HZ BOOKS
华章科技

信息安全
技术丛书

# 黑客免杀攻防

任晓珲 著

## Hacker Anti-AntiVirus Software Technology Offensive and Defensive

- 全方位揭示黑客免杀技术的常用方法、技术细节和思想原理，为反病毒工程师剖析恶意软件和遏制免杀技术提供具体方法和应对策略
- 从攻与防的双重角度详细讲解PE文件知识、逆向工程、C++壳的编写、免杀壳的打造、脱壳、Rootkit等安全技术的细节，为反病毒工程师提供技术指导

机械工业出版社
China Machine Press

信息安全
技术丛书

# 黑客免杀攻防

Hacker Anti-AntiVirus Software Technology
Offensive and Defensive

任晓珲 著

机械工业出版社
China Machine Press

**图书在版编目（CIP）数据**

黑客免杀攻防 / 任晓珲著 . —北京：机械工业出版社，2013.10

ISBN 978-7-111-44042-0

Ⅰ. 黑… Ⅱ. 任… 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（2013）第 218041 号



国内首部关于黑客免杀技术的专著，旨在为反病毒工程师剖析各种恶意软件和应对各种安全威胁提供全面指导。不仅从攻击者（黑客）的视角全方位揭示了黑客免杀技术的常用方法、常用技术和思想原理，还从防御者（反病毒工程师）的视角深入讲解了遏制免杀技术的具体方法策略。从纯技术的角度讲，本书不仅详细讲解了免杀技术的各种细节和方法，还详细讲解了 PE 文件、逆向工程、C++ 壳的编写、免杀壳的打造、脱壳、Rootkit 等安全技术的细节。

全书共 20 章，分为三大部分：基础篇（第 1~6 章）详细介绍了黑客免杀技术的初级技巧，包括查找（修改）特征码、常见特征码绕过技巧、壳在免杀中的应用、花指令和其他免杀基础知识；高级篇（第 7~16 章）深入讲解了 PE 文件、逆向工程、C++ 壳的编写、免杀壳的打造、脱壳、Rootkit 等常用安全技术的原理和细节，以及黑客免杀技术是如何应用它们的，为反病毒工程师应对各种恶意软件提供了原理性指导；扩展篇（第 17~20 章）为遏制黑客免杀技术提供了思路和具体的方案。

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：孙海亮

藁城市京瑞印刷有限公司印刷

2013 年 9 月第 1 版第 1 次印刷

186mm×240 mm • 29.25 印张

标准书号：ISBN 978-7-111-44042-0

定　　价：89.00 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　　投稿热线：（010）88379604

购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

# 前　言

## 为什么要写这本书

计算机安全领域最初且规模最大的博弈莫过于病毒与反病毒的博弈，这也是计算机安全领域的硝烟燃起之处。然而，我们当中的有些人可能并不知晓黑客免杀技术现今已经成为反病毒领域中的主要破坏力量，而究其原因，也许是由此技术带来的大规模病毒木马泛滥与黑客免杀技术本身的隐蔽性所导致的。

但是很幸运，您手中的这本书就是迄今为止第一本详细介绍免杀技术的图书，您和我都应为此而感到庆幸。

2008 年 2 月，我应邀与《黑客 X 档案》杂志的主编一起策划了《黑客免杀入门》的编写工作。《黑客免杀入门》就是本书的雏形，那真的是一个很好的开始。当时还在上大一的我为了使这本书能够快速上市，几乎牺牲了所有课余时间。在经过半年的艰苦写作之后，《黑客免杀入门》终于在 2008 年 10 月正式上市，并在半年内创下了 5000 册销量的佳绩。

但是由于种种原因，使得我对自己的第一本书并不满意，因为要考虑到初学者的接受力与知识储备，因此并未将黑客免杀技术的真正意义体现在那本书里，再加之免杀技术在第一本书发行后的几年里发生了很大变化，因此使我有了编写第二本书的动力。

## 如何阅读本书

本书详细描述了 Windows 系统下黑客免杀的所有技术细节，讲解了为什么病毒、木马在经过免杀处理后就会被反病毒软件误认为是正常的程序。除此之外，本书还详细讲述了黑客

与反病毒工程师都应该掌握的基础知识，包括 PE 文件结构、软件逆向工程、壳的原理及编写思路、Rootkit 等等。在最后，笔者总结了一些遏制免杀技术的方法以及应对策略，相信对于很多反病毒工程师来讲都会有所启发。

