SILIC

QQ 钓 鱼 黑 吃 黑

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) 钓鱼邮件

1.1 虚假 QQ 申诉钓鱼邮件

1.2 专业钓鱼选手

2) 深入调查

2.1 以暴制暴黑吃黑

2.2 钓手

2.3 提权回顾

1) 钓鱼邮件

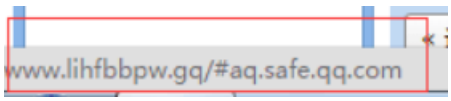
习科攻防团队除了每天的日常工作外,还会时不时的应对来自互联网各处的大牛或小黑们的技术挑衅，近日，习科某核心收到一封 QQ 申诉的钓鱼邮件，于是大伙兴起把这个钓鱼专业户玩坏了。

1.1 虚假 QQ 申诉钓鱼邮件

近日，习科某核心收到一封 QQ 申诉的钓鱼邮件，首先来看一下这是一封什么样的钓鱼邮件。

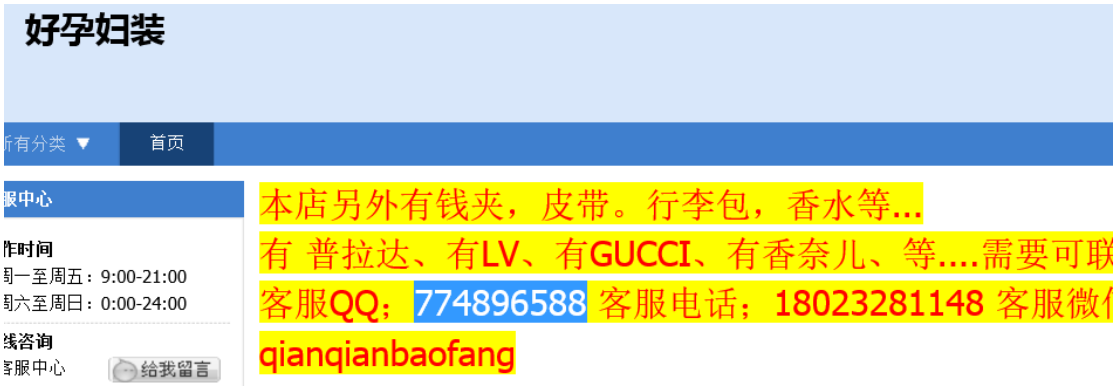
那么接着就要吐槽一下这拙劣的手法，发件人为 sferrht@126.com 邮箱，这完全在恶狠狠的侮辱技术人员的智商，这都能上当的话习科建议以后完全脱离互联网好了，毕竟这么乱的圈(Juàn)不适合这种智商。

接着是“点击取消本次申诉请求”指向的奇怪链接，已经无力吐槽了。



当然了，习科的小伙伴们脑洞大开，在想邮件中的“申诉人”774896588(QQ)会不会就是钓鱼选手的本尊？

于是花了 30 秒对这个账号进行了搜索，来确认这个 QQ 是不是钓鱼选手的本尊。



淘宝 28 元“托腹孕妇骷髅头图案打底裤”，不管你们信不信，反正习科是不信。如果这是一场针对“程序猿”和“黑阔”的营销行为，那只能说孕妇打底裤什么的去死吧，我们要韩版芸能偷拍事件女主充气娃娃全套！

1.2 专业钓鱼选手

邮件中使用的钓鱼网站地址是：www.lihfbbpw.gp，使用 dig 命令得到如下信息：

```
;; QUESTION SECTION:
;www.lihfbbpw.gq.        IN    A
;; ANSWER SECTION:
www.lihfbbpw.gq.  600  IN    A     198.211.3.102
;; AUTHORITY SECTION:
lihfbbpw.gq.          600  IN    NS    f1g1ns1.dnspod.net.
lihfbbpw.gq.          600  IN    NS    f1g1ns2.dnspod.net.
```

为什么这个钓鱼网站的钓鱼手法很拙计，但是仍然称站长是专业钓鱼选手呢，看一张图就知道了。

罗列了一下，服务器中一共解析了 27 个域名：

FTP 账号 jkahtwf 中：

www.zotf.CF
www.kotll.CF
www.ikoiko.CF
www.jeiz.CF
www.ycbgei.GQ
www.ghjjx.GQ
www.rdbi.GQ
www.ddzzdv.GQ
www.dgthjrrn.GQ
www.cummmmg.GQ
www.bntfxguf.GQ
www.lihfbbpw.GQ
www.mucswuu.GQ
www.foarxpq.GQ
www.oeuaoye.GQ
www.sdufpjt.GQ
www.ykeagwo.GQ
www.zvrvlbt.GQ

