信息安全动态

6

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*

FBI 再次警告电子商务站点补漏防黑 3

网络骗钱没商量 3

网上诈骗谁都不能幸免？ 3

网络隐私保护危机四伏 4

Palm 掌上电脑有安全漏洞 4

小心你的电子贺卡——Outlook 又发现安全缺陷 5

当心“可汗”宏病毒 5

当心 Hybris 恶性病毒 6

蠕虫病毒传播全球 6

利用 Gnutella 下载音乐小心电脑病毒 6

爱虫病毒摇身变“婴儿” 7

“爱虫”卷土重来 Navidad 毒踪又现 7

爱虫新变种病毒强级警告 8

✧ 二、*案例篇*

东欧黑客大闹美国 11

东欧黑客卷走百万信用卡资料 12

美航空航天局电脑系统网页遭修改——黑客年仅 15 岁 12

东欧黑客攻击美商务网站 13

少年黑客闯入航天局 13

亚马逊近 10 万用户资料被曝光 13

黑客窃得 Amazon10 万用户资料 13

马来西亚官方网站遭黑客攻击 14

马来西亚政府网站遭到黑客攻击 14

菲律宾 12 家网站遭黑 14

巴激进组织哈马斯网站被黑 14

哈马斯网站被黑 15

“超级黑客”写程序半年提款三十万 15

江苏“超级黑客”自首 15

台报称大陆黑客进入台军事网站 15

黑客攻击 www.china－project.com 16

Sex.com 老板成为全球通缉犯 16

“裸妻”病毒可能源于巴西黑客之手 16

最“成功”入侵－红客“火烧”日本网站 16

✧ 三、*管理篇*

网络安全是必须解决的课题－－“两会”代表、委员畅谈信息产业发展综述之二 19

“两会”关注网络的“内容安全” 20

人大代表呼吁尽快制订《网络安全法》 20

人大代表呼吁网络安全法 20

人大代表关注网络安全 21

多方用力共建安全网 21

网络安全：值得关注的话题－－全国政协九届四次会议网络管理问题提案办理情况通报会侧记 22

网络安全建设是系统工程 23

强化信息网络安全成为热门话题 23

政协委员呼吁：要高度关注信息安全 24

政协委员呼吁：为网络加上“安全锁” 25

韦韦、王皓茹、吴庆洲委员提出建立信息产品安全鉴定委员会 25
俞云波等委员提出：上海一些网站安全意识淡薄 26
周晋峰委员：“垃圾邮件”太坑人 26
人行淮阴市中支计算机信息系统安全评估顺利完成 26
网上欺诈急增美国加强防范 27
ISP 对欧洲网络犯罪法不满 27
美国 HIPAA 条例略览 28

✧ 四、业界动态篇

2001 年数字化中国论坛即将开幕 31
第二届 3C 展 7 月在京登场 31
朗讯“接入技术论坛”在京举行 31
中科网威沪上展示产品 31
冠群金辰召开网络安全巡回研讨会 32
让网络安全无忧—NetScreen 三地巡展活动开锣 32
让网络更加安全无忧——美国 NetSreen 公司将举行宣传促销活动 32
电子商务方案征集活动在深举行 32
瑞星推出杀毒软件服务套餐 33
3.15 瑞星推出服务套餐 33
天创与“863”一起“辉煌” 33
移动互联关注安全 33
一个产品就是一个产业——能士主打安全 VPN 34
国内首个网络安全模拟实验室成立 34
IBM 在印度设立软件实验室 35
IBM 新出数据挖掘技术 35
方正数码网络安全产品首获公安部检测认证 36
方正软件成为冠群金辰网络版产品中国总代理 36
指纹识别破案屡建神功北大在宜昌演示活体采集 36
新 CA3+6 驾驭电子商务 37

CA 展示策略 37
电信选中 CA 产品 37
诺顿产品再度获奖 38
赛门铁克防病毒方案获嘉奖 38
FireGate 领安全“执照” 38
KVM 首度用于安全机构 38
微软公开“Web 窜改防范措施” 39
哈佛教授发明无法破解密码 39
电子商务两方案 39
无线网络无限生机 40
立为科技推出智能停车场管理系统 40
三维辨识技术可防黑客入侵 41
网宿推出新服务－VPN 41
Sybase 推出首个无线移动平台 41
优网通“电子监控”保安全 41
[认人]的笔记本上市 41
MCAfee 杀毒之星上市 42
基于 Web 的网络杀毒软件 42
网络在线杀毒新秀 HouseCall for Interanet 42

