<u>Vulnerability, malicious code appeared in the MBR destruction</u> <u>function using Hangul file</u>

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.

<u>1. The files and services that generate</u>

% 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 <u>after December 10, 2014 11:00 a.m.</u> when a, is set to non-zero value is, the MBR is destroyed feature to work .



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.

10086CE4 C745 FC 000000000 NOU DWORD PIR SS:[EBP-4]. 0 10086CE8 C745 F8 330C8D78 NOU DWORD PIR SS:[EBP-4]. 0 10086CF9 B8 M1000000 NOU EAX. 1 10086D606 B04D EB LEA ECX. DWORD PIR SS:[EBP-18] 10086D16 6PF755 EB MOUZX EDX. 0F7240 WOUZX EDX. 0F7240 10086D14 6PF745 EA MOUZX EAX. 2710 ADD 10086D26 0FF74D EE MOUZX ECX. 64 ADD EAX. WORD PIR SS:[EBP-16] 10086D26 0FF745 F0 MOUZX EAX. WORD PIR SS:[EBP-16] ADD EAX 10086D27 0FF745 F0 MOUZX EAX. WORD PIR SS:[EBP-16] EAX 10086D33 8955 E4	10006CE3	53	PUSH	BBX	
100060CEB C245 F4 000000000 NOU DWORD PTR Ss:[EEP-10] 0 10006CF2 C745 F8 330C0D78 NOU DWORD PTR Ss:[EEP-8], 780D0C33 10006CF2 BS C0 SSC0 TEST EAX. EAX. 10006CF2 85C0 TEST EAX. EAX. 10006CF2 85C4 TEST EAX. EAX. 10006D00 SD4D E8 LEA ECX. DWORD PTR SS:[EEP-19] 10006D10 0FB755 E8 NOUZX EDX. WORD PTR SS:[EEP-16] Kernel32.GetLocalTime>] 10006D14 69D255 E8 NOUZX EAX. WORD PTR SS:[EEP-16] Kernel32.GetLocalTime>] 10006D14 69D2765 E8 NOUZX EAX. WORD PTR SS:[EEP-16] Kernel32.GetLocalTime>] 10006D14 69D2765 E8 NOUZX EAX. WORD PTR SS:[EEP-16] MOUZX EAX. 10006D20 03D1 FEX. ECX. NOUD PTR SS:[EEP-16] ADD EAX. MOUZX 10006D20 03D1 ADD EDX. EAX. NOUD PTR SS:[EEP-16] ADD EAX. 10006D20 03D1 ADD EAX. NOUD PTR SS:[EEP-16] EAX.	10006CE4	C745 FC 00000000	MOU	DWORD PIR SS:[EBP-4], 0	
10986CF2 C745 F8 330C6D78 HOU DWORD PTR SS:[EBP-8], 780D0C33 10986CF2 85C6 TEST EAX. EAX 10986D00 08784 10810000 JE West.10005E20 10986D00 08784 10810000 JE West.10005E20 10986D00 08784 10810000 JE West.10005E20 10986D00 951 PUSH ECX. DWORD PTR SS:[CBP-18] 10986D00 9755 E8 GOLL DWORD PTR SS:[CBP-16] Kernel32.GetLocalTime>] 10986D14 6972 48420F00 IMUL EDX. EDX. WORD PTR SS:[CBP-16] Kernel32.GetLocalTime>] 10986D14 6972 48420F00 IMUL EDX. EDX. WORD PTR SS:[CBP-16] Kernel32.GetLocalTime>] 10986D24 63D0 HUL EAX. WORD PTR SS:[CBP-12] ADD 10986D26 6FC9 64 HUL EAX. WORD PTR SS:[CBP-16] ADD 10986D27 6F745 F0 MOUZX EAX. WORD PTR SS:[CBP-16] ADD 10986D33 8955 E4 MOU EAX. WORD PTR SS:[CBP-16] ADD 10986D38 84D F8 CMP CMP ECX. DWORD PTR SS:[CBP-4].1 2014-12-11 AM 11:00 10986D3	10006CEB	C245 F4 00000000	MOU	BUORD PTR SS:[FRP-1C] 0	
