信息安全动态

9

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、趋势篇

✧ 九、其它

警钟篇

- 中美黑客大决斗，网络安全告警！
- 国家有关部门提醒防范黑客攻击确保网络安全
- CIH 病毒是我国感染率最高的计算机病毒
- 小心网上陷阱
- 留神手机病毒
- 微软 ISA 软件存在安全隐患
- 最新病毒警告

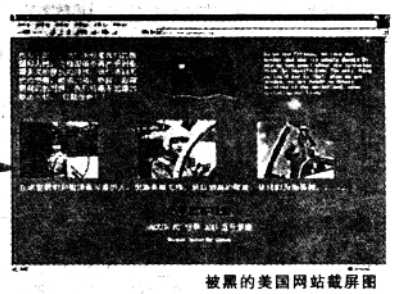
……

中国网友报
China Netizen News
2001年4月30日

“五一”中美黑客大决斗

网络安全告警！

文/本报记者 天 雨



被黑的美国网站截屏图

美国间谍飞机入侵中国领空一事由于美国方面的蛮横而至今仍未得到解决，与外交僵局相照应的却是中美黑客之间如火如荼的网络对决。

“撞机事件”后，中美两国网站每天都要爆发40到50起黑客攻击事件。美国黑客组织POIZONBOX对至少100家中国网站“毁容”，中国电脑黑客发下战书，将在“五一”长假进行大规模反击——

飞刀，又见飞刀

4月1日美军ep-3撞毁我军机后，网下的谈判起伏跌宕，网上中国民众爆发出强烈的谴责和愤慨。中国网友们不仅在各大网站上痛斥美国的非法和霸道行径，还出现了以美军肇事飞机命名的群情激昂的论坛——ep-3.com。而更具戏剧性的是出于义愤中国黑客的出击，一场轰轰烈烈的网络大战就此爆发。

有消息称，“中华黑客联盟”涂改了至少一家美国网站，并在至少十家网站上张贴了纪念王伟的帖子。有黑客涂改了美国海军的两个非保密站点，并在网站上发布了一些谴责美国的霸权行径和赞扬中国飞行员王伟的言论。

自称是“中华黑客联盟”的黑客“悟休”和“蓝色梦缘”袭击了一家位于美国加利福尼亚的网站Iplexmarin.com。网页上用中英文写着：“作为中国人，我们深爱着我们的祖国和人民。当祖国母亲再次受到帝国主义侵扰的时候，我们感到无比的愤慨，能说的是：“祖国！您需要我们的时候，我们将毫不犹豫地献出一切，包括生命！！”（见右上图）

然而美国人并未善罢甘休。美国黑客的报复接踵而至。美国一个名为“PoizonBOx”的黑客曾对域名以“.cn”结尾的部分网站进行了283次之多的攻击，其中绝大多数是最近两周进行的。一个以涂改网页著称的美国黑客甚至叫嚣说：“所有的美国黑客们联合起来吧！把中国的服务器全都搞砸！”对此，我国的网络安全人员积极防备美方黑客的攻击。

美国亚特兰大市X-Force网络安全系统公司的总裁克里斯·罗兰德称，自从美军侦察机撞毁我军战机事件发生后，中美两国的网站上每天都要发生40到50起黑客攻击事件，而撞机事件发生前的这一数字仅为一到两次。

中国黑客们正在为自己的反击作准备，他们将从5月1日起对美国网站进行为期一周的进攻。据称，此次进行的将是分布式拒绝服务器攻击。如果此次攻击真的实施的话，这将是近期以来第二次中国黑客对美国网站进行的联合攻击。上次攻击发生在1999年5月美国战机轰炸中国驻南联盟大使馆之后。美国白宫网站在那

次进行的分布式拒绝服务器攻击中被迫关闭了三天。

精神可嘉　切勿效仿

尽管中国黑客的行为让每一个有民族尊严的国人都感到扬眉吐气，但专家们仍然告诫民众和广大网民，互联网上的黑客行动并不能因为一时出发点的正义就值得鼓励和效仿。黑客行为的泛滥仍然是高悬网络社会头上的一柄达摩克力斯之剑，始终威胁着整个信息社会的安全。

黑客固然也能作出令人尊敬的举动，但他们的行为不能得到全社会的赞同。除了这个队伍自身的鱼龙混杂之外，最重要的原因，还在于黑客的行为标准太过唯心，缺乏社会的控制。其想行善即行善，而一旦作恶后果将不可收拾。一些观察家认为，黑客是人类自身隐秘心理的物化，是在非传统道德观念支配下的极端行为。黑客现象必须认真研究，但黑客的反主流乃至异端化的行为方式，绝对不能提倡和仿效，更不要说讴歌与礼赞。

信息安全　再敲警钟

根据安全人员对美国黑客的入侵过程分析，发现美国黑客并没有采用非常高明的手段，而大多是选择弱者，找那些安全防护措施做得很少的网站进行攻击。入侵者是利用 Unicode 远程漏洞获得系统控制权，多次远程执行命令，了解服务器结构后，修改网站主页。美国黑客的入侵再次为国人敲响了信息安全的警钟。

