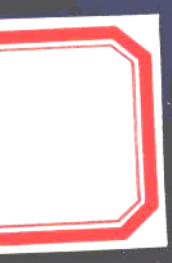
信息安全动态

5

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

信息安全动态第五辑目录索引

✧ 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

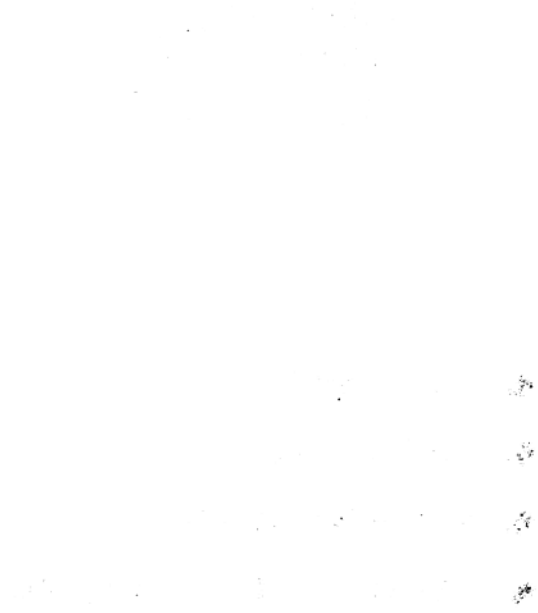
✧ 九、趋 势 篇

✧ 十、安全锦囊

警钟篇

- 高筑“信息边疆”
- 警惕网上“黑社会”
- 计算机安全的潜在威胁
- “克林顿”、“裸妻”等新型病毒出现

……



中国计算机报

2001年2月26日

高筑“信息边疆”

涉及到国家安全经济安全的专用网络与公用计算机网络物理隔离。

利用光缆、微波、卫星等不同通信手段保证网络安全。

加强计算机网络安全的管理。

信息技术永远是一把双刃剑，既造福人类，也带来了信息安全问题。中国工程院院士沈昌祥表示，信息网络国际化、社会化、开放化、个人化的特点使国家的“信息边疆”不断延伸，甚至到了每一个上网者个人。国际上围绕信息的获取、使用和控制的斗争愈演愈烈，信息安全成为维护国家安全和社会稳定的一个焦点，各国都给以极大的关注与投入。信息安全保障能力是21世纪综合国力、经济竞争实力和生存能力的重要组成部分，是世纪之交世界各国在奋力攀登的制高点。我国在发展信息产业的同时，一直把安全问题放在重要位置。吕副部长介绍说，在“十五”期间，要“建设并完善国家级网络管理中心，统一监控并可调度全国网络资源，完善党政专网和应急通信网。涉及到国家及经济安全的专用网络与公用计算机网络物理隔离。利用光缆、微波、卫星等不同通信手段保证网络安全。合理优化光传输网络布局，加强传输网路由保护，提高可靠性。加强计算机网络安全的管理，防止计算机网络受到侵害，防止有害信息的传播。”

技术进步将促进信息产业的经济增长，为信息产业发展提供有力的技术支撑，为国民经济和社会信息化提供有力的技术支撑。

（李滨寒）

中国计算机报

2001年3月8日

网威博士谈安全

网络安全至关重要

随着政府上网、海关上网、电子商务、网上娱乐等一系列网络应用的蓬勃发展，Internet正在越来越多地离开原来单纯的学术环境，融入到社会的各个方面。一方面，网络用户成分越来越多样化，出于各种目的的网络入侵和攻击越来越频繁；另一方面，网络应用越来越深地渗透到金融、商务、国防等等关键要害领域。换言之，Internet网的安全，包括其上的信息数据安全和网络设备服务的运行安全，日益成为与国家、政府、企业、个人的利益休戚相关的“大事情”。安全保障能力是新世纪一个国家综合国力、经济竞争实力和生存能力的重要组成部分。不夸张地说，它在这个新世纪里对一个国家的重要性完全可以与核武器相提并论。

