信息安全动态

11

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

目 录 索 引

✧ 一、*警钟篇*

✧ 二、*案例篇*

✧ 三、管理篇

✧ 四、业界动态篇

✧ 五、技术与产品篇

✧ 六、应用篇

✧ 七、争鸣篇

✧ 八、曝光篇

✧ 九、趋势篇

✧ 十、安全锦囊

警钟篇

- 从“中美黑客大战”看我国网络信息安全
- 网络安全人才先行
- 宝岛一把火——烧出网络安全新话题
- 五千网络安全漏洞随时会被攻击
- 去年全球计算机病毒造成损失 170 亿美元
- 最新病毒警告

……

通信世界 Communications World
2001年5月28日

从“中美黑客大战”看我国网络信息安全

□彭 俊

“五一”期间，中美之间爆发了有史以来规模最大的“网络战争”，数以万计的中美黑客相互攻击对方的网站，数千家中美网站被黑或拒绝服务。根据国家计算机网络与信息安全管理办公室（以下简称“国信安办”）的统计，“五一”中美黑客交手期间，美国被黑网站中，.gov 的网站只占3.4%，而中国则占36.7%。这不得不让人们为我国的信息网络安全担忧，也有理由让每一个从事网络安全管理的从业人员好好反思。

反思之一：问题到底出在哪里？

根据国家计算机网络应急处理协调中心的统计，在本次“黑客大战”中，从技术手段看，中美黑客都无外乎或利用系统安全漏洞和服务漏洞、或进行密码猜解、或采取 DDoS 攻击。据“国信安办”技术组织处处长白硕教授介绍，本次“网络大战”无一新的攻击方式，唯一一点高明的，还是“中国红客联盟”创始人 Lion 编写的 Lion 蠕虫。

根据统计，本次大战中，基于 Windows NT 的平台受侵害的程度严重，在中国被黑的操作平台中，Windows NT:Linux:Unix：其它，为 1250:175:100:75；用的较多较普遍的漏洞有新发现的 IIS 漏洞、IGMP 漏洞、MS-FTP 服务漏洞以及 Windows 的远程终端管理漏洞等。其中，Windows NT/2000 下的 IIS Unicode 漏洞还是我们中国人发现的。黑客们使用的密码猜解工具，也大都是在互联网上可以找到的。由此可见，本次大战并没有利用什么新技术或新手段。

那么，问题到底出在哪里？除了操作系统和安全产品（许多都是国外的产品）等方面的客观原因外，最为主要的还是网络管理员的基本素质不高、安全防范意识淡薄。比如，针对一些系统漏洞，只要我们的管理员安装一些补丁，或在攻击来临前关掉一些没用的服务，其系统就根本不会遭受攻击；又如，许多网站的网络管理员密码和用户名完全一致或过于简单，使黑客利用猜解工具很容易猜解；另外，我们的网络管理员在安装系统时，往往为了省事偷懒，不进行系统配置而采用默认配置，这很容易被黑客利用。由此可见，我们的信息网络安全问题，并不是技术问题，而是管理人员的素质问题、意识问题和管理问题。

反思之二：如何保障我国网络信息安全？

通过以上问题可以看出，与美国等发达国家相比，在信息网络安全防范上，抛开系统因素，我们的差距并不在技术，而是在管理，这也印证了人们常说的“三分技术、七分管理”这句老话。针对这些问题，如何才能保障我国的信息网络安全呢？

首先，要提高网络管理人员的基本素质和安全防范意识。同是在这一次交战中，中美双方的一些主管机构和研究机构都向社会发出过警告，我国公安部、中科院以及“国信安办”在4月底5月初先后发出了预防黑客攻击的公告，但在得到警告之后，美国各网站尤其是重要网站，都进行了很好的防范，而我国的大部分网站，面对警告却无动于衷，照常悠然地去度自己的长假，然后就出现了开始那样的结果，有的网站甚至在遭到攻击后的一个星期里，还没有修改和恢复，可见，我国网络管理人员的素质一斑。

