www.alyac.co.kr

피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차

Part I 11월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

[2011년 11월 1일 ~ 2011년 11월 30일]

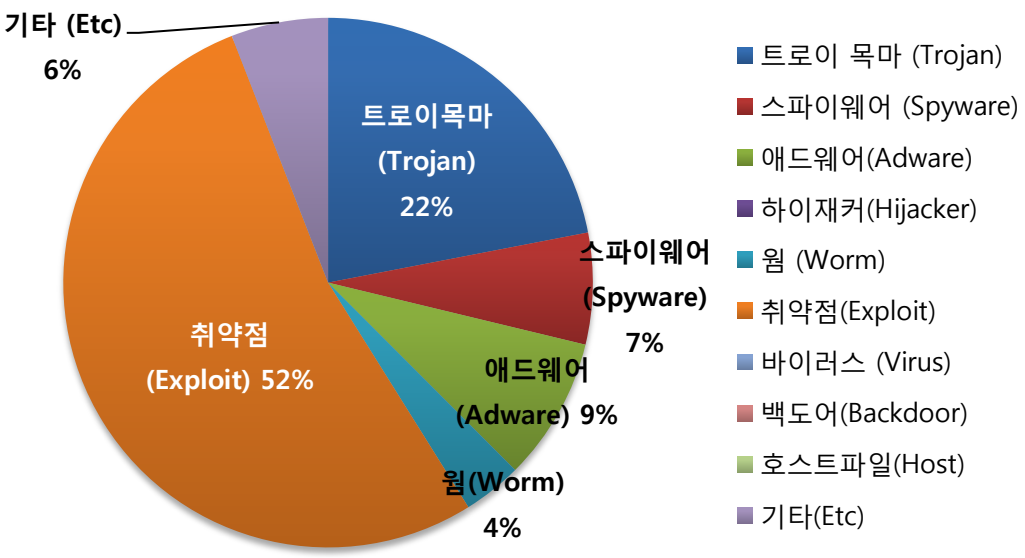
순위		악성코드 진단명	카테고리	합계 (감염자수)
1	New	Script.SWF.C22	Exploit	35,440
2	↓1	K.EXP.SWF.ShellCode.Gen	Exploit	16,933
3	New	Adware.Kraddare.V	Adware	8,644
4	New	Trojan.JS.QGG	Trojan	6,117
5	New	S.SPY.OnlineGames.wsxp	Spyware	4,531
6	↑6	Trojan.Generic.6742288	Trojan	4,184
7	↑4	S.SPY.Lineag-GLG	Spyware	3,724
8	-	V.WOM.Conficker	Worm	3,561
9	New	Variant.Graftor.2730	Etc	3,066
10	↓7	S.SPY.OnlineGames.nsys	Spyware	3,002
11	↓5	V.DWN.Agent.499712	Trojan	2,997
12	New	Trojan.Generic.KDV.404375	Trojan	2,942
13	↓8	V.DWN.Agent.Pinsearch	Etc	2,792
14	↓7	V.DWN.86016	Trojan	2,775
15	New	V.TRJ.Adload.v3	Trojan	2,706

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계입니다.
11월의 감염 악성코드 TOP 15는 Script.SWF.C22이 35,440건으로 TOP 15 중 1위를 차지했으며, K.EXP.SWF.ShellCode.Gen가 16,933건으로 2위, Adware.Kraddare.V가 8,644건으로 3위를 차지했습니다. 이 외에도 11월에 새로 Top 15에 진입한 악성코드는 총 7종입니다.

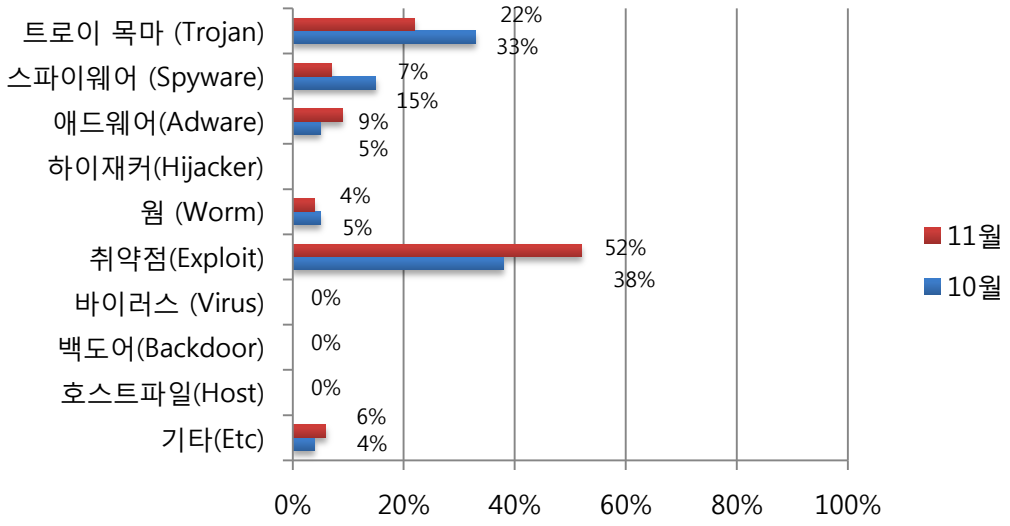
11월에도 주말(대부분 금요일~월요일 사이)을 이용한 온라인 게임 계정 유출 악성코드가 가장 많이 탐지되었습니다. PC의 취약점을 통해 설치된 S.SPY.OnlineGames.nsys의 비율이 감소하였고, 새롭게 S.SPY.OnlineGames.wsxp, S.SPY.Lineag-GLG 관련 비율이 증가하였습니다.
주말 기간 동안 유포되는 악성코드들의 형식이 계속적으로 변화하고 있음을 알 수 있습니다.

(2) 카테고리별 악성코드 유형



악성코드 유형별 비율에서 취약점(Exploit)은 52%로 가장 많은 부분을 차지하였고, 트로이목마(Trojan)가 22%, 스파이웨어(Spyware) 7%, 웜(Worm) 4%와 애드웨어(Adware)가 9%, 기타(Etc) 6%의 비율로 나타났습니다. 가장 높은 비율로 나타난 취약점(Exploit)은 주말에 유포되는 온라인게임 계정 유출 악성코드를 설치하며, 주로 Adobe Flash Player와 MS Internet Explorer 취약점을 이용해 설치됩니다.