美国政府对网络安全的研究起步很早。1985年，美国国防部基于军事计算机系统的保密需要，制订了“可信计算机系统安全评价准则”（TCSEC），随后又制订了关于网络系统、数据库等方面的系列安全建议，形成了安全信息系统体系结构的最早原则。美国政府将网络安全产品当作战略武器，严格限制出口的种类。并且，从新闻报道分析来看，它有意容忍黑客组织的活动，目的是使黑客的攻击置于一定的控制之下，并且通过这一渠道获得防范攻击的实战经验。

目前我国对计算机网络安全产品的认证研究刚开始起步，尚没有对计算机安全发布权威性的标准方案。新刑法中关于计算机网络犯罪的条款也没有解决法律上的问题。例如，上海热线杨威入侵案的审理过程说明了新刑法在新兴的计算机犯罪的定罪和量刑上的模糊不清。所以，不管在设计网络安全方案时，还是在确认事故、攻击、入侵等级时都显得无所适从。对于企业来说，尤其是大的ISP，等待国家去研究发布相应的标准是不恰当的。应当尽快组织自己的IT部门或购买其它公司的相应服务来确立自己企业网的安全策略，并且下决心去实施，而且要定期地检查实际情况与安全策略的差距。

应该说，Internet技术是一把双刃剑，它在为我国国民经济建设、人民的物质文化生活带来促进和丰富的同时，也对传统的国家安全体系提出了严峻的挑战，使得国家机密、金融信息等面临巨大的威胁。

国际经贸消息
2001年3月8日

网络诈骗：电子商务的羁绊

本报讯 连大名鼎鼎的比尔·盖茨的信用卡数据都被黑客盗取，难怪网上消费者对因特网诈骗倍加关注了。这也是电子商务不能得以迅速发展的主要原因之一。

分析家认为，消费者和经销商可能因网上诈骗损失巨大。官方数字很难统计，但美国一个咨询机构近日发表的统计数字显示，2000年全球范围内网上被骗金额为16亿美元，其中大多数事件发生在美国。该机构还推测，随着网上支付数额的增加，预计2005年网上损失金额将达到57亿美元至155亿美元之间，这取决于各国对反网络诈骗技术的投入力度。

网络诈骗已达到了让经销商难以接受的地步，通常他们总收入的10%被骗走。但被诈骗金额比例应该呈下降趋势，因为网络安全技术在不断发展，经销商也变聪明了。

消费者可能被引诱进入诈骗网站，信用卡号轻易地被拿走。有的网上骗子假冒经销商，收了钱却不发货。还有人则用假冒或盗来的信用卡支付账单。

不过，一家网络安全公司认为，随着安全技术的不断完善，网上消费者对网络安全没有必要过度担心。（宁硕）

北京晨报
2001年2月27日

警惕网上“黑社会”

本处于严寒时期的互联网，现在又有一种隐约的不安渗透在行业的核心深处。一向热情高涨、无所畏惧的.com公司变得有些无所适从，这就是商业黑客的频繁行动。这些被世俗之气浸染的黑客们，在显示技术能力的同时，对各网站施展了新的威胁、利诱手段，榨取钱财，并形成一股不可忽视的势力。这个群体被人形象地称为网上黑社会。

先攻击后敲诈
网上黑社会露头

就在一个月前，国内著名网站263网络集团的业务主页服务器遭遇黑客攻击。包括服务器托管、虚拟主机、宽带接入、合作渠道、ASP业务、ISP业务、主叫计费、IDC等业务页面几乎在同一时刻全部被侵入。

像许多被黑的网站一样，利益受损者263对此事选择了高度的低调处理。在实在需要表个态时，263也没有对黑客的行为指责一二，只是告诉消费者和客户们：“263提供的所有业务均不会受到影响，黑客攻击的只是263业务内容的一个很小的服务器。客户不会受到任何损失……”

