信息安全动态

12

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、综合分析与对策研究

✧ 九、曝光篇

✧ 十、趋势篇

✧ 十一、安全锦囊

警钟篇

- 黑客大战见分晓——来自国信安办的统计
- 我国的安全产业有点虚
- 视窗 XP 可能为黑客开方便之门
- Outlook 漏洞可能导致邮件被窃
- 美国黑客充当商业间谍
- 解聘者可能成为攻击者
- 最新病毒警告（12 则）

……

计算机世界
2001年6月11日

黑客大战见分晓

——来自国信安办的统计

◎ 本报记者 胡英

中美撞机事件引发的中美黑客大战，在“五一”期间达到了高潮。5月1－7日之间，虽然各国政府及各类网站早有预料，并做了相应的准备，但在这场没有硝烟的网络大战中，依然有不少的网站被黑，造成了负面的政治影响和直接的经济损失。作为我国网络信息安全的领导机构——国家信息化工作领导小组计算机网络与信息安全管理工作办公室(简称国信安办)预计到了这场网络战争的发生，在“五一”期间组织一些国内安全厂商，在国家计算机网络与信息安全实验室内严密监测着各类网络攻击事件，并根据各类原始材料做了相应的统计。统计结果令人触目惊心，让我们看到目前的网络环境的脆弱性，安全不再是技术层面的事情，而应该从关系到国家安全的角度获得高度的重视。

在采访中，国信安办技术组织处处长白硕先生向记者介绍说，本背景材料中引用的原始数据和被破坏网站截图，来源于世界上专门发布经过核实的网络攻击事件记录及几个著名的网站，包括alldas、H.U.C等等。数据发布时间为2001年4月1日到2001年5月7日。国信安办对其中一部分数据进行了独立的抽样核实，认为这些原始数据基本上是可信的，但不一定是全面的。因此，材料中的绝对统计数字仅供参考，但相对统计数字（百分比）则在统计抽样意义下对理解此次黑客攻击事件的性质而言具有重要的情报价值。

以下，我们将从对比的角度分析各类统计数据的意义。

中美黑客大战引发全球黑客大战

在5月1～7日期间有记载的全球发生的黑客事件共有1124起，其中针对中国(包括香港和台湾)和美国网站的黑客攻击行为占了一大半，与平时有着明显的区别，因此可以认定，中美两国黑客互相攻击产生的结果是引发全球黑客大战，如图1和表1所示。

美国政府网站保护很好 而我国政府网站保护很差

从总数上看，中美之间爆发的网络黑客大战中被黑的网站共有1301个，其中美国网站占了80%，被黑网站数达到1041个，如图2所示。但是，美国被黑的网站中，65%是商业网站，而政府网站只占5%，总数只有50个，说明美国对政府网站保护得很好，如图3所示。我国则正好相反，大陆地区被黑的网站数仅为147个，而其中大部分是政府网站，总数达到54个，如图4及表3所示。

比较结果触目惊心，我国政府网站就像一座座不设防的城市，随时都有被攻克的危险，让人不禁捏了一把汗。由此也启发我们，政府网站的安全是我们极待改进的薄弱环节。

黑客组织分类

双方的黑客组织都比较集中，且均表现出了较强的政治倾向性。由此也再次表明，“五一”期间的黑客大战确实是由双方政治分歧引发，如图5及图6所示。

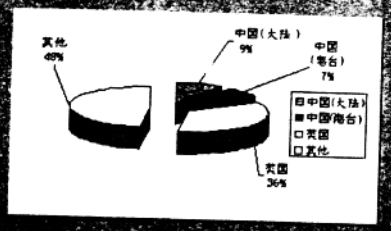
美国商业网站容易被攻破的三大理由

◎赵栋伟

1. 美国的上网计算机数量众多，许多还是20世纪80年代甚至更早年代的计算机，计算机的稳定性以及操作系统都很陈旧，存在很多漏洞和隐患。

2. 由于历史的原因，美国的IP地址资源非常丰富，大部分计算机都是以固定的IP地址上网的，这样寻找攻击目标非常容易。而中国的计算机很多都是拨号上网或通过局域网上网的，这样定位一台计算机非常麻烦。

