Vulnerability, malicious code appeared in the MBR destruction function using Hangul file

Malware Information 2014/12/10 18:12

Vulnerabilities recently received a file with the destruction and MBR destruction capabilities for major extension to the existing file in addition to the backdoor functionality that existed in Hangul document file is received attention is required.

December 9, 2014 received the first vulnerability Hangul document files were used for both groups known vulnerabilities, patching does not work on the latest products. Total of 9 document file has been received, and all of the same malicious file therein.

1. The files and services that generate

% System% registered the generated DLL as a service to the folder / drive upon, information that is used has a list on the inside of malicious code, and select one of the items below at random.

[Service name]

- BitLocker Drive Decryption Service
- Internet Connection Service
- Media Center Service
- Network Storage Service
- Peer Networking Address
- PNRP Machine Name
- Power Policy
- Program Compatibility Service
- Remote Registry Configuration
- Smart Card Management Service
- Tablet PC Management Service
- Task Schedule Manager
- Thread Ordering Service
- WebClient Manage Service
- Windows Color Adjustment
- Windows Modules Management
- Windows Time Synchronization
- Wired Config Service
- WLAN Config Service
- Workstation Management

[Create file]

- Bddsvc.dll

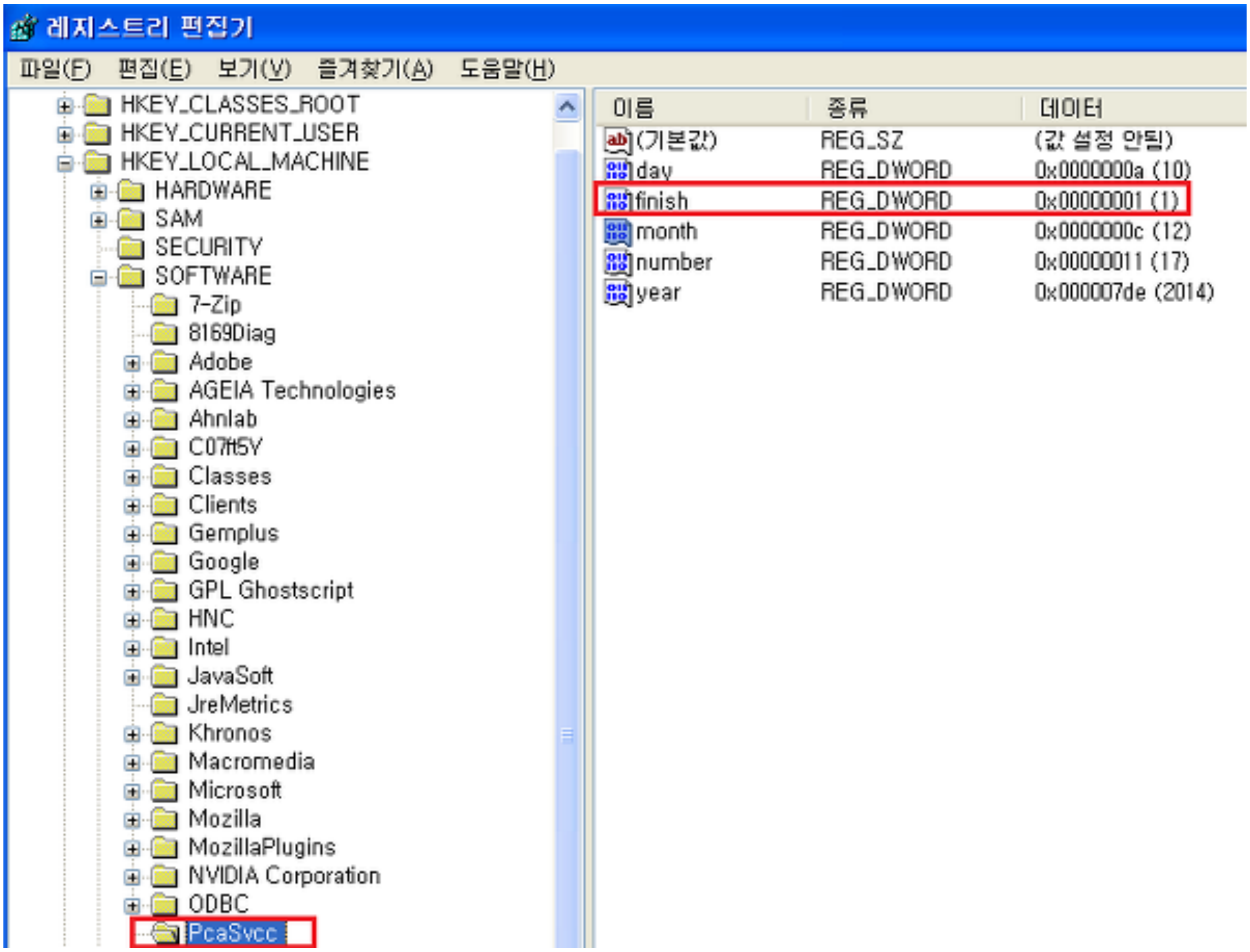
- iconsvc.dll
- ehressvc.dll
- netstsvc.dll
- pnas.dll
- pnrpmchname.dll
- pwpsvc.dll
- pcssvc.dll
- rregconf.dll
- scardmngsvc.dll
- tcpmsvc.dll
- tschmng.dll
- mmthread .dll
- wcmngsvc.dll
- coladj.dll
- wndmodmng.dll
- timesyncsvc.dll
- wiredconfsvc.dll
- wlanconf.dll
- wstmng.dll

