알약
월간 보안동향
보고서.

2015년 3월

알약 3월 보안동향보고서

CONTENTS

2월의 총평

2월에는 국내/해외 가릴 것 없이 다양한 보안이슈가 발생했습니다.

먼저 국내에서는 감염된 시스템의 DNS를 변경하여 사용자를 파밍 홈페이지로 유도하는 악성코드 및 변종들이 많이 유포되었습니다. DNS 변경 악성코드가 일으키는 가장 큰 문제는 백신이 정상적으로 해당 악성코드를 탐지하고 삭제하면 인터넷 연결이 불가능하게 되는 것이었습니다. 이는 악성코드 자체가 감염시스템의 DNS를 로컬호스트로 변경시킨 후 DNS의 역할을 수행했기 때문입니다. 이에 따라 알약에서도 DNS 변경 악성코드와 변종들을 치료하고 감염된 시스템의 DNS 설정을 정상적으로 되돌릴 수 있는 전용백신을 제작하여 사용자들에게 제공한 바 있습니다.

해외에서 발생한 보안이슈 중, 가장 이슈가 되었던 것은 레노버 PC 내에 '슈퍼피시(Superfish)라고 불리는 애드웨어가 탑재되었던 것입니다. 슈퍼피시는 광고를 띄우는 애드웨어 프로그램입니다. PC 제조사인 레노버가 이러한 프로그램을 선 탑재하여 배포한 것 자체도 큰 논란이 되었지만, 더욱 큰 문제는 슈퍼피시가 광고를 띄우기 위해 사용한 방법이었습니다. 만약 공격자가 슈퍼피시를 악용한다면 사용자가 주고받는 데이터를 모두 훔쳐볼 수 있습니다. 슈퍼피시를 탑재했던 레노버도 이 사실에 대해 사용자들에게 사과하고 삭제방법을 안내하였습니다. 또한 슈퍼피시와 같은 애드웨어를 자사제품에 선 탑재하지 않겠다고 약속했습니다.

이 외에도 실제 개최 예정인 행사의 공고내용을 가지고 국내 특정 기업 및 기관을 상대로 한 표적 해킹 공격이 발견되는 등 많은 보안 이슈가 발생한 달이었습니다. 이런 때일수록 조금 귀찮더라도 소중한 나의 개인정보와 재산을 보호한다는 생각을 가지고, 스스로 보안에 좀 더 관심을 기울여야 합니다. 지금이야말로 실천 가능한 보안수칙을 다시 한 번 떠올릴 때입니다.

Part1. 2월의 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.

2015년 2월의 감염 악성코드 Top 15 리스트에서는 3개월 연속으로 Misc.Suspicious.NTZ가 1위를 차지했다. 이번 달에 새롭게 2위를 차지한 Adware.Kraddare.295936는 사용자가 Internet Explorer를 실행할 경우, 사용자가 동의하지 않은 다양한 형태의 광고 모듈을 띄우는 애드웨어이다. 이 애드웨어는 광고창을 팝업시키고 특정사이트 바로가기 아이콘을 생성한다.

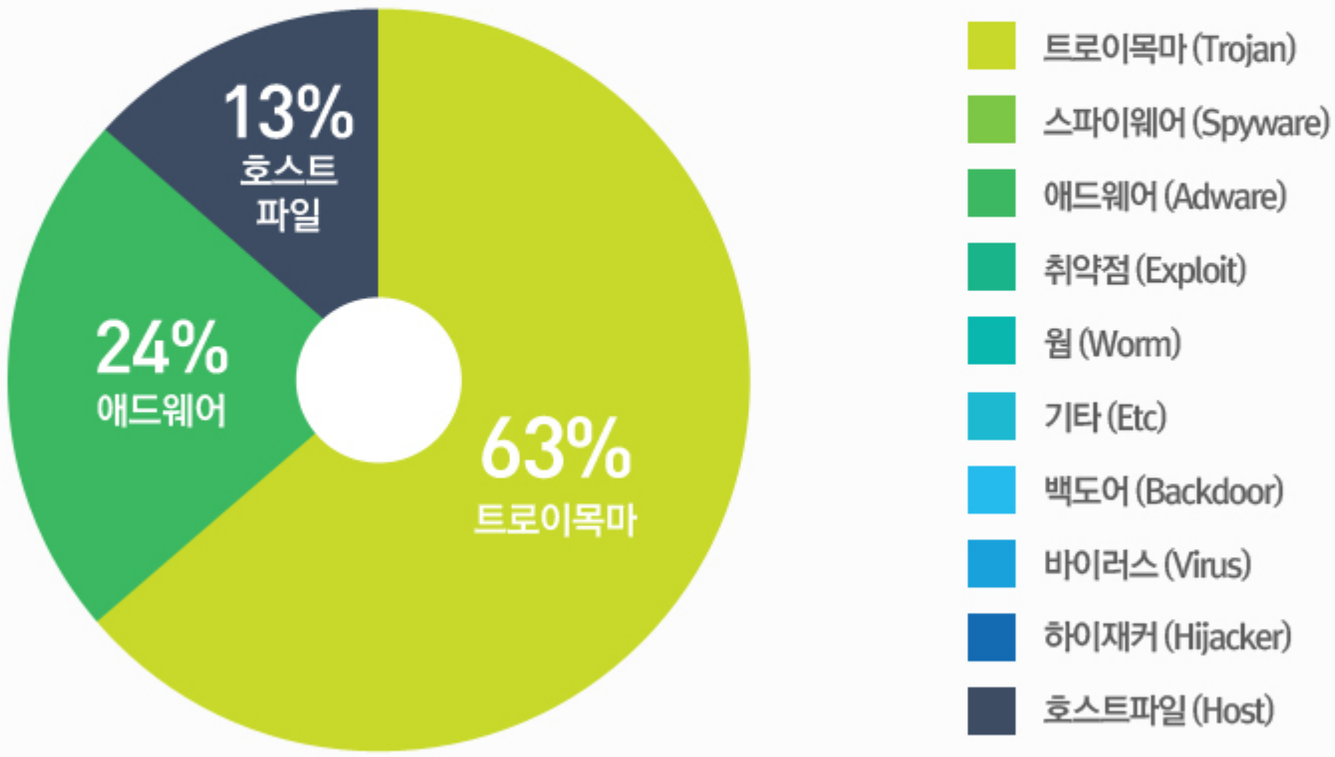
순위	등락	악성코드 진단명	카테고리	합계(감염자수)
1	-	Misc.Suspicious.NTZ	Trojan	5655
2	↑7	Adware.Kraddare.295936	Adware	1433
3	↓1	Misc.Suspicious.KCP	Trojan	1248
4	NEW	Trojan.Generic.12793744	Trojan	1046
5	↑1	Misc.Keygen	Trojan	1036
6	↓2	Trojan.Dropper.KRBanker.Agent	Trojan	843
7	NEW	Gen:Variant.Adware.Graftor.175958	Adware	777
8	-	Adware.SearchSuite	Adware	622
9	NEW	Adware.Kraddare.FJ	Adware	596
10	NEW	Misc.Agent.126672	Trojan	580
11	↑1	Hosts.www.nate.com	Host	568
12	↓2	Hosts.www.nonghyup.com	Host	545
13	NEW	Hosts.kfcc.co.kr	Host	536
14	↑1	Hosts.www.keb.co.kr	Host	536
15	↓2	Gen:Variant.Adware.Graftor.140285	Adware	535

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2015년 02월 01일 ~ 2015년 02월 28일

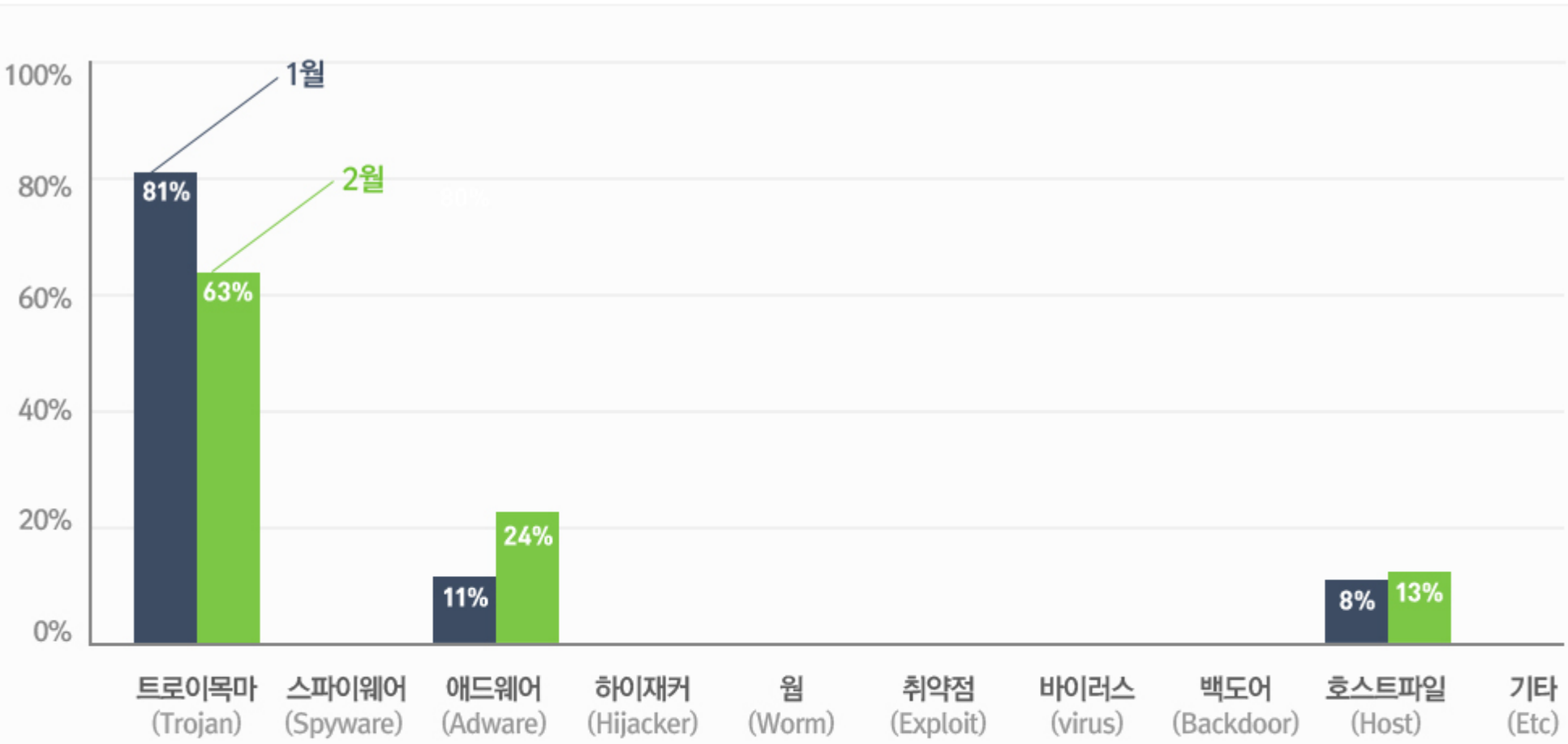
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 63%를 차지했으며, 애드웨어(Adware) 유형이 24%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

2월에는 지난 1월과 비교하여 트로이목마(Trojan) 유형 악성코드 비율이 소폭 감소하였고, 애드웨어(Adware) 유형의 악성코드의 비중이 크게 증가하였다.