3. 美国由于上网的计算机太多，缺乏足够的网络管理人员，一些重要的服务器上，两年前就发现的漏洞到现在还没有补丁，更不要说新的漏洞了。而中国的网络管理人员尽管绝对数量比美国少，但是相对中国的上网计算机数量，特别是有一定商业意义的上网计算机数量来说，中国的比例还是远远高过美国。



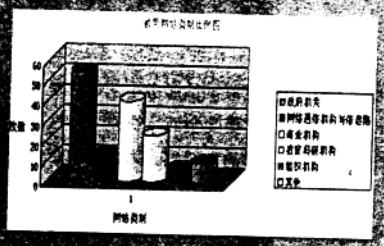
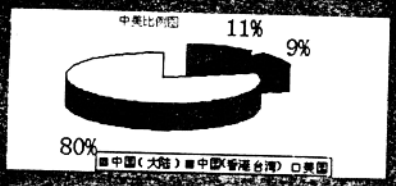
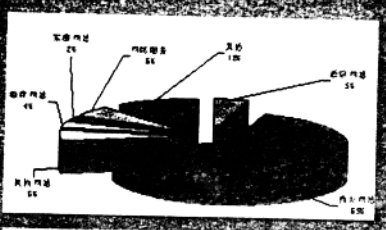


表1 5月1～7日全球部分网络攻击事件

	次数	百分比
中国(大陆)	103	9.2%
中国(港台)	80	7.1%
美国	401	35.7%
其他	540	48.0%
总和	1124	





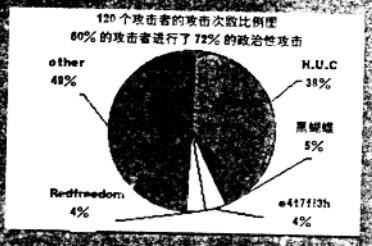
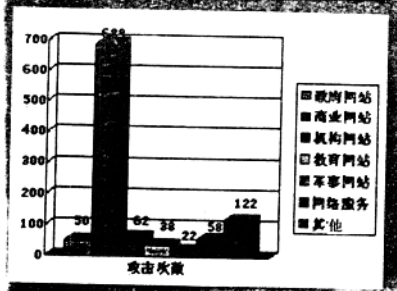


表2 5月1～7日中美被黑网站数

中国(大陆)	147
中国(香港台湾)	113
美国	1041
总和	1301



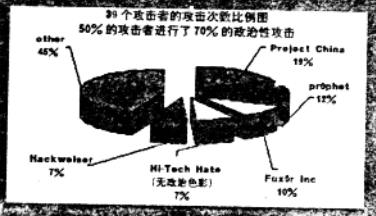


表3 5月1～7日中国被黑网站数

时间	5月1日～5月7日
政府机关	54
网络通信机构与信息港	13
商业机构	40
教育科研机构	23
组织机构	7
其他	10
总和	147

互联网世界

2001年6月1日

中美黑客之争暴露了什么

文／爵也

近日由于撞机事件使得中美关系再一次陷入低谷并导致双方黑客之争。笔者认为这其中爱国主义热情固然占了第一位，但是其中所引发的一系列问题却远比这次攻击事件大的多，远比这次攻击事件的影响大的多。因为，此次事件从最终角度讲，终究是一场黑客之战，目的都是尽量破坏对方网络站点，使之瘫痪或者使其内容改变或者收集对方机密信息。

从目前双方所报道的情况来看各有损失，从总体上来看，美国网站的受损率远没有中国黑客所说的那么严重，其被攻击的网站主要是民间网站，而美国军事网站和政府网站由于系统和设备的独立性根本无法进入，即使有也只是在表面门户上涂鸦而已，没有达到真的被黑。而我国这次所受的攻击却非常严重，至少100家中国网站被黑，损失严重。不管此次事件鹿死谁手，我们更应该关注此次事件所引发的网络安全问题，更应该关注中国的网络安全问题，因为：

