计算机百科知识

计算机网络病毒

(四)

本书编写组　编

山东科学技术出版社

图书在版编目(CIP)数据

计算机百科知识/本书编写组编．—济南：山东科学技术出版社，2003

ISBN 7-5331-1651-8
Ⅰ．计… Ⅱ．本… Ⅲ．计算机网络—基本知识—汇编
Ⅳ．TP39
中国版本图书馆 CIP 数据核字(2003)第 004271 号

山东科学技术出版社出版发行
(济南市玉函路 16 号 250001)
全国各地新华书店经销 莒县新华印刷厂印刷
开本：787×1092 1/32 印张：240 字数：4 000 千字
2003 年 7 月第 1 版 2003 年 7 月第 1 次印刷
印数：1～1 000 册
书号：ISBN 7-5331-1651-8/D·112
定价：698.00 元

目 录

黑客冒充银行骗取密码 工行急发重要提示

经历了骗取个人 OICQ、个人邮箱的密码的“小打小闹”后，不法分子又将“贼眼”瞄上了网上银行客户的卡号和密码。近日有不法分子盗用银行网站公开信箱，假借“网络银行系统升级”名义，给网上银行注册客户发送邮件，索要网上银行注册客户的用户名(登录卡号)和密码。为此，工商银行已发布紧急“重要提示”，提醒网上银行的客户千万不要把密码泄露。

已经收到这样邮件的张先生提供线索时说，他近日就接到了这样一封邮件，是从银行的公开网管邮箱里发来的，上面清楚地写道，因为“网络银行系统升级，为确保您网络银行的安全性,请重新输入用户名与密码!我们将重新帮您查核验证!”后面还留出了客户要填写的网络银行登录卡号、密码的填写位置，并要求客户把填好的表格发至另一个信箱(cLIng@163.com 信箱)。张先生表示，他以前也曾收到过类似的敲诈邮件，都一笑而过，但看到从银行官方网管邮箱里发出的 E-Mail，还真有些犹豫，不知道到底该不该相信？

记者在工商银行的官方网站上看到了刊发在显著位置的“重要提示”，其中写道：“在任何情况下，若发现上述通过邮件、信件或电话等任何方式要求提

供网上银行用户名(登录卡号)和密码的，客户要坚决予以拒绝，防止泄密，保证网上交易的安全正常进行。近期若收到冒充我行公开网管邮箱要求提供网上银行用户名(登录卡号)和密码进行验证的客户，要坚决予以拒绝；若收到类似邮件并已经提供网上银行用户名(登录卡号)和密码的客户，要立刻修改密码。”

有关银行人士介绍说，其实银行自身的网上银行系统安全性是非常高的，采用高强度加密算法、SSL安全加密技术、专门的网上密码以及多种业务控制手段，都要通过全国权威的专门性金融认证，完全能够保证客户的个人资料、信用卡信息不被商户或外界获取。但是相对而言，网管的公开邮箱安全性就要差得多，这也给充当“黑客”的不法之徒以可乘之机。而个人网上银行功能的多样性，能为客户提供账户之间的转账、外汇买卖、证券业务、在线消费支付、代缴费用、异地汇款、个人质押贷款、个人理财等一系列服务。如果客户放松警惕，让不法分子真的这么轻而易举拿到卡号密码，后果将不堪设想。

因此提醒广大市民，千万不要把个人的银行账号、密码告诉他人，即使在银行柜台办理业务，工作人员都不能询问客户账户密码，更别说把银行密码在网上发送。

五月病毒增加 Windows 新病毒有蔓延趋向

领导全球网络防毒及网络内容安全软件与服务的趋势科技近日公布了五月份十大病毒排行榜。计算机病毒爆发率在五月有显著增加，从四月所记录的低水平开始回升，四月是今年以来最平静的月份。趋势科技在五月发表的病毒报告中，包括两个中度风险的`黄色警戒`，与四月相比，危险有增加的趋势。

其中两个新病毒引起了大众的高度警戒，并且排进了前十名。5 月 13 日发现的 FIzzeR 费滋病毒（Worm_FIzzeR.A），通过电子邮件及共享网络的 Kazaa P2P 散播。就像目前许多的`混合式威胁` 型病毒，它包含有后门程序（keyLoggeR）的设计，以便偷取资料。另外，它也可以附着于 IRC（Internet ReLay Chat），此工具常用于程序设计者和黑客之间的沟通渠道。该病毒的角色是设法打乱 IRC 的流量，因此引起许多 IRC 的使用者一起联合对抗此病毒。一些观察家也已经发现 FIzzeR 病毒可以躲在错误的程序或在某些有问题的程序代码中。同时专家也警告说，该病毒在设计者的引发下将可轻易的蔓延开来。

紧跟在 FIzzeR 病毒后面的是 SobIg.B (a.k.a。PaLyh.A) 病毒，可以瞒过 Microsoft 的电子邮件，

假扮成一份从软件公司技术支持人员所传送过来的讯息。整个骗局非常简单，却也足以让许多使用者上当，让他们轻易的打开电子邮件的附件，却从未想过为什么 Microsoft 会随随便便传送档案过来。SobIg.B 还有一个不寻常的功能 - 在它的程序里有一个防止它在 5 月 31 号以后散播的指令。已经被感染的使用者还是需要将该病毒找出来并删除掉病毒附着的档案，还好的是，其内建的有效日期可以降低此病毒在六月份的威胁性。

上述统计数字，是由 HouseCall?趋势科技的线上扫毒及 TRend MIcRo ContRoL ManageR(TMCM) - 专为网络管理者而设计的中央管理解决方案 - 所统计出的受感染计算机数，为 2003 年 5 月 30 日止的最新数据。(资料来源：趋势科技全球病毒实时监控中心，TRend MIcRo World VIRus TRackIng CenteR

趋势科技所列出的在五月份所侦测到的十大病毒中的前两名都是网络上众所皆知的病毒：一个是全新的(Worm_Lovgate.F 后门之爱) 病毒，另一个则是以前的 (PE_FunLove.4099 欢爱) 病毒。这些病毒都是使用网络的连结性，如分享或是网络磁盘驱动器，迅速的将病毒散播到局域网络 (LAN) 上的其它计算机，以致在非常短的时间就有数以千计的计算机被感

染。Lovgate.F 在三月份出现，而现在则成为 Lovgate 病毒家族中一个相当普遍的变种病毒。它可经由电子邮件或网络磁盘驱动器散播出去，或许你可以将它的 成功 归功于它的各种不同病毒前辈所借来的特性组合。Lovgate.F 病毒含有某些低级的攻击手法 - 将文件储存在分享磁盘驱动器、回复所收到的电子邮件信息、窃取网络上隐藏目录的地址、提供后门远程访问、开始字典攻击手法破解密码。趋势科技的研究和网络支持部门资深防毒顾问 Jamz Yaneza 说，『如果其解决方案没有彻底清除并修复功能，就会重复感染网络。』

网络上所流传的病毒可在网络上找到许多藏身之所，导致不容易追踪并且完全消灭它们。除了使用目前最新的防毒软件，公司行号还可经由下列预防方法减轻病毒的攻击：

只分享文件夹给某些有需要的特定使用者，而不要分享整个硬盘。

分享文件夹时，给予那些特定的使用者有限度的分享权限，并使用困难度高的密码来保护所分享的文件夹。

将所有要分享的文件设定成只读模式。

管理者须寻找没有使用的端口并将之关闭。

时常更新操作系统和应用程序。

至于其它方面，一小群已经非常久的混合病毒威胁，如 KLez.H、ELkeRn、NImda.A-O，则是连续第二个月的衰退。五个旧的古典病毒，威胁仍然持续出现在排行榜上，它们是从第 2 到第 6，但是他们的占有率已经不如先前的 12 个月。KLez.H 则是常常出现在名单上，而且总是排列前三名，本月则是滑落到第五名。这指出了一个趋势吗？Jamz Yaneza 说：像 KLez.H 这种长久以来的病毒威胁。它还是可以非常容易的复活，不过就算没有，它的衰退的速度确定会很长而且很慢。KLez.H 和其它持续的威胁现在很少威胁企业的网络，但还是流传于没有保护状态的家庭使用者之中。

介于 FIzzeR 和 SobIg 之间的 PE_CIH.DAM 在病毒名单上则排名第九。它就像损坏或没有安装完全的 PE_CIH，它的另一个名字则是 CheRnobyL。这个病毒，是由一名叫做 Chen Ing-hau 的年轻台湾黑客在 1998 年写出来的，它会在被感染的计算机中格式化硬盘和覆盖 BIOS 的资料，删除所有的资料。CIH 曾在 1998 年和 1999 造成相当大的伤害，尤其在亚洲和中东地区。为什么它还在 2003 年的名单上？因为，一个些微修改的 CIH 版本已在 2002 年卷土重来。

美加强网络安全建设 布什组建网络安全处

近日消息，美国国土安全部称，它将组建一个新的部门解决美国技术基础设施面临的威胁问题。这个由 60 个人组成的新部门称做国家网络安全处，负责解决可能对私营和政府计算机系统造成安全破坏的问题。这个部门的建立是美国总统布什的“国家网络安全战略计划”和“2002 年国土安全法”的组成部分。这个部门由国土安全部信息分析和基础设施保护局领导。

国土安全部部长汤姆.里奇在声明中说，美国的大多数商务活动都不能把网络操作与商务活动的物理部分分开，因为它们是相互依赖的。

这个部门重要的中心工作就是保护美国的网络资产，这样我们就可以最好地保护美国重要的基础设施。国土安全部负责基础设施保护的部长助理 RobeRt LIscouskI 担任这个新成立的国家网络安全处处长。这个处将分成三个部门担负三项职责：一是识别风险和减少政府以及私营网络的；二是管理一个网络安全跟踪、分析和反应中心，以便探测对互连网的攻击并向公众发出警报；三是开发有关安全措施的教育计划。

据国家网络安全处称，该部门是根据原美国重要

基础设施保证署(CIAO)、国家基础设施保护中心、联邦计算机事故反应中心和国家通信系统等部门现有的能力组建的。计算机行业组织美国商业软件协会立即对这一举措表示欢迎。

华为被判对思科侵权 双方都要继续打官司

美东时间 6 月 9 日，思科表示，该公司将继续寻求法律手段解决与华为的知识产权纠纷，与此同时，华为也表示将继续以法律手段保护公司的正常权益。两家公司是在美国一家法院就其知识产权纠纷作出裁决后发表这一评论的。

思科坚持认为，华为公司侵犯了该公司的一些知识产权，其中包括用户手册、在

线帮助文件以及部分软件和源代码产权。但华为公司对此持有异议。

上周五，美国东德克萨斯地区法院作出裁决，禁止华为公司使用思科公司的用户手册和帮助文件以及部分路由器源代码，但该法院拒绝了思科公司要求的范围更加广泛的产品禁止令，称“并无明显证据支持思科的诉讼请求”。

对于这一判决结果，思科的法律顾问认为是一次“胜利”，但思科却表示将继续对华为施压以保护产权和交易秘密，促使华为公司停止侵权行为。

华为公司则表示，禁止令不会对公司在美产品销售造成很大影响，也不会影响公司与 3COM 公司合资企业的经营。公司对于法院的裁决结果表示满意，称“法庭注意到了华为公司在解决产权纠纷方面的积极姿态，因此做出了公正的裁决。”

3Com 认为，法庭的裁决不会影响与华为的合资公司。

AOL 自破门规搞宣传 紧抓客户反垃圾情绪

美国在线（AOL）公司似乎已经在与其他宽带服务供应商的竞争时找到了一件重要的武器，那就是人们对垃圾邮件和病毒广泛的厌恶之情。

在 9 日发起的市场宣传攻势中，AOL 公司公布了其下一代服务将具有的新的安全和隐私功能，如允许父母对孩子上网进行控制和反垃圾邮件等功能。

由于面临来自竞争对手的前所未有的压力，AOL 公司的此次宣传活动显示该公司正在对用户的需求做出回应，并试图在宽带服务领域争得自己的一席之地。

为阻止客户继续流失，AOL 公司在此次市场宣传活动中采取了一些非传统的措施。其中一点就是，AOL 公司将在今年夏天推出 AOL 9.0 软件，这打破了该公司通常在秋季发布新软件的惯例。

而且，AOL 公司在新版软件推出前几周就开始进行市场宣传活动，这在该公司的历史上也属首次。在宣传中 AOL 公司还强调，它将可以解决宽带网络用户所面的一些问题，如垃圾邮件和病毒等。

NAI 为微软提供病毒防护和内容扫描支持

美国网络联盟公司的 McAfee Security 近期宣布，将为微软 Exchange Server2003 提供病毒扫描和反垃圾邮件支持。McAfee Security 专为 Exchange Server2003 开发的两个最新 McAfee 产品将于今年推出，以配合 Exchange Server2003 的发布。通过协助微“妖怪”病毒下手欲窃 1200 家银行账号密码

晨报讯据新华社供本报特稿，美国政府向全球金融机构发出警告称，一种计算机病毒已经把世界范围内的 1200 家银行作为攻击目标，企图通过计算机盗窃公司在这些银行的账号和密码。

据美联社 9 日报道，美国联邦调查局正在对此进行调查。一些安全专家认为，这可能是首例主要以一个单独经济部门为目标的互联网袭击计划。参与调查的反计算机病毒专家惊讶地发现，这种病毒的源代码内含有世界上所有大型金融机构的网址，数量多达 1200 个，其中包括摩根大通公司、美国运通公司、瓦霍维亚公司、美洲银行公司和花旗银行等。

这种被称作“妖怪”的病毒具有很强的破坏性，自从上星期出现以来，已经通过互联网迅速感染了数以万计的电脑。不过，调查人员和专家表示，迄今他们尚不清楚是否有金融机构受到这种病毒的严重影响。

美国金融服务信息共享和分析中心主任苏珊娜·戈尔曼说，这种病毒“曾攻击外围服务器，但它已被拒之门外。人们不会报告说，它进入了他们的机构内部”。戈尔曼说，该中心 5 日从国土安全部接到有关病毒袭击的警报后，就以最高警戒等级迅速向各家银行发出了通知。她说，在病毒源代码中发现这么多银行的网址“吸引了众多的眼球”。美国联邦调查局发言人比尔·默里证实，该局目前正在追查这种计算机病毒的制造者。

计算机专家指出，“妖怪”病毒程序可以判断出是否有客户正在使用这 1200 家银行的电子邮箱。如果符合这一条件，它就会试图窃取客户的账号、密码和其他有助于突破银行安全系统的信息。获得成功后，病毒会把账号、密码发送到源代码中包含的另外 10 个电子邮箱，它们均属于病毒制造者本人。

微软购买杀毒技术要进军杀毒软件服务市场

美国软件巨头微软公司今天宣布，该公司计划购

买反病毒技术，开发自有的反病毒软件产品，以更好的保护用户的利益。据悉，微软公司将从罗马尼亚的 GeCAD 软件公司购买反病毒软件技术。分析人士认为，微软公司此举表明该公司准备进军潜力巨大的杀毒软件和服务市场，开拓新的市场领域。

微软公司表示，该公司已经与 GeCAD 软件公司签署了合作协议，购买这家公司的知识产

权和技术。GeCAD 软件公司是一家总部位于布加勒斯特的软件公司。微软公司计划以这家公司的杀毒技术为基础，开发出自己的杀毒软件产品并且提供相关的服务。由于微软公司的操作系统和软件经常成为病毒的攻击对象，因此微软公司认为开发适合于自己的杀毒软件产品已经十分必要。

微软公司称，公司杀毒解决方案的详细情况，包括产品计划、价格和时间表目前还不便透露，微软公司强烈建议用户使用目前的杀毒软件产品，以保护系统不受病毒侵害。分析人士认为，微软公司进军杀毒软件服务市场将对目前该领域的两大巨头形成巨大威胁，目前杀毒软件市场主要被赛门铁克公司和 Network Associates 公司控制，两家公司的主打产品分别是诺顿和 McAfee。

微软进军反病毒市场是否捆绑销售引人注目

微软周二表示，将从一家罗马尼亚软件公司收购反病毒技术并开发自己的反病毒产品，进入一个长期以来被专业性的安全公司所把持的市场。

微软收购了知识产权、反病毒软件技术以及 GeCAD Software SRL 咨询公司，金额不详。该公司的一些软件开发人员将加入微软。

微软企业安全部门副总裁迈克-纳什表示，微软计划在没有明确指出的日子推出自己的反病毒产品，但是还没有确定是否将基本的反病毒产品与 Windows 操作系统捆绑。

纳什表示，微软要更好地保护客户免遭病毒及其它恶意程序的影响，消息发布后，赛门铁克和 Network Associates 的股价都下跌了，而微软的股价上涨了近 4%。Network Associates 总裁霍奇斯表示，微软告诉他们不会将反病毒产品与 Windows 操作系统捆绑。

Network Associates 上周宣布与微软结盟，共享对 Windows 用户构成威胁的最新信息。霍奇斯说：“我们将继续遵守盟约，除非微软改变计划，不按照跟我们说的那样去做。”

ForResteR 分析师拉斯姆森表示，微软的行为就象是黑手党，对客户收取保护费。他说：“世界不希望微软成为安全产品销售商，他们希望微软提供更安

全的产品。”

雅虎设置过滤屏障 反垃圾邮件成竞争手段

雅虎为了阻塞垃圾邮件，采用了一种目前颇有争议的技术，以帮助其邮件服务系统识别是否为垃圾邮件。

雅虎5月将查询应答技术应用于基于网络的邮件服务，该公司已不是第一次采用这项技术，该技术可以很容易地识别发送者是人还是计算机。从现在开始，人们注册 Yahoo ID 时，会被要求键入一串伪装字符以通过计算机处理的注册。

雅虎是在互联网服务提供商 AOL、微软的 MSN 以及 EaRthLInk 公司之后采用该系统的，上述几家公司今年都发动了反垃圾邮件大战，并将其作为竞争手段。

雅虎认为自己的垃圾邮件方法与其它竞争对手的都不同，因为它的最终目标是把垃圾邮件阻隔出去，而不是把主动提供的邮件放进其成员的收件箱里。

雅虎 3 月份更新了其 SpamGuaRd 软件。该公司强调，人们通过其系统发送的邮件不是每一封都必须经过查询应答检查。该公司为了准确确定垃圾邮件，设立了“用户概况”，把用户常用的频率以及邮件的长

度保存在账户里，一旦接近用户个人设定的界限，系统就会进行垃圾邮件查询。

微软改善 Windows 安全性 收购杀毒商 GeCad

6 月 10 日，微软宣布它将收购 GeCad 软件公司一家罗马尼亚的反病毒技术开发商，此举旨在改善微软 Windows 平台的安全性。

这笔交易的财务条款目前还没有向外界透露，但一位代表称，这笔交易将为微软的开发商团队增添一个反病毒专家小组，并为微软带来为其所有产品提供反病毒系统的能力。GeCad 公司的安全专家还将致力于使Windows操作系统能与第三方反病毒生产商的产品更好地进行工作。

此举很有可能将改变一些反病毒产品生产商的竞争局面，例如 Network Associates 和 Symantec 公司等，而且还会引起 Netscape 通信公司的恐惧。

微软表示，尽管它计划购买 GeCad 公司的知识产权，但它不会继续开发该公司的产品。但微软没有透露它将会保留多少 GeCad 公司的员工。

微软和 GeCad 公司之间的交易是由于微软的“可信赖计算”计划而引起的，该计划旨在改善 Windows 安全性能的纪录。

蠕虫 (Worm.Win32.MofeIR)事态技术分析报告

2003 年 6 月 5 日-8 日，哈工大--安天联合 CERT 小组，通过自行开发的 P-A 监控预警平台陆续截获发一些异常通讯：

在第一批次锁定了若干问题主机后，经过反向检测，初步发现发包机器有如下共性：

1、系统为 Windows 系统（2K 系统居多）。

2、系统超级用户管理员密码为空。

我们及时与多台目标主机管理人员联系，进行了系统取证。

初步检测结果如下：

发现若干异常文件和异常注册表键值：当前态势：目前该蠕虫已经在黑龙江省内一些内网流行，目前已经发现第 2 个变种。

密码破解成功后，将自身 copy 到远端系统的 system32 目录下，并通过 admIn$执行。

该蠕虫的最终目的是为了给系统添加后门，该蠕虫将向系统添加一个名为 tsInternetuseR 的用户（在 Windows Server 系统上这时超级终端服务的内建用户）并将用户口令设置为[此处作了屏蔽]，并将该用户添加到管理员组。

该病毒提供了远端控制命令，并可以执行“批处理文件”，MoFeI.MIS 就是这样的文件。

该蠕虫添加完后门后，可能回从网上 downLoad 一个名为 sckILLeR 的自毁程序，自我删除。

该病毒具有自我更新能力。

用户处理手工处理

NT/2K 用户应该首先为 AdmInIstRator 设置一个强壮的密码，（至少不能在蠕虫的密码档中），之后采用 AntIy ghostbusteRs 的进程服务管理功能

首先中止%WindIR%system32/scaRdsvR32.exe 对应的进程和服务，之后删除掉“系统分析文件列表”中的所有对应所有文件，最后重新启动机器。

用户处理专杀工具

即使采用专杀工具，也需要首先为 Adm InIstRator 设置一个强壮的密码。否则再次被其他感染节点扫描时，仍然会被感染。

网络管理对策：

网管可以在路由或者防火墙上，双向关闭 445/139/135 等端口，以临时避免内网被感染，或者内网感染的主机对外传播。

进一步响应消息：我小组将继续关注态势进展，进一步维护升级报告。

所有的运营者应该站到消费者的立场去考虑互联互通

今年 5 月中旬，中国移动(香港)有限公司董事长兼总经理王晓初在接受某电视媒体采访谈及互联互通时有一段讲话：“互联互通，在任何一个国家开始竞争的时候都会出现一些问题。但我们希望解决问题的过程越短越好，为什么呢？为客户考虑一下，你在互联互通上表面卡的是竞争对手，实质卡的是客户，给客户带来了不便。所以我觉得所有的运营者应该站到消费者的立场去考虑互联互通。同时这种问题是短暂的，你损害了你的竞争对手，同时也损害了你自己。”短短一席话，表明了中国移动集团公司在互联互通问题上最直接的看法。

