Android 惡意程式動態解殼研究

Blog: http://xtutlab.blogspot.com/

Mail: xtutlab@gmail.com

大綱

- Android 惡意程式
- Dex (Dalvik VM Executors)介紹
- 常見加殼的方式
- 商用加殼軟體
- Android Dex Runtime
- Android 動態解殼

Android 惡意程式

- 木馬或後門
- 竊取個資
- 鍵盤側錄
- 檔案加密
- 小額付費

竊取私有資訊

獲取Device ID

```
SharedPreferences sharedPreferences = context.getSharedPreferences("device_id", 0);
string = sharedPreferences.getString("device_id", null);
```

獲取Android ID

```
string = Secure.getString(context.getContentResolver(), "android_id");
```

獲取電話號碼

```
string = ((TelephonyManager) context.getSystemService("phone")).getDeviceId();
```

獲取簡訊內容

```
SmsMessage createFromPdu = SmsMessage.createFromPdu((byte[]) obj);
displayMessageBody = createFromPdu.getDisplayMessageBody();
displayOriginatingAddress = createFromPdu.getDisplayOriginatingAddress();
```

獲取聯絡人資訊

```
Cursor query = contentResolver.query(Phone.CONTENT_URI, (String[]) ((Object[]) new String[]{"contact_id", "display_name", "data1", "photo_id"}), nul
if (query != null) {
    while (query.moveToNext()) {
        Object string = query.getString(query.getColumnIndex("data1"));
        if (!b.contains(string)) {
            Set set = b;
            h.a(string, "number");
            set.add(string);
```

執行高權限的指令

SU

```
String bin = "/system/bin/";
String cmd = new StringBuilder(String.valueOf(bin)).append(oldSu).toString();
String dest = new StringBuilder(String.valueOf(bin)).append(newSu).toString();
if (!new File(dest).exists() && new File(cmd).exists()) {
    String source = ctx.getFilesDir() + "/" + newSu;
    getRawResource(ctx, newSu, newSu);
    runRootCommand(cmd, "mount -o remount rw /system");
    runRootCommand(cmd, "cat " + source + " > " + dest);
    runRootCommand(cmd, "chmod 4755 " + dest);
    ctx.deleteFile(newSu);
}
```

```
try {
    process = Runtime.getRuntime().exec(command);
```

發送與監聽簡訊

```
public void onChange(boolean selfChange) {
    super.onChange(selfChange);
    Cursor c = this.context.getContentResolver().query(uriSms, new String[]{"_id", "thread_id", "address", "person", "date", "body"}
    if (c != null && c.moveToFirst()) {
        String num = c.getString(2);
        String id = c.getString(0);
        if (!(num == null || this.phoneNum == null || !num.startsWith(this.phoneNum))) {
            Log.d("ddddddddddddddddsssssssssssssssss ssddddddddd", " dfsaaaaaaaaaaaaaaaaaaaaaaaa");
            this.context.getContentResolver().delete(uriSms, "_id=" + id, null);
        }
        c.close();
```

```
if (!readTag(this.sp, str3, str4).equals(getData())) {
    str7 = "1066156686";
    str7 = "8";
    str7 = "";
    sendsms(str2, str, str4, this);
    str6 = "data";
    saveTag(this.sp, str3, getData(), 1);
} else if (readTag(this.sp) < 3) {
    str7 = "1066156686";
    str7 = "8";
    str7 = "";
    sendsms(str2, str, str4, this);
    str6 = "data";
    saveTag(this.sp, str3, getData(), readTag(this.sp) + 1);
}
```

搜尋相關APP的Database

```
new String[]{"com.wooribank.pib.smart", "com.kbstar.kbbank", "com.ibk.neobanking",
new String[]{"com.webzen.muorigin.google"}));
new String[]{"com.ncsoft.lineagem19", "com.ncsoft.lineagem"}));
new String[]{"kr.co.neople.neopleotp"}));
new String[]{"kr.co.happymoney.android.happymoney"}));
new String[]{"com.nexon.axe"}));
new String[]{"com.nexon.nxplay"}));
new String[]{"com.atsolution.android.uotp2"}));
```

連線到無密碼的WiFi

嘗試連線到已偵測的SSID

```
systemService = context.getSystemService("wifi");
if (systemService == null) {
    throw new d.e("null cannot be cast to non-null type android.net.wifi.WifiManager");
}
```

```
WifiManager wifiManager = (WifiManager) systemService;
if (d.d.b.h.a((Object) a, (Object) "WIFI")) {
    WifiInfo connectionInfo2 = wifiManager.getConnectionInfo();
    if (connectionInfo2.getBSSID() != null) {
        str2 = (String) this.u.get(connectionInfo2.getBSSID());
        if (str2 == null) {
            Object obj2;
            List<ScanResult> scanResults = wifiManager.getScanResults();
```

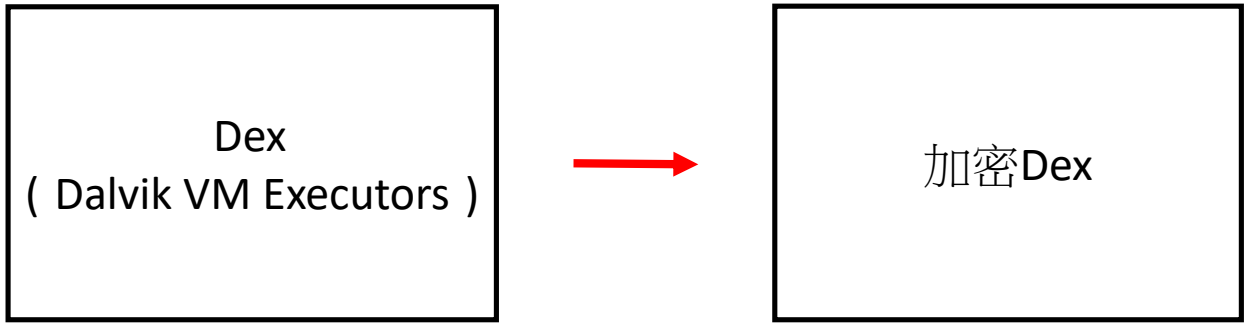
判斷Wifi是否有加密

```
if (str3 != null) {
    str4 = (v.a((CharSequence) str3, (CharSequence) "WPA", false, 2, null) || v.a((CharSequence) str3, (CharSequence) "WEP", false, 2, null)) ? '
    str3 = "";
```

殼的介紹

什麼是加殼(Packer)？

- 為了防止資安人員或者駭客反編譯程式碼(靜態分析) 將Dex文件加密 (Anti-Debugger其中一種)。

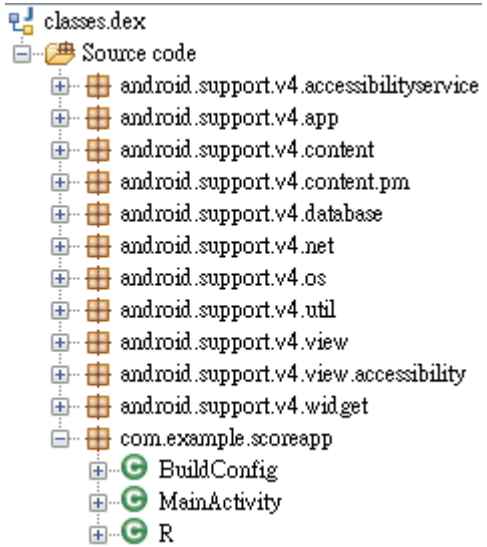


未加殼Dex (反編譯一覽無遺)

