“生产者”负责编写木马病毒程序，“销售商”定制或购进病毒商品后倒卖，“消费者”购买病毒程序后实施网络攻击——

“黑客产业链”瞄上政府网站

□据 新华社

范东东、文超两名仅有初中学历的90后，因非法侵入最高人民检察院反渎职侵权厅网站后台、非法控制长沙质量技术监督局等10多家政府网站，构成非法侵入计算机信息系统罪、非法控制计算机信息系统罪，最近被北京市朝阳区法院一审分别判处有期徒刑1年6个月和1年。

朝阳区法院法官辛祖国告诉记者，此案绝不是个案。国家互联网应急中心的监测报告显示，2010年5月10日至16日一周时间，中国境内有81个政府网站被篡改，其中包括4个省部级网站和25个地市级政府网站。

记者了解到，黑客之所以频繁入侵政府网站，原因之一是企图利用政府网站漏洞进行非法营利活动，并已经形成黑客非法牟利“产业链”。

1 给政府网站挂“黑链”赚钱

今年20岁的范东东，初中文化，新疆维吾尔自治区乌鲁木齐市人；今年20岁的文超，初中文化，四川省江油市人。这两人于2010年3月至5月，在河南省郑州市用计算机上互联网，并通过后门程序先后进入最高人民检察院反渎职侵权厅网站、长沙质量技术监督局、青海质量监督总站、抚顺政务公开网、佛山市高明区档案局、云南楚雄州人大常委会等数家网站后台更改网页源代码，为其他网站提升搜索排名，达到牟取利益的目的。后公安机关接群众举报，将二人查获归案。

范东东和文超虽然没学过计算机编程，但在一次QQ群聊天时，得知给被破解的政府网站挂“黑链”可以赚钱。二人通过“52CC”网站上的教学视频学习了简单编程知识，并通过“A5论坛”、“中国站长论坛”等论坛购买上述网站“权限”。

“网站‘权限’10元一个，黑链代码4元至7元一个，都是通过网上买的，自己不会做。”范东东供述说，使用购买的“权限”登录上述网站后，植入在网上购买的后门程序设定属于自己的“权限”，便于随时登录为“客户”添加黑链。

文超在网络论坛、聊天群等地方发布能添加黑链的帖子以招揽“客户”，并明码标价——“添加一条黑链代码收费4元至7元”。范东东将“客户”提供的关键词如“传奇私服”、“汽车交易”、“美国留学”等添加到黑链代码中，登录上述政府网站添加黑链并进行日常维护。“客户”可以使用“站长帮手网”里的管理工具查看某网站是否有其网站的链接。攻击政府网站3个月间，两人共获利6000元。

考察上述二人的犯罪过程，可看到一条清晰的非法牟利线路。

3月28日，网上大量政府网站被黑客篡改的新闻。

受到攻击的政府网站数量多得惊人。

被告人范东东（左）、文超在法院庭审中。

（本组图片据新华社）

2 黑客入侵政府网站的两个步骤

记者了解到，黑客入侵政府网站有两个步骤。第一步，破解并控制政府网站，即“拿站”。第二步，登录“后门”实施黑客攻击、实现非法营利。

第一步“拿站”一般分四个步骤：

一、熟悉网站、收集信息。先大致浏览入侵网站的相关网页，查看入侵网站网页的内容、设计布局等信息，借助网络输入网站的域名，查询域名注册的详细信息。

二、寻找漏洞、破解密码。技术较高的黑客通常利用自己编写的黑客工具查找网站的安全漏洞，利用漏洞破解网站后台管理员的用户名和密码。

三、查找入口、侵入网站。在破解密码的基础上，查找管理员登录入口。

四、植入后门、控制网站。在登录网站管理后台之后，黑客都会植入木马后门程序，如同管理员一样，修改网页、下载、上传、删除文件等等。

第二步，登录“后门”实施黑客攻击、实现非法营利。

通过第一步破解的网站，黑客会通过网络向外贩卖，业内称“卖漏洞”、卖服务器“权限”，一般均价10元就可以买到一个服务器“权限”。

拥有服务器“权限”，就可以登录网站服务器后台管理系统，常采用以下三种方式实施黑客攻击：

一、种木马病毒（圈内称“挂马”）、“卖流量”。“挂马”对象为有一定浏览量且有安全漏洞的网站。黑客将木马病毒植入政府网站，网民点击该网站的时候，就可能使网民的计算机终端中木马病毒，感染木马病毒的计算机内的银行账号、游戏账号密码、QQ号码、视频照片等信息就会被木马程序的远程控制者偷走，业内称感染木马病毒的计算机为“肉鸡”，种植木马程序的黑客通常根据下载或点击木马病毒产生的流量计费，称为“卖流量”。利用数量庞大的“肉鸡”组成的“僵尸网络”可以实施网络攻击，导致被访问的网站瘫痪。

二、植入黑链接、提高点击率。制作目标网站的超链接，如游戏网站、购物网站等，登录政府网站后门植入黑链接，网民打开政府网时实际上也打开了超链接的目标网站，由于政府网站在搜索引擎中排名靠前，从而可以提高目标网站的搜索排名，提高点击率。

三、修改、添加、删除政府网站信息。通过修改政府网站的内容，为特定需求者提供服务，实现非法获利。

3 黑客为何“偏爱”政府网站

为何政府网站屡屡被黑？为此，记者采访了中国核工业计算机应用研究所专家朱泉等，专家分析主要存在以下几方面原因：

第一，搜索引擎给政府类网站的权威值评重高、网页级别高。黑这类网站易于获得更高的搜索排名、更高的点击率，“挂马者”可以得到更多的“肉鸡”，添加黑链，目标网站可获得更高的点击量，从而实现更多的营利。

第二，部分政府网站尤其是基层政府网站安全漏洞多、安全技术防范薄弱，易于被破解。黑客攻击政府网站多利用的是政府网站这一平台，很少窃取内部信息，看似对政府网站危害不大，使得部分政府网管部门对外网安全重视程度不够。有些网站服务器甚至连防火墙都没装，是名副其实的“裸网”。

其三，部分政府网站提供成绩查询、资格证书编号验证等便民服务，部分不法分子为实现非法目的，不惜高价雇佣黑客修改、添加、删除私人信息，使得此类政府网站易于成为黑客攻击的对象。如2008年的江西省卫生厅被黑客攻破添加假医师资格证书编号案件、湖北省的假车牌案件等。一般而言，此类政府网站的安全级别相对比较高，由于“客户”肯出高价，部分黑客不惜以身试法。

■延伸阅读

黑客

黑客是指利用计算机信息系统安全漏洞非法侵入、控制、破坏计算机信息系统的人。黑客源自英文单词hacker，原意指用斧头砍柴的工人，最初的黑客是指专门研究、发现计算机和网络安全漏洞的计算机爱好者。

危害网络安全谁担刑责？

面对严峻的网络安全形势，2009年，我国刑法新增两款规范打击计算机网络犯罪的规定，新增了非法获取计算机信息系统信息罪、非法控制计算机信息系统罪以及提供用于侵入、非法控制计算机信息系统的程序、工具罪3个罪名。

攻击计算机信息系统的黑客、黑客行为的协助者都有可能被追究刑事责任。