引起电信运营商之间互联互通问题的原因很多，其中一个重要原因就是不合理的网间结算费用体系影响了双方在互联互通方面良好合作的积极性。网间结算费用体系应建立在什么基础上？互不结算究竟可不可取？带着一系列问题，我们近日专访了中国移动通信集团公司负责互联互通工作的王晓琦经理。

合理的网间结算应以成本为基础已经被财经媒体热炒了相当长时间的张昕竹小组正在攻坚的运营商成本结算模型是业界非常关注的话题。王晓琦告诉

本报记者，以成本为基础制定网间结算价格，是目前国际上公认的、合理的原则。对于当下有很多人将互联互通问题与电信资费混为一谈的说法，王晓琦谈了自己的看法。

“现在很多人一说到互联互通总要把它与电信资费联系起来说，这是因为目前的网间结算费用是以电信资费为基础制订的，它存在很多弊病。运营商也不应简单地站在本企业利益的角度来坚持这种不合理的做法。而且从现在最新的发展状况来看，再强调这种做法也是没有任何意义的。我们认为，网间结算费用应该采用国际公认的法则，即以运营商的成本为依据来制订。”王晓琦的说法与日前联通互联互通部总经理涂栋臣接受本报记者采访时的讲法基本一致，他们都认为现在这种改革的脚步更加符合时代环境，也更科学。王晓琦说：“网间结算费用不应被现有的电信业务资费所左右，张博士小组的工作也就是基于这种考虑。他们所做的就是想先确定一种运营商成本计算方法，在此基础上确定网间结算费用。”

“至于选择什么样的成本计算法，目前各运营商对此还没有形成一个统一的意见，不过大家都知道，目前国际上比较通行的做法是采用长期增量成本法，张昕竹小组在报告中也对这种方法给予了推荐。中国

移动正在对这个问题进行研究。”“对于张昕竹小组的几种模型来说，现在还处于一个征求意见的过程，因此并没有一个最终确定的结果。中国移动通信集团公司对这个工作非常支持，我们也正在学习和研究几种推荐的模型，对于那些比较难理解的问题我们也正在和张博士的小组沟通。”王晓琦说。

她告诉记者，确定合理的成本计算法，将为解决互联互通问题打下良好的基础，但这仅仅是迈出了第一步，后面还有很多的工作要做。

应打破互不结算和单向结算格局

互不结算和单向结算是目前互联互通领域比较敏感的两个问题，当记者问到王晓琦的看法时，王坦然陈词。对于现在有些人提出的移动运营商网间互不结算的问题，王表示，这并不合理。“既然各个运营商在建设网络上都有了成本付出，就应该都得到回报，何况，政府加强互联互通管制有多个出发点，比如防止价格战、保障网间通信质量、保障网间业务畅通等等，这些也都需要通过合理的网间结算来保证。”王强调，实践证明，网间结算可有效约束电信运营商的价格行为，将价格竞争限制在一定范围之内，保证整个行业的良性发展。缺乏网间结算的业务更容易出现恶性价格竞争。制定合理的网间结算价格有利于激

发企业搞好互联互通的积极性。

她补充说明道，我国已加入世界贸易组织，如国外实力雄厚的通信企业进入国内电信市场，根据 WTO 的最惠国原则和国民待遇原则，各电信企业必须服从相同的行业管制政策。为创造公平合理的竞争环境，网间互不结算的状况也需要改变。

王总结说："总之，充分利用网间结算手段，通过完善网间结算办法，依靠市场经济手段规范企业行为，可以较好地维护国家、企业和消费者的长远利益。"对目前我国移动与固定网络之间互联互通时，移动运营商需向固网运营商交纳相应网间结算费用、但反过来固网运营商无需向移动运营商支付网间结算费用的问题，王作出这样的回应："这种做法我们认为并不是很合理的，基本上没有考虑运营商成本计算的问题，我们认为如果考虑运营成本，就不会出现这种问题了。因此我们认为成本计算的确立对整个互联互通工作很重要。"显然，王晓琦认为这种做法伤害了移动运营商。

同时，她表示对于"固定网的本地网络建设，移动运营商只使用而没有付出相应费用"的说法也没有道理。"在现在的互联互通过程中，我们在本地传输的使用上都交付了租金，而且在网间结算费用上已经

有所体现了”。

牵出普遍服务问题

现在对于互联互通还有一种声音，就是固网运营商表示，他们在电信业务的普遍服务上付出了很多，而在互联互通中他们在普遍服务的付出并没有得到相应的回报，同时，他们也期望能够在这个领域得到相应的所得。王晓琦认为：“说到普遍服务，我们并不认为只有固网运营商才有付出。就拿我们中国移动集团通信公司来说，为了能够让更多的人使用我们的业务，我们网络覆盖已经涵盖了全国，甚至包括了西藏、青海、新疆这样的地区。近期在登珠峰 50 周年的活动中，已经能从珠峰顶传送手机话音、短信和彩信，这本身就说明移动已经在提供普遍服务上尽了自己最大的努力，能够将移动网络铺设到青藏高原就是最好的例证。因此，我们并不认为只有固定网络运营商独自承担了普遍服务的义务。我认为任何一个运营商都有责任承担普遍服务的义务。至于如何使我国普遍服务的管理和运行机制更加完善是政府和运营商正在研究的另一个课题。”

微软强攻杀毒软件市场现有厂商日子不好过

微软宣布，将从罗马尼亚软件生产商 GeCAD 手中购买杀毒软件技术，在此基础上开发出新的病毒解决

方案以提高 Windows 平台的安全保障，并向第三方提供杀毒软件产品。此举意味着微软将挺身加入杀毒软件市场，必将对该行业带来巨大影响。

微软网络安全部门主管艾米一克洛(Amy CaRRoLL)说，“计算机病毒一直在不断发展中，恶意代码问题还没有得到解决。我们需要投入更多的精力来帮助微软以及其他公司解决这一问题。病毒解决方案一般由两部分解决，即引擎技术和签名更新技术。引擎这部分微软将采取什么样的策略还不清楚，但提供更新签名技术的服务将是要收费的。当然在技术收购还没有完成之前，这一切都只是构想，还是不成熟的”。

美国网络安全服务提供商StenstRom公司总裁格雷戈里一斯坦姆(GRegory StenstRom)说，微软跻身杀毒软件市场对于其他公司来说意味着巨大的竞争压力。就象当年微软进入浏览器市场后挤跨了Netscape 一样，很多公司都将面临危机。“面对微软这样的竞争对手，目前市场上的杀毒软件生产公司如TRend MIcRo 和 Symantec 是没有希望获胜的”。

但杀毒软件的生产商们则对微软公司的决定表示出一定程度的欢迎。Symantec 公司在星期二的一项声明中称，“我们现在还不能够了解这一决定所带来的影响，但是我们对此表示欢迎，因为这意味着用户

可以获得更有效的杀毒软件。”TRend MIcRo 公司则认为，微软此次决定，再加上一个月前建立“病毒信息联盟”的决定，表明了微软投入计算机安全领域的决心。

Sophos 公司的高级安全分析专家克里斯—贝特霍夫(ChRIs BeLthoff)则认为，微软的收购计划还将面临一些问题，推出新的病毒解决方案也不是轻而易举的事。此外他还对收购之后GeCAD的客户表示担心，特别是那些使用其他操作系统如 Linux 的客户，“你认为微软还会继续支持他们吗？ ”

开放源码组织讨伐 SCO 指责其违反了 GPL 协定

近日一些开放源码组织成员指责 SCO 将 Linux 内核中的源代码合并到 SCO UnIx 中的一个模块(称为 Linux 内核个性化功能模块，LKP)后，没有对 Linux 代码作出修改，而且没有标出 Linux 的版权信息。从而违反了 GNU GPL(通用公共许可协定)的有关条款。GNU GPL 协定规定，任何商用组织利用开放源码或修改后必须归还给开放源码组织，或者在引用代

码处明显标出“引自 Linux 代码”标记。

一位不愿透露姓名的知情人士向 eWEEK 表示，SCO UnIx 确实从 Linux 复制了部分代码。据查看过这些混

合代码及参与过这些代码编写工作的人透露，SCO 将 Linux 内核中相关部分“基本上重新改造”成了现在 UnIx 中的“Linux 内核个性化功能模块(LKP)”。LKP 的功能是允许用户在 UnIxWare 系统上兼容 Linux 标准应用程序和 UnIx 标准应用程序。

SCO 发言人 BLake StoweLL 向 eWEEK 表示，尽管 LKP 使用了一些开放源码，但并不是说开放源码就一定是 Linux，这是个概念错误。我们从来没有在 LKP 中使用过 Linux 内核代码，也没有将 UnIx 源码置入 Linux 内核中，因而我们并未违反 GPL 协定。

微软警告用户勿使用测试版的 MSN Messenger6

美国东部时间 6 月 15 日(北京时间 6 月 16 日)消息，微软公司日前向用户发出警告，要求大家不要使用泄漏的正在进行 beta 测试的 MSN Messenger6，因为这些版本的软件目前还没有完全完成，不能提供用户使用。

很多网站都在使用不同版本的 MSN Messenger6，而且每天都会有新的网站使用这一软件。微软称这些在网上提供的版本都是用于内部测试的，不知道是谁将它们泄漏了出去。公

司 MSN 部门在一份声明中称：“我们的这些测试版软件仅用于 beta 测试，MSN 强烈警告用户不要从未

授权的网站下载测试版软件，因为它们的代码还不稳定，信息并不完全”。微软公司 MSN 产品负责人称，公司已经请求个别网站提供测试版的 MSN Messenger6 以供下载，用于软件测试，但用户还需要耐心等待这一软件的公开演示，这一行动可能于未来几周进行。

不过，微软还是对测试版软件的受欢迎程度感到了惊喜。根据 MSN 服务部门的副总裁布莱克-伊文提交的一份备忘录称，超过 200 万的用户下载了泄漏版本的软件。“MSN Messenger6 将很快成为我们开发的最具吸引力的软件之一，每一位使用过它的人都会体会到它的优势，ICQ 的辉煌时代即将过去”。

ICQ 是由以色列 MIRabILIs Ltd.公司开发的一款网络即时通信工具软件，于 1996 年正式推出，一直以来受到世界各国用户的喜爱，特别是在上个世纪 90 年代后期更是如此。MSN Messenger6 对用户界面进行了改进、新增一些个人设置功能，内置了在线游戏和语音及视频聊天等功能。在公开演示之后，MSN Messenger6 的最终版将于几个月后正式推出。

黑客盗走游戏极品“装备”网络案件谁来管

作为一个网络游戏迷，西安市的张先生感到很苦恼，他玩一款在线网络游戏已有一年多了，在游戏中

获得的极品装备价值人民币千元以上，一个月前却被人盗去。

极品装备突然被盗

张先生所玩的是一款名叫奇迹的在线网络游戏。随着玩家在游戏中时间的增长、在不断完成游戏任务的情况下，人物和装备可不断升级。据张先生介绍，5 月 20 日他再次上网玩该游戏时，突然发现辛苦玩了一年多才取得的装备不翼而飞。同时发现，他朋友的一把极品剑被盗，估计是黑客所为。据介绍，此前已有玩家表示愿出 1500 元购买这把剑，但朋友没舍得出让，谁知竟然被盗！发现装备被盗后，他曾与该游戏的运营商联系，希望对方能帮助找回被盗装备，但对方表示除非有警方要求协助查询，否则不能提供数据，也不负责赔偿。

同样是网络游戏迷的刘先生告诉记者，这很可能是一起典型的黑客使用软件盗取玩家账户和密码的事件；另外，他说一些网站还开发有网络游戏的作弊软件，即玩家通常所说的外挂，玩家通过使用外挂，可以实现游戏加速、复制金钱装备、甚至直接修改人物属性和经验等目的。一些外挂开发者更是通过卖外挂获得不菲的利益。

游戏运营商也会受损失

在遭遇作弊者时，游戏的平衡性、公正性受到破坏，也会直接影响大多数玩家的游戏乐趣。同时，由于一些玩家无法在虚拟世界里迅速成为顶级高手或获得顶级装备，就转而用现实货币来交换游戏世界中的虚拟货币、顶级装备或高级别玩家的账号密码，这就使玩家费时费力积累起来的装备、经验级别等具备了相应的现实价值，因此也就有了滋生黑客盗取账号或装备的土壤。

刘先生说，游戏玩家的账号或装备被盗，他在网络上听过很多。而使用外挂的玩家更是比比皆是。他认为，发生这种事情，不仅网络游戏玩家受损失，同时游戏运营商的利益也受到损害。以外挂为例，一款网络游戏正常的盈利时间大约是 18 个月至 3 年，然而一旦有玩家采用外挂，那么游戏的盈利周期将会大大缩短--需要一个月才能修炼成功的魔法或武功，通过外挂只需要三五天就能办到，这对运营商而言简直是场灾难。他追问：网络游戏，究竟可以靠什么`保驾护航`呢？

游戏安全如何保障

在一个法治社会中，寻求法律帮助已成为共识。但据了解，由于缺乏明确的相关规定，公安部门事实

上难以受理这类报案。对此，北京康达律师事务所西安分所的李德松律师解释说：网络游戏中出现的上述行为，一般达不到刑法关于互联网犯罪所要求的严重程度，故不能适用刑法；治安管理处罚条例虽可对侵害个人财产的行为进行处罚，但适用治安管理处罚条例的前提是，有关部门对财产一词做广义的解释。

目前，一些网络运营商已经自觉行动起来。同样以打击外挂为例，过去只是一两家公司小打小闹；如今各大网络游戏公司纷纷响应，有的还打出了借助法律手段的大旗。此外，不少网络游戏公司还对违规者做出了删除档案、在一定时间停权、甚至永久封杀等惩罚措施。李德松认为，在网络游戏中出现的新问题，早期依靠行业自律更具可操作性，时机成熟后应考虑专门立法。

美国 DoubLeCLIck 发表对付垃圾邮件系列构想

美国当地时间 6 月 11 日，DoubLeCLIck 发表了对付垃圾邮件的一系列构想。该构想由策略、调查、教育、技术等部分组成，其目的在于促使营销公司和电子邮件销售业了解并采用该构想。

DoubLeCLIck 发表的构想概要如下：

策略

公司每年发布 4 次名为“PoLIcy and ISP Update Report ’的报告。报告的内容由该公司与策略制定者、互联网接入服务商（ISP）、电子邮件服务提供商定期举行的会议结果得出。该公司的个人隐私小组与监督机构、法律制定者举行会议，并向策略制定者提供关于电子邮件销售和电子邮件服务提供商的作用等相关知识。另外，该公司的 ISP 相关小组与主要的 ISP、电子邮件服务提供商保持会议联系。第 1 份 PoLIcy and ISP Update Report 定于今夏推出。

调查

为了解消费者对垃圾邮件的反应，该公司将展开大规模的调查和教育活动。活动的目的是促使营销者了解电子邮件交流与垃圾邮件的区别。该公司将每年对消费者的电子邮件进行一次调查，此外还将与美国在线合作，为了解消费者对垃圾邮件的态度及反应进行调查。调查结果的主要内容将于 7 月公布，完整的结果将在 9 月份的 ARF 会议上发表。

教育

除了在 Web 上定期举办顾客教育研讨会之外，该公司还将主办垃圾邮件专题会议。为时半天的研讨会的与会者包括监督机构、立法机构、ISP、电子邮件

服务提供商、电子邮件营销商等。

技术

DoubLeCLIck 将致力于电子邮件发送的相关技术解决方案并追加投资。该公司将向通信基础设施 EMail Service PRovIdeR（ESP）投资，进一步扩大与美国 AssuRance Systems 的联系，共同开发面向顾客的电子邮件发送管理工具。另外，该公司还将投资 IRonPort 技术解决方案。“虽然大多数公司支持针对垃圾邮件制定联邦法案，但要消灭垃圾邮件仅靠法令是不够的。只有综合利用法令、技术、教育和业界的通力合作，才能真正最终解决垃圾邮件问题”（该公司营销解决方案部门副总裁兼常务经理 Scott KnoLL）。

专家称:侵权代码进行查验后 SCO 证据很不充分

在对 SCO 集团声称的侵权代码进行查验后，AbeRdeen 集团的分析师克雷布鲁克表示，他无法根据这来判断 SCO 集团的知识产权主张是否是正当的结论。他在一篇报告中描述了查验代码的经历和这起诉讼中双方较大的分岐。

作为 UnIx 内核的前编程人员和计算机科学教授，克雷布鲁克是 SCO 集团邀请的三名了解它认为是由

UnIx System V 移植到 Linux 中代码的三位专家之一，SCO 集团此举的目的在于为其法律主张寻求更多的支持。

克雷布鲁克说，根据最初的查验，他确实在 UnIx 和 Linux 中发现了相同的代码和编程注释。他在报告中指出，我看到的只是 UnIx .c 文件，这只是 SCO 集团提供的一个例子，由 UnIx 拷贝到 Linux 中的代码和注释只有大约 80 行。

即使在 UnIx 和 Linux 中看到了完全相同的代码，但克雷布鲁克表示，这不足以支持 SCO 集团的主张，对二种代码的比较无法得出决定性的信息。他说，由于无法在计算机上看到相同的代码，因此我只能说，我看到了这些代码，但无法判断其真假。

克雷布鲁克说，它还得到了声称自己这些代码出自何处的电子邮件。有开发人员称，所有这些代码都来自 BSD UnIx。他表示，由于没有在计算机上看到相关代码，我不能贸然下结论。他指出，令人不可思议的是，这些代码并没有拷贝全部功能。

克雷布鲁克在报告中称，我曾经询问过SCO集团，它们是否掌握有 IBM 公司将 System V 的源代码拷贝到 Linux 中的直接证据，它们的回答是“没有”，但现在它又改口为，“我们有证据，但现在还不到拿出

相关代码的时间。”克雷布鲁克发现，IBM 公司拷贝代码的主张“很难被相信”。

尽管认为 SCO 集团的证据不够充分，但克雷布鲁克说，他认为这不是一件一目了然的案件。他指出，SCO 集团不是故意地提出不正当主张的。由于没有考虑到主张的合法性，SCO 集团在打击 Linux 的同时犯了众怒。

克雷布鲁克在报告中指出，在 AbeRdeen 集团看来，即使 SCO 集团赢了对 IBM 公司的起诉，也不会对 Linux 构成致命的打击。事实上，这一官司只是表明在Linux发展过程中需要进行某些改变的信号。Linux 厂商和独立软件开发商希望以一种更有组织的方式在 Linux 中添加重要的功能，它们需要一个路线图。他说，已经发生了一些变化，例如开放源代码开发实验室现在更多参与了决定 Linux 内核功能的过程。

ForResteR调研公司的分析师斯塔茜说，尽管SCO集团诉讼的好处还有待证明，但最终，Linux 将继续成为 Windows 和 UnIx 的取代者。

美国防部 2008 年将采纳新的互联网协议 IPv6

美国国防部已经决定采纳一种新的互联网协议，该协议名为 IPv6，将成为美国防部在 2008 年前所有

连网信息系统的标准。

据美国国防部负责网络和信息集成的副国防部长约翰-斯特恩比特表示，上述新的互联网协议版本将提供更好的网络安全和质量更佳的传输服务。

斯特恩比特表示，五角大楼已经决定从现在开始就向 IPv6 靠拢，IPv6 是互联网协议版本 6 的缩写，以便这一协议能够被融入新型武器和通信系统的设计当中。

目前美国国防部的互联网协议名为 IPv4，由于新型协议已经获得了足够的商业支持，所以美国国防部已经开始设计能够同时与 IPv4 和 IPv6 兼容的新软件。斯特恩比特说："如果 IPv6 的相关软件研发获得成功，那么国防部的互联网信息传输速度将大大增强。"五角大楼计划分阶段实施从 IPv4 到 IPv6 的提升，包括国防部大部分网络从 2005 年开始以试点形式提升为 IPv6 协议。但斯特恩比特指出，诸如美国陆军"未来作战系统"和新型激光通信在内的系统定于在 2008 年以后才能改为 IPv6。"未来作战系统"利用信息网络将人工操作和无人操作的作战车辆连为一体。斯特恩比特表示，上述系统的研发商应该很清楚哪种类型的互联网协议将成为"国防部网络的心脏和大脑"。

美新反垃圾邮件法案不提供拒收方式将受罚

美国参议院的一个委员会计划在本星期四就一个反垃圾电邮的法案提议进行投票表决。

由 John McCaIn 主管的美国参议院商业委员会，正在考虑由参议员 Ron Wyden 和 ConRad BuRns 提出的“CAN-SPAM”反垃圾邮件法案。该法案的主要内容为：未被主动要求的商业电邮中，必须提供一个可用的寄信人地址和一种使收信人能够拒绝再次接收该邮件的方法。

在“CAN-SPAM”法案之下，联邦的监察人员和互联网供应商可以控告垃圾邮件的发送者“使用伪造资料或假电邮标题、没有提供拒绝接收机制、向通过不正当手段获取的电邮地址发送邮件”等罪名。

Ron Wyden 和 ConRad BuRns 在上星期促请联邦交易委员会(FTC)应该采取更加积极、更加不择手段地对付垃圾邮件。而参议院商业委员会也有意考虑另一项反垃圾邮件的提议，以赋予 FTC 更多的权力以对抗垃圾邮件发送者，如允许 FTC 向互联网供应商索取其订户的资料、浏览 FBI 的罪犯数据库、与外国相关部门交换敏感信息等。

侵入半岛电视台网站的黑客已在美国出庭受审

一名在伊拉克战争中侵入卡塔尔半岛电视台网站，将网站关闭的黑客 15 日在美国洛杉矶市出庭受审。

在今年 3 月份美英等国发动的伊拉克战争中，一名黑客以半岛电视台工作人员的身份登入电视台的网站，通过修改有关设置将所有该网站的访客引向了另一个他自己制作的网页。

这名 24 岁的黑客约翰·威廉·拉辛又名约翰·布福，被控犯有电信欺诈和非法拦截电子通讯两项罪行。他的律师表示，他已经同意向法庭认罪，并面临缓刑 3 年和 1000 多小时社区劳动的惩处。

