www.alyac.co.kr

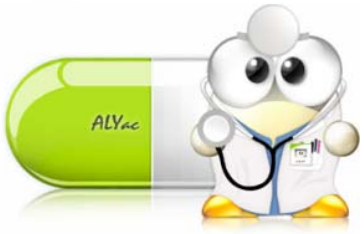
피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차



Part I 8월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

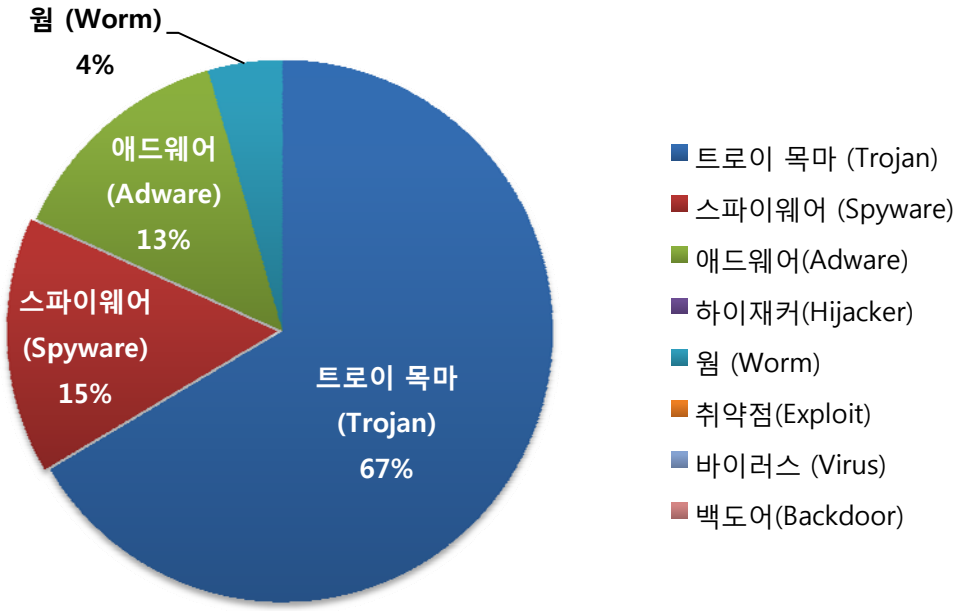
[2010년 8월 1일 ~ 2010년 8월 31일]

순위		악성코드 진단명	카테고리	합계 (감염자수)
1	New	V.DWN.KorAdware.sgi	Trojan	105,316
2	New	V.TRJ.Patched.imm	Trojan	73,657
3	↓1	S.SPY.Lineag-GLG	Spyware	47,154
4	New	S.SPY.OnlineGames.kb	Spyware	29,325
5	↓4	V.DWN.Agent.Pinsearch	Trojan	28,228
6	New	A.ADV.BHO.t120	Adware	26,951
7	New	Variant.Admoke.1	Adware	25,836
8	New	Rootkit.39010	Trojan	25,693
9	New	Trojan.Generic.4567643	Trojan	25,291
10	↑1	V.DWN.el.39xxxx	Trojan	22,845
11	↑3	V.WOM.Conficker	Worm	22,286
12	↓2	V.DWN.VB.paran	Trojan	21,101
13	New	V.TRJ.Agent.1588224	Trojan	20,199
14	↓9	A.ADV.Admoke	Adware	16,156
15	New	V.TRJ.AutoRun	Trojan	10,224

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

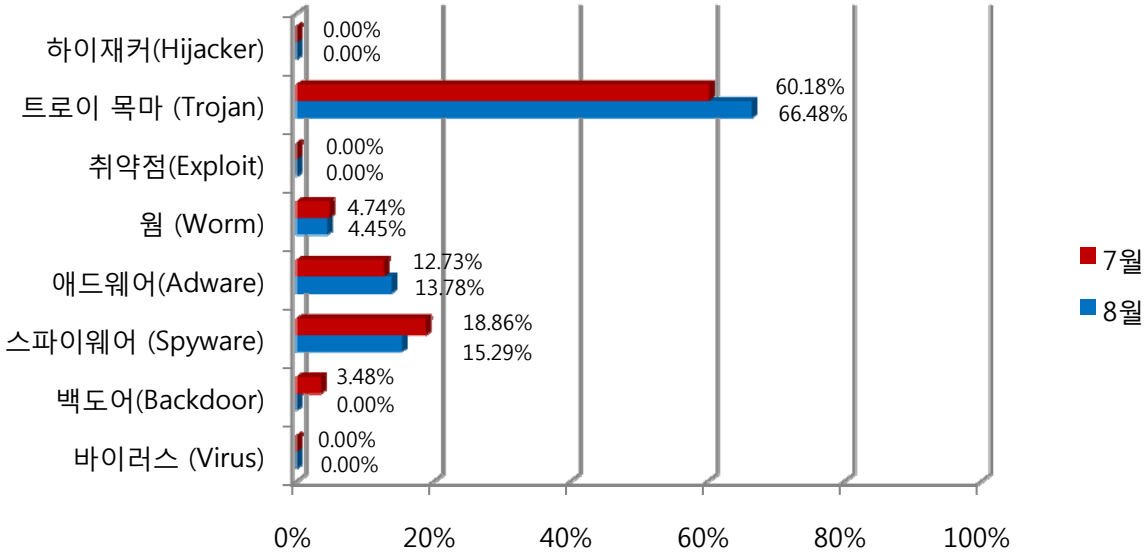
감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계이다.
8월의 감염 악성코드 TOP 15는 V.DWN.KorAdware.sgi이 105,316건으로 TOP 15 중 1위를 차지하였으며, V.TRJ.Patched.imm가 73,657건으로 2위, S.SPY.Lineag-GLG가 47,154건으로 3위를 차지하였다. 이외에도 8월에 새로 Top 15에 진입한 악성코드는 9종이다.
감염 악성코드 1위에 당당히 빛나는(?) V.DWN.KorAdware.sgi은 시작 프로그램에 등록되어 국내 에드웨어로 확인되는 프로그램을 사용자 동의 없이 PC에 다운로드한 후 설치되며, 2위~4위까지의 악성코드는 온라인 게임 계정을 탈취하기 위해 제작된 악성코드이다.

(2) 카테고리별 악성코드 유형



악성코드 유형별 비율은 트로이 목마(Trojan)가 67%로 가장 많은 비율을 차지하고, 애드웨어(Adware)가 14%, 스파이웨어(Spyware)가 15%의 비율을 각각 차지하고 있다. 이번에 67%의 가장 높은 비율을 차지한 트로이목마(Trojan)는 보안이 취약한 웹 사이트에서 유포된 경우가 많이 발견되었다.

