信息安全动态

13

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、安全锦囊

警钟篇

- 信息安全：重中之重
- 信息安全影响我国进电子社会
- 台湾网络犯罪令人担忧
- 电脑病毒传染途径翻新
- 新型国产恶性病毒“陷阱”（相关 3 则）
- 微软产品安全问题（相关 4 则）
- 最新病毒警告（9 则）

……

北京日报

2001年6月27日

日前，国家科技教育领导小组在中南海举办科技知识讲座，邀请中国工程院院士何德全做“信息安全知识”报告。何德全院士分别就我国计算机信息网络的现状、如何做好计算机信息安全工作等方面做了介绍。朱镕基总理、李岚清副总理等出席听课。

信息安全 重中之重

我国信息安全综合得分5.5，介于相对安全和轻度不安全之间

据国家信息安全课题组的《国家信息安全报告》介绍，90年代以来，我国的信息产业和技术及互联网络等虽获得了突飞猛进的发展，但在信息安全领域还存在不少问题和缺陷。如以9分为满分计算，我国的综合得分数只有5.5分，介于相对安全和轻度不安全之间。在前不久举办的“信息时代的国家安全”研究会上，中国工程院院士何德全、中国科学院信息安全研究中心主任哪斯汉、中国国家信息安全测评认证中心主任吴世忠等一批专家学者对我国信息安全的现状提出了警示。

全社会的信息安全意识不很强

何德全院士在会上指出，在全球信息化面前，我国目前尚处于信息劣势。全社会包括一些政府机关，信息安全意识还不是很强。目前，对信息安全的关注呈现“两极”：专门从事信息安全研究的，认为漏洞不少，安全可靠性差；而不少人，包括从事IT业的许多人士认为，信息安全没有想象得那么严重。哪斯汉表示，我国的信息安全研究人员不少，但研究水平参差不齐，重点及关键项目不突出。信息安全产品的质量和性能可靠性不高，不适应大容量、多用户的信息化发展要求。中科院高能物理研究所研究员许榕生说，目前，我国的信息化正面临带动工业化、实现信息化、追赶知识化三重任务，在各地大力推动本地信息化发展的规划中，谈信息化建设的多，谈信息安全的少；谈如何推进信息化建设的多，谈如何应对信息安全的少。在我国准备建设大规模的宽带网之际，安全考虑还停留在早期的认识上。

信息安全威胁主要来自四方面

吴世忠认为，我国信息安全面临的现实威胁主要来自四个方面：一是内容的攻击，即网上充斥的大量反动的、不健康的、无意义的信息；二是泄密和内部人员犯罪；三是计算机病毒；四是黑客。受威胁较大的领域主要集中在三个方面：一是国家的关键性基础设施，包括国防、执法部门等；二是政府上网工程启动后，开展信息化的有关政府部门；三是经济信息网络，包括银行、债券等。从三个领域和面临的四种威胁看，我国信息安全的现状是讨论的多，做的少；许多的网络可能很容易被侵入，在技术的防范上，制度的管理上还没有形成一个实用化的体系。

表现在一是宏观管理上，多头管理，缺乏协调；二是微观上，管理措施较少，缺少一套行之有效的制度。同时，立法上的技术化和孤立化倾向不仅影响着信息安全立法的可行性，也影响着有关法规的可操作性。

据国家有关部门和权威人士介绍，我国目前的信息安全状况之所以不乐观，与信息安全技术不高，一些核心设备和技术尚依赖进口；网络安全人才短缺，整体素质不高，及西方发达国家给我们制造的“紧约束”环境有很大关系。此外，国民的信息安全意识淡薄，警惕性不高，也是一个非常重要的原因。

强化国家信息安全保障体系

在今年召开的“两会”上，信息安全问题就成为“两会”代表的一个热门话题。政协委员有关信息安全问题的提案就有40多个。提交今年人代会审议的“十五”计划纲要（草案），在将国民经济信息化和社会信息化作为重要的发展目标的同时，也特别强调要强化国家信息安全保障体系的建设。

朱镕基总理在听完何德全院士的报告后，发表讲话指出：在今后的产业结构调整中，我们要进一步加大对信息产业发展的支持力度，推进国民经济信息化的进程。同时，有关部门要认真研究制定信息安全的有关政策，采取有力措施，推进信息安全技术的研究和开发。 吴英杰 牛俊峰