而知情人透露出的一些相关信息令记者震惊。如今互联网世界不但每每月黑风高之时，黑客频繁活动，而且渐渐地许多事情在金钱面前改变了方式，找到了答案。一些具备黑客技能的人，开始频频对网站进行敲诈、勒索，甚至索要保护费，宛若旧时的黑社会势力。这令在新经济中曾经充满神秘色彩的网络精英看起来破落不堪。

毫不夸张地说，所有的网站在运行的分分秒秒中，都是在与黑客的较量中度过的。据国内一家知名门户网站透露，从对防火墙的监控中可以看出，平均每天都会有上万次的攻击。一旦哪里出现纰漏，网站就将出现难以收拾的局面。而且很奇怪的情形由远及近，出现在每个网站的视线里：越来越多的黑客在攻击完网站之后，会自动找上门来，谈条件，要么交钱，要么买我的设备，以换得平安。

发生在当前十分火爆的一个聊天软件网站的事件则可以说是比较典型的例子。据这家网站透露，网站的管理层一员收到一封电子邮件，邮件中说，“当天你的网站要受到攻击，如果你们明白怎么办，便可避免此劫。”大家都当是个恶作剧。结果却真的如邮件所言，网站准时遭到了致

命攻击，整个系统瘫痪了数小时。这位人士忧心忡忡地说："侠义的黑客攻击网站本属正常，且对我们的技术提高有好处，但现在的情况却明显是商业化、有组织的行动。这对尚在成长期、需要呵护的互联网产业来说，是个不好的信号。"

一家不愿透露名称的专业门户网站CEO对此深有感触："只要我们一有活动，比如搞市场推广、直播、请嘉宾聊天，网站增加人气、流量大时，几乎百分之百会受到攻击。往往攻击后的半个小时电话就准确地打过来："听说你们遭到攻击了，我们这里有全套的网络安全解决方案和设备，需不需要服务？"另外一种神秘电话是这样："未经允许我们已经扫描了贵网站，找到了5个漏洞，你们需不需要解决一下？"这些看起来雪中送炭似的信息，久而久之就令人觉出滋味不对。事实的确如此，如果你干脆表示没兴趣，对方还跟你展开周旋："那以后类似的攻击还会有不少！"

国防科技大学计算机学院所做的研究课题表明，目前我国95%的与因特网相联的网络管理中心都遭到过境内外黑客的攻击或侵入，其中银行、金融和证券机构是黑客攻击的重点。现在发展到了以商业网站为新目标，国内几乎所有稍具知名度的网站在这个问题上均成为一个阵营的难兄难弟。据说这样的事情并非"中国制造"，许多国外跨国公司也遭遇过同样的命运。微软、YAHOO、CNN等著名网站同样难以回避黑客的光顾。

由于在这样的事情上，更多的网站选择了沉默；由于具有商业目的的黑客活动从不公开，私下的小组织形式也算严密，其群体到底有多大，收益有多少尚难以调查。但业界有关他们的一切感觉却是真实的。

明火执仗为哪般——网站亟待强心剂

不管是资金雄厚的门户网站，还是各类专业网站，对这种新生的商业黑客现象似乎同样缺乏免疫力，只有束手就擒的份儿。这让我们忍不住这样想，是什么因素造成了这个黑社会形成的土壤？网络公司的DNA中到底有什么先天的缺陷令邪恶的势力得以明火执仗？

记者在采访中发现，几乎所有被黑过、被勒索过的网站，都采取了息事宁人的态度。一方面对黑客畏惧有加，一方面是自身抵御的本事有限。

据有关专家介绍，目前互联网使用的是IPV4技术，这源于20年前互联网发展的早期特征。当时互联网的主要应用是军事和教学，注重的是网络的开放、共享和灵活，从技术本身讲，并不具备当前世界无所不在、日益复杂应用的特征。自20世纪90年代起的网络全面商业化之时起，技术人员就不断告诫世人，使用原有的IPV4技术，会造成一系列无法克服、无法回避的网络致命问题，比如网络线路瓶径、安全性差、易受攻击等。但整体的情况却并未得到实质性转变。

