HZ BOOKS
华章科技
Mc Graw Hill

Hacking Exposed

Malware & Rootkits Secrets & Solutions

黑客大曝光

恶意软件和Rootkit安全

Michael A. Davis
(美) Sean M. Bodmer 著
Aaron LeMasters

姚军 等译

机械工业出版社
China Machine Press

信息安全技术丛书

Hacking Exposed

Malware & Rootkits Secrets & Solutions

黑客大曝光

恶意软件和Rootkit安全

Michael A. Davis
(美) Sean M. Bodmer 著
Aaron LeMasters

姚军 等译

机械工业出版社
China Machine Press

互联网的兴起，使黑客的危害越来越引起人们的重视，尤其是许多关键的应用都依赖网络实施的今天，网络安全成为广受关注的领域。本书通过详尽的案例分析，各种安全威胁的介绍和防范方法，特别是针对现行防御体系的深入剖析，令读者注意到在日常工作中难以发现的盲点。本书深入介绍了现有系统的弱点和所需要防御的层面，揭示了恶意软件可能的藏身之地，给出了寻找它们的方法。

本书面向各行各业、政府机关、大专院校关注信息安全的从业人员，是信息系统安全专业人士的权威指南，也可作为信息安全相关专业的重要参考书。

Michael A. Davis, Sean M. Bodmer and Aaron LeMasters ：Hacking Exposed: Malware & Rootkits Secrets & Solutions（ISBN 978-0-07-159118-8）.

本书版权登记号：图字：01-2011-1508

图书在版编目（CIP）数据

黑客大曝光：恶意软件和Rootkit安全 /（美）戴维斯（Davis, M. A.）等著；姚军等译. —北京：机械工业出版社，2011.6

（信息安全技术丛书）

书名原文：Hacking Exposed: Malware & Rootkits Secrets & Solutions

ISBN 978-7-111-34034-8

Ⅰ.黑…　Ⅱ.① 戴…　② 姚…　Ⅲ.计算机网络-安全技术　Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2011）第058398号

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：秦　健

北京京北印刷有限公司印刷

2011年6月第1版第1次印刷

186mm × 240mm　·　18.25印张

标准书号：ISBN 978-7-111-34034-8

定价：55.00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）88378991；88361066

购书热线：（010）68326294；88379649；68995259

投稿热线：（010）88379604

读者信箱：hzjsj@hzbook.com

对本书的赞誉

“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

译 者 序

记得在20世纪90年代初刚刚接触计算机安全领域的时候，病毒的声浪甚嚣尘上，“黑客”对于我们来说还是个神秘的名词，从事计算机工作的年轻人既担心病毒对自己管理的系统进行侵袭，内心中又有一种渴望，希望可以深入地了解病毒和黑客的工作方式。

在看过一篇又一篇对病毒和黑客工作原理的剖析文章之后，各种防病毒工具铺天盖地而来，随着这些工具的日益成熟，病毒似乎不再是我们眼中的可怕角色。互联网的兴起，使我们对黑客的危害重新重视起来，尤其是在许多关键的应用都在网上实施的今天，但是很快又兴起了新的工具，尽管这期间有多次令世人瞩目的蠕虫/木马爆发事件，但是安全界成功的广告攻势，以及许多新的概念，包括入侵检测/入侵预防系统/安全网关等，又让我们重新觉得万事大吉。

我们拿到本书的英文版，还正是陶醉于天下太平的时候，尽管经常收到安全通告，但是在同行间的谈论中，更多的还是认为这些事故不过是安全人员的疏忽造成的，只要我们IT部门还在起作用，就不会有那么严重的事件发生。看完了本书的第一部分，与我们有同样想法的IT人员一定会有如芒刺在背，作者以丰富的经验和实例的剖析，让我们身临其境地看到了现有系统的弱点和所需要防御的层面之广，相信每个人在这个时候都不敢再对安全的态势有过多的乐观。

深入地阅读本书，越来越多引人入胜的内容呈现在我们的面前，详尽的案例分析、各种安全威胁的介绍和防范方法，特别是针对现行防御体系的深入剖析，都令我们获益匪浅，有些防范的方法简单易行，却是安全人员在日常工作中难以注意到的盲点。

完成了本书的翻译工作，我们长长地出了一口气。本书给了我们先于读者一步得到良好的安全知识培训的机会，同时我们也深切希望能够把原作的精彩部分完整地呈现给读者。

本书的翻译工作主要由姚军完成，徐锋、陈绍继、郑端、吴兰陟、施游、林起浪等人也为本书的翻译工作做出了贡献。由于译者时间和水平有限，翻译过程中可能存在不当之处，敬请广大读者朋友批评指正。

译者

2011年1月

序　言

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

⊖　蜜罐（honeypot）是指用来诱使黑客攻击，以达到跟踪其行为的主机。——译者注

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。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。

本书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

前　言

内部威胁不再来自于“内部”

现在的每一次安全会议和研究都关注让企业安全管理员和家庭用户理解来自内部的威胁。内部威胁正在增长并且变得更加具有恶意性。内部攻击最大的3个类别是：窃取经济利益、IT蓄意破坏以及商业利益。安全专家认为用户是问题的起因，用户就是威胁。在技术上这么说是正确的，但是对于一个组织而言，实际的用户本身并不总是真正的威胁，真正的威胁是用户所拥有的角色或者访问权限。如果一位秘书具有的权限足以查看网络文件共享上的财务目录，那么感染她的机器的恶意软件也有同样的权限。

