信息安全动态

10

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

信息安全：守好数字大门 3

病毒：不容忽视的计算机安全问题 5

谨防网络窃贼 6

电子窃贼防不胜防 6

对网络安全切勿掉心轻心 7

Internet 安全问题不断增多 7

警惕“主页”病毒快速传播色情内容 7

当心“主页”病毒 8

“主页病毒“正在全球蔓延 8

计算机恶性病毒“欢乐时光“在我国发作 8

什么是“欢乐时光”病毒? 9

“欢乐时光”今天要滋事 9

一种全新的“快乐时光”网络蠕虫在国内流行 10

专家怀疑“欢乐时光”为“国产病毒” 10

“欢乐时光”施毒部分省区 11

“欢乐时光”今日作恶—我省上午尚无病毒发作报告 12

“欢乐时光”没到来 12

“欢乐时光”乐不起来 13

提防电子邮件病毒大发作 13

“欢乐时光”没乐起来 15
“欢乐时光”没添乱子 15
当心!“恋爱伴侣”是病毒 15
找对象程序是病毒 16
当心 JS-OLVORTEX.A 风暴病毒 16
电脑上网，小心“红娘”病毒 16
网上冲浪小心“暗礁”提醒网友不要“中招” 17
为了您的计算机安全请别“跟耶稣瞎侃” 17
感染 Solaris 的新“蠕虫” 17
“五一”劳动节病毒添新丁 18
库尔尼科娃变种病毒问世 18
“爱虫”蠕虫出现新变种 18
新病毒能自动篡改网页 18

✧ 二、*案例篇*

“阶梯”全球电子监听网遭遇黑客 21
电脑病毒专黑美国间谍网 21
黑客围攻五角大楼 22
俄黑客几度闯入美国防部 23
美发言人证实白宫网站遭到攻击 23
美国务院网络被黑，不得不关闭四星期 23
神秘黑客闯入，国务院网瘫了 23
美著名安全网站遭黑客袭击 24
俄一官方网站被黑 24
江苏网络行窃者一审被判死缓 24
长沙破获首例“黑客”攻击网吧案 24
北京抓了第一个“黑客” 25
网上黑客，“黑”法网 25
北京破获上网帐号被窃大案 26

我省一网站遭黑客攻击 26
广东无辜网站被黑 27
受中美黑客大战影响，福彩网站被黑了 27
上百韩国网站成为中美黑客战的受害者 27
FBI 看上年轻黑客 27
FBI 诱捕电脑黑客 28
黑客搅乱菲律宾 28

✧ 三、管理篇

信息安全：上海走在前 31
网络安全大堤还需加固 31
关于选择我国计算机网络安全服务试点单位的公告 32
关于网络安全的政策法规 32
黑客入侵，没门！ 33
网上银行：安全重于泰山 33
网络管理技术：银行业发展的翅膀 34
电子联行系统安全管理浅谈 36
集中国防病毒产品实施工程之最 38
网络终端与网络银行的渠道选择 39

✧ 四、业界动态篇

各界精英共商信息安全发展大计—“中国信息安全技术与发展战略”高层研讨会在京举行 45
精英共商信息安全发展大计 45
安全+可靠=信息保障 45
市场动态网上走 46
河南信息安全工程研究中心成立 46
武大增设信息安全本科专业 46
信息安全体系国际标准培训班将在京举办 47
ISO17799 致力解决网络安全 47

修建反黑客防线 47
美国 RSA 全力开拓中国市场 48
增强网络安全能力 48
IBM 称雄中国软件世界 48
熊猫卫士抢摊中国网络反病毒市场 49
熊猫卫士签约海事局、人行，成长为企业级市场领导者 49
诺基亚挺进网络安全市场 49
诺基亚揭开无线网络安全方案 50
首次国际“黑客武林”大会在港举行 50
黑客集团制造出“无限制”网络浏览器 50
病毒、黑客攻防实验室 51
英军已开发出软件能阻网络病毒传播 51
“网络安全 119”问世 52
冠群联想新品发布海内外同步行 52
朗新网络安全产品助力北京高法 52
握奇与 CFCA 构筑网络安全体系 53
网络安全的电子钥匙 53
深思洛克推出基于 USB 的 IC 智能卡 53
世纪互联网络安全服务标准化 54
世纪互联推出网络性能监测新服务 54
新型 VPN 服务重安全 54
诺顿克隆精灵 2001 让你有“备”无患 54
光环新网联手英特尔 VPN 服务一条龙 55
赛门铁克推出 Symantec pcAnywhere 10.0 简体中文版 55
所有 KV3000 用户的又一大喜讯 56
书生公司瞄准电子政务软件 56
联想网御，推进信息安全 I 时代 56
eTrust Audit 护航电子商务 57