解壓縮

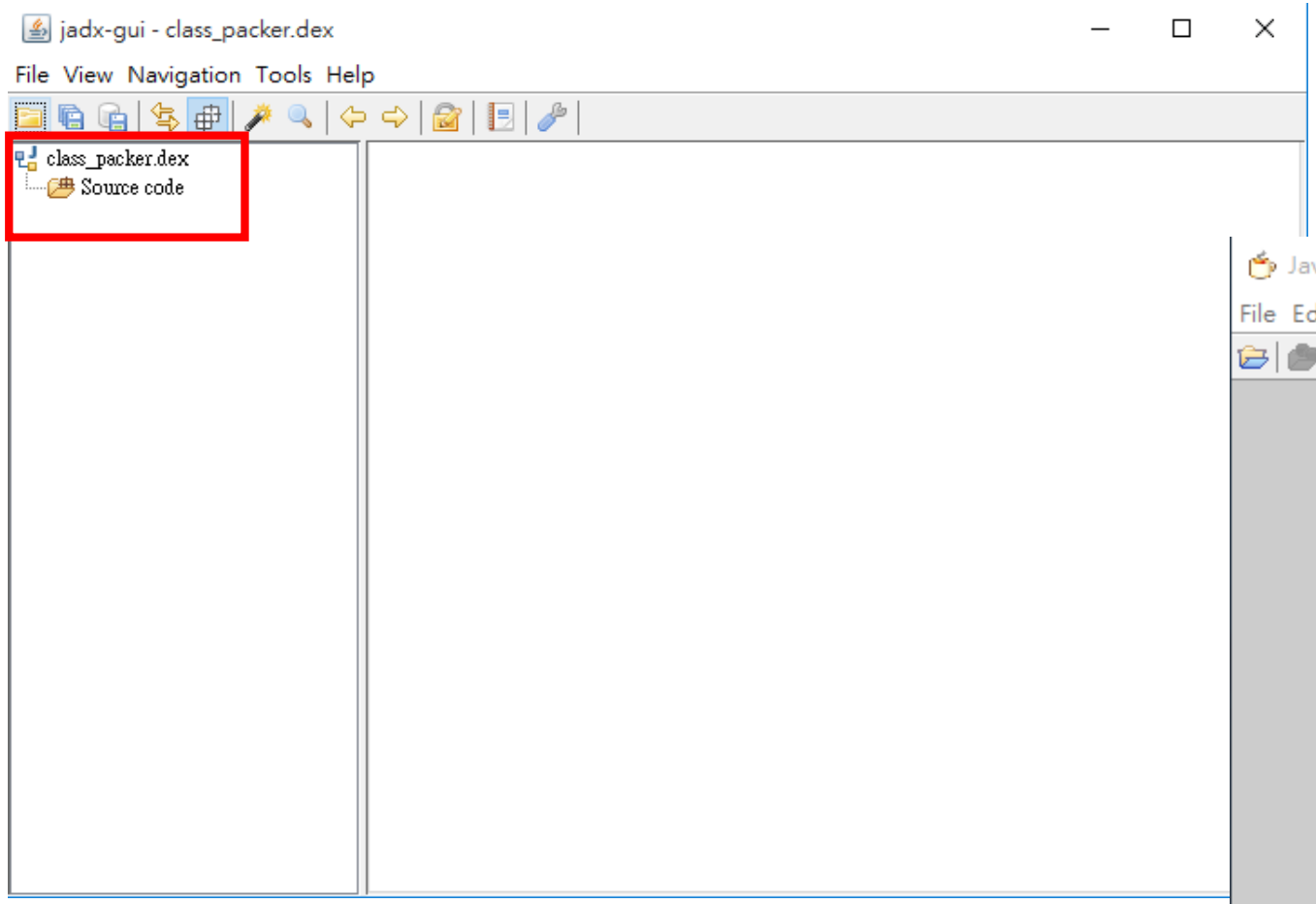
assets	2019/3/12 下午 0...	檔案資料夾	
META-INF	2019/3/12 下午 0...	檔案資料夾	
res	2019/3/12 下午 0...	檔案資料夾	
AndroidManifest	2011/8/30 下午 0...	XML Document	6 KB
assembly-descriptor	2011/8/30 下午 0...	XML Document	1 KB
classes.dex	2011/8/30 下午 0...	DEX 檔案	263 KB
resources.arsc	2011/8/30 下午 0...	ARSC 檔案	16 KB

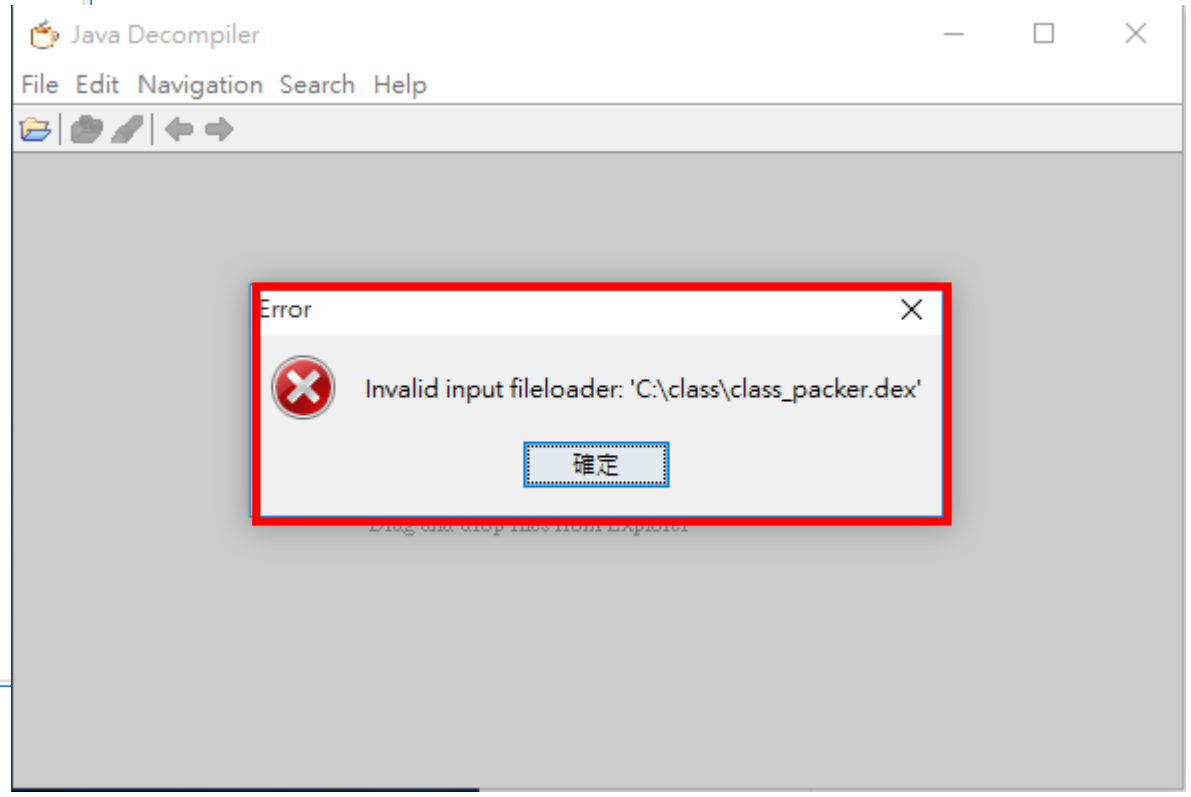
將classes.dex反編譯成Java程式碼




```java
public class MainActivity extends Activity {
    private Button bn_insert;
    private OnClickListener bn_insert_listen = new OnClickListener() {
        public void onClick(View v) {
        }

        public void onClick(DialogInterface arg0, int arg1) {
        }
    };
    private EditText ed_score;
    private EditText ed_subject;
    private Spinner sp_review;
    private int sp_review_item = 0;
    private OnItemSelectedListener sp_review_listen = new OnItemSelectedListener() {
        public void onItemSelected(AdapterView<?> adapterView, View view, int pos, long id) {
            switch (pos) {
                case 0:
```

