The Bible of Hacking and AntiHacking About Trojan

# 黑客技术攻防擂台

Vista/XP/2K
完全适用

# 木马任务大作战

木马是黑客入侵的高段手法，积极洞悉木马攻击伎俩，让黑客无所遁形！

光盘内附
16套木马攻防工具

- 让各大杀毒软件颜面尽失的木马伪装易容术
- 不会写程式也能设计出自己的专属木马
- 杀毒软件永远无法追杀的木马与帮凶工具——有效防护
- 浏览网页或播放多媒体文件就中木马——操作剖析与防护
- 黑客如何利用后门随时进出使用动态 IP 的电脑
- 所有杀毒软件无法追杀的 Windows 后门木马——详细操作与防护
- 木马或帮凶工具如何让防火墙与杀毒软件无效？如何防护
- 突破传统木马无法用於虚拟 IP 电脑的反向连接木马——有效阻挡
- 杀毒软件不追杀、防火墙不阻挡偷取各类密码的超强木马——防护阻挡
- 使用一般的软件或小工具就能制造组合各类木马——黑客发展之道……更多木马攻防密技研究与实现

北京希望电子出版社　总策划
程秉辉　John Hawke　合　著

科学出版社
www.sciencep.com

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

The Bible of Hacking and AntiHacking About Trojan

# 黑客技术攻防擂台

# 木马任务大作战

木马是黑客入侵的高段手法，积极洞悉木马攻击伎俩，让黑客无所遁形！

光盘内附
6套木马攻防工具

- 让各大杀毒软件颜面尽失的木马伪装易容术
- 不会写程式也能设计出自己的专属木马
- 杀毒软件永远无法追杀的木马与帮凶工具——有效防护
- 浏览网页或播放多媒体文件就中木马——操作剖析与防护
- 黑客如何利用后门随时进出使用动态 IP 的电脑
- 所有杀毒软件无法追杀的 Windows 后门木马——详细操作与防护
- 木马或帮凶工具如何让防火墙与杀毒软件无效？如何防护
- 突破传统木马无法用於虚拟 IP 电脑的反向连接木马——有效阻挡
- 杀毒软件不追杀、防火墙不阻挡偷取各类密码的超强木马——防护阻挡
- 使用一般的软件或小工具就能制造组合各类木马——黑客发展之道……更多木马攻防密技研究与实现

北京希望电子出版社　总策划
程秉辉　John Hawke　合　著

科学出版社
www.sciencep.com

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

## 内 容 简 介

这是一本基于病毒、木马攻击与防护技术的系统安全图书。

网络安全问题层出不穷，千万不要因为缺乏准备的头脑而成为下一个替罪羔羊！在来自 Internet 安全领域的战争中，木马攻防是其重要战场之一。高深的网络与系统技术一直是兵家必争之地，本书将彻底颠覆传统观念，独家公开黑客内幕，你不必潜心钻研高深的网络与系统技术，甚至不需要学习程序设计知识，也无须具备诸多常识或经验，只要使用一般的软件及工具，就能够轻松设计出让防毒软件不追杀、防火墙不阻挡……同时具有多种功能的木马。或者让设计不周到的木马或小工具如虎添翼、更加完美，使众多防黑杀毒软件厂家惊慌失措、疲于奔命……将黑客历史的发展推向一个崭新的境界！

本书作者竭尽所能、挖空心思，用尽一切创意和想象，将黑客制作与组合出这类木马的完整过程呈现给大家，同时针对各种木马的弱点提出相应的有效防护办法，希望能够在众多杀毒软件束手无策的情况下，让广大用户走出木马的威胁与阴影，这便是本书的意义和价值所在。

本书适合每位 Windows 联网用户以及各类网络办公企业。同时也适合 Windows——特别是 Vista 和操作系统 DIY 爱好者，更是诸位黑客狂想者的练兵演习的习武之地。

