

# 行動APP安全分析與防護

果核數位技術顧問  
連振道 Eric

# Agenda

- 講師介紹
- APP安全分析
  - 靜態分析
  - 外掛破解
  - 動態注入
  - 實例影片
- APP安全防護
  - 防護重點
  - 解決辦法
- 結語

# 講師介紹



連振道 Eric Lien

- NCTU Applied Mathematics
- 6 years engineer experience
- C/C++、Java、PHP、Python
- Reverse Engineering
- Have protected over a hundred of Apps

# APP安全分析

# 分析需要:

APK

Android逆向助手

JD-GUI

ILSpy +Reflexil或dnspy

IDA-Pro

## 邏輯分析能力以及一些知識

(程式語言、中間語言、組合語言等)

### 其他輔助工具:

Root手機或手機模擬器

HxD HEX Editor

Dalvik Bytecode Editor

rootexplore

Xposed installer、Cydia substrate

Lucky Patcher

....










# 靜態分析實例:旅行青蛙

Google Play 旅かえる

應用程式 搜尋結果 Android 應用程式 所有價格 不限評分

我的應用程式 購物 遊戲 家庭 編輯精選 帳戶 我的訂閱內容 兌換 我的願望清單 我的 Play 動態 家長指南

應用程式

|   |  |  |   |  |
|---|--|--|---|--|
|  <p>旅かえる<br/>Hit-Point Co.,Ltd.<br/>★★★★★ 免費</p> |  <p>漢化中文版攻略for<br/>cherisher<br/>★★★★★ 免費</p> |  <p>漢化中文版助手 for<br/>廈門漫的信息技术有限<br/>★★★★★ 免費</p> |  <p>旅行青蛙 (旅かえる)<br/>arteoning<br/>★★★★★ 免費</p> |  <p>青蛙旅行(中文漢化)<br/>VEGA STUDIO<br/>★★★★★ 免費</p> |
|  <p>攻略 for 旅行青蛙<br/>momdream</p>               |  <p>Guide for Tabikaeru<br/>Mey Media</p>   |  <p>貓咪公寓 - Cat Conc<br/>Zepni Ltd.</p>        |  <p>Tabikaeru (旅かえる)<br/>To Be Honest</p>    |  <p>青蛙旅行-欢乐跳一<br/>Hangzhou Yanguo Tech</p>    |

# 不同平台流竄修改APK、破解APK

木間益智 [下載] 【漢化版】旅行青蛙 v1.0.5 最新中文版! [複製連結]

觀看: 8346 | 回覆: 29 | 好評: 0



even9090

收聽TA

只看該作者

只看大圖

倒序瀏覽

樓主

電梯直達

閱讀模式

網機器人 A3

我的動享

發表於 2018-2-7 10:11

下載

手機型號: OPPO R9

作業系統: Android 6.X

本帖最後由 even9090 於 2018-2-8 18:45 編輯



【軟體名稱】

旅行青蛙 漢化版



【語言】: 中文版

【版本資訊】: V1.0.4.1

【軟體大小】: 57.9MB

【更新日期】: 2018-01-30

【使用權限】: 免費, 已修改, 可不需連網, 免ROOT

【系統支援】: 支持 Android 4.1 以上

【修改作者】: 互联网【檔案來源】: <http://a.4399.cn>

【遊戲介紹】: 旅行青蛙真是最近的熱門遊戲, 說真的不知道可以紅多久, 不過真的很紅啊!! 只是日文的遊戲大家多少還是有點障礙, 若是旅行青蛙中文版我想大家應該會比較熟悉一點

【修改內容】:

1. 無限三葉草
2. 無限抽獎卷

3. 中文版新增: 中文版(無修改)載點

"載點失效已修正"

# 編譯

VS

# 反編譯

C#

Compile

IL(Intermediate Language)

Assemble

CLR(Common Language Runtime)/JIT

```
01001101011011010  
11011010010111000  
10111000101110001  
00000010000110110  
10000110111101100  
01101101111011011  
00011000010111010  
00110010100100001
```



ILSpy

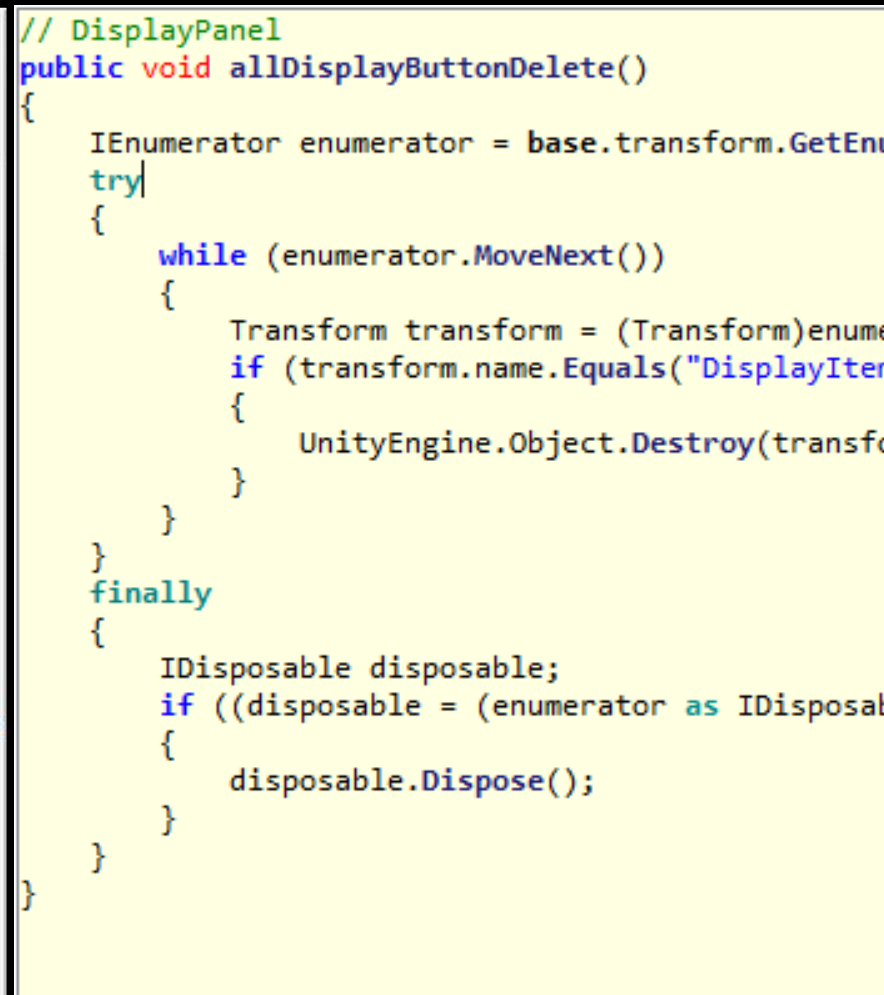
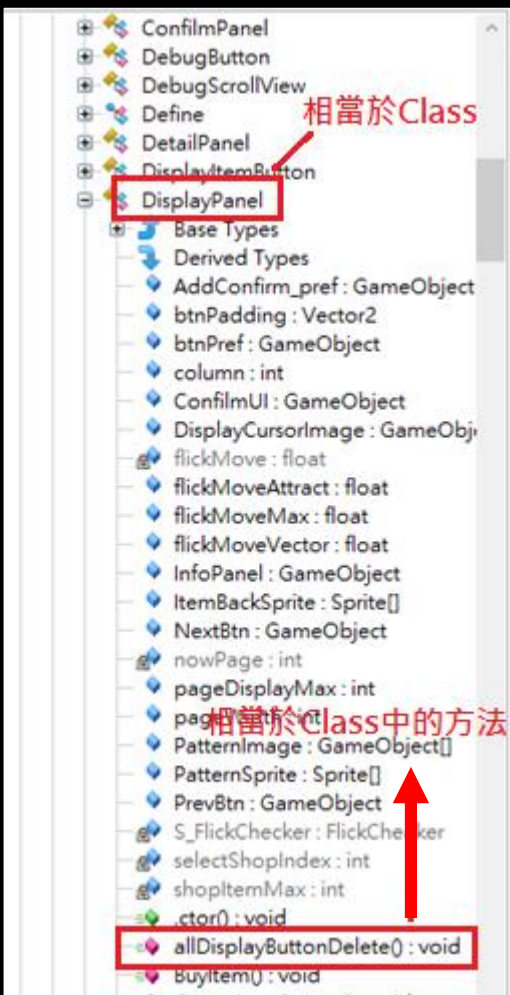
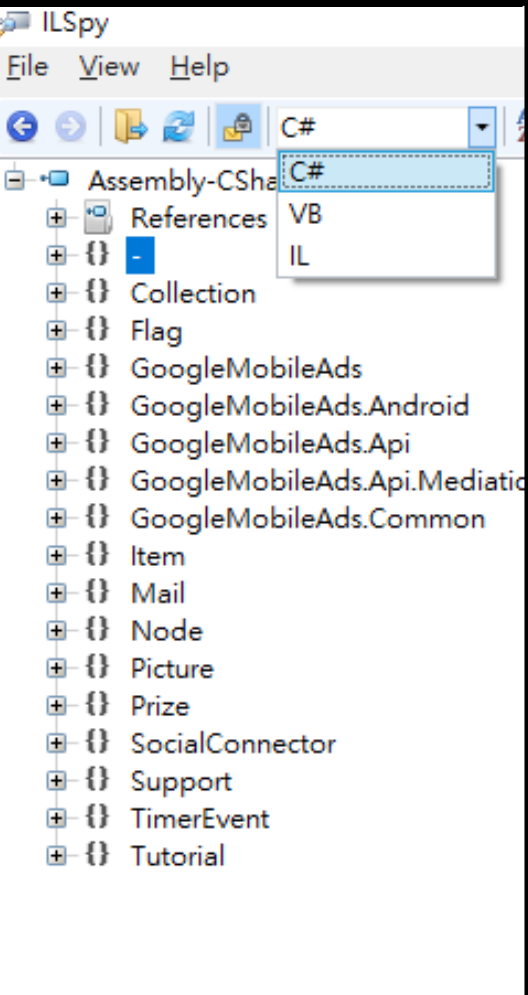
decompile