我们的网络很脆弱：对我们的网站而言，互联网至少有五大脆弱性，芯片不是我们的，操作系统不是我们的、应用系统、数据库、防火墙等几乎都是国外的产品，我们拿来别国的网络产品东补西补，自以为是，这样的产品、这样的防护，国外黑客不进来才怪呢！？

我们的人才很缺少：目前，中国在信息安全的防范上和西方国家如美国面临的问题是同样的，那就是人才缺少，管理混乱，网络技术欠缺的问题。我国现有信息安全专业人才只有3000人左右，远远达不到安全的需求，人是网络安全最为薄弱的环节。

我们的安全意识淡薄：从总体上来说，我们对网络安全的意识很淡薄，无论从物力还是财力还有人力方面投资都是很少的，另外，对安全的防护都不够重视等诸多问题，从而导致我们的安全问题有着较大的漏洞。

我们的产品很稀少：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，国外安全检测自身是否安全也总是让人心生疑窦。

上述问题只是我国网络安全领域的凤毛麟角，全部举出恐怕不是一人可以说得完的，我在这里只是提醒广大黑客和网络斗士们，不要一味的投身于黑客大战中，而应该将自己的力量用于国家的信息化发展和信息安全积极防御的体系建设上来，为我们的网络国门而战！ CIT

北京科技报

2001年6月11日

家里的电脑软件都是美国的谁黑谁

中美网络黑客大战的理智思考

张召忠

成败得失

关于中美黑客网战的战果，众说纷纭、莫衷一是。我认为这次可谓“两败俱伤”，没有胜者。在攻击美国网站的同时，诸多中国网站也遭到程度不同的破坏，而且总的损失可能要远远大于美国。美国黑客的攻击相当有组织，专业水准高，技术先进而且效率明显。

曾有测试表明，我们的金融、财税等部门的网站90%有安全隐忧，初级黑客都能够轻易侵入服务器窃取信息。一旦被黑客侵入并修改信息，可能导致网站形象受损并引发泄密、数据错误等问题，损失难以计量。有些网站遭受攻击之后迅速瘫痪，丧失工作能力，而且很长时间内无法恢复。

合理但不合法

不分青红皂白，逮着谁就黑谁一把，这样做是否有点不道德？如果中美网络大战开了这样的先例，那以后是否会经常进行类似的破坏行动呢？真的这样，我们大家都感到安全吗？

从军事角度讲，在实战中交战双方攻击对方的军用目标是合法的，攻击对方的民用目标是非法的。除个别猖狂反华、妖言惑众的网站被列入黑名单外，一般商业性网站、媒体网站、政府网站、教育网站等都属于民用网站，都不应该被随意攻击和侵入。特别是那些与人民生活有密切关系的网络，比如金

融、保险、税收、民航和铁路调度网络、电力管理网络、广播电视网络、有线和无线通信网络等等，如果这些网络可以随便进行破坏，必然会严重影响人民生活和社会安定。

有的黑客想对美国政府和军队网络系统进行攻击。由于此类网络系统在硬件上是独立的，通常不会与因特网进行硬连接；所以即使是黑客高手也难以攻克此类网站。因此，实际上网络攻击战的目标全部是民用网站，既然攻击民用目标被视为非法，那么无论是国际法还是国内法对网络破坏行动都是禁止的。我们都应该认识到，安全是共同的，秩序需要大家共同来维护，我们痛痛快快黑了别人的同时，就要准备好人家可能要来黑我们。

令人揪心的网络安全

网络安全已经不再是一个新鲜话题，也绝对不是此次网络大战之后才诱发出来的一个新课题，几乎随着网络的出现就已经引起人们的高度关注。在这方面，我们必须注意这样三个问题：