互联网服务商使用专业软件控制垃圾电子邮件

CaRL ShIveRs 一直习惯在半夜起床，这样做只是为了确保垃圾邮件不会使公司的电邮服务器瘫痪。

ShIveRs 是 ARIstotLe 互联网接入公司的系统管理员，该公司是一家位于阿肯色州小石城的互联网服务提供商（ISP），公司用户有 2 万多人。作为管理员，ShIveRs 无法确保在一小时内不让 ISP 服务器发送损害用户电邮账号的垃圾电邮。垃圾邮件的数量不仅在

威胁着电子邮件服务器，而且还渗入了 ISP 原来设置的用来反制垃圾电邮的过滤器。

ShIveRs 说，我们设置了三个过滤功能服务器，但是现在仍然中招。ShIveRs 估计他要花三分之二的时间来处理垃圾电邮问题。他指出，这是一种类似拒绝服务攻击的东西，垃圾邮件制造者正好能够控制我们给他提供的带宽。

一个月前，控制垃圾电邮的努力出现了转机，公司试用了 SpamSqueLcheR Beta 版测试软件，该软件可以分析发来的电邮，软件采用“流量定型”技术（tRaffIc shaPing），以控制作为垃圾电邮温床的宽带连接服务。安装该软件后，互联网服务商就能够像控制水龙头那样锁定带宽。

SpamSqueLcheR 反垃圾电邮软件的力量在于，它依赖于对发进电邮进行随机抽样和网络分析，但是该软件也有潜在弱点。如果合法电邮随着垃圾电邮发送者有意侵入的信息一起进来，那么这封合法电邮也会被屏蔽。这种屏蔽技术使人想起“垃圾邮件黑名单”的做法，黑名单将那些发出大量未经请求的电邮服务器列出，但不管这些服务器也发送过合法电邮。

微软提出 15 桩诉讼欲借助法律阻止垃圾邮件

当地时间本周二，微软公司称，它已经在美国和

欧洲提起了 15 桩诉讼，以扼止垃圾邮件不断增长的趋势。垃圾邮件被认为是促使用户倒戈的重要原因之一。

这 15 名公司或个人被告被指控在微软公司的 MSN 互联网服务中滥发了 20 多亿封推广包括从如何一夜致富到色情网站在内的垃圾邮件。

就在此前不久，微软以及其它一些互联网厂商强化了垃圾邮件过滤技术和在信息共享方面的努力。微软公司的首席律师顾问史密斯表示，我们已经意识到，垃圾邮件是一个全球性的问题，我们正在加强在全球打击垃圾邮件的努力。

史密斯说，微软公司将采用更好的技术，例如阻击和过滤工具，并通过与其它互联网厂商合作，加强保护客户免受垃圾邮件骚扰的努力。微软公司称，这些起诉的目的是使垃圾邮件发送者不再兴风作浪，并获得相应的赔偿。

周二，美国和其它 29 个国家还公布了一项跟踪垃圾邮件发送者、电信营销商的计划，这将使政府能够更方便地对此类案件进行更有效的调查。

垃圾邮件肆无忌惮美国国会要考虑加大立法

塞缪尔有一个名片上没有的头衔，据美国证监会

称，他是“专职互联网垃圾邮件发送者”。塞缪尔与其兄弟亚当一起在美国从事垃圾邮件发送工作。去年，华盛顿州与他们二人和解了一起反垃圾邮件诉讼，2 月份，证监会指控兄弟二人发送了数以百万计的垃圾邮件参与股票欺诈活动。英国非盈利组织“Spamhaus 项目”称将他们二人称作是“140 个最难对付的垃圾邮件发送者”。

这兄弟二人只是危及电子邮件效用的活动的“一角”，电子邮件可以说是互联网上最简单、有用和不朽的发明。促销各种商品的垃圾邮件正在以一年前人们不能想象的方式塞满用户的收件箱。

为美国 10 大 ISP 中的 6 家提供服务的垃圾邮件过滤软件提供商 BRIghtMail 公司估计，根据对其 2.5 亿用户的监测显示，4 月份 46%的电子邮件属于垃圾邮件，2001、2002 年同期的这一比例分别为 10%和 18%。美国在线公司表示，它每天过滤的垃圾邮件数量高达 23 亿封。JunkbusteRs 公司的总裁詹森说，我们处于关健时期，互联网的未来依赖于这一问题的解决。

塞缪尔的律师丹尼尔说，他的客户的业务与电话销售和直邮广告完全一样，垃圾邮件之所以盛行的原因在于有用户对它作出反应。他表示，响应垃圾邮件

的人应当受到谴责，客户通过垃圾邮件购买了伟哥。

监管机关直到最近才开始加强了对垃圾邮件的监管。美国联邦交易委员会的律师布赖恩表示，自1997年以来，针对垃圾邮件发送者采取了53次行动，其中的约半数在去年提起了诉讼。他指出，垃圾邮件不能与电话推销和邮件直销相提并论，因为它的成本非常低，而且极易伪装发送者的身份。詹森表示，高速互联网连接的普及使得垃圾邮件发送者以更低的成本发送更多的垃圾邮件成为可能，只要1%的垃圾邮件得到响应，它们就能够获得巨额利润。而且垃圾邮件发送者还能够非常熟练地使用各种工具从互联网上获得电子邮件地址，他说，垃圾邮件业务的利润非常诱人。

代表DoubLeCLIck等电子邮件营销公司的一家行业组织的代表休斯说，美国有33个州通过了反垃圾邮件法律，但现实情况是，许多垃圾邮件已经因欺诈和不公平行为触犯了现有的联邦法律，他说，有资料显示，有三分之二的垃圾邮件触犯了现有的法律。

他认为，无需更多的法律限制或让ISP更多地使用“黑名单”，更好的解决办法是“针对进行欺诈活动的垃圾邮件发送者采取强硬手段”，我感觉我们需要进行一些杀鸡骇猴式的打击活动。

EaRthLInk 公司的玛丽说，垃圾邮件不仅仅威胁电子邮件的有效性，通过使所有内容传输得非常慢，它还影响了互联网功能的发挥。玛丽表示，垃圾邮件大大增加了互联网服务提供商和消费者的成本。

国会一直在考虑通过新的立法，其中包括让消费者和互联网服务提供商起诉垃圾邮件发送者。美国参议院商业委员会的主席约翰说，他计划于今年夏季向国会提交反垃圾邮件提案。参议员马克曾建议对每封电子邮件征收非常少的税，对于普通用户它不会造成太大的负担，但对于每年发送数千万封电子邮件的垃圾邮件发送商而言，这将是一笔巨额开支。但他现在已经不再提供这一策略，而是与其它国会议员一起要求电子邮件营销商提供合法的回复地址，并使用户能够方便地选择不接受垃圾邮件。马克说，垃圾邮件影响了企业，以及个人和儿童，打击垃圾邮件得到了广泛的社会支持。他还希望能够创建反垃圾邮件的专门组织。

SoBIg 病毒新变种再度猖獗 48 小时将肆虐全球

安全顾问公司 IDefense 本周三预测 W32/SoBIg 病毒变种 48 小时内将成为全球最猖獗的五个病毒之一。Symantec 和 McAfee 两家公司均表示到目前为止，

W32.SobIg.D@mm(简称 SoBIg.D)的威胁尚不足惧，SoBIg.D 较易控制和杀灭。

上个变种 SoBIg.C 在 84 个国家肆虐一周后于 6 月 8 日失效，其继任者 SoBIg.D 失效期限为 7 月 2 日。5 月 31 日是 SoBIg.B 的失效期限，同一天发现 SoBIg.C。

IDefense 资深分析专家 Ken Dunham 表示，SoBIg.D 的作者在安全专家发布 SoBIg.C 病毒警告后等待了好几天才开始有所动作，让人惊奇的是这么多一连串的病毒变种连续发难。SobIg 是对传统安全措施的挑战，表明了紧急安全反应措施和智能化防病毒程序的必要性。

尽管 Symantec 和 McAfee 预测 SoBIg.D 不会构成太大威胁，IDefense 仍然警告这种病毒传播速度很快，应该采取必要行动进行防备，应在网关一级就阻止.exe、.scR、.pIf 等附件文件的进入。通常感染带有如下后缀的文件：.wab .dbx .htm .html .emL .txt。

美国参议员关注网上侵权主张遥控摧毁电脑

ISP 和唱片业之间就版权的争论已经引起了参议院商业委员会主席麦凯因的注意，他表示将就此召开听证会。

唱片业业界组织 RIAA 去年夏天要求 VeRIzon 通

信公司帮助寻找一名非法传播了 600 多首歌曲的用户，但是 VeRIzon 表示在没有法庭传票的前提下不能这么做，法庭本月初要求 VeRIzon 提供姓名。VeRIzon 已经提出了上诉。

参议院司法委员会主席在本周初哈奇表示，他支持开发新技术，通过遥控摧毁从互联网非法下载音乐的电脑。他是在有关滥用版权、打击非法音乐下载的一个听证会上作出这番惊人评论的。他在会上询问科技公司管理人员能否摧毁卷入此类活动的计算机，但是法律专家指出任何这类攻击都违反了美国联邦政府的反黑客法。当时，一家专门从事破坏音乐下载技术开发的科技公司 MedIaDefendeR 表示："没人想要摧毁别人的计算机。" 但是哈奇打断说："我想，这可能是教会一些人尊重版权的唯一方法。"

前司法部官员、乔治华盛顿大学法学院教授科尔说："这只是那些想要执行法律却发现很难执行的人的气话。"他认为，国会"极不可能"批准用黑客的方法保护版权，因为这可能错误打击无辜的用户。

金融机构应是黑客攻击的主要目标

据德勤会计师行 6 月 18 日发表的《全球安全调查》称，39%的金融机构去年至少遭到过一次安全突破。其中有三分之二是来自机构外部的黑客攻击。

过去的两年里，47%的金融机构保持或者增加了IT安全工作人员，78%的金融机构计划采用公共密钥基础设施（PKI）技术。还有差不多相同比例的金融机构计划在其安全系统中采用“智能”身份证。在接受调查的公司中，几乎有一半已经制定了与无线通信有关的安全政策。

尽管如此，在接受调查的人中，只有5%的人对其机构系统拥有良好的防御内部攻击的保护措施充满信心。

总的来说，63%的受访者表示，其管理层认为，IT安全开支对于其业务是完全必要的，并不是随意的开支。一般来说，IT安全开支占一个机构IT预算的6%至8%。

病毒攻击变本加厉如何有效的阻断恶意攻击

现在的病毒攻击已经越来越变本加厉了。据估计，目前流行的病毒有10万种，每个月新产生的病毒200种，平均每15封邮件中就有1封多的附件被感染。仅靠防病毒软件已经不足以应付这种局面，我们需要一个全面的、积极的、自适应的安全威胁管理方法，它应该包括三方面要素：隔离（IsoLate）识别出正在进行的攻击；遏制（ContaIn）防止安全威胁范围扩大；消灭（ExtInguIsh）用合适的补丁程序、

杀毒工具等消除迫在眉睫的威胁，同时采取必要的行动，防止类似攻击再发生。

隔离（IsoLate）

大多数安全问题都是由于各种安全技术之间互不联系造成的。它们之间往往是相互分离的，典型的例子是：一个防火墙发送了一条违反规则的警报，一个 IDS 检测到一个签名与一个攻击工具（一个后门特洛伊木马程序）相匹配，一个病毒程序也检测到了这个特洛伊木马程序。每个程序或者发出警报，或者在工作日志上记录下这些情况，但是却没有分析以上 3 种事件的关联性，因而也就没有发现，也许正有人试图控制服务器，而且已经在其中放入了特洛伊木马程序。

为什么会发生这样的事？因为有太多的系统安全警报和事件，主要的警报反而被忽略了。因此，准确隔离已存在的攻击，分析事件相关性，确定安全保护优先级和恰当的报警，这些绝对是必不可少的。系统一旦具备了智能性，才有可能评估哪个警报是关键性的。智能化安全保护将根据业务价值和业务优先级来设定和加强有关安全保护的政策和优先级，对关键业务的安全威胁必须给予最高的安全保护优先级，并将其迅速隔离。例如，涉及在线商店的问题与涉及内

部培训系统的问题相比，前者可能给业务运行带来的风险要大得多。因此，当这两种路由器发生宕机时，不应该发出级别相同的警报，应该在检查每一个路由器时都要与业务背景相联系，并根据恰当的优先级发出警报。

遏制（ContaIn）

遏制有多种形式。例如，病毒可能而且也应该在PC一级用合适的防病毒软件捕获和隔离。但是，这至多是一种有限的防御方法。由于病毒的某些清晰可辨的个性特征，在网络的进入点遏制攻击将更有效。名为A的电子邮件附件携带的病毒应该由邮件服务器上的过滤器或相应网关检测出来，并立即被截住。为了防止带病毒的附件在公司内被打开，还有必要部署阻塞功能，将部门、服务器甚至个人计算机隔离开。以“Love LetteR”这样的VIsuaL BasIc脚本病毒为例，面对这样的入侵，你可以通过网络迅速发布一个策略在病毒爆发结束之前不要执行VB脚本程序。

在爆发点上迅速应用一系列政策就能实现有效的遏制。当然，此前应该制订好灾难恢复计划。这样，一旦检测到IP攻击，就可以隔离部分网络或改变网络交换机的规则，从而阻止数据包的进入。一个更彻底的遏制方法是部署一个“蜜罐”，用来收集攻击者

留下的证据的自我牺牲型服务器。一旦检测到入侵，你就可以将攻击指向与系统的其余部分隔离的“蜜罐”服务器上。如果你要扭转被动挨打的局面并对那些实施攻击的人提起诉讼，这种方法尤其有用。

消灭（ExtInguIsh）

如果要彻底消灭一个攻击，我们就必须完成一些具体的工作。例如，如果是病毒，你必须解毒，并使用修补程序进行修补，去掉病毒丢下或安装的程序组件。恰当的做法是，清理干净所有受到病毒影响的部分，以保持系统的完整性，同时消除这个威胁或类似威胁再次发生的可能性。例如 KLez 蠕虫，仅将文件解毒是不够的，还要保证去掉所有的更小的病毒元素。否则，它一旦复活，会造成更大的损失。一旦病毒进入系统，就需要从头建立或启用一个可信任的备份恢复系统。

在目前的环境中，企业安全不再仅涉及独立的防病毒软件或入侵检测系统，它需要一个隔离、遏制和消灭安全威胁的全面集成的方法。例如，CA 的 eTRust 在管理内部和外部安全威胁时就采用这种 ICE 的方法，还使用相关智能技术预见性地防御潜在的安全威胁。

有效的威胁管理必须做好对付上述任一或所有

攻击的准备才是有效的，但是还不止这些，威胁管理还必须实现 3 个目标：降低风险、降低保护成本和简化企业部署过程。这些目标只能通过积极的和自适应的威胁管理方法来实现，而且这种管理是以协调一致和智能化方式来隔离、遏制和消灭安全威胁的。

FBI 获准网上版权侵害调查 各界对此褒贬不一

上周四美国国会授权联邦调查局（FBI）负责包括网上版权交换在内的版权侵害事件的调查。在这项代号为 HR－2517 的“2003 版权侵害阻止和教育行动”议案中，指令 FBI 制定具体方案阻止网上版权侵害事件的发生。FBI 将依令发出警告－－版权所有人有权调查可疑侵犯者，还将鼓励法律执行部门、版权所有人和 ISP（Internet 服务提供商）三方间的共同合作。

这项新议案还要求司法部雇佣精通计算机入侵和知识产权知识的专业人才，司法部门要和教育、商业部门通力合作制定民众版权知识普及计划。

电子前线基金会（EFF）的一名律师 Wendy SeLtzeR 认为，该议案存在很多方面的问题，特别是模糊了官方行为和民间行为的界限。该议案使 FBI 更多地涉足知识产权保护领域，给用户们造成一种恐慌心理－－政府就站在我身后。SeLtzeR 还表示，从隐

私的角度考虑，议案中关于要求 ISP 们必须与版权所有人和警方全力合作的条款更是莫名其妙，这样会迫使 ISP 把用户信息毫无保留地提供给美国记录行业协会（RIAA）。

美国记录行业协会（RIAA）和美国电影协会（MPA）对这项议案表示欢迎。RIAA 主席 CaRy SheRman 表示，本议案将加强 FBI 和其它执法部门的职能以打击愈发猖獗的对等网络侵权事件，两部门合作（FBI 和司法部）将使全美联邦检举机关具备充足的（权力）资源和专业能力加强版权侵害法的公正执行－－特别是针对网上大量的音乐版权侵害。早些时候美参议院司法委员会主席 ORRIn Hatch 曾经建议，版权所有人有权对有音乐盗版行为的 PC 进行远程摧毁。

新隐蔽新型“木马”病毒隐蔽性之高前所未见

近期互联网上出现一种威胁程度不明但非常隐蔽的新型“特洛伊木马”病毒，但安全专家声称他们已取得它的源代码。据台湾媒体报道，目前这种“木马”已经被种植在多台 Internet 服务器上(具体数字不详)，目前主要攻击基于 Linux 的系统，但也很容易就转移到其它操作系统上。

据悉，专家们正在积极研究这个名为 55808(根据位组长度而得名)的新型“木马”。这 种“木马”现

身已经月余并一直困扰着安全专家们。本周三有专家们已经获得了一个它的原代码拷贝，希望籍此拷贝搞清这个“木马”究竟想偷盗哪方面的信息。

目前可以明确的是，这种“木马”的隐蔽性之高前所未见。与众不同的是，这种“木马”无法自我复制而需要黑客将其种植在系统中。它可以发送网络噪声信息以迷惑能探测到被感染计算机 IP 地址和黑客 IP 地址的网络扫描工具，每感染一台电脑，它就会发送出 1000 个假冒或伪装 IP 地址。

这种“木马”遵从分布式网络设计，所有的“木马”代理(Agent)和“木马”尸虫(zombies)协同工作，尽管没有直接的通信信道，黑客却可以让它们良好地运转。而安全专家们对此分布式网络机制尚未完全掌握。

微软建议英政府禁用开放源码 尤其是GPL协议

外电 6 月 20 日报道，英国技术行业组织 Intellect 敦促英国政府禁止使用开放源码，特别是 GPL 协议保护下的开放源码。Intellect 技术组织是由微软、IBM、InteL、BAE 等多家 IT 巨头支持，它表示由政府出面支持开放源码软件许可协议会对合同竞争、成品软件质量，甚至对政府部门的机密都会造成恶劣影响。它还建议政府禁用 GNU 通用公共许可协

议(GPL)。GNU和Linux操作系统都是基于GPL协议的。

Intellect 是在英国 E-Envoy 办公室(OEE)及贸易和工业部(DTI)联合举行的关于开放源码使用的咨询会上做出上述建议的，此前该咨询会提议开放源码软件的开发应获得开放源码许可证。这个建议最早出现在 5 月的答复条上，但是直到上周才真正的公开。OEE 和 DTI 正在考虑为政府支持软件建立开放源码许可证默认条款，亦即除非有其它条款特别规定，开放源码许可证条款可默认实行。此举的目的是为了开放源码软件尽可能得到“自由”的开发和利用。

Intellect 表示它不反对实行开放源码许可证制度，但强烈反对采用 GPL 协议，因为 GPL 将会阻止政府从开放源码软件中受益，并会打击正规软件公司的积极性。该组织还暗示政府软件开发的合同竞争性会大大降低，因为软件商们宁愿去竞争一项没有开放源码许可证要求的合同。另外按照政府软件合同开发出来的软件其功能也会大打折扣，原因是开发人员肯定不愿意将他们的“精华”代码写进程序中，那样会迫于开放源码许可协议而公布于众。

Intellect 还建议政府涉密部门不要采用开放源码许可证，这样会将一些政府敏感信息暴露出来。

专家称垃圾邮件泛滥成灾 总量每6个月翻一番

英国的计算机专家经过调查发现，世界垃圾邮件的数量已达到全球电子邮件系统总容量的40%，并且还在以每6个月翻一番的速度增长。专家警告说，由于互联网服务器无法处理如此大的流量，电子邮件系统有可能在未来8到12个月内陷于瘫痪。英国两家主要的垃圾邮件过滤公司估计，英国的垃圾邮件数量在今后 7 个月内将超过目前全部电子邮件总量的50%。在互联网发源地美国，互联网供货商每天要处理大约90亿封电子邮件，其中90%以上是垃圾邮件。

防止垃圾邮件 NAI 独霸零售市场 90%以上

系统和网络防护解决方案领导者美国网络联盟近期宣布 McAfee SpamKILLeR 在 2003 年第一季度占有90%以上的零售市场份额，成为个人反垃圾邮件市场的领导者。McAfee SpamKILLeR 是 McAfee Security 消费者部门开发的防垃圾邮件产品。目前，绝大部分用户都使用这一工具来防止垃圾邮件。

NPD GRoup 最近发表的一份调查报告表明，在今年第一季度的零售产品市场，McAfee SpamKILLeR 领先于所有其它个人反垃圾邮件解决方案供应商。NPD GRoup 通过从零售商、分销商和其它渠道伙伴中搜集

信息来追踪产品的流向。

McAfee Security 认为 SpamKILLeR 成功的原因在于公众对于垃圾邮件泛滥的担忧和对易用、全面解决方案的需求。McAfee Security 消费者部门市场副总裁 LIsa HendeRson 说："个人用户每天被几十亿不请自来的垃圾信息所淹没。McAfee SpamKILLeR 在消费者中广受欢迎是因为它使用方便，并可为他们提供所需的所有功能，从而可将他们从对付垃圾邮件的负担中解脱出来。"