Unity3D遊戲(旅行青蛙)  
Assembly-CSharp.dll



# C#程式碼



# 1. 逆向分析(中文化翻譯)

```
{
    this.BuyItem();
});
confilm.ResetOnClick_No();
confilm.SetOnClick_No(delegate
{
    confilm.ClosePanel();
});
confilm.SetOnClick_No(delegate
{
    this.GetComponent<FlickCheaker>().stopFlick(false);
});
}
else
{
    base.GetComponent<FlickCheaker>().stopFlick(true);
    ConfilmPanel confilm = this.ConfilmUI.GetComponent<ConfilmPanel>();
    confilm.OpenPanel("持有物品已達上限");
    confilm.ResetOnClick_Screen();
    confilm.SetOnClick_Screen(delegate
    {
        confilm.ClosePanel();
    });
    confilm.SetOnClick_Screen(delegate
    {
        this.GetComponent<FlickCheaker>().stopFlick(false);
    });
}
}
else
{
    base.GetComponent<FlickCheaker>().stopFlick(true);
    ConfilmPanel confilm = this.ConfilmUI.GetComponent<ConfilmPanel>();
    confilm.OpenPanel("三葉草不足");
    confilm.ResetOnClick_Screen();
    confilm.SetOnClick_Screen(delegate
```

# 修改IL code(ILspy+Reflexil)

1.

```
base.GetComponent<FlickCheaker>().stopFlick(true);
ConfilmPanel confilm = this.ConfilmUI.GetComponent<ConfilmPanel>();
confilm.OpenPanel("みつ葉が足りません");
confilm.ResetOnClick_Screen();
confilm.SetOnClick_Screen(delegate
{
    confilm.ClosePanel();
});
confilm.SetOnClick_Screen(delegate
```

2.

修改成翻譯的中文字串

| Instructions | Variables | Parameters |          |   |
|--------------|-----------|------------|----------|---|
|              | Offset    | OpCode     |          |   |
|              | 210       | 709        | callvirt |   |
|              | 211       | 714        | stfld    |   |
|              | 212       | 719        | ldloc.s  |   |
|              | 213       | 721        | ldfld    | ConfilmPanel DisplayPanel/<SetInfoPanelData>c__AnonStorey3::confilm |
| ▶            | 214       | 726        | ldstr    | みつ葉が足りません   |
|              | 215       | 731        | callvirt | System.Void ConfilmPanel::OpenPanel(System.String)                  |
|              | 216       | 736        | ldloc.s  | -> (4) (DisplayPanel/<SetInfoPanelData>c__AnonStorey3)              |
|              | 217       | 738        | ldfld    | ConfilmPanel DisplayPanel/<SetInfoPanelData>c__AnonStorey3::confilm |
|              | 218       | 743        | callvirt | System.Void ConfilmPanel::ResetOnClick_Screen()                     |
|              | 219       | 748        | ldloc.s  | -> (4) (DisplayPanel/<SetInfoPanelData>c__AnonStorey3)              |
|              | 220       | 750        | ldfld    | ConfilmPanel DisplayPanel/<SetInfoPanelData>c__AnonStorey3::confilm |

# 2. 逆向分析(修改重要函數)

Before

```
// SuperGameMaster
public static int CloverPointStock()
{
    return SuperGameMaster.saveData.CloverPoint;
}
```

Sebastien Lebreton's Reflexil v2.1  
Method definition

Instructions Variables Parameters Exception Handlers Overrides Attributes Custom attributes

|     | Offset | OpCode | Operand                                  |
|-----|--------|--------|--|
| ▶ 0 | 0      | ldsfld | SaveDataFormat SuperGameMaster::saveData |
| 1   | 5      | ldfld  | System.Int32 SaveDataFormat::CloverPoint |
| 2   | 10     | ret    |  |

After

```
// SuperGameMaster
public static int CloverPointStock()
{
    return 999999;
}
```

Sebastien Lebreton's Reflexil v2.1  
Method definition

Instructions Variables Parameters Exception Handlers Overrides Attributes Custom attributes

|     | Offset | OpCode | Operand |
|-----|--------|--------|---------|
| ▶ 0 | 0      | ldc.i4 | 999999  |
| 1   | 5      | ret    |         |

```
if (SuperGameMaster.CloverPointStock() >= itemDataFormat.price)
{
    if (SuperGameMaster.FindItemStock(shopDataFormat.itemId) < 99)
    {
        base.GetComponent<FlickCheaker>().stopFlick(true);
        ConfilmPanel confilm = this.ConfilmUI.GetComponent<ConfilmPanel>();
        if (itemDataFormat.type == Item.Type.LunchBox)
        {
            confilm.OpenPanel_YesNo(string.Concat(new object[]
            {
                itemDataFormat.name,
                "\nを買いますか？\n(所持数\u3000)",
                SuperGameMaster.FindItemStock(shopDataFormat.itemId),
                ")"
            }));
        }
        else
        {
            confilm.OpenPanel_YesNo(itemDataFormat.name + "\nを買いますか？");
        }
        confilm.ResetOnClick_Yes();
        confilm.SetOnClick_Yes(delegate
        {
            confilm.ClosePanel();
        });
        confilm.SetOnClick_Yes(delegate
        {
            this.GetComponent<FlickCheaker>().stopFlick(false);
        });
        confilm.SetOnClick_Yes(delegate
        {
            this.BuyItem();
        });
        confilm.ResetOnClick_No();
        confilm.SetOnClick_No(delegate
        {
            confilm.ClosePanel();
        });
        confilm.SetOnClick_No(delegate
        {
            this.GetComponent<FlickCheaker>().stopFlick(false);
        });
    }
}
}
```

1.

```
else
{
    base.GetComponent<FlickCheaker>().stopFlick(true);
    ConfilmPanel confilm = this.ConfilmUI.GetComponent<ConfilmPanel>();
    confilm.OpenPanel("みつ葉が足りません");
    confilm.ResetOnClick_Screen();
    confilm.SetOnClick_Screen(delegate
    {
        confilm.ClosePanel();
    });
}
```

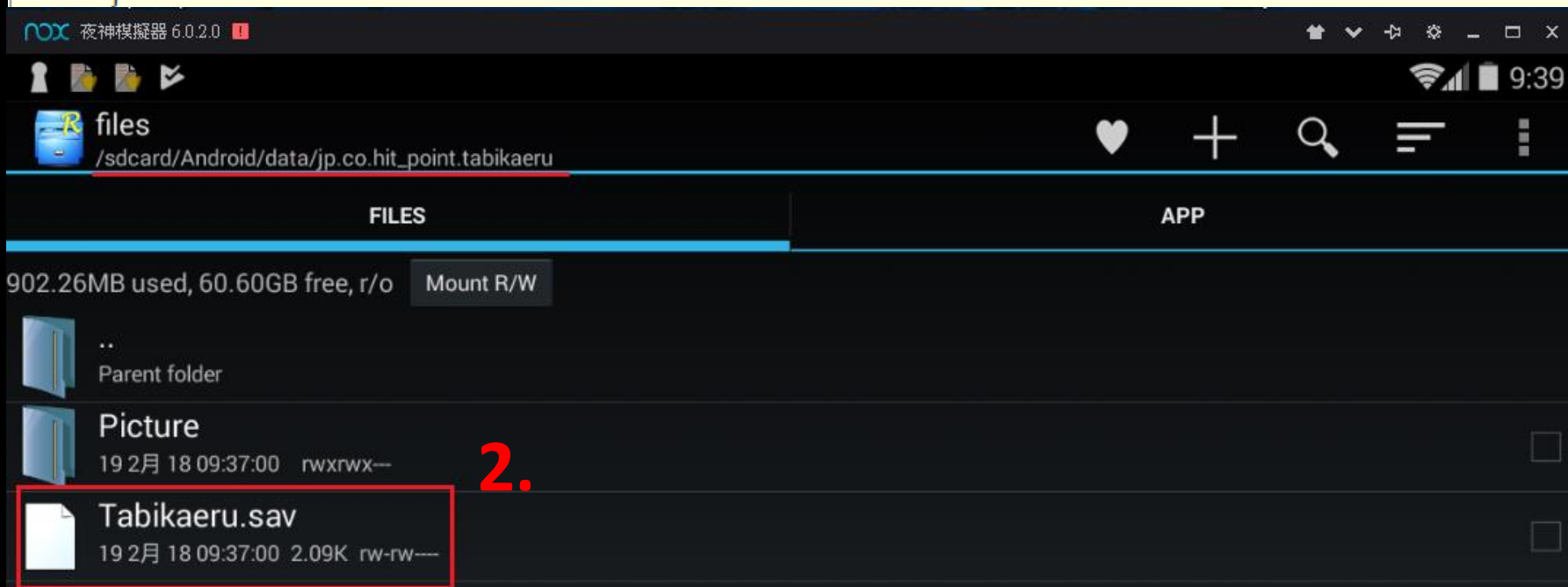
Trace code  
Logical analysis  
Guess  
Test&Prove