一是安全与不安全是相对的。在我们享受计算机和网络带给我们巨大的方便和快捷的时候，安全问题随之而涌现出来，于是有人就喋喋不休地抱怨，似乎一切都归罪于信息科技的发明，甚至归罪于网络黑客的捣乱。其实，安全与不安全都是相对的。坐飞机不安全，但“五·一”期间的飞机票早就预定完毕。我们不能为了追求绝对安全而放弃使用计算机和网络，应该在最大限度使用高科技的同时，加强信息安全。

二是广泛利用和推广黑客实战经验。“不入虎穴，焉得虎子”，黑客自有黑客的道理，只要规范其行动，就可以发扬其优势，使之为国效力。去年克林顿把黑客高手请进白宫，共商网络安全大计，难道我们不可以此为例，大兴发掘黑客特长之道吗？此外，黑客高手们在实战中验证的技术也可转化为信息网络安全产品，逐渐培育和形成信息安全产业，以便为中国的网络防御和信息安全提供坚实的盾牌。

三是消除不安全因素的关键，是加大自主知识产权的创新力度。我们经常听说美国、中国、欧洲哪个国家遭到网络攻击或者黑客破坏，但很少听说俄罗斯的网站遭到破坏。为什么？因为俄罗斯一切都强调自力更生，宁愿不用，也不引进美国的信息产品，包括计算机和网络路由器。这种办法也的确是够绝的，一般国家都做不到。我个人的观点认为，适当引进信息技术产品是需要的，但关键部门的使用要格外警惕，特别是计算机硬件、软件、网络路由器和服务器一定要争取自主研制，不能随便将机密以上的信息资料存储于这类平台之上。但是，对于民用计算机和网络产品，大量引进和使用并无不当，只要加以注意，装个防火墙或者防毒软件就可以了，不必搞得人人自危，风声鹤唳。

应该看到，在信息和网络问题上，中国不仅比美国落后，而且差距相当大；在信息和网络安全问题上，我们必须有强烈的忧患意识和危机感，因为自己的家里安装的都是美国人的锁，连钥匙都是人家给配好了的，不信看看你自己的奔腾芯片、微软的平台？不要说几个黑客高手，几十、几百个也绝对不可能搞垮美国！网络战争是一体化较量，是综合国力的较量，怎能形同儿戏？

篡改几个网站的页面很容易，要想攻击国防部网站就难一些，要钻进五角大楼的数据库、盗取核控制机密、摧毁和瘫痪美军的数据链路、隔断美国地面与太空的联络信道、阻绝各军兵种联合作战的网络空间就更是难上加难。一个一个黑客进行单打独斗和散兵游勇式地在网上乱黑一通，不可能在短期内解决类似的技术难题。

行报

2001年6月19日

网络安全一席谈

前些时候，在网上中美黑客进行了一场网络大战，这期间不少国内网站被国外黑客袭击，有些网站全面瘫痪。这次网上大战所带来的教训，十分深刻，国家软件工程研究中心网络安全分中心主任徐超汉教授表示：“我们要尽快研制出自己的网络安全产品！”

“服务器是人家的、防火墙是人家的、操作系统也是人家的，这想起来都可怕！”徐超汉教授介绍说，网络安全的一个重要环节就是信息安全，而一般情况下这个环节采取的办法都是加密。据了解，加密的形式主要有两种算法：对称算法，即加密和解密用同一条“钥匙”；非对称算法，即加密和解密的“钥匙”不同。前者由IBM（美国著名计算机公司）研制，一般用于金融系统；后者由麻省理工学院等研制，一般用于电子商务网站。

“这两种产品对美国来讲是安全的，但对中国不一定！”徐超汉教授指出，这些产品美国都进行了出口管制，但现在许多网络公司还是迷信于国外的安全产品。事实上，在此次中美黑客大战中最先被攻破的网站，基本上采用的都是美国安全产品。“这很容易理解”，中国红客联盟的一位主要成员对记者说，“此次美方参与攻击的许多黑客就是提供该安全产品的公司职员。”他给记者打了个比喻：就好比卖给你一把锁，他自己却留下了一把钥匙。