10086CP9 88 810000000 NOU ERX 1 10086CPE 85C8 TEST ERX EAX 10086C066 8040 E8 JE MCM = 10000000 10086D06 6F8755 E8 DWORD PTR DS:[(&KERNEL32.GetLocalTime>] 10086D14 6F8755 E8 MOUZX EDX, WORD PTR SS:[EBP-18] 10086D14 6F8755 E8 MOUZX EDX, WORD PTR SS:[EBP-16] 10086D14 6F8755 E8 MOUZX EAX, WORD PTR SS:[EBP-16] 10086D14 6F8745 F0 MOUZX ECX, WORD PTR SS:[EBP-16] 10086D24 6BC9 64 IMUL ECX, ECX, 64 10086D3 03D0 ADD EDX, EAX 10086D3 03D0 ADD EDX, EAX 10086D3 8755 F0 MOU DUVCX ECX, DWORD PTR SS:[EBP-1C] 10086D3 8755 E4 MOU DUVCX ECX, DWORD PTR SS:[EBP-4], 1 10086D36 72 87 610960606 MOU	10006CF2	C745 F8 330C0D78	MOU	DWORD PTR SS:[EBP-8], 780D0C33	
10086CPE 85C8 TEST EAX 10086D060 0F84 1A010000 JE West 10006E20 10086D060 8D4D E8 JE West 10006E20 10086D060 FF15 78208118 JE West 10006E20 10086D06 0F8755 E8 MOUZX EDX, WORD PTR SS:[EBP-18] 10086D14 67B745 EA MOUZX EAX, WORD PTR SS:[EBP-16] 10086D14 67D2 40428F90 IMUL EDX, 0F4240 10086D14 67D2 40428F90 IMUL EDX, WORD PTR SS:[EBP-16] 10086D14 67D2 40428F90 IMUL EDX, 0F4240 10086D14 67D2 40428F90 IMUL EDX, 0F4240 10086D14 67D2 40428F90 IMUL EDX, EAX, 2710 10086D24 63D6 HUL ECX, WORD PTR SS:[EBP-12] ADD 10086D24 68C9 64 IMUL ECX, ECX, 64 ADD 10086D23 63D8 MOUZX EAX, WORD PTR SS:[EBP-1C] EDX 10086D23 63D8 ADD EDX, EAX MOU DWORD PTR SS:[EBP-1C] EDX 10086D33 8955 E4 MOU DWORD PTR SS:[EBP-4],	10006CF9	88 01000000	MOU	EAX, 1	
10086.090 • 0F84 1A010000 JE wes.10005229 10086.080 8040 E8 LEA ECX.DWORD PTR SS:[EBP-18] 10086.080 FF15 78208118 UN PUSH ECX 10086.080 FF15 78208118 CNLL DWORD PTR SS:[EBP-18] kernel32.GetLocalTime>] 10086.010 0FB755 E8 MOUZX EDX.WORD PTR SS:[EBP-16] kernel32.GetLocalTime>] 10086.014 0FB745 EA MOUZX EAX.VORD PTR SS:[EBP-16] kernel32.GetLocalTime>] 10086.024 6308 MOUZX EAX.WORD PTR SS:[EBP-16] ADD 10086.026 0FB74D EE MOUZX ECX.WORD PTR SS:[EBP-12] ADD 10086.026 0FB74D EE MOUZX ECX.WORD PTR SS:[EBP-12] ADD 10086.027 0FB745 F0 MOUZX EAX.WORD PTR SS:[EBP-16] ADD 10086.028 0304 ADD EDX.EAX CHP ECX.DWORD PTR SS:[EBP-16] 10086.028 0304 ADD EDX.EAX WORD PTR SS:[EBP-16] ADD 10086.028 384D F8 CHP ECX.DWORD PTR SS:[EBP-16] 2014-12-11 AH 11:00 10086.038 384D F8 <td>10006CFE</td> <td>85C0</td> <td>TEST</td> <td>EAX EAX</td> <td></td>	10006CFE	85C0	TEST	EAX EAX	
