汇聚攻防实战、管理维护多篇文章　集萃故障诊断、疑难解答专家精华

网管员世界

NETADMIN WORLD MAGAZINE

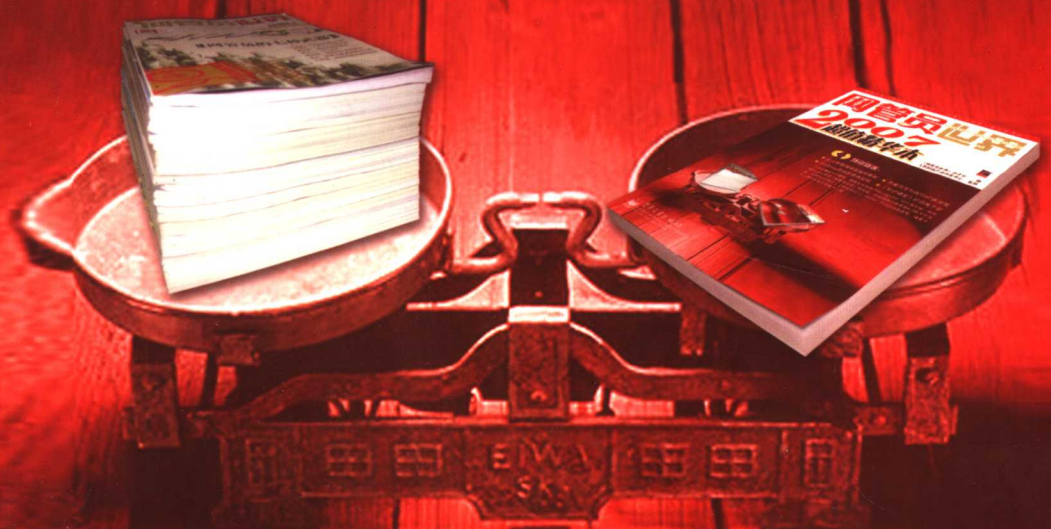
2007超值精华本

《网管员世界》杂志社　编
飞思科技产品研发中心　监制

特别赠送：

- 金山毒霸网络版独家体验
- 思康网安科技SWF体验版
- SiteView网络管理体验版
- 《知识讲堂》栏目电子版

江民杀毒软件下载版、联软安全运维产品Leagview 3.01演示版、科来MSN监控系统《网管员世界》特别版、科来网络分析系统6.3技术交流版、网康Flash短片《上网现形记》、Sniffer Portabel体验版、瑞星卡卡上网安全助手及专杀工具



光盘中收录有10余款网管专用商业软件及网管知识库

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
URL:http://www.phei.com.cn

《网管员世界》杂志社　编
飞思科技产品研发中心　监制

网管员世界

NETADMIN WORLD MAGAZINE

2007超值精华本

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内容简介

《网管员世界》是国内唯一一家专门面向网管员职业的刊物。本书是2006年《网管员世界》各期内容的汇集，内容权威、全面、时效性强，贴近应用实践，收藏价值高。本书按照栏目分类进行汇总，全书分为攻防实战、管理维护、故障诊断、疑难解答4个部分，共精选收录了400多篇实用、精彩的技术文章，是广大网管员不可多得的业务指导书。

随书光盘内容为《网管员世界》杂志"知识讲堂"栏目的电子文档、江民杀毒软件下载版、联软安全运维产品Leagview 3.01演示版、科来MSN监控系统《网管员世界》特别版、科来网络分析系统 6.3 技术交流版、网康提供的Flash短片《上网现形记》等软件。

本书适合作为广大网络管理员入门和提高的技术参考用书。

图书在版编目（CIP）数据

网管员世界2007超值精华本 / 《网管员世界》杂志社编.—北京：电子工业出版社，2007.4
ISBN 978-7-121-04158-7

I. 网… II.网… III.计算机网络－管理 IV.TP393.07

中国版本图书馆CIP数据核字（2007）第044092号

责任编辑：王树伟
印　　刷：北京智力达印刷有限公司
装　　订：北京中新伟业印刷有限公司
出版发行：电子工业出版社
　　北京海淀区万寿路173信箱　邮编：100036
开　　本：880×1230　1/16　印张：30.25　字数：1306.8千字
印　　次：2007年4月第1次印刷
印　　数：6 000册　　定价：49.80元　（含光盘1张）

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系电话：（010）68279077；邮购电话：（010）88254888。

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

服务热线：（010）88258888。

前言

《网管员世界》作为一本专门面向网络管理技术人员的专业杂志，已经走过了 5 年的风雨历程，长期以来，《网管员世界》杂志一直以帮助企业提高企业 IT 基础设施运营水平、提高企业网管人员的管理水平为目标和宗旨，为企业的网络技术人员提供了一个技术和经验交流的平台，成为在网络管理技术人员中颇具影响力的 IT 专业媒体。