CA 的 eTrust Audit 使电子商务安全信息触手可及 57
CA 推出防病毒解决方案 57
CA 推出电子商务数据保护解决方案 57
Novell 为保护企业安全提供最佳组合 58
Toplayer 安全软件悄悄跟踪黑客 58
N etscreen 安全从核心着手 58
VPN 防毒零维护 58
BroadConnex 网关保主机安全 59
Check Point 构架下一代 Internet 管理 59
ERX-1400 边缘路由器提供下一代宽带 IP 服务 59
F-Secure 保护 Linux 防火墙 60
TopLayer Appswitch 实现高速安全 60
指纹，数字时代的身份证 60

✧ 五、技术与产品篇

智能卡的操作系统—COS 63
NOE 加密原理与实现 69
Web 服务器 IIS4 的安全配置 71
VOIP 的关键技术 74
多业务企业网 QoS 保障方案 77
构建证券公司千兆容错交易网络 80
解读 IDC 服务 82

✧ 六、应用篇

企业全国连网解决方案 87
VPN 构架全国一片天 91
银行系统网络安全解决方案（二） 95
工行外汇清算处理系统的发展与架构 96
客户证券保证金系统的设计 97
华泰证券 VPN 解决方案 100

网上税收，集于一体 101
网上社会医疗保险系统的实现 103
透视公安网络系统 106
电力专家“安全”生产—河北电力的网络安全策略 108
陕西移动信息网站解决方案 109

✧ 七、争鸣篇

数据中心的安全分析 113
管理你的网络身份 115
浅谈 Internet 时代的信息安全 119
“悬赏”带不来安全 121
宽带网络安全刍议 122
对 N.323 标准进展的思考 123

✧ 八、曝光篇

日本微软称 Win2000 Server 存在严重安全漏洞 127
微软网络服务器软件不安全 127
Windows 2000 再出 Dos 问题 127
微软防火墙 ISA 中发现 Bug 128
Alcatel 网络产品存在安全漏洞 128
Web 应用程序—黑客的特洛伊木马 128

✧ 九、趋势篇

我惟一，我存在—生物识别技术面面观 133
新概念安全电脑 137
杀毒软件市场重新洗牌 138
信息安全，今年商机 60 亿 139
信息安全市场，谁与分羹？ 139
上市公司垂青“网络安全蛋糕” 140
反病毒市场谁会笑到最后 141

防病毒软件决战[网络安全地带] 142
网络信息安全产品市场将有大幅增长 143
防火墙销售在黑客中成长 143
VPN 销售：好戏在后头 144
2000 年我国网络安全软件市场分析 147
网络安全的“事前”与“事后” 149
发展中的 VoIP 150
虚拟路由保证新型 IP 服务 155
下一代互联网的技术发展方向 156
无线局域网的发展趋势及应用 159
新千年带来的移动性 162
认识网络防火墙的功能指标 164
反击黑客 167
防火墙大阅兵 169
面对 CIH 病毒我们能做什么 170

✧ 十、中美黑客大战专题报道

聚焦中美黑客网上交锋 173
黑客大战中方首回合胜美方 175
中美黑客大战纪实 176
“黑祸”冲击中国网络 177
中美黑客交锋日记 178
中美“黑客”激烈交锋 179
红客联盟宣布收兵 180
“红客联盟”公布“五 一”战报 181
网络安全敲响警钟 183
中美黑客大战我们看到了什么 184
院士何德全谈中美网络战—我反对黑客大战 184
危险的网络秩序 185