具体到我国的商业网站，境况更是令人担心。愿意说实话的网站自己都承认，现在整个互联网的安全措施都比较差。几乎所有的网站在开创及发展时都更注重便利性和实用性，而忽略了最根本的网络安全问题。造成技术、管理和基础设施漏洞百出，有些干脆就是"一座不设防的城市"，包括最需要重视安全防卫的电子商务公司，在网站初建时大多都不设防火墙，或用简单的独立IP形式进行安全防卫。一位真正的黑客说："只要我敲击键盘的速度足够快，可以一天黑掉100个网站。"

网络公司这么做，目的之一是为了省钱，就防火墙产品来说，国内的要20多万元，国外产品则要50多万元，再加上技术人员的费用，对网络公司来说是不能不算计算计的。加之现在就是上市圈到了钱的网站也都将增收节支看成经营头等大事，在外表和内在之间，往往最先选择的是外在的市场炒作而非自身的丰实。二是当一个商业黑客并非难事。互联网上已有3万多个黑客网站，随便在任一家门户上搜索一下，就会发现各种各样的黑客工具，技术不断创新，服务细致齐全，基本的攻击手段就已有800多种，稍具专业知识的人，下载一个黑客工具出一次手并非难事。

在魔道相争的过程中，商业黑客也已摸清了网站的处事之道，黑完之后，立即向这个网站的对手或能打上交道的媒体通报，将事情大张旗鼓地抖落出去，往往这么一来造成的影响是网站最难以承受的，选择低头就范也是不得已的选择，小不忍则乱大谋嘛。

大多数网站对行侠仗义的黑客都敬畏多于反感。因为真正的黑客只是一群技术高手，他们标榜的自我特征就是清高，反商业化。进入网站却极少恶意破坏，只为显示能力。他们也不轻易出手，用一位黑客的话说："更多时以网络安全的管理者、爱好者的身份出现。"网站在标榜自己的技术人员水平高时，最爱用的一句话也是——他们都是黑客级的高手。网站对黑客的这种认识与心态，客观上使商业黑客有机可乘。一位黑客很不屑地抱怨："现在国内黑客群体的道德观与操守尚待重建，那些拿着别人开发的软件四处'撬锁'的商人，还打着黑客的名义，根本不入流。"

法律上的疏漏也责无旁贷。据联合国下属一家互联网政策调查公司的调查，大多数国家并未在遏制网络犯罪方面制定严格的法律条款，或现有的法律不足以对这些势力构成威胁。这不但对网站的运作是个极大利空，并有可能抑制互联网作为一种通信、商务交易以及教育手段得到快速发展的能力。

亡羊补牢为时未晚——紧急搭建防黑网

每一项新技术带给世人的都是浮士德式的交易，他伸出的无形之手，带给你难以抵御的诱惑的同时，也给产业的游戏规则和道德层面带来新挑战。黑客与互联网技术相生相长也是如此。但被黑的网络公司仍觉心有不甘。特别重视信息产业的我国政府部门也从未袖手旁观。各方痛定思痛之后，一层防黑网悄悄搭建。

在黑客搭建的黑社会势力日益壮大的同时，反黑的力量也在壮大。自去年开始，从硅谷回国的留学生在国内创办了大批网络安全公司。启明星辰CEO严望佳告诉记者，这些人都是在美国多年研究反黑技术的人，掌握着世界最前沿的技术。初步统计，国内各类网络安全公司已超过千家，许多网站也愿意把自己的安全问题交给他们管理，这样专业化的分工正成为一种良好趋势。