为了更好地帮助广大网络技术人员提高网络管理技术水平，电子工业出版社与《网管员世界》杂志特别推出《〈网管员世界〉2007 超值精华本》，内容来自于 2006 年全年《网管员世界》杂志“管理维护”、“故障诊断”、“攻防实战”、“问与答”等栏目中精彩文章的汇总。对于这几百篇文章，本书进行了整合，全书共分为 4 章，包括攻防实战、管理维护、故障诊断、疑难解答 4 个方面的内容：

- 攻防实战：专门针对网络安全而推出的网络安全专业手册，文章来自《网管员世界》杂志“攻防实战”栏目，对网络管理人员增强网络安全意识、提高网络安全技能有着重要的指导作用。
- 管理维护：对于广大网络管理人员来说，网络管理和维护是他们的一项重要工作，网络管理维护篇以大量精彩翔实的文章为广大网络管理人员管理和维护网络提供了鲜活的实例和参考，能够帮助网络管理技术人员完成从网络管理菜鸟到高手的转变。
- 故障诊断：收集了《网管员世界》杂志社创刊 5 年来在“故障诊断”栏目中的精华文章和优秀专题，既是网管员在日常工作中排障查错的工具手册，又是网管员提高网络管理水平的技术全书。
- 疑难解答：汇集了网络管理、维护、排障方面遇到的典型问题，可以帮助网络管理技术人员迅速解决一些常见的网络问题，是网络管理人员可以随时随地查阅的问答宝典。

本书光盘内容包括“知识讲堂”电子文档、江民杀毒软件下载版、联软安全运维产品 Leagview 3.01 演示版、科来 MSN 监控系统《网管员世界》特别版、科来网络分析系统 6.3 技术交流版、网康提供的 Flash 短片《上网现形记》等软件。

本书可作为网管员的日常工作手册，在工作中遇到问题时可以通过本书随时查阅；也可以作为网络技术人员或者网络爱好者提高网络管理和维护水平的进阶读本。

由于时间紧张，加之编者水平有限，书中错误之处欢迎读者批评指正，以利于我们今后改进。

《网管员世界》杂志社

飞思科技产品研发中心

联系方式

咨询电话：（010）68134545　88254160

电子邮件：support@fecit.com.cn

服务网址：http://www.fecit.com.cn　http://www.fecit.net

通用网址：计算机图书、飞思、飞思教育、飞思科技、FECIT

反侵权盗版声明

目录

第 1 章　攻防实战

第 2 章　管理维护

第 3 章 故障诊断

第 4 章　疑难解答

NetAdmin World 2007

第 1 章　攻防实战

毒发身亡，还是天下无毒？

——与病毒的博弈

长久以来，病毒一直困扰着广大用户，从早期的CIH、宏病毒，到近期的尼姆达、冲击波、震荡波、MyDoom、NetSky，每一年都会有几个让我们牢牢记住的病毒。直到2005年，似乎没有出现类似的重大病毒。病毒莫非离我们越来越远了？

事实却远非如此。木马、蠕虫或者其他类病毒，正时刻虎视眈眈地注视着我们的网络和系统，哪怕我们的防范策略只出现一点小疏忽，或者防病毒产品出现一点小问题，它们都会毫不客气地杀进来。

那么，我们是等待“毒发身亡”，还是通过前期努力争取“天下无毒”呢？

答案显然是后者！

为了帮助广大网管员正确认识并坦然面对病毒，同时学会做一些“未雨绸缪”和“亡羊补牢”的工作，我们特意组织了这期专题，通过介绍经验丰富的网管员的经验，帮您在与病毒斗争过程中取得胜利。

- 正视病毒——认知篇
- 毒来毒往——面对篇
- 天下无毒——应对篇

随着计算机技术的发展，操作系统日渐完善，杀毒软件的杀毒能力不断提高，病毒的编写水平也达到了前所未有的高度，在这场没有输赢的博弈中，没有最强只有更强。我们既不能盲目乐观，相信天下已无毒，又不能“一朝被蛇咬，十年怕井绳”。下面，让我们一起来揭穿病毒的真面目。

正视病毒——认知篇

文/高征 张四大

认识病毒

《中华人民共和国计算机信息系统安全保护条例》对计算机病毒的定义是：计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。主要特点有以下3点：

- 通过磁盘、磁带和网络等作为媒介传播扩散，能“传染”其他程序的程序。
- 能够实现自身复制且借助一定的载体存在的具有潜伏性、传染性和破坏性的程序。
- 一种人为制造的程序，使计算机的资源受到不同程序的破坏。

直面病毒

在新形式下，用户感染病毒的几率有了什么变化？病毒的破坏能力是否提高了？查杀病毒工作是难是易了呢？下面一一道来。

1．感染几率不断升高

应该说，技术发展到了今天，低级病毒基本已经没有生存空间了，病毒增长数量大大降低了，但计算机感染病毒的几率并没有随之降低。由于因特网的广泛使用，大多数人的计算机水平不高，再加上现在病毒的感染能力不断提高和感染途径不断扩大，感染病毒的几率也不断升高。计算机病毒正以前所未有的速度在增长、蔓延。事实上，只要连上了因特网，就基本没有幸存者，所以对于计算机病毒，我们绝对不能掉以轻心。