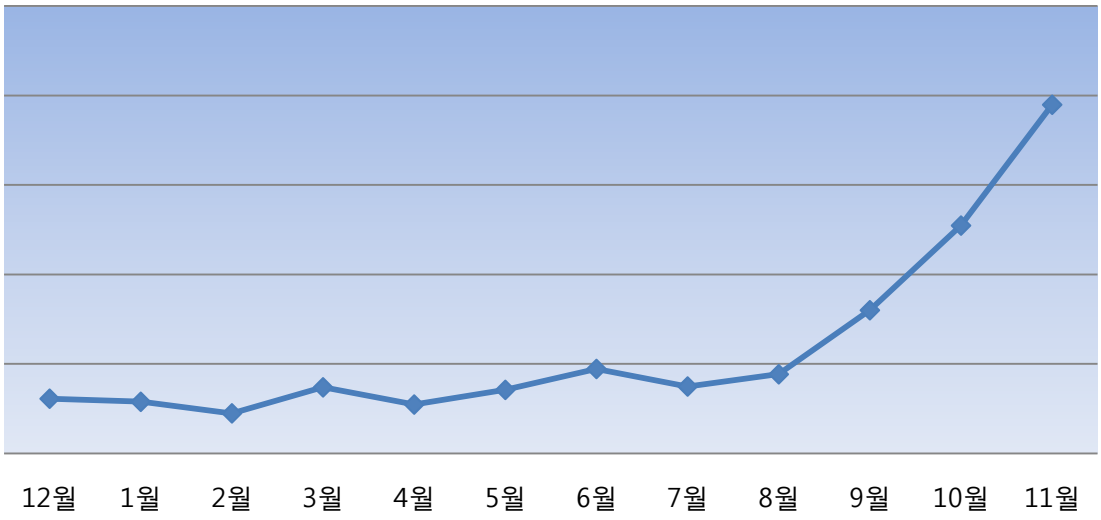
(3) 카테고리별 악성코드 비율 전월 비교



11월의 특이사항으로, 취약점(Exploit)의 비율이 더욱 높아졌습니다. 이는 많은 악성코드의 감염원인이 취약점 또는 보안 패치를 하지 않는 것과 관계가 있음을 나타내고 있습니다.

(4) 월별 피해 신고 추이

[2010년 12월 ~ 2011년 11월]

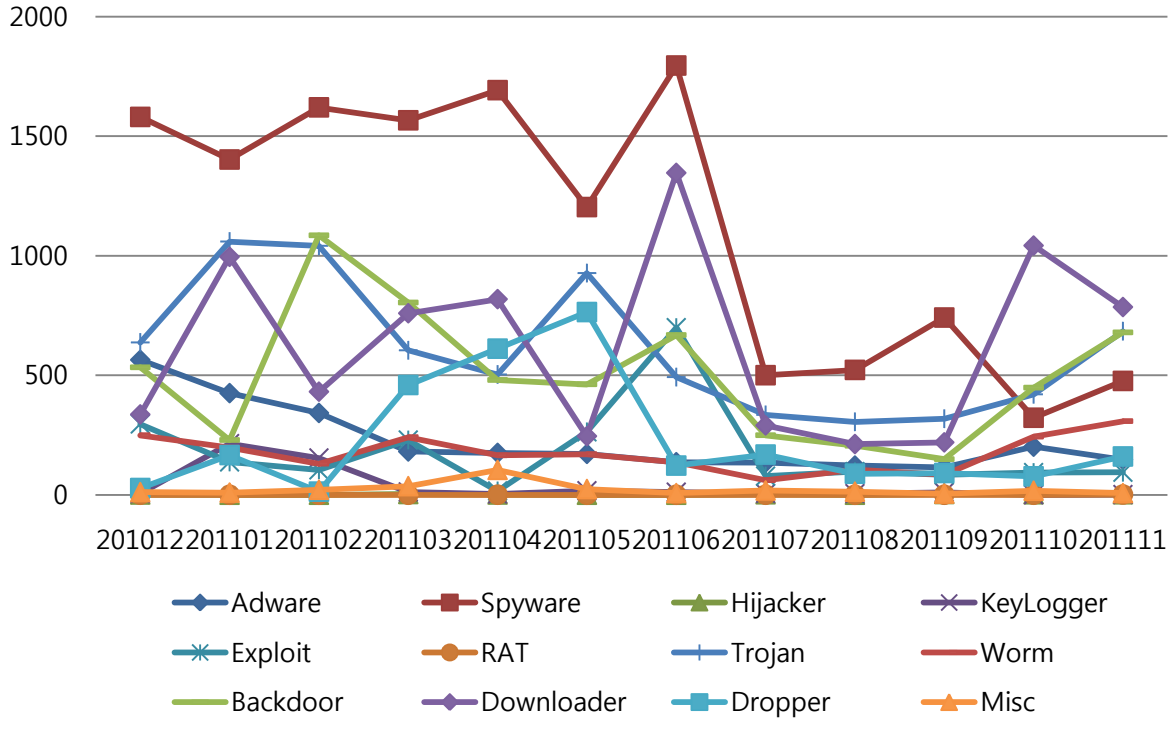


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프입니다. 알약 2.1의 신고가 추가된 8월 이후 신고 건수가 가파르게 증가하고 있습니다. 신고 내용으로는 주말 기간을 통한 온라인 게임 계정 탈취 악성코드 피해가 가장 많았습니다.

(5) 월별 악성코드 DB 등록 추이

[2010년 12월 ~ 2011년 11월]



Part Ⅰ 11 월의 악성코드 통계

2. 악성코드 이슈 분석 – "Trojan.Dropper.OnlineGames.wime"

(1) 개요

Trojan.Dropper.OnlineGames.wime 악성코드는 DLL 파일을 Drop하고 PC에 설치된 백신을 삭제하는 기능을 가지고 있습니다.

또한 Windows 폴더에 spool1sv.exe로 복사한 후 프로세스로 상주하며 스스로 삭제 및 종료되지 않습니다. 만약 ws2help.dll이 삭제되었을 경우 다시 생성하기도 합니다.