✧ *五、技术篇*

移动 Agent 的安全威胁及对策分析 45
网上银行的安全 50
移动 IP 中的安全威胁及对策 56
新的基于 IP 的网络智能 58
第三代移动通信与信号完整性问题 61
为何选择 MPLS VPN 技术 64
隧道技术及其应用 67
基于 ASP 应用程序的安全问题探讨 70

✧ 六、应用篇

山东省特约联行汇兑清算系统的设计 73

同城实时清算网络安全方案 76

建行吉林省分行综合业务网络系统的设计与实施 78

一个网络数据存储备份系统方案的设计与实现 81

网络备份方案选择与实施 86

IDC 解决方案 91

让服务更贴近用户——网达 IDC 解决方案简介 92

惠普 IDC 证券网上交易解决方案 94

广州市社会保险管理信息系统的应用与开发 98

上海公共交通卡系统总体方案 102

税务信息系统网络解决方案 107

建设企业网更上一层楼——大连机车车辆厂企业网的建设 108

接入扩容走新路 110

TCL 先行网络建设校园千兆以太网 112

从应用出发——首都经济贸易大学校园网设计方案 113

宽带智能小区解决方案 114

✧ 七、争鸣篇

被误解的安全概念———个信息安全工作者的疑问 117

信息安全管理体系及其构架 121

Windows 解密为哪般 123

黑客信条对网络世代德性构筑的启示 125

✧ 八、综合分析与对策研究

我国网络银行的发展战略探析 131

农业银行网上银行发展策略 134

人民银行天津分行管理信息系统的设计与实现 138

我国银行卡发展面临的问题及对策研究 143

金融电子化建设的回顾和展望 146
中国 IDC 的现状及前景 150
IDC，离我们有多远？ 152
IDC 从战略节点关注网络安全 158
海缆事件 IDC 市场的一次“考试” 158
进步的足迹——2000 年对应用最具影响力的 10 项技术 159
企业应用牵手 Linux 164
新观点：信息安全保险业务会出现吗？ 170

✧ 九、趋 势 篇

前瞻证券电子商务 175
银行的“网”越织越密 176
21 世纪 Web 数据库的发展 177
企业网络 Napster 化——P2P 网络市场及应用 179
WDM 技术的发展与智能光网络展望（一） 180
第三层交换技术及在 VLAN 子网规划中的应用 183
神奇的生物钥匙 184
2001 年杀毒软件厂家的[网战] 185

✧ 十、安全锦囊

为证券网络的安全支招 189
防火墙规则集的建立与网络安全 191
防火墙技术及选择（上） 193
防火墙——为企业护航 195
以需求确定 VPN 应用 201
多种 VPN 方案满足企业需求 202
嗅探网络漏洞 204
企业防毒什么功能最重要？ 204
网络安全不得不谈 205

邮件管理动起来 207
个人防火墙防“毒”拒“黑” 208
新一代互联网基础设施——互联网流理与内容管理产品一览 209

✧ 十一、其 它

成也黑客败也黑客 215
“毒”场的诱惑 217

警钟篇

- FBI 再次警告电子商务站点：补漏防黑
- 网络骗钱没商量
- 网络隐私保护危机四伏
- Palm 掌上电脑有安全漏洞
- 微软 Outlook 又发现安全缺陷
- 最新病毒警告

……

计算机世界

2001年3月19日

FBI再次警告电子商务站点

补漏防黑

美国联邦调查局(FBI)日前再次警告电子商务站点，要修补它们基于Windows的系统，以防止数据受黑客的攻击。

FBI在日前发布的一份文件中说，在过去几个月中，FBI国家基础设施保护中心(NIPC)一直在对有组织的黑客攻击电子商务站点的活动进行调查。有国外执法机构和私营企业官员参与的调查发现，美国20个州的40多家站点成为攻击的牺牲品。

调查发现，来自俄罗斯、乌克兰以及东欧某些地方的几个黑客组织，利用Windows NT操作系统存在的脆弱性侵入了美国的电子商务系统。Microsoft已经发布了修补这些脆弱性的程序包。

据FBI说，一旦黑客进入公司站点，他们就会下载专有信息、客户数据库和信用卡信息。然后，这些黑客再与受害公司联系，试图通过提供修补系统来勒索金钱。如果这家公司不付钱或者没有雇用该组织提供安全服务的话，威胁就会升级。调查人员还认为，在某些情况下，信用卡信息被出售给了犯罪组织。(IDG 电讯)