本书共分为基础篇、高级篇与扩展篇三大部分，分别面向的是零基础读者、高级读者与反病毒工程师，要完全掌握这三部分，所需的基础知识如下：

**基础篇** 其中所有内容几乎都未过深涉及任何计算机语言，因此只要能熟练操作 Windows 系统，并对硬件有基本的常识性认识，即可顺利阅读这部分内容，除此之外不再需要读者有任何基础。

**高级篇** 要求读者对于 C/C++、汇编语言有基本的了解，并且要有一定的 Windows 程序开发经验，除此之外也需要读者对操作系统的结构有所了解。

**扩展篇** 要求读者熟悉黑客免杀的技术细节，并初步掌握 PE 文件结构、软件逆向工程、壳的原理及编写思路、Rootkit 等高端技术。

## 本书的主要内容

**基础篇** 包括第 1 章～第 6 章，这部分由第 1 章“变脸”开篇，以类比的形式将黑客免杀技术的特点向大家娓娓道来，随后通过对免杀基础知识的介绍，可以迅速让初级读者彻底明白何为黑客免杀技术。

待初级读者理解了何为免杀技术后，随后的几个章节则以比较简单易懂的语言向大家描述与黑客免杀技术密切相关的一些技术，例如特征码、花指令、壳等等。

**高级篇** 包括第 7 章～第 16 章，这部分所讲的内容都是黑客们得以展开较高层面免杀操作的技术基础，同时也是反病毒工程师与大部分软件安全行业从业者必备的技术基础。

本篇详细地阐述了 Windows 下的 PE 文件结构，并着重讲解了软件逆向工程的技术原理与分析思路。除此之外，第 11 章还在纯 C++ 语言的角度描述了一个壳的编写，这在国内来说尚属首次。在本篇的最后，还详细介绍了部分 Rootkit 技术的实现原理与当前黑客免杀技术的最前沿思想。

**扩展篇** 包括第 17 章～第 20 章，这部分主要针对当下的免杀技巧及黑客常用的免杀手法提出了一些反制措施，分别对反特征码定位、遏制 Rootkit 展开了讨论，并在最后对时下的反病毒产品简略地给出了一些改进建议。

## 这正是那酝酿三年的 2.0 版

现在您拿在手里的这本书是以《黑客免杀入门》的部分内容为基础，加入大量新鲜内容后重新组织、编排的一个全新版本，这本书真正考虑到了免杀技术的广度与深度，采用了知识层次分离编写的方式，以求照顾到高中低各层次的绝大多数读者。

**深广结合，高低分离**

本书的全部内容分为三个部分，其中每个部分都相对独立、互成体系，分别面对不同层次的读者。对于基础知识的讲解主要集中在前两部分，第一部分只对相关知识进行了解性讲解，其难度以满足阅读第一部分内容所需的知识储备为标准。第二部分对免杀的所有技术细节进行了细致深入的讲解，可看作是第一部分的延伸与拓展。

**分解难点，注重延续**

第一部分的阅读基础大致定位在非专业人士的层次上。因此为了照顾这部分读者的后续学习能力，对每个重点、难点都进行了相应的拆分讲解，并以第二部分的部分内容作为扩展阅读资源，使得初级读者的技术飞跃成为可能。

**增新改旧，重排章节**

本书新增了大量的技术描述，例如 PE 文件结构、壳的编写技术、Rootkit 技术等，同时删除了第一版中关于突破主动防御的章节并重新整理编写。除此之外，对于其他章节也进行了大量的重写与更新，这些更新使得第一版保留下来的内容不超过 10%。

## 本书的读者

第一篇对应的为初级层次的读者，如果你已经有了一定的基础，且对黑客免杀技术有了一定的了解，可跳过本部分。适合阅读本部分的读者如下：

- ❑ 黑客技术爱好者
- ❑ 信息安全专业的学生
- ❑ 想了解黑客免杀技术的初学者

第二篇对应的为中级层次的读者，如果你已经对 PE 文件、软件逆向、壳的编写、Rootkit 有了较为深入的了解，可跳过本部分。适合阅读本部分的读者如下：

- ❑ 软件安全爱好者
- ❑ 想系统学习 PE 文件结构的人
- ❑ 需要快速掌握软件逆向技术的相关工作人员
- ❑ 想用 C++ 写壳的技术狂人，或仅想写一个壳的爱好者
- ❑ 对于 Rootkit 感兴趣的人