# 3. 逆向分析(竄改本地端遊戲紀錄檔數值)

```
Search
Tabikaeru.sav
.ctor

// Define
static Define()
{
    // Note: this type is marked as 'beforefieldinit'.
    Define.BUILD = string.Empty;
    Define.SaveName Serialize = Application.get_persistentDataPath() + "/GameData.sav";
    Define.SaveName_Binary = Application.get_persistentDataPath() + "/Tabikaeru.sav";
    Define.SaveName_Binary_PicDir = Application.get_persistentDataPath() + "/Picture";
    Define.SaveName_Binary_PicDir_SimplePath = "/Picture";
    Define.PicSaveDict = new Dictionary<SaveType, string>
    {
```

1.



2.



# HEX Editor

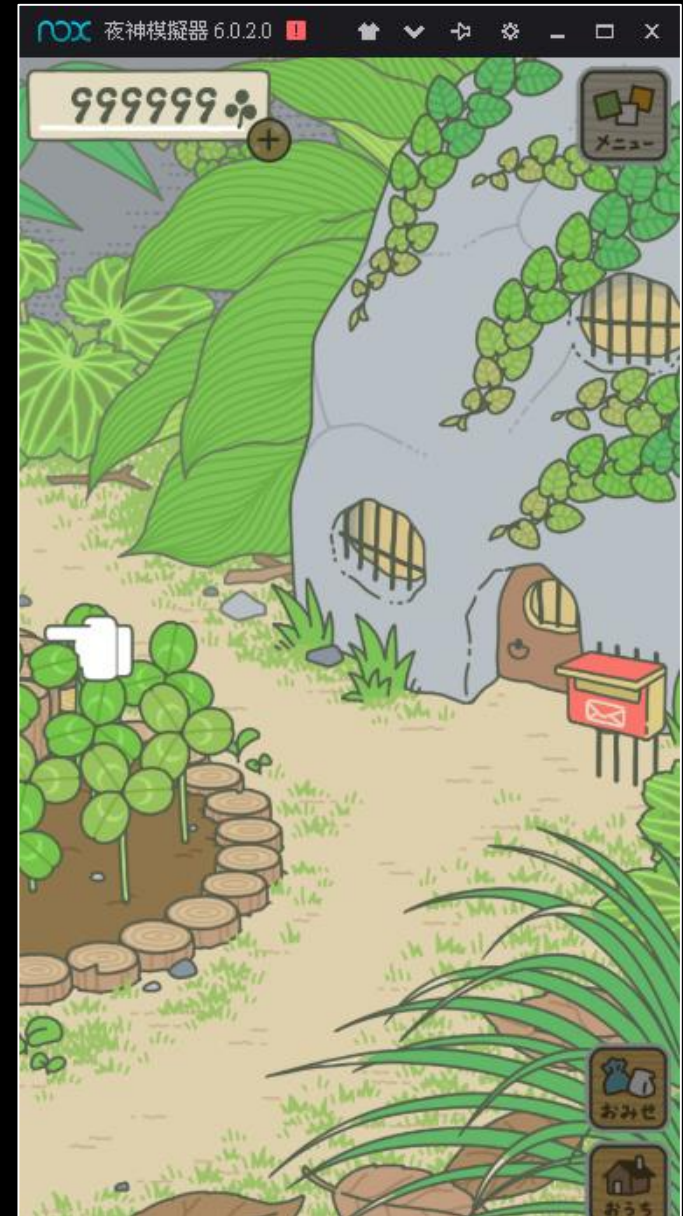
HxD - [C:\Users\ericlien\Desktop\Tabikaeru.sav]

文件(F) 編輯(E) 搜尋(S) 檢視(V) 分析(A) 附加(X) 視窗(W) 關於(A)