2．破坏力更有针对性

从整体来讲，病毒的破坏能力相对而言已温和了一些，不再像以前那样具有直接的破坏力，而是变得更有针对性，病毒的攻击和传播主要通过系统和服务漏洞来实现。

目前计算机病毒主要分为四大类。第一类是系统漏洞类病毒，这类病毒如蠕虫类、SQL注入类，主要通过系统漏洞取得控制权。前者主要是无限制占用系统资源，严重时甚至造成服务中断，一般不会破坏数据；后者针对程序漏洞设计，破坏性难以预料，轻则泄露数据，重则让数据不保，系统崩溃。第二类是木马类病毒（远程控制类），中毒者的计算机对遥控者开放服务，遥控者可轻而易举地浏览、修改中毒者的文件，实时监视屏幕，以及获取密码，风险极高。第三类是脚本类病毒，利用ActiveX控件漏洞修改注册表相关选项，譬如定向主页、修改文件属性等。大部分脚本类病毒属于恶作剧，一般不会毁坏数据。第四类是硬盘类病毒，通过改写引导扇区，或者格式化硬盘，甚至改写硬盘BIOS达到毁坏数据的目的。

对PC用户而言，由于数据重要性普遍不是很高，出现问题无法解决的话最多也就是重装系统，基本不会造成太大

的损失；但是对于服务器而言，却是非常严重的威胁。由于病毒会令服务中断，所以对于计算机病毒，重要的是防患于未然，中毒后首先要抢救数据，然后才是查杀病毒。

3．查杀病毒难题不断

计算机病毒在长期对抗杀毒软件查杀的过程中，也不断应用了一些新型技术，如隐藏进程和线程插入技术，给病毒的查杀增加了难度。

对于漏洞型病毒，由于病毒和服务同为一体，在相应补丁没有发布之前，基本上是不可能清除的，对于这种情况只能是停止服务、备份数据、启用备用设备、封闭不必要的端口和服务，避免再度发生感染，等待补丁发布。对于木马类病毒，由于变异很快，运作方式采用线程插入，对于杀毒软件的查杀可以主动隐藏，甚至屏蔽防火墙，很多时候是杀而不死的，这时断开网络是最好的解决方法，直到杀毒软件具备杀毒的能力。脚本类病毒的查杀相对比较简单一些，病毒防火墙只要保持版本最新，一般都可以轻松查杀；硬盘类病毒的查杀风险很大，稍有不甚就会使数据的毁坏雪上加霜，查杀前一定要做好备份。

从整体上看，计算机感染病毒的几率不断升高，病毒的破坏能力更具针对性，查杀工作难度不断增加，那是不是说我们就对它束手无策了呢？我们是否要受其危害而无法摆脱了呢？事实并非如此！下一篇您将学到如何面对病毒。

毒来毒往——面对篇

文/董未 高征 张四大 王岗

病毒看似强大，其实是只不折不扣的“纸老虎”，既然是纸老虎，就有其致命弱点，下面向您介绍如何面对这只“纸老虎”。以下将和您一起分享：一些可能感染病毒的不良习惯，中毒后的可能表现，如何判断系统是否中毒，如何对付杀毒软件也无能为力的病毒，以及杀毒软件失效时的处理办法。

可能感染病毒的不良习惯

在日常使用中，操作电脑的不良习惯和疏忽很容易导致感染病毒。由于感染途径的扩大，病毒的感染并没有固定的模式，主要分为主动感染和被动感染。主动感染是病毒主动在网络上搜索存在漏洞的计算机，并种植病毒；被动感染是病毒通过伪装、邮件或者网页引诱计算机用户单击链接，从而在用户计算机上种植病毒。一种病毒也可能同时具备此两种感染方式，所以用户必须谨慎，减少感染病毒的机会。

总体来说，可能感染病毒的不良习惯包括：

- 系统不安装杀毒软件及软件防火墙。
- 不能够及时给系统及应用软件打上最新的补丁。
- 浏览含有不良信息的网站。
- 轻易打开来历不明的邮件、附件和一些网友发来的网址、文件。
- 开启太多不需要的服务。
- 系统及系统使用的软件密码过于简单。
- 需要共享的文件夹没有设置适当的存取权限。
- 安装的防病毒产品没有及时更新病毒定义库和杀毒引擎。

中毒后的表现

计算机中毒后由于感染的病毒种类不同，其症状也不同。

虽然病毒隐藏得深，但是只要留心，计算机中毒后的表现还是很容易被发现的。当发现系统缓慢，服务中断，网络和 CPU 利用率很高时，应该警惕是不是中了漏洞类病毒；屏幕上鼠标自己乱动，程序莫名其妙打开，CPU 利用率猛然升高，鼠标和键盘出现暂停响应，就应该怀疑感染上木马类病毒了；当文件无法打开，上网时自动弹出不相关网页时，就应该怀疑是否被脚本类病毒捉弄了；如果系统无法启动、分区大小被改变或者不见了、文件名变成乱码了，那么可能被硬盘类病毒看上了；病毒防火墙无法正常工作，那么防火墙可能是被一种很厉害的病毒攻破了。平时多留意网上对各类病毒的表现的描述，对于及时发现病毒，会有事半功倍的成效。

