信息安全动态

3

主编：四川大学信息安全研究所

吉林科学技术出版社

前　言

为全面、及时地反映国内计算机信息网络安全领域的发展动态，四川大学信息安全研究所选择了国内发行的中央和省市级的日报与经济类报刊以及 IT 业重要报刊(入选报纸的发行量至少 5 万份以上、杂志至少 2 万份以上)，将其中涉及计算机信息网络安全在技术、产品、市场、管理、案例等方面发展动态的报道加以精选并分类整合，逐月汇编为《信息安全动态》，自 2001 年 1 月起，由吉林科学技术出版社正式出版。

《信息安全动态》全年二十四辑，每月出书二辑。我们期望以此来快捷、全面地反映国内信息安全领域的发展动态和国内计算机信息网络安全市场的一些基本状况，能为应用、管理、决策人员提供有益的参考。

因无法与部分作者取得联系，故我们依照有关规定将其稿酬代为保管，同时敬请这部分作者见到本书后及时与我们联系，届时我们会将稿酬及利息汇出。

限于编者的经验，不足之处敬请批评指正。

四川大学信息安全研究所

《信息安全动态》编委会

信息安全动态第三辑目录索引

✧ 一、警钟篇

✧ 二、案例篇

✧ 三、管理篇

✧ 四、业界动态篇

✧ 五、技术篇

✧ 六、应用篇

✧ 七、争鸣篇

✧ 八、曝 光 篇

✧ 十一、其 它

警钟篇

- “网上黑社会”值得警惕
- 安全从自身抓起
- 电脑病毒越来越难灭
- 病毒常伴节日行
- 病毒开始入侵移动通讯
- Internet 环境下的六大安全性威胁
- 黑客偏爱 NT 系统

……

天津青年报 YOUTH DAILY
2001年2月1日

263部分页面被黑 “网上黑社会”值得警惕

本报讯 日前，有关263网络集团的服务器被黑客攻击一事，在网上炒得很是热闹，多项业务都雄踞霸主地位的263网站难道真的被大黑了一把？

263网络集团人士对此显然保持低调，不愿多说。只是想告诉消费者和企业客户们，“263提供的所有业务均不会受到影响，黑客攻击的只是介绍263业务内容的一个很小的服务器。客户不会受到任何损失。”据悉，263已暂时关闭了这个服务器，但很快会恢复使用。

目前，有黑客攻击了263的这个服务器，这个服务器承担的功能很单一，就是介绍263的各种业务，如263数据港、服务器托管、宽带接入、ASP服务、ISP业务、主叫计费、包月上网卡等。黑客还“签”上了自己的名字。

据业内人士介绍，这种攻击，就好比263是个商店，商店的玻璃上写着各种店内商品的介绍，黑客攻击的页面就是将玻璃砸了，而店里的东西都安然无恙，消费者不必担心有什么损失。因为一般网站对这样的页面并不投入重兵把守，黑客攻击相对容易些。

现在几乎所有著名网站均遭遇过黑客的攻击，甚至被勒索要保护费，有些像现实社会中的黑社会。而且，按照一般的规律，越是到假期的时候，黑客们越喜欢攻击一些著名网站，一方面是自己出名，一方面是作为再攻击下一家的资本。业内人士呼吁，有关部门仍须加强网络安全的法律规范及技术支持，让网站更好地为网民服务。（刘书）

北京 经济报
2001年2月1日

263早该被黑？

本报讯 1月30日，263网络集团的ISP、IDC业务网站被黑客攻击，有网友称以前就曾“提醒”过263，但他们“置之不理”！如今被黑了。目前，263被黑的14个页面仍不能打开，263已经将存放这些页面的服务器暂时关闭，263网络集团在接受北京有关媒体记者采访时称，263提供的所有业务均不会受到影响，黑客攻击的只是介绍263业务内容的一个很小的服务器。客户不会受到任何损失。

其实，早在去年10月中旬，便有消息称263的一台邮件服务器留有“后门”，但263有关方面却称他们“没有发现这一‘后门’”。但一些技术人员却称“后门”依然存在。

当时就有人提出：虽然该网站尚未被破坏，却并不意味着263已经彻底没事儿——这种“植入后门”的黑客行为被技术专家称为“最具威胁的攻击行为”，它就像一颗还没有引爆的定时炸弹。利用这个后门，任何一个恶意入侵者都可以轻松地远程取得超级用户权限，也就是说可以做出极具危害性的破坏。甚至可以使它瘫痪。

此次263被黑与上述的“后门”是否有关，我们还无从得知，破坏的程度263目前还没有正式对外公布。人们在谴责黑客行为和论理黑客道德时，263网络集团本身是否有“过失”或者“不作为”呢？（彼阳）