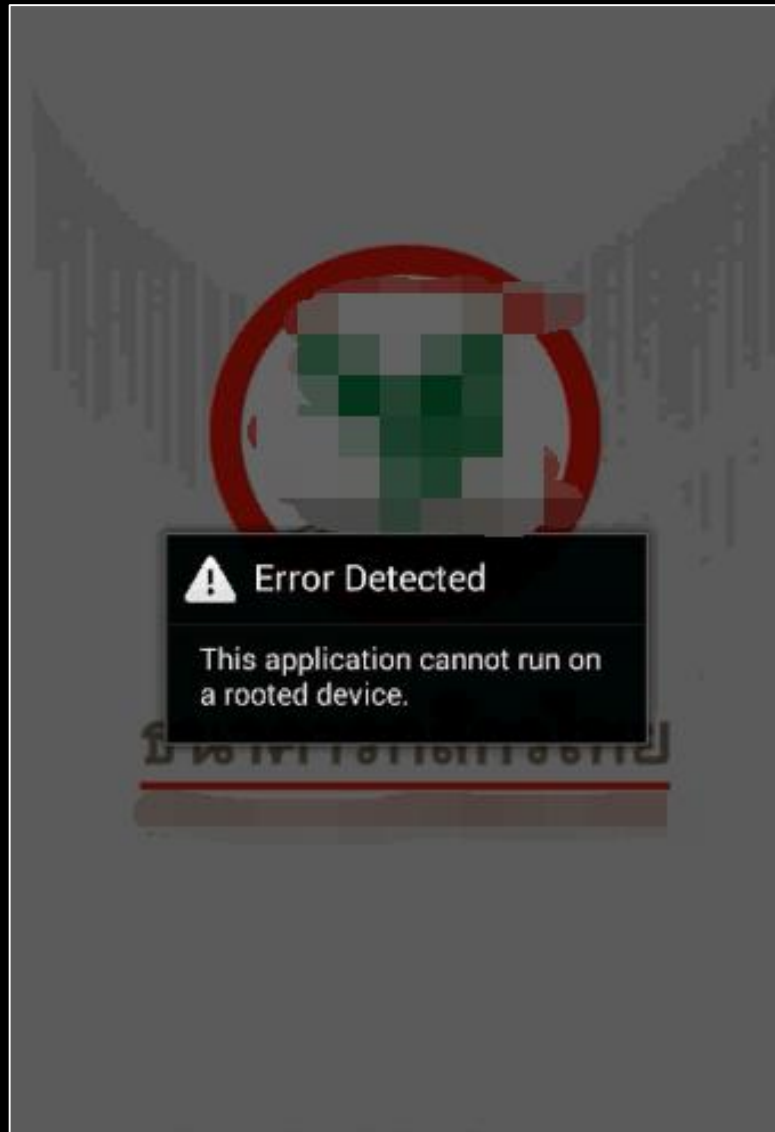
16 ANSI 十六進位

Tabikaeru.sav 三葉草數量

| Offset (h) | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F |
|------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 00000000   | 00 | 00 | 29 | 04 | 00 | 00 | 00 | 00 | 00 | 00 | 0A | 00 | 00 | 00 | 00 | 00 |
| 00000010   | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 0F | 42 | 3E | 00 | 00 |    |    |    |    |
| 00000020   | 00 | 14 | FF | FF | A5 | 92 | 00 | 00 | 00 | 4E | 00 | 00 | 00 | 01 | 00 | 00 |
| 00000030   | 00 | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 07 | 00 | 00 | 07 | B2 | 00 | 00 |
| 00000040   | 00 | 01 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000050   | 00 | 00 | 00 | 00 | 00 | 00 | FF | FF | FF | FF | 00 | 00 | 00 | 16 | 53 | FF |
| 00000060   | FF | EE | 07 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 01 | 00 |
| 00000070   | 00 | 00 | 07 | 00 | 00 | 07 | B2 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 01 | 00 |
| 00000080   | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | FF |
| 00000090   | FF | FF | FE | 00 | 00 | 00 | 1C | 66 | 00 | 00 | 14 | F2 | 00 | 00 | 00 | 00 |
| 000000A0   | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 07 | 00 | 00 | 07 | B2 |
| 000000B0   | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000000C0   | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | FF | FF | FF | FD | 00 | FF | FF | E8 |
| 000000D0   | F2 | FF | FF | FD | A5 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 |
| 000000E0   | 01 | 00 | 00 | 00 | 07 | 00 | 00 | 07 | B2 | 00 | 00 | 00 | 01 | 00 | 00 | 00 |
| 000000F0   | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000100   | 00 | FF | FF | FF | FC | 00 | FF | FF | AC | C2 | FF | FF | ED | BD | 00 | 00 |
| 00000110   | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 07 | 00 | 00 |
| 00000120   | 07 | E2 | 00 | 00 | 00 | 02 | 00 | 00 | 00 | 13 | 00 | 00 | 00 | 09 | 00 | 00 |
| 00000130   | 00 | 28 | 00 | 00 | 00 | 19 | 00 | 00 | 03 | C1 | 00 | 00 | 13 | 63 | 00 | 00 |
| 00000140   | 00 | 43 | 2A | 00 | 00 | 05 | F5 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 01 | 00 |
| 00000150   | 00 | 00 | 01 | 00 | 00 | 00 | 07 | 00 | 00 | 07 | B2 | 00 | 00 | 00 | 01 | 00 |
| 00000160   | 00 | 00 | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000170   | 00 | 00 | 00 | FF | FF | FF | FA | 00 | 00 | 00 | 3D | 7A | 00 | 00 | 20 | 11 |
| 00000180   | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 07 |
| 00000190   | 00 | 00 | 07 | B2 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 00 |
| 000001A0   | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | FF | FF | FF | F9 |
| 000001B0   | 00 | FF | FF | C6 | C7 | FF | FF | EE | 5F | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000001C0   | 01 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 07 | 00 | 00 | 07 | E2 | 00 | 00 | 00 |
| 000001D0   | 02 | 00 | 00 | 00 | 13 | 00 | 00 | 00 | 09 | 00 | 00 | 00 | 28 | 00 | 00 | 00 |
| 000001E0   | 19 | 00 | 00 | 03 | C1 | 00 | 00 | 11 | C2 | 00 | 00 | 00 | 66 | 57 | 00 | 00 |



## 4. 逆向分析(國外銀行被破解root偵測)





# Dalvik Bytecode Editor

com. [redacted] -1.apk/

- assets/
- lib/
- META-INF/
- res/
- AndroidManifest.xml  
16-09-12 16:04:48 13.46K
- classes.dex**  
16-09-12 16:04:48 7.18M
- resources.arsc  
16-09-12 16:03:38 139.77K

com. [redacted] -1.apkCopied

Add File Save ReplaceAxml

/my/com/softspace /Base/a/

- a
- b
- c
- c\$1
- c\$2
- d
- e
- e\$a
- e\$b
- e\$c
- e\$d

StringPool Search Replace SaveDexFile

MethodList

- <init>  
()V
- a  
(Lmy/com/softspace/SSMobileCore/Base/a/j\$a;Landroid/content/Context;)V
- a  
(Ljava/lang/String;Landroid/content/Context;)
- d  
(Landroid/content/Context;)v
- e  
(Landroid/content/Context;)z
- sU  
(Lmy/com/softspace/SSMobileCore/Base/a/j\$a
- sV  
()Z
- sW  
()Z
- sX  
()Z

Search AddMethod

# Dalvik Bytecode Editor(修改Java程式碼中偵測root機制的回傳值)

```
CodeEditor
const/4 v0 0
invoke-virtual {v5} Landroid/content/Context;->g
move-result-object v1
const/4 v2 1
label_6:
invoke-virtual {v1,v4,v2} Landroid/content/pm/P
label_9:
return v0
label_10:
move-exception v0
const/4 v0 0
goto :label_9

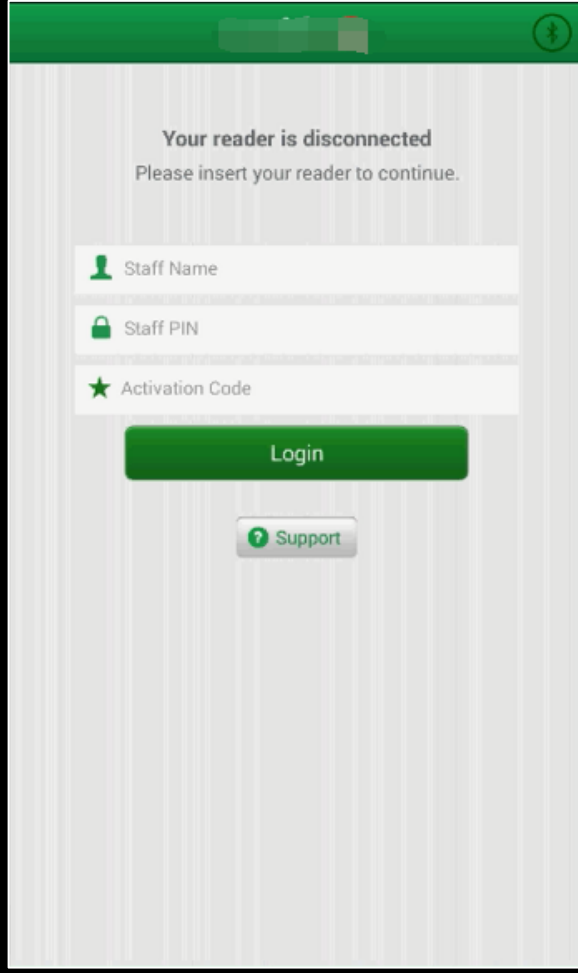
#Handler Exceptions

.catch Landroid/content/pm/PackageManager$
start : label_6
end : label_9
handler : label_10
.end catch
```

```
CodeEditor
const/4 v0 0
invoke-virtual {v5} Landroid/content/Context;->g
move-result-object v1
const/4 v2 0
label_b:
invoke-virtual {v1,v4,v2} Landroid/content/pm/P
label_9:
return v0
label_10:
move-exception v0

Prompt
Is Save?
OK Cancel
.end catch
```

# Root偵測失效



# 5. 通用外掛(幸運破解器 Lucky Patcher)



# 破解內購





# 6.通用外掛(GameGuardian或燒餅修改器)

http://gameguardian.net/download

若要搜尋一個已知的值，點擊"已知(精確)搜尋"進行搜尋。  
如果該值未知或加密的數值，點擊"未知(模糊)搜尋"進行搜尋。

輸入要搜尋的值  
輸入 -1.8e+308 到 1.8e+308 之間的數值

數值 = 9

類型: ???

此數值經過加密

在所有記憶體範圍

|   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | : | h | r | ✕ |
| 6 | 7 | 8 | 9 | 0 | ; | W | X | ✕ |
| A | B | C | D | E | F | Q | 0 | 0 |
| , | . | - | ← | → | ☐ | ↻ | ~ | × |

取消 新搜尋

8.52.0 # Jh,Ch,Ca,Cd,Cb,PS,A.0



SHOP 479 ♣

|                |                 |
|----------------|-----------------|
| えびづるのスコーン 10 ♣ | はこべのサンドイッチ 20 ♣ |
| かぼちゃのベーグル 50 ♣ | のびるのキッシュ 80 ♣   |

シャキシャキの野菜をサンドして  
特製のしょうゆタレであげました  
軽めのお食事にオススメです

にわかさき  
おうち

# 修改記憶體的資料



# 7. 案例分享-動態注入攻擊

首頁 防毒軟體免費下載 APT 攻擊 PC-CILLIN 雲端版與數位生活 重大攻擊事件 FB

## 中國「延邊幫」以行動裝置惡意程式偷走南韓網銀用戶數百萬美元

POSTED ON 2015 年 02 月 25 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

f 讚 156 f Share t Tweet 0 +1 5 Pin it

趨勢科技發表了一份有關中國網路犯罪集團「延邊幫」(Yanbian Gang) 的研究報告，該集團專門利用行動裝置惡意程式將南韓銀行帳戶使用者的存款轉出。從 2013 年起，該集團每天從受害帳戶偷取高達 1,600 美元的韓元。

這份調查報告是我們連續監控網路威脅情勢所獲得的結果。我們一直嚴密監控最新的威脅發展情勢，而中國地下市場在這方面特別活躍。尤其，我們在中國地下市場發現許多行動裝置威脅。