FTP 账号 lrlcayxlyq 中：

www.vjrdvp.ga

FTP 账号 ewrdjye 中

www.cogkm.GQ
www.xrhdi.GQ
www.rmnt.GQ
www.suks.GQ
www.cexkibh.GQ
www.aeuqkw.GQ
www.zlhfttll.GQ
wwqc.wmciksaq.GQ

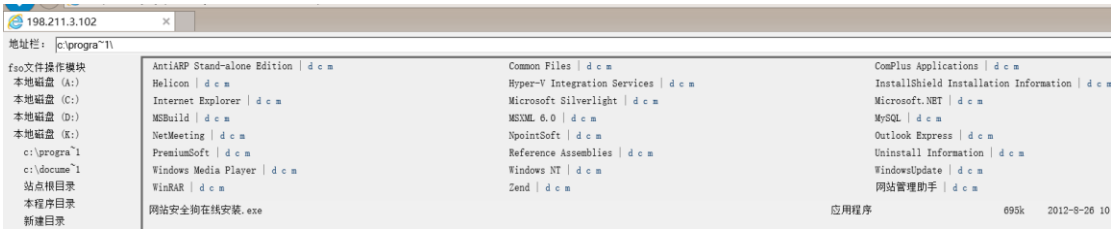
大部分域名都是解析到钓 QQ 账号密码的，也有少部分域名解析到钓取点卡程序中的。

2) 深入调查

就这程度也玩黑？习科建议玩这些钓鱼的小伙们转业去青岛海边捡东西吧，捡手机、金项链、金耳环、钻戒什么的也比玩黑钓鱼赚的多啊，是什么事情让你想不开要玩黑钓鱼的？又是谁给你的自信让你来挑衅习科？

2.1 以暴制暴黑吃黑

所有的钓鱼域名来自免费域名商 freenom。而钓鱼服务器的 ip 地址 198.211.3.102 经过反向解析得到的地址为：102-3-211-198-dedicated.multacom.com，该地址属于云主机商 multacom，作为一名有操守的安全从业人员，我们是不会在 Multacom 租个 2k3 顺便开上 Cain 玩的，作为有操守的安全从业人员，我们会向 Freenom 和 Multacom 索取广告费的。



虽然没装 MSSQL 数据库和 serv-u 之类的软件，系统装了 MySQL，存在一个允许外连的 root 账户，密码为：2CFE99AF51299CB34CF57CBE4E66D63AAF3D9391。但是 MySQL 的服务没跑起来。

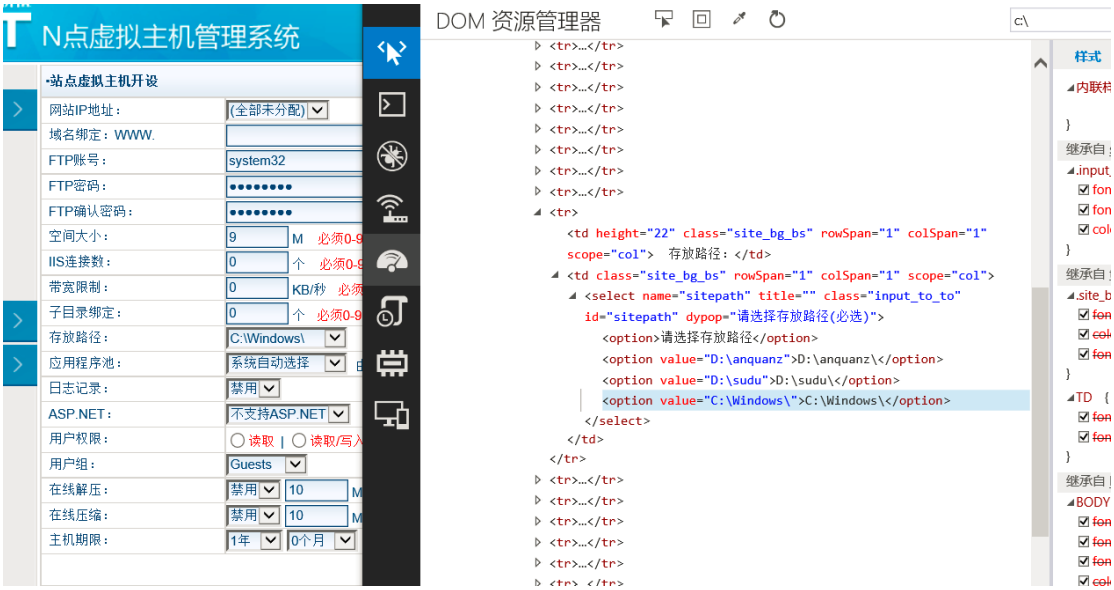
既然是 win2k3 的系统，在控制面板开个 FTP 目录设置为 C 盘下，替换 shift 后门即可。

```
50 name       pwd        realname
51 D:/anquanz/ewrdjye/web/ee/hjk62@$@$#fj21/lin8384^%#775@@!.mdb
52 8384775    1314333    admin
53 D:/anquanz/jkahtwf/web/gg/hjk62@$@$#fj21/lin8384^%#775@@!.mdb
54 8384775    870801     admin
55 D:/anquanz/jkahtwf/web/gg/hjk62@$@$#fj21/
56 1090276644@qq.com    asdasd..     橘子情深一吻
```