2002 年 5 月，为了解决日益严重的垃圾邮件问题，McAfee SpamKILLeR 诞生了。从它推出的那天起，它就得到了评论家和用户的首肯，因为它可有效地阻断不请自来的信息（垃圾邮件）、反溯垃圾邮件至互联网服务供应商源头，并向为垃圾邮件制造者提供服务的企业投诉，同时自动向垃圾邮件制造者返回一条伪造的"退回"信息。

垃圾邮件的问题变得越来越严重，原来只是其数量对用户造成烦恼，现在它已经变成了一个全面爆发的互联网传染病。McAfee 从那时起对此产品做了多次改进，例如支持基于互联网的邮件协议、基于社区的垃圾邮件报告，它更建立了一个世界范围内的"垃圾邮件陷阱"网络，利用这一网络来生成过滤器，以抵

抗最新的垃圾邮件攻击。未来的 SpamKILLeR 版本将增加更多新的、改进的功能，以确保本产品永远领先于垃圾邮件的发展速度。

在这一强大的消费者反垃圾邮件产品之外，美国网络联盟最近又宣布推出用于微软 Exchange 的 McAfee SpamKILLeR 产品，专门帮助小型和成长型企业抵抗垃圾邮件。McAfee SpamKILLeR 企业级产品家族探测垃圾邮件的成功率达 95%，可帮助企业降低责任风险、重新找回存储空间，同时提高员工的工作效率。

IT 复苏在晨曦中挣扎

长期以来对信息技术行业复苏的企盼现在就要得到实现了。比最近华尔街技术股大量反弹更具实质意义的是电脑产品和半导体产品的订单慢慢稳定并渐渐越来越多。然而还存在着许多怀疑者。甚至当复苏真正的开始的时候，行业分析家还在问，是否真是一次真正的反弹？或者是缓慢和不平坦的。在 20 世纪 90 年代时，信息技术是和经济齐头并进，而不是领先于经济发展时，信息产业由于他自己的“新经济”法则看起来更象其他工业行业，而不象商业。

也许华尔街的表现已超过了它自己，仿佛过时的技术反弹正在进行。纳斯达克股价自从 3 月 11 日就

上升了将近 30%，而 StandaRd &amp； Poor`s500 信息技术指数自从去年十月达到新低后最近又上升了 50%。也许，最重要的期待一个有规则的，缓慢的复苏的理由是信息技术的买家的态度的转变，或是计算机硬件和软件、服务的压力。他们在很大程序上控制了该行业的命运。

90 年代的无端的乐观和技术可以单独转化为商业的想法。现在，公司的执行官认为技术只不过是一个简单的工具。如果正确的使用，有可能只是一个无关紧要的工具而已。但是这个工具也相当的昂贵，将近 60%的商业投资的开销都是花在信息技术上来。所以信息技术很能刺激开销。

技术仍是一笔巨大的企业支出，但是在大多数的公司，技术预算如果不下降的话也是与往年持平。对那些高级技术执行官们(CIO)而言，这是一个相当不同的世界，这些 CIO 们长期以来已经习惯了把他们每年的预算提高 10%到 20%。

技术调查公司 GaRtneR 公司的一位调查员 RIchaRd HunteR 说："那些 CIO 们长期以来被要求来用更多的支出来做更多的事，现在他们则被要求用更少的支出来做更多的事。"当今年早些时候调查了 600 个全球的 CIO，GaRtneR 发现他们的最大的三个目标

分别是销减开支，提高信息的安全性和支持革新。“这对 CIO 来相说有相当大的压力，又要销减开支又要支持革新”，HunteR 说。企业支出计划仍是有波折的。CIO 杂志五月公布的调查显示，技术执行官们称他们预计在接下来的 12 个月中对信息技术的购买支出平均将增长 3.3%，而回顾 2000 年，该杂志每月的调查显示这些技术执行官们对此项支出的预算是增长 15%到 20%。甚至技术巨头们，比如微软，也知道企业用户的态度的转变，巴尔默本月在给他的所有员工的年度报告的电子邮件说：“当我和企业用户交流时，他们并不关心技术，只关心用更少的开销来做更多的事”。

《商业评论》的前任总编 NIchoLas G。CaRR 撰写的评论“IT 无关紧要”把许多技术执行官们攻击为异端，这篇评论认为在计算机技术越来越标准化的过程中，企业通过技术投资而使得自己相对于对手有竞争力会变得越来越难。

但是批评掩盖不了信息技术的再次兴起。半导体行业真正的开始了逐渐的复苏，本月早些时候，台积电和联合电子均报以月度销售超过两年前的任何月份。而美国半导体行业协会在最近的预测中估计今年将会复苏，销售比去年上升 10%左右。美林的分析家

Steven MILunovIch 表示：“技术还是带有传奇色彩的”

2000 年通过的儿童互联网保护法就是为了使儿童避免浏览网页中的色情内容

包括美国图书馆协会与美国全民自由联合会在内的反对者对这项法案提出了挑战，认为该法律违反了成人的言论自由权利，而且还会使少数人不能获得诸如有关癌症或大破坏之类的内容。

6 月 23 日，美国最高法院以 6：3 的投票结果否决了批评者的意见，宣称图书馆可以根据要求关闭过滤软件，这样人们就可以更容易地接触到网页内容。

这种观点认为，“由于当事者可以很容易地关闭网页内容过滤软件，因此人们大可不必对过滤软件会限制浏览有关内容感到担忧。”这项法律的实施可能会影响到数以百万计的从图书馆上网的读者。

英特尔欲建全球校园网络 解决数据迟滞问题

英特尔、普林斯顿大学、加州大学巴克莱分校以及其它许多院校和行业重量级公司联手解决全球性的数据中途迟滞问题。PLanetLab 实验室是该项目在互联网上的实验网络，它允许研究人员和其它人员测

试并创建最终能覆盖全球的应用程序。该实验室的工作完成后，将允许世界各地的网站播放视频节目，以协作的方式接入同时蜂拥而致的用户，而且不会因此造成堵塞。病毒追踪器也能更早地发现新病毒或拒绝服务攻击。

虽然许多人以为全球通信很顺畅，但互联网其实并不象它看起来那么稳定。服务器可能会垮，路由器掉线过多也会造成延迟。这些问题随着新应用软件以及各种服务在网上不断推出而日趋严重。解决这些问题的措施之一就是向更多的计算机物理发送应用软件，这也是 PLanetLab 的切入点。该网络一旦完成，将包括遍及世界各地的 1000 台服务器。该网络创建于 2002 年 3 月，包括 16 个国家、65 个网站的 160 台计算机，它运行的是红帽子公司修改版 Linux 系统，年底前有望发展为 300 台，而 1000 台计算机组成的网络则需要几年时间才能完成。

其它参与者包括惠普实验室、麻省科技学院、哈佛大学、CorneLL 大学、RIce 大学、以及其它在以色列、中国、英国、瑞典、我国台湾和德国等地的大学。

微软欲重回历史

简评：当微软巨人不再企求新的改变，它就不会获得高速增长。因此微软正在寻找新的突破点，比

如.NET。

贯穿整个 90 年代，很少有公司像微软那样获得持续增长和现货利润。由于这个软件巨人正好迎合了个人电脑的爆发性需求，它的收入在 90 年代每年平均上升 36%,并且它的股价从 60 美分攀升到了 59.19 美元。但是新世纪微软发生了令人吃惊的变化，微软年收入增长比率最高也只达到了 16%，而从 2000 年 1 月以来，它的股价也下跌了一半多，到 6 月 23 日，它的股价在 26 美元左右。

当别的技术公司的境遇还不确定的时候，微软还在一个很安全的港湾。它的 Windows 和 Office 产品每月给它带来 10 亿美元的收入，现在微软手持 460 亿美元。但微软已经感到它不象当初推出一个产品就很容易受市场欢迎。市场销售不断下滑，微软已经很难再到达当年 320 亿美元的销售神话了。微软不得不更加努力的来挽救他的股价。

一个很明显的迹象就是微软三年前所推出的.NET 和 Web Service，微软就是想用这个在对手的公司商业方向插上一脚，当时微软想象的是连自动售货机也可以使用这技术通过 Web 来共享数据，但是每个公司的 Web Service 产品进展都相当缓慢，而且让他的对手，诸如 IBM 也跟了上来。

许多潜在的.Net 客户都担心那些通过网络传送的主要数据的安全性。也许这种担心对缓慢发展的经济而言并不太重要，但是对高科技公司而言却是致命的。根据市场调查公司 IDC 的调查，全世界技术支出今年将增长有限的 2.3%，而这却是 2000 年以来首次获利。IDC 预计个人电脑单位销量在 2002 年仅为 1.5%之后今年将会上升 6.3%，而最近的 1999 年的增长却为 24%。“由于经济的不稳定，人们不愿意将钱花在任何东西上面。”微软 CFO John Connors 说道，虽然后来他又补充了一句：“形势还是有改善的。”

经济的缓慢强迫微软扩展他的市场而不是单单依靠已经成熟的 PC 行业。幸亏微软财大气粗，尽力利用他的 Windows 操作系统和 Office 套装挤入新的市场而他的竞争对手却一一倒下。

以 Office 为例。很多公司用户感觉到他们可以使用微软在 2000 年，甚至在 1997 年发布的老版本，因为这些版本仍能适用很多公司的要求，因此微软的策略是分割 Office 并为 Office 创造其它的位置。当最新的升级版本将于今秋公布时，一个专为小型企业设计的版本也将面市。微软也将在 Office 品牌之下在诸如“商业智能”领域推出新产品，“商业职能”软件能从不同的计算机系统里析取数据，然后分析这

些数据，并制定生产报告来帮助决策。

微软正在新的市场里寻找发展，比如为中小型企业设计的 “Run-the-busIness”应用软件。这已成为一块独立的领域，许多公司能提供处理各种业务的软件，包括从客户关系管理到人力资源到会计等等软件。但是由于做到经济节约很困难，那些将目标投向大公司的软件公司如 SAP 和 SeIbeL Systems ，都被淘汰出局了。

微软也对视频游戏下了大赌注，自从 2001 年 11 月发布 Xbox 游戏机以来，已经售出 900 万台，略超过任天堂的 GameCube，排在索尼的 PLay StatIon2 之后，这主要归功于微软花了 20 亿美元投入市场宣传。在微软的当前财政年的头 9 个月，微软共亏损了 7 亿 1500 万美元。但是他的现金足够允许 Xbox 的继续亏损。

微软将继续他在软件行业的领军地位，但是，20 世纪 90 年代的高速增长将只能是一个记忆了，分析家认为微软到 6 月底的这个财政年将增长 12%，到 2004 年，微软的销售将只增长 6%，而收入只增长 3%。微软将在 Xbox，小型商业软件甚至.Net 方面来证明他们的价值，使微软的股价重回旧高点。

VCON 推出带有网络共享功能的 IPNexus 产品

全球领先的 IP 视频会议系统供应商-以色列 VCON 通信有限公司宣布推出带有网络共享功能的 IPNexus V1.5 产品。新版 IPNexus 通过加装服务包的形式增加了几项新的功能。其中主要的新功能是网络共享 IPWebShare 功能。利用 IPWebShare 功能，原来 IPNexus 的用户可以利用自己 PC 机中的网络浏览器和任何人分享演示和文档。IPNexus 首先创建一个 URL 联接，允许任意数目的观众浏览演示人员的工作，这就是所谓的网络共享功能。为了方便网络共享功能，IPWebShare 可以按需提供工作栏。

另外，演示人员也可以选择演示模板，这样就可以方便地共享文档或 PoweRPoInt 文件。IPWebShare 界面上设有暂停、运行和停止键，允许演示人员无缝编辑和修改正在演示的内容。独特的 URL 联接允许用户轻松地在任何地点、任何时间创建网络广播，并提供密码保护。

如果想感受新版 IPNexus 增加的功能，请登陆 VCON 网站，下载软件服务包。该软件服务包对所有 IPNexus 用户免费。

以色列 VCON 公司简介

以色列 VCON 通信有限公司是基于 ISDN 和 IP 网络的视频会议系统的开发商、生产制造商和销售商，被视频会议行业誉为商业 IP 视频会议产品的世界领导者。公司提供基于 ISDN，TCP/IP、ATM，卫星、xDSL 和其它网络环境下的从桌面型、小型会议型到会议室型系统全系列视频会议解决方案。VCON 与世界范围内具有领导地位的一些高科技公司建立了战略性的联盟，为用户提供一流的音频、视频与数据协作整体网络多媒体解决方案。VCON 通信有限公司总部在以色列，在美国（奥斯汀、芝加哥、纽约、圣约瑟、华盛顿)、德国、西班牙、英国、日本设有分公司，在中国北京、上海和广州设有销售代表处。

VCON 公司的任务：

VCON 公司一直认识到人们对于把视频、音频和数据集中到一个单一的企业范围内 IP 网络上的需要。VCON 不断寻求并扩展与网络和通信行业中的一流的生产商的伙伴关系，为市场提供完整的企业网络多媒体解决方案。

VCON 的新技术：

作为 IP 视频占有率第一的 VCON 公司通过开发其基于 IP 网络的第四代视频会议技术：交互式 IP 多点广播，VCON PacketAssIst 体系，1.5Mbps 数据速率，

带宽自动调节,Internet Locator SeveR(ILS),非对称网络环境支持(xDSL)VCON 后处理算法(VPP)等将网络视频会议系统推广到世界多媒体通讯市场。

VCON 产品介绍:

会议室型系统

MedIaConnect 9000 系列，基于 SVGA 和 TV 的大型会议室多用途视频会议系统

MedIaConnect9000 多用途视频会议系统,专为在大中型会议室举行的网络视频会议提供更高质量的音频和视频传输，采用了全新的用户界面，并集成 VCON PacketAssIstTM (QoS)和多点广播技术，保证交互式会议的顺利进行。

MedIaConnect9000 多用途视频会议系统,可以对权限用户提供互联网络或公共网络存储文件应用服务，包括管理交流，发送电子邮件，共享或协作文件，公司内部网络文件下载等功能。MedIaConnect9000 包括两种型号，其中标准型包括配套主机 CODEC、变焦摄像头、增强型桌面麦克风，而专业型配置有高保真声音系统、29 英寸 SVGA 显示器、特制可移动式机柜等选件。MedIaConnect9000 配合 VCON 公司强大的 MXM 系统即可实现视频电话功能，如呼叫转移、即时密集会议等。

MedIaConnect6000 系列，基于电视的会议室型视频会议系统

您需要一个专业的，很容易操作的还具有数据共享性能的会议室视频会议吗？基于电视的 MedIa Connect6000 系列是为会议室型视频会议系统最适合那些正寻求低价格、容易操作但具有丰富性能产品的使用者。这个系统还配套带动有一个大的监视器和一个别致的机柜。

MedIaConnect6000 在 LAN/IP 上速率可达 1.5Mbps，在 ISDN 上速率可从 128Kbps 到 384Kbps，加上它可以配置两个、三个监视器的性能，MedIa Connect6000 完全可与其它高终端系统竞争，是会议室和其它视频会议场所的最理想的选择。

FaLcon IP 神鹰双模式系列

FaLcon IPTM 是一种双模式的适用于 IP 及 ISDN 网络的机项盒装置，它结构小巧、易于使用，并可提供群组系统级质量和性能。FaLcon IPTM 是专为那些寻找易于使用的小型视频会议系统，以充分利用其 IP 及 ISDN 网络资源的用户的理想选择。

VIGO 千里眼系列

VIGO 是一种革命性的个人会议电视装置，适用于连接桌面系统和笔记本电脑。利用 USB 热接入方式，

该装置可非常方便的与 PC 及笔记本电脑连接，VIGO 是一种轻便的，可携带的会议系统，无论在办公室或是旅途中，为商务用户提供高质量的视频会议效果。它的用途广泛，设计高雅，极其灵活的配置和漂亮的 One-touch VIGO 按钮使会议电视系统的操作简单的如同打电话一般。由于具备了 VCON 的领先的 VideooveR IP 技术,VIGO 将在 IP 网络上上为用户提供无以匹敌的会议电视质量。

桌面系统

专业的桌面会议视频会议系 CRuIseR384

想让您的台式电脑具有更多的功能吗？试一下新的 CRUISER384 通讯工具一种单板解决方法（所有的东西都在一块板上）。享用一下全屏幕，1.5Mbps 速度的 IP/LAN 和 384Kbps/ISDN30FPS 视频会议系统。或者用一个 MVIP 连接到第三方 V.35，T1/E1 或者 RS449 板上，可以 ISDN 速度冲浪互联网，用 MICROSOFT NETMEETING 共享应用程序的会议功能，并与 VCON 的 PoInt-and -CLIck 会议软件连接。而且您也同时得到一个彩色摄像机,多媒体扬声器及三项音/视频输入、CRUIER384-即插即用。

CRuIseR150 桌面会议系统

想使自己不受束缚吗？把所有的可选功能与

CRuIseR150 一起用上，你不会拥有一切 1.5Mbps 的 LAN 和 128Kbps 的 ISDN，或在 MVIP 接口上另装上一个卡使 ISDN 扩展到 384Kbps 或 RS449,ATM,V.35/E1。这套系统配有 CRUISER150 编码器，内置麦克风的模拟摄像机，软件及听筒。小系统般的价格及其通用性，扩充性使 CRIuseR150 很好的选择。

ESCORT25 PRO 桌面会议系统

喜欢高性低成本的系统吗？ESCORT25 PRO 是用于 LAN 的视频会议系统。如果在 LAN 上增加了一个路由器或者网关，这样 ESCORT 使您能到达任何一个地方。虽然 ESCORT 只是其它系统的部分价格，但却为您提供局域网 LAN 上高达 30fps 的清晰图像质量。ESCORT 是现有市场上成本低且有效的解决方案，并展示共享的 MICROSOFT NETMEETING 的功能。ESCORT 能满足您所有对于视频会议功能的需求-PCI 编码板、摄像机、听筒以及友好的使用软件。

VCON 开发工具包（VDK）

您想使视频应用轻松、顺利的加入到您的专业应用中吗？VCON 开发工具包是您的选择。VDK 是一套完整的 32 位 OCX 定制控制软件，可以用来将 VCON 的视频通讯集成到新的或现有的应用程序中。它是为软件开发者进行软件开发而设计，VDK 能在所有 VCON 桌面

和会议室型产品的基础上创建视频会议应用。VDK 可应用各行各业包括银行、财务、房地产服务，远程咨询，电子商务，远程教育，安全监控，远程医疗，旅游，呼叫中心等广泛领域。

媒体交换管理系统（Video SwItch）

面向运营商和企业的媒体网络管理支撑系统

产品详细介绍： MXM 是一种运行在 Windows NT 服务器上的软件解决方案。利用该软件，管理员可从远程控制台进行集中维护、配置和管理。MXM 支持 VCON 和非 VCON 终端，以及多种 MCU、网关和其他组网设备。MXM 可以提供视频电话服务（比如：呼叫转接、呼叫转移和特服号群组服务），MXM 使用户召开视频会议就象拨打电话一样简单。

VCON 的 MXM 服务器是电信运营商和企业网络里管理 Video OveR IP 应用的重要组件。其功能包括终端集中管理、带宽管理、终端状态监测以及其他功能。VCON 的 MXM 服务器将本应属于网络端的关键功能从终端上脱离出来。网络规划、跟踪和计帐相关的使用报告以及安全和策略定义使 MXM 服务器成为网络媒体解决方案必不可缺少的工具。

通过功能和控制手段移植到网络服务器，大量 IP 视频终端在应用时可比以前拥有更高的可管理性和

更强大的功能。

计算机安全——网上围棋对抗大赛遭攻击黑客冒充选手入侵

昨天下午，中韩围棋新人王对抗赛在中国的新浪网和韩国 cYbeR 网站落子，孔杰七段执白中盘战胜韩国的宋泰坤四段。赛前，由于有人以孔杰的名字入侵比赛的服务器，导致比赛推迟了１０多分钟才正常进行。

这是第一次通过互联网进行的国际围棋比赛，孔杰和一名网络技术人员坐在中国棋院的一个对局室中，比赛原定于下午１点开始，但过了１点钟，比赛还无法正常开始，孔杰索性走到房间的另一端闭目养神起来。原来，主办方为了这次比赛专门开设了一个加密的服务器地址，没想到这个服务器被一个“高手”破解并且以孔杰的名字登录，这样就出现了两个孔杰，被搞糊涂的韩方向中方反映后，技术人员换上了之前为这次比赛备用的一个服务器，用了１０多分钟的时间才让比赛得以正常进行。比赛的韩方 cYbeR 网站代表邢春堂告诉记者，为了这次比赛主办方在技术方面做了很多准备和方案，但是出现这种情况还是让人意外。新浪围棋网负责人宋炯辉说这种情况可以说是黑客入侵，但是他们很难扰乱比赛正常进行，“我

们做了很多准备，可以切换不同的服务器地址。”

昨天的比赛采取每方各一小时的快棋赛，一小时后开始读秒，由于孔杰在前面花的时间比较多，进入读秒阶段后一度有些凶险，最后因宋泰坤右边的大龙出了问题，孔杰劫活后得以中盘获胜。

赢了棋的孔杰显得轻松不少，对于这种“网战”，孔杰表示刚开始读秒的时候听到电脑读秒的声音有点慌，后来就适应了，他还认为这种读秒的方式很好很清楚。比赛结束后，当孔杰得知是有一个“孔杰”入侵后，他笑着说：“这么崇拜我，挺有意思的。”今天下午1时，孔杰和宋泰坤将进行第二回合的比赛。

不是所有的黑客都是罪犯！揭示黑客道德准则

黑客有自己的道德准则：所有的信息都应当是免费的；打破电脑集权；计算机使生活更美好等

普通的电脑程序员要成为黑客也不难，但要成为一名黑客高手，除了智慧，还要有足够的耐心和毅力

网络安全最薄弱的环节并不是系统漏洞，而是人的漏洞

电脑黑客是一群处于地下状态的电脑狂人，尽管技术高超，但他们却不能抛头露面，他们的网站一律以黑色为背景，平添几分神秘色彩。想到黑客，人们脑中就闪现出两个字：罪犯。

不过最近，这些神秘人物聚集在美国匹兹堡，参加最古老的黑客大会—所谓最古老，也不过是 1985 年后才出现的新鲜事。本届大会组织者最重要的任务之一是让公众相信，不是所有的黑客都是罪犯。就连出席大会、目光深邃的 FBI 探员汤姆·加拉索也同意：黑客并不总是利用计算机犯罪或捣乱，一些黑客破解电脑代码只是为了发现更方便使用某个程序的“捷径”。