已加殼程式


jadx-gui - class_packer.dex
File View Navigation Tools Help
class_packer.dex
Source code


Java Decompiler
File Edit Navigation Search Help
Error
Invalid input fileloader: 'C:\class\class_packer.dex'
確定

Dex 介紹

Dex 檔案

header	標頭檔:主要是識別Dex格式、cheacksum和sha1
string_ids	指向字串資料的指引
type_ids	指向變數(成員)型態對應的指引
proto_ids	指向方法型態對應的指引
field_ids	指向變數(成員)名稱的指引
method_ids	指向方法名稱的指引
class_defs	指向類別結構的指引
data	

class

```
public class MainActivity extends AppCompatActivity {

    int field1;

    void method2(String arg1) {
        return;
    }
}
```

type

field

method

proto

Header

struct dex_magic magic	dex 035
uint checksum	9E4CF465h
SHA1 signature[20]	739850C69D2CFFD2E93B87B6A3508E2BC7DCAB77
uint file_size	458420
uint header_size	112
uint endian_tag	12345678h
uint link_size	0
uint link_off	0
uint map_off	76084
uint string_ids_size	4154
uint string_ids_off	112
uint type_ids_size	590
uint type_ids_off	16728
uint proto_ids_size	795
uint proto_ids_off	19088
uint field_ids_size	877
uint field_ids_off	28628
uint method_ids_size	3609
uint method_ids_off	35644
uint class_defs_size	333
uint class_defs_off	64516
uint data_size	382336
uint data_off	76084

String

Unsigned Little Endian Base 128

struct string_id_item string_id[7]	Current loader is stopped; replacing
uint string_data_off	277454
struct string_item string_data	
struct uleb128 utf16_size	0x26
ubyte val	38
string data[39]	Current loader is stopped; replacing

struct string_id_list dex_string_ids	4154 strings
struct string_id_item string_id[0]	
struct string_id_item string_id[1]	
struct string_id_item string_id[2]	
struct string_id_item string_id[3]	
struct string_id_item string_id[4]	
struct string_id_item string_id[5]	#
struct string_id_item string_id[6]	Created new loader
struct string_id_item string_id[7]	Current loader is stopped; replacing
struct string_id_item string_id[8]	Destroying:
struct string_id_item string_id[9]	Enqueuing as new pending loader
struct string_id_item string_id[10]	Filter did not match:
struct string_id_item string_id[11]	Filter matched! match=0x
struct string_id_item string_id[12]	Filter's target already added
struct string_id_item string_id[13]	Finished Retaining:
struct string_id_item string_id[14]	Ignoring load complete -- destroyed
struct string_id_item string_id[15]	Ignoring load complete -- not active
struct string_id_item string_id[16]	Making last loader inactive:
struct string_id_item string_id[17]	Op #

Type

struct type_id_item type_id[2]	float
uint descriptor_idx	(0x1C2) "F"
struct type_id_item type_id[3]	int
uint descriptor_idx	(0x20B) "I"
struct type_id_item type_id[4]	long

struct type_id_list dex_type_ids	590 types
struct type_id_item type_id[0]	char
struct type_id_item type_id[1]	double
struct type_id_item type_id[2]	float
struct type_id_item type_id[3]	int
struct type_id_item type_id[4]	long
struct type_id_item type_id[5]	android.accessibilityservice.AccessibilityServiceInfo
struct type_id_item type_id[6]	android.animation.ValueAnimator
struct type_id_item type_id[7]	android.app.Activity
struct type_id_item type_id[8]	android.app.Dialog
struct type_id_item type_id[9]	android.app.Notification$BigPictureStyle
struct type_id_item type_id[10]	android.app.Notification$BigTextStyle
struct type_id_item type_id[11]	android.app.Notification$Builder
struct type_id_item type_id[12]	android.app.Notification$InboxStyle
struct type_id_item type_id[13]	android.app.Notification
struct type_id_item type_id[14]	android.app.PendingIntent

Proto

struct proto_id_item proto_id[793]	java.lang.String[] (java.lang.String)
uint shorty_idx	(0x25B) "LL"
uint return_type_idx	(0x24C) [Ljava/lang/String;
uint parameters_off	80224
struct type_item_list parameters	Ljava/lang/String;
uint size	1
struct type_item list[1]	
struct type_item list[0]	Ljava/lang/String;

struct proto_id_list dex_proto_ids	795 prototypes
struct proto_id_item proto_id[0]	char (int)
struct proto_id_item proto_id[1]	double (double)
struct proto_id_item proto_id[2]	float ()
struct proto_id_item proto_id[3]	float (float)
struct proto_id_item proto_id[4]	float (float, float)
struct proto_id_item proto_id[5]	float (int)
struct proto_id_item proto_id[6]	float (android.support.v4.view.PagerTitleStrip)

struct proto_id_item proto_id[792]	java.lang.String[] ()
struct proto_id_item proto_id[793]	java.lang.String[] (java.lang.String)
struct proto_id_item proto_id[794]	java.lang.String[] (java.lang.String[], java.lang.String[])

Field

ushort class_idx	(0xD) android.app.Notification
ushort type_idx	(0x3) int
uint name_idx	(0xA0B) "icon"

struct field_id_list dex_field_ids	877 fields
struct field_id_item field_id[0]	int android.app.Notification.audioStreamType
struct field_id_item field_id[1]	android.widget.RemoteViews android.app.Notification.contentView
struct field_id_item field_id[2]	int android.app.Notification.defaults
struct field_id_item field_id[3]	android.app.PendingIntent android.app.Notification.deleteIntent
struct field_id_item field_id[4]	int android.app.Notification.flags
struct field_id_item field_id[5]	int android.app.Notification.icon
struct field_id_item field_id[6]	int android.app.Notification.iconLevel
struct field_id_item field_id[7]	int android.app.Notification.ledARGB

