TURING 图灵程序设计丛书

The Antivirus Hacker's Handbook

黑客攻防技术宝典
反病毒篇

[西] Joxean Koret [美] Elias Bachaalany 著
周雨阳 译

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

TURING 图灵程序设计丛书

The Antivirus Hacker's Handbook

黑客攻防技术宝典
反病毒篇

[西] Joxean Koret [美] Elias Bachaalany 著
周雨阳 译

人民邮电出版社
北京

图书在版编目（CIP）数据

黑客攻防技术宝典. 反病毒篇 / (西) 霍克西恩·科雷特 (Joxean Koret), (美) 埃利亚斯·巴沙拉尼 (Elias Bachaalany) 著 ; 周雨阳译. -- 北京 : 人民邮电出版社, 2017.8
(图灵程序设计丛书)
ISBN 978-7-115-46333-3

Ⅰ. ①黑… Ⅱ. ①霍… ②埃… ③周… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2017)第175659号

内 容 提 要

本书由业界知名安全技术人员撰写，系统介绍了逆向工程反病毒软件。主要内容包括：反病毒软件所采纳的各种具体手段，攻击和利用杀毒软件的多种常见方法，杀毒软件市场现状以及未来市场预估。

本书是逆向工程师、渗透测试工程师、安全技术人员和软件开发人员的必读指南。

◆ 著 [西] Joxean Koret [美] Elias Bachaalany
译 周雨阳
责任编辑 杨 琳
责任印制 彭志环

◆ 人民邮电出版社出版发行 北京市丰台区成寿寺路11号
邮编 100164 电子邮件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京鑫正大印刷有限公司印刷

◆ 开本：800×1000 1/16
印张：17.5
字数：424千字 2017年8月第1版
印数：1－3500册 2017年8月北京第1次印刷
著作权合同登记号 图字：01-2015-6364号

定价：79.00元

读者服务热线：(010)51095186转600 印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

站在巨人的肩上

Standing on Shoulders of Giants

iTuring.cn

站在巨人的肩上

Standing on Shoulders of Giants

iTuring.cn

版权声明

前　言

感谢你购买并阅读本书！通过阅读本书，你会了解到有关反病毒产品和逆向工程的知识。值得一提的是，本书所讨论的逆向工程的相关技术和工具，不仅可以应用在反病毒软件上，也可以应用于其他软件产品。无论你是安全研究员、渗透测试工程师还是其他领域的信息安全专家，都可以从本书中受益。当然，如果你是反病毒工程师，同样能从中受益，因为你将了解到攻击者如何分析反病毒产品，如何将其拆分成不同模块，以及你该如何避免反病毒产品被攻破或者如何增加破解难度。

我想强调的是，虽然本书重点在于讲述与反病毒产品相关的理论知识，但是也提供了一些实战案例，展示了如何在实际的应用程序中运用逆向工程、漏洞挖掘和漏洞利用技术。

本书概述

本书专为那些想更好地了解反病毒产品功能实现原理的读者而撰写，无论你身处攻防战役中的哪一个阵营，都不妨研读一番。本书旨在帮助你了解在实战过程中针对特定的任务目标，何时以及如何选用正确的技术和工具，同时又该重点关注反病毒产品的哪些部分。如果下列描述中有一条或多条与你的情况相吻合，那么没错，本书就是为你而写的：

- 想更深入地了解反病毒产品的安全性；
- 想更深入地了解逆向工程的相关技术（也许目的是逆向分析反病毒产品）；
- 想绕过反病毒产品的防护体系；
- 想动手将反病毒产品拆分成多个模块；
- 想编写攻击反病毒产品的漏洞利用程序；
- 想评估反病毒产品；
- 想从整体上提高自己的反病毒产品的安全性，或者想知道如何编写防御性代码以对付攻击性代码；
- 热爱编程，或者想丰富信息安全领域的相关知识，提升技术水平。

本书结构

全书内容组织如下。

第 1 章，*反病毒软件入门* 带你一览反病毒软件的历史，同时探讨目前市场上主流反病毒产品的典型及非典型功能。

第 2 章，*逆向工程核心* 介绍如何通过调试反病毒软件或禁用反病毒软件的自我保护功能等相关技巧来逆向分析反病毒产品。这一章还将探讨如何结合逆向工程技术使用 Python 为 Avast for Linux 编写附加组建程序，并介绍一款使用 C/C++为 Comodo for Linux 反病毒软件编写的非官方软件开发工具包（software development kit，SDK）。

