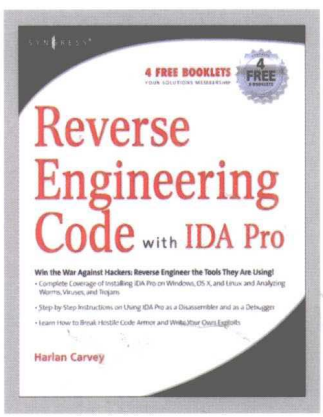
TURING 图灵程序设计丛书 网络安全系列

Reverse Engineering Code with IDA Pro

IDA Pro 代码破解揭秘

Dan Kaminsky
Justin Ferguson
[美] Jason Larsen 著
Luis Miras
Walter Pearce
看雪论坛翻译小组 译



- 安全编程修炼之道!
- 看雪学院等著名安全论坛强烈推荐
- 安全专家兼IOActive公司渗透测试总监Dan Kaminsky经典力作

人民邮电出版社
POSTS & TELECOM PRESS

TURING 图灵程序设计丛书 网络安全系列

Reverse Engineering Code with IDA Pro

IDA Pro 代码破解揭秘

Dan Kaminsky
Justin Ferguson
[美] Jason Larsen 著
Luis Miras
Walter Pearce
看雪论坛翻译小组 译

人民邮电出版社
北京

图书在版编目（CIP）数据

IDA Pro代码破解揭秘 / (美) 卡明斯基(Kaminsky,D.) 等著 ; 看雪论坛翻译小组译. — 北京 : 人民邮电出版社, 2010.8
（图灵程序设计丛书）
ISBN 978-7-115-23416-2

Ⅰ. ①I… Ⅱ. ①卡… ②看… Ⅲ. ①反汇编程序 Ⅳ. ①TP313

中国版本图书馆CIP数据核字(2010)第134621号

内 容 提 要

本书阐述了IDA Pro逆向工程代码破解的精髓，细致而全面地讲述了如何利用IDA Pro挖掘并分析软件中的漏洞。同时也展示了如何对病毒、蠕虫和木马程序的源代码进行分析，从而达到破解的目的。本书注重实践，有大量图示和示例代码供参考使用，可读性和可操作性极强。

本书适合从事逆向工程和计算机安全工作的程序员阅读。

图灵程序设计丛书

IDA Pro代码破解揭秘

◆ 著 [美] Dan Kaminsky Justin Ferguson Jason Larsen Luis Miras Walter Pearce

译 看雪论坛翻译小组

责任编辑 朱 巍

执行编辑 毛倩倩

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街14号

邮编 100061 电子函件 315@ptpress.com.cn

网址 http://www.ptpress.com.cn

中国铁道出版社印刷厂印刷

◆ 开本：800×1000 1/16

印张：17

字数：411千字 2010年8月第1版

印数：1－3 000册 2010年8月北京第1次印刷

著作权合同登记号 图字：01-2009-5726号

ISBN 978-7-115-23416-2

定价：49.00元

读者服务热线：(010)51095186 印装质量热线：(010)67129223

反盗版热线：(010)67171154

版 权 声 明

Elsevier (Singapore) Pte Ltd.

3 Killiney Road

#08-01 Winsland House I

Singapore 239519

Tel：(65)6349-0200

Fax：(65)6733-1817

First Published 2010

2010年初版

看雪致序

IDA Pro是一款非常优秀的反汇编工具，功能强大，对于有经验的程序员和软件安全相关技术人员来说是必用的工具。也许因为它过于强大和专业了，虽然很多人拥有它，但却难以熟练使用它，以至于很难发挥它强大的功能。同时很遗憾的是，IDA Pro附带提供的用户手册内容比较简洁，这同样增加了使用者了解和自如应用这款工具解决问题并将其变为利器的难度。

