

<<游戏外挂攻防艺术>>

图书基本信息

书名：<<游戏外挂攻防艺术>>

13位ISBN编号：9787121195327

10位ISBN编号：7121195321

出版时间：2013-2

出版时间：电子工业出版社

作者：徐胜

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<游戏外挂攻防艺术>>

内容概要

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。

虽然很多游戏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。

<<游戏外挂攻防艺术>>

作者简介

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、R00tkn、防火墙和二进制逆向分析，And roid和iOS客户端软件安全，以及Web和WAP安全。

<<游戏外挂攻防艺术>>

书籍目录

第1篇 游戏和外挂初识篇第1章 认识游戏和外挂 21.1 游戏安全现状 21.2 什么是外挂 31.3 内存挂与游戏的关系 31.4 游戏的3个核心概念 51.4.1 游戏资源的加/解密 51.4.2 游戏协议之发包模型 111.4.3 游戏内存对象布局 161.5 外挂的设计思路 241.6 反外挂的思路 251.7 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 282.1 注册表注入 282.2 远线程注入 292.3 依赖可信进程注入 322.4 APC注入 342.5 消息钩子注入 362.6 导入表注入 392.7 劫持进程创建注入 482.8 LSP劫持注入 502.8.1 编写LSP 522.8.2 安装LSP 562.9 输入法注入 602.10 ComRes注入 66第3章 浅谈无模块化 673.1 LDR_MODULE隐藏 673.2 抹去PE“指纹” 743.3 本章小结 76第4章 安全的交互通道 774.1 消息钩子 774.2 替代游戏消息处理过程 814.3 GetKeyState、GetAsyncKeyState和GetKeyboard State 824.4 进程间通信 844.5 本章小结 89第5章 未授权的Call 905.1 Call Stack检测 905.2 隐藏Call 905.2.1 Call自定义函数头 915.2.2 构建假栈帧 995.3 定位Call 1075.3.1 虚函数差异调用定位Call 1075.3.2 send() 函数回溯定位Call 1105.4 本章小结 112第6章 Hook大全 1136.1 Hook技术简介 1136.2 IAT Hook在全屏加速中的应用 1156.3 巧妙的虚表Hook 1216.3.1 虚表的内存布局 1226.3.2 C++ 中的RTTI 1236.3.3 Hook虚表 1256.4 Detours Hook 1286.4.1 Detours简介 1286.4.2 Detours Hook的3个关键概念 1286.4.3 Detours Hook的核心接口 1306.4.4 Detours Hook引擎 1326.5 高级Hook 1476.5.1 S.E.H简介 1476.5.2 V.E.H简介 1486.5.3 硬件断点 1506.5.4 S.E.H Hook 1536.5.5 V.E.H Hook 1566.5.6 检测V.E.H Hook 1576.6 本章小结 159第7章 应用层防护 1607.1 静态保护 1617.2 动态保护 1657.2.1 反dump 1657.2.2 内存访问异常Hook 1697.3 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 1748.1 分析工具介绍 1748.1.1 GameSpider 1748.1.2 Kernel Detective 1788.2 定位保护模块 1788.2.1 定位ring0保护模块 1798.2.2 定位ring3保护模块 1798.2.3 定位自加载模块 1858.3 分析保护方案 1878.3.1 ring3保护方案 1878.3.2 ring0保护方案 1898.4 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 1949.1 自动开枪 1949.1.1 易语言简介 1959.1.2 易语言版自动开枪外挂 1959.2 反后坐力 1999.2.1 平衡Y轴法 1999.2.2 AutoIt脚本法 2009.3 DirectX Hack 2039.3.1 DirectX简介 2039.3.2 用Direct3D绘制图形 2099.3.3 D3D9的Hack点 2119.3.4 D3D9 Hook 2149.4 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 22410.1 代码篡改检测 22410.2 未授权调用检测 22710.3 数据篡改检测 22910.3.1 吸怪挂分析 22910.3.2 线程转移和消息分流 23010.4 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

<<游戏外挂攻防艺术>>

编辑推荐

网络游戏面临的头号安全威胁就是网络游戏外挂。

近些年来，信息安全技术研究领域的著作很多，但专门针对网络游戏安全研究的可谓凤毛麟角，而且基本上是以网络游戏外挂现象的揭示和平铺直述的文字为主，真正揭开现象背后的本质、讨论反外挂技术的著作还没有看到。

徐胜编著的《游戏外挂攻防艺术》一书填补了这方面图书的空白，首先揭示了网络游戏及其外挂的原理，然后通过代码实例罗列和盘点了网络游戏外挂的注入技术、无模块化隐藏技术、交互通信隐藏技术、函数调用隐藏技术、Hook技术以及游戏的安全保护，最后抛砖引玉，提出了外挂检测与防御的技术。

<<游戏外挂攻防艺术>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>