信息与网络安全研究新进展

全国计算机安全学术交流会论文集

第二十三卷

主办单位

中国计算机学会计算机安全专业委员会

中国科学技术大学出版社

信息与网络安全研究新进展

全国计算机安全学术交流会论文集

第二十三卷

主办单位

中国计算机学会计算机安全专业委员会

中国科学技术大学出版社

·合肥·

图书在版编目（CIP）数据

信息与网络安全研究新进展：全国计算机安全学术交流会论文集.第23卷/中国计算机安全专业委员会组编. —合肥：中国科学技术大学出版社，2008.9
ISBN 978-7-312-02277-7

Ⅰ.信… Ⅱ.中… Ⅲ. 计算机网络—安全技术—中国—文集 Ⅳ.TP393.08-53

中国版本图书馆 CIP 数据核字（2008）第 148767 号

中国科学技术大学出版社出版发行
（安徽省合肥市金寨路 96 号，230026）
合肥现代印务有限公司
全国新华书店经销
开本：889×1194/16 印张：28.75 字数：850 千
2008 年 9 月第 1 版 2008 年 9 月第 1 次印刷
印数：1—1000 册
定价：188.00 元

前　言

2008 年对我们国家来说是极其特殊的一年，既有“1.25”南方凝冻灾害给地方经济带来的灾难，又有“3.14”事件给社会稳定带来的冲击，还有汶川大地震给人民群众带来的创伤；更有北京奥运会给中国带来的历史性的机遇，让中国站在了改革开放的一个新的起点。在这特殊的一年里，这一系列特殊的事件都紧紧地围绕着这样一个术语：“安全”。凝冻灾害涉及的是经济安全，“3.14”事件涉及的是政治安全，汶川大地震涉及的是人身安全，北京奥运会涉及的是信息安全。事实上，所有这些事件，都与我们的学术领域密切相关：凝冻灾害需要的是应急处理与通信安全技术，“3.14”事件需要的是信息内容安全技术，汶川大地震需要的是系统容灾与数据灾备技术，而北京奥运会需要的则是网络安全技术。

在举世瞩目的北京两奥会闭幕之后的一个月，由中国计算机学会计算机安全委员会主办和中国电子学会计算机工程与应用学会计算机安全保密学组协办的第 23 届全国计算机安全学术交流会将于 10 月 12 日至 14 日在上海松江举行。我们从征集到的各位同仁一年来辛勤工作的结晶——学术论文中，细心遴选了 88 篇论文汇编成《全国计算机安全学术交流会论文集（第二十三卷）》呈献给大家。

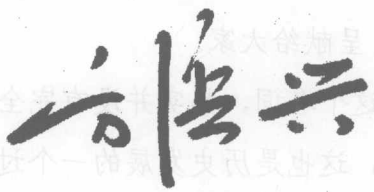
计算机安全这个名词，其实并没有完全包含我们这个领域所从事的全部内容。之所以称之为计算机安全，这也是历史发展的一个过程。众所周知，早期人们所关注的信息安全实际上是数据安全的内容，就是在信息传递过程中要保证所传递的信息不被窃密、不被篡改、不被伪造，不被抵赖，所以也称之为通信安全。到了六七十年代，随着计算机以多用户的形式被更为广泛的人员所使用，计算机系统自身的安全以致计算机内部的信息安全（或曰数据安全）则显得重要起来，因此，围绕着对计算机系统结构、计算机软件以及计算机应用等技术研究的同时，计算机安全技术也被推动起来。与此同时，计算机机房等物理设施也存在着安全保护的问题，因此人们也同时关注着物理安全的问题。到了八九十年代，随着网络技术的普及，计算机系统的问题开始演变成网络的问题，因此计算机安全实际上已经演变为网络安全，但由于历史的原因，我们的计算机安全专委会的名字并没有变成网络安全专委会。到了世纪之交，信息内容安全开始得到了普遍的关注，内容安全也被认可为信息安全的主要研究

领域之一。因此说，尽管我们这个专委会仍然保持着传统的计算机安全专业委员会的称谓，但实际上我们所关注的领域已经贯穿信息安全的各个层面，包括物理安全、网络安全（系统安全、计算机安全）、数据安全（保密）、内容安全。所幸的是，从会议投稿内容的分布情况来看，大家也认同这一观点，因此，本论文集也囊括了所有的上述各领域的内容。

近一两年我们国家的信息安全工作，站在政府需求的角度来看，将会是以科学发展观为指导，立足于贯彻加强中央信息安全保障工作的意见和国家信息安全“十一五”规划，着眼于提高信息网络保障水平和信息安全防护的能力，全面推进信息系统等级保护工作，全面加强互联网安全管理。希望本论文集能对各位同仁有所帮助。