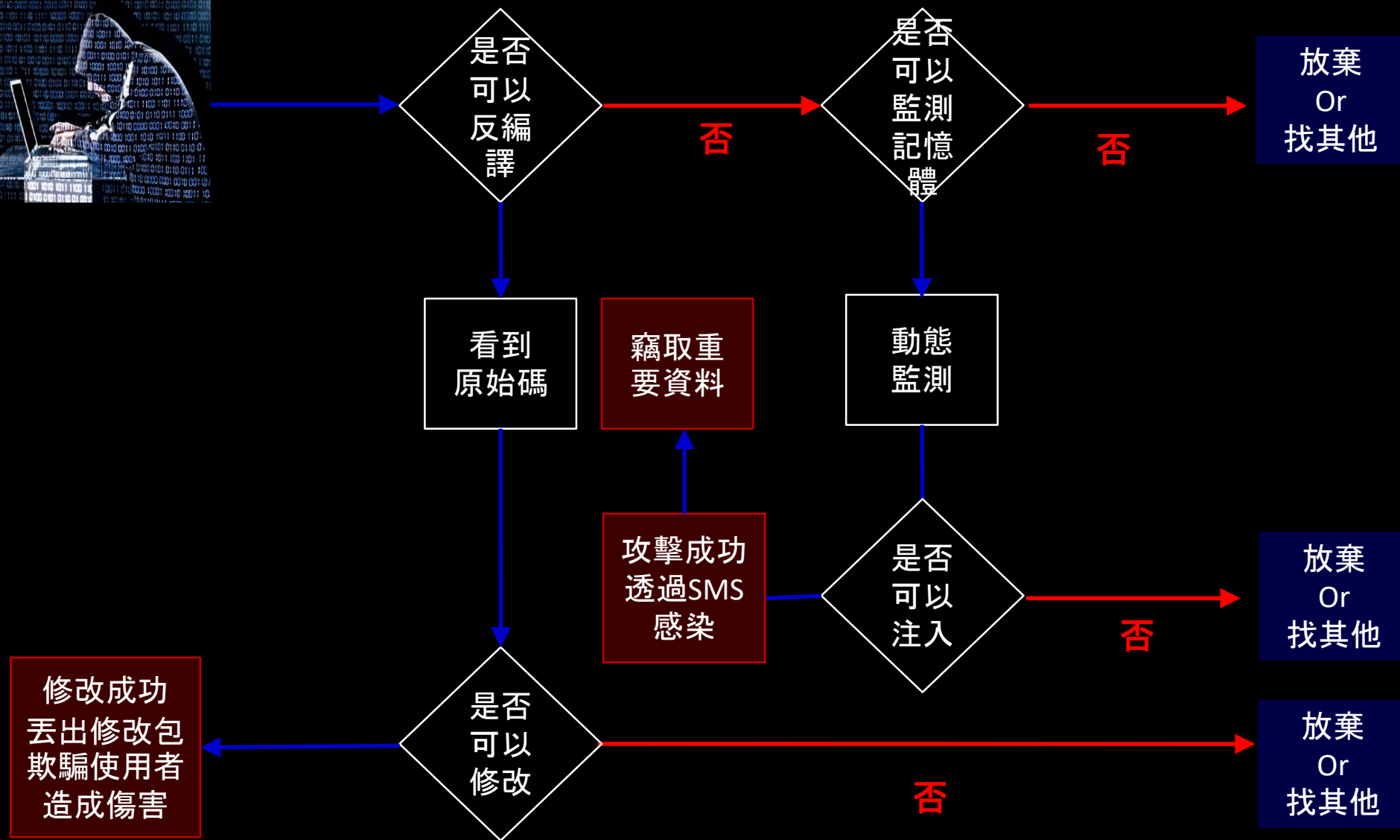
中國「延邊幫」以行動裝置惡意程式偷走南韓網銀用戶數百萬美元



# Demo

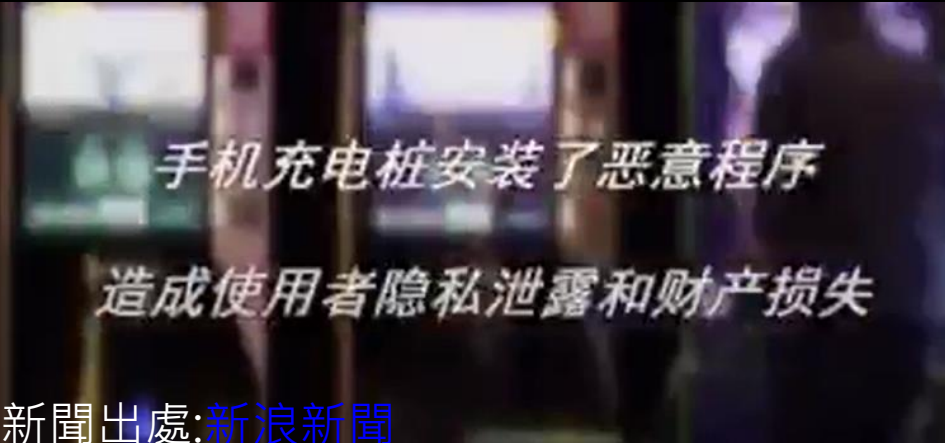
1. 旅行青蛙攻擊實作影片
2. 機敏資料被竊與轉帳被竄改

# 駭客攻擊流程



# APP安全防護

# ● 使用者如何避免惡意程序感染



手机充电桩安装了恶意程序  
造成使用者隐私泄露和财产损失

避免使用免費插座

新聞出處:[新浪新聞](http://www.sina.com.cn)

影片連結: <https://v.qq.com/x/page/s0385ej201n.html>



手機遭駭!?

2013/8/9 上午9:03 中視

被偷拍的是你麼

<http://199.101.117.21/index.php>

SMS簡訊網址不要亂點

聊天軟體網址不要亂點

紐約 20-28

收到"你被偷拍了"簡訊暗藏手機病毒

19:05:48

算賭博 撲克大賽'競技'可望登台

收到"你

# ● 避免從不正常管道下載



APK.TW Android 台灣中文網

討論區 部落格 群組 專題 應用中心 金豆儲

遊戲交流 遊戲下載 手機影視 桌布主題 水族館 手機音樂

討論區 > Android 遊戲/軟體/繁化/交流 > Android 軟體下載

發帖 回覆

[日常工具] **ay錢包】v01.01.05防Root偵測版** [複製連結]

查看: 1169 | 回覆: 5 | 好評: 0

Creppie | 收聽TA | 只看該作者 | 倒序瀏覽 | 閱讀模式

新機器人



APK.TW Android 台灣中文網

起源 石器時代

討論區 部落格 群組 專題 應用中心 金豆儲值 懸賞任務

遊戲交流 遊戲下載 手機影視 桌布主題 水族館 手機音樂 HTC Sony Samsung TWM

討論區 > Android 遊戲/軟體/繁化/交流 > Android 軟體交流 > (軟體)【玉山Wallet】v3.1.2防

發帖 回覆

[分享] (軟體) **Wallet】v3.1.2防root偵測版** [複製連結]

查看: 919 | 回覆: 0 | 好評: 0

hacksnow | 收聽TA | 只看該作者 | 只看大圖 | 樓主 電梯直達

倒序瀏覽 | 閱讀模式

學習期

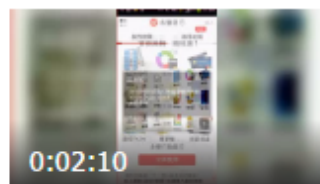
發表於 2016-11-9 00:35



應用破解任我行

全网搜

相关 最新 最热 筛选



应用**破解任我行** 台湾的**银行**安全真是没底气

时间: 2016-08-19

播放量: 211

热搜榜

# ● APP 應該要的保護項目

原始碼保護

儲存資料加密綁定

完整性校驗

APP

SO檔可保護

防記憶體修改

HTML檔可保護

# 解決辦法

# ● APP上線流程

APP  
開發期

APP  
內部  
測試期

APP  
平台  
上架

APP  
正式  
對外服務

APP安全檢驗

APP需提供給APP檢測實驗室做檢驗。  
透過專業認證機構和法規，提高APP安全性  
(認證實驗室)

Source code

需針對Source code做Code Reivew。  
透過工具審查，可降低開發時造成的開發錯誤。

傳輸安全

APP傳輸需要加密。  
透過加密傳輸降低被中間人攻擊  
(HTTPS)

APP相容性

APP需通過大量設備實際測試。  
透過實測確定APP相容性，確保使用者不會無法使用

APP安全性

APP需加裝安全工具。  
透過APP保護工具防止APP被破解或是攻擊

Server端

Server端需做VA、PT  
透過VA、PT了解Server端的問題，降低Server端被攻擊風險

主動式監測系統

了解客戶終端遭受什麼攻擊或問題  
透過主動式監控系統了解客戶端風險，立即解決降低風險

對應資安措施



# ● APP資安四大防護

## 防止逆向工程 阻止反編譯

- ▲ 加密方式  
完全隱藏原始碼
- ▲ 加密技術使用AES對稱性  
加密演算法  
金鑰長度256 bits  
金鑰使用白箱加密保護
- ▲ 分段加解密技術