Service Description

- BDESVC hosts the BitLocker Drive Decryption service.
- Provides network address Translation, Addressing, name resolution and / or Intrusion Prevention Services for a home or Small Office network.
- Allows Media Center to Locate and Connect to the Computer.
- This service Delivers network Notifications (E.
- Enables Multi-party using Peer-to-Peer Communication Connecting.
- This service publishes a machine name using the Peer Name Resolution Protocol.
- MANAGES power policy and power policy Delivery Notification.
- This service Provides Support for the Program Compatibility Assistant (PCA).
- Enables remote users to modify Registry configurations on this Computer.
- Access to Smart Cards MANAGES read by this Computer.
- Enables Tablet PC Ink PEN and functionality
- Enables a user to Configure and Schedule Automated tasks on this Computer.
- Provides Execution ordered for a Group of threads within a specific period of time.
- Enables Windows-based Programs to create, Access, and modify Internet- Files based.
- The service hosts third-party WcasPlugInService Windows Color System color and gamut map Device Model Model Plug-in modules.
- Enables Installation, modification, and Removal of Windows updates and Optional Components.
- Maintains date and time Synchronization on all clients and Servers in the network.
- The Wired AutoConfig (dot3svc) service is responsible for Performing IEEE 802.1X
- The WLANSVC service Logic Provides the Required to Configure, Discover, Connect to, and disconnect from a Wireless local Area network.
- Creates and maintains client network connections to remote server using the SMB protocol

2. MBR destruction time

MBR destruction is done through a 'number' value of the registry key value of the items checked below ("0" if the destructive behavior than the largest value) is set to '0' value at the time of initial infection. The following [Figure 1] shows the contents of the registry key 'PcaSvcc' items registered by the malware. MBR destruction operations to determine the value of number entry through the time information of the user's system **after December 10, 2014 11:00 a.m.** when a, is set to non-zero value is, the MBR is destroyed feature to work .