感谢第 23 届全国计算机安全学术交流会的承办方——公安部第三研究所对本次会议和论文集所做的努力。

中国计算机学会计算机安全专业委员会主任



二〇〇八年九月

目　次

2008年上半年网络安全形势分析报告

张 鑫[1,3] 张 健[1,2,3]

[1]国家计算机病毒应急处理中心，天津市 300457

[2]南开大学信息技术科学学院，天津市 300071

[3]天津市公安局公共信息网络安全监察总队，天津市 300020

摘 要：本文通过对2008年上半年网上计算机病毒、木马等恶意软件的传播和发展情况以及网络犯罪和黑客活动情况进行分析和研判，总结2008年上半年网络安全发展形势。并对2008年下半年网络安全发展趋势进行分析和预测。

关键词：计算机病毒 黑客 网络犯罪 发展趋势

Situation Analysis of Network Security in First Half Year of 2008

ZHANG Xin[1,3] ZHANG Jian[1,2,3]

[1]National Computer Virus Emergency Response Center, Tianjin 300457

[2]College of Information Technical Science, Nankai University, Tianjin 300071

[3]Department of Pubic Network Security Supervision, Tianjin Police Bureau 300020

Abstract: Through analyzing data of malicious software propagation and development, as also the situation of cyber crime activities, we concluded the circumstances of network security in the first half year of 2008 in China. In addition, we made a lot of research on analyzing and forecasting the trends of network security in the last half year of 2008 in China.

Key Words: Computer virus hacker cyber crimes trend

基金资助：国家高技术研究发展计划（863）（课题编号：2007AA01Z450）

作者简介：张鑫（1979— ），男，天津市，助理工程师，硕士 Email:zx@antivirus-China.org.cn

张健（1968— ），男，天津市，高级工程师，博士 Email:zj@antivirus-China.org.cn

1　近年来我国网络安全形式分析

近年来，系统漏洞、网络病毒、垃圾邮件、黑客攻击频频发生；网络色情、淫秽、暴力等有害信息普遍存在；信息系统瘫痪时有发生；由经济利益驱动的网络犯罪在全球日渐猖獗；恐怖组织、极端势力和邪教组织利用互联网渗透和扩张；个人信息及国家敏感信息泄露事件频发。病毒制造、传播者利用病毒木马技术的网络盗窃、诈骗活动，通过网络贩卖病毒、木马，教授制作病毒、木马和各类网络攻击技术等方式非法牟利的犯罪活动明显增多。严重威胁我国互联网的应用和发展，网上治安形势异常严峻。下面我们将对 2008 年上半年的计算机和网络安全情况进行深入的分析。

2　近期计算机病毒等恶意程序的形势分析

通过对互联网的监测发现，2008 年上半年全国没有出现大规模的网络拥塞和计算机病毒疫情,但病毒感染计算机的数量呈现大量增加的趋势。由于经济利益的驱使，目前病毒、木马的行为往往带有目的性，并且控制大量计算机成为黑客作案的有力工具。病毒传播的主

2.1　木马将成为主要威胁并迅速发展

由于“经济利益”的驱动各种盗号木马蓬勃发展，各类网络金融机构、网络游戏、网络交易平台等都成为了黑客的主要目标。网络挂马成为木马传播的主要手段并且出现“批量挂马”和“批量下载”等新方式，当脚本木马侵入网站服务器之后，就会自动搜索硬盘上的所有网页文件，在其中批量插入网页木马，这样，当用户访问带毒网站时，就会被病毒感染。而且通过这种方式传播的，大部分都是“木马下载者”类的木马，当用户在不知情的情况下，下载运行了该木马后，还会继续批量下载其他各类木马感染用户计算机。这样一来，黑客挂马、传播木马、盗窃密码账号自动化越来越多形成有效的循环，效率大大提高，成本降低，盗取各类信息的成功率增大，其危害越来越大，防不胜防。

2.2　新型混合型病毒的攻击

混合型病毒将成为网络传播计算机病毒的主要类型。这类病毒综合了当前流行病毒的大部分功能，结合了蠕虫和木马病毒的特点，能自动传播且传播手段多样，会感染一些特殊格式文件的代码（如：exe、html 等），并且具有 ARP 欺骗和对抗安全软件的功能。它还会感染所有的网页文件，在文件中加入恶意脚本，但用户在查看这些文件时就会下载其指定恶意代码。尤其是一些网站的维护者在被感染后，很容易将被感染的文件传播到网络中去，成为网页挂马的一种手段。由于它结合 ARP 欺骗和对抗安全软件的功能，因此这类病毒对于局域网用户影响尤为明显，局域网中所有的计算机很快被恶意代码感染，所以这种攻击方式具有极大的危害性。

2.3　针对于各类漏洞攻击的恶意代码将会增加

安全漏洞在各种系统中广泛存在，危害性与时间紧密相关。因此利用最新发现的漏洞进行零日攻击最具有威胁性。大量操作系统和各种应用程序的漏洞仍然是恶意用户发动攻击的重要途径之一，目前，病毒编制者主要利用的漏洞包括以下几类：