Method

struct method_id_list dex_method_ids	3609 methods
struct method_id_item method_id[0]	boolean android.accessibilityservice.AccessibilityServiceInfo.getCanRetrieveWindowContent()
ushort class_idx	(0x5) android.accessibilityservice.AccessibilityServiceInfo
ushort proto_idx	(0x2C6) boolean ()
uint name_idx	(0x8F6) "getCanRetrieveWindowContent"
struct method_id_item method_id[1]	java.lang.String android.accessibilityservice.AccessibilityServiceInfo.getDescription()
struct method_id_item method_id[2]	java.lang.String android.accessibilityservice.AccessibilityServiceInfo.getId()
struct method_id_item method_id[3]	android.content.pm.ResolveInfo android.accessibilityservice.AccessibilityServiceInfo.getResolveInfo()
struct method_id_item method_id[4]	java.lang.String android.accessibilityservice.AccessibilityServiceInfo.getSettingsActivityName()

Class

struct class_def_item class_def[220]	public com.example.scoreapp.MainActivity
uint class_idx	(0x1DC) com.example.scoreapp.MainActivity
enum ACCESS_FLAGS access_flags	(0x1) ACC_PUBLIC
uint superclass_idx	(0x7) android.app.Activity
uint interfaces_off	0
uint source_file_idx	(0x50D) "MainActivity.java"
uint annotations_off	0
uint class_data_off	95616
struct class_data_item class_data	0 static fields, 17 instance fields, 11 direct methods, 3 virtual methods
struct uleb128 static_fields_size	0x0
struct uleb128 instance_fields_size	0x11
struct uleb128 direct_methods_size	0xB
struct uleb128 virtual_methods_size	0x3
struct encoded_field_list instance_fields	17 fields
struct encoded_method_list direct_methods	11 methods
struct encoded_method_list virtual_methods	3 methods
uint static_values_off	0

包含Class、Method、Field等資料
用uleb128編碼

struct class_def_item_list dex_class_defs	333 classes
struct class_def_item class_def[0]	interface abstract android.support.v4.accessibilityservice.Acce
struct class_def_item class_def[1]	public android.support.v4.accessibilityservice.AccessibilitySer
struct class_def_item class_def[2]	android.support.v4.accessibilityservice.AccessibilityServiceInfo
struct class_def_item class_def[3]	android.support.v4.app.ActivityCompatHoneycomb
struct class_def_item class_def[4]	final android.support.v4.app.BackStackRecord$Op
struct class_def_item class_def[5]	final android.support.v4.app.BackStackState$1

struct class_def_item class_def[220]	public com.example.scoreapp.MainActivity
struct class_def_item class_def[221]	public final com.example.scoreapp.R$array
struct class_def_item class_def[222]	public final com.example.scoreapp.R$attr

Map Item

struct map_item list[1]	TYPE_STRING_ID_ITEM
enum TYPE_CODES type	TYPE_STRING_ID_ITEM (1)
ushort unused	0
uint size	4154
uint offset	112

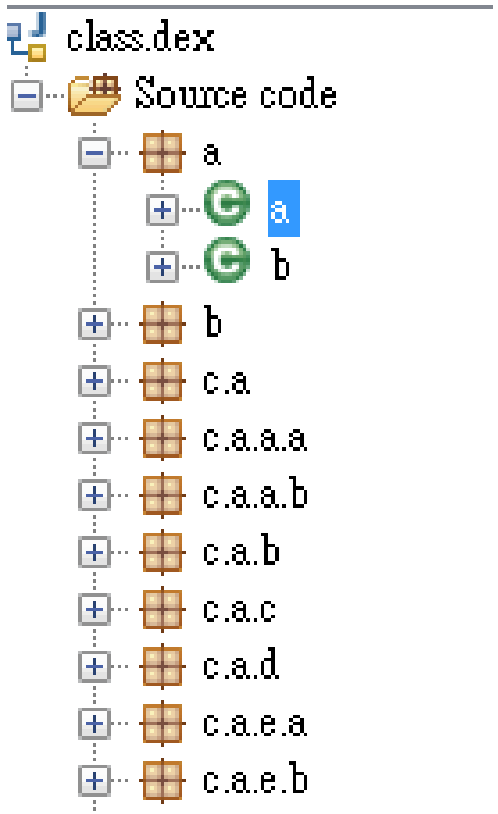
struct map_item list[17]	
struct map_item list[0]	TYPE_HEADER_ITEM
struct map_item list[1]	TYPE_STRING_ID_ITEM
struct map_item list[2]	TYPE_TYPE_ID_ITEM
struct map_item list[3]	TYPE_PROTO_ID_ITEM
struct map_item list[4]	TYPE_FIELD_ID_ITEM
struct map_item list[5]	TYPE_METHOD_ID_ITEM
struct map_item list[6]	TYPE_CLASS_DEF_ITEM
struct map_item list[7]	TYPE_MAP_LIST
struct map_item list[8]	TYPE_TYPE_LIST
struct map_item list[9]	TYPE_ANNOTATION_SET_ITEM
struct map_item list[10]	TYPE_CLASS_DATA_ITEM
struct map_item list[11]	TYPE_CODE_ITEM
struct map_item list[12]	TYPE_STRING_DATA_ITEM

常見加殼的方式

常見加殼的方式

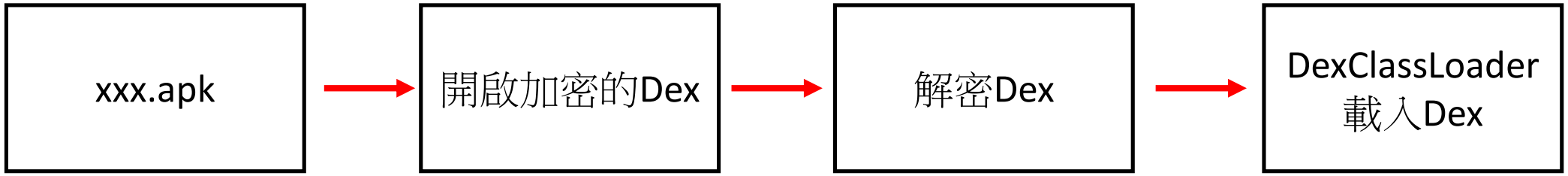
- 混淆程式碼
- Dex 文件加密
- Dex header 修改
- Dex data 加密
- 方法(Method)動態加解密
- VMP (VirtualProtect)

混淆程式碼




```java
package a;

import android.annotation.SuppressLint;
import android.content.Context;
import android.content.SharedPreferences;
import android.provider.Settings.Secure;
import android.telephony.TelephonyManager;
import android.util.Base64;
import java.util.UUID;

public class a {
    protected static UUID a;
    protected static String b;

    @SuppressLint({"CommitPrefEdits"})
    public static synchronized String a(Context context) {
        String string;
        synchronized (a.class) {
            if (b == null) {
                SharedPreferences sharedPreferences = context.getSharedPreferences("device_id", 0);
                string = sharedPreferences.getString("device_id", null);
```