每周电脑报

安全从自身抓起

2001年2月12日

据美国CNN等报道，某个也可能是某几个黑客成功地侵入到达沃斯世界经济论坛的数据库，窃取并泄露了诸如阿拉法特、比尔·盖茨等人的个人信息。是什么造成了这次泄密：是网络露洞引起？是某些工程师卷入其中？还是数据的安全性较差？我们不得而知。

此种窃取行为危害甚大，但真正引起我关注的是世界经济论坛的信息主管Charles McLean的一段话。他说，"这些信息丢失的原因我们还不清楚，如果黑客可以攻破美国五角大楼和美国国务院的安全体系，同样也可能侵入世界经济论坛"我认为，通过指责别人犯的错误来为自己开脱并不可取。

本届世界经济论坛的安全体系花费了500万瑞士法朗（约300万美金）之巨，发生这样的事情，每个人都会认为用在数据安全人员身上的开销是何等不值。现在世界经济论坛主办者可能会后悔，应该将更多的钱用在提高系统的安全性，而不是网站的华丽外表上。世界经济论坛主办者由于自身安全意识差，而自食其果。可他们还在大声疾呼要与入侵者斗争，并大肆使用"罪犯"形容侵入者，却避而不谈其自身的疏忽。

其实事故发生的一个原因在于，安全问题没有被引起广泛的认同，也就更谈不上重视了。可见安全问题的解决已经迫在眉睫了。同时，对于数据安全的不合理的规范也是不利的。例如：一家信用卡公司研发了一种特定的技术并经权威部门批准成为该行业的标准，这样可能会因为法规的某种倾向性，很快形成一种单一的标准，当此标准存在某种弊端时，会影响到使用此标准体系的电子商务的所有[illegible]公司。值得庆幸的是，一些产品化的提议被防止发生此种错误，如开放源代码之所以经常被作为操作系统安全性基准的一个主要原因在于其核心源代码经反复审核被认为是无瑕的。

总的来说，一个重大的疏忽在于财务安排的失误。如果不是因为对安全系统的疏忽，就不会造成信息的泄露使得他们为此付出沉重代价，一切都不会发生。看一下Egghead.com的崩溃，虽然最终是由信用卡公司培偿数百万，但我认为Egghead本身要为这一切负责。那些安全意识差的公司所能做的只是将信用卡公司诉之于法律，以补偿由此造成的损害，让人不可思受。更滑稽的是欧洲某个国家的政府因违背数据保护的法规将几家公司推上法庭。

我们希望信用卡公司和它们的客户之间的这种关系在近期内有所改变，这在短期内会对陷入低潮的电子商务带来麻烦，因为这些公司不得不花上一定的时间和精力进行系统安全措施的完善，但长期来年，每个人都会从中受益。

作为世界经济论坛主办者，一旦获得信息就有义务保护这些数据。在事故发生后无论是为自己开脱还是保持沉默，而无视其数据是如何被窃取的，甚至将矛头指向别人，都是不对的。这对于世界经济论坛的信誉，特别是考虑到近来邀请一些IT界的名人参与论坛，已经引起了广泛的关注，我担心该组织形象会因此而受到损害。

许多网站还没有足够地重视保护个人信息，这种现象仍然将存在。

中国计算机报

2001年2月8日

老杜谈安全

上网你得多留心

越来越多的人们开始使用互联网，越来越多的设备可以连到互联网上，在互联网给人们的生活带来翻天覆地变化的同时，也把人们推到了一个空前危险的状态中。

理论上说，当你的计算机或者其他设备和互联网连结起来之后，它就成为覆盖全球互联网中的一部分了。而你，表面上的主人，能否完全控制你的计算机或其他设备可就难说了，因为任何一个互联网上的用户都有可能在万里之外控制你的计算机设备，让它们更换主人，而你，则可能由此成为它们损害的对象。这时候，越是功能强大的设备，对你产生危害的可能性也就越大。

计算机能做什么呢？计算机能录音，因为越来越多的人配备麦克风，而便携机更是自带麦克，于是它可以成为别人的窃听器，将周围谈话的内容通过网络传出去；很多上网的计算机配备录像设施，它们可能被偷偷启动，在地球的另一端观看发生了什么。我们现在用的都是“通用计算机”，依靠更换不同的软件来更换计算机系统的功能，但是计算机实际在干什么，我们也不知道。同样地，计算机或其他设备中也可能存在一些特殊的硬件设备，留作特殊用途。因此，存在这种可能性：某人通过远程控制，破坏你的计算机或其他设备，甚至使之发生爆炸、燃烧释放特殊物质等。前面所说的控制录音、录像之类的事情，也可以通过藏匿的硬件来实现。

