

피해갈 수 없는 탐지력

# 알약

월간 보안동향 보고서

**ESTsoft**

목차

**Part I 11 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 - “PC와 스마트폰을 동시에 감염시키는 악성코드” ..... 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 ..... 11

4. 스팸 메일 및 악성코드가 포함된 메일 분석 ..... 13

    (1) 일별 스팸 메일 및 악성코드 포함 메일 통계 현황 ..... 13

**Part II 보안 이슈 돋보기 ..... 14**

1. 11 월의 보안 이슈 ..... 14

2. 11 월, 12 월의 취약점 이슈 ..... 16

Part I 11월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

[2013년 11월 01일 ~ 2013년 11월 30일]

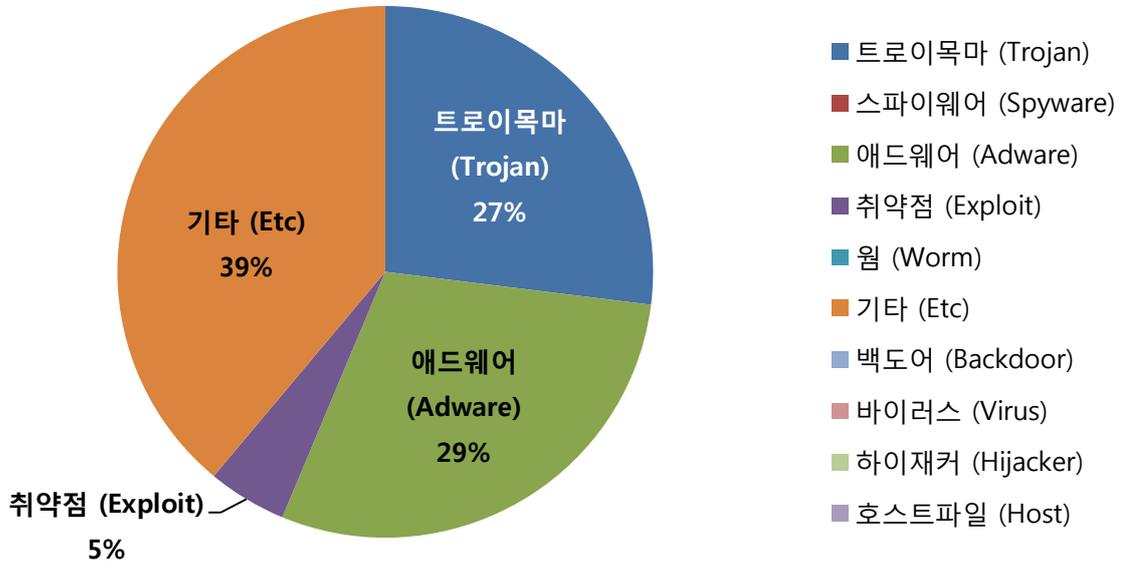
순위		악성코드 진단명	카테고리	합계 (감염자수)
1	-	Variant.Graftor.8654	Etc	4,895
2	↑ 13	Trojan.Downloader.KorAdware.Gen	Trojan	3,199
3	-	Gen:Trojan.Heur.GM.8500010002	Etc	2,314
4	New	Adware.Agent.NSR	Adware	1,569
5	New	Gen:Trojan.Heur.JPgu1@aCzyKfO	Trojan	1,516
6	New	Gen:Variant.Graftor.117786	Etc	1,473
7	New	Gen:Variant.Graftor.120775	Etc	1,428
8	New	Gen:Variant.Adware.Kazy.264370	Adware	1,407
9	-	Gen:Variant.Adware.Graftor.112065	Adware	1,498
10	New	Trojan.GenericKDV.1388504	Trojan	1,271
11	↓ 3	Gen:Variant.Adware.Strictor.6097	Adware	1,247
12	↓ 4	JS:Exploit.BlackHole.PL	Exploit	1,239
13	New	Gen:Trojan.Heur.1yXa4WvQ3@nG	Trojan	1,017
14	New	Adware.Generic.569687	Adware	988
15	New	Adware.Agent.NSS	Adware	898

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계입니다. 11월의 감염 악성코드 TOP 15에서는 지난달 각각 1위와 3위를 차지했던 Variant.Graftor.8654 악성코드와 Gen:Trojan.Heur.GM.8500010002이 이번달에도 동일한 순위를 기록하였습니다. 특이사항은 지난달 15위를 차지했던 Trojan.Downloader.KorAdware.Gen이 무려 13계단을 뛰어올라 새롭게 2위를 차지했다는 것입니다. Trojan.Downloader.KorAdware.Gen는 주로 정상프로그램으로 가장하여 사용자를 속이고 추가 애드웨어를 설치하는 다운로드를 통칭합니다. 10월에 비해 11월에는 악성코드 감염자수가 10%이상 감소하였으며, 전반적으로 애드웨어가 지난달에 비해 크게 증가한 시기였습니다.