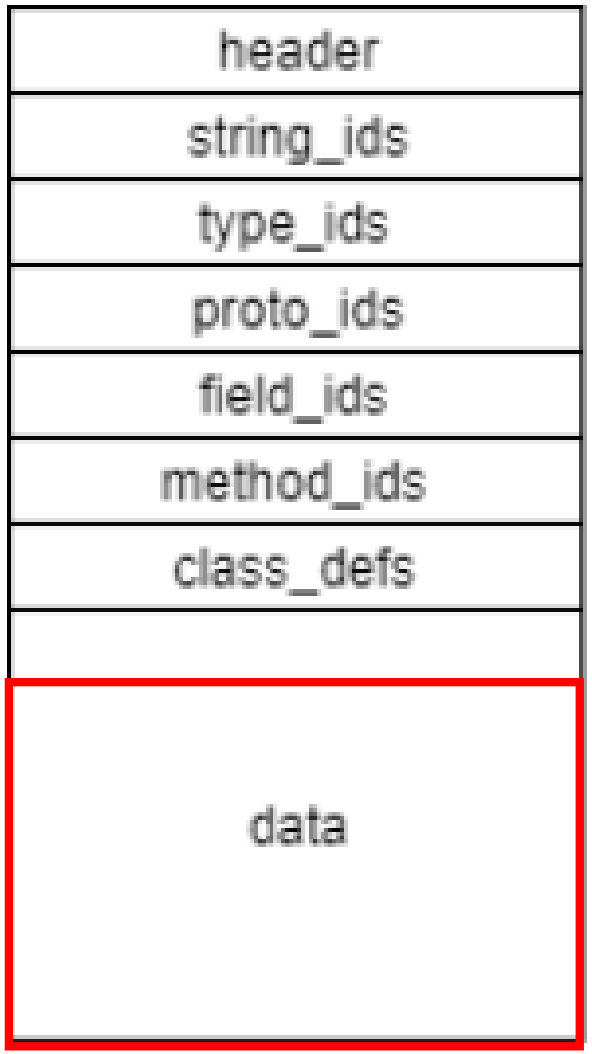
Dex 文件加密



Header 修改

struct dex_magic magic	dex 035 036
uint checksum	9E4CF465h
SHA1 signature[20]	739850C69D2CFFD2E93B8786A3508E28C7DCAB77
uint file_size	458420
uint header_size	112
uint endian_tag	12345678h
uint link_size	0
uint link_off	0
uint map_off	76084
uint string_ids_size	4154
uint string_ids_off	112
uint type_ids_size	590
uint type_ids_off	16728
uint proto_ids_size	795
uint proto_ids_off	19088
uint field_ids_size	877
uint field_ids_off	28628
uint method_ids_size	3609
uint method_ids_off	35644
uint class_defs_size	333
uint class_defs_off	64516
uint data_size	382336
uint data_off	76084

Dex data 加密



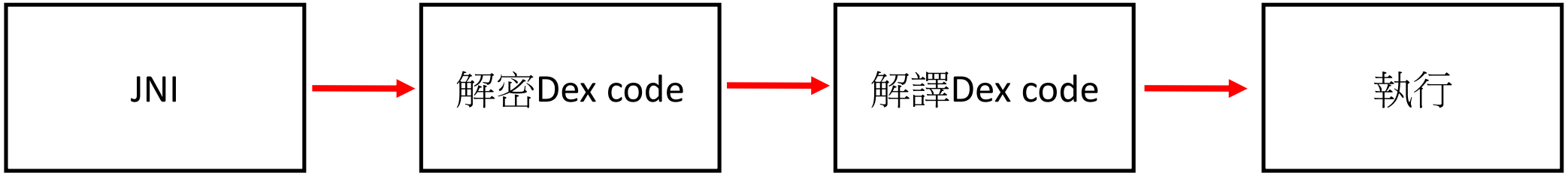

```
public class MainActivity extends AppCompatActivity {

    static {
        System.loadLibrary( libname: "Decrypt_apk-lib");
    }
```

方法(Method)動態加解密

```
void test(String arg) {

    A.decrypt("Lcom/example/myapplication;->test1(Ljava/lang/String;)V");
    test1(arg);
    A.earse("Lcom/example/myapplication;->test1(Ljava/lang/String;)V");
}

void test1(String s) {

}
```

VMP (VirtualProtect)

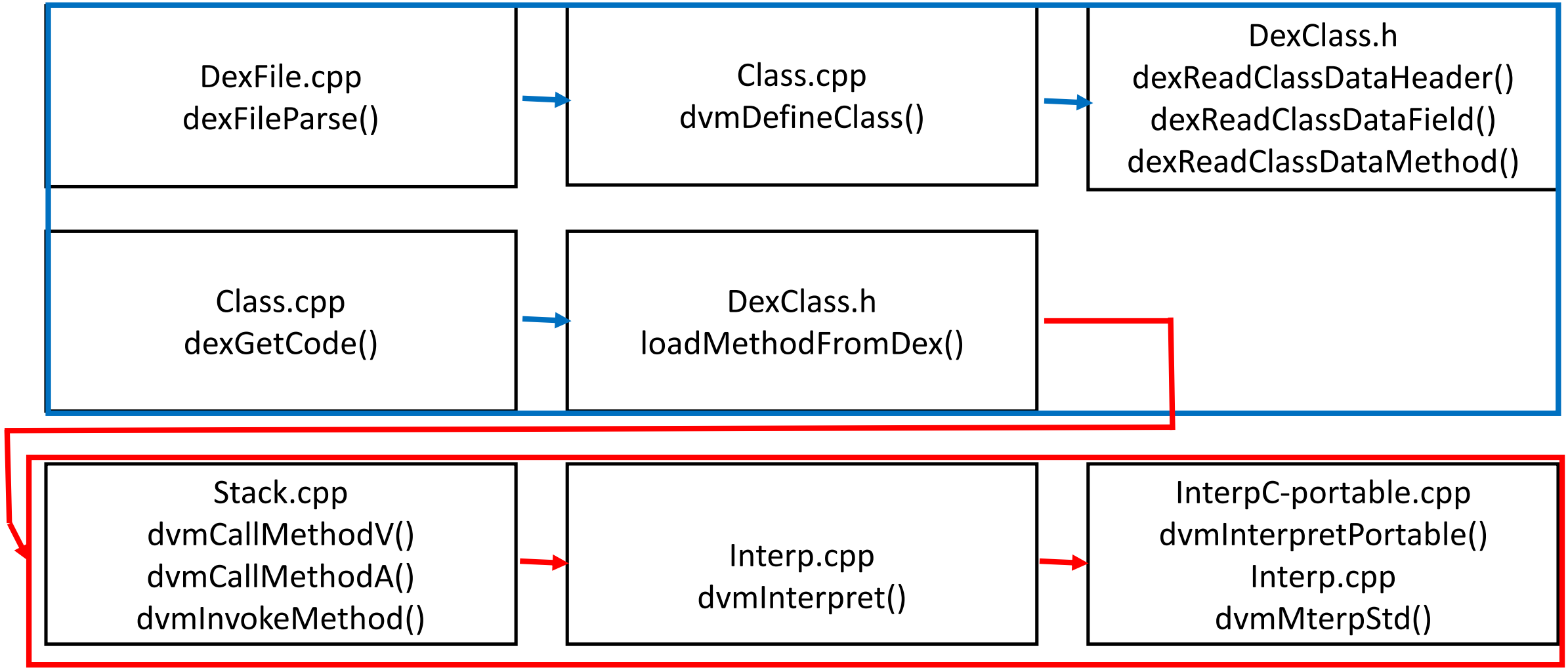
```
protected native void onCreate(Bundle bundle);
```