"我们的网络是脆弱的。"安全专家刘恒说，"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。""据我们的统计资料显示，现在90%以上的互联网存在严重的漏洞。国内一些敏感行业的网站，如政府机构、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人侵者获取系统的最高控制权。

中国青年报 CHINA YOUTH DAILY

2001年4月30日

刘洪波

中美黑客又要大战

"五一"节要到了，网上到处是中美黑客要大战的消息。昨日看了两条与黑客报国相关的报道，一条来自《中国青年报》，忧心"中美黑客开战了，谁来保卫我们的信息安全"，另一条来自千龙新闻网，称"第六次'网络卫国战'即将打响，中国黑客堪称红客"。

这两条报道合在一起看，就看出一点有趣，既然"红客"们要来一场"网络卫国战"，怎么"谁来保卫我们的信息安全"还是一个问题呢？难道他们原来是"卫"不了国的吗？如果这些"战士"只是一路冲杀向前，不顾别人抄了后路，端了老窝，以至他们要保卫的祖国的网站成了牺牲品，即使你要称他们为"红客"，他们自己也会有点不好意思吧。

幸好是在网络上玩，如果真正去到战场上，他们一直冲过去，却丧失了大本营，就真要叫人瓮中捉鳖了。不过，这也正是"红客"的本钱，因为他们虽然是在"卫国"，但终究不过是改改对方的网页就万事大吉，别人再攻过来，又不会叫他们受伤，至于中国网站将会如何，他们是不会负责保卫的。

这次中美黑客大战，或者说"中美红黑客大战"，引爆点当然是撞机事件。当然以前"红"黑客之间也交过手，说不定此前此后，红黑客们还要在一起交流一下技术。而这次撞机后是"红"黑双方哪一个先动手，我没有办法判断。美国黑客网站说是为了报复中国黑客的行动，黑了 100

多家中国网站，红客们似乎没有鲜驳。但红客很有信心在"五一"期间得胜回营，这个得胜当然是只计他们攻破美国网站，并利用这"敌后阵地"搞几分钟或几小时正面宣传（这才好说是"红客"，黑客只满足于"我们来过了"），而不计后面是否有中国网站遭殃。

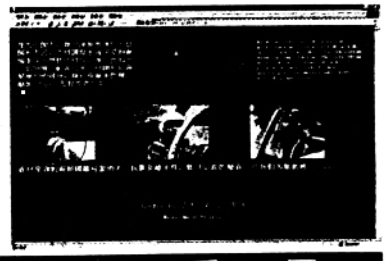
美国黑客，既是名正言顺的黑客，我就不说了。我想，美国既以世界警察自居，又惯以国内法管国际事务，那么如果黑客对中国网站的攻击行为违反美国计算机安全方面的法律，就最好是把国际警察当到底，视破坏中国网站如破坏美国网站一般，给以法律上的制裁。中国的"战士"呢，不管叫不叫黑客，其行为是"攻击计算机系统及通信网络，致使计算机系统及通信网络遭受损害"。这种行为本是有法可依的，只因为中国的法律只管自己的事情，目前又暂无计算机安全的国际法律合作，所以似乎不太可能负法律责任，但面对国内网站遭到报复性的攻击，道义上的责任是跑不了的，不能说你"爱国"了，中国的网站就非做贡献不可。把爱国马甲一披，就自己过攻击瘾，让同胞为你承担后果，是没有道理的。

今年2—3月间，"红客"们进行第五次"网络卫国战争"时，不仅攻击了日本右翼网站和官方网站，而且攻击了企业网、校园网、医院网，在上面贴红旗、刷标语，乃至要打击针对中国的"反动思想"。其时，我国政府表示，关注到这些攻击，反对任何网上不良行为。这就是政府的态度。政府需要考虑国家形象和中国网站安全，而穿了马甲的黑客呢，既能玩攻击的把戏，又能"爱国"，哪有比这更划算的，就只管尽兴了。我想，如果一个人在外国乱丢垃圾能叫"爱国之丢"，那就再好不过了，何况这种'爱国之丢'还保险得很，无须自家人跟着揩屁股呢。

北京信报

2001年5月7日

今天是北京时间5月7日，过了24时是美国当地时间的5月7日，也就是中国驻南斯拉夫大使馆被炸事件的两周年纪念日。记者从中国红客联盟论坛上获知，今天中午该论坛盟主将宣布晚上的攻击目标，中国黑客的网络反击战无疑会在今晚达到另一个高潮。



中国黑客今晚反击

中美撞机事件后，中美黑客之间展开了一场网络大战，其实双方都在危害网络公共安全

背景资料：中美撞机事件后，以PoizonBox为首的美国黑客组织不断攻击中国网站，我国有数百个网站被黑。对此，我国的网络安全人员和极防备美方黑客的攻击，并有一些中国黑客奋起反击，攻击美国网站，"红客联盟"、"中国黑客联盟"等自发的黑客组织和一些"单干"的黑客出于义愤，把五星红旗插上了白宫的网站主页，在美国的网站上奏响了中国国歌，并把王伟的照片贴上了很多网站，让不少中国人着实感到出了一口气。自4月30日中国红客联盟的反击战打响之后，有数百个美国商业网站被黑。5月4日又达高潮，大约有8万人参与了网络反击，一度使白宫网站陷于瘫痪。