## 阻擋Debugger 防記憶體被修改

- ▲ 監控與防護技術  
避免記憶體被修改
- ▲ 讓Debugger工具失效
- ▲ 防止動態程式碼注入攻擊

## 完整性校驗

- ▲ 針對APP做完整性校驗  
確保APP是正版
- ▲ 計算Hash值  
只要被修改就閃退
- ▲ 防止APK被竄改和散佈

## 敏感資料 加密及綁定

- ▲ 針對APP敏感性資料  
做完整加密
- ▲ 加密技術使用AES對稱性  
加密演算法  
金鑰長度256 bits  
金鑰使用白箱加密保護
- ▲ 客製化檔案加密

# 防止逆向工程阻止反編譯

保護前

保護後

Java Decompiler - GooglePlayPurchasing.class

```
package com.unity.purchasing.googleplay;

import android.app.Activity;

public class GooglePlayPurchasing extends BaseClassInitializer {

    public static final int ACTIVITY_REQUEST_CODE = 999;
    protected static final String TAG = "UnityIAP";
    private static GooglePlayPurchasing instance;
    private static final boolean isDebuggable;
    private TabSelector.OnTabPurchaseFinishedListener purchaseListener = new TabSelector.OnTabPurchaseFinishedListener() {

        public void onTabPurchaseFinished(TabResult paramTabResult, Purchase paramPurchase) {

            if (!GooglePlayPurchasing.this.purchaseInProgress)
                return;
            GooglePlayPurchasing.access$100("onTabPurchaseFinished: %s", Boolean.toString(paramTabResult.isSuccess()));
            GooglePlayPurchasing.access$200(paramTabResult.getMessage());
            GooglePlayPurchasing.access$300(GooglePlayPurchasing.this, false);
            if (paramTabResult.isSuccess())
            {
                GooglePlayPurchasing.access$200("Product purchased successfully!");
                GooglePlayPurchasing.this.NotifyOnPurchase(paramPurchase);
                return;
            }
            GooglePlayPurchasing.access$100("Purchase response code:%s", Integer.toString(paramTabResult.getResponse()));
            PurchaseFailureReason localPurchaseFailureReason = PurchaseFailureReason.Unknown;
            switch (paramTabResult.getResponse())
            {
                default:
                case -1009:
                case 1:
                case 2:
                case 3:
                case 7:
            }
        }
    }
}
```

Java Decompiler - BuildConfig.class

```
package com.AppGuard.AppGuard;

public final class BuildConfig {

    public static final boolean DEBUG;
}
```

```
using ...
public class BattlePlayer : MonoBehaviour, IShoutPlayer
{
    private class DisableDrawnCardInfo...
    public struct TutorialDummyCardInfo...
    private const float cStateWarningTime = 300f;
    private const float cSendSuspendWaitTime = 10f;
    private const int UNDECIDED_HAND_ID = 99;
    public const float MONSTER_APPEAR_WAIT_SEC = 0f;
    private const int HandCardCount = 4;
    public const string GraphicsObjectName = "Graphics";
    private const int cTutorialProgressMaxCount = 3;
    public int characterID;
    public int missionID;
    public int startType;
    public int roomType;
    public int friendCharacterID;
    public int chatRoomID;
    public int matchingType;
    public float latitude;
    public float longitude;
    public bool isUseNearFriendBoost;
    private BtStateBase m_State;
    public string CurState = string.Empty;
    private float m_StateTimeCounter;
    private bool m_bSendStateLog;
    private DateTime m_LastSuspendTime;
    public Dictionary<int, PokerHandID> m_OldPokerHandID;
    public Dictionary<int, int> m_KeepHandIDCount;
    public BattleMissionInfo battleMissionInfo = new BattleMissionInfo();
    public BattleBaseData baseData = new BattleBaseData();
    private int m_CurrentBgmsoundID;
    private bool isMimicBattleState;
    public string jsonDataForScoreDungeon = string.Empty;
    public float timeMonsterAppear;
    public float timeMonsterWaitStart;
    public bool requestUpdateAppearMonsterEffect;
```

ILSpy

```
D:\APK_Reverse\龍珠漢克\加蓋後\dragon_poke_1418365470_91_sec\assets\bin\Data\Managed\Assembly-CSharp
// This file does not contain a managed assembly.
```

1. 反編譯工具完全無法使用
2. 原始碼完全加密隱藏
3. 字串完全加密隱藏
4. 命名完全加密隱藏

# ● 阻擋Debugger防記憶體被修改

保護前

保護後

```
ca 命令提示字元 - adb shell
root 9254 2 0 0 c0197718c 00000000 $ kuorker/0:3
app_158 9455 213 310456 31804 ffffffff 40077888 $ com.android.packageinstaller
app_44 9471 213 310308 32476 ffffffff 40077888 $ com.google.android.partnersetup
system 9485 213 310184 31532 ffffffff 40077888 $ com.htc.HtcLinkIfDispatcher:remote3
app_125 9497 213 310100 32652 ffffffff 40077888 $ com.skysoft.kkbox.android.widget.kkbox_player

app_17 9514 213 310128 32032 ffffffff 40077888 $ com.htc.opensense
app_156 9527 213 329932 49236 ffffffff 40077888 $ com.google.android.apps.plus
system 9544 213 326352 35776 ffffffff 40077888 $ com.android.settings
app_205 9559 213 311524 34916 ffffffff 40077888 $ biz.hokhorst.xprivacy
app_26 9571 213 315524 37116 ffffffff 40077888 $ android.process.media
app_204 9593 213 310732 33776 ffffffff 40077888 $ de.robu.android.xposed.installer
app_45 9617 213 313180 33196 ffffffff 40077888 $ com.google.android.googlequicksearchbox
shell 9654 643 872 436 c0109558 40082d4 $ /system/bin/sh
app_203 9661 213 396104 98232 ffffffff 40077888 $ com.lenovgame.tw.dtapk
app_203 9693 213 322192 41456 ffffffff 40077888 $ com.lenovgame.tw.dtapk:pushservice
root 9790 9654 876 440 c0109558 40082d4 $ sh
root 9805 9790 872 436 c0109558 40082d4 $ sh
root 9807 2 0 0 c0197718c 00000000 $ kuorker/0:0
root 9811 2 0 0 c01c060c 00000000 $ migration/1
root 9812 2 0 0 c0197718c 00000000 $ kuorker/1:0
root 9813 2 0 0 c0185494 00000000 $ kssoftirqd/1
root 9814 2 0 0 c0197718c 00000000 $ kuorker/1:1
root 9815 9805 1060 376 00000000 4010f8b8 R ps
root@android:/ # data/local/tmp/gdbserver localhost:1111 --attach 9661
data/local/tmp/gdbserver localhost:1111 --attach 9661
Attached; pid = 9661
Listening on port 1111
Remote debugging from host 127.0.0.1
```

```
ca 命令提示字元 - adb shell
app_196 7029 213 335344 37064 ffffffff 40077888 $ eu.chainfire.supersu
app_154 7042 213 344676 38912 ffffffff 40077888 $ com.android.vending
app_21 7063 213 479492 43632 ffffffff 40077888 $ com.google.android.gms
app_205 7093 213 311548 33888 ffffffff 40077888 $ biz.hokhorst.xprivacy
app_203 7135 213 404788 106776 ffffffff 40077888 $ com.lenovgame.tw.dtapk
app_203 7162 7135 325872 41976 ffffffff 400776e4 $ com.lenovgame.tw.dtapk
app_204 7167 213 318732 32368 ffffffff 40077888 $ de.robu.android.xposed.installer
app_171 7193 213 318288 34700 ffffffff 40077888 $ com.google.android.talk
app_45 7216 213 313180 31684 ffffffff 40077888 $ com.google.android.googlequicksearchbox
app_17 7240 213 317612 34396 ffffffff 40077888 $ com.htc.calendar
app_203 7289 213 333000 54208 ffffffff 40077888 $ com.lenovgame.tw.dtapk:pushservice
app_203 7362 7289 325900 54208 ffffffff 400776e4 $ com.lenovgame.tw.dtapk:pushservice
shell 7482 643 872 428 c0109558 400c52d4 $ /system/bin/sh
root 7527 2 0 0 c0197718c 00000000 $ kuorker/0:1
root 7540 7482 876 436 c0109558 4002b2d4 $ sh
root 7555 7540 1060 372 00000000 400838b8 R ps
root@android:/ # ^C
D:\APK_Reverse>adb forward tcp:1111 tcp:1111

D:\APK_Reverse>adb shell
shell@android:/ # data/local/tmp/gdbserver localhost:1111 --attach 7135
data/local/tmp/gdbserver localhost:1111 --attach 7135
warning: process 7135 is already traced by process 7162
Cannot attach to lwp 7135: Operation not permitted (1)
Exiting
1!shell@android:/ # data/local/tmp/gdbserver localhost:1111 --attach 7162
data/local/tmp/gdbserver localhost:1111 --attach 7162
Cannot attach to lwp 7162: Operation not permitted (1)
Exiting
1!shell@android:/ #
```

The screenshot shows the IDA Pro interface with the assembly view of a function. The assembly code includes instructions like MOV, ADD, and BX, with comments such as 'Attributes: thunk' and 'End of function \_40091179'. The hex view at the bottom shows the corresponding machine code bytes.