幸运的是，Dan Kaminsky（知名的安全专家，或者说世界著名的黑客，你可以在网上查到他的个人信息）和他的朋友不辞辛劳，为我们撰写了一部针对 IDA Pro 的应用指导性书籍 *Reverse Engineering Code with IDA Pro*。也许你已经注意到，国内外的读者和专业人士对本书的评价有很大争议。不可否认的是，作为IDA Pro的技术参考书，它的价值还是被大多数读者认可的，至少我个人是这么认为的。当然，其原著是英文版，对于国内的读者来说，这同样是个问题。

我很高兴看到 *Reverse Engineering Code with IDA Pro* 的中文版能够出版，这是看雪论坛翻译小组的兄弟们经过不懈努力带给我们大家的一份厚礼。更为难能可贵的是，他们都是利用业余时间凭借坚韧的毅力来完成这项工作的，这种吃苦和执着的精神正是我们这些程序员最为可贵的品质，我对他们的努力和成果表示由衷的祝贺和欣喜。

对于一部翻译作品，特别是技术书籍的翻译作品，在技术术语和基本含义正确的情况下，我们也许不该过多苛求信、达、雅的意境。同时我也注意到，本书的译者在一些非技术性描述的语句和章节中融入了意译，我认为这是可以接受和理解的。我认为在翻译技术书籍时，也能够并且应该可以表达译者的情感和思想，而非简单的直译。如果一味直译，读者可能会感到乏味和枯燥；在译作中融入译者的思想，就体现了译者的个性和精神。

看雪软件安全论坛已经走过十年，出版了不少广受读者欢迎的专业书籍，我希望本书能够继往开来，成为我们辉煌历程的新里程碑。再次感谢本书的全体译者，我坚信你们的努力能够被读者认可。

为了看雪下一个更加精彩的十年，让我们一起携手共进。

段钢

于北京

序

翻译很苦，作为翻译了三本书的人，我深有感触；但组织者更难，我是第一次体会。其中的酸甜苦辣不说也罢。这本书能和大家见面，我作为组织者首先要感谢全心参与的四位译者，他们是余洋、任晓枫、崔孝晨和李军。

四位译者虽然专业不同，翻译技能的熟练度不一样，但都一样认真，一样按要求细心修订。我想，所有的荣耀归于他们；如果有责难，就冲我来吧，我作为组织者，责无旁贷。在四位译者中，我最欣赏的是第 7 章和第 8 章的译者崔孝晨。他的行文很流畅，翻译也很到位，最后才了解他原来翻译过《Windows 取证分析》。当然，最令我钦佩的是他的一颗爱心，他主动提出要把稿费捐给地震灾区。

其次，要感谢看雪为这些志同道合的朋友提供了一个自由交流的空间；接下来，要感谢北京图灵文化发展有限公司的各位编辑，在与他们打交道的过程中，虽然一些细节有待商榷，但他们认真负责的态度深深感染了我，我想凭此一条，其他的就已不重要了；我还要借此机会向我的妻子表示感谢，虽然此次组织活动纯属业余活动，但她仍给予我一如既往的支持，理解万岁。

最后，请允许我向论坛上各位等待此书的朋友表示歉意，你们的支持是动力，也是鞭策。thinkSJ、colboy、Anplando、bwin、fool、shellwolf、yingyue、terren、batter、elance、brodbus、combojiang、lixianhuei、wzmooo、鹅蛋壳、太难了、zapline、jordanpz、Second、icetowater、magicfx、iawen、wtxpwh、KENW、安摧、不尽湘江、seagull、goooglеman、克里克里、duanzhu、chinazgj、xuheping、charme、jwtck、lovesuae、hcaihao、riusksk、adomore，感谢你们。