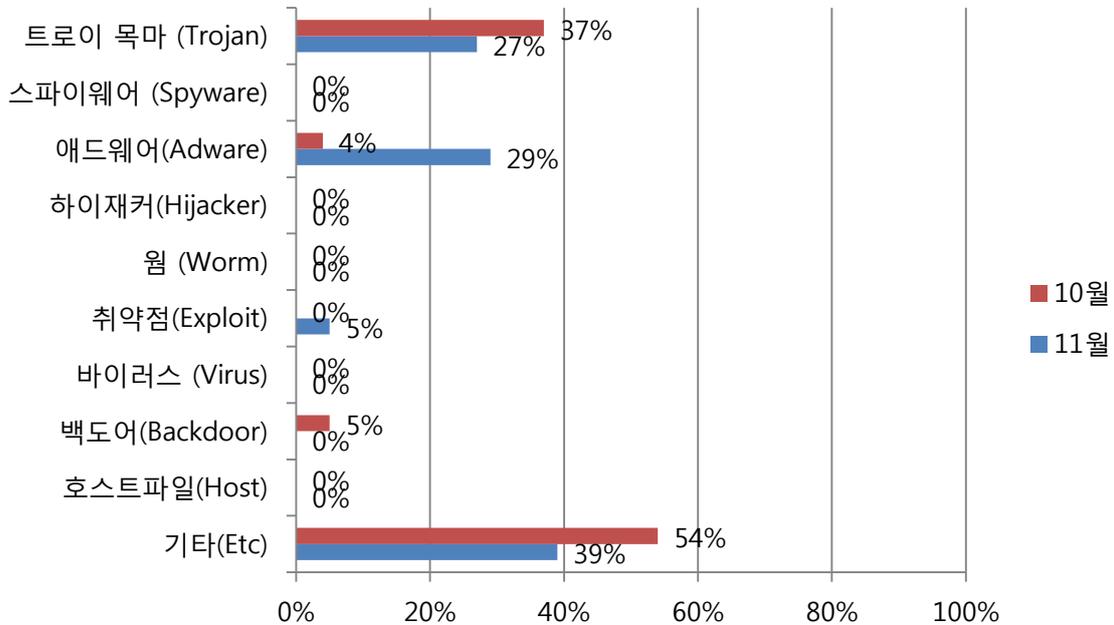


## (2) 카테고리별 악성코드 유형



악성코드 유형별 비율에서 기타(Etc) 유형이 가장 많은 39%를 차지했으며, 애드웨어(Adware)유형이 29%로 2위를 차지했습니다. 이어 트로이목마(Trojan) 유형이 그 뒤를 이었습니다.

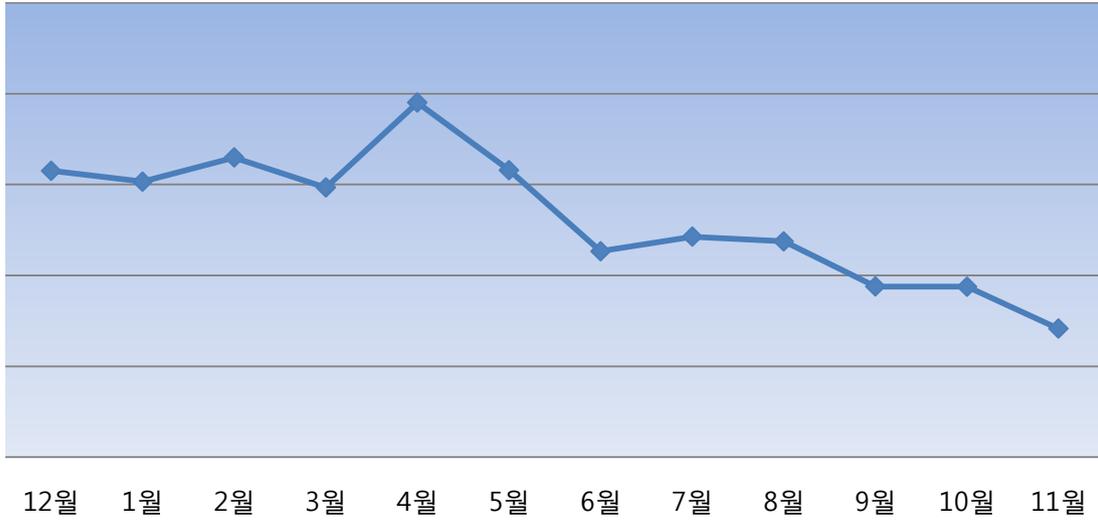
## (3) 카테고리별 악성코드 비율 전월 비교



11월에는 지난 10월과 비교하여 기타 (Etc) 유형 악성코드 비율이 크게 감소하였으며 트로이목마 (Trojan) 유형 악성코드도 함께 감소하였습니다. 다만, 애드웨어 (Adware) 유형의 악성코드들은 7 배 넘게 큰 폭으로 증가하였습니다.

#### (4) 월별 피해 신고 추이

[2012년 12월 ~ 2013년 11월]

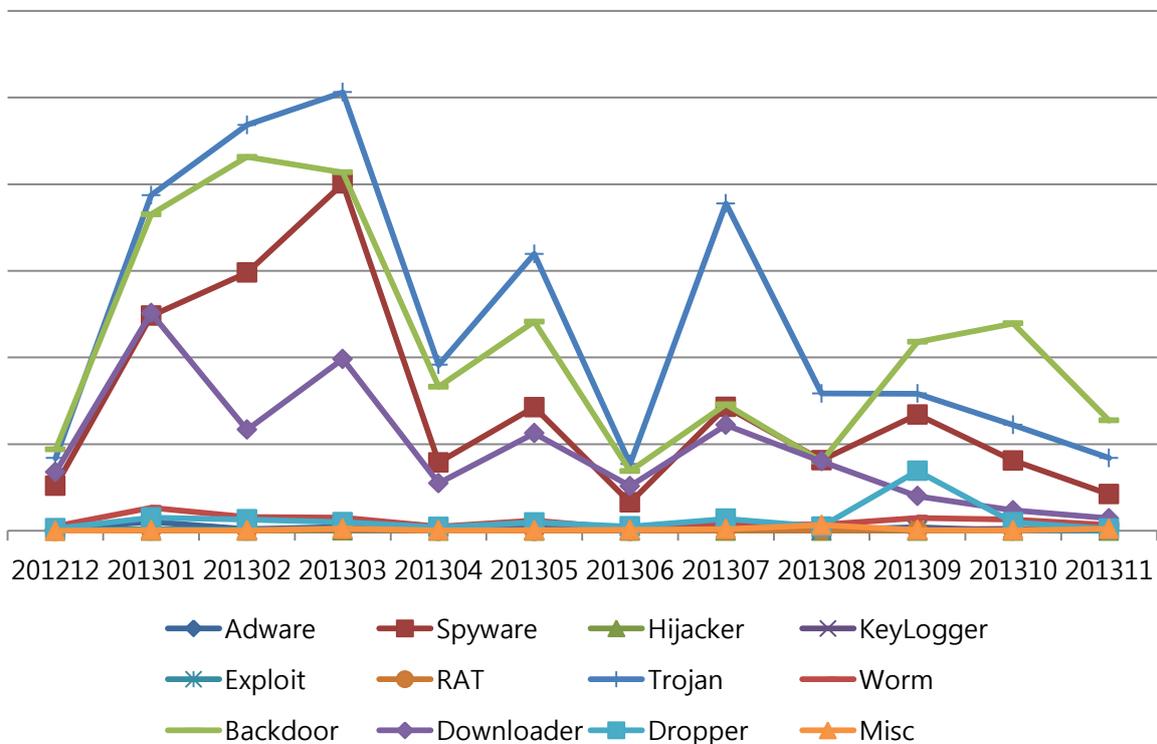


※ 알약 사용자의 신고를 합산해서 산출한 결과임

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

#### (5) 월별 악성코드 DB 등록 추이

[2012년 12월 ~ 2013년 11월]



Part I 11월의 악성코드 통계

2. 악성코드 이슈 분석 - “PC와 스마트폰을 동시에 감염시키는 악성코드”

(1) 개요

OS 취약점을 통해 PC 감염 후, PC에 연결된 안드로이드 스마트폰까지 감염시키는 신종 유포수법이 발견되었다. ‘USB 디버깅 모드’가 설정된 안드로이드 스마트폰 사용자를 타겟으로 하며 기존에 발견되었던 공격 유형에서 크게 벗어나, 향후 안드로이드 악성코드 감염방식의 다양화를 짐작하게 한다.