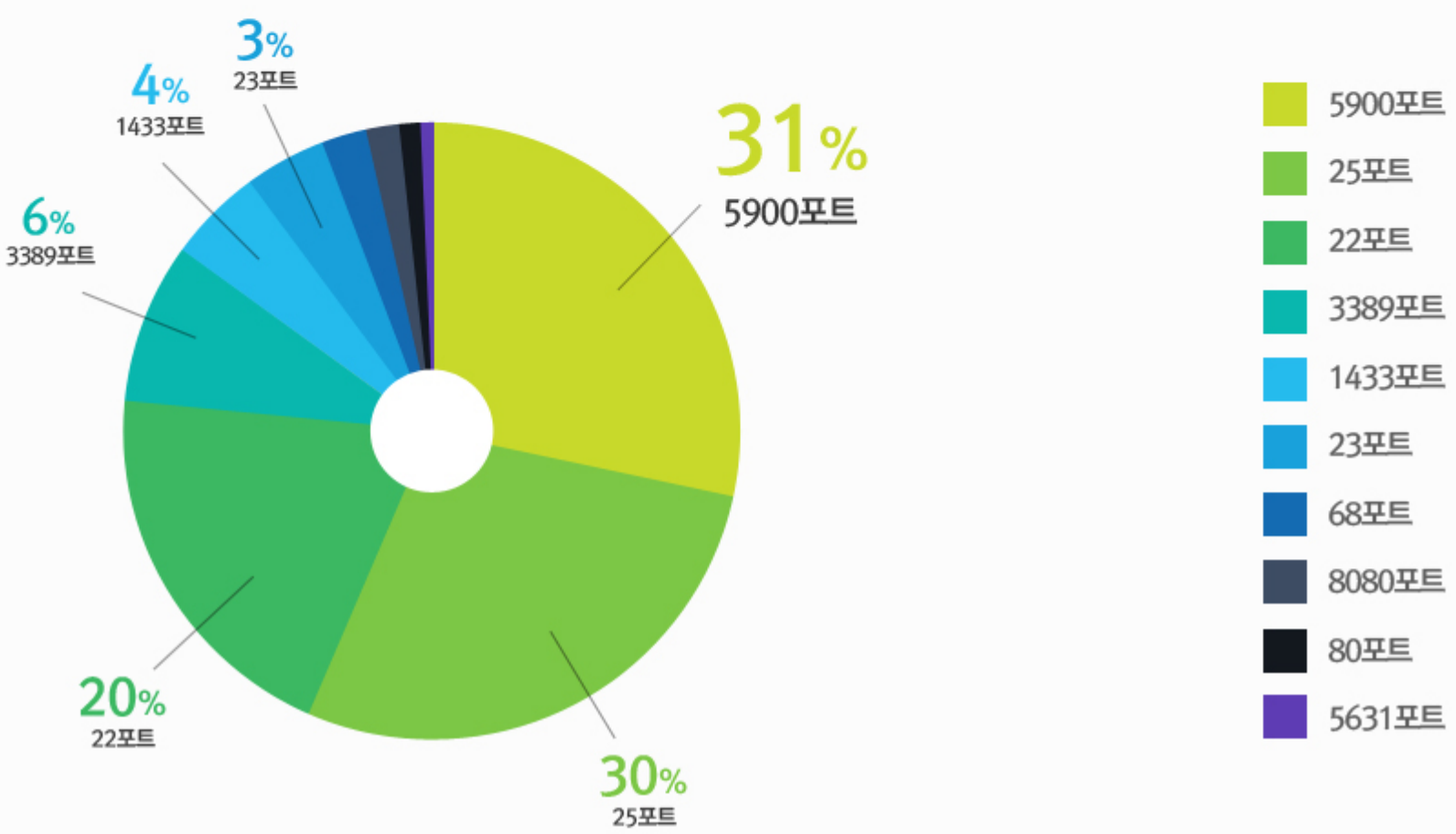


* 악성코드 카테고리 분류 방식이 일부 변경되어, 기존에 기타로 분류되었던 악성코드들이 1월부터 '트로이목마' 카테고리에 포함됨

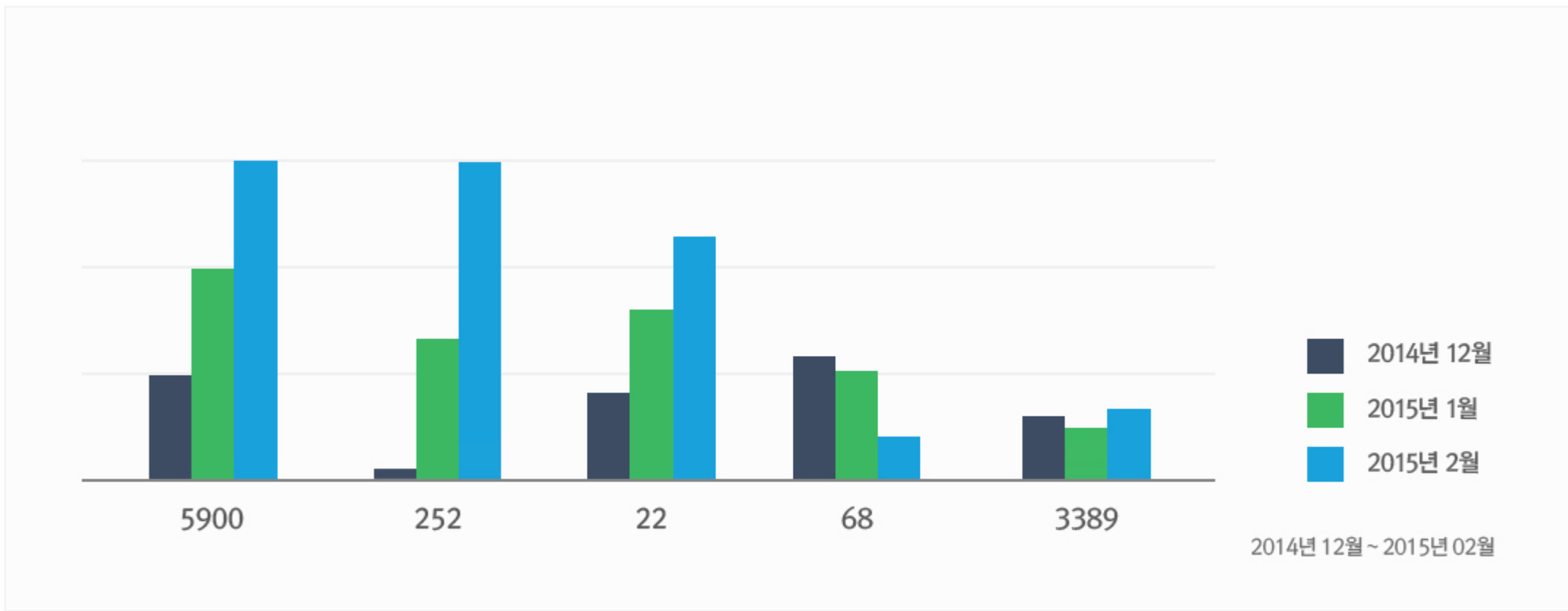
2.허니팟/트래픽 분석

2월의 상위 Top 10 포트

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

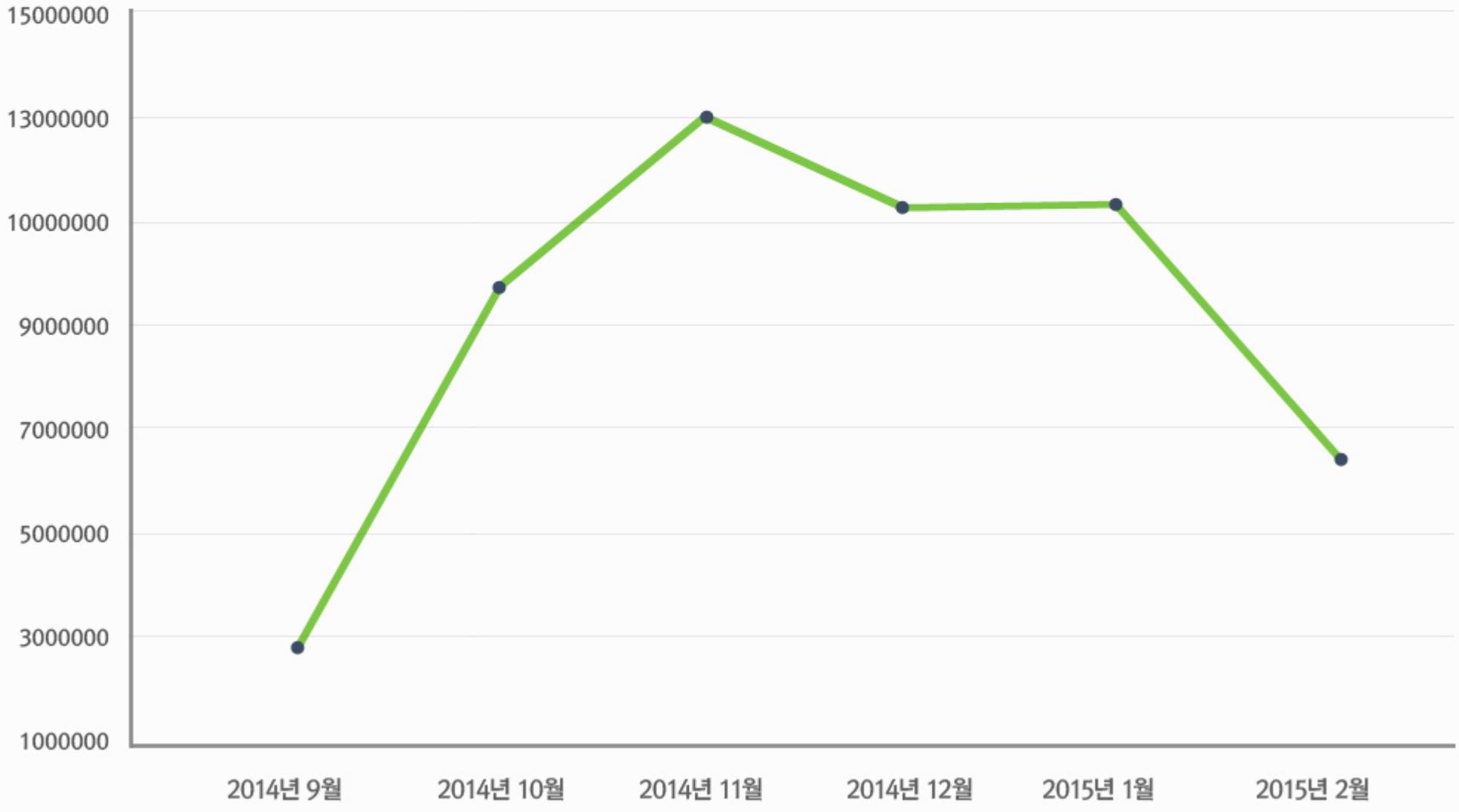


최근 3개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속시도가 감지된 수치



단위 : 악의적 트래픽 접속시도 감지 건수

2014년 09월 ~ 2015년 02월

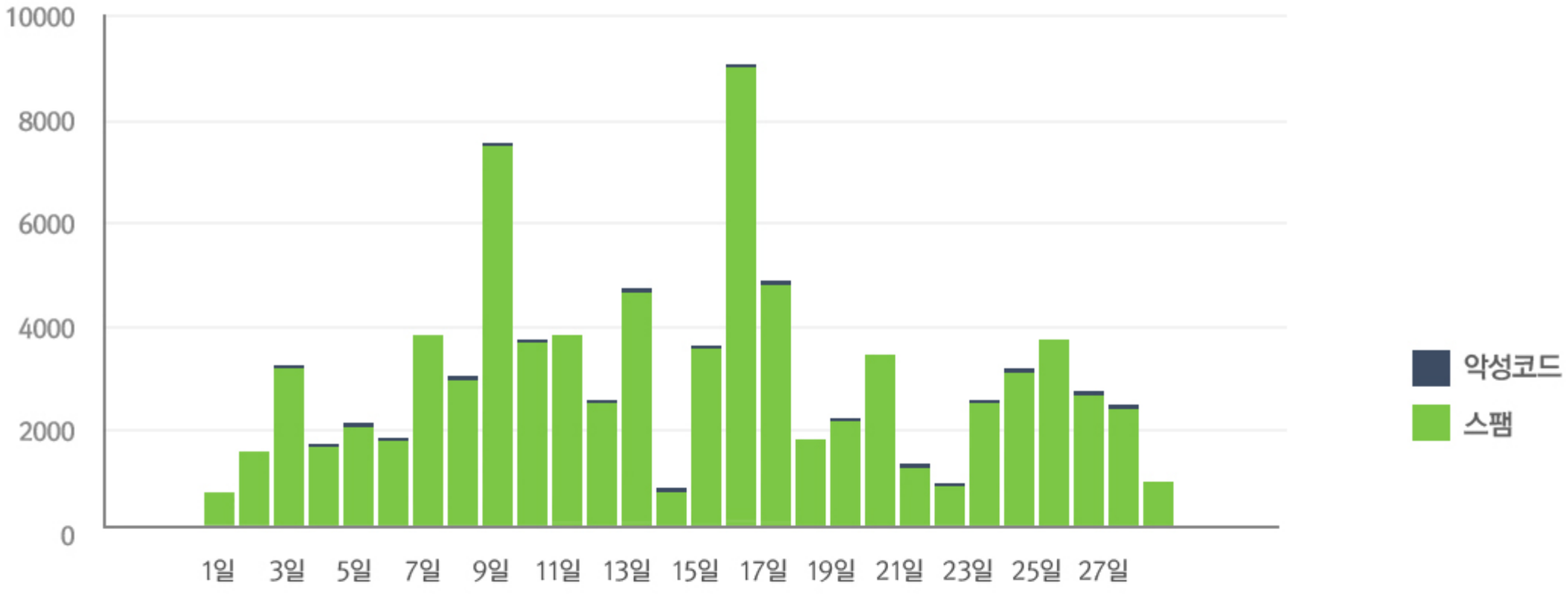
3. 스팸메일 및 악성코드가 포함된 메일 분석

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. 2015년 2월의 경우, 2015년 1월에 비해 스팸메일 유입 수치는 약 2배가량 감소하였으나, 메일에 첨부된 악성코드 수치는 2배 정도 증가하였다.

2월에 가장 많이 발견된 스팸메일 악성코드는 Win32/Upatre.AW이다.
해당 악성코드는 트로이목마계열의 악성코드로 사용자 모르게 악성코드를 포함한 추가적인 다른 프로그램을 사용자 시스템에 설치(드롭)한다. 일단 이렇게 드롭된 악성코드는 사용자 시스템에서 백도어 역할을 하며, 공격자가 원격으로 사용자 시스템을 마음껏 드나들거나 컨트롤할 수 있게 한다.

최근 활발한 스피어 피싱 공격도 위와 같이 이메일에 첨부된 악성코드를 활용하는 경우가 많으므로 주의가 필요하다.



4. 스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2015년 02월 01일 ~ 2015년 02월 28일
총 신고 건수	10,835건

키워드별 신고 내역

키워드	신고 건수	비율
결혼	5336	49.25%
훈련	154	1.42%
택배	127	1.17%
결제	103	0.95%
보험	85	0.78%
배송	79	0.73%
선물	76	0.70%
교육	49	0.45%
돌잔치	39	0.36%
민사소송	31	0.29%

스미싱 신고추이

지난달 스미싱 신고 건수 12,916건 대비 이번 달 10,835건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 2,081건 감소했다. 1월과 마찬가지로 2월에도 결혼 관련 스미싱이 지속적으로 증가했다.

알약이 뽑은 2월 주목할만한 스미싱

특이문자

순위	문자내용
1	고객님의 카드미납연체로 신용불량 처리되였습니다. 확인
2	연예계 숨겨진 사건 이야기들 증권가 찌라시
3	이준상님[알약]무료체험

다수문자

순위	문자내용
1	(축f하♬해e주)세요.^^
2	후)향작 집결장소 및 시간확인후 꼭! 참석하세요
3	(주)고객님의 택배가 이미발송되었습니다.전자영수정확인하세요
4	55000원 결제완료/익월 요금합산청구/잔액확인
5	이번달 보험료 미납요금청구서!

Part2. 2월의 악성코드 이슈 분석

개요

악성코드 분석

- APK 분석
- 설치 및 코드 흐름
- 코드 상세분석

결론

Spyware.Android.PowerOffHijack

1. 개요

Poweroffhijack은 중국에서 발견된 악성 앱으로 중국 안드로이드폰 사용자를 대상으로 동작하는 악성앱이다. 이 악성앱의 특징은 사용자가 스마트폰의 전원을 차단해도 악성앱이 동작하여 지속적으로 사용자의 정보를 수집하는 행위를 한다는 것이다. 최초로 발견된 것은 2014년 11월경으로, 중국에서 발견되었다. Power-offhijack 악성앱은 기기의 power 상태 변화를 감시한다. reboot이나 shut-down등의 요청 시 화면만 검은색으로 바꾸어 기기의 전원이 off 상태인 것처럼 위장하여 사용자를 속이는 행위를 한다. 이후 사용자의 개인 정보를 지속적으로 탈취한다.