其次，尽快建立一个信息网络安全防范体制。从目前的国际政治经济秩序看，我们很可能很快就要面临下一次“网络战争”，因此，我国必须尽快建立一个从中央到地方、从行业到具体企业的安全防范体系。对网络而言，动一环而全网，一个环节出了问题，很可能引起别的环节出问题，一个网站因防范不周受到攻击，很可能导致在同一网络中的别的网站易于受攻击。因此，我们还有必要建立一个类似于“连坐”的处罚机制。

再次，开发自己的操作系统和安全产品，以确保信息网络安全。不知何时，许多中国人染上了崇洋媚外病，什么都是外国的好，计算机操作系统也就罢了，毕竟直到红旗 Linux 出现，我们都没有自己的产品，但是，对许多对网络安全产品，我们居然也盲目的认为国外的产品好。此次攻击事件中，很多政府和教育部门的网站就是用的某国外公司的 Pix 防火墙，据消息说，该公司的网络产品小组中有该国的特工人员，那么在该公司的网络产品中发现后门，我们的网站被攻陷也就不足为奇了。因此，我们一定要有自己的操作系统，自己的网络产品，自己的安全产品，这样，我们才可能防护我们的网络门户，确保我们的网络安全。

最后，我们还要继续加强在技术方面的研究，进行国际交流，不断提高我们的防范技术水平。

反思之三：怎样维护网络秩序？

抛开对网黑客的爱国热情，再来看此次黑客攻击事件，可以相信，我国政府绝不会支持这样的攻击行动。实际上，无论是红客还黑客，只要对网络进行攻击，都是在破坏网络秩序，这一点是不容质疑的。当然，我们也要辩证地看待此次攻击事件，塞翁失马，焉知非福。虽然我们在此次交手中受到更多的伤害，但是，这也给我们的网络安全敲响了警钟，也给许多网站上了一堂非常好的课。同时，通过此次攻击，也使网络战争的概念不再抽象，中国国防大学张召忠教授对此已做了肯定。

但是，警钟也好，示范也好，破坏秩序就不好。因此，我们必须建立一种机制，加强国际合作，共同维护好网络秩序。

黑客(Hacker)不是骇客(Cracker)，黑客更多的是技术发烧友，是为了掌握技术，真正的黑客高手一般不会参加网络攻击的，也是赞成维护网络安全秩序的，中国红客联盟创始人 Lion 在接受《南方周末》记者采访时，也表明了这一点。因此，我们完全可以考虑，组织黑客为维护网络安全和国家安全所用。

另外，我们必须加强网络安全立法。《中华人民共和国刑法》的 285、286、287 条对计算机与网络犯罪做了规定，但如何界定犯罪，存在操作问题。2000 年先后出台了《互联网信息服务管理办法》、《中华人民共和国电信条例》、《关于维护互联网安全的决定》等法规，但是针对网络安全的法律法规还是相对较少，因此，我们还要继续进行研究，加快立法进程，以法律来维护信息网络安全。在采访中，许多专家认为，黑客攻击类似于“劫机”，因此应该参照处理，希望我们的黑客，在进行网络攻击时，要先想想法律后果。

中国电子商务

2001年5月1日

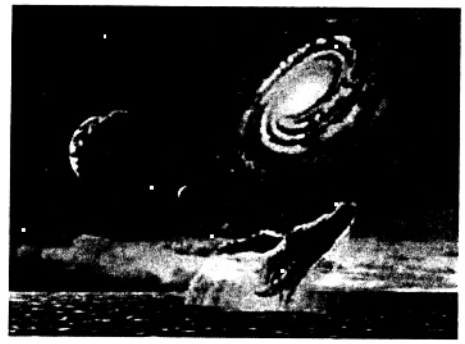
建设我们的网上长城

——由中美黑客大战想到的

● 本刊记者 陈共德

由撞机事件引起的中美黑客大战，至今还“硝烟弥漫”，双方都不肯歇手。

听说，那些“英勇善战”的中国黑客们在网上攻城略地，甚至将五星红旗挂到了白宫主页上。平常就对对美国佬所为很不以为然的国人这下很解气了一回，很扬眉了一回。看来，我们平常不分清红皂白就把黑客视为恶之类的做法是欠妥当的，起码会将一批大大的好人也给冤枉了。