（1）操作系统漏洞

微软操作系统漏洞是黑客攻击的主要手段，因此微软操作系统漏洞成为黑客关注的目标。很多漏洞在微软发布补丁之前，利用该漏洞的攻击代码已经在互联网上传播，称为“0day”攻击。由于广大计算机用户未能及时安装补丁，因此这种攻击的成功率很高，危害性很大。

（2）应用软件漏洞

在压缩工具软件、办公处理软件，甚至各类安全软件也都存在安全漏洞，这些在互联网中广泛安装使用的各类软件所存在的安全漏洞造成的安全威胁不亚于操作系统漏洞。由于应用软件中存在的漏洞更容易被发现和利用。黑客们传播病毒机制已经从利用微软漏洞渐渐转向利用应用软件漏洞。应用软件漏洞已经成为黑客攻击的"新宠"，成为病毒发展的新趋势。

（3）Web 程序安全漏洞

这类漏洞包括 SQL 注入漏洞、XSS 漏洞等等，许多大型网站，包括 MySpace、谷歌和雅虎都曾经因为这些漏洞遭到攻击。病毒制造者侵入带有 Web 漏洞的网站，植入病毒。同时加强对博客的安全防

范，防止利用博客内嵌恶意代码，通过吸引用户访问来进行病毒、木马传播。

2.4 利用DNS服务器脆弱性的新型网络钓鱼将会出现

黑客可能利用“僵尸网络”对DNS服务器进行攻击，他们利用大量的肉鸡攻击想要仿冒的网站服务器，使该网站服务器瘫痪。然后黑客用自身建立的虚假的网站服务器向附近的DNS服务器发送大量仿冒的DNS包。欺骗DNS服务器更改DNS缓存，指向黑客指定的虚假网站，进行网络钓鱼诈骗。因为是针对于DNS服务器的攻击，广大计算机用户很难进行防范。

由于出现了多种针对DNS服务器的攻击方式，这种攻击方式主要针对的是防御措施相对薄弱的DNS服务器，属于DNS级别的攻击。这样用户不仅很难做出有效的防御而且在大多数情况下很难发现。

2.5 DDOS攻击成为网络致命威胁

DDOS是分布式拒绝服务攻击，黑客利用僵尸网络控制大量肉鸡（被攻击者入侵过或可间接利用的主机）向受害主机发送大量看似合法的网络包，从而造成网络阻塞或服务器资源耗尽而导致拒绝服务，分布式拒绝服务攻击一旦被实施，攻击网络包就会犹如洪水般涌向受害主机，从而把合法用户的网络包淹没，导致合法用户无法正常访问服务器的网络资源。这种攻击目前还没有很好的防御方法，已经成为互联网公认的致命威胁。

3 网络犯罪和黑客活动形势分析

网络犯罪案件数量近年来呈逐年上升的趋势，其中利用病毒等恶意代码窃取用户信息、敲诈用户财产成为网络犯罪的主要手段之一，同时，网上贩卖病毒、木马和僵尸网络的活动不断增多，且公开化。利用病毒、木马技术传播垃圾邮件和进行网络攻击、破坏的事件呈上升趋势。因此，种种迹象表明，病毒的制造、传播者追求经济利益的目的越来越强，这种趋利性引发了大量的网络犯罪活动，危及网络的应用与发展。

3.1 智能化的特点

计算机病毒犯罪是一种高智能的犯罪，更需要的是知识和技术或者说是脑力，而不仅仅是需要暴力和凶残。犯罪分子往往不仅懂得如何操作计算机的指令和数据，而且还会编制一定的程序，解读或骗取他人计算机的口令密码。

3.2 网络化的特点

计算机病毒犯罪网络化特点明显，利用计算机病毒犯罪不受时间地点限制，犯罪行为的实施地和犯罪后果的出现地可以是分离的，甚至可以相隔十万八千里。而且受害者一旦感染病毒，犯罪分子可以随时盗取其计算机内的重要信息。比如：犯罪分子在北京，而其挂马的服务器在上海，受害人则有可能在广州。这样从分利用了网络没有空间和时间限制的特点，给侦破工作带来极大难度。

3.3 隐蔽性的特点

隐蔽性包括两方面：一方面任何恶意代码都希望在被感染的计算机中隐藏起来不被发现，因为只有在不被发现的情况下，才能长期实施其破坏行为。为了达到这个目的，许多病毒使用了各种不同的技术来躲避反病毒软件的检验。另一方面，由于近几年对于网上木马的严厉打击，木马病毒等恶意程序制作者已成了惊弓之鸟，作案后很少还会留下蛛丝马迹。对于我们的侦查取证工作带来了巨大困难。