红客联盟的论坛忙着为今天的攻击行动支招

昨天下午，记者看到，红客联盟的"总司令"在论坛里贴上了总结攻击白宫网站行动的帖子。帖子上说，很多盟友用国内的主机攻击，结果造成了自己的带宽不够用，给众多中国网民上网带来不便。同时，美国作了防范，改进了防火墙，可以过滤中国的IP，美国的ISP也限制中国访问，而且整个行动组织得也比较乱。这位名为"Lion"的站长接着鼓励大家"5月7日再来"。自称不爱理记者的"红客联盟"站长明天也将接受媒体的公开采访。为了准备更充分，该站长昨天下午忙着在论坛上给盟友支招。有一位名为"open your eyes"的黑客问站长，"AOL有两个IP，到底攻击哪个？"站长回答说，"不管IP，直接攻击域名。"

"中华黑客联盟"行动的统一页面是黑色背景，上方中间为一面飘动着的五星红旗，下方是飞行员王伟烈士的遗像，左侧有血红色中文字样"作为中国人，我们深爱着我们的祖国和人民。当祖国母亲再次受到帝国主义的侵扰的时候，我们感到无比的愤慨，能说的是：祖国！您需要我们的时候我们将毫不犹豫地献出一切，包括生命！"右侧为白色英语译文。末尾是署名"中华黑客联盟"、组织标识和网址。

此次大战是缘自美国黑客挑衅，被民族自尊心所激发的中国黑客不甘落后地给予反击

在反击行动中，我国的网站也暴露出了一些问题。在这场网络大战里，中国起码可以吸取几个教训：一是我们没有自己的操作平台，这次被黑的网站大部分是用WINDOWS平台的；二是很多网络安全产品如防火墙都是国外的，意味着还有一把钥匙留在外人手里，然后人家又据此来攻击你的家门，自然要容易得多；三是美国大多数被黑的网站很快就可以恢复原状，比如攻下的白宫网站只堵塞了3小时，而中国的网站被黑后却迟迟找不到修复的办法，说明在破坏时双方黑客的水平相差不大，但国内网站管理员的修复能力显然不够。中国的IT企业真的需要自强，只有我们拥有自己知识产权与核心技术的时候，我们才有足够的实力和别人平等竞争。

这次网络大战的起因是来自美国黑客组织的无耻挑衅，被民族自尊心所激发的中国黑客和网络爱好者们也不甘落后地给予反击，但是，这种反击带来的结果却值得反思。被黑的美国网站大多是商务网站，政府类的却很少。

无论黑客还是红客的行为，都是危害网络公共安全的

无论黑客还是红客，这种网络大战都是不值得提倡的，因为这是利用网络攻击手段危害网络公共安全的违法行为。它具有潜在危险，会造成灾难性后果。中国大量的路由设备都是从国外进口的，操作平台以WINDOWS为主，如果美国这些设备、软件的研发者都充当黑客，中国的很多网站将瘫痪。

顾国认定网络社会信息共享，蓄意入侵各种网站的黑客确实不少，但也有一部分黑客是因为要展示自己的电脑知识而存在，而且，还有不少网络管理员通过在黑客网站上学习安全漏洞知识，才更好地在自己维护的网站上打"补丁"。

记者在"中国红客联盟"的"纪律声明"中看到，成员不得违反国家关于网络安全的相应法律法规，更不得无端攻击普通用户和合法网站，违者从联盟名单中剔除。

这次激烈异常的中美网络大战，是因为美国的霸权主义政策，我国黑客反对霸权的民族心理是正义的，但是，通过这种方式显然不可取，我们要做的，是使祖国更强大。 信报记者 贺文华

图片说明：一家位于美国加利福尼亚的网站遭到中国黑客攻击，至今尚未恢复。网页上用中文写着："这里我们向祖国最可爱的人，民族英雄王伟，致以崇高的敬意，让我们为他祈祷……"

网络报
Net@China
2001年4月30日

中国黑客联手 五一大反击

尚北京/文

今年4月1日，中美撞机事件发生以后，事态在中美双方的努力之下正在妥善解决，然而就在此时，美国黑客组织PoizonBOx竟然公开向中国的网络挑衅，并扬言要将中国网络彻底摧毁！他们利用漏洞扫描软件对http://www.***.com.cn域名进行漏洞检测，并将其中存在UNICODE漏洞的系统作为攻击对象，批量修改中文主页页面。至4月24日，这个组织已经利用UNICODE漏洞修改了503个网站，其中不但涉及政府机构主页，甚至包括教育、科研以及非盈利性组织等，而这些网站正是美国人们口中的“黑客手册”(Hacker hand)中明确规定不得攻击的。另外，有消息说一些中国黑客正在着手准备在“五一”期间对美国黑客发动反击。

