Technique and Defense for Hacker Mission About Trojan

本书列举74个问题详细告诉你黑客使用木马的各种手法与相对应的防护方式

希望 Beijing Hope Electronic Press www.bhp.com.cn

本书光盘包含：全球IP地址列表 / 端口列表 / TaskInfo/ Startup/ ASPack/ SyGate 个人防火墙 / Magic Mail Monitor/ ExeBinder/ PECompact/ EXE Stealth/ Angry IP Scanner/ IP Hacker/ VNN/ Optix Pro/ WinShell/ NTRootKit/ 黑客之门 / Protected Storage/ SuperScan/ NetBrute/ GetRight/ GetRight 中文版

Windows 黑客任务实战系列 程秉辉

— 黑客任务实战系列 —

# 木马防护全攻略

## [含恶意、间谍程序的攻击原理及防护]

北京希望电子出版社 总策划

程秉辉 John Hawke 合 著

* 许多木马并不会被杀毒软件所找出来，如何找出它们并彻底消灭
* 公开各种木马技巧与手法，让黑客无所遁形
* 针对木马入侵的各环节进行防护，使木马无法进入你的电脑
* 首度公开多种木马伪装易容术，彻底破解杀毒软件的盲区
* 木马植入、自动运行与藏匿技巧完全曝光
* 对多种类型木马进行专论研究，针对个别特性进行防护与破解
* 许多伪装的木马 Nortorn AntiVirus 与瑞星都无法抓出来，要怎么办？如何破解
* 杀毒软件抓不到、任务管理器没踪迹、系统服务看不到、网络连接看不出、隐藏IP无效…可穿过防火墙、仿真IP…
  第四代寄生嵌入式 DLL 木马彻底剖析、破解大公开
  …and More

**本书中所有实作都经过多次严格测试，绝不告诉你无法实现的方法！**

Internet 完全适用 局域网

科学出版社 www.sciencep.com

Technique and Defense for Hacker Mission About Trojan

本书列举74个问题详细告诉你黑客使用木马的各种手法与相对应的防护方式

本书光盘包含：全球IP地址列表 / 端口列表 / TaskInfo/ Startup/ ASPack/ SyGate 个人防火墙 / Magic Mail Monitor/ ExeBinder/ PECompact/ EXE Stealth/ Angry IP Scanner/ IP Hacker/ VNN/ Optix Pro/ WinShell/ NTRootKit/ 黑客之门 / Protected Storage/ SuperScan/ NetBrute/ GetRight/ GetRight 中文版

Windows 黑客任务实战系列 程秉辉

— 黑客任务实战系列 —

# 木马防护全攻略

## [含恶意、间谍程序的攻击原理及防护]

北京希望电子出版社 总策划
程秉辉 John Hawke 合著

* 许多木马并不会被杀毒软件所找出来，如何找出它们并彻底消灭
* 公开各种木马技巧与手法，让黑客无所遁形
* 针对木马入侵的各环节进行防护，使木马无法进入你的电脑
* 首度公开多种木马伪装易容术，彻底破解杀毒软件的盲区
* 木马植入、自动运行与藏匿技巧完全曝光
* 对多种类型木马进行专论研究，针对个别特性进行防护与破解
* 许多伪装的木马 Nortorn AntiVirus 与瑞星都无法抓出来，要怎么办？如何破解
* 杀毒软件抓不到、任务管理器没踪迹、系统服务看不到、网络连接看不出、隐藏 IP 无效…可穿过防火墙、仿真 IP…第四代寄生嵌入式 DLL 木马彻底剖析、破解大公开
…and More

**本书中所有实作都经过多次严格测试，绝不告诉你无法实现的方法！**

Internet 完全适用 局域网

科学出版社 www.sciencep.com

## 内 容 简 介

本书中我们公开了所有木马伪装易容的技巧与防护方式，也详细讨论木马可能藏匿的所有地方与自动运行的方法，本书最精华之所在就在于针对多个具代表性的木马进行详细完整的个案研究，仔细分析它们的运作方式与技术，然后找出相对应的防护之道，让你免除同类型木马的威胁，特别是寄生嵌入式 DLL 木马与反向连接技术，我们将彻底剖析它。