光盘内容为书中所用部分软件工具的安装程序。

**图书在版编目（CIP）数据**

黑客技术攻防擂台—木马任务大作战 / 程秉辉　Jonh Hawke 合著. —北京：科学出版社，2008

ISBN 978-7-03-021803-2

Ⅰ. 黑…　Ⅱ. ①程… ②J…　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（2008）第 060668 号

责任编辑：但明天　/责任校对：全　卫
责任印刷：双　青　/封面设计：康　欣

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

*

2008 年 6 月第　一　版　开本：787×960 1/16
2008 年 6 月第一次印刷　印张：29 1/4
印数：1—5000　字数：535 200

**定价：48.00 元（配 1 张光盘）**

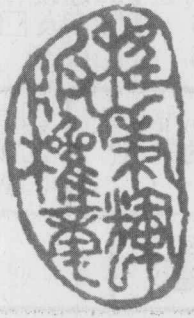
# 作者感言

所谓长江后浪推前浪、一代新人换旧人，在网络安全的战争中，魔与道似乎也不断地在依循此方式进行永无止境的争斗，而木马攻防更是其中主要的战场之一，在传统上高深的网络与系统技术一直是兵家必争之地，然而天有不测风云、电脑也有旦系祸福(是这样吗!?!)，某些黑客回归自然，不再努力钻研高深的技术与刁钻的方法，改用**一般唾手可得的各种工具就能制造组合出多种类型的木马**，让众杀毒软件厂商惊慌失措、疲於奔命……也将黑客历史的发展推向另一个里程碑。

这种旧瓶装新酒的做法并没有什么高深难懂的技术，相反地，反而是再简单不过的东东，重点在于创新与发挥想像力，就如同许多化学物质一般，两个无毒的东西混在一起就变成剧毒……就是这种旧瓶新酒木马最贴切的描述。所以在本书中，小弟竭尽所能、挖空心思，用尽一切的创意与想像，终于将黑客制作与组合出这类木马的完整过程呈现在大家的眼前，并针对各种类型木马的弱点提出相关的有效防护，希望能在众家杀毒软件束手无策之外，让广大的网民能够走出此类木马的威胁与阴影，这也是小弟写本书最主要的意义与目的。

虽然本书内容已经包含目前大多数木马技术的攻防，不过并不能也不想涵盖其他黑客攻防主题，所以有兴趣的读者可以参考小弟的另一本书——**黑客任务大作战**，与本书合并研读相信就可以打通任督二脉，彻底了解与掌握黑客的各种行为，如此才能让你的电脑远离各种威胁与伤害。

请填写**本书光盘中的读者服务卡**或
下一页的读者资料卡，然后发
E-mail 到: hawkegg@gmail.com



程秉辉
*Hawke Cheng*
*2008.4.7*

**请注意：本书内容完全以学习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！**

请将下表数据填妥后E-mail到 **hawkegg@gmail.com**
我们将会不定期地提供你有关各种Windows、Internet与多媒体的最新信息与相关软件，请多多利用，谢谢！
你也可以到我们的网站: **http://www.faqdiy.cn/**上来获得相关的更新文件与最新信息!!


**若你有使用电子邮件，则请使用本书光盘中所附的读者服务卡，不必使用这个读者服务卡。**

## 讀者服務卡 REGISTER CARD

| | | | | | |
|---|---|---|---|---|---|
| 书名 | 木马任务大作战 | | 本书序列号 | 北京希望2K80501 | |
| 姓名 | | 性别 | ☐先生 ☐小姐 | 年龄 | |
| 学历 | ☐硕士 ☐学士 ☐大专 ☐高中职 ☐初中 ☐小学以下 | | | | |
| 你的电邮地址 | | | | | |
| 传真号码 | | | | | |
| 购买地区(选择最近城市) | ☐北京 ☐上海 ☐南京 ☐广州 ☐深圳 ☐武汉 ☐重庆<br>☐成都 ☐福州 ☐天津 ☐大连 ☐南昌 ☐苏州 ☐杭州<br>☐青岛 ☐长沙 ☐开封 ☐合肥 ☐哈尔滨 其他: _____ | | | | |
| 职业 | ☐学生 ☐电脑业或IT部门<br>☐非电脑业 ☐其他: _____ | | 您觉得本书 | ☐简单<br>☐适中 ☐艰深 | |
| 使用Windows时常遇到什么样的的困扰与麻烦? | | | | | |
| 你从何处知道本书 | ☐连锁书店 ☐一般书店 ☐电脑专卖店 ☐同学 ☐展览<br>☐亲友 ☐广告函 ☐因特网 ☐报纸: _____<br>☐杂志: _____ ☐其他: _____ | | | | |
| 你还需要哪些方面的书籍? | ☐其他Windows排困解难 ☐黑客攻防研究<br>☐防黑防毒 ☐网页设计排困解难 ☐Java语言设计<br>☐Windows程序设计(MFC,SDK) 其他: _____ | | | | |
| 你对本书有何建议 | | | | | |