China Industrial Economy News
CIEN产经新闻
2001年6月26日

信息安全影响我国进电子社会

专家提醒，如果不注意信息安全，“黑客”或敌国很可能利用网络攻击我国核心行业，使整个社会陷入瘫痪

本报讯 随着网络经济和网络社会时代的到来，我国的军事、经济、社会、文化各方面都越来越依赖于网络。与此同时，计算机网络上出现利用网络盗用他人账号上网，窃取科技、经济情报进行经济犯罪等电子攻击现象。今年春天，我国有人利用新闻组中查到的普通技术手段，轻而易举地从多个商业站点窃取到8万个信用卡号和密码，并标价26万元出售。同传统的金融管理方式相比，金融电子化如同金库建在计算机里，把钞票存在数据库里，资金流动在计算机网络里，金融计算机系统已经成为犯罪活动的新目标。据有关资料，美国金融界每年由于计算机犯罪造成的经济损失近百亿美元。我国金融系统发生的计算机犯罪也逐年上升趋势。近年来最大一起犯罪案件造成的经济损失高达人民币2100万元。

对我国金融系统计算机网络安全状况，目前有一些形象的比喻：使用不加锁的储柜存放资金（网络缺乏安全保护）；使用“公共汽车”运送钞票（网络缺乏安全保障）；使用“邮寄托寄”的方式传送资金（转账支付缺乏安全渠道）；使用“商店柜台”方式存取资金（授权缺乏安全措施）；使用“平信”邮寄机密信息（敏感信息缺乏保密措施）。在银行计算机犯罪案件中，最具破坏性的犯罪类型是篡改数据，而各银行对计算机数据的保护、操作密码保护和储户密码保护都缺乏有力的措施。

到目前，我国已发生了200多起利用计算机进行金融犯罪的案件。在老百姓普遍关注的证券市场，近来屡屡受“电脑黑客”的攻击。最大的一起电子犯罪事件是两年前，上海一“电脑黑客”入侵上海交易所某席位，盗卖了价值2.6亿元的股票。

公共网络轻易被攻击。据国内著名反黑客专家、中科院院物理所研究员许榕介绍，他与有关部门对国内多家网站的安全性进行测试，90%都存在着不同程度的安全问题，无法有效地抵抗电子攻击。去年，我国网络安全管理员就被美国黑客嘲笑为“只有12岁儿童的水平”。

电子攻击可分为三个层次。低层次威胁是局部的威胁，包括消遣性黑客、破坏公共财产者；第二个层次是有组织的威胁，包括一些机构黑客、有组织的犯罪、工业间谍；最高层次是国家规模上的威胁，包括敌对的外国政府、恐怖主义组织发起的全面信息战。

据悉，近几年来，我国利用计算机网络进行各类违法犯罪的行为在我国以每年30%的速度增长，仅去年就破获了黑客案件数百起。目前我国发生的“电脑黑客”事件，大多属于低层次的攻击事件。面对着最低层次的攻击行为，我们基本上还是无能为力，无从防范。那么，我们又能如何防范高层次的电脑黑客呢？

连续两次完成我国全国范围大规模信息产业调查的张爱国认为，如果不注意信息安全的话，“黑客”或敌国很可能利用网络对我国各个核心行业进行攻击，从而令整个社会处于瘫痪状态。信息安全，严重影响我国大步迈向网络时代，制约了国内电子商务的纵深发展。

（曾华国）

法制日报
2001年6月28日
http://www.legaldaily.com.cn

台湾网络犯罪形形色色 负面影响令人担忧

日前，台北县刑警队网络犯罪专责小组破获台湾首宗非法复制他人网页牟利案。警方已将从事复制的犯罪嫌疑人及非法使用他人网页的5家旅行社负责人依妨害著作权法罪移送法办，并将此案列为重大案例。

据台湾警方介绍，一位旅游网站的制作人日前向刑警队举报，称他制作的名为“神秘的塞班目录”网页，被一家旅行社擅自复制到他们的网站，并借此从事营利活动，严重侵害了他的著作权。刑警队电脑犯罪小组循线查出名叫刘永成的网民是擅自复制该网页的始作俑者，刘复制后再通过网络传给旅行社网站。警方继续侦查，查出有5家旅行社采用该网页为自己网站宣传页。

