于分析恶意软件和攻击者的特征、模式和行为。最为引人注目的是，他花费了多年的时间来领导高级入侵检测系统（honeynet）的运作和分析，这一系统能够捕捉和分析入侵者及其工具的动机和目的，从而生成对进一步保护用户网络有价值的信息。在过去的 10 年中，Sean 已经为华盛顿特区的多个联邦政府机构和私人公司负责过各种系统安全工程。Sean 在全美国的业界会议，如 DEFCON、PhreakNIC、DC3、NW3C、Carnegie Mellon CERT 和 Pentagon 安全论坛上发表过演讲，主题包括对攻击特征和攻击者的剖析，这些剖析能够帮助识别网络攻击的真正动机和意图。

Aaron LeMasters，CISSP，GCIH，CSTP

Aaron LeMasters（乔治·华盛顿大学理科硕士）是一位精通计算机取证、恶意软件分析和漏洞研究的安全研究人员。他在职业生涯的头 5 年用在保护不设防的国防部网络上，现在他是 Raytheon SI 的高级软件工程师。Aaron 乐于在大的安全会议（如 Black Hat）和较小的区域黑客会议（如 Outerzone）上分享研究成果。他更愿意关注与 Windows 内部构件、系统完整性、逆向工程和恶意软件分析相关的高级研究和开发问题。他是一位热心的原型构造者，很喜欢开发增强其研究趣味性的工具。在业余时间，Aaron 喜欢打篮球、画素描、摆弄他的 Epiphone Les Paul 电吉他，以及和妻子一起去纽约旅行。

贡献者 Jason Lord

Jason Lord 目前是 d3 Services 的 COO，该公司是提供网络安全解决方案的顾问公司。Jason 在过去 14 年中都活跃于信息安全领域，主要关注计算机取证、事故响应、企业安全、

⊖ Honeynet 是一种学习工具，是一个包含安全缺陷的网络系统。当它受到安全威胁时，入侵信息就会被捕获并接受分析，这样就可以了解黑客的一些情况。——译者注

渗透测试和恶意代码分析。在这段时间里，Jason 应对过全球数百个计算机取证和事故响应案例。他还是高技术犯罪调查学会（HTCIA）、InfraGard 和国际系统安全学会（ISSA）的活跃成员。

技术编辑 Jong Purisima

Jong Purisima 从 1995 年第一次分析恶意软件起就从事威胁和恶意软件研究工作。从职业上说，他是从加入 Trend Micro 的病毒医生团队开始与计算机行业的亲密接触的，在该团队中，他分析恶意软件以生成检测、补救措施和面向客户的恶意软件报告。从那时起，他主要从事安全实验室的运营工作，特别是技术产品管理，为 Trend Micro、Webroot、GFI-Sunbelt、Cisco 和 Malwarebytes 等公司提供以威胁为中心的安全解决方案。

闲暇之余，Jong 忙于业余手工制作和木匠活，喜欢徒步和自驾游，与家人在“欢迎来到……”的标语下合影。

前　言

感谢你选择本书的第 2 版。从本书第 1 版出版以来，安全领域发生了许多变化，本版将反映这些变化和更新，但是会保留第 1 版中信息的历史相关性为代价。在第 1 版的基础上，我们介绍攻击者所使用技术的改进和变化，以及安全研究人员如何改变，以对抗如今新型恶意软件技术和方法论。

遵循第 1 版的精神，我们将焦点放在对抗恶意软件威胁中有效和无效的防护手段。正如第 1 版中所强调的，不管你是家庭用户还是全球百强企业安全团队的一员，对恶意软件保持警惕都会给你带来回报——从个人和职业上都是如此。

导航

本书中，每种攻击技术都用如下的方法突出显示：

这是攻击图标

这个图标表示某种恶意软件类型和方法，便于识别。书中对每种攻击都提出了实用、恰当并且实际测试过的解决方案。

这是对策图标

在这里介绍修复问题和将攻击者拒之门外的方法。

- 特别注意代码列表中加粗显示的用户输入。
- 每种攻击都带有一个更新过的危险等级，这个等级的确定是根据作者的经验以下 3 部分因素得出的：

流行性	对活动目标使用该攻击方法的频率，1 表示使用最少，10 表示使用最广泛
简单性	执行该攻击所需要的技能，1 表示需要熟练的安全编程人员，10 表示只要很少甚至不需要技能
影响	成功执行该种攻击可能产生的危害，1 表示泄露目标的普通信息，10 表示入侵超级用户账户或者等价的情况
危险等级	上面三个值平均后给出的总体危险等级

致　谢

我要感谢 Wendy Rinaldi 和 Meghan Manfre 的信任，没有他们的耐心和支持，本书就不可能成为今天的样子。说到耐心，我要真诚地感谢 LeeAnn Pickrell 出色的编辑工作，以及对我总在变化和难以预测的工作和差旅安排的耐心和宽容。

非常感谢 Lance James 在百忙之中抽出时间为本书作序，感谢 Jong Purisima 使本书的技术内容保持在业界前沿。

特别要感谢我的合著者们。正是你们的专业知识、时间和天赋使本书成为安全行业的重要资产。

——Christopher C. Elisan

目　录

第二部分 Rootkit

第三部分 预防技术

第一部分
恶意软件

案例研究：请在季度会议之前进行审核

让我们来观察一个组织成为攻击目标的场景。周二下午3点20分，一家中型制造企业的管理层的十位主管收到一封伪造得很逼真的电子邮件，这封邮件似乎来自公司的CEO，标题为“请在我们的会议之前进行审核”，并且要求收信人保存邮件附件并且将文件扩展名从.zip改为.exe，然后运行该程序。这个程序是用于周五的季度会议的插件，对于查看会议中播放的视频来说是必需的。CEO在邮件中提到，因为邮件服务器的安全要求不允许他发送可执行文件，所以主管们必须更改该附件名。