当今的恶意软件通过避开外部防护、在机器上执行程序，以及在内部用户账户中运行等手段，接管或者模拟内部角色，使恶意软件能够进行攻击、控制，并且和内部人员一样访问资源。所以在本书中，我们关注当今世界上的恶意软件的功能和所适用的技术。恶意软件是内部人员以及想要保持对这一内部角色控制权的攻击者。现在，我们关注对恶意软件威胁有效及无效的防护，最终也是对内部威胁防护的关注。不管你是家庭用户还是全球百强企业的安全团队成员，都必须要警惕。从个人和专业出发，对恶意软件保持警惕都会给你带来回报。别让你的机器成为恶意软件大军用于“借尸还魂”的又一个工具。

导航

本书中，每种攻击技术都用如下的方法突出显示：

这是一个攻击图标

这个图标使得特定的恶意软件类型和方法易于识别。对每种攻击都提出了实用、合适并且实际测试过的解决方案，每种方案都有自己特殊的图标。

这是对策图标

了解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得出的3部分因素：

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	前述的三个值平均后给出的总体危险等级

关于网站

因为恶意软件和Rootkit不断发布，你可以在本书的网站（http://www. malware hackingexposed.com）上找到最新的工具和技术。该网站包含了本书中提到的代码片段和工具，以及附录中讨论的一些从未发布的工具。我们将保留书中提到的所有工具的一份拷贝，你甚至可以在维护者停止编写这些工具之后下载。

致谢

感谢编辑Jane，她尽其所能地使本书顺利出版，尽管很多时候这看上去几乎不可能。还要感谢Savid Technologies的杰出团队，他们让我能抽出时间进行写作。

——Michael A. Davis

首先，感谢编辑Jane，她给了我们很多积极的反馈和建设性的批评。这是我出版的第一本书，没有她，很多时候我都不知道该怎么办。还要感谢我的年轻朋友Tj Egan，当我的写作遇到困难而需要减轻压力时，他在Forgotten Coast 游戏服务器（GO ALLIANCE）上帮助我杀怪兽[⊖]。我也要感谢Zac Culbertson和Cowboy Café给了我一个在写书时能进行思考的地方。没有比弗吉尼亚州的Arlington更好的地方了，在那里可以在逃离华盛顿的混乱时吃、喝并且思考。

——Sean Bodmer

我希望表达对技术编辑Alex Eisen的感谢和赞赏，没有他，我就没有机会写这篇致谢。感谢Alex（直到下次合作）。我还要感谢编辑和合著者给了我这个机会，并且和我一起分担这段痛苦的创作历程。在我的母校密西西比州立大学，没有Ray Vaughn博士和其他卓越的教授的指导，也就没有我今天的成就。如果我没有提到社区中的安全研究者们在过去、现在和未来创造的价值，那是我的失职，他们充满激情的工作造就了这个行业，并且继续对网络安全边界做出新的定义。

——Aaron LeMasters

⊖ 这里指的是《魔兽世界》游戏。——译者注

作者简介

Michael A. Davis

Michael A. 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 M. Bodmer，CISSP，CEH

Sean M. 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。

⊖ 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

技术编辑简介

Alexander Eisen是FormalTechnologies.com的CEO，高级科技大学（University of Advancing Technology）的副教授，还是一位公务员——国防部的企业架构师。他始终是一位打破传统的实验者，从1999年开始，他在渗透测试、企业事故响应、取证、RE和安全软件评估领域承担了所有的任务——攻击和防守、战术和战略，并获得了由美国国家安全局（NSA）主办的为计算机科学、密码学和法律等多学科研究颁发的“Information Assurance Fellowship”奖，这是对他的工作的肯定。他曾经为美国国防部和所属的组织领导过十几个主要的红队[⊖]和从事事故响应工作，媒体广泛报道了其中的许多次经历，例如“五角大楼1500台电脑遭到黑客攻击”。作为美国国家网络安全计划的核心成员，他曾经研究大规模企业事故响应和软件保障方法。由于他拥有国防语言学院、抵御网络犯罪中心培训学院、国际信息系统安全核准联盟（(ISC) 2）以及国家安全系统委员会的认证，所以是InfraGard、AFCEA、IEEE以及各种联邦顾问委员会的积极成员。他曾经在许多国际业界会议（如Black Hat Japan和乌克兰IT节以及五角大楼这样的内部会议）上发表关于新出现的安全问题的演讲，并曾经在商业杂志上发表过关于国家基础设施保护和IPv6的文章。通过执教信息安全课程并且支持高级科技大学的NSA优秀学术中心，他已经转向利用学术界的才能和资源研究开创性的社会经济学技术主题。他热心于通过服务奖学金计划（Scholarship for Service programs）招募有追求的年轻人，并且帮助他们开始职业生涯。

⊖ 红队是政府用于对自己的系统进行攻击测试的专家组。——译者注

目　录

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

根据Symantec和GFI 2009年4月发表的最新安全研究，定制和针对性的垃圾邮件和恶意软件攻击数量再次上升。而且，由于恶意软件业界的专业化，这种代码定制已经使安全界的防护和检测率有了明显的下降。Symantec在2008年中检测出近166万种恶意代码威胁，和2007年相比有明显的上升。新的恶意代码特征码同期增长了265%。随着恶意软件制作者持续地开发代码并且确保这些代码在新的环境中工作正常，他们将会不断地调整这些恶意软件以得到最佳的投资回报（ROI）。特洛伊木马占了前50种恶意代码的将近70%，这是因为它们对于日后保持对受害机器的远程访问非常有效。通过创建新的独特恶意代码，结合从网络仿冒得到的定制电子邮件技术和对防病毒软件进行欺骗的新方法，使前述的方案成为可能。

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。这封邮件的标题为“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刚刚削减了工资，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，他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IRC，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几率。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