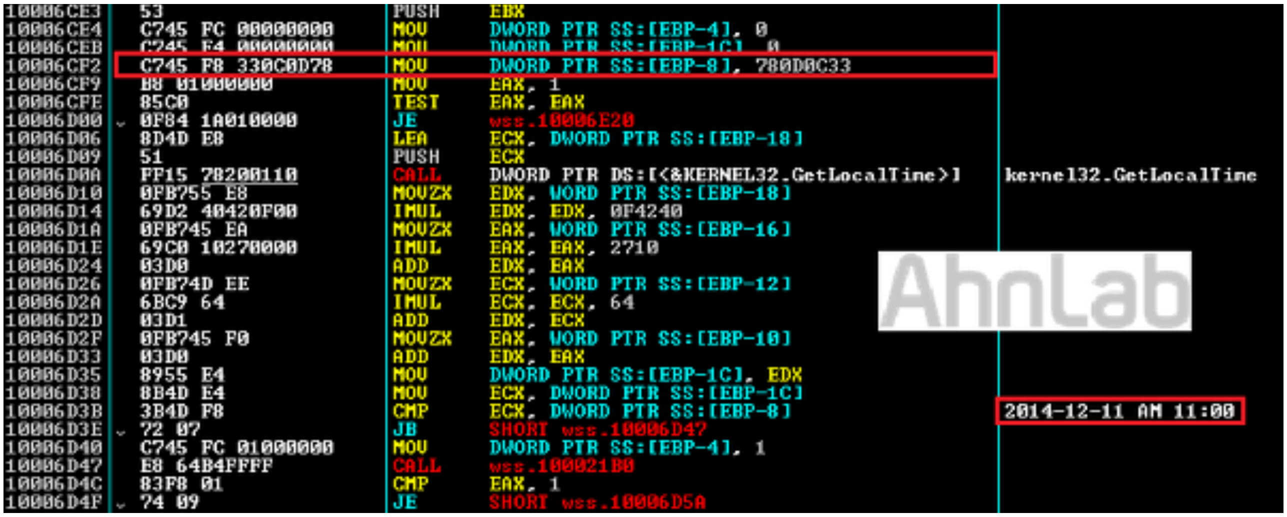


HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HARDWARE
SAM
SECURITY
SOFTWARE
7-Zip
8169Diag
Adobe
AGEIA Technologies
Ahnlab
C07ft5Y
Classes
Clients
Gemplus
Google
GPL Ghostscript
HNC
Intel
JavaSoft
JreMetrics
Khronos
Macromedia
Microsoft
Mozilla
MozillaPlugins
NVIDIA Corporation
ODBC
PcaSvcc

이름	종류	데이터
(기본값)	REG_SZ	(값 설정 안됨)
day	REG_DWORD	0x0000000a (10)
finish	REG_DWORD	0x00000001 (1)
month	REG_DWORD	0x0000000c (12)
number	REG_DWORD	0x00000011 (17)
year	REG_DWORD	0x000007de (2014)

Figure -1] MBR destruction upon reference to the registry value

In [Figure 2] shows a code section that compares the time information for determining a destruction inside MBR infection. Malicious code stored in the internal "0x780D0C33" value and the operation to compare the time information through a specific operation of the system time obtained by the GetLocalTime function call can be seen that true.