美国的这次黑客行动并没有什么值得炫耀之处，他们所利用的UNICODE漏洞实际上是NT系统中不可避免的一个编码转换漏洞，即使在美国，也存在大量有此漏洞的主机。我国的黑客曾在有关论坛中讨论过这个漏洞，并且达成共识……没有必要，也不应该利用这个“危害金属的”漏洞报复美国。

在同中国几个公认“红客”谈话之后得知，这次反攻并非真要与美国黑客拚个你死我活，只是有计划的警告并有针对美国一些“不懂事”的黑客而已。因为遵照《黑客守则》，一名真正的黑客是不会在侵入目标系统之后对系统进行破坏的，同时也不可以对诸如教育、非盈利性机构等全人类共有类目进行攻击。如此一来，这个中国黑客的反攻目标便明确了，此次反攻的目标主要针对美国的一些主动攻击黑客，而并不会将矛头指向全美国。

这些美国的恶意黑客凭借手中的简单工具加上相对熟练的UNICODE漏洞利用，对中国进行大批量进攻，因此反攻的第一目标便成为了PoizonBOx组织，对他们进行打击的主要手段也是采取UNICODE漏洞，不过于美国黑客不同的是，中国黑客只进行此漏洞的扫描工作，并将存在此漏洞的美国本土服务器报告给相关系统管理员，这样做是要告诉PoizonBOx组织，中国并非没有黑客，也并非没有懂得此技术的人，只不过不屑于用此漏洞去做事而已。

当然，对于存在此漏洞的，并且主页内容有反对和侮辱我中华民族言论的网络服务器，中国的黑客也不会手软，也会仿效PoizonBOx组织，在他们的页面上留下一些信息，而信息的主要内容则是：“我中华是团结的，中华民族也是团结的，美国的行为并非禁人，请不要再来中伤我们！”

此次攻击日期定于“五一节”放假期间，这个时间并没有做任何保密措施，恰恰相反，对于此次攻击中国黑客是完全公开的，并不怕美国黑客知道反攻时间，同时也高然宣告美国黑客，中国绝对有能力摧毁美国无端挑衅的各种组织以及支持这些组织的权限提供商服务器。

至此，中国黑客已经开始了自1997年以来的第六次“网络捍卫战”。长久以来，“黑客”始终被多数人士认为是罪恶之源，其实真正的黑客拥有自己的守则——《黑客守则》，并且也为维护网络的健康发展贡献了不小的力量，除了被人们熟知的多次“网络捍卫战”之外，与此性质类似的正义行动一刻都没有停止过。例如为反对日本对华侵略，纪念“九一八”事件，中国黑客每年都要在9月18日对日本反华网站进行警告；另外中国的不少黑客也自发性地组织起了网络垃圾清理活动，反对网络色情、暴力等不良内容。

虽然黑客的行为并不值得提倡，但是对于如此的爱国和侠义心肠，我们还是为他们喝彩。

中国因特网历史上的五次“网络捍卫战”

1，1997年，由于印度尼西亚受东南亚金融危机的困扰，国内发生了一系列排华反华事件，许多华裔人被印尼暴徒杀死，商店被疯狂抢劫，一些华裔妇女遭到反华暴徒的蹂躏。面对印尼反华暴徒的暴行，中国黑客通过因特网向印尼反华暴徒的网站发动了攻击，黑客们在侵入系统后，留下了中华人民共和国的五星红旗以示警告。

2，1999年5月，在以美国为首的北约轰炸中国驻南联盟大使馆后，中国上下一片愤怒，中国黑客利用特殊手段袭击了美国能源部、内政部及其所属的美国家公园管理处等美国政府机构网站，并向白宫网站发动了进攻，致使白宫网站服务器瘫痪长达72小时之久。

3，1999年7月李登辉公然抛出“两国论”之后，台湾“国民大会”、“行政院”、“监察院”、“台湾新闻处”、“中华日报”等军政部门和传媒的计算机信息网络均遭到了大陆黑客们的攻击，并修改了台湾多达百台服务器的网页页面，其修改内容义正词严，维护中华民族统一。

4，2000年1月23日，日本右翼在大阪国际和平中心进行了以“南京大屠杀：20世纪最大的谎言”为主题的大型集会，公然为南京大屠杀翻案。在中国政府和南京等地人民进行抗议的同时，中国黑客和海外华人黑客也以自己的方式多次侵入日本网站，以实际行动回击日本右翼的丑行。据日本媒体报道，电脑黑客们在侵袭的日本网站上留下大量抨击的文字，日本总务厅和科技厅的网站被迫关闭，而当首相小渊惠三对袭击浪潮表示“遗憾”后不久，中国黑客的新一轮攻击又马上卷土重来。