徐教授还指出，我国软件开发人员在开发软件时也不太注意安全问题。他认为主要原因是“搞应用的不懂操作系统，懂系统的不去开发”，结果有些技术人员连操作系统里到底有哪些安全设置都不知道。

中国计算机报

2001年6月14日

网络安全在我国确实是热，据统计，截止到2001年3月份，国内计算机安全企业已经接近千家，但是通过调查发现，部分安全产品的核心软件来自网上，某些领域重复投资严重……面对这些不安全的因素，我们应该怎么办呢？

我国的安全产业有点虚

【国信安办　刘欣然】

网络安全产业一片火热

最近两年来，互联网上频繁发生的大规模黑客入侵与计算机病毒泛滥事件，已经波及到了世界很多国家。我国在这一系列事件中也未能幸免，很多政府部门、国家重要行业、商业和教育机构等，都受到了不同程度的侵害，有些甚至造成了很坏的社会影响和重大的经济损失。在这种情况下，信息系统安全问题已经逐步引起了人们的重视，很多单位在建立自己信息网络的同时，开始同步地考虑安全问题。随着我国信息化进程的不断加快，预计安全方面的需求在未来几年内，将处于一个快速稳定增长的态势。

出于对安全领域市场的看好，国内做安全的企业数目也在不断增加。据统计，截止到2001年3月份，国内主营和兼营计算机安全业务的企业已经接近千家，其中有相当比例的企业都是最近两年内成立的，而且这个数目还在上升。

表面繁荣下还有点虚

但是在这种表面的繁荣之下，也有一些现象值得我们深思。

安全软件来自网上免费源代码

首先，由于目前Internet上有很多免费的(有一些还提供源代码)安全软件，很多成立不久的安全企业为了尽早地推出产品，采取了将这些源代码进行分析，再进行一些改造完善后变成自己的产品推向市场的经营策略。这样做的确可以降低成本、缩短开发周期，但缺少了认真的市场调查，不了解用户真正的需求，这种产品是很难得到用户认可的，这也是目前一些新成立的企业生存异常艰难的重要原因。

重复投资现象严重

另外，安全企业界目前存在的严重的重复投资现象也很令人担忧。一些安全企业不顾市场的供求关系，还在盲目地开发一些已经完全成熟、技术含量不高的产品。例如，仅防火墙产品一项，国内目前叫得出名的产品就有二百多个，入侵检测和隐患扫描类的产品也有七八十个之多。但事实上，我国的安全市场尚处于培育阶段，根本没有这么大的需求，很多企业开发的产品销售量低得可怜就是最好的证明。这种目的性不强的开发行为，除造成了人力财力上的巨大浪费外，还加剧了产品间的恶意竞争，从而制约了我国安全产业的健康发展。

产品还存在空白

尽管目前市场上充斥着大量的安全产品，但安全市场方面还存在着很多空白。例如，防火墙、IDS产品虽然很多，但几乎都是面向局域网络的(大都是百兆以太网)，有一些企业的产品在网络负载接近饱和时还经常出现工作不正常、可靠性差的现象，真正能应用于高速（如千兆）、大规模网络环境的产品则极为有限。还有一些领域，如系统审计、安全网管、数据恢复等产品尚处于研发和推广的初期，缺乏高度智能化、易于使用的产品。如果国内安全企业能将研发重点放到这些领域，开发出真正满足用户需求、技术含量高的产品，对于提高企业的竞争力和抗风险能力是很有帮助的。