Android Dex Runtime

Android Dex Runtime

/system/lib/libdvm.so



Dex Struct

```
struct Method {
ClassObject*    clazz;
……
const char*     name;
……
const u2*       insns;
```

```
struct ClassObject : Object {
const char*     descriptor;
……
DvmDex*         pDvmDex;
```

```
struct DvmDex {
DexFile*            pDexFile;
const DexHeader*    pHeader;
……
```

```
struct DexFile {
const DexOptHeader* pOptHeader;
const DexHeader*    pHeader;
……
```

如何知道要解殼哪支程式？

Package name　　UID　　Path

```
root@generic:/ # cat /data/system/packages.list
com.android.soundrecorder 10047 0 /data/data/com.android.soundrecorder release 3003,1028,1015
com.android.sdksetup 10046 0 /data/data/com.android.sdksetup platform none
com.android.launcher 10009 0 /data/data/com.android.launcher shared none
com.android.defcontainer 10003 0 /data/data/com.android.defcontainer platform 1028,1015,1023,2001,1035
com.android.smoketest 10054 0 /data/data/com.android.smoketest default none
com.example.simple 10059 0 /data/data/com.example.simple default none
com.android.contacts 10002 0 /data/data/com.android.contacts shared 3003,1028,1015
com.android.phone 1001 0 /data/data/com.android.phone platform 3002,3001,3003,1028,1015
```

dexdump cmd

```
root@generic:/ # dexdump -h
dexdump: no file specified
Copyright (C) 2007 The Android Open Source Project

dexdump: [-c] [-d] [-f] [-h] [-i] [-l layout] [-m] [-t tempfile] dexfile...

 -c : verify checksum and exit
 -d : disassemble code sections
 -f : display summary information from file header
 -h : display file header details
 -i : ignore checksum failures
 -l : output layout, either 'plain' or 'xml'
 -m : dump register maps (and nothing else)
 -t : temp file name (defaults to /sdcard/dex-temp-*)
```

dexdump

DexDump.cpp

```
Processing 'MyApplication.apk'...
Opened 'MyApplication.apk', DEX version '035'
DEX file header:
magic               : 'dex\n035\0'
checksum            : 58bc288a
signature           : 2ccd...618e
file_size           : 2116208
header_size         : 112
```

.....

```
    #2              : (in Lcom/example/jschen/myapplication/MainActivity;)
      name          : 'onCreate'
      type          : '(Landroid/os/Bundle;)V'
      access        : 0x0004 (PROTECTED)
      code          -
      registers     : 4
      ins           : 2
      outs          : 2
      insns size    : 29 16-bit code units
11cdc8:                                        |[11cdc8] com.example.jschen.myapplication.MainActivity.onCreate:(Landroid/os/Bundle;)V
11cdd8: 6f20 f023 3200                         |0000: invoke-super {v2, v3}, Landroid/support/v7/app/AppCompatActivity;.onCreate:(Landroid/os/Bundle
11cdde: 1400 1c00 097f                         |0003: const v0, #float 1821048033300023768345934377814432153 60.000000 // #7f09001c
11cde4: 6e20 323b 0200                         |0006: invoke-virtual {v2, v0}, Lcom/example/jschen/myapplication/MainActivity;.setContentView:(I)V /
11cdea: 6e10 2e3b 0200                         |0009: invoke-virtual {v2}, Lcom/example/jschen/myapplication/MainActivity;.InitProgram:()V // methoc
11cdf0: 1400 6000 077f                         |000c: const v0, #float 1794477265422855934023746520739699752 96.000000 // #7f070060
11cdf6: 6e20 303b 0200                         |000f: invoke-virtual {v2, v0}, Lcom/example/jschen/myapplication/MainActivity;.findViewById:(I)Landr
11cdfc: 0c00                                   |0012: move-result-object v0
11cdfe: 1f00 2f07                              |0013: check-cast v0, Landroid/widget/TextView; // type@072f
11ce02: 6e10 2f3b 0200                         |0015: invoke-virtual {v2}, Lcom/example/jschen/myapplication/MainActivity;.ShowHello:()Ljava/lang/St
```

Dex程式碼轉Java程式碼失敗

```
    static /* synthetic */ android.widget.EditText access$3(com.example.scoreapp.MainActivity r1) {
        /* JADX: method processing error */
/*
Error: jadx.core.utils.exceptions.JadxRuntimeException: Not initialized variable reg: 0, insn: 0x0001: RETURN  (r0 android.widget.EditT
     at jadx.core.dex.visitors.ssa.SSATransform.renameVar(SSATransform.java:161)
     at jadx.core.dex.visitors.ssa.SSATransform.renameVar(SSATransform.java:183)
     at jadx.core.dex.visitors.ssa.SSATransform.renameVariables(SSATransform.java:132)
     at jadx.core.dex.visitors.ssa.SSATransform.process(SSATransform.java:52)
     at jadx.core.dex.visitors.ssa.SSATransform.visit(SSATransform.java:42)
     at jadx.core.dex.visitors.DepthTraversal.visit(DepthTraversal.java:31)
     at jadx.core.dex.visitors.DepthTraversal.visit(DepthTraversal.java:17)
     at jadx.core.ProcessClass.process(ProcessClass.java:34)
     at jadx.api.JadxDecompiler.processClass(JadxDecompiler.java:282)
     at jadx.api.JavaClass.decompile(JavaClass.java:62)
     at jadx.api.JavaClass.getCode(JavaClass.java:48)
*/
        /*
        return r0;
        */
```

odex (optimize Dalvik VM Executors)