10086006 10086009 10086009 10086009 10086009 10086014 10086014 10086014 10086014 10086014 10086014 10086015 10086015 10086015 10086015 10086015 10086024 10086024 10086026 10086026 10086026 10086027 10086029 10080020 100800000 100800000 10000000000	10006000	• 0F84 1A010000	JE	wss.10006E20	
10006009 51 PUSH ECX 100060040 FF15 78200110 DWORD PTR DS:[(&KERNEL32.GetLocalTine>] 100060014 0FB755 6902 40428F900 IMUL DWORD PTR SS:[EBP-18] 100060014 0FB745 FA MOUZX EAX, WORD PTR SS:[EBP-16] Kernel32.GetLocalTine>] 10006014 0FB745 FA MOUZX EAX, WORD PTR SS:[EBP-16] MOUZX EAX, UPRD PTR SS:[EBP-16] 100060124 0306 HULL ECX, EAX, 2710 ADD EDX, EAX, VORD PTR SS:[EBP-12] ADD 100060220 0301 ADD EDX, EAX, WORD PTR SS:[EBP-12] ADD EDX, EAX 100060220 0304 HULL ECX, ECX, 64 MOUZX EAX, WORD PTR SS:[EBP-16] ADD 10006023 0304 ADD EDX, EAX MOUZX EAX, WORD PTR SS:[EBP-16] ADD 10006023 0304 ADD EDX, EAX MOUZ ADD EDX, EAX 10006033 8955 F4 MOU DWORD PTR SS:[EBP-16] EDX 2014-12-11 AM 11:00 10006034 C745 FC 8100060060 CMP ECX, DWORD	10006D06	8D4D E8	LEA	ECK, DWORD PTR SS:[EBP-18]	
10086009A FF15 78208110 ChLL DWORD PTR DS:[{&KERNEL32.GetLocalTime>] 10086010 0FB755 E8 MOUZX EDX, WORD PTR SS:[EBP-18] kernel32.GetLocalTime>] 10086014 0FB745 EA MOUZX EDX, WORD PTR SS:[EBP-16] kernel32.GetLocalTime>] 10086014 0FB745 EA MOUZX EAX, WORD PTR SS:[EBP-16] kernel32.GetLocalTime>] 10086014 0FB745 EA MOUZX EAX, WORD PTR SS:[EBP-16] AddetSo:[EBP-16] 10086024 0508 ADD EDX, EAX 2710 10086026 0FB74D EE MOUZX ECX, WORD PTR SS:[EBP-12] AddetSo:[EBP-12] 10086027 0511 ADD EDX, EAX WOUZX EAX 10086028 0514 ADD EDX, EAX WOUZX EAX 10086027 0FB745 F0 MOUZX EAX, WORD PTR SS:[EBP-10] AddetSo:[EBP-12] 10086038 8955 E4 MOU EAX, WORD PTR SS:[EBP-16] 2014-12-11 AH 11:00 10086038 384D F8 CHP ECX, DWORD PTR SS:[EBP-4], 1 2014-12-11 AH 11:00 10086047 E3 6484FFFF MOU DWORD PTR SS:[EBP-4], 1 2014-12	10006009	51	PUSH	ECX	
10006010 0FP755 E8 NOU2X EDX, WORD PTR SS: [EBP-18] 10006014 67D2 40420F00 IMUL EDX, WORD PTR SS: [EBP-16] 10006014 0FP745 EA NOU2X EAX, WORD PTR SS: [EBP-16] 10006014 06P745 EA NOU2X EAX, WORD PTR SS: [EBP-16] 10006012 06P740 EE NOU2X ECX, WORD PTR SS: [EBP-16] 10006020 06P740 EE NOU2X ECX, WORD PTR SS: [EBP-16] 10006020 0300 ADD EDX, EAX 10008020 0300 ADD EDX, EAX 10008020 0300 ADD EDX, EAX 10008020 0300 ADD EDX, EAX 10008023 0300 ADD EDX, EAX 10008023 83940 ADD EDX, EAX 10008023 83840 F8 CMP ECX, DWORD PTR SS: [EBP-10] 10008023 3840 F8 CMP ECX, DWORD PTR SS: [EBP-4], 1 10008024 C745 FC 810096000 NOU DWORD PTR SS: [EBP-4], 1 100806047 E8 64B4FFFF OU DWORD PTR SS: [EBP-4], 1 100806047 E8 64B4FFFF CHP	10006D0A	FF15 78200110	CALL	DWORD FIR DS:[<&KERNEL32.GetLocalTime>]	kernel32.GetLocalline