技艺精湛

一名昔日黑客告诉记者，依靠黑客工具，普通的电脑程序员要成为黑客也不难，但要成为一名黑客高手，除了智慧，还要有足够的耐心和毅力。

现成的黑客工具可以通过扫描上网者的 IP 地址寻找到目标计算机，并列出漏洞清单。但如果你水平不够，即便看到这个清单也无法加以利用。

黑客们为了不暴露自己的 IP 地址，通常使用两种方法，一种是利用代理服务器，将自己的 IP 地址伪装起来，这种代理服务器很多都可以在网上免费得到。另一种是“跳板”技术，也就是说，寻找一台正在上网的电脑，假借这台电脑的地址隐藏自己，这台电脑通常被黑客们称为“肉机”。许多“肉机”主人在被安全部门找到时，还往往莫名其妙，一脸无辜。

找到一台可以“嫁祸”的个人电脑要费很长时间，因为个人用户不会在网上逗留很久，每台电脑的实际情况也都不一样。而微软这样的公司也会一直推出补丁程序来修补他们的漏洞，所以黑客需要不断发现新漏洞。“总而言之，要掌握真正的黑客技术，是很难很难，很繁琐的”。

历史上最著名的黑客莫过于凯文·米特尼克。15岁时，米特尼克就成功入侵“北美空中防务指挥系统”，成为经典案例。16岁时的一天，他在看FBI的电脑网络，发现FBI正在调查一名黑客，便饶有兴趣地看起来，看着看着，突然大吃一惊：被调查者竟然是他自己！

在很短的时间里他频频进入各大公司，修改用户资料，害得这些公司哭笑不得，连连向客户道歉。媒体称他无所不能，还被《时代》选为封面人物。但他最终还是被FBI绳之以法，据说，是他的作案风格，而不是他的技术，让他露出了马脚。米特尼克不但被判5年监禁，一切上网工具包括计算机、手机都不准触摸—因为他只需敲击5个键就可入侵一家网站。

绝大多数的黑客只是一些电脑技术的狂热爱好者，他们入侵各种网站，只是以此为乐。一名黑客告诉记者：“第一次成功入侵后，很兴奋，看到了别人

公司的客户资料、财务报表，真是有点心惊胆战，但5分钟后我就发现，这些资料对我而言，也没有任何用处。”因为如果要利用黑客技术犯罪，就必须冒坐牢的风险，一般人是不会那么做的。

黑客们有自己的道德准则(theHackeREthIc)。史蒂夫·利维在其著名的《黑客电脑史》一书中对于“黑客道德准则”作出了详细的解释，包括：所有的信息都应当是免费的；打破电脑集权；计算机使生活更美好等。这些东西被黑客们看作是“江湖规矩”，反正你只要想成为一个黑客，这些就一定要遵守。

黑客大会的组织者图姆波尔说：“那些任意涂改网页或者摧毁像 eBay 和亚马逊网站系统的人不应被称做黑客，我把他们叫做破坏分子。”中国的黑客组织黑客联盟也宣称：作为黑客，其职责就是寻找漏洞、维护网络安全。

前不久，一所美国大学宣布将于今年秋季开设教授如何编写病毒软件的课程，消息一公布，就招致极大争议。大学方面的理由是，要成为反病毒专家，就应该知道如何制造病毒。但反对者认为，你不需要写病毒才能理解它，世界上已经有6万种电脑病毒需要消灭，这种做法不能被社会道德所接受。

在绝大多数黑客看来，研究黑客技术的目的只能

是一个，那就是以提高电脑技术水平为目的，以不搞破坏为底线。

人是最大漏洞

对黑客持宽容态度的人认为，一个网站被黑，恰恰说明它有。事实上，很早就有人知道这些易受攻击的弱点了，但是普通人根本就没有电脑安全方面的意识。

已经金盆洗手的凯文·米特尼克日前在接受采访时说，网络安全最薄弱的环节并不是系统漏洞，而是人的漏洞。他就曾假扮摩托罗拉公司员工，并成功说服该公司的工程师将最新的电话系统软件发送给他。他说，虽然黑客以前发动攻击只是为了好玩，但现在很多攻击的目的却远不止此，它们的目标更多地锁定在了机密的商业和个人信息，以获得非法利益。

面对这些潜在的巨大威胁，政府和许多企业都投入了大量的财力和物力用于安全防范，预计今年一年投入的资金将高达 135 亿美元，比 2000 年翻了一番。但安全专家认为，仅仅购置安全软件是远远不够的，政府和企业必须充分注意到人的因素，因为最薄弱的环节很可能是大意的人，而不是软件的漏洞。米特尼克攻陷了许多极为繁复的网络，靠的不光是高超的技术，更多的是利用人的弱点。他的名言是：“愚蠢是

没有补药的！”

米特尼克认为，计算机和解调器都不是问题的关键，人才是最重要的，只有把人的安全防范意识提升到一个相当高的地步，黑客攻击的破坏性才能够从根本上降低。这个曾经被称为“地狱黑客”的电脑高手现在创建了一家安全咨询公司，专为客户提供安全防护服务。

SobIg.E 主攻美国用户跃居病毒排行榜首位

近日消息，SobIg 病毒的最新变种仍然在网上恣意肆虐，凸显出邮件病毒仍是人们挥之不去的阴影。美国电子邮件服务商 MessageLabs 表示，在过去的 24 个小时里，这种叫做 SobIg.E 的病毒给美国计算机用户带来了极大的不便。该公司的研究表明，被 SobIg.E 病毒感染的案例，有 70%来自美国，18%来自英国。

MessageLabs 的首席技术员抱怨道，“SobIg.E 自本周工作日开始就不停的进行破坏，一定是某位美国破坏者故意在网络上释放的病毒。” SobIg.E 病毒传播之广使其跃居 MessageLab`s 病毒排行榜榜首。

SobIg.E 象其他病毒一样，经常以“申请回复”等容易让接收者迷惑的面貌出现。它经常在邮件中写道，“详情请见附件”。而附件是一个 80kb 的恶意程序，只要被打开，它将感染任何装有微软 Windows 操

作系统的计算机。SobIg.E 从 Windows 地址簿、浏览器收藏夹里收集邮件地址，并给地址发送邮件。可恶的是，SobIg.E 还能以随机的方式发送邮件，因此被感染的邮件有可能传到任何一个网络使用者。SobIg.E 比其他病毒厉害的地方在于它不需等待命令能在同一时间发送多份邮件，而其他病毒有时还要等待命令，且通常一次只发一封邮件。SobIg.E 还有一个特点，它对家庭用户的打击更厉害，报告表明家庭用户感染的几率十倍于商业用户。

微软出售的一种软件可以让企业每月发出 1 万封电子邮件

微软现在出售的一种软件可以让企业每月发出 1 万封电子邮件,售价为 299 美元。它提供的一个软件中捆绑有垃圾邮件过滤软件,售价为 9.95 美元。苦于邮箱太小而垃圾邮件太多的人还可以向微软订购额外的电子邮箱空间,费用是每年 19.95 美元。微软坚称,所有这些与电子邮件相关的产品都是为合法用户设计的。

但在密苏里、密歇根和加利福尼亚等州,一些禁止未经收信人同意就向其发出商业电子邮件的法案均招致微软反对。微软提出,应当允许所有公司在未征得收信人同意的情况下向其发送电子邮件,前提是

不得在发送邮件时采取欺骗性技术手段以躲避垃圾邮件过滤软件的筛选,而收信人在收到信件后可以选择今后是否继续接收此类信件。

此前在密苏里州,州众议院已经投票通过了一项反垃圾邮件法案。但在微软的游说下,该州参议院上月在最后一刻否决了该法案。

垃圾邮件可变为传播病毒的工具

一家安全公司说,垃圾电邮发送者正在通过家庭电脑让病毒散发匿名的垃圾电邮。

MessageLabs 公司称,公司的分析数据表明,来自网络电脑的群发垃圾电邮正在不断增加,它们通过电子邮件的附件来散发邮件。

位于新西兰的邮件安全公司资深反垃圾电邮技术人员 SeRgeant 说,这里有高度的相关性,大约有 3 万台机器有开放代理服务器软件,正是这些机器发出了病毒。

所谓开放代理,又称开放转发,是指能够重发电子邮件或其他网络数据的电脑,在转发过程中系统删除了能够确认流量源头的原始地址信息。这 3 万台电脑占MessageLabs登记的大规模主动发送电邮开放式转发电脑中的 14%,也就是所谓的垃圾电邮。

如果此事是真的,这项发现就能够为反垃圾电邮

的活动增加动力。本月早些时候，美国联邦交易委员会要求国会给它更大权力，以便惩罚那些垃圾电邮的散发者。

五月中旬，联邦交易委员会和其他国家的执法机构一起向1000多家电邮服务器运营商发出了警告信，敦促后者屏蔽服务器的开放转发功能。

MessageLabs公司说，垃圾电邮构成的网络流量占网络电邮总流量的30-75%，而将近70%的垃圾信息来自这些开放式转发电邮服务器。反垃圾电邮专家说，这是一个有趣的数据，它能够证明垃圾电邮转发和病毒转发的相关性，然而，人们很难确定这些被感染的机器。

反病毒专家说，这种垃圾电邮与病毒的联系还可以从其他角度解释，例如，那些易受病毒感染的电脑更有可能下载那些让系统成为开放转送通道的程序。专家同时还强调，有14%的相关性没有得到证实。

全球政客与专家云集峰会 共同对付垃圾邮件

最近全球的反垃圾邮件峰会上，政客与行业的领军人物称，对于垃圾邮件的泛滥，有必要进行一次全球打击。

在所有议会参与的国际组织的峰会上，英国、欧

盟和美国的政府官员和安全公司对于泛滥的垃圾邮件表示了不满，并号召跨区域合作。这些合作包括相应的立法等，以阻止垃圾邮件的快速增长。

英国电子商务部长 Stephen TImms 称，垃圾邮件不仅仅是英国与欧洲的问题。许多垃圾邮件来自于欧洲以外，例如美国。因此有必要与美国共同讨论出一个解决方法。

垃圾邮件没有国界。在美国，联邦贸易委员会也向政府提交了相应的报告，要求加大打击垃圾邮件的力度。在这次峰会上，许多代表指望美国提出一个解决方案。这并不是因为美国在反垃圾邮件立法上有着先进的经验，而是因为美国是一个垃圾邮件滋生地。

英国的一些官员称，美国是世界上垃圾邮件的首都。不下 200 个官员称，欧洲的 90%以上的垃圾邮件来自美国。因为这些邮件的地址在美国。

美国的官员则表示反驳。他们称，世界上有 80%的以上的垃圾邮件是用英文写的，这并不表明，这些垃圾邮件是说英语的国家的“杰作”。

专家称，事实不可能找到垃圾邮件“真凶”。目前，针对垃圾邮件，美国已经向白宫与参议院提交了立法申请。但是，BRIghtMail 的首席执行官 EnRIque SaLem 称，严格的立法并不是最有效的，因为单一的

手段是不会见效的。

专家称，垃圾邮件十分猖獗。专家预测，不久的将来，垃圾邮件将达到 50%，也就是说每 2 封信中就有 1 封是垃圾邮件。专家称，这么高的比例已经是一个标志，全球应当对垃圾邮件进行处理。

垃圾邮件的代价—每位员工每年损失 874 美元

根据独立调查公司“核子调查”最新的报告显示，垃圾邮件对美国公司的工作效益产生重大影响，每位员工每年的损失达到 874 美元。

这份报告的题目为“垃圾邮件：无声的 ROI 杀手”。它的调查结果来自对美国 76 家公司员工和 IT 管理人员的访问。874 美元的损失是以每小时工资 30 美元、每年 2080 个工作小时的标准进行计算而得出的。

调查得出的其它发现包括：公司因垃圾邮件每年每位员工的生产力损失大约为 1.4%、平均每位员工每天收到 13.3 封垃圾邮件、每位员工平均每天要花 6.5 分钟来管理垃圾邮件。

根据“核子调查”公司的报告显示，使用垃圾邮件过滤办法并不能显著地提高员工的生产力。因为垃圾邮件过滤办法只能过滤 26%的垃圾邮件，因此有或没有都不会显著改善员工的生产力。

“核子调查”公司指出，有效解决垃圾邮件的办法并不是使用最新的反垃圾邮件技术，而是公司应当到法庭或国会来寻求对垃圾邮件的扼制。微软与其它公司最近对垃圾邮件制造者的法律行动比反垃圾邮件技术更加有效。

美政府警告黑客将对数千家网站发动攻击竞赛

美国政府与私人技术专家周三发出警告，黑客计划在周日一次松散组织的“竞赛”中发动对数千家网站的攻击，这可能会破坏互联网的传输。

这次“竞赛”的组织者专门成立了一个名为“网页篡改挑战”的网站，它已于周三傍晚被关闭。在遭到关闭之前，这一网站用蹩角的英语为可能参加“竞赛”的黑客列出的比赛规定，它还发出警告“网页篡改属于违法行为”。

美国土安全部周三表示，他们已经了解了黑客的计划，但是并不打算发出任何正式的公众警告。而美国首席信息官委员会则警告美国各个机构和它们的专家严密注意联邦机构网站的安全。

技术行业的一家早期预警网络通知各家公司，表示已收到“可靠信息”黑客将发动进攻，而且已经侦测到黑客对公司和政府网络的扫描活动，这些扫描目

的是发现网络存在的弱点以便入侵。

网络安全与重点基础设施协调机构驻纽约办公室警告称，黑客的目标是在 6 个小时内对 6000 个网站进行破坏，家庭用户不会成为黑客袭击的目标。

纽约官员要求公司改变他们的缺省计算机密码，开始更加严密地监视网站活动，减少服务器一些不必要的功能和安装最新的软件补丁程序来防止黑客的攻击。

据称这次“竞赛”对黑客的奖励将是 500 兆字节的网上存储空间，这一奖励对计算机黑客来说根本不算什么，因为他们有能力进入数千台计算机，可以轻易地偷走公司网络的存储空间。

日本 03 年上半年电脑病毒感染数比上年少 4 成

趋势科技于 2003 年 7 月 2 日，整理并公布了 2003 年上半年（1 月—6 月）日本国内的电脑病毒感染情况。该报告显示，半年期间的受电脑病毒感染数为 1 万 7026 件，与上年同期（2 万 8938 件）减少了约 4 成。

病毒感染数量减少是因为企业和 ISP 针大都对电子邮件附件型病毒积极采取措施以及一般用户不再贸然打开附件等因素。该报告分析称，电子邮件附件

型病毒曾经在短时间内造成大范围的感染，但通过采取措施使受害数大幅减少。

而取代电子邮件附件型病毒造成新的损害病毒将有两种，（1）只要查看 Web 网站或 HTML 电子邮件便会感染的脚本（ScRIpt）型病毒；（2）通过网络共享文件夹感染的蠕虫型病毒。

2003 年上半年病毒感染的明细如下，从多到少依次为求职信病毒（WORM KLEZ），共计 2844 件；VBS REDLOF，共计 1617 件；OPASERV（WORM OPASERV），共计 1038 件。

黑客比赛清晨结束 美国紧急统计网站灾情

来自国外媒体的报道称，黑客团体发动的比赛已经于今天早间结束，黑客们宣称已经成功的把几千个网站变脸，不过，受灾网站的数目还在了解过程中。截止到目前，国外还没有传出有知名网站被黑的消息，国内也没有这样的消息传出。

根据报道，被黑客们变脸的几千个网站当中，多是一些大家都没听过的小网站，网友熟知的大网站，包括知名企业、政府以及各大入口网站，都没有传出灾情。让国内媒体和网站松了一口气的是，中国网站不在被攻击之列。

周一早间，记者从各大安全厂商处获悉，国内一

切平静如常，没有任何遭受到大规模攻击的迹象。同时，国内也没有网站传出被“变脸”的消息。倒是周末时分，“博客中国”网站被攻击瘫痪，根据专家分析，攻击方式是 DDOS，和此次国外黑客的行事不相符合。

不过许多专家依然提醒到，国内网站安全防范之薄弱，根本无法承受起如此大规模的攻击，专家仍然呼吁国内网站加强安全防范。

索尼发出警告：警惕欺骗顾客服务的电子邮件

索尼的美国法人 Sony ELectRonIcs 于当地时间 7 月 3 日发出警告称，目前假冒 Sony 公司发出的诈骗电子邮件正在流行。该诈骗电子邮件的主题名为“SonystyLe user and EMail addRess”，它假冒 SonyStyLe CustomeR Service 发出的信息，要求客户提供用户名、密码以及电子邮件地址等个人信息。

Sony ELectRonIcs的e-SoLutIons业务总裁MIke FasuLo 说明称，“该信息并非由 SonystyLe.com 等索尼网站或索尼法人发送的。我们将保护顾客个人信息当做最优先的任务，我们正在与有关当局合作争取迅速解决这一问题”。另外该公司还补充说，“Sony ELectRonIcs 的所有的 Web 网站已经采取了可靠的安全措施，没有迹象表明 SonystyLe.com 以及该网站的

数据安全性受到侵害”。

Sony ELectRonIcs 提出警告，如果收到该诈骗电子邮件务必立即删除。可以通过该公司的 Web 网站获取当万一不慎回复该诈骗电子邮件时的处理方法。另外在联邦交易委员会（FTC）的 Web 网站上也刊登了关于个人信息被盗的详细信息。

垃圾邮件失控!03 年年中邮箱里 50%邮件全没用

市场研究公司 PRobe ReseaRch LLC 于 7 月 8 日发表一篇报告称，垃圾电子邮件失去了控制，到 2003 年年中，全部电子邮件中将有 50%是垃圾邮件。

垃圾邮件，也就是未经许可发送的商业性电子邮件，威胁到了电子邮件作为通信媒介的有用性。例如，在美国在线和微软的 MSN 网络，发往这些网络域名的电子邮件中有 70%-80%包含垃圾邮件内容。

PRobe 公司研究经理 ALan MosheR 认为，垃圾邮件已经增加了网络服务提供商的运营成本，因为网络服务提供商需要增加电子邮件服务器和存储容量来处理日益增长的通信量。

他说：“垃圾邮件迫使网络服务提供商配置额外的工具帮助用户控制发往其邮箱的电子邮件。网络服务提供商还不得不增加第三方服务来拦截大量的垃圾邮件，防止这些邮件进入用户信箱。”

MosheR 表示，即使使用了封锁和过滤的方法，垃圾电子邮件仍可以突破封锁到达最终用户那里。他认为，垃圾电子邮件不是很容易解决的问题，需要从许多方面与其作斗争，包括在管理和立法领域与其作斗争。

黑客“操纵”上千计算机 用以提供色情服务

电脑安全专家周五指出，近 2,000 台使用 Windows 操作系统和高速上网的 PC，已遭一支行踪隐密的程度挟持，并正在被用来发送色情广告。

来自波士顿的电脑安全顾问史密斯(RIchaRd M。SmIth)表示，目前尚不清楚，这种所谓的“特洛伊木马”程度究竟是如何传播到全球受害者的电脑中，而这些人很可能还对此事一无所知。

安全软件制造商 Network Associates ，将这支特洛伊木马程度列为低危险级，因为它看起来并未蔓延到更大范围，且对受害电脑并未造成损害。

史密斯说，特洛伊木马程序最典型的传播方式是通过电子邮件，也可以透过浏览的网页潜入电脑。

他表示，这支被称作“移入的黑手党”(MIgmaf)特洛伊木马程序，会将被害电脑变成代理服务器，扮演网络浏览者与色情电子邮件或网站之间的中间人。

史密斯怀疑，MIgmaf 可能来自俄罗斯，因为它所

涉及的一些电邮地址可追溯到位于俄罗斯的服务器。此外部分涉及的网域名称也包含俄语。

中国垃圾邮件暴增 立法工作迫不容缓

半年以前，《广州日报》曾经花大篇幅对反垃圾邮件进行了报道，当时垃圾邮件还是一个不痛不痒的东西。半年过去了，全球垃圾邮件的增长速度已经远超出年初业界的预测，危害程度急剧上升，连微软、雅虎、AOL 这样的国际 IT 巨头都纷纷跳出来要求立法。

记者从中国互联网协会了解到，由于对反垃圾邮件工作重视不够，中国已经成为全球垃圾邮件比较严重的国家之一，而且正面临成为全球垃圾邮件温床的危险。现状垃圾邮件占正常邮件一半“垃圾邮件的增长已经到了不可不管的地步了。”在接受记者采访时，中国互联网协会的一位负责人如此表示。

根据该机构刚发布的调查报告，目前我国网民平均每周收到 16 封电子邮件，其中垃圾邮件占 8.3 封，垃圾邮件数量已经与正常邮件数量相当，并将很快扩大与正常邮件的数量“优势”。根据国外一家叫做丘辟特的调查公司的一份调查报告预测，到 2007 年每个网民平均每年将收到 3900 封垃圾邮件。

而作为中国反垃圾协调小组发起人之一的263网

络集团副总裁田健最近也在高度关注垃圾邮件的增长情况。田健告诉记者，垃圾邮件的增长速度远超出了先前的估计，作为中国最大的邮件运营商，263 去年同期每天屏蔽掉的垃圾邮件约两三百万封，而现在每天多达 2000 多万封，几乎增长了十倍。

据邮件过滤服务商 M essage Labs 公司统计，目前平均每 2.6 封邮件就有一封垃圾邮件。田健告诉记者，每一封垃圾邮件造成的损失至少是一美元，这包括占用的带宽资源、上网费用以及病毒破坏等，全世界的公司企业每年大概要花费 80 亿至 100 亿美元来解决垃圾电子邮件问题，并且这一数字每五个月会翻一番。