（1）网络犯罪分子抓住网络存在的技术漏洞和人们安全防范意识不强的环节，利用病毒、木马等黑客技术和网络欺诈手段，具有极强的隐蔽性。犯罪分子利用的木马和病毒，对被感染的计算机的系统影响越来越小，感染后几乎没有明显的特征，木马或病毒在机器中潜伏几个月甚至几年都有可能不被发现。当受害者发现网络银行或者重要信息被盗时，犯罪分子早就毁灭证据，逃之夭夭了。

（2）网络犯罪分子在网络一般都使用虚拟身份，并且使用网络通讯工具进行联系，犯罪分子之间也没有见过面，这使得很难确定其在现实生活中的真实身份。充分利用“虚拟社会”的特点，对于犯罪分子的抓获带来了极大的麻烦。

3.4 集团化、产业化的趋势

目前的病毒犯罪早已摆脱了独立的散兵游勇状的个人行为，而转变为并不严密但却绝对保密的小集团性质的集体行为，犯罪团伙组成有十到上百人不等。近期破获的几起病毒案，病毒团伙成员分工明确、组织严密各司其职，人员数量庞大，逐渐

形成了明显的病毒产业链：病毒木马编写者→专业盗号人员→销售渠道→最终玩家。

3.5　作案成本低，办案成本高

计算机病毒犯罪案件作案时间短、过程简单，可以单独行动，而且犯罪工具很容易获得，犯罪分子很容易就可以在网上下载或者购买的相关的木马或病毒。存在目击者的可能性很少，而且即使有作案痕迹，也可被轻易销毁，发现和侦破都十分困难。如例用黑客程序的犯罪，只要几封电子邮件，被攻击者一打开，就完成了，因此，不少犯罪分子越来越喜欢用互联网来实施犯罪，只需要坐在电脑旁，动动手指就能使资金往来。与此相反，公安机关只能采用跨地域侦查取证的办案方式，成本高、效率低。

3.6　DDOS 攻击可能成为网络犯罪的主要手段

DDOS 会对目标网络发起拒绝服务攻击，攻击者虽然没有直接获得利益，但攻击者可以令目标服务商减少收益或增加成本。从以前的一些案例中，我们知道，DDOS 有以下几种犯罪方法：

（1）网络黑社会的打劫

发现某家网站经营业绩好，黑客就会向该家网站收取所谓的“保护费”，如果不给，就用 DDOS 对其网站进行攻击，造成该网站网络瘫痪就会给其经营者造成重大损失。很多经营者无力解决这些问题，只好将保护费拱手送上。

（2）网络敲诈

某些不太合法，但收益还不错的网站，会成为黑客利用 DDOS 攻击的重点目标。比如：某些色情网站，赌博网站，网络游戏的私服。这些地方即使被攻击了也不敢向警方报案，只能向黑客妥协。

（3）网络恐怖组织

国外势力、敌对势力很能会利用其控制的僵尸网络，在某一敏感时期或重要活动期间，对国内重要单位网站或重要网络节点进行 DDOS 攻击，造成大规模网络瘫痪，形成网络恐慌，严重影响国内网络安全。

4　2008 年下半年计算机病毒、木马发展趋势预测

通过对上半年计算机病毒发展趋势的分析，目前我国计算机网络安全形势仍然十分严峻，计算机病毒表现出了众多新特征。反病毒行业面临着巨大的挑战，需要不断地研究并推出更加先进的计算机反病毒技术，做到“魔高一尺，道高一丈”才能应对和超越计算机病毒的发展，为个人计算机和互联网络的安全提供可靠的安全保障。

4.1　奥运将成为病毒用来传播的新热点

每次重大事件的发生或者重要节日的临近都会成为病毒传播的良机，举世瞩目的奥运会将在 8 月份召开，预计将会有大量病毒利用奥运热点进行传播。通过垃圾邮件和网页上关于奥运会的热点话题，吸引广大计算机用户点击，将会成病毒传播的主要途径之一。并且奥运相关的钓鱼网站预计在网络也会大量存在，利用中奖信息或者购票信息等奥运热门话题吸引计算机用户进行诈骗。

4.2　综合利用多种编程新技术的病毒将成为主流

从 Rootkit 技术到映象劫持技术，磁盘过滤驱动到还原系统 SSDT HOOK 和还原其他内核 HOOK 技术，病毒为达到目的所采取的手段已经无所不用其极。通过 Rootkit 技术和映象劫持技术隐藏自身的进程、注册表键值，通过插入进程、线程避免被杀毒软件查杀，通过实时监测对自身进程进行回写，避免被杀毒软件查杀，通过还原系统 SSDT HOOK 和还原其他内核 HOOK 技术破坏反病毒软件，其中仅映象劫持技术就包括“进程映像劫持”、“磁盘映像劫持”、“域名映像劫持”、“系统 DLL 动态连接库映像劫持”等多种方式。目前几乎所有的盗取网络游戏账号的木马病毒都具备了以上一种以上的技术特征，几乎所有最新的程序应用技术都被病毒一一应用，电脑一旦感染病毒，普通用户根本无能力彻底清除，只能求助专业技术人员。