金陵晚报

2001年3月8日

网络骗钱没商量

全球去年网上欺诈16亿美元

本报综合消息 美国政府筹建了一家互联网欺诈投诉中心，该中心运行后的前6个月里共接到2万起投诉。该中心在3月6日发表的报告中称，约64%的投诉是在网上拍卖过程中产生的，其中拍卖成交后不送货的占22%。信用卡欺诈占5%，剩下的投诉包括投资欺诈和其他各类网上欺诈。据估计，2000年，全球利用网上支付方式进行欺诈所涉及的金额达16亿美元，其中多数欺诈发生在美国。

计算机世界

2001年3月19日

网上诈骗

谁都不能幸免？

根据来自Internet诈骗投诉中心(IFCC)的最新研究报告《Internet诈骗行为》，新技术的广泛采用为诈骗行为创造了新的机会，没有任何Internet用户能够幸免于难。

IFCC是美国联邦调查局和国家高级犯罪中心合作的产物。这份报告记录了2000年5月到2000年11月的网上诈骗犯罪行为。

这些诈骗行为中最多的是网上拍卖诈骗，占总数的近66%。居第二位的是订货之后不送货或者不付款的诈骗行为，占22%。另外有关信用卡和借记卡的诈骗行为也占到了5%。

这些诈骗行为造成的损失高达4600万美元，平均每个受害者损失894美元。只有17%的受害者的损失超过1000美元，大部分受害者的损失不到500美元。投资诈骗往往导致很大的损失。同时拍卖诈骗和借记诈骗最需要犯罪分子的智力，因而平均损失最低。

诈骗的犯罪分子主要是男性，其中92%是居住在大城市的美国人，其中17.3%居住在加利福尼亚。50%的受害者最初是通过电子邮件接触诈骗分子的，38%是通过浏览网页接触的。诈骗中主要的付款方式是信用卡和现金订单。(IDG 电讯)

生活時報

2001年3月13日

网事追踪

前黑客披露网络隐私保护危机四伏

由于目前互联网安全制度不够完善，人们的防范意识也较弱，因此在网上窃取他人信息简直易如反掌，有时就好像天下掉馅饼一样。曾经当过网络黑客的凯文·米特尼克近日为网络安全网站 SecurityFocus.com 撰写的专栏文章中如是说。针对安全隐患，米特尼克建议金融机构采纳除个人信息之外的其他方式对用户的身份予以确认。他说："政府及私营机构应该采取新的确认技术和方式，使得用户的社会安全号码或是出生日期等数据不再成为确认他们身份的主要依据，这样黑客才没有漏洞可钻。"

米特尼克撰文称，金融机构及各大网上服务公司用以确认用户身份的密码、用户名、社会安全号码、驾驶执照编号以及其他数据均可以在互联网上获取到。这位前黑客表示："很多政府及私营机构将公众的'私人信息'存储在互联网数据库里，但这些数据库的安全性令人怀疑，因此给了网上黑客很多机会窃取这些重要信息。正是因为万维网、大量在线数据库、搜索引擎以及公共文档的存在，才使得电脑黑客可以在更加便利的条件下获取他人信息。"

就目前而言，黑客窃取的他人信息主要用于进行信用卡欺诈，包括直接将受害者银行帐户里的资金转入自己的腰包里。米特尼克表示，一些专业黑客经常对网上的数据库进行搜索，以找到有关公众出生和死亡日期、家谱信息或是电话号码的站点，然后再对这些信息进行分析综合，以便为其确定最终的"被黑对象"打下基础。

据米特尼克称，还有一些黑客利用向美国邮政服务机构发送更换地址通知的方式来获取相关信息，他们冒充受害者以电子邮件的方式通知相关邮政机构自己的住址已改动，要求将相关私人信息转送给另外一家邮局，这样在受害者尚未弄清发生了什么事情之前，黑客已从另外一家邮局得到了受害者的全部信息。

米特尼克本人过去曾对多家政府及企业的官方网站进行过黑客攻击，造成经济损失上百万美元，他为此坐了5年牢，直到2000年1月份才获释。 朱文

中国计算机报

2001年3月15日

Palm掌上电脑有安全漏洞

许多使用Palm公司掌上电脑的用户都是通过设置密码的方法来保护自己存储在电脑中的重要个人资料的，但是最近有人发出警告称，在Palm掌上电脑中设置的密码根本起不到保护作用。据悉，Palm的操作系统软件存有"后门"，任何一个掌握了相应开发工具的人都能够打开Palm掌上电脑的加密数据。据悉，美国Handspring公司生产的Visor和日本索尼公司生产的Clie掌上电脑都已经使用了Palm公司的掌上电脑操作系统。

中国计算机报

2001年3月12日

小心你的电子贺卡

——Outlook又发现安全缺陷

Microsoft公司近日承认，其流行的电子邮件软件Outlook处理电子卡片有关生日数据的程序存在缺陷，它使电脑用户收到的电子贺卡中可能夹带恶性病毒，如“特洛伊木马”病毒。