中国安全专家为美国黑客号脉 185
白宫新闻发言人访谈 186
中美网络大战挑战法律安全 187
著名军事专家评说中美网络大战 190
谁能打赢未来网络战争 191
网络战争向我们走来 192
我们一定要有自己的操作系统 193
中美黑客激战后的深思 194
黑客大战后的反思 194
中美网上大战谁在黑暗中窃笑 195
“红客”“黑客”都对网络秩序构成危害 195
人民时评：“红客”“黑客”都对网络秩序构成危害 196
中美黑客大战内幕大曝光 196
“黑客大战”置疑互联网未来 197
黑客行为是爱国还是违法？ 198
中国黑客，白卫反击 199
关于第一次接触网络战急 200
美国“黑客帝国”美梦止酣 201
最大赢家：网络安全公司 202
黑客大战忙坏安全公司 203
中美黑客大战忙坏国内网络安全公司 203
中国黑客“五一反攻”结束 204
与中国鹰派对话 206
更多的是一种发泄—专访“中国红客联盟”负责人 Lion 206
中国黑客首领访谈 208
中国三大黑客组织结构大剖析 209
美国黑客瞄准中国政府网站 209
长沙 E-mail 出国节点被封 210

✧ 十一、安全锦囊

提高 Windows NT 安全的方法 213

安全的双网隔离型电脑 215

防止 PPTP 被攻击 217

都是病毒惹的祸 219

防黑客致胜六招 219

微软防病毒新招：禁止附件 220

黑客帝国之八种武器 220

警钟篇

- 信息安全：守好数字化大门
- 病毒：不容忽视的计算机安全问题
- 谨防网络窃贼
- 警惕“主页”病毒快速传播色情内容
- “欢乐时光”病毒跟踪报道
- 最新病毒警告

……

2001年5月12日

信息安全

守好数字大门

上个世纪70年代，臭名昭著的JohnDraper通过用一种饼干盒制造的哨声侵入长途电话线路而赢得了"嘎扎上尉"的绰号；1988年11月，美国康乃尔大学学生玛瑞斯的"蠕虫"病毒通过因特网，致使网络中7000多台计算机被传染，造成经济损失约1亿美元；1999年10月，世界最大的电脑软件生产商微软公司网站被黑客攻陷；2000年末，首都在线服务器磁盘阵列发生故障，丢失了大量用户资料；今年年初，中美电缆因事故断裂，造成网络通讯大量拥塞……随着信息化社会的到来，信息安全、网络安全成了新时代人们面临的新问题。

黑客大战敲警钟

4月1日美军ep－3撞毁我军机后，网下的谈判正在进行，网上的斗争却已经开始，黑客大战自美国黑客对部分中国网站的恶意攻击拉开帷幕，被激怒的中国"红客"相继在网上展开了一场民族自卫战。

然而，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，致使我国网络受到相当沉重的打击。在已经掌握的4月份国际互联网上发生的数千起黑客事件中，针对中国大陆的就有数百起之多，占13.82%。在所有被攻击的网站中，商业网站占54%，政府网站占12%，教育和科研网站占19%，其他类型网站占15%。据国内某知名IDC企业的技术人员介绍，他们在4月份内检测到的针对他们所运营网络的扫描和探测行为达到每天8万起，实际发生的攻击数量为每天100起以上，大大超出了平时的水平。江西宜春政府网、西安信息港、贵州方志与地情网、中国青少年发展基金会网、福建外贸信息网、湖北武昌区政府信息网以及桂林图书馆、中国科学院理化技术研究所、中国科学院心理研究所等网站遭到攻击，一些大型门户网站也相继被黑。这是近年来中国网络安全受到的最大的挑战。

很多计算机安全专家称，此次中美黑客大战告诉人们的唯一警示就是有很多计算机在面临网络蠕虫攻击时将会变得非常脆弱。篡改网页只是一些更为复杂的数字涂画行为，黑客们在网站上留下自己的标语证明自己已经成功攻击了这一网站，仅这一点来说并不会产生大的影响。但既然黑客对网页进行了修改，就表明他们已经进入了该网站，这一点的难度要比单纯写写画画要大得多。用一些安全专家的话说，这种攻击就像是偷偷进入某个人的家中，在他的墙上乱写乱画。