主管们按照得到的指令运行该程序。那些存有疑问的人看到他们的同事都收到相同的邮件，于是觉得这封邮件肯定是合法的。而且，因为这封邮件在这天较晚的时候发送，有些人直到下午5点之前才收到，他们没有时间去证实CEO是否发送了这封邮件。

邮件的附件确实是一个在每台机器上安装击键记录程序的恶意软件。谁会创建这个程序？他们的动机是什么？让我们来认识这位攻击者。

我们遇到的攻击者Bob Fraudster是本地一家小公司的编程人员。他主要使用基于Web的技术（如ASP.NET）进行编程，并制作动态网页和Web应用程序来支持该公司的市场活动。因为经济衰退，Bob刚刚遭到降薪，所以他决定获取一些额外的收入。Bob访问Google.com搜索bot程序和僵尸网络（botnet），因为他听说这些工具能给运作者带来许多金钱，认为这可能是赚取额外收入的一个好的途径。在这一个月中，他加入了聊天室，听取其他人的意见，并且了解到在许多在线论坛上可以订购到bot软件，这些程序能够实现单击欺诈（click fraud）并且为他带来一些收入。通过研究，Bob知道大部分防病毒软件能够发现预编译的bot程序，因此他决定获取一份源代码来编译自己的bot。Bob专门订购了一个通过HTTP上的SSL与他租赁的主机通信的bot程序，从而减少了bot出站通信被安全软件拦截的概率。因为Bot使用HTTP上的SSL，bot的所有通信流量将被加密并且能够通过大部分内容过滤技术。Bob在各种搜索引擎上注册了广告经营者（Ad Syndicator），作为广告经营者，他将在自己的网站上显示来自搜索引擎的广告轮换程序（如AdSense）的广告，对于他在网站上的每次广告单击，他可以得到一点小小的收入（几分钱）。

Bob使用一些与bot一同订购的利用程序（exploits），加上一些订购的应用程序级漏洞

来入侵全世界的Web服务器。使用标准的Web开发工具，他修改了网站上的HTML或者PHP页面，载入他的广告经营用户名和密码，这样他的广告就代替了网站自己的广告。实际上，Bob强迫他所破解的网站加入广告经营，这样当用户单击这些广告时，就将把钱送给他，而不是实际的网站经营者。这种通过用户单击网站广告赚钱的方法被称为按单击付费广告（pay-per-click，PPC），是Google所有收入的来源。

接下来，Bob使用armadillo packer软件打包恶意软件，使它看上去像来自于公司CEO的一个新PowerPoint幻灯片文件。他编写一封具体的定制电子邮件，让主管们相信附件是合法的并且来自于CEO。

现在主管们必须打开这个文件。Bob大约每过30分钟就向他购买的多个小公司的电子邮件地址发送这个幻灯片的拷贝，这个拷贝实际上安装了他所制作的bot程序。因为Bob曾经做过市场工作，并且实施过一些电子邮件活动，所以知道能够从互联网上的一个公司那里很容易地购买电子邮件地址列表。互联网上可供购买的电子邮件地址多得令人惊讶，Bob将精力集中于较小的公司而不是集团公司的邮件地址，因为他知道许多企业在电子邮件网关上使用防病毒软件，他不想让防病毒软件供应商注意到他的bot。

Bob获得电子邮件地址的另一种方法是访问小型企业的网页，提取或者猜测主管们的电子邮件地址，这些地址通常可以在网站的“关于我们”或者“企业领导”部分找到。

Bob很聪明，知道许多通过IRC通信的bot程序更容易被发现，所以他购买了一个通过HTTP上的SSL与私人租赁主机通信的bot。使用定制的GET请求，这个bot程序通过向他的Web服务器发送命令和带有具体数据的控制消息来进行交互。由于Bob的bot程序通过HTTP进行通信，所以不用担心所感染的机器上运行的防火墙阻挡bot访问他所租赁的Web服务器，因为大部分防火墙都允许端口443上的出站通信。而且，他也不用担心Web内容过滤，因为传输的数据看上去是无害的。另外，当他打算窃取查看受害者公司集团的PowerPoint幻灯片的财务数据时，只需要将数据加密，这样Web过滤程序就无法看到这些数据。他没有使用大量繁殖的蠕虫来发布他的bot，因此受害者的防病毒软件没有发现这个bot的安装，因为防病毒软件没有这个bot的特征码。

这个bot程序一旦安装，就作为一个浏览器助手对象（Browser Helper Object，BHO）代替Internet Explorer，这使bot程序能访问该公司的所有常规HTTP通信和Internet Explorer的所有功能，例如HTML解析、窗口标题以及访问网页的密码字段。这是Bob的bot程序嗅探发送到公司的信用卡联盟和各种网上银行数据的方法。这个bot开始连接Bob的bot主服务器，并且从服务器上读取已入侵网站的列表，连接到这些网站开始单击广告。

bot程序接收到访问连接列表之后，就会保存这个列表并且等待受害者正常使用Internet Explorer。当受害者浏览CNN.com了解最新的世界时事时，bot程序访问列表中的网站寻找可单击的广告。这个bot了解广告网络的工作方式，所以它使用受害者实际查看的网站（例如CNN.com）的引用，使广告的单击看上去像是合法的。这种方法骗过了广告公司的防欺诈软件。bot单击广告并且查看了广告的登录页面之后，就转向列表中的下一个链