4.3　下载者类病毒将成传播木马的源头

下载者病毒是近年来发展迅速已经成为病毒排行榜上的新星。该类型病毒与木马不同，一般本身并不具备盗取用户信息等行为，而是通过破坏杀毒软件，然后再从指定的地址下载大量其他病毒、木马进入用户电脑，进而通过其他病毒木马实现其非法目的。而且它还会根据黑客的指令经常改变木马的下载地址，以达到防止追踪和下载大量其他木马的目的。2008 年上半年发现的新病毒中下载者病毒增长最为迅猛，已经成为木马威胁的主要源头之

一。

下载者病毒可以说是病毒流程化入侵的第一步。一旦用户电脑遭遇下载器病毒入侵，通常电脑内将会发现几种甚至几十种木马，而且这些木马将几乎涉及市面上所有流行的在线游戏的盗号木马，危害非常严重。

4.4 ARP病毒仍将成为局域网的主要威胁

ARP病毒已经成为近年来企业、网吧、校园网络等局域网的最大威胁。此类病毒采用ARP局域网挂马攻击技术，利用MAC地址欺骗，传播恶意广告或病毒程序，使得ARP病毒猖獗一时。ARP病毒发作时，通常会造成网络掉线，但网络连接正常，内网的部分电脑不能上网，或者所有电脑均不能上网，无法打开网页或打开网页慢以及局域网连接时断时续并且网速较慢等现象。更为严重的是，ARP病毒新变种能够把自身伪装成网关，在所有用户请求访问的网页添加恶意代码，导致杀毒软件在用户访问任意网站均发出病毒警报，用户下载任何可执行文件，均被替换为病毒，严重影响到企业网络、网吧、校园网络等局域网的正常运行。

参考文献

[1] 中国互联网络信息中心．中国互联网络发展状况统计报告．www.cnnic.net.cn，2008

[2] 国家计算机病毒应急处理中心．2008年中国计算机病毒疫情调查技术分析报告，2008

[3] Roger Grimes．Malicious Mobile Code: Virus Protection for Windows.O' Reilly Media, Inc.; 1 edition (August 2001)

[4] Worldwide Economic Impact of Malware. Computer Economics ,June, 2007

[5] 国家计算机网络应急技术处理协调中心．CNCERT/CC 2007年网络安全工作报告，2007

[6] G. McGraw and G. Morrisett．Attacking malicious code: A report to the infosec research council. IEEE Software, 17(5):33–44, 2000

[7] http://www.microsoft.com/security/glossary.mspx

[8] Alisa Shevchenko, Malicious Code Detection Technologies,http:// www.kaspersky.com , 2008

2008年上半年互联网挂马报告，http://www.sucop.com/html/1216711564.html，2008

2008年中国计算机病毒疫情调查技术分析报告

张　健[1,2,3]　杜振华[1]　张　鑫[1,3]　舒　心[1]　梁　宏[1,3]
[1]国家计算机病毒应急处理中心，天津市　300457　[2].南开大学信息技术科学学院，天津市　300071
[3]天津市公安局公共信息网络安全监察总队，天津市　300020

摘　要：本文通过对2008年中国计算机病毒疫情调查数据的分析，得出我国目前计算机病毒的疫情特点、技术发展趋势，以及网络犯罪的新特征和病毒防治工作中存在的问题，并提出防治策略，促进我国信息网络安全的发展。

关键词：计算机病毒　疫情　防治　网络犯罪

2008 Technical Analysis Report of Chinese Computer Virus Survey

ZHANG Jian[1,2]　DU Zhenhua[1]　ZHANG Xin[1]　SHU Xin[1]　LIANG Hong[1]
[1]National Computer Virus Emergency Response Center ,Tianjin　300457
[2]College of Information Technical Science, Nankai University, Tianjin　300071
[3]Department of Pubic Network Security Supervision　,Tianjin Police Bureau　300020

Abstract: Through analyzing data of Chinese computer virus survey in 2008, we can conclude the characteristics of computer virus epidemic, technical trends and the new features of cyber crime, as well as the problems on computer virus prevention and control, then we propose the prevention and control strategies to promote the development of information network security in China.