5，2001年2月，由于年初时日本国事端不断，三菱事件、日航事件、松下事件、教科书事件、《台湾论》等等，激起了中国人民的强烈愤慨。中国黑客在一次对日本右翼反动网站进行了有力的反击，同时在其“黑”的网页上涂满了“打倒日本帝国主义”、“灭绝日本鬼子”等口号，鲜艳的五星红旗在主页上居中向…一个取名“红客联盟”的黑客组织在攻击得手后，自豪地宣称他们是一群为了“守住祖国统一的国家主权，打击一切对中国有反动思想”的热血青年。

国内知名

近期横行网络的人很难说是黑客

黑客(Hacker)，源于英语动词Hack，意为“劈，砍”，引申为“干了一件非常漂亮的工作”。早期麻省理工学院的校园俚语中，“黑客”则有“恶作剧”之意，尤指手法巧妙，技术高明的恶作剧。在日本《新黑客词典》中，对黑客的定义是“喜欢探索软件程序奥秘，并从中增长了其个人才干的人”。

一般认为，黑客起源于50年代麻省理工学院的实验室中，他们精力充沛，热衷于解决难题。六七十年代，“黑客”一词极富褒义，用于指代那些独立思考，奉公守法的计算机迷，他们智力超群，对电脑全身心投入，从事黑客活动意味着对计算机的最大潜力进行智力上的自由探索，为电脑技术的发展做出了巨大贡献。现在黑客使用的侵入计算机系统的基本技巧，例如破解口令(Password cracking)，开天窗(Trap door)，走后门(Back door)，安放特洛伊木马(Trojan-horse)等，都是在这一时期发明的。

朴天副总经理沈洋首先指出，这个时代的“黑客”不过是媒体刻意塑造的神话人物，公开露面于电影公告板里。对他来说，使用Hacker一词感觉要好些，至少著名黑客coolfire的文章里面早就翻译过。

姚远认为：“在当前的中国，黑客是一个被年轻人羡慕崇尚的代词，规范地说，应该称其为Hacker(黑客)和Cracker(骇客)，这是清华一本书里的专业翻译。我认为国内安全技术工作者一般也有两类，一类人借鉴别人的资料，从中获得技术，自己不能发现新东西，因为没有程序基础和专业知识，只有一个相关职位，比如一些翻译英文安全文献的人；另一类人是真正涉入技术的专家级人物，比如绿盟的袁仁广，他擅长Debug，发现了很多危害性比较大的系统漏洞。比如badboy，他写了针对微软NT ISS4.0/5.0系统的unicode(编码漏洞)的详细介绍，文章里就有很多其独特的攻击思维方式。照此意义，我觉得国内能叫‘黑客’的不上五人。了解一个漏洞，黑一个站点，这些算不上什么。了解一个漏洞，我五分钟就能教你黑掉某网站，你就可以炫耀自己是黑客。”

Ipxodi说：“其实黑客Hacker在原始意义上就是技术专家，但是不够专，guru才是众望所归的技术精英。但是，现在国内的媒体好像认为黑站的就是黑客。我们教育网里面的技术爱好者，对于新闻媒体报道的所谓黑客，都是一笑置之。至于其它什么自称红客的人物，大概是为了出名而搞的噱头。”

朴天公司范礼认为，技术目前还是单纯的，不应该沾染上任何政治和利益色彩。至少，他从不入侵。范礼说：“黑客是这样的——一群奇怪的人，各自有各自的信念，对某些事物进行深入钻研。”他解释说奇怪就是普通，普通得像你邻家楼上的姐姐，你不可能看到一个人，马上反应出他电脑玩得好——电脑技术好不好，这确实没有什么外在特征可循。而现在好多对黑客的看法甚至延伸到“表象”特点，就全是胡说八道。“黑客其实是引申出来的，比如你玩Word，你可以玩出别人玩不出的花样，你就是Word hacker，同理，那群人不过是Computer hacker。”

关于什么才是黑客，中联绿盟副总经理高永安表示：“如果是指那些痴迷于计算机高深技术，研究系统安全漏洞并将其公之于众以推动网络技术的整体进步，并且有着良好的道德品质的专家的话，绿盟成员是真正意义上的黑客。去年微软对自己的系统发布了100条安全漏洞公告，其中有6条是中联绿盟发现并提供的，我们的手中现在还有十几条准备逐步发布。如果按照国内某些人的观点，把无牌的导游也称为黑客的话，那我们不是黑客，我们是安全专家。”

其间曾提到一个有趣的问题，就是为什么国内的女技术员总比男技术员少？中联绿盟袁仁广认为这很简单，“女性擅长现象思维，男性擅长逻辑思维，而技术的核心在于其后”。

姚远则一语否定了“技术员男女比例的统计数字”这种提法。他认为国内基本都是男技术员，至于圈子里有点声望的“女技术员”，其实他们并没真正涉入技术，女性网络安全工作者可能会在一些安全频道担任网管，经常与安全工作者们打交道，但她们或者只是网络安全公司里一名擅长英文的翻译人员，算不上技术员。就算有些男技术员，懂得技术也不深入技术。比如范礼，他的工作责任是是下载，帮公司里找工具，作安全资料的收集。