总体来说，计算机中毒后大概有以下几种症状：

- 屏幕上突然出现特定画面或一些莫名其妙的信息。如“离关机时间还有××秒”或屏幕黑屏等。
- 原来运行良好的程序，突然出现了异常现象或荒谬的结果；一些可执行文件无法运行或突然丢失等。
- 计算机运行速度明显降低。
- 计算机经常莫名其妙地宕机、不能正常启动。
- 系统无故进行磁盘读写或格式化操作，无缘无故访问软驱和光驱。
- 文件长度奇怪地增加、减少，或产生特殊文件。
- 磁盘上突然出现坏的扇区或磁盘信息严重丢失。
- 磁盘空间仍有空闲，但不能存储文件，或提示内存不够。
- 打印机、扫描仪等外围设备不能正常使用。
- 计算机运行时突然有蜂鸣声、尖叫声、报警声或重复演奏某种音乐等。
- 系统资源和网络资源被大量占用。

判断系统中毒的方法

计算机看似中毒，但并不一定是真的中毒，有可能是其他正常程序造成的。譬如，打开网页后出现短暂的暂停响应，可能是 CPU 忙；程序莫名其妙打开可能是有定时计划或者误碰了快捷键；系统缓慢、服务中断，也需要查明究竟是内部需求增加还是外部连接造成的；文件不能打开，可以看看系统资源是不是太少了；系统无法启动、分区改变、文件出现乱码，很有可能是硬盘的损坏造成的；病毒防火墙不能正常工作，也可能是程序出现错误了。判断系统是否真正中毒很重要，可以避免误认中毒而执行不必要的操作，导致浪费人力、物力。

判断系统是否中毒的方法很多，下面简单介绍几种。

（1）使用杀毒软件进行全面病毒扫描，一般的已知病毒都能查杀出来。

（2）进行手动检查。

1）使用 msconfig 命令启动系统配置文件，查看启动选项和加载服务选项，如果发现非正常的启动项，应该是有病毒入侵。

2）利用一些功能比较强的计算机线程查看工具，查看计算机运行时有哪些线程在运行，可以查找可疑线程。

3）查看计算机打开端口及连接。使用专门的端口监视软件或 netstat 命令查看计算机打开的端口，出现异常端口通信应该是有病毒入侵。

4）打开注册表编辑器，找到 Run/RunOnce/RunOnceEx/RunService 键值，查看是否有可疑程序在计算机启动时自动运行。

注意

对可疑程序进行定位、查找的过程中，要显示所有文件和文件夹。找到可疑程序文件，可以查看文件创建时间，如果是在计算机出现问题的那几天创建的，一般来说就是计算机感染了病毒。

5）在企业中使用虚拟服务器或虚拟计算机组成“蜜罐”来诱捕病毒，查看防火墙日志，监控网络流量，使用入侵监控系统捕捉等。

对付“顽固”的病毒

安装了杀毒软件，并不意味着就可以高枕无忧了。有时，对于已知病毒的变种或者未知病毒，杀毒软件可能是无能为力的。出现这种情况时，首先要判断是已知还是未知病毒，这一步很关键。

对于已知的计算机病毒，我们在 Windows 正常状态下无法查杀，可以启动到安全模式下使用杀毒软件查杀。有些病毒在安全状态下也运行（如 Rootkit 类病毒），我们就要在纯 DOS 或使用 Linux 启动盘启动后查杀，一般情况下都能解决问题。

对于未知病毒，在企业中首先要找到计算机病毒的源头，然后再进行病毒分析。

找到感染病毒的计算机后，首先要断开网络，依据不同中毒特征分别处理。首先备份计算机中的有用文件；然后处理内存及系统核心病毒，杀死病毒线程，修补被病毒破坏的系统；最后，删除病毒体及病毒所衍生的垃圾文件，给系统安装好补丁后接入网络。

提示

备份重要数据时，要断开网络，使用工具软件清除内存中的病毒线程，清除病毒的加载项，使用系统盘恢复被病毒破坏的系统文件，删除病毒体及其衍生的文件，重新启动后给系统打好补丁，更新杀毒软件的病毒库。如果是 Windows XP 可以使用系统还原功能还原到以前未感染病毒的系统。

杀毒软件失效及处理办法

失效原因：

（1）毒软件未能及时更新病毒库，造成无法查杀新的病毒（最主要原因）。

（2）有些病毒对专门的杀毒软件进行处理，使用加壳或一些捆绑软件加密病毒体，造成与病毒库代码对比不同而漏杀。

（3）有些用户为了提高上网速度关闭杀毒软件的实时监控功能，下载文件或直接打开邮件附件而不进行病毒扫描。

（4）有些杀毒软件本身的漏洞造成病毒漏网。

处理办法：

（1）将计算机连接到因特网，在线更新病毒库。如果无法接入因特网，就找一台能上网的计算机下载离线升级包升级，升级后使用杀毒软件进行查杀。

（2）如果无法启用杀毒软件，根据病毒特性，使用手动方法删除计算机内的病毒，不要求完全杀光病毒，至少要求计算机再次启动时内存没有病毒线程即可。重新启动计算机，安装杀毒软件，更新病毒库，使用杀毒软件查杀。