今年年初，四川中城网络、中科陆军曙光公司、中科红旗软件公司、光明传媒股份、东方蓝牙通信等12家著名企业成立中国C网联盟，集合众家优势，开发出中国人可以自主的开放、高效、安全的互联网络。各种各样的网络安全论坛也多了起来，一种共同反黑的气氛陡然间浓烈起来。

另一个比较好的迹象是，这个行业的顶尖高手正充实着反黑力量。当年赫赫有名的四大网络安全组织中，深圳辰光工作室、福建天行软件王国、湖南中国黑客技术研究组织、安盟科技，加上著名的绿色兵团，都能够从黑客的独特思维方式入手，研发反黑战术。他们为这个行业带来的正义气息甚至大于其技术贡献。

国家在研发领域上的战线也已悄悄拉开。据有关方面介绍，目前国内一些部门已开发研制了防火墙、安全路由器、安全网关、黑客放侵检测、系统脆弱性扫描软件等。国家还成立了有关信息安全产品评测认证机构，已有100多个产品进行了评测检验。

法律的跟进工作同样在进行之中。《关于维护网络安全和信息安全决定(草案)》中规定，“利用互联网实施违法行为，尚不构成犯罪的，由公安机关依照《治安管理处罚条例》予以处罚；违反其他法律、行政法规，尚不构成犯罪的，由有关行政管理部门依法给予行政处罚。此外，据记者了解，地处北京的各网站与公安部门一直都保持着密切联系，并定期回馈有关黑客攻击、病毒等情况，大的方向尚能在官方掌控之中。

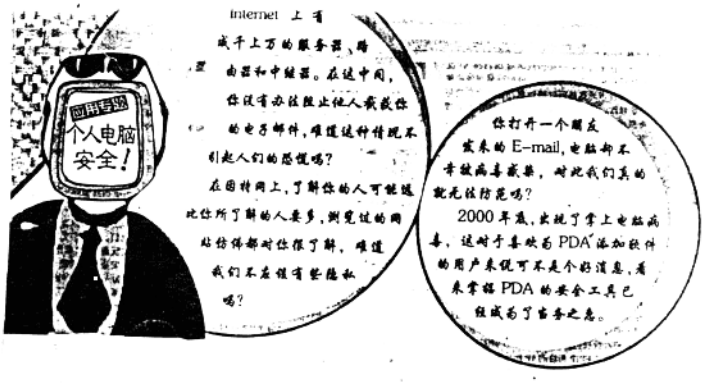
业内专家认为，有互联网就必定有黑客的存在。当前出现的这种运用类似黑社会手段行事的商业黑客，已属技术讹诈范畴。如何对待这种现象，对新兴的互联网产业来说，尚是新课题。可悲的是，黑客的DNA似乎总有许多变种，让人无所适从。正义的一方总是渴望完全破译魔道的世界，但似乎总在门外徘徊。

也许网络公司生存的奥妙本是玄机莫测，通向答案的道路也不只一条。各方对商业黑客有足够的重视与打击之后，互联网公司也许真的可以安心享受纯粹的技术魅力与快乐时光。这一天的到来，也许在不久，也许要永远。

晨报记者 刘书

中国计算机报

2001年3月5日



计算机安全的潜在威胁

——防御黑客、跟踪者和病毒的攻击

【北京 杨兵】

现在假设你收到一封新的信件，信的标题表明这是一位林小姐的简历。可你并不认识她，但有一点可以肯定：E-mail的附件里有一个文件名为Resume.doc的Word文档。那么，看一眼这个附件应该不会有问题吧？

不，请再仔细想一想！打开一封来自未知地址的E-mail，尤其是同时又有附件的信，相当于告诫你的孩子从陌生人手中拿糖果一样危险。如果你打开那个Resume.doc，可能会将简历病毒(Killer Resume Virus)带到你的计算机中。病毒程序将会抹去所有从A盘到Z盘的数据。不仅如此，如果你使用Outlook收发E-mail，含有病毒的文件会被发往地址通讯薄中的每一个E-mail信箱，以至于病毒给你带来的悲哀同样会波及到你的朋友、家庭成员、同事或者你的客户。