초기의 Poweroffhijack은 몇 가지 제약이 있어 중국 이외의 국가에서는 발견되지 않았다. 그 첫 번째 이유는 중국에서 사용되는 기기에만 존재하는 데이터나 프로세스를 활용하는 코드의 사용으로 다른 지역에서는 설치된다 해도 제대로 동작하기 어렵기 때문이다. 두 번째 이유로는 사용자 기기가 루팅 상태여야만 전원관리 코드를 훅하여 전원 관리 상태를 공격자의 의도대로 변경할 수 있기 때문이다.

본 분석 보고서의 대상 샘플은 기존 Poweroffhijack의 변종으로 시스템에 의존적인 코드가 제거되어 있다. 따라서 지역과 기기의 루팅 여부와 상관없이 스파이 행위를 하도록 코드가 변경된 것으로 판단된다.

2. 악성코드 분석

APK 분석

파일정보

A. 파일 이름 : 14D9F1A92DD984D6040CC41ED06E273E.apk
B. MD5 : 14D9F1A92DD984D6040CC41ED06E273E
C. 패키지 명 : com.google.progress
D. 주요 사용 퍼미션

Permission	내용
RECEIVE_SMS	앱이 SMS 메시지를 수신하고 처리할 수 있도록 허용한다. 이는 앱이 사용자에게 표시하지 않고 기기로 전송된 메시지를 모니터링 또는 삭제할 수도 있다는 것을 의미한다.
SEND_SMS	앱이 SMS 메시지를 보낼 수 있도록 허용한다. 이 경우, 악성 앱이 사용자의 확인 없이 메시지를 전송해 요금이 부과될 수 있으므로 예상치 못한 통화 요금이 부과될 수 있다.
WRITE_SMS	앱이 태블릿 또는 SIM 카드에 저장된 SMS 메시지에 쓸 수 있도록 허용한다. 이 경우 악성 앱이 이 기능을 이용하여 메시지를 삭제할 수 있다.
READ_CONTACTS	특정인과 전화, 이메일 또는 기타 수단으로 연락한 빈도를 포함하여 사용자 태블릿에 저장된 연락처에 대한 데이터를 앱이 읽도록 허용한다. 이 권한을 사용하면 앱이 연락처 데이터를 저장할 수 있으며, 악성 앱이 사용자 모르게 연락처 데이터를 공유할 수도 있다.
CALL_PHONE	앱이 사용자의 조작 없이 전화번호로 전화를 걸 수 있도록 허용한다. 이 경우 예상치 못한 통화 요금이 부과될 수 있다. 앱이 비상 전화를 걸도록 하는 권한은 주어지지 않으나, 사용자의 확인 없이 전화를 걸어 요금이 부과될 수 있습니다.
PROCESS _OUTGOING_CALLS	통화를 다른 번호로 리디렉션하거나 통화를 완전히 중단하는 옵션을 사용하여, 앱에서 발신 통화 중에 전화를 거는 번호를 볼 수 있게 허용한다.
WRITE_CALL_LOG	앱에서 수신 및 발신 통화 데이터를 포함하여 태블릿의 통화 기록을 수정할 수 있도록 허용한다. 이 경우 악성 앱이 통화 기록을 지우거나 수정할 수 있다.
ACCESS_FINE _LOCATION	앱에서 GPS 또는 기지국 및 Wi-Fi와 같은 네트워크 위치 제공자를 사용하는 위치 서비스를 통해 내 정확한 위치를 알 수 있도록 한다. 앱에서 이를 사용하도록 하려면 기기에서 위치 서비스를 사용하도록 설정해야 한다. 위치 서비스를 사용하면 앱에서 내 위치를 파악할 수 있으나, 배터리 소모량이 증가할 수 있다.
RECEIVE_BOOT _COMPLETED	앱이 시스템 부팅이 끝난 후 바로 시작할 수 있도록 허용한다. 이 경우 앱이 항상 실행되어 전체 태블릿 속도가 느려질 수 있다.
RECORD_AUDIO	앱이 마이크로 오디오를 녹음할 수 있도록 허용한다. 이 권한을 사용하면 앱이 사용자의 확인 없이 언제든지 오디오를 녹음할 수 있다.

[표 1] 앱이 사용하는 주요 권한

행위

앱은 다음의 행위들을 수행하는 코드를 가지고 있다.

A. 오디오 녹음
   발신 통화 녹음, 사용자 도청

B. 문자 목록 가져오기
   사용자 문자 메시지 수집

C. 네트워크 정보 가져오기
   사용자 기기를 항상 네트워크를 사용할 수 있는 환경으로 유지

D. GPS로 위치 확인
   사용자 위치 파악

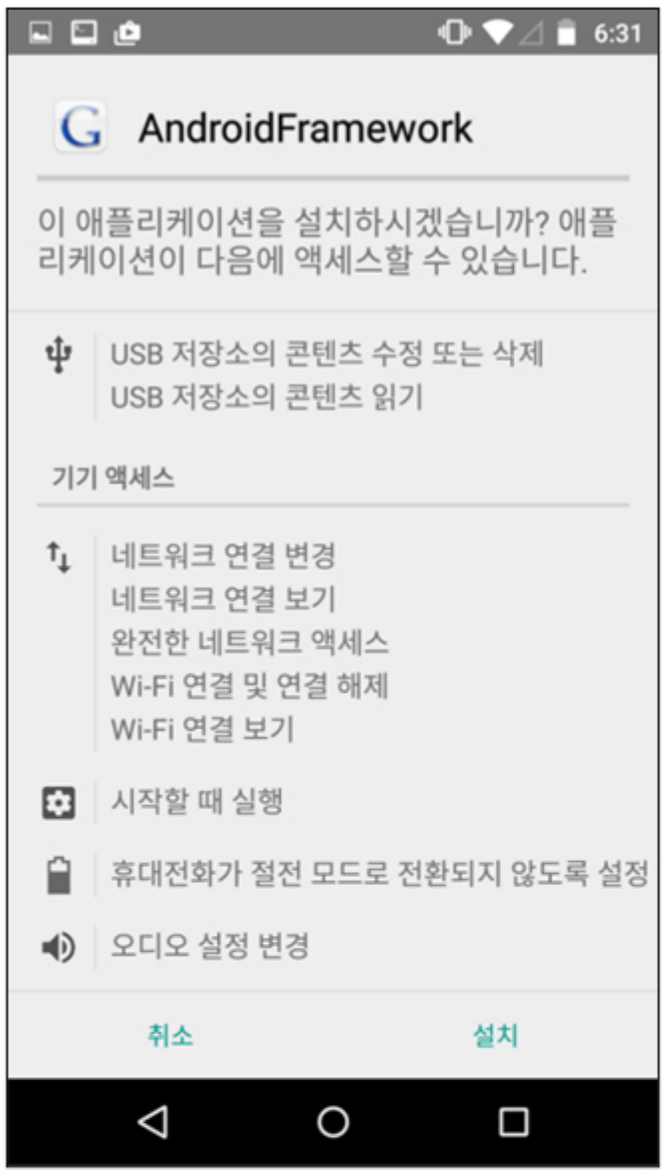
E. 통화 내역 가져오기
   사용자 통화 내역 수집

F. 연락처 목록 가져오기
   기기에 저장된 연락처 정보 수집. 이름, 이메일, 전화번호 수집

– 설치 및 코드 흐름

설치

앱의 다운로드가 완료되어 사용자가 설치를 시작하면 다음과 같은 화면을 마주하게 된다.

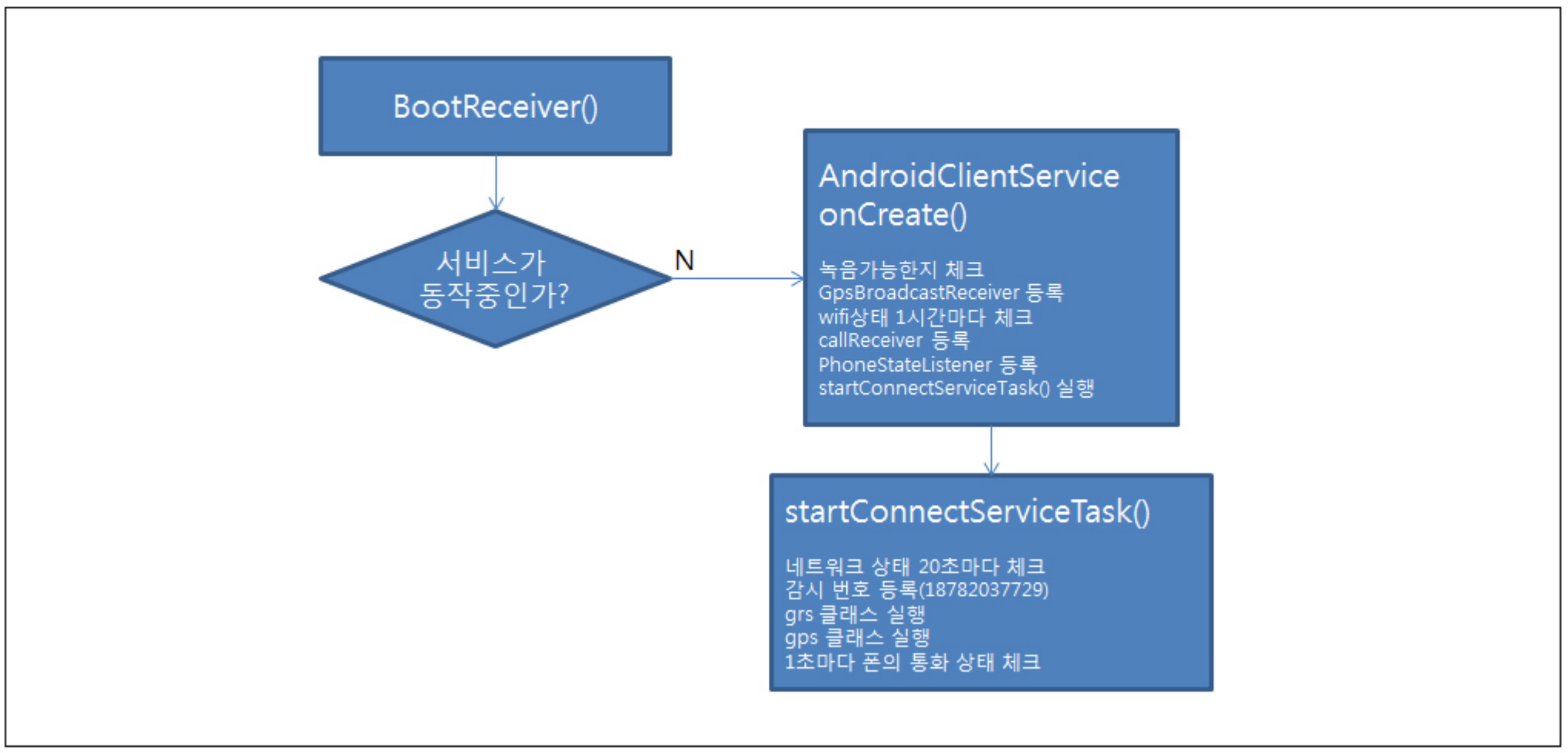


[그림 1] 악성앱 설치 화면

설치가 완료되면 앱의 최초 실행인 열기 버튼이 비활성화되어 있는 상태이기 때문에 앱을 실행 할 수 없다.
이후 악성앱에 대한 흔적은 실행 프로세스 목록 등에서 확인할 수 있다.

코드 흐름도

다음 [그림 2]는 앱이 설치되어 최초로 실행될 때의 코드 흐름이다. 각 클래스별로 역할이 나뉘어져 있으며, 대부분의 코드는 사용자 기기의 상태를 점검하여 정보 수집 및 탈취를 위한 환경을 설정한다.



[그림 2] 최초 실행 코드 흐름도

초기 실행 코드에서는 다음과 같은 부분을 체크하고 있다.

- 오디오 및 마이크 상태
- GPS 상태
- Wifi 상태
- 공격자 번호 등록 (그림 2에서는 감시 번호)

[그림 2]에서 감시 번호 등록은 공격자의 전화번호를 의미한다. 이는 공격자의 스마트폰에서 피해자에게 직접 공격 명령을 내릴 수 있다는 뜻이다. 공격은 도청에 한하여 수행되는 것으로 기존의 악성앱들과는 확연히 다른 공격 방법을 사용하고 있다.

[그림 2]의 주요 클래스에 대해 살펴 보자.

- BootReceiver

이 클래스는 엔트리 포인트로 BOOT_COMPLETED, SMS_RECEIVED, NEW_OUTGOING_CALL, SCREEN_OFF, PACKAGE_INSTALL의 리시버 코드가 있다. 최초 실행 코드는 자신의 설치 여부를 확인하는 “PACKAGE_INSTALL” 메시지를 리시브 하여 AndroidcliendService를 시작시킨다.

- AndroidClientService

서비스로 동작하며 백그라운드에서 사용자 기기의 상태를 감시한다. 감시 행위는 다음과 같다.

- 전화 수신, 발신 감시
- Gps 위치 수집 및 전송
- 공격자 서버와 연결 유지
- 공격자 명령 수행
- 네트워크 상태 체크

[그림 3]은 전화 상태 변경 시 동작하는 코드 흐름이다. 상태는 3가지로 나뉘며, 상태마다 수행하는 동작은 [그림 3]과 같다.