# 目 录


木马任务大作战

## Part 1 什么是木马 (Understand and Realize the Trojan)



## Part 2 木马伪装与破解 (Disguise Trojan and Break It)

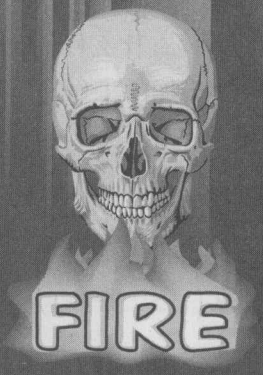
## Part 3 诱骗技巧与运行木马 (Execution and Defense about Trojan)

## Part 5 各类型木马专论剖析 (Study and Defense for Trojans)

# PART 1

## 什么是木马

**Understand and Realize the Trojan**




木马任务大作战

菲因解难 DIY 系列


# 木马任务大作战

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，而黑客利用木马入侵则是其中最危险、最不可测的事情，而且还可能造成重大损失与伤害，甚至让你痛不欲生、捶胸顿足、欲哭无泪……有那么严重吗? Yes! 的确可能会如此，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在作怪……而让它继续的予取予求，所以除非你完全不上网 (包含局域网)，否则不论是一般的用户或是电脑专家，都绝对有必要深入认识与了解木马的种种，所以在本章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?
- 区分与了解各种不同类型的木马与木马的发展。
- 黑客选择、查找与获取木马的方式。
- 黑客利用木马入侵的流程。
- 针对木马入侵的各个环节进行防护、阻挡与破解。

1 什么是木马、恶意或间谍程序、后门程序、跳板程序、病虫？它们有什么样的危险性？

2 使用木马与其他黑客入侵或攻击的手法有何不同之处？

3 木马与一般病毒有何不同？它可以拿来做什么？

4 为何许多人很想做黑客？是出于什么样的心态与心理？

5 哪种黑客最喜欢而且善用木马？做黑客可以挣钱吗？

相关问题请见 Q6

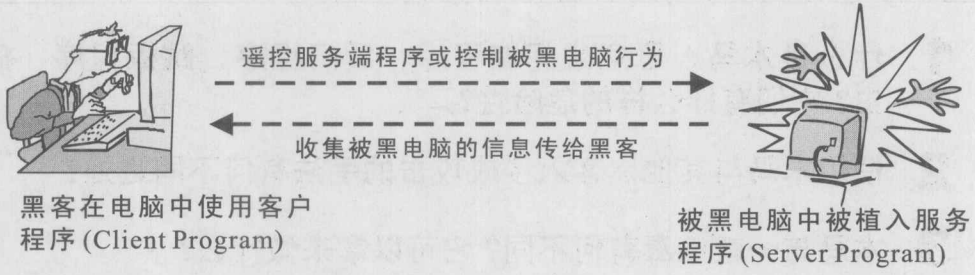
相信各位都听过木马，也知道它是黑客使用的工具之一，但是它与一般病毒到底有什么不同呢？与其他黑客手法与行为又有何相异之处？它可以帮黑客做什么事？哪些黑客特别喜欢使用木马？想要彻底防止木马入侵，当然就要对它有深入的认识与了解，所以在本问题中将与你详细讨论这些内容。

