

## <<黑客任务之华山论木马>>

### 图书基本信息

书名：<<黑客任务之华山论木马>>

13位ISBN编号：9787030259004

10位ISBN编号：7030259009

出版时间：2010-1

出版时间：程秉辉 科学出版社，北京希望电子出版社 (2010-01出版)

作者：程秉辉

页数：379

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>

## <<黑客任务之华山论木马>>

### 内容概要

《黑客任务之华山论木马》深入剖析与讨论10种最常见组合式木马，以木马软件的基本原理和技术为中心，用实例说明相关问题，并针对各种不同组合式木马的特性提出相对应和有效的防护之道。

《黑客任务之华山论木马》以配图、图释、标注、指引线框等丰富的图解手段，辅以浅显易懂的语言，通过对黑客攻击计算机的一般方法、步骤，以及所使用的工具的全面剖析，进而详细地讲述了防御黑客攻击的方法，并对入侵过程中常见问题进行必要的说明与解答。

全书共分为8章，包括：木马发展、何为组合式木马、木马的植入与运行、组合式木马的主架构与设计、各类账户密码木马攻防、信件与交谈日志木马攻防、后门木马攻防和重要、机密、隐私文件木马攻防。

《黑客任务之华山论木马》内容丰富、图文并茂、深入浅出，不仅适用于广大网络使用者，而且适用于网络安全从业人员及网络管理员。

## <<黑客任务之华山论木马>>

### 作者简介

程秉辉，大学毕业后就无所事事、逐水草而居。

精通汇编、C、Windows、API与Windows系统有十多年的奋斗经验与深刻了解，与微软的爱恨情仇更是生命中的转折点。

从事写作至今十余年，发表过近百篇杂志文章，两岸三地共出书四十余本，Windows排困解难与黑客任务实战系列是许多读者所熟知的作品。

## &lt;&lt;黑客任务之华山论木马&gt;&gt;

## 书籍目录

第1章 反璞归真——自然是最佳的保护1-1木马发展故事1-1-1 传统EXE程序文件木马1-1-2传统DLL / VXD木马1-1-3替换挂钩式DLL木马1-1-4注入式DLL木马1-1-5 最简单、方便的方式制作木马1-2高深的技术——优点、盲区?1-3魔与道的回潮战争——半吊子黑客的光明大道?1-4最安全的软件最危险?1-5 本书的设计与阅读方式第2章 工欲善其事，必先利其器Q1 何谓组合式木马(Combination Trojan)?Q2 黑客如何选择使用简单、自然、方便的工具设计木马?Q3 不会编程(或编程经验不多)的黑客会选择什么工具设计木马?Q4 不必写程序也能设计木马吗?如何实现?Q5 使用安装生成工具设计木马对黑客有哪些优缺点?Q6 黑客是如何选择最适合的安装生成工具设计木马的?Q7 安装生成工具如何避免被黑客利用设计成木马?Q8 黑客是如何利用MS-Office文件(.mda、.xls、.doc、.ppt等)或HTML文件设计木马或恶意源码的?Q9 如何有效防止MS-Office文件或HTML文件被黑客利用设计成木马或恶意源码?第3章 木马的植入与运行Q10 黑客通常使用哪些方法将木马植入被黑电脑中运行?其特点是什么?Q11 黑客通常利用哪些借口、管道与方式诱骗被黑者下载(或保存)木马后运行它?如何防范?第4章 组合式木马的主架构与设计Q12 组合式木马的主要架构应该具备哪些功能?Q13 黑客如何利用安装生成工具设计出组合式木马的基本架构?Q14 黑客如何选择适合的借口搭配所播放的多媒体文件(如影片、动画、Flash小游戏或音乐)诱骗被黑者运行组合式木马?Q15 黑客如何在组合式木马中设计播放多媒体文件(如影片、动画、Flash小游戏或音乐)诱骗被黑者观看?Q16 黑客如何查找与获取被黑者有兴趣的多媒体文件(如影片、动画、Flash小游戏或音乐)?Q17 黑客如何在组合式木马中加入真正可使用的某种功能诱骗被黑者使用?如何有效防范?Q18 黑客如何将组合式木马设计成Windows系统修补工具?如此不仅可以真的修补漏洞还有机会使木马更广泛地流传。