安全服务市场尚欠规模

需要说明的是，一个装备着先进安全产品的网络系统并不能表明它就是安全的，没有一个客观的安全需求分析、恰当的安全产品选型、安装与配置、日常的维护与监控和及时的应急响应，安全产品是不可能发挥其应有的作用的，信息系统也就不可能达到设计的安全等级，这些问题的钥匙就是目前很受重视的安全服务。据估算，在欧美一些发达国家中，网络与信息安全方面的投资已经达到了其信息化总投资的10～15%，其中安全服务与安全产品的市场规模已经基本持平，“花钱买服务”的观念已经成为这些国家的用户们的广泛共识。

到目前为止，我国的安全服务市场还没有形成规模，但已经有一些安全企业开始提供专业的安全服务，为用户解决了很多网络运营中出现的安全问题，取得了一些成功的经验。网络安全服务涉及的面非常广，如网络风险评估、安全解决方案的提供、系统配置更新、日常安全维护、网络状态监控、应急事件处理、数据恢复等，甚至还包括协助用户建立安全管理体系(组织规章制度等)。随着人们对安全认识的不断增加，安全服务必将像安全产品一样逐步得到人们的认可，其市场前景十分可观。

经济日报
ECONOMIC DAILY
2001年6月7日

网络安全软件和你并肩前行

李 捷

当好心的朋友关切地问你：你的网上生活安全吗？你可能会不无得意地说：“那还用说？我早就装了杀毒软件了！”你认为自己已经未雨绸缪，当然可以随心所欲地在网上冲浪了。

这样的观念一度很流行，但是今年以来，传统的杀毒软件市场出现了新情况，个人网络安全软件替代以往的杀病毒软件成为市场新热点。

信息安全是国家领导同志十分关心的问题，6月4日，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作“信息安全知识”报告，中共中央政治局常委、国务院总理朱镕基，中共中央政治局常委、国务院副总理李岚清等国务院领导同志和国务院各部门的负责人出席听课。何德全院士在计算机信息安全领域从事科学研究和科技管理工作多年，在这一天的讲座中，他分别就我国计算机信息网络的现状、如何做好信息安全工作等方面作了介绍。

我们曾经把防毒、杀毒看成网络安全的全部内涵，以为只要把电脑病毒拒之门外就万事大吉了。殊不知，网络安全是一个系统的概念，它包括病毒防治、隐私控制、抵御非法程序和黑客入侵的防火墙。而且，非法程序和黑客入侵造成的后果比病毒来得更惨痛。

仅仅查毒杀毒是不够的

及时地安装一套网络安全软件是非常必要的。在经历了许多无谓的牺牲之后，人们都希望为自己的电脑构建一个安全防护网，而不仅仅是杀毒。今年年初就已经面向个人用户推出网络安全软件的赛门铁克公司的有关人员告诉笔者：“目前，网民已渐渐认识到了网络安全的重要性，意识到了防毒、杀毒只是其中一小部分。”的确，这是一个观念的进步。在我国，计算机技术起步较晚，网络也未完全普及，因特网安全技术企业基本限于防杀毒软件制造商，瑞星杀毒、金山毒霸、KV3000、诺顿等都创造了可圈可点的杀毒业绩。但是，目前安全维护问题在一定程度上成为国内个人用户的瓶颈。

个人也需要网络安全吗？

是的，伴随网络的普及，这已经是确定无疑的了。

过去，自家的PC出了病毒，到单位的计算机房借个杀毒盘回家，杀一次毒至少管一两个月；现在不行了，网上的病毒也越来越多，而且，在家上网的频率越来越高，遭遇的就不仅仅是病毒，还有非法入侵等等。可以预见，在未来，因特网迅猛普及和用户的素质相应提高的情况下，能否为用户提供全面的解决方案将成为众网络安全软件技术上的一个分水岭，单纯的查毒、杀毒软件将会滞销，网络安全软件越来越受欢迎。

网络安全产品作用何在

作为网络安全产品，隐私控制和抵御非法入侵的能力是其区别于普通杀毒软件的重要标志，赛门铁克的诺顿网络安全特警2001作为迄今为止针对中国个人用户市场的第一个因特网