전화 상태

- CALL_STATE_RINGING

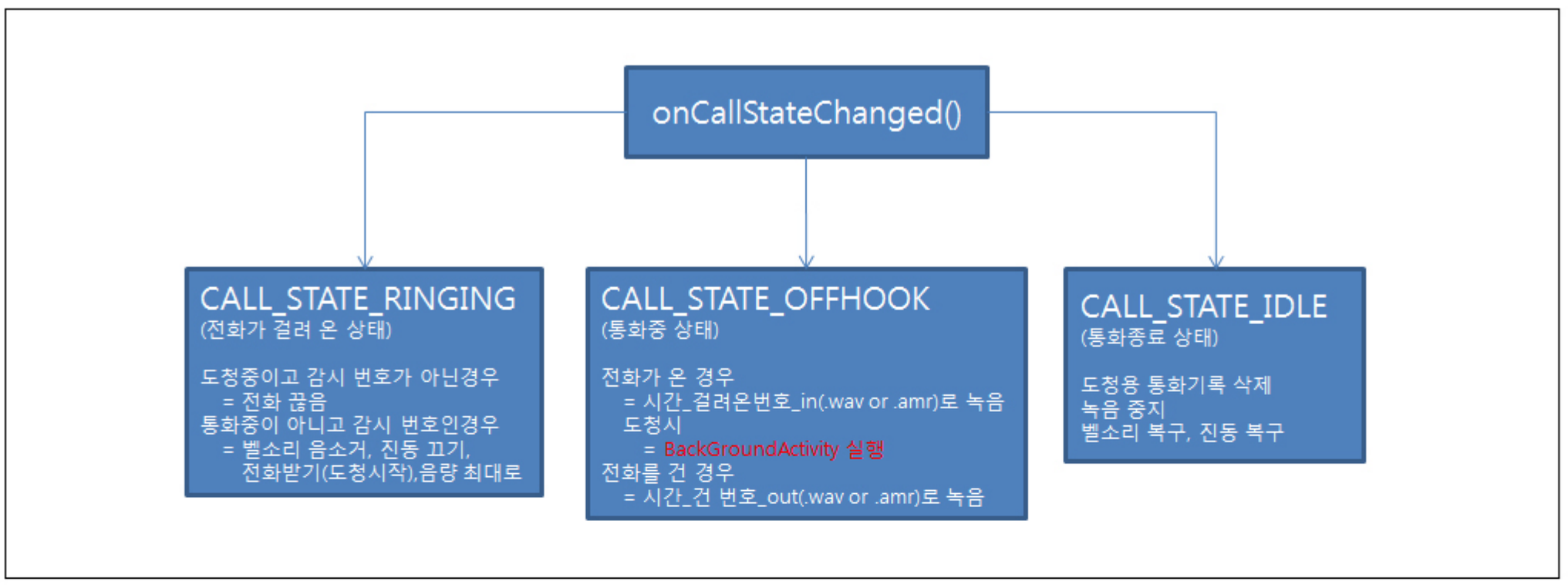
전화벨이 울리는 상태로 2가지 경우로 상태를 분류할 수 있다.
1. 현재 공격자에 의해 도청이 이루어지고 있는 상태에서 벨이 울리는 경우, 발신번호가 공격자의 번호가 아니면 전화를 끊는다.
2. 도청 상태가 아닌 상태에서 벨이 울리는 경우, 발신 번호가 공격자의 번호라면 벨소리와 진동 등을 없애고 전화를 받는다.

- CALL_STATE_OFFHOOK

통화 중인 상태이다. 이 경우에도 2가지 상태로 분류된다. 첫 번째는 전화가 온 경우(수신 전화)로, 발신 번호가 공격자의 번호라면 도청을 수행하기 위해 BackGroundActivity를 시작시킨다. 만일 공격자가 아니라면 통화 녹취를 수행한다. 두 번째는 전화를 건 경우(발신 전화)로 통화 녹취를 시작한다.

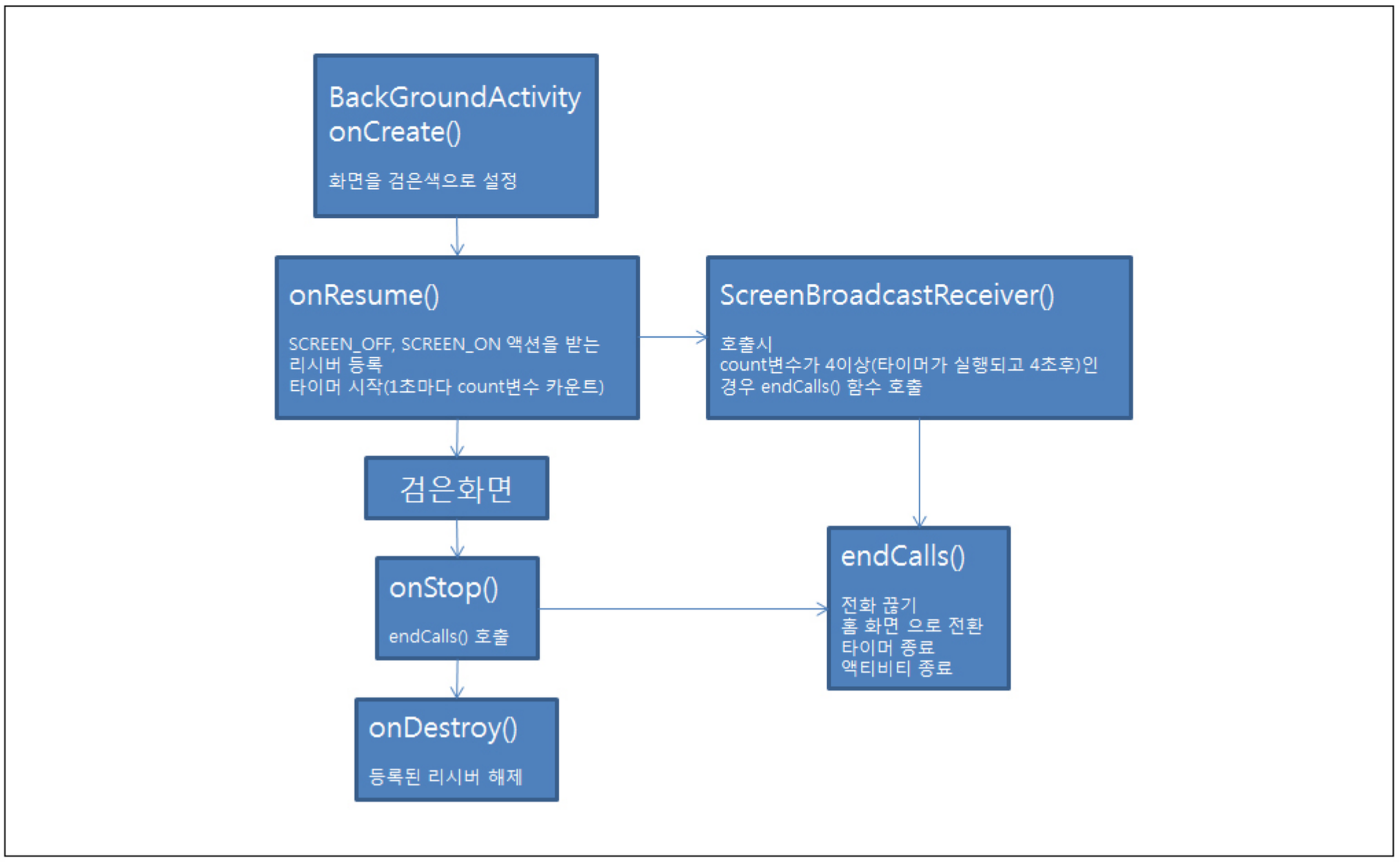
- CALL_STATE_IDLE

통화가 종료되는 상태로 도청 중이라면 도청을 중지한다. 통화 중인 경우에는 통화 녹취를 중지한다.



[그림 3] 전화 상태 변경 시 코드 흐름도

[그림 4]는 도청 공격 시 동작하는 코드 흐름이다. 이 코드는 공격자가 사용자의 스마트폰으로 전화를 거는 것을 신호로 동작한다. 공격자의 번호로 전화가 오면 코드는 화면을 검은색으로 바꾼다. 이후 스크린 On/Off 리시버를 등록하여 도청을 수행하고, 도청이 끝나면 전화를 끊고 홈 화면으로 이동한다.



[그림 4] 공격자가 사용자 폰 도청 시 수행 되는 코드

[그림 5]는 BakcGroundActivity가 실행되면 최초로 수행되는 코드이다. 단지 화면을 검게 만드는 코드만 존재한다.

```
protected void onCreate(Bundle paramBundle)
{
  super.onCreate(paramBundle);
  LinearLayout localLinearLayout = new LinearLayout(this);
  localLinearLayout.setBackgroundColor(-16777216);
  getWindow().setFlags(128, 128);
  setContentView(localLinearLayout);
}
```

[그림 5] BackGroundActivity의 진입 코드

– 코드 상세분석

각 클래스 별로 코드 상세 분석을 수행하였다.

부트 리시버

앱 실행 시 최초 실행 코드이며, 주요 동작은 AndroidClientService의 구동이다.

```
public void onReceive(Context paramContext, Intent paramIntent)
{
  this.context = paramContext;
  String str = paramIntent.getAction();
  System.out.println("接收到广播---->" + str);
  if ((str.equals("android.intent.action.BOOT_COMPLETED")) || (str.equals("android.provider.Telephony.SMS_RECEIVED")) ||
  {
    if (!isServiceRunning())
    {
      Log.e("service", "服□未存□□□,即□□□服□");
      Intent localIntent = new Intent(paramContext, AndroidClientService.class);
      localIntent.setAction("com.google.ACTION_START_CALL_RECORD");
      paramContext.startService(localIntent);
    }
  }
  else {
    return;
  }
  Log.e("service", "服□正在□行");
}
```

[그림 6] BootReceiver 코드

스크린 On/Off 리시버

화면 on/off 상태를 감시하기 위해 다음의 리시버를 등록한다. 화면상태 변경 감지 시, 도청을 중지시킨다.

```
public void registerScreenOffBroadcastReceiver()
{
  this.receiver = new ScreenBroadcastReceiver();
  IntentFilter localIntentFilter = new IntentFilter();
  localIntentFilter.addAction("android.intent.action.SCREEN_OFF");
  localIntentFilter.addAction("android.intent.action.SCREEN_ON");
  registerReceiver(this.receiver, localIntentFilter);
}

public void startTimer()
{
  this.timer = new Timer();
  this.task = new TimerTask()
  {
    public void run()
    {
      BackGroundActivity localBackGroundActivity = BackGroundActivity.this;
      localBackGroundActivity.count = (1 + localBackGroundActivity.count);
    }
  };
  this.timer.schedule(this.task, 0L, 1000L);
}

public class ScreenBroadcastReceiver
  extends BroadcastReceiver
{
  public ScreenBroadcastReceiver() {}

  public void onReceive(Context paramContext, Intent paramIntent)
  {
    if (BackGroundActivity.this.count > 3)
    {
      System.out.println("count----->" + BackGroundActivity.this.count);
      BackGroundActivity.this.endCalls();
      Log.e("call", "挂□□□----->ScreenOffBroadcastReceiver");
    }
  }
}
```

[그림 7] ScreenBroadcastReceiver

와이파이 상태 및 GPRS 상태 확인

다음 코드는 와이파이 상태 및 GPRS의 상태를 확인하는 코드이다.

```
public void run()
{
  this.hasGprs = false;
  try
  {
    begin();
    if (!checkWifiNetworkState())
    {
      if (checkGPRSNetworkState()) {
        break label188;
      }
      Log.e("wifi", "手机目前□有□□,即□□□GPRS□□");
      if (!this.hasGprs) {}
    }
    else
    {
      return;
    }
  }
```

[그림 8] 네트워크 상태 체크

문자 가져오기

사용자의 문자를 수집하는 코드이다.

```
public String readSMSList()
{
  ContentResolver localContentResolver = this.context.getContentResolver();
  Cursor localCursor1 = localContentResolver.query(this.URI_SMS_INBOX, this.PROJECTION, null, null, "thread_id asc");
  Log.i("***", "<------sms------>");
  if ((localCursor1 != null) && (localCursor1.getCount() > 0))
  {
    Log.i("***", "sms cursor--->" + localCursor1.getCount());
    StringBuilder localStringBuilder = new StringBuilder();
    String str;
    if (localCursor1.moveToFirst())
    {
      localStringBuilder.append(localCursor1.getString(0) + " ");
      str = localCursor1.getString(1);
      if (str == null) {
        break label394;
      }
      if (str.startsWith("+86")) {
        str = str.substring(3);
      }
      localStringBuilder.append(str + " ");
      Cursor localCursor2 = localContentResolver.query(Uri.withAppendedPath(Contacts.People.CONTENT_FILTER_URI, str), new String[]
      if ((localCursor2 == null) || (!localCursor2.moveToFirst())) {
        break label383;
      }
      localStringBuilder.append(localCursor2.getString(localCursor2.getColumnIndex("display_name")) + " ");
```

[그림 9] 사용자의 SMS 문자 수집 코드

위치 확인

GPS 좌표 데이터를 활용하여 사용자의 현 위치를 파악하는 코드이다.

```
public String getLocation()
{
  localStringBuffer1 = new StringBuffer();
  try
  {
    this.gsm = ((GsmCellLocation)this.telManager.getCellLocation());
    int i = this.gsm.getCid();
    int j = this.gsm.getLac();
    String str1 = this.telManager.getNetworkOperator();
    int k = Integer.valueOf(str1.substring(0, 3)).intValue();
    int m = Integer.valueOf(str1.substring(3, 5)).intValue();
    JSONObject localJSONObject1 = new JSONObject();
    localJSONObject1.put("version", "1.1.0");
    localJSONObject1.put("host", "maps.google.com");
    localJSONObject1.put("request_address", true);
    JSONArray localJSONArray = new JSONArray();
    JSONObject localJSONObject2 = new JSONObject();
    localJSONObject2.put("cell_id", i);
    localJSONObject2.put("location_area_code", j);
    localJSONObject2.put("mobile_country_code", k);
    localJSONObject2.put("mobile_network_code", m);
    localJSONArray.put(localJSONObject2);
    localJSONObject1.put("cell_towers", localJSONArray);
    DefaultHttpClient localDefaultHttpClient = new DefaultHttpClient();
    HttpPost localHttpPost = new HttpPost("http://www.google.com/loc/json");
    StringEntity localStringEntity = new StringEntity(localJSONObject1.toString());
    localHttpPost.setEntity(localStringEntity);
    HttpResponse localHttpResponse = localDefaultHttpClient.execute(localHttpPost);
    System.out.println("GPS□取□□度得到□□");
    HttpEntity localHttpEntity = localHttpResponse.getEntity();
    BufferedReader localBufferedReader = new BufferedReader(new InputStreamReader(localHttpEntity.getContent()));
    StringBuffer localStringBuffer2 = new StringBuffer();
    String str4;
    for (Object localObject = localBufferedReader.readLine();; localObject = str4)
    {
      if (localObject == null)
      {
        JSONObject localJSONObject3 = new JSONObject(localStringBuffer2.toString());
        JSONObject localJSONObject4 = new JSONObject(localJSONObject3.getString("location"));
        String str2 = localJSONObject4.getString("latitude");
        String str3 = localJSONObject4.getString("longitude");
        localStringBuffer1.append("□度:" + str2);
        localStringBuffer1.append(" □度:" + str3);
        localStringBuffer1.append(" 位置:" + "(基站)打□地□□看");
        return localStringBuffer1.toString();
      }
      localStringBuffer2.append((String)localObject);
      str4 = localBufferedReader.readLine();
    }
    return localStringBuffer1.toString();
```