악성으로 변조된 ws2help.dll의 경우 원본 윈도우 ws2help 파일의 함수를 실행시켜주기 위해 Export 함수 문자열을 백업한 wimedump.dll로 간단히 링크합니다.

(2) 악성코드 분석

2-1) u.exe or spool1sv.exe

최초 Windows 폴더에서 실행되었는지를 체크하여 다른 폴더에서 실행된 경우 처음으로 동작하는 것으로 판단하여 이후 버전 파일을 확인합니다.

```
push    offset Buffer                   ; Source
push    eax                             ; Dest
call    strcpy
lea     eax, [ebp+FileName]
push    offset aWinurl_dat              ; "₩₩winurl.dat"
push    eax                             ; Dest
call    strcat
add     esp, 10h
lea     eax, [ebp+FileName]
push    eax                             ; lpFileName
push    [ebp+lpString]                  ; lpString
push    offset KeyName                  ; "status"
push    offset AppName                  ; "data"
call    WritePrivateProfileStringA
```

이후 "C:₩₩WINDOWS₩₩tasks₩₩SA01.dat" 파일을 생성하고 파일 시그니쳐를 3030으로 수정합니다. SA01.dat의 경우 파일 내부에 리소스 형태로 되어있고 악성 DLL 파일로 나중에 파일이 삭제되었을 경우 복구용으로 사용됩니다.

```
strcat(&v3, "₩₩tasks₩₩SA01.dat");
strcpy((char *)&NumberOfBytesWritten, Buffer);
strcat((char *)&NumberOfBytesWritten, "₩₩tasks₩₩SA02.dat");
strcpy(&v5, Buffer);
strcat(&v5, "₩₩");
strcat(&v5, "spoo1sv.exe");
GetSystemDirectoryA(&MultiByteStr, 0xFFu);
strcat(&MultiByteStr, "₩₩dllcache₩₩");
strcat(&MultiByteStr, "ws2help.dll");
create_Malware_DLL_and_change_signature_to_3030(&v3, (HRSRC)0x82, "00");
```

OFFSET	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	30	30	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	D8	00	00	00
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00
00000080	53	41	DE	DA	17	20	B0	89	17	20	B0	89	17	20	B0	89
00000090	94	3C	BE	89	14	20	B0	89	17	20	B1	89	16	20	B0	89

ASCII
00▌.....ÿÿ..
¸.....@.....
.....
.....Ø...
..º..´.Í!¸.LÍ!Th
is program canno
t be run in DOS
mode....$.....
SAÞÚ. °▌. °▌. °▌
▌<¾▌. °▌. ±▌. °▌

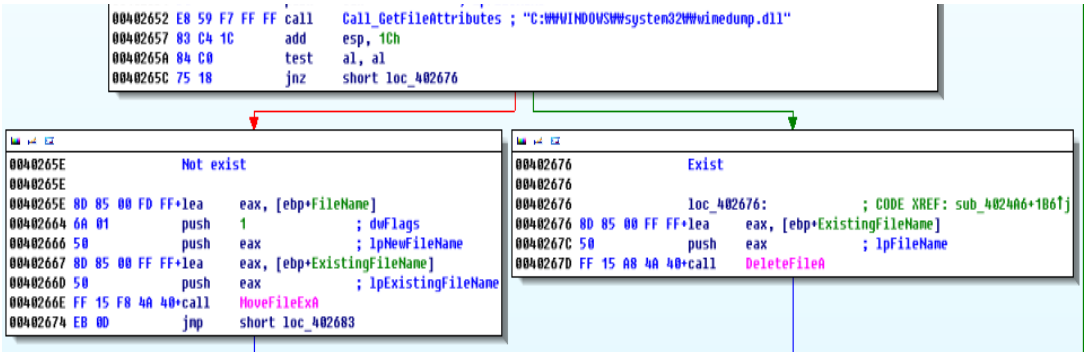
복구용 악성 DLL 파일의 시그니쳐

또한 자신을 SA02.dat와 spoo1sv.exe로 복사하고 SA02.dat의 경우 0000으로 시그니쳐를 수정합니다.

```
push    1               ; bFailIfExists
mov     esi, offset Filename
push    eax             ; lpNewFileName
push    esi             ; lpExistingFileName
call    CopyFileA       ; "C:₩₩WINDOWS₩₩tasks₩₩SA02.dat"
lea     eax, [ebp+var_400]
push    1               ; bFailIfExists
push    eax             ; lpNewFileName
push    esi             ; lpExistingFileName
call    CopyFileA       ; "C:₩₩WINDOWS₩₩spoo1sv.exe"
lea     eax, [ebp+NumberOfBytesWritten]
push    edi             ; lpBuffer
push    eax             ; NumberOfBytesWritten
call    change_signature_of_SA02_to_00
```

작업이 완료되면 다음과 같이 system32 폴더 및 cache 폴더 각각의 ws2help.dll 파일의 WFP(Windows File Protection)을 해제하고, "%system32%₩wimedump.dll"이 있는지 확인한 뒤 없으면 ws2help.dll 파일을wimedump.dll로 이름을 변경합니다.
원본 DLL 파일에 대한 백업 파일을 생성하는 것 과정입니다.

```
sfc_os_load_and_WFP_clear(v1);                  // ws2help.dll
sfc_os_load_and_WFP_clear(v2);                  // cache 폴더의 ws2help.dll
if ( (unsigned __int8)Call_GetFileAttributes(&FileName) )
  DeleteFileA(&ExistingFileName);
else
  MoveFileExA(&ExistingFileName, &FileName, 1u);
```