病毒程序会搜索计算机的数据，或在电脑上即时安装程序、载入病毒。如果没有特殊的工具，你根本无法察觉到。也许在你上网时，有些公司正在跟踪你在网上的每一个动作，收集你上网的常用数据，从而改进它们的广告宣传策略。或者，它们可以将所有从你的姓名、地址到购物习惯的数据提供给需要的公司，也可能将这些信息建成邮件表。同样，所有这些操作都不会让你发现自己是目标。我们无法完全摆脱通过Internet网络进行的这些跟踪，同样也无法拒绝使用那些有安全漏洞的软件。

当然，我们不能为防止病毒或跟踪就切断网络连接，那么该怎么做呢？我们教你如何预防安全问题，怎样处理出现的各种灾难。首先介绍一下可能的安全问题。

窃取信用卡号

你最近检查过你信用卡上的钱款吗？很有可能一个陌生人已成功地从你的信用卡上刷走了很多钱，而他从没有看过你的信用卡。

即使你想尽了一切可能措施保护信用卡

号，也未必是安全的。如果你在某个商店用了信用卡购物，该商店会保存相应的交易记录，一般存放在某处的数据库中，也许就会有人侵入数据库窃取你的信用卡号。

如果想预防，你需要熟悉网络安全和加密算法的相关知识。其中，加密算法可以加密数据，几乎任何人都不可能读取。这样，就可以保证数据在网上安全地传输，从而改进公司的安全策略。

我们可以知道你是谁

上文我们提到直销公司无时不在想尽一切办法跟踪人们的上网习惯，一般他们都通过Cookies的文件实现习惯数据的采集。如果没有Cookies，网络站点就无法了解你是怎样从一个网页转到另一个网页。如今网上普遍的在线购物车也不可能实现，因为站点无从了解顾客在以前访问网页上的选择项。

Cookies文件是网站发往用户计算机上的小文件，这样公司可以了解顾客在网上的行为。如果我们使用了基于网页的E-mail信箱并选择了允许浏览器"记住"你的密码，以后再访问E-mail时就不用再敲密码了，因为密码信息已经被保存在计算机的Cookie文件。信息是否被加密取决于访问的网站如何使用Cookie（如果Cookie中包括敏感信息，网站一般都会对信息加密）。

一般情况下，Cookies不会有安全威胁，而且还会带来方便。理论上，最理想的是只有存储Cookie的网站有权使用它。像其它跟踪行为的技术一样，Cookie应该仅限于正当的使用。

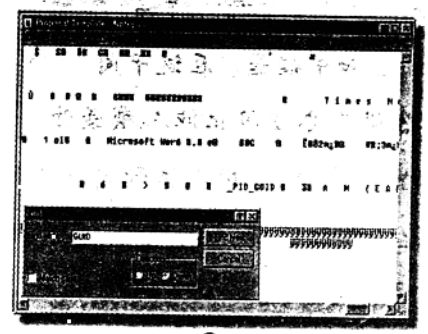
我们可以用浏览软件或第三方应用软件管理Cookies，但要欺骗每一个网站保持的服务器端访问日志是非常困难的。一个网站可以知道用户在访问它的网页之前浏览的站点，并在进入该网站后记录在每一个页面上的停留时间，同时标记在网站上填写的数据，比如你的年龄和婚姻状况等。我们建议你在填写数据时不要将任何可选信息的数据填入表单。下文我们将给出一些高级技巧帮助你摆脱网站的追踪。

