黑客时代 打响网络保卫战

◎我们身边的黑客攻击事件

车城房产网遭遇黑客攻击

2010年11月18日至23日，十堰“车城房产网”遭遇黑客攻击，网站一度无法打开页面，服务器瘫痪，网站长达几天的不稳定运行甚至停摆，令网站信誉受到影响。黑客还以继续攻击相要挟向受害人索要人民币2000元，被拒绝后持续发动攻击，致网站再次瘫痪，网站所在网络及六里坪某学校等互联网宽带出口也受到严重影响。

该案是我市首起网络攻击案。接到报警后，十堰网安部门抽调精干警力，成立专班，迅速开展内查外调，于2010年11月25日成功锁定犯罪嫌疑人藏身地。随后，侦破专班驱车1300多公里奔赴浙江温州，在该市瓯海区新桥街道富新路将正在网上实施黑客攻击的犯罪嫌疑人何某当场抓获。

经查明：犯罪嫌疑人何某，贵州省余庆县人，系浙江省温州市某公司员工。2010年11月18日至24日，犯罪嫌疑人何某利用黑客软件扫描到存在漏洞的服务器，然后多次非法侵入浙江、福建等地服务器，并植入攻击工具，然后远程登录至服务器，并利用事先植入的黑客攻击软件对我市车城房产网发动持续网络攻击，致该网站多次瘫痪，同时导致多家互联网运营商服务受阻，全市万余宽带用户受到影响。

白浪牵情网吧被网络攻击

2011年1月17日，网安支队接十堰经济开发区牵情网吧业主报案称：该网吧自1月13日起，屡次遭受不明黑客攻击，导致网络异常拥堵，网吧无法正常营业。

这起案件是继车城房产网遭网络攻击之后，我市发生的又一起针对网络实施的案件。市网安支队迅速抽调警力组成侦破专班，从摸排网络攻击来源入手，全力开展侦破工作。2011年1月27日，网安支队经过几天的连续奋战，成功侦破牵情网吧被网络攻击一案，抓获违法嫌疑人赵某（白浪某网吧业主），及时打击了黑客的违法行为，有力整治了网吧之间恶意竞争的不正之风。

经查，因赵某的网吧与牵情网吧地理位置较近，商业竞争激烈，为了争抢客源，违法嫌疑人赵某从网上购买黑客软件，多次对牵情网吧进行网络攻击。

日前，工业和信息化部发表公开数据称，中国网民数量已达4.77亿，已备案网站数量达382万个。全球领先的信息安全厂商卡巴斯基实验室也发布数据称，2011年第一季度，卡巴斯基实验室共拦截了412,790,509次恶意程序试图感染本地计算机的行为。排名前十的恶意软件资源国中，美国以28.56%的恶意软件资源比例高居榜首，而互联网发展历史只有短短十几年的中国，则以7.65%的数值居第四。

过去，黑客好比拥有盖世奇功的武林高手，而现在几乎会上网就能当一名黑客。调用别人的电脑资料就像掏自己的兜，在电脑里埋个“木马”、偷个QQ号，顶多就是只“菜鸟”。我们的生活不知不觉进入了黑客时代。在“抬手就黑”的年代，学一点反黑技巧已成了行走网络江湖必备的防身术。

记者 闵波
通讯员 毛群

◎行走网络江湖必备防身术

黑客时代 六大防身利器

黑客攻击手段可分为非破坏性攻击和破坏性攻击两类，最常用的攻击手段包括后门程序、信息炸弹、拒绝服务、网络监听、密码破解等。下面，介绍几种简单的“防黑”技巧。

屏蔽可疑IP地址

这种方式见效最快，一旦网络管理员发现了可疑的IP地址申请，可以通过防火墙屏蔽相对应的IP地址，这样黑客就无法再连接到服务器上了。

过滤信息包

通过编写防火墙规则，可以让系统知道什么样的信息包可以进入，什么样的应该放弃，如此一来，当黑客发送有攻击性信息包的时候，在经过防火墙时，信息就会被丢弃，从而防止黑客的进攻。

修改系统协议

对于漏洞扫描，系统管理员可以修改服务器的相应协议，例如漏洞扫描是根据对文件的申请返回值对文件存在进行判断的，这个数值如果是200则表示文件存在于服务器上，如果是404则表明服务器没有找到相应的文件。但是管理员如果修改了返回数值，或者屏蔽404数值，那么漏洞扫描器就毫无用处了。

经常升级系统版本

任何一个版本的系统发布之后，在短时间内都不会受到攻击，一旦其中的问题暴露出来，黑客就会蜂拥而致。因此管理员在维护系统的时候，可以经常浏览著名的安全站点，找到系统的新版本或者补丁程序进行安装，这样就可以保证系统中的漏洞在没有被黑客发现之前，就已经修补上了，从而保证了服务器的安全。

及时备份重要数据

亡羊补牢，如果数据备份及时，即便系统遭到黑客攻击，也可以在短时间内修复，挽回不必要的经济损失。数据的备份最好放在其他电脑或者驱动器上，这样黑客进入服务器之后，破坏的数据只是一部分，因为无法找到数据的备份，对于服务器的损失也不会太严重。一旦受到黑客攻击，管理员不要只设法恢复损坏的数据，还要及时分析黑客的来源和攻击方法，尽快修补被黑客利用的漏洞，然后检查系统中是否被黑客安装了木马、蠕虫或者被黑客开放了某些管理员账号，尽量将黑客留下的各种蛛丝马迹和后门分析清除干净，避免黑客的下一次攻击。

使用加密机制传输数据

对于个人信用卡、密码等重要数据，在客户端与服务器之间的传送，应该先经过加密处理再进行发送，这样做的目的是防止黑客监听、截获。对于现在网络上流行的各种加密机制，都已经出现了不同的破解方法，因此在加密的选择上应该寻找破解困难的，例如DES加密方法，这是一套没有逆向破解的加密算法，因此黑客得到这种加密处理后的文件时，只能采取暴力破解法。