如何防范?Q19 除了用Windows系统修补工具加入木马外，黑客还常利用哪些功能诱骗被黑者?Q20 黑客如何设计木马每次进入Windows就自动运行?Q21 黑客会将木马自动运行设置在哪些地方?如何找出来删除与防护?Q22 黑客如何让木马不必一直运行却可以经常进行黑客任务?如此就不容易被熟悉系统的被黑者发现。

Q23 黑客如何决定木马在被黑电脑中是否要一直运行，或是在特定的日期与时间才运行?如此可降低被发现的概率第5章 各类账户密码木马攻防Q24 大多数人的电脑中保存有哪些用户名与密码?保存在什么地方?黑客会用什么方法获取?Q25 若用户名与密码没有保存在被黑电脑中，黑客又如何获取?Q26 黑客如何设计获取各种拨号上网用户名与密码(如电话拨号上网账户、ADSL上网账户等)的木马?如何有效防护?Q27 黑客使用什么方法获得木马在被黑电脑中获取的各种信息或文件?Q28 若组合式木马或配合的小工具被杀毒软件查杀，黑客会用哪些方法躲避?Q29 黑客如何设计获取各种电子邮件软件(如Windows Mail、Outlook、Outlook Express，Thunderbird，Hotmail / MSN mail，Gmail，Eudora等)所保存邮箱账户与密码的木马?如何有效防护?Q30 黑客如何不留痕迹地获取被黑者在收信服务器中还未读取的信件?如何有效防护?Q31 黑客如何设计获取实时通信软件(如Windows Live Messenger、MSN、雅虎通、Google Talk、ICQ Lite等)登录账户密码的木马?如何有效防护?Q32 获取被黑者的实时通信软件账户密码后，黑客会进行哪些工作?Q33 我希望使用实时通信软件可以自动登录，又希望不被组合式木马获取密码，要如何实现?Q34 黑客如何设计木马获取IE浏览器所保存进入某些网页的账户与密码(如网络银行、各种网上交易、各种网站会员、网络游戏、Web-Mail等)?如何有效防护?Q35 黑客如何设计木马获取被黑者登录其他电脑的账户与密码(通常是通过端口)?如何有效防护?Q36 黑客如何获取IE自动完成功能所保存的各种用户名与密码?如何彻底防护?Q37 黑客如何找出被黑电脑最近浏览过哪些网站?然后利用这些信息分析找出某些账户密码。

Q38 我不使用IE浏览器，为何有些账户密码也会被黑客窃取?如何防范?Q39 若黑客使用密码寻回工具组合的木马无法找出被黑者实时通信软件(如Windows Live Messenger、MSN、雅虎通、Google Talk、ICQ Lite等)的账户密码，还会使用什么方法找出来?Q40 若黑客无法从IE自动完成信息与Cookies信息中找出某个(或某些)用户名与密码(如无名相簿密码、上网账户、网络银行账户、游戏账户、Web-Mail邮箱账户、进入某个网页的会员账户等)，还会使用什么方法找出来?Q41 若黑客不可用密码寻回工具找出邮箱用户名与密码，还会使用什么方法找出来?Q42 黑客如何在他人电脑中设置按键监控工具获取各种用户名与密码?如何不被杀毒软件发现?如何有效防护?Q43 黑客利用账户密码寻回工具只找出

## <<黑客任务之华山论木马>>

某个账户的名称却没有密码，会再使用什么方法找出密码?：第6章 重要机密、隐私文件木马攻防Q44  
黑客如何利用一般的设计软件(如安装生成工具)，不必认真编写程序也不需要配合其他工具，就能设计出窃取他人电脑中任意文件(如.doc、.xls、.mda、.ppt、.pdf,各种影片或音频文件等)的木马!而且不会被杀毒软件查杀。

如何对这类木马进行有效防护? Q45 如何设计出可依照黑客指示进行查找与窃取被黑电脑中的某个或某些文件?Q46 被黑电脑中可能有许多有价值的文件，黑客如何不留痕迹、一点一滴地窃取?Q47 木马可能植入两台或更多被黑电脑中，黑客要如何设计木马依据不同的被黑电脑进行不同的查找与窃取文件?Q48 对于被黑电脑中的大文件(通常是多媒体文件)，黑客要如何加快上传速度，如此才容易窃取文件?.....第7章 信件与交谈记录木马攻防第8章 后门木马攻防