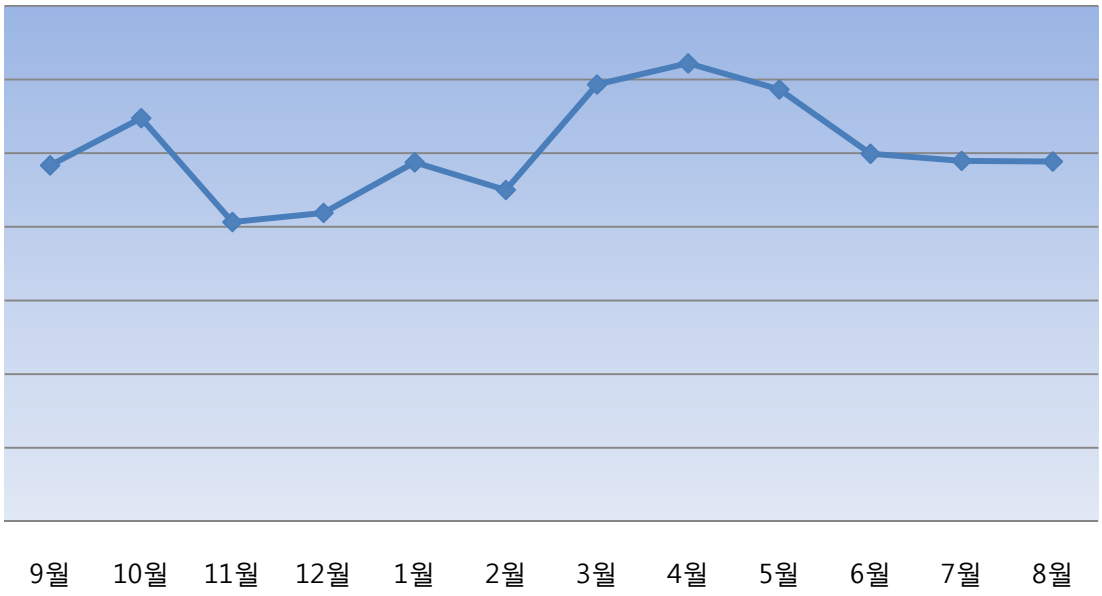
(3) 카테고리별 악성코드 비율 전월 비교



카테고리별 악성코드 비율을 전월과 비교하면, 트로이목마(Trojan)의 경우 전달에 비해 6.3% 정도 비율로 증가하였고, 스파이웨어의 경우(Spyware) 3.57% 정도 감소하였다. (바이러스, 취약점 등의 경우 Top15를 기준으로 했을 때 차지하는 비율이 없다는 것이다.)

(4) 월별 피해 신고 추이

[2009년 9월 ~ 2010년 8월]

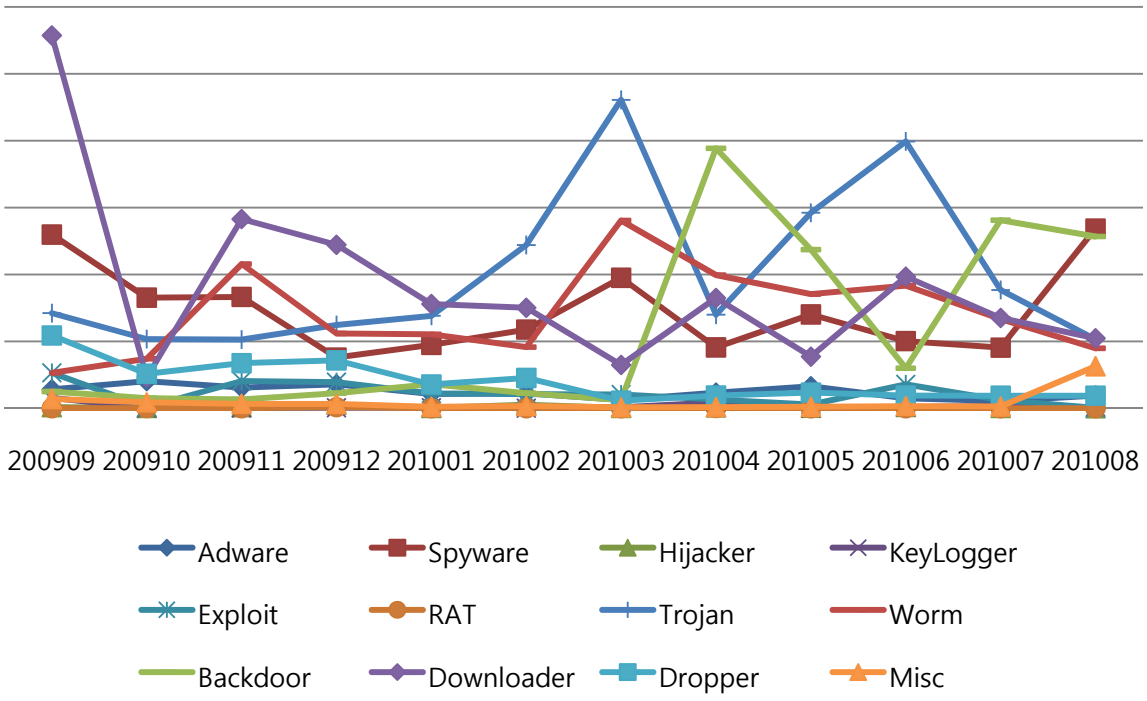


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프이다. 8월의 경우 전달(7월)보다 신고 건수는 증감하지 않았다.

(5) 월별 악성코드 DB 등록 추이

[2009년 09월 ~ 2010년 8월]



Part I 8월의 악성코드 통계

2. 악성코드 이슈 분석 – "V.DRP.SalityLnk 악성코드"

지난 7월 19일에 공개된 Lnk 취약점(CVE-2010-2568)을 악용한 감염형 바이러스가 기업 환경을 중심으로 상당수 발견되어 분석을 시작하게 되었으며, V.DRP.SalityLnk가 파일 감염을 비롯한 스팸메일 발송, 계정 탈취, 자동실행(Autorun) 등 다양한 악성 행위를 하는 것으로 보여진다. 특히 공유폴더 및 네트워크폴더를 이용한 전파방식은 개인보다는 기업을 주 타켓(Target)으로 제작되었다고 볼 수 있다.

1) 네트워크를 통한 파일 생성(V.DRP.SalityLnk)

해당 파일(V.DRP.SalityLnk)은 실행 된 PC에서 파일을 생성시키지 않고, 네트워크를 통해 파일을 생성하는 것이 특징이다.

- 뮤텍스 생성
  MutexName = "woemnm593jfe"
- 레지스트리 생성
  HKEY_CURRENT_USER₩Software₩zrfke "session" = "29"
- WnetOpenEnumA, WNetEnumResourceA API를 사용하여 네트워크 폴더 접근

```
DWORD WNetOpenEnum(
  __in    DWORD dwScope,
  __in    DWORD dwType,
  __in    DWORD dwUsage,
  __in    LPNETRESOURCE lpNetResource,
  __out   LPHANDLE lphEnum);
DWORD WNetEnumResource(
  __in      HANDLE hEnum,
  __inout   LPDWORD lpcCount,
  __out     LPVOID lpBuffer,
  __inout   LPDWORD lpBufferSize);
```

분석 시 "lpBuffer" 에 들어가는 값이 검색 된 네트워크 공유 폴더 목록들이 확인되었다.

```
VMware Shared Folders
Microsoft 터미널
Microsoft Windows 네트워크
Web Client Network
WORKGROUP
```

- 공유폴더를 통한 파일생성(w랜덤.tmp)
  네트워크 공유폴더를 찾아 조건이 맞는 폴더를 찾을 경우 그곳에 w(랜덤).tmp 파일로 생성시킨다.

```
CALL to CreateFileA from 1.00401348
FileName = "₩₩네트워크에 연결 된 컴퓨터₩공유폴더₩w1b0b25.tmp"
Access = GENERIC_WRITE
ShareMode = FILE_SHARE_WRITE
pSecurity = NULL
Mode = CREATE_ALWAYS
Attributes = HIDDEN|ARCHIVE
hTemplateFile = NULL
```

- 공유폴더를 통한 파일생성(Lnk)

  조건에 따라 Lnk 파일 앞에 "_" 또는 "~" 문자열이 붙는다.

```
lstrcpyA(&FileName, lpString2);
if ( (unsigned __int16)sub_40101A() % 100 > 30 )
{
  if ( (unsigned __int16)sub_40101A() % 100 <= 80 )
    lstrcatA(&FileName, "_");
  else
    lstrcatA(&FileName, "~");
}
v3 = sub_40101A();
lstrcatA(&FileName, (&lpString2)[4 * (unsigned __int16)v3 % 60]);
MultiByteToWideChar(0, 0, lpMultiByteStr, -1, &String, 260);
v4 = CreateFileA(&FileName, 0x40000000u, 2u, 0, 2u, 0x20u, 0);
hObject = v4;
if ( v4 == (HANDLE)-1 )
{
  result = v6;
}
else
{
  v8 = 2 * lstrlenW(&String) + 142;
  memcpy(&Dst, "L", 0x8Eu);
  v5 = lstrlenW(&String);
  memcpy(&v21, &String, 2 * v5);
  WriteFile(hObject, &Dst, v8 + 2, &NumberOfBytesWritten, 0);
  CloseHandle(hObject);
  result = 1;
}
return result;
```

자신의 ".data 섹션"에 담겨져 있는 Lnk파일의 헤더를 모든 Lnk파일이 생성될 때 공유하여 쓴다.

```
00415824  4C 00 00 00 01 14 02 00 00 00 00 00 C0 00 00 00   L.......?..
00415834  00 00 00 46 FF 00 00 00 00 00 00 00 00 00 00 00   ...F ..........
00415844  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00415854  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00415864  00 00 00 00 00 00 00 00 00 00 00 00 00 FF 14 00   .............  .
00415874  1F 00 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30   .???i↖.+0
00415884  30 9D 14 00 2E 1E 20 20 EC 21 EA 3A 69 10 A2 DD   0?..  ??i♬
00415894  08 00 2B 30 30 9D 0C 01 00 00 00 00 00 00 00 00   .+00?........
004158A4  00 00 00 6A 00 00 00 00 00 00 00 00 00 00 00 00   ...j............
```

00 00 00 6A 00 00 00 00 00 00 00 00 00 00 00 00값 뒤에 생성된 w(랜덤).tmp 파일명이 들어온다.