- 1. 可被使用Debugger工具
- 2. 駭客可以任意動態追蹤

- 1. 無法使用Debugger工具
- 2. 讓駭客無法任意動態追蹤
- 3. 讓記憶體相關的攻擊確定失效

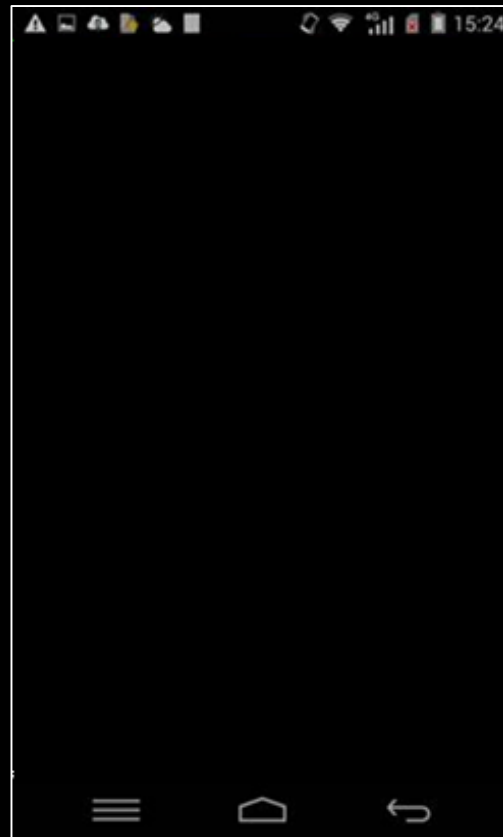
# ●完整性校驗

保護前



- 1.市面上會出現修改包
- 2.造成商譽損失

保護後



- 1.只要被竄改就Crash
- 2.避免市面上出現修改包

# ●敏感資料加密及綁定

保護前

保護後

```
com.kway.gphone.activity.MainActivity.xml
<string name="LOGIN_ACC">9804650</string>
<string name="S_HIS_CODE_0">2884</string>
<string name="ECAFATER_C120834274">20160508235959</string>
<string name="I_HIS_NAME_0">加權指數</string>
<string name="CAPWD_C120834274"></string>
<string name="LoginPwd_88409804650">polaris2</string>
name="KEYSET_C120834274">o1uoiLiGw7r+HwvF+pp2k+rFmkEE25akXwfbm+JFp3ys6RckaIE2NyJjV
Z80ET+iakbkbp+D3072RY0mdq+oTUyCis5ZFy89YrWYBVNxD1Su6G31PdV3qdFs+U+u/9RiUtp3k1M1TR
Og2Xq9e14hr156+itw5/dbHST1sAjGaw8ohm/
mkN4+HizY9yk31B2U61v0Lxt9gdyq7tqh1k8h0ToQly6wtPmd1+r1/G1eWd/Jh1YxnTr/
jk31MtU7BMMGYD2ZwLu49chaF10X7sJgnCHNRU+Z9czYgeVocE2UN8fhZVa4IaZa27SxiGd1YjYrIIA2f
+hQxPpBgHfU9R+DIT8BgsOmF8VG38HQDUJ8chffsF0m/LbPcZfxC+Cl9clBiU9cul2TeVu2LGRqUP/
w88p9NuGR/0MB1M8oeouSh0F3GLBeAOablkh7dkv/
o07G1FUQBU89p0Iw33abj03s9p121KOedev6yQ11r5rRrA2h0xN4A1A1Ukazd+9tYzRk0Bev+59Q1ApnJm1
0EmpwRLmw06p20ke01a5dFv0YzEQf3p9FxcLLYD1X1ttl3CWsv9VJvbKw1aohmF+45fcZ551/
Sc1Q06Jy34ymasavpvt9p6ehdyD7JC+ZDTC1D3r/dnt8Y2pmhPAMrvxywt85MIAkysDyxx1Kh/
W6E9S7kByHg0p1MEHrgZ13A+pgs710a8u25mLgRjF6HuvZsAgzqTQJue+Itr1RCvyJ8waKur/2hVlNCKqXxyY4J
BPn/uwBDjrB5JYEs+SCGQLJsXskTf/
hHUNK18jHnJ0YRlRvYD0AE6LLjX991MzpzW6GVbvfjzAEy7m1Y1TDW6Gxp1oXewkMwF+1vLLsh0wtPewRA9
kmpn7U07cncRZV0ASmJ4YbZ2fnNHUU49cWh6ypq3HakXU0HpsH7t8fsvf3+8Vt4CuLTDJ6jLIMFCu87yWzRPd
Ds+HmoJG5rx+LJ7HJRZ1X0+1AYWzQ5Aq2R81DS1syXkMJeV1/
UJ1FRhb20AScb451rk55CFZ/2qkFtSapPLsJm15kZEk2jR+0L3zaibIRwmUw8E9A91KKSf3NzTof40111t
```

```
com.kway.gphone.activity.MainActivity.xml
00900101b570d188j0R000000( 00a00-
0100L00Z V#00qx0000u R5nNW!om000iU0P_0(00Vn0000c980700J0yV' 0000 f0! '08c0x0K0d0 00 0040
e 0. 000000/
0000000 U000 00a00 1100=109000 070qQ L#0 Ep; 00E0tkeF3Q[00040IiHa000 ++*fD0000; 0+0 00) 0A
000000000000? 0f80L'0h0%1]0 000T0 . $ !0. 000000; | kD
[50000710+0q 00 -Q0000 0a 0R0-0000" 0000000(0_0 0DE y w0y0*Cvm04000000?0n=00unX0 0h|g9' U
X!00 0S 1/0S
90r 0 0000T0 000 u200000Rj0) 0JnJ28e00rU+0kn0000 00x 0010p3 500000 000 00y000qzI@*60QY0000
0Y 0, 00X0gU0000 0T0u000000t P0k0g=0, 0000000i0e0K000 08 Uut00E2 00 m0 1. 000000
40-0-0000? 0z0000002000-03; 00Z0<0%0000ED 0 000000Y000000010 0- 70i0_2755yP-0000T5
0000Q0|K| 00E0- = BX0V 0S00I0"0000 0 0000u, A00 500D0V0x000 0D 0k9000m3' JA0x000 00m00
r 0 00000000000000]000 00h0'0 zu0Y00[0i.140% ] 0Y9D 0000V05000 060010000070|0K0@0?| 000
I0EJ0m00Z00k00 C'Km0T0: 00 1f0000" 00
P00000000Y000: 680. r0000 *00Y000Tk00 000 000000Y0 0000 (0
0 0000 0A-0 000000 X ;WT)L: 000 75 ]10, 0 b0000X3' f05)160000 C 0000' 0: k00
1030= [0Rf0G0|k00L: 00000 00."1h0000 8 0i0V000000vY0Q0002F0-0#0- I0 02d0
S0000m 007N00QR zHX0 00n -0000 k0D7
}|000+08Z 0'000 X+0 y00 my000A,Xj0X00i f0C0 {3 0000 [J0k @0Q^0i0_0
c0000 u0E00 (&x00000000000010f, 0(0000a00D04 0000SZNJ0000L0 00( | 09Y) 00=00000R0E 0 000 0 00
0 0, 0 000000 0000000 000000 000000 = \ 00X0 N305000Y0Q0T000000000/0
01 j000Y+0n"GVRF0f: 0000001-0P00000000002000000000003000f0000000000000000 0000+000 0 s 0 0? 0
0r C0Z000000 00/00X0000Z0 0 200 D00 000Z000 0087000c 0 000500 0: Hy004 K0i=/
0000 00011000' 000 "080R SCX8 5000DZ0 0 00000 10000(10K0000 00: v0000R0000F0S0
```