WFP 해제 뒤 안전(?)하게 ws2help.dll을 제거 하고, 다시 내부 리소스를 확인하여 악성 DLL인 ws2help.dll을 시스템에 생성합니다.

```
v3 = GetModuleHandleA(0);
if ( hResInfo == 130 )
  hResInfo = FindResourceA(v3, 0x82, "MYDLL");
nNumberOfBytesToWrite = SizeofResource(v3, hResInfo);
v5 = LoadResource(v3, hResInfo);
v4 = LockResource(v5);
if ( v4
  && (v6 = CreateFileA(lpFileName, 0xC0000000u, 3u, 0, 2u, 0x80u, 0),
      v6 != -1HINSTANCE_ERROR|HANDLE_FLAG_PROTECT_FROM_CLOSE|HANDLE_FLAG_INHERIT) )
{
  WriteFile(v6, v4, nNumberOfBytesToWrite, &NumberOfBytesWritten, 0);
  CloseHandle(v6);
  if ( sub_402AD0(lpBuffer) )
    change_signature_of_SA02_to_00(lpFileName, lpBuffer);
  result = 1;
}
```

마지막으로 "C:₩₩WINDOWS₩₩system32₩₩ws2help.dll"을
"C:₩₩WINDOWS₩₩system32₩₩dllcache₩₩ws2help.dll"로 복사합니다.
이렇게 모든 작업이 완료되면 자신의 상태를 나타내는 일종의 플래그 파일인 "winurl.dat", "version.dat"을 windows 폴더에 생성하고 자신을 삭제합니다.

악성 DLL의 경우 spoo1sv.exe을 실행시켜주며 각종 온라인 게임에 대한 계정을 해킹하는 역할을 합니다. 또한 원본 DLL의 역할을 위해 export table을 다음과 같이 수정합니다.

WahCloseApcHelper	100187E7	1
WahCloseHandleHelper	10018802	2
WahCloseNotificationHandleHelper	10018820	3
WahCloseSocketHandle	1001884A	4
WahCloseThread	10018868	5
WahCompleteRequest	10018880	6
WahCreateHandleContextTable	1001889C	7
WahCreateNotificationHandle	100188C1	8
WahCreateSocketHandle	100188E6	9
WahDestroyHandleContextTable	10018905	10
WahDisableNonIFSHandleSupport	1001892B	11
WahEnableNonIFSHandleSupport	10018952	12
WahEnumerateHandleContexts	10018978	13
WahInsertHandleContext	1001899C	14
WahNotifyAllProcesses	100189BC	15
WahOpenApcHelper	100189DB	16

```
000187E0  63 61 74 69 6F 6E 00 77  69 6D 65 64 75 6D 70 2E  cation.wimedump.
000187F0  57 61 68 43 6C 6F 73 65  41 70 63 48 65 6C 70 65  WahCloseApcHelpe
00018800  72 00 77 69 6D 65 64 75  6D 70 2E 57 61 68 43 6C  r.wimedump.WahCl
00018810  6F 73 65 48 61 6E 64 6C  65 48 65 6C 70 65 72 00  oseHandleHelper.
00018820  77 69 6D 65 64 75 6D 70  2E 57 61 68 43 6C 6F 73  wimedump.WahClos
00018830  65 4E 6F 74 69 66 69 63  61 74 69 6F 6E 48 61 6E  eNotificationHan
00018840  64 6C 65 48 65 6C 70 65  72 00 77 69 6D 65 64 75  dleHelper.wimedu
00018850  6D 70 2E 57 61 68 43 6C  6F 73 65 53 6F 63 6B 65  mp.WahCloseSocke
00018860  74 48 61 6E 64 6C 65 00  77 69 6D 65 64 75 6D 70  tHandle.wimedump
00018870  2E 57 61 68 43 6C 6F 73  65 54 68 72 65 61 64 00  .WahCloseThread.
00018880  77 69 6D 65 64 75 6D 70  2E 57 61 68 43 6F 6D 70  wimedump.WahComp
00018890  6C 65 74 65 52 65 71 75  65 73 74 00 77 69 6D 65  leteRequest.wime
000188A0  64 75 6D 70 2E 57 61 68  43 72 65 61 74 65 48 61  dump.WahCreateHa
000188B0  6E 64 6C 65 43 6F 6E 74  65 78 74 54 61 62 6C 65  ndleContextTable
```

export table문자열에 wimedump를 삽입

wimedump.dll은 자신이 원본을 백업한 파일이기 때문에 간단하게 export함수를 원본 파일로 링크를 걸고 다시 Dropper로 돌아가 spoo1sv.exe로 실행이 된 드럽퍼는 일정시간 주기로 국내 백신 프로그램을 방해하고 최초 루틴을 반복적으로 실행합니다.

```
00402A57
00402A57
00402A57                ; Attributes: noreturn
00402A57
00402A57                sub_402A57 proc near    ; CODE XREF: sub_402A57+24↓j
00402A57                                        ; start-B0AB↓p
00402A57 E8 DE F4 FF FF call    Anti_V3Lite
00402A5C E8 E6 F5 FF FF call    Anti_V3365
00402A61 E8 03 F8 FF FF call    Anti_NaverAV
00402A66 E8 E9 F6 FF FF call    Anti_Alyac
00402A6B E8 53 FC FF FF call    initial_routine
00402A70 68 20 4E 00 00 push    4E20h           ; dwMilliseconds
00402A75 FF 15 9C 4A 40+call    Sleep
00402A7B EB DA          jmp     short sub_402A57
00402A7B                sub_402A57 endp
00402A7B
```