10006014 69D2 40420F00 IHUL EDX, 674240 10006014 6FB745 EA MOUZX EAX, WORD PTR SS:[EBP-16] 10006014 6FB745 EA MOUZX EAX, WORD PTR SS:[EBP-16] 10006014 6700 102700008 IHUL EDX, EAX, 2710 100060126 0FB74D EE MOUZX EAX, WORD PTR SS:[EBP-12] 100060126 0FB74D EE MOUZX ECX, WORD PTR SS:[EBP-12] 100060127 03D1 ADD EDX, EAX, WORD PTR SS:[EBP-16] 100060133 03D4 ADD EDX, EAX 100060133 03D4 ADD EDX, EAX 100060133 03D4 ADD EDX, EAX 100060135 8955 E4 MOU DWORD PTR SS:[EBP-1C], EDX 100060138 884D F4 MOU ECX, DWORD PTR SS:[EBP-8] 2014-12-11 AM 11:00 100060138 384D F8 CMP ECX, DWORD PTR SS:[EBP-4], 1 2014-12-11 AM 11:00 100060140 C745 FC 8100060060 MOU DWORD PTR SS:[EBP-4], 1 2014-12-11 AM 11:00 100080147 E8 6484FFFF CALL West_10008047 100080504 2014-12-11 AM 11:00	10006D10	0FB755 E8	MOUZX	EDX, WORD PTR SS:[EBP-18]	
1000601A 0FB745 EA NOU2X EAX. WORD FTR SS:[EBP-16] 1000601E 69C8 10270008 INUL EAX. WORD FTR SS:[EBP-16] 1000601E 69C8 10270008 INUL EAX. WORD FTR SS:[EBP-12] 100060126 0FB74D EE NOU2X ECX. VORD FTR SS:[EBP-12] 10006020 0301 ADD EDX. EAX 10006027 0FB745 F0 NOU2X ECX. VORD PTR SS:[EBP-10] 10006033 0300 ADD EDX. EAX 10006038 8955 E4 NOU DWORD PTR SS:[EBP-1C] EDX 10006038 8940 F8 CHP ECX. DWORD PTR SS:[EBP-1C] E00400494 10006038 3840 F8 CHP ECX. DWORD PTR SS:[EBP-4] 2014-12-11 AN 11:09 100060404 C745 FC 010000008 NOU DWORD PTR SS:[EBP-4], 1 2014-12-11 AN 11:09 10006047 E8 6484FFFF CALL wss.100021 N9 2014-12-11 AN 11:09 1000804047 E8 6484FFFF CALL wss.100021 N9 2014-12-11 AN 11:09 1000804047 E8 6484FFFF CHP EAX, 100081 Mss.1000500 2014-12-11 AN 11:09	10006D14	69D2 40420F00	IMUL	EDX, EDX, 0F4240	
1008601E 69C8 162780000 IHUL EAX. EAX. 2716 10086024 03D8 ADD EDX. EAX. 10086026 0FE74D FE MOUZX ECX. WORD PTR SS:[EBP-12] 10086020 03D1 ADD EDX. EAX. 10086020 03D1 ADD EDX. ECX. 10086020 03D1 ADD EDX. ECX. 10086020 03D1 ADD EDX. ECX. 10086021 03D1 ADD EDX. ECX. 10086033 03D8 ADD EDX. EAX. 10086033 83D8 ADD EDX. EAX. 10086035 8955 E4 NOU DWORD PTR SS:[EBP-1C] 10086038 3B4D F8 CMP ECX. DWORD PTR SS:[EBP-1C] 10086038 3B4D F8 CMP ECX. DWORD PTR SS:[EBP-4] 10086040 C745 FC 810906000 NOU DWORD PTR SS:[EBP-4] 1 10086047 E8 64B4FFFF OU DWORD PTR SS:[EBP-4] 1 10086047 E8 64B4FFFF CHP EAX. 1000021 DB 10086047 8378 91 CHP FAX. 100005 D60 <	10006D1A	ØFB745 EA	MOUZX	EAX, WORD PTR SS:[EBP-16]	