入侵根本就不是黑客的大道

史蒂夫·利维在其著名的《黑客电脑史》中指出五条“黑客道德准则”(the Hacker Ethic)：

通往电脑的路不止一条
所有的信息都应当是免费的
打破电脑集权
在电脑上创造艺术和美
计算机将使生活更美好

有些安全工作者认为这些道德准则中的某一条充斥着诡辩精神。近来极少在绿色兵团IRC频道出现的沈洋解释说，当前真正的技术讨论者越来越少，许多人本着对“黑客”一词的好奇来涉入技术，他在绿色兵团IRC频道就不止一次遇到类似的情况。从那些孩子有模有样的发言中，他不能看到国内网络安全事业的光明前途，却更多嗅到一种盲目崇拜的肤浅。沈洋以为呈现在眼前的事实明显可笑，“有些人以为入侵一台日本或者美国主机，修改它的页面，就能摇身变为黑客或红客。有一些不道德入侵者，利用这种盲目的崇拜情绪，可以使不明真相的人产生对技术事实的错误理解。比如，某人非法进入别人的系统，再于各大BBS上张帖诸如‘www.ribenzhu.com这个网站被我黑了’，‘用户名和密码是 ribenren 123’之类的贴子，

深圳特区报
SHENZHEN SPECIAL ZONE DAILY
2001年5月4日

国家有关部门负责人提醒网络运营者注意

防范黑客攻击 确保网络安全

【新华社北京5月3日电】国家计算机网络与信息安全管理工作办公室负责人今天在接受新华社记者专访时说，进入4月中旬以来，针对我国网络的攻击事件频繁发生。他提醒我国网络运营者注意防范黑客攻击，确保网络安全。

这位负责人介绍说，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。

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的技术人员缺乏，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。

这位负责人说，据他了解的情况，针对有可能发生的大规模网络攻击事件，国内安全服务企业的技术人员已经全部到位，实行24小时不间断值守，随时监测网络的运行状态，接受用户的报警，提供必要的救援和咨询服务，以减少网络攻击带来的损失，防止事件进一步扩大。北京启明星辰网络技术有限公司已经发起了"光明网站"活动，在5月免费提供安全咨询、漏洞修补建议，并针对北京地区的政府网站提供网站监测与恢复软件的免费安装。

这位负责人提醒，如果发现网络攻击事件，请将有关情况上报国家计算机网络应急处理协调中心（网址是：http://www.cert.org.cn）。

重庆商报
2001年5月3日

安全专家"提醒"

国内网站须防美国黑客

最近在美军撞毁我军机事件的同时，美国的黑客也对我国的网站进行了攻击，对此我国的黑客们也发起反击。中科院高能所网络安全组的信息安全专家表示，国内互联网用户应尽快检查自己网站漏洞，避免被黑客侵入。

中科院信息安全专家告诉记者，"据有关统计，目前中美两国每天都要发生40到50起黑客攻击事件，而在撞机前这一数字仅为1到2起。"

对于中国黑客的行为，中科院信息安全专家认为："网民在虚拟的世界中，选择一种更容易、更直接的方式宣泄自己的愤怒便会成为黑客，对美国黑客攻击我国网站进行反击，只是网民表达自己气愤心情的一种方式。"

"目前，中美两国黑客的攻击还是以选择比较脆弱的网站进入系统、修改内容为主。"中科院信息安全专家表示，"因此，我们建议国内的互联网用户应该使用隐患扫描器对自己的网站进行检查，将发现的漏洞全部修复，这是在短期内最有效的防范手段。"中科院信息安全专家提醒广大互联网用户要加强安全防范意识。 据人民网

河南日报

2001年5月4日

有关负责人提醒网络运营者

防范黑客攻击 确保网络安全

据新华社北京5月3日电（记者李佳路）国家计算机网络与信息安全管理工作办公室负责人今天在接受新华社记者专访时说，进入4月中旬以来，针对我国网络的攻击事件频繁发生。他提醒我国网络运营者注意防范黑客攻击，确保网络安全。

这位负责人介绍说，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。

这位负责人说，据他了解的情况，针对有可能发生的大规模网络攻击事件，国内安全服务企业的技术人员已经全部到位，实行24小时不间断值守，随时监测网络的运行状态，接受用户的报警，提供必要的救援和咨询服务，以减少网络攻击带来的损失，防止事件进一步扩大。北京启明星辰网络技术有限公司已经发起了"光明网站"活动，在5月免费提供安全咨询、漏洞修补建议，并针对北京地区的政府网站提供网站监测与恢复软件的免费安装。

这位负责人提醒，如果发现网络攻击事件，请将有关情况上报国家计算机网络应急处理协调中心（网址是：http://www.cert.org.cn）。

湖北日报

2001年4月27日

CIH病毒是我国感染率最高的计算机病毒

据4月21日央视国际：我国首次计算机病毒网上调查结果表明，全国共发现了十几个新的病毒样本。该调查同时确认，CIH病毒是我国感染率最高的计算机病毒。

新都市报 NEW NEW NEW

2001年4月25日

我国CIH病毒感染率最高

我国首次计算机病毒网上调查结果于近日公布：共发现了十几个新的病毒样本，同时确认CIH病毒是我国感染率最高的计算机病毒。

国家信息化工作领导小组计算机网络与信息安全管理办公室表示："爱虫病毒以前听说挺多，闹得并不凶，这次发现还有上升的趋势，其次蛆虫、冰河这样的黑客程序也有抬头的趋势。"　刘玉