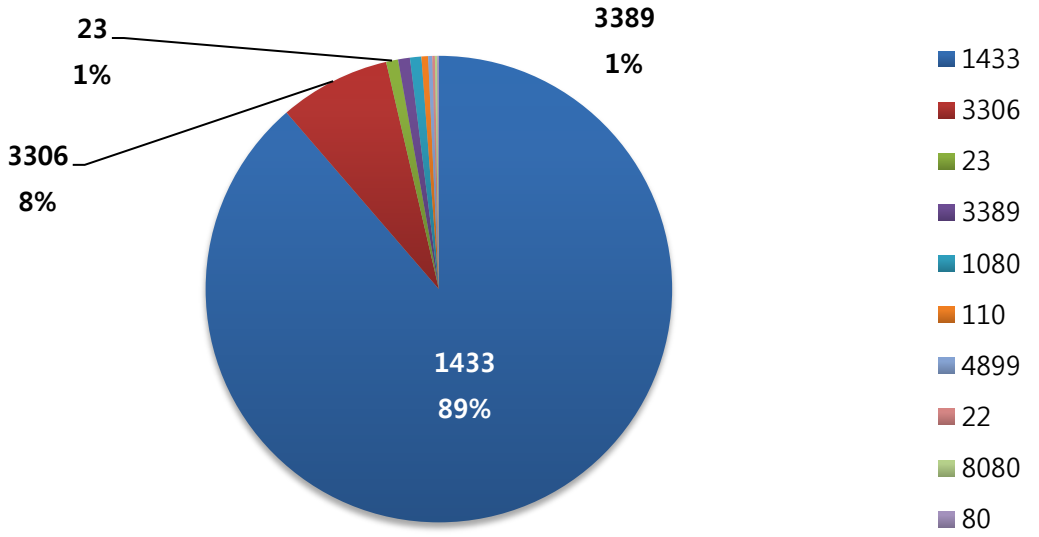
(3) 결론

이번 악성코드의 특이 점은 백신을 먼저 삭제하지 않고 악성 파일을 먼저 Drop 했다는 점입니다. 그 만큼 악성코드 제작자들도 사전에 준비를 많이 하는 것으로 보여집니다. 앞으로도 이런 과감한 형태의 악성코드 유포에 대해서 주의를 기울어야 할 것 입니다.

Part I 11월의 악성코드 통계

4. 허니팟/트래픽 분석

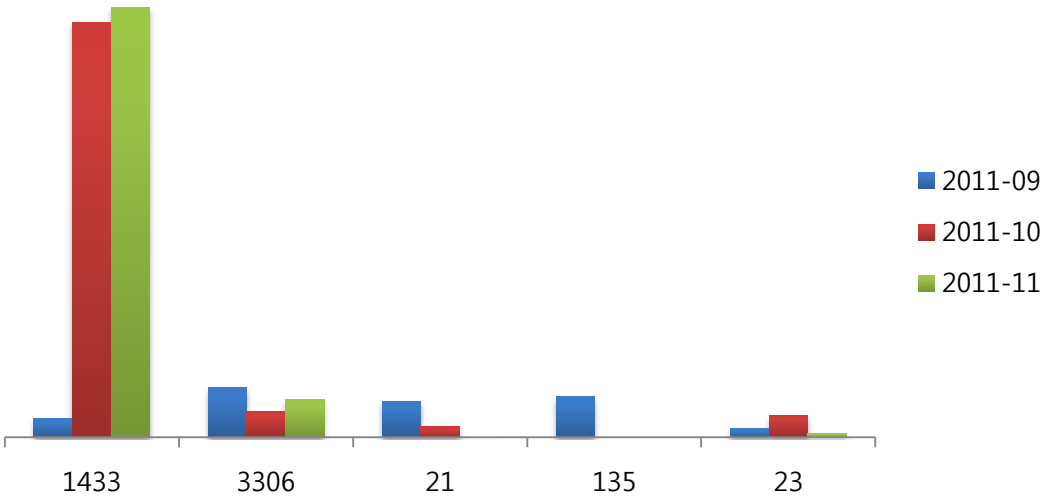
(1) 상위 Top 10 포트



11월에는 Microsoft SQL Server에서 사용하는 1433 포트에 대한 트래픽 유입이 가장 많았습니다. 특히 MSSQL Server의 관리자 계정인 "sa"에 대한 패스워드 대입 시도(Brute force)가 많았습니다. 데이터베이스 서버를 운영 중인 IT 관리자는 "sa" 계정의 패스워드를 단순하게 사용하고 있지 않는지 반드시 점검해야 하고, 패스워드가 없거나 단순한 (예: 1234, abc123 등) 하다면 반드시 강력한 패스워드로 변경해야 합니다.

(2) 상위 Top 5 포트 월별 추이

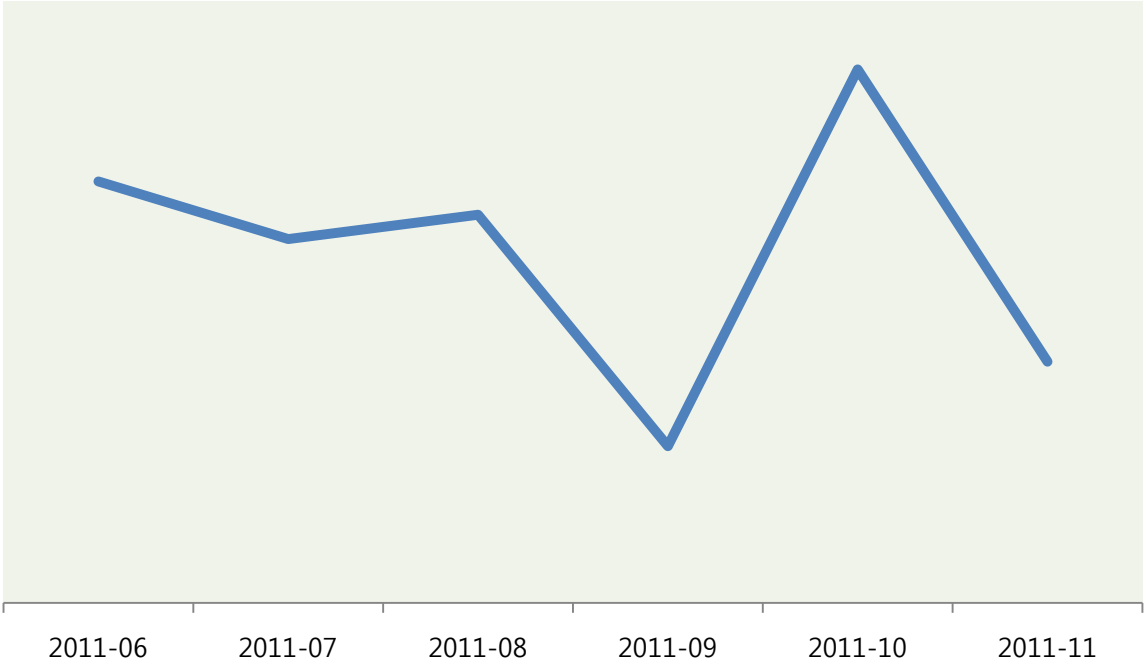
[2010년 09월 ~ 2011년 11월]



3개월 추이에서도 전체적으로 1433 포트의 트래픽 증가했으며, MySQL DBMS가 주로 사용하는 3306 포트의 유입이 다시 증가하였습니다.