作者为中国台湾地区著名黑客和网络安全工作者，本书是作者长期工作与实践经验的倾情奉献。全书共 5 部分和一个附录组成，包括：木马概论,木马伪装术与破解,木马植入研究,自动运行与藏匿技巧,各类型木马专论剖析，附录为 IP 列表，端口列表，各种网络安全小工具的使用等内容。

本书光盘包括各种安全小工具，全球最新 IP 列表，端口列表等。

本书适合所有上网用户提高网络安全意识和安全性，也是专业网络安全人员不可缺少的参考。

**图书在版编目（CIP）数据**

木马防护全攻略/ 程秉辉，霍克（Hawke.J）著.—北京：科学出版社，2005

（黑客任务实战）

ISBN 7-03-015301-4

Ⅰ.木... Ⅱ.①程... ②霍... 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（2005）第 026894 号

责任编辑：大成 / 责任校对：李兴旺

责任印刷：双青 / 封面设计：梁运丽

科学出版社 出版

北京东黄城根北街16号

邮政编码:100717

http://www.sciencep.com

双青印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2005 年 6 月第 一 版 开本：787×960 1/16

2005 年 6 月第一次印刷 印张：31 1/4

印数：1-5 000 字数：561 330

**定价：42.00 元（配光盘）**

# 作者感言

在 Internet 成为许多人日常生活中的一部分之后，网络安全已经是每一位上网者所必须严肃面对的问题，然而大多数的个人 (包含许多公司、单位) 对于网络安全的态度都是很消极的，甚至等到灾害造成了才想办法解决，完全忽视预防重于治疗的重要性，因此让许多黑客有机可趁，而黑客技术也不断在精进，虽然各式杀毒软件、防火墙也不断的与魔斗法，然而所能达到的效果依然有限，木马要躲过杀毒软件的追杀、突破防火墙与仿真 IP 的限制已非难事，因此如何加强自己的防黑观念与知识便成为将黑客阻挡在门外的最有效方法，而这也是小弟呕心吐血撰写本书的最大目标。

经过一年多的努力这本木马防护全攻略终于与各位读者见面，由于之前已有不少读者来信询问本书何时出来，让小弟着实压力颇大，再加上木马技术的进步快速，各种不同毒性、不同功能的木马如雨后春笋般的出现，使得小弟遍尝百毒、穿肠破肚，好不容易才完工本书，让各位看到小弟用生命换来的研究成果，也才完成小弟的大愿。

本书中我们公开了所有木马伪装易容的技巧与防护方式，也详细讨论木马可能藏匿的所有地方与自动运行的方法，而本书最精华之所在就在于针对多个具代表性的木马进行详细完整的个案研究，仔细分析它们的运作方式与技术，然后找出相对应的防护之道，让你免除同类型木马的威胁，特别是**寄生嵌入式 DLL 木马**与反向连接技术，在本书中着墨甚多，而这也是目前最常见、最狡猾、最会隐藏的木马，所以小弟将它大卸八块，彻底剖析它，让你掌握它的一举一动，让它无法越雷池一步。

本书是使用传统章节与Q&A并用的方式来帮助你更快速的阅读、了解与使用本书，虽然我们力求完善与详尽，不过总会有遗珠之憾的地方，因此希望你能来信给我们批评与指教，帮助我们更加进步与完美，谢谢!!

照例若有任何问题与不解之处都可以来信询问，不过我们只能针对本书中内容的疑问来回答，而无法回答其他问题，请见谅!

请注意：

- 若您有使用电子邮件则填写**本书光盘中的读者服务卡**。
- 下一页读者资料卡中的电子邮件地址请写清楚，不要太草!