(2) 악성코드 분석

① 유포경로

최초 유포 경로는 12월 22일 오후 5시 경부터 변조 된 사이트에서 드라이브 바이 다운로드(Drive-by-download) 방식을 이용하여 생성 된 파일로 인해 유포 된 내역이 확인 되었다.

유포에 사용 된 경유 URL과 유포 URL 리스트는 아래와 같다.

일 시	경유 URL	유포 메인 URL	유포 파일 URL
12-22 17:07	hxxp://www.xx.com	hxxp://yy.com/index.html	hxxp://zz.com/svchas.exe

유포메인 URL은 Dadong Exploit Kit을 사용하였으며, Java Exploit(CVE-2011-3544, CVE-2012-0507, CVE-201-1723, CVE-2012-4681, CVE-2013-0422, CVE-2013-2465), IE Exploit(CVE-2012-1889), Flash Exploit(CVE-2013-0634) 취약점이 사용되었다.

② 악성파일 분석

※ 현재까지 확인 된 사항을 토대로 보고서 작성

※ 분석 파일은 가장 최근에 발견 된 변종파일로 분석 되었음

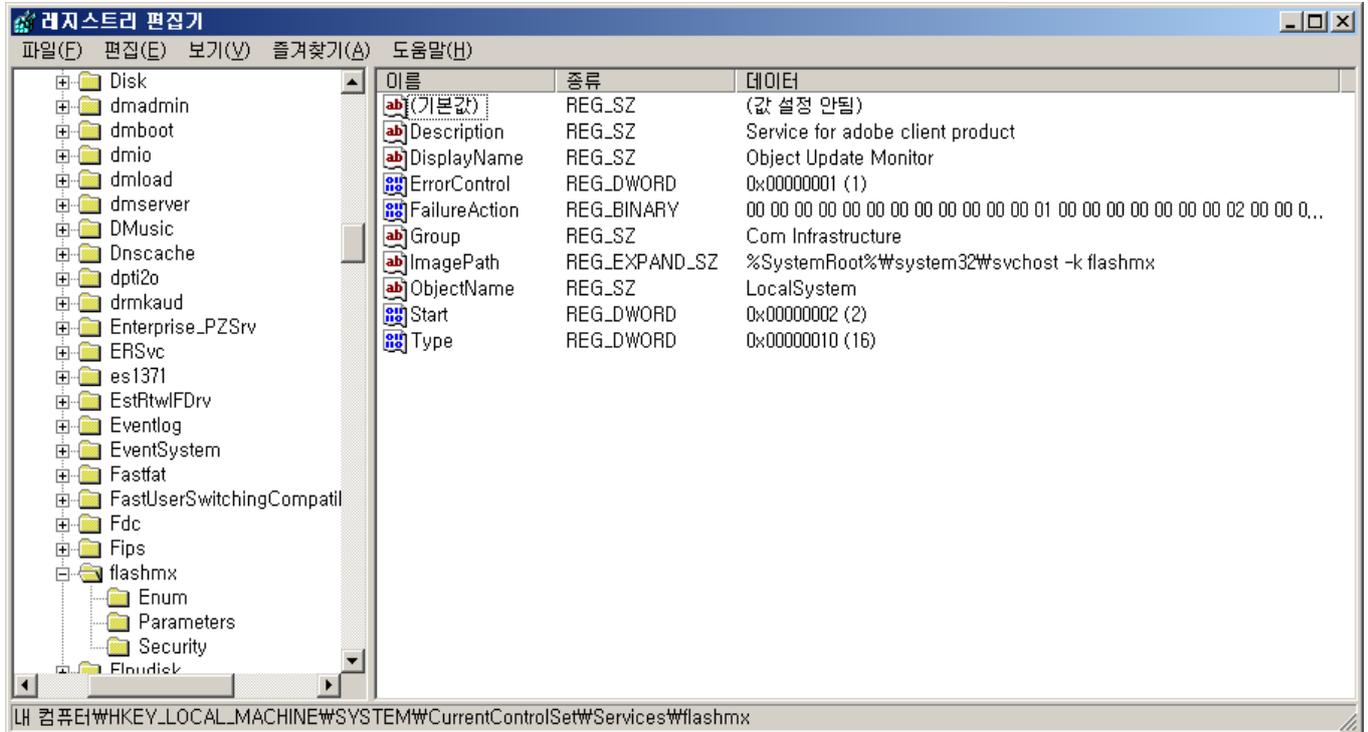
Detection Name	File Name	악성 행위
Trojan.Downloader.Agent.34304	svchas.exe	메인 드롭퍼
Trojan.Downloader.Agent.34304	flashmx32.xtl	다운로드 및 실행
(Alyac Mobile) Trojan.Android.SMS.Stech.Gen	AV-cdk.apk	인터넷 뱅킹용 악성파일

a. svchas.exe

- 파일 생성

해당 파일이 실행되면 C:\WINDOWS\system32 폴더에 flashmx32.xtl 파일을 생성시키고, 서비스 레지스트리를 생성하여 동작 시킨다.