(3) 악성 트래픽 유입 추이

[2011년 06월 ~ 2011년 11월]

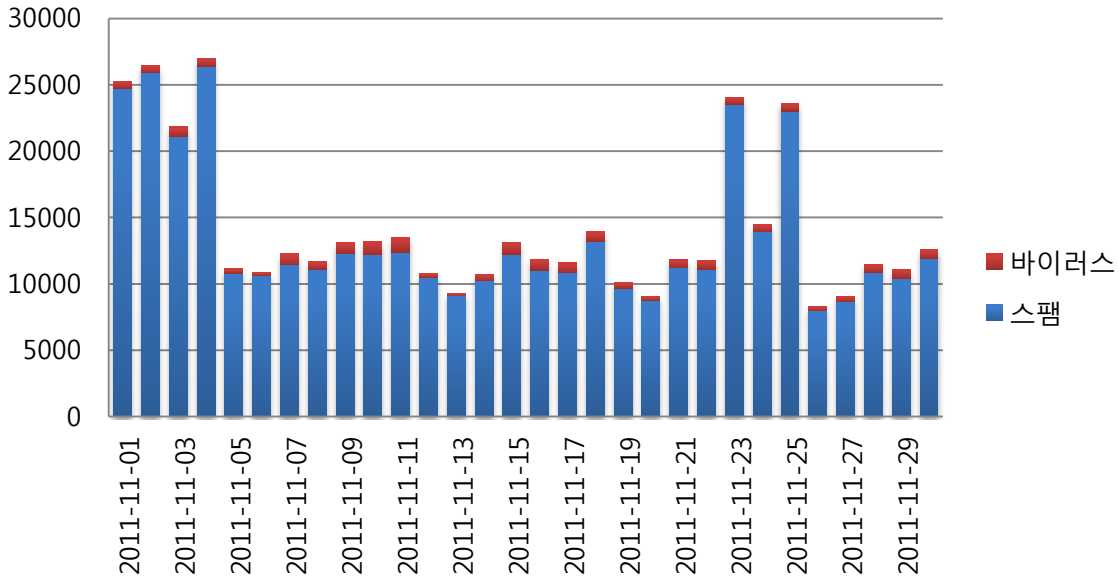


전체적인 악성 트래픽 유입이 11월에는 감소하였습니다.
11월에는 주로 단순한 패스워드를 사용하는 Microsoft SQL Server와 MySQL DBMS를 노린 유해 트래픽이 많았습니다.
현재 악성코드에 의해 자동적으로 DB 서버로 패스워드 대입 공격(Brute force attack)을 시도하는 경우가 많이 발견되고 있으므로 DB Server의 패스워드를 주기적으로 변경해야 하며, 단순한 패스워드 사용을 피해야 합니다.

Part I 11월의 악성코드 통계

5. 스팸 메일 분석

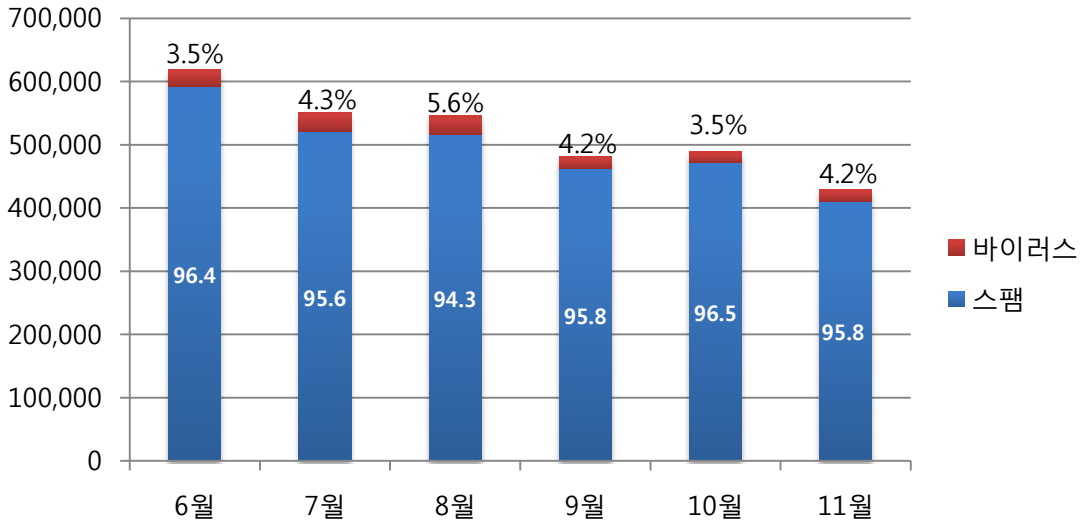
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 오는 바이러스 및 스팸 메일의 개수를 나타내는 그래프입니다. 11월 10일과 11일에는 악성코드 메일이 평소의 두 배 이상 증가하였으며, 스팸 메일 발송은 월초에 더 많았습니다.

(2) 월별 통계 현황

[2011년 6월 ~ 2011년 11월]



월별 통계 현황은 악성코드 첨부 및 스팸메일이 전체메일에서 차지하는 비율을 나타내는 그래프입니다. 11월의 스팸 메일은 95.8%, 바이러스 메일은 4.2%를 차지하였으며, 대표적으로 "Bill payment canceled" 제목으로 된 악성코드 첨부 메일이 상당수 발견되었습니다.

(3) 스팸 메일 내의 악성코드 현황

[2011년 11월 1일 ~ 2011년 11월 30일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Mytob	7,122	41.19 %
2	W32/MyDoom	3,566	20.62 %
3	Mal/ZipMal	2,337	13.51 %
4	W32/Virut	1,487	8.60 %
5	W32/Bagz	983	5.68 %
6	Mal/BredoZp	759	4.39 %
7	Troj/Invo	504	2.91 %
8	W32/MyDoom	185	1.07 %
9	W32/Bagle	176	1.02 %
10	Troj/ZipMal	173	1.00 %

스팸 메일 내의 악성코드 현황은 11월 바이러스 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프입니다. 현재 W32/Mytob이 41.19%로 1위를 차지하였으며, 2위는 20.62%를 차지한 W32/Mydoom, 3위는 13.51%를 차지한 Mal/ZipMal-B입니다.