10986 D24 03 D8 ADD EDX. FAX 10986 D26 0FB74D EE MOUZX ECX. WORD PTR SS:[EBP-12] 10986 D26 6BC9 64 IMUL ECX. ECX. 64 10986 D27 03 D1 ADD EDX. ECX FCX 10986 D27 03 D1 ADD EDX. ECX. 64 10986 D27 03 D1 ADD EDX. ECX FCX 10986 D23 03 D4 ADD EDX. ECX MOUZX ECX. UNCD PTR SS:[EBP-10] 10986 D35 8955 E4 MOU DWORD PTR SS:[EBP-1C] EDX 10986 D38 884D F4 MOU ECX. DWORD PTR SS:[EBP-1C] EDX 10986 D38 384D F8 CMP ECX. DWORD PTR SS:[EBP-1C] EDX 10986 D36 C745 FC 818980698 CMP ECX. DWORD PTR SS:[EBP-4] 2814-12-11 AM 11:08 10986 D47 E8 6484FFFF MOU DWORD PTR SS:[EBP-4] 1 10986 D47 E8 6484FFFF CALL WWEI_18006D47 2814-12-11 AM 11:08 10986 D47 E8 6484FFFF CMP ENX. 1 10986 D50 10986 D47 FC 899 JE SH	10006D1E	69C0 10270000	IMUL	EAX, EAX, 2710	
10006026 0FD74D EE NOUZK ECX. WORD FTR SS:[EBP-12] 10006020 0301 ADD ECX. ECX. 64 10006020 0301 ADD ECX. ECX. 10006027 0FB745 F0 NOUZK EAX. WORD PTR SS:[EBP-10] 10006033 0300 ADD EDX. EAX. 10006038 894D E4 NOU DWORD PTR SS:[EBP-1C]. EDX. 10006038 894D F8 CHP ECX. DWORD PTR SS:[EBP-1C] 2014-12-11 AN 11:00 10006038 384D F8 CHP ECX. DWORD PTR SS:[EBP-4] 2014-12-11 AN 11:00 10006038 384D F8 CHP ECX. DWORD PTR SS:[EBP-4] 2014-12-11 AN 11:00 10006036 C745 FC 010006000 NOU DWORD PTR SS:[EBP-4] 1 10006047 E8 64B4FFFF CALL wcs.100021 N9 2014-12-11 AN 11:00 10006047 B3F8 01 CHP EAX.100021 N9 2 10008047 FC 010006009 CHP EAX.100021 N9 2 10008047 FC 010006009 CHP EAX.100005 D50 2	10006D24	03D0	ADD	EDX. EAX	
10986D2A 6BC9 64 IHUL ECX. ECX. 64 10986D2D 03D1 ADD EDX. ECX. 64 10986D2F 05P745 F0 MOU2X EAX. WORD PTR SS:[EBP-10] 10986D33 03D8 ADD EDX. EAX. 10986D35 8955 E4 MOU DWORD PTR SS:[EBP-1C]. EDX. 10986D38 894D E4 MOU ECX. DWORD PTR SS:[EBP-1C] EDX. 10986D38 384D F8 CMP ECX. DWORD PTR SS:[EBP-1C] E044-12-11 AN 11:09 10986D36 C745 FC 810060000 NOU DWORD PTR SS:[EBP-4]. 2014-12-11 AN 11:09 10986D47 E8 64B4FFFF CML wss.18006D47 100980147 10986D47 E8 64B4FFFF CMP ECN. 109961900 10986D47 E8 64B4FFFF CML wss.18006D47 10996190 10986D47 E8 64B4FFFF CMP ECN. 10996190 10996190	10006D26	ØFB74D EE	MOUZX	ECK, WORD PTR SS:[EBP-12]	
1000602D 03D1 ADD EDX, ECX 1000602F 0FB745 F0 MOUZX EAX, WORD PTR \$\$:[EBP-10] 10006033 03D0 ADD EDX, EAX 10006035 8955 E4 MOU DWORD PTR \$\$:[EBP-1C], EDX 10006038 884D E4 MOU ECX, DWORD PTR \$\$:[EBP-1C] 10006038 3B4D F8 CMP ECX, DWORD PTR \$\$:[EBP-1C] 10006038 3B4D F8 CMP ECX, DWORD PTR \$\$:[EBP-1C] 10006038 3B4D F8 CMP ECX, DWORD PTR \$\$:[EBP-4] 10006036 C745 FC 81000000 MOU DWORD PTR \$\$:[EBP-4], 1 10006047 E8 64B4FFFF CALL wss.18006192 10006047 E8 64B4FFFF CALL wss.18006050 10006047 E8 64B4FFFF CALL wss.18006050 10008046 C745 FC 81000000 CMP FR \$\$:[EBP-4], 1 10008046 C745 FC 81000000 MOU DWORD PTR \$\$:[EBP-4], 1 10008047 E8 64B4FFFF CALL wss.180061000 10008046 C745 FC 81000000 CMP FR \$\$:[EBP-4], 1	10006D2A	6BC9 64	IMUL	ECX. ECX. 64	