读取了硬盘中的几个 MDB 数据库的账号和密码，一个 QQ 赫然出列：1090276644。于是就有了“然后”。。。

在进行下一步“然后”之前，简单提一句，在这个 VPS 这种关于 N 点虚拟主机提权的问题，也就是替换 sethc.exe 是怎么完成的。

N 点虚拟主机创建虚拟站点账户的时候，会以 FTP 账户名为文件名，在网站目录中创建子目录。如果网站目录设置为 C:\windows，FTP 账户名为 system32，那么创建网站完成后，FTP 账户 system32 将拥有 c:\windows\system32 这个目录的权限。



这里开设 system32 目录下的 FTp 只需要使用 IE 的 F12 即可操作完成，开设界面 POST 表单中的变量值本地重写一个 value，这个路径的 value 只要格式合法(不含特殊字符，不含 admin 等敏感路径)就可以创建。

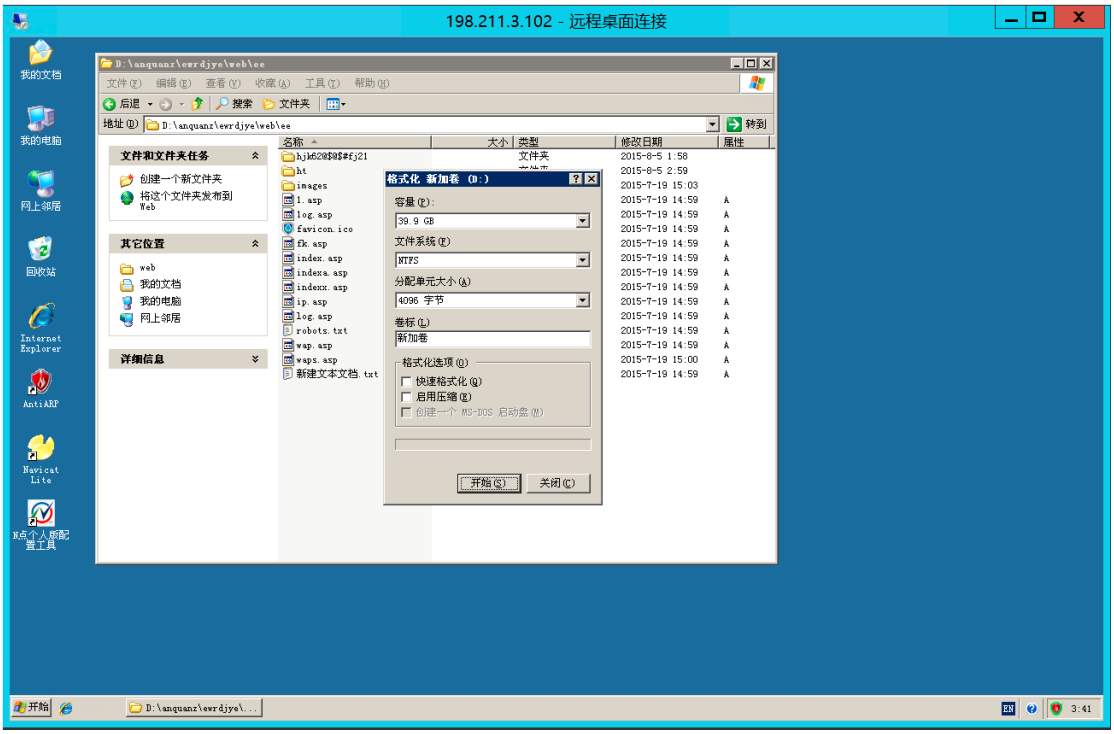
至于效果嘛，如图所示：

首先删除 system32 目录下子目录 dlcache 中的 sethc.exe(先删 system32 的会被重新创建)。然后上传一个自己的 sethc.exe 好了。