5家旅行社负责人到案后，均称刘永成欠他们债务，以帮他们制作网页方式抵债，他们不知道自己行为是侵权。

除网页侵权外，最近一段时间，台湾通过电子邮件或BBS散播谣言的数量暴增。许多谣言的受害商家损失惨重，其中包括统一、大黑松小倆口等著名厂商。

台湾许多“网民”都在网络上看到了这样一些消息，如“统一超商‘关东煮’都是味精”、“白兰氏鸡精用的都是淘汰鸡”、“大黑松小倆口牛轧糖里有蟑螂”等等，“新光人寿”则被传为“强迫B型肝炎患者退保”。这些谣言让业者痛苦万分，不停地“上网”消毒，但总显得有口说不清。

律师陈家俊指出，只要是“上网”传播或转寄含有不实之词的邮件的，就会涉及诽谤及妨害名誉罪，针对目前众多网站上的谣言流传的现象，应该成立申诉机构，还业者以清白。

台湾“刑事局”最近还逮捕了一名连续利用网络聊天室对女子诱奸并诈财的惯犯。现年38岁的梁倜伦因性侵犯、诈欺和流氓等罪被捕。该犯从去年年底开始在台北县市各地冒充法官，上网结交年幼无知的女网友骗财骗色，作案超过10起。

梁犯通过网络认识网友后，常假冒多家公司董事长、政府高层亲戚、法官等，以协助被害人找工作、帮助投资理财为由，带年轻女网友前往高级饭店诈财骗色，甚至让被害人刷卡支付现金供其挥霍。被害人往往误以为梁犯是豪门子弟，而任其摆布，直到被害人所有积蓄被榨干、身心受创才恍然大悟向警方报案。

在台湾，互联网络对社会的负面影响正在日益显现出来。据台湾ISP业者的最新统计，台湾每天上色情网站的超过70万人次，有85%的上网者浏览过色情网站。由于目前台湾中、小学近八成的学生都已学会使用互联网，所以，难以杜绝的色情网站对青少年构成了新的污染源，这已经成为台湾家长们日益头疼的一个大问题。

宗 和

中国青年报

2001年6月25日

病毒追踪

安全专家警告 电脑病毒传染途径翻新

安全顾问警告说，有两种以新型途径传染的病毒已经出现。

防毒技术专家日前指出，一种名为“God Message”的病毒可让黑客在网页上放上ActiveX程序代码，只要是使用IE的网友在不知情下连进该网站，就会受到感染。该病毒的压缩文件会被立即下载，然后潜伏在机主电脑中，在下次开机时即会被解压缩，然后依此方法继续传播。

据介绍，如果网站没有良好防护，就容易被黑客入侵，然后放置该病毒，“如果是MSN首页遭感染，大概全球有一半电脑一夜之间都会被感染。”

据悉，God Message依赖网络浏览器的漏洞而传染，但只要定时更新防毒软件，应该不会受到影响。

另一种叫Choke的病毒，则是透过即时传讯软件来传播，一经感染，它便会将臭虫传给“好友名单”中的每一部电脑。据悉，这种病毒可以躲过防毒软件，使用者无论是传出或接受到这种病毒都无法得知。

www.sina.com.cn

2001年6月25日

新型国产恶性病毒“陷阱”出现

本报记者 刘丽萍

国家计算机病毒应急处理中心近日通过监测，发现国内出现一种名为“陷阱”的新型恶性病毒。该病毒与前一阶段发现的“欢乐时光”病毒相类似，可以感染后缀为HTM，PLG，ASP，HTML和VBS的文件，造成网站感染，并可通过邮件传播，造成网络阻塞。目前，国内已有一些网站和用户遭受该病毒的感染，出现系统瘫痪、文件丢失的严重后果。

反病毒权威专家王江民指出，该病毒发作条件多样，并可直接摧毁硬盘数据，因此是一种危害相当严重的恶性计算机病毒。

该病毒属于一种脚本语言病毒，当感染该病毒后，病毒会修改系统注册表，并在默认值为C：WINDOWS上创建profile.vbs病毒文件。

如果当前操作的驱动器是硬驱或网络驱动器时，找到扩展名为HTM,PLG,ASP的文件，并且文件大小如果小于100000时，就感染文件最前端的Script文件，并删除C盘的Readme.html文件。