- 생성 되는 Lnk 파일 목록

Copy of New Folder.lnk, Copy of New File.lnk, Copy of Shortcut.lnk, New Shortcut.lnk, New Folder.lnk, Shortcut.lnk, Drivers.lnk, Anna Benson Sex video.lnk, Kate Beckinsale nude pictures.lnk, Jenna Elfman sex anal deepthroat.lnk, Miss America Porno.lnk, Porno Screensaver.lnk, Serials.lnk , Barrett Jackson nude photos.lnk, Britney Spears XXX.lnk, Paris Hilton XXX Archive.lnk, XXX hardcore.lnk, XXX.lnk, XXX archive.lnk, groom.lnk, Fotograf.lnk, Photoalbum.lnk, My photoalbum.lnk, Myphotos.lnk, My photos.lnk, My beautiful person.lnk, beautiful.lnk, Gallery photos.lnk, caroline.lnk, Katrina.lnk, kleopatra.lnk, Caitie.lnk Mary-Anne.lnk, Lisa.lnk, Bad girl.lnk, Julie.lnk, Aline.lnk, Anna.lnk, Barbi.lnk, Katrina.lnk, Juli.lnk ,Mary.lnk , Mandy.lnkSara.lnk, rebecca.lnk, Jammie.lnk, kate.lnk, Audra.lnk, stacy.lnk, Rena.lnk, elley.lnk, Tammy.lnk, Picture.lnk, My Photos.lnk, Photoalbum.lnk

2) Drop 파일 (V.TRJ.Sality.75776)

- 뮤텍스 생성

  MutexName = "uxJLpe1m"

- 레지스트리 수정

  ① 폴더 옵션의 숨김 파일 보기를 할 수 없도록 레지스트리 값을 수정한다.

```
HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩Advanced
"Hidden" = "2"
```

  ② 작업 관리자를 비활성화 하고 수정할 수 없도록 레지스트리 값을 수정한다.

```
HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩Policies₩system
"DisableTaskMgr" = "1"
"DisableRegistryTools" = "1"
```

  ③ 기본 브라우저가 항상 온라인 모드로 실행 되도록 레지스트리 값을 수정한다.

```
HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩Internet Settings
"GlobalUserOffline" = "0"
```

  ④ (사용자 계정 컨트롤)가 비활성화 되도록 레지스트리 값을 수정한다.

```
HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩policies₩system
"EnableLUA" = "0"
```

⑤ Windows 방화벽에 네트워크 접근을 할 수 있도록 레지스트리 값을 수정한다.

```
HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩SharedAccess₩Parameters₩
FirewallPolicy₩StandardProfile₩AuthorizedApplications₩List
"%TEMP%₩랜덤.exe" = "%TEMP%₩랜덤.exe:*:Enabled:ipsec"
```

⑥ 보안센터의 경고기능을 해제하기 위해 레지스트리 값을 수정한다.

```
HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Security Center
"AntiVirusOverride" = "1"
"AntiVirusDisableNotify" = "1"
"FirewallDisableNotify" = "1"
"FirewallOverride" = "1"
"UpdatesDisableNotify" ="1"

HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Security Center₩Svc
"AntiVirusOverride" = "1"
"AntiVirusDisableNotify" = "1"
"FirewallDisableNotify" = "1"
"FirewallOverride" = "1"
"UpdatesDisableNotify" ="1"
"UacDisableNotify" = "1""DisableTaskMgr" = "1"
"DisableRegistryTools" = "1"
```

⑦ Windows 방화벽 기능을 해제 할 수 있도록 레지스트리 값을 수정한다.

```
HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩SharedAccess₩Parameters₩
FirewallPolicy₩StandardProfile
"EnableFirewall" = "0"
"DoNotAllowExceptions" = "0"
"DisableNotifications" = "1"
```

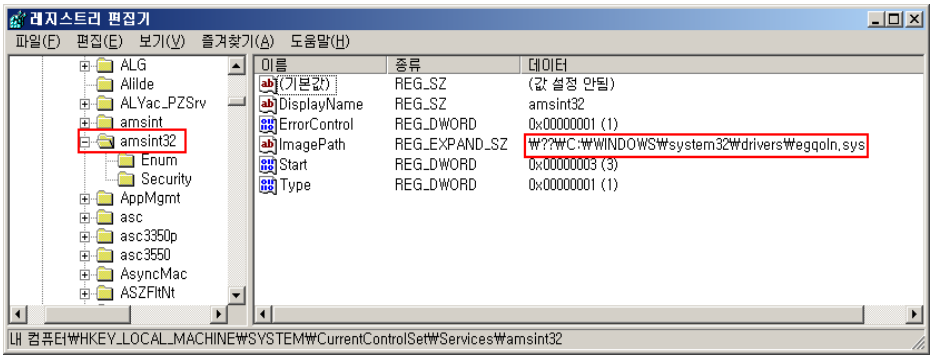
⑧ Windows 방화벽 기능을 해제 할 수 있도록 레지스트리 값을 수정한다.

```
HKEY_CURRENT_USER₩SYSTEM₩CurrentControlSet₩Control₩SafeBoot
HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩SafeBoot
```

⑨ 보안관련 서비스를 종료시키고 서비스를 삭제한다.

AVP, Agnitum Client Security Service, ALG, Amon monitor, aswUpdSv, aswMon2, aswRdr, aswSP, aswTdi, aswFsBlk, acssrv, AV Engine, avast! iAVS4 Control Service, avast! Antivirus, avast! Mail Scanner, avast! Web Scanner, avast! Asynchronous Virus Monitor avast! Self Protection, AVG E-mail Scanner, Avira AntiVir Premium Guard, Avira AntiVir Premium WebGuard, Avira AntiVir Premium , MailGuard, BGLiveSvc, BlackICE , CAISafe, ccEvtMgr, ccProxy, ccSetMgr, COMODO Firewall Pro Sandbox Driver cmdGuard, cmdAgent, Eset Service, Eset HTTP Server, Eset Personal Firewall, F-Prot Antivirus Update Monitor, fsbwsys, FSDFWD, F-Secure Gatekeeper Handler Starter, FSMA, Google Online Services, InoRPC, InoRT, InoTask, ISSVC, KPF4, KLIF, LavasoftFirewall, LIVESRV, McAfeeFramework, McShield, McTaskManager, MpsSvc, Navapsvc, NOD32krn, NPFMntor, NSCService, Outpost Firewall main module, OutpostFirewall, PAVFIRES, PAVFNSVR, PavProt, PavPrSrv, PAVSRV, PcCtlCom, PersonalFirewal, PREVSRV, ProtoPort Firewall service, PSIMSVC, RapApp, SharedAccess, SmcService ,SNDSrvc, SPBBCSvc, SpIDer FS Monitor for Windows NT, SpIDer Guard File System Monitor, SPIDERNT, Symantec Core LC, Symantec Password Validation, Symantec AntiVirus Definition Watcher, SavRoam, Symantec AntiVirus, Tmntsrv, TmPfw, UmxAgent, UmxCfg, UmxLU, UmxPol, Vsmon, VSSERV, WebrootDesktopFirewallDataService, WebrootFirewall, Wscsvc, XCOMM

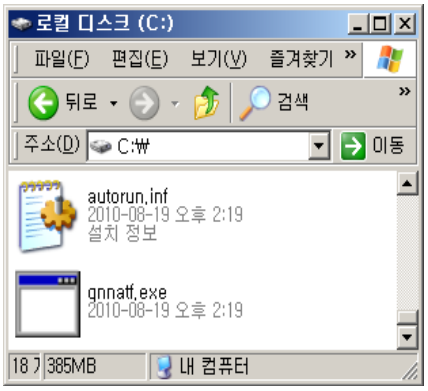
- 5,157 byte크기를 가진 랜덤 한 이름의 드라이버 파일을 생성시키며, 서비스로 동작된다.