- 생성 된 레지스트리  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\flashmx



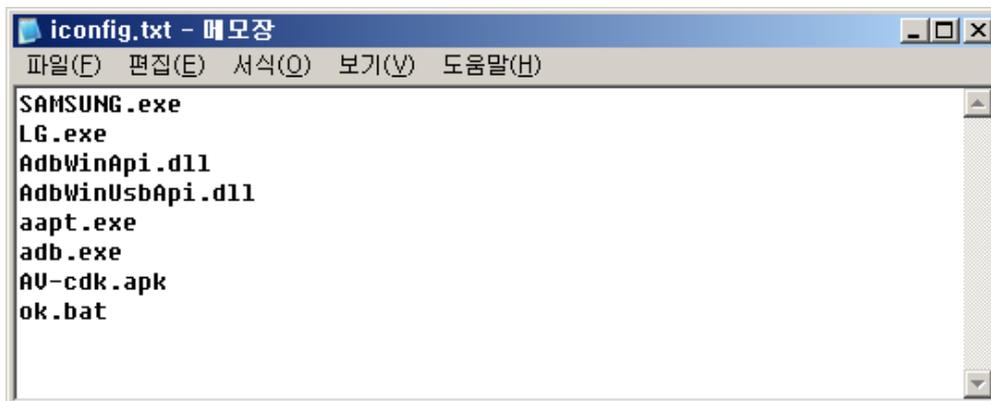
(그림. 생성 된 레지스트리 화면)

**b. flashmx32.xtl**

- 파일 다운로드

해당 파일이 실행되면 C:\WINDOWS\CrainingApkConfig 폴더를 생성 후 특정서버에 접속하여 iconfig.txt 파일을 다운로드 받는다.

iconfig.txt 파일은 hxxp://xia2.dyndns-web.com 서버에서 다운로드가 시도되며, 파일 내용은 아래와 같다.



(그림. 다운로드 할 파일 목록 리스트)

※ iconfig.txt 파일에 적혀있는 파일명들은 모두 다운로드 되는 파일로서 자세한 정보는 아래에 기재해 두었다.

<p>SAMSUNG.exe – SAMSUNG USB Driver for Mobile Phones                  LG.exe – LG United Mobile Driver InstallShield Wizard                  aapt.exe – Android Asset Packaing Tool                  adb.exe - Android Debug Bridge                  AdbWinApi.dll - Android ADB API Module                  AdbWinUsbApi.dll - Android ADB API (WinUsb) Module  <b>AV-cdk.apk – Android Malware (Alyac Mobile Detection : Trojan.Android.SMS.Stech.Gen)</b>                  ok.bat – Setup Install Batch File</p>
--

**- 어플리케이션 설치**

파일 다운로드가 완료되면, adb.exe 파일을 이용하여 AV-cdk.apk 파일을 USB에 연결 된 사용자 모바일 단말기에 설치를 시도한다.

```
memset(&OutputString, 0, 0x104u);
v0 = LoadLibraryA("kernel32.dll");
v1 = v0;
v2 = GetProcAddress(v0, "GetWindowsDirectoryA");
((void (__stdcall *)(CHAR *, signed int))v2)(&String2, 260);
FreeLibrary(v1);
lstrcatA(&String2, "WWWCrainingApkConfigWWW"); // 다운로드 된 폴더
lstrcpyA(&String1, &String2);
lstrcatA(&String1, "adb.exe");
lstrcatA(&String2, "AV-cdk.apk"); // 설치 할 악성 어플리케이션
wprintfA(&OutputString, "%s install %s", &String1, &String2); // adb.exe install AV-cdk.apk 로 실행
sub_10002470(&OutputString);
return sub_10002290(&OutputString) != 0;
```

(그림. 악성 어플리케이션 실행 코드 화면)

※ adb.exe로 설치 할 경우, 사용자 단말기에서 "USB 디버깅"이 설정되어 있어야 하며, 기본적인 어플리케이션 설치 시 보여지는 퍼미션 정보 화면이 보여지지 않고 바로 설치 됨으로 주의해야 한다.

**c. AV-cdk.apk**

**- 사용자 정보 유출 및 감시**

단말기의 버전정보, 폰번호, imsi, issms, 통신사 정보를 외부로 유출시키며, 전화 및 문자내용을 감시 한다.

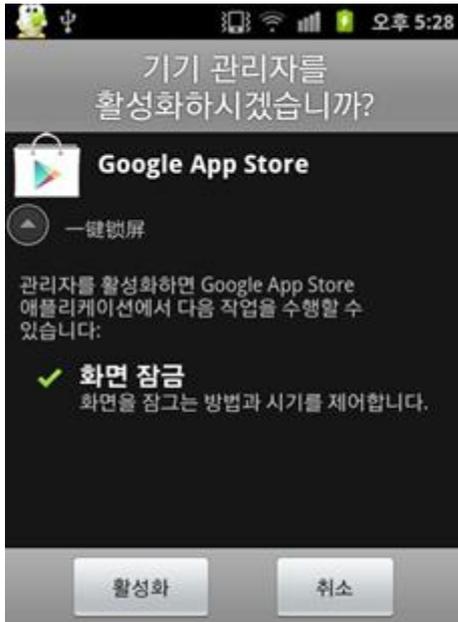
**- 악성 어플리케이션 파일 다운로드**

국내 인터넷 뱅킹 어플리케이션(NH뱅크, 신한S뱅크, 하나N Bank, 원터치개인)을 악성으로 대체할 파일들을 특정 서버에서 다운로드 받을 수 있다.

hxxp://www.slmoney.co.kr/Apk/KR\_NHBank.apk (농협 위장)  
 hxxp://www.slmoney.co.kr/Apk/KR\_SHBank.apk (신한은행 위장)  
 hxxp://www.slmoney.co.kr/Apk/KR\_HNBank.apk (하나은행 위장)  
 hxxp://www.slmoney.co.kr/Apk/KR\_WRBank.apk (우리은행 위장)

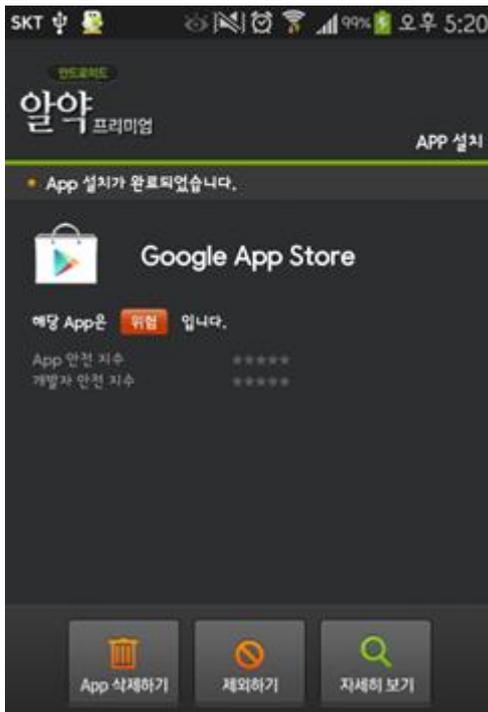
**- 기기관리자 등록**

디바이스 어드민권한을 이용하여 기기관리자에 등록해, 사용자가 삭제하기 어렵도록 설치한다.