（3）上网给系统打好补丁。

计算机感染病毒，一般和计算机使用者的不良习惯有关系。计算机网络日益发展的今天，随着我们对网络的依赖程度越来越高，更应该提高预防病毒的警惕性，做到防毒之心不可无。

在中毒后查杀病毒并不是最聪明的做法，如果在事前做好防范工作，就可以更彻底地把病毒拒之门外。下一篇您将学到如何未雨绸缪，应对病毒。

上一篇我们学到了如何面对病毒，事实上，防患于未然远比亡羊补牢的补救好很多。以下向您介绍如何应对病毒，您将分享到：从中毒事件中可以汲取什么教训，如何设置可以远离病毒的威胁。

天下无毒——应对篇

文/董未 高征 吴树丰

对于计算机病毒，防范总比查杀更能保障计算机的安全，平时要多积累经验。对于企业，需要做好防毒指导、加强宣传、维护好病毒服务器和防火墙、定时检查病毒版本、做好病毒预告、控制好上网通道、过滤不良网站、封堵多余端口、限制文件的传输和聊天软件的使用、及时打补丁、封堵有危险的漏洞等，有条件的话使用公司的网站邮箱，便于集中控制及过滤垃圾邮件，如此病毒就不会频频光顾，甚至消声匿迹了。

吸取的教训

在遭受病毒攻击事件后，认真总结经验教训，以防再一次遭受攻击，也不失为一种聪明的做法。

总结起来，遭受病毒攻击主要有以下几点原因。

（1）缺少防范病毒的意识，没有认识到计算机感染病毒后带来的严重后果和资源的浪费。

计算机病毒主要是通过读写文件或网络传播的。但这些操作又是不可缺少的，因此必须根据其传播途径采取适当措施加以防范。

1）争取单人单机，避免多人公用一台计算机。

2）使用移动介质交换数据，要做好使用前的病毒查杀工作。

3）网上下载要到口碑较好的网站。网上下载要谨慎，一定要到安全可靠的知名网站、大型网站，不要选择一些小型网站。在使用网上下载的东西之前最好先做病毒扫描，确保安全无毒。

4）管好、用好电子邮件（E-mail）系统。电子邮件已经成为计算机病毒传播的主要载体，其比例占所有计算机病毒传播媒介的 60%，几乎所有类型的计算机病毒都可能通过电子邮件来进行快速传播，如 Nimda（尼姆达）病毒。为防止计算机通过电子邮件渠道感染，需要及时升级电子邮件收发程序，并且为操作系统打上必要的补丁。在收到电子邮件时，绝不打开来历不明邮件的附件，对看来可疑的电子邮件不要打开，马上删除。

（2）企业用户我行我素，缺少与本单位网络管理员的配合，不能及时按照管理员的要求做好防范病毒工作。

1）用户不按照要求安装防病毒软件，造成计算机完全没有防护地暴露在网络中。

2）自行安装杀病毒软件，不按规定统一部署，致使病毒定义码和引擎不能及时更新，对新出现的病毒防杀不利。

3）随意共享文件夹，不注意访问权限的设置，为病毒通过网络传播留下途径。

4）不能按照管理员的要求及时安装系统补丁，为病毒的入侵留下了漏洞。

（3）没有养成备份重要数据的工作习惯，一旦计算机感染病毒崩溃，用户损失巨大。

对存储重要数据的计算机来说，数据备份也是很重要的一个环节。病毒一旦发作，经常会导致系统崩溃或文件丢失。如果重要数据受损，后果将不堪设想。所以，养成定期备份数据的习惯是安全使用计算机的重要环节之一。

远离病毒的妙招

1. 杜绝不良习惯

对企业用户来讲未给系统打补丁、未使用杀毒软件，不更新病毒库，电子邮件系统、网页系统、数据库系统有漏洞，使用 QQ、MSN、ICQ 传输文件，下载软件及影视文件，使用 P2P 软件都是一些不良习惯，要坚决克服。

2. 加强安全意识

无论企业还是个人，在使用计算机过程中要有安全意识，对病毒、黑客等要有足够的知识。

3. 增强自己的知识

以下是一些小技巧，做到之后可以较大限度地防范计算机病毒。

- 谨慎打开不明邮件。
- 打开附件前请查杀病毒。
- 上网时要打开杀毒软件的实时监控功能。
- 使用防火墙（软件、硬件）对网络进行监控。
- 使用入侵监测系统防范黑客入侵。
- 企业要有完善的网络安全规章制度，工作人员要按照规定行事。
- 最重要的一点是要经常备份重要的数据，以防病毒的破坏。

本专题分析了病毒的现状，告知网管员要正确认知病毒；中毒后不要惶恐，要坦然面对病毒；要从中毒事件中汲取教训，学会应对病毒的技巧、设置。学会了这些，就能在与病毒的博弈中克敌制胜，真正做到天下无毒。