新动向部分运营商传输垃圾邮件

垃圾邮件之所以泛滥成灾，说到底是利益驱动使然。记者在与业内人士交流中了解到，一个从非法贩卖邮箱地址到专业发送垃圾邮件的黑色产业链已经形成，一些个人或小公司利用各种手段在互联网上猎取用户邮箱地址，然后以低价向一些广告公司出售，从而利用极其低廉的成本达到促销或其他宣传目的，一个小时能够发送多达 100 万封垃圾邮件。

据“时代营销”负责人冯英健介绍，利用垃圾邮件促销成本极低，覆盖面又广，因此成了一种新的“网

络营销”手段。冯认为，垃圾邮件歪曲了“网络营销”的本意，随着网民对垃圾邮件的反感程度加强，它不但起不到促销的作用，反而会损害企业的形象，实际成本并不低。

冯英健告诉记者，他曾经搜集到十多种专门用于发送垃圾邮件的软件并在网站上公开曝光，结果接到不少恐吓电话。“只要有需求，垃圾邮件就不会消失，因此必须正视这个问题”。

田健告诉记者，由于短期利益的驱使，部分运营商也在暗地充当“垃圾邮件提供商”的角色，尤其是一些免费邮箱。相比来讲，国外的一些免费邮箱比如微软的 HOTMAIL 虽然也有垃圾邮件，但是数量要少得多。

预测垃圾邮件或向中国转移

就在微软、雅虎、AOL 等纷纷要求为反垃圾邮件立法的时候，美国联邦贸易委员会日前宣布出台相关规定，垃圾制造者可能面临高达 20 万美元以上罚款，5 年监禁的重罚，并终身禁止参与促销活动。在欧洲这样的立法工作也在加紧进行。而目前中国由于此立法一片空白等原因，全球垃圾邮件的制造中心正开始向中国转移，中国面临成为全球垃圾邮件温床的危险。“中国有成为全球垃圾邮件温床的危险！”半年前

在接受记者采访时，中科院信息安全技术工程研究中心主任卿斯汉就曾经发出这样的担忧。

田健告诉记者，尽管中国反垃圾邮件协调小组已经成立，与国际组织的合作大大加强，但许多邮件提供商并不重视这个问题，拿技术和人员投入来说，263每年都投入几百万，但国内还没有同行愿意这样做。田健认为，要解决垃圾邮件主要涉及三个层面：政府、企业和个人，其中政府是最关键的，最迫切的问题是立法，但目前进展缓慢。

在接受记者采访时，专家和企业家普遍认为，中国反垃圾邮件已经到了不得不重视的时刻，否则国外的垃圾邮件会肆无忌惮地向中国转移，将中国作为其“制造中心”，这样造成的后果是中国的许多正规网站被国外屏蔽，造成中国网站“出国难”的问题，严重的话会使中国某些地区出现“信息孤岛”现象。

垃圾邮件引诱用户打开十种标题最具欺骗性

日前，反垃圾邮件专业机构 FRontBRIdge 确定了十种最具欺骗性的电子邮件标题，垃圾邮件制造者会利用这些标题引诱用户打开他们的邮件。这十种标题是 FRontBRIdge 从 1200 个企业邮箱域名中过滤分析出来的。FRontBRIdge 预计会有更多带有这种欺骗性标题的邮件出现，并报告说今年上半年欺骗性垃圾邮

件的数量上涨了 50%。

美反垃圾邮件:垃圾邮件制造者与 ISP 开拉锯战

笔者本人每天要收到 30 封左右的垃圾邮件。内容都是些号称“能赚大钱”、“减少欠款”等字眼儿的金融商品、求职和跳槽信息，以及解除性生活与肥胖困扰的药物等等。这些邮件来自世界各地。由于笔者申请了个人.com 域名，作为管理者，笔者的个人信息与邮件地址被用英语公开。垃圾邮件正是利用了这些信息。

对于个人来说，每天只收到 30 封左右，还不足以对工作造成大的影响。但目前在美国这一问题却变得日益严重了。比如，根据美国 Network Associates 公布的调查结果，目前美国有半数网络用户每周要花费至少 40 分钟时间用于删除垃圾邮件。还有一项调查结果显示，“垃圾邮件给美国企业造成的损失相当于每名雇员 874 美元”。

美国目前正加紧制订垃圾邮件对策，已经筛选了各种各样的应对方案。原本势不两立的各大竞争对手们也携起手来，开展声势浩大的反垃圾邮件运动。但目前他们似乎还难以扭成一股绳，技术课题也堆积如山。下面我们就来看一看美国反垃圾邮件的现状。

垃圾邮件制造者与 ISP 展开拉锯战

今年 4 月份出现了一条令人吃惊的消息：“美国在线（AmeRIca Online）开始起诉总计发送 10 亿封以上垃圾邮件的企业和个人”。美国在线服务的客户端软件，有一个向服务中心报告垃圾邮件的按键“Report Spam”，该公司通过这一按键收到会员的投诉达 800 万起。

对于垃圾邮件发送者一方（垃圾邮件制造者）来说，要想发送必须有邮件地址，因此他们就采用名为“词典攻击”的随机地址生成方法。通过运行软件将字母依次组合起来形成地址。在这种情况下肯定会出现大量实际并不存在的地址，但他们对此并不在乎。只要其中有百分之几的地址实际存在，能顺利将邮件发送过去就行了。他们无视对 ISP 的损害，而发送出大量的邮件。

大型 ISP 试图通过服务器来阻止这些行为，美国《纽约时报》网络版曾刊登过这方面的情况。文章表示，ISP 对词典攻击活动要提前察觉到，在开始向实际存在的邮件地址发送邮件之前就进行阻断。为此，ISP 准备了大量实际并不存在的虚假邮件地址，由于这些地址并不存在用户，所以邮件也不可能发送过去。但实际上却进行了大量发送活动。这就成了垃圾

邮件的证据。

ISP 对这些邮件的内容进行分析，从中找出某种共通的东西，并以此为基础制作“过滤器”，以排除送给有真正用户邮件地址的类似邮件。

但垃圾邮件制造者也想出了巧妙对策。如在每个邮件上随机加上几个文字，（对个人电脑来说）就不再被视为大批量相同内容邮件了。此外，针对 ISP 过滤器排除含有关键字的邮件，垃圾邮件制造者在文字间加入数字或符号来进行回避，如“V1agRa”、“dOMain”、“Money”等。

对于这些非常规的拼写方法，ISP 也采取措施让过滤软件做出反应，但需要每天都及时更新过滤器。在前面提到的《纽约时报》刊登的文章中，美国在线公司技术总管 ChaRLes StILes 说：“过滤器在今天有效，到明天就 不能再用了。因此，我们要时刻不停地进行更新”。

三巨头构筑合作体制，其他业者冷眼旁观

针对这种情况，经营 ISP 业务的美国微软、美国雅虎、美国在线三公司，在反垃圾邮件问题上建立了协作体制。三公司与业界其他团体合作，推动制订技术标准与行动指南。如禁止利用 ISP 的邮件服务器发送垃圾邮件、对来自可能会进行非法中继的服务器的

邮件进行限制、采用行动强化法律限制。另外还制定商用宣传邮件规范，研究如何通过技术手段将其与垃圾邮件区分开来。

尽管上述三公司在反垃圾邮件问题上采取了积极行动，但同样致力于这一问题的其他企业和团体却对此冷眼旁观。究其原因，目前正在蔓延的垃圾邮件大部分是通过这 3 家 ISP 的邮件服务器发送的。特别是微软更成了人们批评的焦点。例如，在加入微软因特网服务“MSN”后的 2 个月内，可以免费使用邮件服务器。垃圾邮件制造者利用盗用的信用卡号码加入 MSN，发送垃圾邮件。当开始对卡扣钱，发现是盗用的号码时，这个帐户已经不再使用了。据说这种现象非常普遍。

“微软处在最显眼位置，经常谈论他们的高难技术如何受欢迎。但很早以前，他们的服务系统就成了垃圾邮件的温床，微软应当对此做出反省”这就是他们想要说的。

在采取法律限制方面问题堆积如山

在采取法律限制方面似乎有了进展。如进入本月后，加利福尼亚州议会在众议院委员会上通过了对垃圾邮件进行罚款的法案。美国国会及加州以外的其他各州也开始讨论有关垃圾邮件的法案。其中多数是对

垃圾邮件制造者处以高额罚款，在美国似乎总觉得，如果离开经济手段就不能减少垃圾邮件。

另一方面，还存在如何找到垃圾邮件制造者的技术性问题，以及是否对 ISP 也处以罚款的责任范围问题。而且如何界定垃圾邮件也不明确。围绕法律限制问题，仍存在着大量课题。

提起“垃圾邮件的定义”，即便是完全相同的邮件，既可以当作垃圾邮件，也可以不是。在前面提到的文章中就有这么一段：

去年 11 月，针对许多用户抱怨美国大型服装公司 Gap 向美国在线会员发送宣传邮件，美国在线发出了阻断发送的警告。但 Gap 公司对此却主张“我公司的邮件全都是用户已经同意‘接受’的，所以不是垃圾邮件”。美国在线公司经过调查发现，Gap 公司提出了“输入自己邮件地址的人购买商品时打九折”这一优惠条件。这样在 Gap 公司收集的邮件地址中，有约三分之一不是本人的，而是胡乱编造的地址。但胡乱编造的地址中却有许多是实际存在的。一部分发给编造地址的邮件就变成了垃圾邮件。

笔者个人的对策

最后谈一谈笔者是如何应付垃圾邮件的。答案也非常简单。笔者采用的是具有自动判断与甄别功能的

邮件软件。软件的使用方法很简单，在最初开始使用的一段时间里，将收到的垃圾邮件归类为“垃圾邮件”，软件的语言过滤器就开始分析这类邮件的性质。在进行一定程度的分析后切换到自动模式。以后收到的邮件就能自动甄别了，由垃圾邮件过滤器进行区分。由于区分的精度相当高，所以作为客户端的自卫手段也非常有效。

前天在网上发现使用同一软件的某人发表的评论。这个人的来信名单中有一个讨厌的家伙，投稿数量很多，而且都用同样的开头。于是他将这种稿件作为垃圾邮件来让软件学习。随后就能准确进行区分了。没想到客户端软件还能有这样的应用。

仔细想来，在“找上门来的推销活动惹人烦”这一点上，垃圾邮件与 DM 及推销电话等是一样的。只是在后一类情况下，发送者要花邮寄费和电话费等，在某种程度上可以说比较公平。他们需要根据邮寄物品的数量或电话通话时间、以及与对方的距离来支付相应的费用。因此，有必要摸索出一套更有效的方法。为了避免无谓的浪费，需要想方设法让对方产生好感。但垃圾邮件的发送费用却不会随着件数和距离的增加而增长。相对于邮件质量，他们更看重邮件的数量，而且这样对他们也不会有什么损失。

考虑到这些，我们不由得为目前正迅速普及的 IP 电话是否也会充斥骚扰电话而担心。IP 电话不仅便宜，对电话号码进行词典攻击也比邮件地址更简单。还可以通过自动录音进行推销。要是每天不分昼夜都有来自全世界的大量“骚扰呼叫”，这将如何是好？这下子可就真的无法工作了。

电脑病毒侵扰多防范意识要提高

一份对国内上半年的电脑病毒发作情况的统计报告显示，上半年平均每个用户遭遇的病毒数量为 2．11 个，“红色结束符”等 12 个病毒是目前国内计算机用户的主要威胁。

据统计，有 82％的电脑病毒灾害是由近一两年出现的新病毒及其变种造成的。同时随着网络的普及，病毒传播速度和广度都迅速提高，“在线杀毒”用户反馈显示，上半年平均每个用户遭遇的病毒数量为 2．11 个。

2003 年上半年破坏范围最广的 12 个病毒排行如下：1．红色结束符、2．爱情后门、3．FUNLOVE、4．未知邮件病毒、5．尼姆达、6．求职信、7．CIH、8．WYX、9．劳拉、10．硬盘杀手、11．垃圾桶、12．巨无霸。

自 2002 年以来，通过网络漏洞和邮件系统进行传播的蠕虫病毒就开始成为新宠，数量上已经远远超

过了系统病毒。在上述 12 种危害最大的病毒中，有一半以上是蠕虫病毒。

与此同时，病毒特性越来越呈现出蠕虫与其他种类混合的趋势。

电子邮件无疑是目前最主要的信息沟通方式之一，这导致了邮件病毒迅速增长，蠕虫病毒、木马病毒、恶意程序等病毒纷纷利用该平台进行传播。特别是未知种类的邮件病毒，在数量上以 5．8％的比例位居第四。专家提醒用户：不要打开陌生的邮件、给系统打补丁是最好的防范措施。

信息安全专家认为，从 2003 年上半年病毒发作情况来看，用户需要做的不仅仅是安装合格的反病毒产品，更重要的是要提高自身的防范意识。对于个人用户，其实操作并不复杂，首先是及时升级杀毒软件，其次是在使用计算机时打开必要的监控系统，如内存监控和邮件监控。

KDDI:每月手机垃圾邮件的咨询数量突破了 5 万

KDDI 从 7 月 15 日开始强化手机服务“au ”的反垃圾邮件措施。该公司将新成立主管反垃圾邮件的部门，并开设受理有关垃圾邮件的投诉电话和电子邮件。

在 au 服务中，用户对垃圾邮件的咨询急剧增加。

4月份约为1万8000件,5月份急剧增加到约4万6000件。6月份突破了5万件。其中多数垃圾邮件来自au手机之间收发的“C Mail”。4月份收到咨询的80%、5月份和6月份收到咨询的95%均与C Mail相关。

如果用户收到的垃圾邮件申诉数超过一定数量（该数量不予公开），KDDI将通过电子邮件向发信人发出警告。如果仍然不停止发送垃圾邮件则将采取最长停机6个月的措施。KDDI一直都在采取同样的措施，此次为了尽快发现垃圾邮件的发信人进一步强化了这一措施。

黑客疯狂攻击安全事故大幅上升

ChinaByte7月16日消息 互联网安全系统（ISS）公司曾警告说，使用已知安全缺陷的黑客正在“疯狂地攻击”企业，远程攻击将使情况变得更糟糕。在其下半年的《互联网风险影响摘要报告》中，ISS预测说。黑客的目标将瞄准使用宽带连接在家办公的人员以及使用无线技术、文件共享和消息应用程序的人员。

尽管FTP、HTTP仍然排在10大攻击目标中，但在过去的一年半的时间中，对这些端口的攻击已经分别下降了46%和96%，这可能与安全缺陷的修正和对FTP、HTTP端口进行了更好的保护有关。

ISS 在报告中指出，截止今年第二季度，严重互联网安全事故数量增长了 13.7%。据 ISS 称，安全事故的增长是由黑客使用了被广泛宣传、但没有被 IT 部门修正的、过时的技术和安全缺陷造成的。ISS 公司的发言人克里斯说，安全事故的增加给不能及时修正系统中安全缺陷的公司带来了很大麻烦。大多数公司必须解决的问题是，在其内部发现和修正最危急的缺陷。由于黑客总是攻击保护措施不得力和新的系统，因此作为一个长期目标，企业需要将系统中的安全数量减少到最低限度。

ISP 正忙于修补 CIsco 路由故障

互联网服务供应商（ISP）因 CIsco 路由器中存在的漏洞而处于易受攻击的状况中。CIsco 路由器的安全隐患可能造成一些 Web 网站和服务器无法访问。尽管故障的详细情形还不清楚，但显然这个故障波及广泛，影响到大型 ISP 公司的许多网络基础架构。CNET 新闻网周三对此进行了报道。

CIsco 公司没有立刻对上述消息发表评论，但电信服务供应商 SpRInt 公司证实 CIsco 路由器确实存在问题。SpRInt 公司发言人称，SpRInt 公司的互联网主干网络正在进行调整，客户无需担心服务中断。CIsco 路由的可能被攻击者利用使得路由器崩溃。网

络管理人员为此不得不重新启动路由器恢复服务。

SpRInt 公司预计在周四上午可以更新它的网络硬件设备。

其他的一些 ISP 商，包括 LeveL3 和 AT&amp；T 等，没有马上对上述消息做出评论。不过有消息称这些公司也在升级它们的网络设备。

视窗系统都有重大缺陷 Server2003 未能幸免

新浪科技讯美国时间 7 月 16 日消息，微软公司周三承认几乎所有视窗操作系统软件当中都存在一个关键性的缺陷，而且这一缺陷还将是首个对其最新款 Windows Server2003 软件产生影响的缺陷。微软表示，上述缺陷有可能导致黑客在互联网上控制使用视窗系统的计算机，窃取数据、删除文件或是入侵电子邮件系统。微软为此敦促其用户立即登录微软的网站下载并安装一个免费的补丁程序。

这次承认上述缺陷对于微软而言尤其令其尴尬不已，因为就连微软最新的 Windows Server2003 软件也未逃过这一劫，而微软曾号称 Windows Server2003 软件是其有史以来最安全的产品。Windows Server2003 软件瞄准的是大型企业用户，而且是去年微软董事会主席比尔-盖茨大张旗鼓宣布“产品安全计划”后公司推出的最具影响力的软件。

上述缺陷是被波兰西部的研究人员发现的，它还会对家用电脑上安装的视窗操作系统产生影响。一位分析人士表示："这是迄今为止最严重的视窗缺陷之一。"微软表示企业的防火墙通常可以阻止企业外部的黑客获得发动攻击时所需的数据连接途径，但上述缺陷却使得用于在计算机网络当中共享数据文件的视窗技术遭到破坏。上述分析人士称，在一些安全保障并不非常有效的企业网络当中，除非企业立即安装补丁程序，否则任何人都可以轻而易举地出入企业的服务器系统。

微软发 Windows 安全补丁 波兰黑客帮忙堵漏

微软再次发行补丁，该漏洞可使黑客控制运行任何 Windows 版本（除 Windows ME 以外）的计算机。是一个波兰黑客组织兼独立安全咨询集团发现了该漏洞并与微软共同修补了该漏洞。

该集团在刊登在网站上的报告中称："该漏洞非常危险，用户必须马上采用微软所提供的补丁。"该集团称，专门利用该漏洞的程序将很快出现在互联网上。

该漏洞存在于可使其它计算机要求Windows系统执行活动或服务的操作系统元件中。该元件通常被称

为远程过程调用（RPC）处理，可帮助文件共享或使其它计算机使用同一台 PC 上打印机的活动。

黑客通过向 RPC 处理发送过多的数据从而可导致系统同意可完全访问该系统。

微软在其报告中表示：“这将使黑客在他们所希望的服务器上进行任何活动，例如，黑客可以改变 Web 页面，重新格式硬盘或向本地管理程序添加新用户等。”

欧盟采取共同措施打击“垃圾电子邮件”

本报布鲁塞尔 7 月 16 日电欧盟委员会 7 月 15 日要求成员国采取共同措施，打击“不请自来的商业电子邮件”，同时呼吁国际社会，“同这种日益猖獗的现象做斗争”。

欧盟委员会负责信息事务的委员利卡宁在 15 日举行的新闻发布会上指出：“抵制垃圾

邮件已经成为涉及我们每一个人的问题。”他要求各成员国最晚于今年 10 月底拿出禁止“垃圾邮件”法律的实施举措，对“侵犯私人生活”而受到的处罚细节做出具体规定。他说，受害者可以向垃圾邮件来源国主管信息安全的部门投诉。

欧盟将采取的措施包括，从源头上禁止一切未经接收者允许的垃圾邮件向外发送，以及在接到投诉后

对发送者进行“严惩”。欧盟希望明年 1 月在布鲁塞尔以“经济合作与发展组织”的名义召开有关国际会议，并要求今年 12 月中旬在日内瓦举行的“信息社会世界首脑会议”上将“加强国际合作，共同清除网上垃圾”提上议事日程。

据统计，目前在国际互联网上流通的电子邮件中，垃圾邮件占了将近一半的比例。2002 年，清理垃圾邮件给欧盟企业造成的损失约达 25 亿欧元。

欧盟已于 2002 年 7 月颁布了一项法令，在欧盟范围内禁止向个人发送垃圾邮件。鉴于许多邮件来自欧盟以外地区，欧盟认为，加强国际合作才能有效地制止垃圾邮件。

调查显示无用电子邮件使企业每年损失数百万

对高级员工进行的一项新调查显示，英国企业在无用的电子邮件上花费了大量的时间和资金。

这一问题与垃圾邮件无关，办公室员工更喜欢向同事发送电子邮件，而不愿意走到同事的办公桌前与他们进行语言交流。EmphasIs 公司通过调查发现，这种现象每年使企业损失数百万美元。它对英国最大企业进行的调查显示，它们每年平均用在每个员工身上读、写不必要的垃圾邮件上的开支为数万美元，但大多数公司目前都没有采取必要的措施来提高电子邮

件的效率。

EmphasIs 公司的高级顾问罗伯特?阿斯顿说，电子邮件的直观性是一把双刃剑，它使人们进行大量无用的通讯成为可能，在开始“真正的工作”之前，人们通常必须选处理 30-40 封电子邮件。

EmphasIs 公司的调查显示，太多的通讯对象以及复制的滥用并非电子邮件给企业造成沉重负担的唯一方式，许多人发出的电子邮件都晦涩难懂，20%的电子邮件被认为书写有问题，不好理解。

尽管人们通常能够对拼写错误和语法错误持宽容的态度，但他们却不能容忍在电子邮件中闲聊。阿斯顿表示，用三个词就能够表达清楚自己的意思，但许多人却使用了十个词。他们忘记了，电子邮件与在电话上说话一样是不能修改或收回去的。

