

## <<木马防护全攻略>>

### 图书基本信息

书名：<<木马防护全攻略>>

13位ISBN编号：9787030153012

10位ISBN编号：7030153014

出版时间：2005-6

出版时间：科学

作者：程秉辉,John Hawke

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>

## <<木马防护全攻略>>

### 内容概要

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，本书是作者长期工作与经验的倾情奉献。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。

## <<木马防护全攻略>>

### 书籍目录

Part1 木马概论(UnderstandandRealizetheTrojan) 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？

Q6 木马有哪几种类型？

如何区分？

各有何优缺点？

Q7 如何针对不同类型木马的特性来找出可能隐藏在电脑中的不速之客？

Q8 木马技术在发展与演变上是如何进行？

分成那几个阶段？

各使用什么样的技术？

Q9 黑客利用木马入侵流程为何？

Q10 如何针对木马入侵的各环节进行防护、阻挡与破解？

Q11 黑客如何选择、查找与获取所要使用的木马？

Q12 有那些方法可以防止黑客查找与获取所想要的木马？

有何优缺点？

Part2 木马伪装术与破解(DisguiseforTrojanandAntiTrojan) 木马伪装技术的演变 木马伪装测试流程 不必伪装的木马 木马伪装易容术 测试伪装的木马 Q13 黑客为何要伪装木马程序？