第 3 章，*插件系统* 讨论各式反病毒产品是如何使用插件的，这些插件是如何被加载和分发的，以及使用反病毒插件的目的。

第 4 章，*反病毒特征码技术* 带你一览反病毒产品中最典型的几种特征码技术，以及一些高级特征码。

第 5 章，*反病毒软件的更新系统* 阐释反病毒软件是如何实现更新的，更新系统是如何开发的，以及更新协议是如何工作的。这一章末尾还将通过一个实例展示如何逆向分析一个简易的更新协议。

第 6 章，*绕过反病毒软件* 概述如何绕过反病毒软件，使程序文件避开相关检测。这一章将讨论一些一般性技巧，并且探讨应该避免使用的技术。

第 7 章，*绕过特征码识别* 紧接第 4 章内容，带领你探索如何绕过各种特征码检测技术。

第 8 章，*绕过扫描器* 以反病毒扫描器为核心，继续讨论如何绕过反病毒软件。这一章将介绍如何绕过静态启发式扫描引擎、反汇编、反模拟和其他反病毒技术，还将介绍如何编写一个用以生成绕过反病毒扫描器检测的可执行文件的自动化工具。

第 9 章，*绕过启发式引擎* 展示如何同时绕过反病毒软件采用的静态和动态启发式引擎，以此来结束反病毒防护绕过技术的讨论。

第 10 章，*确定攻击面* 介绍攻击反病毒产品的有关技术，指导你发现反病毒软件暴露的本地和远程攻击面。

第 11 章，*拒绝服务攻击* 讨论如何利用反病毒软件的漏洞和缺陷，在本地和远程向反病毒产品发起拒绝服务攻击。

第 12 章，*静态分析* 带领你学习如何静态审计反病毒软件来挖掘其中存在的漏洞，包括一些真实案例。

第 13 章，*动态分析* 继续讨论如何挖掘反病毒产品的漏洞，但这里将利用动态分析技术。这一章将会重点介绍现今最流行的漏洞挖掘方法——模糊测试，并向你阐释如何搭建一个统一管理的分布式模糊测试工具，来自动挖掘和分析反病毒产品的缺陷。

第 14 章，*本地攻击* 介绍利用本地漏洞攻击反病毒产品的过程，并将重点关注逻辑漏洞、后门和内核泄漏的利用。

第 15 章，*远程漏洞* 讨论如何利用反病毒产品中的内存损坏漏洞，编写远程漏洞利用程序。同时，还将展示如何针对反病毒软件的更新服务进行攻击，并给出一个针对某个更新服务协议的完整的漏洞利用程序。

第 16 章，*当前反病毒防护趋势* 讨论利用反病毒软件缺陷的攻击者会瞄准哪些反病毒产品

用户，而哪些用户不太可能成为该类恶意攻击的目标。同时，本章还会带你一窥滋生该类缺陷的“黑暗世界”。

第 17 章，一些建议和未来展望　最后，为反病毒软件的用户和供应商提供一些建议，并展望未来反病毒产品可以采用哪些防护策略。

目标读者

本书主要面向拥有中级技术水平的个人开发者和逆向工程师，不过资深逆向工程师同样会从本书所讨论的技术内容中获益。如果你是反病毒工程师或恶意软件逆向工程师，那么本书能帮助你了解攻击者会如何利用软件漏洞。同时，本书也阐释了如何避免一些不利情况，如攻击者利用你的反病毒产品中的漏洞攻击你要保护的用户。

更资深的专业人士可以通过阅读本书的几个特定章节，来获得更多的相关知识和技能。比如，如果你想要了解如何编写针对反病毒软件的本地和远程攻击利用程序，可以参考第三部分“分析与攻击”。在该部分中，你将了解从确定攻击面开始到发现漏洞再到利用漏洞的整个过程。如果你对绕过反病毒防护感兴趣，那不妨参考第二部分“绕过反病毒软件”。总之，你可以从头到尾阅读本书，也可以根据自己的需求，有选择性地进行阅读。

所需工具

强烈的求知欲是你阅读本书前最需要的准备。尽管我已经尝试尽可能在书中使用开源的免费软件来做演示，但是有的地方还是会用到一些收费软件。比如，在本书的很多案例中，我用到了商业版软件 IDA，因为除个别软件外，大多数反病毒产品都是闭源的商业软件。这就要求我们在分析过程中用到逆向软件，而 IDA 是最常用的一款。其他所需的工具包括编译器、解释器（比如 Python）和其他一些没有开源但是可以免费下载的工具，比如 Sysinternals。

网络资源

为了让你能够简单快速上手，本书中可能需要用到的一些基础工具都可以在 Wiley 为本书建立的页面上下载：http://www.wiley.com/go/antivirushackershandbook。

总结

本书旨在帮助读者了解反病毒产品是什么、不是什么，以及对它们应该有什么期待；这些信息可能并不为大众所熟知。本书并不是要阐释反病毒产品的工作原理，而是展示在你可能正在使用的反病毒软件中真实存在的漏洞缺陷、漏洞利用代码和相关技术。同时，本书还深入探讨了绕过反病毒产品的防护技巧，以及相关的漏洞挖掘和利用方式。学习如何攻破反病毒产品不仅对攻击者们来说大有裨益，也可以帮助你理解如何提升反病毒产品的防护效果，以及反病毒产品的用

户如何才能最大程度地保护自己。

电子书

扫描如下二维码，即可购买本书电子版。

致　　谢

我要感谢 Mario Ballano、Ruben Santamarta、Victor Manual Alvarez，以及所有给予我帮助、与我分享意见和建议、跟我讨论想法的朋友们。最要感谢的是我的女友，在整个写作过程中，她给予了我莫大的理解和支持。十分感谢 Elias Bachaalany，没有他的鼎力相助，本书就不可能写成。另外，特别鸣谢 Wiley 的每一位工作人员，与你们的合作十分愉快。最后，还要感谢曾经帮助和支持我的 Daniel Pistelli、Carol Long、Sydney Argenta、Nicole Hirschman 和 Marylouise Wiack。

目　录

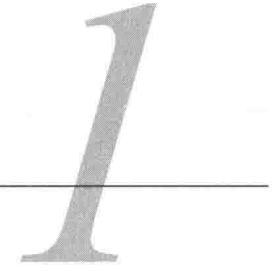
第一部分　反病毒技术入门

第四部分　当前趋势与建议

第一部分

反病毒技术入门

第 1 章 反病毒软件入门



反病毒软件通过监测手段保护计算机免受恶意软件感染，并适时移除恶意软件，使计算机脱离感染状态。在本书中，恶意软件（malicious software或malware）也称为“样本”，它有许多种类，包括木马病毒、感染型病毒、Rootkit、下载者病毒、蠕虫病毒等。

本章将阐述反病毒（antivirus，AV）软件的定义及其工作原理。同时，还将介绍反病毒软件的简史，并简单分析反病毒软件的演进。

1.1 何谓反病毒软件

反病毒软件是旨在为原生操作系统（如Windows、Mac OS X）提供更好安全防护的特殊软件。在多数时候，它被用作预防性安全方案。一旦防护失效，反病毒软件就成了从操作系统中彻底清除恶意软件、使计算机摆脱感染的解决方案。

反病毒软件使用多种技术来侦测潜藏在操作系统深处且带有自我保护功能的恶意软件。高级恶意软件可能会使用未公开的系统功能和混淆技术来躲避侦测并持续潜伏在计算机中。如今，用户面临着来自四面八方的安全威胁，反病毒软件的使命就是处理出自可信以及不可信来源的恶意文件。反病毒软件要处理的恶意文件来源有：网络数据包、邮件附件、浏览器漏洞攻击利用程序、文档阅读器，以及运行在操作系统上的可执行程序。