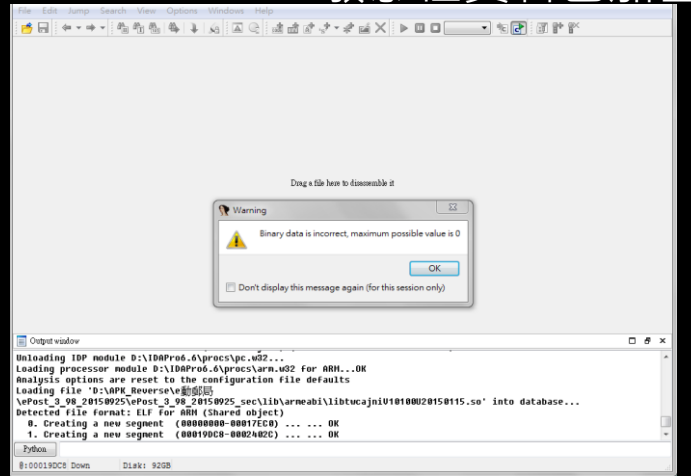
敏感性資料未加密

敏感性資料已加密

```
Function name
sha2_hmac_starts
sha2_hmac_update
sha2_hmac_finish
sha2_hmac_reset
sha2_hmac
sha2_self_test
authentication
encryptTrippDES
decryptTrippDES
decryptTrippDES
decryptTrippDES
randomTrippDESkey
setDeviceKey
getDeviceKey
genM2Key
verifyToken
setVerified
resetHistory
getAuthentic
setAuthentic
sub_14454
byteArrayToInt
intToByteArray
hexEncode
hexDecode
base64Encode
base64Decode

0001417A getDeviceKey:3
int __fastcall getDeviceKey(void *a1)
2 {
3 int result; // r002
4 int u2; // r008
5 int u3; // [sp+0h] [bp-20h]j00
6 int u4; // [sp+10h] [bp-10h]j01
7
8 v4 = --_stack_chk_guard;
9 if ( deviceKey )
10 {
11 j_j__memcpy(a1, deviceKey, 0x18u);
12 result = 0;
13 }
14 else
15 {
16 u2 = getHacAddress(k09);
17 if ( !u2 )
18 SetDeviceKey(k09, 20);
19 result = u2;
20 }
21 if ( u4 != _stack_chk_guard )
22 j_j__stack_chk_fail(result);
23 return result;
24 }
```

SO檔未加密



SO檔加密，駭客工具失效



# ● 敏感資料加密及綁定

保護前

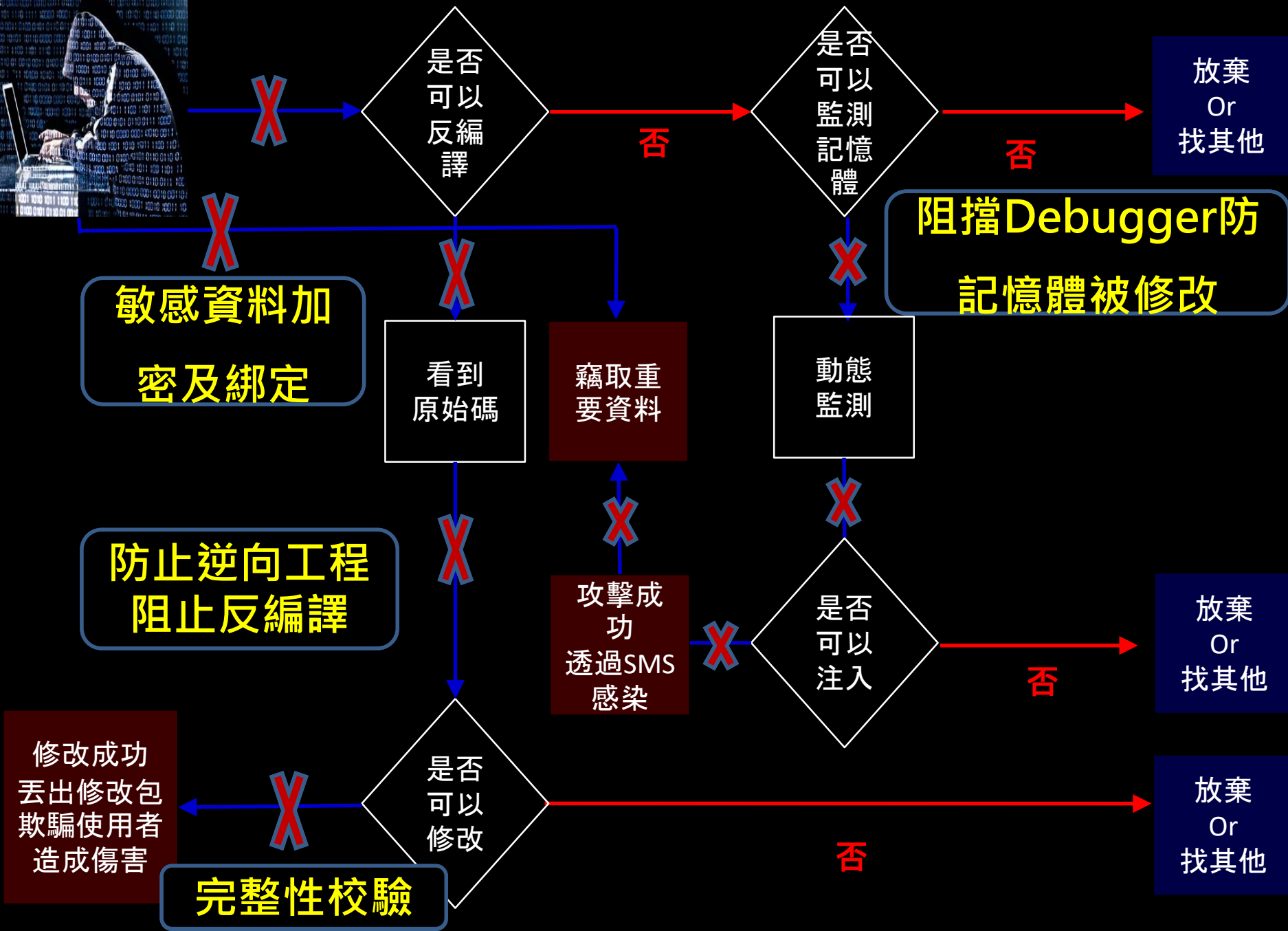
保護後

```
1 <?xml version="1.0" encoding="utf-8" android:label="@string/title_trade_confirm" android:windowBackground="@color/white" android:theme="@style/Theme.AppCompat.NoActionBar" >
2 <include layout="@layout/content_trade_confirm" />
3 </include>
4 <android.support.design.widget.TextInputLayout
5     android:id="@+id/text_input_layout"
6     android:layout_width="match_parent"
7     android:layout_height="wrap_content"
8     android:padding="16dp"
9     android:background="@color/white"
10    >
11     <android.support.design.widget.TextInputEditText
12         android:id="@+id/text_input_edit_text"
13         android:layout_width="match_parent"
14         android:layout_height="wrap_content"
15         android:padding="16dp"
16         android:background="@color/white"
17         android:inputType="text"
18         android:maxLength="100"
19         android:visibility="visible"
20         android:layout_marginBottom="16dp"
21         android:android:onClick="http://schemas.android.com/apk/res/android"
22         >
23     </android.support.design.widget.TextInputEditText>
24 </android.support.design.widget.TextInputLayout>
25 </android.support.design.widget.TextInputLayout>
26 </android.support.design.widget.TextInputLayout>
27 </android.support.design.widget.TextInputLayout>
28 </android.support.design.widget.TextInputLayout>
29 </android.support.design.widget.TextInputLayout>
30 </android.support.design.widget.TextInputLayout>
31 </android.support.design.widget.TextInputLayout>
32 </android.support.design.widget.TextInputLayout>
33 </android.support.design.widget.TextInputLayout>
```

APK內含資源檔未加密

```
1 <?xml version="1.0" encoding="utf-8" android:label="@string/title_trade_confirm" android:windowBackground="@color/white" android:theme="@style/Theme.AppCompat.NoActionBar" >
2 <include layout="@layout/content_trade_confirm" />
3 </include>
4 <android.support.design.widget.TextInputLayout
5     android:id="@+id/text_input_layout"
6     android:layout_width="match_parent"
7     android:layout_height="wrap_content"
8     android:padding="16dp"
9     android:background="@color/white"
10    >
11     <android.support.design.widget.TextInputEditText
12         android:id="@+id/text_input_edit_text"
13         android:layout_width="match_parent"
14         android:layout_height="wrap_content"
15         android:padding="16dp"
16         android:background="@color/white"
17         android:inputType="text"
18         android:maxLength="100"
19         android:visibility="visible"
20         android:layout_marginBottom="16dp"
21         android:android:onClick="http://schemas.android.com/apk/res/android"
22         >
23     </android.support.design.widget.TextInputEditText>
24 </android.support.design.widget.TextInputLayout>
25 </android.support.design.widget.TextInputLayout>
26 </android.support.design.widget.TextInputLayout>
27 </android.support.design.widget.TextInputLayout>
28 </android.support.design.widget.TextInputLayout>
29 </android.support.design.widget.TextInputLayout>
30 </android.support.design.widget.TextInputLayout>
31 </android.support.design.widget.TextInputLayout>
32 </android.support.design.widget.TextInputLayout>
33 </android.support.design.widget.TextInputLayout>
```

APK內含資源檔已加密



是否可以反編譯

是否可以監測記憶體

放棄  
Or  
找其他

阻擋Debugger防  
記憶體被修改

敏感資料加  
密及綁定

看到  
原始碼

竊取重  
要資料

動態  
監測

防止逆向工程  
阻止反編譯

攻擊成  
功  
透過SMS  
感染

是否  
可以  
注入

放棄  
Or  
找其他

修改成功  
丟出修改包  
欺騙使用者  
造成傷害

是否  
可以  
修改

放棄  
Or  
找其他

完整性校驗

- 保護APP的安全
- 避免APP被竄改或竊取
- 保護公司及個人權益



# 結語

舉安全之盾，防事故之患。