服务导报

2001年4月26日

CIH：明天会不会来？

对于网民和PC用户来说，4月26日是一个特殊的日子。三年前的4月26日，陈盈豪炮制的全球迄今以来杀伤力最大(造成全球损失100亿美元)的电脑病毒首次发作。人们不禁要问，陈盈豪：你的毒还在不在，明天你还会不会来？

1998年4月26日 CIH病毒在亚洲首次现身；7月26日，CIH的恶性病毒在美国开始了大面积传播；8月26日，CIH病毒入侵中国。CIH病毒静悄悄地蛰伏在计算机中，并且通过软盘、光盘和刚刚兴起的互联网进行着大面积的传播。

1999年4月26日 幽灵现身，CIH在中国全面发作。这一天，简直成了中国PC用户的灾难日，CIH病毒第一次对中国用户发起了大规模的进攻，造成直接经济损失8000万元，间接经济损失包括因硬盘数据丢失造成的重复劳动、延误工时及机会成本达11亿元。CIH成为热门的社会话题。

2000年4月26日 中国的电脑用户们再一次经历了CIH的侵害，其中很多用户是第一次有了病毒体验，而代价却是新购置的电脑主板和硬盘遭到洗劫。

4.26从此成为电脑病毒的纪念日。每年4月26日之前，对CIH病毒又是一片防、查、杀之声，虽然"CIH"病毒每年破坏的电脑数量一再下降，但它对人们的工作和生活仍然造成了很大的影响。

刚刚跨入2001年4月，在各大专业媒体上，各大反病毒软件厂商防范"CIH"病毒的警告一次又一次地出现，人们不禁要问，历史还会不会重演，"CIH"明天还会不会来？

据了解，在CIH大规模入侵后，国内各大网络安全公司均加强了防杀CIH及其变种病毒的力度，相继推出了一系列相关产品。最近，刚刚进入国内反病毒软件市场的金山公司，更提出了全新的防范"CIH"方式——"终身免疫CIH"。4月中旬，金山公司在其主打的杀病毒软件"金山毒霸"最新升级版中，内置了"CIH"终身免疫程序，据称，免疫程序一经安装，电脑就像打了预防针一样，不会再担心遭受到"CIH"侵害，用户可以放心大胆地在4月26日使用电脑。而且，只要电脑中有免疫程序，每年的4月26日都不用再担心了。但其效果如何，尚需明日再见分晓。

由于目前电脑病毒以每天二十种左右的程度不断出现，相当于三年前的5—6倍，而防杀病毒的软件在事实上不可能与病毒的发作实现完全的同步，杀毒软件永远只能跟在病毒的后面苦苦追赶。欧洲的熊猫卫士号称拥有世界最大的病毒库，瑞星则称病毒库做到最大并无实用价值。同样，金山公司建立的全球病毒监测网，通过它及时捕获最新流行的国内外病毒，并在第一时间提出安全的解决方案，一样无法阻挡随时都有可能出现的新的恶意病毒全球发作的趋势。因此，我们可能永远告别CIH的"4.26"，但我们却难以摆脱数着数字过日子的尴尬。 毕春富

齐鲁晚报

2001年4月26日

特别提示

CIH病毒今日又要作恶 电脑用户开机务必谨慎

自1998年4月26日起，一种专门感染Windows 95/98 32位操作系统、能够破坏PC机主板"快闪"BIOS、使电脑瘫痪的病毒——CIH开始四处作恶，每年这一天它都要给电脑用户和厂商造成巨大损失，一时间，人们谈CIH色变。今日CIH又来了！据希望软件专卖店的夏工程师介绍，如果用户事先没有进行相关处理(如提前将日期改为4月26日以后的任一日期，或者安装了KV3000、瑞星、金山毒霸等杀毒软件)，今天尽量不要开机，一旦你的电脑里潜伏着CIH病毒，开机后，电脑遭殃的可能性极大。(崔京良)

CIH病毒资料

原理 CIH病毒有多个变种，只感染WIN95、WIN98的EXE的PE格式文件，病毒代码分解为一个或多个不同大小的碎块，潜伏在文件内部的不同地方，文件总长度无变化。PE文件格式是32位的，文件头部存放了文件各模块参数。CIH病毒修改了这些32位参数，使其首先指向病毒的程序体。

发作 CIH病毒出现至今已演化出至少多个变种，有的病毒只在4月26日发作，而有的变种则每月26日都会发作。

表现 CIH病毒发作时，硬盘出现"颠簸"(即硬盘驱动器狂转不止)，硬盘上所有数据(包括分区表)被破坏，必须重新FDISK方才有可能挽救硬盘；同时，对于部分厂牌的主板，会将"快闪BIOS"清掉，造成开机后系统根本无反应。这时根本无法用软件对BIOS进行重新写入，只能将PC机送回主板制造商修理或请专业人士通过特殊手段重新烧入BIOS。