Key Words: Computer virus　epidemic　prevention and control　cyber crime

基金资助：国家高技术研究发展计划（863）（课题编号：2007AA01Z450）

作者简介：张鑫（1979－ ），男，天津市，助理工程师，硕士　Email:zx@antivirus-China.org.cn
张健（1968－ ），男，天津市，高级工程师，博士　Email:zj@antivirus-China.org.cn

1 我国计算机病毒疫情网上调查简介

为掌握我国信息网络安全和计算机病毒疫情现状和发展变化趋势，宣传、普及信息网络安全知识，提高广大用户网络安全防范意识。自从 2001 年 4 月，由公安部主办了我国首次计算机病毒疫情网上调查工作以来，今年已经是第八次调查活动。每次调查活动，国家计算机病毒应急处理中心和计算机病毒防治产品检验中心以及国内、外各病毒防治产品生产厂家和计算机用户都积极参与。本次调查活动的主题是“共同关注信息安全、维护奥运网络和谐”。通过调查，全面了解、掌握我国目前网络安全现状，存在的问题，同时了解当前计算机病毒的种类、感染比例、分布情况和病毒防治工作中存在的问题。每次调查活动都极大地推动我国信息网络安全的发展，调查分析报告对提高我国信息网络安全水平具有指导意义。

2 我国当前面临的计算机病毒疫情

在过去的一年中，全球的计算机网络安全状况继续保持较为平稳的态势，没有出现大规模网络拥塞和系统瘫痪事件。我国网络安全态势也继续延续 2007 年的发展趋势，网上制作、贩卖病毒、木马的活动日益猖獗，利用病毒、木马技术的网上侵财活动呈快速上升趋势，这些情况表明我国网上治安形势严峻。

2.1 我国计算机用户病毒 6BD2 感染情况

截至 2007 年 12 月，我国互联网用户如图 1 所示，已经从 2001 年的 2650 万激增到 2.1 亿，人数略低于美国的 2.15 亿，位于世界第二位。截至 2008 年 6 月底，我国网民数量达到了 2.53 亿，首次大幅度超过美国，跃居世界第一位。同时，宽带网民数达到 2.14 亿人，也跃居世界第一，互联网大国规模初显。而我国计算机病毒感染率如图 2 所示，在去年出现较大反弹达到91.47%后，今年下降到85.5%。自从 2001 年以来，如图 3 所示，在受病毒感染的用户中，感染病毒 3 次以上的用户超过 56.65%，特别是 2003 年，感染病毒三次以上的用户数量有较大增长，曾经达到 83.67%，2007 年为 53.64%，今年为 66.8%，仍然维持在较高水平。

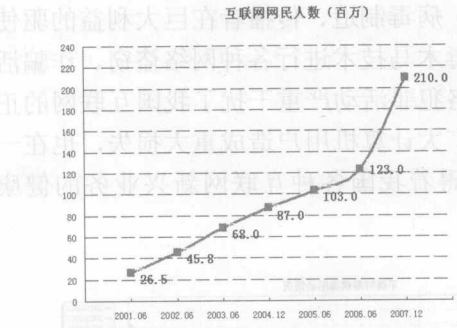


图 1 互联网网民人数

图 2 计算机病毒感染率

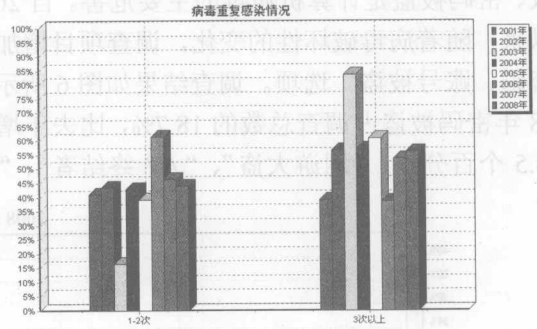


图 3 病毒重复感染情况

2007 年 5 月至 2008 年 5 月，全国没有出现影响全网运行安全的病毒疫情。自 2006 年 11 月至 2007 年 5 月，我国连续出现 “熊猫烧香”、“仇英”、“艾妮”等盗取网上用户密码、账号的病毒和木马。此次调查显示今年又先后出现 “AV 终结者”、“机器狗”、“磁碟机” 等病毒和木马。它们都具有对抗杀毒软件以及下载木马的功能，可以通过 ARP 攻击、可移动存储介质、网页挂马、感染 EXE 文件等方式进行传播，中毒后的受害程度取决于最终所下载的木马的功能，如：丢失网游账号、网银账号、

QQ 号、MSN 账号等个人敏感信息，而如果系统被灰鸽子等木马远程控制，还将丢失更多的个人信息或文档资料。病毒制造、传播者在巨大利益的驱使下，利用病毒木马技术进行各种网络盗窃、诈骗活动。这些网络犯罪活动严重干扰了我国互联网的正常秩序，给广大计算机用户造成重大损失，也在一定程度上阻碍着我国各种互联网新兴业务的健康发展。