当然，对这次中国黑客的枪口一致对外，国人的态度是“仁者见仁，智者见智”。举手反对者，也会是齐刷刷的一大片。反对的理由也无不冠冕堂皇。如，国家大事有出入皆高级轿车的人来担当、做主，我们草民们犯不上去“先天下之忧而忧”去。何况，各有千军万马、核武库支持的中美外交人士用了近半个月、想尽各种办法都摆不平的事，一到网上，手无寸铁的黑客们就能拿一个“城下之盟”回来交差？还是别给政府添乱，赶紧停吧。

不过，据悉，这一次的黑客之争，是由美方先动手的。“来而不往非礼也”，向来文质彬彬的中国人也只得“自卫反击”了。如今，和平是世界主流。想等着世界大战，自己有热闹瞧，或发国难财的人是肯定没戏了。但是，不同立场的人却能够将各种争执和火气发泄到互联网上，用黑客之手段去攻击对方。信息大战倒是有可能一触即发。只要世界还没有大同，就难免有黑客的你争我斗和杀杀打打。

这次黑客大战，可说是向我们敲响了警钟。面对着来自网上的攻击，我们准备好了吗？

据了解，最近发生的网络攻击事件有一些比较显著的特点，即攻击手法相对以往比较单一，大多数利用现有的工具对近期发现的一系列操作系统漏洞进行攻击。但是由于国内很多网站技术人员缺乏，管理水平较低，不能针对具体攻击的特点拿出有效的防护措施，导致系统持续处于被破坏状态而造成不良影响。

这一次行动中，美国一个黑客组织便攻破国内500余家网站，其中许多是政府、科研单位及教育网站，这明显暴露出中国网站安全防范意识很差。美国网站已经有所准备，展开攻击可谓难于上青天，即使攻击了，不过几分钟，对方也很快就恢复了。倒是中国的网站遭到攻击后，很长很长的时间不能恢复。美国方面的攻击成果比国内黑客要多，主要是国内的网络管理员对安全的若无其事造成的。

其实，中国的网络安全问题由来已久，并不是一日之寒。不少人的脑中没有“安全”这根筋。据中国计算机报的统计，中国已经上网的所有企业中，有55%的企业没有防火墙，46．9%的企业没有安全审计系统，67．2%的企业没有入侵监视系统，72．3%的企业没有网站自动恢复功能。通过这个数字，我们可以非常清楚看到企业的网络安全问题真是吓人一大跳的。固然，你可以说，你是商人，不关心政治，大可不必为担心政体和国体的屈人之兵而食寝不安的。但是，没有网络安全，又哪来你的电子商务？

由这次黑客大战，我们看出，中国要成为网上强国，不只是要有锐利的矛，而且更要有牢不可破的盾。我们中国要建设网上的万里长城，要布置网上的"导弹防御系统"。害人之心不可有，防人之心不可无。面对动不动就舞枪弄棍的无赖们，中国人得多个心眼，早防一手，没有坏处。所以，网上安全是大事，儿戏不得啊！ ■

中国计算机报

2001年5月31日

网威博士谈安全

“黑客大战”告诉我们什么

前一段时间的黑客事件引起业内的普遍关注，国内网站受到美国黑客攻击，其攻击方法是这样的。据了解，这次黑客攻击的服务器主要是 Windows NT 系统，只要入侵成功，基本上都更改了对方的主页，从攻击手法及所造成的影响来看，攻击者所采用的依然是微软近来不断被披露的 IIS 漏洞，其中包括 Unicode 解码漏洞，Htr、Htw、Ida、Idq、Dc 等映射漏洞，以及 Front Page Extension 等等。还有一些是远程溢出，即直接获得超级权限，对网站进行修改。而这些漏洞，厂商都已经做出了补丁的，如果国内的各个网站的网络管理员平时注意网络安全建设，及时去下载补丁，并进行一些设置的话，完全可以不会在这次网络大战中成为受害者。

事后，引发了我们对网络安全的重新认识和思考。当今社会计算机和网络与人们生活的关系越来越紧密。一个现代化国家的社会信息网络如果遭到毁灭性打击，足以使人们的生活倒退几十年。目前我们的网络安全防护系统十分脆弱。据安全专家分析，这次美国黑客的攻击手法极其简单，他们利用中国用户对某些网络系统软件的不够熟悉，利用某些功能设置的不当来跨过防火墙进入我们的网络系统。