Part II 보안 이슈 돋보기

1. 11월의 보안 이슈

유명 게임업체가 해킹공격을 받아 고객 개인정보를 대량으로 유출했습니다. 그 밖에 웹하드 등록제 시행, 광고배너를 이용한 악성코드 유포, 안드로이드 악성코드의 급증 등이 11월의 이슈가 되었습니다.

- **웹하드 사업자 등록제 시행**

그 동안 방치돼 있었던 웹하드 서비스의 보안이 앞으로는 한층 강화될 것으로 보입니다. 지난 11월 21일부터 P2P, 웹하드 사업자 등 특수한 유형의 부가통신서비스가 사업을 하려면 반드시 방송통신위원회에 등록하도록 의무화되었습니다. 등록을 하려면 기술적인 이용자 보호 계획을 작성하여 제출해야 하기 때문에, 사업자들은 최소한의 보안투자를 고려할 수 밖에 없게 되었습니다. 7.7 DDOS, 3.3 DDOS 등에 이용된 악성 봇의 주요 감염 경로가 되어 불명예를 안았던 웹하드 서비스들이 보다 안전한 서비스로 인식되기를 기대합니다.

- **주요 포털 '메인 배너'에서 악성코드 유포**

국내 주요 포털사이트들의 메인페이지에서 악성코드가 유포되었습니다. 각 사이트에 제공된 배너광고에 악성코드가 포함되어 있었던 것이 원인으로 확인되었습니다.
광고를 제공한 광고대행사는 서버가 해킹되어 광고에 악성코드가 포함되었다며, 재발방지 대책을 세우겠다고 발표했습니다. 광고를 이용한 악성코드 유포는 이전부터 있었지만 광고를 이용한 감염공격의 규모가 커지고 있으므로 인터넷 이용자는 취약점 패치와 백신 사용 등의 조치를 통해 악성코드가 감염되지 않도록 하는 적극적인 주의가 필요합니다.

- **게임 사 개인정보유출**

게임회사의 서버가 해킹되어 특정 게임을 이용하던 이용자 1300만명의 개인정보가 유출되었습니다. 개인정보법 시행 이후 처음 발생한 대규모 개인정보유출 사고라는 점에서 더욱 주목을 받았습니다. 경찰조사가 진행되었으며 게임사는 사과발표를 하고 비밀번호 변경캠페인을 진행했습니다.

- **안드로이드 악성코드 급증**

안드로이드 플랫폼에서 동작하는 악성코드가 2011년 하반기들어 계속 증가세를 보이고 있습니다. 11월 한달 간 많은 보안연구소들은 안드로이드 악성코드의 증가세를 통계로 발표했습니다. 증가율은 기관 별 보고서마다 달랐지만 상반기 대비 최소 수 배~수십 배가 증가했다는 결과가 나왔습니다.

- **알약 VB100 획득**

알약이 체크마크에 이어 VB100 인증을 획득했습니다.

- **어도비 모바일 플래시 개발 중단**

엄청난 사용자 수로 인해서, 보안문제와 취약점 악용사례 역시 잦았던 Adobe가 Mobile 버전의 FlashPlayer개발 중단을 선언했습니다. 하지만 버그개선과 보안업데이트는 계속 제공된다고 합니다. 이와 관련해 일각에서는 Flash Player의 보안 문제를 어도비가 인정한 것으로 해석하기도 했으며, 어도비는 향후 HTML5와 관련된 기술에 집중할 것이라고 밝혔습니다.

- **페이스북에 음란, 폭력영상 확산**

페이스북에서 관심을 끌만한 문구로 이용자를 유도해 음란, 폭력영상을 확산시킨 공격이 발생했습니다. 페이스북 측은 대변인을 통해 공격자의 신원을 파악했으며 해당 게시물을 삭제하는 한편, 법적-기술적 조치를 취했다고 밝혔습니다.

Part Ⅱ 보안 이슈 돋보기

2. 11월의 취약점 이슈

• Microsoft 11월 정기 보안 업데이트

TCP/IP의 취약점으로 인한 원격 코드 실행 문제, Windows Mail 및 Windows Meeting Space의 취약점으로 인한 원격 코드 실행 문제, Active Directory의 취약점으로 인한 권한 상승 문제 등을 해결한 Microsoft 11월 정기 보안 업데이트를 발표하였습니다.

<해당 제품>

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

<취약점 목록>

TCP/IP의 취약점으로 인한 원격 코드 실행 문제점(2588516)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 공격자가 대상 시스템 상의 닫힌 포트로 특수하게 조작된 UDP 패킷을 연속적으로 보낼 경우 이 취약점으로 인해 원격 코드 실행이 허용될 수 있습니다.

Windows Mail 및 Windows Meeting Space의 취약점으로 인한 원격 코드 실행 문제점 (2620704)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 DLL(동적 연결 라이브러리) 파일과 동일한 네트워크 디렉터리에 있는 합법적인 파일(예: .eml 또는 .wcinv 파일)을 여는 경우 원격 코드 실행이 허용될 수 있습니다. 이렇게 하면 합법적인 파일을 열 때 Windows Mail 또는 Windows Meeting Space가 DLL 파일 로드 및 포함된 코드 실행을 시도할 수 있습니다. 공격에 성공하려면, 사용자가 신뢰할 수 없는 원격 파일 시스템 위치 또는 WebDAV 공유를 방문하거나 이러한 위치에서 취약한 응용 프로그램이 로드되는 합법적인 파일(예: .eml 또는 .wcinv 파일)을 열어야 합니다.

Active Directory의 취약점으로 인한 권한 상승 문제점(2630837)

이 보안 업데이트는 Active Directory, ADAM(Active Directory Application Mode) 및 AD LDS(Active Directory Lightweight Directory Service)에서 발견되어 비공개적으로 보고된 취약점 1건을 해결합니다. 이 취약점으로 인해 Active Directory가 LDAPS(LDAP over SSL)를 사용하도록 구성되고 공격자가 유효한 도메인 계정과 관련된 해지된 인증서를 획득한 다음 그 인증서를 사용하여 Active Directory 도메인에 인증을 받는 경우 권한 상승이 발생할 수 있습니다. 기본적으로 Active Directory는 LDAP over SSL을 사용하도록 구성되지

않습니다.