这一Script Worm在一些特定环境下通过Outlook邮件传播，向Outlook地址簿的用户发送邮件，附件为：Readme.html，并无条件向一些特定用户发送邮件。

而且，如果有C：\InerPut\wwwroot，就在index.html文件上插入病毒代码。这样，会直接攻击网站，造成网站感染。当用户浏览被病毒感染的网站时，同时会被病毒感染。

如果用户Domain、网络名、计算机名等名称中遇有特殊字符，该病毒将把删除C盘所有文件夹的命令插入到C：\AUTOEXEC.BAT文件，并在下一次重启计算机时，删除C盘所有文件夹。

当系统时间为7月5日创建75.htm文件，该病毒将利用Windows BUG来修改Internet Explore开始页面，因此一旦执行Internet Explore就会出现Blue Screen。

据悉，目前国内已有KV3000杀毒软件可查杀这一恶性病毒，专家提醒广大用户及时升级自己的杀毒软件，以免计算机系统遭受这一恶性病毒的损害。

深圳商报 SHENZHEN ECONOMIC DAILY

2001年6月26日

恶性病毒布下“陷阱”

我国发现一种新型计算机病毒，它先感染网站，后通过邮件传播

【本报广州25日电】(记者 古国真 通讯员 夏晓露) 省公安厅公共信息网络安全监察处今天提请广大计算机用户注意，日前，我国又出现一种新型的恶性病毒“陷阱”，目前国内已有用户遭受该病毒的感染。

据介绍，该病毒与“欢乐时光”病毒相类似，可以感染后缀为HTM,PLG,ASP,HTML和VBS的文件，造成网站感染，并可通过邮件传播，造成网络阻塞。

该病毒属于一种脚本语言病毒，感染该病毒后，病毒会修改系统注册表，并创建病毒文件。这一病毒在一些特定环境下通过Outlook邮件传播，向Outlook地址簿的用户发送邮件，附件为Readme.html，并无条件向一些特定用户发送邮件。

如果计算机硬盘中有c:\InetPut\wwwroot目录，即提供了web服务，就在index.html文件上插入病毒代码，直接攻击网站，造成网站感染。当用户浏览被病毒感染的网站时，同时会被病毒感染。如果用户Domain、网络名、计算机名等名称中遇有白宫、CIA、布什、USA等词，该病毒将把删除C盘所有文件夹的命令插入到C:\AUTOEXEC.BAT文件，并在下一次重启计算机时，删除C盘所有文件夹。

珠海特区报

2001年7月5日

专家提醒计算机用户

今天小心“陷阱”病毒爆发

新华社北京7月4日电 7月5日是“陷阱”病毒全面爆发日。有关专家今天在此间提醒广大计算机用户加强防范意识，及时升级杀毒软件消灭该病毒。

据了解，“陷阱”病毒与前不久出现的“欢乐时光”病毒类似，可以感染后缀为HTM、PLG、ASP、HTML和VBS的文件，造成网络感染，并可通过邮件传播，造成网络阻塞。该病毒属于一种脚本语言病毒，当感染该病毒后，病毒会修改系统注册表，并创建病毒文件。“陷阱”病毒具有较大的破坏性，它会导致使用WIN95、97或者98系统的计算机蓝屏，但在WIN2000下没有这个现象。

China Industrial Economy News
CIEN产经新闻

2001年6月26日

微软软件漏洞引麻烦 600万网站安全受威胁

本报讯 据微软公司(美国当地时间)6月18日宣布:已经被600多万家网站所使用的网络服务器软件中发现一个"危害性极大漏洞"。黑客或在线蓄意破坏者可利用这个漏洞来控制用户的电脑。

据发现这个漏洞的eEye数字安全公司的负责黑客事件的主管Marc Maiffre称,这个安全漏洞是在微软的互联网信息服务软件(IIS)中发现的。微软的IIS软件一般是由网络服务器默认安装的。Marc Maiffre称:"使用微软软件的服务器极易受到攻击。任何黑客都可进入电脑最高级的管理权限。"