**- 파일 탐지**

알약 안드로이드에서는 해당 어플리케이션을 **Trojan.Android.SMS.Stech.Gen** 으로 탐지 중이다.



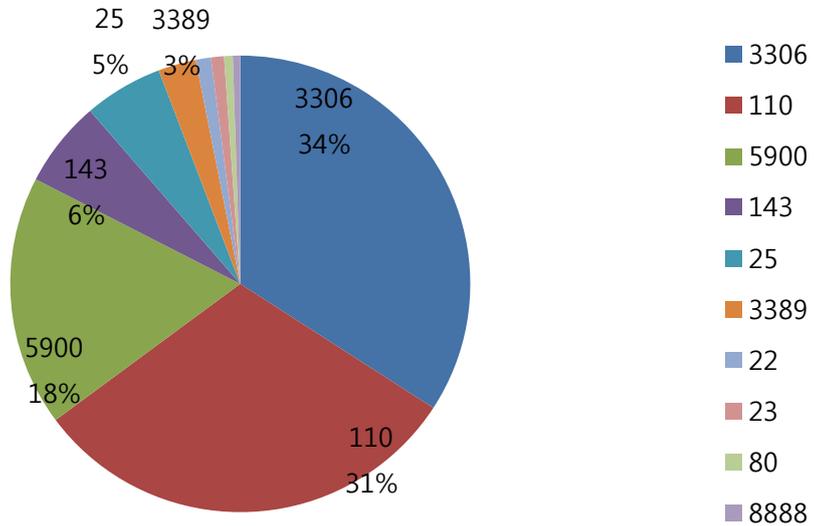
### (3) 결론

안드로이드 OS 버전에 따라 USB디버깅 상태를 확인하는 경로나 방식이 약간씩 다를 수 있으므로, 환경설정 메뉴에서 각자의 OS 상황에 맞게 USB디버깅 모드 메뉴를 찾아서 디버깅 모드 상태가 비활성화되어 있는지 확인하는 것이 안전하다.

Part I 11월의 악성코드 통계

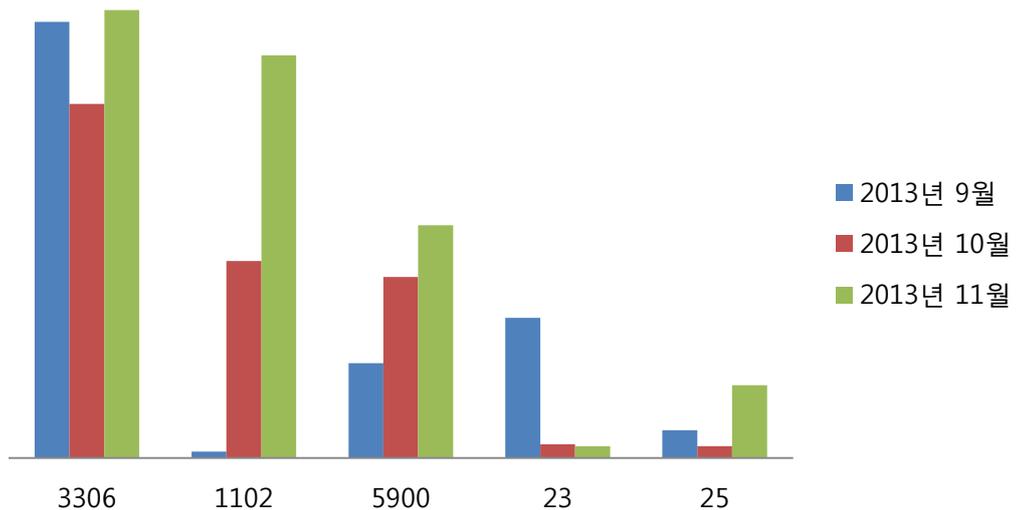
3. 허니팟/트래픽 분석

(1) 상위 Top 10 포트



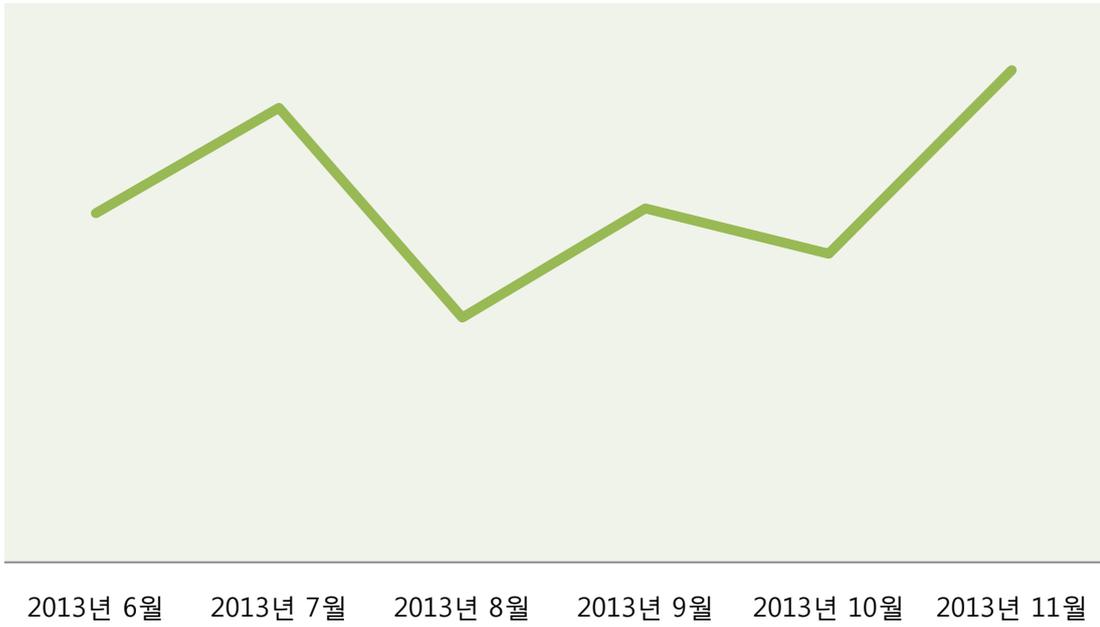
(2) 상위 Top 5 포트 월별 추이

[2013년 09월 ~ 2013년 11월]