在这之前，管理员将 temp 目录、zend 目录、回收站目录以及 cmd.exe 等全都锁死了。然而使用 N 点虚拟主机控制面板只需要建立权限、删除重传即可。

顺便说一句，除了解除了目录限制，埋了 cmd 和提权 exp，我们还改了 php.ini，埋了

dll hijack。。。至于结果嘛



2.2 钓手

从数据库中获得了钓卡号的管理员 1090276644(QQ)，那么必然是要折腾一番的。

该 QQ 主人资料如下：

杨洋，1990 年 8 月 25 日，吉林省四平市公主岭

身份证号：220381199008254256　　电话号码：18737222258　　QQ：1090276644

常用用户名/密码：fkljylove110/mxinyu163

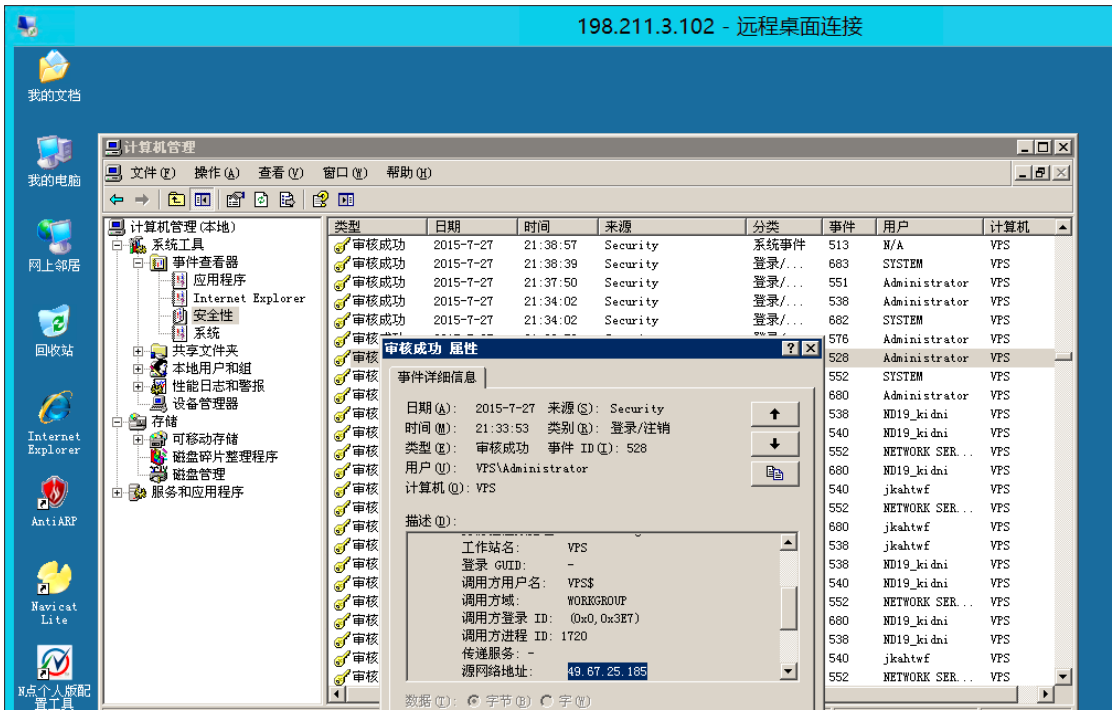
现居：安阳市殷都区安钢大道王裕口小庄村村委会对面

职业：以游戏(DNF)代练、盗号洗号为生。

父亲：杨占生(220381195612194212)，电话：13180932011

母亲：李春华

从钓鱼程序后台的登陆记录来看，钓鱼盗号洗号洗点卡一条龙里面这个杨洋只是参与过钓鱼而已，并不是真正的幕后实施者。



看到上面的信息，有些人沾沾自喜的以为这件事被背了黑锅，殊不知在报告中被我们爆出信息的人其实我们是打算放过他的，真正被上报网监的是这个南通市的 49.67.25.165。

至于这个幕后实施者，查其在另一个国内虚拟主机运营商“你拍一科技”(查无此公司，业务实际运营人李景绍)中开通名为 siooef3 的 FTP 账户(绑定域名 wfgchsn.gq)，之所以还没有获得钓鱼选手的支付宝信息，是因为李景绍的“你拍一科技”似乎问题更大一些，其购买的 VPS 开设虚拟主机卖给的满是国内做六合彩、博彩的站点，然而更大的问题比方说广西南宁的贩毒(htgs168.com)这样的也是在其服务器上面。

习科只想说，并不是不抓你，而是金额不够大。因此送你们四个字：零存整取。最后再送一句话，习科并不妨碍黑产白产怎么挣钱，但是不要自己想不开来挑衅习科的技术。