微软在其网站上建议其用户立即下载一个新的补丁。微软的建议书中写道:"这是一个非常严重的安全漏洞。微软敦促所有用户立即采取行动,给这个漏洞打上补丁。"

微软的Windows NT、Windows 2000和Windows XP中都包含有IIS系统,且都有这个安全漏洞。换言之,这个漏洞会影响600多万家网站,约占全球21%的网站。

这个安全漏洞是在微软的IIS服务器的一个代码中发现的。这个主要是支持索引。这个模又名为Indexing Service ISAPI(索引服务ISAPI)过滤器。它不能正确检查缓冲器是否过载。这种问题在软件中经常遇到。据Maiffret估计,至少有50%的IIS服务器仍然使用的是默认设置。

最近微软的软件的漏洞可谓层出不穷。微软三次为Exchange的电子邮件服务器打补丁。据微软称,只要用户用上最新的补丁,就可解决后顾之忧了。并表示正在为Windows XP操作系统打补丁。

(丽 瑜)

2001年6月25日

微软产品又出安全隐患

本报讯 微软(德国)公司发言人鲍姆加特内尔19日在德国慕尼黑宣布,微软公司开发的"互联网信息管理器"5.0版有重大安全隐患,微软公司为其定的警报级别为红色。

鲍姆加特内尔介绍说,这个软件可以与各种版本的"视窗"软件配合,用户可以利用这个软件建立自己的网页。但是如果有"恶意黑客"向其发送的信息数据量过大,超过了该软件的承受能力,软件就会再现安全漏洞。黑客就能够掌握有关的计算机,进行比如消除硬盘等破坏。

目前,微软公司正在向"互联网信息管理器"正版软件的用户发出相应警报,并指导其从网上下载相关程序,堵塞软件中的这一安全漏洞。

计算机世界报

2001年6月26日

宏病毒在Word里"没完没了"

微软公司上周四称,在该公司流行的Word字处理软件中存在的一个安全漏洞,使得宏病毒可以在没有警告的前提下自行执行。

微软公司已为此发布了补丁程序并劝告客户立即应用。从Word97到Word2002各个版本都有此漏洞。早期版本的Word也可能有这种漏洞,但微软公司不再提供技术支持。

Word字处理软件中包含一种安全机制,当Word文档中含有宏病毒时,系统能自动发出警报。这次发现的安全漏洞使得一些恶意用户能够修改Word文件,使Word字处理软件中的安全扫描器无法识别嵌入在Word文件中的宏。

结果,当用户打开文件时,宏就可以自动执行。宏命令是简单而功能强大的一连串Word命令,能被嵌入在Word文件中,可在用户操作的计算机上执行任何命令。合法用户依赖于宏命令自动地执行例行性任务。病毒作者也经常使用宏命令。1999年在全世界传播的梅丽莎病毒就是Word宏病毒。

Word字处理软件中的宏检查漏洞是由一位名叫Steven McLeod的独立的安全顾问发现的。他在4月向微软公司报告了这个问题。他说,在用户能够保护自己之前,他不打算公布如何制作通过漏洞,使Word宏扫描器文件失效的细节。

经济信息时报
ECONOMIC INFORMATION TIMES
2001年6月19日

新型病毒专门攻击Word用户

有反病毒研究人员表示，微软Word中的一个安全漏洞使PC用户有遭到一种新的特洛伊木马病毒攻击的危险。

这种被称为Goga的病毒把自己伪装成一个保存为Rich Text Format格式的文件，但它实际上会通过互联网运行一个存储在一家俄罗斯网站上的Word宏。据首先发现这种病毒的英国反病毒软件厂商Kaspersky Labs称，这种特洛伊木马病毒以保存为RTF格式文本文件的电子邮件附件的形式出现。