## 什么是木马、恶意或间谍程序、后门程序、跳板程序、病虫？

不论是木马、恶意源码、间谍程序、后门程序、跳板程序、病虫等，其实广义上说都可以统称木马，因为都是潜藏在被黑电脑中进行各种活动，而依照它的行为而出现许多种不同的名称，例如：间谍程序、后门程序、跳板程序、病虫、僵尸程序、傀儡程序、键盘侧录程序、桌面监控程序等等。

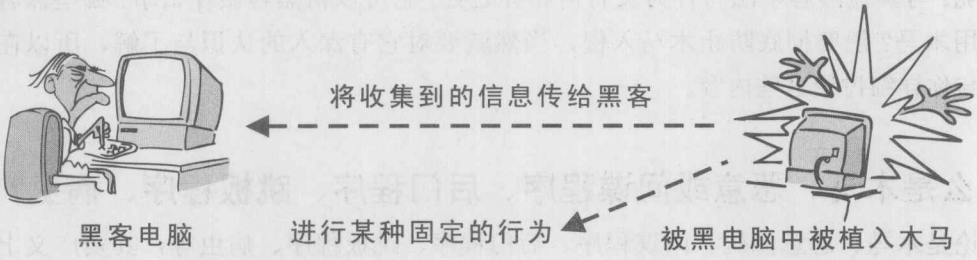
木马最主要的目标就是潜伏在被黑电脑中进行各式各样黑客指定的工作，从连接的行为上可将木马分为两类：一类是黑客可通过远程控制的方式来获取被黑电脑中的信息或控制被黑电脑的行为，木马就是植入被黑电脑中的**服务程序** (Server Program)，而黑客则使用**客户程序** (Client Program) 对伺服端程序进行远程遥控操作，如下图所示。


## 木马任务大作战




这类木马最典型的就是多功能木马，例如：Sub7、Back Orifice、Optix PRO等，另外跳板程序、对黑客指定的服务器进行拒绝服务攻击……也都可以算是此类木马。

另一类木马则是属于单兵作业，它会自行收集某些数据并传给黑客或控制被黑电脑进行某种行为 (如：打开后门、自动查找与感染其他电脑等)，可算是特定功能的木马，例如：恶意或间谍程序、傀儡或僵尸程序、后门程序、病虫、键盘记录软件、桌面监控程序、MSN 木马等，如下图所示。




**Note**

在 **Q6** 中会对种木马的区分、优缺点……做更深入的讨论。

### 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、某些账户与密码被窃、信件被偷看、一举一动被监视、收集各种信息、控制被黑电脑的行为等，进行任何未经被黑者允许的行为，这样的程序就是木马，就好像电脑中有一个内贼一般。

这样理解了吧?! 你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，或将被黑电脑当成代罪羔羊，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?!)，默默地进行黑客工作，而被黑者却可能完全不知道它的存在。

所谓会叫的狗不咬人 (真是这样吗?!)，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，至商业机密，甚至国家安全都有可能出现重大的伤害。小弟就曾经实验性地获取他人的电子邮件信箱账户与密码、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是难以预料，因此这也是小弟写本书的最主要原因，让大家更清楚、更深入地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**

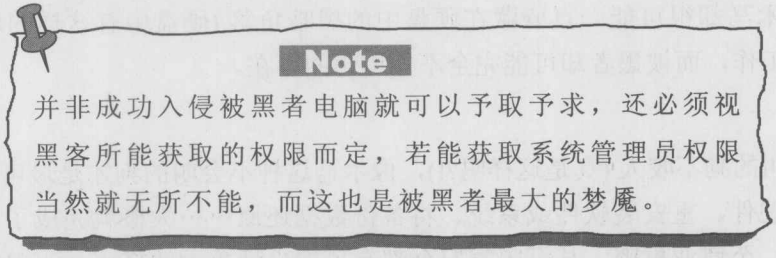
木马当然也可以实现病毒的破坏行为 (视木马的功能而定，综合型的大多可以)，要看黑客是否要如此打草惊蛇地进行而已 (因为很可能会被被黑者发现)，所以广义的定义应该是：病毒是属于木马的一种，而不是将木马当成病毒的一种。