网络安全隐患多

我们的网络是脆弱的。对于中国企业来讲，互联网至少有四大脆弱性，芯片不是我们的，应用系统、数据库、防火墙等几乎都是国外的产品，这也给我国的网络安全留下了严重的隐患。据统计资料显示，目前90%以上的互联网存在严重的漏洞，特别是政府、金融、证券行业等在网络安全上都存在很严重的漏洞。网上购物时的信息、个人的邮件、信用卡的账号和密码，每个商家的信息数据，一些政府的资料都在网上传递，完全有可能被截获。

根据国内一些网络安全研究机构的资料，国内电子商务站点的网络管理人员至少有90%以上没有受过正规的网络安全培训；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 Internet 的新手，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。很多服务器至少有三种以上的漏洞可以使入侵者获取系统的最高控制权。

中国开发的网络安全检测软件尚属凤毛麟角，各大 ISP 和各行业的网络安全检测工作基本上要靠国外一些网络安全公司的安全扫描产品，且不说国外产品的易用性如何，国外安全检测软件自身是否安全也总是让人心生疑窦。网上甚至有消息称，国外某著名网络安全公司在其软件上安装有泄密的后门。

人才储备存忧患

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、企业也需要电子商务方面的人才；互联网本身的漏洞也急需这些人来解决。有专家称，我国现有信息安全专业人才 3000 人左右，在企业和机关工作的信息安全专业人才还不能满足需要，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，那么来自民间的白帽子黑客，算是对网络安全人才一个很大的补充。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。

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，有关部门也意识到问题的严重性，目前在政策、资金上，给予一些民营网络安全公司很大的扶持。有消息称，一个关于“信息安全产品采购白皮书”的政策也正在酝酿，对网络安全而言，这无疑是一大利好。

信息战备需做好

有识之士指出：未来信息战的可能性是存在的。

美国在今年 4 月份已经建立“红色小组”，专门从事信息战的研究及规划；中国近期也积极招募“网军”，成立相应的对抗部门。

当今社会的信息化程度越来越高，计算机和网络与人们的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。这种战争比较文明，不会造成人员伤亡，但破坏力绝不比一场常规战争小。相对于传统的战争和能造成地球毁灭的核战争而言，信息战的可能性也许更大。在网络更加发达的未来社会，除了高能量电磁波的攻击外，信息对抗战的主力将是网络安全专家、黑客。

无可否认，在计算机领域上我们的技术整体上比西方发达国家落后。Internet 基础协议是开放的，Unix 系统的代码基本上是开放的，操作系统开放源代码是必然的趋势。硬件是别人的，但软件可以是自己的。在计算机领域，中国的软件技术明显优于硬件。黑客技术不是一个非常底层的领域，其开放性尤其明显。对系统极具破坏力的攻击程序代码和脚本在 Internet 上不难免费得到，相对于获得商业软件产品的源代码来说，黑客程序的源代码更容易设法获取。Internet 的开放和互联的特征决定黑客技术可以跨国攻击，它既可以用于攻击，也可以用于防御。用兵之道，必须攻防兼备。所以未来信息战的胜负有赖于一个国家的整体黑客技术水平，这些毋庸讳言。 □三江/文

新安晚报 XIN'AN WANBAO
2001年5月6日

病毒：不容忽视De计算机安全问题

计算机技术的高度发展为人类提供了高度的自动化和现代化，使社会经济、科学技术等向前迈进了一大步。然而，在人们深切享受着使用计算机带来的便利的同时，在对计算机高度依赖的背后，计算机安全问题越来越成为社会关注的一个大问题。