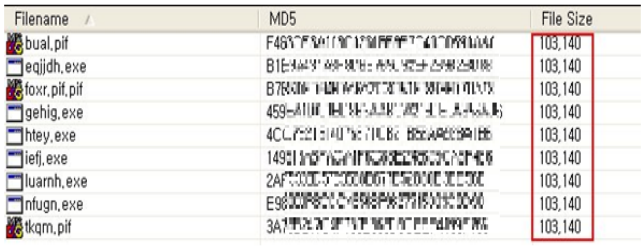


- 해당 드라이버 파일은 보안관련 사이트 접속을 차단한다.

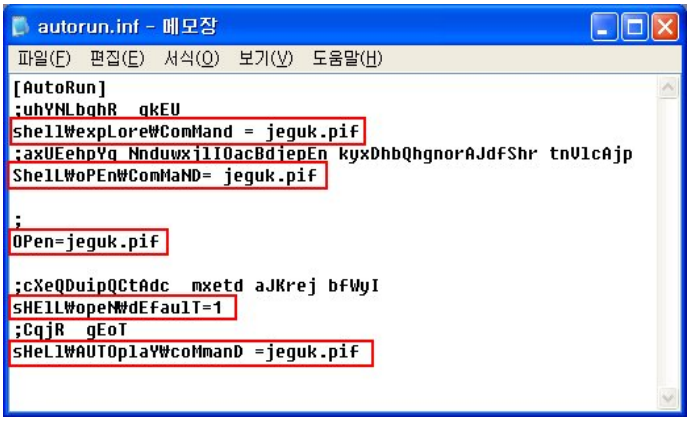
upload_virus, sality-remov, virusinfo, cureit, drweb, onlinescan.Spywareinfo, Ewido, Virusscan, Windowsecurity, Spywareguide, Bitdefender, Pandasoftware, Agnmitum, Virustotal, Sophos, Trendmicro, etrust.com, Symantec, Mcafee, f-secure, eset.com, kaspersky,

- 이동식디스크 전파를 위해 시스템루트에 해당 파일을 생성한다.
  생성 되는 파일은(exe, pif 확장자) 모두 100KB(103,140 Byte)로 생성되는 특징이 있다.





• Autorun.inf 파일은 보안프로그램 탐지를 피하려고 불필요한 문자들이 포함되어 있다. 또한 EXE와 PIF 파일 속 특정한 스트링을 담고 있다. (Hello world! Caption)




```
00000000h: 4D 5A 90 00 03 00 00 00 04 00 00 00 50 45 00 00 ; MZ?.......PE..
00000010h: 4C 01 01 00 79 72 66 3C 5B 4C 6F 72 64 50 45 5D ; L...yrf<[LordPE]
00000020h: E0 00 0F 01 0B 01 06 00 00 02 00 00 00 00 00 00 ; ?...............
00000030h: 00 00 00 00 40 10 00 00 00 10 00 00 0C 00 00 00 ; ....@...........
00000040h: 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 ; ..@.............
00000050h: 00 00 00 00 04 00 00 00 00 00 00 00 00 50 01 00 ; .............P..
00000060h: 00 02 00 00 00 00 00 00 02 00 00 00 00 00 10 00 ; ................
00000070h: 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 ; ................
00000080h: 10 00 00 00 00 00 00 00 00 00 00 00 60 10 00 00 ; ............`...
00000090h: 3C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; <...............
000000a0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000b0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000c0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000d0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000e0h: 00 00 00 00 00 10 00 00 10 00 00 00 00 00 00 00 ; ................
000000f0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000100h: 00 00 00 00 2E 74 65 78 74 00 00 00 00 40 01 00 ; .....text....@..
00000110h: 00 10 00 00 00 32 01 00 00 02 00 00 00 00 00 00 ; .....2..........
00000120h: 00 00 00 00 00 00 5C 00 00 20 00 00 E0 00 10 00 ; ......\. ..?...
00000130h: 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 ; ................
00000140h: 00 00 00 00 00 00 00 00 60 10 00 00 3C 00 00 00 ; ........`...<...
00000150h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000160h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000170h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000180h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000190h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000001a0h: 00 10 00 00 10 00 00 00 00 00 00 00 00 00 00 00 ; ................
000001b0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000001c0h: 2E 74 65 78 74 00 00 00 E2 00 00 00 00 10 00 00 ; .text...?......
000001d0h: 00 02 00 00 00 02 00 00 00 00 00 00 00 00 00 00 ; ................
000001e0h: 00 00 00 00 20 00 00 E0 00 00 00 00 00 00 00 00 ; .... ..?.......
000001f0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000200h: AC 10 00 00 00 00 00 00 C8 10 00 00 00 00 00 00 ; ?......?......
00000210h: 48 00 65 00 6C 00 6C 00 6F 00 20 00 77 00 6F 00 ; H.e.l.l.o. .w.o.
00000220h: 72 00 6C 00 64 00 21 00 00 00 00 00 43 00 61 00 ; r.l.d.!.....C.a.
00000230h: 70 00 74 00 69 00 6F 00 6E 00 00 00 00 00 00 00 ; p.t.i.o.n.......
00000240h: 60 E8 00 00 00 00 5B 81 C3 6D 02 00 00 53 74 03 ; `?...[?m...St.
00000250h: 42 30 E2 C3 6A 00 FF 15 00 10 40 00 C3 90 90 90 ; B0輸j.  ...@.?
00000260h: 9C 10 00 00 00 00 00 00 00 00 00 00 BA 10 00 00 ; ?.........?..
```

• 악성파일에 하드코딩 되어있는 특정서버에 접속하여 다른 악성파일을 다운로드 한다.

http://bi***ntek****.com/images/lo***.gif
http://ame***om****alty.com/images/lo***.gif
http://bh***irc****ge.com/images/lo**.gif
http://www.raf****.y***.pl/images/m***.gif
http://yu**lca****.com/lo***_s.gif
http://www.v***.wz.cz/lo***.gif
http://ra***n_m****r.fm.inte***.pl/m***.gif
http://m**.wz.cz/lo***.gif
http://b****bi****r.com/images/m****.gif