不过确实也有一些嵌入式具有跟踪能力的幽灵，比如微软对其产品添加的GUID(全球惟一标识）就使用了一个标识数字对Office 97文档进行标记，这样可以在必要时回溯到原始用户。微软声称这样可以帮助用户记住文档的每一次修改，但也有人猜测微软会计划用GUID搜集用户数据。如软件Office 97，我们可以在记事本中打开Office 97文档，查看是否有一个GUID嵌在文档里(见图1)。早几年，Intel公司由于在它的Pentium Ⅲ处理器产品内嵌入统一编号的数字标识而受到谴责，因为该数字曾被用作跟踪用户行为的线索。公众的反对虽迫使Intel公司放弃原来的主张，但在软件和硬件产品上使用标识符的尝试仍然有可能会持续下去。

密码盗用和文件窃取

恶意的人总是将高级技术应用于形式古老的诡计，盗用用户的账号密码和被传输的文件。在技术上，他们使用的技巧类似于IP包探测器。Internet网上传输的数据在传送前被分成许多很小的数据包，每一个包都有发送数据包源计算机和接收数据包目的计算机的IP地址。如果某一个计算机的IP与目的IP地址不相符，它是不能在中途拦截数据包的，但数据包探测技术可以帮助做到这一点。数据包探测技术可以检查所有落入其范围的数据包，甚至能够通过设置来攫取所有的数据包。不过，运用密码技术可以阻挡数据包探测的企图。

说到恶作剧的手段，简直数不胜数。最新的



图❶

一种诡计做法染指到网站PayPal (http://www.paypal.com/)。PayPal站点允许会员方便快捷地进行网上交易。罪犯给人们发一封好像来自于PayPal站点的E-mail，并在E-mail里提供PayPal网站登录页或者看起来像是登录页的链接。这些窃贼同时建立外观很像PayPal站点的网页，然后在用户链接到该网页登录时捕获所有的用户名和密码。随着目前越来越多的网上服务出现真钞交易，这种欺骗手段就会不断滋生，所以我们必须知道如何保护自己的财产。

病毒的繁殖

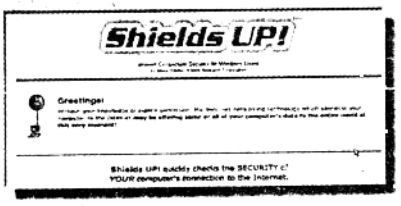
大多数计算机使用者都听说过病毒。这种令人讨厌的代码片段确实名副其实：只要一台计算机感染了病毒，就会导致毁灭性的破坏，然后再传播到另外一台机器上。因此，给自己的机器安装好的防火墙，随时更新杀毒软件，尽管不是100%有效，但却是非常必要的。

有些潜伏病毒更是可怕，比如以前出现的Hybris虫(一种破坏性的程序，其中有一部分代码允许程序自我复制直到充满整个目标驱动器或网络，从而使计算机无法工作)。一旦这种病毒出现在你的机器上，它会通过网络自动升级，使病毒创建者更容易控制你的机器。目前这些恶毒的程序手法越来越老练，因此需要更好地了解防范病毒的工具和技术。

宽带网的入侵机会

DSL(Digital Subscriber Line)和电缆调制解调器等宽带网络的连接设备正风靡全球，因为它们提供了拨号网络无法达到的性能和便捷。ISP网络服务商声称这种连接是永久的，即它们一直在运行状态中，因此不需要用户每次上网时都要拨号。尽管宽带网的这个特征确实很方便，但同时使网络更易于遭到安全攻击。

当拨号网络的用户结束网上冲浪，断开网络连接时，他们就已安全地远离了外部攻击。但宽带网的用户除了要面对以上危险，还会有更多的危险等待他们。当他们关闭浏览器，开始使用办公软件或玩游戏时，网络连接仍然存在。除非安装高级安全软件或硬件，计算机对外界是可见的。比如入侵者可以通过端口扫描器探测你的计算机系统的安全漏洞，任何一个打开的端口都会成为接受攻击的入口。