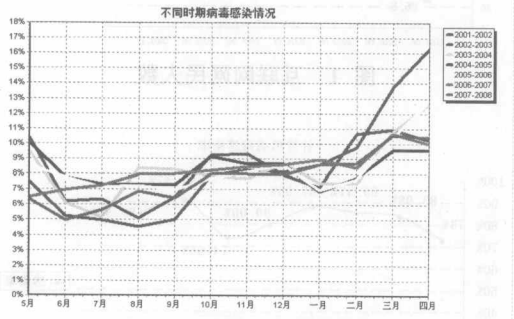


图 4　不同时期病毒感染情况

2.2　病毒的主要危害和发展趋势

今年调查结果如图 5 所示，系统（网络）使用受限或无法使用、数据受损或丢失、浏览器配置被修改、密码被盗是计算机病毒的主要危害。自 2006 年以来，随着病毒破坏性的变化，调查项目增加了“密码、账号被盗”选项。调查结果如图 6 所示，2008 年密码被盗占调查总数的 18.7%，比去年增长了 4.5 个百分点。“网游大盗”、“AV 终结者”、“磁碟机”、“机器狗”等病毒利用多种传播渠道进行传播并下载木马，攫取非法经济效益，给被感染的用户带来重大损失。脚本类病毒大量出现，主要为其他木马病毒传播起到“代理人”作用。如：JS.Agent、JS.RealPlr、JS.Psyme、HTML.IFrame 等病毒。这些病毒木马主要利用 Windows 系统、RealPlayer、百度工具栏、暴风影音、迅雷和联众等应用软件的漏洞通过网页“挂马”方式进行传播。其中黑客主要采用入侵网站和建立恶意网站进行“挂马”，垃圾邮件也与“挂马”相结合，垃圾邮件不再利用附件传播病毒木马，而是在邮件内容中含有指向“挂马”网站的恶意链接。当用户一旦访问“挂马”网页，用户的系统如果存在操作系统或者应用软件的漏洞，就会自动下载运行木马程序。另外，病毒木马制作工具化导致变种速度快，难于防范。同时，网上贩卖病毒、木马以及利用僵尸网络进行 DDos 攻击的活动频繁，且日益呈现组织化、公开化的特点。继“熊猫烧香”之后，复合型病毒呈增多趋势，这种病毒不仅具有传统病毒的传染文件的特点，还具有蠕虫、木马或者僵尸程序的特征，一旦感染系统更加难于清除。因此，种种迹象表明，网上病毒木马攻击技术不断提高，方式和手段日趋多样化，网上侵财活动日益增多。我们需要高度重视这一发展趋势，一方面提高用户安全防范意识，不断改进防护技术；另一方面不断增强对网络犯罪活动的发现和打击能力，遏制网络犯罪活动的上升势头。