• 다운로드 된 파일은 암호화 되어있으며 디코딩 루틴을 통해 정상적인 PE파일로 변환된다.

```
00000000h: 8B 36 50 7B F5 F9 22 C4 3C BD 49 AB EB 28 ED B8 ; ?P{蠢"?<?I?(磁
00000010h: 1B FE A4 3B CB C7 5C BC 5C 01 2D 44 43 07 E1 2A ; .  ;改\?.-DC.?
00000020h: 9D BB 4A AF 6C 44 B7 2D 17 04 79 BF 78 14 40 4B ; 쒕J쥘D?..y쾽.@K
00000030h: C8 33 19 75 52 DE FE EC BC 76 2E 06 A7 74 BD 26 ; ?.uR柬耳v..晉?
00000040h: DC 39 8C 36 5C E1 45 05 43 A7 04 EE 8D 4D 66 FA ; ??\?.C??Mf?
00000050h: BF 92 3C 15 5E 0B 84 3E C0 4C 3A 44 B1 B4 36 A2 ; 폮<.^.?폴:D곤6?
00000060h: 78 0A 68 60 05 F2 3A 9D 8B FE 9E 67 C1 36 16 CF ; x.h`.?쑺?g?.?
00000070h: 9D 46 7F C2 8E 27 A2 A9 78 13 9B A8 9E 0D 00 9D ; 쒯혦'˜x.썾?.?
00000080h: 12 BB 49 E4 27 46 C5 F2 3D E9 B8 0F 7D F6 64 E3 ; .뒂?F뵛=勇.)??
00000090h: 6E 23 58 42 AF AA DF AD 44 E5 3C FF 0E 79 8A 95 ; n#XB?쑬D?  .y뒘
000000a0h: 16 C4 36 A0 93 1A 58 8B EF F3 24 A5 BB 8D DB EC ; .?쥧.X뎰??띈?
000000b0h: 2A 53 C7 CF 58 51 55 A7 15 B0 1A 5E B6 68 DE 3F ; *S하XQU??^탯?
000000c0h: 07 8D 5C 87 81 24 69 3B DA C2 AD AE 2A F0 FA AE ; .?뉣$i;敏?*種?
```

```
00000000h: 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 ; MZ?........    ..
00000010h: B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ; ?.......@.......
00000020h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000030h: 00 00 00 00 00 00 00 00 00 00 00 00 D8 00 00 00 ; ............?..
00000040h: 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ; ..?.???L?Th
00000050h: 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F ; is program canno
00000060h: 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 ; t be run in DOS
00000070h: 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 ; mode....$.......
00000080h: E5 08 6C 53 A1 69 02 00 A1 69 02 00 A1 69 02 00 ; ?lS쥙..쥙..쥙..
00000090h: 22 75 0C 00 A3 69 02 00 49 76 08 00 AA 69 02 00 ; "u..즀..Iv..쵁..
000000a0h: 49 76 06 00 A3 69 02 00 A1 69 02 00 A7 69 02 00 ; Iv..즀..쥙..쥧..
000000b0h: C3 76 11 00 A8 69 02 00 A1 69 03 00 F3 69 02 00 ; 퀇..쒭..쥙..?..
000000c0h: 49 76 14 00 A0 69 02 00 52 69 63 68 A1 69 02 00 ; Iv..젰..Rich쥙..
```

3) 파일 감염

• 다음 확장자를 확인하여 감염 시킨다.

*.EXE *.SCR

• 다음 레지스트리 값에 있는 파일을 참조하여 다음 감염파일을 찾는다.

HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩ShellNoRoam₩MUICache
HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run
HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩Run

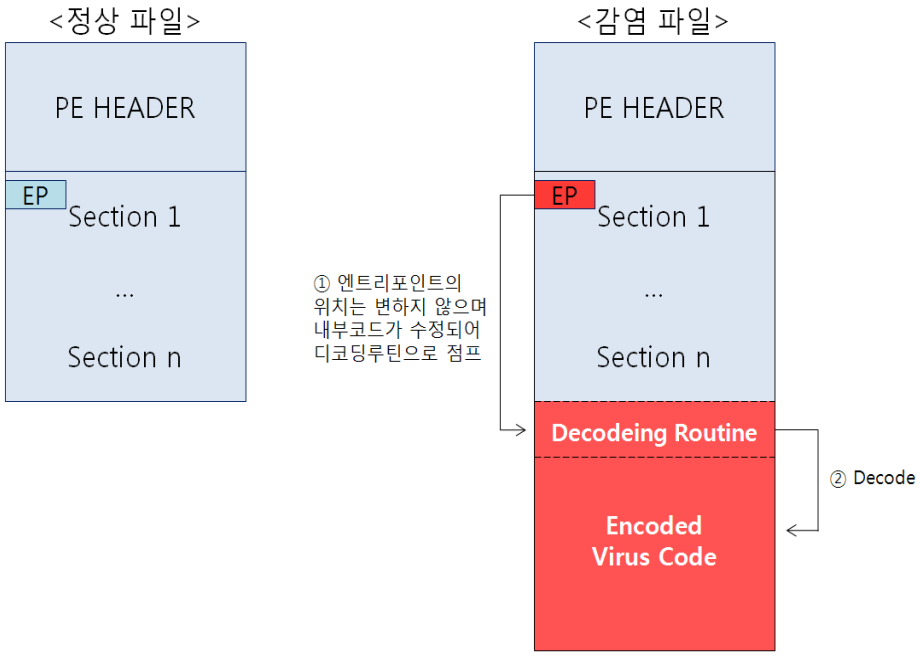
• %TEMP% 폴더에 존재하는 파일의 확장자를 다음과 비교하여 삭제한다.

%TEMP%₩*.exe	%TEMP%₩*.Rar

• 파일이름이 다음 스트링으로 시작하거나 Windows System File Checker(SFC)에 보호받는 파일은 감염에서 제외된다.

AVPM, A2GUARD, A2CMD, A2SERVICE, A2FREE, AVAST ,ADVCHK, AGB, AKRNL, AHPROCMONSERVER, AIRDEFENSE, ALERTSVC, AVIRA, AMON, TROJAN, AVZ, ANTIVIR, APVXDWIN, ARMOR2NET, ASHAVAST, ASHDISP, SHENHCD, ASHMAISV, ASHPOPWZ, ASHSERV, , ASHSIMPL, (중략...) XCOMMSVR, ZLCLIENT, ZONEALARM 등

• **감염파일과 정상파일의 차이**

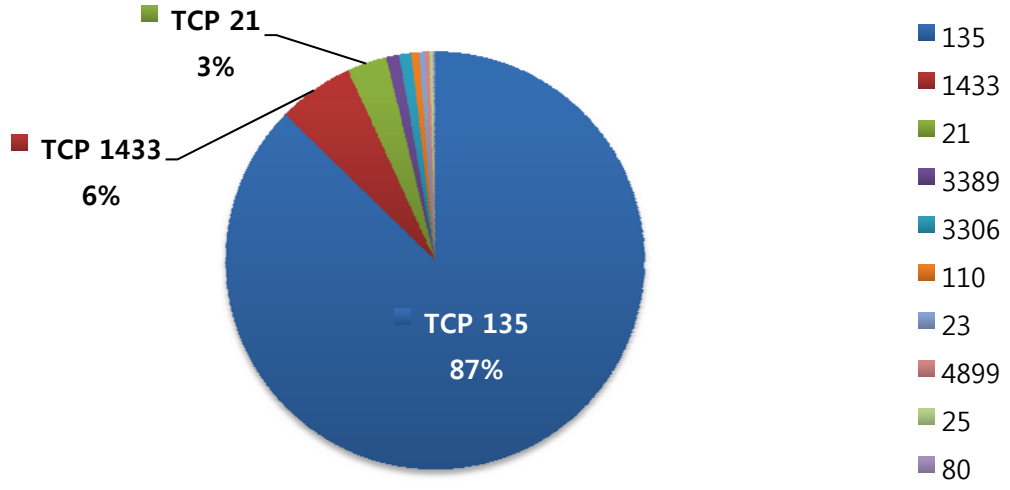


이번에 악성코드가 사용 한 Lnk 취약점은 현재 마이크로소프트에서 긴급패치가 이루어진 상태이다. 사용자는 윈도우 보안 업데이트를 최신으로 패치하는 것이 좋으며, 파일감염 바이러스까지 존재하는 악성코드이므로 보안제품의 실시간을 사용해야 효과적으로 방지할 수 있다.