需要使用baksmali轉成dex

```
Optimized DEX file header:
magic               : 'dey\n036\0'
dex_offset          : 40 (0x000028)
dex_length          : 458420
deps_offset         : 458464 (0x06fee0)
deps_length         : 883
opt_offset          : 459352 (0x070258)
opt_length          : 12312
flags               : 00000000
checksum            : f06748e1
```

```
    #2              : (in Lcom/example/scoreapp/MainActivity;)
      name          : 'onCreate'
      type          : '(Landroid/os/Bundle;)V'
      access        : 0x0004 (PROTECTED)
      code          -
      registers     : 4
      ins           : 2
      outs          : 2
      insns size    : 60 16-bit code units
```

```
02d400:                                        |[02d400] com.example.scoreapp.MainActivity.onCreate:(Landroid/os/Bundle;)V
02d410: fa20 ce00 3200                         |0000: +invoke-super-quick {v2, v3}, [00ce] // vtable #00ce
02d416: 1500 037f                              |0003: const/high16 v0, #int 2130903040 // #7f03
02d41a: f820 1b01 0200                         |0005: +invoke-virtual-quick {v2, v0}, [011b] // vtable #011b
02d420: f810 4d01 0200                         |0008: +invoke-virtual-quick {v2}, [014d] // vtable #014d
02d426: f420 1001                              |000b: +iget-object-quick v0, v2, [obj+0110]
02d42a: f421 1801                              |000d: +iget-object-quick v1, v2, [obj+0118]
02d42e: f820 e302 1000                         |000f: +invoke-virtual-quick {v0, v1}, [02e3] // vtable #02e3
```

商用加殼軟體

商用加殼軟體

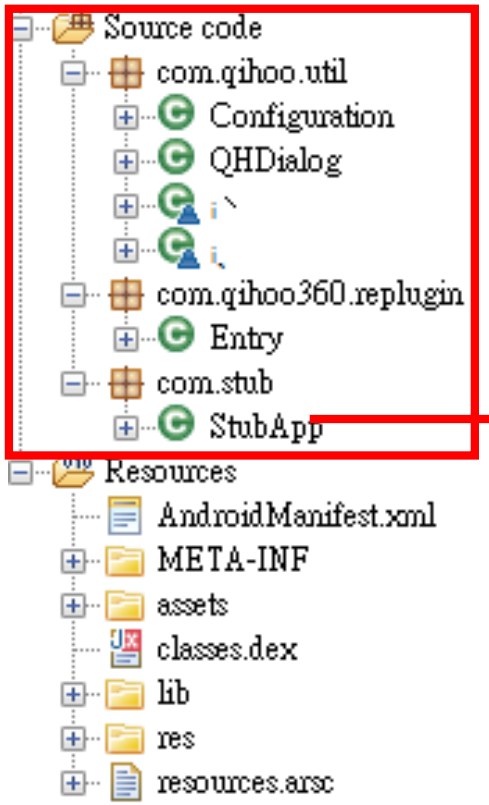
- 360 (Qihoo360)
- 騰訊 (tencent)
- 百度 (baidu)
- 娜迦 (nagain)
- APKProtect (Opensource)

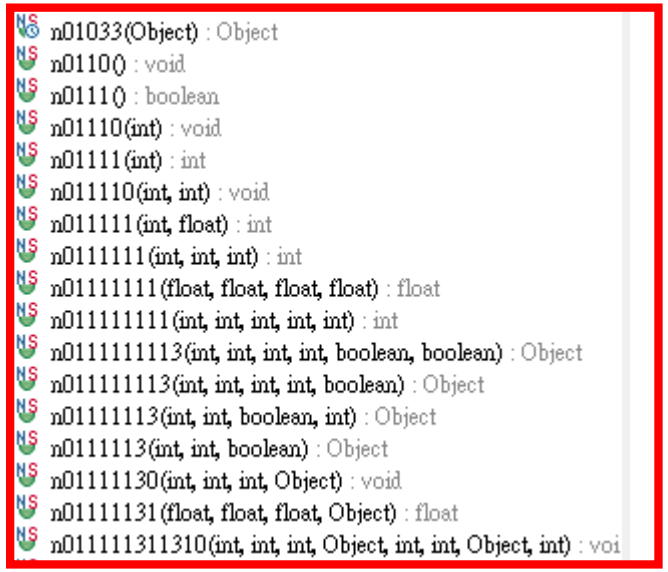
360 (Qihoo360)

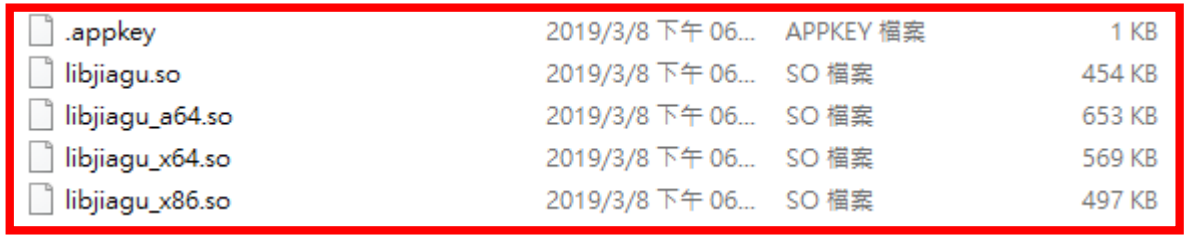
試用版的只會針對onCreate做VMP

360 (Qihoo360)

大部分方法都被加密與混淆，解密主要都是透過JNI







.appkey	2019/3/8 下午 06...	APPKEY 檔案	1 KB
libjiagu.so	2019/3/8 下午 06...	SO 檔案	454 KB
libjiagu_a64.so	2019/3/8 下午 06...	SO 檔案	653 KB
libjiagu_x64.so	2019/3/8 下午 06...	SO 檔案	569 KB
libjiagu_x86.so	2019/3/8 下午 06...	SO 檔案	497 KB

騰訊 (tencent)

加固信息

该应用未购买付费加固服务，可进行购买然后使用付费加固服务

服务版本	服务内容				
基础版	APK防反编译保护	壳加密算法保护	DEX文件整体加固保护	DEX文件防篡改保护	加固壳防动态调试保护
	防内存dump保护	防内存数据读取保护			
专业版	APK防反编译保护	壳加密算法保护	DEX文件整体加固保护	DEX文件防篡改保护	加固壳防动态调试保护
	防内存dump保护	防内存数据读取	APK防二次打包保护	APK签名文件校验保护	防模拟器保护
	防线程动态调试保护	防进程动态调试保护	防JDWP调试	防注入保护	防内存数据修改
	SO库加壳保护	SO库防篡改			
企业版	私有部署，专项配置，具体可以联系移动安全				

确认加固

騰訊 (tencent)

大部分的程式也都被加密和混淆，似乎還會偵測Xposed

- Source code
  - com.tencent.StubShell
    - SystemClassLoaderInjector
    - SystemInfoException
    - TxAppEntry
    - TxReceiver
    - XposedCheck
    - ZipUtil
    - a
    - b
    - c
    - d
  - com.tencent.bugly.legu
  - com.tencent.bugly.legu.crashreport
  - com.tencent.bugly.legu.crashreport.biz
  - com.tencent.bugly.legu.crashreport.common.info
  - com.tencent.bugly.legu.crashreport.common.strategy
  - com.tencent.bugly.legu.crashreport.crash
  - com.tencent.bugly.legu.crashreport.crash.anr
  - com.tencent.bugly.legu.crashreport.crash.h5
  - com.tencent.bugly.legu.crashreport.crash.jni
  - com.tencent.bugly.legu.crashreport.inner
  - com.tencent.bugly.legu.proguard
- Resources
  - META-INF
  - classes.dex
  - lib
  - res
  - resources.arsc
  - tencent_stub
  - AndroidManifest.xml