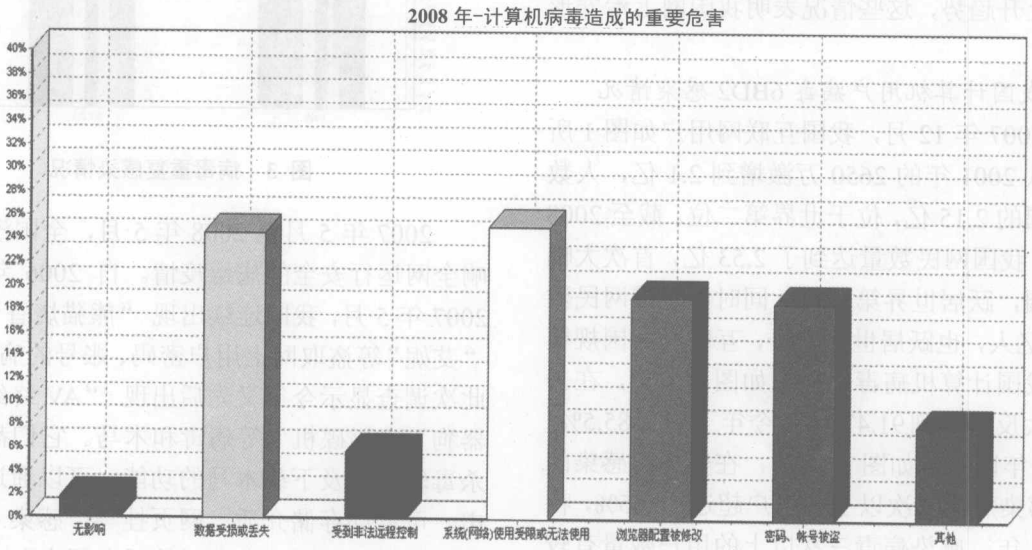


图 5　2008年计算机病毒造成的主要危害

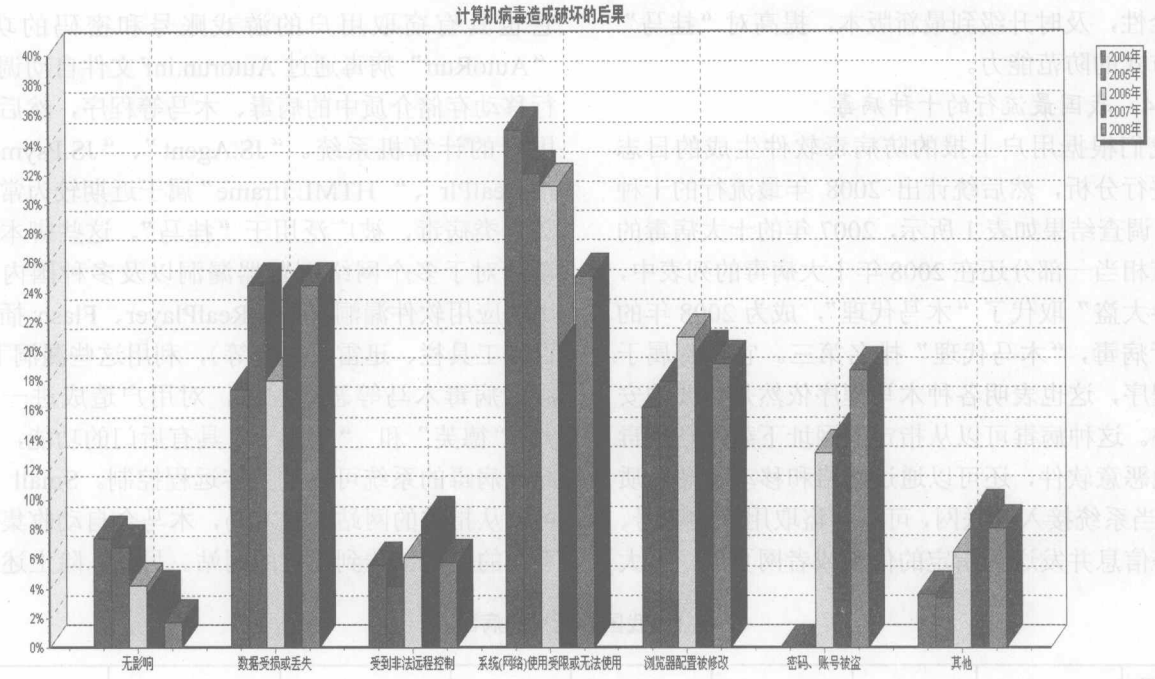


图 6 计算机病毒造成破坏的后果

2.3 我国计算机病毒传播的主要途径

我国计算机病毒主要通过网页浏览或下载、电子邮件、局域网和移动存储介质等途径传播。通过调查发现，病毒通过移动存储介质传播的比例有所下降，从2007年的33.99%下降到2008年的19.29%。由于优盘等各种类型的移动存储介质的广泛使用，病毒、木马通过 Autorun.inf 文件自动调用执行移动存储介质中的病毒、木马等程序，然后感染用户的计算机系统，进而感染其他移动存储介质。这种传播途径比例的下降表明我国计算机用户在移动存储介质的管理上有所加强，防护能力有所提高。但我们依然不能掉以轻心，还应继续加强管理，通过修改系统配置、关闭系统自动运行功能等方法，提高系统的安全级别。

今年的问卷调查结果如图7所示，通过网络下载或浏览感染病毒的比例相对去年有较大幅度上升，从2007年的9.17%上升到2008年的53.77%，是今年计算机病毒感染的主要途径。通过网络监测和用户求救的情况看，网络犯罪分子越来越倾向于通过网页“挂马”方式来传播病毒。“挂马”是指在网页中嵌入恶意代码，当存在安全漏洞的用户访问这些网页时，会自动下载、激活木马程序，然后盗取用户敏感信息或者进行各种攻击、破坏。这种通过网页浏览方式进行攻击的方法具有较强的隐蔽性，用户难于发现，因此，潜在的危害性较大。广大计算

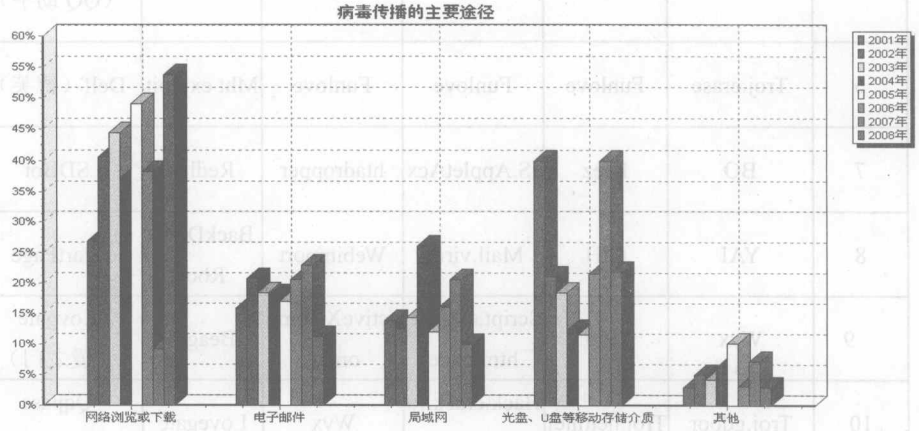


图 7 病毒传播的主要途径