大家不会忘记 1998 年 CIH 病毒带来的那场灾难，数十万台用户的计算机无法启动，硬盘遭到破坏，许多重要宝贵的资料丢失，造成的损失高达几十亿元；1999 年 Happy 99、Melissa 大爆发，部分欧美国家损失惨重，大批网络瘫痪，受影响的计算机超过百万台；去年 5 月 4 日，"I Love You" 病毒又席卷了全球，造成美法等国家网络大面积瘫痪，其变异速度之快令人惊讶，一日内竟发现其十余个变种，据专家估计，由此造成的损失至少在百亿美元以上；今年 3 月 6 日，一种具备特洛伊木马和蠕虫双重性质的名为"裸奏"的病毒在欧美的互联网上迅速传播，它几乎可以删除用户电脑上所有重要的系统文件，甚至能使用户的 WINDOWS 操作系统崩溃；根本就不给人们挽息的机会，今年情人节期间发作的"库尔尼科娃"病毒又再次为我们敲响了警钟。据公安部门的调查资料表明，我国有 75%以上的计算机感染过计算机病毒，造成的经济财产等各方面损失无可估量。

由此可知，一个小小的计算机病毒程序，可以使一台计算机、一个大型计算机系统甚至计算机网络陷于瘫痪，这一方面反映了计算机系统的脆弱性，同时也证明了一点，计算机病毒已对计算机安全构成了极大的影响，而这种影响可能是彻底毁灭性的。如今网络越来越受到普及，随着 Internet 的广泛应用，计算机病毒无论从传染途径、传染速度、传染方法还是其编程方法上都起了很大的变化。可以这样说，计算机病毒有向更隐蔽化、智能化、多变化、复杂化、有向恶性病毒方面发展的趋势。网络的普及发展使人们在工作生活等方面得到了极大的便利，但也使计算机病毒的散播成为一件轻而易举的事情。过去，一种病毒在国外出现之后，需要半年多的时间才能传入我国，但如今通过网络，病毒在数秒钟内就可以传遍全球的各个角落。

计算机病毒实际上是人为编制的一种程序，它就像生物学中所称的病毒一样，在计算机系统中利用软件资源生存、繁殖和传播，并像生物学中病毒给动植物体带来疾病那样，对计算机系统资源造成严重的破坏。所以人们就借用了生物学名词来形象的描述这种特殊的计算机程序，称它为"计算机病毒"。人们常说的"病毒"是个广义的概念。从严格意义上来说，计算机病毒是能够复制自身或自身的变种，能够寄生在磁盘、程序软件中的一个程序、一段可执行码，并能通过系统数据共享的途径再次进行传染和繁衍。它具有潜伏性、传染性、寄生性、破坏性、自我复制能力和诱发因素等特征。其种类可以分为系统型病毒、引导型病毒、文件型病毒、复合型病毒、覆盖型病毒、隐形病毒、变形病毒、伴随型病毒、宏病毒、HTML 病毒等。这样一来，人们常说的"特洛伊木马"和"电脑蠕虫"等程序便没有包含在其中。特洛伊木马是一个程序或是程序的一部分，带有很危险的破坏行为，它们通常修改一些程序，使这些程序看上去能"正常"的运行，但其中隐藏着破坏性的指令，因为此类程序不会复制自身，所以不划入计算机病毒中。电脑蠕虫是网络上的一种寄生程序，会通过电脑网络等途径进行迅速的大面积的自我拷贝传播，也带有损害行为，但是它不感染文件，不改变文件和资料信息。还有一类程序，像 YAI，既是木马后门程序又感染 PE 格式的可执行文件，又如 MTX，既是木马后门程序又是蠕虫同时也感染 PE 格式的执行文件，我们称之为混合型病毒。众所周知，计算机病毒对计算机安全带来的威胁是极其严重的。它能产生破坏计算机磁盘文件分配表，造成磁盘信息丢失；破坏程序和数据文件或覆盖文件；格式化或删除所有或部分磁盘内容；造成磁盘产生大量虚假坏簇；产生垃圾文件造成磁盘存储空间变小；破坏硬盘主引导扇区使计算机无法启动；破坏屏幕正常显示，干扰打印机和键盘输入；影响系统运行效率甚至引起系统崩溃等等不良后果。