(3) 악성 트래픽 유입 추이

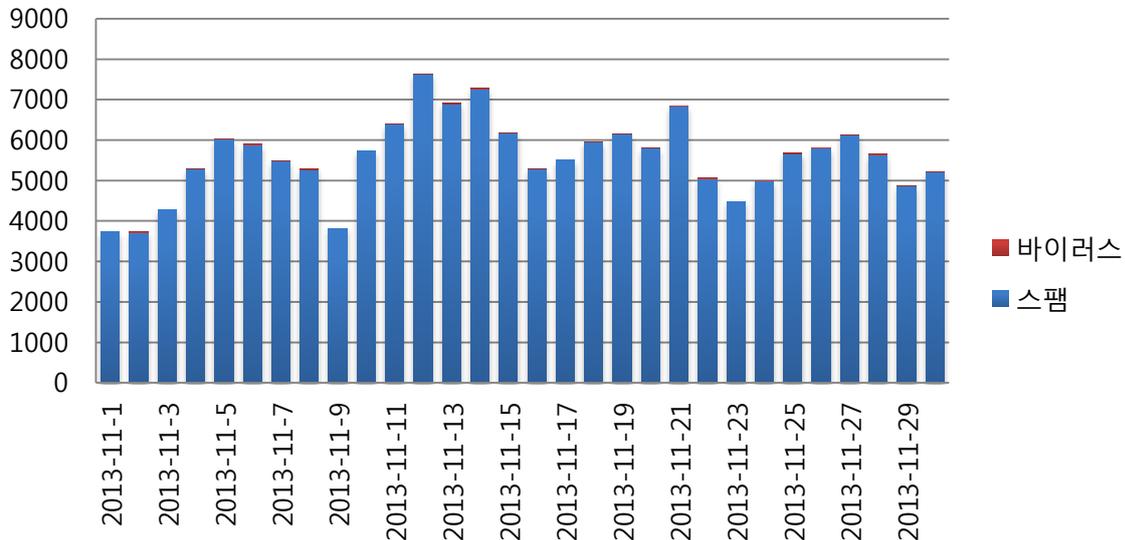
[2013년 06월 ~ 2013년11월]



Part I 11월의 악성코드 통계

4. 스팸 메일 및 악성코드가 포함된 메일 분석

(1) 일별 스팸 메일 및 악성코드 포함 메일 통계 현황



일별 스팸 및 악성코드 통계 현황 그래프는 하루에 허니팟 및 정보수집용 메일서버를 통해 유입되는 악성코드 및 스팸 메일의 개수를 나타내는 그래프입니다. 11월의 경우 메일서버 및 스팸 솔루션 교체 이후 처음 집계하는 통계입니다.

전체 메일 대비 약 10%가 살짝 밑도는 수준의 스팸메일이 접수되고 있으며 악성코드가 포함된 메일의 경우는 약 5%가 살짝 넘는 수준을 보이고 있습니다.



## Part II 보안 이슈 돋보기

### 1. 11월의 보안 이슈

RSA가 돈을 받고 암호화 SW에 백도어를 심었다고 합니다. 한국은행은 비트코인을 화폐로 인정할 수 없다고 했습니다. 그 밖에 SC, 씨티은행 고객 대출정보 13만여건 유출, MS가 노키아 인수의 최종관문을 통과 한 것 등이 11월의 이슈가 되었습니다.

#### • 한국정보화진흥원, 개인정보보호 인증(PIPL) 본격 시행

한국정보화 진흥원은 개인정보보호 인증제도(PIPL)를 1일부터 본격 시행하였습니다. 개인정보보호 인증은 정부가 개인정보보호법 준수기관을 인증해 주는 제도로서, 공공기관 뿐만 아니라 대기업, 중소기업, 소상공인까지 모든 개인정보 처리자가 해당 기관의 특성에 맞게 유형별로 신청할 수 있다. 인증절차는 공공기관과 민간 기업이 기관별로 사전에 인증심사기준에 대한 준비를 마친 후 인증을 신청하면 기관의 유형에 따라 심사가 실시됩니다.

#### • 한국은행, 비트코인, 화폐로 인정할 수 없다.

새로운 전자화폐인 '비트코인'을 두고 기획재정부, 한국은행, 금융위원회, 금융감독원이 논의를 한 결과, 국내 이용자가 극소수에 불과하고, 발행 주세 부재, P2P를 통한 보안 금융 사고의 위험성이 높기 때문에, 비트코인을 금융수단으로 인정하기에는 무리가 있다는 결론을 내렸습니다.

#### • MS 노키아 인수, 최종관문 통과

미국 정부와 유럽연합은 MS와 노키아의 사업영역이 겹치치 않아 시장이 불공정한 경쟁을 유발하지 않는다고 판단하여 마이크로 소프트(MS)의 노키아 휴대폰사업 인수를 승인하였습니다. 이에 따라, 마이크로소프트(MS)가 노키아 휴대폰사업을 인수하게 되었습니다. MS는 지난 9월 초, 72억 달러에 노키아 단말기 및 서비스 사업을 인수하고 노키아 특허에 대한 10년 라이선스를 체결했으며, 이 계약은 내년 1분기 마무리 될 전망입니다.

#### • NSA 감청 맞서 MS - 애플 - 구글 - 페북 뭉쳤다

마이크로소프트, 애플, 구글, 페이스북 등 미국 8개 주요 IT기업들이 국가안보국 등 감시기관의 정보수집 논란과 관련해 전면적인 개혁을 촉구하였습니다. 정부 감시활동 개혁 그룹은 웹사이트에 버락 오바마 미국 대통령과 의회 앞으로 보내는 서한을 공개하였으며, 정부의 정보수집과 관련하여 5가지의 원칙을 제시했습니다.

#### • SC, 씨티은행 고객 대출정보 13만여건 유출

한국스탠다드차타드 은행과 씨티은행의 고객 대출 정보 13여건이 유출되는 사건이 발생하였습니다. 이번 사건은 은행권의 개인정보 유출로는 사상 최대 규모로서, SC은행은 10여만건, 씨티은행은 3만여건의 개인정보가 유출 된 것으로 확인되었습니다. 이번 사고로 유출된 개인정보들은 향후 금융 사기에 이용될 가능성이 있어 사용자들의 각별한 주의가 필

요합니다.

• **내년 8월부터 주민번호 수집 금지**

개인정보보호법이 개정되면서, 2014년 8월부터 기업의 주민번호 수집이 전면 금지됩니다. 이전에 수집해 놓았던 주민번호도 2년 내 모두 삭제해야 합니다. 이에 따라 기업들은 법령에 명시된 예외적인 경우에만 주민번호를 수집하거나 이용할 수 있으며, 법 시행 이후 2년 이내인 2016년 8월까지 수집해 놓은 주민번호도 모두 삭제해야 합니다.