罗爱国

关于 IOActive

IOActive 成立于 1998 年，现已成功跻身于西北部计算机安全界的领导者行列（西北部计算机安全界致力于基础架构评估服务、应用程序安全服务、可管理服务、事件响应服务及教育服务）。公司为财富 500 强中的多数公司提供从企业风险管理到中立的安全硬件及众多应用程序验证服务。此外，公司还为大多数保险公司、州政府及能源公司提供 IT 灾难恢复及业务持续性计划服务。IOActive 的顾问都是公认的本地区或全国性计算机安全组织的成员和积极的撰稿人，这些安全组织包括 SANS、Agora、CRIME、ISSA、CTIN、WSA、HoneyNet 研究联盟、OWASP、华盛顿州立大学信息保险学院等。

技术编辑及著作者

Dan Kaminsky IOActive公司的渗透测试主管。Dan自1999年起（在去Cisco及Avaya上班前）在安全圈内就非常活跃。使他广为人知的是他在黑帽子大会上一系列的“Black Ops”演讲，此外，他还是唯一一位出席并在每届微软内部训练活动“Blue Hat”上发言的人。Dan致力于设计层面的故障分析，特别针对大规模的网络应用程序。Dan经常收集世界各地互联网的详细健康数据，最近用这些数据检测大部分rootkit在世界各地的繁殖情况。Dan是这个世界上少数几个同时拥有技术专长及执行层咨询技巧和能力的人。

特约作者

Justin Ferguson IOActive公司的安全顾问及研究员。他通过IOActive的应用安全实践，帮助财富500强公司理解并减轻复杂软件计算环境里的风险。Justin涉足从金融行业到联邦政府的各行业，在逆向工程、源代码审计、恶意程序分析、企业安全分析等方面有超过6年的经验。

我非常感激我的父亲 Bruce Dennis Ferguson，他是我心目中的伟人；我从来没有后悔，也不会为成为现在这样的人而感到歉意。我感谢所有来自波士顿的蓝领阶层，他们为了使儿女过上好的生活日夜操劳。当然，还有他们的另一半，每天在旁边默默支持他们的女士，你们在我心目中是最美的。我想借此机会问候来自南端和布罗克顿/南岸，仍在苦苦挣扎的每一个人，他们相信忍受不应得的苦难是一种赎罪。圣徒犹大，为我们祈祷吧。

Jason Larsen 渗透并拥有这个星球上最严密的一些系统。他的职业生涯开始于他在爱达荷州立大学发现互联网范围的秘密扫描时。为了支持他深入研究并开发检测系统，以及奖励他作为真能屏蔽渗透的第一代入侵保护系统的著作者之一，他被授予二次奖学金。出于国家安全的考量，Larsen先生不能公开所做的大部分工作。他通过爱达荷国家实验室，为能源部的大多数SCADA和PCS系统的安全问题开发更简练的解决方案。几个行业中的数百家客户，包括美国和国外的都从他的安全工作中获益。

我想把本书献给有着无限忍耐力并理解我的女友。感谢你听到最近的问题时微微点头示意，感谢你偶尔推开房门放进一缕缕阳光。每个电脑迷都应该拥有一位纹身的伴侣。

Luis Miras 一位独立安全研究员。他曾为一些安全产品厂商及主流咨询公司工作。他的兴趣包括漏洞研究、二进制分析和硬件/软件逆向。在过去，他曾涉足数字化设计和嵌入式编程。他曾出席CanSecWest、Black Hat、CCC Congress、XCon、Recon、DefCon及其他世界级的会议。他若偶尔放下IDA或集成电路工作，你便很可能发现他在制做一些甜粉。

谨以此书献给我的父母与兄弟。我要感谢Don Omar、Nancy和Nas，他们为我提供了编码配乐。我还想问候我所有的朋友并告诉他们我还活着，而且不会再消失了。

感谢 Sebastian “topo” Muniz 与我讨论 IDA 及他们那些跳跃的思维。

Walter Pearce　为 IOActive 提供应用安全和渗透测试服务，研究和开发自动化 IT 安全测试和保护功能的高级工具。他的职业生涯从 12 岁开始，他的第一个职业角色是在线零售商数据中心群集的操作员，而这使他最终成为金融服务公司和行业里的资深编程工程师。他在金融行业工作期间，专攻内部威胁的概念，并从事设计工作以降低此类事件发生的概率。客户经常要求 Pearce 先生提供专家级的应用安全服务，这涉及多种平台和（编程）语言。