以上这些听起来是不是很可怕？但是我认为这些都并非危言耸听，而且随着互联网应用的发展，威胁会更大。然而尽管如此，发展还是必须继续的，只是同时安全技术也能做到同步发展就可以了。就目前的情况而言，防火墙是不容忽视的。在很多情况下，它可以检查通过这到屏障的所有内容，正常的允许通过，不正常的禁止通过。这样，只要你能说清哪些是你正常上网所发生的数据，就可以防止其他人通过互联网控制你的计算机了。然而不幸的是，互联网底层的实现技术对大多数人而言太复杂了，他们无法做出这种区分；同时，很多非法的操作是通过合法数据格式实现的，防火墙有时也无法区分，于是我们的这个安全屏障，有时因为无法合理设置，有时因为能力有限，而不能确保我们的安全。其中前一点尤其严重，这个现象应该引起厂家和学术界的重视了。仅靠普及互联网恐怕是不足以解决这个问题的。

看来，在网上幸福遨游的同时，你还得多悠着点儿。

电子&电脑
2001年1月1日

Internet环境下的六大安全性威胁

■ Woody Leonhard / 李 琳 天 云 编译

责任编辑：项红 xh@pcc.com.cn 李丽 lily@pcc.com.cn

多虑了吗？并非如此。其实你的处境比你想像的要危险得多。可怎样才能保护自己和你的公司呢？

总有一天他们会威胁到你。只要你的Web站点、你公司的网络、你和员工在家中或旅途中使用的计算机与Internet连接或互相之间连接，就容易受到攻击。这就意味着在你的商业活动中有很大的风险。偷盗者可能会盗走你公司的机密和重要的客户信息。或者，他们只是为了寻求刺激而闯入，留下的是只有经过非常细心地检查才能发现的踪迹，更有甚者根本不留任何踪迹。

你不必费心去查找那些踪迹，有些情况下你只需快速检查一下公司的系统，确保装了最新发布的安全补丁。保护好你的网络和Web站点可不那么简单——但至少你晚上可以睡得安稳些。以下就是你必须了解的在Internet环境下最危险的安全性威胁以及应该如何应付的方法。此外，还向大家介绍了一些国内外著名厂商提供的相关产品。

Internet环境下的六大安全性威胁

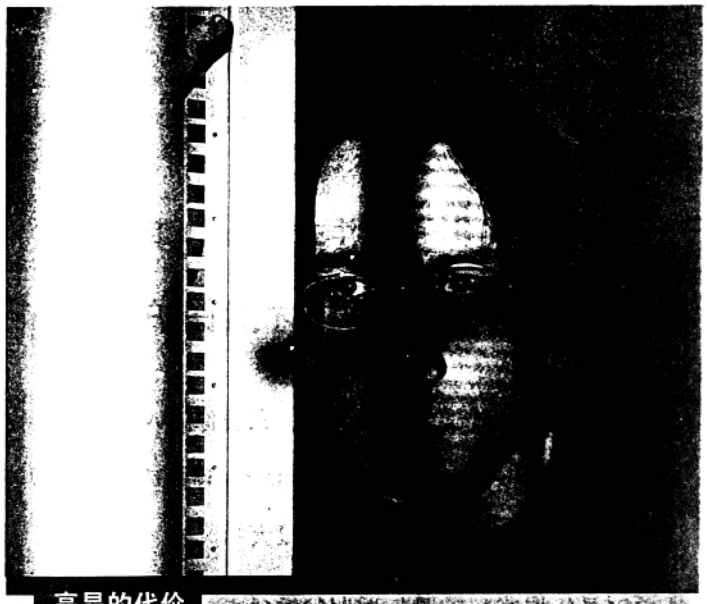
威胁：你的Web站点对外来攻击门户大开

FBI（联邦调查局）查找去年二月份传得沸沸扬扬的“拒绝服务”(denial-of-service)攻击的来源时，嫌疑人之一是一个叫库里奥(Coolio)的17岁的辍学中学生。虽然库里奥还不一定是案犯，但他承认攻击过洛杉矶警察局的反毒网站，上载了一个手臂上扎着毒品注射器的唐老鸭图片。

黑客们闯入并修改网站的行为已经不仅仅限于上载吸毒的鸭子图片了。总统预选期间，有Gallup Organization投票结果的网站被暗中修改了；黑客们丑化白宫、美国参议院和海军服役作战中心的Web站点；美联社的站点也受到了攻击；受到攻击的还有：C-SPAN、ABC、Yahoo、Greenpeace和Weather Channel。