Q14 什么情况或条件下黑客不需要伪装木马，而且还可以名正言顺的叫被黑客者运行？

Q15 为什么遥控软件也可以当木马？

为何它比真正的木马更容易成功？

Q16 为何许多木马无法被杀毒软件找出来？

是什么原因？

Q17 有那些方法可以找出杀毒软件无法找到的木马？

Q18 黑客使用那些方法来伪装木马？

有何优缺点？

Q19 如何找出伪装的木马后将它斩首？

Q20 黑客如何检验伪装后的木马？

有何盲区与注意之处？

Q21 同一个伪装后的木马，为何有的杀毒软件找得出来，有些却没发现？

这是什么原因？

Q22 黑客可能设计出任何杀毒软件或网络防护程序都无法找出来而且永久有效的伪装方式吗？

Part3 木马植入研究(TrojanImplantationandDefense) Q23 黑客常使用那些方式将木马植入被黑者电脑中？

各有何优缺点？

Q24 黑客通常使用那些方式直接进入被黑者电脑中，然后植入木马？

各有何优缺点？

如何防护？

Q25 我未接收邮件，也未下载任何网络程序，只是上网就被植入木马？

这是什么原因？

如何防范？

## <<木马防护全攻略>>

Q26 我使用最新的杀毒软件，也有防火墙，从不下载或运行任何网络上东西，也经常修补系统与各种网络程序的漏洞，为何还是被植入木马？

这是什么原因？

如何防范？

Q27 黑客如何利用电子邮件将木马植入被黑者电脑？

有那些方式？

各有何优缺点？

如何阻挡？

Q28 什么是电子邮件钓鱼？

黑客如何利用它来将木马植入被黑者电脑与运行它？

如何防护？

Q29 黑客会使用那些说法或借口欺骗被黑者接受木马程序，然后运行它？

Q30 什么是网站钓鱼？

黑客如何利用它来将木马植入被黑者电脑与运行它？

如何防护？

Q31 黑客如何利用P2P软件（例如：文件下载、实时通讯...等）、免费软件、共享软件与注册破解程序...等将木马植入被黑者电脑与运行它？

如何防护？

Part4 自动运行与藏匿技巧(AutoExecutionandHideTechniqueforTrojan) Q32 黑客会使用那些方法让植入的木马自动运行？

流程为何？

Q33 黑客有那些方法让植入的木马立该运行？

各有何优缺点？

如何防护？

Q34 黑客如何使用at命令运行被黑者电脑中的任何程序？

如何防护？

Q35 黑客如何使用net命令来运行被黑者电脑中的木马？

如何防护？

Q36 木马如何设置每次启动进入Windows就自动运行？

Q37 黑客植入的木马程序都藏匿在那些地方？

各有何优缺点？

如何找出来砍头？

Q38 我知道木马的自动运行设置就是藏在注册表中，为何就是未找到呢？

Q39 木马如何使用替换某个系统文件的方式来自动运行？

有何优缺点？

如何防护？

Q40 木马隐藏在被黑者电脑中的方式有那些新的技术与发展方向？

如何道比魔高？

Q41 黑客会使用那些方法让被黑者的电脑尽快或立该重新启动，让植入的木马运行？

如何防护？

Q42 黑客如何以简单的欺骗方式就可以使被黑者很听话的重新启动？

Q43 黑客如何将一般木马程序转换成系统服务方式来运行？

如此就可逃过工作管理员或TaskInfo的追杀。

如何防护？

Q44 如何查找、判断与干掉以系统服务方式运行的木马？

有那些困难之处？

Q45 木马成功运行与启动后，黑客要如何使用它？

## <<木马防护全攻略>>

可以阻挡吗？

要怎么做？

Q46 黑客已经成功植入与启动木马，为何还会失败？

有那些原因？

Q47 什么是ICMP木马？

它的原理为何？

它如何突破防火墙的阻挡？

如何防护？

Q48 那些情况下即使木马成功植入而且启动，但黑客无法获取被黑者IP或是与木马连接？

Q49 黑客如何让植入局域网电脑（或网吧电脑）的木马也可以正常运作？

Q50 木马服务器端程序在使用仿真IP的被黑者电脑中如何与黑客的客户程序进行连接？

Q51 我要与位于某个局域网中的电脑进行远程遥控，要如何做到？

Part5各类型木马专论剖析(StudyandDefenseforManyKindofTrojan) 综合型木马 特定型木马 Q52 Sub7木马程序对被黑者进行那些黑客行为？

会造成那些损失与伤害？

如何进行防护？

Q53 如何找出我的电脑中是否有Sub7木马程序藏匿？

如何彻底干掉它？

Q54 OPTIX\_Pro木马程序对被黑者进行那些黑客行为？

会造成那些损失与伤害？

如何进行防护？

Q55 如何找出我的电脑中是否有OPTIX\_Pro木马程序藏匿？

如何彻底干掉它？

Q56 什么是寄生嵌入式DLL木马？

为什么很难发现它？

它是如何嵌入系统文件与自动运行？

Q57 黑客这门是怎样的木马？

它如何借由寄生系统文件来隐藏自己？

为何在TaskInfo、TCPView、系统服务中都未找到它的踪迹？

它如何穿过仿真IP与防火墙与黑客电脑连接？

Q58 如何找出我们的电脑中是否有黑客之门藏匿？

如何彻底干掉它？

Q59 是否有专门针对突破仿真IP、防火墙的木马？

Q60 是否有只进行反向连接、文件小巧的后门木马？

Q61 黑客使用不具知名度的遥控软件可对被黑者进行那些黑客行为？

会造成那些损失与伤害？

如何进行防护？

Q62 如何找出我的电脑中是否有某个遥控软件藏匿？

如何彻底干掉它？

Q63 WinShell木马程序对被黑者进行那些黑客行为？

会造成那些损失与伤害？

如何进行防护？

Q64 如何找出我的电脑中是否有WinShell木马程序藏匿？

如何彻底干掉它？

Q65 NTRootKit是怎样的木马后门程序？

它是如何寄生在系统中？

它如何躲避TaskInfo、TCPView的查看与端口监控？

## <<木马防护全攻略>>

提供黑客那些功能？

如何找出、删除与防护它？

Q66 NTRootKit如何作为DDoS瘫痪攻击木马？

有可优缺点？

Q67 Keylogger是什么样的木马程序？

为何许多黑客都喜欢使用它？

它会对被黑者造成那些损失与伤害？

如何防护与阻挡？

Q68 如何找出我的电脑是否有Keylogger木马藏匿？

如何彻底干掉它？

Q69 ProtectedStorage是什么样的木马？

它如何偷取在IE、OE或MSNExplorer中曾经输入的各种帐户与密码？

如何防护？

Q70 MSN木马会进行那些工作？

对被黑客会造成那些损失与伤害？

Q71 黑客通常使用那些方法获取被黑者的帐户密码与交谈记录？

如何防护与阻挡？

Q72 黑客会使用那些方法打开被黑电脑的Telnet后门？

Q73 为何杀毒软件、防火墙无法找到或阻挡黑客利用Telnet后门入侵？

Q74 如何防止黑客利用Telnet后门进行入侵？

附录1 各地IP地址详细列表附录2 端口列表附录3 TaskInfo附录4 Startup附录5 ASPack附录6 SyGate个人防火墙附录7 MagicMailMonitor附录8 DeceptionBinder附录9 FreshBind附录10 MicroJoiner附录11 ExeBinder附录12 PECcompact附录13 UPXG附录14 EXEStealth附录15 TCPView附录16 AngryIPScanner附录17 IPHacker附录18 AppToService附录19 VNN(VitualNativeNetwork)附录20 SubSeven附录21 OptixPro附录22 COOL!RemoteControl附录23 RemotelyAnywhere附录24 WinShell附录25 NTRootKit附录26 黑客之门附录27 PerfectKeylogger附录28 ProtectedStorage附录29 SuperScan附录30 FakeMSN附录31 Splone附录32 tftp32附录33 at命令说明附录34 GetRight

## <<木马防护全攻略>>

### 编辑推荐

知己知彼才能找到制胜克敌之道，本书深入黑客的内心世界，从木马的选择到植入被黑者电脑中进行运作，详细讨论与研究其中个环节与技巧，然后找出最佳防护方式与破解之道，将各类型木马阻挡在门外，彻底保障你电脑的安全。

此外，本书是使用传统章节与问答形式并用的方式来帮助你更快速的阅读、了解和使用本书。该书是上网用户和专业网络安全人员的必备参考书。

<<木马防护全攻略>>

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>