1000602F 0FP745 F0 NOU2X EAX. WORD FTR SS:[EBP-10] 10006033 03D0 ADD EDX. EAX. 10006038 8955 E4 NOU DWORD FTR SS:[EBP-1C]. EDX. 10006038 884D E4 NOU ECX. DWORD PTR SS:[EBP-1C] 10006038 384D F8 CHF ECX. DWORD PTR SS:[EBP-8] 10006036 72.07 JB SHORT wer.10006047 10006047 E8 64B4FFFF CALL wer.100021 M9 10006047 E8 64B4FFFF CALL wer.100021 M9 10006047 F8 641 CHF EAX. 1 10006047 F8 64B4FFFF CALL wer.100021 M9 10006047 F8 64B4FFFF CAL wer.100021 M9 10006047 F8 64B4FFFF CALL wer.100021 M9 10006047 F8 64B4FFFF CAL wer.100021 M9 10006047 F8 64B4 CHF EAX. 1	10006D2D	03D1	ADD	EDX, ECX	
10006033 0300 ADD EDX EAX 10006033 8955 E4 MOU DWORD PTR SS:[EBP-1C] EDX 10006038 8940 E4 MOU ECX DWORD PTR SS:[EBP-1C] 10006038 3840 F8 CHP ECX DWORD PTR SS:[EBP-8] 10006038 3840 F8 CHP ECX DWORD PTR SS:[EBP-8] 10006047 C745 FC 010000000 MOU DWORD PTR SS:[EBP-4], 1 10006047 E8 6484FFFF C1L wss.10006047 10006047 E8 6484FFFF C1L wss.10006047 10006047 E8 6484FFFF C1L wss.10005109 10006047 E8 6484FFFF C1L wss.10005109 10006047 E8 6484FFFF C1L wss.10005109	10006D2F	0FB745 F0	MOUZX	EAX, WORD PTR SS:[EBP-10]	
10006D35 8955 E4 NOU DWORD PTR SS:[EBP-1C], EDX 10006D38 8B4D E4 MOU ECX, DWORD PTR SS:[EBP-1C] 10006D38 3B4D F8 CMP ECX, DWORD PTR SS:[EBP-1C] 10006D3E -72 07 JB SHORI wss.18006D47 10006D40 C745 FC 010000000 MOU DWORD PTR SS:[EBP-4], 1 10006D47 E8 64B4FFFF CRLL wss.1800021B0 10006D47 83F8 01 CMP EAX, 1 10006D47 _2 84 9 JE SHORI wss.19006D50	10006D33	03D0	ADD	EDX, EAX	
10006038 8B4D E4 NOU ECX. DWORD PTR SS:[EBP-1C] 2014-12-11 AM 11:00 10006038 3B4D F8 CMP ECX. DWORD PTR SS:[EBP-4] 2014-12-11 AM 11:00 10006038 -72 87 JB SNORT were.10006042 2014-12-11 AM 11:00 10006040 C745 FC 010000000 HOU DWORD PTR SS:[EBP-4].1 2014-12-11 AM 11:00 10006047 E8 64B4FFFF CALL were.100021 M0 2014-12-11 AM 11:00 10006047 E8 64B4FFFF CALL were.100021 M0 2014-12-11 AM 11:00 10006047 E8 64B4FFFF CALL were.100021 M0 2014-12-11 AM 11:00 10006047 E8 64B4FFFF CALL were.100021 M0 2014-12-11 AM 11:00	10006D35	8955 E4	MOU	DWORD PIR SS:[EBP-1C], EDX	