[그림 10] GPS 정보와 구글을 통해 현재 위치 수집

통화 내역 수집

통화 기록을 조회하여 내역을 수집하는 코드이다.

```
public String getCallLog()
{
  StringBuffer localStringBuffer = new StringBuffer();
  Cursor localCursor = this.context.getContentResolver().query(CallLog.Calls.CONTENT_URI, new String[] { "date", "name", "number",
  if (localCursor != null)
  {
    int i = 0;
    if (i >= localCursor.getCount()) {
      return localStringBuffer.toString();
    }
    localCursor.moveToPosition(i);
    localStringBuffer.append(new SimpleDateFormat("yyyy-MM-dd HH:mm:ss").format(Long.valueOf(localCursor.getLong(0))));
    localStringBuffer.append(" ");
    label135:
    label200:
    int j;
    String str;
    if (localCursor.getString(1) == null)
    {
      localStringBuffer.append("未命名 ");
      localStringBuffer.append(localCursor.getString(2) + " ");
      switch (localCursor.getInt(3))
      {
      default:
        j = localCursor.getInt(4);
        if (j < 60) {
          str = j + "秒";
        }
        break;
      }
    }
```

[그림 11] 통화 내역 수집 코드

연락처 수집

연락처를 수집하는 코드이다. 수집 대상은 각 연락처의 이름, 이메일, 전화번호이다.

```
private String getEmail(String paramString)
{
  StringBuffer localStringBuffer = new StringBuffer();
  Cursor localCursor = this.cr.query(Contacts.ContactMethods.CONTENT_EMAIL_URI, null, "person=?", new String[] { paramString }, null);
  if (localCursor.moveToFirst()) {
    do
    {
      localStringBuffer.append(localCursor.getString(localCursor.getColumnIndex("data")) + "  /  ");
    } while (localCursor.moveToNext());
  }
  return localStringBuffer.toString();
}
```

[그림 12] 연락처의 이메일 수집 코드

3. 결론

Spyware.Android.PowerOffHijack 악성앱은 사용자 정보를 탈취하는 것이 주된 목적이다. 이 악성앱의 위협적인 부분은 피해자가 자신도 모르게 실시간으로 도청당할 수 있다는 점과 공격자가 내 위치를 실시간으로 파악할 수 있다는 점이다.

이러한 악성앱의 설치를 막기 위해서는 다음과 같은 조치를 취해야 한다.

- 스미싱을 진단할 수 있는 앱 사용
- 백신을 사용하여 주기적으로 검사
- 다운로드 받은 파일의 설치 전 백신 검사 실행
- '알 수 없는 소스' 옵션 비활성화 (공식 마켓을 통한 앱 설치 권장)
- 스마트폰의 구조를 임의로 변경하지 않기

Part3. 보안 이슈 돋보기

2월의 보안이슈

2월의 취약점

2월의 보안 이슈

알약이 뽑은 TOP 이슈

– 데이터를 인질로…'랜섬웨어' 연초부터 공포

컴퓨터에 중요 파일들을 인질로 잡고 페이팔 등 온라인 결제 서비스나 비트코인과 같은 온라인 가상화폐로 돈을 요구하는 랜섬웨어가 연초부터 국내에 급속히 확산되고 있다. 국내에서 주로 발견된 랜섬웨어는 'CTB-Locker'로, 이메일 첨부파일로 위장, 유포되며 이외에도 다양한 변종이 확산 중에 있다.

– 국내기업 97%, 정보보호 예산 편성 5% 미만… 정보보호 투자 인색 여전

한국인터넷진흥원 조사결과에 따르면 국내 기업들의 97%는 전체 예산 중 정보보호 예산의 비중이 5%도 안되는 것으로 나타났다. 지난 몇 년간 수 많은 보안사고를 경험했으나, 기업들의 정보보호 투자는 여전히 인색한 것으로 나타났다.

– 北 해킹조직 '킴수키'2년 전에도 원전 공격 시도한 듯

한국수력원자력을 공격한 해커와 연계되었다는 의혹을 받고 있는 북한의 해킹조직 '킴수키(kimsuky)'가 2년 전에도 국내 원전 관련 기관들을 공격한 정황이 발견되었다. 2013년 8월 말 '제 57차 국제원자력기구(IAEA) 총회 참가자료'라는 제목의 한글 파일이 국내 백신 업체들에 포착되었으며, 악성코드가 포함되어 있는 것으로 확인되었다.

– 수표 뒷면 주민등록번호 금지, 보안 주의 필요

금융위원회와 금융감독원은 금융분야 개인정보 유출 재발방지 종합대책의 후속조치로 전 금융권에 '주민등록번호 수집, 이용 가이드라인'을 배포했다. 이에 따라 마트나 백화점, 인터넷에서 회원가입을 할 때 주민등록번호 제출을 요구하는 것은 불법이며, 수표를 사용할 때 역시 신분증을 확인하는 건 되지만, 수표 뒷면에 주민등록번호 뒷자리까지 모두 적게 하는 것은 금지된다.

– 원전 해킹 잊었다… 관련 예산 삭감

산업통상자원부가 올해 국가 사이버안전센터 예산을 5억 3100만 원으로 전년도 보다 3.3% 삭감함에 따라 2012년 이후 3년 연속 예산이 줄었다. 이에 지난해 '원자력발전소 사이버 테러 위협'이 사회적으로 큰 혼란을 일으켰던 만큼 사이버 안전을 강화해야 하는 시점임에도 정부의 예산 정책은 거꾸로 가고 있다는 지적이 있었다.

– 금융보안 3종 세트 필수설치 의무 폐지

인터넷뱅킹과 전자상거래 시 보안 관련 프로그램들을 줄줄이 설치하도록 했던 법 규정을 삭제한 '전자금융감독규정' 일부 개정안을 최근 공포해 시행에 들어갔다. 개정 규정에서 금융당국은 '해킹 등 침해 행위로부터 전자금융거래를 보호하기 위한 이용자의 전자적 장치(휴대전화, PC 등)에 보안프로그램 설치 등 보안대책을 적용할 것'이라는 표현을 삭제했다.

– 국내 기업, 기관 노린 표적 해킹 공격 주의보

지난해 연말부터 현재까지 국내 특정 기업과 기관을 상대로 한 표적 해킹공격의 징후가 연이어 포착되어 왔으며, 이는 특정한 기업과 기관을 대상으로 공격하는 유사한 패턴의 표적 해킹 방식으로 확인되었다. 이 공격 유형은 일명 'Sykipot 캠페인'으로, 이러한 공격을 예방하려면 출처가 불분명한 이메일의 첨부 파일을 열어보지 말아야 한다.

2월의 취약점

Microsoft 2월 정기 보안 업데이트

- Internet Explorer용 보안 업데이트(3034682)

이 보안 업데이트는 Internet Explorer의 공개된 취약성 1건과 비공개적으로 보고된 취약성 40건을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 Internet Explorer를 사용하여 특수 제작된 웹 페이지를 볼 경우 원격 코드 실행을 허용할 수 있습니다. 이러한 취약성 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.

- Windows 커널 모드 드라이버의 취약성으로 인한 원격 코드 실행 문제(3036220)

이 보안 업데이트는 Microsoft Windows의 공개된 취약성 1건과 비공개적으로 보고된 취약성 5건을 해결합니다. 공격자가 사용자에게 특수 제작된 문서를 열거나 포함된 트루타입 글꼴이 있는 신뢰할 수 없는 웹 사이트를 방문하도록 유도할 경우 가장 심각한 취약성은 원격 코드 실행을 허용할 수 있습니다.

- 그룹 정책의 취약성으로 인한 원격 코드 실행 문제(3000483)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약성을 해결합니다. 도메인 구성 시스템을 사용하는 사용자가 공격자 제어 네트워크에 연결하도록 공격자가 유도하는 경우 이 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다. 이 취약성 악용에 성공한 공격자는 영향받는 시스템을 완전히 제어할 수 있습니다. 이렇게 되면 공격자가 프로그램을 설치할 수 있을 뿐 아니라 데이터를 보거나 변경하거나 삭제하거나, 모든 사용자 권한이 있는 새 계정을 만들 수도 있습니다.

- Microsoft Office의 취약성으로 인한 원격 코드 실행 문제(3032328)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Office의 취약성 3건을 해결합니다. 사용자가 특수 제작된 Microsoft Office 파일을 열면 이 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다. 이 취약성 악용에 성공한 공격자는 현재 사용자와 동일한 사용자 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 고객은 관리자 권한으로 작업하는 고객에 비해 영향을 적게 받습니다.

- Microsoft Office의 취약성으로 인한 보안 기능 우회 문제(3033857)

이 보안 업데이트는 Microsoft Office의 공개된 취약성 1건을 해결합니다. 사용자가 특수 제작된 Microsoft Office 파일을 열면 이 취약성으로 인해 보안 기능 우회가 허용될 수 있습니다. 보안 기능을 우회하는 것만으로는 임의의 코드 실행이 허용되지 않지만 공격자는 이 보안 기능 우회 취약성을 원격 코드 실행 취약성 등과 같은 다른 취약성과 함께 사용하여 임의의 코드를 실행할 수 있습니다.

- 그룹 정책의 취약성으로 인한 보안 기능 우회 문제(3004361)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약성을 해결합니다. 공격자가 메시지 가로채기(man-in-the-middle) 공격 방식으로, 대상 시스템의 그룹 정책 보안 구성 엔진 정책 파일이 손상되거나 읽을 수 없게 하면 이 취약성으로 인해 보안 기능 우회가 허용될 수 있습니다. 이로 인해 시스템의 그룹 정책 설정이 기본값으로 되돌아가고 잠재적으로 보안 수준이 낮아지게 됩니다.

Part3.보안 이슈 돋보기

- Microsoft Windows의 취약성으로 인한 권한 상승 문제(3031432)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약성을 해결합니다. 이 취약성으로 인해 공격자는 가장 수준 보안 검사 부족을 이용하여 프로세스 만들기 중에 권한을 상승시킬 수 있습니다. 이 취약성 악용에 성공한 인증된 공격자는 관리자 자격 증명을 얻고 이 자격 증명을 사용하여 권한을 상승시킬 수 있습니다. 이렇게 되면 공격자가 프로그램을 설치할 수 있을 뿐 아니라 데이터를 보거나 변경하거나 삭제하거나, 모든 관리자 권한이 있는 새 계정을 만들 수도 있습니다.

- Microsoft 그래픽 구성 요소의 취약성으로 인한 정보 유출 문제(3029944)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약성을 해결합니다. 이 취약성으로 인해 사용자가 특수 제작된 TIFF 이미지가 포함된 웹 사이트로 이동할 경우 정보가 공개될 수 있습니다. 이 취약성으로 인해 공격자가 직접 코드를 실행하거나 해당 사용자 권한을 상승시킬 수는 없지만 영향받는 시스템의 손상을 악화시키는 데 사용할 수 있는 정보를 얻을 수 있습니다.

- Virtual Machine Manager의 취약성으로 인한 권한 상승 문제(3035898)

이 보안 업데이트는 비공개적으로 보고된 VMM(Virtual Machine Manager)의 취약성을 해결합니다. 이 취약성으로 인해 공격자가 영향받는 시스템에 로그온하는 경우 권한 상승이 허용될 수 있습니다. 이 취약성을 악용하려면 공격자가 유효한 Active Directory 로그온 자격 증명을 가지고 있고 해당 자격 증명으로 로그온할 수 있어야 합니다.

- 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/library/security/ms15-Feb
영문 : https://technet.microsoft.com/en-us/library/security/ms15-Feb

아래한글 DLL 하이재킹 취약점 보안 업데이트 권고

한글과컴퓨터社의 한글 등 오피스 프로그램에서 DLL 하이재킹 취약점이 발견됨

- 사용자가 특수하게 조작된 DLL 파일과 동일한 디렉토리 경로에 존재하는 정상파일을 한글 프로그램을 통하여 열람 및 추가 기능을 사용할 경우, 임의코드가 실행될 수 있는 취약점이 존재. 영향 받는 버전의 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 보안 업데이트를 권고함

- 상세정보

영향 받는 소프트웨어

제품군	세부제품	영향받는 버전
한컴오피스 2010	공통 요소	8.5.8.1509 이전버전
	한글	8.5.8.1447 이전버전
	한셀	8.5.8.1359 이전버전
	한쇼	8.5.8.1503 이전버전

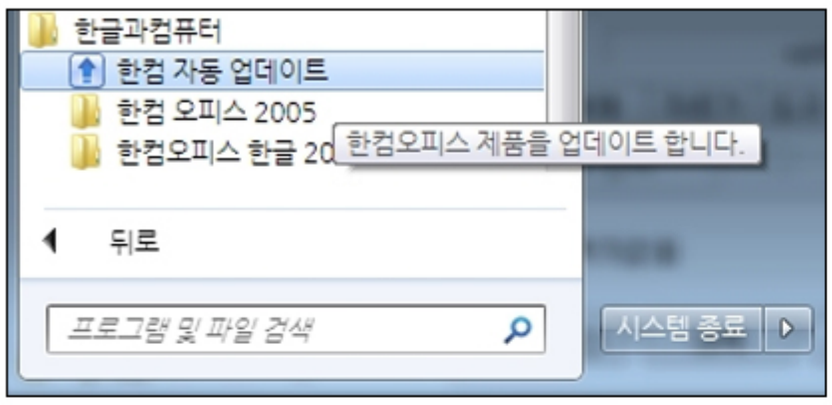
- 해결법

한글과컴퓨터 홈페이지에서 보안업데이트 파일을 직접 다운로드 받아 설치하여 영향 받지 않는 버전(보안#26)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

Adobe Flash Player 신규 취약점 주의 권고

Adobe社의 Flash Player에 영향을 주는 신규 취약점이 발견됨
공격자는 취약점을 이용하여 웹브라우저를 통해 악성코드 유포 등 drive-by-download 공격이 가능

- 상세정보

임시 권고 사항

현재 해당 취약점에 대한 보안업데이트는 발표되지 않았음

- 패치가 발표 될 때까지 Flash Player 사용 자제
- Adobe社는 2월 1주내 패치 발표 예

- 해결법

취약점에 의한 피해를 줄이기 위하여 사용자는 다음과 같은 사항을 준수해야함

- 신뢰되지 않는 웹 사이트의 방문 자제
- 출처가 불분명한 이메일 및 링크를 열어보지 않음
- 사용하고 있는 백신프로그램의 최신 업데이트를 유지하고, 실시간 감시기능을 활성화