• **RSA, 암호화 SW에 '백도어' 심고 '뒷돈' 챙겨**

미국 보안솔루션 업체 EMC RSA가 미국 국가안보국으로 1천만달러를 받고 전산시스템에 몰래 접근할 수 있는 우회통로(백도어)를 미리 심어둔 것으로 나타났습니다. 암호화 기술은 원래 무작위로 숫자를 생성해야 하지만, RSA B세이프는 고정된 동일한 숫자들을 다수 알고리즘에 내장하여, 이 숫자를 알고 있는 사람이라면 누구나 암호문을 해독할 수 있습니다. 이에 따라, 민간 보안기술 전문업체가 정부기관과 뒷거래를 통해 사찰을 도왔다는 사실이 드러남에 따라 보안업체에 대한 신뢰도가 추락할 것으로 예상됩니다.

## 2. 11월, 12월의 취약점 이슈

### • 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 8.1
- 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 사용자에게 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 사용자에게 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 사용자에게 비해 영향을 적게 받습니다.

#### **Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점(2885093)**

이 보안 업데이트는 Microsoft Office에서 발견되어 비공개적으로 보고된 취약점 3건을 해결합니다. 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 사용자에게 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 거부 발생 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 로그인하고 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 로그인 자격 증명을 가지고 로컬로 로그인할 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 거부 발생 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>

**• Microsoft 12월 정기 보안 업데이트**

Microsoft Graphics Component의 취약점으로 인한 원격 코드 실행 문제, Internet Explorer 누적 보안 업데이트, Microsoft Scripting Runtime 개체 라이브러리의 취약점으로 인한 원격 코드 실행 문제 해결 등을 포함한 Microsoft 12월 정기 보안 업데이트가 발표되었습니다.

**<해당 제품>**

- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012

**Microsoft Graphics Component의 취약점으로 인한 원격 코드 실행 문제점 (2908005)**

이 보안 업데이트는 Microsoft Windows, Microsoft Office, Microsoft Lync의 공개된 취약점을 해결합니다. 취약점으로 인해 사용자가 특수하게 조작된 TIFF 파일이 포함된 공유 콘텐츠를 볼 경우 원격 코드 실행이 허용될 수 있습니다.

**Internet Explorer 누적 보안 업데이트(2898785)**

이 보안 업데이트는 Internet Explorer에서 발견되어 비공개적으로 보고된 취약점 7건을 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 사용자에게 비해 영향을 적게 받습니다.

**Windows의 취약점으로 인한 원격 코드 실행 문제점 (2893294)**

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 사용자나 응용 프로그램이 영향을 받는 시스템에서 특수하게 조작되고 서명된 이식 가능한 실행(PE) 파일을 실행 또는 설치할 경우 원격 코드 실행이 허용될 수 있습니다.

**Microsoft Scripting Runtime 개체 라이브러리의 취약점으로 인한 원격 코드 실행 문제점 (2909158)**

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 공격자가 사용자를 특수하게 조작된 웹 사이트나 특수하게 조작된 콘텐츠를 호스팅하는 웹 사이트를 방문하도록 유도할 경우 원격 코드 실행이 허용될 수 있습니다. 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.

**Microsoft Exchange Server의 취약점으로 인한 원격 코드 실행 문제점 (2915705)**

이 보안 업데이트는 Microsoft Exchange Server의 공개된 취약점 3건과 비공개적으로 보고된 취약점 1건을 해결합니다. Microsoft Exchange Server의 WebReady 문서 보기 및 데이터 손실 방지 기능에 이 중 가장 심각한 취약점이 있습니다. 공격자가 영향을 받는 Exchange 서버 사용자에게 특수하게 조작된 파일이 포함된 전자 메일 메시지를 보낸 경우 이러한 취약점은 LocalService 계정의 보안 컨텍스트에서 원격 코드 실행을 허용할 수 있습니다. LocalService 계정에는 로컬 시스템의 최소 권한이 있으며 네트워크에서 익명 자격 증명을 제시합니다.

**Microsoft SharePoint Server의 취약점으로 인한 원격 코드 실행 문제점(2904244)**

이 보안 업데이트는 Microsoft Office 서버 소프트웨어에서 발견되어 비공개적으로 보고된 여러 취약점을 해결합니다. 인증된 공격자가 SharePoint 서버에 특수하게 조작된 페이지를 보내는 경우 이러한 취약점으로 인해 원격 코드 실행이 허용될 수 있습니다. 이 취약점을 성공적으로 악용한 공격자는 대상 SharePoint 사이트의 W3WP 서비스 계정의 보안 컨텍스트에서 임의의 코드를 실행할 수 있습니다.

**Windows 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점 (2880430)**

이 보안 업데이트는 Microsoft Windows에서 발견되어 비공개적으로 보고된 취약점 5건을 해결합니다. 가장 위험한 취약점으로 인해 공격자가 시스템에 로그인하고 특수하게 조작된 응용 프로그램을 실행할 경우 권한 상승이 허용될 수 있습니다. 이 취약점을 악용하려면 공격자가 유효한 로그인 자격 증명을 가지고 로컬로 로그인할 수 있어야 합니다.

**LRPC 클라이언트의 취약점으로 인한 권한 상승 문제점(2898715)**

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 공격자가 LRPC 서버를 스푸핑하여 특수하게 조작된 LPC 포트 메시지를 LRPC 클라이언트로 보내는 경우 이 취약점으로 인해 권한 상승이 허용될 수 있습니다. 취약점 악용에 성공한 공격자는 프로그램을 설치하거나 데이터를 보고 변경하거나 삭제하고 모든 관리자 권한이 있는 새 계정을 만들 수 있습니다. 이 취약점을 악용하려면 공격자가 유효한 로그인 자격 증명을 가지고 로컬로 로그인할 수 있어야 합니다.

#### **ASP.NET SignalR의 취약점으로 인한 권한 상승 문제점(2905244)**

이 보안 업데이트는 비공개적으로 보고된 ASP.NET SignalR의 취약점을 해결합니다. 이 취약점으로 인해 공격자가 특수하게 조작된 JavaScript를 대상 사용자의 브라우저에 리플렉션할 경우 권한을 상승시킬 수 있습니다.