请电邮到: hawkes@ms29.hinet.net

程秉辉
*Hawke Cheng*

**请注意：本书内容完全以学理与技术实务的角度来针对有关黑客攻略与防护进行讨论与研究，所以若有将本书内容使用于任何违反法律之行为，必须自行承担各种相关的法律责任，请各位读者慎之！慎之！**

# 目 录

木马防护全攻略
黑客任务实战系列

## Part 1 木马概论 (Understand and Realize the Trojan)



## Part 2 木马伪装术与破解 (Disguise for Trojan and AntiTrojon)

## Part 4 自动运行与藏匿技巧 (Auto Execution and Hide Technique for Trojan)

# PART 1

## 木马概论

**Understand and Realize the Trojan**


黑客任务实战

木马防护全攻略

排困解难 DIY 系列


不可否认，Internet 绝对是改变世界与人类生活的重要功臣之一，然而就与所有的事物一样，它也有正反两面，正面是它带给大家更方便、更快速的完成你要做的事，而反面则是有被病毒破坏或黑客入侵的危险，而其中黑客利用木马入侵则又是其中最危险、最不可测，而且还可能造成重大损失与伤害，甚至让你痛不欲生、欲哭无泪…有那么严重吗? Yes! 的确是有可能会如此，甚至已经造成严重损害之后，被黑者却完全不知道是自己电脑中的木马程序在作怪…而让它继续的予取予求，所以除非你完全不上网，否则不论是一般的用户或是电脑专家，都有绝对的必要认识与了解木马，所以在 Part 1 中我们将与你讨论下列内容：

- 木马具有什么样的危险性? 与其他黑客入侵或攻击的手法有何不同之处? 能帮助黑客进行什么样的工作?
- 如何区分与了解各种不同类型的木马?
- 黑客如何选择、查找与获取木马的方式。
- 黑客利用木马入侵的流程。
- 针对木马入侵的各环节进行防护、阻挡与破解。

**Note**

由于许多网站的恶意或间谍程序 (Spyware) 的行为与木马没两样，只是搜集的数据不同而已，所以在本书中也将这类程序视为木马的一种。

**Q1** 木马具有什么样的危险性?

**Q2** 木马与其他黑客入侵或攻击的手法有何不同之处?

**Q3** 木马与一般病毒有何不同?它可以拿来做什么?

**Q4** 为何许多人很想做黑客?是因为什么样的心态与心理?

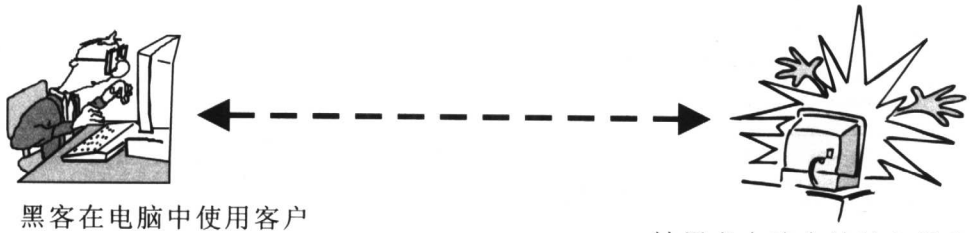
**Q5** 那种黑客最喜欢且善用木马?做黑客可以赚钱?

相关问题请见 Q6

相信各位都听过木马，也知道它是黑客使用的工具之一，但是它与一般病毒到底有什么不同呢?与其他黑客手法与行为又有何相异之处?它可以帮黑客做什么事?那一类的黑客特别喜欢使用木马?想要彻底防止木马入侵，当然就要对它有深入的认识与了解，所以在本问题中将与你详细讨论这些内容。

## ✍ 什么是木马?

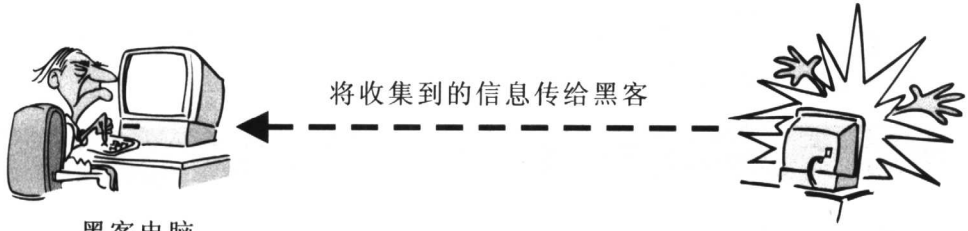
其实木马最主要的目标就是潜伏在被黑者的电脑中收集各式各样的资料，然后发送给黑客，通常木马可分为两种，一种是黑客可通过远程控制的方式来获取信息，木马就是植入被黑者电脑中的**服务端程序** (Server Program)，而黑客则使用**客户端程序** (Client Program)，这种多半是多功能的木马，如下图所示。



黑客在电脑中使用客户端程序 (Client Program)

被黑者电脑中被植入服务端程序 (Server Program)