利用这个缺陷，恶意电脑攻击者可以将特定数据存放在电子卡片生日字段中以电子邮件形式发出。用户一旦用Outlook 2000、Outlook 97、Outlook Express 5.01或Outlook Express 5.5打开邮件，随带的病毒代码就会使Outlook陷入瘫痪，用户只能运行黑客允许执行的程序，陷入其设下的圈套。

这种由计算机安全公司@Stake发现的软件缺陷，使收件人无法相信任何邮件附件。Microsoft主管程序安全的经理Scott Culp说，Microsoft已经和@Stake公司密切合作了两个多月以期尽快解决这个问题。

Microsoft推荐Outlook和Outlook Express的用户从公告的网站处下载相关的预防和修复工具。同时，Windows 2000 SP2和IE5.01和5.5套装中也将附带该工具。（IDG电讯）

2001年3月9日

当心“可汗”宏病毒

本报讯 日前，一家著名公司公布了最新病毒预告，其全球病毒监测网捕捉到一个名为“可汗”（W97M/Cham.A）的宏病毒，该病毒随Outlook传播。病毒运行通过Microsoft Word对象“ThisDocument.”中加载的宏“Document—Open”，并自动禁止“宏报警”。它每次感染Word模版都会将自身的名称改变，将部分代码加密。

“可汗”病毒会将自身复制到“C:\My Documents\<username>.doc”，每次运行都会产生大量的邮件，病毒会按照Outlook通讯簿中的所有地址发送邮件，主题为：“<username>—Curriculum Vitae”，附件为“C:\My Documents\”下感染的文件<username>.doc，username为接收邮件的用户名。

这家公司的技术专家提醒广大用户，该病毒集邮件病毒、蠕虫病毒和黑客程序于一体，破坏性十分严重，建议用户选择使用经过国际多家权威机构认证具备完善实时反病毒、查杀多种压缩文件功能的反病毒软件。

KILL系列防病毒产品的用户应及时到www.kill.com.cn下载最新病毒特征库以保护自己的计算机；或到KILL授权服务中心拷贝最新升级文件。KILL 21.10版本可以将该病毒清除。

金陵晚报

2001年3月5日

当心 Hybris 恶性病毒

据了解，Hybris是一种电子邮件病毒，在Windows环境下发作，该感染程序非常典型，它会修改WSOCK32.DLL，截取外发的信息，该蠕虫病毒会自动附加在受感染的邮件上，一旦收信人执行附件程序，蠕虫就会感染个人主机；在Windows System目录下生成一个WSOCK32.DLL的副本，副本的文件名是随机生成的8个字母，没有文件扩展名，由于病毒自身有修补连接、发送与接收数据功能，从而会感染这一副本文件；病毒还会修改Windows目录下的WININIT.INI文件，使下次Windows启动时原WSOCK32.DLL文件被覆盖。

有关技术专家提醒广大用户，该病毒集邮件病毒、蠕虫病毒和黑客程序于一体，破坏性十分严重，建议用户选择使用经过国际多家权威机构认证具备完善实时反病毒、查杀多种压缩文件功能的反病毒软件。

劳动午报

2001年3月17日

蠕虫病毒传播全球

午报讯 据《文汇报》报道，赛门铁克防病毒研究中心(SARC)的研究人员近日发现并确认了一种在欧洲蔓延的W32.Magistr.24876@mm电脑蠕虫病毒，该病毒于15日晚上传播到全球。

据专家介绍，这是一种具有电子邮件蠕虫特点的多形态电脑病毒，传播速度非常迅速。一旦被激活或执行，该蠕虫病毒会通过MicrosoftOutlook和Windows地址簿将自己发送到被感染用户地址簿中所有邮件地址，然后附上任意六个随机文件，同时随机生成一个包含多达60个字符的主题。据悉，这种病毒会感染除扩展名为DLL之外的所有可执行Windows文件，还会试图更改网络驱动器中的Win.ini文件。由于该病毒通过STMP处理器传播，所以它不必像其他蠕虫病毒那样需要通过MSOutlook或Netscape等电子邮件客户程序传播。

该病毒定义目前还正在破译中。专家建议，系统管理员应当立即把以VBS为扩展名的附件过滤掉，赛门铁克的用户可以通过诺顿防病毒的侦测功能修复该病毒引发的破坏，还可以在赛门铁克防病毒研究中心的网址www.sarc.com更新病毒定义。

(戴敦峰)