#### **Microsoft Office의 취약점으로 인한 정보 유출 문제점(2909976)**

이 보안 업데이트는 비공개적으로 보고된 Microsoft Office의 취약점을 해결합니다. 이 취약점으로 인해 사용자가 악의적인 웹 사이트에서 호스팅되는 Office 파일을 열 경우 정보 유출이 허용될 수 있습니다. 이 취약점 악용에 성공한 공격자는 대상 SharePoint 사이트 또는 다른 Microsoft Office 서버 사이트에서 현재 사용자 인증에 사용되는 액세스 토큰을 확인할 수 있습니다.

#### **Microsoft Office 공유 구성 요소의 취약점으로 인한 보안 기능 우회(2905238)**

이 보안 업데이트는 현재 악용되고 있는 Microsoft Office의 공유 구성 요소의 공개된 취약점을 해결합니다. 이 취약점으로 인해 사용자가 Internet Explorer와 같이 COM 구성 요소를 인스턴스화할 수 있는 웹 브라우저에서 특수하게 조작된 웹 페이지를 볼 경우 보안 기능 우회가 허용될 수 있습니다. 웹 검색을 통한 공격의 경우, 이 취약점 악용에 성공한 공격자는 다양한 취약점 클래스로부터 사용자를 보호해 주는 ASLR(Address Space Layout Randomization) 보안 기능을 우회할 수 있습니다. 보안 기능을 우회하는 것만으로는 임의의 코드 실행이 허용되지 않지만 공격자는 이 ASLR 우회 취약점을 다른 취약점 즉, ASLR 우회를 통해 임의의 코드를 실행할 수 있는 원격 코드 실행 취약점 등과 함께 사용할 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-dec>

영문 : <http://technet.microsoft.com/en-us/security/bulletin/ms13-dec>

• 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

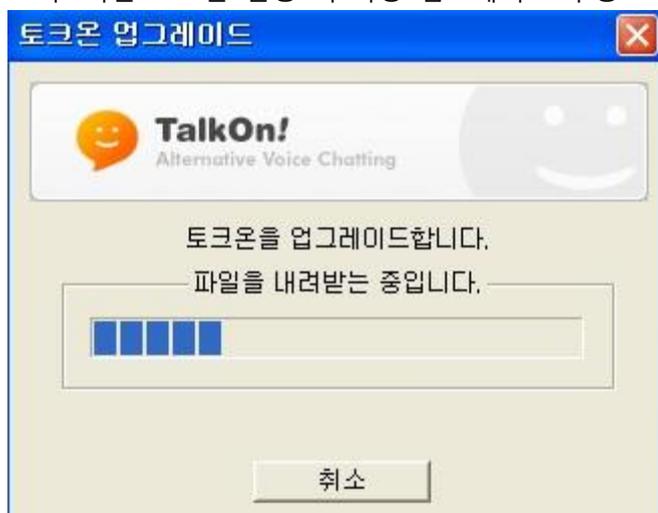
낮은 버전의 토크온 사용자는 악성코드 감염으로 인한 정보유출, 시스템 파괴 등의 피해를 입을 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

<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, 악성 코드에 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, 웹 페이지 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) : 엘더스社 와 마이크로소프트社가 공동 개발한 래스터 화상 파일 형식

<해결방법>

- 취약점으로 인한 위협을 경감시키기 위해 다음의 조치를 취할 수 있음
- 마이크로소프트社에서 제공하는 Fix it 51004(좌측 아이콘)를 다운로드 후 실행



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 열람 할 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>

## • Adobe 12 월 정기 보안 업데이트 권고

Adobe社는 Adobe Flash Player 및 Shockwave Player에 영향을 주는 취약점을 해결한 보안 업데이트를 발표

낮은 버전 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

Adobe Flash Player에서 발생하는 2개의 취약점을 해결하는 보안 업데이트를 발표

- 임의코드 실행으로 이어질 수 있는 타입 컨퓨전(Type Confusion) 취약점(CVE-2013-5331)
- 임의코드 실행으로 이어질 수 있는 메모리 손상 취약점(CVE-2013-5332)

Adobe Shockwave Player에서 발생하는 2개의 취약점을 해결하는 보안 업데이트를 발표

- 임의코드 실행으로 이어질 수 있는 메모리 손상 취약점(CVE-2013-5333, CVE-2013-5334)

### <해당제품>

- Adobe Flash Player(윈도우즈 및 맥) 11.9.900.152 및 이전버전
- Adobe Flash Player(리눅스) 11.2.202.327 및 이전버전
- Adobe AIR(윈도우즈 및 맥) 3.9.0.1210 및 이전버전
- Adobe AIR(안드로이드) 3.9.0.1210 및 이전버전
- Adobe AIR SDK 3.9.0.1210 및 이전버전
- Adobe AIR SDK&Compiler 3.9.0.1210 및 이전버전
- Adobe Shockwave Player(윈도우즈 및 맥) 12.0.6.147 및 이전버전

### <해결방법>

**윈도우, 맥, 리눅스 환경의 Adobe Flash Player 사용자**

- Adobe Flash Player Download Center(<http://get.adobe.com/kr/flashplayer/>)에 방문하여 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드

**윈도우, 맥 환경의 Adobe AIR 사용자**

- Adobe AIR Download Center(<http://get.adobe.com/kr/air/>)에 방문하여 Adobe AIR 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드

#### **안드로이드 환경의 Adobe AIR 사용자**

- Adobe AIR가 설치된 안드로이드 폰에서 '구글 플레이 스토어' 접속 → 메뉴 선택 → 내 애플리케이션 선택 →  
Adobe AIR 안드로이드 최신 버전으로 업데이트 하거나 자동업데이트를 허용하여 업그레이드

#### **Adobe AIR SDK 사용자**

- <http://www.adobe.com/devnet/air/air-sdk-download.html> 에 방문하여 Adobe AIR SDK 최신 버전을 설치

#### **윈도우, 맥 환경의 Adobe Shockwave Player 사용자**

- Adobe Download Center(<http://get.adobe.com/shockwave/>)에 방문하여 최신 버전을 설치하거나 자동 업데이트를 이용하여 업그레이드

#### **<참고사이트>**

<http://helpx.adobe.com/security/products/flash-player/apsb13-28.html>

<http://helpx.adobe.com/security/products/shockwave/apsb13-29.html>

Contact us...

**(주)이스트소프트 알약대응팀**

Tel : 02-3470-2999

E-mail : [help@alyac.co.kr](mailto:help@alyac.co.kr)

알약 홈페이지 : [www.alyac.co.kr](http://www.alyac.co.kr)