抵御DDoS攻击三剑客

福建/邱晓理

分布式拒绝服务（DDoS，Distributed Denial of Service）攻击是一种特殊形式的拒绝服务攻击。它利用多台已经被攻击者所控制的傀儡机器对某一台单机发起攻击，在带宽相对的情况下，被攻击的主机很容易失去反应能力。作为一种分布、协作的大规模攻击方式，分布式拒绝服务（DDoS）攻击主要瞄准比较大的站点，像商业公司、搜索引擎和政府部门的站点。由于它利用一批受控制的机器向一台机器发起攻击，来势迅猛，而且往往令人难以防备，具有强大的破坏性。

对DDoS攻击来说并没有百分之百有效的防御手段。但是由于攻击者必须付出比防御者大得多的资源和努力才能实现有效的攻击，所以只要我们更好地了解DDoS攻击，积极部署防御措施，还是能在很大程度上缓解和抵御这类安全威胁的。另外，加强用户的安全防范意识，提高网络系统的安全性也是很重要的措施。

监控骨干网络设备，减少骨干网主机的漏洞

加强对骨干网络设备的监控，常用的方法包括限制连接队列的长度及减少处理延时等。前者可以缓解系统资源的耗尽，虽然不能完全避免拒绝服务的发生，但是至少在一定程度上降低了系统崩溃的可能性，而后者能够加强系统的处理能力。通过减少延时，我们能以更快的速度抛弃队列里等待的连接，而不是任其堆满队列。不过这种方法也不是在所有的情况下都有效，因为很多DDoS的攻击机制并不是建立在类似SYN Flood这样以畸形连接淹没队列的方式之上的。

几乎所有的主机平台都有抵御DDoS的设置，基本的设置有以下4种。

（1）关闭不必要的服务。确保从服务器相应的目录或文件数据库中删除未使用的服务，如FTP或NFS。Wu-Ftpd等守护程序存在一些已知的漏洞，黑客通过根攻击就能获得访问特权系统的权限，并能访问其他系统——甚至是受防火墙保护的系统。确保运行在UNIX主机上的所有服务都有TCP封装程序，限制对主机的访问权限。

（2）限制同时打开的SYN半连接数目。

（3）缩短SYN半连接的time out时间。

（4）及时更新系统补丁。确保所有服务器采用最新系统，并打上安全补丁。计算机紧急响应协调中心发现，几乎每个受到DDoS攻击的系统都没有及时打上补丁。因此应当及早发现系统存在的攻击漏洞，及时安装系统补丁程序。

合理配置路由器及防火墙，实现IDS和防火墙的联动

企业网的网络设备可以从防火墙与路由器上考虑。这两个设备是与外界的接口设备。需要注意的是，防DDoS的设置是以牺牲效率为代价的。

路由器（以Cisco路由器为例）设置如下：

- Cisco Express Forwarding（CEF）。
- 使用unicast reverse-path。
- 访问控制列表（ACL）过滤。
- 设置SYN数据包流量速率。
- 升级版本过低的ISO。
- 为路由器建立log server。

其中使用CEF和Unicast设置时要特别注意，使用不当会造成路由器工作效率严重下降，升级IOS也应谨慎。

在Cisco路由器上使用ip verfy unicast reverse-path网络接口命令，这个功能检查每一个经过路由器的数据包。在路由器的CEF表该数据包所到达网络接口的所有路由项中，如果没有该数据包源IP地址的路由，路由器将丢弃该数据包。例如，路由器接收到一个源IP地址为1.2.3.4的数据包，如果CEF路由表中没有为IP地址1.2.3.4提供任何路由（即反向数据包传输时所需的路由），则路由器会丢弃它。单一地址反向传输路径转发（Unicast Reverse Path Forwarding）在ISP（局端）实现阻止SMURF攻击和其他基于IP地址伪装的攻击，这能够保护网络和客户避免受来自因特网其他地方的侵扰。使用Unicast RPF需要打开路由器的“\CEF swithing\”或“\CEF distributed switching\”选项，不需要将输入接口配置为CEF交换（switching）。只要该路由器打开了CEF功能，所有独立的网络接口都可以配置为其他交换（switching）模式。RPF（反向传输路径转发）属于在一个网络接口或子接口上激活的输入端功能，处理路由器接收的数据包。

防火墙设置如下：

- 禁止对主机的非开放服务的访问。
- 限制同时打开的SYN最大连接数。
- 限制特定IP地址的访问。
- 启用防火墙的防DDoS属性。
- 严格限制对外开放的服务器的向外访问。

要限制在防火墙外与网络文件共享，因为这会使黑客有机会截获系统文件，并以特洛伊木马替换它，文件传输功能无疑将陷入瘫痪。

利用防火墙来加固网络的安全性，配置好这些设备的安全规则，过滤掉所有可能的伪造数据包。在受到攻击时，迅速确定来源地址，在路由器和防火墙上做一些屏蔽。

在防火墙上运行端口映射程序或端口扫描程序。大多数事件是由于防火墙配置不当造成的，使 DoS/DDoS 攻击成功率很高，所以一定要认真检查特权端口和非特权端口。

现在有很多防火墙产品集成了反 DdoS 的功能，进一步提高了对常见 DDoS 攻击包的识别能力。这样的产品可以在很大程度上增强 DDoS 防御能力，并且可以做到不对数据包进行完全检查就能够发现“恶意行为”。这是非常有用的功能，如果判断 DDoS 攻击所耗费的处理越少，就越不容易被耗尽处理能力，从而极大地增加攻击者的成本。包括很多路由器产品在内的网络设备都具备一些防火墙功能，我们应该尽可能充分利用。