- 참고사이트

https://helpx.adobe.com/security/products/flash-player/apsa15-02.html
http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-discovers-new-adobe-flash-zero-day-exploit-used-in-malvertisements/

Lenovo Superfish 애드웨어 삭제 권고

Lenovo社는 자사 노트북 등에 취약점이 존재하는 악성 애드웨어 Superfish를 설치한 후 출고한 것을 공지하고,
해당 악성 애드웨어 삭제를 권고
공격자가 해당 애드웨어의 취약점을 악용할 경우 전송 데이터 변조 및 도청 등의 공격이 가능할 수 있으므로 해당 악성 애드웨어 반드시 삭제

- 상세정보

Lenovo社의 웹서버와 악성 애드웨어가 설치된 Lenovo社 제품 간 전송 데이터 변조 및 도청 등이 가능한 취약점

영향 받는 제품

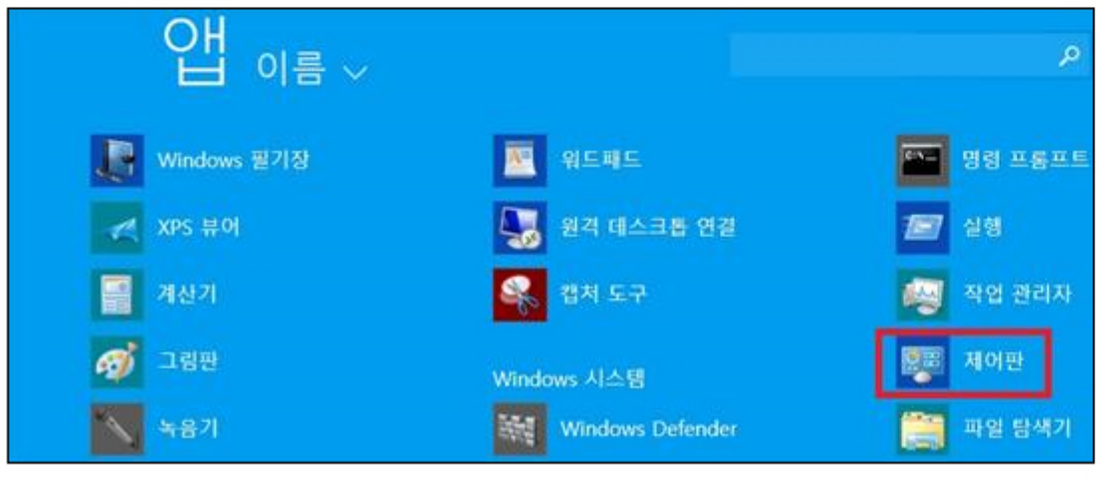
G Series : G410, G510, G710, G40-70, G50-70, G40-30, G50-30, G40-45, G50-45, G40-80
U Series : U330P, U430P, U330Touch, U430Touch, U530Touch
Y Series : Y430P, Y40-70, Y50-70, Y40-80, Y70-70
Z Series : Z40-75, Z50-75, Z40-70, Z50-70, Z70-80
S Series : S310, S410, S40-70, S415, S415Touch, S435, S20-30, S20-30Touch
Flex Series : Flex2 14D, Flex2 15D, Flex2 14, Flex2 15, Flex2 Pro, Flex 10
MIIX Series : MIIX2-8, MIIX2-10, MIIX2-11, MIIX 3 1030
YOGA Series : YOGA2Pro-13, YOGA2-13, YOGA2-11, YOGA3 Pro
E Series : E10-30

– 해결법

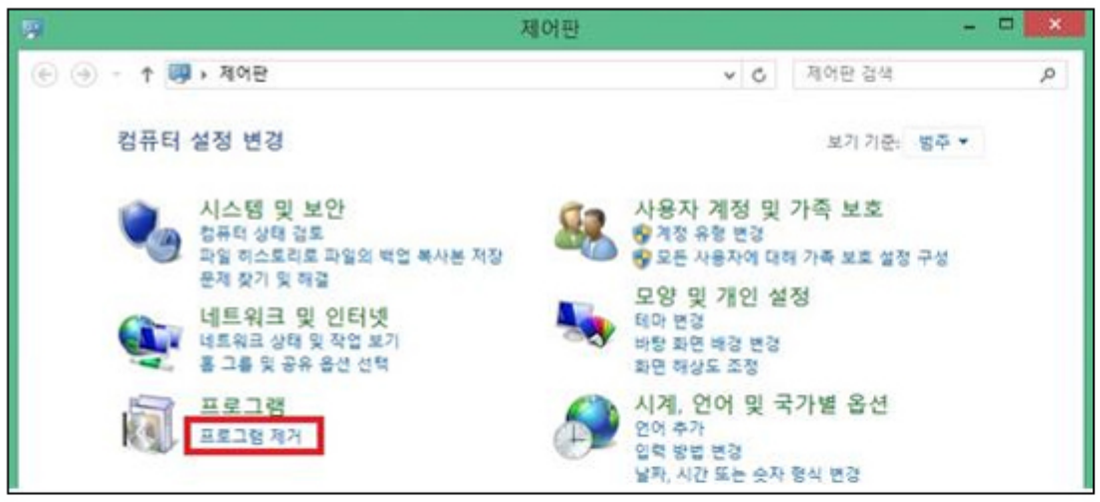
Superfish 애드웨어 삭제

– '시작' → 관리패널 열기

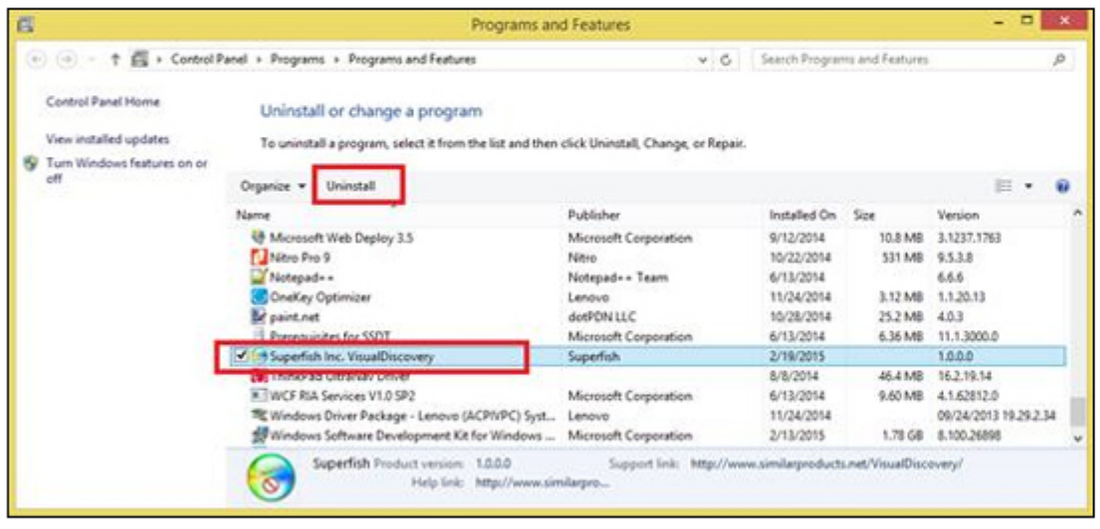
– '제어판' 열기



– '프로그램 제거' 열기

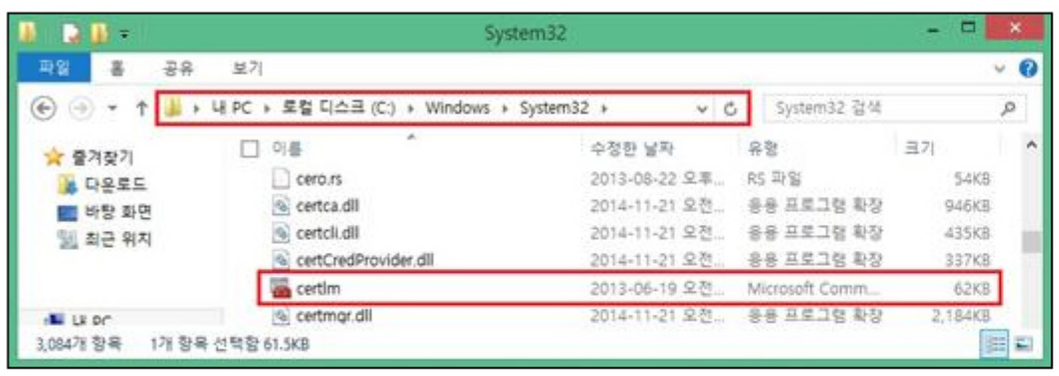


– 'Superfish Inc. Visual Discovery' 제거

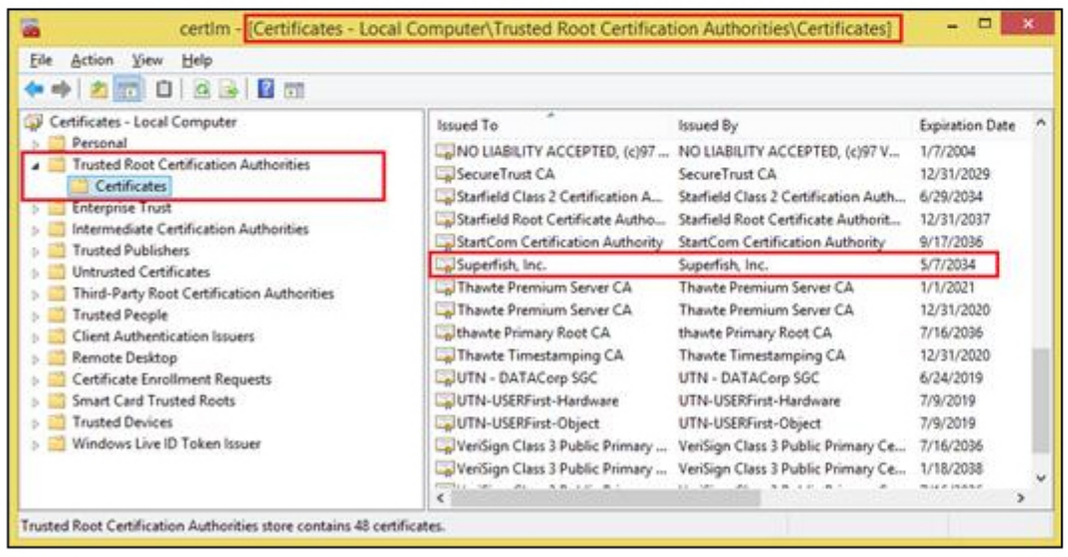


Superfish 인증서 삭제

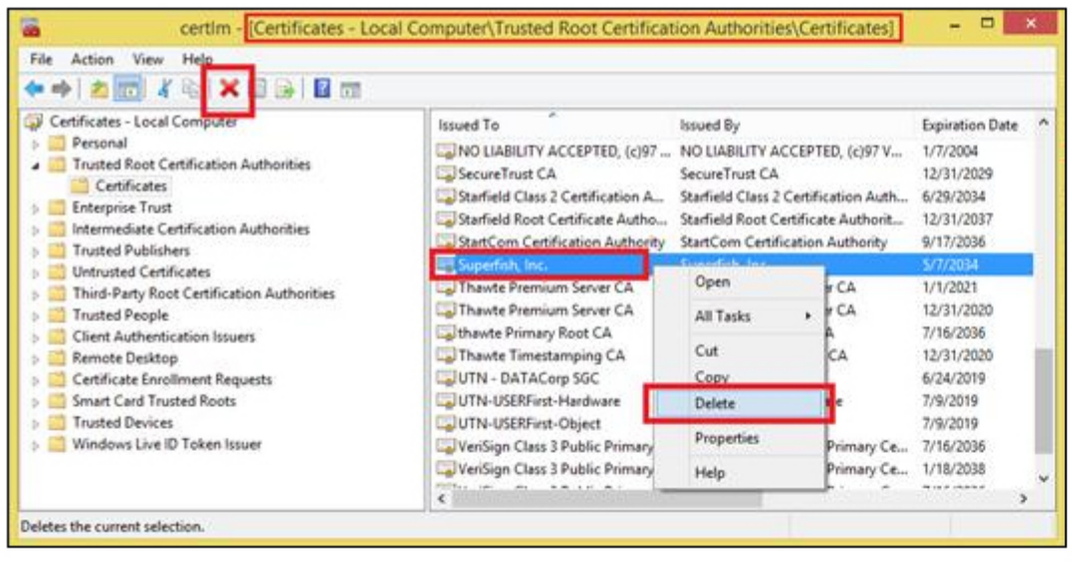
– '인증서 관리' 열기



'Superfish, Inc' 인증서 찾기



'Superfish, Inc' 인증서 삭제



시스템 재부팅

– 참고사이트

http://news.lenovo.com/article_display.cfm?article_id=1929

http://support.lenovo.com/us/en/product_security/superfish_uninstall

Adobe Flash Player 신규 취약점 보안 업데이트 권고

Adobe社는 최근 'Angler Exploit Kit'이 악용하고 있는 Flash Player 취약점(CVE-2015-0311)에 대해 보안 업데이트를 발표
- 자동 업데이트를 설정한 사용자는 보안 업데이트 파일이 자동으로 다운로드되어 설치
- 수동으로 직접 내려 받아 설치할 수 있는 업데이트 파일은 1.26(현지시간) 제공될 예정

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

- 상세정보

영향 받는 소프트웨어

Adobe Flash Player

소프트웨어 명	동작환경	영향받는 버전
Adobe Flash Player Desktop Runtime	Windows, Mac	16.0.0.287 및 이전버전
Adobe Flash Player Extended Support Release	Windows, Mac	13.0.0.262 및 이전버전
Adobe Flash Player	Linux	11.2.202.438 및 이전버전