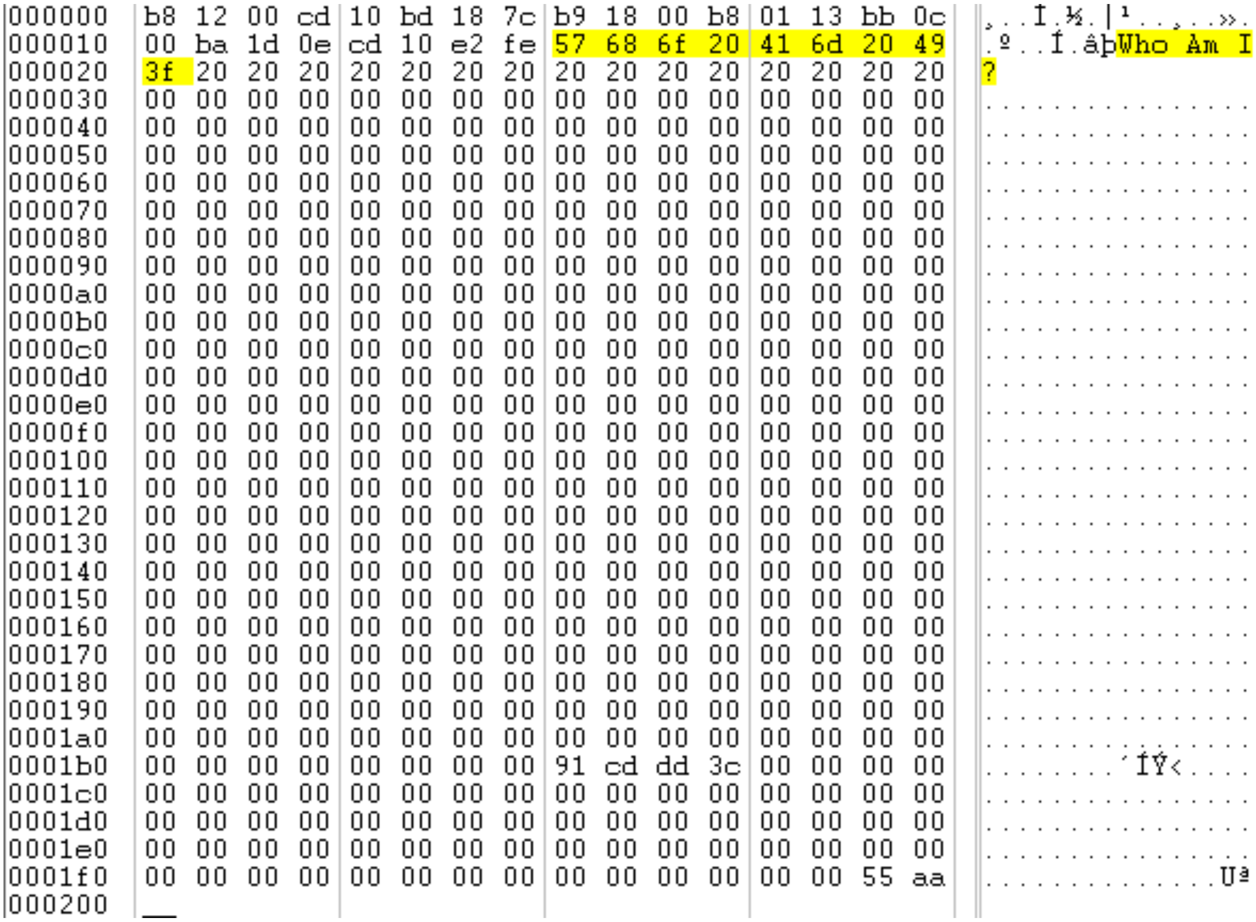


```
10006CE3    53                PUSH   EBX
10006CE4    C745 FC 00000000  MOV    DWORD PTR SS:[EBP-4], 0
10006CEB    C745 E4 00000000  MOV    DWORD PTR SS:[EBP-1C], 0
10006CF2    C745 F8 330C0D78  MOV    DWORD PTR SS:[EBP-8], 780D0C33
10006CF9    B8 01000000       MOV    EAX, 1
10006CFE    85C0              TEST   EAX, EAX
10006D00  ⌄ 0F84 1A010000     JE     wss.10006E20
10006D06    8D4D E8           LEA    ECX, DWORD PTR SS:[EBP-18]
10006D09    51                PUSH   ECX
10006D0A    FF15 78200110     CALL   DWORD PTR DS:[<&KERNEL32.GetLocalTime>]   kernel32.GetLocalTime
10006D10    0FB755 E8         MOVZX  EDX, WORD PTR SS:[EBP-18]
10006D14    69D2 40420F00     IMUL   EDX, EDX, 0F4240
10006D1A    0FB745 EA         MOVZX  EAX, WORD PTR SS:[EBP-16]
10006D1E    69C0 10270000     IMUL   EAX, EAX, 2710
10006D24    03D0              ADD    EDX, EAX
10006D26    0FB74D EE         MOVZX  ECX, WORD PTR SS:[EBP-12]
10006D2A    6BC9 64           IMUL   ECX, ECX, 64
10006D2D    03D1              ADD    EDX, ECX
10006D2F    0FB745 F0         MOVZX  EAX, WORD PTR SS:[EBP-10]
10006D33    03D0              ADD    EDX, EAX
10006D35    8955 E4           MOV    DWORD PTR SS:[EBP-1C], EDX
10006D38    8B4D E4           MOV    ECX, DWORD PTR SS:[EBP-1C]
10006D3B    3B4D F8           CMP    ECX, DWORD PTR SS:[EBP-8]             2014-12-11 AM 11:00
10006D3E  ⌄ 72 07             JB     SHORT wss.10006D47
10006D40    C745 FC 01000000  MOV    DWORD PTR SS:[EBP-4], 1
10006D47    E8 64B4FFFF       CALL   wss.100021B0
10006D4C    83F8 01           CMP    EAX, 1
10006D4F  ⌄ 74 09             JE     SHORT wss.10006D5A
```

Figure -2] MBR destruction timecode to compare

3. MBR destruction techniques

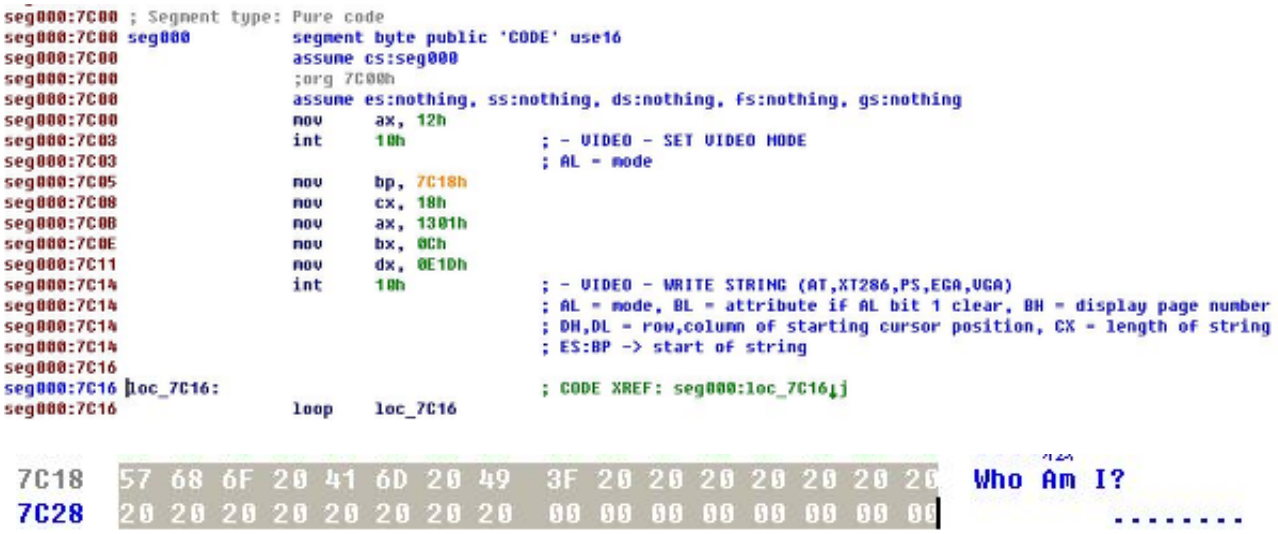
MBR destruction is overwritten for the 0x200 (512 bytes), it can be seen the data filled in as shown in [Figure 3] below. Infection, 'A' ~ 'Z', the same process is repeated for all the drives.



```
000000  b8 12 00 cd 10 bd 18 7c b9 18 00 b8 01 13 bb 0c  ¸..Í.½.|¹..¸..».
000010  00 ba 1d 0e cd 10 e2 fe 57 68 6f 20 41 6d 20 49  .º..Í.âþWho Am I
000020  3f 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  ?
000030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0001a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0001b0  00 00 00 00 00 00 00 00 91 cd dd 3c 00 00 00 00  ........'ÍÝ<....
0001c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0001d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0001e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0001f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 aa  ..............Uª
000200
```

Figure -3] MBR data

The following [Figure 4] is overwritten with the contents of the MBR code, and has the ability to output the string during boot "Who Am I?".

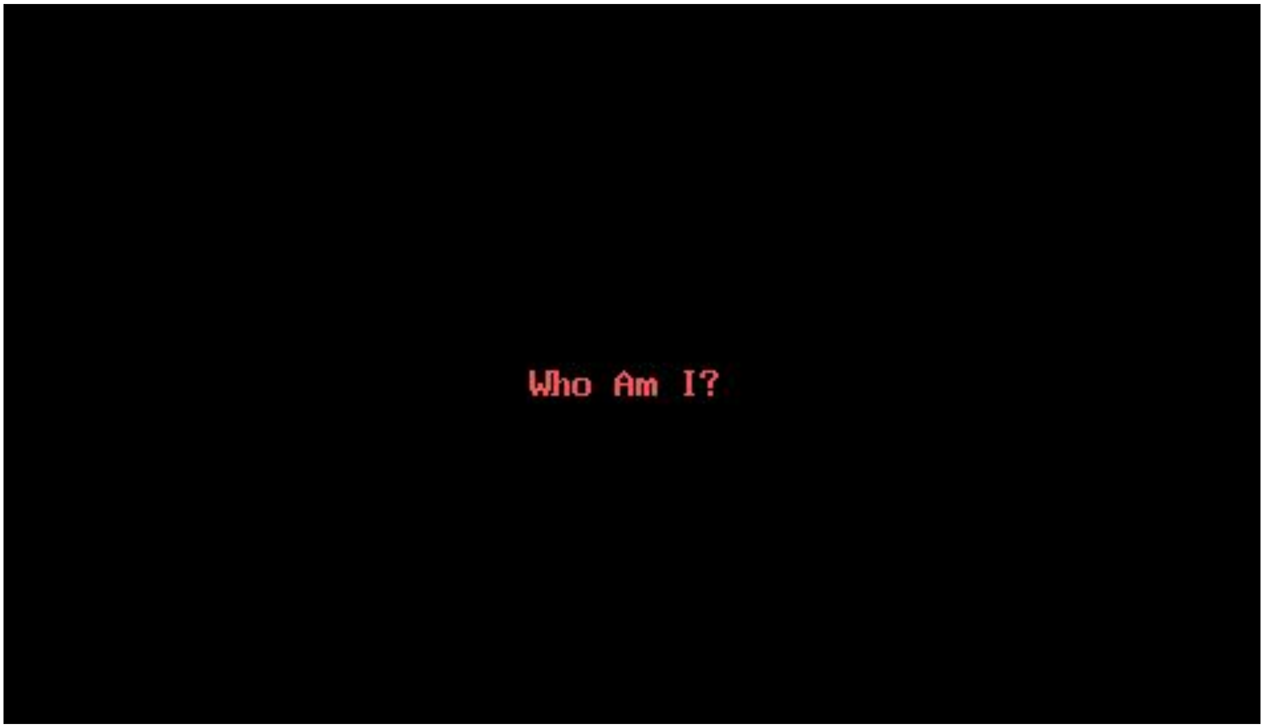


```
seg000:7C00 ; Segment type: Pure code
seg000:7C00 seg000          segment byte public 'CODE' use16
seg000:7C00                 assume cs:seg000
seg000:7C00                 ;org 7C00h
seg000:7C00                 assume es:nothing, ss:nothing, ds:nothing, fs:nothing, gs:nothing
seg000:7C00                 mov     ax, 12h
seg000:7C03                 int     10h             ; - VIDEO - SET VIDEO MODE
seg000:7C03                                         ; AL = mode
seg000:7C05                 mov     bp, 7C18h
seg000:7C08                 mov     cx, 18h
seg000:7C0B                 mov     ax, 1301h
seg000:7C0E                 mov     bx, 0Ch
seg000:7C11                 mov     dx, 0E1Dh
seg000:7C14                 int     10h             ; - VIDEO - WRITE STRING (AT,XT286,PS,EGA,VGA)
seg000:7C14                                         ; AL = mode, BL = attribute if AL bit 1 clear, BH = display page number
seg000:7C14                                         ; DH,DL = row,column of starting cursor position, CX = length of string
seg000:7C14                                         ; ES:BP -> start of string
seg000:7C16
seg000:7C16 loc_7C16:                               ; CODE XREF: seg000:loc_7C16↓j
seg000:7C16                 loop    loc_7C16

7C18  57 68 6F 20 41 6D 20 49  3F 20 20 20 20 20 20 20  Who Am I?
7C28  20 20 20 20 20 20 20 20  00 00 00 00 00 00 00 00          ........
```

Figure -4] MBR code

The following [Figure 5] After MBR infection, a screen visible to the user reboots.



Who Am I?

[Figure 5] boot screen

4. File destructive features

Malicious code can destroy the functionality of a file having a particular extension in addition to destruction together also has functions for the MBR. Destroy the target file identified to date are:

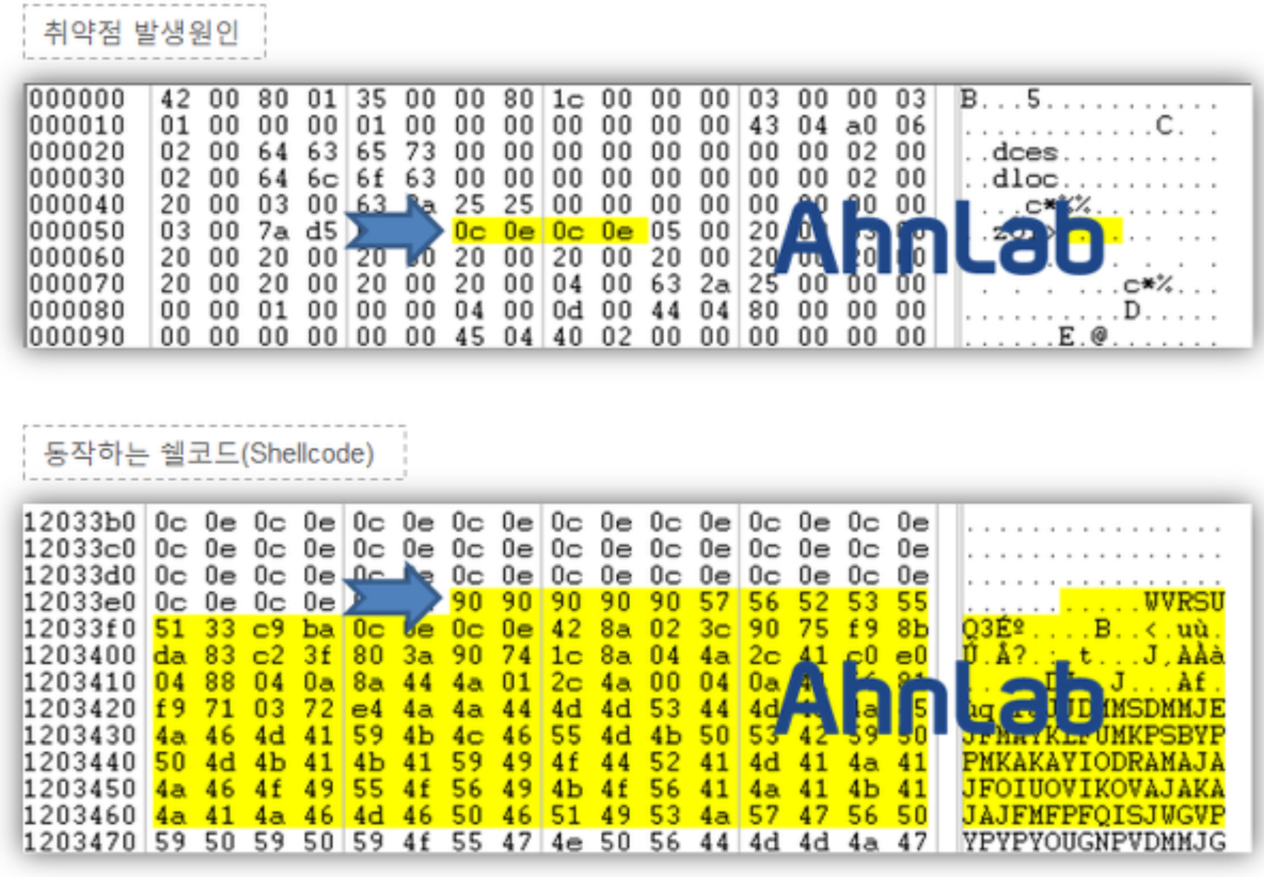
- HWP
- doc

- PDF
- docx
- ALZ
- ZIP
- RAR
- egg
- iso
- EXE
- dll
- sys

Locate the files with the extension of the above 'A' ~ 'Z' drive changes and performs a process to fill a NULL value to 4096 bytes (4K) size.

5. Hangul vulnerability information

Received nine vulnerabilities Hangul document and the contents hereof are both used the same vulnerability varies. In [Figure 6] shows the portion of the shell part and the operation code for generating a vulnerability. The layout of paragraphs in Hangul document and vulnerability occurs in the course of processing the part that is responsible ('HWPTAG_PARA_LINE_SEG') and, shellcode (ShellCode) and heap spray insert a paragraph of text for (Heap Spray) ('HWPTAG_PARA_TEXT') is used was.



취약점 발생원인

```
000000  42 00 80 01 35 00 00 80 1c 00 00 00 03 00 00 03  B...5...........
000010  01 00 00 00 01 00 00 00 00 00 00 00 43 04 a0 06  ............C...
000020  02 00 64 63 65 73 00 00 00 00 00 00 00 00 02 00  ..dces..........
000030  02 00 64 6c 6f 63 00 00 00 00 00 00 00 00 02 00  ..dloc..........
000040  20 00 03 00 63 2a 25 25 00 00 00 00 00 00 00 00  ....c*%.........
000050  03 00 7a d5 [illegible] 0c 0e 0c 0e 05 00 20 00 [illegible]  ..z.>...........
000060  20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00  ................
000070  20 00 20 00 20 00 20 00 04 00 63 2a 25 00 00 00  ..........c*%...
000080  00 00 01 00 00 00 04 00 0d 00 44 04 80 00 00 00  ..........D.....
000090  00 00 00 00 00 00 45 04 40 02 00 00 00 00 00 00  ......E.@.......
```

동작하는 쉘코드(Shellcode)

```
12033b0  0c 0e 0c 0e 0c 0e 0c 0e 0c 0e 0c 0e 0c 0e 0c 0e  ................
12033c0  0c 0e 0c 0e 0c 0e 0c 0e 0c 0e 0c 0e 0c 0e 0c 0e  ................
12033d0  0c 0e 0c 0e 0c 0e 0c 0e 0c 0e 0c 0e 0c 0e 0c 0e  ................
12033e0  0c 0e 0c 0e [illegible] 90 90 90 90 90 57 56 52 53 55  ...........WVRSU
12033f0  51 33 c9 ba 0c 0e 0c 0e 42 8a 02 3c 90 75 f9 8b  Q3Éº....B..<.uù.
1203400  da 83 c2 3f 80 3a 90 74 1c 8a 04 4a 2c 41 c0 e0  Ú.Â?.:.t...J,AÀà
1203410  04 88 04 0a 8a 44 4a 01 2c 4a 00 04 0a [illegible] 81  ....DJ..J...Àf.
1203420  f9 71 03 72 e4 4a 4a 44 4d 4d 53 44 4d 4d 4a 45  ùq.räJJDMMSDMMJE
1203430  4a 46 4d 41 59 4b 4c 46 55 4d 4b 50 53 42 59 50  JFMAYKLFUMKPSBYP
1203440  50 4d 4b 41 4b 41 59 49 4f 44 52 41 4d 41 4a 41  PMKAKAYIODRAMAJA
1203450  4a 46 4f 49 55 4f 56 49 4b 4f 56 41 4a 41 4b 41  JFOIUOVIKOVAJAKA
1203460  4a 41 4a 46 4d 46 50 46 51 49 53 4a 57 47 56 50  JAJFMFPFQISJWGVP
1203470  59 50 59 50 59 4f 55 47 4e 50 56 44 4d 4d 4a 47  YPYPYOUGNPVDMMJG
```

[Figure 6] vulnerability occurs Hangul part

6. Related Files

MD5 and V3 diagnostic information on malicious files identified vulnerability Hangul file and generated by the current is as follows.

```
- 54783422cfd7029a26a3f3f5e9087d8a (V3: HWP / Exploit, 2014.12.10.06)
- b5b6e93ab27cec75f07af2a3a6a40926 (V3: HWP / Exploit, 2014.12.10.02)
- 800866bbab514657969996210bcf727b (V3: HWP / Exploit, 2014.12.10.02)
- ead682b889218979b1f2f1527227af9b (V3: HWP / Exploit, 2014.12. 10.02)
- f09ea2a841114121f32211faac553e1b (V3: HWP / Exploit, 2014.12.09.06)
- 9daf088fe4c9a9580216e98dbb7d1fca (V3: HWP / Exploit, 2014.12.09.06)
- 3ec69ee7135272e5bed3ea5378ade6ee (V3: HWP / Exploit, 2014.12.11.05)
- 33874577bf54d3c209925c9def880eb9 (V3: HWP / Exploit, 2014.12.11.05)
- af792a34548a2038f034ea9a6ff0639a (V3: HWP / Exploit, 2014.12.11.05)
- 3BA8A6815F828DFC518A0BDBD27BBA5B (V3: Trojan / Win32.Destroyer,
2014.12.10.00)
```

7. Countermeasures

In order to prevent a malware infection is necessary to always maintain a Hangul program, and program-to-date antivirus update state. In addition, the vulnerability has been identified as Hangul document files are disseminated in the form of a person to e-mail attachments. For unascertained sender or unresolved attachment, the procedure to ensure that there is no problem in security is required before execution.