有道是，世间万物都是相生相克的，杀毒软件的出现使得计算机安全有了保障，病毒再也不能为所欲为了。这些年来我国一直在反病毒方面处于优势地位，国内反病毒技术，从产品形成发展至今已具备相当的市场规模，许多大公司也都陆续推出了自己的防毒杀毒产品。这些软件的技术、售后服务和杀毒效果都很不错。用户在选择此类软件时，除了关心价格和杀毒效果等因素外，像是否通过公安部检测认证、是否识别 MAIL 压缩格式、是否具备完善的内存解毒功能、能否迅速在线智能增量升级等方面也是十分重要的。不过需要特别注意的一点是，千万别使用盗版或是经过破解的杀毒软件！此类软件不光在杀毒效果方面大大降低以外，还存在其它一些问题。我的一位朋友曾使用过盗版的杀毒软件碰到了一些问题，后经检查发现，此软件被一些别有用心的人修改，虽然也能使用但其已经具备木马特征，能够在用户不知情的情况下窃取用户电脑中的机密资料并不定期的向外发送。笔者也碰到过多次因使用破解过的杀病毒软件而将硬盘锁死的情况。在此，再次忠告各位，至于杀毒软件，无论如何要到正规渠道购买正版的，千万不要图一时之利，以免到时后悔莫及。花两三百元保护价值几千元的电脑，还是值得的。

但仅仅光靠杀毒软件还是远远不够的，病毒的传播速度之快，传播范围之广再加上新病毒的不断产生，完全可能在你不经意期间进入你的计算机侵蚀你的系统；所以我们必须要具备完善的计算机安全意识，这样才能做到防患于未然。对于我们来说，一定要养成不乱用外来磁盘、不乱下载文件、不打开不明程序、不使用盗版或经破解的杀毒软件、不进入不安全网站、定期升级杀毒软件进行查杀病毒等良好习惯。如果遇到计算机蜂鸣器发出异常声音或音乐、正常的外部设备无法使用、文件的日期时间或长度发生变化、磁盘读写异常、屏幕出现一些无意义的画面或信息、以往能运行的程序发生错误、系统运行速度忽然明显变慢等情况，应立即关闭计算机，用干净的杀毒软盘引导机器进行查毒或杀毒，以将损失降到最低点。

计算机安全问题是一个永久的话题，计算机病毒的真延是不分国界的，只要计算机应用不能发展和普及，计算机病毒和利用计算机犯罪的现象就会不断产生，计算机的安全就会受到威胁。这是环以人的意志为转移的。我们必须对此予以高度的重视并保持高度的警惕性，在实践学习中不断提高和进步，使计算机的安全得到真正的保障。

胡辉民

中国计算机报

2001年5月24日

谨防网络窃贼

据北京晚报2001年5月5日报道，海淀公安分局刑侦支队于4月29日破获了北京市第一起利用“黑客”手段在网上盗窃、贩卖上网账号的特大案件。犯罪嫌疑人，某大学计算机系的学生卢某被抓获归案。该生盗用某信息技术有限公司163上网账号，自今年1月份起，该公司累计损失共40余万元，仅1月20日这一天，其费用就高达5.2万余元。据悉，卢某将盗来的账号和密码送给他人使用，并在网上发布广告十余次，以每3个月100元的价格向他人出售上网账号和密码。

这只是众多网络盗窃案件的一例。据有关部门介绍，仅“某热线”近2年来因用户名和密码被窃取使用，用户拒付费用的金额就有200多万元。由此可见，窃取用户名和密码上网的现象已成为带有一定普遍性的社会问题。给网加“网”，已迫在眉睫。

据电信部门的不完全统计，目前，网上偷窃主要的非法入侵手段有两种：技术窃取（俗称黑客）和一般窃取。前者所花费的时间、精力比较大，而且成功率又非常低，使用的人很少。绝大多数违规者会选择后一种方法。从发现的一般窃取情况看，又以三类现象较常见：一种是在家中使用电脑时，用户名和密码无意间被旁人看见，最终被他人使用；二是电脑公司人员来家中安装、维修电脑时，顺手牵羊，将私人的用户名和密码窃取，有的是自己使用，有些人却进行买卖，一般是数十元一个用户名和密码，这占此类现象的40%；三是发生在大学寝室内，同学间窃取用户名和密码的现象普遍存在。