另外，实现 IDS 和防火墙的联动也是有效抵御 DDoS 攻击的有效手段。

加强网络管理，建立合理的应对策略

（1）确保手头有一张最新的网络拓扑图。这张图应该详细标明 TCP/IP 地址、主机、路由器及其他网络设备，还应该包括网络边界、非军事区（DMZ）及网络的内部保密部分。

（2）在网络管理方面，要经常检查系统的物理环境，禁止那些不必要的网络服务。建立边界安全界限，确保输出的包受到正确限制。经常检测系统配置信息，并注意查看每天的安全日志，检查所有网络设备和主机/服务器系统的日志，只要日志出现漏洞或时间出现变更，几乎可以肯定相关的主机安全受到了威胁。

（3）与网络服务提供商协调工作，让网络服务提供商帮助实现路由的访问控制和对带宽总量的限制。

（4）当用户发现自己正在遭受 DDoS 攻击时，应当启动自己的应付策略，尽可能快地追踪攻击包，并及时联系 ISP 和有关应急组织，分析受影响的系统，确定涉及的其他节点。

（5）确保管理员对所有主机进行检查，而不仅针对关键主机。这是为了确保管理员知道每个主机系统在运行什么？谁在使用主机？哪些人可以访问主机？不然，即使黑客侵犯了系统，也很难查明。

（6）对一些重要的信息（例如系统配置信息）建立和完善备份机制。对一些特权账号（例如管理员账号）的密码设置要谨慎。

通过以上一系列的举措可以把攻击者的可乘之机降低到最小。

病毒预警

最近有一个病毒特别值得注意，它伪装成流行的网上聊天工具 MSN 8 的测试版本，通过 MSN 进行传播。中毒电脑可被黑客远程控制，如添加/删除程序、盗取隐私信息等。

兰迪斯变种 F(Backdoor. Landis.f)是一个可以在 Windows 9x/NT/2000/XP 系统上运行的后门程序。病毒运行后会自动向 MSN 好友发送 MSN 8 新版发布的消息，如果用户运行了假冒的“MSN 8”，病毒还会自动向其 MSN 好友发送消息“http://****beta8.com/im.php?msn=XXXX@ XXXX.com”，诱骗其他人单击该病毒网址。该地址指向黑客建立的一个仿冒微软风格的下载网站，用户只要从这个网站下载运行“MSN 8.0 测试版”，电脑就会中毒。中毒电脑可被黑客远程控制，如运行程序、盗取密码等。该病毒还会禁止一些国外杀毒软件运行，降低用户计算机的安全系数，使染毒计算机感染其他病毒的几率大大增加。

专家建议用户不要随便打开通过 QQ、MSN 等即时通信工具发来的网站地址或文件，要及时升级杀毒软件并打开文件监控功能来防范此类病毒。

狙击 IRC Trojan

文/余海发

“IRC Trojan”这个词最早是由 CERT 组织在 1994 年提出的。随后，IRC Trojan 的数量不断增加，特性不断丰富，其产生的破坏力也不容小觑了。近一两年中出现的僵尸网络（BotNet）事件多与此有关，攻击者常常通过 IRC 控制上万台受感染的主机发动 DDoS 攻击，这类事件造成的危害也是非常巨大的。本文试图对 IRC Trojan 进行分析和探讨，希望能有助于提高大家对于 IRC Trojan 的安全意识和防范能力。

IRC Trojan 是什么

如果从 1994 年 CERT 发现的 Trojan Horse 算起，IRC Trojan 已经有 11 年的历史了。最初的 IRC Trojan 最主要的一个特征就是它会在被感染机器与 IRC 服务器之间开放一个隐匿的连接，通过这个隐匿连接，攻击者可以发送控制命令到受感染的机器，从而遥控受感染的机器执行各种命令。具有这一特征的程序都可以称为 IRC Trojan。

从这一特征来看，IRC Trojan 应该被看做是一个重要的安全风险，因为通过 IRC 往往可以使一个人方便地同时控制成千上万台主机。最近两年控制几万甚至上百万台主机进行 DDoS 攻击的事件频频出现，其中散播 IRC Trojan 就是一种常见的控制方法之一。

随着技术不断地更新，许多 IRC Trojan 借鉴了病毒、蠕虫等部分技术。IRC Trojan 有时候像一个病毒，它可以被常

见的杀毒软件所发现和清除。实际上，从技术发展趋势来看，Trojan Horse 有与蠕虫、木马等相互融合的趋势，即 Trojan Horse 也开始具备蠕虫的传播复制、病毒的隐藏变体等特征，蠕虫也会包含 IRC Trojan 以增强其传播和破坏能力。比如，Win32.Mytob.B 蠕虫病毒就同时具有 IRC Trojan 功能，利用 IRC Trojan 来达到允许未经授权的用户进入并远程控制被感染的主机的目的。