对于中国企业来讲，我们的网络是脆弱的。芯片不是我们的，操作系统、各类应用系统、数据库、防火墙等也几乎都是国外的产品，这给我国的网络安全留下严重隐患。据有关统计资料显示，现在 97% 以上的互联网存在严重的漏洞。国内一些敏感行业的网站，如政府、金融、证券行业等在网络安全上也都存在漏洞。面对内忧外患的网络安全现状，发展有自主产权的民族产品尤为重要。国家也意识到问题的严重性，在政策、资金上，给网络安全公司予以很大的扶持，并专门成立“国信安办”，负责推行“保障国家网络空间安全计划”。有消息称，一个关于“信息安全产品采购白皮书”的计划正在酝酿中，这对于我国的网络安全而言，无疑是一件好事。

网络安全最薄弱的环节是人。网络技术的竞争，从根本上说还是人才的竞争。网络安全领域涉及到国家命脉，影响到国家的安全和主权。除了军队、公安等部门对高级网络安全人才的需要外，政府、企业也需要网络安全方面的人才，互联网本身的漏洞也急需这些人来解决。这几年中国的 Internet 处于发展建设阶段，大部分的 ISP 和其它从事信息产业的公司都没有精力对网络安全进行必要的人力和物力投入，很多重要站点的管理员都是新手，一些操作系统如 Unix，它们在那些有经验的系统管理员的配置下尚且有缺陷，在这些新手的操作中更是漏洞百出。

“落后就要挨打”，我们在 IT 硬件与软件技术方面还处在落后状态，所以导致了我们互联网系统安全的脆弱性。因此，以北京中科网威信息技术有限公司为代表的一批国内专业网络安全公司，正在不断地努力，缩短这方面的差距，为中国的网络安全构筑自己坚实的长城。

中国计算机报

2001年6月7日

网络安全人才先行

【 刘宝旭 】

网络安全作为一个全新的产业，受到了社会的普遍关注。既然新，发展就肯定有困难，我国网络安全产业目前最缺的是什么？是人才。我国的反黑客专家许榕生曾经说过：网络安全的攻与守完全是高素质人才的对抗，他建议，中国应该加快培养高水平的网络安全人才，以适应社会各方面的需求。

美国政府最近公布的一份国家安全报告认为，21世纪对美国国家安全威胁最严重的是网络恐怖主义。今年美国还宣布，政府将投入20亿美元用于网络安全，2003年将达到83亿美元。由于我国，网络信息安全研究起步晚、投入较少，成果的孵化率、产品化和市场占有率都不高，整个网络安全产业尚未形成较大的规模。虽然国内一些厂商已研制开发出防火墙、安全路由器、安全网关、黑客入侵检测、系统脆弱性扫描等软硬件，但这些产品在安全技术的完善性、规范化和实用性等方面还存在许多不足，特别是在多平台的兼容性、多协议的适应性和多接口的满足性方面存在很大差距。

看来，在未来的信息社会，要掌握自己的命运，就必须在网络安全防护技术、网络安全人才和相关法律政策上构建自己的网上长城，建筑自己的安全体系，只有这样，才能保证国家信息系统处于安全状态，才能真正让“信息化”为中国腾飞带来希望。

各国抢网络安全人才

据华盛顿5月22日消息，美国政府21日宣布，将为一个“网络军团”项目提供860万美元的奖学金，这个“网络军团”将由200名学生组成，他们同意毕业后到政府部门就职于电脑安全方面的工作。美国国家科学基金会称该组织已经选择了6所大学来参与这一计划，目的是为了缓解美国联邦政府中电脑安全专家短缺的问题。参加这一计划的学生必须是信息安全或相关专业的研究生或大学生，美国政府将为他们支付两年的学费。他们将首先作为政府部门的暑期实习生工作，然后在完成学业后，到政府机关任职。