家庭用户的用户名和密码被窃取并加以使用，一般来说，较公司容易发现。由于有的公司电脑每天24小时都处在使用状态，他们对如何防止公司电脑上网的密码被窃取这个问题看得较淡。因此他们的损失程度可能远远大于个人用户。公司电脑的用户名和密码被窃取，大致也可分为两种：一是公司员工辞职后，在家中仍照旧使用原公司电脑的用户名和密码；二是公司员工将单位电脑的用户名和密码告诉亲朋好友，让他们一起使用。

因此，用户必须增强自我保护意识，必须注意以下几方面的问题：一是要经常更改自己的密码；二是经常在网上查询自己近期上网情况，从及时发现自己用户名和密码是否被窃取；三是对于自己私人的用户名和密码要保密，不要随意告诉旁人。

当然，法制建设是维护社会正常秩序的有力武器，这其中自然也包括网络社会。虽然我们的法律法规对于网络犯罪这个新生事物，显得有些措手不及，但互联网并不是法律真空。根据1997年12月30日公安部发布的《计算机信息网络国际联网安全保护管理办法》第六条的规定：未经允许，进入计算机信息网络或者使用计算机信息网络资源的，以及其他危害计算机信息网络安全的行为，由公安机关给予警告，有违法所得的，没收违法所得，对个人可以并处5000元以下的罚款，对单位可以并处15000元以下的罚款；构成违反治安管理行为的，依照治安管理处罚条例的规定处罚；构成犯罪的，依法追究刑事责任。

但目前对网络犯罪的立法工作还远远跟不上网络及其技术发展的速度，公安机关依照这一《办法》处理的案子仅占一小部分。这使得某些案件由于电子证据不足而导致所受处罚较轻，有的不过是在一段时间内被禁止离开住宅或处以罚款。这在一定程度上助长了网络犯罪者的气焰，先进的黑客软件令现今的黑客们如鱼得水，叫人防不胜防，所以加强关于网络犯罪的立法及惩罚力度，已迫在眉睫。

网上犯罪应引起社会各方的关注。依法上网应该成为每一个公民的自觉行动，让我们共同努力，来净化网上的空气。

新民晚报 XINMIN EVENING NEWS

2001年5月17日

电子窃贼防不胜防

网友沙龙

一些网站容易受黑客攻击的原因，是其应用软件审核作业和探测黑客的过程需要耗费较多的时间。安全软件专家认为，在电子商务的网络零售站点内，全部的购物车应用软件中，估计有三分之一的程序设计容易被电子小偷采用调换价格标签的伎俩进行攻击。

亚特兰大的一家网络安全公司在进行调查中发现，竟有11个购物车应用软件存在上述问题，其中还有3个程序至今未打上补丁。许多网站甚至不知道自己存在易受攻击的漏洞，因为他们是雇请外来的软件设计师来建设他们的网站，自己根本不熟悉软件。

黑客往往会使用搜索引擎查找易受攻击的网站，实际上是在找隐含文件。这些隐含文件是程序员藏在网页中的使用说明，一般人无法看到，但通过点击网络浏览器中的“编辑页”命令，隐含文件就变得可以看见了。许多HTML编码器只是简单地把价格放在一个HTML隐藏标签区，而不是结合后端逻辑程序用数据库去核实商品的价格。所以，任何文本编辑器都能改变隐藏区的价格，如把999美元改成999美分。

网络安全分析家约翰·P估计，网络服务器受到的攻击中有75%是在应用软件级，而不是在网络级。虽然网络应用软件的弱点在几年前就被发现，在黑客的BBS上也有所讨论，但很少有解决这些问题的安全产品推出。因为大多数公司都把注意力集中在配置网络防火墙和为在网络上传输的数据加密技术上，很少有人对他们网站的应用软件予以足够的重视。因此，电子窃贼的空空妙手防不胜防也就不足为奇了。

肖佐