10006038 384D F8 CHP ECX. DWORD PTR SS:[EBP-8] 2014-12-11 AN 11:00 10006038 28 72 07 JB SHORT wcs.1000604? 1000604? 1000604? 1000604? NOU DWORD PTR SS:[EBP-4], 1 1000604? 10000604? <td>10006D38</td> <td>8B4D E4</td> <td>MOU</td> <td>ECX, DWORD PTR SS:[EBP-1C]</td> <td></td>	10006D38	8B4D E4	MOU	ECX, DWORD PTR SS:[EBP-1C]	
10006D3E 72 87 JB SHORT wss.10006D47 10006D40 C745 FC 010060000 NOU DWORD PTR SS:[EBP-4], 1 10006D47 E8 6484FFFF CALL wss.100021B0 10006D4C 83F8 01 CHP EAX, 1 10006D4F 24 09 JE SHORT wss.10006D50	10006D3B	3B4D_F8	CHP	ECX, DWORD PTR SS:[EBP-8]	2014-12-11 AM 11:00
10986040 C745 FC 81008090 NOU DWORD PTR SS:[EBP-4], 1 10986047 E8 6484FFFF CALL wss.10092106 10986047 83F8 01 CMP EAX, 1 10986047 B3F8 01 CMP EAX, 1 10986047 B3F8 01 CMP EAX, 1	10006D3E	~ 72 07	JB	SHORT wss.10006D47	
10906047 E8 64B4FFFF CHL west 10002100 1090604C 83F8 91 CHP EAX, 1 1090604F 24 69 JE SHORT west 10006050	10006D40	C745 FC_01000000	MOU	DWORD PIR SS:[EBP-4], 1	
10996D4C 83F8 01 CHP EAX, 1 10996D4F 24 89 JE SHORT was 10996D50	10006D47	E8 64B4FFFF	CALL	wss.100021B0	
10006D4F July 74 69 JE SHORT was 10006D5A	10006D4C	83F8 01	CHP	EAX, 1	
	10006D4F	~ 74 09	JE	SHORT was.10006D5A	

Figure -2] MBR destruction timecode to compare

<u>3. MBR destruction techniques</u>

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

000000 000010 000030 000040 000050 000060 000070 000080 000090 000080 000000 000000 000000 000000 000000	b8 3f 00	12 ba 20 00 00 00 00 00 00 00 00 00 00 00 00	00 1d 20 00 00 00 00 00 00 00 00 00 00 00 00	cd 0e 20 00 00 00 00 00 00 00 00 00 00 00 00	10 cd 20 00 00 00 00 00 00 00 00 00 00 00 00	bd 10 20 00 00 00 00 00 00 00 00 00 00 00 00	$\begin{array}{c} 18\\ e2\\ 20\\ 00\\ 00\\ 00\\ 00\\ 00\\ 00\\ 00\\ 00\\ 0$	7c fe 20 00 00 00 00 00 00 00 00 00 00 00 00	b9 57 20 00	18 68 20 00 00 00 00 00 00 00 00 00	00 6f 20 00 00 00 00 00 00 00 00 00 00 00 00	b8 20 00	01 41 20 00	13 6d 20 00 00 00 00 00 00 00 00 00 00 00 00	bb 20 20 00 00 00 00 00 00 00 00 00 00 00	0c 49 20 00 00 00 00 00 00 00 00 00 00 00 00	
000100	00	ŌŌ	ŌŌ	ŌŌ	00	ŌŌ	ŌŌ	ŌŌ	00	ŌŌ	ŌŌ	ŌŌ	00	ŌŌ	ŌŌ	ŌŌ	
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	
000150	ŌŌ	ÕÕ	ÕÕ	ÕÕ	ÕÕ	ÕÕ	ÕÕ	ÕÕ	ÕÕ	ÕÕ	ÕÕ	ÕÕ	ÕÕ	ÕÕ	ÕÕ	ÕÕ	
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	
000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0001a0	ŌŌ	ÕÕ	ŌŌ	ÕÕ	ŌŌ	ÕÕ	ÕÕ	ÕÕ	ŌŌ	ÕÕ	ŌŌ	ÕÕ	ŌŌ	ŌŌ	ŌŌ	ÕÕ	
0001b0	00	00	00	00	00	00	00	00	91	cd	dd	3c	00	00	00	00	ÍÝ<
000100		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 000200	00	ŌŌ	ŌŌ	ŌŌ	ŌŌ	ŌŌ	ŌŌ	ŌŌ	ŌŌ	ŌŌ	ŌŌ	ŌŌ	ŌŌ	ŌŌ	55	aa	

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?".