第三篇对应的为高级层次的读者，此部分内容并没有具体的技术细节，着重讲解了相关技术的核心思想，适合具备一定基础的人阅读：

- ❑ 反病毒工程师
- ❑ 免杀技术爱好者

## 勘误和支持

本书从创意到落实写作，再到最终完成，整整度过了三年的时间，其中有足足两年的时

间是用于本书的写作，这是我用人生最精彩的一段时间撰写的一本书，因此也期望这本书能同样精彩。

但是，事实总是残酷的，由于本人的水平有限，而且感觉两年的时间还是太少了，书中难免还会有一些不足。记得俄罗斯的“斯坦尼斯拉夫斯基”用了一生的时间才写出了《演员的自我修养》这本书，这是没有认真写书经历的人难以体会的。

我是一个不愿妥协的人，在撰写本书之初就是如此，但是很不幸的是我还是一次次地被残酷的事实打败。在我与之对抗了两年之后，才感觉这本书可以拿出来见人了，我承认它离完美还有相当长的一段距离。

这本 40 余万字的图书是我目前为止做过的最大的一个“工程”，我承诺会在精力允许的前提下，在本书出版之前不放弃任何一次修正本书错误的机会，但是我知道它最终还是会带着若干错误与读者们见面，请原谅我无法修复这些错误，这有可能是我的精力问题，也有可能是我的能力问题。但是，我非常期望能收到您的来信，指导我修正本书中的错误，为这本书走向完美“添砖加瓦”。

为此，我在黑客反病毒论坛中建立了一个专门的分区来处理本书中的所有问题，包括读者反馈、勘误列表与本书的相关资源下载，本书的交流专区：http://book.hackav.com/。本书相关资源还可到华章官网下载，华章的官网：http://www.hzbook.com/。

除此之外，您还可以通过邮件与我取得联系，我的邮箱：0x0026@gmail.com、a1pass@163.com。

## 特别致谢

首先请允许我借此机会感谢我的父母在事业上、写作上以及生活上对我的支持与关爱，我因拥有你们的爱而变得更加坚强与勇敢，我的所有荣耀都属于你们。

其次，尽管只有我的名字被印在了本书的封面上，但是您手中的这本 40 余万字的书显然不是一个人的工作成果，本书的顺利出版得益于众多朋友的鼎力相助。在此，我要感谢那些在我写作的过程中为我提供过帮助的人。

钱林松　感谢您将我引荐给杨福川，这使得我有了完成自己写作梦想的机会。

薛亮亮　我的创业伙伴，没有你的理解与担当就不可能有这本书的面世。

黄　瀚　为本书提供了大量一手资料，感谢你一直以来对于本书的关注与支持。

段　刚　段老师预读了本书的部分章节，并对本书的定位提出了很多特别好的建议。

李常坤　审阅了本书的第 11 章和第 12 章，并提出了宝贵建议。

卢超超　在本书的定位方面及前期的策划时发挥了重要作用，并在初期提出了宝贵建议。

彭燕青　对第 14 章和第 15 章的编写提供了宝贵的技术方面的建议。

许晓明　审阅了本书的第 7 章和第 9 章，并修改了一些技术上的错误。

吴　彬　在写作初期向我详细阐述了反病毒工程师的各个工作流程。

全珠荣　为本书提出了不错的建议，感谢你在写作上对我的帮助。

杨福川　首席策划，感谢您在整本书的写作期间所做的大量协调工作。
孙海亮　我的编辑，感谢您对本书的审校工作，您的敏锐思维能力让我很欣赏。
杨绣国　我的编辑，十分细心地审阅了本书的大部分章节，感谢您对此做出的工作。
白　宇　我的编辑，帮我熟悉了整套图书出版的流程，感谢您的帮助。
最后，感谢北京蓝森科技有限公司的所有同事，这本书的顺利出版离不开你们的理解与支持，是你们在我写作的过程中为我承担了大部分的工作。另外，感谢黑客反病毒组织（www.hackav.com）中对本书提出过宝贵意见的所有网友，是你们的投票保证了本书内容安排的合理性。

任晓珲
于北京

# 目　录