Part I 8월의 악성코드 통계

3. 허니팟/트래픽 분석

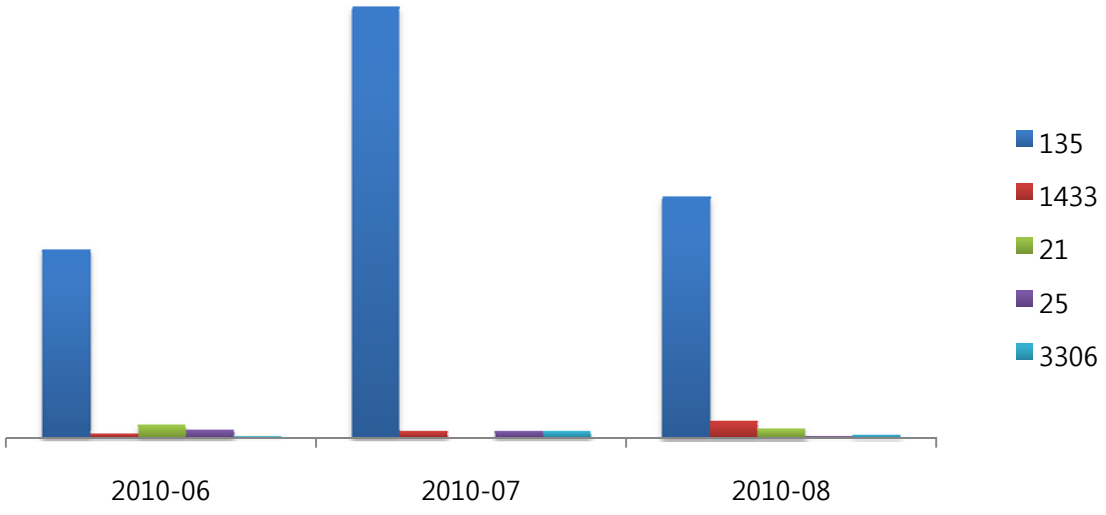
(1) 상위 Top 10 포트



8월에도 지속적으로 윈도우 자체의 취약점을 대상으로 한 TCP 135 포트 침입 시도가 가장 많았다. 135 TCP 포트에 대한 침입시도는 RPC(Remote Procedure Call) 버퍼 오버런이 가능한 보안 취약점을 주로 이용한다.
취약점을 이용한 공격이 성공할 경우 PC에 악성코드를 감염시킬 수 있다.

(2) 상위 Top 5 포트 월별 추이

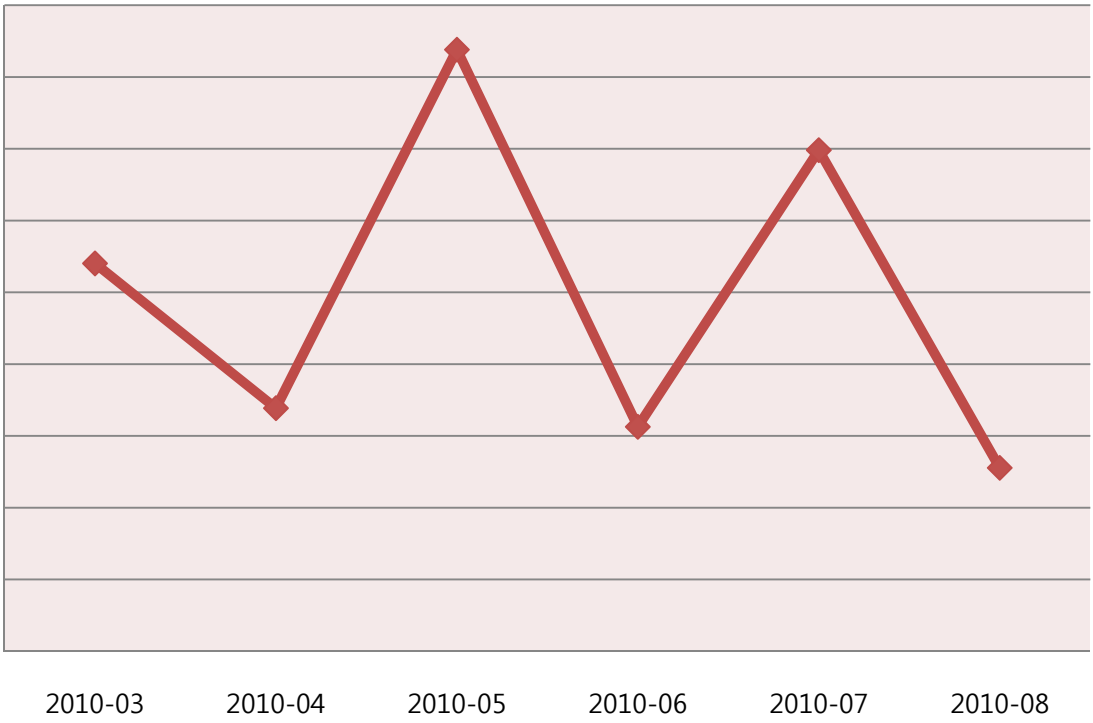
[2010년 6월 ~ 2010년 8월]



전체적으로 악성 트래픽 유입이 전달에 비해 감소하였고 TCP 135번 이외의 포트들은 악성 트래픽 유입이 증가하였다. 외부에서 135번 포트로 접근이 불필요한 경우 방화벽이나 IPS에서 차단하는 것이 보안 예방 효과에 좋다.

(3) 악성 트래픽 유입 추이

[2009년 3월 ~ 2010년 8월]

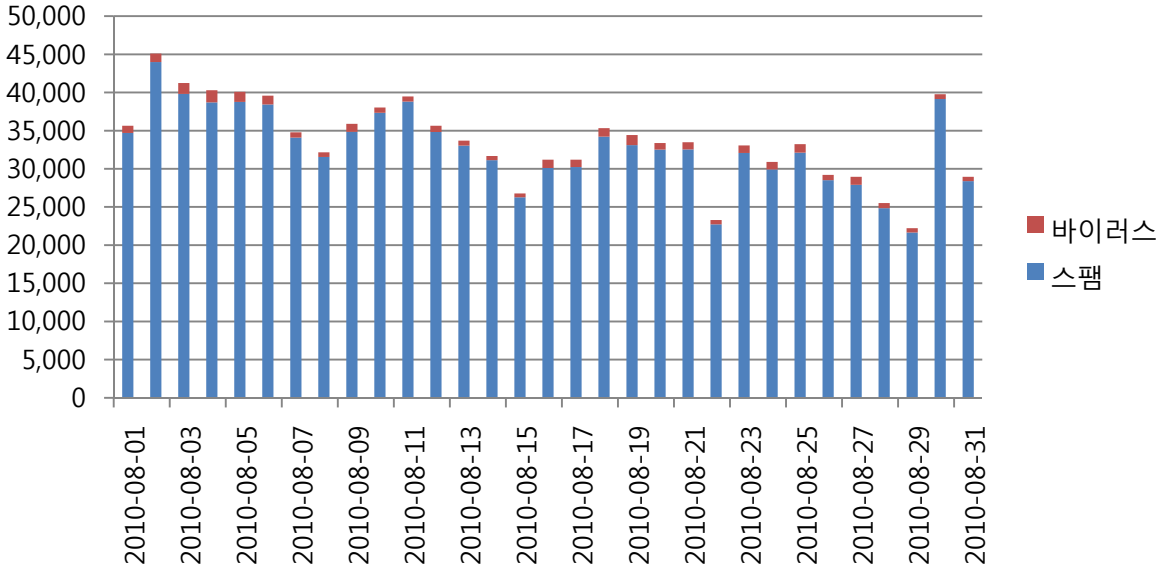


지난 달에 비해 악성 트래픽 유입이 다시 감소하였다.
최근에 누구나 SNS(Social Network Service)를 이용한 의사소통이 활발하기 때문에 SNS를 악성코드의 유포 혹은 C&C 서버로 사용하거나 단축 URL 주소의 링크를 통해 악성코드를 내려 받도록 시도한 사례가 있었다.
개개인이 사용하는 PC에 담긴 정보나 PC 자원은 악성코드 제작자에겐 금전적 이득을 얻기 위한 목표가 되기 때문에 이용자 스스로도 보안에 주의를 기울여야 한다.