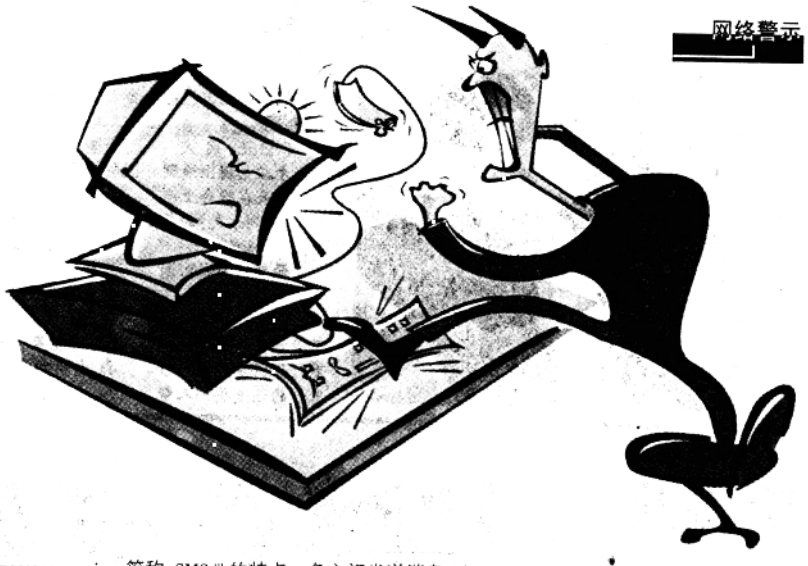
如果打开该附件，RTF文件将与一家俄罗斯网站上的一个Word模板文件连结起来，模板文件可以把被感染的计算机中的地址簿的登录口令等信息传到另外一个网站上。对该网站进行调查后发现，这种病毒还没有大面积地流行。把一个宏以模板的形式保存在另外的计算机上，特洛伊木马病毒就能骗过Windows，使宏得以运行，而不会被认为存在潜在的危险性。

安全专家认为，由于不是在计算机之间互相传播的，Goga不应该被认为是一种计算机病毒或者蠕虫，但它表明，计算机用户不能信任任何形式的电子邮件附件。

音乐LIFE生活报
2001年6月20日

网络警示

无线有线都一样 病毒将随SMS游动



短信息服务 short message service，简称：SMS〃的特点是能让移动电话用户相互发送简短的文字信息。尽管我们理应用移动电话来做一些更复杂的事情，因为曾有人向消费者许诺，移动电话将可以接入互联网、收发电子邮件，并能在移动电话和其他与无线应用协议 WAP 等时髦辞汇相关的设备之间进行无缝通讯。

事实上就连 WAP 也没多少人用，也许对于普通人来说，他们只用那些方便沟通的东西，SMS 持久的魅力也正在于此。当然，SMS 爆炸式的发展也给 SMS 带来了一些不利因素。主要的担心是：病毒。为了让人安心，防病毒软件制造商们说，迄今为止，尚无有关全球移动通讯系统〃GSM〃病毒的证据，尽管已有个别的事件发生，有报告称文字信息会莫名其妙地锁住键盘或通讯录。

SMS 最初是为技术人员设计的信息服务，它所具有的灵活性使它不仅可处理文字，还能处理其他二进制数据，如发送电话铃声等。它还支持信息传播，这为第三方服务打开了大门，如股票报价或发布体育比赛的得分等，只要营运商同意交换 SMS 信息，用户能低价向全球发送信息，也可以在电话与 ICQ 等以互联网为基础的信息服务之间发送消息。

由于 SMS 的多份拷贝的能力，很容易发生同时向大量移动电话用户发送垃圾邮件的情况。一封针对某人的 SMS 炸弹可能带给他来自营运商的额外收费，使他的电话死机。事实上较为先进的电话显然容易受到攻击：去年，日本的 NTT 移动通讯的 i－mode 系统就受到了一种负载在信息上的病毒的攻击，这种病毒会在用户不知道的情况下拨通急救号码。随着移动电话更加先进，使用更广泛，它们成了更受骇客青睐的目标。据 Trend Micro Inc. J. TDM〃的防病毒研究负责人乔·哈特曼 Joe Hartman 说，病毒作者已经相互挑战，看谁先编写出移动电话病毒。

由于没有可取代的新技术，预计 SMS 会进一步进入你的生活。将于今年下半年推出的拥有拓展式信息服务 EMS 的移动电话将在 SMS 文本模式的基础上，增加不同字体、图像、旋律和动画。虽然大多数人都不会因为信息上增加了有趣的音响和跳舞的圣诞老人就欢喜不已，但它意味着不用慢吞吞的 WAP，我们也能获得互联网式的内容，它也应该更便于操作。

文/安 吉