另一种则是木马植入后，自行收集数据然后发送给黑客 (使用电子邮件、发送 MSN 或 ICQ 信息…等)，这种通常是特定功能的木马，如下图所示，在 **Q6** 中对于木马的区分、优缺点…有更深入的讨论。




黑客电脑

被黑者电脑中被植入木马

## ✍ 木马与病毒的不同之处

虽然许多人都将木马视为病毒的一种 (其实这是杀毒软件误导大家的错误观念)，但事实上两者是不一样的，而且有着很大的不同，下面就是病毒与木马正确的定义与说明：

- **病毒**－以各种可能的方法进入你的电脑中，造成软硬件的损坏、无法操作、不能启动、文件无法读取、某些功能不能使用…等各式各样的破坏行为，这样的程序就是病毒。

- **木马**－以各种可能的方法进入你的电脑中，造成某些文件被偷或被看

某些帐户与密码被窃、信件被偷看、一举一动被监视、收集各种信息…进行任何未经被黑者允许的行为，这样的程序就是木马，就好像电脑中有个内贼一般。

这样了解了吧?! 可以看出病毒完全针对电脑的软硬件…以破坏为主，然而木马却是像窃贼一般，到处翻箱倒柜，查看与偷走有价值的东西，就如同现实生活中的三只手，不过其中最大的差别是…三只手光顾之后通常很快就会被发现，但是木马却很可能一直躲藏在硬盘中的黑暗角落 (硬盘中有这样的地方吗?!)，默默的进行黑客工作，而被黑者却完全不知道它的存在。

所谓会叫的狗不咬人 (真的吗?!)，像木马这种不会叫的狗才是最可怕的，病毒的破坏最多重买硬件、重安装软件或系统、将备份数据还原…大概就完成了，而木马的破坏从个人隐私…乃至商业机密，甚至国家安全都有可能出现重大的伤害，小弟就曾经实验性的获取他人的电子邮件信箱帐户与密码、看过某旅行社内部的最低报价、某房屋中介的数据库…等，当然小弟对这些并没兴趣，所以看看就算了，不过有心者或同业竞争者看到这些东西，可就完全不一样了，后续可能造成的影响与伤害更难以预料，因此这也是小弟写本书的最主要原因，让大家更清楚、更深入的了解木马的可怕与危险，然后才能真正的对症下药，进行彻底有效的防护。

**Note**

木马当然也可以做到病毒的破坏行为 (视木马的功能而定，综合型的大多可以)，要看黑客是否要如此打草惊蛇的进行而已 (因为很可能会被被黑者发现)，所以广义的定义应该是：病毒是属于木马的一种，而不是将木马当成病毒的一种。


## ✍ 与其他黑客手法相异之处

在网络的世界中黑客入侵与攻击的方法有很多种，但类型不外乎是**直接入侵**、**外部攻击**与**木马潜伏**…这三种，其中木马潜伏在前面已经详细说明过了，因此下面说明另外两种：

- **直接入侵**－顾名思义当然就是直接进入被黑的电脑中，最常见的方法就是通过端口 139 入侵，也就是 Windows 直接入侵法，使用**资源管理器**就可以进入被黑者电脑中 (详细的说明与防护请见**黑客任务实战－Windows 全攻略 Part 3**，希望电子出版)；另一种则是利用漏洞 (如：Windows 系统漏洞或 IIS 漏洞) 入侵被黑电脑或服务器中 (**黑客任务实战－服务器攻防篇**有相关讨论)…两种方法都在入侵成功后，查看与偷取文件、运行程序、删除文件…等，当然也可植入木马程序，进行更多黑客任务。

> **Note**
>
> 并非成功入侵被黑者电脑就可为所欲为，必须视黑客所能获取的权限而定，若能获取系统管理员权限当然就无所不能，而这也是被黑者最大的梦魇。

- **外部攻击**－顾名思义就是通过网络直接 (或间接) 向被黑者发动攻击，最常见的就是数据包攻击，例如：对服务器最具威胁性的分布式拒绝服务攻击 (Distributes Denial of Service，简称 DDoS)，让被黑服务器无法提供服务 (例如：无法浏览)，若被攻击的是股票、期货、外汇交易的服务器，当然就会造成重大影响与伤害，有关更详细的讨论与研究见**防黑防毒全攻略 Q95**。