来源：toinet&#39; blog 作者：toinet  
  
又是一个美好的周末，老婆约了同事出去玩了，就留我一个人猫在家里玩电脑。大概7点多钟，正在逛着论坛，QQ突然传来一阵‘滴滴’声，平常我都是隐身状态，而且不爱聊天，纳闷着的我打开消息一看，HOHO，一个小男孩加我。我们在这里暂且称呼他为a吧，资料上写的是来自山东，19岁。  
  
“在吗？想跟你聊聊！”-------a发出了加为好友的邀请，  
  
“不在”，  
  
“不在？不在你怎么说话的！”------a似乎还有点幽默感，仍然坚持着。  
  
“你有什么事？”我依然在拒绝加入的框框里回复着他。  
  
“这样太不方便拉，我有些事情想跟你说，真有事”…….他还急了。  
  
“就这样说吧，我这里回复你不是很麻烦！”嘿嘿一笑，继续看着黑防被黑的帖子。  
  
“你把我网站给黑了，我要拿回来。你先加我QQ再说”…….a的话好象不太客气了  
  
　　不开玩笑了，我心里一紧，nnd，从来没有改过别人的网页啊，顶多也就是拿个webshell，试试我的新木马能不能免杀。这不至于被人发现了吧，反正应该没什么事，加了他再说。  
  
　　“你刚才说什么？”至少我觉得没理由啊，即使我在他网站上种了马，或者试过新的asp木马，他也不可能知道是我做的啊！tmd，搞的我紧张西西，看来没有好心情去体会这个安逸的周末了。  
  
　　“我的网站被你黑了，[www.xxx.com](http://www.xxx.com/)，你在我的后门上留了QQ，所以我过来找你了”。…..a说的理直气壮，小犬参拜‘人民公厕’时的理由跟他一样充分。  
  
　　呵呵，看着他发过来的消息，我哭笑不得。原来，今天下午在对我的webshell 例行检查的时候，图（一）  
  
　　居然发现这个网站下居然还有个莫名的asp文件，打开一看，靠啊，是个asp木马。图（二）  
  
　　看来是个小菜，直接从网上下的站长助手6，除了改过名字和密码，什么也没动！username一栏填的是“1987”，密码那里往下应该是用SCRENC.EXE加过密，一堆乱玛。想着好笑，在ie地址栏把我的马换成了他的马，连接，登陆框出来了，填入“1987”，回车。进去了（社会工程学）~~~那还有什么说的，直接把木马内容删除了，同时留下了我的QQ。图（三）  
  
“你是站长？”我一头雾水。  
  
“是啊，那个站长助手是我朋友帮我装上去的，方便我远程管理。你们平时不都是这样做的吗？”  
  
“哦，”我老脸一红“我还从来没有建过站了”  
  
“现在不管了，你把那个站长助手还给我啊，”  
  
“你不是吧，自己去搞，大不了以后我不碰你了”  
  
“都跟你说了，是我朋友帮我装的，用那个后门管理挺方便的。那朋友出差了，都不知道什么时候能回，你既然能改成这样拉，那你也能给我复原了。”…….a的口气越来越严厉了，我甚至可以联想出他的模样和电影里的小太君完全是一个模子里刻出来的。  
  
　　唉，怎么说了，反正是自己做的了，这种小事真没必要再去冤枉其他人，犯不着说是别人故意留的我QQ，来栽赃嫁祸吧。  
  
“ok，哥们答应你了，等会给你还原。”一个小站，我还没放在眼里。  
  
　　down一个站长助手，加密，还是他的username和password，哈，1987，好垃圾的密码。还真是个小菜。用我的后门上传，试了一下连接，跟我下午操作时一模一样，连asp木马的文件名都改成了他那原来的模样。5分钟后，一切搞定，随即在QQ里通知他完工了。  
  
　　多么可怜的周末啊，就这样被个小菜给毁了，继续看我的帖子吧！  
  
　　。。。。。。  
  
　　要说故事到这里本没什么希奇的，相信大家可能都会碰到类似的事情，可是，正是有着他的不寻常，才有了这个故事的标题：社会工程学。就让我带着读者继续吧。  
  
　　。。。。。依旧在网上晃悠着，转眼都11点了，正要关电脑准备睡觉的时候，QQ又是一阵吵闹，又有人加我了。深更半夜谁那么无聊啊。  
  
“有事找你聊聊”，我打开资料介绍，男，22岁，地址来自福建，我们称他为b吧  
  
“都是男人有什么好聊的”我拒绝了  
  
“你黑了我的站，[www.xxx.com](http://www.xxx.com/)，为什么？”  
  
“有没有搞错啊”我一下子愤怒起来，“什么鸟站，还这么多管理员跑过来嚷嚷，不都已经帮你们把后门给改过来了吗？还让我怎么样？我都说过以后再不碰你们了。”我的忍耐力终于不是那么完善，手指和键盘急速撞击产生的刺耳噪音顿时将我的房间充斥。  
  
　　余怒未消，“还亏我把你们站的漏洞补了又补，现在你们说一声我就走人了，你们还想怎么样？再说了，不就是装了一个木马吗？我还没装远程控制了，凭这就说我黑了你们的站？你们是不是有毛病啊！”  
  
“我不知道你在说什么，你可以去看看主页。最好能给我个交代，要不然我就报警。”这丫的也不含糊。  
  
“操，懒的理你，娘西皮的！”我终于没好气了，跟这种人犯不着生气，何况我都一把年纪了。  
  
　　今天真是郁闷透了，去看看怎么回事也好。连上我的木马。晕，居然还在，看来那小子还真是个菜鸟，这样都找不到我的马儿，只不过他之前安装的那个马也没了，估计是换了名字。除此以外，这站看起来一切正常。另开一个窗口，再来看看他的主页。  
  
　　。。。。。。我终于明白《大腕》里的葛优为什么能一下子就疯掉了，在我眼前出现的IE里，显示出来的是我们大家都非常熟悉的‘黑客帝国’场景，而非是原来的主页，‘我的QQ’四个猩红的大子后面跟出来的数字竟然是我的号码。TMD，我被那小子骗了。现在最急迫的事情就是修复好b的网站了，其他的以后再说。  
  
　　是男人就不能在同一个坑再栽下去，在QQ上得到b的ip，然后ping一下网站，返回的结果和bQQ的ip 一致。可以说明一点问题，但还是不保险。反正自己的webshell还在，一切都还简单。再次连上我的asp木马，传cmd.asp和鸽子上去，运行鸽子服务器，然后远程桌面，b的屏幕出现在我的眼前，看见了他的QQ上有我，正准备给我发送信息了，毋庸质疑，确定b就是管理员了。接下来的事情当然要说清楚了的好。  
  
　　老老实实的打开qq将我之前发生的事情原原本本的告诉了b。然后帮助b把他的网站恢复备份，清除了a在网站上留下改过名的木马，当然还有我种下的asp木马和鸽子。随后还花了大力气看了一遍所有的网页以防止被a种上了网页木马。  
  
　　一翻折腾下来，看了看时间，都已经是3点多了，唉，我还以为今天是个愉快的周末了，社会工程学真是害人啊。  
  
　　学黑的人，每天可能都在应用着社会工程学，可我今天就吃了这个亏，奶奶的。虽说自己的心理很不舒服，但从另外一个角度来看的话，19岁的小孩子都能运用的这么好，那这项技术绝对是黑客们永远追求下去的其中一个主题，**道理人人都会说，真正能彻底懂的人又有多少呢？**