传播途径

不良攻击者散布 IRC Trojan 的方法与散布病毒、蠕虫等的方法类似，常见的散布手段包括以下几种。

挂站传播：不良攻击者在攻陷网站后，会将 IRC Trojan 隐藏在含有恶意代码的网页中，当用户访问相关网页时，就会运行恶意代码，从而植入 IRC Trojan。

邮件传播：不良攻击者也会通过群发邮件的方法，将 IRC Trojan 隐藏于邮件或附件中，诱使用户打开并运行它们，从而植入 IRC Trojan。

入侵种植：不良攻击者攻陷了主机之后，也可能植入 IRC Trojan 做后门，以便日后使用。

通过 IRC：RC-Worm.Mooze. enc、IRC-Worm.Mooze 等就是通过修改 MIRC 的脚本来传播自己的。

通过文件共享：它尝试利用管理员弱口令连接网络共享，如果成功，它将自身复制到共享目录中，并运行。所以，在企业局域网中如果你的电脑还没有给管理员设置口令（密码为空），很容易受到病毒的攻击和感染。

蠕虫传播：将 IRC Trojan 与蠕虫相结合，利用蠕虫的强大传播能力进行传播。

软件下载：IRC Trojan 会将自己伪装成一些极具诱惑力的软件来诱使您去下载运行，比如，屏幕保护程序、MP3 歌曲、图片等，很多用户很可能会下载这些文件去运行，从而感染 IRC Trojan。

感染目标及危害

IRC Trojan 针对的目标是普通的家庭用户及企业中的普通用户，这些用户通常缺乏足够的安全意识及安全保护措施，比较容易植入 IRC Trojan。此外，随着宽带用户的增长，大量电脑长期连接在因特网上，这些对于黑客来说是非常宝贵的资料，所以黑客会想尽方法来感染更多的机器。当然有些管理不慎的服务器也难以幸免。

IRC Trojan 能通过 IRC 通信传递控制信息、操纵受感染机器执行各种命令。传播者可能通过 IRC Trojan 从事以下活动。

- 利用受感染机器组成僵尸网络，对目标系统进行各种分布拒绝服务攻击（通过 PING、SYN、UDP 等产生拒绝服务攻击）。
- 利用隐藏的 IRC 通信从受感染机器盗取各种文件、数据、系统信息。
- 利用隐藏的 IRC 通信来收集受感染机器及网络的流量数据等。
- 利用隐藏的 IRC 通信来删除、窜改受感染机器上的文件，甚至破坏操作系统。
- 利用隐藏的 IRC 通信来删修改受感染机器上的系统配置，比如开放共享、新建账号等。
- 利用隐藏的 IRC 通信在受感染机器上执行各种命令，比如终止杀毒软件进程、安装其他程序等。

IRC Trojan 示例

- trojan/crypt.e：是利用 Kazaa 共享及 mIRC 传播的后门程序。可连接指定 IRC 服务器，加入指定 IRC 通道，侦听黑客指令。该后门运行后，自我复制到系统目录及 Windows 启动目录下，并修改注册表，以实现病毒程序的开机自启。在 Kazaa 上创建共享目录，并利用某些常用软件的名称将自己复制到 Kazaa 共享目录下，以欺骗他人下载。在系统目录下生成键击日志文件，并将盗取的操作系统信息及 IP 地址、用户名等信息发送到 IRC 服务器。另外，该程序可终止某些防火墙及杀毒软件的进程并可对指定目标执行 DOS 攻击。
- backdoor/tometa.a：是用 C++编写、用 UPX 压缩的后门程序，通过 IRC 和群发邮件进行传播，并可将用户计算机变为黑客代理服务器。该后门运行后，修改注册表，实现开机自启。连接特定 IRC 服务器，并加入一个 IRC 频道，侦听黑客指令，接收自我卸载、关闭特定链接、访问黑客指定站点等黑客指令。将后门程序作为附件，群发带毒邮件。
- Trojan.Glitch：又名 IRC 克隆人，它是用 VB 编写的，拥有许多变种。它的工作流程大致是：首先生成名为 stde9.exe 的安装包，当这个包运行时，会自动把文件安放到 system 目录下，并修改注册表的 run 项，进行自启动。同时，启动 mirc 程序并将窗口设成隐藏。然后攻击者可以利用 mIRC 的功能发送控制指令进行攻击和破坏。
- trojan/psw.pswsniffer.b：“密码针”是一个可利用微软的 dcomrpc（MS03-026）等漏洞进行传播的木马。该木马可连接 IRC 通道，远程控制用户计算机。“密码针”在用户计算机内搜索注册表，若发现用户计算机内装有虚拟机，则不会在此计算机内运行。该木马运行后，自我复制到系统目录下修改注册表，使“密码针”在安全模式下也能启动；开启 TCP6556 端口，侦听黑客指令，可盗取系统信息；利用记录键击或从缓冲区盗取用户密码信息；终止黑客指定进程；连接黑客指定站