## <<黑客任务之华山论木马>>

### 章节摘录

插图：在网络安全战争中，木马是主要战场之一，因此魔与道两方都努力向前发展，希望能保持领先地位。

本书是要详细讨论有关木马的发展与演变方向，从而了解最新木马的设计与弱点，然后可以对症下药进行有效防护。

在本章中我们先来了解有关木马的发展概况，魔与道彼此的竞争与演变，最后分析黑客以最简单、方便的方式设计木马的想法与原因。

1—1 木马发展故事所谓木马（指木马病毒程序，本书简称为“木马”）是指黑客将具有某种特定功能（如窃取某个账户与密码，或者窃取文件与打开后门）的程序放到被黑（指被病毒感染）电脑中运行，在被黑者不知道的情况下非法盗取他人账户密码等。

这样的程序被称为木马程序（取自希腊神话中特洛伊木马典故）。

可以看出，木马程序的目的是侵犯他人的隐私权，因此木马的设计者的目标之一是不被发现，这样它就能在被黑电脑中安稳、长久、顺利、默默地进行它的工作。

由此可知，木马攻防战的胜负取决于是否被发现。

若木马程序被被黑者或杀毒软件发现（通常是后者），肯定难逃“一死”，对黑客而言就是任务失败；反之若没被发现，黑客任务成功 $2/3$ ，只要再躲过防火墙的阻挡，那么木马任务几乎可以算是完全成功。

正因为如此，木马程序的发展重点一直是在逃过杀毒软件的查杀与躲过防火墙的阻挡。

木马技术大致是依循如下所示的流程发展演变的。

## &lt;&lt;黑客任务之华山论木马&gt;&gt;

## 编辑推荐

《黑客任务之华山论木马》详细讨论、实作与应用10种不同功能的组合式木马与有效防护全球唯一组合式木马设计与全面防护圣经杀毒软件无法追杀的组合式木马设计宝典深入浅出了解、设计、实现组合式木马与全面防护一般小软件，Windows本身就能轻易设计出各种组合式木马组合式木马的植入与执行可接受黑客指示进行工作的组合式木马攻防重要、机密、隐私档案的木马攻防信件与聊天记录的木马攻防.....更多组合式木马应用、设计与技巧电脑与网络安全的战争中，木马是重要的主战场之一，木马与杀毒软件不断地在技术较量中相互促进，不过《黑客任务之华山论木马》彻底颠覆传统观念。独家公开黑客内幕。

不必钻研最新与高深的网络和系统技术，也不需要深厚的程序设计功力，更不必积累大量的知识与经验，只要使用一般的软件或小工具（甚至只使用Windows提供的工具）就能轻易地设计出杀毒软件无法查杀、防火墙不阻挡等各种不同功能，甚至接受黑客指示来进行工作的组合式木马（Combination Trojan），使众多杀毒软件厂商惊慌失措、疲于奔命...也将木马攻防的发展推向一个新的里程碑。

设计与使用上简单、方便、迅速的组合式木马已快速成为网络与电脑安全的最大威胁，由于杀毒软件对它无可奈何，更使得它快速流窜、横行无阻，《黑客任务之华山论木马》作者从黑客的内心深处，竭尽所能、挖空心思，用尽一切的创意与想象，将黑客制作与组合出各类木马的完整过程呈现在大家的眼前，并针对各种组合式木马的弱点提出相应的有效防护之道，希望能在众家杀毒软件束手无策时，能让广大的网民们远离组合式木马的威胁，这也是《黑客任务之华山论木马》最大的意义与价值所在。

第1章 返璞归真——自然是最佳的保护第2章 工欲善其事必先利其器第3章 木马的植入与执行第4章 组合式木马的主架构与设计第5章 各类账户密码木马攻防第6章 重要、机密、隐私档案木马攻防第7章 信件与交谈记录木马攻防第8章 后门木马攻防

<<黑客任务之华山论木马>>

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>