Part I 8월의 악성코드 통계

3. 스팸 메일 분석

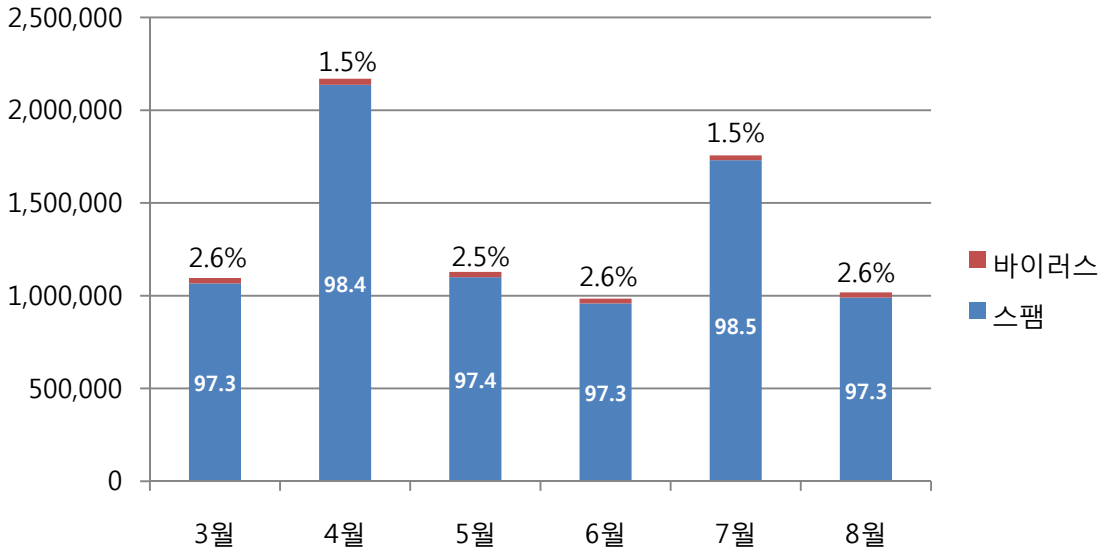
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 수신된 악성코드 첨부, 스팸메일의 개수를 나타낸 그래프이다. 최근 스팸 메일이 진화하면서 스크립트를 첨부한 스팸 메일, 안내 주문을 위장한 스팸 메일, 페이스북(Facebook), 트위터(Twitter) 메일로 위장한 스팸 메일 등 예전의 스팸 메일과는 비교할 수 없는 정교한 형태를 띄고 있어 문제가 심각하다. 이 같은 피해를 줄이려면 이 메일(E-mail) 확인 시 발신인이 불분명하거나 수상한 첨부 파일 있는 것은 가급적 읽지 말고 바로 삭제해야 한다.

(2) 월별 통계 현황

[2010년 3월 ~ 2010년 8월]



월별 통계 현황은 악성코드 첨부 및 스팸메일이 전체메일에서 차지하는 비율을 나타내는 그래프이다.

8월의 스팸 메일은 97.3%, 바이러스 메일은 2.6%를 차지하였다. 7월에 비해 스팸메일이 1.2% 감소, 바이러스 메일이 1.1% 비율로 증가하였다.

(3) 스팸 메일 내의 악성코드 현황

[2010년 8월 1일 ~ 2010년 8월 31일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Virut-T	8,872	34.49%
2	Mal/ZipMal-B	3,527	12.92%
3	W32/MyDoom-H	3,327	12.18%
4	W32/Mytob-C	2,538	9.29%
5	Mal/BredoZp-B	1m929	7.06%
6	Troj/CryptBx-ZP	925	3.39%
7	Troj/Invo-Zip	892	3.27%
8	W32/Mytob-R	752	2.75%
9	Troj/JSRedir-CH	637	2.33%
10	Troj/Iframe-EZ	450	1.65%

스팸 메일 내의 악성코드 현황은 8월 바이러스 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프이다. 현재 W32/Virut-T이 34.49%로 계속 1위를 차지하고 있다.

2위는 15.41%를 차지한 Mal/ZipMal-B, 3위는 12.55%를 차지한 W32/MyDoom-H이다.

8월은 SNS(social Network Service) 서비스인 페이스북(Facebook), 트위터(Twitter)를 위장해 악의적인 스팸 메일을 발송하는 사례가 많았으며, HTML 파일이 첨부된 형태가 많았다.

이와 관련된 악성 스크립트 탐지명들은 Troj/Iframe-EZ, Troj/JSRedir-CH이다.

Part II 8월의 이슈 돋보기

1. 8월의 보안 이슈

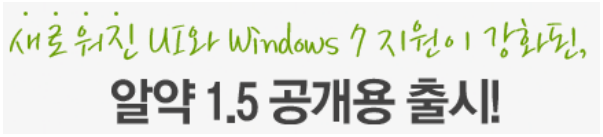
8월에는 새로운 UI와 윈도우7 지원이 강화된 알약 1.5 공개용 출시와 국내 IE6 (Internet Explorer 6) 퇴출 운동, USB 악성코드 인해 미국 국방부 해킹에 대한 보안 이슈가 있었습니다.

- **알약 1.5 공개용 버전 출시**

더욱 새로워진 UI와 윈도우7 운영체제 지원 강화, 악성 봇(Malicious Bot) 사전 방역 기능을 추가한 알약 1.5 공개용이 새롭게 출시되었습니다.

이번 알약 1.5 버전에서는 1.4 이전 버전의 UI를 버리고 더욱 깔끔해지고 넓어진 메인 메뉴 및 아이콘들을 제공하게 되었으며, 윈도우 7에서 Thumnail Button과 Taskbar Button Progress들을 지원해 알약의 작업상태와 진행 상황을 쉽게 확인할 수 있게 되었습니다. 이외에도 악성 봇 사전 방역 기능으로 내 PC가 좀비 PC가 되지 않도록 악성 봇 감염 의심시 사용자에게 바로 공지해드리고, 의심 파일의 경우 간편하게 신고하실 수 있습니다.

기존에 알약 1.4와 이하 버전을 사용하고 계시는 사용자께서는 "업데이트(UPDATE)" 버튼만 누르시면 1.5 버전으로 자동 업데이트 되며, 이스트소프트 알약 홈페이지에서 새로운 설치 파일을 내려 받아서 새로운 PC에 설치하셔도 됩니다.



• Internet Explorer 6 사용 이제는 그만~!

Internet Explorer 6이 처음 출시된 후 벌써 9년이라는 시간이 흘렀습니다.

9년의 시간 동안 낡아버릴 때로 낡아 버린 IE6 버전을 지금 우리나라에서는 아직도 상당수의 많은 PC에서 사용되고 있습니다.

현재 IE 6은 너무나 많은 보안 취약점을 가지고 있고, 웹 표준에도 맞지 않아 이제는 사용이 부적합 합니다. 그래서 윈도우를 사용하시는 사용자들은 무료로 제공되는 최신 버전인 IE 8을 설치하시거나 파이어폭스(Firefox), 오페라(Opera), 구글 크롬(Chrome), 애플 사파리(Safari) 같은 대안 브라우저를 사용하실 수도 있습니다.

<미국 콜로라도 덴버시에서 IE 6의 장례식이 열렸고, MS의 IE 개발진들이 조화를 보내기도 하였습니다.>

• 2년전 악성코드에 감염된 USB로 인해 미군 지휘 통제망 해킹 사실 인정

2008년 중동의 미군 기지에서 악성코드에 감염된 USB를 연결해 미군의 지휘 통제망이 해킹을 당했으며 이로 인해 외국 정보기관이 관리하는 서버로 기밀 자료 일부가 유출되었다고 미국 국방부 부장관인 윌리엄 린(William Lynn)이 밝혔습니다.

우리 군에서도 악성코드에 의해 외부로 기밀 자료가 일부 유출된 적이 있고. 많은 기업과 PC에서도 쉽게 USB를 사용하고 있어 결코 남의 일만으로 볼 수 없을 것 같습니다.

USB의 Autorun 기능을 이용해 전파되는 악성코드는 윈도우의 자동 실행 기능 차단과 알약 같은 최신의 백신을 사용해야만 예방 할 수 있습니다.