黑客们丑化网站最常用的伎俩是贴一个令人震惊的页面，页面的设计通常是业余水平，外加令人费解的文字垃圾。然而更阴险的是对原有网页的修改，这种修改可能不大容易被检查出来。想像一下把Gallup网站上的投票结果篡改成一个没什么名气的候选人获胜，或者使美联社发布虚假的自然灾害报道，该是怎样的后果呢？如果你公司的联系电话被改成你竞争对手的怎么办？或者客户点击你站点上的“购买”按钮却将自己的信用卡号码发送给了不法之徒又怎么办？

要用冒牌网页替换你的网页，首先黑客必须能够访问到你的Web服务器。防范此类攻击的第一个要点就是禁止访问保存网页的目录。如果你的Web站点放在Internet服务提供商那里，则要查明为了保护你的站点不人修改他采取了哪些安全措施。如，MSN通过MSN Passport系统



高昂的代价

忽视Web站点的安全不仅会造成经济损失，还会使客户对你不信任。加拿大一家移动电话和寻呼公司对此深有体会。两个来自威尔士的少年闯入该公司的Web服务器，偷走了客户的信用卡号码并公布出来。Hexedit网络安全公司逮住过攻击者的Chris Davis（见照片）说“没有人会百分之百的安全，但如果大们能够保证所用的安全软件及时更新，则被攻击的机率相对要小得多。”（Hexedit负责保护该无线通信公司的网络安全）。但电话公司一位发言人承认“每天都会发现新的安全漏洞”。

Internet环境下的六大安全性威胁

所有的访问，并且在服务器上做全面的安全检查。你有权享有ISP提供的全部安全服务。

同时也要关注大型网站最近是否被攻击过。如果你的ISP也是被攻击的目标，则更要加倍仔细地检查你的站点。要获得最新被攻击站点的列表，可参看www.attrition.org/mirror/attrition。如果要将Web上的网页和你保存在计算机中的原稿进行比较，则Romeo Tango Software(www.romeotango.com)定价5美元的共享程序File Compare效果不错。

如果你的Web服务器运行的是Unix，则安全问题更复杂。Sun Solaris 2.x的用户应该在www.sunworld.com/sunworldonline/common/security-faq.html上查看Peter Galvin提供的Sun安全FAQ。该站点提供了大量很有价值的提高安全性的技巧。对于www.redhat.com/support/errata/rh61-errata-security.html处的Red Hat Linux 6.x安全公告板也应该高度关注。（该产品的注册用户可以通过Red Hat的FTP站点上的Priority Updates更快地获得这些信息。）

由Microsoft正式发布的关于Windows NT和Internet Information Server的安全性信息可在www.microsoft.com/security处找到，而且你还可以在www.microsoft.com/technet/security/iischk.asp找到来自Michael Howard的特别有价值的检查列表。

五个保护网站安全的好方法

如果是由ISP管理你公司的Web站点，那么以下是你目前能够做的最重要的事，以确保你站点的安全性得到保障。

1、与ISP联系并询问他们采取了什么安全措施来保护你的Web页面不被人非法修改。你（或他们）还能够怎样进一步提高安全性？

2、确保更新Web站点的人员必须注意：要定期更改口令；在离开计算机之前退出正在修改的Web文件。

3、每天都要对你站点上的重要页面做备份，这只要浏览那些页面并选择File（文件）和Save As（另存为）即可完成。

4、将Web页面的备份像其他重要数据一样保存好。

5、备份的时候，将每个当前页面和最近一次的备份进行比较。如果发现它们之间有不同之处，则应该从你的ISP那要一份日志查看一下什么人访问过你的站点。

威胁：黑客可能利用你去搞垮其他公司

去年二月份使Yahoo、eBay、Amazon.com、Buy.com、ZDNet和其他很多网站陷入瘫痪状态的“拒绝服务”攻击并不新鲜。但这些事件在以下两方面有别于其他类似事件：造成损失的程度（估计超过了12亿美元）和所采用的技术。

对Web网站进行“拒绝服务”攻击的基本原理很简单：攻击者频繁地访问一个站点，使合法的访问者无法进入。在分布式攻击中，黑客接管了大量连接到Internet的计算机，并让这些计算机同时发起对该站点的攻击。这些被秘密占用的计算机被当作“炮台”，响应来自攻击者的攻击命令，而攻击者则自得地躲在幕后。

最容易受到“拒绝服务”攻击的站点是那些你已经有所耳闻的eBay、Yahoo、Amazon.com等。很多不知