致 Becca、妈妈和 David。我爱你们

目　录

第 1 章

导　言

曾几何时，信息安全专家驰骋的疆场已经发生了翻天覆地的变化。我们的任务不再是防范那些窥视我们重要资产的好奇的年轻人，而是变成了防御那些在金融或地缘政治利益驱使下的有组织犯罪，这样的攻击尤其残酷无情又手段高超。

应用程序和通信协议中的安全漏洞层出不穷，因特网也变得日益庞大而复杂，敏感信息随处可见，所有这些都为我们的对手创造了“多目标作战环境”。这些“对手”使用不同的高级软件规避 IDS、IPS 和 AV 的检测引擎，并在“肉鸡”上实现完整的远程控制和窃取数据的功能。为了了解和预测这些恶意软件会产生怎样的影响，我们免不了会利用高级逆向工程技术，使用 Data Rescue 和 Zynamics 等公司开发的行业标准工具。

本书作者为业内资深人士。本书为我们带来了逆向工程领域的前沿思想，我相信大家一定可以从中找到必要的信息，从而走向计算机安全的最前沿。

非常感谢 Lauren Vogt、Ted Ipsen、Dan Kaminsky 、Jason Larsen、Walter Pearce、Justin Ferguson、Luis Miras，以及使这本书顺利出版的 Syngress 的热心人。

Joshua J. Pennell

IOActive 公司创始人与 CEO

1.1　代码调试器概述

对我们来说，迟早都需要了解可执行文件的一切底细。比如说，你可能想知道：

- 它调用的精确内存地址；
- 它正写入数据的准确内存区域；
- 它正在从哪里读取数据；
- 它正在使用哪个寄存器。

当你没有源代码而又想分析可执行文件时，调试器可以通过对文件进行反汇编帮助你。这一般发生在分析恶意软件的时候，在这种情形下，你还指望找到它的源代码？本部分的内容不是教你熟练使用这些调试器，而是介绍一些可能会用到的调试器。调试器非常强大，要想熟练掌握，需要长时间的练习才行。

调试器中的“精英”也即本书介绍的重点是 Data Rescuse 公司的 IDA Pro（Interactive Disassembler Pro）。如果你打算在企业级环境下使用调试器，它将是你的首选。总的来说，它的价格还不算太贵，可以说是物有所值。


提示

Data Rescuse 在其网站 www.datarescue.com/idabase/index.htm 提供了 IDA Pro 的试用版。当然，试用版会有一些限制。比如说，只能处理少数几种格式的文件和适用于少数处理器类型，有使用时间的限制，只能在 Windows 平台上使用等。

IDA Pro 不仅是简单的调试器，而且是一个可编程的交互式反汇编器和调试器。有了 IDA Pro，你所能见到的可执行文件格式或应用程序应该都不在话下。IDA Pro 可以处理各种平台上的文件，从 Xbox、Playstation、Nintendo 到 Macintosh，从 PDA 到 Windows、UNIX 等，几乎包含所有类型的平台。图 1-1 显示了 IDA Pro 启动时出现的界面。注意，界面上显示了各种文件类型及选项卡，帮助你为反汇编的文件选择合适的分析引擎。