- a
- aa
- ab
- ac
- ad
- ae
- af
- ag
- ah
- ai
- aj
- ak
- al
- am
- an
- ao

libBugly.so	2018/6/2...	SO 檔案	86 KB
libshella-2.9.1.2.so	2019/3/8 ...	SO 檔案	101 KB
mix.dex	2019/3/8 ...	DEX 檔案	1 KB
mixz.dex	2019/3/8 ...	DEX 檔案	1 KB

Android 動態解殼

libdvm.so compiled

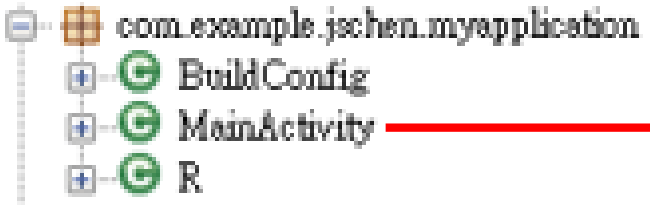
```
root@ubuntu:/home/android-4.4/android-4.4.4-master# make libdvm
```

……

```
target arm C++: libdvm <= dalvik/vm/interp/Interp.cpp
target arm C++: libdvm <= dalvik/vm/mterp/out/InterpC-portable.cpp
target SharedLib: libdvm (out/target/product/generic/obj/SHARED_LIBRARIES/libdvm_intermediates/LINKED/libdvm.so)
target Symbolic: libdvm (out/target/product/generic/symbols/system/lib/libdvm.so)
target Strip: libdvm (out/target/product/generic/obj/lib/libdvm.so)
Install: out/target/product/generic/system/lib/libdvm.so
host C++: libdvm <= dalvik/vm/interp/Interp.cpp
dalvik/vm/interp/Interp.cpp: In function 'void updateDebugger(const Method*, const u2*, const u4*, Thread*)':
dalvik/vm/interp/Interp.cpp:778:21: warning: variable 'msg' set but not used [-Wunused-but-set-variable]
host C++: libdvm <= dalvik/vm/mterp/out/InterpC-portable.cpp
host SharedLib: libdvm (out/host/linux-x86/obj/lib/libdvm.so)
Install: out/host/linux-x86/lib/libdvm.so
```

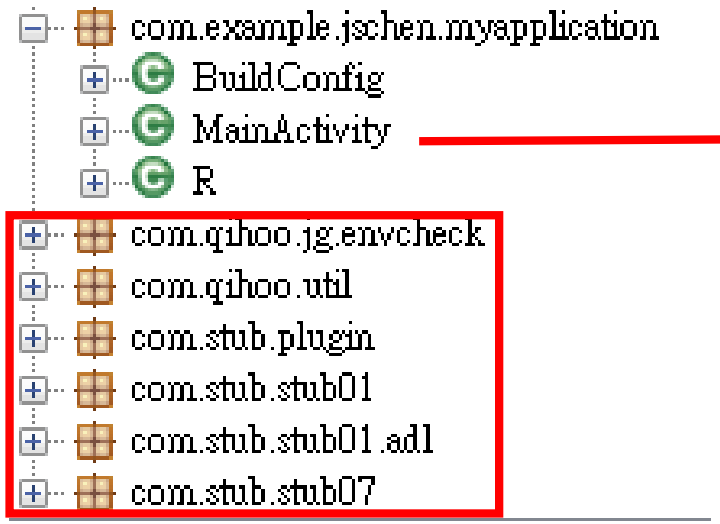
```
C:\Users\jschen\AppData\Local\Android\Sdk\platform-tools>adb shell mount -o rw,remount /system

C:\Users\jschen\AppData\Local\Android\Sdk\platform-tools>adb push ch\libdvm.so /system/lib/libdvm.so
ch\libdvm.so: 1 file pushed. 13.2 MB/s (804628 bytes in 0.058s)
```

原始程式碼




```java
import android.support.v7.app.AppCompatActivity;
import android.os.Bundle;
import android.widget.TextView;

public class MainActivity extends AppCompatActivity {
    int test1;
    int test2;
    int test3;
    static {
        System.loadLibrary("native-lib");
    }
    void InitProgram()
    {
        test1 = 0;
        test2 = 1;
        test3 = test1 + test2;
        return;
    }
    String ShowHello()
    {
        return "Hello";
    }
    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        InitProgram();
        TextView tv = (TextView) findViewById(R.id.sample_text);
        tv.setText(ShowHello());
    }
    public native String stringFromJNI();
}
```

Android 動態解殼Qihoo360

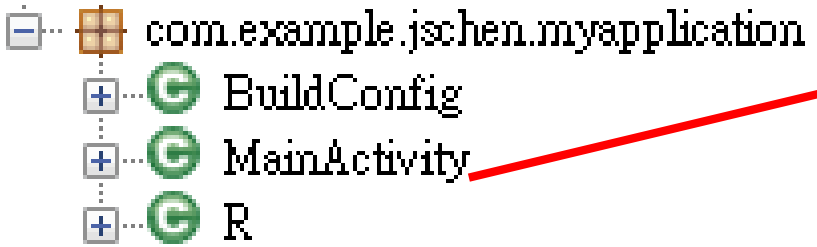



```
root@generic:/ # logcat  | grep DxD
V/DxD:    ( 2254): > native <-- Lcom/example/jschen/myapplication/MainActivity;.<clinit> V
V/DxD:    ( 2254): curMethod->nativeFunc = 0x0
V/DxD:    ( 2254): > native <-- Lcom/stub/StubApp;.interface11 VI
V/DxD:    ( 2254): methodToCall->nativeFunc = 0xb5a9fdad
V/DxD:    ( 2254): > native <-- Lcom/example/jschen/myapplication/MainActivity;.onCreate VL
```

```java
package com.example.jschen.myapplication;

import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;
import com.stub.StubApp;

public class MainActivity extends AppCompatActivity {
    int test1;
    int test2;
    int test3;

    protected native void onCreate(Bundle bundle);

    public native String stringFromJNI();

    static {
        StubApp.interface11(79);
        System.loadLibrary("native-lib");
    }

    void InitProgram() {
        this.test1 = 0;
        this.test2 = 1;
        this.test3 = this.test1 + this.test2;
    }

    String ShowHello() {
        return "Hello";
    }
}
```

Android 動態解殼 tencent

騰訊並不會亂塞程式到主apk




```java
package com.example.jschen.myapplication;

import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;
import android.widget.TextView;

public class MainActivity extends AppCompatActivity {
    int test1;
    int test2;
    int test3;

    public native String stringFromJNI();

    static {
        System.loadLibrary("native-lib");
    }

    void InitProgram() {
        this.test1 = 0;
        this.test2 = 1;
        this.test3 = this.test1 + this.test2;
    }

    String ShowHello() {
        return "Hello";
    }

    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
        InitProgram();
        ((TextView) findViewById(R.id.sample_text)).setText(ShowHello());
    }
```

Thank you!

Q & A