# 木马任务大作战

## 与其他黑客手法相异之处

在网络世界中，黑客入侵与攻击的方法有很多种，但主要类型不外乎是直接入侵、外部攻击与木马潜伏这 3 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者的电脑中，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 (详细的说明与防护可参见**黑客任务大作战 Part 3**)；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。两种方法都是在入侵成功后，查看与偷取文件、运行程序、删除程序等行为，当然也可植入木马程序，进行更多黑客任务。




- **外部攻击**——顾名思义就是通过网络直接 (或间接) 向被黑电脑发动攻击，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、研究与操作请见**黑客任务大作战 Q137**。

不过在许多情况下，黑客会综合运用多种方式，而非只使用单一方法，例如：要成功植入木马，黑客可能先进行直接入侵成功后再将木马植入，以后就使用木马进行黑客任务。另外若要集合众电脑之力对被黑服务器进行 DDoS 攻击，可能必须先要将攻击程序植入许多代罪羔羊服务器中，然后设置同一时间对被黑服务器进行 DDoS 攻击——也就是说，许多黑客任务都是综合运用多种方式与技巧完成的，并非仅靠单一方法就可成功，因此我们的黑客防护当然也是全面性的，不能只针对某种类型或某个方法进行防护就认为可以高枕无忧了。

## ✍ 木马可以帮黑客做什么事?

其实在前面两节的讨论中你大概也可以看出木马可以帮黑客做什么事情，当然最主要的还是决定于黑客想要获取什么东西。例如，若是同行竞争，当然就是想要获取被黑者的业务机密或公司数据；若是情报间谍，当然就希望获取有用的国家机密或信息；若是入侵好友电脑，当然就是想知道更多对方的隐私与秘密——也就是说木马只负责获取数据与收集信息，要如何判断与使用或是有进一步的行动，那就是黑客自己的事情了，因此对被黑者会造成怎样的影响与伤害是很难预估的，所以不怕一万、只怕万一，在木马的防护上预防是远比事后治疗来得重要。

### 讨论与研究 (反制黑客)

由前面的说明你可以了解，其实黑客利用木马就如同间谍偷取情报一样，只是间谍这个角色由人变成了木马而已。既然如此，现实生活中有所谓的反间计，应该也可以使用在这里啰?! 没错，当你发现不幸有木马在电脑中，而且并不知道它已经存在多久，则先不删除它，尽快将各种重要的文件与数据搬移到安全的磁盘或其他电脑中，然后花点时间监视它到底在查找哪方面的文件或数据，然后给它假的。由于黑客不容易判断所获取数据的真假，因此黑客使用假的数据再进行下一步行动当然就会错误，就达到反间计的效果。不过这应该是知易行难的，大多数人发现木马都唯恐杀之不及，哪还可能会施行反间计呢?!

## ✍ 喜欢使用木马的黑客 (职业黑客)

基本上由于木马这个内贼的角色，所以大概没有不喜欢使用木马的黑客，也因为它间谍般的特性，造成另类非法行业的出现——代客入侵的职业黑客。也就是说，帮客户入侵指定的电脑或服务器，获取客户所需要的文件或信息，然后收取费用 (在中国大陆已有黑客在网站上公开招揽客户)，虽然这在许多国家都是违法的，但是若黑客的技巧高超、被黑电脑是在国外、或是被黑电脑所在国家并没有相关法律规定……则还是可以成功的，也因此造成全世界出现不少职业黑客，甚至出现网络勒索集团。2004 年，美国有一个在线赌博网站 (在美国是合法的) 被网络勒索集团攻击到无法营业，最后付款 100 万美元才解决了事，像这类新形态的 Internet 网络犯罪日趋严重，亟需各国政府的相互合作来防止，只是各国在各种不同利益与政策考虑下，对这类跨国网络犯罪能有多少拦阻作用就有待考验。