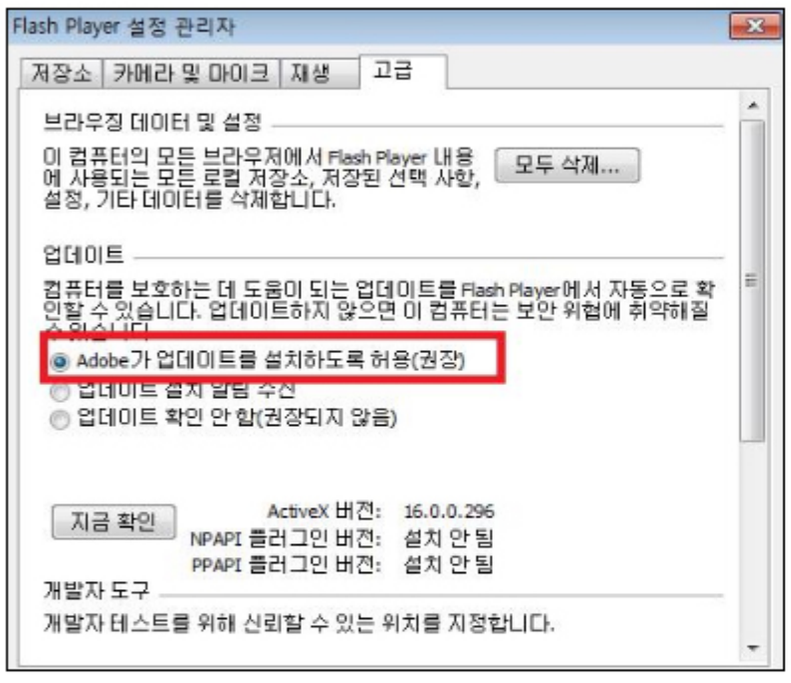
- 해결법

자동 업데이트를 이용하여 Adobe Flash Player16.0.0.296 버전으로 업데이트 적용

- Flash Player버전 확인 및 자동 업데이트 설정 방법

1. 제어판에서 Flash Player를 클릭(아이콘이 보이지 않을 경우 보기기준을 '큰아이콘'으로 변경)

2. Flash Player 설정 관리자에서 고급탭 클릭 후 "Adobe가 업데이트를 설치하도록 허용(권장)"을 선택



- 참고사이트

http://helpx.adobe.com/security/products/flash-player/apsa15-01.html

http://blogs.adobe.com/psirt/?p=1160

리눅스 Ghost 취약점 보안 업데이트 권고

※ '15. 1. 30. 업데이트 내용 : 첨부문서(리눅스 Ghost 취약점 대응방안 권고 v2.pdf)에 영향 받는 플랫폼 OS, FAQ 추가

미국 US-CERT는 리눅스 GNU C 라이브러리(glibc)에서 임의코드를 실행할 수 있는 취약점(CVE-2015-0235)이 발견되었다고 발표
CVE-2015-0235는 해당 라이브러리의 gethostbyname( ) 함수 처리 과정에서 발생하는 버퍼오버플로우 취약점
GNU C 라이브러리 : 리눅스 계열 운영체제에서 기본적으로 사용하는 소프트웨어

- 상세정보

라이브러리에 존재하는 특정 함수(__nss_hostname_digits_dots( ))의 잘못된 메모리 사용으로 인해 오버플로우가 발생하여 프로그램의 실행 흐름 변경이 가능

- * __nss_hostname_digits_dots( ) 함수 : 도메인 주소를 IP 주소로 변환할 때 사용하는 함수인gethostbyname( )를 호출 시 내부적으로 호출되는 함수

- 해결법

취약한 버전의 라이브러리를 사용하는 시스템은 상위 버전으로 업데이트

※ 실행파일에 취약한 버전의 라이브러리를 포함하여 컴파일 한 경우, 상위 버전의 라이브러리로 재컴파일 하여 설치 필요

다음 참고사이트의 내용을 참조하여 보안업데이트 수행

- 참고사이트

http://lists.centos.org/pipermail/centos/2015-January/149413.html
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=776391
https://access.redhat.com/articles/1332213
http://www.ubuntu.com/usn/usn-2485-1/

Apple (OS X, Safari, iOS, Apple TV) 보안 업데이트 권고

Apple社는 자사 제품에서 발견된 임의코드 실행 및 원격제어 가능 취약점을 해결한 보안 업데이트를 발표
공격자가 취약점을 이용하여 원격조종 등 피해를 발생 시킬 수 있으므로 해당 Apple 제품을 최신 버전으로 업데이트

- 상세정보

임의코드 실행 및 Apple 제품에 대한 원격제어 가능 취약점

영향 받는 소프트웨어

- OS X : Mountain Lion v10.8.5, Mavericks v10.9.5, Yosemite v10.10, v10.10.1
- Safari : Mountain Lion v10.8.5, Mavericks v10.9.5, Yosemite v10.10.1
- iOS : iPhone 4s 이상, iPod Touch 5세대 이상, iPad 2 이상
- Apple TV : Apple TV(3세대 이상)

– 해결법

OS X 및 Safari

– 직접 설치 : http://support.apple.com/downloads/를 통해 해당 버전을 다운로드하여 업데이트 진행

– Apple 앱스토어 이용 : Mac 메뉴에서 [소프트웨어 업데이트] 선택

iOS

– [설정]→[일반]→[소프트웨어업데이트] 선택

– [다운로드 및 설치]→[동의] 선택하여 업데이트

Apple TV

– [설정] → [일반] → [소프트웨어업데이트] 선택

– 참고사이트

https://www.us-cert.gov/ncas/current-activity/2015/01/27/Apple-Releases-Security-Updates-OS-X-Safari-iOS-and-Apple-TV

http://support.apple.com/en-us/HT204244

http://support.apple.com/en-us/HT204243

http://support.apple.com/en-us/HT204245

http://support.apple.com/en-us/HT204246

Adobe Flash Player 신규 취약점 보안 업데이트 권고

Adobe社의 Flash Player에 영향을 주는 신규 취약점(CVE-2015-0313)에 대해 보안 업데이트를 발표

– 자동 업데이트를 설정한 사용자는 보안 업데이트 파일이 자동으로 다운로드되어 설치

– 수동으로 직접 내려 받아 설치할 수 있는 업데이트 파일은 2.5(현지시간) 제공될 예정

공격자는 취약점을 이용하여 웹브라우저를 통해 악성코드 유포 등 drive-by-download 공격이 가능

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

– 상세정보

공격자는 취약점을 이용하여 웹브라우저를 통해 악성코드 유포 등 drive-by-download 공격이 가능

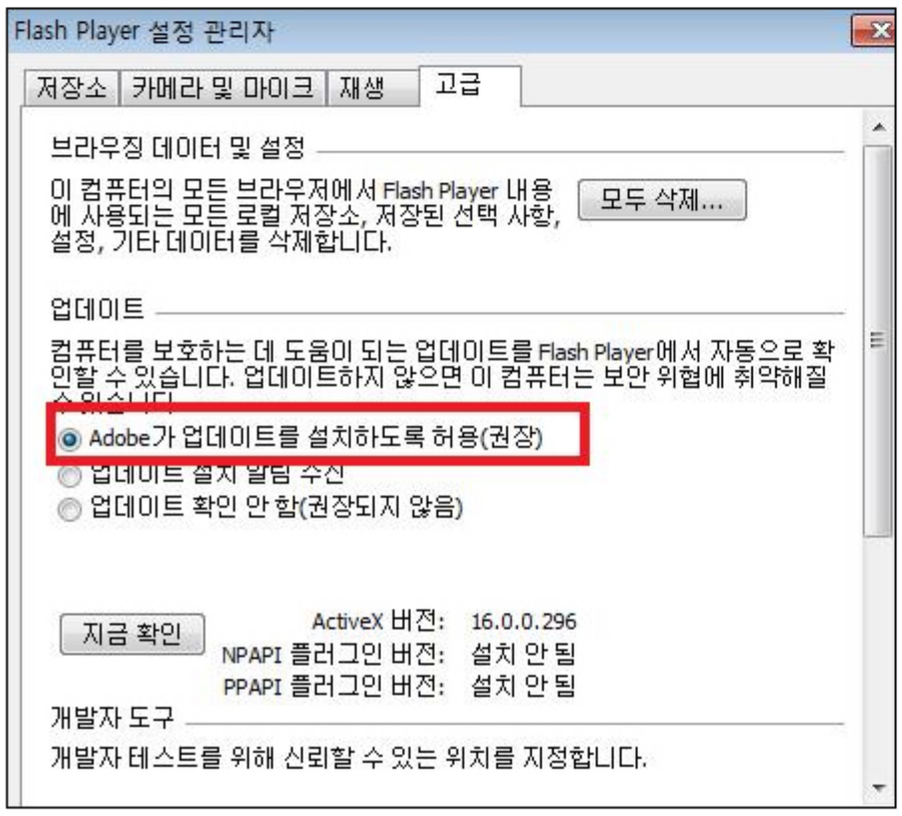
– 해결법

자동 업데이트를 이용하여 Adobe Flash Player16.0.0.305 버전으로 업데이트 적용

– Flash Player버전 확인 및 자동 업데이트 설정 방법

1. 제어판에서 Flash Player를 클릭(아이콘이 보이지 않을 경우 보기기준을 '큰아이콘'으로 변경)

2. Flash Player 설정 관리자에서 고급탭 클릭 후 "Adobe가 업데이트를 설치하도록 허용(권장)"을 선택



– 참고사이트

https://helpx.adobe.com/security/products/flash-player/apsa15-02.html

http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-discovers-new-adobe-flash-zero-day-exploit-used-in-malvertisements/

Part4. 해외 보안 동향

영미권

중국

일본

1.영미권

미 거대 의료보험사 Anthem, 직원 및 고객 개인 정보 유출

Anthem Data Breach — 6 Things You Need To Know

미국에서 두 번째로 큰 의료보험사인 Anthem이 지난 수요일 8천만명 이상 고객들의 개인정보를 도난당했다고 밝혔다. 이는 사상 가장 큰 데이터 유출 사건으로, 2013년에 발생한 타겟 데이터 유출 사건의 두 배이다.

최고 경영자를 포함한 직원 및 현재, 과거 고객들의 주소, 생년월일, 의료식별번호, SSN, 이메일 주소, 소득 수준 정보가 유출되었다. 8천만명은 어마어마한 숫자이다. 이는 캘리포니아, 텍사스, 일리노이주의 인구를 모두 합친 것과 같은 수준이다.

이들은 고객들의 문제를 해결하기 위하여 보안업체 FireEye의 Mandiant부문을 고용했다. 이러한 노력에도 불구하고 아직까지 해커의 신원을 밝혀내지 못한 상황이다.

해커가 정교한 악성 소프트웨어를 이용하여 Anthem 네트워크에 침입한 후, 직원의 로그인 계정을 획득하는 방법을 통해 정보 유출이 일어난 것으로 추측되고 있다. 데이터 유출이 발생한 직후부터, '신용 보호 서비스'에 가입을 권유하며 개인정보를 요구하는 가짜 스팸 메일이 성행하고 있다. 지난 금요일, Anthem은 미국 내 고객들에게 이메일을 통한 사기를 조심하라고 당부했다.

Anthem은 해커들이 고객들의 의료기록을 훔쳐간 것으로 보이지 않는다고 주장했다. 하지만 SNS, 주소, 이메일 주소와 함께 의료식별번호(medical identification number)가 유출되었기 때문에, 다른 의료사기에 충분히 악용될 수 있다.

출처 : Hacker News (http://thehackernews.com/2015/02/anthem-data-breach.html)

피싱 공격에 설득력을 실어주는 IE 취약점 발견

Major Internet Explorer vulnerability could lead to convincing phishing attacks

한 보안연구원이 있는 IE의 심각한 보안 취약점을 발견하였다. 이 취약점을 해커들이 악용할 경우, 설득력이 높은 피싱 공격을 실행하고 유저의 브라우저에 악성 코드를 삽입할 수 있다.

David Leo는 Daily Mail 웹사이트에서 이 취약점을 이용하여 직접 실험한 결과의 링크를 포함한 상세 정보를 공개하였다. 이 버그는 윈도우 7, 8.1에서 사용되는 IE 11버전에서만 동작하는 XSS 취약점이며, 동일 오리진 정책(Same-Origin Policy)을 우회한다. Leo의 취약점 악용 예시 페이지에는 Daily Mail 웹사이트로 연결되는 링크를 클릭할 수 있는 페이지가 표시되어 있다. IE 사용자가 이를 클릭하면 정상 페이지를 볼 수 있지만, 7초 후에는 "Hacked by Deusen"이라는 페이지로 변경된다.

이번 취약점을 이용한 피싱 공격으로 Daily Mail의 웹사이트 자체는 해킹되지 않았지만, 사용자의 동의 없이 브라우저에 다른 콘텐츠가 표시된다. 공격자가 이를 악용하여 주소창의 URL이 바뀌지 않은 상태에서 가짜 로그인 페이지 등의 피싱 페이지를 출력한다면, 사용자들은 의심스러운 점을 찾지 못하고 피싱 공격에 당할 수 있다.

Vulture South에서는 지난 금요일 이 결함에 대해 MS에 전달하였다. MS는 패치를 개발 중이라고 입장을 밝혔으나, 정확한 일정은 받지 못했다고 전했다.

출처 : Hot for Security (http://www.hotforsecurity.com/blog/major-internet-explorer-vulnerability-could-lead-to-convincing-phishing-attacks-11310.html)

다른 사용자의 포토 앨범을 삭제할 수 있는 페이스북 취약점 발견

Facebook Vulnerability Allows Hacker to Delete Any Photo Album

권한이 없는 누구라도 페이스북 포토 앨범을 삭제할 수 있는 페이스북의 심각한 취약점이 보고되었다.

보안전문가 Lazman Muthiyah는 이 취약점이 페이스북의 그래프 API 메커니즘에 존재하며, 해커가 타인의 페이스북 포토 앨범도 삭제할 수 있다고 밝혔다. 일반적으로 페이스북 그래프 API는 사용자 데이터를 읽고 쓰는데 접근 토큰(access token)을 요구한다. 이는 앱에 제한된 접근을 제공한다. 하지만 Laxman은 모바일 버전을 위해 생성된 그의 접근 토큰을 악용하면 다른 페이스북 사용자가 포스팅한 포토 앨범을 삭제할 수 있다는 사실을 알아냈다.

공격자는 다른 사용자의 페이스북 포토 앨범을 삭제하기 위해서, 타겟의 포토 앨범 ID와 공격자가 생성한 '안드로이드용 페이스북 앱'용 접근 토큰과 함께 HTTP 기반의 Graph API 요청을 보내기만 하면 된다. 페이스북 버그 바운티 프로그램에서는 그에게 이 크리티컬한 결점을 제보한 대가로 한화 1,400만 원 상당의 상금을 지급하였다.