除了浪费时间外，利用电子邮件中伤同事也是十分常见的，越来越多的人使用电子邮件来获得相对于同事的竞争优势。

欧盟今年 10 月底开始执行全面禁止垃圾邮件法

欧盟各国近日通过了一项决议，决议规定从今年 10 月底开始，欧盟各成员国将执行统一的反垃圾电子邮件法律。据参加会议的欧盟代表称，垃圾邮件已成

为一种社会公害，目前垃圾邮件已经占到互联网电邮总数的一半以上。此外，欧盟正在同美国和日本等国加紧协商，力争在全球范围内构筑防范垃圾邮件的网络。

分析人士说，虽然已有一些国家制定了反垃圾邮件法规，但是欧盟的全面禁止垃圾邮件法在世界上还是首次。该法律名为《关于通讯的指令》，欧盟所有成员国已同意了这项法令。法律的基本内容是：在发送广告等电子邮件时，必须得到接收方事先同意；如果违反了此项规定，应当由成员国制定的相关法律予以惩罚。

欧盟代表称，垃圾电子邮件近年来一直在不断地增长。2001 年垃圾邮件仅占电邮总量的 7%，到 2002 年即达到 29%，今年则超过了 51%。垃圾邮件的发送成本已经超过了 25 亿欧元。关于垃圾邮件分类，据欧盟今年 6 月统计，在垃圾邮件中，一般商品广告占 37%、色情广告消息占 24%、金融服务广告占 12%。

欧盟计划明年在日内瓦召有关信息技术的专门会议，会议将提出在国际范围内反垃圾邮件的问题。

网上出现黑客代码 目标锁定思科路由器漏洞

公共邮件列表中已经贴出了能够用来攻击和破坏思科路由器的代码。

7 月 18 日上午在“大曝光”(FuLL-DIscLosure)安全邮件列表中贴出的代码能够用来导致许多网络连接到互联网的思科路由器硬件瘫痪。赛门铁克和互联网安全系统这两家安全公司已经提高了思科路由器漏洞对接入互联网的企业可能造成的威胁等级。

赛门铁克安全反应小组高级工程经理 AL HugeR 表示，令人担心的问题是，有人将使这种攻击自动化，使用这种代码对没有升级路由器人们进行大规模拒绝服务攻击。我无意充当报警者。但是，我认为，这种担心是合理的。

赛门铁克 7 月 18 日把这个威胁等级从 2 级提高到 3 级。HugeR 表示，在过去两年里，在 5 级威胁等级里出现 3 级威胁等级的次数很少。SLammeR 蠕虫、红色代码和熊熊虫病毒都被定为 3 级威胁。

赛门铁克的入侵探测系统已经检测到利用这个实施攻击的轻微的行动。但是，能够引起人们担心的攻击事件还没有发现。

思科更新了，提醒用户这个已经公开发布了，但是，思科并不认为黑客正在利用这个。思科发言人 JIm BRady 称，我们没有证实任何受到了影响，我们没有接到任何网络遭到成功的攻击的报告。

然而，这个使安全专家不断提出吓唬人的警告，

是因为思科路由器占企业网络硬件的 80%，占互联网硬件的 90%。应用这样广泛的硬件如果遭到攻击将会造成网络大面积中断。

不过，安全公司似乎并不认为肯定不会出现问题。虽然网络服务提供商都忙着修复思科路由器漏洞，但是，现在还不清楚企业和网络零售商能够用多快的速度修复他们的网络。

互联网安全系统公司也把思科路由器漏洞的安全威胁提高到了 3 级。赛门铁克和互联网安全系统公司都是在思科路由器漏洞和微软 Windows 公开的前一天把威胁等级从 2 级提高到 3 级的。

CIsco IOS 漏洞工具亮相 管理员需要尽快应对

美国 CERT/CC 于当地时间 7 月 18 日宣布，一种针对前不久公布的 CIsco IOS 的工具（ExpLoIt）目前已在互联网上公开。ExpLoIt 可用于检测漏洞，同时也容易被人恶意使用。目前，运行以路由器为主的 IOS 的网络设备的管理员，应根据美国思科系统公布的信息尽快采取措施。

在思科路由器和交换机的专用 OS??CIsco IOS 中，日前发现了一个漏洞，如果接收到特定的数据包，设备就有可能停止运行。IOS11.x 以上版本几乎均受影响。漏洞被恶意使用后即便停止运行，网络设备也

不会发出警告或自动重新起动。考虑到思科生产的网络设备的市场份额，可以说是一种非常严重的漏洞。

漏洞公开时，曾有人担心是否存在 ExpLoIt，目前已证实这样的工具已经亮相并在网上公开。笔者就是通过某个有关安全的邮件列表，查找到保存有 ExpLoIt 站点的 URL 的。因此，极有可能产生一种通过互联网上脆弱的公开服务器、对网络设备实施攻击的、恶意使用 ExpLoIt 的蠕虫等病毒。CERT/CC 强烈建议根据思科公开的信息尽快采取对策。

思科已于美国当地时间 7 月 17 日公布了相关信息“RevIsIon1.0”，目前也追加了最新信息。比如，明示了会受到漏洞影响的协议，追加了有关 ACL 的信息等。与 CERT/CC 公布的信息一样，思科也追加了 ExpLoIt 已经公开的信息。强烈建议管理员再次进行确认。

亚洲地区最大的反垃圾邮件会议将在釜山召开

由 APCAUCE（www.apcauce.org）主持召开的亚洲最大的反垃圾邮件会议将在韩国的釜山召开。APCAUCE 是亚洲最大的反垃圾邮件组织之一，这次会议还联合了一些知名的亚洲电子邮件发行商参与。亚洲电子邮件经营商之一〃现在网〃成为其主要赞助

商。

亚洲国家由于其电子邮件的运做机制，和一些ISP提供商对客户的过于宽泛，很多ISP们被认为是“窝藏”垃圾邮件经营者的港湾，已经被世界多个反垃圾邮件组织列入黑名单。一些合法的专业EMail营销服务商因此受到影响，不得不奋起自救，这也是在亚洲经营7年EMail营销服务的“现在网”赞助这次会议的原因之一。

〃APCAUCE的八月会议将集结亚洲各国的本领域专业人士，群策群力，针对目前关于EMail的通讯和网络基础构造进行讨论，找出对策。〃现在网的首席执行官Danny LevInson先生说。“会议有分别来自中国互联网协会（ISC）、韩国、新加坡、日本以及其他国家的代表。这将是一个来自不同国家和组织的共同对抗垃圾邮件的令人鼓舞的时刻，能作为赞助商，能够参与这一历史性的时间，这是我们的荣幸。”

另外，来自美国和欧洲的一些专业人事也将在会上发言，来自美国的Anne P。MItcheLL女士从事互联网及其法律研究和实践已经有15年了，在加入著名反垃圾邮件组织Habeas并成为其CEO之前，MItcheLL女士曾是美国反垃圾邮件服务的先锋组织MAPS（Mail Abuse PReventIon System）的公共事务

主管。同时来自英国赫尔大学的 BRaIn Tompsett 先生也将出席会议并发言，他在 1989-1992 年期间为英国互联网协会（The UK Internet consortlum）工作，担任理事。

微软再发警告 DIRectX 发现极为严重

对一些再次发出了一些警告，其中包括一个对大多数 Windows 电脑都有影响的“严重”漏洞。最严重的涉及到大多数电脑游戏使用的一种图形和多媒体编程指令库 DIRectX。这种漏洞能够让恶意用户随意在有这种漏洞的计算机上运行恶意代码。

据微软的称，这个影响面非常广，从 DIRectX5.2 版到目前的 9.0 版

都受到了影响。DIRectX 可以在 Windows 98 到 Windows Server2003 等各种版本的 Windows 操作系统上运行。

微软给这个评定了最严重的等级。这个涉及到 DIRectX 处理 MIDI 音乐文件的方式。变形的 MIDI 音乐文件可能造成 DIRectX 程序中的缓存溢出，这样嵌入在这个文件中的其它程序就可能被执行。

利用这个可以制作一个恶意的变形的 MIDI 文件。有这种的 Windows 计算机用户可能通过电子邮件或者网页受骗，执行这个恶意文件。微软安全反应中心的

Stephen TouLouse 表示，目前各种版本的 OutLook 电子邮件软件和 IE 浏览器软件的缺省设置都不能阻止运行这个程序。

TouLouse 表示，这个是由 eEye DIgItaL 安全公司发现的。虽然现在还没有发现有人利用这个，但是，受影响的 Windows 用户应该尽快采用补丁程序。

此外，微软还发布了修复以前宣布的 SQL 服务器软件的补丁。这个漏洞的等级是“重要”。

微软发布的第三个补丁是修复可能对运行 Windows NT4.0 操作系统的计算机实施拒绝服务攻击的一个。这个的等级是“中等”。

Windows 的音乐软件中存在危急的安全缺陷

当地时间本周四，微软公司表示，它已经发布了一款修正Windows中一个被新发现的危急安全缺陷的补丁软件，该缺陷能够使黑客控制用户的计算机或在用户的计算机上运行恶意代码。

如果被利用了，该缺陷能够使黑客删除文件、查找记录、发送电子邮件，甚至是从被控制的计算机上发动新的攻击。

微软公司安全响应中心的安全经理斯蒂芬表示，问题出在 DIRectX 中处理 MIDI 文件的技术上。黑客可以编写一个旨在利用该缺陷的 MIDI 文件，并通过

电子邮件、把它托管在互联网网站或放在共享网络上进行传播。通过打开或预览电子邮件，恶意代码就可以自动运行，除非用户运行较新版本的 OutLook 或已经下载并安装了 OutLook E-Mail Security Update 软件。

TRuSecuRe 公司的库珀说，这种攻击能够绕开反病毒软件和电子邮件网关。他指出，黑客只要发动攻击，一般情况下总能得手，因为这种文件被认为是安全的。

微软公司表示，除了 Windows Server2003 外，所有版本的 Windows 中的这一缺陷都是“危急的”，但目前还没有获得利用该缺陷发动攻击的报告。

《纽约时报》计算全球垃圾邮件消耗的总费用

垃圾邮件现在已成为互联网上一大祸害，由于发送垃圾邮件的费用低廉，每封垃圾邮件的成本仅为 0.025 美分，所以大量的垃圾邮件开始充斥互联网，不仅堵塞网络而且还导致互联网服务提供商耗费更多的资源来处理这些邮件，再加上过滤垃圾邮件、抓获垃圾邮件发送者的成本以及弥补垃圾邮件给企业和个人用户带来损失的费用，垃圾邮件消耗的总费用自然就达到了天文数字。

FeRRIs 研究公司的数据显示，今年全美因为垃圾

邮件泛滥而消耗的总费用大约为 110 亿美元，该公司估计全球范围内垃圾邮件消耗的总费用更是高达 205 亿美元。NucLeus 研究公司的数据更高，其估计对于全美每个拥有电子邮箱的办公室员工而言，每年因为垃圾邮件而损失的费用为 874 美元，这一数字乘以 1 亿名员工，全美一年因垃圾邮件遭受的损失就高达 870 亿美元。

NucLeus 公司的研究主管维特曼表示："垃圾邮件是对生产力产生严重打击的因素之一，每天每位员工平均都收到 13.3 封垃圾邮件，这些邮件需要花费 6.5 分钟来处理，这意味着员工 1.4%的效益时间都被无端占用了。"一位用户表示，他每天收到的电子邮件当中有 60%都是垃圾邮件，因此每天一上班第一件事情就是删除电子邮箱里的垃圾邮件，这让他感到很是无可奈何。

我国八成以上计算机遭病毒攻击并呈上升趋势

对于网络系统的安全来说，网络病毒的危害丝毫不亚于非典病毒对人类的影响。最新统计表明，在 2003 年的上半年，我国计算机病毒感染率约有85%，并呈现出继续上升趋势。

在 29 日举办的 2003 中国网络病毒技术发展

趋势及对策高级论坛上，国家计算机病毒应急处理中心副主任张健介绍，从国家计算机病毒应急处理中心日常监测结果看来，计算机病毒呈现出异常活跃的态势。在2001年，我国有73%的计算机曾感染病毒，到了2002年，这个数字上升到近84%，2003上半年又增加到85%。

据了解，当前的网络入侵主要来自于蠕虫病毒，这些隐藏在网络上的“杀手”，正呈现出功能强，传播速度快，破坏性大等新特点。不仅可以感染可执行文件，通过电子邮件、局域网和聊天软件等多种途径进行传播，同时还兼有黑客后门功能，能进行密码猜测，实施远程控制，并且终止反病毒软件和防火墙的运行。

2003年的1月25日，仅在SQL1434病毒出现的当天，我国就有80%的网络服务供应商先后遭受此蠕虫病毒的攻击，造成许多网络的暂时瘫痪。网络病毒的危害由此可见一斑，然而这还不是惟一的一次。“国内像这样的重大病毒事件，到2003年7月，国家计算机病毒应急处理中心已处理了15次之多。”张健介绍说。

针对目前网络病毒传播和破坏方式的多样化，公安部公共信息网络安全监察局副局长袁旭阳表示，从

今年开始，我国地市级以上城市都将逐步建立信息网络安全报警处置系统。

专家们指出，对于防范病毒不能“坐诊”，而要加强网络的主动控制能力。在开发应用网络主动预警系统，提高发现干预能力的同时，还要加强计算机安全培训，提高用户的安全防范意识和病毒防治技术。

OIS 举行专题讨论 制定新的披露指南

ChinaByte7 月 31 日消息 互联网安全组织(OIS)在拉斯维加斯举行的“BLack Hat BRIefIngs”安全大会上举行了一次专题讨论会，就有关制定安全研究人员向软件厂商报告的标准方法回答了一些问题。目前，安全研究人员处理漏洞信息采用了各种不同的方法。有些人立即就在互联网上公布这个信息，有些人则与软件厂商合作解决这个漏洞问题。

OIS 希望研究人员至少给软件公司 30 天的时间制作的补丁，然后再公开这个漏洞。微软安全计划经理、OIS 成员 Scott CuLp 强调说，给予更长的时间并不意味着软件公司不重视安全。这些公布的指南并没有使我们放松，而是增加了对我们的压力。

OIS在7月29日发布的指南要求安全研究人员给予软件公司 30 天的时间制作补丁，然后再公布的细节。

这样宽松的时间是安全团体一个有争议的让步。在过去 10 年里，安全研究人员一直在与保持沉默的软件厂商打交道。软件厂商承认和解决问题的拖延导致了所谓的公开披露运动，许多安全研究人员都加入了这个运动。在公开披露的原则下，只要一发现就立即公开披露。

OIS 成员、原来漏洞披露指南的编写者 WysopaL 表示，在过去的 7 年里，环境已经发生了变化。我们意识到过早地公开披露代码是有害无益的。他说，如果将来软件公司仍拖延修复漏洞，改变当前的环境，我们就需要对现在的文件进行修改。

有些成员担心，禁止立即公开的信息会使某些安全公司受益。例如，互联网安全系统公司等安全公司可以向客户出售有关的早期信息。能够早期接触到这种信息的计算机应急反应小组协调中心也可以这样做。

OIS 对这类问题没有制定出政策，因为意见不统一。但是，WysopaL 表示，这个披露指南还是瑕不掩瑜的，好处还是很多。

商业安全岌岌可危 APEC 全力打击互联网犯罪

“致力于打击计算机犯罪的国家必须联合起来，

利用法律条文来进行有效的管理。”APEC 代表于上周五在泰国曼谷举行的 APEC 安全任务小组会议上发表此番言论。APEC 希望全面而多方位地完善我们现有的法律结构，打击计算机犯罪，同时建立法律强制机构调查研究计算机犯罪行为。

互联网的广泛使用为计算机犯罪分子提供了更多的犯罪机会。

APEC 代表强调“计算机犯罪不分国界，不管你是什么法律和经济体制都不能幸免。只有国家之间的强强联手，才能打击犯罪，根本保护大家在这个互联世界里的个人利益和商业机密。所以，解决问题的关键是各个经济体制国家通力合作，共同实施打击政策，彻底地将计算机犯罪分子绳之以法。”

所有的 APEC 经济组织成员一致通过以下这些决议，以推进和完善法律和经济结构：

严格管理计算机系统的访问权限，杜绝因权限泄露而造成的非法入侵。

允许法律执行部门对电子证物的收集取证

允许各经济团体之间联合调查起诉计算机犯罪分子

在计算机犯罪越来越猖狂的今天，APEC 急需一群专业人士来打击这伙犯罪分子，维护各大经济团体间

的正常运作。

计算机犯罪分子会隐藏在每一台计算机终端，他们有可能攻击抽奖程序系统，也可能伪装在银行网络中，又或在拍卖网络中捣鬼。并且，这些犯罪分子是通过移动电话上网，很难寻觅踪影。

近日，澳大利亚权威人士提醒使用抽奖程序的用户注意，犯罪分子可能通过短信服务的文本信息来实施犯罪，应当警觉！

计算机病毒十大新特点 专家提出5项防范措施

7月29日，在2003年中国网络病毒技术发展趋势及对策高级论坛上，国家计算机病毒应急处理中心张健博士针对近期出现的计算机病毒，分析并总结概括其十大新特点，即传播方式和途径多样化，病毒欺骗性增强，计算机病毒破坏方式更加多样化，传播速度极快，制作成本降低，病毒变种增多，难于控制、难于根治，病毒传播的不确定性和跳跃性，计算机病毒具有版本自动在线升级和自我保护能力，病毒编制采用了集成方式。

为此，张博士提出了防范计算机病毒的五项措施：需要强有力的依法治毒措施；建立一套行之有效的病毒预警系统；下大力量研究网络的主动控制技

术，提高管理和控制能力；进一步加强计算机安全培训，提高全体网民安全防范意识和病毒防治技术；加大对制造、传播计算机病毒犯罪行为的打击力度。做到积极预防病毒、及时发现病毒、快速反应消除病毒、确保恢复系统数据和有效打击利用计算机病毒犯罪的行为。

调查显示网络容易“死灰复燃”

据 CNET 美国当地时间 7 月 30 日（北京时间 8 月 1 日）报道 一项针对互联网进行的研究显示，一半左右的容易受到攻击的系统在出现后的 30 天内仍然未对漏洞进行修补。这项研究还显示，一些并不会随着时间的推移而自动消失，相反，它们反而会卷土重来。例如，“代码红色”和“SQL SLammeR”等蠕虫病毒就是利用在互联网上反复出现的。

进行上述研究的 QuaLys 网络评估公司的首席技术官 GeRhaRd EscheLbeck 表示：“由于企业不可避免地会在网络系统中安装一些过时的软件，所以死灰复燃的现象并不新鲜。”

QuaLys 公司是在对诸多网络进行了历时一年半的跟踪之后得出上述结论的。这一研究凸显了用户应该在安装补丁程序方面更加积极主动，同时软件制造商应该在软件研发阶段就尽可能排除的重要性。

研究发现，越严重，企业安装补丁程序的速度就越快，而对那些企业认为严重性不高的，一般安装补丁程序的速度也就较慢，有时甚至超过 60 天还没有安装补丁程序。研究人员称，如果企业在安装补丁程序方面动作太慢，等他们想起来要安装时黑客们发布有关代码来利用这些漏洞兴风作浪的机率可能已经达到了 80%。

研究人员还对软件制造商提出了指责，称在软件研发阶段没有尽可能排除最严重的是导致服务器安全程度不高的主要原因之一。对此，甲骨文公司的首席安全官 MaRy Ann DavIdson 表示，甲骨文一向在采购软件系统时对安全性非常重视，但其他一些公司却在这一问题上不够谨慎。她说："软件企业如果注重自己的声誉就应该象对待自己公司的网络一样对待提供给客户的软件，尤其是在安全性方面应该格外小心。"

专业机构称 Windows 漏洞不断 系统依然脆弱

Windows 中可能存在的一直备受人们关注，现在，美国计算机应急反应小组协调中心(CERT／CC)再次发布了类似警告，指出 Windows 系统中依然存在着可以被黑客利用的漏洞。该中心互联网安全分析师杰夫

-哈夫利拉称：“我们不断收到网站被黑的报告，而这些用户的系统都是已经安装微软安全补丁的。”

曾于 7 月 16 日公布的一个 Windows 漏洞与 Windows NT4、Windows2000、Windows XP 和 Windows Server2003 中的远程程序呼叫协议(RPC)有关，该协议的功能是帮助远端计算机运行计算机执行代码。微软的 TechNet 网站上可以下载针对这一漏洞的安全补丁。CERT／CC 还对更新系统遭受拒绝服务攻击的报告进行了跟踪，这一漏洞也与 RPC 有关。哈夫利拉指出：“这种漏洞仅存在于 Windows2000 中，微软称它与 RPC 无关，因此它们的补丁不能解决这一问题”。他还说，微软正在研究一种专门用于 Windows2000 的新补丁。

微软公司的一名发言人证实了哈夫利拉的廉洁，并声称公司方面正就此事进行调查和开发新的补丁，但至于新补丁什么时候到位还不能确定。在微软提供新补丁之前，CERT／CC 建议 Windows2000 用户对系统的 135、139 和 445 端口进行封锁。CERT／CC 称，在对此前发现的 RPC 漏洞进行攻击时黑客们一般使用三种工具，攻击之前总会对 Windows 系统的端口进行扫描，这些工具已经出现了两个星期，很有效，很多黑客都在使用。不过目前还未发现针对这一漏洞的蠕虫

病毒。哈夫利拉说：“我们还没有证据证明相关蠕虫病毒的存在，也就是说目前进行的主要是一些零星攻击，针对的是某个特定的网站。尽管如此，我们还是接到了相当数量的攻击报告。”

美网络安全大会将召开 破解黑客威胁成焦点

美国东部时间8月3日(北京时间8月4日)消息，近日来，微软软件产品的漏洞导致了大量计算机网络被黑客肆意攻击。在此情况下，今年最大规模的网络安全会议将于本周六在美国加斯维加斯郊区召开，届时网络专家、政府机构代表以及 IT 精英都将出席，预计到会人数将达到 5000 人。会上将从理论和实践对黑客的威胁进行讨论，将介绍一些最新的攻击方法，从电话到卫星到冰箱。但在当前形势下，此次会议的最大焦点是如何应对目前真实世界中正在上演的黑客大战。