268000:100	u ; sequent type:	Lale code		
seg888:7C8	8 seg888	segment by	te public 'COD	DE' use16
seg000:7C0	0	assume cs:	seg000	
seg888:7C8	0	;org 7000h		
seg888:7C8	8	assume es:	nothing, ss:no	othing, ds:nothing, fs:nothing, gs:nothing
seg000:7C0	0	nov ax	, 12h	
seg888:7C8	3	int 18	h	: - VIDEO - SET VIDEO HODE
seq000:7C0	3			; AL - node
seg888:7C8	5	nov bp	7C18h	
seq000:700	8	nov cx	, 18h	
seq000:7C0	B	nov ax	, 1301h	
seg888:7C8	E	nov bx	, OCh	
seq888:7C1	1	nov dx	. ØE1Dh	
seg000:7C1	4	int 10	h	; - UIDEO - WRITE STRING (AT, XT286, PS, EGA, UGA)
seq888:701	4			; AL = mode, BL = attribute if AL bit 1 clear, BH = display page number
seq888:7C1	4			; DH,DL - row,column of starting cursor position, CX - length of string
seq000:7C1	4			; ES:BP -> start of string
seg000:7C1 seg000:7C1	6			; ES:BP -> start of string
seg000:7C1 seg000:7C1 seg000:7C1	6 6 Loc 7016:			; ES:BP -> start of string ; CODE XREF: seq000:loc 7C161j
seg000:701 seg000:701 seg000:701 seg000:701	4 6 6 µoc_7016: 6	100p 10	c 7C16	; ES:BP -> start of string ; CODE XREF: seg000:loc_7C16ij
seg000:701 seg000:701 seg000:701 seg000:701	4 6 6 µoc_7016: 6	loop lo	c_7C16	; ES:BP -> start of string ; CODE XREF: seg000:loc_7C16ij
seg000:7C1 seg000:7C1 seg000:7C1 seg000:7C1	6 6 μος_7016: 6	100p 10	c_7C16	; ES:BP -> start of string ; CODE XREF: seg000:loc_7C16ij
seg000:701 seg000:701 seg000:701 seg000:701	δ 6 μος_7016: 57 68 6F 2	100p 10	c_7016 ე 20 ს0	; ES:8P -> start of string ; CODE XREF: seg000:loc_7C16jj 2E 28 28 28 28 28 28 28 28 Ubo 0m 12
seg000:701 seg000:701 seg000:701 seg000:701 seg000:701	6 poc_7016: 57 68 6F 2	100p 10	c_7616 D 20 49	; ES:BP -> start of string ; CODE XREF: seg000:loc_7C16ij 3F 20 20 20 20 20 20 20 20 Who Am I?
seg000:701 seg000:701 seg000:701 seg000:701 7018 7018 7028	57 68 6F 2	100p 10 10 41 6 10 20 2	c_7616 D 20 49 0 20 20	; ES:BP -> start of string ; CODE XREF: seg000:loc_7C16ij 3F 20 20 20 20 20 20 20 20 Who Am I? 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.



[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

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

Locate the files with the extension of the above 'A' \sim '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 빌	발생원	길인	_														
000000 000010 000020 000030 000040 000050 000050 000060 000070 000080 000090	42 01 02 20 03 20 20 00 00 00	00 00 00 00 00 00 00 00 00 00	80 00 64 03 7a 20 20 01 00	01 00 63 60 d5 00 00 00 00	35 01 65 61 63 20 20 00 00	00 00 73 63 8a 80 00 00 00	00 00 00 25 00 20 20 04 45	80 00 00 25 0e 00 00 00 00	1c 00 00 00 00 20 04 0d 40	00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 05 20 63 44 00	00 00 00 00 00 00 2a 04 00	03 43 00 00 20 20 25 80 00	00 04 00 00 00 00 00 00 00	00 a.0 02 02 10 00 00 00 00	03 06 00 00 00 00 00 00 00 00	B. 5.
동작하는	쉘크	크드(Shel	llcod	le)]											
12033b0 12033c0 12033d0 12033f0 1203400 1203410 1203420 1203420 1203420 1203450 1203450 1203460 1203470	0c 0c 0c 51 da 04 f9 4a 50 4a 50 59	0e 0e 33 88 71 46 44 46 41 50	0c 0c 0c c9 c2 04 03 4d 4b 4f 4a 59	0e 0e 0e 3f 0a 72 41 41 49 46 50	0c 0c 80 80 80 80 80 80 80 80 80 80 80 80 80	0e 0e 3a 44 4b 41 41 4f 4f 4f	0c 0c 90 90 4a 4c 59 55 55	0e 0e 90 0e 74 01 44 46 49 49 46 47	0c 0c 90 42 1c 2c 4d 55 4f 4b 51 4e	0e 0e 90 8a 4a 4d 4d 4d 4f 49 50	0c 0c 90 02 04 00 53 4b 52 56 53 56	0e 0e 57 3c 4a 04 44 50 41 41 41 4a 44	0c 0c 56 90 2c 0a 4d 53 4d 53 4d 57 4d	0e 0e 52 75 41 42 41 41 41 47 4d	0c 0c 53 f9 c0 4a 59 4a 4b 56 4a	0e 0e 55 8b e0 91 50 41 41 50 47	O3É ² B. <.uù. Ŭ.Å?.:t.J.ÅÅà II JÅf. Ng JII (MSDMMJE JFMATKL-UMKPSBYP PMKAKAYIODRAMAJA JFOIUOVIKOVAJAKA JAJFMFPFQISJWGVP 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.