<미국 국방부 부장관인 윌리엄 린(William Lynn)과 미국 국방부 펜타곤>

Part Ⅱ 8월의 이슈 돋보기

2. 8월의 취약점 이슈

• Microsoft 8월 정기 보안 업데이트

윈도우 커널 취약점으로 인한 권한 상승 문제점과 MS 워드, 엑셀로 인한 원격코드 실행 문제점 등을 해결한 Microsoft 8월 정기 보안 업데이트를 발표하였습니다.
최근 이들 취약점을 이용한 악성코드 유포가 있으므로 윈도우 PC 사용자들은 반드시 보안 패치를 적용하시기 바랍니다.

<해당 제품>

- Microsoft Windows XP Service Pack 3 (32bit, 64bit CPU 환경)
- Microsoft Windows 2003 Service Pack 2 (32bit, 64bit CPU 환경)
- Microsoft Windows Vista Service Pack 1~2 (32bit, 64bit CPU 환경)
- Microsoft Windows 2008 Server Service Pack 2 (32bit, 64bit, Itanium CPU 환경)
- Windows 7 (32bit, 64bit CPU 환경)
- Windows 2008 R2 (64bit, Itanium CPU 환경)
- Microsoft Excel 2002~2003, Word 2002~2007

<취약점 목록>

[MS10-047] Windows Kernel 취약점으로 인한 권한 상승 문제
[MS10-048] Windows 커널 모드 드라이버 취약점으로 인한 권한상승 문제
[MS10-049] Windows SChannel 취약점으로 인한 원격코드실행 문제
[MS10-050] Windows Movie Maker 취약점으로 인한 원격코드실행 문제
[MS10-051] Microsoft XML Core Services 취약점으로 인한 원격코드실행 문제
[MS10-052] Microsoft MPEG Layer-3 Codecs 취약점으로 인한 원격코드실행 문제
[MS10-053] Internet Explorer 누적 업데이트
[MS10-054] SMB Server 취약점으로 인한 원격코드 실행문제
[MS10-055] Cinepak Codec 취약점으로 인한 원격코드 실행문제
[MS10-056] Microsoft Office Word 취약점으로 인한 원격코드 실행문제
[MS10-057] Microsoft Office Excel 취약점으로 인한 원격코드 실행문제
[MS10-058] TCP/IP 취약점으로 인한 권한 상승문제
[MS10-059] Tracing Feature for Services 취약점으로 인한 권한 상승문제
[MS10-060] Microsoft .NET Common Language Runtime and in Microsoft Silverlight 취약점으로 원격코드 실행문제

<해결책>

Windows Update를 수행하거나 Microsoft 보안 공지 요약 사이트에서 해당 취약점들의 개별적인 패치 파일을 다운로드 받을 수 있습니다.
한글 : http://www.microsoft.com/korea/technet/security/Bulletin/ms10-aug.mspx
영문 : http://www.microsoft.com/technet/security/Bulletin/ms10-aug.mspx

• Adobe Acrobat/Flash 계열 제품 보안 업데이트 권고

Adobe Acrobat/Flash 계열의 제품군에 대한 코드 실행 관련 취약점을 패치하는 보안 업데이트가 발표 되었습니다.
공격자는 해당 취약점을 악용하여 영향 받는 소프트웨어를 비정상적으로 종료시키거나, 임의의 명령을 실행하여 시스템에 대한 권한 획득할 수 있습니다.
낮은 버전의 Adobe Flash Player/Adobe Air 사용으로 악성코드 감염 등의 사고가 발생할 수 있으므로 사용자의 주의 및 최신버전 설치를 권고합니다.

<해당 제품>

- Adobe Reader 9.3.3 and earlier versions for Windows, Macintosh, and UNIX
- Adobe Acrobat 9.3.3 and earlier versions for Windows and Macintosh
- Adobe Flash Player 10.1.53.64 and earlier 10.x versions
- Adobe Flash Player 9.0.277.0 and earlier 9.x versions
- Adobe AIR 2.0.2.12610 and earlier versions

<취약점 목록>

CVE-2010-2862 : These updates resolve an integer overflow vulnerability that could lead to code execution
CVE-2010-1240 : These updates further mitigate a social engineering attack that could lead to code execution.
CVE-2010-0209 : This update resolves a memory corruption vulnerability that could lead to code execution
CVE-2010-2188 : This update resolves a memory corruption vulnerability that could lead to code execution
CVE-2010-2213 : This update resolves multiple memory corruption vulnerabilities that could lead to code execution
CVE-2010-2214 : This update resolves a memory corruption vulnerability that could lead to code execution
CVE-2010-2215 : This update resolves a vulnerability that could lead to a click-jacking attack.
CVE-2010-2216 : This update resolves a memory corruption vulnerability that could lead to code execution

<해결책>

Adobe Flash와 Acrobat 계열 제품을 Adobe 홈페이지에서 최신으로 업데이트하거나 개별 패치를 다운로드하여 설치합니다. (Adobe Reader : http://get.adobe.com/kr/reader/)

<참고 사이트>

http://www.adobe.com/support/security/bulletins/apsb10-16.html
http://www.adobe.com/support/security/bulletins/apsb10-17.html

• **안전하지 않은 라이브러리 로딩으로 인한 취약점 문제**

윈도우에 설치된 특정 애플리케이션이 안전하지 않은 DLL 파일을 로딩할 때의 취약점으로 인해 공격자가 원격에서 코드를 실행할 수 있거나 권한 상승이 가능한 취약점이 존재합니다.

<해당 제품>

Microsoft 제품 및 3rd party 소프트웨어 제품

<취약점 설명>

공격자가 특정 파일을 사용자가 열게하여 WebDAV 및 원격 네트워크 공유, USB 드라이브의 DLL 로드를 통해 원격에서 코드실행 및 권한 상승을 할 수 있으며 이 공격을 "binary planting" or "DLL preloading attacks"라고 부르고 있습니다.

<해결책>

* 임시 대응 방안

1) WebDAV와 원격 네트워크 공유에서 라이브러리 로딩 비활성화 처리
2) WebClient 서비스 비활성화 처리
3) 방화벽에서 TCP 139 및 445 포트 차단
4) Dynamic-Link Library Security 가이드라인이 적용된 3rd-party 프로그램 설치

<참고 사이트>

http://www.us-cert.gov/current/index.html#microsoft_releases_security_advisory5
http://www.microsoft.com/technet/security/advisory/2269637.mspx

• **안전하지 않은 라이브러리 로딩으로 인한 취약점 문제**

Apple iPhone, iPod Touch, iPad 운영체제가 PDF의 폰트를 처리할 때 원격코드 실행이 가능한 신규취약점이 발견되어 사용자의 주의가 필요합니다. Apple iPhone, iPod Touch, iPad에서 악의적으로 작성된 PDF 문서를 열어볼 경우 악성코드가 설치되거나 임의의 명령을 실행할 수 있습니다.

해당 취약점은 Jamebreakme.com 사이트에서 탈옥을 위해 PDF를 이용하는 취약점으로 원격코드실행이 가능합니다. 따라서 Apple iPhone, iPod Touch, iPad에서 신뢰할 수 없는 PDF 파일을 열어보는 것을 자제하는 등 사용자들의 주의가 요구됩니다.

<해당 제품>

Apple iOS 4.0.1 버전이 설치된 iPhone 4, 3GS, iPhone 3G, iPod Touch 2G, 3G 및 iPad

<해결책>

해당 취약점 문제(CVE-2010-1797)를 포함한 보안 패치가 발표되었습니다.
PC에 iTunes를 실행하고 iPhone (iPod, iPad) 장비를 연결해 업데이트를 실행합니다
참고사이트: http://us-cert.gov/current/index.html#apple_releases_ios_4_0

Contact us…

㈜이스트소프트 알약보안대응팀

Tel : 02-881-2364

E-mail : help@alyac.co.kr

알약 사이트 : www.alyac.co.kr