美国国家安全部网络安全分部主管马克斯—萨克斯(MaRcus Sachs)说，“每隔一年或两年，就会出现大范围的黑客攻击现象，导致众多系统陷于瘫痪，今年的情况更为严重。主要是由于微软公司最近发布的 LqwR 漏洞涉及到多种 WnIdows 产品，而这些产品广泛应用于商业领域中”。黑客专门开发了针对这些漏洞的恶意程序，并且在互联网上广泛传播，使得事

态不断恶化。美国政府顾问警告说，一周之前公布的最新病毒情况已经于本周四再次更新，提醒用户密切注意。

据称，目前至少有 2000 台机器在网络上搜索易受攻击的计算机目标，从这些目标中可能会爆发新一轮的攻击。AtStake 公司安全顾问克里斯一威斯波尔(ChRIs WysopaL)说，“这绝对是近几年来最严重的黑客袭击事件，范围之广前所未有”。另外，萨克斯说，还有一种名为“MIMail”的新型病毒正在传播，这种病毒可以通过系统管理员在电子信箱中快速传递。此次会议的另外一个主题是家庭自动化系统的安全问题。因为某些系统从灯光、咖啡壶到冰箱都是通过计算机网络控制的，很有可能成为新的攻击对象。

电脑病毒日益肆虐 7 个月中国出现 15 次大疫情

渐露凶相的“狼群”

计算机的发明以及随之而来的互联网应用的普及，大大提高了生产力并渗透到社会各个领域，推进了整个人类社会的文明进程。但是，伴随着信息网络的发展，计算机病毒这个 信息时代的“幽灵”也逐渐露出了狰狞的面目。1991 年，全球病毒数量不到 500 种；1998 年，病毒数量不足 1 万种；但到了 2002

年，病毒数量已增至 6 万种。自 2000 年以后，病毒以每年将近 2 万种的数量激增。病毒已不再是黑暗中隐藏的“黑手”，而是渐露凶相的“狼群”。

进入 2003 年，计算机病毒呈现异常活跃的态势。在日前举行的 2003 中国网络病毒技术发展趋势及对策高级论坛上，国家计算机病毒应急处理中心公布了今年我国出现的重大计算机病毒事件的情况：在过去的 7 个月中，我国共出现重大计算机病毒事件 15 次，平均每月超过 2 次。其中 SQL1434 病毒和“口令蠕虫”病毒造成的危害最大。

据国家计算机病毒应急处理中心的张健博士介绍，今年 1 月 25 日，仅在 SQL1434 病毒出现的当天，我国就有 80%的网络服务供应商先后遭受了此蠕虫病毒的攻击，许多用户在上网时明显感到浏览速度减慢，收发邮件时间延长，网络一度瘫痪。在该中心和其他机构的共同努力下，网络才恢复了正常。3 月 8 日，“口令蠕虫”病毒突然袭击我国互联网，国内的教育科研网遭受的破坏最大，很多高校的校园网瘫痪，骨干互联网也出现明显拥塞，个别局域网近于瘫痪。并且，该蠕虫病毒开设后门，还可以导致远程攻击和进一步的破坏。

在这两次大的病毒事件之后，“爱之门”病毒、“老

板公司”病毒、“非典”病毒、木马病毒等相继发作，也造成了不同程度的破坏。根据国家计算机病毒应急处理中心上半年不完全的统计，我国计算机病毒感染率约为 85%，且呈现继续上升的趋势。而这个数字在 2001 年是 73%，在 2002 年是 83%。

网络病毒成主流

为什么计算机病毒的发作越来越频繁，传染的速度越来越快，造成的破坏也越来越严重？专家指出，主要是因为计算机病毒的发展有了新变化。

国家“863”计划反计算机入侵和防病毒研究中心主任严明研究员指出，计算机病毒目前已经开始向纵深发展，随着互联网的广泛应用，像 CIH 这类通过文件进行传播的系统病毒已经退居二线，而作为网络病毒的代表者—蠕虫病毒，一跃成为病毒主流。在流行的恶性病毒中，有 90%以上的病毒是蠕虫病毒。蠕虫被划为一种网络程序，它生存在网络的节点中，依靠网络的漏洞在网上大量繁殖，造成网络阻塞之类的破坏，早期只消耗资源，并不破坏文件。但是，现在的蠕虫开始继承其他病毒的特征，不断地改良自己，像“求职信”病毒运行时，会释放出 FUNLOVE 病毒，而“杀手 13”病毒则会删除计算机硬盘中的所有文件。

严明提醒广大用户，电子商务、电子政务的进一

步发展，会使网络病毒持续以极高的速度增长，尤其是黑客技术与病毒技术融合在一起的混合型病毒会越来越多。病毒的划分因此会很困难，当你看到一个命名为 WORM 的蠕虫病毒时，千万不要单纯地认为此病毒只会阻塞网络，它往往还会感染文件、驻留系统，造成更多的破坏。

张健博士也指出，当前病毒的入侵主要来自于蠕虫病毒，同时病毒呈现综合性的特点，功能越来越强大，既可以感染可执行文件，通过电子邮件、局域网、聊天软件甚至浏览网页等多种途径进行传播，同时还兼有黑客后门功能，进行密码猜测，实施远程控制，并且终止反病毒软件和防火墙的运行。此外，病毒的欺骗性也有所增强，常利用邮件、QQ、手机、信使服务和 BBS 等通讯方式发送含有病毒的网址，以各种吸引人的话题和内容诱骗用户上当，如“爱虫”病毒就使用“ILOVEYOU”作为邮件的主题。

多管齐下综合治理

专家们建议，面对计算机病毒发展的新变化，要多管齐下，进行综合治理。

首先，要建立一套行之有效的病毒预警体系。张健博士认为，根据计算机病毒的特点和多年病毒防治工作的经验来看，从根本上完全杜绝和预防计算机病

毒的产生和发展是不可能的。病毒的种类越来越多，破坏方式日趋多样化，计算机病毒已经突破简单的技术范畴，而成为一种威胁巨大的恐怖活动。因此，建立一种快速、有效的预警机制，成为当今急需解决的问题。目前，病毒应急中心和各防病毒厂家还是处于“坐诊”的局面。计算机用户和网络运营商在遭受攻击后，由于种种原因，往往没有在第一时间与应急部门取得联系，不能快速地判断事件的性质和原因，延误了时间，造成了巨大的损失。

其次，需要强有力的依法治毒措施。我国在 1994 年颁布实施了《中华人民共和国信息系统安全保护条例》，1997 年出台的新《刑法》中增加了有关对制作、传播计算机病毒进行处罚的条款。2000 年 5 月，公安部颁布实施了《计算机病毒防治管理办法》，进一步加强了我国对计算机病毒的预防和控制工作。但是从近两年的病毒侵害事件来看，我们对计算机信息系统和网络的安全监督力度不够，用户的安全防范意识淡漠，防范工作迟滞，整体安全水平不高。这些问题需要通过强有力的依法监督制度来规范和促进。

第三，要加强自主知识产权反病毒技术的研究。严明主任指出，我国的反病毒软件引擎，不少是依赖国外技术装备或反向工程破解技术支撑起来的，这就

潜伏着信息安全的巨大隐患。我们的计算机软件还面临市场垄断和价格歧视的威胁。在国外厂商几乎垄断了我国计算机软件核心市场包括操作系统的情况下，加强具有自主知识产权的反病毒技术的研究十分迫切。

第四，加强计算机安全培训，提高全民的安全防范意识。根据计算机病毒的特点，网络的安全需要全体网络用户的共同保障。我国互联网的用户数量已经达到 6800 万，和去年同期相比增长 48.5%，我国在进入互联网高速发展期的同时，计算机病毒的危害也呈现同步增长趋势。面对如此之大和快速增长的用户数量和频繁突现的病毒侵害事件，我们急需建立一套安全培训机制，提高全民的安全防范意识。

互联网协会将公布垃圾邮件服务器的黑名单

中国互联网协会与中国互联网络信息中心将在北京梅地亚中心举办《中国互联网发展报告》的首发式。

据悉，该报告详细介绍了中国互联网络去年全年的整体发展情况以及未来中国互联网络的发展趋势预测。同时，在报告首发式后，中国互联网协会与中国互联网络信息中心还将公布发送垃圾邮件的服务器黑名单。

来的蠕虫病毒将只攻击特定地区

据 NewsclentIst 网站美国当地时间 8 月 4 日报道,计算机安全方面的权威人士宣称，未来的蠕虫病毒将会设计成为只攻击一个特定国家的网络系统。

周日乔纳森.威格诺在拉斯维加斯举行的“Defcon11”安全研讨会作了有关蠕虫病毒的最新研究报告。威格诺是英国数据与网络安全研究委员会的成员之一，该组织是一个非盈利性的专家小组。

威格诺重点强调了蠕虫病毒制造者为了使病毒更有效地传播所使用的技术。他指出，其中一项技术能够限制蠕虫病毒活动的地理区域。这将会使蠕虫病毒变为信息战中一项非常有效的武器，因为它能够被用来攻击一个特定的国家，而不是随机地攻击与互联网相连接的计算机。

这种蠕虫病毒在感染了主机后，一般会随机地对远端的能够被感染的计算机进行扫描。但是威格诺也提到，该蠕虫病毒能够下载一份网络协议的备份清单。在清单上列有将要被攻击的 IP 地址，通常来自于简易服务器或计算机组。这样将可以避免重复发送请求给每台机器，而这正是现有的蠕虫病毒的传播途径的瓶颈。“这意味着它能够迅速传播。”威格诺对 New SclentIst 的记者说，“而且你可以根据 IP 地址选定

一个特定的国家进行攻击，那么当蠕虫病毒传播之后，该国网络将会陷入瘫痪。”

加利福尼亚大学伯克利分校的计算机科学家尼古拉斯.威沃一直在研究迅速传播的电脑蠕虫病毒。他说，在理论上，这只是蠕虫病毒被用来锁定攻击某一特定国家的一种方式而已，而另外一种方式是阻止计算机运行特定的语言。在 2003 年 7 月被释放的名为“MIgmaf ”的“特洛伊木马 ”程序，就可以使配备俄语键盘的计算机无法操作。但是英国反病毒公司 Sophos 的总工程师格雷姆.克鲁利说，只有特定类型的电脑黑客才会对这种针对特定国家的手段感兴趣。一般的病毒制造者只是一心想让他们的病毒尽可能广的传播。

威沃在接受采访时指出，使用 IP 地址的攻击目标清单将会影响病毒的传播速度。尽管协作扫描是非常有用的，但是它有滞后的命令效应，只有当易受攻击的计算机中有 50%左右被感染后才会出现。他同时也提到，使用攻击目标清单会提高黑客被发觉的危险。虽然对攻击者来说，攻击网络变得更容易，但是也更容易暴露他们的行踪。而依靠单独进行随机攻击的特性，一些蠕虫病毒被证明是非常有效的。2001 年 7 月发作的“红色代码 ”蠕虫毒，就是近年来最成

功的病毒，它就是利用这种方法，感染了成百上千的计算机。在 2003 年 1 月，“SLammeR”蠕虫病毒同样感染了成千上万的互联网服务器，不过它在进行扫描时限制了带宽从而传播的更加迅速。

黑客技术是把双刃剑 网络安全检测显身手

DefCon 大会日前组织了一场年度“夺旗”竞赛??Root Fu，由 8 个小组进行网络攻防战，每个小组必须在保护自己服务器和应用程序正常的情况下破坏其他 7 个小组的服务器。

ImmunIx 首席科学家 CRIspIn Cowan 表示，此类对抗性竞赛可比一般标准更好地检验网络安全性能。

尽管美国政府的高层官员一直认为网络黑客是一种威胁，并制定了数字前年版权法案以及网络安全增强法案等惩罚黑客，但有见识的安全专家们则认为在类似 Root Fu 的竞赛中展示黑客技能是改善安全性能的一个必须途径。

在竞赛中，每个小组必须运行在 UNIX 的一个变体 BSD 上运行 5 个网络服务，包括音乐流应用 IceCast、基于 SLashcode 的网络新闻接口、2 个广告以及一个基于文本的多用户角色扮演网络游戏 FuRRyMuck。只有维持上述服务运行，小组就可得分，运行的时间越长，得的分数就越高。但如果服务被破

坏，该小组就要被减分。

Defense Information Systems Agency 安全工程师 ALan HaRpeR 表示，此类竞赛旨在表明，黑客行为并非只有破坏作用，虽然所采用的技术是一样的，但目的是不同的。只有了解如何攻击系统才能更好地学会如何保护系统。

Root Fu 之名来自于 Unix 系统的超级用户名“Root”加上“功夫(Kung Fu)”的后一个音节“Fu”组成。

中国互联网协会发布垃圾邮件情况统计报告

2003 年 8 月 8 日，中国互联网协会在北京梅地亚中心召开了“垃圾邮件情况通报会”。中国互联网协会黄澄清副秘书长对目前垃圾邮件的状况和中国互联网协会反垃圾邮件协调小组即将采取的行动进行了通报。

黄澄清副秘书长指出：一段时间以来，虽然国内外的互联网运营商、邮件服务提供商采取了大量的技术和管理手段试图遏制这种状态，但令人遗憾的是，垃圾邮件仍然保持着增长的势头。据中国互联网信息中心公布的数据显示，2002 年 12 月份我国网民每周收到的正常电子邮件数为 7.7 封、垃圾邮件数是 8.3 封，而半年后的 2003 年 7 月份正常电子邮件数是 7.2

封，圾邮件数为 8.9 封。另据中国互联网协会反垃圾邮件协调小组最近的调查显示，国内拥有邮件服务器的企业普遍受到垃圾邮件的侵扰，对企业造成了沉重的负担，如：有的企业每周收到上万封垃圾邮件，有的企业每年为应付垃圾邮件投入上百万元的设备和大量的人力。

由于我国目前在垃圾邮件管理上，尚存在法律、管理的空白点，国外的许多垃圾邮件发送者，通过中国的邮件服务器向国外大量转发垃圾邮件，还有少数国内的垃圾邮件发送者也经常向国外发送垃圾邮件，导致国外反垃圾邮件组织封杀来自中国的 IP 地址，导致网络不畅正常的信息交流受阻，不仅影响了我国互联网业务的正常发展，也损害了中国互联网和广大网民的声誉。

为遏制垃圾邮件在我国的泛滥，2003 年 6 月份协调小组组织各成员单位开展了检查并关闭开放转发(Open ReLay)功能和清除网站上的群发软件和垃圾邮件发送软件自查工作。此项工作得到了协调小组各成员单位的积极响应，从近期中国互联网协会对网上垃圾邮件所作的跟踪统计表明，对开放转发(Open ReLay)功能的整治工作取得了明显效果，如：所统计的近 3600 个垃圾邮件发送服务器中，只有 6 个中国境内的

邮件服务器具有开放转发(Open ReLay)功能。

会上中国互联网协会反垃圾邮件协调小组依照“中国互联网协会反垃圾邮件协调小组全体会议决议”，正式公布了一批境内外垃圾邮件服务器名单。这份名单中包含 225 个垃圾邮件服务器 IP 地址、域名和使用者信息。其中：中国内陆地区 23 个、中国台湾地区 97 个、中国香港地区 4 个、中国以外地区 101 个。

会议希望被公布的相关单位尽快对垃圾邮件进行治理，中国互联网协会反垃圾邮件协调小组将密切跟踪所公布名单服务器的治理情况。如果被公布名单上的单位在 9 月 8 日前未能采取有效措施对垃圾邮件予以治理，协调小组将保留采取进一步行动的权利，甚至拒绝该服务器的接入，如果在期限内进行了有效处理，经协调小组研究同意后，可以从名单中撤除。

今后，中国互联网协会反垃圾邮件协调小组将定期在中国互联网协会网站上公布垃圾邮件服务器名单，以监督这些服务器对垃圾邮件的治理。同时我们呼吁政府主管部门加快对治理垃圾邮件的立法工作，由政府、行业组织、企业和社会共同建立反垃圾邮件体系，希望通过广大从业者的工作和全社会的共同努力，积极探索出中国治理垃圾邮件的道路。

2005 年，将有 20％的企业遭受严重的网络攻击

美国 GaRtneR 于当地时间 8 月 7 日公布了关于互联网危险性的调查结果。据该调查结果显示，2005 年将有 20％的企业遭受病毒等严重侵害。

该公司建议，“虽然大多数企业将不会面临类似的攻击，但也应该准备必要的应对措施”。“如果受到攻击时没有采取防护措施，那么所蒙受的损失将有可能高于措施成本”（该公司）。另外 GaRtneR 公司副董事长兼 FeLLow RIchaRd HunteR 指出，“只要网络中有一台不能确保安全性的机器，便可能使整个网络面临危险”。

关于企业信息安全性方面最有可能受攻击的地方，该公司列举了以下 3 项：

使用具有安全性问题的商用软件

补丁升级不够完善

用户警惕性低，认为遭受安全性损失是别人的事，与自己无关

“企业试图解决安全性方面的问题，不过由于新技术的大量出现从而使问题增多。例如，Web 服务在应用软件的安全性领域撕开了新的”裂缝“。不安全的无线 LAN 成为企业网络中的严重弱点，即时信息造

成的漏洞令人担心。”

超强蠕虫病毒现踪美国传播的迅速危害带宽

安全专家产称，当地时间本周一，美国出现一种利用Windows中最近被发现的安全缺陷的互联网蠕虫病毒，它能够使系统崩溃，并迅速向容易受到攻击的系统蔓延。

这一被称为 LoveSan、BLasteR 或 MSBLasteR 的蠕虫病毒利用了 Windows2000 和 Windows XP 中由远程过程调用托管的分布式组件对象服务。

SANS 学院互联网风暴中心的技术总监约翰尼斯说，一旦传播到容易受到攻击的系统上，它就会从已经被感染的计算机上下载能够进行自我复制的代码，然后扫描互联网发现其它容易受到攻击的计算机，并对它们进行攻击。他说，有时候，该蠕虫病毒能够使计算机崩溃，但不感染它。MSBLasteR 蠕虫病毒的传播非常迅速，它已经感染了数千台计算机。

约翰尼斯表示，MSBLasteR 蠕虫病毒还会使被感染的计算机在 8 月 16 日对微软公司的一个网站发动分布式拒绝服务攻击（DDOS）。受到 DDOS 攻击的网站会因收到的服务请求太多而不能处理正常的请求。TRuSecuRe 公司的库珀尔说，从这一角度看，它是非常危险的，它可能消耗大量的带宽

据 SANS 学院称，这一蠕虫病毒的代码中包括下面的内容："BILLy Gates why do you make This Possible Stop makIng money and fIx your Software"（比尔 盖茨，你为什么要使这种攻击成为可能？不要再挣更多的钱了，好好修正你发行的软件吧。）。

反病毒软件提供商 Network Associates 公司将这一蠕虫病毒的危险等级定为中，而赛门铁克公司则把它传播的危险程度定为高，而将它造成危害的危险程度定为低。

ChinaByte："冲击波"爆发显示企业补漏不得力

本周 MSBLast(冲击波)病毒的爆发提出了有关软件补丁有效性的老问题。MSBLast 病毒的传播能力强烈地表明，目前修复方法太耗费时间，不能够对严重的作出及时的反应。这个结果就是 MSBLast 病毒已经在互联网上迅速传播。

这个病毒已经感染了 10 万台计算机，造成许多公司和互联网服务提供商网络中断。例如，佛罗里达州立大学因为一台计算机通过拨号网络被感染，造成数百台计算机被感染。该 大学的一位网络安全工程师 Jordan WIens 表示，他们已经采取了措施用补丁修复漏洞，但是还是出现了这个问题。

微软表示，它正在与执法部门合作，查找发布这

个病毒的个人或者团体。

这次病毒爆发的教训是，人们不能单纯依赖软件补丁来保证计算机安全。微软安全计划经理 Stephen TouLouse 表示，没有一个单独的方案可以解决计算机安全问题。我们鼓励深入防御，同时也鼓励用户使用软件补丁。

深入防御战略不仅要求企业保证与互联网连接的服务器和网络设备的安全，而且还要保证其内部网络的安全。

专业人士表示，个人用户并不能积极跟踪 Windows 的更新。有些人甚至不知道有软件补丁。因此，有些地区性互联网服务提供商采用封锁有漏洞的软件地址或者端口的方法阻止病毒传播，并且用电子邮件通知被感染的用户。但是，这样非常耗费时间。

企业一般都知道软件漏洞的存在，并且需要修复这些漏洞。但是，他们总是没有足够的时间。软件补丁也有质量问题。有些软件补丁可能造成系统死机，有些补丁甚至还能意外地修改商业程序。因此，企业要对软件补丁进行测试，才能使用。

上述问题表明，目前修复方法太耗费时间，不能够对严重的作出及时的反应。

垃圾邮件玩猫捉鼠游戏 手段愈发隐蔽高超

这是真实的一幕：当 Joe Stewart 在认真查看新病毒“SoBIg”复杂原代码想要弄清楚其来龙去脉时，该病毒已经开始感染了他的主机，并且利用他的主机发出一系列的垃圾邮件。这种肮脏的手段就是在垃圾信息世界里公开的惯例。

散发垃圾邮件和反垃圾的人就象玩着猫捉老鼠的游戏。老鼠总是利用一切机会跑在猫的前头。他们做坏事的手段越来越隐蔽、高超。

与黑客军团和技术相结合

研究报告指出：目前有 70%的垃圾邮件，大约 60-70 亿条消息是通过被感染的家庭主机转发出去的。很多前黑客军团加入这场垃圾游戏，并从中获益菲浅。许多家庭主机受感染后仍不知情，当被告知时还不相信这是事实。

工作地点在家里，工具简单

大部分是在家里做案，使用的并非高科技的价值上亿电脑系统，而是简单的网络和与其他做案者共同修改的软件。他们组成网上俱乐部，交流共享攻击目标地址，非法宽带，做案软件等等。

一天可以发送一千万封垃圾邮件

一名前垃圾邮件散播者接受MSNBC.com秘密访问

时表示，他能够一天发出一千万封垃圾邮件。电脑必须二十四小时工作才能带来收入。为了逃避EaRthLInk等公司的追查，使用老式的拨号帐户上网。这令到追查工作更加艰难。