图❷

我们曾经听到过这样的事：某个宽带网用户收到一封言辞很生气的E-mail，信中用不确定的术语告诫该宽带网用户不要再扫描他的机器端口，其实该用户根本没有运行过端口扫描软件。这表明中间有个入侵者闯入了收信用户的计算机，远程安装端口扫描软件并控制该用户的计算机去探测其他网上用户的系统。这样，原始入侵者就不易被发现。不过，下面的文章中将教你使用防火墙和代理服务器把那些坏人拒之门外，或使用杀毒和其他安全软件帮助系统在有害文件和病毒产生损害之前就摆脱它们。

你是攻击目标吗

很多主要的安全问题，如上文所述，虽很少见但随时可能发生。但使用者可以通过很多方法使自己的系统更安全。

首先，不要立即升级软件的最新版本，尤其是网络浏览器、E-mail收发程序、操作系统软件和办公等方面的软件。多数病毒会伴随某一个特定的软件，而且更多的是利用新版本软件的安全漏洞编制病毒。例如，几乎每一次微软发行最新的Internet Explorer版本时，黑客就能发掘出其安全漏洞。所以，通常情况下最好等到补丁或服务包出来后再升级老的却很安全的软件。升级后还应时刻关注软件开发商的站点上有关安全的警告和解决办法。

如果你担心网上被跟踪，可以尝试使用Anonymizer.com公司提供的软件(http://www.anonymizer.com/)，它可以虚拟地抹去你在浏览网页时的标识。也可以试试Gibson Research的Shields UP!软件(见图2)(http://www.grc.com/)，它可以告诉你PC机的安全漏洞并会给出问题可能出现区域的完整报告。

计算机产品与流通

2001年2月26日

让病毒远离无线设备

目前，在国内的许多杀毒软件正在由单机版向网络版发展的时候，针对无线设备的国外杀毒软件开发工作已经热火朝天了。

去年年末，国外针对无线领域的杀毒软件已有多家见于报道：Central Command以及它的合作伙伴宣布推出面向手持设备的反病毒产品AVX；McAfee推出无线设备病毒扫描引擎；Brightmail推出邮件过滤产品防止垃圾广告邮件；美国网络联盟开发了用于移动手机的无线反病毒技术等。当无线设备领域病毒还没有真正肆虐之前，许多国外厂商就瞄上这块肥肉了。

先前，已经有许多专家预测无线设备病毒的到来，但是目前还没有大规模出现的迹象。11月末在东京举行的电脑病毒国际会议“AVAR 2000”上，多位专家对“手机病毒”发出了警告，虽然目前还没有关于手机感染病毒的报告。不过，据说今后随着在手机中附加Java功能的增多，将有可能出现手机病毒。

由于当前以及未来移动设备的反病毒安全要求可能差异很大，当前大多数蜂窝电话不能够重新编程，这样可以防止用户向移动设备输入恶意代码，但高度智能化可编程的下一代手机将很脆弱地面临对病毒袭击。

增长的标准化

短消息服务SMS (Short Message Service)是一个相对标准的peer-to-peer通讯系统。当前，它允许手机用户互相发送文本消息。在将来，SMS将允许发送程序，这就增加了传播蠕虫的危险。在目前，无线供应商还没有统一的标准，针对一种移动设备而设计的病毒袭击将不会象病毒制造者希望的那样——产生大规模的效果。比如，Windows NT或者Microsoft Outlook Express不会受到病毒攻击的影响。当无线设备用户增加了，可能建立起统一的标准，到那时恶意代码作者发动大规模的移动设备进攻就要容易得多了。

还没有单一的方案解决移动设备的病毒保护问题，这是因为大家日益认识到，每个商务系统安全的脆弱性就像它们的商务活动一样，与别人是不一样的。然而，好的反病毒安全方案将移动设备作为整个商务信息系统的一部分。什么是好的方案呢？

保护网络级别的移动设备

通过家庭商务网络或者外部资源，一个好的安全方案能够保护每一个移动设备免受病毒感染。既然每一