샘플 요청

```
Request :-
DELETE /<Victim's_photo_album_id> HTTP/1.1
Host : graph.facebook.com
Content-Length: 245
access_token=<Your(Attacker)_Facebook_for_Android_Access_Token>
```

출처 : The Hacker News (http://thehackernews.com/2015/02/hacking-facebook-photo-album.html)

2.중국

휴대폰이 꺼져있는 상황에서도 정보를 탈취하는 악성코드

휴대폰이 종료되어 있는 상황에서도 사용자 정보를 빼내는 악성코드가 등장했다. PowerOffHijack 악성코드에 감염되면, 해당 악성코드는 루트 권한을 획득하고 'system_server' 파일을 건드려 종료 프로세스에 개입한다. 또한, mWindowManagerFuncs 인터페이스를 부분적으로 가로채어 사용자가 전원 버튼을 누르는 순간 가짜 종료 팝업창을 띄운다. 하지만 휴대폰은 여전히 켜져 있는 상태이며, 백그라운드에서는 공격자에 의해 정보가 탈취된다. 공격자는 이를 통해 통화 내역, GPS 정보를 탈취할 뿐만 아니라, 문자 및 채팅 대화 기록 등 다양한 개인정보를 탈취할 수 있다.

PowerOffHijack 악성코드는 안드로이드5.0 이하 버전에서만 동작하는 것으로 확인되었다. 해당 악성코드는 서드파티 마켓을 통하여 유포되고 있으나, 어떤 어플리케이션을 위장하여 유포되고 있는지는 아직 밝혀지지 않았다. 또한 어떤 방법을 통하여 루트 권한을 획득하는지도 밝혀지지 않은 상태이다.

해당 악성코드는 중국에서 처음 발생한 것으로 확인되며, 현재까지 10,000개가 넘는 기기를 감염시킨 것으로 나타났다.

출처 : http://thehackernews.com/2015/02/poweroffhijack-android-malware.html

3개 회사가 휴대폰에 '악성코드' 심어서 유포, 전화번호부 2000만 개 이상 유출

휴대폰 내에 설치된 악성코드와 유사한 '번들 프로그램'이 해당 플러그인을 통한 원격 조종으로 광고를 띄워 광고비를 번 것이 확인되었다. 이는 3개의 회사가 연합하여 안드로이드 계열의 내수 스마트폰을 타겟으로 설치한 것으로 밝혀졌다. 이 번들 프로그램은 광고뿐만 아니라 사용자 위치정보, 사용자 sim 카드 정보 등을 읽을 수 있다. 또한, 휴대폰 내의 문자, 통화 기록, 전화부 등의 개인정보를 몰래 탈취했다. 조사결과 현재까지 약 2000만 건의 전화번호를 탈취한 것으로 나타났다. 해당 작업을 진행한 폰들은 주로 삼성과 HTC 내수폰이었다. 이들은 애플 버전도 연구하였지만 실패한 것으로 밝혀졌다.

출처 : http://news.sohu.com/20150227/n409200722.shtml

3. 일본

– 가짜 통판 사이트가 구글검색의 상위에 노출

偽通販サイトがグーグル検索上位に登場

라쿠텐의 가짜 통판 사이트가 이슈가 되고 있는 가운데, 문제가 되고 있는 사이트가 구글 검색결과의 상위에 표시된다. 따라서 검색 결과의 상위에 노출되었다고 해서 쉽게 믿어서는 안 된다.

라쿠텐 위조사이트 경고, 2700 이상의 가짜 사이트 확인

이러한 가짜 통판 사이트는 크게 2가지의 목적으로 구분할 수 있다. 첫 번째는 돈을 목적으로 한 사기이다. 가짜 브랜드 상품을 보내거나, 상품자체가 오지 않는 경우도 있다. 위에 소개한 통판 사이트는 판매 사기의 가능성이 높다. 두 번째 패턴은 신용카드 정보와 계정정보의 탈취를 목적으로 하는 것이다. 2월 초순부터 문제가 되고 있는 라쿠텐의 가짜 사이트는 정보 탈취를 목적으로 하고 있을 가능성이 크다. 라쿠텐에서는 라쿠텐을 사칭한 가짜 사이트에 대해 '라쿠텐을 위장한 사이트를 주의해주세요.'라고 밝히며 사용자의 주의를 환기시켰다.

다수의 가짜 사이트가 라쿠텐 시장의 로고를 사용하고 있었으며, 2월 26일 기준 2722개의 URL이 가짜 사이트로 밝혀졌다. 라쿠텐 시장의 탑 페이지와 완전히 똑같은 디자인의 가짜 사이트가 양산되고 있었고 URL의 일부에 'rakuten' 등의 문자를 넣은 경우가 많았다. 또한, 멀웨어를 감염시키는 파일을 첨부한 메일도 확산되고 있다.

이러한 라쿠텐의 가짜 사이트는 ID, 패스워드, 신용카드 정보의 탈취가 목적으로 생각되나, 판매 사기의 패턴에 해당될 가능성도 있다. 일본어가 이상하거나 가격이 저렴한 경우, 판매 사기를 의심해 보아야 한다.

가짜 통판 사이트의 대처방법은 아래와 같다.
-신뢰 가능한 대형 사이트의 탑 페이지에서 검색
-검색 결과나 광고는 신뢰하지 말 것.
-주소, 전화번호 표기를 확인할 것.
-메일 링크는 클릭하지 말 것

*라쿠텐 : 인터넷 쇼핑 서비스를 시작으로 인터넷 서비스를 제공하고 있는 일본의 기업

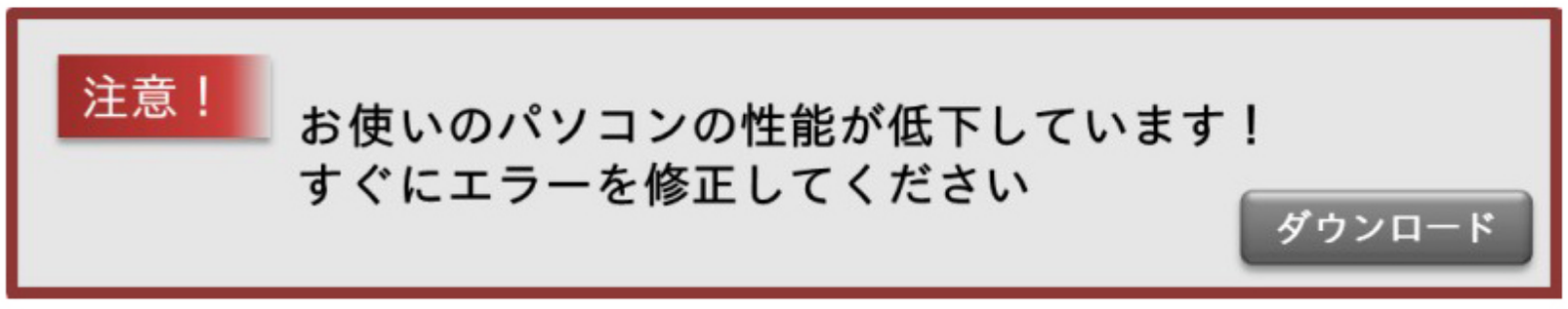
출처 : YOMIURI ONLINE
(http://www.yomiuri.co.jp/it/security/goshinjyutsu/20150227-OYT8T50119.html)

– 경고 메시지에 당황하지 마세요! 소프트웨어를 팔기 위한 악질의 수법

警告メッセージに慌てるな！ ソフトを売り込む悪質な手口

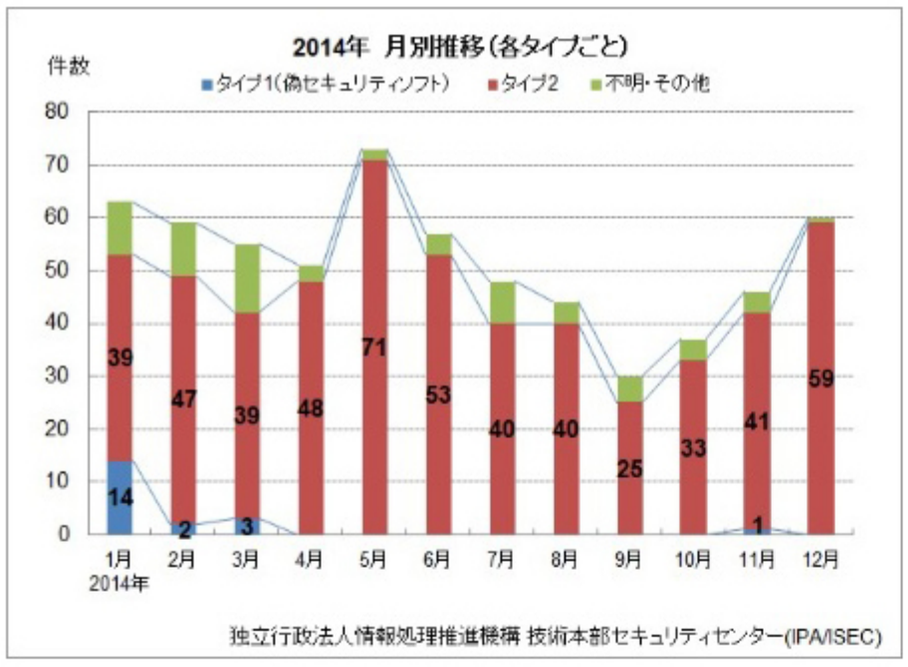
정보처리추진기구(IPA)는 2015년 2월 2일, 웹 페이지 상의 가짜 경고 메시지를 표시하여 소프트웨어의 구매를 유도하는 수법이 잇달아 발생하고 있다고 밝혔다. 그러나 해당 수법은 실제로 PC에 문제가 발생하고 있는 것이 아니므로 당황하지 말 것을 당부했다.

IPA는 '컴퓨터의 상태가 이상해진 것 같다. 성능이 저하되고 있다는 오류메시지가 뜬다.'는 상담이 다수 들어오고 있다고 밝혔다. 웹 사이트를 열람하고 있으면 컴퓨터의 이상을 경고하는 메시지가 표시된다.

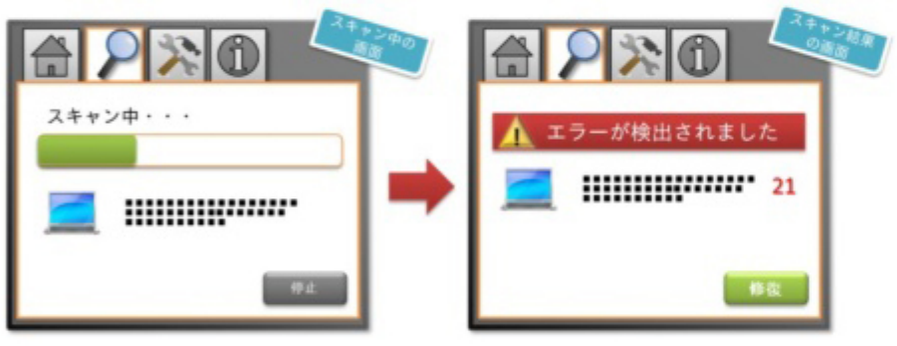


언뜻 보면, OS가 표시하고 있는 것처럼 생각될 수 있으나 실제로는 웹 페이지의 콘텐츠 중 일부이며 특정 소프트웨어의 판매를 목적으로 띄우고 있는 것이다. 사용자가 경고 메시지의 배너를 클릭하면 (1) 취약점을 뚫고 보안프로그램이 설치되거나, (2) 특정의 소프트웨어의 무료 버전을 배포하는 웹 사이트로 연결된다.

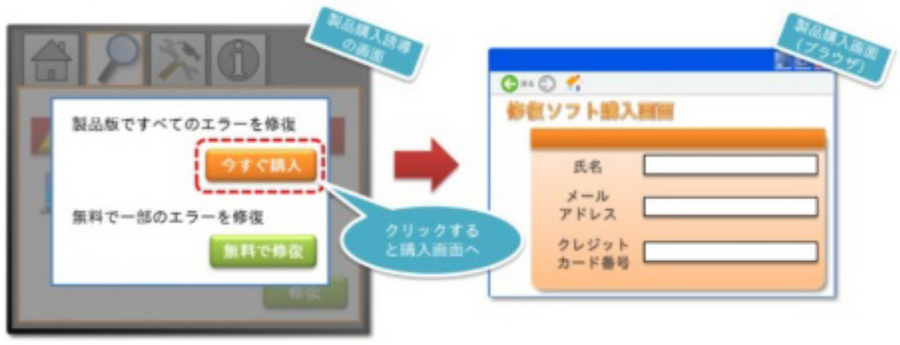
IPA에 의하면 2013년에는 (1)의 타입이 빈번하게 발생하였으나, 2014년도부터는 (2)의 타입이 대부분을 차지했다고 밝혔다



(2) 타입에서는 경고 메시지를 클릭하면 검사나 복구작업은 시작되지 않고, 무료 버전의 소프트웨어를 다운받을 수 있는 사이트로 연결된다. 무료 버전을 설치하면 컴퓨터의 스캔이 시작되고 스캔 결과가 표시된다. 이러한 과정들은 사용자를 당황시키기 위한 가짜 화면이며 문제가 없어도 '오류가 검출되었습니다.'라고 표시된다.



스캔결과화면의 '복구' 버튼을 누르면 '구매' 버튼이 표시된다. 이 버튼을 누르면 소프트웨어의 구매화면으로 연결된다.



IPA에 들어오고 있는 상담의 내용은 크게 3가지로 분류된다.

(A) 경고 메시지를 보고 나니 불안하다.
(B) 모르는 사이에 스캔 화면이 표시되어 화면을 지우고 싶다.
(C) 컴퓨터를 스캔하는 소프트웨어가 삭제되지 않는다.

(A)에 대해서는 아무것도 하지 않는 것이 올바른 대처법이다. 경고 메시지는 웹 콘텐츠의 하나로, 컴퓨터에 이상이 있는 것이 아니다. 따라서 별도의 웹 페이지로 이동하거나, 웹 브라우저를 닫으면 더 이상 표시되지 않는다. (B)는 스캔 화면을 표시하는 소프트웨어가 이미 설치되어 있으므로 Windows의 제어판에서 삭제해야 한다. 삭제하려고 해도 삭제되지 않는 (C)의 경우, Windows의 '시스템 복원' 기능으로 소프트웨어가 설치되기 전의 상태로 돌려야 한다.

출처 : ITpro (http://itpro.nikkeibp.co.jp/atcl/news/15/020200374/)

알약 3월 보안동향보고서

Contact us

㈜이스트소프트 보안대응팀 Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr