

# 游戏外挂攻防艺术



[游戏外挂攻防艺术 下载链接1](#)

著者:徐胜

出版者:电子工业出版社

出版时间:2013-2

装帧:平装

isbn:9787121195327

随着网络的普及，网络游戏得到了众多网民的青睐。但是，网络游戏的盛行，也给游戏玩家和游戏公司带来了很多安全问题，如木马盗号、外挂作弊等。对于正常的游戏玩家和游戏公司来说，外挂的危害尤其突出。因为一款免费的外挂，不仅可能携带游戏木马，还会影响游戏的平衡，甚至伤害其他玩家的感情。虽然很多玩家和安全爱好者对

外挂和反外挂技术有强烈的兴趣，但目前市面上很难找到一本能够深入浅出地讲解这部分知识的书。《游戏外挂攻防艺术》将带领读者走近外挂和反外挂技术这个神秘的领域，让读者了解外挂的制作过程、作弊过程以及反外挂检测技术，从而提升读者对游戏安全的认识。

《游戏外挂攻防艺术》是作者（徐胜）长期分析外挂软件和反外挂的经验所得，分5篇，共10章，包括游戏和外挂初识、外挂技术、游戏保护方案探索、射击游戏安全和外挂检测技术。本书内容循序渐进，层层解剖外挂涉及的一些关键技术，包括注入、隐藏、交互、Hook和Call函数等，让读者对外挂产生直观和深刻的认识，独创性的外挂分析和检测方法对安全从业者而言也有很好的借鉴意义。

作者介绍：

徐胜，2009年于电子科技大学获得计算机科学与工程硕士学位，现就职于阿里巴巴，从事移动安全的研究和移动产品的研发，主要研究方向包括：Windows平台下的木马、外挂、Rootkit、防火墙和二进制逆向分析，Android和iOS客户端软件安全，以及Web和WAP安全。

目录: 第1篇 游戏和外挂初识篇

第1章 认识游戏和外挂 2

1.1 游戏安全现状 2

1.2 什么是外挂 3

1.3 内存挂与游戏的关系 3

1.4 游戏的3个核心概念 5

1.4.1 游戏资源的加/解密 5

1.4.2 游戏协议之发包模型 11

1.4.3 游戏内存对象布局 16

1.5 外挂的设计思路 24

1.6 反外挂的思路 25

1.7 本章小结 26

第2篇 外挂技术篇

第2章 五花八门的注入技术 28

2.1 注册表注入 28

2.2 远线程注入 29

2.3 依赖可信进程注入 32

2.4 APC注入 34

2.5 消息钩子注入 36

2.6 导入表注入 39

2.7 劫持进程创建注入 48

2.8 LSP劫持注入 50

2.8.1 编写LSP 52

2.8.2 安装LSP 56

2.9 输入法注入 60

2.10 ComRes注入 66

第3章 浅谈无模块化 67

3.1 LDR\_MODULE隐藏 67

3.2 抹去PE“指纹” 74

3.3 本章小结 76

第4章 安全的交互通道 77

4.1 消息钩子 77

4.2 替代游戏消息处理过程 81

4.3 GetKeyState、GetAsyncKeyState和GetKeyboardState 82

|                           |     |
|---------------------------|-----|
| 4.4 进程间通信                 | 84  |
| 4.5 本章小结                  | 89  |
| 第5章 未授权的Call              | 90  |
| 5.1 Call Stack检测          | 90  |
| 5.2 隐藏Call                | 90  |
| 5.2.1 Call自定义函数头          | 91  |
| 5.2.2 构建假栈帧               | 99  |
| 5.3 定位Call                | 107 |
| 5.3.1 虚函数差异调用定位Call       | 107 |
| 5.3.2 send() 函数回溯定位Call   | 110 |
| 5.4 本章小结                  | 112 |
| 第6章 Hook大全                | 113 |
| 6.1 Hook技术简介              | 113 |
| 6.2 IAT Hook在全屏加速中的应用     | 115 |
| 6.3 巧妙的虚表Hook             | 121 |
| 6.3.1 虚表的内存布局             | 122 |
| 6.3.2 C++ 中的RTTI          | 123 |
| 6.3.3 Hook虚表              | 125 |
| 6.4 Detours Hook          | 128 |
| 6.4.1 Detours简介           | 128 |
| 6.4.2 Detours Hook的3个关键概念 | 128 |
| 6.4.3 Detours Hook的核心接口   | 130 |
| 6.4.4 Detours Hook引擎      | 132 |
| 6.5 高级Hook                | 147 |
| 6.5.1 S.E.H简介             | 147 |
| 6.5.2 V.E.H简介             | 148 |
| 6.5.3 硬件断点                | 150 |
| 6.5.4 S.E.H Hook          | 153 |
| 6.5.5 V.E.H Hook          | 156 |
| 6.5.6 检测V.E.H Hook        | 157 |
| 6.6 本章小结                  | 159 |
| 第7章 应用层防护                 | 160 |
| 7.1 静态保护                  | 161 |
| 7.2 动态保护                  | 165 |
| 7.2.1 反dump               | 165 |
| 7.2.2 内存访问异常Hook          | 169 |
| 7.3 本章小结                  | 171 |
| 第3篇 游戏保护方案探索篇             |     |
| 第8章 探索游戏保护方案              | 174 |
| 8.1 分析工具介绍                | 174 |
| 8.1.1 GameSpider          | 174 |
| 8.1.2 Kernel Detective    | 178 |
| 8.2 定位保护模块                | 178 |
| 8.2.1 定位ring0保护模块         | 179 |
| 8.2.2 定位ring3保护模块         | 179 |
| 8.2.3 定位自加载模块             | 185 |
| 8.3 分析保护方案                | 187 |
| 8.3.1 ring3保护方案           | 187 |
| 8.3.2 ring0保护方案           | 189 |
| 8.4 本章小结                  | 191 |
| 第4篇 射击游戏安全专题              |     |
| 第9章 射击游戏安全                | 194 |
| 9.1 自动开枪                  | 194 |
| 9.1.1 易语言简介               | 195 |

|                     |     |
|---------------------|-----|
| 9.1.2 易语言版自动开枪外挂    | 195 |
| 9.2 反后坐力            | 199 |
| 9.2.1 平衡Y轴法         | 199 |
| 9.2.2 AutoIt脚本法     | 200 |
| 9.3 DirectX Hack    | 203 |
| 9.3.1 DirectX简介     | 203 |
| 9.3.2 用Direct3D绘制图形 | 209 |
| 9.3.3 D3D9的Hack点    | 211 |
| 9.3.4 D3D9 Hook     | 214 |
| 9.4 本章小结            | 222 |
| 第5篇 外挂检测技术篇         |     |
| 第10章 外挂的检测方法        | 224 |
| 10.1 代码篡改检测         | 224 |
| 10.2 未授权调用检测        | 227 |
| 10.3 数据篡改检测         | 229 |
| 10.3.1 吸怪挂分析        | 229 |
| 10.3.2 线程转移和消息分流    | 230 |
| 10.4 本章小结           | 238 |
| 附录A 声明              | 239 |
| 附录B 中国计算机安全相关法律及规定  | 240 |
| • • • • • (收起)      |     |

[游戏外挂攻防艺术](#) [下载链接1](#)

## 标签

外挂

黑客

计算机

逆向工程

游戏开发

安全

信息安全

软件调试

## 评论

这书这么少人读？不对啊

随便看看，了解下大概，收货不大。

想对作者说一句：还我钱来！！全书读来感觉像大教授写的综述性论文，洋洋洒洒数百页，但对想写点外挂玩玩的读者而言没有任何帮助。

没有一定的领域基础看起来比较困难，好在这些都玩过，所以速度了一遍。  
gamespider那个外挂分析工具跟我做的某个工具有异曲同工之处。 seh  
veh硬件断点HOOK及检测异常访问的思路不错。

最后一章分析外挂用的线程转移+消息分发不是一个好的方法，可以用apimonitor来分析，或者构建一个沙盒环境来分析。

翻过

矛与盾从来都是没有输赢，只有更上一层楼。

这书写的挺好的，涉及的知识点很多，看完之后收获还是很大的。不过那些以为单看这本书就能做外挂的我也是呵呵了，你以为做个外挂这么容易？而且我也不相信没有windows编程，反汇编，操作系统知识背景可以把这本书看懂，这本书的目标对象应该是有以上的背景知识基础，但是对外挂不太了解的人，看完之后其实可以入门了。我之前看过一些C++反汇编，PE,数据加密解密的书，win32API，操作系统也比较熟悉，看完之后，就可以尝试写一些挂了，再找一些开源或者不开源的程序(反编译)看一看，就可以继续深入了。不过没有这些技术背景，那些想找一本宝典，轻松看完就能写一个外挂来玩玩的还是省省吧。

这样的书居然7.5分 3分左右很给面子了

[游戏外挂攻防艺术 下载链接1](#)

## 书评

这书写的挺好的，涉及的知识点很多，看完之后收获还是很大的。不过那些以为单看这本书就能做外挂的我也是呵呵了，你以为做个外挂这么容易？而且我也不相信没有windows编程，反汇编，操作系统知识背景可以把这本书看懂，这本书的目标对象应该是有以上的背景知识基础，但是对外挂...

[游戏外挂攻防艺术 下载链接1](#)