目前在我国，网络安全人才培养方面的投入还有较大的欠缺，在教育系统，专门针对网络安全开设的专业与社会需求相比，也还远远不够，科研院所进行的安全专业人员的培养力度与国外相比，有相当差距。但让人欣慰的是，随着我国各级部门对网络安全认识的不断提高，对网络安全人才培养方面所投入的人力物力也在逐渐加强。有些院校开设相关专业、研究机构培养专门人才，职能部门有针对性地举办多次相关培训，各地纷纷设立相关机构负责网络安全人才的培养与管理工作。

据报道，经国家教育部批准，武汉大学计算机学院将增设信息安全本科专业，2001年秋季起正式面向全国招生。迄今为止，这是我国在高校开办的惟一一个信息安全本科专业。我国目前只有少数高等院校开设了“信息安全”课程，而且目前还不能涵盖信息安全的主要内容，因此信息安全方面的人才很少，而金融、商业、公安部门、军事部门和政府部门对信息安全人才的需求是很大的。要解决这种供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。

人才培养是关键

反黑客专家许榕生研究员曾表示，网络安全的攻与守完全是高素质人才的对抗，而我国很多网络的系统管理员是大学计算机系刚毕业的学生，根本不具备管理一个大型系统的能力。他建议，中国应该建设一支反黑客的“快速反应部队”，同时要加快培养高水平的网络安全人才，以适应社会各方面的需求。

网络安全领域涉及到国家命脉，影响到国家的安全和主权。除了军队、公安等部门对高级网络安全人才的需要外，互联网本身的漏洞也急需这些人来解决。据介绍，我国现有信息安全专业人才3000人左右，目前在企业和机关工作的信息安全专业人才还不能满足需要，也跟不上迅猛发展的信息化进程。假如这3000人属于正规军的话，那么来自民间的黑客，算是对网络安全人才的一个很大的补充，事实上，活跃在企业的网络安全技术人才大部分来自后者。尽管如此，国内网络安全专业人才仍存在较大缺口，高级的战略人才和专业技术人才尤其匮乏。所以，解决网络安全建设问题的关键是解决网络安全人才的匮乏，解决途径当然是大力培养网络安全人才。

网络发展到现在，关于网络安全问题的解决方法问题，大家已经形成一种共识，那就是，网络安全体系的建立关键在于人，尤其是网络安全人才，因为所有的网络安全技术、措施、工具都只能是安全体系建设的辅助手段，策略的制定、技术工具的实施和最终规划落实都要靠人。

2001年5月31日

宝岛一把火——烧出网络安全新话题

追踪报道

记者 张路宁 李冰心综合报道

网络"防火墙"能够防住来自网络的"火灾"侵袭，但对于熊熊燃烧的大火只能徒呼奈何。日前，台湾汐止县东方科学园区大楼发生重大火灾，在这幢摩天大楼上发生的火灾延续了整整43小时，使总部设在楼内的130多家网站陷入瘫痪。连台湾新浪网也极不情愿地贴出了"暂时中止服务"的启事。

据初步统计，此次大火造成的保险赔偿金额高达130亿元新台币，但更重要的是因火灾造成的服务中断、资料焚毁，使网络公司遭受到了无法统计的巨大损失，许多企业用户网络存储的资料丢失甚至引起了恐慌。

网络是美丽的，但也是娇弱的，其实这次造成台湾IT业"大面积烧伤"的真正原因只是这130多家公司的代理服务器SeedNet由于火灾停了几分钟电。过去谈论的网络安全问题往往局限于病毒、"黑客"、身份认证等，现在"火烧摩天楼"又烧出了新的网络安全问题。网站硬件损伤和网络资料备份问题被拎到了台前，使人们警醒到安全的另一面。

很多人对不久前国内ChinaRen"主页大巴"事故还记忆犹新。由于ChinaRen数据服务器的RAID卡损坏，两块服务器硬盘数据全部被改写或丢失，导致当时ChinaRen主页大巴800万访问量全部中断，超过30万的个人主页无一幸免成了网上冤魂。幸而其中不涉及企业数据资料，损失有限。

连续发生的事件使企业对于挑选网络资料中心(IDC)进行资料备份更加谨慎，关心的不再仅是IDC供应商是否有先进的防火墙、能否有效防止黑客入侵、设备是否具有安全扫描设计等，有否完善的资料备份更成了重中之重。这也为资料备份设备市场提供了巨大的商机，许多厂家开始投入巨资扩大生产，以抢夺市场。