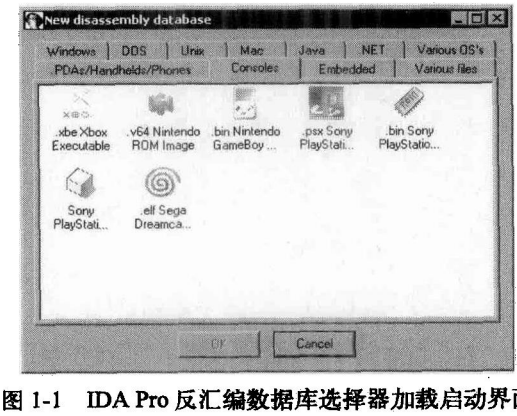


图 1-1　IDA Pro 反汇编数据库选择器加载启动界面

在图 1-2 中，IDA Pro 加载了名为 instantmsgre.exe 的 WootBot 变种。从图 1-2 中我们看到，它被打包软件 Molebox 处理过。此外，你还可以看到它正在生成的内存调用，以及调用了哪些 Windows DLL。当你需要击退病毒或恶意软件，特别是为了修复系统而编写专杀工具时，这些信息可都是无价之宝。

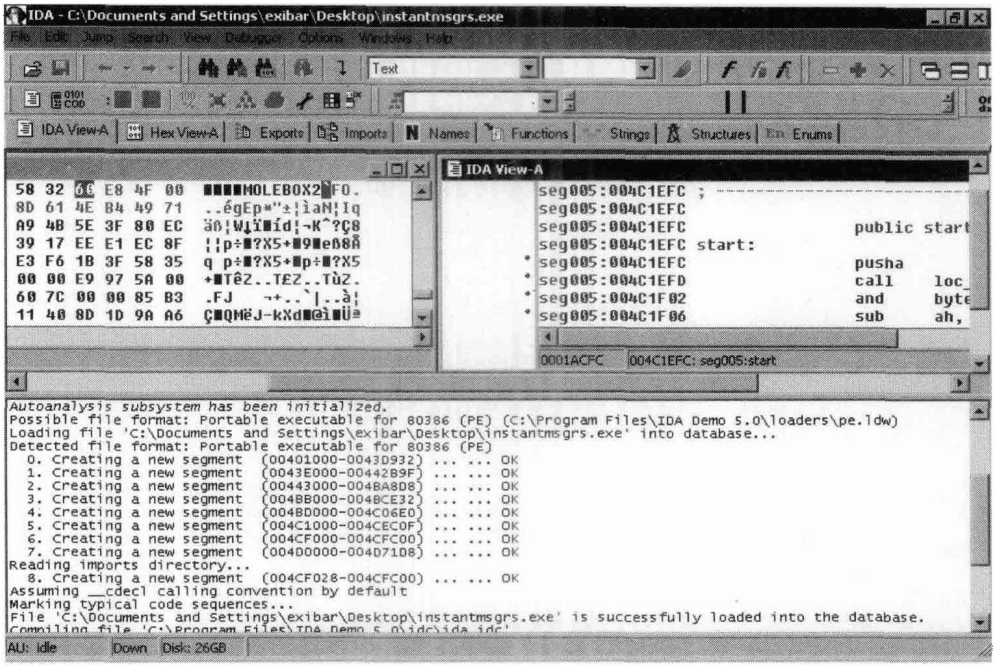


图 1-2 IDA Pro 反汇编 WootBot 的变种——instantmsgre.exe

1.2 小结

IDA 是 Windows 下众多调试工具中颇受大家欢迎的一种。IDA Pro 首先是一个反汇编器，可以显示二进制汇编码（可执行文件或 DLL（Dynamic Link Library，动态链接库)），它提供的某些高级功能使我们更容易理解汇编代码。其次，它又是一个调试器，用户可以逐条调试二进制文件中的指令，从而确定当前正在执行哪条指令，以及执行的顺序等。在本书中，我们会一一介绍这些内容。IDA Pro 广泛应用于恶意软件分析、软件漏洞研究等目的。你可以直接在 www.datarescue.com 上订购 IDA Pro。

第 2 章

汇编及逆向工程基础

本章内容：

- 汇编语言及 IA-32 处理器
- 堆、栈及二进制可执行文件中的其他区段
- 最新的 IA-32 指令集及参考资料

☑ 小结