传播 CIH目前主要是通过Internet、电子邮件或软盘、光盘等渠道传播，而通过Internet或电子邮件传播的病毒有很强的隐蔽性。

防治 因为病毒不断会有新变种出现，所以旧的杀毒软件不保险，要使用各种最新的具有实时监测功能的杀毒软件杀毒；修改主机日期，跳过26日，可以避免病毒发作；将主板的Flash Rom跳线设置为Disable，阻止病毒改写BIOS。当然，现在有许多主板自带防CIH功能。

中国计算机报

2001年5月10日

小心网上陷阱

【 刘宝旭 李恩宝 】

计算机犯罪的威胁程度，正随着人们对计算机及网络的越来越依赖而迅速膨胀，电子商务中的欺诈行为已经成了一个大问题。随着其全球化进程的推进，电子商务反诈骗与防护技术的研究正在成为一个世界性的问题。

13国联合对抗网上诈骗

近来，在报刊杂志、网站发布的信息中，“网上诈骗”成为一个热问：只要你在中文雅虎搜索引擎中输入该关键词，便可一下搜索出2000多篇相关文章。最近有一篇报道说，美国联邦贸易委员会（FTC）表示，美国与澳大利亚、加拿大、丹麦、芬兰、匈牙利、墨西哥、新西兰、挪威、韩国、瑞典、瑞士以及英国13个国家准备合作建立一个统一的数据库，专门存放网络消费者的投诉，并采取相关措施防止消费者再受骗，他们将联手对互联网诈骗活动进行重拳出击。同时这些国家将对国内消费者的相关投诉进行整理，并互通信息，以便针对跨国界的网络诈骗犯罪予以严厉打击。根据达成的协议，各国的执法部门均可以通过登录一个设有密码的统一网站，进入上述数据库，获取相关信息。FTC的官员表示，该数据库可以为上述国家提供实时信息，使执法人员了解全球互联网诈骗活动的最新动态，从而成为执法机构采取相关行动的主要信息来源，有了上述数据库之后，这种跨国界调查将变得非常简便。

这则消息告诉我们：计算机犯罪对人们的威胁程度，与人们对计算机及网络的依赖程度和所从事的业务的重要程度密切相关。随着电子商务在全球的飞速发展，需高速核实与认证的电子商务安全问题变得非常重要。欺诈性电子商务已然成了一个大问题，随着其全球化进程的推进，电子商务诈骗行为与防护技术的研究正在成为一个世界性的问题。

小心电子世界中的陷阱

现在，我们的世界正在向一个电子化世界（E-World）演变，所有的信息正在全面数字化，电子世界中四通八达的网络把人们联系在一起。在网络中，天涯变为咫尺，人们可以运筹帷幄，决胜于千里之外。电子商务成为一个充满机遇和挑战的新领域。国际国内一片喧嚣，展示会、研讨会、演讲、广告，“E-Commerce”、“E-Business”铺天盖地而来，声势浩大。发展电子商务是大势所趋，电子商务作为网络时代发展的必然，已经在经济生活及社会生活中掀起了新浪潮，它把互联网作为一种互动的商务工具来使用，它超越了时空的限制，使交易的范围大大扩大、交易的成本大大降低。

但是，当传统的商务方式应用在Internet上时，便会带来许多源于安全方面的问题，如：传统贷款和借款卡支付保证方案及数据保护方法、电子数据交换系统、日常信息安全管理等。如果不能建立一整套完善的网上信用保证制度，那么，电子商务可能成为某些不法之徒手中的欺诈工具。如果不重视网上诈骗问题，势必会对电子商务网站的整体信誉度产生不良影响，影响电子商务的健康发展。所以，诈骗行为已成为影响电子商务迅速发展的主要障碍之一。

想想看，连大名鼎鼎的比尔·盖茨的信用卡数据都被黑客盗取，难怪网上消费者对因特网的诈骗倍加关注了。美国联邦贸易委员会最新公布的《扫荡网络诈骗》报告中，列举了全球十大最流行、最猖獗的网上欺诈手法，其中以网上拍卖名列榜首，受害人大多数反映中标付款后却收不到商品。执法人员指出，大部分的网络诈骗其实都是老把戏，人们多是因贪小便宜而不慎中计，其他九种诈骗手段分别为：网络服务契约、信用卡、提供免费网页、多层直销、商学机会、投资及保健产品。例如，网络公司会先行送出“折扣券”支票，当消费者真的把支票兑现，就意味着自动同意该公司成为他的网络服务供应商，以后，每月硬性收取费用以及骗取长途电话费。还有，一些网站表面上会让网友进行所谓的免费浏览某些色情和游戏网站，但当用户尝试打开某些图片或运行某些游戏时，会被要求下载某一软件以观看该图片或运行该游戏。实际上，这个软件是一个拨号软件，用户在下载后运行这一软件时，电脑将自动关闭调制解调器的声音，切断用