1.2 反病毒软件的历史与现状

最早的反病毒产品在严格意义上只能算作扫描器，因为它们仅是在可执行程序中侦测恶意代码的命令行扫描程序。不过，在此之后，反病毒软件经历了天翻地覆的变化。比如，反病毒软件已不再含有命令行式的扫描器了。如今，大多数反病毒产品有了图形用户界面（graphical user interface，GUI），会检查操作系统或用户程序产生、修改或访问的每一个文件。它们还配备了防火墙功能，来侦测通过网络感染计算机的恶意文件；安装了浏览器插件，来侦测基于Web的漏洞利用攻击；为网络支付创造了安全隔离环境；从系统驱动底层，实现了自我防护和安全沙盒功能等。

在DOS和其他古老的操作系统时期，软件产品只需要跟随系统更新而更新。但在此之后，随

着数量惊人的恶意软件产生，反病毒软件也不断提高了更新的频率。20世纪90年代，反病毒企业在一周内只会收到几个关于恶意程序的报告，而且往往都是文件感染型病毒；而如今，它每天都会收到成千上万完全不同的恶意文件样本（这里的“不同”是指类似MD5、SHA-1文件散列值不同）。这迫使反病毒企业致力于开发自动化侦测方案，类似启发式引擎（heuristics），通过动态和静态两种手段来侦测未知病毒。第3章和第4章将会深入探讨反病毒软件的工作原理。

金钱是驱使恶意软件和反病毒软件产品频繁升级对抗的根本原因。早期，病毒制作者（virus creator或vxer）往往只是因为想博人眼球或挑战自我而编写一些采取新破坏手段的文件感染型病毒。如今，恶意软件开发已经成了敲诈计算机用户的暴利产业。无论是偷取用户在诸如eBay、Amazon、Gmail等网站的账户登录凭证，还是入侵用户在支付平台（如Paypal）的账号，其最终目的是一致的：不择手段地获取尽可能多的钱财。

恶意软件制作者可以通过病毒窃取你的Yahoo邮箱或Gmail登录凭证，然后以你的名义向别的用户大量扩散垃圾邮件或传播恶意软件。他们还可以使用窃取到的信用卡信息将你账户内的资金转移到恶意账户上去，或是通过“钱骡”洗钱。因此，他们的犯罪活动正变得越来越难以追踪。

另一种日益典型的恶意软件主要用以监听民众的通信，其幕后推手是权利机构、灰色组织，或是向权利机构出售间谍软件的黑客公司。也有一些恶意软件开发是为了破坏他国的基础设施。

恶意软件也可以为了监视政府机构、公司或个人而开发。监视软件的两个典型案例是FinFisher和Hacking Team。政府、执法部门和安全部门采购商业版的FinFisher和Hacking Team来监视罪犯和嫌疑人。

恶意软件的换代升级以及恶意软件市场大量的资本涌入，迫使反病毒工业在最近十年内发生了显著的改变和升级。遗憾的是，在攻防博弈中，反病毒软件一直处在被动局面。通常，反病毒软件厂商无法侦测未知病毒，尤其是那些在开发过程中采取了一些免杀手段的恶意软件。这其中的原因很简单：免杀是恶意软件开发的重要一环；对于攻击者来说，保证开发的恶意软件不被反病毒软件查杀，时间越长越好。无论是否合法，许多商业版本的恶意软件包都有一定的支持服务期限。在服务支持期间，恶意软件产品会根据反病毒软件或是操作系统的查杀情况适时作出更新。另外，恶意软件也会通过升级来应对和修补bug，添加新功能等。反病毒软件也可能成为攻击目标，比如有幕后支持的Mask病毒，就利用了卡巴斯基的一个零日漏洞。

1.3 反病毒扫描器、内核和产品

通常，计算机用户可能只会把反病毒软件简单地看成一个软件套装，但是攻击者必须要有从更深层次来分析反病毒软件的能力。

本章将详细阐释反病毒软件的各个组成部分：反病毒内核、命令行扫描器、GUI扫描器、守护进程或系统服务、文件系统防护驱动、网络防护驱动，以及反病毒软件的其他一些功能模块。

以ClamAV为例，它是一个扫描器，也是目前仅有的一款开源反病毒软件。它的工作方式是，根据特征扫描计算机内的恶意软件，每查杀到一个恶意软件，就生成一条警告消息。不过，ClamAV既没有使用基于文件行为的启发式查杀系统，也没有修复感染文件的能力。