Windows 커널 모드 드라이버의 취약점으로 인한 서비스 거부 문제점(2617657)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 사용자가 전자 메일 첨부 파일로 받은 특수하게 조작된 TrueType 글꼴 파일을 열거나 특수하게 조작된 TrueType 글꼴 파일이 있는 네트워크 공유 또는 WebDAV 위치로 이동하는 경우 이 취약점으로 인해 서비스 거부가 발생할 수 있습니다. 공격이 성공하려면 사용자가 특수하게 조작된 글꼴 파일을 포함한 WebDAV 공유나 신뢰할 수 없는 원격 파일 시스템 위치에 방문하거나 해당 파일을 전자 메일 첨부 파일로 열어야 합니다. 그러나 어떠한 경우에도 공격자는 강제로 사용자가 이러한 작업을 수행하도록 만들 수 없습니다. 대신 공격자는 사용자가 전자 메일 메시지 또는 메신저 메시지의 링크를 클릭하여 그렇게 하도록 유도하는 것이 일반적입니다.

<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/ms11-nov

영문 : http://technet.microsoft.com/en-us/security/bulletin/ms11-nov

• MS 윈도우 TrueType 글꼴 구문 분석 엔진 제로데이 취약점

CVE Number : CVE-2011-3402

윈도우 Win32k TrueType 글꼴 구문 분석 엔진에서, 임의의 코드를 실행시킬 수 있는 취약점이 발견되었습니다. 공격자는 웹 게시, 스팸 메일, 메신저 링크 등을 통해 특수하게 조작된 워드문서(.doc)파일을 사용자가 열어보도록 유도하여 다음과 같은 악성행위를 수행할 수 있으므로 주의가 요구됩니다.

※ 이 조치로 인해 글꼴과 관련된 일부 기능에 문제가 발생할 수 있으므로 주의가 필요합니다.

<해당 제품>

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

<해결 방법>

현재 해당 취약점에 대한 보안업데이트가 발표되지 않았습니다. 취약점으로 인한 위협을 경감시키기 위해 MS 홈페이지 "Fix it for me"섹션의 "Microsoft Fix it 50792"를 설치할 수 있습니다. 취약점에 대한 정식 패치가 발표되면 최신 보안업데이트를 설치한 뒤, 원상태로 복구하기 위해 "Microsoft Fix it 50793"을 적용하시기 바랍니다.

Microsoft Fix it 50793

- Enable : http://go.microsoft.com/?linkid=9788941
- Disable : http://go.microsoft.com/?linkid=9788942

<참고 사이트>

http://technet.microsoft.com/ko-kr/security/advisory/2639658
http://support.microsoft.com/kb/2639658

• Adobe Shockwave Player 취약점 업데이트 권고

CVE Number : CVE-2011-2448, CVE-2011-2446, CVE-2011-2447

Adobe Shockwave Player에 발생하는 코드 실행 취약점을 해결한 보안업데이트가 발표되었습니다. 낮은 버전의 Adobe Shockwave Player 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 하시기 바랍니다.

<해당 제품>

• Adobe Shockwave Player 11.6.1.629 및 이하 버전

<해결 방법>

윈도우, 매킨토시 환경의 Adobe Shockwave Player 11.6.1.629 및 이전 버전 사용자는 http://get.adobe.com/shockwave 방문하여 11.6.3.633 버전을 설치하거나 자동 업데이트를 이용하여 업그레이드해야 합니다.

<참고 사이트>

http://www.adobe.com/support/security/bulletins/apsb11-27.html

• Adobe Flash Player 및 AIR 다중 취약점 업데이트 권고

CVE Number : CVE-2011-2445 외

Adobe Flash Player 및 AIR에 영향을 주는 다중의 취약점을 해결한 보안 업데이트가 발표되었습니다. 취약점을 이용한 공격으로 인해 악성코드 감염등의 사고가 발생할 수 있으므로 낮은 버전의 Adobe Flash Player/Adobe Air 사용자는 반드시 최신버전으로 업데이트 하시기 바랍니다.

<해당 제품>

- 윈도우, 매킨토시, 리눅스, 솔라리스 환경에서 동작하는 Adobe Flash Player 11.0.1.152 및 이전 버전
- 안드로이드 환경에서 동작하는 Adobe Flash Player 11.0.1.153 및 이전 버전
- 윈도우, 매킨토시 환경에서 동작하는 Adobe AIR 3.0 및 이전 버전
- 안드로이드 환경에서 동작하는 Adobe AIR 3.0 및 이전 버전

<해결 방법>

Adobe Flash Player Download Center에서 Adobe Flash Player 11.0.1.152 버전을 설치하거나 자동 업데이트를 이용하여 최신버전으로 업그레이드 하시기 바랍니다.
http://get.adobe.com/kr/flashplayer

<참고 사이트>

http://www.adobe.com/support/security/bulletins/apsb11-28.html

• 한글 스택 버퍼오버플로우 취약점 업데이트 권고

워드프로세서 '한글'의 스택 버퍼오버플로우 취약점을 해결한 보안 업데이트가 발표되었습니다. 공격자는 해당 취약점을 악용하여 영향 받는 소프트웨어를 비정상적으로 종료시키거나, 이 취약점을 이용해 악의적인 코드를 실행할 수 있습니다. 낮은 버전의 한글 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 하시기 바랍니다.

<해당 제품>

- 한글 2004 6.0.5.770 이전버전
- 한글 2005 6.7.10.1067 이전버전
- 한글 2007 7.5.12.623 이전버전
- 한글 2010 8.5.6.1131 이전버전

<해결 방법>

아래 한글과컴퓨터 홈페이지를 방문하여 보안업데이트 파일을 다운받아 설치하거나, 자동업데이트 기능을 통해 한글 최신버전으로 업데이트 하시기 바랍니다.
http://www.hancom.co.kr/downLoad.downPU.do?mcd=001

<참고 사이트>

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

Contact us...

㈜이스트소프트 알약대응팀

Tel : 02-881-2364

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr

http://advert.estsoft.com/?event=200910081275558