北京电子报

2001年3月12日

利用 Gnutella 下载音乐 小心电脑病毒

利用Gnutella系统下载音乐的网友可能面临病毒威胁。美国免费音乐交换网站Nap-ster的网友，若想转往其它音乐网站可得小心电脑病毒了。

这只别名"Mandragore"的电脑蠕虫试图伪装成用户想要的音乐或电影档案，用户若下载并执行这一伪装档案便会启动内藏的病毒，然后这种病毒常驻在中毒的电脑中，并散播给其他找寻音乐或电影档案的用户。

北京科技报

2001年3月9日

病毒提示

爱虫病毒摇身变“婴儿”

反病毒专家提醒，最新发现的“Myba”病毒是组成爱虫电码的 Visual Basic 脚本的一个改进版本，并且在许多方面完全相同。

该病毒作为电子邮件附件到达，标题是：“我的婴儿照片”，全文是：“这是我生气勃勃的婴儿照片(!)”附件为 MYBABYPIC.EXE。

如果这个文件被打开，一个婴儿的一幅照片就弹出，然后病毒多次将自己复制到 Windows 系统姓名地址录，并且增加注册表入口，允许它在 Windows 启动时实施。该病毒还重新散布自己到 Outlook 地址簿中建立的电子邮件地址上。

专家提醒说，Myba 能在计算机上轻易地毁坏重要数据。依靠当前的时间和日期，它能打开或关闭 NumLock、CapsLock 和 ScrollLock 锁钥。该病毒还向键盘缓冲器发送“.IM-BESIDES-YOU-”这样的信息，然后连上 www.youvebeenhack.com 网站，并且发送下面文本信息中的一个：“FROM BUGGER”、“HAPPY VALENTINES DAY FROM BUGGER”、和“HAPPY HALLOWEEN FROM BUGGER”。该病毒还侵占所有可利用的磁盘空间，用以下的扩展破坏文件：VBS、VBE、JS、JSE、CSS、WSH、SCT、HTA、PBL、CPP、PAS、C、H、JPG、JPEG、MP2 和 MP3。

克服这个病毒的校正措施，已经可以在大多数反病毒供应商的网站上获取。

杭州日报

2001年3月8日

“爱虫”卷土重来 Navidad毒踪又现

本周，一种新的“爱虫”病毒变种开始迅速传播，其附件是一个采用 Visual Basic 语言编写的可执行文件——MyBabyPic.EXE。邮件的主题栏写着“My baby pic !!!”，邮件的正文是“Its my animated baby picture !!”。这种病毒有两个特殊之处，一是它在本地的文件系统中进行自我复制后 10 分钟左右，才向 Outlook 地址簿上的每一个地址发出一封电子邮件，使用户在打开邮件当时并不能发现问题，起到了麻痹的作用。另一个特殊的是这种病毒还会生成一组文件，并加入到 Windows 系统注册表的启动部分，每当被感染的电脑启动一次，它就会自动执行一次，防不胜防。

另外，臭名昭著的圣诞节病毒 Navidad 出现了新变种 Navidad.B。这次，它显示的图标是 shockwave flash player 的图标，感染机器将在 Windows 的任务栏系统盘显示一个 ICQ flower 格式的图标。如果你从来都没有使用过 ICQ 那就肯定是中招了。

廣西日報
GUANGXI RIBAO
2001年3月8日

爱虫新变种病毒强级警告

最近，一种新的“爱虫”病毒变种开始迅速传播，这种病毒名叫“w32.MyBabyPic.worm”。这种病毒仍然是通过电子邮件传播（只能通过 Outlook 传播），附件是一个采用 VisualBasic 语言编写的可执行文件——MyBabyPic.EXE。邮件的主题栏写着“Mybabypic!!!”，邮件的正文是“Itsmyanimatedbabypicture!!”。如果接收者打开附件，将会看到非常低级淫秽的图片。

这种病毒拥有很强的危害性和隐蔽性，能轻易删除被感染电脑上的数据。根据目前的时间和日期，它还可以激活/关闭键盘上的 NumLock,CapLock 和 ScrollLock 键；可以向键盘缓冲发出“.IM_BESIDES_YOU_”信息，并发送不同的文本信息。并感染和破坏以 VBS，VBE,JS,JSE，CSS，WSH，SCT，HTA，PBL，CPP，PAS，C，H，JPG，JPEG，MP2 和 MP3 等为扩展名的文件。目前，金山公司位于珠海的反病毒监测中心已经捕获到此病毒，并进行了迅速的病毒样本分析，最新金山毒霸病毒升级包 2001.3.2 版本能实现对本次“爱虫”新变种病毒的查杀，金山毒霸的用户可到 www.iduba.net 进行版本升级。