然而，闻风而动总不如未雨绸缪，如台湾宏基科技公司等企业早已把"灾害资料复元"作为重点研究方向，NetBackup Professional等产品趁机大举占领市场份额。但据Internet Research Group研究机构估算，这一市场仍然有约50亿美元的商机有待争夺。资料备份设备技术门槛并不高，国内许多厂商具有生产能力，分羹而食，时不我待。

广东通信报

2001年5月31日

五千网络漏洞随时会被攻击

网络安全专家论坛披露

本报讯 “五·一”中美黑客大战后，网络安全再度成为热闹话题。为此，5月20日下午，广州市电信局在中华广场举办了“因特网发展和网络安全”专家论坛。此次论坛请到中科院著名网络安全专家邓小丹博士、广州市公安局计算机技术监察办的网络专家廖晨光、广州电信信息服务中心主任邹匡国担任主讲，同时邀请了本地多家知名网络安全公司、IT企业、银行的专家以及数十名网友参加交流。有关专家在此次论坛上爆出惊人信息：目前已经发现并命名的网络操作系统漏洞就有5000多种，其中2000多种都是近两年发现的。这些漏洞对网络安全构成了严重威胁。

网络安全漏洞重重

邓小丹在发言中说，目前已发现并命名的网站操作系统漏洞达5000多种，其中有2000多种都是近两年发现的。尚未发现的更加难以估计。这些漏洞严重威胁着网络安全。就是说，目前采用的攻击网络方法就有5000多种。有的可以删除系统中的任何一个文件并更改网页；有的可以导致网站“拒绝服务”，让银行、电子商务类网站损失惨重……他认为，我国在堵漏洞上并不落后，但是，电脑核心芯片、国际互联网骨干网络、操作系统都不是我们自己的，这是巨大的安全隐患。

据廖晨光证实，“五·一”期间接到报案，有企业和政府部门网站被黑客攻击；同期广东某网络安全公司接到上千封求救邮件和200个求救电话。信息产业部副总长张春江近日也表示：我国的网络安全形势十分严峻，今年“两会”召开期间与网络有关的提案发言就有100多个。

专家给你安全建议

邓小丹表示：目前网络安全的首要问题是众多网民还没有足够的安全意识，也不太清楚如何防范攻击。广东省网络安全中心的资料显示，现有的网站近九成连防范攻击的防火墙都没有安装。与会专家建议网民到有关安全网站下载安全检查扫描工具；选用经国家公安部认证的、更新速度尽可能快的网络安全产品，如升级快的杀毒软件等。

为防止网站被攻破，专家还建议：网络管理员要了解操作系统的缺陷并及时打上补丁，比如到 www.microsoft.com/downloads 下载；同时应关闭不必要的服务端口，比较危险的服务端口有 TEL-NET、23FINGER、79等。

另外，专家们认为：所谓“五·一”的中美黑客大战，是传媒的刻意炒作，我国政府并不提倡为了爱国热情而攻击他国网站。专家们也不主张成立“黑客联盟”或“红客联盟”，认为这些“黑客”对国外网站的攻击是低层次的，是违反国家有关法律和国际关系法的。最后，专家们提醒广大网民要做一个守法的网民。（罗抗）

中国化工报

2001年5月29日

去年全球计算机病毒造成损失170亿美元

本报讯 葡萄牙一家网络病毒专业监测公司发表的报告指出，尽管全球越来越多的人开始使用电子邮件传递信息，但网络安全保护措施却没有相应加强。与此同时，五花八门的电脑病毒却层出不穷，仅世人熟知的“爱虫”病毒，目前就有32个变种。2000年全球病毒邮件的数量比上年增加了66%，预计今年与去年相比，增幅可能达到200%以上。如果网络安全措施仍然没有加强，这一趋势将会继续恶化下去。去年，电脑病毒在全球造成的经济损失就已超过170亿美元。

另据一家网络独立调查机构的数据显示，目前全球各种电脑病毒的数量已超过5万种，其中DOS病毒占4万种，可在视窗95、98、2000和NT上运行的病毒也有近千种。（尚民）